

PRODUCT MANUAL
ID5 TD CM
MANUAL VERSION 1.2/1221
ORIGINAL VERSION

This manual is valid from software version 03.01.

COMMEND INTERNATIONAL GMBH
Saalachstraße 51
A-5020 Salzburg – Austria
www.commend.com
PRODUCT MANUAL

Edition: 2021/12/23
Manual version: 1.2/1221

The manufacturer guarantees the functionality of its products as described in the data sheets and/or other technical documents. For error-free operation of the Intercom system, faultless transmission paths are mandatory. The functionality of transmission paths, in particular of IP networks, exclusively is the responsibility of the operating company of the transmission path and therefore the manufacturer cannot be responsible in any manner, for errors and problems, which result from problems or malfunctioning of the transmission path.

It is not allowed to copy any text of this document without permission of COMMEND INTERNATIONAL GMBH.

The technical data contained herein has been provided solely for informational purposes and is not legally binding. IoIP®, OpenDuplex® and Commend® are trademarks registered by COMMEND INTERNATIONAL GMBH. All other brands or product names are trademarks or registered trademarks of the respective owner and have not been specifically earmarked.

TABLE OF CONTENTS

1.	GENERAL INFORMATION.....	9
1.1.	Using this documentation.....	9
1.2.	Safekeeping.....	9
2.	SECURITY.....	10
2.1.	IT Security.....	10
2.1.1.	Password management.....	10
2.1.2.	Ports.....	11
2.1.3.	Authentication.....	12
2.1.4.	Certificates.....	12
3.	GENERAL DESCRIPTION.....	14
3.1.	Symphony MX Features.....	14
3.2.	LED behaviour.....	16
3.3.	USB devices.....	16
4.	DEVICE DISPLAY DESCRIPTION.....	17
4.1.	Prevent image persistence.....	17
4.2.	Introduction.....	17
4.2.1.	Views.....	17
4.2.2.	Boot views.....	18
4.3.	Layouts.....	19
4.3.1.	Indoor.....	20
4.3.2.	Door.....	25
4.3.3.	Frame.....	27
4.3.4.	Customised visualization.....	32
4.3.5.	Contact management.....	33
4.4.	Call views.....	34
4.4.1.	Outgoing Call.....	35
4.4.2.	Incoming Call.....	38
4.4.3.	In Call.....	40
4.4.4.	Call ended.....	45
4.5.	Search.....	46
4.6.	PIN code.....	48
4.6.1.	User actions.....	50
4.7.	Confirmation dialogue.....	51
4.8.	Settings.....	52
4.8.1.	Audio.....	53
4.8.2.	Display.....	54
4.8.3.	Language.....	56
4.8.4.	System information.....	57
5.	WEB INTERFACE DESCRIPTION.....	62
5.1.	Introduction.....	62
5.1.1.	Availability.....	62
5.1.2.	Privacy.....	62
5.1.3.	Menu bar.....	63
5.1.4.	Notification boxes.....	64

5.1.5.	Activities and action sequences.....	65
5.2.	Landing page.....	66
5.2.1.	Device Information.....	66
5.2.2.	Symphony Cloud Platform Information.....	67
5.3.	Overview.....	69
5.3.1.	Device Information.....	70
5.3.2.	Symphony Cloud Platform Information.....	71
5.3.3.	Network State.....	72
5.3.4.	ONVIF.....	72
5.3.5.	SIP Servers.....	73
5.4.	General.....	74
5.4.1.	General.....	75
5.4.2.	DNSv4 Server.....	75
5.4.3.	DNSv6 Server.....	76
5.4.4.	802.1X Authentication.....	76
5.4.5.	IEEE 802.1Q (VLAN).....	78
5.4.6.	Quality of Service.....	78
5.5.	IPv4.....	79
5.5.1.	IPv4.....	79
5.5.2.	NAT.....	81
5.6.	IPv6.....	82
5.7.	Advanced Services.....	84
5.7.1.	Symphony Cloud Platform Settings.....	84
5.7.2.	SSH Server.....	85
5.7.3.	Set-UP Tool Settings.....	85
5.7.4.	API Security.....	85
5.8.	TLS.....	86
5.8.1.	Server Certificates.....	86
5.8.2.	Client CA certificates.....	87
5.9.	ONVIF.....	88
5.9.1.	ONVIF Configuration.....	89
5.9.2.	ONVIF Users.....	90
5.9.3.	ONVIF Information.....	90
5.10.	SIP.....	91
5.10.1.	SIP Settings.....	92
5.10.2.	SIP Server.....	94
5.11.	Call Settings.....	96
5.11.1.	In Call.....	97
5.11.2.	Incoming Call.....	97
5.11.3.	Outgoing Call.....	98
5.12.	Advanced Options.....	99
5.12.1.	Registrarless.....	99
5.12.2.	SIP Servers.....	100
5.13.	Certificates.....	101
5.13.1.	SIP Certificates.....	101
5.13.2.	SIP CA Certificates.....	102
5.14.	Device.....	103
5.14.1.	Create a new layout.....	104
5.14.2.	Edit Layout Name.....	105

5.14.3.	Device states.....	105
5.15.	Audio.....	117
5.15.1.	Volume.....	118
5.15.2.	Audio Devices.....	120
5.15.3.	Audio Optimisation.....	123
5.15.4.	Advanced Audio Settings.....	124
5.15.5.	Loudspeaker/Microphone Surveillance.....	126
5.15.6.	Audio Monitoring.....	127
5.15.7.	Sound Pressure Level.....	128
5.16.	Video.....	129
5.17.	Motion Detection.....	130
5.18.	Advertising.....	131
5.18.1.	Advertising Mode.....	131
5.18.2.	Advertisements.....	133
5.19.	IOs.....	134
5.20.	Activity.....	135
5.20.1.	Activities.....	135
5.20.2.	Add activity.....	136
5.20.3.	Editing an activity.....	137
5.20.4.	Cronjob syntax.....	138
5.20.5.	Pre-configured activities.....	139
5.21.	Action Sequences.....	141
5.21.1.	Add Action Sequence.....	141
5.21.2.	Edit Action Sequence.....	142
5.21.3.	Pre-configured Action Sequences.....	144
5.22.	Contacts.....	147
5.22.1.	Edit Contact.....	149
5.22.2.	Add Call Buttons.....	150
5.23.	Contact Management.....	150
5.23.1.	Sticky Buttons and Directory Buttons.....	151
5.23.2.	Directories.....	152
5.23.3.	Contact.....	153
5.23.4.	Button Configuration.....	153
5.23.5.	Contact configuration.....	154
5.24.	Audio Files.....	156
5.24.1.	Edit Audio File.....	157
5.25.	Snapshots.....	157
5.26.	Images.....	158
5.26.1.	Edit Images.....	159
5.27.	System.....	160
5.27.1.	System.....	161
5.27.2.	Language and Region.....	162
5.27.3.	Time and Date.....	163
5.27.4.	Email Configuration.....	163
5.27.5.	Keypad Settings.....	164
5.28.	Backup.....	164
5.28.1.	Backup.....	165
5.28.2.	Backup Storage.....	165
5.29.	User Management.....	166
5.29.1.	Users.....	166

5.29.2.	Profile.....	167
5.29.3.	Roles.....	173
5.29.4.	Edit Role.....	174
5.30.	Codecs.....	175
5.30.1.	Audio Codecs.....	176
5.30.2.	Video Codecs.....	177
5.31.	Logging.....	177
5.31.1.	SystemLog.....	178
5.31.2.	Trace.....	178
5.31.3.	EventLog.....	179
5.31.4.	General.....	179
5.32.	SNMP.....	180
5.33.	Remote Maintenance.....	181
5.34.	Available actions.....	182
5.34.1.	Change Audio Device.....	182
5.34.2.	Play Audio File.....	182
5.34.3.	Output.....	183
5.34.4.	Change Display Brightness.....	183
5.34.5.	Change Display Mode.....	184
5.34.6.	Send DTMF Tone.....	184
5.34.7.	Send Email.....	185
5.34.8.	Cancel Call.....	185
5.34.9.	On Hold.....	185
5.34.10.	HTTP Client Action.....	186
5.34.11.	Disconnect IP Secure Connector.....	187
5.34.12.	Chain Call.....	187
5.34.13.	Change Volume.....	188
5.34.14.	Change Layout.....	188
5.34.15.	Set LED.....	188
5.34.16.	Mute Microphone.....	189
5.34.17.	Parallel Call.....	189
5.34.18.	Switch Pictogram.....	190
5.34.19.	Call.....	191
5.34.20.	Answer Call.....	191
5.34.21.	Change Audio Device.....	192
5.34.22.	Snapshot.....	192
5.34.23.	Play Info Message at the Remote Station.....	192
5.34.24.	Delayed Action.....	193
5.34.25.	Switch Video.....	193
5.34.26.	Interrupt Advertisement.....	194
5.34.27.	Change Advertising Mode.....	194
5.34.28.	Show View.....	194
5.35.	Upload Window.....	195
5.36.	Video Stream.....	196
5.37.	Still picture.....	198
6.	INSTALLATION.....	199
6.1.	Import server certificate.....	199
6.2.	Configure ONVIF motion alarm event.....	199

6.3.	Add activity and action sequence.....	201
6.4.	Configure loudspeaker-microphone surveillance.....	203
6.5.	Interrupt advertisement through motion detection.....	209
6.6.	Import backup.....	211
7.	STARTUP.....	213
7.1.	Launching the Web Interface.....	213
7.1.1.	Launching the Web Interface via zeroconf.....	213
7.1.2.	Launching the Web Interface via IPv6 address.....	213
7.1.3.	Launching the Web Interface via IPv4 address.....	214
7.2.	Logging into the Web Interface.....	214
8.	MAINTENANCE.....	216
8.1.	Updating via USB stick.....	216
9.	APPENDIX.....	218
9.1.	JSON file for contact management.....	218
9.1.1.	contacts.....	218
9.1.2.	nodes.....	219
9.1.3.	addresses.....	219
9.1.4.	medias.....	219
9.1.5.	activityEvents.....	220
9.1.6.	actions.....	220
9.1.7.	actionSets.....	220
9.1.8.	activityCards.....	220
9.1.9.	buttons.....	221
9.1.10.	buttonGroups.....	221
9.1.11.	components.....	221
9.1.12.	mediaData.....	222
9.1.13.	Example of a JSON file.....	222
9.2.	ID5 DKGM or ID5 DKHSGM.....	223
9.2.1.	Configuring audio devices.....	225
9.2.2.	Enabling display of the “Push-to-Talk” pictogram.....	225
9.2.3.	Configuring “In Call” for Push-to-Talk calls.....	226
9.2.4.	Configuring DTMF tones for Push-to-Talk calls in VirtuoSIS.....	228
9.3.	EB3E2A-AUD.....	230
9.4.	Remote controlling a device via HTTP requests.....	231
9.4.1.	Parameters.....	232
9.4.2.	Configuring device remote control.....	232
9.5.	SNMP for Symphony MX.....	234
9.5.1.	SNMP for Symphony MX.pdf.....	235
9.6.	Licencing notes.....	239
9.6.1.	XFree86-1.1.....	239
9.6.2.	Original SSLeay.....	239
9.6.3.	OpenSSL.....	239
9.6.4.	LGPL-3.0+.....	239
9.6.5.	LGPL-3.0.....	240
9.6.6.	LGPL-2.1+-with-GCC-exception.....	240
9.6.7.	LGPL-2.1+.....	242
9.6.8.	LGPL-2.1.....	242
9.6.9.	LGPL-2.0+.....	242

- 9.6.10. LGPL-2.0.....244
- 9.6.11. LGPL.....244
- 9.6.12. IJG.....244
- 9.6.13. FTL.....245
- 9.6.14. BSD-4-Clause.....245
- 9.6.15. Apache-2.0.....246
- 9.6.16. APACHE-1.1.....251
- 10. LIST OF FIGURES.....252**
- 11. LIST OF TABLES.....257**

1. GENERAL INFORMATION

1.1. USING THIS DOCUMENTATION

The present version of this documentation is the original edition.

This documentation is part of the product. This documentation is intended for all persons who work with the product.

Complementing the product training courses, this documentation is designed to provide additional essential knowledge about the safe, adequate and economic use of the product provided by Commend. It is intended to help operators to avoid dangers, reduce repair costs and downtimes, and maximise the reliability and lifespan of the product.

1.2. SAFEKEEPING

The complete documentation must be stored near the point of use of the product. It must be constantly available and accessible.

2. SECURITY

2.1. IT SECURITY

As a provider of security-specific solutions, Commend has a tradition of passionate commitment to security, both physical and digital. We are acutely aware of what is at stake, as users depend – and in extreme cases even stake their lives – on the reliability of our systems. Where cyber security is concerned, we make every effort to ensure cyber security best practices in the design, production and rigorous testing of every component to rule out exploitable vulnerabilities as much as possible.

The following sections describe configuration steps required to maintain cyber security.

2.1.1. PASSWORD MANAGEMENT

Using a secure password is essential to ensure basic-level protection and to prevent unauthorised access. For this reason, ensure that you change the default password for each Commend system device before using it for the first time. The password must comply with your company's IT security policy and related requirements. A good rule of thumb for a secure password is "length before complexity".

Requirements:

- The password must be at least 12 characters long (the maximum is 64 characters).
- The password may include any of the following characters: [SPACE] _ a b c d e f g h i j k l m n o p q r s t u v w x y z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0 1 2 3 4 5 6 7 8 9 ^ \$? . * + - & [{ () }] | \ / ! # % : ; , = @ ~
- The password must contain at least one digit, one special character (where applicable), one upper-case letter and one lower-case letter.
- The password must not contain the user name or dictionary words.
- The password must be unique to prevent access to other devices.

A password generator can help you to generate randomised secure passwords. Online services are available that allow you to check how often a particular password is being used, and if it complies with security standards.

Recommendation: Use a dedicated software tool for managing your passwords.

2.1.1.1. PASSWORD-PROTECTED ACCESS

Access options:

- Protection against brute-force attacks: a 180 second timeout is enforced after three unsuccessful attempts to log into the web interface.
- Administrator.
- User.
- Web interface remote session.
- SIP account.
- PIN code for executing action sequences and waking the device from advertising mode.

2.1.1.2. PASSWORD-PROTECTED CONFIGURATION

Configuration options:

- 802.1X authentication ([see "802.1X Authentication", page 76](#)).
- SNMP community string ([see "SNMP", page 180](#)).
- Email address ([see "Email Configuration", page 163](#)).

2.1.2. PORTS

Several ports on Commend systems must be enabled to allow the exchange of payload data such as audio and video streams. The following tables list the ports and services that are used, depending on the configuration of the device. External access to network infrastructures must be controlled via a properly configured firewall to comply with company-internal IT security requirements.

Recommendation: Reduce the number of enabled ports to a minimum.

2.1.2.1. UDP PORTS AND SERVICES

Service	Port	Description
DHCP	68	DHCP client service (only active when DHCP is activated)
NTP	123	NTP (Network Time Protocol), used for system clock synchronisation
SNMP	161	SNMP (Simple Network Management Protocol), used for monitoring device information
SNMP Trap	162	Used for sending SNMP trap packages.
UPnP/SSDP	1900	Used for discovering and linking devices
ONVIF	3702	ONVIF discovery function
SIP	5060 ¹⁾	SIP (Session Initiation Protocol), used for signalling and controlling multimedia communication sessions in VoIP applications
mDNS	5353	Used for discovering the device via zeroconf
RTP	16384 to 16640 ²⁾	Starting port for media transmission, plus up to two ports per call (used only during conversations and for outgoing and incoming calls)

Table 1: UDP ports and services

2.1.2.2. TCP PORTS AND SERVICES

Service	Port	Description
SSH	22	“Secure Shell”, used for maintenance and debugging
HTTP	80	Default port for HTTP (Hypertext Transfer Protocol), used for device configuration and control; HTTP requests are automatically forwarded as HTTPS requests
HTTPS	443	Default port for HTTPS (Hypertext Transfer Protocol Secure), used for device configuration and control
RTSP	554	Default port for RTSP (Real-Time Streaming Protocol), used for network-internal communication

Table 2: TCP ports and services

¹⁾ This port number is configurable.

²⁾ This port number is configurable.

Service	Port	Description
SIP	5060 ³⁾	SIP (Session Initiation Protocol), used for signalling and controlling multimedia communication sessions in VoIP applications; SIP via TLS may also use port "5060" for signalling.
SIP over TLS	5061 ⁴⁾	SIP (Session Initiation Protocol) over "Secure Transport Layer" (TLS), used for signalling and controlling multimedia communication sessions in VoIP applications

Table 2: TCP ports and services

2.1.2.3. OTHER PORTS AND SERVICES

Service	Port	Description
ICMPv6	58	Raw ICMPv6, router discovery (active only if DHCP is activated)

Table 3: Other ports and services

2.1.3. AUTHENTICATION

Commend systems provide the following default authentication mechanisms for secure network access (see "802.1X Authentication", page 76):

802.1X authentication support:

- EAP-MD5
- EAP-TLS

Recommendation: Use network authentication for the local network to protect the system against unauthorised access.

2.1.4. CERTIFICATES

Public key certificates provide security for data transmission between SIP clients, SIP trunks and SIP servers. SIP signalling data are transmitted in encrypted format using the "TLS" network protocol. By activating SRTP, sensitive audio data can also be transmitted in encrypted format. X.509 certificates contain the following information:

Information:

- Unique name of the issuer.
- Unique name of the owner.
- Validity period.
- Length of the public key
- RSA encryption algorithm.

Recommendation: Use unique names for certificates.

Example: "<host name>_<serial number>.pem" for client certificates and "<issuer>_<application>.crt" for client authority certificates.

³⁾ This port number is configurable.

⁴⁾ This port number is configurable.

Certificates can be uploaded to the device to activate client authentication and server authentication.

Options:

- SIP certificate for peer-to-peer calls ([see "SIP Settings", page 92](#)).
- SIP certificates ([see "SIP Certificates", page 101](#)).
- SIP client authority certificates ([see "SIP CA Certificates", page 102](#)).
- Server certificates ([see "Server Certificates", page 86](#)).
- Client authority certificates ([see "Client CA certificates", page 87](#)).

3. GENERAL DESCRIPTION

3.1. SYMPHONY MX FEATURES

General

- Support of the Symphony Cloud Platform.
- Adaptive brightness mode.
- Advanced rules engine with trigger and actions, including device states.
- Configurable RGB LED visualisation.
- Optimised layouts for various use cases.
 - Indoor areas.
 - Door applications.
 - Contact management for visitor orientation, including a tree-like directory structure.
 - Customised visualisation, with or without Commend call views.
 - Frame layout with different button formats.
- Pictogram support.
- Time-based actions with cronjobs.
- Extensive list of Symphony MX accessories.
 - EB1E1A.
 - EB3E2A-AUD.
 - AFIL-USB.
 - Handset, including wall mount option.
 - ID5 DKGM, including push-to-talk function and talk/listen visualisation.
- Motion detection.
- Video streaming to external devices.
- Advertising mode, including PIN code.
- User and permission management.
- Actions can be executed only by certain users.
- Email notifications.
- Various languages available.
- Power over Ethernet (PoE).
- Scroll tolerance control for scrollable views.
- Pre-defined symbols for buttons.

Network and IT security

- Secure communication via IP networks. No additional cabling required.
- X.509 certificate for SIP and TLS.
- Transport Layer Security support (TLS 1.2 and TLS 1.3).
- HTTPS for configuration via the web interface.
- Brute force attack protection.
- Token-based security.
- SIP over TLS (SIPS) support.
- SRTP (Secure Real-Time Transport Protocol) support.
- Secure video streaming to external devices.
- 802.1X authentication (EAP-TLS, EAP-MD5).
- VLAN support.
- DSCP support.
- STUN support.
- SNMPv2 for monitoring.

- Integrated web server for configuration and software update.
- IPv4 support and IPv6 support.
- Discovering via zeroconf.
- DHCP Option 12 (Hostname) and Option 60 (Vendor).
- Control of devices with HTTP(S) methods (GET/PUT/POST/DELETE) via JSON, XML and plain text content.
- PIN code for on-device user login.
- Tamper contacts either directly on device or easily retrofitted.
- Additional security in combination with an IP-CON.
- Manual and automatic (randomised) PIN code configuration.
- Support of NAPT and SRV.

Audio

- uHD voice, up to 16 kHz audio bandwidth for optimum intelligibility and compatibility.
- Full duplex for natural, hands-free communication.
- Playback of audio files with up to 20 kHz audio bandwidth.
- Easy and expert configuration mode.
- Beamforming.
- Acoustic echo canceller (AEC).
- Single-channel acoustic noise cancellation (ANC).
- Multi-channel post-filter (MCPF).
- Automatic gain control (AGC).
- Noise gate.
- Intelligent Volume Control (IVC).
- Adaptive jitter buffer.
- Loudspeaker/microphone surveillance.
- Support of audio monitoring, including remote control API.
- Real-time sound pressure level measurement, including remote control API.
- Graphic equalizer.
- Configuration of sampling rate.

SIP

- SIP server redundancy.
 - Parallel.
 - Sequential.
 - Cisco mode.
- Operation without registration possible.
- SIP over TLS support (SIPS) with certificates.
- SIP over TCP and UDP support.
- SIP video (H.264 support).
- Complies with SIP standard for easy use with almost any 3rd-party SIP server.
- Advanced SIP settings for additional compatibility modes with various 3rd-party SIP servers.

Calls

- Video call preview.
- Chain call support for automatic processing of call sequences.
- Automated call acceptance.
- Support of up to 10,000 contacts.
- Contact list with direct call option.
- Call history (missed, outgoing, incoming).
- Live video call (SIP video).
- Combination of audio call with an external video source such as an MJPEG camera.
- Playback of info messages at remote stations.

- DTMF tones via RTP event (RFC 2833) or SIP info.
- Adaptation of the call behaviour to the configuration in VirtuoSIS.

Interface

- ONVIF Profile S support (video).
- HTTPS remote control.
- MX Device API for controlling Symphony MX devices and for monitoring device events and states via 3rd-party installations.

3.2. LED BEHAVIOUR

The lighting behaviour of the LED indicates one of the operating states of the device described below.

LED behaviour:

- **Steady orange light:** The device is starting up. As soon as power is supplied to the device, the LED lights up.
- **Flashing orange light:** The device is being updated. The LED flashes slowly or quickly. The device must not be disconnected from the power supply. If the update was successful, the device starts up.
- **Flashing red light:** A hardware error occurred when starting up the device.
Recommendation: If this behaviour occurs repeatedly, contact the technical support.
- **LED off:** The device is ready to operate.

3.3. USB DEVICES

It is possible to connect external USB devices to the device. The device supports the connection of a maximum of one USB device of the same type at any time.

Example: One EB3E2A-AUD and one EB1E1A.

4. DEVICE DISPLAY DESCRIPTION

4.1. PREVENT IMAGE PERSISTENCE

Modern displays are resistant to traditional screen burn-in. With new display technologies, image persistence (image sticking) can occur. It occurs when static content is displayed for an extended period. When switching to new content on the display, “ghost images” may be created that are superimposed over the existing image on the display.

Commend uses only high-quality displays. These displays have very good properties that prevent image persistence. However, the measures described below should be observed to prevent image persistence.

Measures:

- Use the advertising mode or configure the display so it switches off automatically after 10 minutes of inactivity.
- If it is not possible to use the advertising mode or to switch off the display at certain times of the day, use these functions at other times such as during the night.
- Configure the display brightness as low as possible.

4.2. INTRODUCTION

4.2.1. VIEWS

The touch display provides the following views:

Views:

- **Home:** Shows the main view. This view is shown in the configured layout.
- **Contacts:** Shows the contact list. Calls can be initiated to configured contacts. This view is only available in the layout “Indoor”.
- **Recent:** Shows the call history. Calls can be initiated to configured contacts. This view is only available in the layout “Indoor”.
- **Settings:** Configure the device settings. This view is only available in the layout “Indoor”.
- **Incoming Call:** Shows incoming calls that have not been accepted yet.
- **Outgoing Call:** Shows outgoing calls that have not been accepted yet.
- **In Call:** Shows a list of accepted calls.

The device can be operated using the touch display. The displayed view can be navigated through long and short tapping gestures.

Tapping a button in a view without a scroll bar on the right triggers the function immediately. Tapping a button in a view with a scroll bar on the right triggers the function only if the finger tap does not exceed the scroll tolerance of the display.

If the view is switched from “Home” to the view “Keypad”, “Contacts” or “Call History” and the display is not touched for 30 seconds, the view automatically reverts to “Home”. If the view is switched from “Home” to view “Settings”, the view does not revert to “Home” automatically.

4.2.2. BOOT VIEWS

The following views are shown when the device is booting:

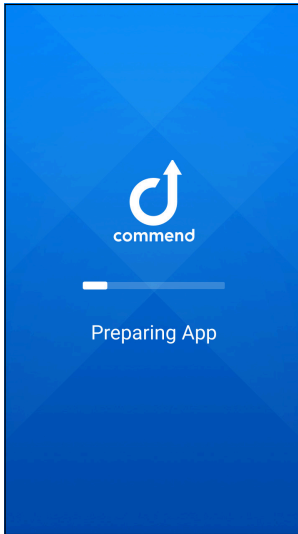


Figure 1: Boot view "Preparing App"

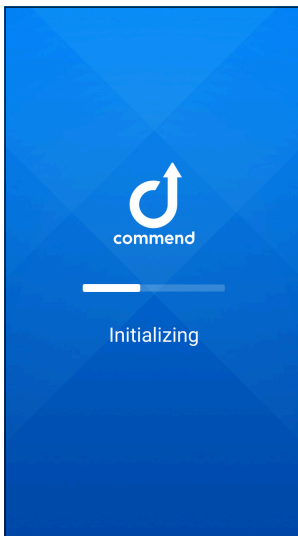


Figure 2: Boot view "Initializing"

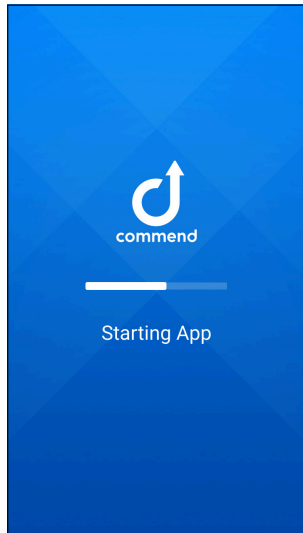


Figure 3: Boot view “Starting App”

When the booting process is complete, a noise signal for audio calibration and a short signal tone are played back. The view “Home” is shown.

4.3. LAYOUTS

Home is the default view. The device is in the device state “Idle” or “Error”.

In the default configuration, only the button for the “Example Contact” is shown. To be able to initiate a call to a remote device, the example contact must be configured.

4.3.1. INDOOR

The following functions are available:

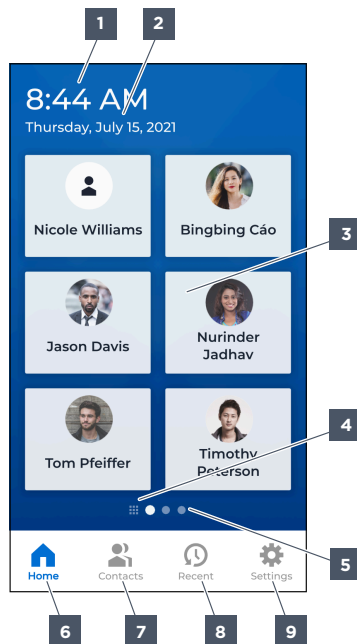


Figure 4: Indoor - Format "Small"

1	Time	2	Date	3	Buttons
4	Keypad	5	Pages	6	Home
7	Contacts	8	Recent	9	Settings

If the format "Small" is selected, up to 6 buttons can be displayed per page. If no avatar or icon is configured, the initials for the button name are shown instead.

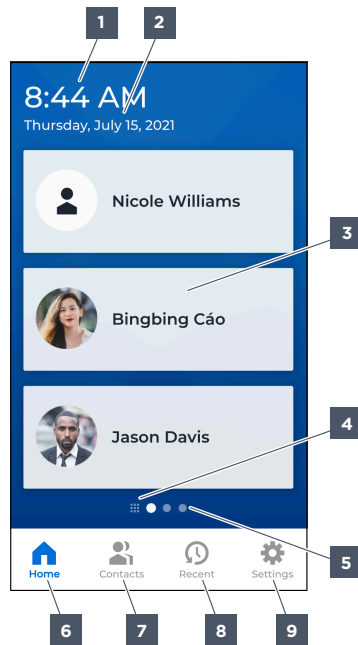


Figure 5: Indoor - Format "Large"

1	Time	2	Date	3	Buttons
4	Keypad	5	Pages	6	Home
7	Contacts	8	Recent	9	Settings

If the format "Large" is selected, up to 3 buttons can be displayed per page. If no avatar or icon is configured, the initials for the button name are shown instead.

If the display is not touched for 30 seconds, the view automatically reverts to "Home". If several pages are configured, page 1 is displayed.

[1] Time: Shows the current time.

[2] Date: Shows the day of the week and the date.

[3] Buttons: Tap to initiate calls or trigger functions.

[4] Keypad: Swipe right to switch to the view "Keypad".

[5] Pages: Swipe left or right to navigate the pages. By default only one page is configured.

[6] Home: Shows that the view "Home" is selected.

[7] Contacts: Tap to switch to the view "Contacts".

[8] Recent: Tap to switch to the view "Recent".

[9] Settings: Tap to switch to the view "Settings".

4.3.1.1. KEYPAD

The following functions are available:



Figure 6: Indoor - Keypad

1	Entry	2	Digits	3	Call
4	Delete	5	Keypad	6	Pages
7	Home	8	Contacts	9	Recent
10	Settings	11	Dot		

If the display is not touched for 30 seconds, the view reverts to “Home”.

To be able to initiate a call to remote devices, the device must be registered at a SIP Server. The call numbers or user IDs that should be available for calls must be configured at the SIP server. Call numbers or user IDs do not have to be linked to a contact on the device. If the device is operated in registrarless mode, the call is cancelled directly and is not listed in the view “Recent”.

[1] Entry: Shows the call number or user ID.

[2] Digits: Tap to enter call numbers or IP addresses.

[3] Call: Tap to initiate a call.

[4] Delete: Tap to delete the last character of the entry.

[5] Keypad: Shows that the view “Keypad” is selected.

[6] Pages: Swipe left or right to navigate the pages. By default only one page is configured.

[7] Home: Shows that the view “Home” is selected.

[8] Contacts: Tap to switch to the view “Contacts”.

[9] Recent: Tap to switch to the view “Recent”.

[10] Settings: Tap to switch to the view “Settings”.

[1] Dot: Tap to add a dot while entering IP addresses.

4.3.1.2. CONTACTS

The following functions are available:

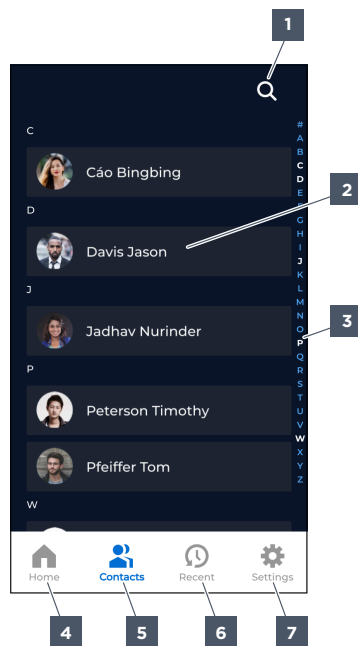


Figure 7: Indoor – Contacts

- 1 Search...
- 4 Home
- 7 Settings

- 2 Buttons
- 5 Contacts

- 3 Navigation bar
- 6 Recent

If the display is not touched for 30 seconds, the view reverts to “Home”.

The contact list can be scrolled by swiping up or down.

Contacts are sorted by last name.

[1] Search...: Tap to search for button texts such as contacts or actions.

[2] Buttons: Tap to initiate a call or trigger functions.

[3] Navigation bar: Tap to jump to the selected letter in the contact list. The contacts are sorted alphabetically by last name. Swipe to scroll the contact list. Letters that are highlighted in white in the navigation bar indicate that contacts are configured for that letter.

[4] Home: Tap to switch to the view “Home”.

[5] Contacts: Shows that the view “Contacts” is selected.

[6] Recent: Tap to switch to the view “Recent”.

[7] Settings: Tap to switch to the view “Settings”.

4.3.1.3. RECENT

The following functions are available:

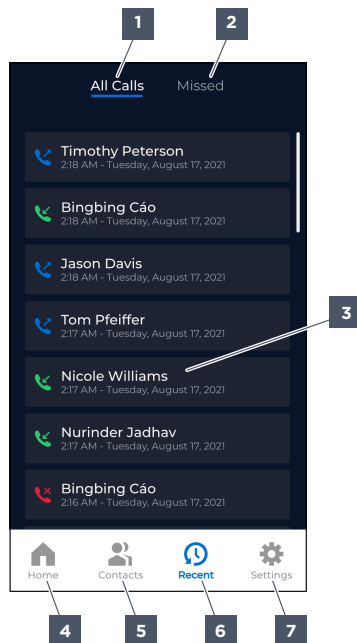


Figure 8: Indoor – Recent

- 1 All Calls
- 4 Home
- 7 Settings

- 2 Missed
- 5 Contacts

- 3 Buttons
- 6 Recent

If the screen is not touched for 30 seconds, the view reverts to “Home”.

[1] All Calls: Tap to remove any filter on the call history list.

[3] Missed: Tap to filter the call history list for missed calls.

[3] Buttons: Tap to initiate a call. Shows call details such as contact, date and time. Call events are sorted chronologically. Only call events linked to individual call targets are shown. Call events linked to multiple targets (e. g. chain calls or parallel calls) are not included in the list. The most recent call event is shown at the top of the list. Up to 200 call events can be stored, based on the FIFO principle (“first in, first out”). The icon on the left shows the following call events:

Call events:

- **Blue handset:** An outgoing call has been initiated. The call has been accepted or has not been accepted.
- **Green handset:** An incoming call has been accepted.
- **Red handset:** An incoming call has not been accepted (missed call).

[4] Home: Tap to switch to the view “Home”.

[5] Contacts: Tap to switch to the view “Contacts”.

[6] Recent: Shows that the view “Recent” is selected.

[7] Settings: Tap to switch to the view “Settings”.

4.3.2. DOOR

The following functions are available:

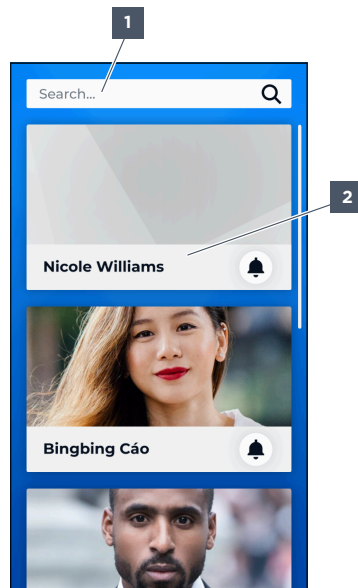


Figure 9: Indoor - Format "Large"

1 Search...

2 Buttons

If the format "Large" is selected, the avatar image is displayed above the button label. An icon can be configured to be displayed next to the avatar. If no avatar or icon is configured, a placeholder image is shown instead.

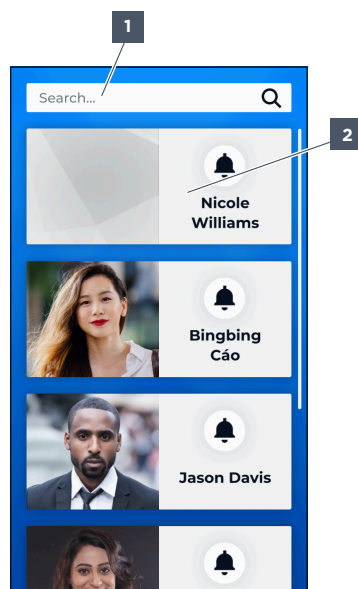


Figure 10: Indoor - Format "Small"

1 Search...

2 Buttons

If the format "Small" is selected, the avatar image is displayed to the left of the button label. An icon can be configured to be displayed above the button label. If no avatar or icon is configured, a placeholder image is shown instead.

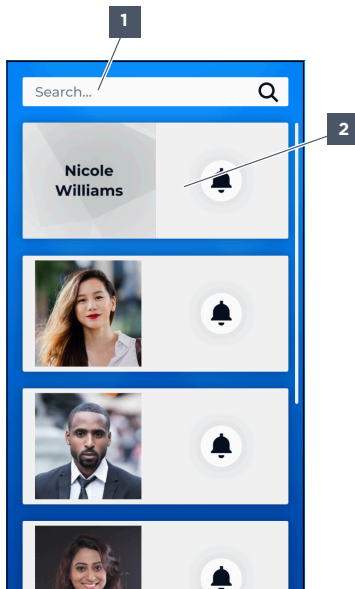


Figure 11: Indoor – Format “Small (Image or Text)”

- 1 Search...
- 2 Buttons

If the format “Small (Image or Text)” is selected, the avatar image is displayed on the left. If no avatar is configured, the button label is shown on the left. An icon can be configured to be displayed on the right.

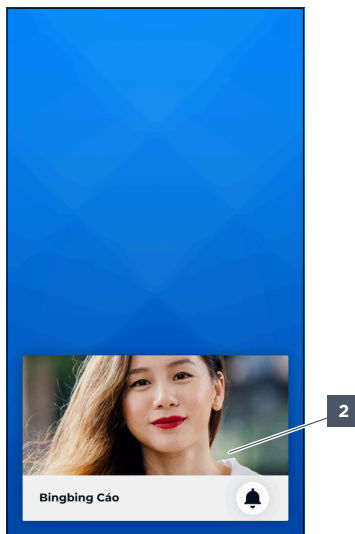


Figure 12: Indoor – 1 button, format “Large”

- 2 Buttons

If only 1 button is configured, the search box is hidden. If more than 1 button is configured, the buttons are aligned to the top.

If more buttons are configured than can be displayed on the display, the search bar is displayed at the top. If more buttons are configured than can be displayed on the display, the buttons that are not displayed can be displayed by scrolling.

If the layout “Door” is displayed, the views “Keypad”, “Contacts” and “Call History” cannot be shown. The view “Settings” can only be brought up by an action or action sequence.

If the display is not touched for 30 seconds, the view automatically reverts to “Home”. If several buttons are configured, the top button is displayed.

[1] Search...: Tap to search for button texts such as contacts or actions.

[2] Buttons: Tap to initiate calls or to trigger functions.

4.3.3. FRAME

The following functions are available:

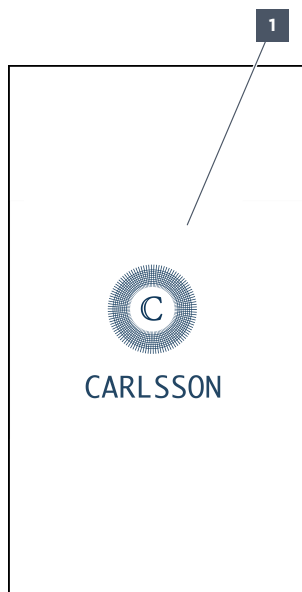


Figure 13: Frame “1 Button”

1 Buttons

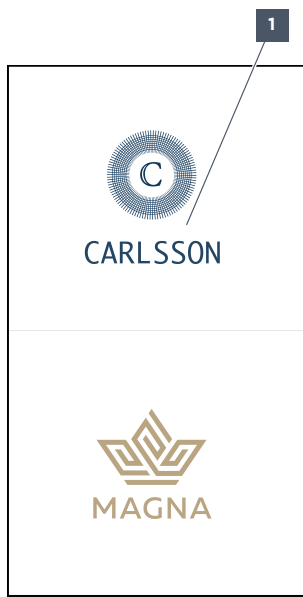


Figure 14: Frame "2 Buttons (1/2, 1/2)"

1 Buttons

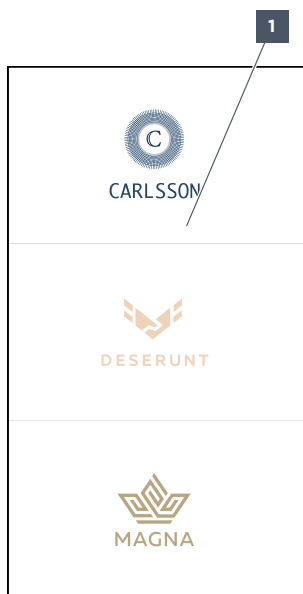


Figure 15: Frame "3 Buttons (1/3, 1/3, 1/3)"

1 Buttons

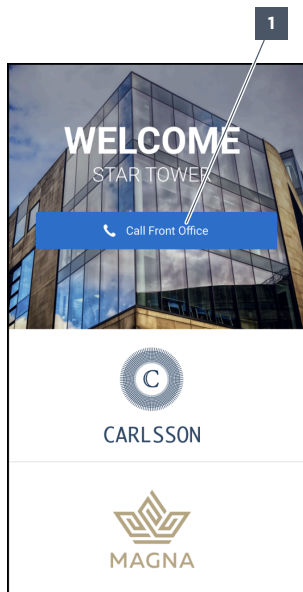


Figure 16: Frame "3 Buttons (1/2, 1/4, 1/4)"

1 Buttons

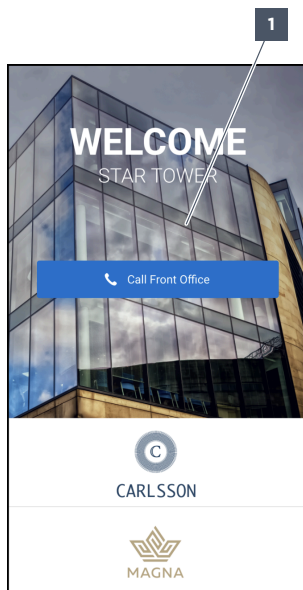


Figure 17: Frame "3 Buttons (2/3, 1/6, 1/6)"

1 Buttons

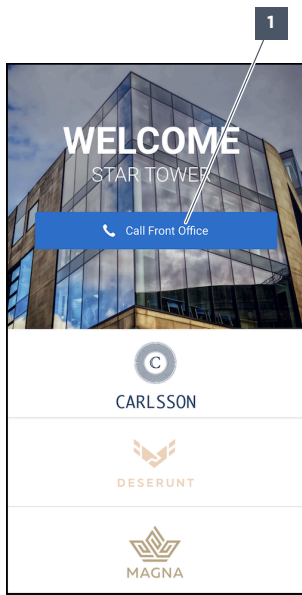


Figure 18: Frame "4 Buttons (1/2, 1/6, 1/6, 1/6)"

1 Buttons

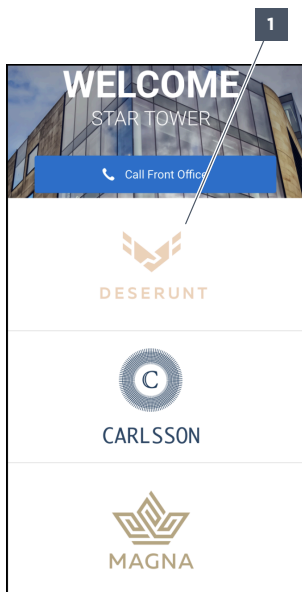


Figure 19: Frame "4 Buttons (1/4, 1/4, 1/4, 1/4)"

1 Buttons

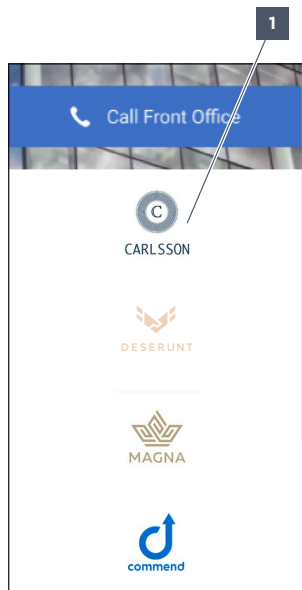


Figure 20: Frame "5 Buttons (1/5, 1/5, 1/5, 1/5, 1/5)"

1 Buttons

If the layout "Frame" is activated, the views "Keypad", "Contacts" and "Call History" cannot be shown. The view "Settings" can only be brought up by an action or action sequence.

If the display is not touched for 30 seconds, the view automatically reverts to "Home". If several buttons are configured, the top button is displayed.

[1] Buttons: Tap to initiate a call or trigger functions. Standard calls and emergency calls can be configured.

4.3.4. CUSTOMISED VISUALIZATION

The following functions are available:

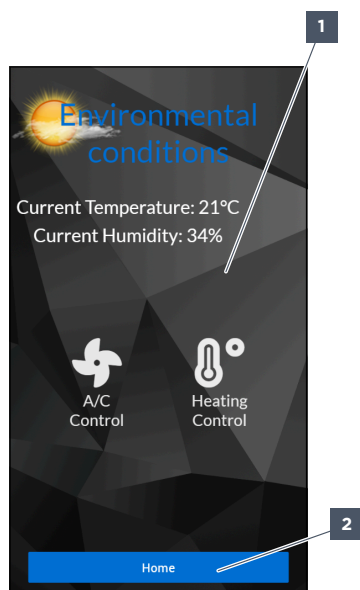


Figure 21: Customised visualisation

1 Content

2 Buttons

When the layout “Customised Visualisation” is displayed, the views “Keypad”, “Contacts” and “Call History” cannot be shown. The view “Settings” can only be brought up by an action or action sequence.

[1] Content: Shows custom content.

[2] Buttons: Tap to initiate a call or to trigger a function. Up to 2 buttons can be configured.

4.3.5. CONTACT MANAGEMENT

The following functions are available:

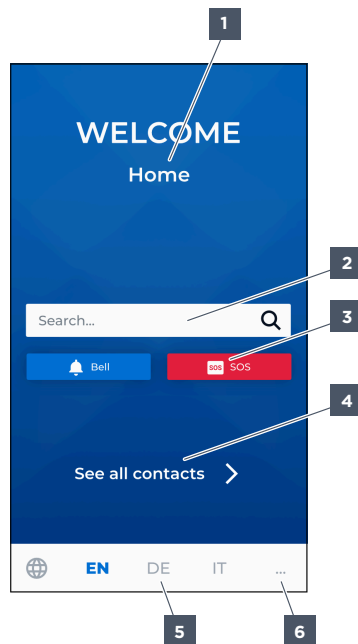


Figure 22: Contact management

- | | | |
|---------------------------|--------------------|-------------------------|
| 1 Name | 2 Search... | 3 Sticky buttons |
| 4 See all contacts | 5 Language | 6 All languages |

If the display is not touched for 30 seconds, the view automatically reverts to “Home”.

[1] Name: Shows the parent name.

[2] Search...: Tap to search for button texts such as contacts or actions.

[3] Sticky buttons: Tap to initiate a call or trigger functions. Up to 2 sticky buttons may be defined.

[4] See all contacts: Tap to view buttons, contacts and subdirectories.

[5] Language: Tap to change the language. If the screen is not touched for 30 seconds, the language reverts to the configured language.

[6] All languages: Tap to show all languages. If the screen is not touched for 30 seconds, the language reverts to the configured language.

Options:

- English
- German
- French
- Spanish
- Russian
- Dutch
- Italian
- Polish

4.3.5.1. DIRECTORY

The following functions are available:

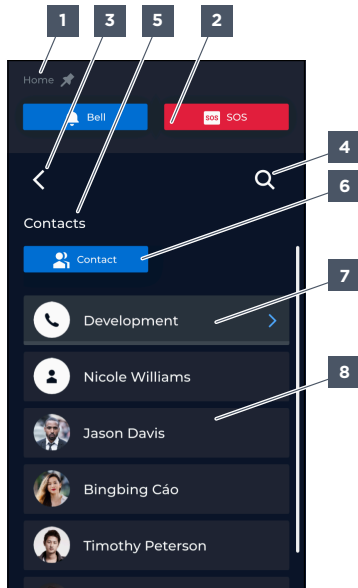


Figure 23: Contact Management – Directory

- | | | |
|----------------|------------------|---------------------|
| 1 Name | 2 Sticky buttons | 3 Back |
| 4 Search... | 5 Path | 6 Directory buttons |
| 7 Subdirectory | 8 Buttons | |

Sticky buttons and directory buttons can be configured as described below:

Configuration options:

- Up to 4 sticky buttons und 0 directory buttons.
- 0 sticky buttons and up tp 4 directory buttons.
- Up to 2 sticky buttons and up to 2 directory buttons.

- [1] Name:** Shows the parent name.
- [2] Sticky buttons** Tap to initiate a call or trigger functions.
- [3] Back:** Tap to change to the parent directory or to view “Home”.
- [4] Search...:** Tap to search for button texts such as contacts or actions.
- [5] Path:** Shows the directory path. Tap to change to a parent directory.
- [6] Directory buttons:** Tap to initiate calls or to trigger functions.
- [7] Subdirectory:** Tap to navigate to the subdirectory.
- [8] Buttons:** Tap to initiate calls.

4.4. CALL VIEWS

For each call status the views described below are available:

Views:

- Outgoing Call
- Incoming Call
- In Call
- Call Ended

Call views can be configured to show control buttons or pictograms. Call control buttons are optimised for indoor applications: They can be used to adjust the volume, mute the audio output, put a call on hold or bring up the keypad for after-dialling. Pictograms are optimised for use in outdoor or passageway applications to offer graphical indication of the current status.

4.4.1. OUTGOING CALL

The following functions are available:

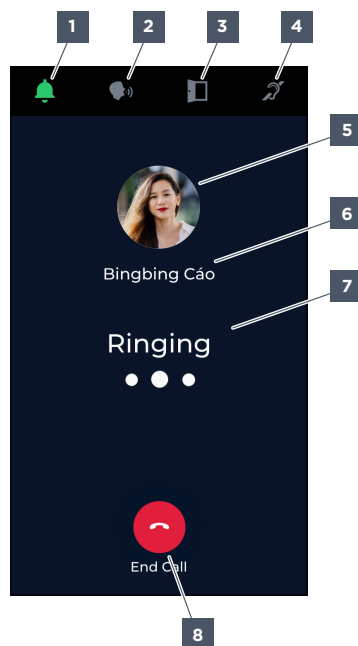


Figure 24: Outgoing Call - Type "Standard" with pictograms

- | | | |
|-----------|------------|-------------|
| 1 Ringing | 2 Speak | 3 Door open |
| 4 AFIL | 5 Avatar | 6 Name |
| 7 State | 8 End Call | |

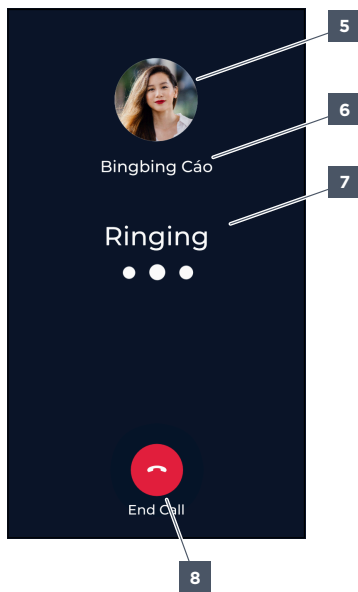


Figure 25: Outgoing Call - Type "Standard" without pictograms

- 5 Avatar
- 6 Name
- 7 State
- 8 End Call

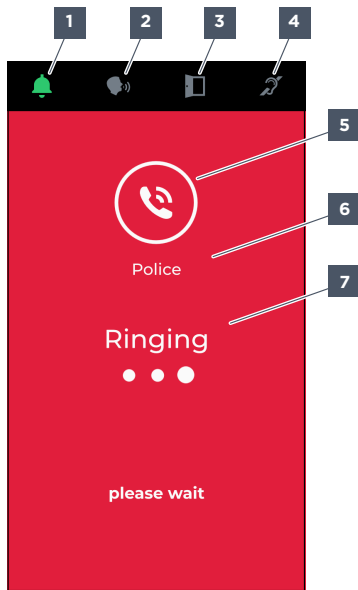


Figure 26: Outgoing Call - Type "Emergency" with pictograms

- 1 Ringing
- 2 Speak
- 3 Door open
- 4 AFIL
- 5 Avatar
- 6 Name
- 7 State

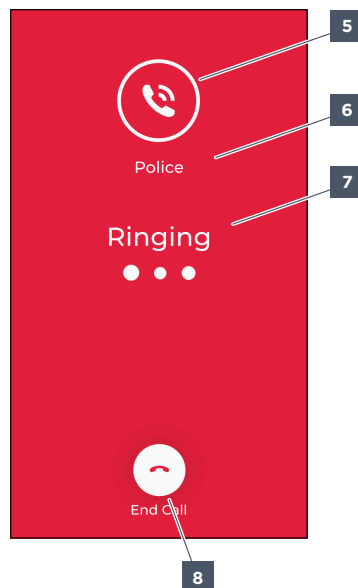


Figure 27: Outgoing Call - Type "Emergency" without pictograms

5	Avatar	6	Name	7	State
8	End Call				

[1] Ringing: Shows the ringing pictogram. If the pictogram is highlighted, this indicates that the call has not been answered yet.

[2] Speak: Shows the speak pictogram. If the pictogram is highlighted, this indicates that the call has been established. The caller can start speaking.

[3] Door open: Shows the speak pictogram. If the pictogram is highlighted, this indicates that the door opener function has been activated. The door can be opened.

[4] AFIL: Shows the AFIL pictogram. If the pictogram is highlighted, this indicates that audio signals are being transmitted via an induction loop. This pictogram is only shown if an ADIL-USB is connected to the device.

[5] Avatar: Shows the avatar or the icon. If no avatar or icon is configured, the initials are shown as a placeholder instead. If the button of the type "Emergency" is configured, no avatar is shown.

[6] Name: Shows the contact to which a call is being initiated.

[7] State: Shows the current call status.

[8] End Call: Tap to end the call. The end call button can be displayed or hidden separately for the types "Standard" and "Emergency". Calls are automatically ended after a configurable timeout ([see "Outgoing Call", page 98](#)).

4.4.2. INCOMING CALL

The following functions are available:

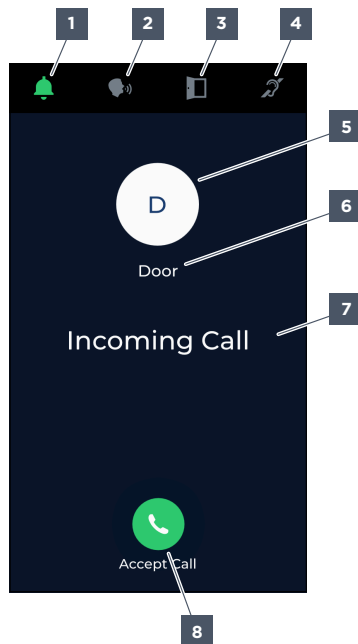


Figure 28: Incoming Call - with pictograms

- | | | |
|-----------|---------------|-------------|
| 1 Ringing | 2 Speak | 3 Door open |
| 4 AFIL | 5 Avatar | 6 Name |
| 7 State | 8 Accept Call | |

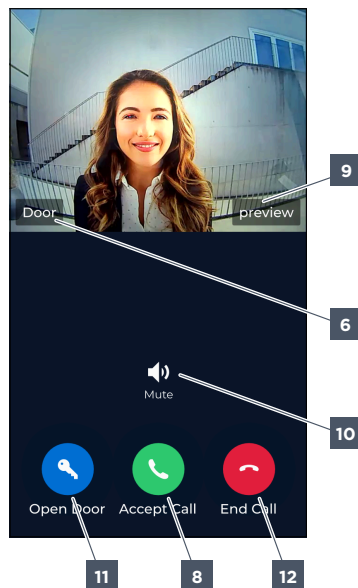


Figure 29: Incoming Call - with call control buttons

- | | | |
|---------|---------------|-------------|
| 6 Name | 8 Accept Call | 9 Preview |
| 10 Mute | 11 Open Door | 12 End Call |

- [1] Ringing:** Shows the ringing pictogram. If the pictogram is highlighted, this indicates that the call has not been answered yet.
- [2] Speak:** Shows the speak pictogram. If the pictogram is highlighted, this indicates that the call has been established. The caller can start speaking.
- [3] Door open:** Shows the speak pictogram. If the pictogram is highlighted, this indicates that the door opener function has been activated. The door can be opened.
- [4] AFIL:** Shows the AFIL pictogram. If the pictogram is highlighted, this indicates that audio signals are being transmitted via an induction loop. This pictogram is only shown if an ADIL-USB is connected to the device.
- [5] Avatar:** Shows the avatar or the icon. If no avatar or icon is configured, the initials are shown as a placeholder instead.
- [6] Name:** Shows the contact to which a call is being initiated. If the contact is not configured on the device, the display name of the remote device is shown instead.
- [7] State:** Shows the current call status.
- [8] Accept Call:** Tap to answer the call. The accept call button can be shown or hidden as needed.
- [9] Preview:** Shows the video preview. The function **Request Video Preview** must be activated ([see "Incoming Call", page 97](#)).
- [10] Mute:** Tap to mute the ringtone temporarily.
- [11] Open:** Tap to activate the door opener function. The door open button can be shown or hidden as needed.
- [12] End Call:** Tap to end the current call. The end call button can be shown or hidden as needed.

4.4.3. IN CALL

The following functions are available:

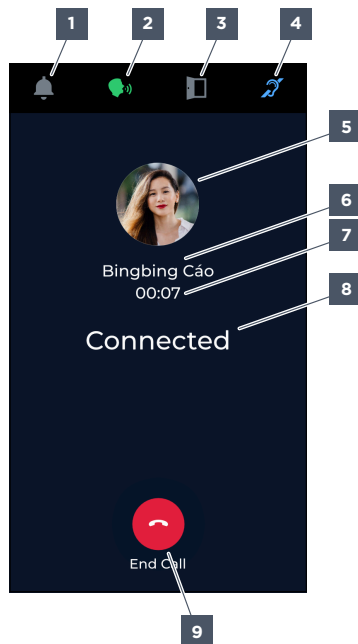


Figure 30: In Call - Type "Standard" with pictograms

- | | | |
|-------------|----------|-------------|
| 1 Ringing | 2 Speak | 3 Door open |
| 4 AFIL | 5 Avatar | 6 Name |
| 7 Call time | 8 State | 9 End Call |

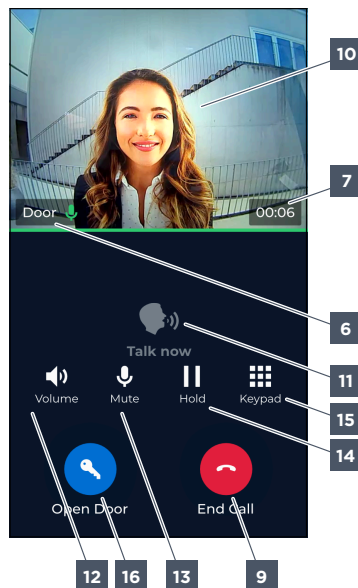


Figure 31: In Call - Type "Standard" without pictograms

- | | | |
|----------------|------------------------------|------------|
| 6 Name | 7 Call time | 9 End Call |
| 10 Video image | 11 Talk/listen visualisation | 12 Volume |
| 13 Mute | 14 Hold | 15 Keypad |

16 Open Door

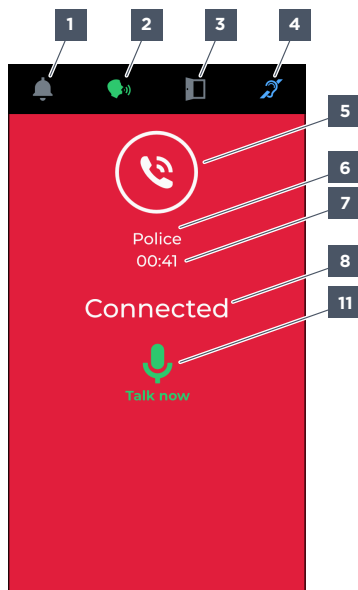


Figure 32: In Call - Type "Emergency" with pictograms

- 1 Ringing
- 4 AFIL
- 7 Call time

- 2 Speak
- 5 Avatar
- 8 State

- 3 Door open
- 6 Name
- 11 Talk/listen visualisation

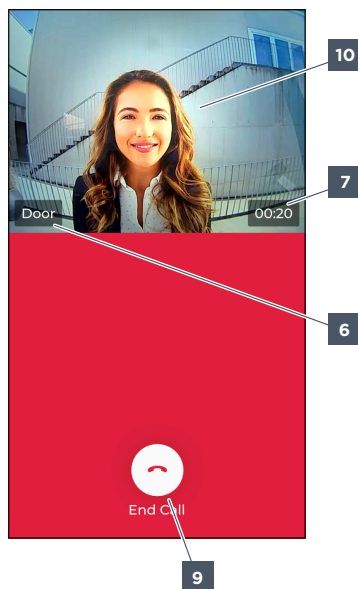


Figure 33: In Call - Type "Standard" without pictograms

- 6 Name
- 10 Video image

- 7 Call time

- 9 End Call

[1] Ringing: Shows the ringing pictogram. If the pictogram is highlighted, this indicates that the call has not been answered yet.

[2] Speak: Shows the speak pictogram. If the pictogram is highlighted, this indicates that the call has been established. The caller can start speaking.

[3] Door open: Shows the door open pictogram. If the pictogram is highlighted, this indicates that the door opener function has been activated. The door can be opened.

[4] AFIL: Shows the AFIL pictogram. If the pictogram is highlighted, this indicates that audio signals are being transmitted via an induction loop. This pictogram is only shown if an ADIL-USB is connected to the device.

[5] Avatar: Shows the avatar or the icon if the video image is deactivated on the device or at the remote device. If no avatar or icon is configured, the initials are shown as a placeholder instead. If the button of the type “Emergency” is configured, no avatar is shown.

[6] Name: Shows the contact to which a call is being initiated. If the contact is not configured on the device, the display name of the remote device is shown instead.

[7] Call time: Shows the current duration of the ongoing call.

[8] State: Shows the current call status.

[9] End Call: Tap to end the call. The end call button can be displayed or hidden separately for the types “Standard” and “Emergency”. Calls are automatically ended after a configurable timeout ([see “In Call”, page 97](#)).

[10] Video image: Shows the video image of the remote device. Video images are shown only if the video image function is activated both on the device and the remote device. If a talk/listen visualisation is configured, a green line at the bottom of the video image and a green microphone symbol next to the name indicate that the person at the remote device may start speaking. A grey line at the bottom of the video image and a greyed-out microphone symbol indicate when the person at the device may start speaking.

[11] Talk/listen visualisation Shows the talk/listen visualisation on the display. An ID5 DKGM or ID5 DKHSGM must be connected to the device or a remote device. The push-to-talk pictogram must be enabled. A greyed-out push-to-talk pictogram indicates when the person at the remote device may start speaking. A green push-to-talk pictogram indicates when the person at the device may start speaking.

[12] Volume: Tap to bring up the volume control slider. The volume control button is highlighted. Tap the volume control slider to hide it again. The call control buttons can be shown and hidden as needed.

When an EB3E2A-AUD is connected to the device and the option “Headset” is selected in **EB3E2A-AUD Mode**, additional functions are available ([see “Audio Devices and Volume”, page 43](#)). A loud-speaker symbol shows that the built-in microphone and the built-in loudspeaker are used. A headset symbol shows that a headset connected to the EB3E2A-AUD is used.

[13] Mute: Tap to mute incoming or outgoing audio signals. The mute button is highlighted. Tap to unmute the audio signal again. The call control buttons can be shown and hidden as needed.

[14] Hold: Tap to hold a call. The hold button is highlighted. An “On hold” message is shown on the display. The call can be resumed by tapping. The call control buttons can be shown and hidden as needed.

[15] Keypad: Tap to show the keypad. The keypad button is highlighted. Using the keypad, DTMF tones can be sent to transmit in-call dial tones to the SIP server or the remote device. Tap the keypad to hide it again. The call control buttons can be shown and hidden as needed.

[16] Open: Tap to activate the door opener function. The open door button lights up in green. The call is ended automatically after 5 seconds. The open door button can be shown or hidden as needed.

4.4.3.1. KEYPAD

The following functions are available:

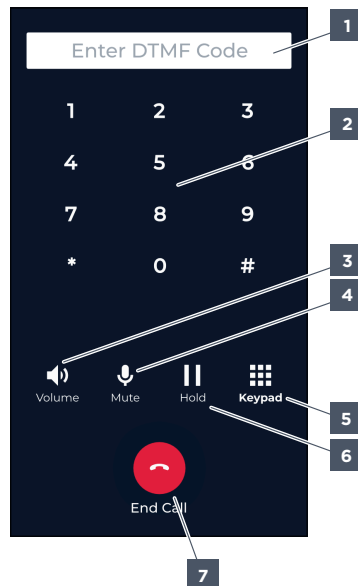


Figure 34: In Call – Keypad

- | | | |
|--------------------|---------------------|-----------------|
| 1 DTMF code | 2 DTMF tones | 3 Volume |
| 4 Mute | 5 Hold | 6 Keypad |
| 7 End Call | | |

[1] DTMF code: Shows the dialled DTMF tones.

[2] DTMF tones: Tap to send DTMF tones to the SIP server or the remote station. DTMF tones are transmitted immediately when dialled.

[3] Volume: Tap to bring up the volume control slider. The volume control button is highlighted. The keypad is hidden. Tap the volume control slider to hide it again. The call control buttons can be hidden and unhidden as needed.

[4] Mute: Tap to mute incoming or outgoing audio signals. The mute button is highlighted. Tap to unmute the audio signal again. The call control buttons can be hidden and unhidden as needed.

[5] Hold: Tap to hold a call. The hold button is highlighted. An “On hold” message is shown on the screen. The call can be resumed by tapping. The call control buttons can be hidden and unhidden as needed.

[6] Keypad: Tap to hide the keypad. The call control buttons can be hidden and unhidden as needed.

[7] End Call: Tap to end the call. The end call button can be displayed or hidden separately for the types “Standard” and “Emergency”. Calls are automatically ended after a configurable timeout ([see “In Call”, page 97](#)).

4.4.3.2. AUDIO DEVICES AND VOLUME

When an EB3E2A-AUD is connected to the device and the option “Headset” is selected in **EB3E2A-AUD Mode**, additional functions are available ([“Audio Devices with EB3E2A-AUD”](#)).

The following functions are available:

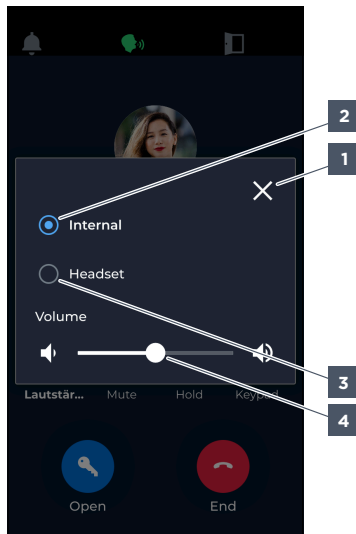


Figure 35: In Call - Audio devices

1 Close

2 Internal

3 Headset

4 Volume

[1] Close: Tap to close the audio settings.

[2] Internal: Tap to use the built-in microphone for audio input and the built-in loudspeaker for audio output.

[3] Headset: Tap to use a headset connected to the EB3E2A-AUD for audio input and audio output.

[4] Volume: Adjust the volume of the selected audio device. Range of values: "0" to "12". Default: "8".

4.4.4. CALL ENDED

The following functions are available:

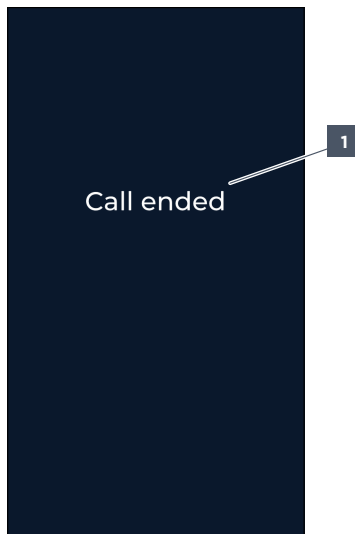


Figure 36: Call ended

1 State

When a call is ended, the view "Call ended" is shown for a short time.

[1] State: Shows the current call status.

4.5. SEARCH

The following functions are available:

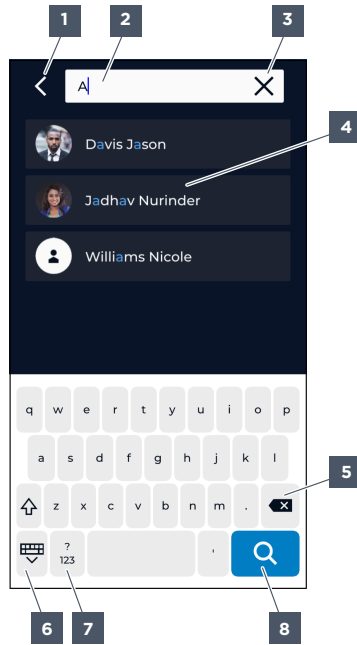


Figure 37: Search - Layout "Indoor"

- | | | |
|--------------|----------------|---------------|
| 1 End search | 2 Entry | 3 End search |
| 4 Buttons | 5 Delete | 6 Hide keypad |
| 7 Symbols | 8 Show results | |

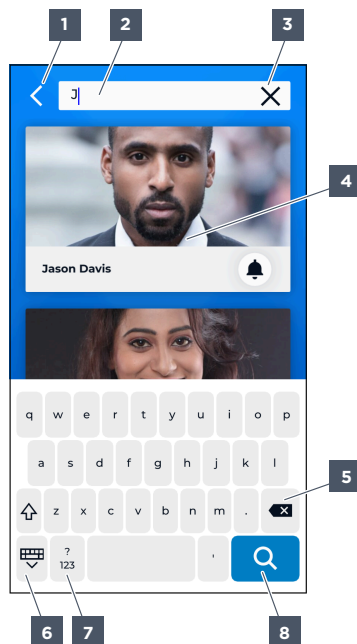


Figure 38: Search - Layout "Door"

- | | | |
|--------------|---------|--------------|
| 1 End search | 2 Entry | 3 End search |
|--------------|---------|--------------|

- | | | |
|------------------|-----------------------|----------------------|
| 4 Buttons | 5 Delete | 6 Hide keypad |
| 7 Symbols | 8 Show results | |

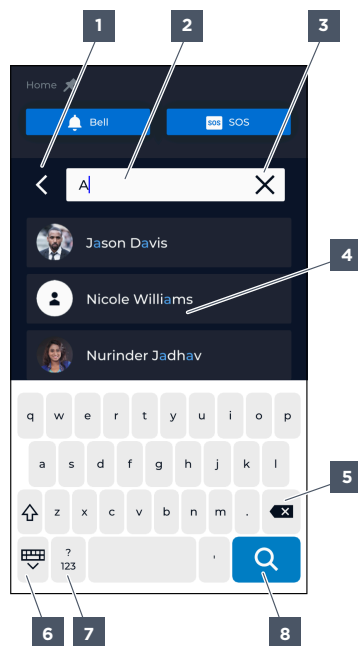


Figure 39: Search - Layout "Contact Management"

- | | | |
|---------------------|-----------------------|----------------------|
| 1 End search | 2 Entry | 3 End search |
| 4 Buttons | 5 Delete | 6 Hide keypad |
| 7 Symbols | 8 Show results | |

If more buttons are configured in the layout "Door" than can be displayed on the display, the search bar is shown at the top.

The layout "Contact Management" provides a list of all configured contacts. A search for contacts includes all subdirectories.

The keypad language can be selected in the view "Home".

The search function uses the instant search method. When a character is entered in the search bar, the matching results are shown in real time. To view the search results, it is not necessary to tap **[8] Show results**.

Long-tapping a character brings up a selection of related special characters.

[1] End search: Tap to delete the entered search term and quit the search.

[2] Entry: Shows the entered search term. The cursor can be positioned by tapping or swiping to delete or add characters.

[3] End search: Tap to delete the input and quit the search function.

[4] Buttons: Tap to initiate calls or trigger functions.

[5] Delete: Tap to delete the last character of the entry.

[6] Hide keypad: Tap to hide the keypad and show the search results. To show the keypad, tap the magnifying glass symbol.

[7] Characters: Tap to switch between letters, digits and special characters.

[8] Show results: Tap to hide the keypad and show the search results.

4.6. PIN CODE

The following functions are available:

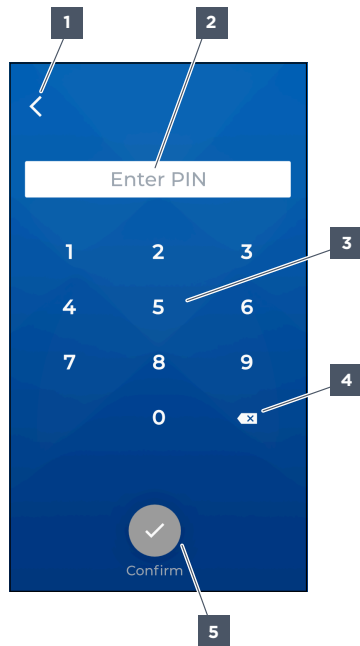


Figure 40: PIN code

- 1** Home
- 4** Delete

- 2** PIN code
- 5** Confirm

- 3** Digits

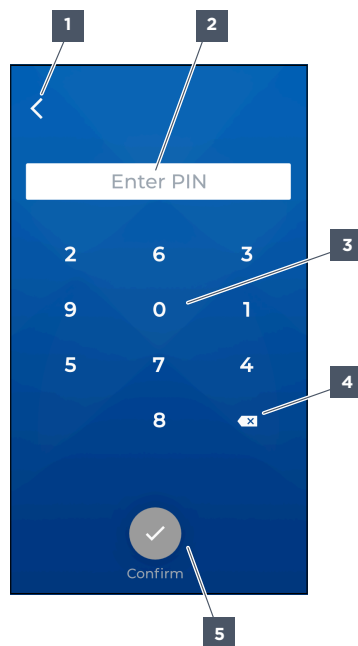


Figure 41: Shuffled keypad numbers for code input

- | | | |
|-----------------|-------------------|-----------------|
| 1 Home | 2 PIN code | 3 Digits |
| 4 Delete | 5 Confirm | |

The arrangement of the keypad numbers can be randomised ([see "Keypad Settings", page 164](#)). Randomising the keypad numbers prevents 3rd parties from guessing the access code by tracing the fingerprints of the user on the screen.

[1] Home: Tap to switch to the view "Home".

[2] PIN code: Shows the entered PIN code digits. The entered PIN code digits are shown as dots.

[3] Digits: Tap to enter the PIN code.

[4] Delete: Tap to delete the last character of the entered PIN code.

[5] Confirm: Tap to confirm the PIN code input. If the entered PIN code is invalid, the entered PIN code is deleted. After 3 unsuccessful attempts of entering the PIN code, a 5-second timeout has to pass before a new try. After 4 unsuccessful attempts of entering the PIN code, a 10-second timeout has to pass before a new try. After 5 unsuccessful attempts of entering the PIN code, a 20-second timeout has to pass before a new try. After 6 unsuccessful attempts of entering the PIN code, a 30-second timeout has to pass before a new try. After 7 unsuccessful attempts of entering the PIN code, a 60-second timeout has to pass before a new try. The device can be configured to show the view "Home" or an advertisement during the timeout.

4.6.1. USER ACTIONS

The following functions are available:

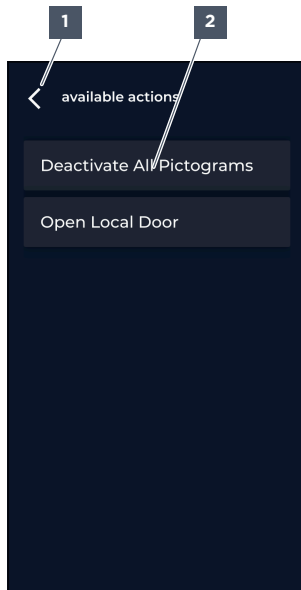


Figure 42: User actions

1 Home

2 Action sequences

If the required PIN code has been entered correctly and allowed action sequences are configured for the user, the view “Action Sequences” is shown. If only one allowed action sequence is configured for the user, it is executed immediately when the correct PIN code has been entered.

[1] Home: Tap to switch to the view “Home”.

[2] Action sequences: Tap to execute an allowed action sequence for the user ([“Allowed Action Sequences”](#)).

4.7. CONFIRMATION DIALOGUE

The following functions are available:

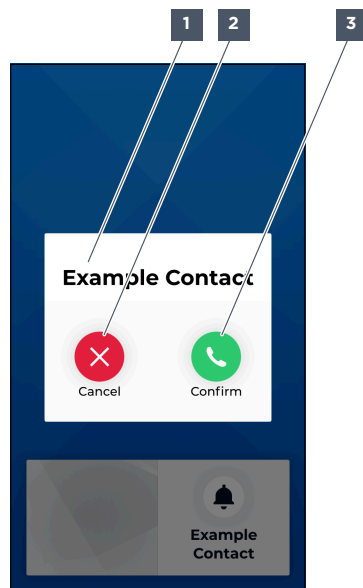


Figure 43: Confirmation dialogue

1 Name

2 Cancel

3 Confirm

When **Confirm Action Execution** is activated, a confirmation dialogue is shown before actions like calls or action sequences are performed ([see "Idle", page 107](#)). The confirmation dialogue is only shown in the layouts "Door" and "Frame".

[1] Name: Shows the name or the image depending on the configuration.

Options:

- **Layout "Door" without image:** The configured text is shown.
- **Layout "Door" with image:** The configured image is shown.
- **Layout "Frame" without image:** The configured text is shown.
- **Layout "Frame" with image:** Neither the configured text nor the configured image is shown.

[2] Cancel: Tap to not perform the action.

[3] Confirm: Tap to perform the action.

4.8. SETTINGS

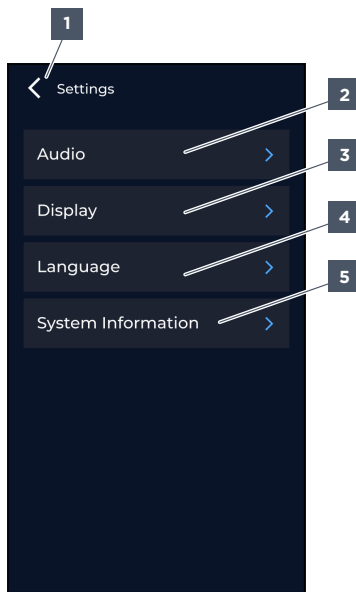


Figure 44: Settings

1 Home

2 Audio

3 Display

4 Language

5 System Information

Actions or action sequences can be used to switch to the view “Settings”. In the layout “Indoor”, the button “Settings” can be used to switch to the view “Settings”.

[1] Home: Tap to switch to the view “Home”.

[2] Audio: Tap to configure the volume settings.

[3] Display: Tap to configure the display settings.

[4] Language: Tap to configure the language settings.

[5] System Information: Tap to view information about the network, SIP connections and the device.

4.8.1. AUDIO

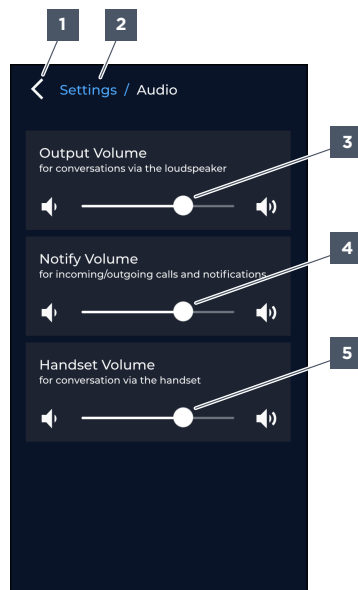


Figure 45: Settings – Audio

- | | | |
|------------------------|-------------------------|------------------------|
| 1 Home | 2 Path | 3 Output Volume |
| 4 Notify Volume | 5 Handset Volume | |

Configuration changes are applied without the need to save them. If the web interface is open, the browser window must be refreshed to see the changes.

[1] Home: Tap to switch to the view “Home”.

[2] Path: Shows the directory path. Tap to change to a parent directory.

[3] Output Volume: Adjust the loudspeaker volume setting for notification sounds and audio files. Range of values: “0” to “12”. Default: “8”.

[4] Notify Volume: Adjust the loudspeaker volume for calls and announcements. Range of values: “0” to “12”. Default: “8”.

[5] Handset Volume: Adjust the volume setting for the USB handset. Switch off the device before connecting the USB handset. Range of values: “0” to “12”. Default: “8”.

i NOTE

Handset Volume

Handset Volume is displayed when a USB handset is connected for the first time. **Handset Volume** is displayed when a USB handset is connected after restoring the factory settings.

If the USB handset is disconnected from the device, **Handset Volume** is still displayed. The configuration remains as is.

4.8.2. DISPLAY

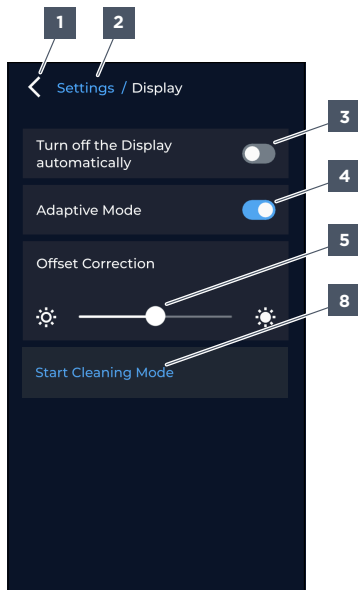


Figure 46: Settings - Display "Adaptive"

- 1 Home
- 2 Path
- 3 Turn off the Display automatically
- 4 Adaptive Mode
- 5 Offset Correction
- 8 Start Cleaning Mode

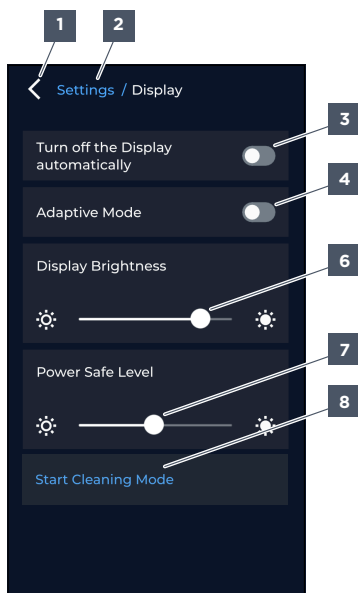


Figure 47: Settings - Display "Manually"

- 1 Home
- 2 Path
- 3 Turn off the Display automatically
- 4 Adaptive Mode
- 6 Display Brightness
- 7 Power Save Level
- 8 Start Cleaning Mode

Configuration changes are applied without the need to save them. If the web interface is open, the browser window must be refreshed to see the changes.

[1] Home: Tap to switch to the view “Home”.

[2] Path: Shows the directory path. Tap to change to a parent directory.

[3] Turn off the Display automatically: Activate to turn off the display automatically after a configurable time ([see “All”, page 105](#)). If the advertisement mode is activated, the display is not turned off. Default: activated.

[4] Adaptive Mode Activate to adjust the display brightness automatically to the lighting conditions. Default: activated.

[5] Offset Correction: Adjust the automatic adaptation of the display brightness to the lighting conditions. By automatically adapting the display brightness, content is displayed more legibly depending on the lighting conditions. The display brightness of the device is optimised. In very dark areas, an adjustment of up to -50% may be necessary. Using the offset correction, the absolute value cannot fall below “0%” and the absolute value cannot exceed “100%”. In very bright areas, an adjustment of up to +50% may be necessary. This function is available only if **[4] Adaptive Mode** is activated. Range of values: “-50%” to “+50%”. Default: “0%”.

[6] Display Brightness: Adjust the display brightness when the power save mode is deactivated. This function is available only if **[4] Adaptive Mode** is deactivated. Range of values: “2%” to “100%”. Default: “80%”.

[7] Power Save Level: Adjust the display brightness when the power save mode is activated. To prevent display dimming, set the level to “100%”. This function is available only if **[4] Adaptive Mode** is deactivated. Range of values: “2%” to “100%”. Default: “50%”.

[8] Start Cleaning Mode: Start the cleaning mode. When the cleaning mode has been started, the display is turned insensitive for 30 seconds and cannot be operated during this time.

Incoming calls or changing the layout interrupt the cleaning mode.

Recommendation: Use the cleaning mode for cleaning the display.

4.8.3. LANGUAGE

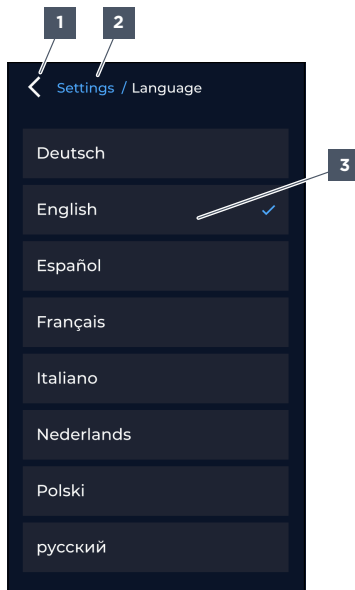


Figure 48: Settings - Language

1 Home

2 Path

3 Language

Configuration changes are applied without the need to save them. If the web interface is open, the browser window must be refreshed to see the changes.

[1] Home: Tap to switch to the view "Home".

[2] Path: Shows the directory path. Tap to change to a parent directory.

[3] Language: Tap to change the language.

Options:

- English
- German
- French
- Spanish
- Russian
- Dutch
- Italian
- Polish

4.8.4. SYSTEM INFORMATION

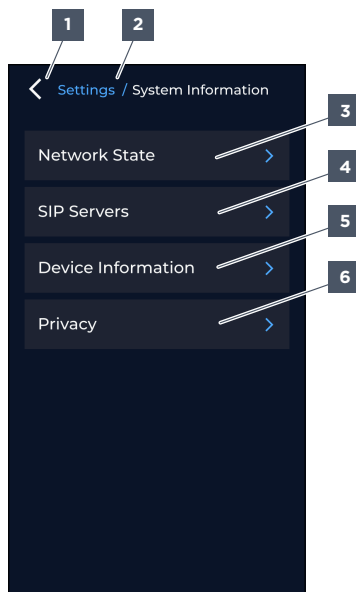


Figure 49: Settings – System Information

1	Home	2	Path	3	Network State
4	SIP Servers	5	Device Information	6	Privacy

[1] Home: Tap to switch to the view “Home”.

[2] Path: Shows the directory path. Tap to change to a parent directory.

[3] Network State: Tap to view network details.

[4] SIP Servers: Tap to view SIP connection details.

[5] Device Information: Tap to view device details.

[6] Privacy: Tap to view data privacy information.

4.8.4.1. NETWORK STATE



Figure 50: Settings – System Information – Network State

1	Home	2	Path	3	IPv4 Method
4	IPv4 Address	5	IPv4 Default Gateway	6	IPv6 Method
7	IPv6 Address	8	Hostname	9	MAC Address

There is nothing to configure in this view.

If any of the information items is not configured, only its name and no value is shown.

[1] Home: Tap to switch to the view “Home”.

[2] Path: Shows the directory path. Tap to change to a parent directory.

[3] IPv4 Method: Shows the IPv4 mode.

[4] IPv4 Address: Shows the IPv4 address.

[5] IPv4 Default Gateway: Shows the IPv4 standard gateway.

[6] IPv6 Method: Shows the IPv6 mode.

[7] IPv6 Address: Shows the IPv6 address. If multiple IPv6 addresses are configured, they are listed on top of each other.

[8] Hostname: Shows the host name.

[9] MAC Address: Shows the MAC address.

4.8.4.2. SIP SERVERS

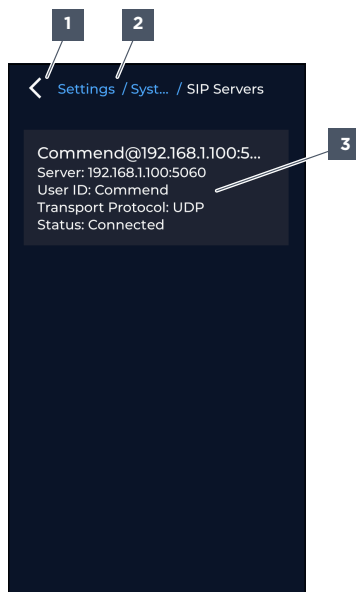


Figure 51: Settings - System Information - SIP Servers

[1] Home

[2] Path

[3] SIP connection

There is nothing to configure in this view.

[1] Home: Tap to switch to the view “Home”.

[2] Path: Shows the directory path. Tap to change to a parent directory.

[3] SIP connection: Shows the SIP connection details. If multiple SIP connections are configured, they are listed on top of each another.

Information items:

- **Server:** Shows the IP address and the port or the host name of the SIP server.
- **User ID:** Shows the user ID of the SIP account.
- **Transport Protocol:** Shows the transport protocol being used for the signal exchange between the device and a SIP device or a SIP server.
- **Status:** Shows the SIP connection state.

4.8.4.3. DEVICE INFORMATION

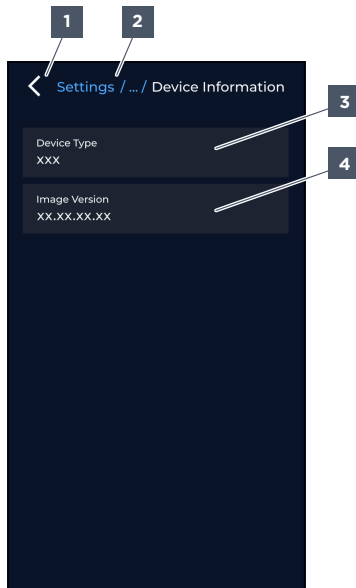


Figure 52: Settings – System Information – Device Information

- 1 Home
- 2 Path
- 3 Device Type
- 4 Image Version

There is nothing to configure in this view.

[1] Home: Tap to switch to the view “Home”.

[2] Path: Shows the directory path. Tap to change to a parent directory.

[3] Device Type: Shows the device name.

[4] Image Version: Shows the software version.

4.8.4.4. PRIVACY

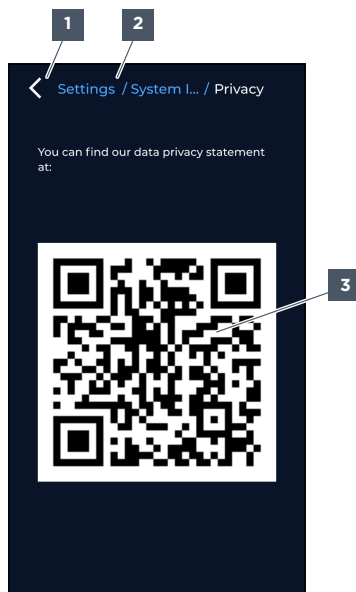


Figure 53: Settings – System Information – Privacy

[1] Home

[2] Path

[3] QR code

There is nothing to configure in this view.

[1] Home: Tap to switch to the view “Home”.

[2] Path: Shows the directory path. Tap to change to a parent directory.

[3] QR code: Shows a QR code that points to the web page with Commend's data privacy policy.
Link: <https://www.commend.com/web/privacy-policy.html>

5. WEB INTERFACE DESCRIPTION

5.1. INTRODUCTION

5.1.1. AVAILABILITY

The web interface of the device can be accessed in the network environment via a web browser on a computer, a smartphone or a tablet device. The web interface can be accessed only if the device is fully booted up. A brief signal sound indicates when the device is booted up and ready.

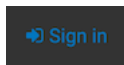


Figure 54: Web interface can be accessed

If the network connection to the device is lost, this is indicated by an icon for “Disconnected” on the right at the top.

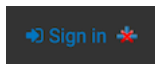


Figure 55: Web interface cannot be accessed

When the connection is restored, the icon for “Disconnected” disappears.

5.1.2. PRIVACY

Every page of the web interface provides a link to data privacy details in the footer.



Figure 56: Privacy

1 Copyright

2 Privacy

[1] Copyright: Shows copyright details.

[2] Privacy: Click on <https://www.commend.com/web/privacy-policy.html>, where Commend’s data privacy statement can be found.

The footer is omitted in the following screenshots.

5.1.3. MENU BAR

The following functions are available:

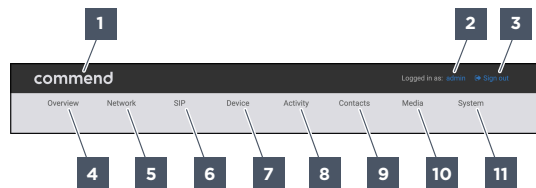


Figure 57: Menu bar

1 Commend	2 admin	3 Sign out
4 Overview	5 Network	6 SIP
7 Device	8 Activity	9 Contacts
10 Media	11 System	

[1] Commend: Open the **Overview** page.

[2] admin: Open the **Profile** page to edit user details. If a user other than the default user (“admin”) is logged in, the name of that user is shown instead.

[3] Sign out: Sign out the currently signed-in user.

[4] Overview: Open the following subpages:

Options:

- **Overview:** Shows information about the device.

[5] Network: Open the following subpages:

Options:

- **General:** Configure general device settings.
- **IPv4:** Configure the IPv4 settings.
- **IPv6:** Configure the IPv6 settings.
- **Advanced Services:** Configure advanced network settings.
- **HTTPS:** Manage HTTPS server certificates and HTTPS client CA certificates.
- **ONVIF:** Configure the ONVIF settings.

[6] SIP: Open the following subpages:

Options:

- **SIP:** Configure SIP connections.
- **Call Settings:** Configure the call behaviour of the device.
- **Advanced Settings:** Configure advanced SIP settings.
- **Certificates:** Manage SIP certificates and SIP Certificate Authority certificates.

[7] Device: Open the following subpages:

Options:

- **Device:** Configure the device settings.
- **Audio:** Configure the audio settings.
- **Video:** Configure the video settings.
- **Motion Detection:** Configure the motion detection function.
- **Advertising:** Configure advertisements.
- **IOs:** Configure the settings for an IP-CON.

[8] Activity: Open the following subpages:

Options:

- **Activity:** Configure action sequence triggers.
- **Actionbook:** Configure action sequences.

[9] **Contacts:** Open the following subpages:

Options:

- **Contacts:** Manage contacts.
- **Contact Management:** Configure the contact management settings.

[10] **Media:** Open the following subpages:

Options:

- **Audio Files:** Manage audio files.
- **Snapshots:** Manage snapshots.
- **Images:** Manage images.

[11] **System:** Open the following subpages:

Options:

- **System:** Configure the system settings.
- **Backup:** Manage backup files.
- **User Management:** Manage user profiles.
- **Codecs:** Manage audio codecs and video codecs.
- **Logging:** Manage log files.
- **SNMP:** Configure SNMP settings.
- **Remote Maintenance:** Configure remote maintenance for support purposes.

5.1.4. NOTIFICATION BOXES

Notification messages about modifications, confirmations and errors are shown in the bottom section of the web browser window.

Modification notifications

A modification message is shown whenever the configuration is changed. Most changes are not saved automatically. The modification message is shown until the modification is saved or discarded. If a different web interface page is opened after making changes, the notification box is hidden and those changes are discarded.



Figure 58: Change notice

1 Note text

2 Save

3 Discard

[1] **Note text:** Shows a reminder that changes have not been saved.

[2] **Save:** Save all modifications.

[3] **Discard:** Discard all modifications.

Confirmation notification

A confirmation message is shown if the current configuration has been saved.

Example: “Changes saved successfully.” or “Contacts imported successfully.”



Figure 59: Confirmation notice

- 1 Note text
- 2 Close

[1] Note text: Shows the notification message.

[2] Close: Close the confirmation notification box.

Error notification

If an error occurs, a notification to that effect is shown.

Example: “Invalid configuration!”, “Connection error!” or “Server error!”



Figure 60: Error message

- 1 Note text
- 2 Close

[1] Note text: Shows the notification message.

[2] Close: Close the error notification box.

5.1.5. ACTIVITIES AND ACTION SEQUENCES

Use activities to configure triggers for action sequences. The action sequences are executed automatically if the trigger conditions are met.

Example: An action sequence is triggered if a call to a specific contact is initiated.

Action sequences are used to configure actions in the form of logical command sequences. Action sequences activate system functions.

Example: The door opener is activated.

An activity triggers an action sequence as described below.

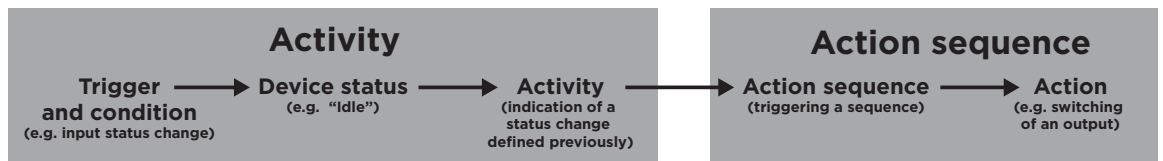


Figure 61: Activities and action sequences

Example: In the device state “Idle”, an intrusion sensor detects an input status change. An activity triggers an action sequence. The action sequence switches an output relay, activating an alarm system.

5.2. LANDING PAGE

The following functions are available:

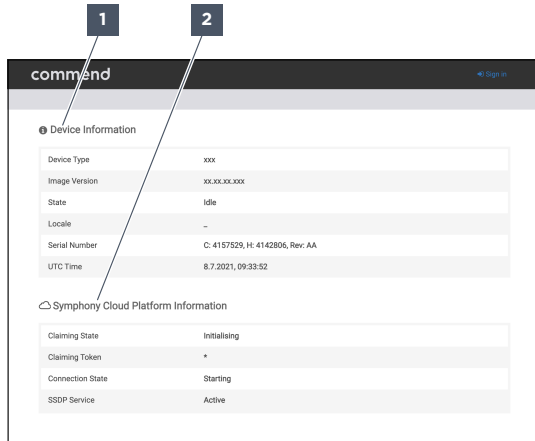


Figure 62: Landing page

- 1 Device Information
- 2 Symphony Cloud Platform Information

[1] **Device Information:** Shows the device details.

[2] **Symphony Cloud Platform Information:** Shows the details for the Symphony Cloud Platform.

5.2.1. DEVICE INFORMATION

The following functions are available:

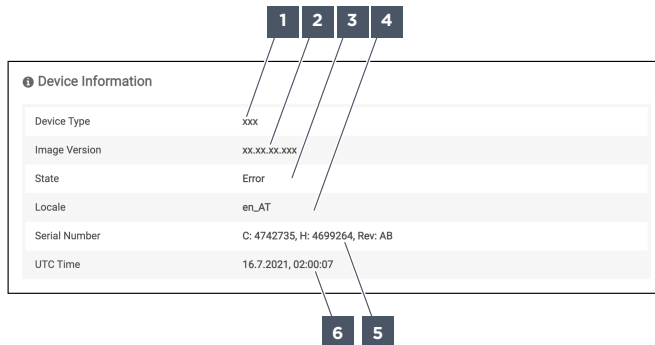


Figure 63: Overview - Device Information

- 1 Device Type
- 2 Image Version
- 3 State
- 4 Locale
- 5 Serial Number
- 6 UTC Time

[1] **Device Type:** Shows the device name.

[2] **Image Version:** Shows the software version.

[3] **State:** Shows the current device state.

At any one time, the device can be in one device state.

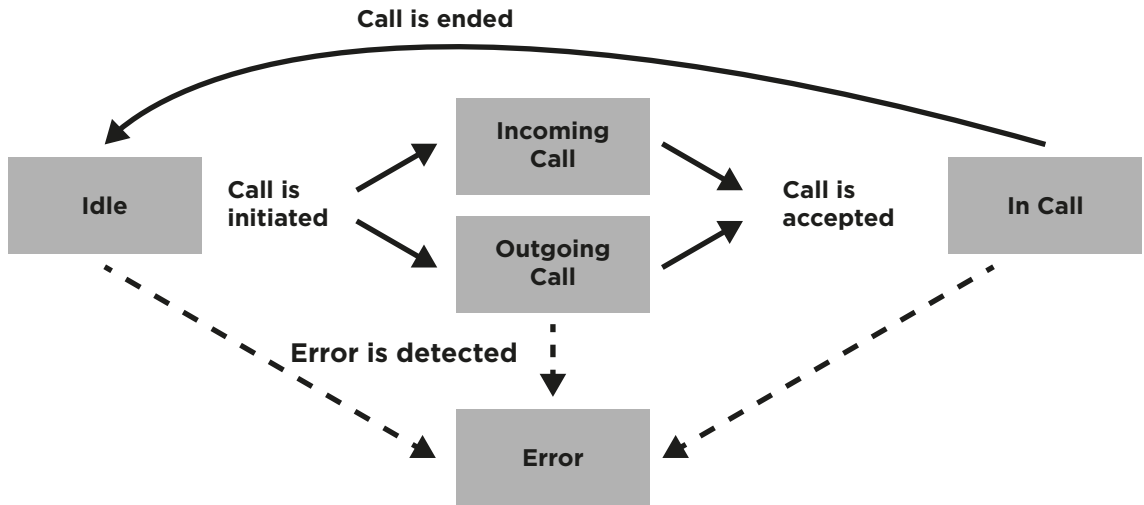


Figure 64: Device states

Options:

- **Idle:** The device is in this device state if neither a call is being established, nor a call has been established, nor the device is in the device state “Error”.
 - **Incoming call:** The device is in this device state if a call to the device is being established.
 - **Outgoing Call:** The device is in this device state if a call from the device is being established.
 - **In Call:** The device is in this device state if a call has been established. If the call is ended, the device switches to the device state “Idle”.
 - **Error:** The device is in this state if errors have been detected. If the errors are resolved or the configuration is changed, the device switches to the device state “Idle”.
- Example:** The connection to the SIP server is interrupted.

[4] Locale: Shows the device language and the device locale. The device language and the user language of the web interface can be configured independently of each other.

[5] Serial Number: Shows the serial numbers.

Information:

- **C:** Device serial number. For older devices, “N/A” is shown.
- **H:** Mainboard serial number.
- **Rev:** Hardware version.

[6] UTC Time: Shows the device time in the UTC format.

5.2.2. SYMPHONY CLOUD PLATFORM INFORMATION

The following functions are available:

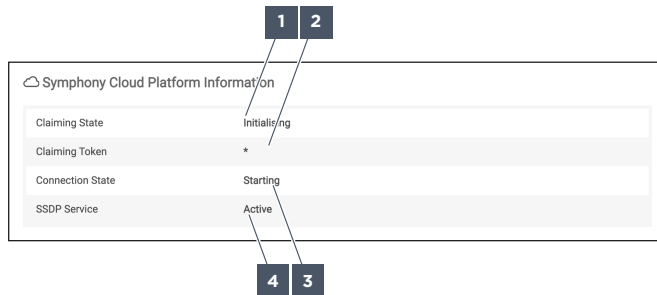


Figure 65: Overview – Symphony Cloud Platform Information

- 1** Claiming State
- 2** Claiming Token
- 3** Connection State

4 SSDP Service**5** SIP Connection State (not shown)

Symphony Cloud Platform Information This is shown only if a valid Commend certificate is available and **Symphony Cloud Platform enabled** is activated.

[1] Claiming State: Shows the device claiming state.

Options:

- **Initialising:** The device is not registered at the Symphony Cloud Platform.
- **Registered:** The device is connected to the Symphony Cloud Platform and is ready to be claimed by a user.
- **Claimed:** The device is claimed by a user. It can now be used with the Symphony Cloud Platform.

[2] Claiming Token: Shows "*" and the 4 last digits of the claiming token. The claiming token can be used to claim the device via the Symphony App.

[3] Connection State: Shows the state of the connection between the device and the Symphony Cloud Platform.

Options:

- **Initialising:** The device is not registered.
- **Registering:** The device is registering.
- **Registered:** The device is registered.
- **Registration error:** The device was unable to register.
- **Connecting:** The device is establishing a connection.
- **Reconnecting:** The device is re-establishing a previously interrupted connection.
- **Connected:** The device is connected.
- **Connection error:** The device was unable to establish a connection or the connection is interrupted.
- **Twin connecting:** The twin is establishing a connection.
- **Twin ready:** The twin is connected. The twin is receiving data from the Symphony Cloud Platform.
- **Twin error:** The twin was unable to establish a connection.
- **Device ready:** The device is ready to be used with the Symphony Cloud Platform.
- **No certificates:** The device has no certificates or no valid certificates. The device cannot be used with the Symphony Cloud Platform.
- **Disconnected:** There is no connection.
Example: Due to a reboot.

[4] SSDP Service: Shows the status of the SSDP service.

[5] SIP Connection State (not shown): Shows the state of the connection between the SIP server and the Symphony Cloud Platform. The SIP connection state is shown only if the device is connected to the Symphony Cloud Platform.

5.3. OVERVIEW

The following functions are available:

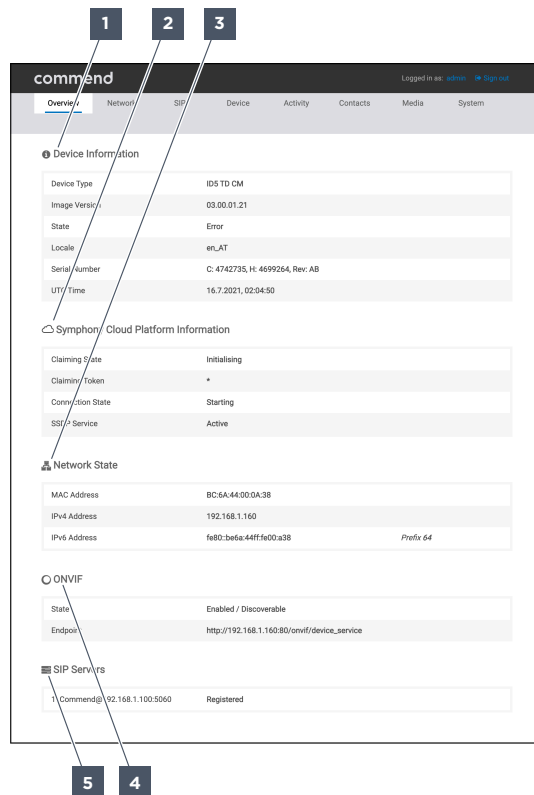


Figure 66: Overview

- 1** Device Information
- 2** Symphony Cloud Platform Information
- 3** Network State
- 4** ONVIF
- 5** SIP Servers

[1] Device Information: Shows the device details.

[2] Symphony Cloud Platform Information: Shows the details for the Symphony Cloud Platform.

[3] Network State: Shows the network details.

[4] ONVIF: Shows the ONVIF details.

[5] SIP Servers: Shows the SIP server details.

5.3.1. DEVICE INFORMATION

The following functions are available:

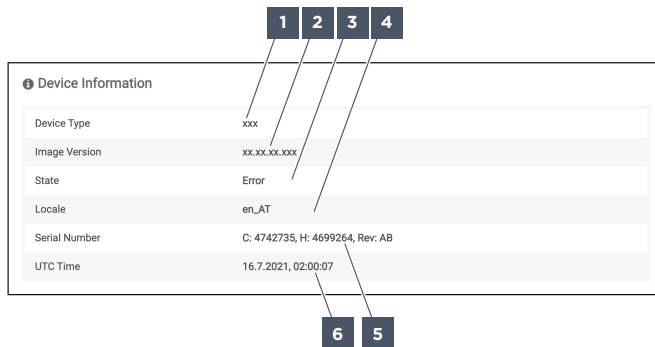


Figure 67: Overview – Device Information

- 1 Device Type
- 2 Image Version
- 3 State
- 4 Locale
- 5 Serial Number
- 6 UTC Time

[1] Device Type: Shows the device name.

[2] Image Version: Shows the software version.

[3] State: Shows the current device state.

At any one time, the device can be in one device state.

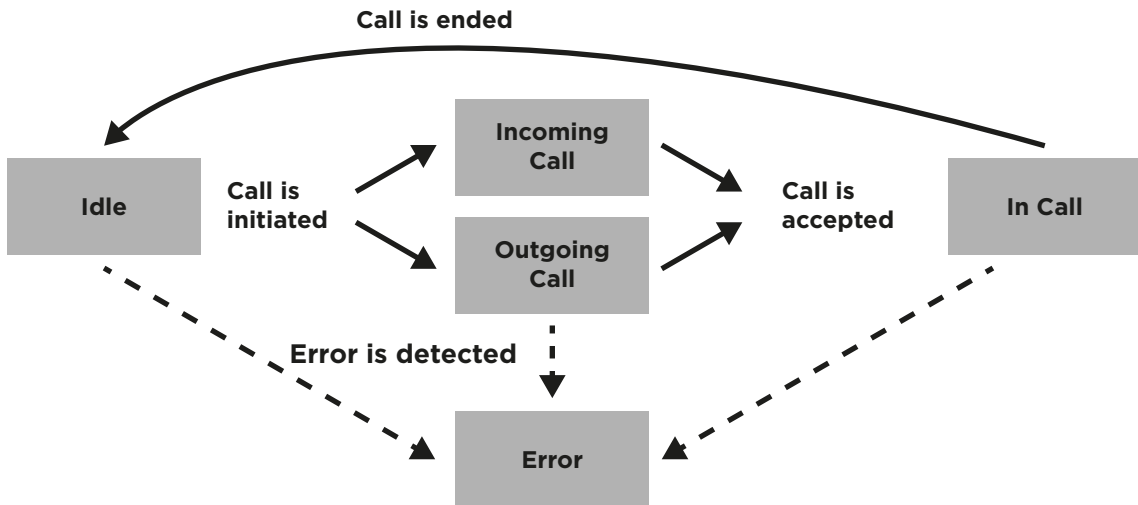


Figure 68: Device states

Options:

- **Idle:** The device is in this device state if neither a call is being established, nor a call has been established, nor the device is in the device state “Error”.
- **Incoming call:** The device is in this device state if a call to the device is being established.
- **Outgoing Call:** The device is in this device state if a call from the device is being established.
- **In Call:** The device is in this device state if a call has been established. If the call is ended, the device switches to the device state “Idle”.
- **Error:** The device is in this state if errors have been detected. If the errors are resolved or the configuration is changed, the device switches to the device state “Idle”.

Example: The connection to the SIP server is interrupted.

[4] Locale: Shows the device language and the device locale. The device language and the user language of the web interface can be configured independently of each other.

[5] **Serial Number:** Shows the serial numbers.

Information:

- **C:** Device serial number. For older devices, “N/A” is shown.
- **H:** Mainboard serial number.
- **Rev:** Hardware version.

[6] **UTC Time:** Shows the device time in the UTC format.

5.3.2. SYMPHONY CLOUD PLATFORM INFORMATION

The following functions are available:

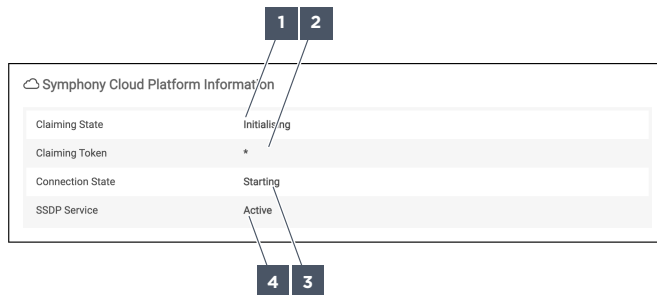


Figure 69: Overview – Symphony Cloud Platform Information

- | | | | | | |
|---|----------------|---|----------------------------------|---|------------------|
| 1 | Claiming State | 2 | Claiming Token | 3 | Connection State |
| 4 | SSDP Service | 5 | SIP Connection State (not shown) | | |

Symphony Cloud Platform Information This is shown only if a valid Commend certificate is available and **Symphony Cloud Platform enabled** is activated.

[1] **Claiming State:** Shows the device claiming state.

Options:

- **Initialising:** The device is not registered at the Symphony Cloud Platform.
- **Registered:** The device is connected to the Symphony Cloud Platform and is ready to be claimed by a user.
- **Claimed:** The device is claimed by a user. It can now be used with the Symphony Cloud Platform.

[2] **Claiming Token:** Shows “*” and the 4 last digits of the claiming token. The claiming token can be used to claim the device via the Symphony App.

[3] **Connection State:** Shows the state of the connection between the device and the Symphony Cloud Platform.

Options:

- **Initialising:** The device is not registered.
- **Registering:** The device is registering.
- **Registered:** The device is registered.
- **Registration error:** The device was unable to register.
- **Connecting:** The device is establishing a connection.
- **Reconnecting:** The device is re-establishing a previously interrupted connection.
- **Connected:** The device is connected.
- **Connection error:** The device was unable to establish a connection or the connection is interrupted.
- **Twin connecting:** The twin is establishing a connection.
- **Twin ready:** The twin is connected. The twin is receiving data from the Symphony Cloud Platform.

- **Twin error:** The twin was unable to establish a connection.
- **Device ready:** The device is ready to be used with the Symphony Cloud Platform.
- **No certificates:** The device has no certificates or no valid certificates. The device cannot be used with the Symphony Cloud Platform.
- **Disconnected:** There is no connection.
Example: Due to a reboot.

[4] SSDP Service: Shows the status of the SSDP service.

[5] SIP Connection State (not shown): Shows the state of the connection between the SIP server and the Symphony Cloud Platform. The SIP connection state is shown only if the device is connected to the Symphony Cloud Platform.

5.3.3. NETWORK STATE

The following functions are available:

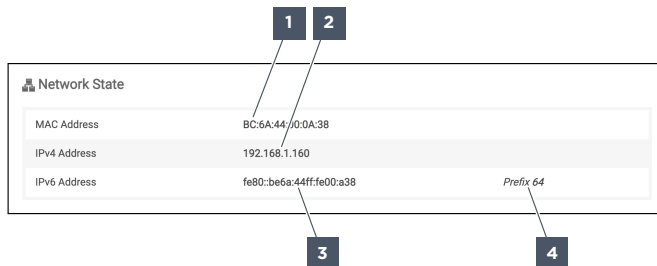


Figure 70: Overview – Network State

- 1 MAC Address
- 2 IPv4 Address
- 3 IPv6 Address
- 4 Prefix

[1] MAC Address: Shows the MAC address to identify the device.

[2] IPv4 Address: Shows the IPv4 address of the device.

[3] IPv6 Address: Shows the IPv6 address of the device.

[4] Prefix: Shows the prefix of the IPv6 address.

5.3.4. ONVIF

The following functions are available:

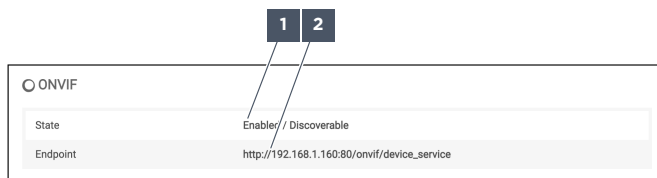


Figure 71: Overview – ONVIF

- 1 State
- 2 Endpoint

[1] State: Shows the ONVIF state.

Options

- **Disabled/Undiscoverable:** The ONVIF function is deactivated. The device cannot be discovered through the ONVIF discovery function.
- **Disabled/Discoverable:** The ONVIF function is deactivated. The device can be discovered through the ONVIF discovery function.

- **Enabled/Undiscoverable:** The ONVIF function is activated. The device cannot be discovered through the ONVIF discovery function.
- **Enabled/Discoverable:** The ONVIF function is activated. The device can be discovered through the ONVIF discovery function.

[2] **Endpoint:** Shows the URL for accessing the ONVIF service.

5.3.5. SIP SERVERS

The following functions are available:



Figure 72: Overview – SIP Servers

- 1 SIP Connection 2 SIP Connection State

Shows all configured SIP connections.

[1] **SIP Connection:** Shows the type of SIP connection. Peer-to-peer connections are shown as “Registrarless”. For SIP server connections, the information shown includes the following items:

Information:

- User ID
- SIP server IP address/host name
- SIP server port

[2] **SIP Connection State:** Shows the SIP connection state.

Options:

- **Unknown:** The connection state is unknown.
Example: When booting the device.
- **Registering:** The device is registering on the SIP server.
- **Registered:** The device is registered on the SIP server.
- **Logging out:** The device is logging out of the SIP server.
- **Logged out:** The device has logged out of the SIP server.
- **Idle:** When in redundancy mode “Sequential”, the device is not connected to the low-priority SIP server. The device is connected to a higher-priority SIP server.
- **Connecting:** The device is establishing a connection to the SIP server.
- **Available:** When in redundancy mode “Cisco”, the device can access a low-priority SIP server. The device is connected to a higher-priority SIP server.
- **Connection failed:** The device is unable to connect to the SIP server.
- **Authentication failed:** Authentication on the SIP server has failed due to an invalid user ID, an invalid password or an invalid authentication ID.
- **Error:** A connection error has occurred.

5.4. GENERAL

The following functions are available:

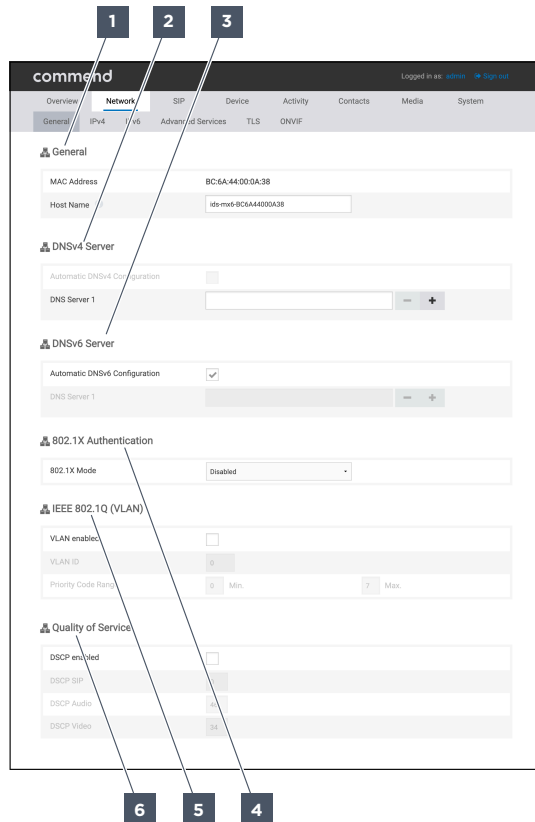


Figure 73: General

- | | | |
|--------------------------------|-----------------------------|-----------------------------|
| 1 General | 2 DNSv4 Server | 3 DNSv6-Server |
| 4 802.1X-Authentication | 5 IEEE 802.1Q (VLAN) | 6 Quality of Service |

[1] General: Shows the MAC address and the user can configure the host name.

[2] DNSv4 Server: Configure the DNSv4 server.

[3] DNSv6 Server: Configure the DNSv6 server.

[4] 802.1X Authentication: Configure the authentication via 802.1X.

[5] IEEE 802.1Q (VLAN): Configure the VLAN function.

[6] Quality of Service: Configure the prioritisation of IP data packets.

5.4.1. GENERAL

The following functions are available:

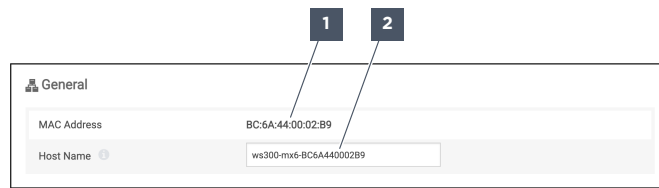


Figure 74: General - General

- 1** MAC Address **2** Host Name

[1] MAC Address: Shows the MAC address for identifying the device.

[2] Host Name: Enter the network host name of the device. If a new network host name is configured, the device must be restarted. If no network host name is configured and if the configuration is saved, the default network host name is used. The network host name is sent using the “DHCP Option 12” function. Default: “<device type>-<processor model>-<MAC address>”.

5.4.2. DNSV4 SERVER

The following functions are available:

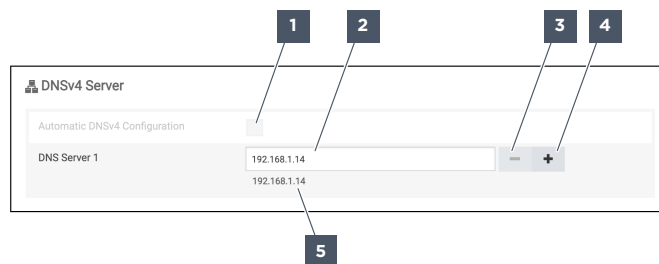


Figure 75: General - DNSv4 Server

- 1** Automatic DNSv4 Configuration **2** DNS Server 1 **3** Delete DNS Server
4 Add DNS Server **5** Current value

[1] Automatic DNSv4 Configuration: Activate to automatically assign an IPv4 address using a DNS server. The DHCP server must be in the same network as the device. The DHCP server must be available via a configured DNSv4 server. Default: activated.

[2] DNS Server 1: Enter the IPv4 address of the DNSv4 server. Default: empty.

[3] Delete DNS Server: Delete the DNSv4 server.

[4] Add DNS Server: Add a DNSv4 server.

[5] Current value: Shows the current configuration. This information serves as a configuration aid. If this value and the value in the corresponding field differ, this may indicate a faulty network configuration.

5.4.3. DNSV6 SERVER

The following functions are available:

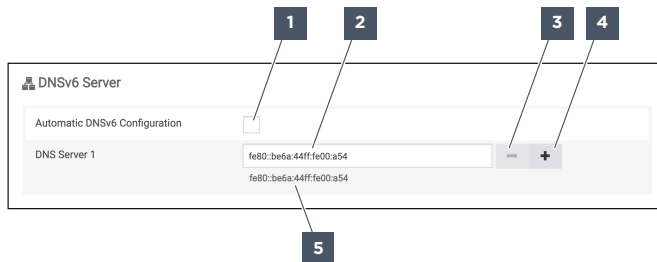


Figure 76: General - DNSv6 Server

- 1 Automatic DNSv6 Configuration
- 2 DNS Server 1
- 3 Delete DNS Server
- 4 Add DNS Server
- 5 Current Value

[1] Automatic DNSv6 Configuration: Activate to automatically assign an IPv6 address using a DNS server. The DHCP server must be in the same network as the device. The DHCP server must be available via a configured DNSv6 server. Default: activated.

[2] DNS Server 1: Enter the IPv6 address of the DNSv6 server. Default: empty.

[3] Delete DNS Server: Delete the DNSv6 server.

[4] Add DNS Server: Add a DNSv6 server.

[5] Current value: Shows the current configuration. This information serves as a configuration aid. If this value and the value in the corresponding field differ, this may indicate a faulty network configuration.

5.4.4. 802.1X AUTHENTICATION

The following functions are available:



Figure 77: General - 802.1X Authentication "Disabled"

- 1 802.1X Mode

[1] 802.1X Mode: Select the 802.1X authentication mode. Default: "Disabled".

Options:

- **Disabled:** 802.1X authentication is deactivated.
- **EAP-MD5:** 802.1X authentication is carried out with the EAP-MD5 method.
- **EAP-TLS:** 802.1X authentication is carried out with the EAP-TLS method. An available public key infrastructure is required to use the EAP-TLS method.

Figure 78: General – 802.1X-Authentication „EAP-MD5“

- 1** 802.1X Mode **2** Username **3** Password

[1] 802.1X Mode: Select the 802.1X authentication mode. Default: “Disabled”.

Options:

- **Disabled:** 802.1X authentication is deactivated.
- **EAP-MD5:** 802.1X authentication is carried out with the EAP-MD5 method.
- **EAP-TLS:** 802.1X authentication is carried out with the EAP-TLS method. An available public key infrastructure is required to use the EAP-TLS method.

[2] Username: Enter the user name.

[3] Password: Enter the password.

Figure 79: General – 802.1X Authentication „EAP-TLS“

- 1** 802.1X Mode **4** Identification **5** Client Key
6 Client Key Password **7** Client Certificate **8** CA Certificate (optional)

[1] 802.1X Mode: Select the 802.1X authentication mode. Default: “Disabled”.

Options:

- **Disabled:** 802.1X authentication is deactivated.
- **EAP-MD5:** 802.1X authentication is carried out with the EAP-MD5 method.
- **EAP-TLS:** 802.1X authentication is carried out with the EAP-TLS method. An available public key infrastructure is required to use the EAP-TLS method.

[4] Identification: Enter the device name.

[5] Client Key: Upload a client key for the client certificate.

[6] Client Key Password: Enter the password for the client key. The password is optional.

[7] Client Certificate: Upload a client certificate that is issued by the certificate authority.

[8] CA Certificate (optional): Upload a certificate authority certificate. The certificate authority certificate is used to check the validity of the authentication server.

5.4.5. IEEE 802.1Q (VLAN)

The following functions are available:

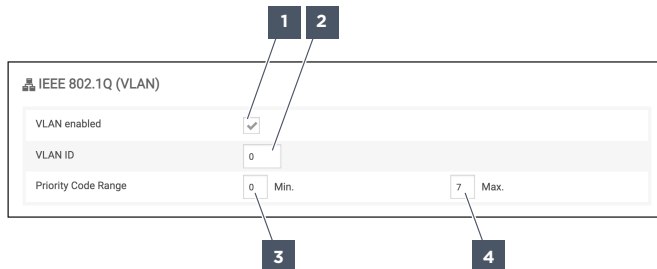


Figure 80: General - IEEE 802.1Q (VLAN)

- 1 VLAN enabled
- 2 VLAN ID
- 3 Min.
- 4 Max.

The VLAN functions cannot be used together with an IP-CON.

[1] VLAN enabled: Activate to ensure that the VLAN function can be used. Default: deactivated.

[2] VLAN ID: Enter the ID of the VLAN that the device is a part of. Range of values: "0" to "4094". Default: "0".

[3] Min.: Adjust the minimum priority of the priority code point. The network interface uses this parameter to prioritise the network communication in the VLAN. Range of values: "0" to "7". Default: "0".

[4] Max.: Adjust the maximum priority of the priority code point. The network interface uses this parameter to prioritise the network communication in the VLAN. Range of values: "0" to "7". Default: "7".

5.4.6. QUALITY OF SERVICE

The following functions are available:

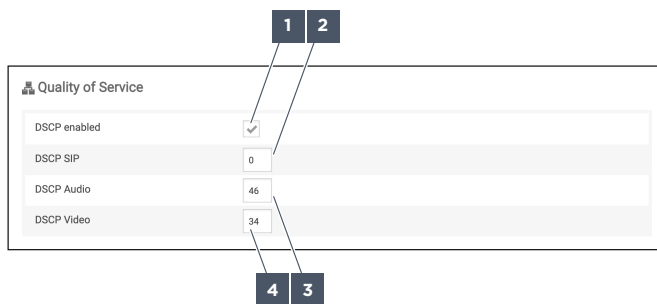


Figure 81: Allgemein - Quality of Service

- 1 DSCP enabled
- 2 DSCP SIP
- 3 DSCP Audio
- 4 DSCP Video

[1] DSCP enabled: Activate to use DiffServ for prioritising IP data packets. Default: deactivated.

[2] DSCP SIP: Enter the priority of SIP data packets. Range of values: "0" to "56". Default: "0".

[3] DSCP Audio: Enter the priority of RTP audio data packets. Range of values: "0" to "56". Default: "46".

[4] DSCP Video: Enter the priority of RTP video data packets. Range of values: “0” to “56”. Default: “34”.

5.5. IPV4

The following functions are available:

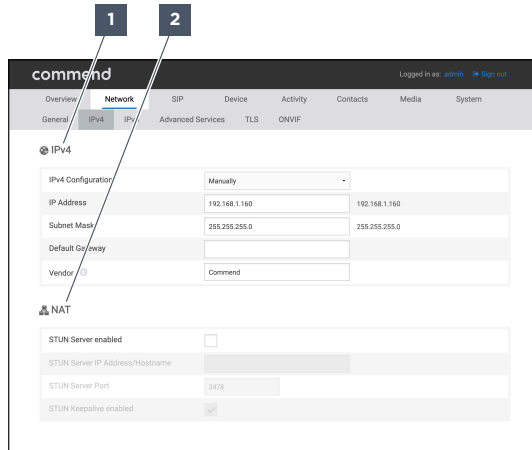


Figure 82: IPv4

1 IPv4

2 NAT

[1] IPv4: Configure the IPv4 settings.

[2] NAT: Configure the STUN server.

5.5.1. IPV4

The following functions are available:



Figure 83: IPv4 – IPv4 „Disabled“

1 IPv4 Configuration

2 Vendor

[1] IPv4 Configuration: Select the IPv4 mode. Default: “DHCP”.

Options:

- **Disabled:** The IPv4 settings are deactivated. The device does not have an IPv4 address. The device can be accessed only via an IPv6 address.
- **DHCP:** The IPv4 settings are requested from a DHCP server. The IPv4 settings cannot be configured manually.
- **Manual:** The IPv4 address can be configured manually.

[2] Vendor: Enter the vendor class identifier specified in “DHCP Option 60”. If a new vendor class identifier is configured, the device must be restarted. Default: “Commend”.

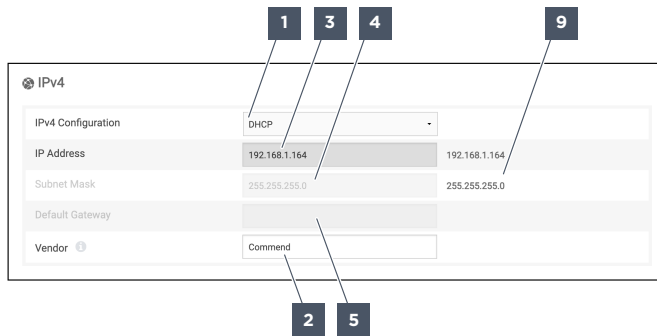


Figure 84: IPv4 - IPv4 „DHCP“

- 1 IPv4 Configuration
- 2 Vendor
- 3 IP Address
- 4 Subnet Mask
- 5 Default Gateway
- 9 Current value

[1] IPv4 Configuration: Select the IPv4 mode. Default: “DHCP”.

Options:

- **Disabled:** The IPv4 settings are deactivated. The device does not have an IPv4 address. The device can be accessed only via an IPv6 address.
- **DHCP:** The IPv4 settings are requested from a DHCP server. The IPv4 settings cannot be configured manually.
- **Manual:** The IPv4 address can be configured manually.

[2] Vendor: Enter the vendor class identifier specified in “DHCP Option 60”. If a new vendor class identifier is configured, the device must be restarted. Default: “Commend”.

[3] IP Address: Shows the IPv4 address.

[4] Subnet Mask: Shows the subnet mask.

[5] Default Gateway: Shows the default gateway.

[9] Current Value: Shows the current configuration. This information serves as a configuration aid. If this value and the value in the corresponding field differ, this may indicate a faulty network configuration.

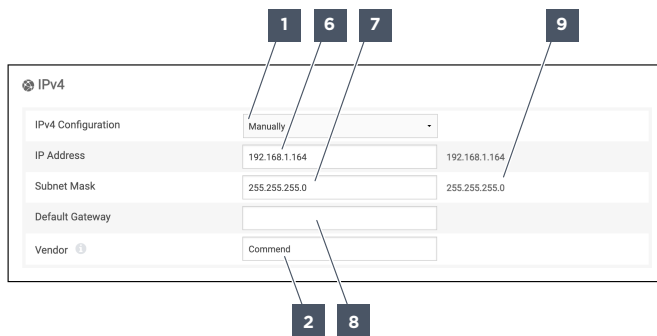


Figure 85: IPv4 - IPv4 „Manual“

- 1 IPv4 Configuration
- 2 Vendor
- 6 IP Address
- 7 Subnet Mask
- 8 Default Gateway
- 9 Current Value

[1] IPv4 Configuration: Select the IPv4 mode. Default: “DHCP”.

Options:

- **Disabled:** The IPv4 settings are deactivated. The device does not have an IPv4 address. The device can be accessed only via an IPv6 address.
- **DHCP:** The IPv4 settings are requested from a DHCP server. The IPv4 settings cannot be configured manually.
- **Manual:** The IPv4 address can be configured manually.

[2] Vendor: Enter the vendor class identifier specified in “DHCP Option 60”. If a new vendor class identifier is configured, the device must be restarted. Default: “Commend”.

[6] IP Address: Enter the IPv4 address. If a new IP address is configured, the device must be restarted. By default, the IPv4 address is generated automatically and randomly. Default: “169.xxx.xxx.xxx”.

⚠ CAUTION

Multiple allocation of the same IP address

IP address conflict and malfunction

Use only unique IP addresses within the network.

[7] Subnet Mask: Enter the subnet mask. Default: “255.255.255.0”.

[8] Default Gateway: Enter the IPv6 address of the router or the default gateway.

[9] Current Value: Shows the current configuration. This information serves as a configuration aid. If this value and the value in the corresponding field differ, this may indicate a faulty network configuration.

5.5.2. NAT

The following functions are available:

The screenshot shows the NAT configuration page with the following fields and callouts:

- Callout 1: STUN Server enabled (checkbox checked)
- Callout 2: STUN Server IP Address/Hostname (text field)
- Callout 3: STUN Server Port (text field with value 3478)
- Callout 4: STUN Keepalive enabled (checkbox checked)

Figure 86: IPv4 - NAT

- 1 STUN Server enabled
- 2 STUN Server IP Address/Hostname
- 3 STUN Server Port
- 4 STUN Keepalive enabled

[1] STUN Server enabled: Activate to ensure that the STUN function can be used. Default: deactivated.

Recommendation: Activate this function if the SIP server does not have a proxy function.

[2] STUN Server IP Address/Hostname: Enter the IP address or the host name of the STUN server. Default: empty.

[3] STUN Server Port: Enter the port number of the STUN server. Default: “3478”.

[4] STUN Keepalive enabled: Activate to keep the STUN function alive after penetrating through NAT routers. Default: activated.

5.6. IPV6

The following functions are available:

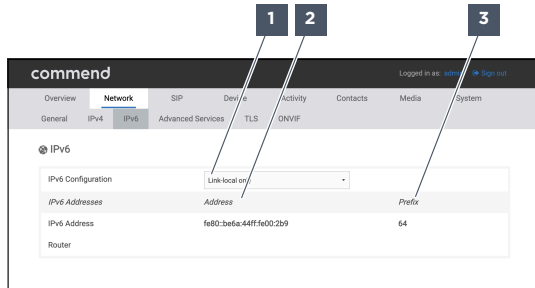


Figure 87: IPv6 “Link-local only”

- 1 IPv6 Configuration
- 2 Address
- 3 Prefix

The device has always a link-local address, which cannot be modified. The link-local IPv6 address is derived from the MAC address. If the IPv4 settings are deactivated or if there is an IP address conflict, the device can be accessed in the local network via the link-local IPv6 address.

[1] IPv6 Configuration: Select the IPv6 mode. Default: “Automatic”.

Options:

- **Link-local only:** The device has an IPv6 address only for the local network.
- **Automatic:** In addition to the link-local IPv6 address, the device automatically obtains global IPv6 addresses. The global IPv6 addresses are generated via a DHCPv6 server or via SLAAC.
- **Manual:** In addition to the link-local IPv6 address, additional IPv6 addresses can be configured manually.

[2] Address: Shows the link-local IPv6 address.

[3] Prefix: Shows the prefix of the IPv6 address.

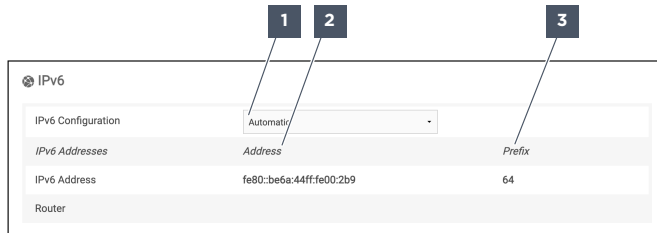


Figure 88: IPv6 „Automatic“

- 1 IPv6 Configuration
- 2 Address
- 3 Prefix

[1] IPv6 Configuration: Select the IPv6 mode. Default: “Automatic”.

Options:

- **Link-local only:** The device has an IPv6 address only for the local network.
- **Automatic:** In addition to the link-local IPv6 address, the device automatically obtains global IPv6 addresses. The global IPv6 addresses are generated via a DHCPv6 server or via SLAAC.
- **Manual:** In addition to the link-local IPv6 address, additional IPv6 addresses can be configured manually.

[2] Address: Shows the IPv6 addresses.

[3] **Prefix:** Shows the prefixes of the IPv6 addresses.



Figure 89: IPv6 „Manual“

1	IPv6 Configuration	2	Address	3	Prefix
4	Current Value	5	Delete	6	Add
7	Router				

[1] **IPv6 Configuration:** Select the IPv6 mode. Default: “Automatic”.

Options:

- **Link-local only:** The device has an IPv6 address only for the local network.
- **Automatic:** In addition to the link-local IPv6 address, the device automatically obtains global IPv6 addresses. The global IPv6 addresses are generated via a DHCPv6 server or via SLAAC.
- **Manual:** In addition to the link-local IPv6 address, additional IPv6 addresses can be configured manually.

[2] **Address:** Shows the link-local IPv6 address.

[3] **Prefix:** Shows the prefix of the IPv6 address.

[4] **Current Value:** Shows the current configuration. This information serves as a configuration aid. If this value and the value in the corresponding field differ, this may indicate a faulty network configuration.

[5] **Delete:** Delete the IPv6 address and the prefix.

[6] **Add:** Add an IPv6 address and a prefix.

[7] **Router:** Enter the IPv6 address of a router that is part of the same network.

5.7. ADVANCED SERVICES

The following functions are available:

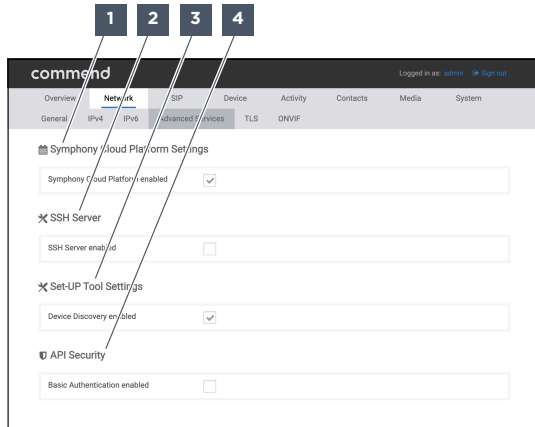


Figure 90: Advanced Services

- 1 Symphony Cloud Platform
- 2 SSH Server
- 3 Set-UP Tool Settings
- 4 API Security

[1] Symphony Cloud Platform Settings: Configure the connection to the Symphony Cloud Platform.

[2] SSH Server: Configure the SSH server service.

[3] Set-UP Tool Settings: Configure the discovery function for the Commend Set-UP tool.

[4] API Security: Configure the token authentication.

5.7.1. SYMPHONY CLOUD PLATFORM SETTINGS

The following functions are available:

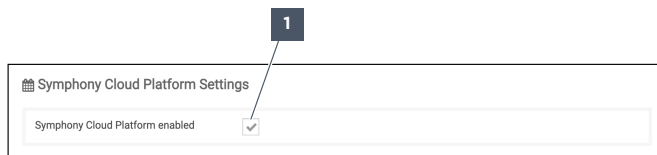


Figure 91: Advanced Services – Symphony Cloud Platform Settings

- 1 Symphony Cloud Platform enabled

When the device is connected to the Symphony Cloud Platform, it cannot be accessed via the web interface. Only the landing page of the web interface is shown (see "Landing page", page 66). The device can be managed only via the Symphony Cloud Platform.

[1] Symphony Cloud Platform enabled: Activate to allow the device to connect to the Symphony Cloud Platform. The device is trying to establish a connection to the Symphony Cloud Platform. In case of an incompatible hardware version or software version, this function is greyed out. Default: activated.

5.7.2. SSH SERVER

The following functions are available:

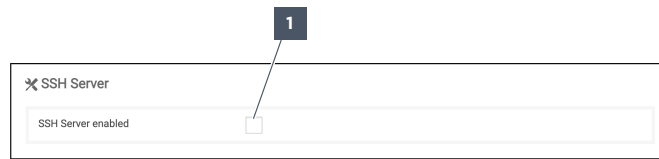


Figure 92: Advanced Services – SSH-Server

1 SSH Server enabled

[1] SSH Server enabled: Activate to allow the use of the SSH server service. The SSH server service allows access to the console of the device. Default: disabled.

Example: Activate this function for on-site support or remote maintenance.

5.7.3. SET-UP TOOL SETTINGS

The following functions are available:

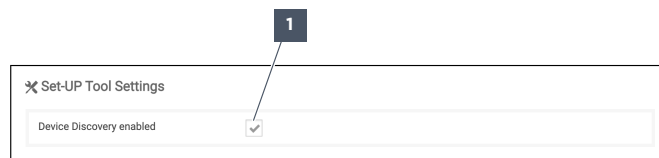


Figure 93: Advanced Services – Set-UP Tool Settings

1 Device Discovery enabled

[1] Device Discovery enabled: Activate to allow the use of the discovery function for the Commend Set-UP tool. If this function is deactivated, no mDNS broadcast messages are sent. If this function is deactivated, the web interface of the device cannot be accessed via zero-conf. Default: activated.

5.7.4. API SECURITY

The following functions are available:

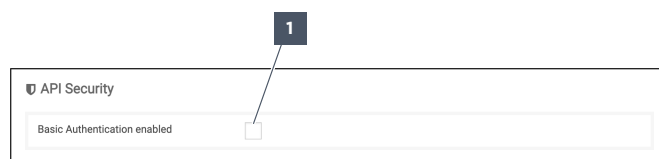


Figure 94: Advanced Services – API Security

1 Basic Authentication enabled

The device uses the digest authentication mode.

[1] Basic Authentication enabled Activate to use the basic authentication mode and the digest authentication mode in parallel. The basic authentication mode allows the use of any of the tokens that are configured for the device. Default: deactivated.

Recommendations:

- Use the same configuration for all devices that are authenticated via tokens.
- For IT security reasons, activate the basic authentication mode only if the device needs to communicate with legacy devices that do not support digest authentication.

5.8. TLS

The following functions are available:

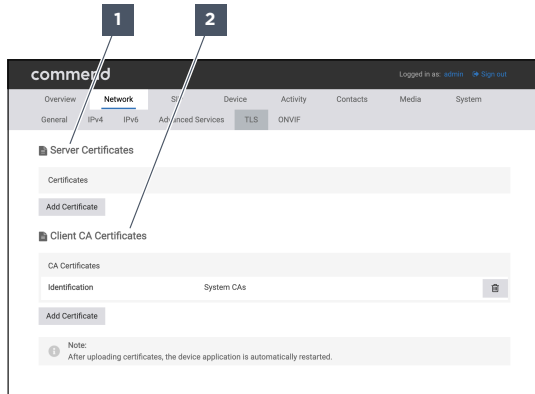


Figure 95: TLS

- 1 Server Certificates
- 2 Client CA Certificates

[1] Server Certificates: Manage the server certificates.

[2] Client CA Certificates: Manage the client certificate authority certificates.

5.8.1. SERVER CERTIFICATES

The following functions are available:

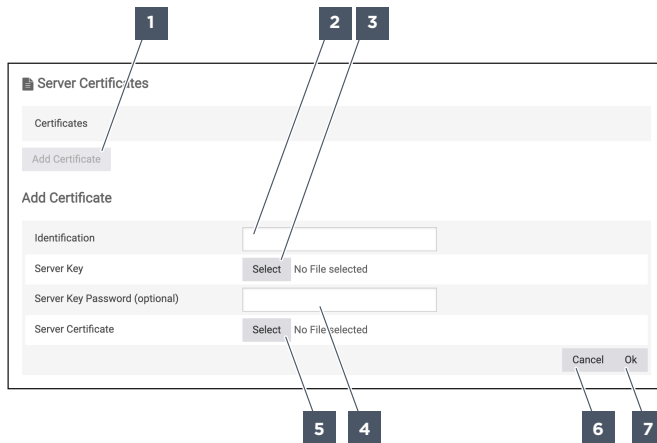


Figure 96: TLS - Server Certificates

- 1 Add Certificate
- 2 Identification
- 3 Server Key
- 4 Server Key Password (optional)
- 5 Server Certificate
- 6 Cancel
- 7 Ok

Server certificates verify the connection between the device and a web browser.

Address bar of the web browser without server certificate:

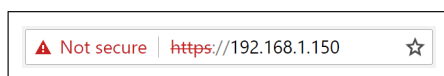


Figure 97: Web browser "Not secure"

Address bar of the web browser with server certificate:

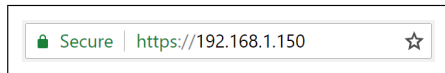


Figure 98: Web browser “Secure”

[1] Add Certificate: Add a new server certificate. The device can only use one server certificate. The existing server certificate is overwritten by adding a new server certificate.

[2] Identification: Enter a name for the server certificate.

[3] Server Key: Upload the server key for the server certificate.

Recommendation: Upload server key in format KEY or PEM.

[4] Server Key Password (optional): Enter the password for the server key. The password is optional.

[5] Server Certificate: Upload the server certificate. The server certificate must be formatted in the X.509 standard.

Recommendation: Upload server certificates in format CERT, CRT, DER or PEM.

[6] Cancel: Cancel and do not add a server certificate.

[7] OK: Add the server certificate.

5.8.2. CLIENT CA CERTIFICATES

The following functions are available:

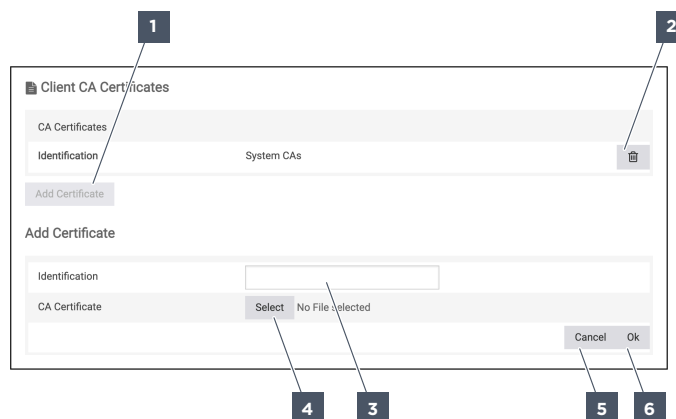


Figure 99: TLS – Client CA Certificates

- | | | |
|--------------------------|-----------------------------|-------------------------|
| 1 Add Certificate | 2 Delete certificate | 3 Identification |
| 4 CA Certificate | 5 Cancel | 6 Ok |

Client certificate authority certificates authenticate access to the device from other devices.

Example: For remote control via HTTP GET actions.

[1] Add Certificate: Add a client certificate authority certificate. The device already has a collection of certificate authority certificates (“system CAs”) when it leaves the factory.

[2] Delete certificate: Delete the client certificate authority certificate. The certificate “System CAs” can only be restored by restoring the factory settings.

Recommendation: Do not delete the certificate “System CAs”.

[3] Identification: Enter a name for the client certificate authority certificate.

[4] CA Certificate: Upload a client certificate authority certificate. The client certificate authority certificate must be formatted in the X.509 standard.

Recommendation: Upload client certificate authority certificates in format CER, CRT, DER or PEM.

[5] Cancel: Cancel and do not add a client certificate authority certificate.

[6] OK: Add the client certificate authority certificate.

5.9. ONVIF

The following functions are available:

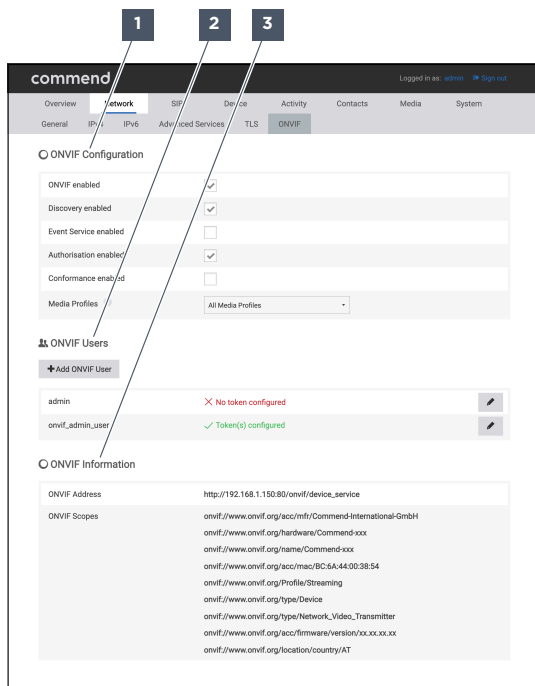


Figure 100: ONVIF

- 1** ONVIF Configuration
- 2** ONVIF Users
- 3** ONVIF Information

The device provides ONVIF video streams with the following properties.

Features

- **Resolution:** 320 x 240, 640 x 480, 800 x 600, 1024 x 768, 1280 x 960 pixels
- **Codecs:** MJPEG and H.264

ONVIF is provided as Profile S (standard ONVIF security mechanism). For further information on the integration of the device into a VMS system (video management software), see manual “ONVIF Configuration”.

[1] ONVIF Configuration: Configure the ONVIF function.

[2] ONVIF Users: Manage the users with ONVIF permissions.

[3] ONVIF Information: Shows the ONVIF URIs.

5.9.1. ONVIF CONFIGURATION

The following functions are available:

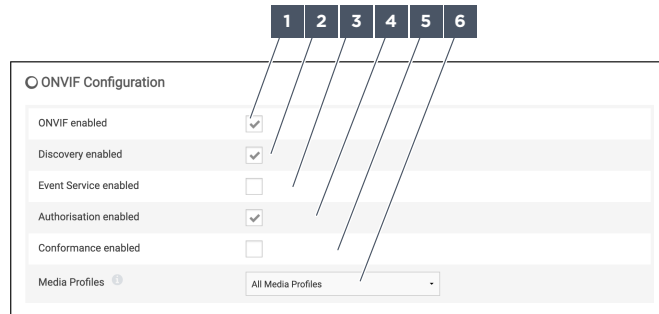


Figure 101: ONVIF - ONVIF Configuration

- | | | |
|--------------------------------|------------------------------|--------------------------------|
| 1 ONVIF enabled | 2 Discovery enabled | 3 Event Service enabled |
| 4 Authorisation enabled | 5 Conformance enabled | 6 Media Profiles |

[1] ONVIF enabled: Activate to ensure that the ONVIF function can be used. Default: deactivated.

[2] Discovery enabled: Activate to ensure that the ONVIF discovery function for compatible devices can be used. The device responds to ONVIF probe messages. The device sends “hello” messages after a restart. Default: activated.

Recommendation: Deactivate this function if the device is integrated into a VMS system. The device does not respond to ONVIF probe messages from 3rd-party systems.

[3] Event Service enabled: Activate to send ONVIF events automatically. Default: deactivated.

[4] Authorisation enabled: Activate to ensure that ONVIF authorisation with tokens can be used. When a VMS system wants to access the ONVIF functions of the device, a user with tokens is required. This user must have the required ONVIF permissions assigned to them. Default: deactivated.

[5] Conformance enabled: Activate to ensure compliance with ONVIF Profile S. If the device is restored to its factory settings using ONVIF, the functions **[1] ONVIF enabled** and **[2] Discovery enabled** are automatically activated. If this function is activated, a confirmation dialogue appears. If this function is not activated, the ONVIF function is deactivated after the device is restored to the factory settings (see “System”, page 161). Default: deactivated.

Recommendation: Activate this function for ONVIF tests in connection with the user “onvif_admin_user”.

[6] Media Profiles: Select the ONVIF media profile to be sent to the VMS system on request. An option other than “All Media Profiles” is required if the VMS system can process only one ONVIF media profile. Default: “All Media Profiles”.

Options:

- **All Media Profiles:** All ONVIF media profiles are sent sequentially in ascending order of resolution first as H.264 and then in ascending order of resolution as MJPEG.
- **1280x960, H.264:** Only the ONVIF media profile with a resolution of 1280 x 960 pixels is sent in the H.264 format.
- **1024x768, H.264:** Only the ONVIF media profile with a resolution of 1024 x 768 pixels is sent in the H.264 format.
- **800x600, H.264:** Only the ONVIF media profile with a resolution of 800 x 600 pixels is sent in the H.264 format.
- **640x480, H.264:** Only the ONVIF media profile with a resolution of 640 x 480 pixels is sent in the H.264 format.
- **320x240, H.264:** Only the ONVIF media profile with a resolution of 320 x 240 pixels is sent in the H.264 format.
- **1280x960, MJPEG:** Only the ONVIF media profile with a resolution of 1280 x 960 pixels is sent in the MJPEG format.

- **1024x768, MJPEG:** Only the ONVIF media profile with a resolution of 1024 x 768 pixels is sent in the MJPEG format.
- **800x600, MJPEG:** Only the ONVIF media profile with a resolution of 800 x 600 pixels is sent in the MJPEG format.
- **640x480, MJPEG:** Only the ONVIF media profile with a resolution of 640 x 480 pixels is sent in the MJPEG format.
- **320x240, MJPEG:** Only the ONVIF media profile with a resolution of 320 x 240 pixels is sent in the MJPEG format.

5.9.2. ONVIF USERS

The following functions are available:

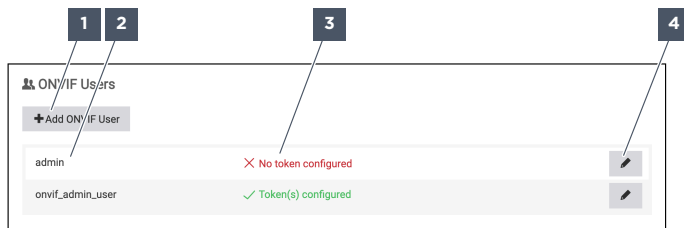


Figure 102: ONVIF – ONVIF User

- 1 Add ONVIF User
- 2 User
- 3 Token
- 4 Edit ONVIF User

[1] Add ONVIF User: Add a new user. **Profile** is opened.

[2] Users: Shows the users with ONVIF permissions ("[Users](#)"). Default: "admin" and "onvif_admin_user".

[3] Tokens: Shows the configuration of tokens for the user. ONVIF permissions require a separate token. Default: only the default token configured for "onvif_admin_user".

[4] Edit ONVIF User: Edit the user with ONVIF permissions. **Profile** is opened.

5.9.3. ONVIF INFORMATION

The following functions are available:

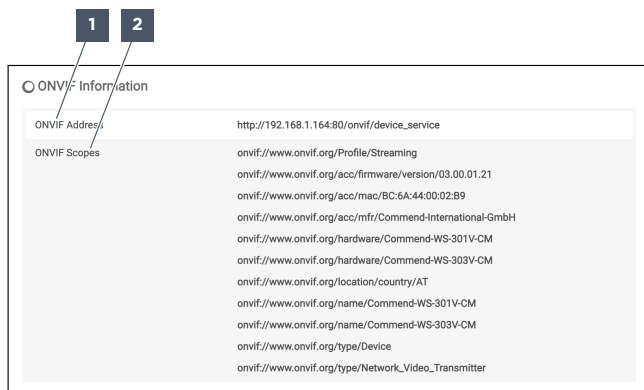


Figure 103: ONVIF – ONVIF Information

- 1 ONVIF Address
- 2 ONVIF Scopes

[1] ONVIF Address: Shows the URL through which the ONVIF service (endpoint) is available. If a VMS system cannot find the device using the ONVIF discovery function, the ONVIF function of the device can be accessed through this URL. Default: "http://192.168.1.150/onvif/device_service".

[2] ONVIF Scopes: Shows the URIs that are used to provide general information about the device to a VMS system. These URIs are defined and standardised by ONVIF.

Information:

- onvif://www.onvif.org/Profile/Streaming
- onvif://www.onvif.org/acc/firmware/version/xx.xx.xx.xxx
- onvif://www.onvif.org/acc/mac/BC:6A:44:00:18:09
- onvif://www.onvif.org/acc/mfr/Commend-International-GmbH
- onvif://www.onvif.org/hardware/Commend-ID-5-TD-CM
- onvif://www.onvif.org/location/country/AT
- onvif://www.onvif.org/name/Commend-ID-5-TD-CM
- onvif://www.onvif.org/type/Device
- onvif://www.onvif.org/type/Network_Video_Transmitter

5.10. SIP

The following functions are available:

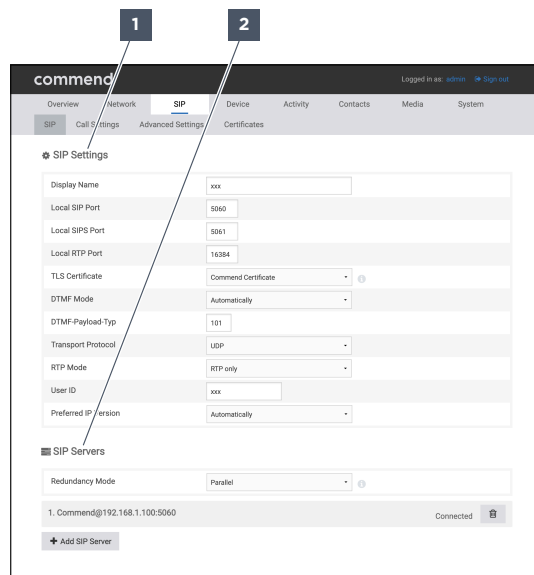


Figure 104: SIP

- 1** SIP Settings **2** SIP Servers

[1] SIP Settings: Configure general SIP settings.

[2] SIP Servers: Configure the SIP connections.

5.10.1. SIP SETTINGS

The following functions are available:

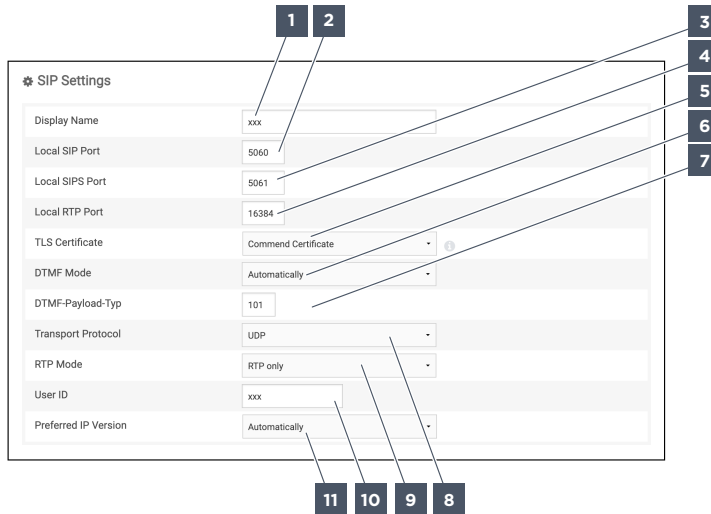


Figure 105: SIP – SIP Settings

- | | | |
|--------------------|-------------------------|-------------------|
| 1 Display Name | 2 Local SIP Port | 3 Local SIPS Port |
| 4 Local RTP Port | 5 TLS Certificate | 6 DTMF Mode |
| 7 DTMF-Payload-Typ | 8 Transport Protocol | 9 RTP Mode |
| 10 User ID | 11 Preferred IP Version | |

[1] Display Name: Enter a caller designation for the device. The display name must not be longer than 40 characters and must not contain any special characters. Default: "ID5".

[2] Local SIP Port: Enter the port number for the SIP protocol. The port numbers of the local SIP port and the local SIPS port must not match. Range of values: "1024" to "65535". Default: "5060".

[3] Local SIPS Port: Enter the port number for the SIP protocol for transmission via TLS. The port numbers of the local SIP port and the local SIPS port must not match. Range of values: "1024" to "65535". Default "5061".

[4] Local RTP Port: Enter the port number for the RTP protocol. For calls without video, 2 RTP ports are used. For calls with video, 4 RTP ports are used. When a call is initiated, RTP ports are used randomly in a range of 256 port numbers above the configured RTP port. For reasons of compatibility with older SIP servers, only even RTP port numbers are automatically used. Range of values: "1024" to "65406". Default: "16384".

[5] TLS Certificate: Select the SIP certificate that is used for peer-to-peer calls. Default: "Commend Certificate".

"Commend Certificate" is not shown in **Certificates** and cannot be deleted.

[6] DTMF Mode: Select the DTMF mode. Default: "Automatic".

Options:

- **Automatic:** The device adjusts signal transmission automatically.
- **RTP Event (RFC 2833):** The device transmits signals according to the RFC 2833 protocol.
- **SIP Info:** The device transmits signals according to the SIP protocol.

[7] DTMF Payload Type: Enter the payload type number for DTMF tones. The payload type number indicates that transmitted packets contain DTMF tones. This function is available only if the option

“Automatic” or the option “RTP Event (RFC 2833)” is selected in DTMF Mode. Range of values: “96” to “127”. Default: “101”.

[8] Transport Protocol: Select the transport protocol for signalling from the device to a SIP device or to a SIP server. Default: “UDP”.

Options:

- **UDP:** The device uses the transport protocol “UDP”.
- **TCP:** The device uses the transport protocol “TCP”. The remote station must support the transport protocol “TCP”.
- **TLS:** The device uses the transport protocol “TLS” for encrypted transmission. The remote station must support the transport protocol “TLS”. In **[9] RTP Mode**, the option “SRTP preferred” is selected automatically. In **[9] RTP Mode**, another option can be selected.
- **TLS only:** The device uses only the transport protocol “TLS” for encrypted transmission. Incoming calls that are not initiated via TLS are declined automatically. The remote station must support the transport protocol “TLS”. In **[9] RTP Mode**, the option “SRTP preferred” is selected automatically. In **[9] RTP Mode**, another option can be selected. This option is greyed out if a SIP connection is configured. If this option is selected and a SIP connection is configured, the option “TLS” is selected automatically after saving the configuration.

[9] RTP Mode: Select the transport protocol for media encryption from the device to a SIP device or to a SIP server. Default: “RTP only”.

Options:

- **RTP only:** The device uses the transport protocol “RTP”. Incoming calls that are initiated via SRTP are transmitted automatically in an unencrypted format via RTP. If the remote station does not allow this, the call may be ended automatically.
- **SRTP only:** The device uses the transport protocol “SRTP” for encrypted transmission. The remote station must support the transport protocol “SRTP”. Incoming calls that are not initiated via SRTP are declined automatically. The option “SRTP only” must be configured at the device and at the remote station. If the option “SRTP only” is configured at the device and the option “SRTP preferred” is configured at the remote station, or vice versa, the call may be declined automatically.
- **SRTP preferred:** The device primarily uses the transport protocol “SRTP”. If the remote station supports only RTP, the transport protocol “RTP” is used.

[10] User ID: Enter the user ID of the SIP account for registration at the SIP server. The user ID must not be longer than 50 characters. If the domain in the user ID is also required for the SIP server, this domain must follow the user ID. Default: “id5”.

[11] Preferred IP Version: Select the preferred IP version for signalling from the device to a SIP device or to a SIP server. Default “AUTO”.

Options:

- **AUTO:** The device preferably adjusts the IP version automatically.
- **IPv4:** The device preferably uses IPv4.
- **IPv6:** The device preferably uses IPv6.

5.10.2. SIP SERVER

The following functions are available:

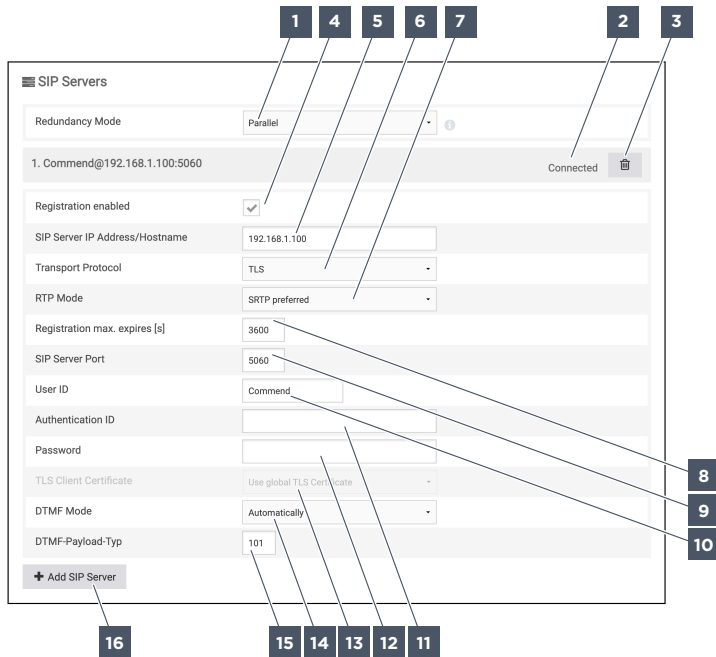


Figure 106: SIP - SIP-Server

- | | | |
|---------------------------|----------------------------------|----------------------|
| 1 Redundancy Mode | 2 SIP connection status | 3 Delete Server |
| 4 Registration enabled | 5 SIP Server IP Address/Hostname | 6 Transport Protocol |
| 7 RTP Mode | 8 Registration max. expires [s] | 9 SIP Server Port |
| 10 User ID | 11 Authentication ID | 12 Password |
| 13 TLS Client Certificate | 14 DTMF Mode | 15 DTMF-Payload-Typ |
| 16 Add SIP Server | | |

For TLS connections between the device and VirtuoSIS, in CCT 800 below **Subscribers > Device Properties > SIP Terminal > Settings** in **NAT**, the option “force_rport” must be selected (see “**Intercom Server Configuration**” manual).

[1] Redundancy Mode: Select the SIP server redundancy behaviour. Default: “Parallel”.

Options:

- **Parallel:** The device registers at all configured SIP servers.
- **Sequential:** The device checks the availability of the SIP server with the highest priority at configured registration intervals. The device registers only at the available SIP server with the highest priority. As long as this SIP server is available, SIP servers with a lower priority are not checked.
- **Cisco:** The device checks the availability of all SIP servers at configured registration intervals. The device registers only at the available SIP server with the highest priority.

[2] SIP connection status: Shows the connection status to the SIP servers.

Options:

- **Unknown:** The connection state is unknown.
Example: When booting the device.
- **Registering:** The device is registering on the SIP server.

- **Registered:** The device is registered on the SIP server.
- **Logging out:** The device is logging out of the SIP server.
- **Logged out:** The device has logged out of the SIP server.
- **Idle:** When in redundancy mode “Sequential”, the device is not connected to the low-priority SIP server. The device is connected to a higher-priority SIP server.
- **Connecting:** The device is establishing a connection to the SIP server.
- **Available:** When in redundancy mode “Cisco”, the device can access a low-priority SIP server. The device is connected to a higher-priority SIP server.
- **Connection failed:** The device is unable to connect to the SIP server.
- **Authentication failed:** Authentication on the SIP server has failed due to an invalid user ID, an invalid password or an invalid authentication ID.
- **Error:** A connection error has occurred.

[3] Delete Server: Deletes the connections to the SIP servers.

[4] Registration enabled: Activate to ensure that the device can be registered at a SIP server. Default: disabled.

[5] SIP Server-IP Address/Hostname: Enter the IP address or hostname of the SIP server. Default: empty.

Recommendation: Enter the IP address of the SIP server if the SIP server is not accessible via the hostname.

[6] Transport Protocol: Select the transport protocol for signalling from the device to an SIP device or SIP server. Default: “UDP”.

Options:

- **UDP:** The device uses the transport protocol “UDP”.
- **TCP:** The device uses the transport protocol “TCP”. The remote station must support the transport protocol “TCP”.
- **TLS:** The device uses the transport protocol “TLS” for encrypted transmission. The remote station must support the transport protocol “TLS”. In **[9] RTP Mode**, the option “SRTP preferred” is selected automatically. In **[9] RTP Mode**, another option can be selected.
- **Automatic:** The device automatically uses the transport protocol that was sent to the device via SRV when registering at the SIP server. The device selects a transport protocol from this list. If the SIP server SRV is not supported, the transport protocol “UDP” is used. Due to the automatic process when registering at the SIP server, the SIP server port is “5600” and the port for TLS connections is “5601”. If the SIP server supports the transport protocol “TLS”, a corresponding certificate must be uploaded using **Certificates** (see [“Certificates”, page 101](#)). Without a corresponding certificate, the device cannot register at the SIP server if the transport protocol “TLS” is selected.

[7] RTP Mode: Select the transport protocol for media encryptions from the device to an SIP device or SIP server. Default: “RTP only”.

Options:

- **RTP only:** The device uses the transport protocol “RTP”. Incoming calls that are initiated via SRTP are transmitted automatically in an unencrypted format via RTP. If the remote station does not allow this, the call may be ended automatically.
- **SRTP only:** The device uses the transport protocol “SRTP” for encrypted transmission. The remote station must support the transport protocol “SRTP”. Incoming calls that are not initiated via SRTP are declined automatically. The option “SRTP only” must be configured at the device and at the remote station. If the option “SRTP only” is configured at the device and the option “SRTP preferred” is configured at the remote station, or vice versa, the call may be declined automatically.
- **SRTP preferred:** The device primarily uses the transport protocol “SRTP”. If the remote station supports only RTP, the transport protocol “RTP” is used.

[8] Registration Interval [s]: Enter the maximum time in seconds in which the device re-registers at the SIP server. Value Range: “20” to “86400”. Default: “3600”.

[9] SIP Server Port: Enter the SIP port number of the SIP server. Default: “5060”.

[10] User ID: Enter the user ID of the SIP account for registration at the SIP server. The user ID must not be longer than 50 characters. If the domain in the user ID is also required for the SIP server, this domain must come after the user ID. Default: "id5".

[11] Authentication ID: Enter the authentication ID for the SIP server. The authentication ID is required only for certain SIP servers. Default: empty.

[12] Password: Enter the password of the SIP account. Default: empty.

[13] TLS Client Certificate: Select the TLS client certificate for this SIP server connection. If only the default certificate is available, this function is greyed out. Default: "Use Global TLS Certificate".

[14] DTMF Mode: Select the DTMF mode. Default: "Automatic".

Options:

- **Automatic:** The device adjusts signal transmission automatically.
- **RTP Event (RFC 2833):** The device transmits signals according to the RFC 2833 protocol.
- **SIP Info:** The device transmits signals according to the SIP protocol.

[15] DTMF Payload Type: Enter the payload type number for DTMF tones. The payload type number indicates that transmitted packets contain DTMF tones. This function is available only if the options "Automatic" or "RTP Event (RFC 2833)" are selected in **DTMF Mode**. Value Range: "96" to "127". Default: "101".

Recommendation: Configure the SIP server with the same payload type number to ensure correct interpretation of DTMF tones.

[16] Add SIP Server: Add a connection to a SIP server.

5.11. CALL SETTINGS

The following functions are available:

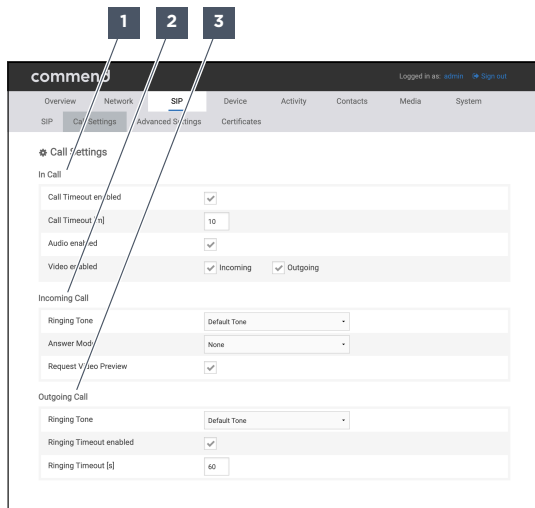


Figure 107: Call Settings

- 1 In Call
- 2 Incoming Call
- 3 Outgoing Call

[1] In Call: Configure the call behaviour in the device state "In Call".

[2] Incoming Call: Configure the call behaviour in the device state "Incoming Call".

[3] Outgoing Call: Configure the call behaviour in the device state “Outgoing Call”.

5.11.1. IN CALL

The following functions are available:

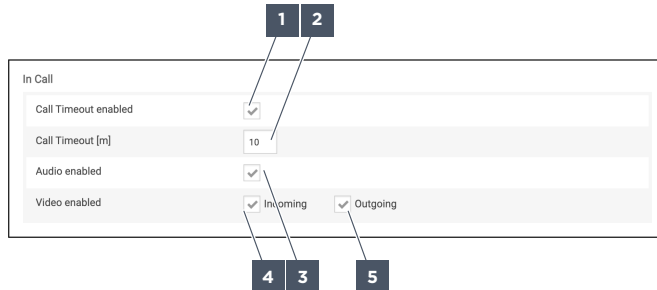


Figure 108: Call Settings – In Call

- 1** Call Timeout enabled
- 2** Call Timeout [m]
- 3** Audio enabled
- 4** Incoming
- 5** Outgoing

[1] Call Timeout enabled: Activate to end calls automatically after exceeding the timeout. Default: activated.

[2] Call Timeout [m]: Enter the time in minutes after which calls are ended automatically. Range of values: “1” to “600”. Default: “10”.

[3] Audio enabled: Activate to transmit audio signals during calls. Default: activated.

[4] Incoming: Activate to transmit incoming video streams during calls. Default: activated.

[5] Outgoing: Activate to transmit outgoing video streams during calls. Default: activated.

5.11.2. INCOMING CALL

The following functions are available:

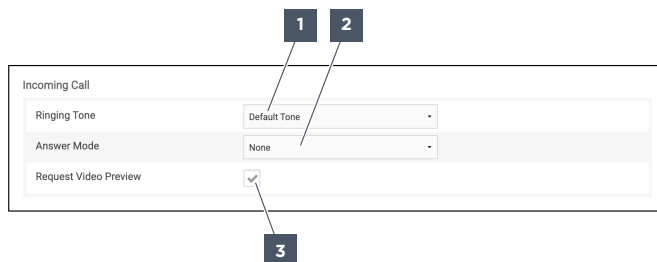


Figure 109: Call Settings – Incoming Call

- 1** Ringing Tone
- 2** Answer Mode
- 3** Request Video Preview

[1] Ringing Tone: Select the ringtone. Default: “Default Tone”.

Options:

- **Default Tone:** The default ringtone is played back.
- **No Tone:** No ringtone is played back.
- **Audio Files:** An audio file is played back that has been uploaded to the device through **Audio Files**. If there are no audio files available on the device, this option is greyed out.

[2] Answer Mode: Select the answer mode. Default: “None”.

Options:

- **None:** Incoming calls can be accepted manually.
- **Decline Call:** Incoming calls are declined automatically.
- **Answer Call:** Incoming calls are accepted automatically.

[3] Request Video Preview: Activate to request the video image from the remote station before accepting calls. The video preview cannot be requested if **Video enabled** is deactivated for incoming calls. The video preview cannot be requested if an option other than “None” is selected for **Answer Mode**. Default: activated.

5.11.3. OUTGOING CALL

The following functions are available:

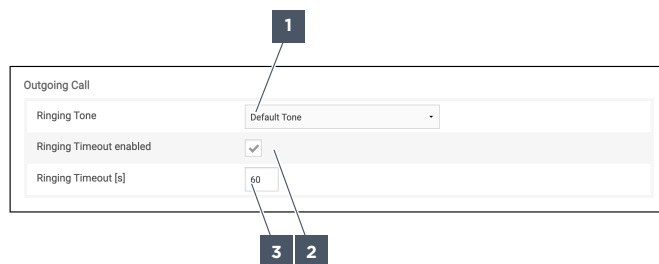


Figure 110: Call Settings – Outgoing Call

- 1 Ringing Tone 2 Ringing Timeout enabled 3 Ringing Timeout

[1] Ringing Tone: Select the ringtone. Default: “Default Tone”.

Options:

- **Default Tone:** The default ringtone is played back.
- **No Tone:** No ringtone is played back.
- **Audio Files:** An audio file is played back that has been uploaded to the device through **Audio Files**. If there are no audio files available on the device, this option is greyed out.

[2] Ring Timeout enabled: Activate to end calls automatically after exceeding the timeout if these calls are not accepted. Default: activated.

[3] Ring Timeout [s]: Enter the time in seconds after which calls are ended automatically if these calls are not accepted. Range of values: “1” to “600”. Default: “60”.

5.12. ADVANCED OPTIONS

The following functions are available:

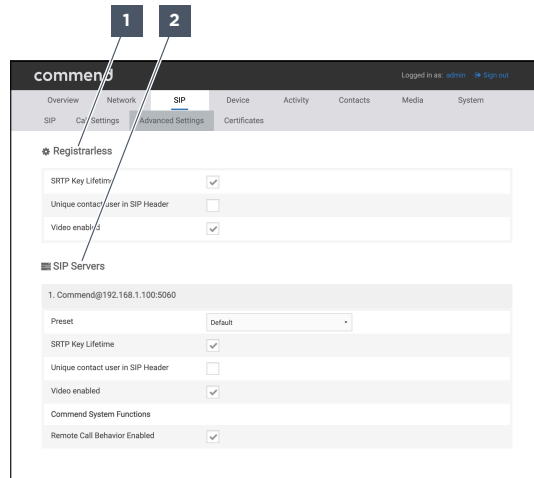


Figure 111: Advanced Options

- 1** Registrarless **2** SIP Servers

[1] Registrarless: Configure the settings for registrarless SIP connections.

[2] SIP Server: Configure advanced settings for individual SIP connections.

5.12.1. REGISTRARLESS

The following functions are available:

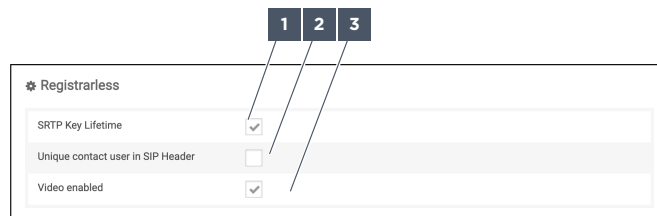


Figure 112: Advanced options - Registrarless

- 1** SRTP Key Lifetime **2** Unique contact user in SIP Header **3** Video enabled

[1] SRTP Key Lifetime: Activate to send the SRTP key lifetime parameter during calls. This function must be supported by the remote station. Default: deactivated.

[2] Unique contact user in SIP Header: Activate to use contact information in the SIP header. The user ID in the field “Contact” of the SIP message header is expanded by adding one unique value. For incoming calls, the device can use this value to identify the SIP account. This function is required to ensure data transmission between the remote station and the device via TLS. Certain devices cannot interpret the user ID in the field “Contact”. Default: deactivated.

Example: “Contact: <sip:6000-0x1256ce@192.168.1.150:5060>”.

[3] Video enabled: Activate to allow video for calls. If this function is deactivated, calls can only be initiated without video. This function must be supported by the remote station. Default: activated.

5.12.2. SIP SERVERS

The following functions are available:

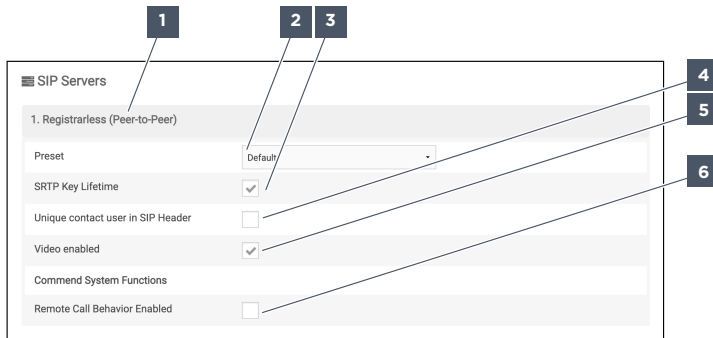


Figure 113: Advanced Options – SIP-Server

- 1** SIP Connection
- 2** Preset
- 3** SRTP Key Lifetime
- 4** Video enabled
- 5** Unique contact user in SIP Header
- 6** Remote Call Behavior Enabled

One SIP configuration interface is displayed per SIP connection.

⚠ CAUTION

Incorrect or incomplete configuration

Device or software malfunction

- Have experts carry out the configuration.

[1] SIP Connection: Shows the SIP connection.

[2] Preset: Select the preset for configuring the SIP connection. Changing the configuration affects the parameters below. Default: "Default".

Options:

- **Default:** SIP connections are optimised for operation with Commend devices.
- **User-defined:** User-specific settings are configured. This option is automatically selected if the performed configuration does not match any of the presets.
- **Asterisk 11:** SIP connections are optimised for operation with Asterisk 11 and VirtuoSIS.

[3] SRTP Key Lifetime: Activate to send the SRTP key lifetime parameter during calls. This function must be supported by the SIP server. Default: deactivated.

[4] Video enabled: Activate to allow video for calls. If this function is deactivated, calls can only be initiated without video. This function must be supported by the SIP server. Default: deactivated.

[5] Unique contact user in SIP Header: Activate to use contact information in the SIP header. The user ID in the field "Contact" of the SIP message header is expanded by adding one unique value. For incoming calls, the device can use this value to identify the SIP account. This function is required to ensure data transmission between the VirtuoSIS (Version 9.0 or later) and the device via TLS. Certain SIP servers cannot interpret the user ID in the field "Contact". Default: deactivated.

Example: "Contact: <sip:6000-0x1256ce@192.168.1.150:5060>"

[6] Remote Call Behavior Enabled: Activate to adjust the call behaviour of the device to the call behaviour configured in VirtuoSIS. The call behaviour configured in the device such as Answer Mode or group calls is deactivated through configuration in VirtuoSIS. The ringtone of the device is used. All

other ringtones are provided by the SIP server. This function can be used with VirtuoSIS from version 11.0. Default: deactivated.

5.13. CERTIFICATES

The following functions are available:

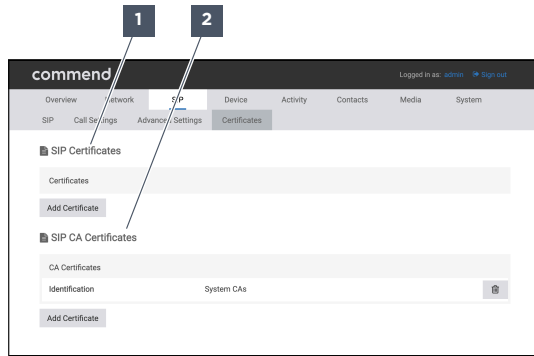


Figure 114: Certificates

- 1 SIP Certificates
- 2 SIP CA Certificates

[1] SIP Certificates: Manage SIP certificates.

[2] SIP CA Certificates: Manage SIP certificate authority certificates.

5.13.1. SIP CERTIFICATES

The following functions are available:

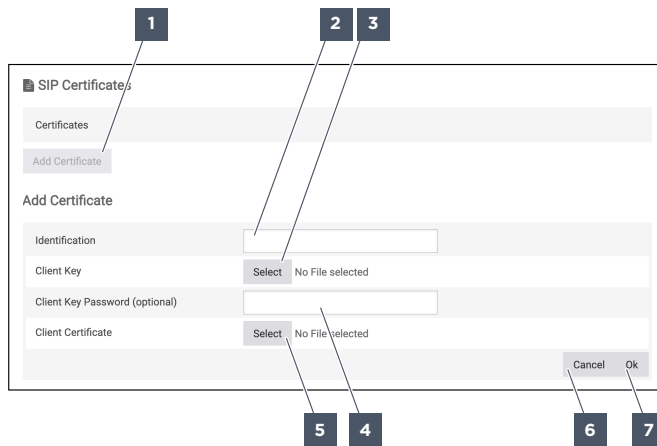


Figure 115: Certificates – SIP Certificates

- 1 Add Certificate
- 2 Identification
- 3 Client Key
- 4 Client Key Password (optional)
- 5 Client Certificate
- 6 Abort
- 7 OK

SIP client certificates can be used to authenticate the device at other SIP devices or SIP servers. SIP client certificates can also be used for peer-to-peer calls.

[1] Add Certificate: Add a new SIP client certificate. The maximum key length of SIP client certificates is 2048 bits.

[2] Identification: Enter a name for the SIP client certificate.

[3] Client Key: Upload a client key for the SIP client certificate.

Recommendation: Upload the client key in the KEY or PEM format.

[4] Client Key Password (optional): Enter the password for the client key. The password is optional.

[5] Client Certificate: Upload the SIP client certificate. The SIP client certificate must be formatted in the X.509 standard.

Recommendation: Upload SIP client certificates in the CERT, CRT, DER or PEM format.

[6] Abort: Cancel the process and do not add a SIP client certificate.

[7] OK: Add the SIP client certificate.

5.13.2. SIP CA CERTIFICATES

The following functions are available:

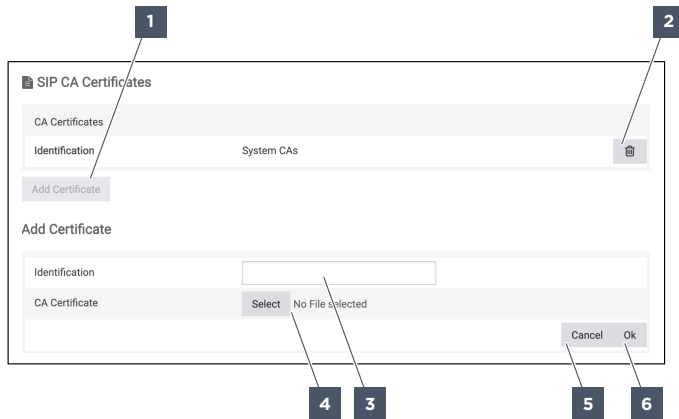


Figure 116: Certificates - SIP CA Certificates

- 1** Add Certificate **2** Delete Certificate **3** Identification
- 4** CA Certificate **5** Cancel **6** OK

SIP certificate authority certificates authenticate access to the device from SIP servers.

[1] Add Certificate: Add a SIP certificate authority certificate. The device has a collection of certificate authority certificates (“System CAs”) ex works. The maximum key length of SIP certificate authority certificates is 2048 bits.

[2] Delete Certificate: Delete the SIP certificate authority certificate. The “System CAs” certificate can only be restored by resetting the device to its factory defaults.

Recommendation: Do not delete the “System CAs” certificate.

[3] Identification: Enter a name for the SIP certificate authority certificate.

[4] CA Certificate: Upload a SIP certificate authority certificate. The SIP certificate authority certificate must be formatted in the X.509 standard.

Recommendation: Upload SIP certificate authority certificates in the CERT, CRT, DER or PEM format.

[5] Cancel: Cancel the process and do not add a SIP certificate authority certificate.

[6] OK: Add the SIP certificate authority certificate.

5.14. DEVICE

The following functions are available:

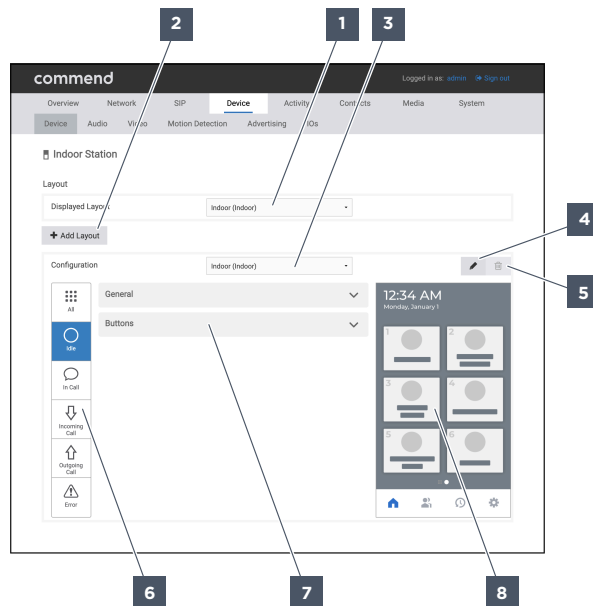


Figure 117: Device

- | | | | | | |
|---|---------------------|---|---------------|---|---------------|
| 1 | Displayed Layout | 2 | Add Layout | 3 | Configuration |
| 4 | Edit Layout Name | 5 | Delete Layout | 6 | Device states |
| 7 | Configuration areas | 8 | Preview | | |

[1] Displayed Layout: Select the layout that should be shown on the touch display of the device. When the layout is changed, the view “Home” is shown. Other views like “Cleaning Mode”, “Settings” or “User Actions” are closed. Default: “Indoor”.

Options:

- **Door:** Layout optimised for door applications. An unlimited number of individual buttons can be configured. From 5 buttons, a scrollable list is shown.
- **Indoor:** Layout optimised for desk and wall applications. Up to 6 buttons can be configured per page. Up to 10 pages can be configured.
- **Frame:** Layout optimised for individual content and Advanced Security Building Intercom Systems (ASBIS). 7 different formats with different button areas are available. For a clear identification of the button areas, button images must be configured for every button area.
- **Contact management:** Layout optimised for applications with many contacts such as public buildings, universities and hotels. Contacts and actions can be configured in different directories.
- **Customized Visualization:** Layout optimised for displaying custom content such as timetables or building controls. Static or interactive content can be displayed. Up to 2 buttons can be configured. This function can be used with VirtuoSIS.
“Customized Visualization” applications and 3rd-party content can significantly impact the performance and usability of the Commend system. To ensure correct display on the device and proper functioning, external content must be technically checked by Commend. Display of external content without verification by Commend is not permitted. For this, contact your Commend sales partner. The user must ensure that the rights of 3rd parties are not violated by displaying content.

[2] Add Layout: Add a new layout. By default, only the layouts “Indoor” and “Door” are configured. A maximum of 12 layouts can be managed.

[3] Configuration: Select the layout that should be configured. The selected layout is not shown on the touch display. Default: “Indoor”.

[4] Edit Layout Name: Edit the layout name.

[5] Delete Layout: Delete the layout that is selected in **[3] Configuration**. The layout cannot be deleted if the layout is selected in **[1] Displayed Layout**. If you delete a layout to which you can switch via an action sequence, the action sequence is also deleted.

[6] Device states: Select the device state that is selected in **[3] Configuration** and should be configured.

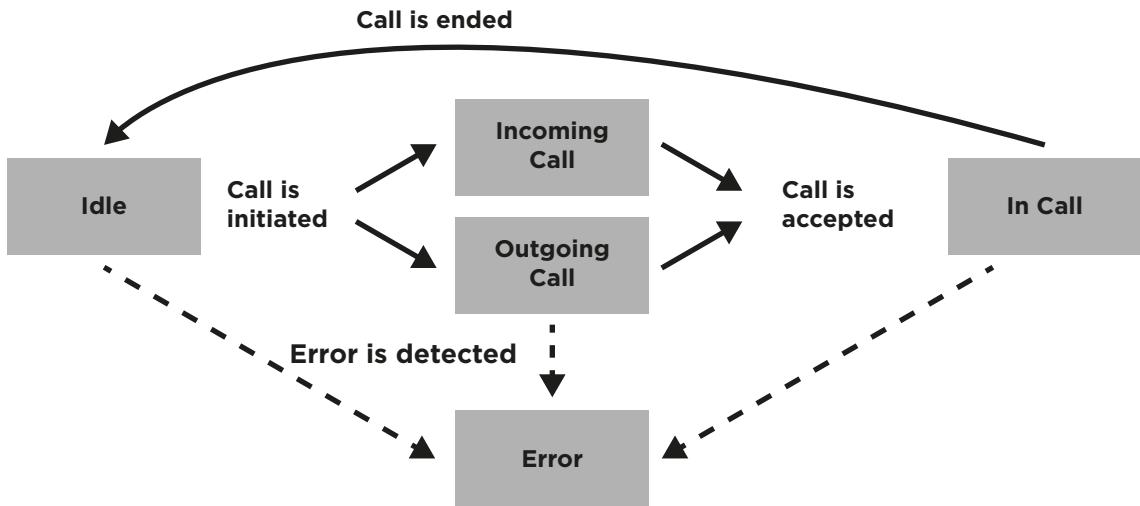


Figure 118: Device states

Options:

- **Idle:** The device is in this device state if neither a call is being established, nor a call is established, nor the device is in the device state “Error”.
 - **Incoming call:** The device is in this device state if a call to the device is being established.
 - **Outgoing Call:** The device is in this device state if a call from the device is being established.
 - **In Call:** The device is in this device state if a call is established. If the call is ended, the device switches to the device state “Idle”.
 - **Error:** The device is in this state if errors are detected. If the errors are resolved or the configuration is changed, the device switches to the device state “Idle”.
- Example:** The connection to the SIP server is interrupted.

[7] Configuration areas: Configure the configuration areas. The configuration areas of “All”, “Idle”, “In Call”, “Incoming Call”, “Outgoing Call” and “Error” differ from each other.

[8] Preview: Displays the schematic layout for the respective device state.

5.14.1. CREATE A NEW LAYOUT

The following functions are available:

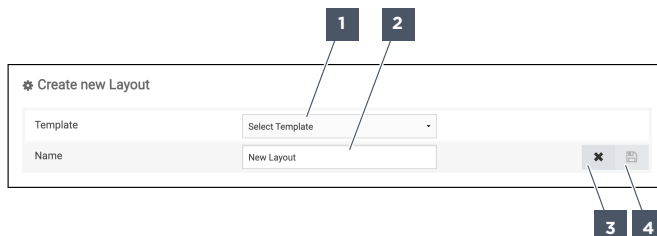


Figure 119: Create a new layout

- 1** Template
- 2** Name
- 3** Cancel
- 4** Save

[1] Template: Select the template.

Options:

- **Door:** Layout optimised for door applications. An unlimited number of individual buttons can be configured. From 5 buttons, a scrollable list is shown.
- **Indoor:** Layout optimised for desk and wall applications. Up to 6 buttons can be configured per page. Up to 10 pages can be configured.
- **Frame:** Layout optimised for individual content and Advanced Security Building Intercom Systems (ASBIS). 7 different formats with different button areas are available. For a clear identification of the button areas, button images must be configured for every button area.
- **Contact management:** Layout optimised for applications with many contacts such as public buildings, universities and hotels. Contacts and actions can be configured in different directories.
- **Customized Visualization:** Layout optimised for displaying custom content such as timetables or building controls. Static or interactive content can be displayed. Up to 2 buttons can be configured. This function can be used with VirtuoSIS.
 “Customized Visualization” applications and 3rd-party content can significantly impact the performance and usability of the Commend system. To ensure correct display on the device and proper functioning, external content must be technically checked by Commend. Display of external content without verification by Commend is not permitted. For this, contact your Commend sales partner. The user must ensure that the rights of 3rd parties are not violated by displaying content.

- [2] Name:** Enter a name for the layout.
- [3] Cancel:** Cancel and do not add a layout.
- [4] Save:** Save the layout.

5.14.2. EDIT LAYOUT NAME

The following functions are available:



Figure 120: Edit Layout Name

- 1** Name
- 2** Cancel
- 3** Save

- [1] Name:** Enter a name for the layout.
- [2] Cancel:** Cancel and do not edit the name of the layout.
- [3] Save:** Save the name of the layout.

5.14.3. DEVICE STATES

5.14.3.1. ALL

The following functions are available:

General

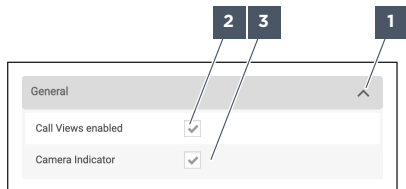


Figure 121: Device - All - General

- 1** Configuration area
- 2** Call Views enabled
- 3** Camera Indicator

- [1] Configuration area:** Maximise or minimise the configuration area.

[2] Level active: Show the views “Incoming Call”, “Outgoing Call”, “In Conversation” and “Call ended” views during a call. If this function is deactivated, custom content can be shown instead. This function is available for the layout “Customized Visualization” only. Default: activated.

[3] Camera indicator: Activate to show the status LED in red during video streams and video calls. Default: activated.

Display Settings

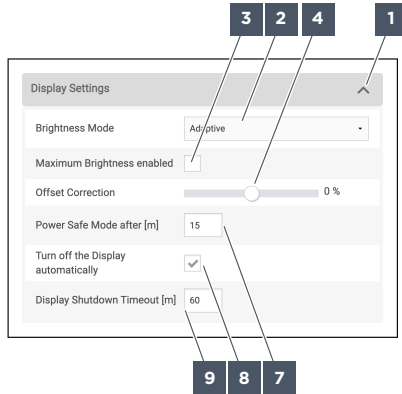


Figure 122: Device - All - Display Settings

- 1** Configuration area
- 2** Brightness Mode
- 3** Maximum Brightness enabled
- 4** Offset Correction
- 5** Brightness Level (not shown)
- 6** Power Safe Model Level (not shown)
- 7** Power Safe after [m]
- 8** Turn off the Display automatically
- 9** Display Shutdown Timeout [m]

[1] Configuration area: Maximise or minimise the configuration area.

[2] Brightness Mode: Select the brightness mode. Default: “Adaptive”.

Options:

- **Adaptive:** The display brightness is automatically adjusted depending on the lighting conditions. **[3] Maximum Brightness enabled** and **[4] Offset Correction** are shown.
- **Manually:** The display brightness can be configured manually. **[5] Brightness Level (not shown)** and **[6] Power Safe Model Level (not shown)** are shown.

[3] Maximum Brightness enabled: Activate to automatically increase the display brightness to 100% during calls and display operation. This function is available only if the option “Adaptive” is selected in **[2] Brightness Mode**. Default: deactivated.

[4] Offset Correction: Adjust the automatic adaptation of the display brightness to the lighting conditions. By automatically adapting the display brightness, content is displayed more legibly depending on the lighting conditions. The display brightness of the device is optimised. In very dark areas, an adjustment of up to -50% may be necessary. Using the offset correction, the absolute value cannot fall below “0%” and the absolute value cannot exceed “100%”. In very bright areas, an adjustment of up to +50% may be necessary. This function is available only if the option “Adaptive” is selected in **[2] Brightness Mode**. Range of values: “-50%” to “+50%”. Default: “0%”.

Recommendation: Adjust the offset correction for special requirements only.

[5] Brightness Level (not shown): Adjust the display brightness when the power save mode is not active. This function is available only if the option “Adaptive” is selected in **[2] Brightness Mode**. Range of values: “2%” to “100%”. Default: “80%”.

[6] Power Safe Model Level (not shown): Adjust the display brightness when the power save mode is active. If the display brightness should not be dimmed, “100%” must be configured. This function

is available only if the option “Manually” is selected in **[2] Brightness Mode**. Range of values: “2%” to “100%”. Default: “50%”.

[7] Power Safe after [m]: Enter the time in minutes after which the display brightness is automatically dimmed if there is no touch or no incoming call. If the option “Manually” is selected in **[2] Brightness Mode**, the display brightness is dimmed by the value configured in **[6] Power Safe Model Level (not shown)**. If **[8] Turn off the Display automatically** is activated, the configured value must be smaller than the value configured in **[9] Display Shutdown Timeout [m]**. Range of values: “1” to “1440”. Default: “15”.

[8] Turn off the Display automatically: Activate to automatically turn off the display after the time configured in **[9] Display Shutdown Timeout [m]** has elapsed. If the advertising mode is activated, the display is not turned off. Default: activated.

[9] Display Shutdown Timeout [m]: Enter the time in minutes after which the display is automatically turned off if there is no touch or no incoming call. If the display is turned off, it can be woken up again by touching, an incoming call or an action sequence. This function is displayed only if **[8] Turn off the Display automatically** is activated. Range of values: “2” to “1440”. Default: “60”.

Pictograms

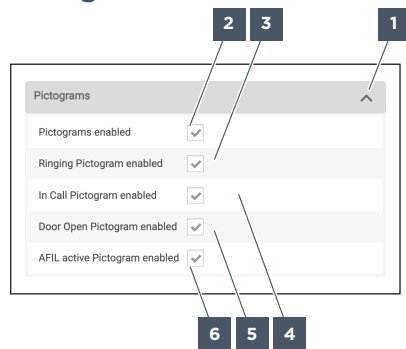


Figure 123: Device - All - Pictograms

- | | | |
|------------------------------------|--------------------------------------|--|
| 1 Configuration area | 2 Pictograms enabled | 3 Ringing Pictogram activated |
| 4 In Call Pictogram enabled | 5 Door Open Pictogram enabled | 6 AFIL active Pictogram enabled |

[1] Configuration area: Maximise or minimise the configuration area.

[2] Pictograms enabled: Activate to show the pictograms. The pictograms can be activated or deactivated individually. Default: activated.

[3] Ringing Pictogram activated: Activate to show the ringing pictogram for incoming calls or for outgoing calls. Default: activated.

[4] In Call Pictogram enabled: Activate to show the “in call pictogram” during calls when no video image is being transmitted. Default: activated.

[5] Door Open Pictogram enabled: Activate to show the “door open pictogram” after activating the door opener function. Default: activated.

[6] AFIL active Pictogram enabled: Activate to show the “AFIL active pictogram” when AFIL signals are being transmitted. Default: activated.

5.14.3.2. IDLE

The following functions are available:

General

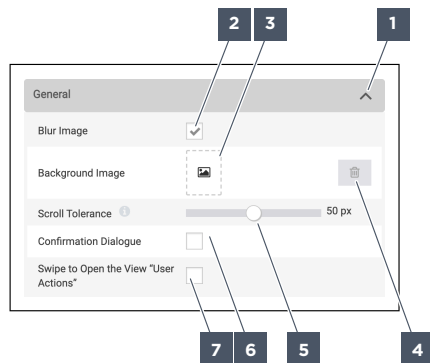


Figure 124: Device - Idle - General

- | | | |
|---|---------------------------|--------------------------------|
| 1 Configuration area | 2 Blur Image | 3 Upload an image |
| 4 Delete Background Image | 5 Scroll Tolerance | 6 Confirmation Dialogue |
| 7 Swipe to Open the View
"User Actions" | | |

[1] Configuration area: Maximise or minimise the configuration area.

[2] Blur Image: Activate to show the background image blurred. Default: activated.

[3] Upload an image: Select or upload a background image. The background image is shown in all views in the device state "Idle". A different background image can be configured for every layout. Default: no image selected.

Image properties:

- **File size:** max. 6 MB.
- **File format:** JPG, PNG.

Recommendation:

- **Size (W x H):** 720 x 1280 pixels.
- **Resolution:** 72 dpi.
- **File format:** JPEG.
- **Colour space:** sRGB.
- **Compression/Quality:** 60/7 to 8.

Recommendation: Do not use a white or too bright background image. The text or symbols may not be visible or may be difficult to discern on the display.

In the layouts "Indoor" and "Contact Management", the background image is shown darkened.

If the background image has the same proportions as the display, the background image is not cut off. If the background image is larger than the display with the same proportions as the display, the background image is not cut off.

If the background image is disproportionately larger than the display, the background image is centred on the display. A background image that is too wide is cut off at the right and left sides. A background image that is too high is cut off at the top and bottom.

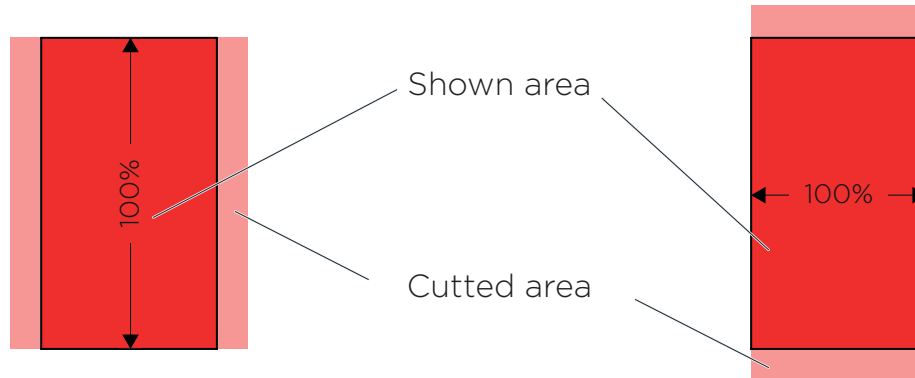


Figure 125: Background image too wide (left) and too high (right)

[4] Delete Background Image: Delete the background image.

[5] Scroll Tolerance: Adjust the scroll tolerance for tapping the display in scrollable views such as “Contacts” or “Home”. The configured value determines the maximum vertical movement, after touching the display, to trigger a touch event instead of scrolling. The usability of the device is improved for inexperienced users. Accessibility is guaranteed. A value of “0 px” deactivates this function and no swiping motion must be performed when touching the display. In non-scrollable views, the scroll tolerance is deactivated. Range of values: “0 px” to “100 px”. Default: “50 px”.

Example: If “50 px” is configured and an accidental swipe during typing does not exceed this scroll tolerance, a call is initiated.

[6] Confirmation Dialogue: Activate to show a confirmation dialogue to perform actions like calls and action sequences (see [“Confirmation dialogue”, page 51](#)). This function is only available for the layouts “Door” and “Frame”. Default: deactivated.

[7] Swipe to Open the View “User Actions”: Activate to open the view “User Actions” by swiping (see [“User actions”, page 50](#)). If this function is activated, a drop-down list is shown in which the swipe direction can be configured. The swipe must be performed horizontally over at least half the width of the display. The swipe must not be performed too slow. This function is available in the layouts “Door”, “Frame” and “Contact Management” only. Default: deactivated.

Options:

- **Left** (available for the layouts “Door”, “Frame” and “Customized Visualization” only)
- **Right**
- **Left or Right** (available for the layouts “Door”, “Frame” and “Customized Visualization” only)

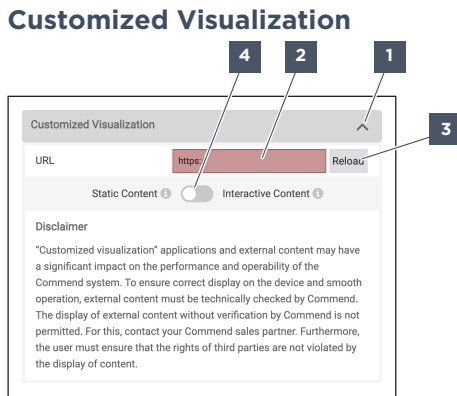


Figure 126: Device – Idle – Customized Visualization

- 1 Configuration area
- 2 URL
- 3 Reload
- 4 Content type

This configuration area is available for the layout “Customized Visualization” only.

[1] Configuration area: Maximise or minimise the configuration area.

[2] URL: Enter the URL with the content that should be displayed. This URL must be accessible for the device via the Internet or the local network. Default: empty.

The content provided via a URL must comply with the specifications in the Customized Visualization Guide “**Symphony MX**”.

For the layout “Customized Visualization”, buttons can be configured. Depending on the button configuration, the resolutions described below are available. If a transparent background colour is configured for the buttons, the full resolution of the display is available. Informative content should nevertheless not be displayed in the button area.

Resolutions:

- **No buttons:** 720 x 1280 pixels.
- **Small:** 720 x 1150 pixels.
- **Medium:** 720 x 1120 pixels.
- **Large:** 720 x 1100 pixels.

Example: The URL can be used to display custom content such as real-time timetables or building control user interfaces on the display of the device.

[3] Reload: Refresh the content on the screen.

[4] Content type: Select the content type. Default: “Static Content”.

Options:

- **Static Content:** JavaScript and Web Forms are deactivated.
- **Interactive Content:** JavaScript and Web Forms are activated.

Buttons

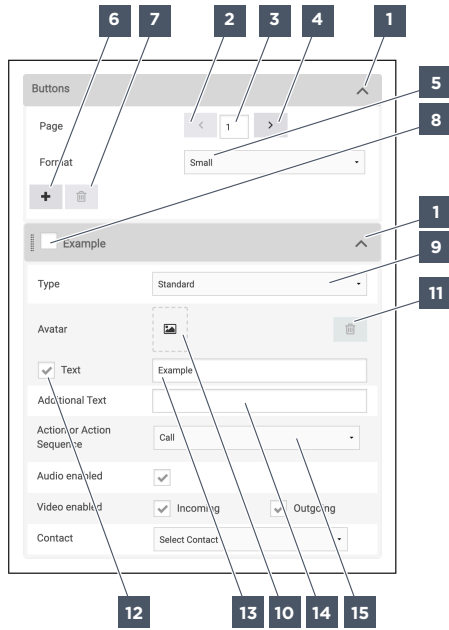


Figure 127: Device - Idle - Buttons for the layouts "Indoor" and "Door"

- | | | |
|---------------------------|--------------------|------------------------------|
| 1 Configuration area | 2 Previous | 3 Page |
| 4 Next | 5 Format | 6 Add Button |
| 7 Delete selected Buttons | 8 Select button | 9 Type |
| 10 Upload an image | 11 Delete Image | 12 Show text |
| 13 Text | 14 Additional Text | 15 Action or Action Sequence |

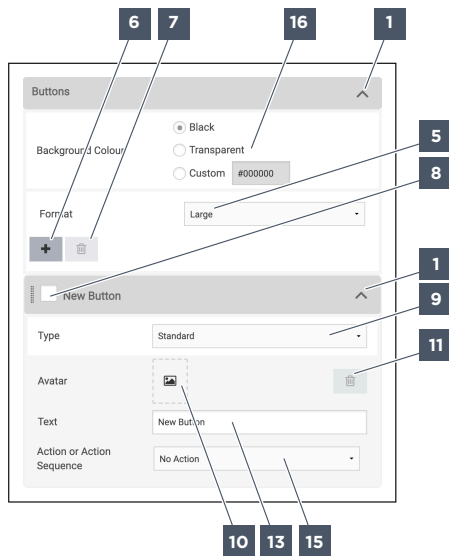


Figure 128: Device - Idle - Buttons for the layouts "Indoor", "Door" and "Frame"

- | | | |
|---------------------------|-----------------|----------------|
| 1 Configuration area | 5 Format | 6 Add a button |
| 7 Delete selected Buttons | 8 Select button | 9 Type |
| 10 Upload an image | 11 Delete Image | 13 Text |



Figure 129: Device - Idle - Buttons for the layout "Frame"

- | | | |
|------------------------------|--------------------|--------------|
| 1 Configuration area | 5 Format | 6 Add Button |
| 7 Delete selected Buttons | 8 Select button | 9 Type |
| 10 Upload an image | 11 Delete Image | 13 Text |
| 15 Action or Action Sequence | 17 Separator Lines | |

[1] Configuration area: Maximise or minimise the configuration area.

[2] Previous: Navigate to the previous page. This function is available for the layout "Indoor" only.

[3] Page: Enter the page number of the page that should be configured. This function is available for the layout "Indoor" only.

[4] Next: Navigate to the next page. This function is available for the layout "Indoor" only.

[5] Format: Select the format in which the buttons should be displayed.

Options for the layout "Indoor":

- **Small:** Up to 6 buttons can be configured per page.
- **Large:** Up to 3 buttons can be configured per page.

Options for the layout "Door":

- **Small (Image or Text):** Small buttons with an image or text can be configured. An icon can be configured. Default: bell icon.
- **Small:** Small buttons with an image and text can be configured. An icon can be configured. Default: bell icon.
- **Large:** Large buttons with an image and text can be configured. An icon can be configured. Default: bell icon.

Options for the layout "Frame":

- **1 Button:** 1 full-screen button can be configured. Dimensions for button images: 720 x 1280 pixels.
- **2 Buttons (1/2, 1/2):** 2 buttons of the same size can be configured. Dimensions for button images: 720 x 640 pixels.
- **3 Buttons (1/3, 1/3, 1/3):** 3 buttons of the same size can be configured. Dimensions for button images: 720 x 427 pixels.
- **3 Buttons (1/2, 1/4, 1/4):** 1 medium-sized and 2 small buttons can be configured. Dimensions for button images: 720 x 640 pixels (1/2) and 720 x 320 pixels (1/4).

- **3 Buttons (2/3, 1/6, 1/6):** 1 large and 2 small buttons can be configured. Dimensions for button images: 720 x 854 pixels (2/3) and 720 x 213 pixels (1/6).
- **4 Buttons (1/2, 1/6, 1/6, 1/6):** 1 large and 3 small buttons can be configured. Dimensions for button images: 720 x 640 pixels (1/2) and 720 x 213 pixels (1/6).
- **4 Buttons (1/4, 1/4, 1/4, 1/4):** 4 buttons of the same size can be configured. Dimensions for button images: 720 x 320 pixels.
- **5 Buttons (1/5, 1/5, 1/5, 1/5, 1/5):** 5 buttons of the same size can be configured. Dimensions for button images: 720 x 256 pixels.

Options for the layout “Customized Visualization”:

- **Small:** Up to 2 small buttons can be configured.
- **Medium:** Up to 2 medium-sized buttons can be configured.
- **Large:** Up to 2 large buttons can be configured.

Buttons for the layout “Contact Management” are configured in **Contact Management**.

[6] Add Button: Add a button. In the layout “Indoor”, buttons can be configured on a maximum of 10 pages. In the layout “Indoor”, buttons must be configured separately for every page. Buttons can be moved within a page. Buttons cannot be moved from one page to another. In the layout “Door” and in the layout “Frame”, any number of buttons can be configured. If more buttons are configured than can be displayed in the selected format, the buttons that are not displayed can be displayed by scrolling.

[7] Delete selected Buttons: Delete the selected buttons.

[8] Select button: Activate to select the button.

[9] Type: Select the call type. This function affects the actions “Call”, “Chain Call” and “Parallel Call” only. Default: “Standard”.

Options:

- **Standard:** Calls are initiated using the standard call views.
- **Emergency:** Calls are initiated using the emergency call views.

[10] Upload an image: Select or upload a button image. In the layouts “Door” and “Frame”, the button images are adapted proportionally to the available frame. Button images with the orientation “Portrait” are aligned horizontally to the available frame. Button images with the orientation “Landscape” are aligned vertically to the available frame. Default: no button image available.

Image properties:

- **File size:** max. 6 MB.
- **File format:** JPG, PNG.

Recommendation:

- **Size (W x H):** Depends on the layout and the configuration.
- **Resolution:** 72 dpi.
- **File format:** PNG 24, with transparencies.
- **Colour space:** sRGB.
- **Compression/Quality:** 60/7 to 8.
- Choose square dimensions for buttons in the layouts “Indoor” and “Door” so that images are not distorted on the display.
- Depending on the selection in **[5] Format**, select button-filling images for the layout “Frame”.

In the layouts “Door” and “Frame”, lines with a height of one pixel are used as separators between buttons. For undistorted display of the button images, this dividing line must be taken into account as described below.

Position of the button:

- **The button is placed at the very top:** 1 pixel must be subtracted at the bottom.
- **The button is placed between 2 buttons:** 1 pixel must be subtracted at the top and 1 pixel at the bottom.
- **The button is placed at the very bottom:** 1 pixel must be subtracted at the top.

[11] Delete Image: Delete the button image.

[12] Show text: Activate to display the button text. This function is available for the layout "Indoor" only. Default: activated.

[13] Text: Enter text for the button. A maximum of 50 characters can be entered. Words that have more than 15 characters are shown as "..." from the 15th character. Special characters can be entered. Default: "New Button".

[14] Additional Text: Enter additional button text. A maximum of 50 characters can be entered. Words that have more than 15 characters are shown as "..." from the 15th character. Special characters can be entered. Default: empty.

[15] Action or Action Sequence: Select an action or an action sequence ([see "Available actions", page 182](#)). If a contact is selected for the actions "Call", "Chain Call" and "Parallel Call", the contact name is automatically used. If a profile picture is configured for the contact, the profile picture is automatically used.

[16] Background Colour: Select the background colour behind the buttons. This function is available for the layout "Customized Visualization" only. This function is required only if at least one button is configured. Default: "Black".

Options:

- **Black:** The background is shown in black. The hexadecimal value "#000000" is automatically entered in the field next to **Custom**.
- **Transparent:** The background is shown in black. The hexadecimal value "#00000000" is automatically entered in the field next to **Custom**.
- **Custom:** The background colour can be entered as a hexadecimal value in the field next to **Custom**.
Recommendation: Do not use a blue background, as the buttons are blue and can be difficult to see.

[17] Separator Lines: Activate to show a 1 pixel high separator line between each button. If this function is activated, 1 pixel must be subtracted in the height of each button image for a distortion-free display. This function is only available for the layout "Frame". Default: deactivated.

5.14.3.3. IN CALL

The following functions are available:

General

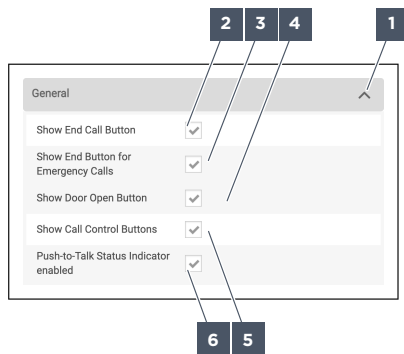


Figure 130: Device - In Call - General

- | | | |
|--------------------------------|------------------------------------|--|
| 1 Configuration area | 2 Show End Call Button | 3 Show End Button for Emergency Calls |
| 4 Show Door Open Button | 5 Show Call Control Buttons | 6 Push-to-Talk Status Indicator enabled |

[1] Configuration area: Maximise or minimise the configuration area.

[2] Show End Call Button: Activate to display the button for ending calls of the type “Standard”. Default: activated.

[3] Show End Call Button for Emergency Calls: Activate to display the button for ending calls of the type “Emergency”. Default: activated.

[4] Show Door Open Button: Activate to display the button for activating the door opener function. This function is available for the layouts “Indoor” and “Customized Visualization” only. Default: activated.

[5] Show Call Control Buttons: Activate to display the buttons for changing the volume, for muting, for holding or for displaying the keypad. This function is available for the layouts “Indoor” and “Customized Visualization” only. Default: activated.

[6] Push-to-Talk Status Indicator enabled: Activate to display the pictograms for the talk/listen visualisation during a push-to-talk call. To display the talk/listen visualisation at the remote device, the remote device must be configured accordingly. Default: activated.

5.14.3.4. INCOMING CALL

The following functions are available:

General

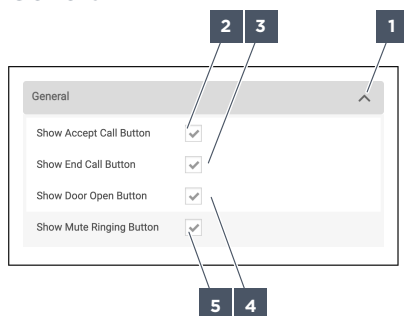


Figure 131: Device - Incoming Call - General

- | | | |
|--------------------------------|-----------------------------------|-------------------------------|
| 1 Configuration area | 2 Show Call Accept Button | 3 Show End Call Button |
| 4 Show Door Open Button | 5 Show Mute Ringing Button | |

[1] Configuration area: Maximise or minimise the configuration area.

[2] Show Call Accept Button: Activate to display the buttons for accepting calls. Default: activated.

[3] Show End Call Button: Activate to display the button for ending calls. Default: activated.

[4] Show Door Open Button: Activate to display the button for activating the door opener function. This function is available for the layouts "Indoor" and "Customized Visualization" only. Default: activated.

[5] Show Mute Ringing Button: Activate to display the button for muting the ringtone. This function is available for the layouts "Indoor" and "Customized Visualization" only. Default: activated.

5.14.3.5. OUTGOING CALL

The following functions are available:

General

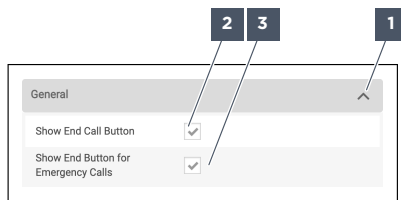


Figure 132: Device - Outgoing Call - General

- 1** Configuration area
- 2** Show End Call Button
- 3** Show End Button for Emergency Calls

[1] Configuration area: Maximise or minimise the configuration area.

[2] Show End Call Button: Activate to display the button for ending calls. Default: activated.

5.14.3.6. ERROR

No functions are available.

5.15. AUDIO

The following functions are available:

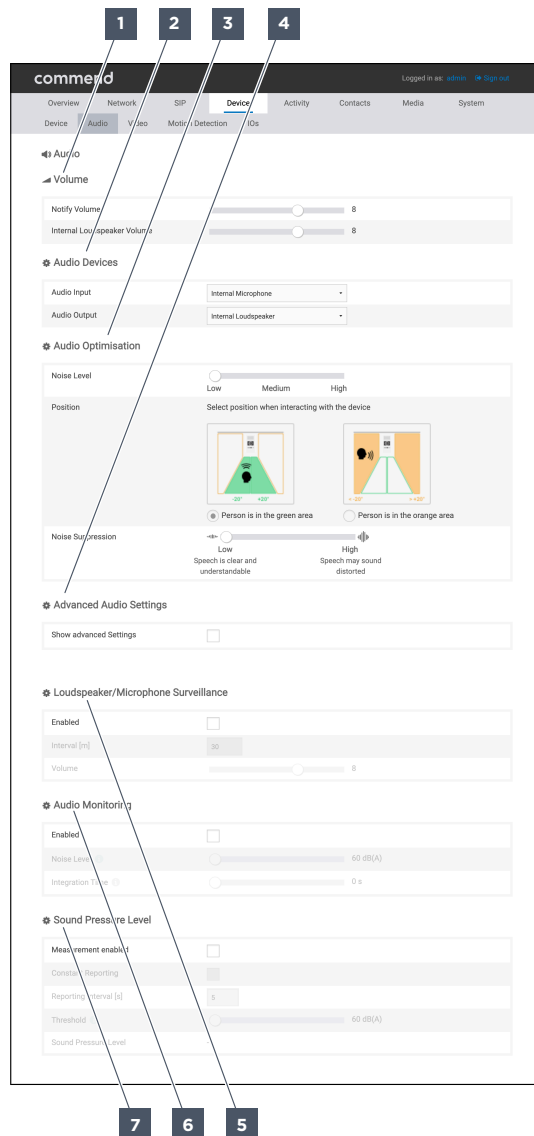


Figure 133: Audio

- | | | |
|----------------------------------|--|-----------------------------|
| 1 Volume | 2 Audio Devices | 3 Audio Optimisation |
| 4 Advanced Audio Settings | 5 Loudspeaker/Microphone Surveillance | 6 Audio Monitoring |
| 7 Sound Pressure Level | | |

[1] Volume: Configure the audio volume.

[2] Audio Devices: Configure the input and output devices.

[3] Audio Optimisation: Easily adapt the device to the acoustic conditions.

[4] Advanced SIP Audio Settings: Carry out detailed adaptation of the device to the acoustic conditions.

[5] Loudspeaker/Microphone Surveillance: Configure loudspeaker/microphone surveillance.

[6] Audio Monitoring: Configure audio monitoring for triggering action sequences.

[7] Sound Pressure Level: Configure the sound pressure level measurement.

5.15.1. VOLUME

The following functions are available:

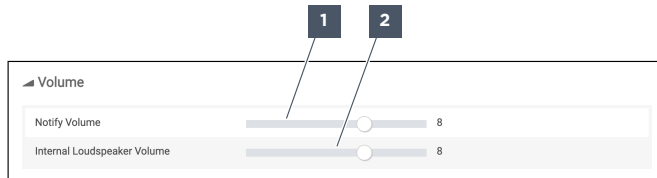


Figure 134: Volume

- 1** Notify Volume
- 2** Internal Loudspeaker Volume

[1] Notify Volume: Adapt the volume of the loudspeaker for notification tones and audio files. Value range: “0” to “12”. Default: “8”.

[2] Internal Loudspeaker Volume: Adapt the volume of the loudspeaker for conversations and announcements. Value range: “0” to “12”. Default: “8”.

Recommendation: To avoid echoes during OpenDuplex calls, do not exceed the volume level “10”.

5.15.1.1. VOLUME WITH HANDSET

If a handset is connected to the device, additional functions are available. The handset must be connected to the device when it is switched off.

The following functions are available:

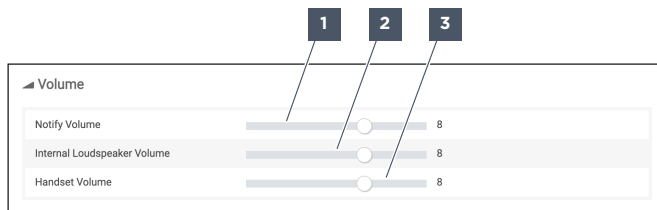


Figure 135: Volume

- 1** Notify Volume
- 2** Internal Loudspeaker Volume
- 3** Handset Volume

[1] Notify Volume: Adapt the volume of the loudspeaker for notification tones and audio files. Value range: “0” to “12”. Default: “8”.

[2] Internal Loudspeaker Volume: Adapt the volume of the loudspeaker for conversations and announcements. Value range: “0” to “12”. Default: “8”.

Recommendation: To avoid echoes during OpenDuplex calls, do not exceed the volume level “10”.

[3] Handset Volume: Adapt the volume of the USB handset. Value range: “0” to “12”. Default: “8”.

i NOTE**Handset Volume**

Handset Volume is displayed when a USB handset is connected for the first time. The **Handset Volume** is displayed when a USB handset is connected after restoring the factory settings.

If the USB handset is disconnected from the device, the **Handset Volume** is still displayed. The configuration remains as is.

5.15.1.2. VOLUME WITH EB3E2A-AUD

If an EB3E2A-AUD is connected to the device, additional functions are available. The EB3E2A-AUD must be connected to the device when it is switched off.

The following functions are available:

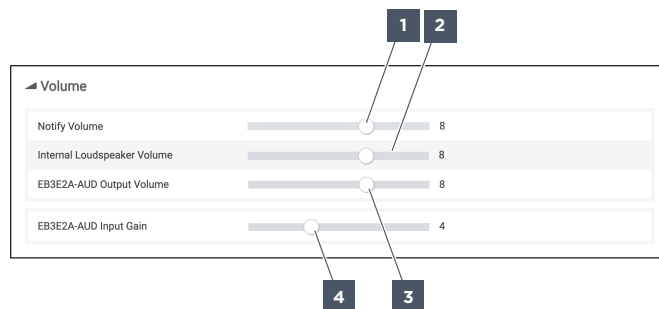


Figure 136: Volume with connected EB3E2A-AUD

- 1** Notify Volume
- 2** Internal Loudspeaker Volume
- 3** EB3E2A-AUD Output Volume
- 4** EB3E2A-AUD Input Gain

[1] Notify Volume: Adapt the volume of the loudspeaker for notification tones and audio files. Value range: “0” to “12”. Default: “8”

[2] Internal Loudspeaker Volume: Adapt the volume of the loudspeaker for conversations and announcements. Value range: “0” to “12”. Default: “8”.

Recommendation: To avoid echoes during OpenDuplex calls, do not exceed the volume level “10”.

[3] EB3E2A-AUD Output Volume: Adapt the output volume of the EB3E2A-AUD. The output volume applies to all modes of the EB3E2A-AUD (see “Audio Devices with EB3E2A-AUD”, page 121). Value range: “0” to “12”. Default: “8”.

[4] EB3E2A-AUD Input Gain: Adapt the input gain of the EB3E2A-AUD. The input volume applies to the line-in and the microphone input (see “Audio Devices with EB3E2A-AUD”, page 121). The input gain can be adjusted in 1-dB steps. The value “0” equals an input gain of 4 dB. Input signals can be amplified by a maximum of 16 dB. Value range: “0” to “12”. Default: “4”.

i NOTE**Output volume and input gain of an EB3E2A-AUD**

EB3E2A-AUD Output Volume and **EB3E2A-AUD Input Gain** are displayed when an EB3E2A-AUD is connected for the first time. **EB3E2A-AUD Output Volume** and **EB3E2A-AUD Input Gain** are displayed when an EB3E2A-AUD is connected after restoring the factory settings.

If an EB3E2A-AUD is disconnected from the device, **EB3E2A-AUD Output Volume** and **EB3E2A-AUD Input Gain** are still displayed. The configuration remains as is.

5.15.2. AUDIO DEVICES

The following functions are available:

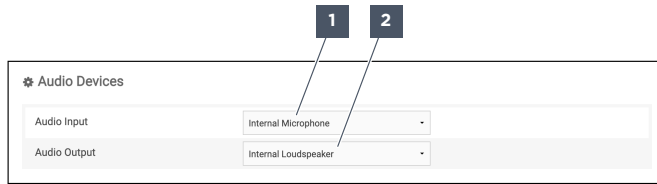


Figure 137: Audio Devices

- 1 Audio input
- 2 Audio output

[1] Audio Input: Select the audio input or microphone. Default: “Internal Microphone”.

i NOTE
Accessories
 This function is displayed only if an accessory is connected.

[2] Audio Output: Select the audio output or loudspeaker. Default: “Internal Loudspeaker”.

i NOTE
Accessories
 This function is displayed only if an accessory is connected.

5.15.2.1. AUDIO DEVICES WITH ID5 DKGM OR ID5 DKHSGM

If an ID5 DKGM or ID5 DKHSGM is connected to the device, additional functions are available. The ID5 DKGM or ID5 DKHSGM must be connected to the device when it is switched off.

The following functions are available:

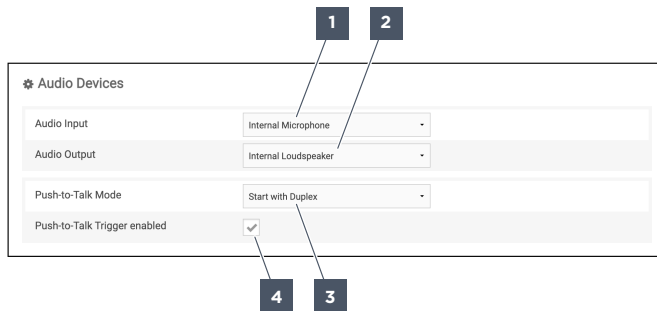


Figure 138: Audio Devices

- 1 Audio Input
- 2 Audio Output
- 3 Push-to-Talk Mode
- 4 Push-to-Talk Trigger enabled

[1] Audio Input: Select the audio input or microphone. Default: “Internal Microphone”.

i NOTE
Accessories
 This function is displayed only if an accessory is connected.

[2] Audio Output: Select the audio output or loudspeaker. Default: “Internal Loudspeaker”.

i NOTE

Accessories

This function is displayed only if an accessory is connected.

[3] Push-to-Talk Mode: Selecting the call behaviour when using the accessory ID5 DKGM or ID5 DKHSGM. Default: “Start with Duplex”.

Options:

- **Start with Duplex:** Calls are established in duplex mode. The person at the device and the person at the remote station can speak simultaneously. When the Push-to-Talk button is pressed, the device switches to the simplex-like mode.
 - **Start with Simplex:** Calls are established in the simplex-like mode. The person at the device can speak only when the “Push to Talk” button is pressed. The person at the remote station can speak only when the “Push to Talk” button is not pressed.
- Recommendation:** Use this option for door applications.
- **Disable Push to Talk function:** Calls are established in duplex mode. Pressing the “Push to Talk” button does not change the call behaviour.

i NOTE

Accessories

Accessories options can be configured only when the respective accessory is connected.

[4] Push-to-Talk Trigger enabled: Enable in order to use the “Push to Talk” button as a trigger for action sequences. This function must be activated for Push to Talk calls. Default: enabled.

Example: see “Operating the door opener”, page 127.

i NOTE

Accessories

Accessories options can be configured only when the respective accessory is connected.

5.15.2.2. AUDIO DEVICES WITH EB3E2A-AUD

If an EB3E2A-AUD is connected to the device, additional functions are available. The EB3E2A-AUD must be connected to the device when it is switched off.

The following functions are available:

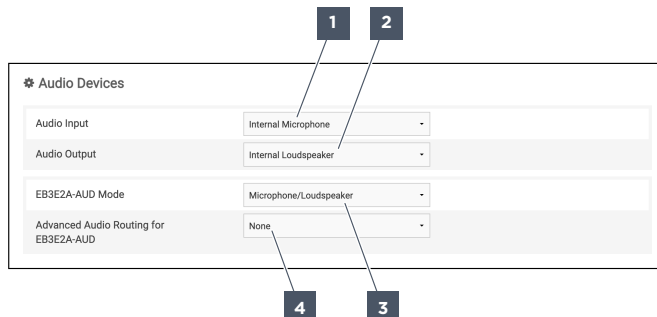


Figure 139: Audio Devices with EB3E2A-AUD

1 Audio input

2 Audio output

3 EB3E2A-AUD Mode

4 Advanced Audio Routing
for EB3E2A-AUD

[1] Audio Input: Select the audio input or microphone. Default: "Internal Microphone".

i **NOTE**

Accessories

This function is displayed only if an accessory is connected.

[2] Audio Output: Select the audio output or loudspeaker. Default: "Internal Loudspeaker".

i **NOTE**

Accessories

This function is displayed only if an accessory is connected.

[3] EB3E2A-AUD Mode: Select the operation mode for the EB3E2A-AUD. In **[1] Audio Input**, the option "EB3E2A-AUD Input" must be selected, and in **[2] Audio Output**, the option "EB3E2A-AUD Output" must be selected. Default: "Microphone/Loudspeaker".

Options:

- **Microphone/Loudspeaker:** Audio input is done via "MIC" and audio output is done via "LS" of the EB3E2A-AUD.
- **Line-in/Line-out:** Audio input is done via "LINE IN" and audio output is done via "LINE OUT" of the EB3E2A-AUD.
- **Handset:** Audio input and audio output are done via "HAND SET" of the EB3E2A-AUD.
- **Headset:** Audio input and audio output are done via "HEAD SET" of the EB3E2A-AUD.
- **Gooseneck Microphone:** Audio input and audio output are done via "GOOSENECK MIC" of the EB3E2A-AUD.

[4] Advanced Audio Routing for EB3E2A-AUD: Select the advanced audio routing of the EB3E2A-AUD. Default: „None“.

Options:

- **None:** No advanced audio routing is used.
- **Provide Call Recording Mix to Line Out:** Audio signals of calls are put out through the connections "LINE OUT" of the EB3E2A-AUD. When an ID5 DKGM or an ID5 DKHSGM is used in simplex mode, the audio channel that cannot currently speak is muted depending on the push-to-talk function. Only the audio channel that can currently speak is put out at the line-out.
Example: For analogue call recording.
- **Provide any Device Audio to Line OUT:** Audio signals of the device are put out through the connections "LINE OUT" of the EB3E2A-AUD.
Example: For amplifying audio signal of the device through a PA.
- **Feed Line In to Audio Output in Idle:** Audio signals, which are present at the connections "LINE IN" of the EB3E2A-AUD, are put out through the device. The audio signals are only put out in the device state "Idle".
Example: For analogue music feed-in.

5.15.3. AUDIO OPTIMISATION

The following functions are available:

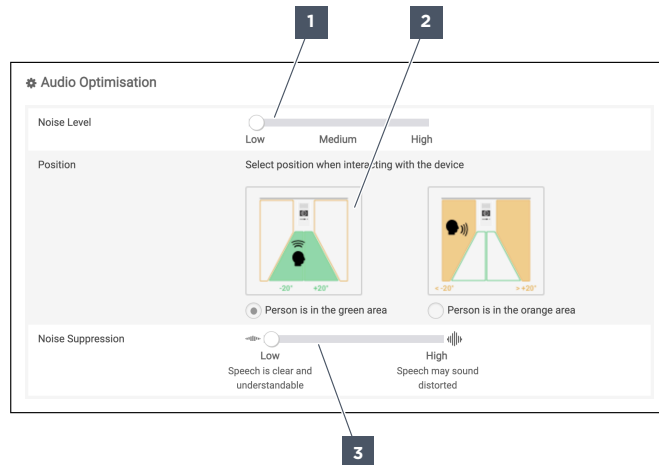


Figure 140: Audio Optimisation

1 Noise Level

2 Position

3 Noise Suppression

Changing the configuration affects the parameters in **Advanced Audio Settings**.

[1] Noise Level: Select the noise level of the environment. Default: “Low”.

Options:

- **Low:** Environment with low noise level.
Example: One-person offices.
- **Medium:** Environment with medium noise level.
Example: Entrance areas of buildings.
- **High:** Environment with high noise level.
Example: Subway stations.

[2] Position: Select the default position of the person speaking. Default: “Person is in the green area”.

Options:

- **Person is in the green area:** The person speaking is normally in front of the device.
- **Person is in the orange area:** The person speaking is normally to the side of the device.

[3] Noise Suppression: Adjust the noise suppression in five steps. Default: “Low”.

The further the controller is in the “Low” position, the clearer and more understandable the speech is. Noise such as static or background noise is only weakly suppressed or are not suppressed at all.

The further the controller is in the “High” position, the more distorted the speech can be. Noise such as static or background noise is effectively suppressed.

5.15.4. ADVANCED AUDIO SETTINGS

The following functions are available:

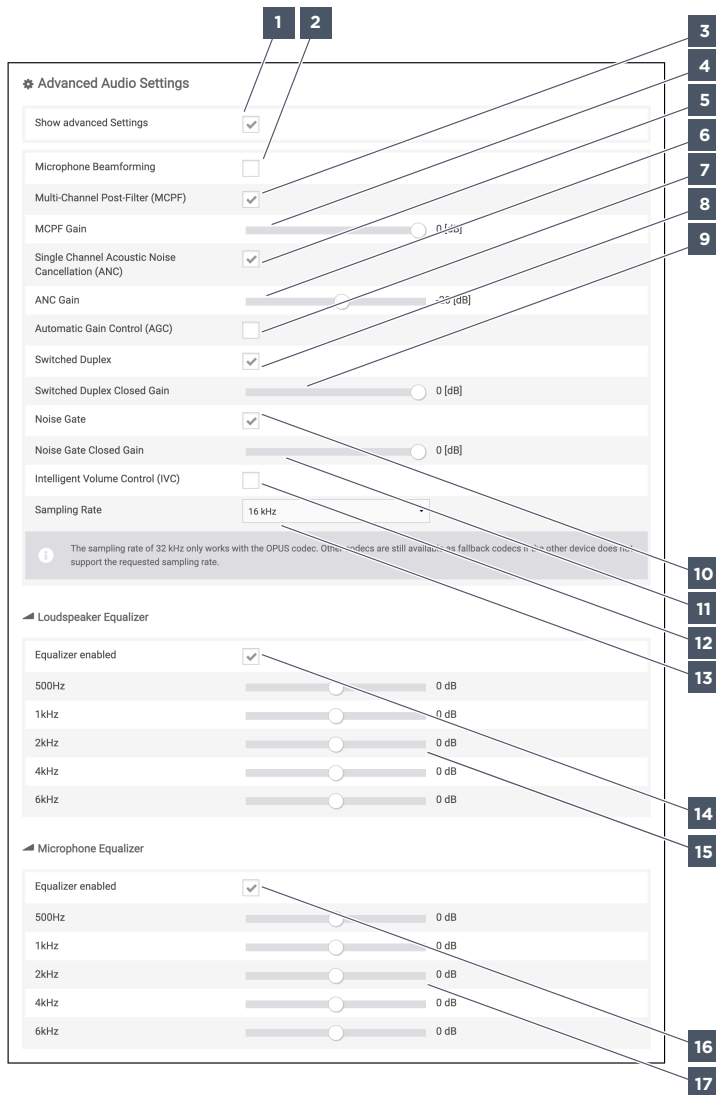


Figure 141: Advanced Audio Settings

- | | | |
|---------------------------------------|---|--|
| 1 Show advanced Settings | 2 Microphone Beamforming | 3 Multi-Channel Post-Filter (MCPF) |
| 4 MCPF Gain | 5 Single Channel Acoustic Noise Cancellation (ANC) | 6 ANC Gain |
| 7 Automatic Gain Control (AGC) | 8 Switched Duplex | 9 Switched Duplex Closed Gain |
| 10 Noise Gate | 11 Noise Gate Closed Gain | 12 Intelligent Volume Control (IVC) |
| 13 Sampling Rate | 14 Equalizer enabled | 15 Frequencies |
| 16 Equalizer enabled | 17 Frequencies | |

⚠ CAUTION**Incorrect or incomplete configuration**

Device or software malfunction

- Have experts carry out the configuration.

If too many interfering signal portions are transmitted, useful signal portions at the remote device are masked by the interfering signal portions at higher volumes.

To suppress loud background noise, the device has to be additionally configured. The configuration depends on the installation location of the device.

Recommendation: If the device is installed outdoors under free-field conditions (mostly direct sound, hardly any diffuse sound), activate **[2] Microphone Beamforming**, activate **[3] Multi-Channel Post-Filter (MCPF)** and adjust **[4] MCPF Gain** to “-6 [dB]” or lower. If the noise suppression is not enough, activate **[5] Single Channel Acoustic Noise Cancellation (ANC)** and adjust **[6] ANC Gain** to a lower value.

Recommendation: If the device is installed indoors (much diffuse sound), activate **[5] Single Channel Acoustic Noise Cancellation (ANC)** and adjust **[6] ANC Gain** to “-6 [dB]” or lower.

[1] Show advanced Settings: Activate to show advanced settings. “Audio Optimisation” is deactivated. Default: deactivated.

[2] Microphone Beamforming: Activate to automatically focus the recording area with the highest sensitivity on the person who is speaking. Default: deactivated.

[3] Multi-Channel Post-Filter (MCPF): Activate to reduce the diffuse sound portions in the signal. Default: deactivated.

[4] MCPF Gain: Adjust the reduction of the diffuse sound portions. At most, the diffuse sound portions are reduced by this value. Range of values: “0 [dB]” (dBFS) to “-45 [dB]” (dBFS). Default: “0 [dB]”.

[5] Single Channel Acoustic Noise Cancellation (ANC): Activate to reduce the useful signal portions by weakening the interfering signal portions. Default: deactivated.

[6] ANC Gain: Adjust the noise suppression. At most, the interfering signals are reduced by this value. Range of values: “0 [dB]” (dBFS) to “-45 [dB]” (dBFS). Default: “-20 [dB]”.

[7] Automatic Gain Control (AGC): Activate to adjust the input signal level automatically. Low input signal levels of other devices are increased by up to 24 dB. This reduces possible compatibility problems. Default: deactivated.

Recommendation: Activate this function for calls to or from third-party devices.

[8] Switched Duplex: Activate to enable calls in Switched Duplex mode. Calls are established in Switched Duplex mode only if this function is activated on both devices. Default: deactivated.

[9] Switched Duplex Closed Gain: Adjust the reduction of signals from the remote station when someone is speaking into the device. Range of values: “0 [dB]” (dBFS) to “-96 [dB]” (dBFS). Default: “0 [dB]”.

[10] Noise Gate: Activate to transmit signals that exceed the threshold of the noise gate. Default: deactivated.

[11] Noise Gate: Adjust the reduction of signals below the threshold. Range of values: “0 [dB]” (dBFS) to “-96 [dB]” (dBFS). Default: “0 [dB]”.

[12] Intelligent Volume Control (IVC): Activate to automatically raise or lower the loudspeaker volume and microphone volume. The speaking conditions are adjusted based on the background noise. Default: deactivated.

[13] Sampling Rate: Select the sampling rate for audio signals. Default: "16 kHz".

Options:

- **8 kHz:** Low audio quality and low data transmission rate.
- **16 kHz:** Standard audio quality and moderate data transmission rate.
- **32 kHz:** High audio quality and high data transmission rate. This sampling rate is supported only by the audio codec "Opus". If this sampling rate is not supported by other devices, the other audio codecs are still available as fall-back options.

[14] Equalizer enabled: Activate to use the graphic equalizer for the built-in loudspeaker. Audio signals can be optimised in situations involving challenging acoustics. Default: deactivated.

⚠ CAUTION

Incorrect Configuration

Unusable audio signal or poor intelligibility

- Have experts carry out the configuration.

The device is acoustically optimised ex works for the intended use.

[15] Frequencies: Adjust the frequency ranges of the graphic equalizer. Range of values: "-12 dB" to "12 dB". Default: "0 dB".

[16] Equalizer enabled: Activate to use the graphic equalizer for the built-in microphone. Audio signals can be optimised in situations involving challenging acoustics. Default: deactivated.

⚠ CAUTION

Incorrect Configuration

Unusable audio signal or poor intelligibility

- Have experts carry out the configuration.

The device is acoustically optimised ex works for the intended use.

[17] Frequencies: Adjust the frequency ranges of the graphic equalizer. Range of values: "-12 dB" to "12 dB". Default: "0 dB".

5.15.5. LOUDSPEAKER/MICROPHONE SURVEILLANCE

The following functions are available:



Figure 142: Loudspeaker/Microphone Surveillance

- 1 Enabled
- 2 Intervall [m]
- 3 Volume

The loudspeaker reproduces a white noise test signal at configurable intervals. This is recorded by the microphone. The internal digital signal processor (DSP) analyses the frequency spectrum of the recorded signal. In case of a fault, the device repeats this process. If the fault recurs, the device switches to the device state "Fault".

Action sequences can be initiated through activities.

Example: Sending an e-mail.

Loudspeaker/microphone surveillance functions only with the built-in microphones and the built-in loudspeaker. Loudspeaker/microphone surveillance cannot be used with external components such as a gooseneck microphone or a separate loudspeaker.

[1] Enabled: Enable in order to perform loudspeaker/microphone surveillance automatically at the configured intervals. Default: disabled.

[2] Interval [m]: Enter the interval time in minutes. Value Range: "1" to "525600". Default: "30".

[3] Volume: Adapt the volume of the test signal. Value Range: "0" to "12". Default: "8".

Recommendation: Configure the volume level as low as possible to avoid the test signal from being perceived as disturbing. Loud environments require a higher volume level in order to ensure that loudspeaker/microphone surveillance can be performed reliably.

5.15.6. AUDIO MONITORING

The following functions are available:

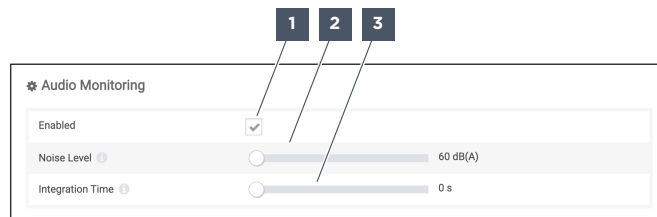


Figure 143: Audio Monitoring

1 Enabled

2 Noise Level

3 Integration Time

[1] Enabled: Enable in order to use the Audio Monitoring function. Action sequences can be initiated. SNMP trap packets can be sent. The Audio Monitoring function is disabled during calls and when performing action sequences. Default: disabled.

[2] Noise Level: Adjust the threshold. If the threshold is exceeded, the audio monitoring function is initiated. Value Range: "60 dB(A)" to "87 dB(A)". Default: "60 dB (A)".

[3] Integration Time: Adjust the integration time in seconds. The threshold must exceed at least this integration time to initiate the Audio Monitoring function. Value Range: "0 s" to "15 s". Default: "0 s".

5.15.7. SOUND PRESSURE LEVEL

The following functions are available:

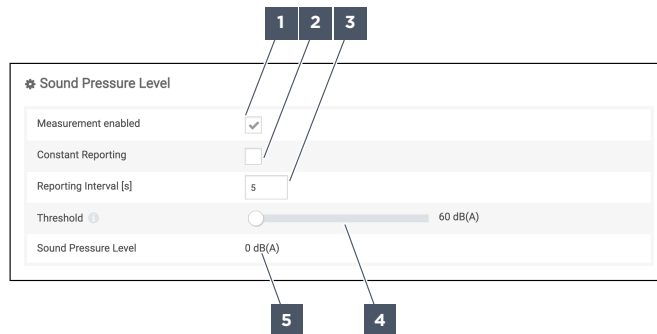


Figure 144: Sound Pressure Level

- | | | |
|------------------------------|-------------------------------|---------------------------------|
| 1 Measurement enabled | 2 Constant Reporting | 3 Reporting Interval [s] |
| 4 Threshold | 5 Sound Pressure Level | |

The sound pressure level measurement can be performed at constant intervals or if the threshold is exceeded.

[1] Measurement enabled: Enable in order to measure the sound pressure level using the built-in microphones or an external microphone. Action sequences can be initiated. SNMP trap packets can be sent. Default: disabled.

[2] Constant Reporting: Enable in order to constantly send the sound pressure level as SNMP trap packets. **[4] Threshold** is disabled. Default: enabled.

[3] Interval [s]: Enter the interval time in seconds. The interval time defines the intervals at which constant sound pressure level measurements are performed. Value Range: "5" to "86400". Default: "5".

[4] Threshold: Adjust the threshold. If the threshold is exceeded, action sequences can be initiated or SNMP trap packets sent. "60 dB(A)" to "87 dB(A)" value range. Default: "60 dB (A)".

[5] Sound Pressure Level: Shows the last detected sound pressure level in dB(A).

5.16. VIDEO

The following functions are available:

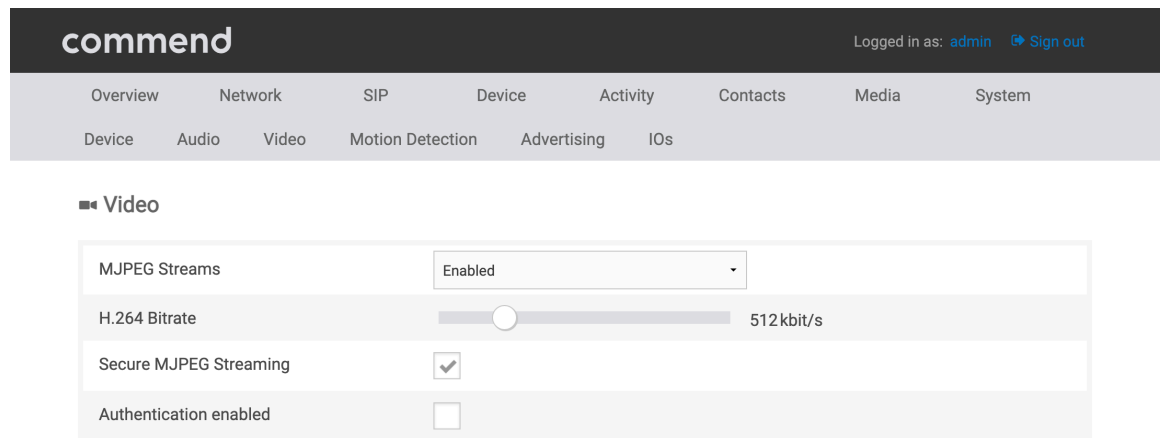


Figure 145: Video

- 1 MJPEG Streams
- 2 H.264 Bit Rate
- 3 Secure MJPEG Streaming
- 4 Enable Authentication

[1] MJPEG Streams: Selects the video streaming behaviour. Default: “Enabled”.

Options:

- **Enabled:** Up to six video streams can be called up simultaneously within a network using the device.
- **Example:** Using computers, smartphones, tablets.
- **Limited:** Using the device, only one video stream can be called up during a call. Devices within a network cannot access the camera image of the device.
- **Disabled:** No video streams can be called up using the device.

[2] H.264 Bit Rate: Adjust the bit rate for H.264 video streams. Value Range: “128 kbps” to “2048 kbps”. Default: “512 kbps”.

[3] Secure MJPEG Streaming: Enable in order to call up video streams of the device via HTTPS. If this function is not enabled, video streams of the device can be called up via HTTP and HTTPS. Default: enabled.

Recommendation: If this function is activated, activate **[4] Enable Authentication**.

[4] Enable Authentication: Enable in order to ensure that video streams and still pictures can be called up only after authentication. If this function is enabled and the URL for video streams or still pictures are entered in the address bar of a web browser, a dialogue appears. In this dialogue, the login data of the user must be entered in order to call up video streams or still pictures. For the user, an API token must be configured. Default: disabled.

5.17. MOTION DETECTION

The following functions are available:

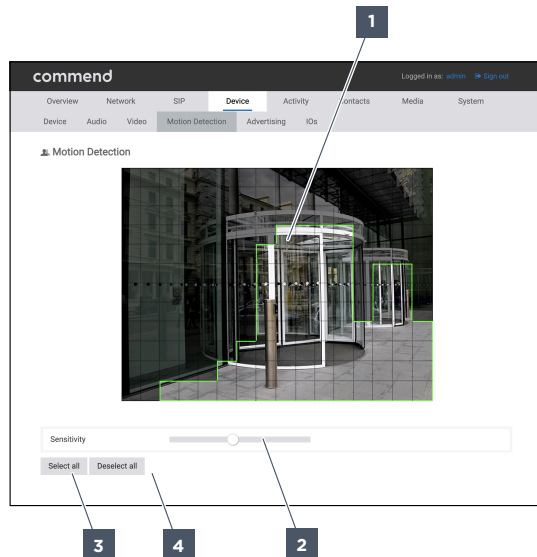


Figure 146: Motion detection

- | | | | | | |
|---|--------------|---|-------------|---|------------|
| 1 | Video image | 2 | Sensitivity | 3 | Select all |
| 4 | Deselect all | | | | |

“True” messages are sent every 2 seconds for the duration of motion detection. If no more motion is detected, a “false” message is sent. If incoming or outgoing calls are initiated, a “false” message is sent. The “false” message interrupts continuing action sequences. The Motion Detection function is disabled during calls.

If the option “Limited” or “Disabled” is selected in **MJPEG Streams**, only one still picture is shown as a video preview (see “Video”, page 129). The still picture is created when **Motion Detection** is called up.

[1] Video image: Displays the video preview in real time or as a still picture. Select the box in the area of the video preview in which motion is detected. A 12 x 16 grid of boxes can be enabled in the video preview. Default: “All selected”.

Options:

- **Normal brightness and green border:** The boxes in the video preview are enabled for motion detection.
- **Shaded and no border:** The boxes in the video preview are disabled for motion detection.

Recommendation: Only enable the boxes in the area of the video preview in which the motions of people in front of the device can be detected. Disable the boxes in the area of the video preview in which unwanted motion such as road traffic, trees or clouds can be detected.

[2] Sensitivity: Adjust the sensitivity for motion detection in the enabled boxes.

[3] Select all: Enable all boxes in the video preview for motion detection.

[4] Deselect all: Disable all boxes in the video preview for motion detection.

5.18. ADVERTISING

The following functions are available:

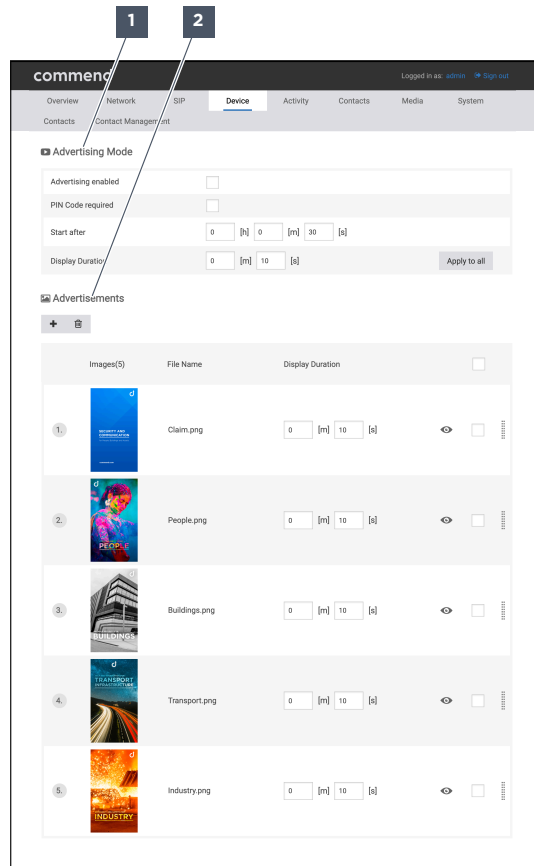


Figure 147: Advertising

1 Advertising Mode **2** Advertisements

[1] Advertising Mode: Configure the advertising mode.

[2] Advertisements: Manage advertisements.

5.18.1. ADVERTISING MODE

The following functions are available:

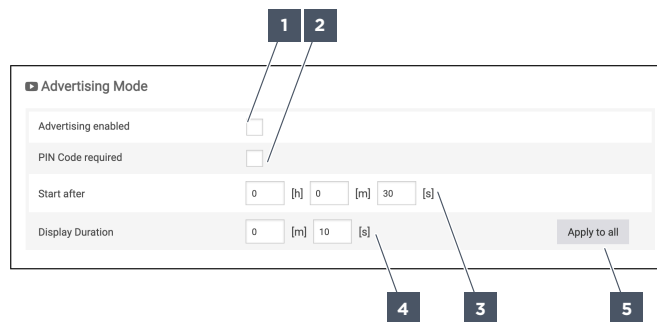


Figure 148: Advertising - Advertising Mode

1 Advertising enabled **2** PIN Code required

3 Start after

4 Display Duration**5** Apply to all

Advertisements can only be shown in device state “Idle”. Advertisements can be interrupted by incoming calls, touching the display or action sequences.

[1] Advertising enabled: Activate to display advertisements. When the advertising mode is activated, the display can be turned off automatically after a configurable timeout. In software versions lower than 03.00.01, the display is not turned off while the advertising mode is activated if a timeout is configured. When updating from a software version of 02.09 or lower to the software version 03.00.01 or higher, the timeout for turning off the display is deactivated. The advertising mode can be used as screen saver. Default: enabled.

[2] PIN Code required: Activate to require entry of the PIN code to interrupt the advertising mode on the device (see [“Passwords”, page 169](#)). Default: disabled.

[3] Start after: Enter the time in hours, minutes and seconds after which the advertising mode is started. Default: “30 [s]”.

[4] Display Duration: Enter the time in minutes and seconds after which the next advertisement is displayed. Default: “10 [s]”.

[5] Apply to all: Apply the time configured in **[4] Display Duration** to all advertisements. The display duration time of all advertisements is exceeded.

5.18.2. ADVERTISEMENTS

The following functions are available:

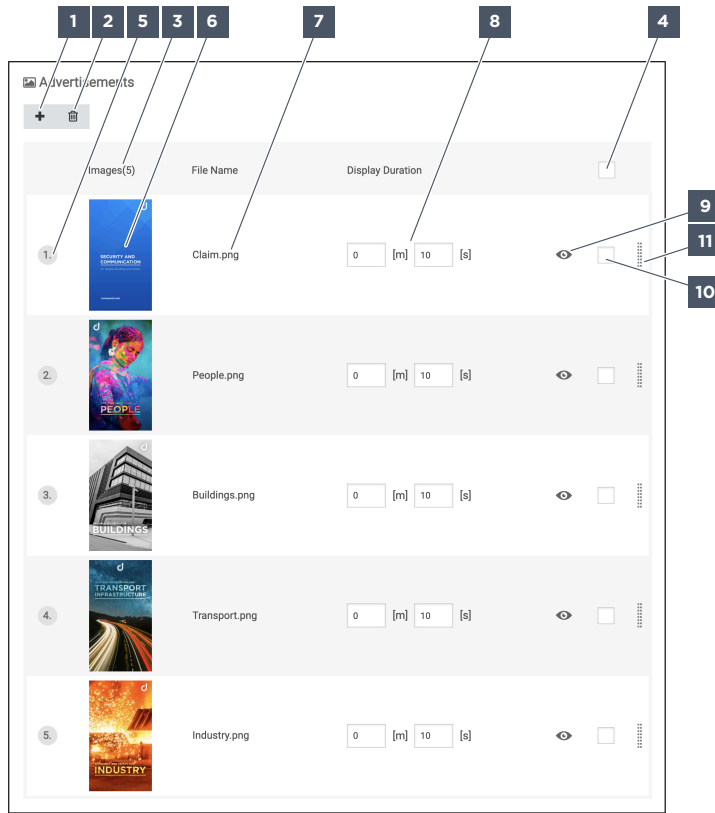


Figure 149: Advertising - Advertisements

- | | | |
|------------------------------------|---|-----------------------------------|
| 1 Add Advertisement | 2 Delete Selected Advertisement(s) | 3 Available Advertisements |
| 4 Select All Advertisements | 5 Advertisement Display Sequence | 6 Image |
| 7 File Name | 8 Display Duration | 9 Hide |
| 10 Select Advertisement | 11 Move Advertisement | |

By default, 5 advertisements are available on the device.

Recommendation: Disable all ad blockers in the web browser during configuration. Ad blockers in the web browser prevent images from being displayed.

If different advertisements need to be displayed for certain purposes, the device can be configured for these purposes. The configuration can be exported. If a certain configuration is required for advertisements, the configuration can be imported for these purposes.

Recommendation: Give the exported configuration a unique name.

[1] Add Advertisement: Adds an advertisement. A maximum of 25 advertisements can be managed. Several images can be uploaded simultaneously.

Recommendation: If the advertising mode shall be used over a longer period without interruption, use different images. Various images prevent damage to the display and image persistence.

[2] Delete Selected Advertisement(s): Deletes the selected advertisements.

[3] Available Advertisements: Shows the total number of available advertisements.

[4] Select All Advertisements: Enable in order to select all advertisements.

[5] Advertisement Display Sequence: Shows the order in which the advertisement images are shown.

[6] Image: Shows the image of the advertisement. Uploads an image for the advertisement.

Image properties:

- **Image size:** max. 6 MB.
- **File format:** JPG, PNG. The transparencies of a PNG file are kept.

Recommendation:

- **Size (W x H):** 720 x 1280 pixels.
- **Resolution:** 72 dpi.
- **File format:** JPG.
- **Colour space:** sRGB.
- **Compression/quality:** 60/7 to 8.

[7] File Name: Shows the file name of the advertisement. The file name is applied when the image is uploaded. The file name cannot be changed in the web interface of the device.

[8] Display Duration: Enter the time in minutes and seconds in which the advertisement should be displayed on the device. Default: "10 [s]".

[9] Hide: Hides the advertisement.

Example: Shows or hides certain advertisements for events.

[10] Select Advertisement: Select the advertisement.

[11] Move Advertisement: Change the advertisement display sequence by moving the advertisement to the desired spot.

5.19. IOS

The following functions are available:

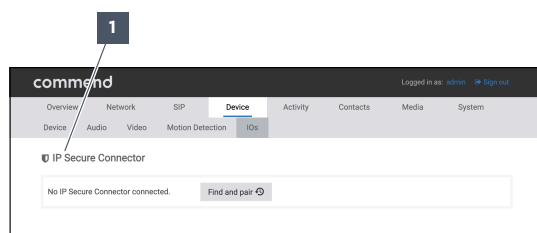


Figure 150: IOs

1 Find and pair

IP-CON supplies the device with power when the "Pairing" button on the IP-CON is pressed. Once the "Pairing" button is pressed, the device can be paired with the IP-CON within 5 seconds.

When the device is started and connected to the "Display" socket of the IP-CON, the device automatically pairs with the IP-CON. The device also pairs with the IP-CON automatically when the device is connected to the Symphony Cloud Platform.

If the device was previously paired with another IP-CON, this configuration is overwritten.

[1] Search and Pair: Pairs the device with an IP-CON.

5.20. ACTIVITY

The following functions are available:

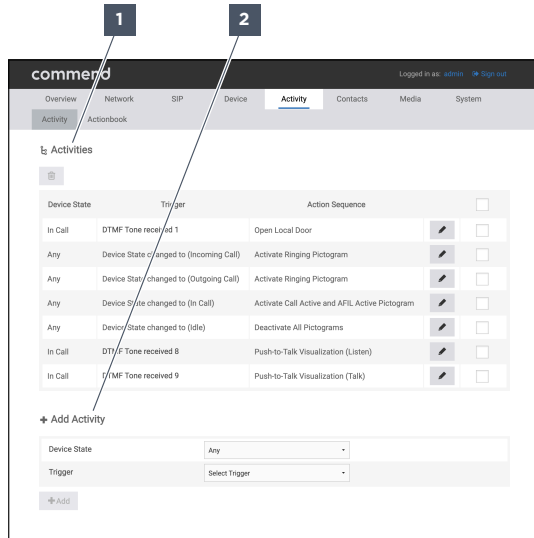


Figure 151: Activity

- 1 Activities
- 2 Add Activity

Activities can be used to trigger automatic action sequences.

[1] **Activities:** Manage activities.

[2] **Add Activity:** Add new activities.

5.20.1. ACTIVITIES

The following functions are available:

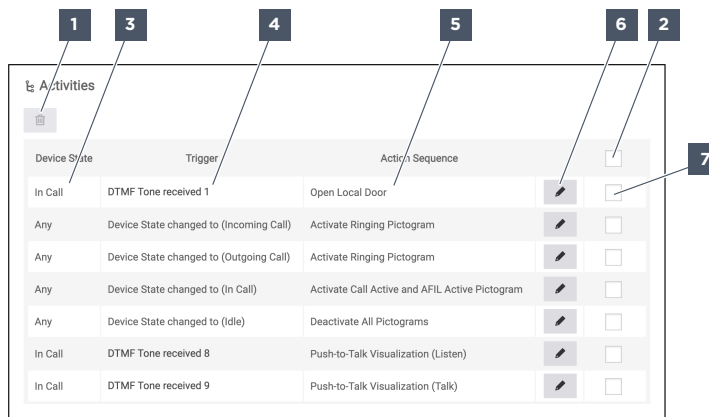


Figure 152: Activity - Activities

- 1 Delete Activity
- 2 Select all Activities
- 3 Device State
- 4 Trigger
- 5 Action Sequence
- 6 Edit
- 7 Edit Activity

[1] Delete Activity: Delete the selected activities.

[2] Select All Activities: Enable this option to select all activities at once.

[3] Device State: Shows the state of the device when the action sequence is triggered.

[4] Trigger: Shows the trigger for the action sequence. If external hardware that was configured for an activity is removed or no longer available, a “(removed)” or “(unreachable)” label is shown in red next to the activity in question.

[5] Action Sequence: Shows the action sequence to which the activity is linked.

[6] Edit: Edit the activity.

[7] Select Activity: Tick the box of an activity to select it.

5.20.2. ADD ACTIVITY

The following functions are available:

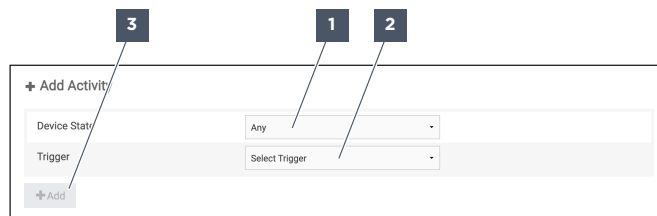


Figure 153: Activity – Add Activity

1 Device State 2 Trigger 3 Add

An activity cannot be added more than once with the same configuration settings. An activity can only have one action sequence linked to it. An activity cannot trigger different action sequences under different conditions, e. g. at different times of day or days of the month.

[1] Device State: Select the state that the device should be in when the action sequence is triggered.

Options:

- **All:** The trigger will fire regardless of the device’s state at the time.
- **Idle:** The trigger will fire only if the device is in device state “Idle”.
- **Active (Call):** The trigger will fire only if the device is in device state “In Call”.
- **Incoming Call:** The trigger will fire only if the device is in device state “Incoming Call”.
- **Outgoing Call:** The trigger will fire only if the device is in device state “Outgoing Call”.
- **Error:** The trigger will fire only if the device is in device state “Error”.

[2] Trigger: Select the trigger for the action sequence.

Options:

- **Current Sound Pressure Level:** The trigger will fire only if sound pressure level gauging is activated and the configured threshold level is exceeded.
- **Audio Monitoring:** The trigger will fire only if the audio monitoring function is activated and the configured threshold level is exceeded.
- **Outgoing Call:** The trigger will fire only when an outgoing call is detected.
- **Motion Detection:** The trigger will fire only when an outgoing call is detected.
- **Cronjob:** The trigger will fire only if the conditions of the configured cronjob pattern are met (see “Cronjob syntax”, page 138). Cronjobs can be used to trigger action sequences automatically at specific times, dates or intervals. It is also possible to set time schedules for automated systems. This function uses the local device time for scheduling.
- **DTMF Tone received:** The trigger will fire only when the configured DTMF tone is received.

- **Input Change:** The trigger will fire only if a change in the input signal is detected on an accessory unit.
 - **1k5:** Button 1
 - **2k2:** Button 2
 - **2k7:** Button 3
 - **3k3:** Button 4
 - **4k7:** Button 5
 - **6k8:** Button 6
 - **8k2:** Button 7
 - **10k:** Button 8
 - **15k:** Button 9
- **Incoming Call:** The trigger will fire only when an incoming call is detected.
- **Device State changed:** The trigger will fire only when the device switches to the specified device state.
- **HTTP Request received:** The trigger will fire only when the configured HTTP request is received. It is possible to configure an HTTP or HTTPS request.
- **Loudspeaker/Microphone Surveillance:** The trigger will fire only if the loudspeaker/microphone self-monitoring function returns a positive or negative result.
- **Push-to-Talk Button:** The trigger will fire only when the Push-to-Talk button is pressed or released. An ID5 DKGM or ID5 DKHSGM must be connected to use this trigger.

[3] **Add:** Add the activity.

5.20.3. EDITING AN ACTIVITY

The following functions are available:

Figure 154: Activity - Editing an activity

- | | | |
|----------------------------------|-----------|----------|
| 1 Device State | 2 Trigger | 3 Option |
| 4 Action Sequence to be executed | 5 Edit | 6 Back |

[1] Device State: Shows the state of the device when the action sequence is triggered. Once the device state condition has been set, it cannot be changed. To change the device state condition, you will have to delete the activity and add a new one with the desired condition.

[2] Trigger: Shows the trigger for the action sequence. If external hardware that was configured for an activity is removed or no longer available, a “(removed)” or “(unreachable)” label is shown in red next to the activity in question. Once the trigger condition has been set, it cannot be changed. To change the trigger condition, you will have to delete the trigger and add the desired one.

[3] Option: Select an option for the trigger. Options are provided only for certain triggers.

[4] Action Sequence to be executed: Select the action sequence that should be run.

[5] Edit: Edit the action sequence selected under **[4] Action Sequence to be executed** . If no action sequence has been selected under **[4] Action Sequence to be executed**, you can add one. The action sequence will be added under **Action Sequences** .

[6] Back: Navigate back to **Activities**. Any unsaved changes of activity settings will be lost.

5.20.4. CRONJOB SYNTAX

A Cronjob trigger consist of 6 parts separated by a space. Each part can be scheduled in specific time units, such as seconds, hours or days. The syntax elements of a Cronjob are structured as follows.

Syntax elements:

- **<Second>:** "0" to "59".
- **<Minute>:** "0" to "59".
- **<Hour>:** "0" to "24". Time is specified in 24-hour format.
- **<Day of Month>:** "1" to "31". The value range depends on the month.
- **<Month of Year>:** "1" to "12". "1" stands for "January", "12" stands for "December".
- **<Day of Week>:** "1" to "7". "1" stands for "Monday", "7" stands for "Sunday".

The names of days and months have to be entered in English.

Syntax exceptions:

- Multiple values for a parameter can be specified in sequence, separated by a comma.
Example: "1,3".
- A parameter's value range can be defined by inserting a hyphen between the start and end values.
Example: "1-5".
- An asterisk (*) can be used as a wildcard to indicate the entire possible value range of a parameter.
Example: "*" can be used as a wildcard for "every minute", "every hour" or "every day".
- A "?" may be used to indicate that a parameter should be ignored. Using a "?" is useful for avoiding redundant input.
Example: Entering "1-7" for parameter **<Day of Week>**: makes it unnecessary to enter a value for parameter **<Day of Month>**.
- After an asterisk "*" or value range, the character "/" followed by any value can be entered in order to run actions within a fixed time interval.
Example: Entering "0-23/2" for parameter **<Hour>** causes the specified action to be executed once every two hours. Entering "**/4" for parameter **<Minute>** causes the specified action to be executed once every four minutes.

Recommendation: You should use a generator to create Cronjob triggers. Example: <https://freeformatter.com/cron-expression-generator-quartz.html>

Cronjob examples:

- ***/5 * * * *:** Executes the specified action automatically every 5 seconds.
- **0 */5 * * * *:** Executes the specified action automatically every 5 minutes.
- **0 */5 * * * *:** Executes the specified action automatically every 5 hours.
- **00 * * * *:** Executes the specified action automatically every hour on the hour.
- **000 * * * *:** Executes the specified action automatically every day at midnight.
- **0001 * * * *:** Executes the specified action automatically at 00:00 (midnight) on the first day of every month.
- **00031 * * * *:** Executes the specified action automatically at 00:00 (midnight) on the 31st day of every month.
- **55 5 * * * *:** Executes the specified action automatically every hour 5 minutes 55 seconds after the hour.
- **007 ? * MON-FRI:** Executes the specified action automatically at 7 a.m. every day from Monday to Friday.
- **00029 2 * * * *:** Executes the specified action automatically at 00:00 (midnight) on February 29th.

- **0 0 * * * MON-FRI:** Executes the specified action automatically from Monday to Friday every hour on the hour.
- **0 0 * * * SUN,MON:** Executes the specified action automatically on Sundays and Mondays every hour on the hour.

5.20.5. PRE-CONFIGURED ACTIVITIES

By default, the system provides the following pre-configured activities, which can be used, edited or deleted as needed.

DTMF Tone received 1

When the device receives DTMF tone “1”, it triggers action sequence “Open Local Door”.

Recommendation: Do not delete this activity.

Default configuration:

- **Device State:** “Active (Call)”.
- **Trigger:** “DTMF Tone received 1”.
- **DTMF Tone:** “1”.
- **Action Sequence to be executed:** “Open Local Door”.

Device State changed to (Incoming Call)

A change to device state “Incoming Call” will trigger action sequence “Activate Ringing Pictogram”. This action is required for displaying the “Ringing” pictogram. If this action is deleted, pictogram “Ringing” will no longer be shown in green when an incoming call is received.

Recommendation: Do not delete this activity.

Default configuration:

- **Device State:** “All”.
- **Trigger:** “Device State changed to”.
- **Until:** “Incoming Call”.
- **Action Sequence to be executed:** “Activate Ringing Pictogram”.

Device State changed to (Outgoing Call)

A change to device state “Outgoing Call” will trigger action sequence “Activate Ringing Pictogram”. This action is required for displaying the “Ringing” pictogram. If this action is deleted, pictogram “Ringing” will no longer be shown in green when an outgoing call is initiated.

Recommendation: Do not delete this activity.

Default configuration:

- **Device State:** “All”.
- **Trigger:** “Device State changed to”.
- **Until:** “Outgoing Call”.
- **Action Sequence to be executed:** “Activate Ringing Pictogram”.

Device State changed to (Active (In Call))

A change of the device state to “In Call” will trigger action sequence “Activate Call Active and AFIL Active Pictogram”. This action is required for displaying the “In Call” and “AFIL active” pictograms. If this activity is deleted, the pictograms “In Call” and “AFIL active” will not be shown in green during calls.

Recommendation: Do not delete this activity.

Default configuration:

- **Device State:** “All”.
- **Trigger:** “Device State changed to”.

- **Until:** "Active (Call)".
- **Action Sequence to be executed:** "Activate Call Active and AFIL Active Pictogram".

Device State changed to (Idle)

Ending a call triggers action sequence "Deactivate All Pictograms". This action is required for deactivating pictograms "Ringing", "In Call" and "AFIL active". If this activity is deleted, pictograms "Ringing", "In Call" and "AFIL active" will not be deactivated when calls are ended.

Recommendation: Do not delete this activity.

Default configuration:

- **Device State:** "All".
- **Trigger:** "Device State changed to".
- **Until:** "Idle".
- **Action Sequence to be executed:** "Deactivate all Pictograms".

DTMF Tone received 8

If an ID5 DKGM or ID5 DKHSGM is connected to the remote station and the Push-to-Talk button is pressed during a call, action sequence "Push-to-Talk Visualisation (Listen)" will be triggered. At that point, the person at the other end of the can start talking. You will have to enable pictogram "Push-to-Talk" to use this function. If this action is deleted, pictogram "Push-to-Talk" will not display correctly during Push-to-Talk calls.

Recommendation: Do not delete this activity.

Default configuration:

- **Device State:** "Active (Call)".
- **Trigger:** "DTMF Tone received".
- **Until:** "8".
- **Action Sequence to be executed:** „Push-to-Talk Visualisation (Listen)".

DTMF Tone received 9

When an ID5 DKGM or ID5 DKHSGM is connected to the remote station and the Push-to-Talk button is released during a call, action sequence "Push-to-Talk Visualisation (Talk)" is triggered. At that point, the person using the device can start talking. You will have to enable pictogram "Push-to-Talk" to use this function. If this action is deleted, pictogram "Push-to-Talk" will not display correctly during Push-to-Talk calls.

Recommendation: Do not delete this activity.

Default configuration:

- **Device State:** "Active (Call)".
- **Trigger:** "DTMF Tone received".
- **Until:** "9".
- **Action Sequence to be executed:** "Push-to-Talk Visualisation (Talk)".

5.21. ACTION SEQUENCES

The following functions are available:

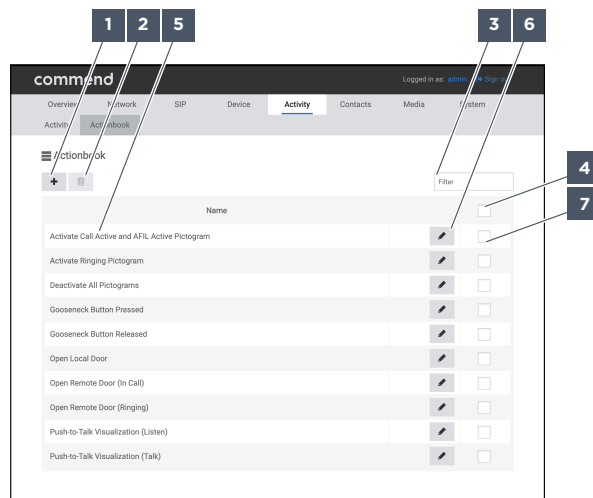


Figure 155: Action Sequences

- 1** Add Action Sequence
- 2** Delete selected Action Sequence
- 3** Filter
- 4** Select all Action Sequences
- 5** Name
- 6** Edit Action Sequence
- 7** Select Action Sequence

Actions sequences can be initiated via buttons or automatically via activities.

- [1] Add Action Sequence:** Adds an action sequence.
- [2] Delete selected Action Sequence:** Deletes the selected action sequences.
- [3] Filter:** Enter a search term in order to filter the action sequences accordingly.
- [4] Select all Action Sequences:** Enable in order to select all action sequences.
- [5] Name:** Shows the name of the action sequence.
- [6] Edit:** Edit the action sequence.
- [7] Delete selected Action Sequence:** Enable in order to select the action sequence.

5.21.1. ADD ACTION SEQUENCE

The following functions are available:

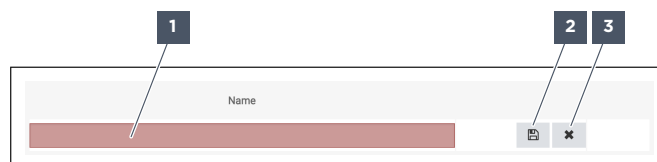


Figure 156: Action Sequence - Add Action Sequence

- 1** Name
 - 2** Save
 - 3** Abort
- [1] Name:** Enter a name for the action sequence.

[2] Save: Save the action sequence. Action sequences cannot be initiated until they have been added.

[3] Abort: Cancels the process and no action sequence is added.

5.21.2. EDIT ACTION SEQUENCE

The following functions are available:

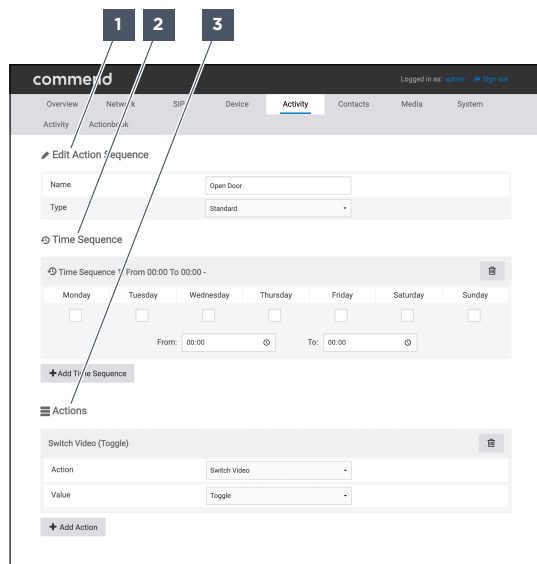


Figure 157: Action Sequence - Edit Action Sequence

- 1** Edit Action Sequence
- 2** Time Sequence
- 3** Actions

[1] Edit Action Sequence: Configure the basic settings.

[2] Time Sequence: Configure the times when the action sequence can be initiated.

[3] Actions: Configure the actions in the action sequence.

5.21.2.1. EDIT ACTION SEQUENCE

The following functions are available:

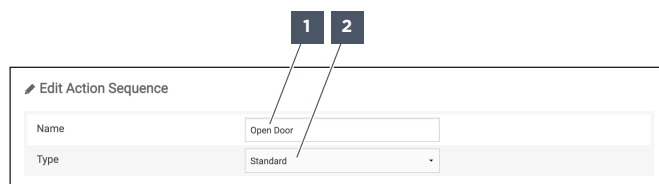


Figure 158: Action Sequences - Edit Action Sequence

- 1** Name
- 2** Type

[1] Name: Enter a name for the action sequence.

[2] Type: Select the call type. This function has an effect only on the actions “Call”, “Chain Call” and “Parallel Call”. Default: “Default”.

Options:

- **Default:** Calls are established with the default call views.
- **Emergency:** Calls are established with the emergency call views.

5.21.2.2. TIME SEQUENCE

The following functions are available:

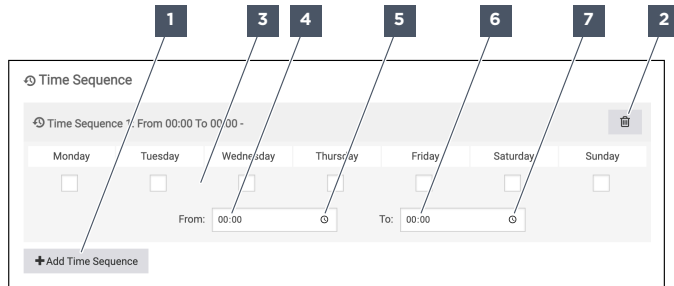


Figure 159: Action Sequence - Time Sequence

- | | | |
|----------------------------|-------------------------------|------------------|
| 1 Add Time Sequence | 2 Delete Time Sequence | 3 Weekday |
| 4 Time | 5 Time From | 6 Time |
| 7 Time To | | |

Several time sequences can be configured in an action sequence.

Example: If the action sequence should not be initiated during lunch breaks, two time sequences must be configured. A time sequence determines the time from the start of work until the lunch break. A time sequence determines the time from the lunch break until the end of work.

[1] Add Time Sequence: Adds a time sequence.

[2] Delete Time Sequence: Deletes the time sequence.

[3] Weekday: Enable in order to select the weekdays on which the action sequence can be initiated.

Options:

- Monday
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday
- Sunday

[4] From: Enter the time at which the action sequence can be initiated.

[5] Time From: Select the time at which the action sequence can be initiated.

[6] To: Enter the time until the action sequence can be initiated.

[7] Time To: Select the time until the action sequence can be initiated.

5.21.2.3. ACTIONS

The following functions are available:

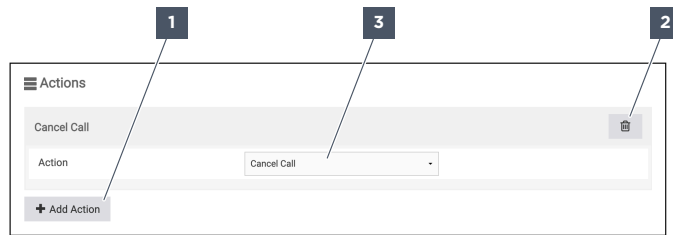


Figure 160: Action Sequences – Actions

1 Add Action

2 Action

3 Delete Action

Several actions can be configured in an action sequence.

Example: If a snapshot needs to be created and an output for enabling the light needs to be switched using the “Motion Detection” trigger, two actions must be configured.

[1] Add Action: Adds an action.

[2] Delete Action: Deletes the action.

[3] Action: Select the action ([see “Available actions”, page 182](#)).

5.21.3. PRE-CONFIGURED ACTION SEQUENCES

The action sequences described below are pre-configured by default. These action sequences can be used, changed or deleted.

Recommendation: Adjust the action sequences depending on the country-specific standards.

Activate Call Active and AFIL Active Pictogram

If the action “Device State changed to (In Call)” is triggered, this action sequence is run. This action sequence is required for displaying the pictograms “In Call” and “AFIL active”. If this action sequence is deleted, the pictograms “In Call” and “AFIL active” are not coloured green during calls.

Recommendation: Do not delete this activity.

Default configuration:

- **Action:** “Switch Pictogram”.
 - **Pictogram:** “In Call”.
 - **Mode:** “On”.
- **Action:** “Switch Pictogram”.
 - **Pictogram:** “AFL active”.
 - **Mode:** “On”.
- **Action:** “Switch Pictogram”.
 - **Pictogram:** “Ringing”.
 - **Mode:** “Off”.

Activate Ringing Pictogram

If the action “Device State changed to (Outgoing Call)” or “Device State changed to (Incoming Call)” is triggered, this action sequence is run. This action sequence is required for displaying the pictogram “Ringing”. If this action sequence is deleted, the pictogram “Ringing” is not coloured green during incoming calls.

Recommendation: Do not delete this activity.

Default configuration:

- **Action:** “Switch Pictogram”.
 - **Pictogram:** “Ringing”.
 - **Mode:** “On”.
- **Action:** “Switch Pictogram”.
 - **Pictogram:** “In Call”.
 - **Mode:** “Off”.
- **Action:** “Switch Pictogram”.
 - **Pictogram:** “AFL active”.
 - **Mode:** “Off”.

Deactivate all Pictograms

If the action “Device State changed to (Idle)” is triggered, this action sequence is run. This action sequence is required for disabling the displayed pictograms “Ringing”, “In Call” or “AFIL active”. If this action sequence is deleted, the pictograms “Ringing”, “In Call” and “AFIL active” are not disabled after calls are ended.

Recommendation: Do not delete this activity.

Default configuration:

- **Action:** “Switch Pictogram”.
 - **Pictogram:** “Ringing”.
 - **Mode:** “Off”.
- **Action:** “Switch Pictogram”.
 - **Pictogram:** “In Call”.
 - **Mode:** “Off”.
- **Action:** “Switch Pictogram”.
 - **Pictogram:** “AFL active”.
 - **Mode:** “Off”.

Gooseneck Button Pressed

An activity for pressing the “Push to Talk” button must be added. An activity for pressing the “Push to Talk” button must be added and linked with this action sequence. An ID5 DKGM or an ID5 DKHSGM must be connected to the device. The “Push-to-Talk” pictogram indicates that the person at the device can speak. Activate the “Push-to-Talk” pictogram before using this function. If this action sequence is deleted, the pictogram “Push-to-Talk” is not correctly displayed in a “Push-to-Talk” call.

The DTMF tone can be changed. The DTMF tone “1” is reserved for the door opener function. Different DTMF tones must be configured for the action sequences “Gooseneck Button Pressed” and “Gooseneck Button Released”. If the DTMF tone is changed, this DTMF tone must be changed in all other devices.

Recommendation: Do not delete this activity.

Default configuration:

- **Action:** “Send DTMF Tone”.
 - **DTMF Tone:** “8”.

Gooseneck Button Released

An activity for releasing the “Push to Talk” button must be added and linked with this action sequence. An ID5 DKGM or an ID5 DKHSGM must be connected to the device. The “Push-to-Talk” pictogram indicates that the person at the remote station can speak. Activate the “Push-to-Talk” pictogram before using this function. If this action sequence is deleted, the pictogram “Push-to-Talk” is not correctly displayed in a “Push-to-Talk” call.

The DTMF tone can be changed. The DTMF tone “1” is reserved for the door opener function. Different DTMF tones must be configured for the action sequences “Gooseneck Button Pressed” and “Goose-

neck Button Released". If the DTMF tone is changed, this DTMF tone must be changed in all other devices.

Recommendation: Do not delete this activity.

Default configuration:

- **Action:** "Send DTMF Tone".
 - **DTMF Tone:** "9".

Open Local Door

If the action "DTMF Tone received 1" is triggered, this action sequence is run. This action sequence is required for displaying the pictogram "Open Door". If this action sequence is deleted, the pictogram "Open Door" is not displayed after actuating the door opener function.

For compatibility reasons, the DTMF tone "2" is not sent as acknowledgement to the remote station through which the door opener was operated. If the DTMF tone "2" needs to be sent to the remote station as acknowledgement, an action must be added in the action sequence "Open Local Door".

Recommendation: Do not delete this activity.

Default configuration:

- **Action:** "Switch Pictogram".
 - **Pictogram:** "Open Door".
 - **Mode:** "On".
- **Action:** "Delayed Action".
 - **Delay [s]:** "5".
 - **Debouncing:** Disabled.
 - **Action:** "Switch Pictogram".
 - **Pictogram:** "Open Door".
 - **Mode:** "Off".

Open Remote Door (In Call)

This action sequence can be used if the door opener function at the remote station needs to be activated in the device state "In Call". One activity or one button can be linked with this action sequence.

Default configuration:

- **Action:** "Send DTMF Tone".
 - **Pictogram:** "1".
- **Action:** "Delayed Action".
 - **Delay [s]:** "6".
 - **Debouncing:** Disabled.
 - **Action:** "Cancel Call".

Open Remote Door (Ringing)

This action sequence can be used if the door opener function at the remote station needs to be activated in the device state "Incoming Call". One activity or one button can be linked with this action sequence.

Default configuration:

- **Action:** "Answer Call".
 - **Audio enabled:** Enabled.
 - **Incoming:** Disabled.
 - **Outgoing:** Disabled.
- **Action:** "Delayed Action".
 - **Delay [s]:** "2".
 - **Debouncing:** Disabled.

- **Action:** “Send DTMF Tone”.
- **DTMF Tone:** “1”.
- **Action:** “Delayed Action”.
 - **Delay [s]:** “8”.
 - **Debouncing:** Disabled.
 - **Action:** “Cancel Call”.

Push-to-Talk Visualisation (Listen)

If the action “DTMF Tone received 8” is triggered, this action sequence is run. An ID5 DKGM or an ID5 DKHSGM must be connected to the remote station. The “Push-to-Talk” pictogram indicates that the person at the remote station can speak. Activate the “Push-to-Talk” pictogram before using this function. If this activity is deleted, the pictogram “Push-to-Talk” is not correctly displayed in a “Push-to-Talk” call.

Default configuration:

- **Action:** “Switch Pictogram”.
 - **Pictogram:** “Push-to-Talk enabled”.
 - **Mode:** “Off”.

Push-to-Talk Visualisation (Talk)

If the action “DTMF Tone received 89” is triggered, this action sequence is run. An ID5 DKGM or an ID5 DKHSGM must be connected to the remote station. The “Push-to-Talk” pictogram indicates that the person at the device can speak. Activate the “Push-to-Talk” pictogram before using this function. If this activity is deleted, the pictogram “Push-to-Talk” is not correctly displayed in a “Push-to-Talk” call.

Default configuration:

- **Action:** “Switch Pictogram”.
 - **Pictogram:** “Push-to-Talk enabled”.
 - **Mode:** “On”.

5.22. CONTACTS

The following functions are available:

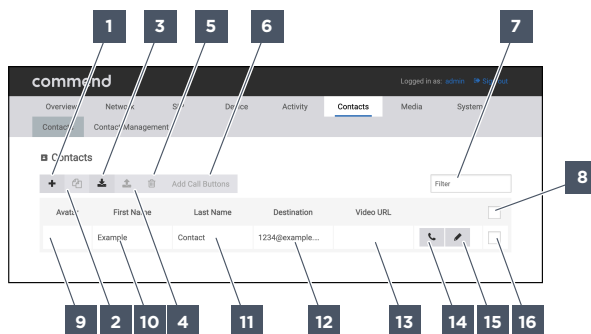


Figure 161: Contacts

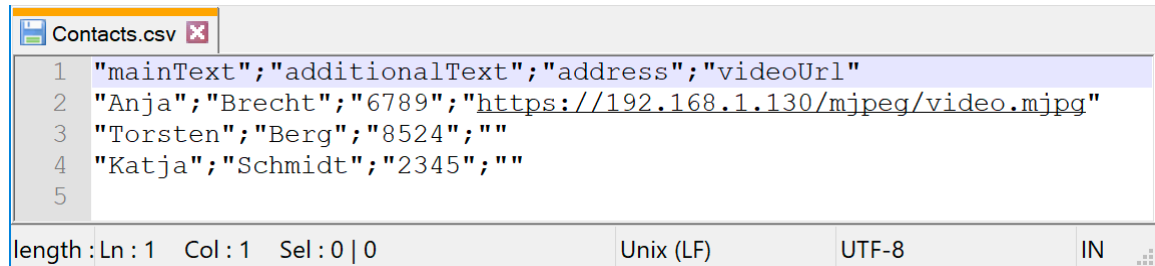
- | | | |
|----------------------------|----------------------------|--------------------|
| 1 Add Contact | 2 Copy selected Contacts | 3 Import Contacts |
| 4 Export selected Contacts | 5 Delete selected Contacts | 6 Add Call Buttons |
| 7 Filter | 8 Select all Contacts | 9 Avatar |
| 10 First Name | 11 Last Name | 12 Destination |
| 13 Video URL | 14 Call | 15 Edit |
| 16 Select Contact | | |

The “Example Contact” is configured by default. The “Example Contact” can be deleted or edited.

[1] Add contact: Adds a contact.

[2] Copy Selected Contacts: Copies the selected contacts.

[3] Import contacts: Imports contacts. The contacts to be imported must be in one CSV file. The CSV file may contain only text. The CSV file may not contain any images. Avatars can be added after importing contacts via the web interface. The CSV file must be UTF-8-coded in order to properly interpret special characters and umlauts.



```

1 "mainText";"additionalText";"address";"videoUrl"
2 "Anja";"Brecht";"6789";"https://192.168.1.130/mjpeg/video.mjpg"
3 "Torsten";"Berg";"8524";""
4 "Katja";"Schmidt";"2345";""
5
length: Ln: 1 Col: 1 Sel: 0 | 0      Unix (LF)      UTF-8      IN

```

Figure 162: Import contacts via a CSV file

Formatting:

- **Column “A”, “mainText”:** First name of the contact.
- **Column “B”, “additionalText”:** Last name of the contact.
- **Column “C”, “address”:** IPv4 address, IPv6 address or SIP call destination of the contact.
- **Column “D”, “videoUrl”:** Video URL of the contact in HTTP format or HTTPS format.

Recommendation: Edit the contacts to be imported with Notepad+ or another text editor. The process of conversion in Excel may be faulty.

[4] Export Selected Contacts: Exports the selected contacts.

[5] Delete Selected Contacts: Deletes the selected contacts. If a contact is used for a button or in an action sequence, this contact cannot be deleted.

Example: The “Example Contact” cannot be deleted until the configuration of the button available in the “Indoor” or “Door” layout by default is changed.

[6] Add Call Buttons: Add call buttons created through selected contacts ([see “Add Call Buttons”, page 150](#)).

[7] Filter: Enter a search term in order to filter the contacts accordingly.

[8] Select All Contacts: Enable in order to select all contacts.

[9] Avatar: Shows the avatar.

[10] First Name: Shows the first name.

[11] Last Name: Shows the last name.

[12] Destination: Shows the IPv4 address, IPv6 address or SIP call destination.

[13] Video URL: Shows the video URL for calls with an external IP video camera of the contact. The video URL can be based on HTTP or HTTPS. If a video URL is configured for the contact, the external IP video camera is used for video calls instead of the built-in camera of the remote station.

[14] Call: Initiates a call to the contact. When the call is initiated from the computer web browser, a smartphone or a tablet, the audio devices configured for the web browser are used.

[15] Edit: Edits the contact ([see “Edit Contact”, page 149](#)).

[16] **Select Contact:** Selects the contact.

5.2.2.1. EDIT CONTACT

The following functions are available:

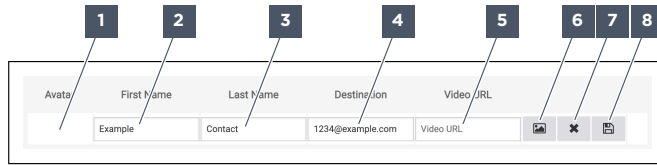


Figure 163: Contacts - Edit contacts

- | | | |
|---------------|--------------|-----------------|
| 1 Avatar | 2 First Name | 3 Last Name |
| 4 Destination | 5 Video URL | 6 Upload Avatar |
| 7 Cancel | 8 Save | |

[1] **Avatar:** Shows the profile picture.

[2] **First Name:** Enter the first name.

[3] **Last Name:** Enter the last name.

[4] **Destination:** Enter the IPv4 address, the IPv6 address or the SIP call destination. For peer-to-peer calls, the SIP URI of the remote device must be entered. For peer-to-peer calls using a DNS server, the SIP URI or a user ID and the host name must be entered in the format "<IP address/user ID>@<host name>". The user ID can be freely chosen.

Recommendation: Enter the Display Name as user ID.

Options:

- **Without DNS server:** Enter the IP address of the remote device.
Example: "192.168.1.151".
- **With DNS server:** Enter the IP address or a user ID and the host name of the remote device. The host name must be configured at a DNS server that is reachable in the network.
Example: "192.168.1.151" or "id5@doorstation".

[5] **Video URL:** Enter the video URL in HTTP format or HTTPS format.

[6] **Upload Avatar:** Upload a profile picture.

Image properties:

- **File size:** max. 6 MB.
- **File format:** JPG, PNG.

Recommendation:

- **Size (W x H):** 100 x 100 pixels for the layout "Indoor" and "Outdoor". 400 x 400 pixels for the layout "Contact Management".
- **Resolution:** 72 dpi.
- **File format:** PNG 24, with transparencies.
- **Colour space:** sRGB
- If the avatar is used as a button image, choose square dimensions.

[7] **Cancel:** Cancel and do not edit the contact.

[8] **Save:** Save the contact.

5.22.2. ADD CALL BUTTONS

The following functions are available:

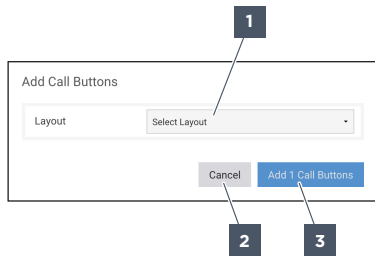


Figure 164: Contacts - Add Call Buttons

- 1** Layout
- 2** Cancel
- 3** Add # Call Buttons

[1] Layout: Select an existing layout in which the call buttons are to be added ("[Device](#)"). Call buttons can only be added in the layouts "Indoor", "Door" and "Frame". For the layout "Indoor", the page to which the call buttons are to be added can be selected.

[2] Cancel: Cancel and do not add call buttons.

[3] Add # Call Buttons: Add the call buttons. Call buttons are added at the bottom of existing call buttons.

5.23. CONTACT MANAGEMENT

The following functions are available:

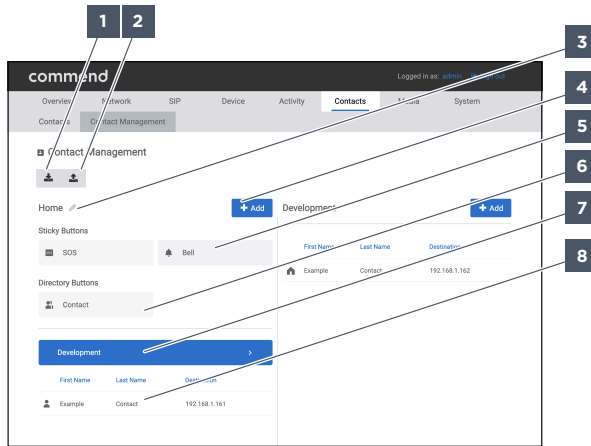


Figure 165: Contact Management

- 1** Import Contact Management Configuration
- 2** Export Contact Management Configuration
- 3** Edit Directory Name
- 4** Add
- 5** Sticky Button
- 6** Directory Button
- 7** Directory
- 8** Contact

A contact can be in different directories at the same time. Contacts and directories can be moved by drag and drop. Contacts can be copied to another directory by drag and drop and pressing the CTRL key.

50 subdirectories and 100 contacts can be managed per directory.

[1] Import Contact Management Configuration: Import a contact management configuration in JSON format. Additional contact information can be configured using the property “userData” in the JSON file. The imported contacts are added to **Contacts** .

Example: Import the contact management configuration for mass updates at regular intervals via a JSON file.

[2] Export Contact Management Configuration: Export the contact management configuration in JSON format. If several devices have to be configured with the same contacts, the configuration can be carried out on one device. This contact management configuration can be exported and imported to the other devices.

[3] Edit Directory Name: Enter the name that is shown on the home screen in the layout “Contact Management”. Default: “Home”.

[4] Add: Add a contact management element.

Options:

- **Create Directory:** Create a new subdirectory. Up to 10 subdirectory levels can be managed.
- **Create Contact:** Create a new contact. Up to 10,000 contacts without a profile picture can be managed. Up to 5,000 contacts with a profile picture can be managed.
- **Add existing Contact:** Add a contact from **Contacts** (see “Contacts”, page 147).
- **Add Sticky Button:** Add a button that is displayed at the top of all directories. Up to 2 sticky buttons can be managed. Sticky buttons can be added in the directory “Home” only.
- **Add Directory Button:** Add a button that is displayed at the top of the directory. Up to 2 directory buttons can be managed per directory.

[5] Sticky Button: Configure the sticky button. Default: no sticky button.

[6] Directory Button: Configure the directory button. Default: no directory button.

[7] Directory: Configure the directory. Default: no directory.

[8] Contact: Configure the contact. Default: “Example Contact” available.

5.23.1. STICKY BUTTONS AND DIRECTORY BUTTONS

The following functions are available:

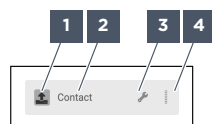


Figure 166: Contact Management – Sticky Buttons and Directory Buttons

- 1 Upload Icon
- 2 Name
- 3 Edit
- 4 Move

The configuration is the same for sticky buttons and directory buttons.

[1] Upload Icon: Select or upload a profile picture. Default: handset icon.

Image properties:

- **File size:** max. 6 MB.
- **File format:** JPG, PNG.

Recommendation:

- **Size (W x H):** 100 x 100 pixels for the layout “Indoor” and “Outdoor”. 400 x 400 pixels for the layout “Contact Management”.
- **Resolution:** 72 dpi.
- **File format:** PNG 24, with transparencies.

- **Colour space:** sRGB
- If the avatar is used as a button image, choose square dimensions.

[2] Name: Enter the name for the button.

[3] Edit: Configure the button.

Options:

- **Edit Button:** Configuring the button (["Button Configuration"](#)).
- **Delete Button:** Delete the button.
- **Upload Icon:** Select or upload a profile picture.

[4] Move: Change the order by moving the button to the left or to the right.

5.23.2. DIRECTORIES

The following functions are available:

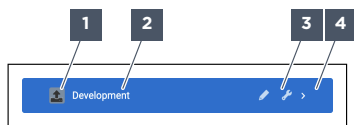


Figure 167: Contact Management - Directory

- | | | |
|-----------------|--------|--------|
| 1 Upload Avatar | 2 Name | 3 Edit |
| 4 Open | | |

[1] Upload Avatar: Upload a profile picture.

Image properties:

- **File size:** max. 6 MB.
- **File format:** JPG, PNG.

Recommendation:

- **Size (W x H):** 100 x 100 pixels for the layout "Indoor" and "Outdoor". 400 x 400 pixels for the layout "Contact Management".
- **Resolution:** 72 dpi.
- **File format:** PNG 24, with transparencies.
- **Colour space:** sRGB
- If the avatar is used as a button image, choose square dimensions.

[2] Name: Enter the directory name.

[3] Edit: Configure the directory.

Options:

- **Delete Directory:** Delete the directory.
- **Upload Image:** Select or upload a profile picture.

[4] Open: Open the directory to the right to be able to configure the contacts and subdirectories.

5.23.3. CONTACT

The following functions are available:

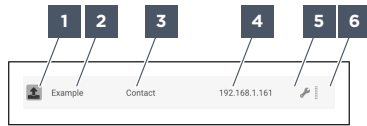


Figure 168: Contact Management - Buttons

- | | | |
|----------------------|---------------------|--------------------|
| 1 Upload Icon | 2 First Name | 3 Last Name |
| 4 Destination | 5 Edit | 6 Move |

[1] Upload Icon: Select or upload a profile picture.

[2] First Name: Enter the first name.

Recommendation: Do not use spaces between multiple words as words after a space will not be included in the search. If “Building number 12” is entered, “12” cannot be searched for through the search function. In **First Name** enter “Building number” and in **Last Name** enter “12” or use a hyphen or an underscore.

[3] Last Name: Enter the last name.

Recommendation: Do not use spaces between multiple words as words after a space will not be included in the search. If “Building number 12” is entered, “12” cannot be searched for through the search function. In **First Name** enter “Building number” and in **Last Name** enter “12” or use a hyphen or an underscore.

[4] Destination: Enter the IPv4 address, the IPv6 address or the SIP call destination. For peer-to-peer calls, the SIP URI of the remote device must be entered.

[5] Edit: Configure the button.

Options:

- **Edit Contact:** Configure the information for the contact ([“Contact configuration”](#)).
- **Upload Avatar:** Upload a profile picture.
- **Remove Contact:** Delete the contact.

[6] Move contact: Change the order by moving the contact to a new position.

5.23.4. BUTTON CONFIGURATION

The following functions are available:

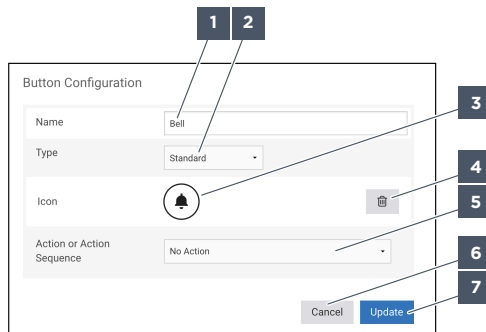


Figure 169: Contact Management - Button Configuration

- | | | |
|----------------------|------------------------------------|----------------------|
| 1 Name | 2 Type | 3 Upload Icon |
| 4 Delete Icon | 5 Action or Action Sequence | 6 Cancel |

7 Save

The button configuration is the same for sticky buttons and directory buttons.

[1] Name: Enter the name for the button.

[2] Type: Select the call type. This function affects the actions “Call”, “Chain Call” and “Parallel Call” only. Default: “Standard”.

Options:

- **Standard:** Calls are initiated using the standard call views.
- **Emergency:** Calls are initiated using the emergency call views.

[3] Upload Icon: Upload or select an icon. Default: bell icon.

[4] Delete Icon: Delete the icon.

[5] Action or Action Sequence: Select an action or an action sequence. Any configured action sequence can be selected. Default: “No Action”.

[6] Cancel: Cancel and do not edit the button.

[7] Save: Save the button.

5.23.5. CONTACT CONFIGURATION

The following functions are available:

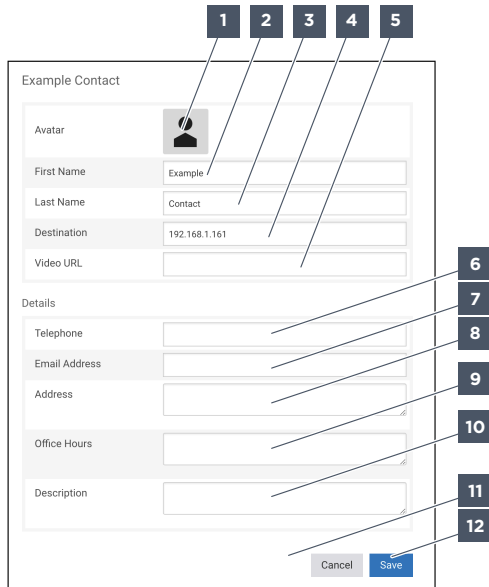


Figure 170: Contact Management - Edit contact

- | | | |
|------------------------|---------------------|-----------------------|
| 1 Upload Avatar | 2 First Name | 3 Last Name |
| 4 Destination | 5 Video URL | 6 Telephone |
| 7 Email address | 8 Address | 9 Office Hours |
| 10 Description | 11 Cancel | 12 Save |

[1] Avatar: Select or upload a profile picture.

Image properties:

- **File size:** max. 6 MB.
- **File format:** JPG, PNG.

Recommendation:

- **Size (W x H):** 100 x 100 pixels for the layout "Indoor" and "Outdoor". 400 x 400 pixels for the layout "Contact Management".
- **Resolution:** 72 dpi.
- **File format:** PNG 24, with transparencies.
- **Colour space:** sRGB
- If the avatar is used as a button image, choose square dimensions.

[2] First Name: Enter the first name.

[3] Last Name: Enter the last name.

[4] Destination: Enter the IPv4 address, the IPv6 address or the SIP call destination. For peer-to-peer calls, the SIP URI of the remote device must be entered.

Options:

- **Without DNS server:** Enter the IP address of the remote device.
Example: "192.168.1.151".
- **With DNS server:** Enter the IP address or a user ID and the host name of the remote device. The host name must be configured at a DNS server that is reachable in the network.
Example: "192.168.1.151" or "id5@doorstation".

[5] Video URL: Enter the video URL in HTTP format or HTTPS format.

[6] Telephone: Enter the call number of a landline or mobile phone. This field is optional and is not shown if it is empty.

[7] Email address: Enter the email address. This field is optional and is not shown if it is empty.

[8] Address: Enter the contact address. This field is optional and is not shown if it is empty.

[9] Office Hours: Enter the hours during which the contact can be reached. This field is optional and is not shown if it is empty.

[10] Description: Enter a description for the contact. This field is optional and is not shown if it is empty.

[11] Cancel: Cancel and do not edit the contact.

[12] Save: Save the contact.

5.24. AUDIO FILES

The following functions are available:

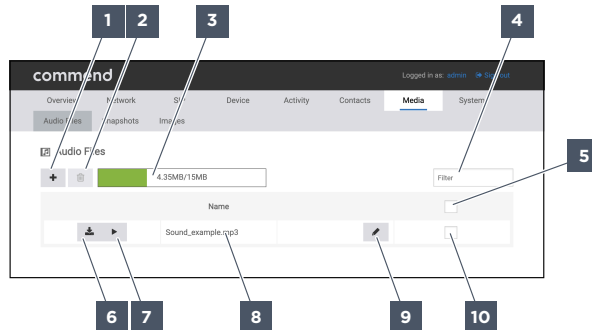


Figure 171: Audio Files

- | | | |
|----------------------|--------------------------|-------------|
| 1 Upload | 2 Delete | 3 File Size |
| 4 Filter | 5 Select all Audio Files | 6 Download |
| 7 Play | 8 Name | 9 Edit |
| 10 Select Audio File | | |

[1] Upload: Uploads an audio file in MP3 format or WAV format. Audio files with a maximum file size of 6 MB can be uploaded. Audio files with a maximum sampling rate of 48 kHz can be uploaded. Stereophonic audio files are played back in mono. Several files can be uploaded simultaneously. Default: No audio files available.

Recommendation: To make efficient use of storage space, upload mono audio files only.

[2] Delete: Deletes the selected audio files. If audio files configured in actions or action sequences are deleted, no note is displayed. No audio files are played using these actions or action sequences.

[3] Available Storage Space: Shows the storage space in use and the available storage space. Max. 15 MB of audio files can be managed.

[4] Filter: Enter a search term in order to filter the audio files accordingly.

[5] Select all Audio Files: Enable in order to select all audio files.

[6] Download: Downloads the audio file in the computer web browser, smartphone or tablet.

[7] Play: Plays the audio file. When the audio file is played from the computer web browser, a smartphone or a tablet, the audio devices configured for the web browser are used.

[8] Name: Shows the file name.

[9] Edit: Edits the audio file ([see page 157](#)).

[10] Select Audio File: Selects the audio file.

5.24.1. EDIT AUDIO FILE

The following functions are available:

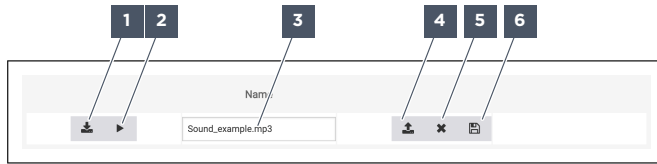


Figure 172: Audio File – Edit Audio File

- | | | |
|--------------------------------------|----------------|---------------|
| 1 Download | 2 Play | 3 Name |
| 4 Replace existing Audio File | 5 Abort | 6 Save |

[1] Download: Downloads the audio file in the computer web browser, smartphone or tablet.

[2] Play: Plays the audio file. When the audio file is played from the computer web browser, a smartphone or a tablet, the audio devices configured for the web browser are used.

[3] Name: Enter the file name.

[4] Replace existing Audio File: Uploads an audio file in MP3 format or WAV format. The existing audio file is overwritten. Audio files with a maximum file size of 6 MB can be uploaded. Audio files with a maximum sampling rate of 48 kHz can be uploaded. Stereophonic audio files are played back in mono. Default: No audio files available.

Recommendation: To make efficient use of storage space, upload mono audio files only.

[5] Abort: Cancels and the user refrains from editing the audio file.

[6] Save: Saves the audio file.

5.25. SNAPSHOTS

The following functions are available:

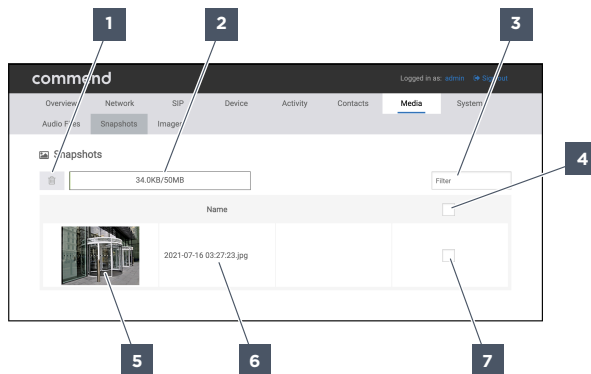


Figure 173: Snapshots

- | | | |
|-------------------------------|----------------------------------|-----------------|
| 1 Delete | 2 Available storage space | 3 Filter |
| 4 Select all Snapshots | 5 Download | 6 Name |
| 7 Select Snapshots | | |

[1] Delete: Deletes the selected snapshots.

[2] Available Storage Space: Shows the storage space in use and the available storage space. Max. 50 MB of snapshots can be managed. When the available storage space is full, the oldest snapshots are deleted automatically in accordance with the First In, First Out principle.

[3] Filter: Enter a search term in order to filter the snapshots accordingly. Snapshots can be filtered by the time or date.

[4] Select All Snapshots: Enable in order to select all snapshots.

[5] Download: Downloads the snapshot in the computer web browser, smartphone or tablet.

[6] Name: Shows the file name. Snapshots are named according to the time and date of creation.

[7] Select Snapshot: Select the snapshot.

5.26. IMAGES

The following functions are available:

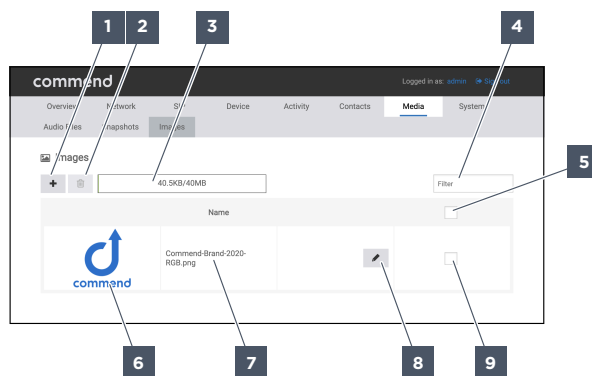


Figure 174: Images

- | | | |
|-----------------|----------------------------|----------------------------------|
| 1 Upload | 2 Delete | 3 Available storage space |
| 4 Filter | 5 Select all Images | 6 Download |
| 7 Name | 8 Edit | 9 Select Image |

[1] Upload: Uploads an image in JPG format or PNG format. Images with a maximum file size of 6 MB can be uploaded. Several files can be uploaded simultaneously. Default: No images available.

[2] Delete: Deletes the selected images. If images configured in contacts, in buttons or as a background image are deleted, no note is displayed.

[3] Available Storage Space: Shows the storage space in use and the available storage space. Max. 40 MB of images can be managed.

[4] Filter: Enter a search term in order to filter the images accordingly.

[5] Select all Images: Enable in order to select all images.

[6] Download: Downloads the image in the computer web browser, smartphone or tablet.

[7] Name: Shows the file name.

[8] Edit: Edits the image ([see page 159](#)).

[9] Select Image: Select the image.

5.26.1. EDIT IMAGES

The following functions are available:

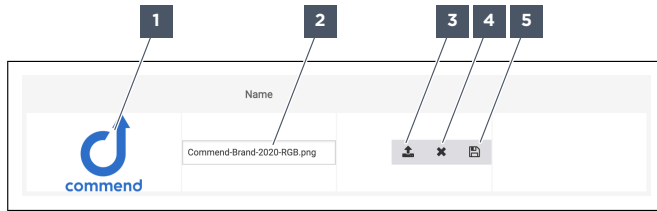


Figure 175: Images

1 Download

2 Name

3 Replace Existing Image

4 Abort

5 Save

[1] Download: Downloads the image in the computer web browser, smartphone or tablet.

[2] Name: Enter the file name.

[3] Replace Existing Image: Uploads an image in JPG format or PNG format. The existing image is overwritten. Images with a maximum file size of 6 MB can be uploaded.

[4] Abort: Cancels and the user refrains from editing the image.

[5] Save: Saves the image.

5.27. SYSTEM

The following functions are available:

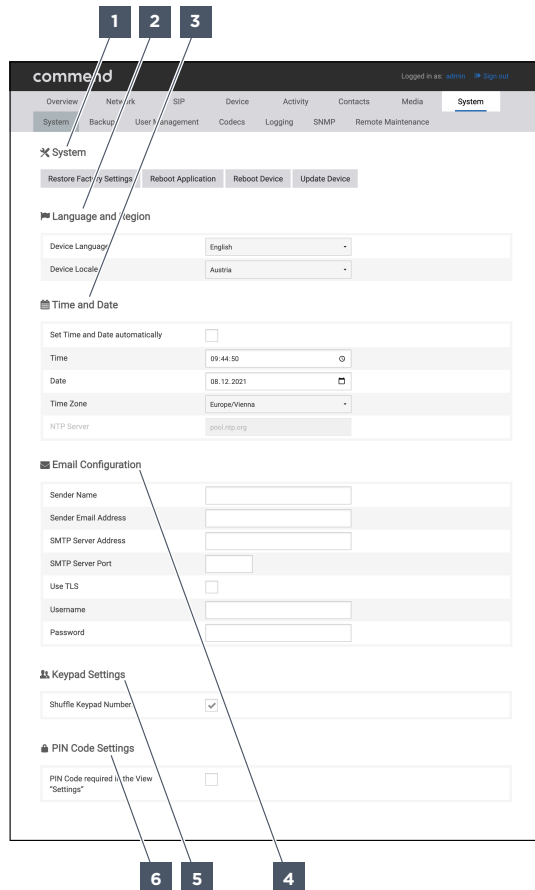


Figure 176: System

- | | | |
|------------------------------|------------------------------|----------------------------|
| 1 System | 2 Language and Region | 3 Time and Date |
| 4 Email Configuration | 5 Keypad Settings | 6 PIN Code Settings |

[1] System: Manage the device firmware.

[2] Language and Region: Configure the device language and the device locale.

[3] Time and Date: Configure the device time.

[4] Email Configuration: Configure the email settings.

[5] Keypad Settings: Configure the keypad settings.

[6] PIN Code Settings: Configure the PIN code settings.

5.27.1. SYSTEM

The following functions are available:

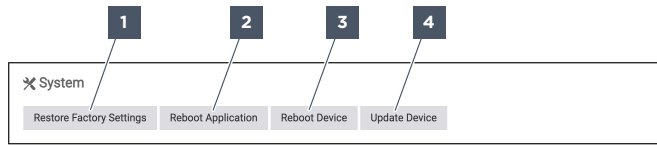


Figure 177: System - System

- 1 Restore Factory Settings
- 2 Rboot Application
- 3 Reboot Device
- 4 Update Device

[1] Restore Factory Settings: Restores the factory defaults. When restoring the factory defaults, all data and configurations such as network settings are lost. The process of restoring the factory defaults may take several minutes. The device cannot be used while the factory defaults are being restored. The web interface of the device cannot be called up while the factory defaults are being restored. When restoring to factory defaults, the login data of the administrator are also restored. When logging in to the web interface with the user "admin", a new password must be set.

Recommendation: Export a backup before restoring the factory defaults.

[2] Restart Application: Restarts the device software. The process of restarting the device software may take several minutes. The device cannot be used during the restart. The web interface of the device cannot be called up during the restart.

[3] Restart Device: Restarts the device. The process of restarting the device software may take several minutes. The device cannot be used during the restart. The web interface of the device cannot be called up during the restart.

[4] Update Device: Updates the device software. The process of updating the device software may take several minutes. The device cannot be used while the device software is being updated. The web interface of the device cannot be called up while the device software is being updated. All snapshots are deleted when updating the device software.

Update files can be downloaded using cLibrary Online.

i NOTE

Skipping several major versions when updating the device software

Parts of the configuration can be lost

No major versions may be skipped during the update process. This prevents the loss of parts of the configuration. Major versions are "02.09.xx.xx" or "03.01.xx.xx". When updating the device, minor versions within major versions can be skipped. Minor versions are "03.01.01.xx" or "03.01.15.xx".

Example: When updating from Version 02.03 to Version 02.09, update the device successively with versions 02.04, 02.05, 02.06, 02.07, 02.08 and 02.09.

Downgrades are possible. When downgrading from major versions, the factory defaults of the device are restored.

Update files for the device may contain software for accessories. The accessories must not be disconnected from the device while updating the device software.

Only update files intended for the device may be used for the device. If an update file is selected that is not intended for the device, a warning message appears in the web interface. The syntax elements for naming update files are structured as follows.

Syntax elements:

- <Product ID>
- update
- <Software version>
- img

Example: "id5_update_xx_xx_xx_xxx.img".

Recommendation: Do not load any software updates with a version lower than 02.09.01 in devices with the hardware revision "AG" or higher.

If a software update is performed from version 02.06 or lower to version 02.07.83 or higher, the authentication must be reconfigured with tokens. Password-based authentication is no longer valid. Token-based authentication meets the latest security standards.

5.27.2. LANGUAGE AND REGION

The following functions are available:

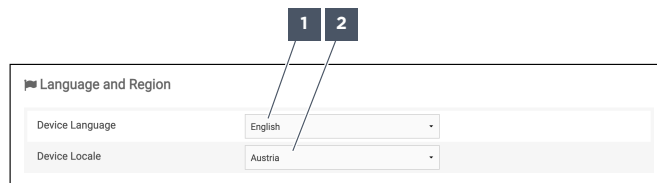


Figure 178: System - Language and Region

- 1 Device Language 2 Locale

[1] Device Language: Select the device language. Default: "English".

Options:

- English
- German
- French
- Spanish
- Russian
- Dutch
- Italian
- Polish

[1] Locale: Select the country where the device is installed. Default: "Austria".

5.27.3. TIME AND DATE

The following functions are available:

Figure 179: System – Time and Date

- | | | |
|--|---------------------|---------------|
| 1 Set Time and Date automatically | 2 Time | 3 Date |
| 4 Time Zone | 5 NTP Server | |

[1] Set Time and Date Automatically: Enable to set the time and date automatically via an NTP server. A valid NTP server address is required in **[5] NTP Server**. For cryptographic and time-based operations such as validating certificates, exchanging token keys or cronjobs, this function must be activated. Default: enabled.

[2] Time: Enter the time. If **[1] Set Time and Date Automatically** is enabled, the time is displayed. Default: The time is displayed automatically

[3] Date: Enter the date. If **[1] Set Time and Date Automatically** is enabled, the date is displayed. Default: The date is displayed automatically.

[4] Time Zone: Select the time zone where the device is installed. Default: “Europe/Vienna”.

[5] NTP Server: Enter the NTP server address. If the default NTP server address is configured, the device must be connected to the Internet in order to display the correct time. Default: “pool.ntp.org”.

5.27.4. EMAIL CONFIGURATION

The following functions are available:

Figure 180: System – Email Configuration

- | | | |
|---------------------------|-------------------------------|------------------------------|
| 1 Sender Name | 2 Sender Email Address | 3 SMTP Server Address |
| 4 SMTP Server Port | 5 Use TLS | 6 Username |
| 7 Password | | |

A sender email address must be configured in order to send emails through actions and action sequences.

The function “Allow less secure apps” must be activated in the settings for Google Mail and Google Workspace accounts.

[1] Sender Name: Enter the sender name. Default: empty.

[2] Sender Email Address: Enter the email address of the sender. Default: empty.

[3] SMTP Server Address: Enter the SMTP server address for the email address of the sender. Default: empty.

[4] SMTP Server Port: Enter the SMTP port number for the email address of the sender. Default: empty.

[5] Use TLS: Enable in order to send the email from the device in an encrypted format. Default: empty.

[6] Username: Enter the username for the email address of the sender. Default: empty.

[7] Password: Enter the password for the email address of the sender. Default: empty.

5.27.5. KEYPAD SETTINGS

The following functions are available:

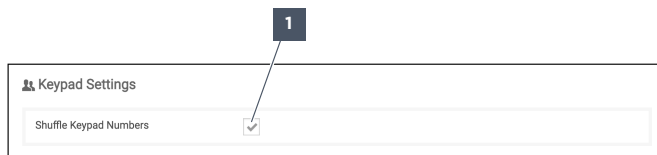


Figure 181: System – Keypad

1 Shuffle Keypad Numbers

[1] Shuffle Keypad Numbers: Enable in order to re-shuffle the numbers on the device keypad for entering the PIN code during every call-up. By shuffling the keypad numbers, the PIN code cannot be traced back to the fingerprints on the screen. Default: enabled.

5.28. BACKUP

The following functions are available:

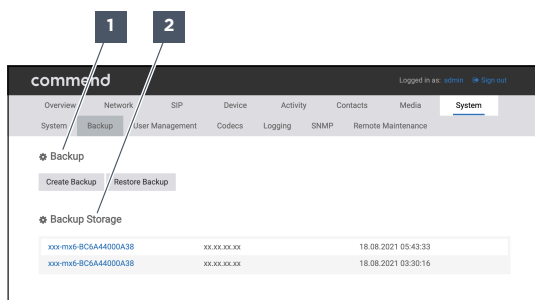


Figure 182: Backup

1 Backup **2** Backup Storage

[1] Backup: Export or import backups.

[2] Backup Storage: Manage backups.

5.28.1. BACKUP

The following functions are available:



Figure 183: Backup – Backup

1 Create Backup **2** Restore Backup

[1] Create Backup: Exports a configuration in BAK format. The syntax elements for naming backups are structured as follows.

Syntax elements:

- <Product ID>
- <Host name>
- <Date>
- <Time>

Example: “ID5TDCM_ID5-mx6-BC6A44000E69_2021_07_05_13-51.bak”.

[2] Restore Backup: Imports a configuration in BAK format. The existing configuration is overwritten.

5.28.2. BACKUP STORAGE

The following functions are available:

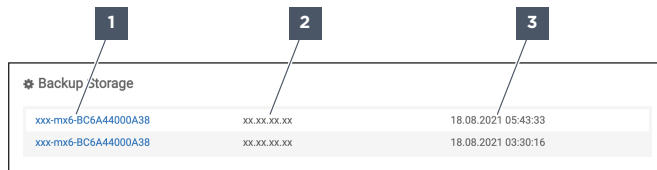


Figure 184: Backup – Backup Storage

1 Download **2** Software Version **3** Creation Date

The last 5 backups are saved. If a new backup is created, the oldest backup is deleted. The sequence of the backup storage is chronological, from top to bottom.

[1] Download: Downloads a backup in BAK format. Shows the backup name. The syntax elements for the backup name are structured as follows

Syntax elements:

- <Product ID>
- <Host name>

Example: “ID5TDCM_ids-mx6-000CAB0A034F”.

[2] Software Version: Shows the software version used to create the backup.

[3] Creation Date: Shows the date when the backup was created.

5.29. USER MANAGEMENT

The following functions are available:

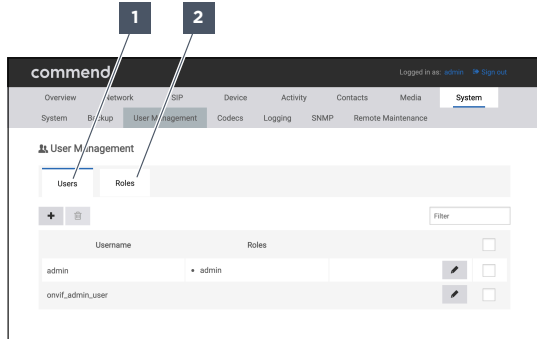


Figure 185: User Management

- [1] Users
- [2] Roles

[1] Users: Manage the users for the web interface of the device.

[2] Roles: Manage the roles for the users.

5.29.1. USERS

The following functions are available:



Figure 186: User Management - Users

- [1] Create User
- [2] Delete selected User
- [3] Filter
- [4] Select all User
- [5] Username
- [6] Roles
- [7] Edit
- [8] Select User

By default, the users “admin” and “onvif_admin_user” are available.

When updating from software version 03.00 or lower to software version 03.01 or higher, the user “onvif_admin_user” is automatically added. The user “onvif_admin_user” is configured with a default token that is reset to the default token value after restoring the factory settings (see ["API Tokens", page 170](#)).

Recommendation: Use the user “onvif_admin_user” for ONVIF tests (see ["ONVIF", page 88](#)).

[1] Create User: Adds a user. **Profile** is opened.

[2] Delete selected User: Deletes the selected users.

[3] Filter: Enter a search term to filter the users accordingly.

[4] Select all Users: Activate to select all users.

[5] **Username:** Shows the username.

[6] **Roles:** Shows the roles assigned to the user.

[7] **Edit:** Edit the user. **Profile** is opened.

[8] **Select User:** Activate to select the user.

5.29.2. PROFILE

The following functions are available:

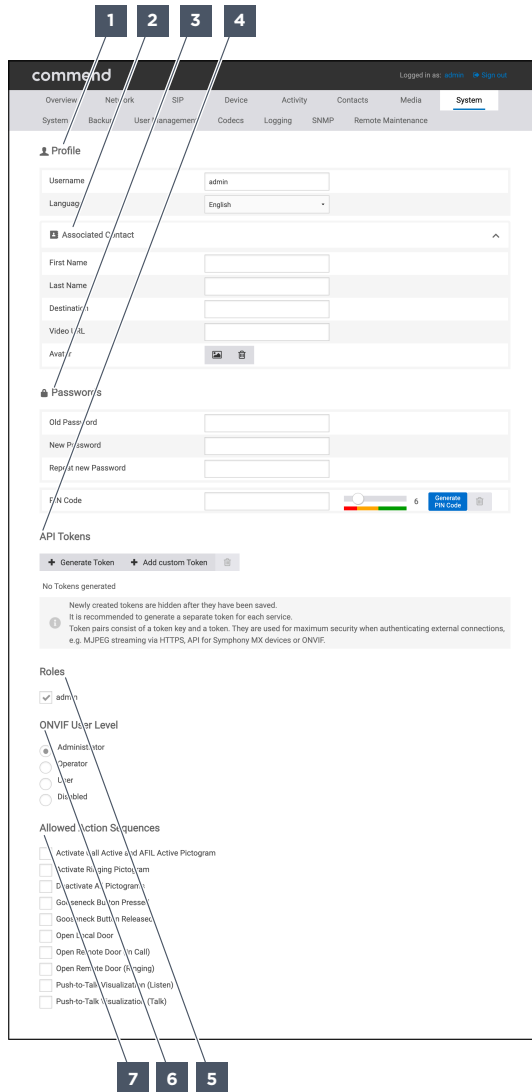


Figure 187: User Management – Profile

1 Profile

2 Passwords

3 API Tokens

4 Roles

5 ONVIF User Level

6 Allowed Action Sequences

[1] **Profile:** Manage the settings for the user.

[2] **Passwords:** Manage the passwords for the user.

[3] **API Tokens:** Manage the API tokens for the user.

[4] **Roles:** Manage the roles for the user.

[5] ONVIF User Level: Manage the ONVIF permissions for the user.

[6] Allowed Action Sequences: Manage the action sequences for the user.

5.29.2.1. PROFILE

The following functions are available:

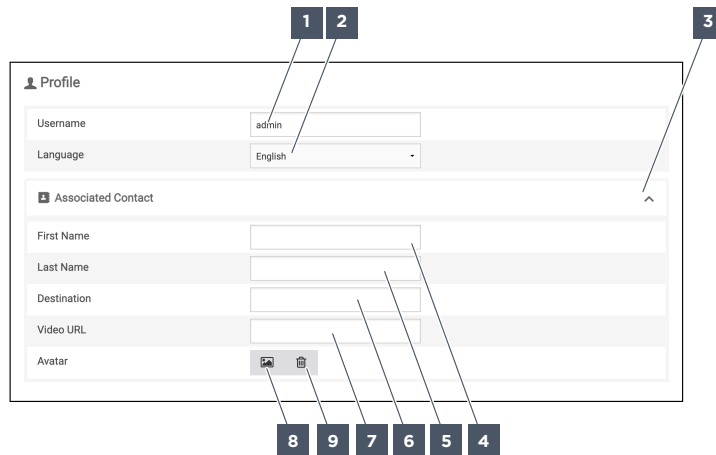


Figure 188: User Management - Profile - Profile

- | | | |
|---------------------|--------------------|---|
| 1 Username | 2 Language | 3 Show / Hide Associated Contact |
| 4 First Name | 5 Last Name | 6 Destination |
| 7 Video URL | 8 Upload | 9 Delete |

[1] Username: Enter the username. The username must not match the **First Name** and **Last Name**.

[2] Language: Select the user language for the web interface of the device. When the user logs in, this language is displayed.

Options:

- English
- German
- French
- Spanish
- Russian
- Dutch
- Italian
- Polish

[3] Show/Hide Associated Contact: Shows the contact with which the user is linked. The contact configuration can be hidden. When an associated contact is created, the contact is added to **Contacts**.

[4] First Name: Enter the first name.

[5] Last Name: Enter the last name.

[6] Destination: Enter the IPv4 address, IPv6 address or SIP call destination. The SIP URI of the remote station must be entered for peer-to-peer calls.

[7] Video URL: Enter the video URL in HTTP format or HTTPS format.

[8] Upload: Uploads an avatar.

Image properties:

- **File size:** max. 6 MB.
- **File format:** JPG, PNG.

Recommendation:

- **Size (W x H):** 100 x 100 pixels for the layout “Indoor” and “Outdoor”. 400 x 400 pixels for the layout “Contact Management”.
- **Resolution:** 72 dpi.
- **File format:** PNG 24, with transparencies.
- **Colour space:** sRGB
- If the avatar is used as a button image, choose square dimensions.

[9] Delete: Deletes the avatar.

5.29.2.2. PASSWORDS

The following functions are available:

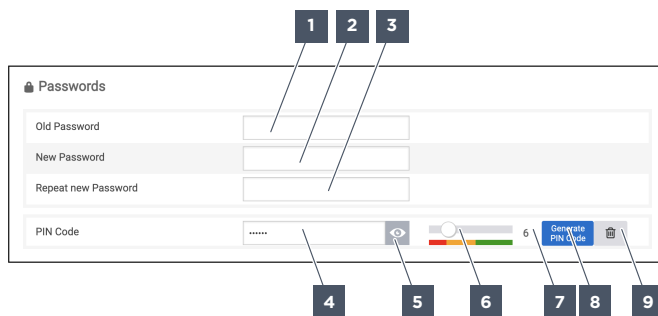


Figure 189: User management – Profile – passwords

- | | | |
|--------------------------|----------------------------|------------------------------|
| 1 Old Password | 2 New Password | 3 Repeat new Password |
| 4 PIN Code | 5 Hide | 6 Security |
| 7 Security Number | 8 Generate PIN Code | 9 Delete |

[1] Old Password: Enter the old password if the password needs to be changed. When a new user is created, a password must be entered.

[2] New Password: Enter the new password if the password needs to be changed.

[3] Repeat new Password: Enter the new password again if the password needs to be changed.

[4] PIN Code: Enter a PIN code that is unique within the device and between 4 and 16 digits. When the PIN code is generated using **[7] Generate PIN Code**, the PIN code is displayed in **[4] PIN Code**. After the PIN code is entered or generated, it is displayed until the configuration is saved. After saving, an eight-digit placeholder for the PIN code is displayed. Only users with the permission “User Management” can change the PIN code for users. Default: empty.

Recommendation: Write down the PIN code before saving.

[5] Hide: Hides the PIN code. The PIN code can only be displayed after it is entered or generated. The PIN code can no longer be displayed after it is saved.

[6] Security: Adjust the digits for the PIN code that needs to be generated. The more digits the PIN code has, the stronger the PIN code is. Value Range: “4” to “16”. Default: “6”.

[7] Security Number: Shows the number of digits for the PIN code that will be generated.

[8] Generate PIN Code: Generate a PIN code for the user. This PIN code is unique in the device.

[9] Delete: Deletes the PIN code.

5.29.2.3. API TOKENS

The following functions are available:

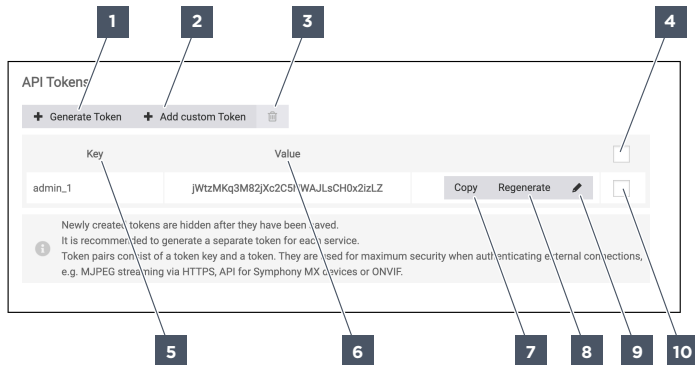


Figure 190: User Management – Profile – API-Token

- | | | |
|---------------------------|---------------------------|-----------------|
| 1 Create Token | 2 Add custom Token | 3 Delete |
| 4 Select all Token | 5 Key | 6 Value |
| 7 Copy | 8 Regenerate | 9 Edit |
| 10 Select Token | | |

The device uses tokens for authentication. The tokens consist of a token key and a token value. By default, the digest authentication mode is used for authentication. The basic authentication mode can also be activated for authentication.

Example: Tokens are used to call up MJPEG streams via HTTPS, to allow access to MX Device API or to access ONVIF functions of the device using a VMS system.

In software version 02.07.00.83 and higher, tokens are required for all services that are connected to the device and require authentication. User-based authentication is no longer possible. To migrate from one software version lower than 02.07 to 02.07 or higher, all relevant access requirements must be observed. If a service such as a video stream has been used with authentication, the username and password must be used for this service. One user must be created for API communication. All required roles must be assigned to the user. The username may not be identical with a name used for authentication. After creating the username, the user can create a token pair for each service. Tokens can be generated automatically. For migration of an older software version, an existing username can be configured as the token key and the password as the token value for the token pair. Several tokens can be created. One token can be used for several services.

Benefits:

- A separate token can be used for each service to ensure the best possible security.
- One token key and one token value are required for each user. User-specific data such as the username and password are not transferred in the network.
- Existing connections to a camera, an API or a ComPLC remain compatible.
- Existing connections do not need to be re-configured. User-specific tokens can be created with the username as the token key and the password as the token value.

Recommendation: Use a separate token for each service.

By default, the default token “onvif_admin” is available for the user “onvif_admin_user”. The default token value for the default token is: 4XkqzPOx9C83K7ePGoULj2L7fw4xJHKL

[1] Create Token: Adds a token whose token value is generated automatically. Automatically generated tokens guarantee the best possible security.

Recommendation: Always set tokens to generate automatically.

[2] Add custom Token: Adds a token whose token value can be entered.

[3] Delete: Deletes the selected tokens.

[4] Select all Tokens: Activate to select all tokens.

[5] Key: Shows the token key. The token key may not match an existing token key or a username.

[6] Value: Shows the token value. After the token value is entered or generated, it is displayed until the configuration is saved. After saving, a placeholder for the token value is displayed.

Recommendation: Write down the token value before saving.

[7] Copy: Copies the token value. If the token value is too long and not completely displayed, the token value can be copied.

[8] Regenerate: Regenerates the token value. When the token value is being regenerated, a manually entered token value is overwritten. If the configuration is saved after the token value is regenerated, the old token value is invalid.

[9] Edit: Edit the token. If the token has been generated automatically, the token value cannot be edited.

[10] Select Token: Activate to select the token.

5.29.2.4. EDIT API TOKEN

The following functions are available:

Figure 191: User Management – Profile – edit API-Token

1 Key
4 Use

2 Value

3 Abort

[1] Key: Enter the token key. By default, the user name and a consecutive number are entered automatically.

Recommendation: Enter a token key that does not match the username.

[2] Value: Enter the token value. The token value can be entered only if a user-specific token has been added. The token value must be between 12 and 64 characters long. The token value may contain the following characters: [SPACE] _ a b c d e f g h i j k l m n o p q r s t u v w x y z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0 1 2 3 4 5 6 7 8 9 ^ \$? . * + - & [{ () }] | \ / ! # % : ; , = @ -

[3] Abort: Cancels the process and the user refrains from editing the token.

[4] Use: Saves the token.

5.29.2.5. ONVIF USER LEVEL

The following functions are available:

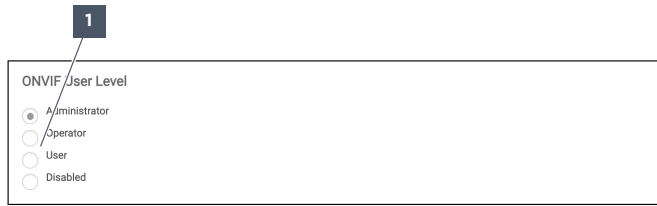


Figure 192: User Management – Profile – ONVIF User Level

1 ONVIF User Level

[1] ONVIF User Level: Select the ONVIF user level. Default: “Disabled”.

Options:

- **Administrator:** The user has the administrator permissions defined in ONVIF Profile S.
- **Operator:** The user has the operator permissions defined in ONVIF Profile S.
- **User:** The user has the user permissions defined in ONVIF Profile S.
- **Disabled:** The user has no ONVIF permissions.

5.29.2.6. ROLES

The following functions are available:



Figure 193: User Management – Profile – Roles

1 Roles

[1] Roles: Activate to assign roles to the user. Default: “admin”.

5.29.2.7. ALLOWED ACTION SEQUENCES

The following functions are available:

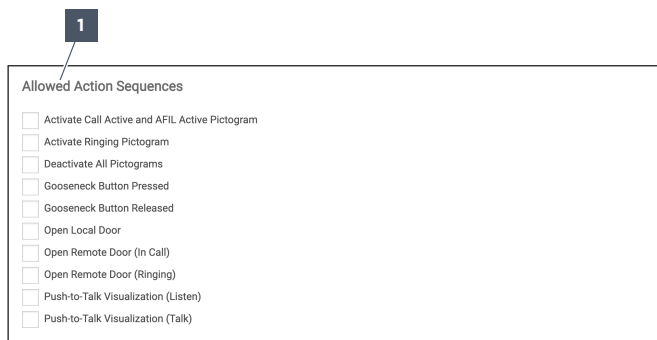


Figure 194: User Management – Allowed Action Sequences

1 Action Sequences

[1] Action Sequences: Activate to allow the user to run action sequences. If the user wants to run action sequences, a PIN code must be configured for the user. Default: none.

5.29.3. ROLES

The following functions are available:

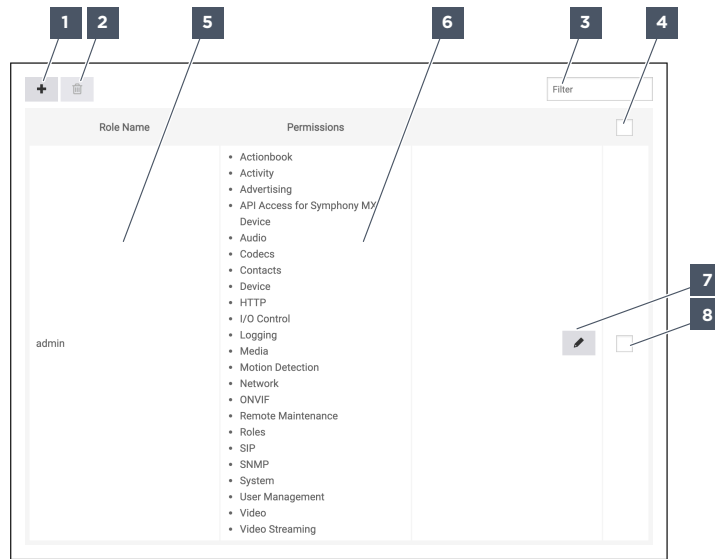


Figure 195: User Management – Roles

- | | | |
|---------------------------|-------------------------------|----------------------|
| 1 Add new Role | 2 Delete selected Role | 3 Filter |
| 4 Select all Roles | 5 Role Name | 6 Permissions |
| 7 Edit | 8 Select Role | |

By default, the roles “admin”, “ONVIF Administrator”, “ONVIF Operator” and “ONVIF User” are available.

Recommendation: Use only the default ONVIF roles for ONVIF purposes. Do not change the default ONVIF roles.

- [1] Add new Role:** Adds a role.
- [2] Delete selected Role:** Deletes the selected roles.
- [3] Filter:** Enter a search term to filter the roles accordingly.
- [4] Select all Roles:** Activate to select all roles.
- [5] Role Name:** Shows the role name.
- [6] Permissions:** Shows the permissions for the role.
- [7] Edit:** Edit the role.
- [8] Select Role:** Activate to select the role.

5.29.4. EDIT ROLE

The following functions are available:

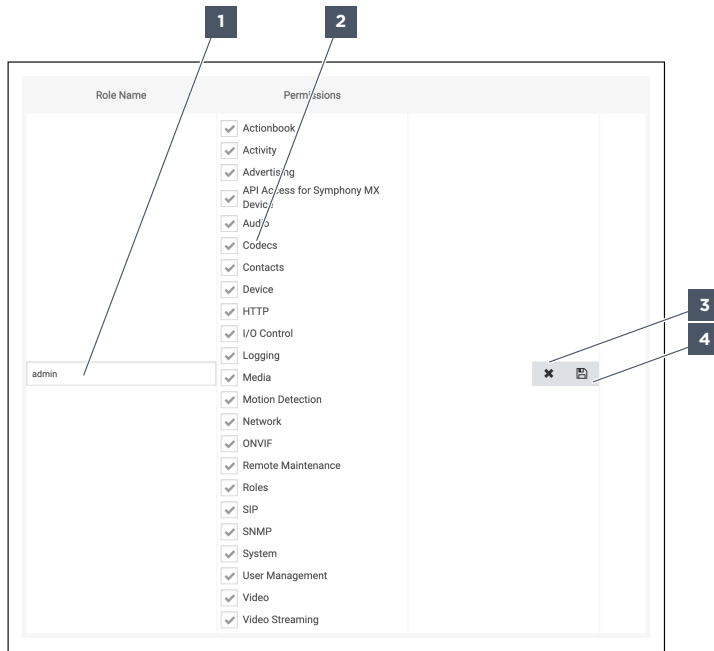


Figure 196: User Management – edit Role

- 1 Role Name
- 2 Permissions
- 3 Abort
- 4 Save

[1] Role Name: Enter the role name.

[2] Permissions: Activate to assign permissions for the role. Permissions in roles determine which pages and functions can be used by a user.

The permissions “ONVIF Actuate”, “ONVIF Read Media”, “ONVIF Read System”, “ONVIF Read System Secret”, “ONVIF Read System Sensitive”, “ONVIF Unrecoverable” and “ONVIF Write System” are defined in the ONVIF standard.

Example: If the role “User Management” is not activated for a user, this user cannot call up the **User Management** page. The user cannot manage other users.

Options:

- **Action Sequences:** The **Action Sequences** page can be called up.
- **Activity:** The **Activity** page can be called up.
- **API access for Symphony MX Device:** The device can be remote controlled via the MX Device API interface.
- **Audio:** The **Audio** page can be called up.
- **User Management:** The **User Management** page can be called up. A user with this permission can add or delete other users. A user with this permission can change the PIN code and the password of another user. Changes can be made to the user without requiring the password of the user.
Recommendation: Activate this permission only for roles that are provided for administrators.
- **Motion Detection:** The **Motion Detection** page can be called up.
- **Codecs:** The **Codecs** page can be called up.
- **Remote Maintenance:** The **Remote Maintenance** page can be called up.
- **Device:** The **Device** page can be called up.
- **HTTP:** HTTP requests can be received by the user and their password.

- **I/O Control:** The **IOs** page can be called up.
- **Contacts:** The pages below **Contacts** can be called up.
- **Logging:** The **Logging** page can be called up.
- **Media:** The pages below **Media** can be called up.
- **Network:** The pages below **Network** can be called up.
- **ONVIF:** The **ONVIF** page can be called up.
- **Roles:** The **Roles** page can be called up.
- **SIP:** The pages below **SIP** can be called up.
- **SNMP:** The **SNMP** page can be called up.
- **System:** The **System** page can be called up.
- **Video:** The **Video** page can be called up.
- **Video Streaming:** Video streams and the still picture of the camera of the device can be called up.
- **Advertising:** The **Advertising** page can be called up.

[3] **Abort:** Cancels the process and the user refrains from editing the role.

[4] **Save:** Saves the role.

5.30. CODECS

The following functions are available:

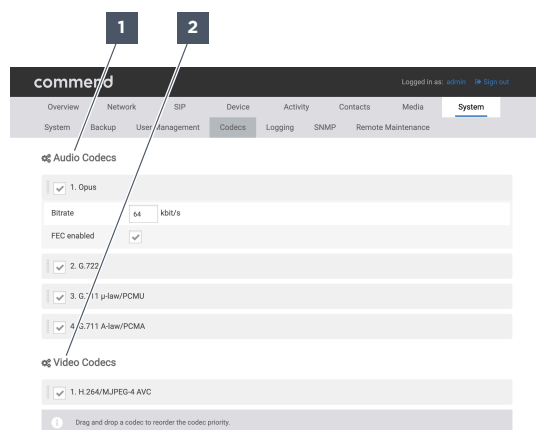


Figure 197: Codecs

1 Audio Codecs

2 Video Codecs

[1] **Audio Codecs:** Configure the audio codecs.

[2] **Video Codecs:** Configure the video codecs.

5.30.1. AUDIO CODECS

The following functions are available:

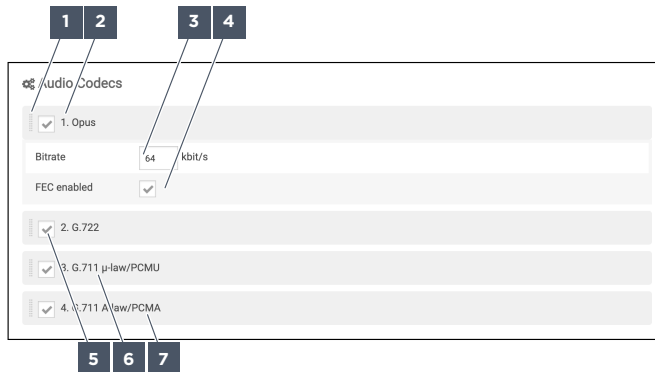


Figure 198: Codecs - Audio Codecs

- | | | |
|---------------------------|----------------|--------------------------------|
| 1 Move Codecs | 2 Opus | 3 Bitrate |
| 4 FEC aktiviert | 5 G.722 | 6 G.711 μ -law/PCMU |
| 7 G.711 A-law/PCMA | | |

At least one audio codec must be enabled.

[1] Move Codecs: Change the codec sequence by moving the codec to the desired spot. “1.” is the highest priority, “4.” is the lowest priority. If the audio codec of the device with the highest priority is not supported by the remote station, the audio codec with the next highest priority is used. Default: 1. “Opus”, 2. “G.722”, 3. “G.711 μ -law/PCMU”, 4. “G.711 A-law/PCMA”.

The device used to initiate a call determines the audio codec to be used.

Example: The codec sequence on the device is 1. “Opus”, 2. “G.722”, 3. “G.711 μ -law/PCMU”, 4. “G.711 A-law/PCMA”. The codec sequence on the remote station is 1. “G.722”, 2. “G.711 μ -law/PCMU”, 3. “G.711 A-law/PCMA”, 4. “Opus”. When calls are initiated using the device, the audio codec “Opus” is used. When calls are initiated using the remote station, the audio codec “G.722” is used.

Recommendation: Do not change the standard codec sequence for the device.

[2] Opus: Enable in order to compress the audio signals in accordance with the “Opus” standard. Default: enabled.

[3] Bitrate: Enter the bitrate for Opus audio signals in kbps. Value Range: “6” to “510”. Default: “64”.

[4] FEC enabled: Enable in order to use the forward error correction for the transmission of audio signals. If this function is disabled, the error probability is higher and the data transfer rate is lower when transmitting audio signals. Default: enabled.

[5] G.722: Enable in order to compress the audio signals in accordance with the “G.722” standard. Default: enabled.

[6] G.711 μ -law/PCMU: Enable in order to compress the audio signals in accordance with the “G.711 μ -law/PCMU” standard. Default: enabled.

[7] G.711 A-law/PCMA: Enable in order to compress the audio signals in accordance with the “G.711 A-law/PCMA” standard. Default: enabled.

5.30.2. VIDEO CODECS

The following functions are available:

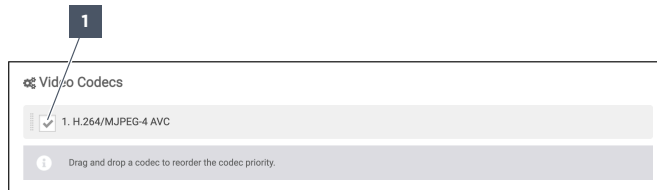


Figure 199: Codecs – Video Codecs

1 H.264/MJPEG-4 AVC

[1] H.264/MJPEG-4 AVC Enable in order to compress the video signals in accordance with the “H.264” standard. This function cannot be disabled. Default: enabled.

5.31. LOGGING

The following functions are available:

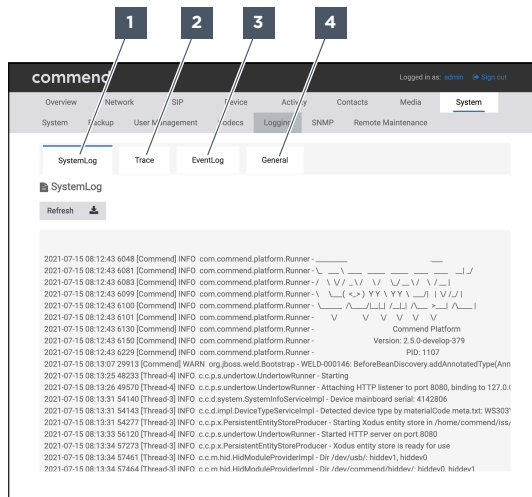


Figure 200: Logging

1 SystemLog

2 Trace

3 EventLog

4 General

⚠ CAUTION

Sensitive Data

Unauthorised access to sensitive data or to the system

Assign the permission “Logging” only to administrators. Assign the permission “Logging” only to the users who are authorised to view sensitive data.

[1] SystemLog: Shows the processes of the device.

[2] Trace: Shows incoming and outgoing data packets of the device that are transmitted via the network.

[3] EventLog: Shows the events of the device.

[4] **General:** Configure general logging settings.

5.31.1. SYSTEMLOG

The following functions are available:

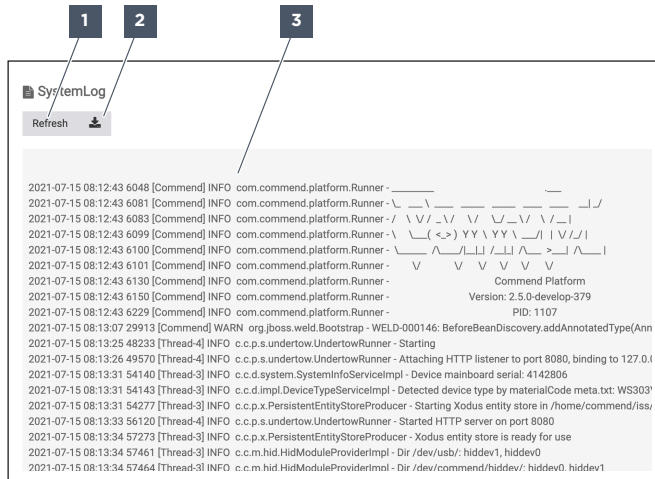


Figure 201: Logging – SystemLog

- 1 Refresh
- 2 Download SystemLog
- 3 Logs

[1] **Update:** Updates the displayed SystemLog entries.

[2] **Download SystemLog:** Downloads the SystemLog entries as a TXT file.

[3] **Logs:** Shows the SystemLog entries.

5.31.2. TRACE

The following functions are available:

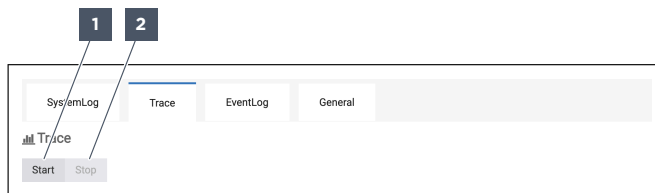


Figure 202: Logging – Trace

- 1 Start
- 2 Stop

[1] **Start:** Start tracing. When started, a PCAP file is added on the local computer. In this file, all incoming and outgoing data packets are saved chronologically in an ongoing process until the tracing is stopped. Only after the tracing is stopped, the PCAP file can be opened. Every time the tracing is started again, a new PCAP file is added.

If the system load of the device fluctuates heavily, individual network packets like RTP packets containing audio streams may not be saved correctly.

Recommendation: Use tracing only for a quick overview of the network traffic.

[2] **Stop:** Stop tracing.

5.31.3. EVENTLOG

The following functions are available:

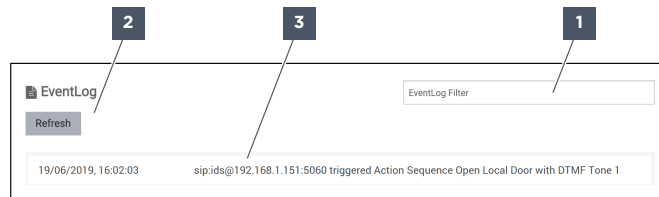


Figure 203: Logging - Eventlog

- 1** EventLog Filter
- 2** Refresh
- 3** Logs

[1] EventLog-Filter: Enter a search term in order to filter the event logs accordingly.

[2] Update: Updates the displayed event log entries.

[3] Logs: Shows the event log entries. Only events and actions triggered by DTMF tones are shown.

5.31.4. GENERAL

The following functions are available:

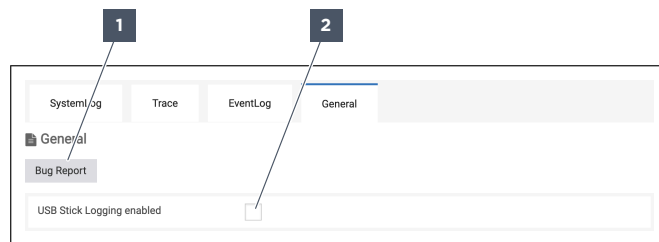


Figure 204: Logging - General

- 1** Bug Report
- 2** USB Stick Logging enabled

[1] Bug Report: Downloads the bug report as a ZIP file. A backup is created and added to the ZIP file. The bug report contains information for the support team.

[2] USB Stick Logging enabled: Enable in order to save log data to a USB stick. Log files are saved to the USB stick, regardless of the device state. Log files are saved to the USB stick when starting up or restarting. The USB stick must be connected before enabling the function. The USB stick is linked with the device. The function must be disabled before the USB stick is removed. The USB stick must be formatted with the "FAT32" file system. The loss of log files is prevented by restoring the factory defaults. Default: disabled.

Recommendation: Zip the log files on the USB stick and make them available to the support team.

5.32. SNMP

The following functions are available:

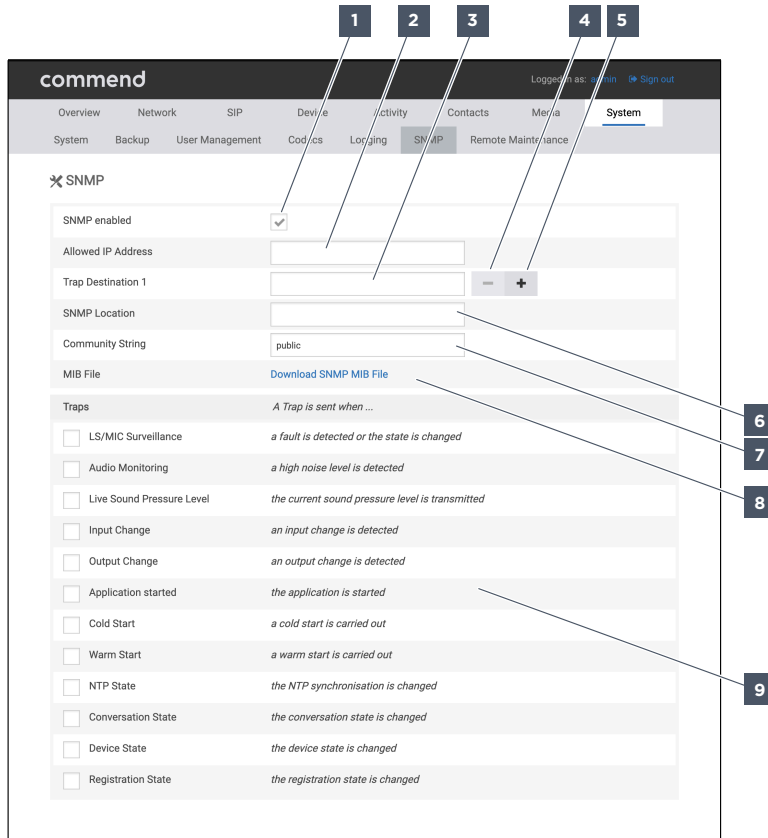


Figure 205: SNMP

- | | | |
|----------------------------------|-------------------------------|-----------------------------|
| 1 SNMP enabled | 2 Allowed IP Address | 3 Trap Destination 1 |
| 4 Delete Trap Destination | 5 Add Trap Destination | 6 SNMP Location |
| 7 Community String | 8 MIB File | 9 Traps |

[1] SNMP enabled: Enable to ensure that SNMP trap packets can be sent. Default: disabled.

[2] Allowed IP Address: Enter the IPv4 address or IPv6 address. Users can access the MIB database from this IP address. When this field is empty, no restrictions apply. Default: empty.

The syntax elements for inputs and the syntax elements for outputs are structured as follows when calling up the MIB database in an MIB browser.

Syntax elements:

- **<Product ID>:** The device on which the inputs and outputs are located. **Example:** "EB3E2A-AUD".
- **<Serial Number>:** The serial number of the device. **Example:** "3878517".
- **<Name>:** The input designation or output designation. **Example:** "input1".

The syntax elements are separated by a hyphen.

Example: "EB3E2A-AUD-3878517-input1".

[3] Trap Destination 1: Enter the IPv4 address or IPv6 address. This IP address automatically receives SNMP trap packets. These SNMP trap packets contain the traps enabled in **[9] Traps**. Default: empty.

[4] Remove Trap Destination: Removes the trap destination.

[5] Add Trap Destination: Adds a trap destination. A maximum of 3 trap destinations can be managed.

[6] SNMP Location: Enter the location of the device. The device can be localised by an authorised computer using this location. Default: empty.

Example: “Entrance hall”, “Elevator”, “Package deliverer entrance”.

[7] Community String: Enter the password for accessing the MIB database. Default: “public”.

[8] MIB File: Downloads the MIB file.

[9] Traps: Enable in order to send SNMP trap packets for the following functions. Default: disabled.

SNMP trap packets:

- **Loudspeaker/Microphone Surveillance:** Sent when a fault is detected by the loudspeaker/microphone surveillance or the device state changes.
- **Audio Monitoring:** Sent when the threshold level is exceeded.
- **Current Sound Pressure Level:** Sent when the last measured sound pressure level is transmitted.
- **Input Change:** Sent when an input change to the accessories is detected.
Example: EB3E2A-AUD, IP-CON.
- **Output Change:** Sent when an output change to the accessories is detected.
Example: EB3E2A-AUD, IP-CON.
- **Application Started:** Sent when the application is started.
- **Cold Start:** Sent when a cold start is performed.
- **Warm Start:** Sent when a warm start is performed.
- **NTP Status:** Sent when no NTP synchronisation is possible.
Example: When starting the device, when the connection to an NTP server has failed.
- **Conversation State:** Sent when the conversation state is changed.
- **Device State:** Sent when the device state is changed.
- **Registration State:** Sent when the registration state at a SIP server is changed.

5.33. REMOTE MAINTENANCE

The following functions are available:

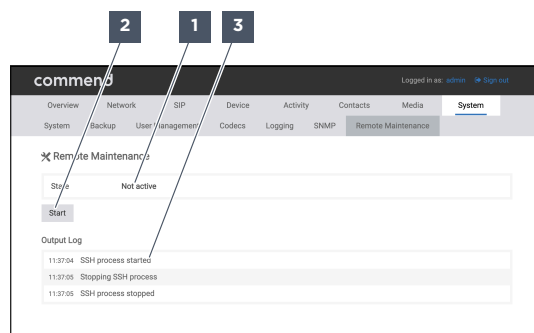


Figure 206: Remote Control

1 State

2 Start

3 Output Log

[1] State: Shows the state of remote maintenance.

Information:

- **Not active:** No connection has been established.
- **Active:** A connection has been established.

[2] Start: Starts remote maintenance for support purposes. The device must be connected to the Internet. Remote maintenance can be stopped.

Recommendation: Do not stop remote maintenance until Support prompts you to do so.

[3] Output Log: Shows log information for the connection. The displayed port number is required by Support to connect with the device.

Example: “/usr/bin/dbclient: Allocated port 50511 for remote forward to localhost:22”.

5.34. AVAILABLE ACTIONS

Actions can be triggered via buttons, via contact management and via action sequences.

5.34.1. CHANGE AUDIO DEVICE

The following functions are available:

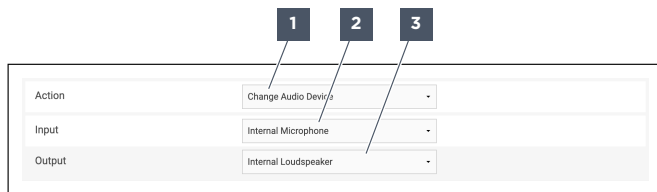


Figure 207: Available actions - Change Audio Device

1 Action

2 Input

3 Output

[1] Action: The audio device for input or output is changed.

[2] Input: Select the audio input.

[3] Output: Select the audio output.

5.34.2. PLAY AUDIO FILE

The following functions are available:



Figure 208: Available actions - Play Audio File

1 Action

2 Media File

3 Play back during Calls

[1] Action: An audio file is played back.

[2] Media File: Select the audio file that should be played back. Audio files are uploaded via **Audio Files**.

5.34.5. CHANGE DISPLAY MODE

The following functions are available:

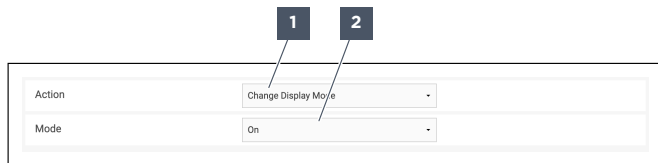


Figure 211: Available actions - Change Display Mode

- 1** Action
- 2** Mode

[1] Action: The display mode is changed. If the display is switched off, the display can be switched back on by tapping, by incoming calls or by changing the display mode via an action sequence.

Example: Switching on the display via an action sequence that is triggered by motion detection.

[2] Mode: Select the display mode.

Options:

- **On:** The display is switched on.
- **Off:** The display is turned off.

5.34.6. SEND DTMF TONE

The following functions are available:

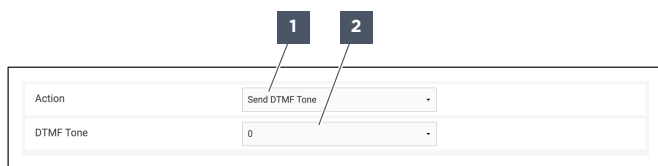


Figure 212: Available actions - Send DTMF Tone

- 1** Action
- 2** DTMF Tone

[1] Action: A DTMF tone is sent to a SIP device. This function is supported only in the modes “SIP Info” and “RTP Event (RFC 2833)” (see “SIP Server”, page 94).

[2] DTMF Tone: Select the DTMF tone.

Options:

- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- A
- B
- C
- D

- *
- #

5.34.7. SEND EMAIL

The following functions are available:

Action	Send Email
Receiver	
Subject	
Content	

Figure 213: Available actions - Send Email

- 1 Action
- 2 Receiver
- 3 Subject
- 4 Content

[1] Action: An email is sent. The device must be connected to the Internet.

[2] Receiver: Enter the email address of the recipient.

[3] Subject: Enter the subject.

[4] Content: Enter the message.

5.34.8. CANCEL CALL

The following functions are available:

Action	Cancel Call
--------	-------------

Figure 214: Available actions - Cancel Call

- 1 Action

[1] Action: The call is ended. If the device is in the device states "Idle" and "Error", this action is not performed.

5.34.9. ON HOLD

The following functions are available:

Action	On Hold
Value	Toggle

Figure 215: Available actions - On Hold

- 1 Action
- 2 Value

[1] Action: The call is held. The call can be resumed by changing the value or via the action “Answer Call”. If the device is in the device states “Idle”, “Incoming call”, “Outgoing call” or “Error”, this action is not performed.

[2] Value: Select the value.

Options:

- **On:** The call is held.
- **Off:** The call is resumed.
- **Toggle:** If the call is held, the call is resumed. If the call is not held, the call is held.

5.34.10. HTTP CLIENT ACTION

The following functions are available:

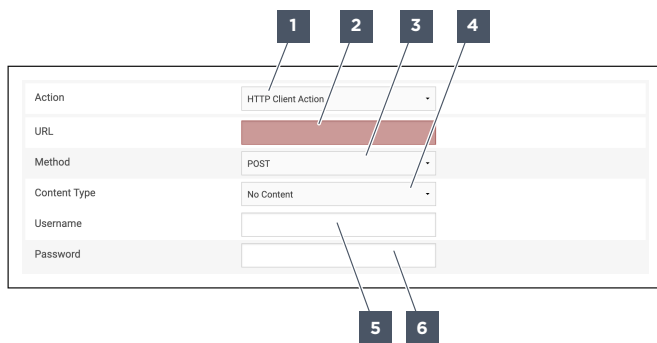


Figure 216: Available actions - HTTP Client Action

- | | | |
|-----------------------|-------------------|-------------------|
| 1 Action | 2 URL | 3 Method |
| 4 Content Type | 5 Username | 6 Password |

[1] Action: An HTTP client request is sent to a SIP device.

[2] URL: Enter the URL of the HTTP client request.

[3] Method: Select the method. The methods can be sent in JSON format, in XML format or as plain text.

Options:

- **GET**
- **POST**
- **PUT**
- **DELETE**

[4] Content Type: Select the content type. This function is only available for the method “POST”. Default: “No Content”.

Options:

- **No Content**
- **JSON**
- **XML**
- **Text/Plain**

[5] Username: Enter the user name for authentication.

[6] Password: : Enter the password for authentication.

5.34.11. DISCONNECT IP SECURE CONNECTOR

The following functions are available:



Figure 217: Available actions – Disconnect IP Secure Connector

1 Action

[1] Action: The connection to the IP-CON is disconnected. If no IP-CON is connected to the device, this action is not performed.

5.34.12. CHAIN CALL

The following functions are available:

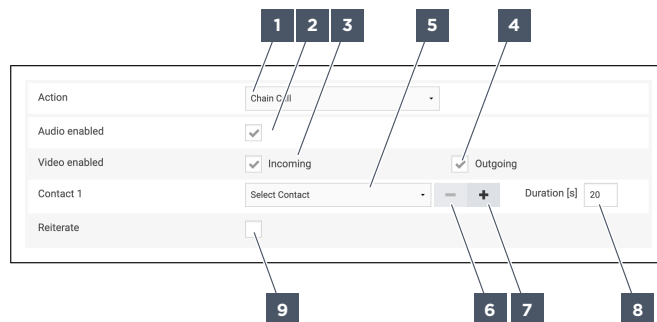


Figure 218: Available actions – Chain Call

1 Action	2 Audio enabled	3 Incoming
4 Outgoing	5 Contact 1	6 Remove Contact
7 Add Contact	8 Duration [s]	9 Reiterate

[1] Action: A call is initiated to several contacts one after the other. If the call is not accepted by a contact in the configured sequence, the call is forwarded to the next contact.

[2] Audio enabled: Activate to transmit audio signals during calls.

[3] Incoming: Activate to transmit incoming video streams during calls.

[4] Outgoing: Activate to transmit outgoing video streams during calls.

[5] Contact 1: Select the contact.

[6] Remove Contact: Remove the contact.

[7] Add Contact: Add a contact. A maximum of 32 contacts can be configured.

[8] Duration [s]: Enter the maximum time in seconds after which the call is forwarded to the next contact if it is not accepted. Range of values: "1" to "120".

[9] Reiterate: Activate to forward the call back to the first contact in the sequence after reaching the last contact in the sequence. If this function is not activated, the call is ended after the maximum time for the last contact has elapsed.

5.34.13. CHANGE VOLUME

The following functions are available:

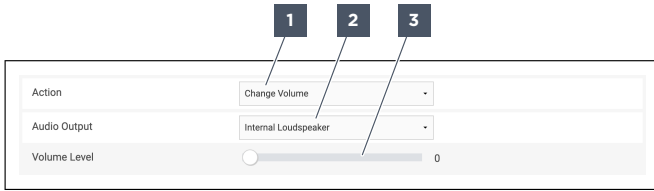


Figure 219: Available actions - Change Volume

- 1** Action
- 2** Audio Output
- 3** Volume Level

[1] Action: The volume level is changed.

[2] Audio Output: Select the audio output.

Recommendation: To avoid echoes during OpenDuplex calls, do not exceed the volume level “10”.

[3] Volume Level: Adjust the volume. Range of values: “0” to “12”.

5.34.14. CHANGE LAYOUT

The following functions are available:

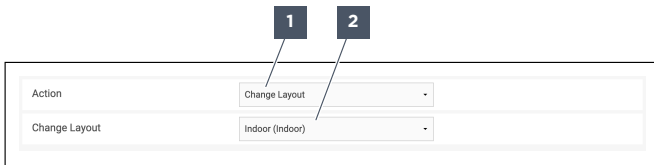


Figure 220: Available actions - Change Layout

- 1** Action
- 2** Change Layout

[1] Action: The layout that should be shown on the device is changed.

[2] Change Layout: Select the layout. A layout can be selected from all the configured layouts.

5.34.15. SET LED

The following functions are available:

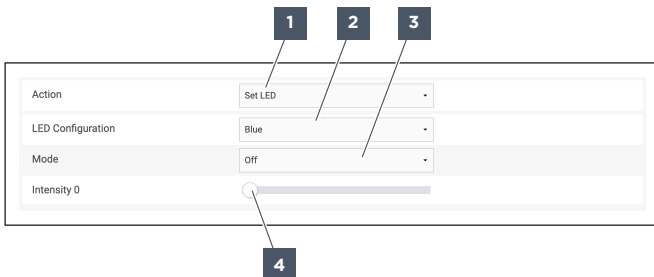


Figure 221: Available actions - Set LED

- 1** Action
- 2** LED Configuration
- 3** Mode
- 4** Intensity

[1] Action: An LED is switched.

[2] LED Configuration: Select the LED that should be switched.

[3] **Mode:** Select the state.

Options:

- **On:** The LED is switched on.
- **Off:** The LED is switched off.
- **Slow:** The LED flashes slowly.
- **Fast:** The LED flashes quickly.

[4] **Intensity:** Adjust the intensity of the LED. Range of values: "0" to "10".

5.34.16. MUTE MICROPHONE

The following functions are available:

Figure 222: Available actions - Mute Microphone

1 Action 2 Value

[1] **Action:** The microphone is muted. The microphone that is configured as audio input is muted.

[2] **Value:** Select the value.

Options:

- **On:** The microphone is switched on.
- **Off:** The microphone is muted.
- **Toggle:** If the microphone is switched on, the microphone is muted. If the microphone is muted, the microphone is switched on.

5.34.17. PARALLEL CALL

The following functions are available:

Figure 223: Available actions - Parallel Call

1 Action 2 Audio enabled 3 Incoming
 4 Outgoing 5 Contact 1 6 Remove Contact
 7 Add

[1] **Action:** A call is initiated to several contacts at the same time. If a contact accepts the call, the call is ended at all other contacts. If the call is declined by one or more contacts, the call remains active until it is accepted by a contact or it is ended via a timeout.

[2] **Audio enabled:** Activate to transmit audio signals during calls.

[3] Incoming: Activate to transmit incoming video streams during calls.

[4] Outgoing: Activate to transmit outgoing video streams during calls.

[5] Contact 1: Select the contact.

[6] Remove Contact: Remove the contact.

[7] Add Contact: Add a contact. A maximum of 32 contacts can be configured.

5.34.18. SWITCH PICTOGRAM

The following functions are available:

Action	Switch Pictogram
Pictogram	Ringing
Mode	On

Figure 224: Available actions – Switch Pictogram

1 Action

2 Pictogram

3 Mode

[1] Action: A pictogram is shown or switched. Pictograms can be shown in the device states “Incoming Call”, “Outgoing Call” and “In Call”.

[2] Pictogram: Select the pictogram.

Options:

- **Ringing**
- **In Call**
- **Open Door**
- **AFIL active**
- **Push-to-Talk enabled:** This pictogram is shown only when an ID5 DKGM or an ID5 DKHSGM is connected.

[3] Mode: Select the mode.

Options:

- **On:** The pictogram is shown.
- **Off:** The pictogram is not shown.

5.34.19. CALL

The following functions are available:

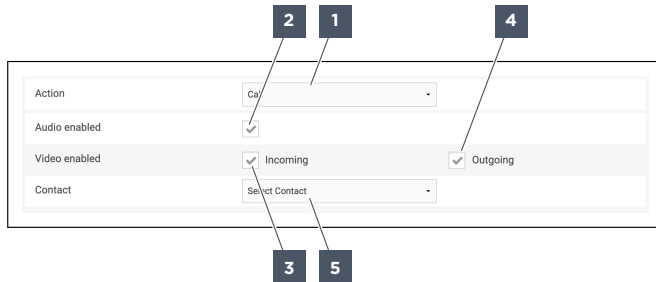


Figure 225: Available actions - Call

- 1** Action
- 2** Audio enabled
- 3** Incoming
- 4** Outgoing
- 5** Contact

[1] Action: A call to a contact is initiated.

[2] Audio enabled: Activate to transmit audio signals during calls.

[3] Incoming: Activate to transmit incoming video streams during calls.

[4] Outgoing: Activate to transmit outgoing video streams during calls.

[5] Contact: Select the contact.

5.34.20. ANSWER CALL

The following functions are available:

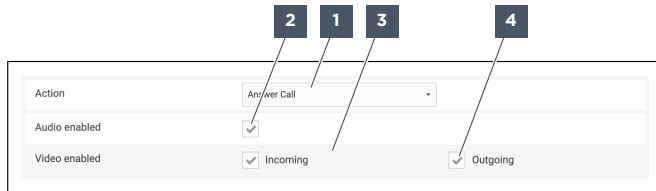


Figure 226: Available actions - Answer Call

- 1** Action
- 2** Audio enabled
- 3** Incoming
- 4** Outgoing

This action overrides the call behaviour configured in VirtuoSIS for the device if this function is activated (see ["SIP Servers", page 100](#)).

[1] Action: An incoming call is accepted.

[2] Audio enabled: Activate to transmit audio signals during calls.

[3] Incoming: Activate to transmit incoming video streams during calls.

[4] Outgoing: Activate to transmit outgoing video streams during calls.

5.34.21. CHANGE AUDIO DEVICE

The following functions are available:

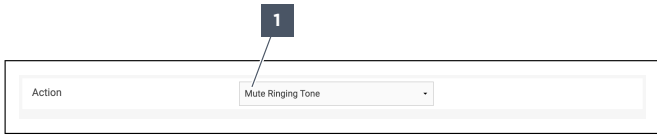


Figure 227: Available actions - Mute Ringing Tone

1 Action

[1] Action: The ringing tone is temporarily muted. The call remains unaffected.

5.34.22. SNAPSHOT

The following functions are available:

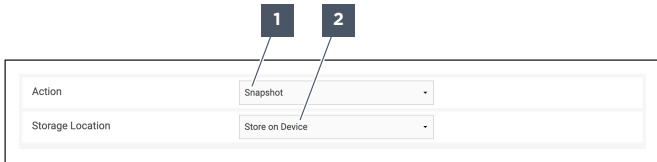


Figure 228: Available actions - Snapshot

1 Action **2** Storage Location

[1] Action: A photo is taken via the camera.

[2] Storage Location: Select the storage location for the photo.

Options:

- **Store on Device:** Photos are stored on the device. Photos can be viewed or downloaded via **Snapshots**.
- **Store in ActionSet Context:** Photos can be sent as attachments to emails. To be able to send photos as attachments to e-mails, an action sequence must be created. Photos are not stored on the device.

5.34.23. PLAY INFO MESSAGE AT THE REMOTE STATION

The following functions are available:

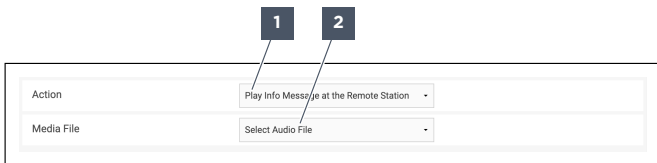


Figure 229: Available actions - Play Info Message at the Remote Station

1 Action **2** Media File

[1] Action: In the device state “In Call”, an audio file is played back at the remote station.

[2] Media File: Select the audio file that should be played back. Audio files are uploaded via **Audio Files**.

5.34.24. DELAYED ACTION

The following functions are available:

Figure 230: Available actions - Delayed Action

- 1 Action
- 2 Delay [s]
- 3 Debouncing
- 4 Action

[1] Action: Start an action only after a configured time has elapsed.

[2] Delay [s]: Enter the delay time in seconds. Range of values: "1" to "3600".

Recommendation: Long delay times can cause undesirable device behaviour. Select a delay time that is as short as possible.

[3] Debouncing: Activate to avoid performing the same actions and action sequences several times in a row. If this function is activated, the same actions or action sequences are not performed more than once during the configured delay time. If this function is deactivated, the same actions and action sequences can be performed several times. Every action or action sequence is performed in succession at intervals of the configured delay time.

[4] Action: Select the action.

5.34.25. SWITCH VIDEO

The following functions are available:

Figure 231: Available actions - Switch Video

- 1 Action
- 2 Value

[1] Action: The camera is switched on or off during calls.

[2] Value: Select the value.

Options:

- **On:** The camera is switched on.
- **Off:** The camera is muted.
- **Toggle:** If the camera is switched on, the camera is switched off. If the camera is switched off, the camera is switched on.

5.34.26. INTERRUPT ADVERTISEMENT

The following functions are available:

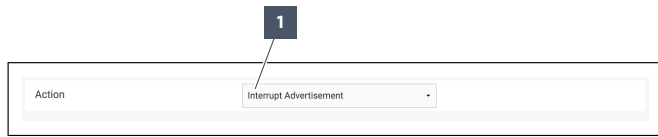


Figure 232: Available actions - Interrupt Advertisement

1 Action

[1] Action: The advertisement is interrupted. **Home** is shown. The advertising mode is not deactivated. If the advertising mode is not active, no action is performed.

5.34.27. CHANGE ADVERTISING MODE

The following functions are available:

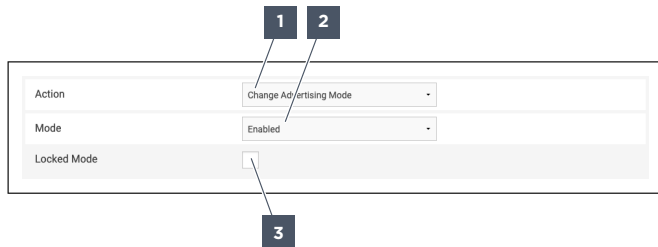


Figure 233: Available actions - Change Advertising Mode

1 Action

2 Mode

3 Locked Mode

[1] Action: The advertising mode is changed.

[2] Mode: Select the mode.

Options:

- **Enabled:** The advertising mode is activated.
- **Disabled:** The advertising mode is deactivated.

[3] Locked Mode: Activate to avoid interrupting the advertising mode by touching the display or by the action “Interrupt Advertising”. The advertising mode is shown until an incoming call is initiated or the advertising mode is changed.

5.34.28. SHOW VIEW

The following functions are available:

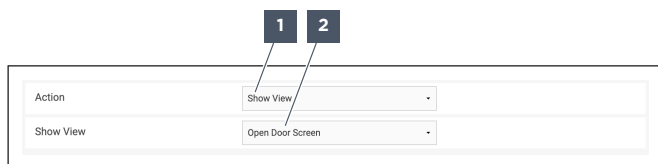


Figure 234: Available actions - Show View

1 Action

2 Show View

[1] Action: The view on the device is changed.

[2] Show View: Select the view.

Options:

- **Open Door Screen**
- **Settings Screen**
- **Show user-defined Actions**

5.35. UPLOAD WINDOW

The following functions are available:

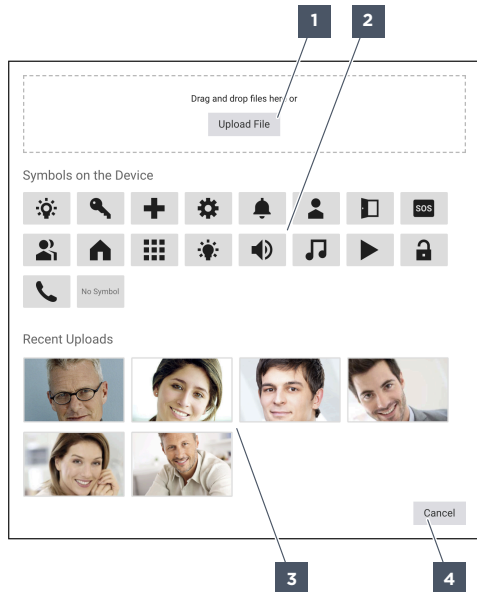


Figure 235: Upload Window

- | | | |
|---------------|-------------------------|-----------------|
| 1 Upload File | 2 Symbols on the Device | 3 Last Uploaded |
| 4 Abort | | |

If an image or symbol needs to be selected or uploaded, the Upload window appears.

[1] Upload File: Uploads one or multiple files. Files can be moved to the bordered area using drag and drop in order to upload them.

[2] Symbols on the Device: Shows symbols on the device. A symbol can be selected by clicking on it. The symbol is inserted at the desired position.

[3] Last Uploaded: Shows images on the device. An image can be selected by clicking on it. This image is inserted at the desired position.

[4] Abort: Cancels and no image or symbol is uploaded or selected.

5.36. VIDEO STREAM

The following functions are available:

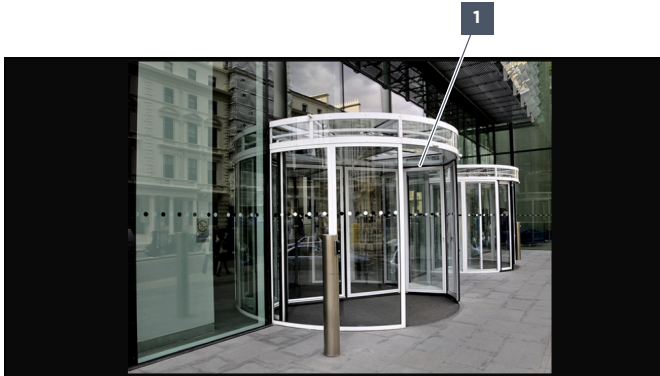


Figure 236: Videostream

1 Videostream

The IP address and “/mjpeg/video.mjpg” must be entered in the address bar of the web browser in order to call up a video stream. The entry is case-sensitive.

If the option “Enabled” is selected in **MJPEG-Streams**, up to six video streams can be called up simultaneously. If the option “Limited” is selected in **MJPEG-Streams**, only one video stream can be called up when the device is in the device state “Outgoing Call” or a call without video is established.

If **Authentication enabled** is enabled, the user’s login data must be entered to call up the video stream. A user role with the permission “Video Streaming” must be allocated to this user. Depending on the program, the user’s login data can also be entered in the URL according to the following scheme: “https://<Token Key>:<Token Value>@<IP Address>/mjpeg/video.mjpg”.

The video stream is shown in the web browser with a resolution of 480 x 640 pixels by default. A video stream requires a bandwidth of 2 to 6 Mbps.

When the video stream is called up in a web browser and **Camera Indicator** is enabled, the status LED lights up in red on the device.

[1] Video Stream: Shows the video stream of the device. The syntax elements for URL are structured as follows.

Syntax elements:

- **https://**
- **<IP address>**
- **/mjpeg/video.mjpg**

Example: “https://192.168.1.150/mjpeg/video.mjpg”.

The resolution of the video stream can be configured by the URL. The configuration “?resolution=” can be entered after the URL.

Options:

- **320x240:** The video stream is shown with a resolution of 320 x 240 pixels.
- **640x480:** The video stream is shown with a resolution of 640 x 480 pixels.
- **800x600:** The video stream is shown with a resolution of 800 x 600 pixels.
- **1024x768:** The video stream is shown with a resolution of 1024 x 768 pixels.
- **1280x960:** The video stream is shown with a resolution of 1280 x 960 pixels.

Example: "https://192.168.1.150/mjpeg/video.mjpg?resolution=320x240".

The frame rate of the video stream can be configured by the URL. The configuration "?fps=" can be entered after the URL. The frame rate can be configured with 1 to 15 images per second.

Example: "https://192.168.1.150/mjpeg/video.mjpg?fps=10".

The video stream can be transmitted via RTSP. **ONVIF enabled** must be enabled in order to transmit video streams via RTSP. The syntax elements for URL are structured as follows.

Syntax elements:

- **rtsp://**
- **<Token key>**
- **:<Token value>**
- **@<IP address>**
- **:554**

Options:

- **/h264/320x240:** The video stream is shown using the video codec H.264 and the resolution 320 x 240 pixels.
- **/h264/640x480:** The video stream is shown using the video codec H.264 and the resolution 640 x 480 pixels.
- **/h264/800x600:** The video stream is shown using the video codec H.264 and the resolution 800 x 600 pixels.
- **/h264/1024x768:** The video stream is shown using the video codec H.264 and the resolution 1024 x 768 pixels.
- **/h264/1280x960:** The video stream is shown using the video codec H.264 and the resolution 1280 x 960 pixels.
- **/mjpeg/320x240:** The video stream is shown using the video codec MJPEG and the resolution 320 x 240 pixels.
- **/mjpeg/640x480:** The video stream is shown using the video codec MJPEG and the resolution 640 x 480 pixels.
- **/mjpeg/800x600:** The video stream is shown using the video codec MJPEG and the resolution 800 x 600 pixels.
- **/mjpeg/1024x768:** The video stream is shown using the video codec MJPEG and the resolution 1024 x 768 pixels.
- **/mjpeg/1280x960:** The video stream is shown using the video codec MJPEG and the resolution 1280 x 960 pixels.

Example: "rtsp://admin:commend@192.168.1.150:554/h264/1024x768".

5.37. STILL PICTURE

The following functions are available:

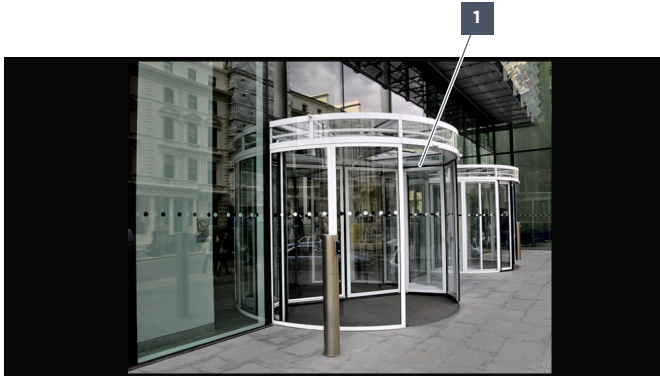


Figure 237: Standbild

1 Standbild

The IP address and “/jpeg/camimg.jpg” must be entered in the address bar of the web browser in order to call up a still picture. The entry is case-sensitive.

MJPEG-Streams has no influence on how many still pictures can be called up simultaneously.

If **Authentication enabled** is enabled, the user’s login data must be entered to call up the still picture. A user role with the permission “Video Streaming” must be allocated to this user. Depending on the program, the user’s login data can also be entered in the URL according to the following scheme: “https://<Token Key>:<Token Value>@<IP Address>/jpeg/camimg.jpg”.

The still picture is shown in the web browser with a resolution of 480 x 640 pixels by default.

When the still picture is called up in a web browser and **Camera Indicator** is enabled, the status LED lights up in red on the device for one second.

[1] Still Picture: Shows the stationary picture of the device. The still picture is created when the URL is called up. By reloading the window in the web browser, the still picture can be refreshed. The syntax elements for URL are structured as follows.

Syntax elements:

- **https://**
- **<IP address>**
- **/jpeg/camimg.jpg**

Example: “https://192.168.1.150/jpeg/camimg.jpg”.

The resolution of the still picture can be configured by the URL. The configuration “?resolution=” can be entered after the URL.

Options:

- **320x240:** The still picture is shown with a resolution of 320 x 240 pixels.
- **640x480:** The still picture is shown with a resolution of 640 x 480 pixels.
- **800x600:** The still picture is shown with a resolution of 800 x 600 pixels.
- **1024x768:** The still picture is shown with a resolution of 1024 x 768 pixels.
- **1280x960:** The still picture is shown with a resolution of 1280 x 960 pixels.

Example: “https://192.168.1.150/jpeg/camimg.jpg?resolution=320x240”.

6. INSTALLATION

6.1. IMPORT SERVER CERTIFICATE

Requirements:

- Valid server certificate available.

Windows (10)

1. Open the program “Microsoft Management Console”.
 2. Select the folder “Trusted Root Certification Authorities”.
 3. Navigate to **Action > All Tasks > Import...** .
 4. Click on **Next**.
 5. Click on **Open**.
 6. Select the certificate.
 7. Click on **Next**.
 8. Click on **Next**.
 9. Click on **Finish**.
 10. Click on **OK**.
 11. Restart the web browser.
- ✓ In the web browser, the web interface of the device is shown as “secure”.

Mac (macOS 11.3)

1. Open the program “Keychain Access”.
 2. Navigate to **File > Import Items ...**
 3. Select the certificate.
 4. Click on **Open**.
 5. Double-click the certificate.
 6. In **When using this certificate**, select “Always Trust”.
 7. Close the window. If it is necessary to enter the password for saving the configuration, enter the password.
 8. Restart the web browser.
- ✓ In the web browser, the web interface of the device is shown as “secure”.

6.2. CONFIGURE ONVIF MOTION ALARM EVENT

Requirements:

- Permission “Activity” assigned.
- Permission “ONVIF” assigned.

1. Navigate to **Network > ONVIF**.



Figure 238: ONVIF Configuration

- 1 ONVIF enabled
- 2 Event Service enabled

2. Activate [1] **ONVIF enabled**.
3. Activate [2] **Event Service enabled**.
4. Navigate to **Activity > Activity**.

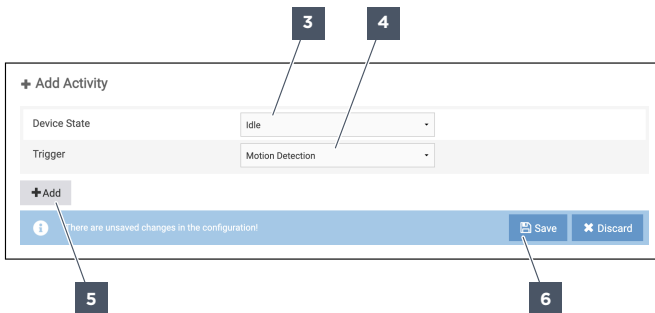


Figure 239: Configure action

- 3 Device state
- 4 Trigger
- 5 Add
- 6 Save

5. In [3] **Device State**, select “Idle”.
6. In [4] **Trigger**, select “Motion Detection”.
7. Click on [5] **Add**.
8. Click on [6] **Save**.

✓ ONVIF motion alarm events are sent to a VMS system if motion is detected via the camera. ONVIF custom call events are sent to a VMS system.

To send ONVIF motion alarm events, no action sequence needs to be configured. If action sequences should be triggered via the motion detection function, action sequences can be linked to this activity.

ONVIF motion alarm events are specified according to ONVIF Profile S (Imaging Service).

As long as a motion is detected, motion alarm messages with the value “true” are sent at intervals of two seconds. If no more motion is detected, an ONVIF motion alarm event is sent with the value “false”.

ONVIF motion alarm events cannot be sent in the device states “Incoming Call”, “Outgoing Call” and “In Call”. The motion detection function is active only in the device states “Idle” and “Error”.

6.3. ADD ACTIVITY AND ACTION SEQUENCE

Requirements:

- Permission "Actionbook" assigned.
- Permission "Activity" assigned.

1. Navigate to **Activity > Activity**.

Figure 240: Add Activity and Action Sequence – Add Activity

1 Device State
4 Add Activity

2 Trigger
5 Save Activity

3 Option

2. In [1] **Device State**, select the device state.
3. In [2] **Trigger**, select the trigger.
4. In [3] **Option**, select the option. Options are available for certain triggers only.
5. Click on [4] **Add**.
6. Click on [5] **Save**.

Figure 241: Add Activity and Action Sequence – Add Activity

6 Edit

7. Click on [6] **Edit**.

Figure 242: Add Activity and Action Sequence – Add Activity

7 Add Action Sequence

- Click on **[7] Add new Action Sequence**. The action sequence is added to **Actionbook**.

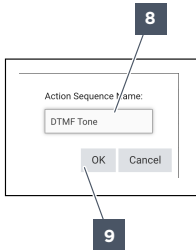


Figure 243: Add Activity and Action Sequence - Name the Action Sequence

- 8** Name of the Action Sequence
- 9** OK

- In **[8] Action Sequence Name**, enter a name.
- Click on **[9] OK**.

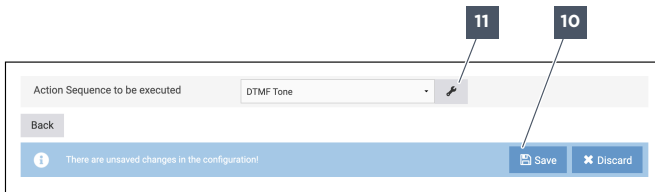


Figure 244: Add Activity and Action Sequence - Edit Action Sequence

- 11** Save
- 12** Edit

- Click on **[10] Save**.
- Click on **[11] Edit**.

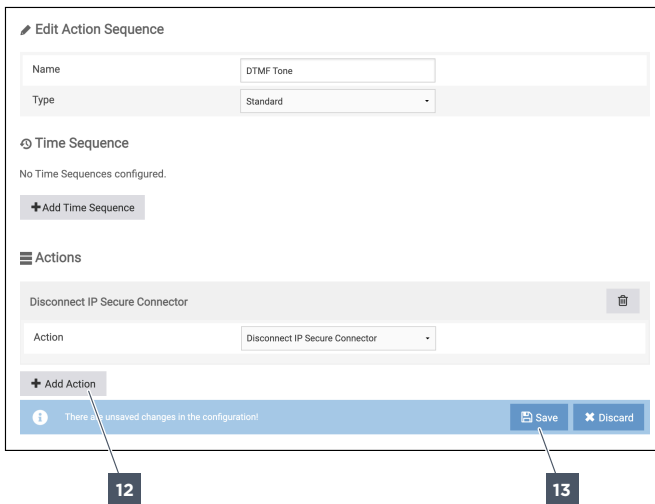


Figure 245: Add Activity and Action Sequence - Edit Action Sequence

- 12** Add
- 13** Save

- Click on **[12] Add Action**.
 - Configure the action sequence.
 - Click on **[13] Save**.
- ✓ An activity and an action sequence have been created. The action sequence is linked to the activity.

6.4. CONFIGURE LOUDSPEAKER-MICROPHONE SURVEILLANCE

Requirements:

- Permission “Actionbook” assigned.
- Permission “Activity” assigned.
- Permission “Device” assigned.
- Built-in loudspeaker configured as audio output.
- Built-in microphone configured as audio input.

1. Navigate to **Activity > Activity**.

Figure 246: Loudspeaker Microphone Surveillance – Add Activity

- | | | |
|-----------------------|------------------|-------------|
| 1 Device State | 2 Trigger | 3 To |
| 4 Add | 5 Save | |

2. In **[1] Device State**, select “Any”.
3. In **[2] Trigger**, select “Loudspeaker/Microphone Surveillance”.
4. In **[3] To**, select “Failed”.
5. Click on **[4] Add**.
6. Click on **[5] Save**.

Figure 247: Loudspeaker-Microphone Surveillance – Edit Activity

- | |
|---------------|
| 6 Edit |
|---------------|

7. Click on **[6] Edit**.

Figure 248: Loudspeaker-Microphone-Surveillance – Add Action Sequence

- | |
|------------------------------|
| 7 Add Action Sequence |
|------------------------------|

- Click on **[7] Add new Action Sequence**. This action sequence is needed to show on the device if the loudspeaker-microphone surveillance test has failed.

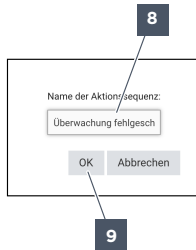


Figure 249: Loudspeaker-microphone surveillance - Name action sequence

- Name of the action sequence
 - OK
- In **[8] Action Sequence Name**, enter a name.
Example: "Surveillance failed".
 - Click on **[9] OK**.

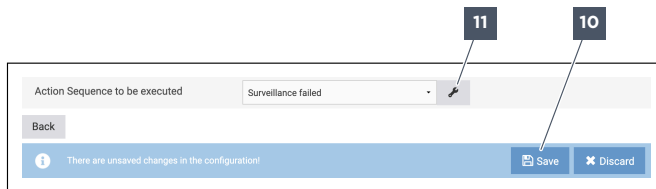


Figure 250: Loudspeaker-Microphone-Surveillance - Edit Action Sequence

- Save
 - Edit Action Sequence
- Click on **[10] Save**.

12. Click on **[11] Edit**.

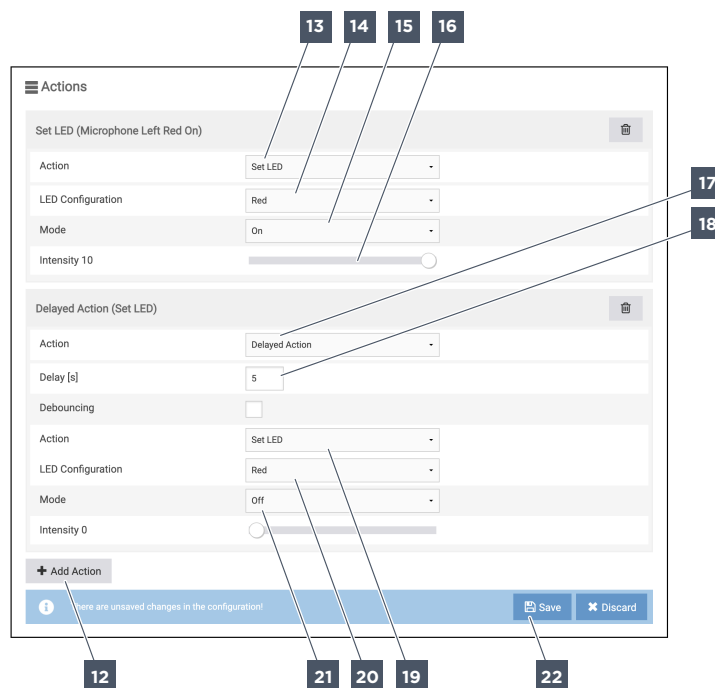


Figure 251: Loudspeaker-Microphone-Surveillance – Edit Action Sequence

12	Add Action	13	Action	14	LED Configuration
15	Mode	16	Intensity	17	Action
18	Delay [s]	19	Action	20	LED Configuration
21	Mode	22	Save		

13. Click on **[12] Add action**.
14. In **[13] Action**, select “Set LED”.
15. In **[14] LED Configuration**, select “Red”.
16. In **[15] Mode**, select “On”.
17. In **[16] Intensity**, select a value.
Recommendation: “10”.
18. Click on **[12] Add Action**.
19. In **[17] Action**, select “Delayed Action”.
20. In **[18] Delay [s]**, enter a value.
Recommendation: “5”.
21. In **[19] Action**, select “Set LED”.
22. In **[20] LED Configuration**, select “Red”.
23. In **[21] Mode**, select “Off”.
24. Click on **[22] Save**.

25. Navigate to **Activity > Activity**.

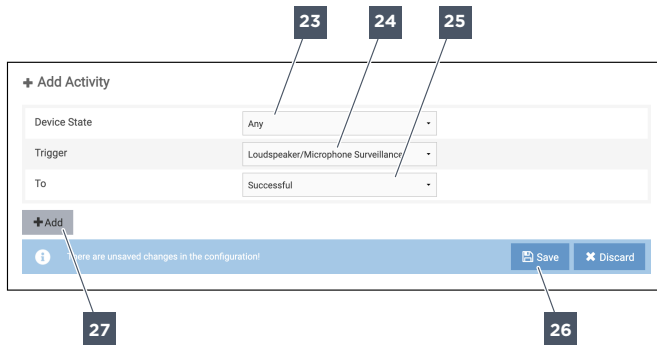


Figure 252: Loudspeaker-Microphone-Surveillance - Add Activity

- 23 Device State
- 24 Trigger
- 25 To
- 26 Save
- 27 Add

26. In [23] **Device State**, select “Any”.

27. In [24] **Trigger**, select “Loudspeaker/Microphone Surveillance”.

28. In [25] **To**, select “Successful”.

29. Click on [26] **Save**.

30. Click on [27] **Add**.

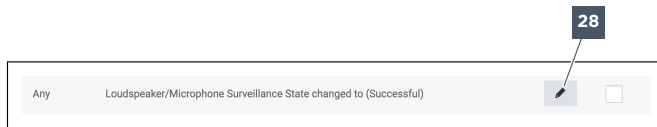


Figure 253: Loudspeaker-Microphone-Surveillance - Edit Activity

- 28 Edit

31. Click on [28] **Edit**.



Figure 254: Loudspeaker-Microphone-Surveillance - Add Action Sequence

- 29 Add Action Sequence

32. Click on [29] **Add new Action Sequence**. This action sequence is needed to show on the device if the loudspeaker-microphone surveillance test is successful.

33. In [30] **Action Sequence Name**, enter a name. **Example:** “Surveillance successful”.

34. Click on [31] **OK**.

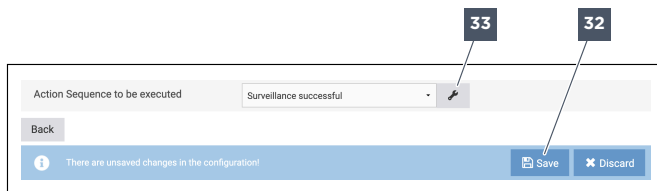


Figure 255: Loudspeaker-Microphone-Surveillance - Edit Action Sequence

- 32 Save
- 33 Edit

35. Click on [32] **Save**.

36. Click on [33] **Edit**.

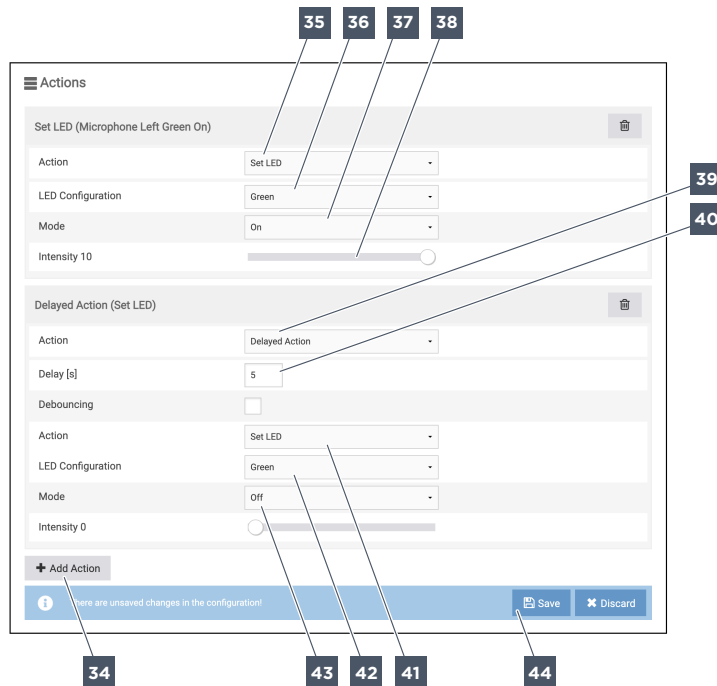


Figure 256: Loudspeaker-microphone surveillance – Edit Action Sequence

34	Add Action	35	Action	36	LED Configuration
37	Mode	38	Intensity	39	Action
40	Delay [s]	41	Action	42	LED Configuration
43	Off	44	Save		

37. Click on [34] **Add Action**.

38. In [35] **Action**, select “Set LED”.

39. In [36] **LED Configuration**, select “Green”.

40. In [37] **Mode**, select “On”.

41. In [38] **Intensity**, select a value.
Recommendation: “10”.

42. Click on [34] **Add Action**.

43. In [39] **Action**, select “Delayed Action”.

44. In [40] **Delay [s]**, enter a value.
Recommendation: “5”.

45. In [41] **Action**, select “Set LED”.

46. In [42] **LED Configuration**, select “Green”.

47. In [43] **Mode**, select “Off”.

48. Click on [44] **Save**.

49. Navigate to **Device > Audio**.

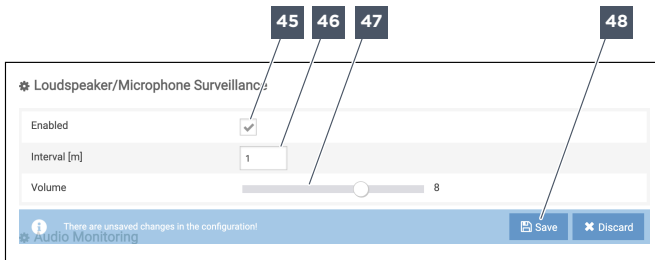


Figure 257: Loudspeaker-Microphone-Surveillance - Edit Loudspeaker-Microphone-Surveillance

- 45 Enabled
- 46 Interval [m]
- 47 Volume
- 48 Save

50. Activate **[45] Enabled**.

51. In **[46] Interval [m]**, enter a value.
Recommendation: "1".

52. In **[47] Volume**, enter a value.
Recommendation: "1".

53. Click on **[48] Save**.

✓ The loudspeaker-microphone surveillance test is configured.

54. Wait until the loudspeaker-microphone surveillance is performed.
 If the LED turns red for 5 seconds, the test has failed. Repeat the steps "[step 52](#)" and "[step 53](#)" with the next higher volume level.
 If the LED turns green for 5 seconds, the test is successful.

55. Repeat the test successfully 5 times.

56. Select the next higher volume level to ensure successful loudspeaker-microphone surveillance.

57. In **[46] Interval [m]**, enter a value.
Recommendation: "30".

58. Click on **[48] Save**.

✓ The loudspeaker-microphone surveillance is configured.

59. Navigate to **Activity > Actionbook**.

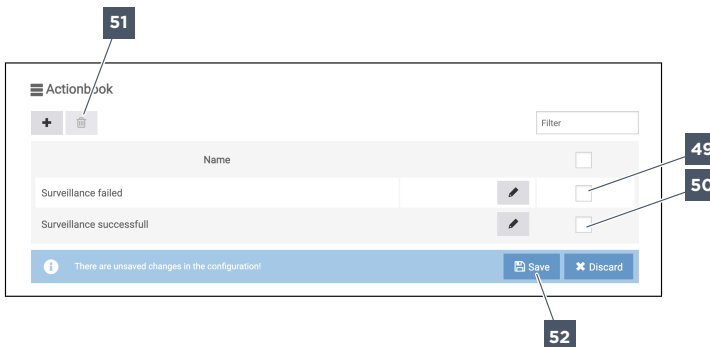


Figure 258: Loudspeaker-Microphone-Surveillance - Delete Action Sequences

- 49 Select
- 50 Select
- 51 Delete selected Action Sequences
- 52 Save

60. Activate the action sequence "[step 9](#)" by **[49]** selection.
 61. Activate the action sequence by **[50]** selection.
 62. Click on **[51] Delete selected Action Sequences**.
 63. Click on **[52] Save**.
- ✓ The action sequences needed for the test have been deleted.

6.5. INTERRUPT ADVERTISEMENT THROUGH MOTION DETECTION

Requirements:

- Permission "Actionbook" assigned.
- Permission "Activity" assigned.
- Permission "Motion Detection" assigned.

1. Navigate to **Activity > Activity**.



Figure 259: Interrupt Advertisement - Add new Action Sequence

- 1 Device State
- 2 Trigger
- 3 Add
- 4 Save

2. In **[1] Device State**, select "Idle".
3. In **[2] Trigger**, select "Motion Detection".
4. Click on **[3] Add**.
5. Click on **[4] Save**.



Figure 260: Interrupt Advertisement - Edit Action

- 5 Edit

6. Click on **[5] Edit**.



Figure 261: Interrupt Advertisement - Add new Action Sequence

- 6 Add Action Sequence

- Click on **[6] Add new Action Sequence**.

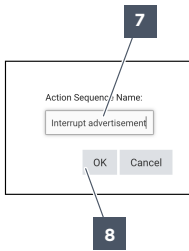


Figure 262: Interrupt Advertisement - Name action sequence

- 7** Name of the action sequence
- 8** OK

- In **[7] Action Sequence Name**, enter a name.
Example: "Interrupt advertisement".

- Click on **[8] OK**.

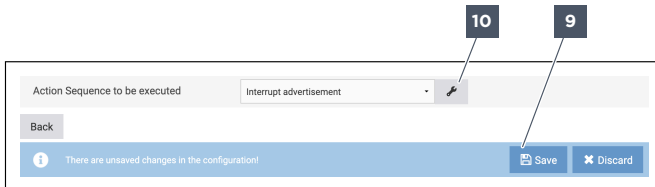


Figure 263: Interrupt Advertisement - Edit Action Sequence

- 9** Save
- 10** Edit

- Click on **[9] Save**.
- Click on **[10] Edit**.

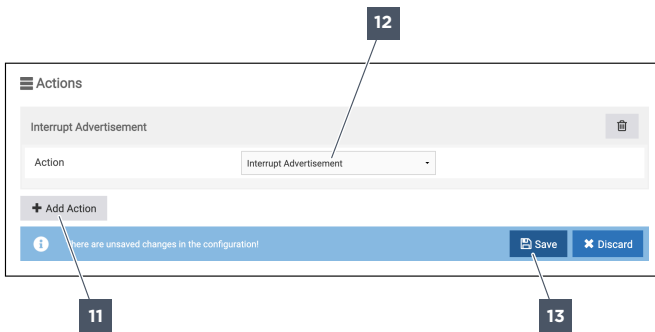


Figure 264: Interrupt Advertisement - Edit Action Sequence

- 11** Add Action
- 12** Action
- 13** Save

- Click on **[11] Add Action**.
- In **[12] Action**, select "Interrupt Advertisement".
- Click on **[13] Save**.

15. Navigate to **Device > Motion Detection**.

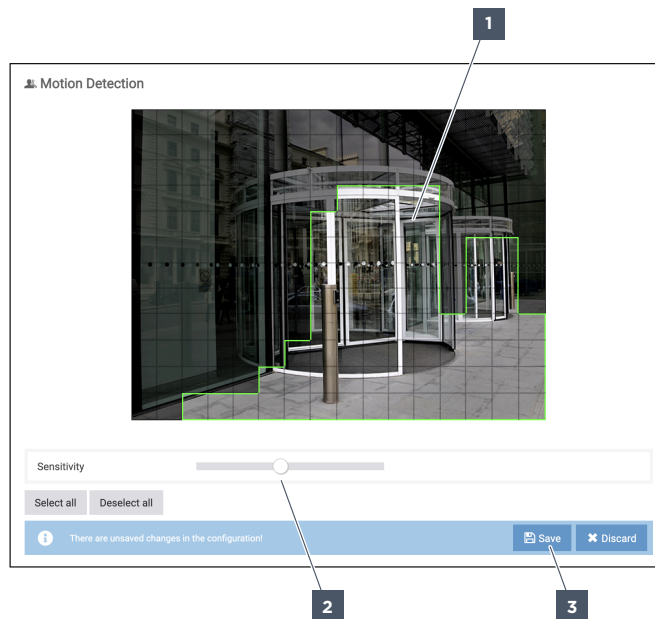


Figure 265: Configure Motion Detection

14 Video image

15 Sensitivity

16 Save

16. In [14] **Video image** activate the boxes where a person in front of the device can be detected.
Recommendation: Only enable the boxes in the area of the video preview in which the motions of people in front of the device can be detected. Disable the boxes in the area of the video preview in which unwanted motion such as road traffic, trees or clouds can be detected.
17. In [15] **Sensitivity**, select a value.
Recommendation: Have a person walk up to the device. If the motion detection function detects the person, select the next higher sensitivity level.
18. Click on [16] **Save**.

✓ The advertisement is interrupted by the motion detection function.

The motion detection function does not deactivate the advertising mode. The advertisement is interrupted and the device shows **Home**.

6.6. IMPORT BACKUP

Requirements:

- Permission "Backup" assigned.

1. Navigate to **System > Backup**.



Figure 266: Import Backup

1 Restore Backup

2. Click on **[1] Restore Backup**.

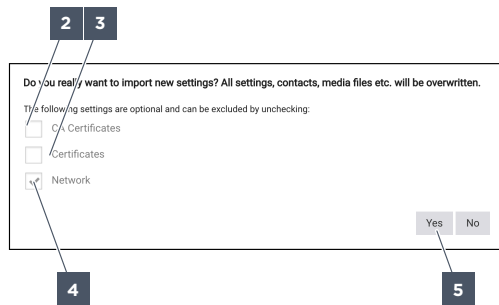


Figure 267: Import settings

- 2** CA Certificates
 - 3** Certificates
 - 4** Network
 - 5** Yes
3. Activate **[2] CA Certificates** if the certificate authority certificates should be overwritten when importing the configuration.
 4. Activate **[3] Certificates** if the certificates should be overwritten when importing the configuration.
 5. Activate **[4] Network** if the network configuration should be overwritten when importing the configuration.
 6. Click on **[5] Yes**.
- ✓ The configuration from the backup has been imported.

7. STARTUP

7.1. LAUNCHING THE WEB INTERFACE

The device's Web Interface can be launched using its IPv4 address, its IPv6 address or zeroconf. The easiest method is zeroconf. With zeroconf, the host name is used in the local DNS namespace and is found via Multicast DNS (mDNS). In certain networks, zeroconf requires the DNS namespace to be configured. The syntax elements for zeroconf are as follows:

Syntax elements:

- **https://:** Identifies the URL protocol as "HyperText Transfer Protocol Secure" (HTTPS).
- **<host name>**: the device's host name. By default, the host name consists of the device type, the processor name, and the MAC address. The MAC address can be found on the label on the rear of the device or on the packaging. The host name can be edited ([see "General", page 75](#)). Restoring the device's factory settings will reset the host name to its factory default setting.
Example: "ids-mx6-bc6a44000a38".
- **.local:** Identifies the URL string as a local URL.

If there is no valid server certificate for the web interface, the web browser may classify it as "unsafe" ([see page 199](#)).

7.1.1. LAUNCHING THE WEB INTERFACE VIA ZEROCONF

Requirements:

- Have the device's MAC address, locale and (if changed) host name information at hand.
- The device must be reachable on the network.
- The computer, smartphone or tablet device must be reachable on the device's local network.
- A web browser must be installed.
Recommendation: Use the latest version of Google Chrome.
- The device must not be connected to the Symphony Cloud Platform.
- The required ports must be enabled ([see "Ports", page 11](#)).
- Service "Bonjour" (used for device discovery on private and public networks) must be activated.

1. Open the web browser.
 2. Enter "https://" followed by the host name and the string ".local" in the search bar.
Example: "https://ids-mx6-bc6a44000a38.local".
 3. Click on "Advanced" if there is no valid server certificate available on your system.
 4. Click on "Proceed to... (unsafe)" if there is no valid server certificate available on your system.
- ✓ The Web Interface opens.

7.1.2. LAUNCHING THE WEB INTERFACE VIA IPV6 ADDRESS

Requirements:

- Have the device's MAC address and locale information at hand.
- The device must be reachable on the network.
- The computer, smartphone or tablet device must be reachable on the device's local network.
- A web browser must be installed.
Recommendation: Use the latest version of Google Chrome.
- The device must not be connected to the Symphony Cloud Platform.
- The required ports must be enabled ([see "Ports", page 11](#)).

1. Using a MAC-to-IPv6 address converter, find the link-local IPv6 address.
 2. Open the web browser.
 3. Enter the link-local IPv6 address (from step 1 above).
Example: "https://[fe80::be6a:44ff:fe00:1dd7]/".
 4. Click on "Advanced" if there is no valid server certificate available on your system.
 5. Click on "Proceed to... (unsafe)" if there is no valid server certificate available on your system.
- ✓ The device's Web Interface is launched.

7.1.3. LAUNCHING THE WEB INTERFACE VIA IPV4 ADDRESS

Requirements:

- Have the device's MAC address and locale information at hand.
 - The device must be reachable on the network.
 - The computer, smartphone or tablet device must be reachable on the device's local network.
 - A web browser must be installed.
Recommendation: Use the latest version of Google Chrome.
 - The device must not be connected to the Symphony Cloud Platform.
 - The required ports must be enabled ([see "Ports", page 11](#)).
1. If a DHCP server is configured on the network, open DHCP Server Configuration.
 2. If a DHCP server is configured on the network, find the device's IPv4 address from its MAC address.
 3. Open the web browser.
 4. Enter the IPv4 address (from step 2 above).
 5. Click on "Advanced" if there is no valid server certificate available on your system.
 6. Click on "Proceed to... (unsafe)" if there is no valid server certificate available on the system.
- ✓ The device's Web Interface is launched.

7.2. LOGGING INTO THE WEB INTERFACE

Requirements:

- The device's Web Interface must be accessible.
- The device must not be connected to the Symphony Cloud Platform.
- Using the Web Interface requires Administrator credentials.

1. Launch the Web Interface.

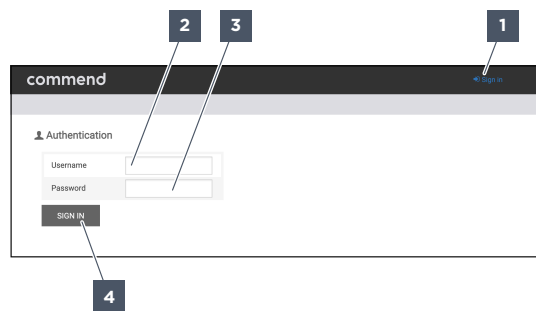


Figure 268: Accessing the web interface

- | | | |
|----------------|--------------------|-------------------|
| 1 Login | 2 User Name | 3 Password |
| 4 Login | | |

2. If the **Authentication** dialogue is not shown, click **[1] Login**.
3. Under **[2] User Name** enter “admin”.
4. Under **[3] Password** enter “commend”.
5. Click **[4] Login**.

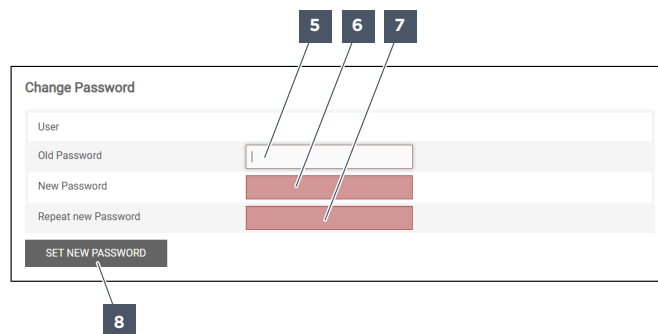


Figure 269: Changing the password

- | | | |
|-----------------------------|-----------------------|------------------------------|
| 5 Old Password | 6 New Password | 7 Retype New Password |
| 8 Apply New Password | | |

6. Under **[5] Old Password** enter “commend”.
 7. Under **[6] New Password** enter a new password ([see “JSON file for contact management”, page 218](#)).
 8. Under **[7] Retype New Password** enter the new password again.
 9. Click **[8] Apply New Password**.
- ✓ Default user “admin” is logged in.

Recommendation: Note down the password of default user “admin”. If the password is lost, the device must be reset via a USB stick. Resetting a device will delete all its data and its custom configuration settings.

8. MAINTENANCE

8.1. UPDATING VIA USB STICK

Updating a device via a USB stick will reset the device to its factory default settings. Any data and configuration settings (such as network settings) will be lost. The device software update process may take several minutes to complete. The device cannot be operated while its software is being updated. The device's Web Interface cannot be accessed while the device software is being updated. When updating a device via USB stick, the administrator credentials will be reset. To log into the Web Interface as "admin" you will have to configure the password again.

Recommendation: Create and export a backup file before updating.

Update files for the device may contain software for accessories. The accessories must not be disconnected from the device while updating the device software.

Only update files intended for the device may be used for the device. If an update file is selected that is not intended for the device, a warning message appears in the web interface. The syntax elements for naming update files are structured as follows.

Syntax elements:

- <Product ID>
- **usb_stick_update**
- <Software Version>
- zip

Example: "id5_usb_stick_update_xx_xx_xx_xxx.zip".

Recommendation: Do not load any software updates with a version lower than 02.09.01 in devices with the hardware revision "AG" or higher.

If a software update is performed from version 02.06 or lower to version 02.07.83 or higher, the authentication must be reconfigured with tokens. Password-based authentication is no longer valid. Token-based authentication meets the latest security standards.

Requirements:

- USB stick present.
 - File for USB-based update available on USB stick.
 - Free USB port on device.
 - PoE power supply available.
1. Format a USB stick with the file system FAT32.
 2. Decompress the update file on a computer.

3. Copy the folder named "update" to the USB stick.

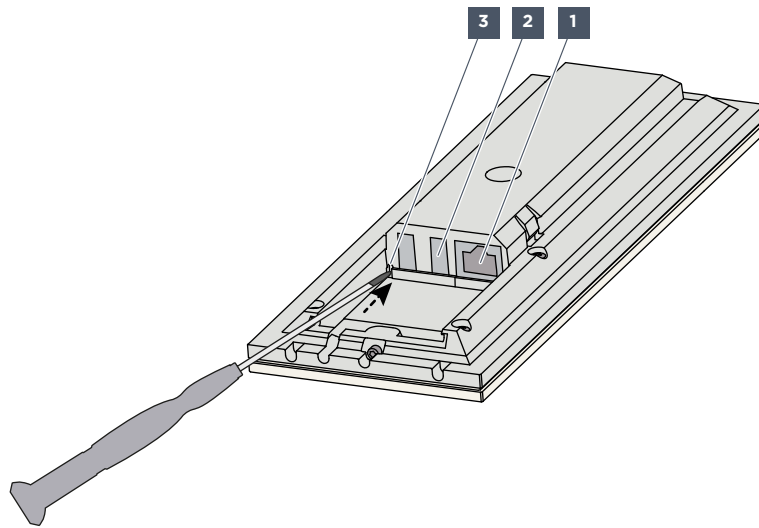


Figure 270: Updating via USB stick

1 Ethernet Cable

2 USB Port

3 Factory Reset

4. Disconnect the **[1] Ethernet cable** from the device.
5. Plug the USB stick into a free **[2] USB Port** on the device.
6. Press and hold **[3] Factory Reset**.
Example: If necessary, use a thin slotted screwdriver.
7. Reconnect the **[1] Ethernet cable** to the device.
8. Release **[3] Factory Reset** after about 20 seconds.
9. Wait for the device to boot completely. A noise signal for audio calibration and a short signal tone are played back.
10. Verify that the update has been successful.
Recommendation: Compare the software version on the **Overview** with the version of the update file.

9. APPENDIX

9.1. JSON FILE FOR CONTACT MANAGEMENT

Contacts and the directory structure for the “Contact Management” layout can be imported from a JSON file. The JSON file must be configured for importing.

Recommendation: Configure at least one contact in the web interface and export it. It will provide the structure needed for configuring the JSON file.

Existing system variables (e.g. “phone”, “additionalText” or “officeHours”) must not be translated or changed.

Recommendation: Do not set parameter “deletable” to “false”. Otherwise the entry can only be deleted by restoring the factory settings.

The IDs can be selected freely. Note, however, that they must be configured in UUID (Universally Unique Identifier) format.

Recommendation: Use an UUID generator.

If you do not want to configure an optional information item, omit the entire string to prevent a blank field from being displayed.

A JSON file consists of the following sections:

Sections:

- **contacts:** Configure the contacts.
- **nodes:** Configure directories.
- **addresses:** Configure call destinations for contacts.
- **medias:** Configure avatar images.
- **activityEvents:** Configure triggers for activities.
- **actions:** Configure actions in action sequences.
- **actionSets:** Configure action sequences that are linked to activities.
- **activityCards:** Configure activities.
- **buttons:** Configure buttons.
- **buttonsGroups:** Configure groups that have buttons assigned.
- **components:** Configure hardware components that are assigned to actions or action sequences.
- **mediaData:** Configure Base64-encoded images.

9.1.1. CONTACTS

You may configure up to 10,000 contacts without an avatar image and 5,000 contacts with an avatar image. To prevent the contact’s details from being displayed, omit all strings under “userData”.

```
"_type": "com.commend.iss.telephony.contact.Contact" 1)
"id": "<unique contact ID (UUID)>"
"deletable": true 2)
"externalId": " " 2)
"userId": null 2)
"mainText": "<first name>"
"additionalText": "<last name>"
"avatar": "<UUID of the corresponding avatar image>/null"
```

```

"videoUrl": " " 2)
"callMode": "PARALLEL" 1)
"certSubjectDN": " " 2)
"certIssuerDN": " " 2)
"userData": 1)
  "phone": "<telephone number>" 2)
  "email": "<email address>" 2)
  "address": "<street address>" 2)
  "officeHours": "<regular office hours>" 2)
  "isEmergencyContact": "false/true" 2)
  "isHelpContact": "false/true" 2)

```

1) Must not be modified or omitted.

2) Optional.

9.1.2. NODES

Up to 10 directory levels may be defined. Up to 50 sub-directories and 100 contacts may be defined per directory. The main directory requires the value of the “parent” string to be set to “null”.

```

"_type": "com.commend.iss.telephony.contact.ContactNode" 1)
"id": "<unique directory ID (UUID)>"
"deletable": true 2)
"externalId": " " 2)
"parent": "<unique ID (UUID) of the parent directory, if re-
          quired>"/null
"contacts":1)
  "<contact's UUID>",
  "<contact's UUID>",
  ...
"avatar": "<UUID of the corresponding avatar image>"/null
"nodeData": 1)
  "name": "<directory name>"
  "sortOrdner": "<sequential number>" 2)
  "mainContactId": "<contact's UUID>"

```

1) Must not be modified or omitted.

2) Optional.

9.1.3. ADDRESSES

```

"_type": "com.commend.iss.telephony.contact.Address" 1)
"id": "<unique address ID (UUID)>"
"deletable": true 2)
"externalId": " " 2)
"address": "<street address>"
"contactId": "<contact's UUID>"
"timeout": <timeout (default: 20)> 2)
"sorting": <sequential number (default: 0)> 2)

```

1) Must not be modified or omitted.

2) Optional.

9.1.4. MEDIAS

```

"_type": "com.commend.iss.media.Media" 1)
"id": "<unique avatar ID (UUID)>"
"deletable": true 2)
"externalId": " " 2)

```

```

"category": "avatars" 1)
"displayName": "<Avatar image file name>"
"mimeType": "image/jpeg" / "image/png" 1)
"lastModified": <generated automatically> 2)
"size": <generated automatically> 2)
"scaled": true 1)

```

¹⁾ Must not be modified or omitted.

²⁾ Optional.

9.1.5. ACTIVITYEVENTS

```

"_type": "com.commend.iss.device.keyboard.<activity>" 1)
"id": "<unique UUID for the activity>"
"deletable": true 2)
"externalId": "" 2)
"buttonId": "<UUID for the corresponding button>"
"state": "DOWN" 1)

```

¹⁾ Must not be modified or omitted.

²⁾ Optional.

9.1.6. ACTIONS

The parameters after "sorting" may have to be configured further, depending on the action in question.

```

"_type": "com.commend.iss.device.keyboard.<action>" 1)
"id": "<unique UUID for the action>"
"externalId": "" 2)
"deletable": true 2)
"actionSet": "<UUID for the corresponding action sequence>"
"sorting": 0 2)

```

¹⁾ Must not be modified or omitted.

²⁾ Optional.

9.1.7. ACTIONSETS

```

"_type": "com.commend.iss.device.keyboard.ActionSet" 1)
"id": "<unique UUID for the action sequence>"
"externalId": "" 2)
"deletable": true 2)
"displayName": "" 2)
"classifier": "STANDARD" / "EMERGENCY" 1)
"system": true 2)

```

¹⁾ Must not be modified or omitted.

²⁾ Optional.

9.1.8. ACTIVITYCARDS

```

"_type": "com.commend.iss.device.keyboard.ActivityCard" 1)
"id": "<unique UUID for the activity>"
"externalId": "" 2)
"deletable": true 2)

```

```
"activityEvent": "<UUID for the corresponding trigger>"
"actionSet": <UUID for the corresponding action sequence>
"telephonyState": null 1)
"system": true 2)
```

- ¹⁾ Must not be modified or omitted.
²⁾ Optional.

9.1.9. BUTTONS

```
"_type": "com.commend.iss.device.buttons.VirtualButton" 1)
"mode": false 2)
"showText": true 2)
"translationKey": null 2)
"id": "<unique UUID for the button>"
"deletable": true 2)
"externalId": "" 2)
"displayName": "NodeButton1.1" 3)
"buttonGroup": "<UUID for the corresponding button group>"
"contact": null/"<UUID for the corresponding contact>"
"wantIncVideo": true/false 2)
"offerOutVideo": true/false 2)
"wantIncAudio": true/false 2)
"offerOutAudio": true/false 2)
"sorting": 0 2)
"sortingLexical": "ddd" 3)
"classifier": "STANDARD"/"EMERGENCY" 3)
"page": 1 3)
"buttonFormat": "LARGE"/"SMALL" 3)
"additionalText": null 2)
"avatar": null/"<UUID of the corresponding avatar image>" 2)
"icon": null/"<UUID of the corresponding icon>" 2)
"symbol": null 2)
"visible": true/false 2)
```

- ¹⁾ Must not be modified or omitted.
²⁾ Optional.
³⁾ Must be adjusted, depending on the type, (sequential) number or path.

9.1.10. BUTTONGROUPS

```
"_type": "com.commend.iss.device.buttons.ButtonGroup" 1)
"id": "<unique UUID for the button group>"
"deletable": true 2)
"externalId": "" 2)
"key": "commend.layout.tree.node<UUID for the corresponding button>"/"commend.layout.tree.node"
"sortMode": "ASCENDING" 1)
"sortBy": "FIRSTNAME" 1)
"system": false 2)
```

- ¹⁾ Must not be modified or omitted.
²⁾ Optional.

9.1.11. COMPONENTS

Hardware components that are configured for triggers or actions must be configured in the JSON file.

Recommendation: To find the required numbers of the hardware components, configure the activities and action sequences in the Web Interface and export the contact management configuration.

```

"_type": "com.commend.device.config.<hardware component>" 1)
"barcode": 1)
  "_type": "com.commend.device.Barcode" 1)
  "barcodeVersion": <number>
  "serialNumber": <number>
  "materialCode": "<article code of the hardware component>" 1)
  "majorVersion": <number>
  "minorVersion": <number>
  "supplierID": <number>
  "productionWeek": <number>
  "consecutiveNumber": <number>
"nameKey": "<name of the hardware component>"
"id": "<unique UUID for the hardware component>"
"externalId": " " 2)
"deletable": true 2)
"state": "<state of the hardware component>"
"interval": null 2)

```

1) Must not be modified or omitted.

2) Optional.

9.1.12. MEDIADATA

Section “mediaData” is where Base64-coded images are saved. To associate an avatar image with a contact, the UUID must be entered under “id” in section “medias”. The required size of avatar images is 100 × 100 pixels.

9.1.13. EXAMPLE OF A JSON FILE

The following example illustrates the configuration of a contact record with avatar image.

```

{
  "version": "v1.0",
  "contacts": [
    {
      "_type": "com.commend.iss.telephony.contact.Contact",
      "id": "2be2c818-d224-4a2f-a5fc-ff8dc746507c",
      "mainText": "James",
      "additionalText": "Hill",
      "avatar": "540898e2-2107-4a23-b549-d61526a9213e",
      "videoUrl": "",
      "userData": {
        "email": "james.hill@mail.co.uk",
        "officeHours": "9 am to 5 pm",
        "isEmergencyContact": "false",
        "isHelpContact": "false"
      }
    }
  ],
  "nodes": [
    {
      "_type": "com.commend.iss.telephony.contact.ContactNode",
      "id": "e62d123d-610f-4657-a578-6999a380f2ff",
      "parent": null,
      "contacts": [

```

```
    "2be2c818-d224-4a2f-a5fc-ff8dc746507c"
  ],
  "nodeData": {
    "name": "Company ABC",
    "root": "true"
  }
},
"addresses": [
  {
    "_type": "com.commend.iss.telephony.contact.Address",
    "id": "92696629-c1d2-4724-9154-b37b8346c3a5",
    "address": "192.168.1.151",
    "contactId": "2be2c818-d224-4a2f-a5fc-ff8dc746507c",
    "timeout": 20,
    "sorting": 0
  }
],
"medias": [
  {
    "_type": "com.commend.iss.media.Media",
    "id": "540898e2-2107-4a23-b549-d61526a9213e",
    "category": "avatars",
    "displayName": "jameshill.jpg",
    "mimeType": "image/jpeg",
    "scaled": true
  }
],
"mediaData": [
  {
    "540898e2-2107-4a23-b549-d61526a9213e": "<Base64-coded image>"
  }
]
}
```

9.2. ID5 DKGM OR ID5 DKHSGM

An ID5 DKGM or ID5 DKHSGM can be connected to the device. To enable Push-to-Talk calls, the device and remote station must be configured accordingly.

After connecting an ID5 DKGM or ID5 DKHSGM to the device, it must be rebooted. Note that the ID5 DKGM and the ID5 DKHSGM are not hot-pluggable.

To enable calls between two Intercom stations, only one of them may be connected either to an ID5 DKGM or an ID5 DKHSGM.

Overview

Master Device	Connection	Remote Station	PPT Support	Remarks and Limitations
Device with ID5 DKGM or ID5 DKHSGM	Peer-to-Peer	Symphony MX Device	Yes	Push-to-Talk is supported for Simplex-like calls. Talk/listen visualisation is supported on both devices. Symphony MX devices require further configuration.
Device with ID5 DKGM or ID5 DKHSGM	Peer-to-Peer	Symphony BF Device	Yes	Push-to-Talk is supported for Simplex-like calls. Talk/listen visualisation is not supported on the Symphony BF device.
Device with ID5 DKGM or ID5 DKHSGM	VirtuoSIS	Symphony MX Device	Yes	Push-to-Talk is supported for Simplex-like calls. Talk/listen visualisation is supported on both devices. Symphony MX devices and VirtuoSIS require further configuration.
Device with ID5 DKGM or ID5 DKHSGM	VirtuoSIS	Symphony BF Device	Yes	Push-to-Talk is supported for Simplex-like calls. Talk/listen visualisation is not supported on the Symphony BF device. VirtuoSIS requires additional configuration (Door Opener). On Symphony BF devices, the configured DTMF tones must not be used for other functions (such as conferences).
Device with ID5 DKGM or ID5 DKHSGM	VirtuoSIS	VoIP Device	Yes	Push-to-Talk is supported for Simplex-like calls. Talk/listen visualisation is not supported on the VoIP device. VirtuoSIS requires additional configuration (Door Opener). On VoIP devices, the configured DTMF tones must not be used for other functions (such as conferences).
Device with ID5 DKGM or ID5 DKHSGM	VirtuoSIS	Mix of different device types (Symphony MX, Symphony BF, VoIP)	Yes	Push-to-Talk is supported for Simplex-like calls. Talk/listen visualisation is only possible with Symphony MX devices. VirtuoSIS requires additional configuration (Door Opener). On VoIP and Symphony BF devices, the configured DTMF tones must not be used for other functions (such as conferences).

Table 4: Overview

Master Device	Connection	Remote Station	PPT Support	Remarks and Limitations
Device with ID5 DKGM or ID5 DKHSGM	Symphony Cloud Platform	Symphony MX Device	No	Push-to-Talk is currently not supported for Simplex-like calls.

Table 4: Overview

9.2.1. CONFIGURING AUDIO DEVICES

Requirements:

- ID5 DKGM or ID5 DKHSGM connected to the device.
- “Audio” rights held by the current user.

1. Navigate to **Device > Audio**.

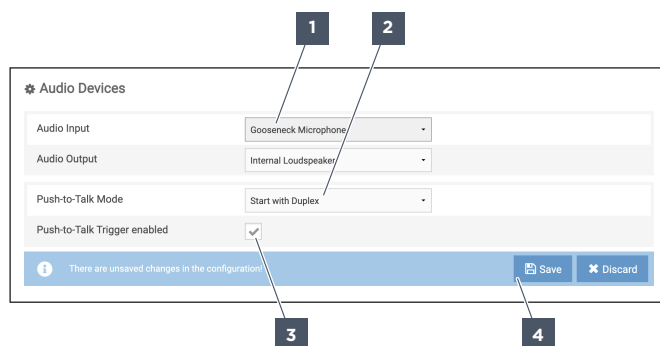


Figure 271: ID5 DKGM or ID5 DKHSGM – Configure Audio Devices

- 1** Audio Input
- 2** Push-to-Talk Mode
- 3** Push-to-Talk Trigger enabled
- 4** Save

2. Under **[1] Audio Input** enable option “Gooseneck microphone”.
 3. Under **[2] Push-to-Talk Mode** select the desired call behaviour.
 4. Ensure that **[3] Push-to-Talk Trigger activated** is enabled.
 5. Click **[4] Save**.
- ✓ The gooseneck microphone of the ID5 DKGM or ID5 DKHSGM will be used.

9.2.2. ENABLING DISPLAY OF THE “PUSH-TO-TALK” PICTOGRAM

Requirements:

- ID5 DKGM or ID5 DKHSGM connected to the device or a remote station.
- “Device” rights held by the current user.

1. Navigate to **Device > Device**.

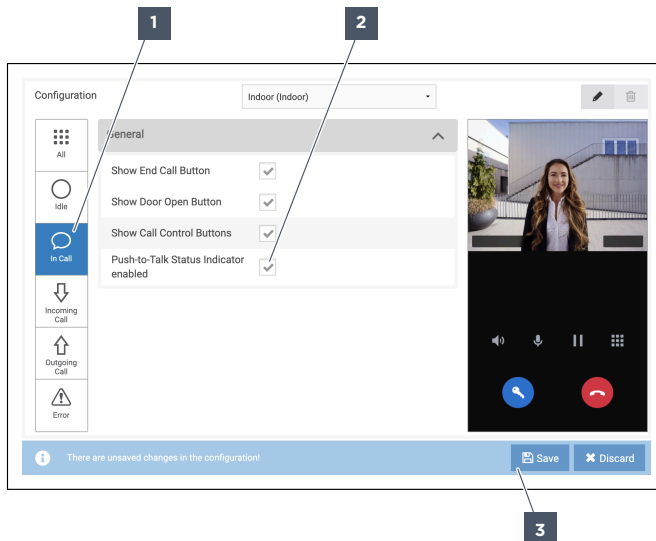


Figure 272: ID5 DKGM or ID5 DKHSGM - Activate the "Push-to-Talk" Pictogram

- 1 In Call
- 2 Push-to-Talk Status Indicator enabled
- 3 Save

2. Navigate to **[1] In Call** on the sidebar menu on the left.
 3. Enable **[2] Push-to-Talk status display enabled**.
 4. Click **[3] Save**.
- ✓ In ongoing calls, pictogram "Push-to-Talk" indicates which party is currently set to talk.

9.2.3. CONFIGURING "IN CALL" FOR PUSH-TO-TALK CALLS

Requirements:

- ID5 DKGM or ID5 DKHSGM connected to a remote station.
- "Action Sequences" rights held by the current user.
- "Device" rights held by the current user.

1. Navigate to **Device > Device**.

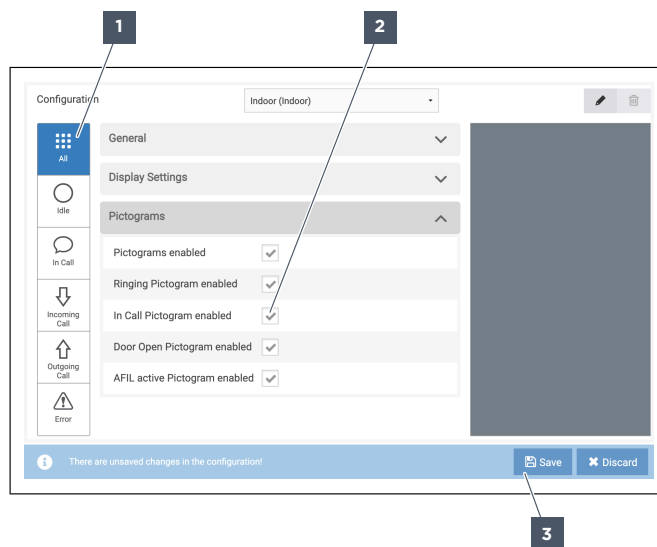


Figure 273: ID5 DKGM or ID5 DKHSGM – Activate the “In Conversation” Pictogram

- 1 All
- 2 In Call Pictogram enabled
- 3 Save

2. Navigate to **[1] All** on the sidebar menu on the left.
3. Activate **[2] In Call Pictogram enabled**.
4. Click **[3] Save**.
5. Navigate to **Activity > Actionbook** on the sidebar menu on the left.



Figure 274: ID5 DKGM or ID5 DKHSGM – Edit Action Sequence

- 4 Edit

6. Click **[4] Edit**.

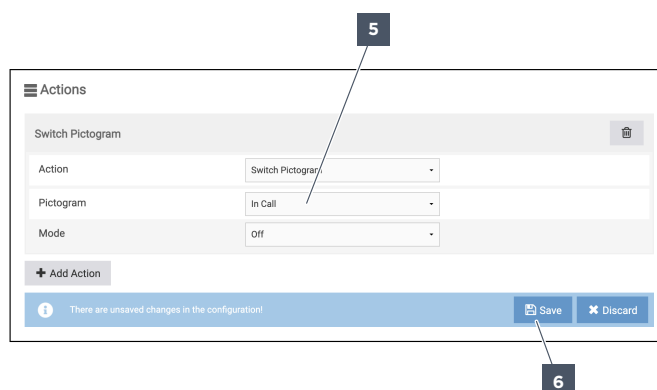


Figure 275: ID5 DKGM or ID5 DKHSGM – Edit Action Sequence

- 5 Pictogram
- 6 Save

7. Under **[5] Pictogram** enable option “In Call”.
8. Click **[6] Save**.

- Navigate to **Activity > Activities**.



Figure 276: ID5 DKGM or ID5 DKHSGM - Edit Action Sequence

7 Edit

- Click **[7] Edit**.

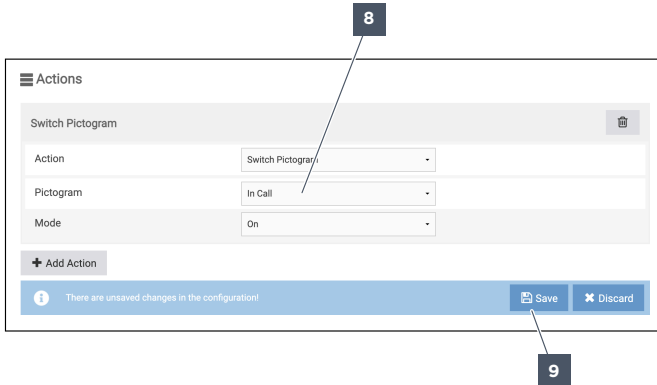


Figure 277: ID5 DKGM or ID5 DKHSGM - Edit Action Sequence

8 Pictogram

9 Save

- Under **[8] Pictogram** enable option “In Call”.

- Click **[9] Save**.

✓ In Push-to-Talk calls, pictogram “In Call” will be shown instead of pictogram “Push-to-Talk” for Talk/Listen Visualisation.

In Talk/Listen Visualisation, pictograms “Push-to-Talk” and “In Call” can also be displayed simultaneously.

9.2.4. CONFIGURING DTMF TONES FOR PUSH-TO-TALK CALLS IN VIRTUOSIS

DTMF tones for the Push-to-Talk function can be configured as needed. DTMF tone “1” is reserved for the door opener function. DTMF tones “4” to “9” require action sequences to be configured in Virtuosis to prevent interpretation problems. The same DTMF tones must be configured for the device and Virtuosis. In the following, DTMF tone “8” is configured for “Push-to-Talk Button pressed”, and DTMF tone “9” is configured for “Push-to-Talk Button released”.

Push-to-Talk calls can be conducted with SIP-C subscribers and loIP subscribers. Sending and receiving DTMF tones for Talk/Listen Visualisation is only supported by Symphony MX devices.

On loIP devices, the configured DTMF tones must not be used for other functions (such as conferences).

The Push-to-Talk Button of an ID5 DKGM or ID5 DKHSGM can be used for various actions. The Push-to-Talk Button of an ID5 DKGM or ID5 DKHSGM does not have the same function as the T Button on loIP devices.

Example: On an ID5 DKGM or ID5 DKHSGM, the Push-to-Talk Button cannot be used to initiate a 6T conference or 7T conference.

If DTMF tones “8” and “9” on an IoT subscriber are configured for the door opener function, these subscribers can no longer use the conference function.

Requirements:

- ID5 DKGM or ID5 DKHSGM connected to the device.
- Device fully configured.
- VirtuoSIS ready and licensed.
- Subscriber configured in VirtuoSIS.
- CCT 800 installed.
- Two free action sequence instances available for the subscriber.

1. Open CCT 800.
2. Download the VirtuoSIS configuration (see also manual “**Intercom Server Configuration**”).
3. Navigate to **Subscriber > Device Properties > SIP Terminals > Action Sequences**.

Liz	IS-T	Rufnummer	Bezeichnung	Aktionssequenz 1	Aktionssequenz 2	Aktiv
1/1-1	SIS-SPC-8 (i)	101	Station 101	BA01	BA02	<input type="checkbox"/>
1/1-2	SIS-SPC-8 (i)	102	Station 102			<input type="checkbox"/>
1/1-3	SIS-SPC-8 (i)	103	Station 103			<input type="checkbox"/>
1/1-4	SIS-SPC-8 (i)	104	Station 104			<input type="checkbox"/>
1/1-5	SIS-SPC-8 (i)	105	Station 105			<input type="checkbox"/>

Figure 278: ID5 DKGM or ID5 DKHSGM – Configure VirtuoSIS

- 1 Action Sequence 1
- 2 Call number OUT 1
- 3 DTMF-Sequence 1
- 4 Action Sequence 2
- 5 Call number OUT 2
- 6 DTMF-Sequence 2

4. Activate **[1] Action Sequence 1**.
5. Under **[2] Call Number OUT 1** enter a call number for this output. This step is optional. You can also use the pre-set default call number.
6. Under **[3] DTMF Sequence 1** specify the DTMF tone for “Push-to-Talk Button pressed”.
Example: “8”.
7. Activate **Enable [4] Action Sequence 2**.
8. Under **[5] Call Number OUT 2** enter a call number for this output. This step is optional. You can also use the pre-set default call number.
9. Under **[6] DTMF Sequence 2** specify the DTMF tone for “Push-to-Talk Button released”.
Example: “9”.
10. Navigate to **Outputs > General Settings**.

Output	Subscriber	Call number	Parallel call number	Description	Display text	Display text
1/0-4	SIS-GSP			OUT 1-0/54	OT:10/54	OUT 1-0/54
1/0-5	SIS-GSP			OUT 1-0/55	OF:10/55	OUT 1-0/55
1/1-1	SIS-SPC-8 (E-01)	Station 101 (101) -> SIP -> OUT1	BA01	Dummy Output for DTMF tone 8	OF:10/52	OUT 1-0/52
1/1-1	SIS-SPC-8 (E-02)	Station 101 (101) -> SIP -> OUT2	BA02	Dummy Output for DTMF tone 9	OF:10/53	OUT 1-0/53

Figure 279: ID5 DKGM or ID5 DKHSGM – Configure VirtuoSIS

- 7 Description
- 8 Description

11. Under **[7] Label** enter an action sequence label to be used for DTMF tone “8”.
Example: “Dummy Output for DTMF Tone 8”.
12. Under **[8] Label** enter an action sequence label to be used for DTMF tone “9”.
Example: “Dummy Output for DTMF Tone 9”.

13. Navigate to **Subscriber > Door Opener > Open Door.**

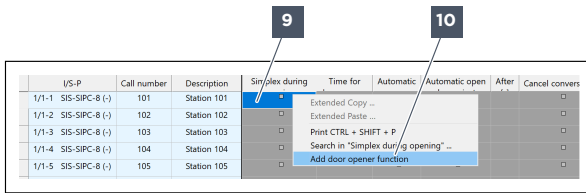


Figure 280: ID5 DKGM or ID5 DKHSGM – Configure VirtuoSIS

- 9 Subscriber
- 10 Add door opener function

14. Right-click the [9] Subscriber.
15. Click [10] Add Door Opener function.
16. Navigate to **Subscriber > Door Opener > # Subscriber.**

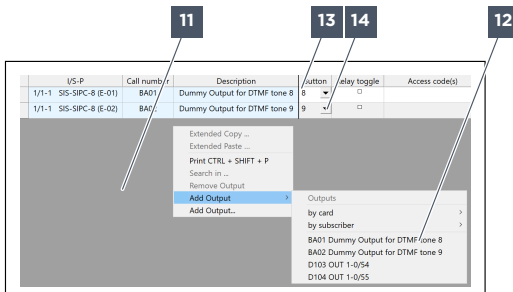


Figure 281: ID5 DKGM or ID5 DKHSGM – Configure VirtuoSIS

- 11 Gray area
- 12 Output
- 13 Button
- 14 Button

17. Right-click anywhere within the [11] grey window background area.
 18. Navigate to **Add Output.**
 19. Click the [12] Output for DTMF tone “8”.
 20. Under [13] Button select option “8”.
 21. Right-click anywhere within the [11] grey window background area.
 22. Navigate to **Add Output.**
 23. Click the [12] Output for DTMF tone “9”.
 24. Under [14] Button select option “9”.
 25. Repeat steps “3.” to “24.” for all subscribers to which DTMF tones “8” and “9” may be sent.
 26. Upload the configuration to VirtuoSIS.
- ✓ DTMF tone “8” for “Push-to-Talk Button pressed” and “9” for “Push-to-Talk Button released” are now interpreted correctly by VirtuoSIS.

9.3. EB3E2A-AUD

An EB322A-AUD can be connected to the device.

The connection “Headset” of the EB3E2A-AUD can be used from hardware revision “AC”.

If a handset is connected to the EB3E2A-AUD and the operating mode “Handset” is configured, calls can be controlled via the handset as described below.

Call control:

- If the handset is lifted during calls, the audio signals are automatically transmitted via the handset.
- Incoming calls can be answered by lifting the handset.
- Calls can be ended by replacing the handset.

Audio functions can be used with the EB3E2A-AUD. The limitations described below must be considered.

Limitations:

- Beamforming cannot be used.
- Multi-Channel Post Filter (MCPF) cannot be used.
- If the operation mode is “Line-in/Line-out” or “Gooseneck Microphone” and the extended audio routing is “Provide any Device Audio to Line Out”, the following functions cannot be used ([see “Audio Devices with EB3E2A-AUD”, page 121](#)):
 - Loudspeaker/microphone surveillance
- If the extended audio routing is “Feed Line In to Audio Output in Idle”, the following functions cannot be used ([see “Audio Devices with EB3E2A-AUD”, page 121](#)):
 - Loudspeaker/microphone surveillance
 - Audio monitoring function
 - Sound pressure level measurement

The absolute values of the audio monitoring function and the sound pressure level measurement can only be determined through the built-in microphone and the built-in loudspeaker.

9.4. REMOTE CONTROLLING A DEVICE VIA HTTP REQUESTS

The device can be remote controlled via HTTP requests that are sent by other devices. The device can remote control other devices by sending them HTTP requests. HTTP requests are sent in the form of URLs. This way, it is possible to trigger certain functions, run action sequences or change configuration settings. Users need only “HTTP” rights to use this function.

Options:

- The device is remote controlled either via a web browser or via another device.
- The device remote controls another device. The other device must be capable of interpreting HTTP requests.

To control one another via HTTP requests, the devices have to be on the same network and available. The IP address is required to remote control the device or another devices.

The interpretation of HTTP request is case sensitive. It is important to use the correct case of characters in the request.

HTTP requests for configuration changes include a user’s credentials (name and password).

The system supports both HTTP requests and HTTPS requests.

9.4.1. PARAMETERS

Available URL items:

- **volume (https://<token key>:<token value>@<IP address>/api/http/<HTTP request suffix>?volume=<value>):** Remote control the device's volume setting.
Example: "https://admin:mETNustl8GFQ4ONNEVOttZ2rv0Y4xE1Y@192.168.1.150/api/http/change?volume=1".
 - **<value>:** Adjust the volume setting. Value range: "0" to "12".

The syntax elements for HTTP Request URLs are as follows:

Syntax elements:

- **https://:** Identifies the URL protocol as "HyperText Transfer Protocol Secure" (HTTPS).
- **<token key>:** The user's individual token key.
- **<token value>:** The user's individual token value.
- **<IP address>:** The device's IP address.
- **/api/http/:** Identification as HTTP interface.
- **<HTTP request suffix>:** The individual suffix for the request sequence.
Example: "change".
- **<value>:** The value to be set.
Example: "10".

Example: "https:// <token key>:<token value>/api/http/<HTTP request suffix>?volume=<value>".

9.4.2. CONFIGURING DEVICE REMOTE CONTROL

Requirements:

- "Activity" rights held by the current user.
- "Action sequence" rights held by the current user.
- "HTTP" rights held by the current user.
- Audio file uploaded to the device.

1. Navigate to **Activity > Activity**.

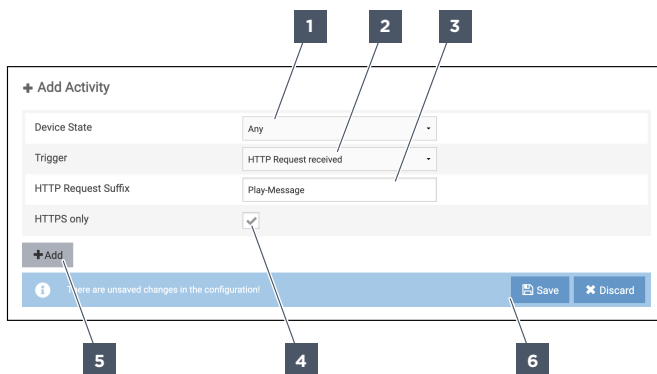


Figure 282: Configuring device remote control – Adding an activity

- | | | |
|----------------|-----------|-----------------------|
| 1 Device State | 2 Trigger | 3 HTTP Request Suffix |
| 4 HTTPS Only | 5 Add | 6 Save |

2. Under [1] **Device State** select "All".
3. Under [2] **Trigger** select "HTTP Request received".
4. Under [3] **HTTP Request Suffix** enter the appropriate suffix. You need to specify only the suffix. The previous parts (such as the prefix and IP address) are only required when entering the URL in

a web browser or on another device.

Example: “Play Message”.

5. Activate **[4] HTTPS Only** if the action sequence will be triggered exclusively via HTTP requests.
6. Click **[5] Add**.
7. Click **[6] Save**.

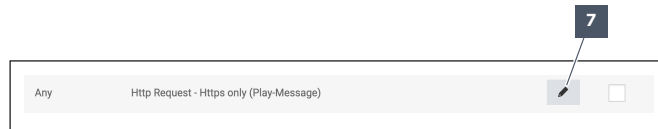


Figure 283: Configuring device remote control - Editing an activity

7 Edit

8. Click **[7] Edit**.



Figure 284: Configuring device remote control - Adding an action sequence

8 Add Action Sequence

9. Click **[8] Add Action Sequence**.

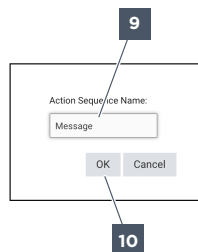


Figure 285: Configuring device remote control - Naming an action sequence

9 Action Sequence label **10** OK

10. Under **[9] Action Sequence Label** enter a name for the action sequence.
Example: “Message”.
11. Click **[10] OK**.

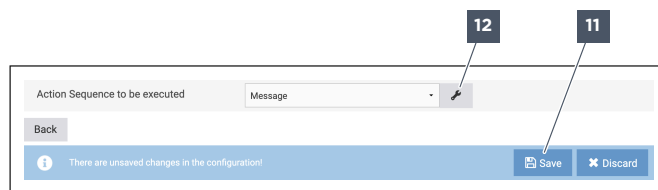


Figure 286: Configuring device remote control - Editing an action sequence

11 Save **12** Edit

12. Click **[11] Save**.

13. Click [12] Edit.

Figure 287: Configuring device remote control - Editing an action sequence

- | | | |
|-------------|-----------------|------------------------|
| [13] Action | [14] Media File | [15] Play During Calls |
| [16] Save | | |

14. Under [13] **Action** Select option “Play Audio File”.
15. Under [14] **Media File** select the audio file to be played.
16. Activate [15] **Play During Calls** to allow the audio file to be played back during calls.
17. Click [16] **Save**.

✓ The audio file will be played when the URL is entered and submitted via a web browser or another device.

Example: “https://admin:mETNustI8GFQ4ONNEVOttZ2rv0Y4- xE1Y@192.168.1.150/api/http/Play-Mes-
sage” is submitted via a web browser.

9.5. SNMP FOR SYMPHONY MX

["SNMP for Symphony MX.pdf"](#)

SNMP for Symphony MX

General

Name	OID	Element type	Description	Possible values
commendStationCommonStationType	1.3.6.1.4.1.37568.2.1.1.1	Octet string	Device type	Commend Symphony MX
commendStationCommonStationSubType	1.3.6.1.4.1.37568.2.1.1.2	Octet string	Device subtype	WS 301V CM WS 303V CM WS 311V CM WS 311V CM DA ID5 TD CM ID5 TD OD10 TD CM OD5 TD CM OD5 TD IM6
commendStationCommonStationSoftwareVersion	1.3.6.1.4.1.37568.2.1.1.3	Octet string	Software version	e.g. "02.09.00.80"
commendStationCommonStationLocation	1.3.6.1.4.1.37568.2.1.1.12	Octet string	Location name	e.g. "Kitchen"
commendStationCommonStationSystemState	1.3.6.1.4.1.37568.2.1.1.20	Octet string	Device state (as shown in the web interface)	"Telephony State Change: <STATE>" STATE = { INITIALIZING, IDLE, ACTIVE, RINGING, DIALLING, ERROR } INITIALIZING = startup IDLE = device is ready, no calls ACTIVE = device is in call RINGING = incoming call DIALLING = outgoing call ERROR = state "Error"
commendStationConnectivitySipAccountTable	1.3.6.1.4.1.37568.2.1.2.5.40	Sequence "AccountTableEntry"	SIP accounts	accountTableEntry = { accountNumber, accountDisplayName, accountUserId, accountServer, accountState } accountNumber = UUID of the account accountDisplayName = display name, e.g. "Fam. Williams" accountUserId = SIP server user name accountServer = SIP server address accountState = SIP registration state: STATE = { UNKNOWN, REGISTERING, REGISTERED, UNREGISTERING, UNREGISTERED, INACTIVE, CONNECTING, REACHABLE, CONNECTION_FAILED, AUTHENTICATION_FAILED, ERROR }
commendStationAudioLsMicStatus	1.3.6.1.4.1.37568.2.1.3.4.1	Octet string	Loudspeaker-microphone surveillance state	STATE = { UNKNOWN, SUCCESSFUL, FAILED }

commendStationInputTable	1.3.6.1.4.1.37568.2 .1.4.20	Sequence "InputTableEntry"	Input states	<p>InputTableEntry = { inputName, inputState }</p> <p>ID5 TD, ID5 TD CM:</p> <p>Indoor Station-<Serial>-ambient.light.infrared = for internal use only Indoor Station-<Serial>-ambient.light.visible = for internal use only</p> <p>WS 301V CM, WS 303V CM, WS 311V CM, WS 311V CM DA: WS <300V or model> CM-<Serial>-ambient.light.infrared = for internal use only WS <300V or model> CM-<Serial>-ambient.light.visible = for internal use only WS <300V or model> CM-<Serial>-sabotInput = Open: tampering detected, Short: no tampering detected WS <300V or model> CM-<Serial>-saboError = Open: no error, Short: error detected</p> <p>OD10 TD CM: OD10-<Serial>-ambient.light.infrared = for internal use only OD10-<Serial>-ambient.light.visible = for internal use only OD10-<Serial>-input1 = see "multistate input" OD10-<Serial>-input2 = see "multistate input" OD10-<Serial>-input3 = see "multistate input" OD10-<Serial>-sabotInput = Open: tampering detected, Short: no tampering detected OD10-<Serial>-saboError = Open: no error, Short: error detected</p> <p>OD5 TD CM: OD5-<Serial>-ambient.light.infrared = for internal use only OD5-<Serial>-ambient.light.visible = for internal use only</p> <p>IM6: IM6-<Serial>-input1 = see "multistate input" IM6-<Serial>-input2 = see "multistate input" IM6-<Serial>-input3 = see "multistate input" IM6-<Serial>-mic1Detection = see "microphone detection" IM6-<Serial>-mic2Detection = see "microphone detection"</p> <p>EB3E2A: EB3E2A-AUD-<Serial>-input1 = see "multistate input" EB3E2A-AUD-<Serial>-input2 = see "multistate input" EB3E2A-AUD-<Serial>-input3 = see "multistate input"</p> <p>EB1A: none</p> <p>EB1E1A: EB1E1A-<Serial>-input1 = see "4-state input"</p> <p>IP Secure Connector: IP CON-<Serial>-input1 IP CON-<Serial>-input2</p>
commendStationOutputTable	1.3.6.1.4.1.37568.2 .1.5.20	Sequence "OutputTableEntry"	Output states	<p>OutputTableEntry = { outputName, outputState }</p> <p>WS 301V CM, WS 303V CM, WS 311V CM, WS 311V CM DA: none</p> <p>OD10 TD CM: OD10-<Serial>-output1 = see "digital output" OD10-<Serial>-output2 = see "digital output"</p> <p>OD5 TD CM: none</p> <p>IM6: IM6-<Serial>-output1 = see "digital output" IM6-<Serial>-output2 = see "digital output"</p> <p>EB3E2A: EB3E2A-AUD-<Serial>-output1 = see "digital output" EB3E2A-AUD-<Serial>-output2 = see "digital output"</p> <p>EB1A: EB1A-<Serial>-output1 = see "digital output"</p> <p>EB1E1A: EB1E1A-<Serial>-output1 = see "digital output"</p> <p>IP Secure Connector: IP CON-<Serial>-output1 = see "digital output" IP CON-<Serial>-output2 = see "digital output" IP CON-<Serial>-output3 = see "digital output"</p>

Digital input

States: Short, Open

Multistate input

States: Short, R560, R1K, R1K5, R2K2, R2K7, R3K3, R4K7, R6K8, R8K2, R10K, R15K, R22K, R33K, R56K, Open

4-state input

States: Short, R3K3, R15K, Open

Microphone detection

States: NoMic, Mic, Line

Digital output

States: On (physical output is active, also if blinking or in sequence), Off (physical output is inactive, also if blinking or in sequence)

Traps

Variable binding 1: Every trap is sent with the variable binding 1 heading "sysUpTime" ("iso.org.dod.internet.mgmt.mib-2.system.sysUpTime").

Trap name	Variable binding 2		Variable binding 3	
	Name	Value	Name	Value
Application Start	snmpTrap OID 1.3.6.1.6.3. 1.1.4.1	commendStationObjectStatusNoti fications 1.3.6.1.4.1.37568.2.10	commendStationApplicationS tart 1.3.6.1.4.1.37568.2.20	
Cold Start	snmpTrap OID 1.3.6.1.6.3. 1.1.4.1	ColdStart 1.3.6.1.6.3.1.1.5.1		
Warm Start	snmpTrap OID 1.3.6.1.6.3. 1.1.4.1	WarmStart 1.3.6.1.6.3.1.1.5.2		
NTP State	snmpTrap OID 1.3.6.1.6.3. 1.1.4.1	commendStationCommonStation NtpNotification 1.3.6.1.4.1.37568.2.1.1.26	commendStationCommonSta tionNtpState 1.3.6.1.4.1.37568.2.1.1.25	"NTP synchronization successful" "NTP synchronization failed"
LS/MIC Monitoring	IsMicMonit oring	commendStationAudioLsMicSurv eillanceNotification 1.3.6.1.4.1.37568.2.1.3.11	commendStationAudioLsMic Status 1.3.6.1.4.1.37568.2.1.3.4.1	"Loudspeaker/Microphone Surveillance detection <STATE>" STATE = { UNKNOWN, SUCCESSFUL, FAILED }
Audio Monitoring	audioMonit oring	commendStationAudioMonitoring AlarmNotification 1.3.6.1.4.1.37568.2.1.3.12	commendStationAudiomonit oringStatus 1.3.6.1.4.1.37568.2.1.3.5.1.0	"Audio Monitoring triggered"
Input Change	snmpTrap OID 1.3.6.1.6.3. 1.1.4.1	commendStationInputChangedNo tification 1.3.6.1.4.1.37568.2.1.4.9.3	commendStationLastInputCh ange 1.3.6.1.4.1.37568.2.1.5.1.0	"<MODEL>-<SERIAL>-<INPUT_ID>, State: <STATE>" e.g. "EB1E1A-123109-input1, state: Short" For various models and input IDs, see "commendStationInputTable" in the table "General".
Output Change	snmpTrap OID 1.3.6.1.6.3. 1.1.4.1	commendStationOutputChanged Notification 1.3.6.1.4.1.37568.2.1.5.9.1	commendStationLastOutputC hange 1.3.6.1.4.1.37568.2.1.7.1.0	"<OUTPUT_ID> on <MODEL>-<SERIAL>, State: <MODE>" MODE = { ON, OFF, TOOGLE, FLASHING, ON_OFF_SEQUENCE } e.g. "output1 on EB1E1A-123109, State: TOGGLE"

Registration State (SIP account state change)	snmpTrap OID 1.3.6.1.6.3.1.1.4.1	commendStationObjectStatusNoti fications 1.3.6.1.4.1.37568.2.10	commendStationConnectivity SipAccount 1.3.6.1.4.1.37568.2.1.2.5.5	<p>"Account State changed, <STATE>, Account ID: <ACCOUNT_ID>"</p> <p>STATE = { UNKOWN, REGISTERING, REGISTERED, UNREGISTERING, UNREGISTERED, INACTIVE, CONNECTING, REACHABLE, CONNECTION_FAILED, AUTHENTICATION_FAILED, ERROR }</p> <p>See manual for state descriptions</p> <p>e.g. "Account State changed, REGISTERING, Account ID: 8d806dd0-5cab-4bfb-ab4a-6eb87ac9cef8"</p>
Conversation State (call state change)	snmpTrap OID 1.3.6.1.6.3.1.1.4.1	commendStationObjectStatusNoti fications 1.3.6.1.4.1.37568.2.10	commendStationCommonSta tionCallState 1.3.6.1.4.1.37568.2.1.1.80	<p>"Peer State Change, Direction: <DIRECTION>, Address: <ADDRESS>, State: <STATE>"</p> <p>DIRECTION = { INCOMING, OUTGOING }</p> <p>ADDRESS = "<HOST>" or "<USERID>@<HOST>"</p> <p>STATE = { NONE, DIALLING, IN_PROGRESS, FINISHED, BUSY, CANCEL, RINGING, EARLY_MEDIA, FORBIDDEN, TIMEOUT, ON_HOLD, DECLINED }</p>
Device State	snmpTrap OID 1.3.6.1.6.3.1.1.4.1	commendStationObjectStatusNoti fications 1.3.6.1.4.1.37568.2.10	commendStationCommonSta tionSystemState 1.3.6.1.4.1.37568.2.1.1.20	<p>"Telephony State Change: <STATE>"</p> <p>STATE = { Initializing, Idle, In Call, Incoming Call, Outgoing Call, Error }</p> <p>e.g. "Telephony State Change: Idle"</p>
Live Sound Pressure Level (SPL change)	snmpTrap OID 1.3.6.1.6.3.1.1.4.1	commendStationObjectStatusNoti fications 1.3.6.1.4.1.37568.2.10	Audio SplMeasurement 1.3.6.1.4.1.37568.2.1.3.5.1.0. 5.3.6.3	<p>"SplMeasurement [<SPL>]"</p> <p>SPL = sound pressure level (dB)</p>

9.6. LICENCING NOTES

The following licences require an additional notice in the documentation:

9.6.1. XFREE86-1.1

This product includes software developed by The XFree86 Project, Inc (<http://www.xfree86.org/>) and its contributors.

9.6.2. ORIGINAL SSLEAY

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

9.6.3. OPENSLL

9.6.4. LGPL-3.0+

This product includes a library "ffmpeg-3.4.2" under the Lesser GNU Public License Version 3.

This product includes a library "libeigen-3.3.5" under the Lesser GNU Public License Version 3.

This product includes a library "python3-3.5.5" under the Lesser GNU Public License Version 3.

This product includes a library "dfu-util-0.9" under the Lesser GNU Public License Version 3.

This product includes a library "util-linux-2.32.1" under the Lesser GNU Public License Version 3.

9.6.5. LGPL-3.0

9.6.6. LGPL-2.1+-WITH-GCC-EXCEPTION

This product includes a library "flac-1.3.2" under the Lesser GNU Public License Version 2.1+.

This product includes a library "ffmpeg-3.4.2" under the Lesser GNU Public License Version 2.1+.

This product includes a library "gstreamer1.0-1.14.4.imx" under the Lesser GNU Public License Version 2.1+.

This product includes a library "gstreamer1.0-plugins-good-1.14.4.imx" under the Lesser GNU Public License Version 2.1+.

This product includes a library "libgudev-232" under the Lesser GNU Public License Version 2.1+.

This product includes a library "boost-1.66.0" under the Lesser GNU Public License Version 2.1+.

This product includes a library "atkmm-2.24.2" under the Lesser GNU Public License Version 2.1+.

This product includes a library "barebox-1.0" under the Lesser GNU Public License Version 2.1+.

This product includes a library "iso-codes-3.75" under the Lesser GNU Public License Version 2.1+.

This product includes a library "acl-2.2.52" under the Lesser GNU Public License Version 2.1+.

This product includes a library "alsa-lib-1.1.5" under the Lesser GNU Public License Version 2.1+.

This product includes a library "attr-2.4.47" under the Lesser GNU Public License Version 2.1+.

This product includes a library "glibc-2.26" under the Lesser GNU Public License Version 2.1+.

This product includes a library "gnome-themes-standard-3.22.3" under the Lesser GNU Public License Version 2.1+.

This product includes a library "libcgroup-0.41" under the Lesser GNU Public License Version 2.1+.

This product includes a library "chromium-52.0.2743.76" under the Lesser GNU Public License Version 2.1+.

This product includes a library "glib-2.0-1_2.52.3" under the Lesser GNU Public License Version 2.1+.

This product includes a library "glibmm-2.54.1" under the Lesser GNU Public License Version 2.1+.

This product includes a library "busybox-1.27.2" under the Lesser GNU Public License Version 2.1+.

This product includes a library "cairo-1.14.12" under the Lesser GNU Public License Version 2.1+.

This product includes a library "dbus-1.12.16" under the Lesser GNU Public License Version 2.1+.

This product includes a library "dbus-glib-0.108" under the Lesser GNU Public License Version 2.1+.

This product includes a library "dietlibc-cross-0.33" under the Lesser GNU Public License Version 2.1+.

This product includes a library "curl-7.54.1" under the Lesser GNU Public License Version 2.1+.

This product includes a library "gdk-pixbuf-2.36.8" under the Lesser GNU Public License Version 2.1+.

This product includes a library "gstreamer1.0-plugins-bad-1.14.4.imx" under the Lesser GNU Public License Version 2.1+.

This product includes a library "gobject-introspection-1.54.1" under the Lesser GNU Public License Version 2.1+.

This product includes a library "gststreamer1.0-plugins-base-1.14.4.imx" under the Lesser GNU Public License Version 2.1+.

This product includes a library "libgpg-error-1.27" under the Lesser GNU Public License Version 2.1+.

This product includes a library "gtk+3-3.22.17" under the Lesser GNU Public License Version 2.1+.

This product includes a library "gtk+-2.24.31" under the Lesser GNU Public License Version 2.1+.

This product includes a library "gtkmm-2.24.5" under the Lesser GNU Public License Version 2.1+.

This product includes a library "imx-lib-1_7.1.2" under the Lesser GNU Public License Version 2.1+.

This product includes a library "imx-gst1.0-plugin-4.4.5" under the Lesser GNU Public License Version 2.1+.

This product includes a library "kbd-2.0.4" under the Lesser GNU Public License Version 2.1+.

This product includes a library "kmod-25+gitAUTOINC+aca4eca103" under the Lesser GNU Public License Version 2.1+. This product includes a library "libconfig-1.5-r2.zip" under the Lesser GNU Public License Version 2.1+.

This product includes a library "libimxvpuapi-0.10.3" under the Lesser GNU Public License Version 2.1+.

This product includes a library "libexif-0.6.21" under the Lesser GNU Public License Version 2.1+.

This product includes a library "libndp-1.6" under the Lesser GNU Public License Version 2.1+.

This product includes a library "libdaemon-0.14" under the Lesser GNU Public License Version 2.1+.

This product includes a library "libcroco-0.6.12" under the Lesser GNU Public License Version 2.1+.

This product includes a library "libdbus-c++-0.9.0" under the Lesser GNU Public License Version 2.1+.

This product includes a library "libeigen-3.3.5" under the Lesser GNU Public License Version 2.1+.

This product includes a library "libgphoto2-2.5.8" under the Lesser GNU Public License Version 2.1+.

This product includes a library "libnl-1_3.2.29" under the Lesser GNU Public License Version 2.1+.

This product includes a library "libsndfile-1.0.28" under the Lesser GNU Public License Version 2.1+.

This product includes a library "libsigc++-2.0-2.10.0" under the Lesser GNU Public License Version 2.1+.

This product includes a library "librsvg-2.40.18" under the Lesser GNU Public License Version 2.1+.

This product includes a library "libproxy-0.4.14" under the Lesser GNU Public License Version 2.1+.

This product includes a library "mozjs-17.0.0" under the Lesser GNU Public License Version 2.1+.

This product includes a library "mm-common-0.9.10" under the Lesser GNU Public License Version 2.1+.

This product includes a library "opencv-3.1.0" under the Lesser GNU Public License Version 2.1+.

This product includes a library "python-2.7.15" under the Lesser GNU Public License Version 2.1+.

This product includes a library "python3-3.5.5" under the Lesser GNU Public License Version 2.1+.

This product includes a library "sbc-1.3" under the Lesser GNU Public License Version 2.1+.

This product includes a library "procps-3.3.12" under the Lesser GNU Public License Version 2.1+.

This product includes a library "pango-1.40.14" under the Lesser GNU Public License Version 2.1+.

This product includes a library "libusb1-1.0.21" under the Lesser GNU Public License Version 2.1+.

This product includes a library "linux-imx-4.14.98" under the Lesser GNU Public License Version 2.1+.

This product includes a library "libusb-compat-1_0.1.5" under the Lesser GNU Public License Version 2.1+.

This product includes a library "pulseaudio-13.0" under the Lesser GNU Public License Version 2.1+.

This product includes a library "pangomm-2.40.1" under the Lesser GNU Public License Version 2.1+.

This product includes a library "libtheora-1.1.1-r1.zip" under the Lesser GNU Public License Version 2.1+.

This product includes a library "util-linux-2.32.1" under the Lesser GNU Public License Version 2.1+.

This product includes a library "taglib-1.11.1" under the Lesser GNU Public License Version 2.1+.

This product includes a library "systemd-1_234" under the Lesser GNU Public License Version 2.1+.

This product includes a library "wireless-tools-1_30.pre9" under the Lesser GNU Public License Version 2.1+.

This product includes a library "jna-4.5.2" under the Lesser GNU Public License Version 2.1+.

This product includes a library "logback-classic-1.2.3" under the Lesser GNU Public License Version 2.1+.

This product includes a library "logback-core-1.2.3" under the Lesser GNU Public License Version 2.1+.

This product includes a library "resteasy-cdi-3.0.26.Final" under the Lesser GNU Public License Version 2.1+.

This product includes a library "tinymce.min.js.zip" under the Lesser GNU Public License Version 2.1+.

This product includes a library "jaxws-undertow-httpspi-1.0.1.Final" under the Lesser GNU Public License Version 2.1+.

9.6.7. LGPL-2.1+

9.6.8. LGPL-2.1

9.6.9. LGPL-2.0+

This product includes a library "flac-1.3.2" under the Library GNU Public License Version 2.0+.

This product includes a library "ffmpeg-3.4.2" under the Library GNU Public License Version 2.0+.

This product includes a library "gstreamer1.0-1.14.4" under the Library GNU Public License Version 2.0+.

This product includes a library "gstreamer1.0-plugins-good-1.14.4" under the Library GNU Public License Version 2.0+.

This product includes a library "libgudev-232" under the Library GNU Public License Version 2.0+.

This product includes a library "cairomm-1.12.0" under the Library GNU Public License Version 2.0+.

This product includes a library "barebox-1.0" under the Library GNU Public License Version 2.0+.

This product includes a library "at-spi2-atk-2.26.1" under the Library GNU Public License Version 2.0+.

This product includes a library "atk-2.26.1" under the Library GNU Public License Version 2.0+.

This product includes a library "alsa-utils-1.1.5" under the Library GNU Public License Version 2.0+.

This product includes a library "alsa-lib-1.1.5" under the Library GNU Public License Version 2.0+.

This product includes a library "at-spi2-core-2.26.2" under the Library GNU Public License Version 2.0+.

This product includes a library "gststreamer1.0-libav-1.14.4" under the Library GNU Public License Version 2.0+.

This product includes a library "glibc-2.26" under the Library GNU Public License Version 2.0+.

This product includes a library "libgnome-keyring-2.32.0" under the Library GNU Public License Version 2.0+.

This product includes a library "e2fsprogs-1.43.8" under the Library GNU Public License Version 2.0+.

This product includes a library "chromium-52.0.2743.76" under the Library GNU Public License Version 2.0+.

This product includes a library "glib-2.0-1_2.52.3" under the Library GNU Public License Version 2.0+.

This product includes a library "glibmm-2.54.1" under the Library GNU Public License Version 2.0+.

This product includes a library "dietlibc-cross-0.33" under the Library GNU Public License Version 2.0+.

This product includes a library "gdk-pixbuf-2.36.8" under the Library GNU Public License Version 2.0+.

This product includes a library "gststreamer1.0-plugins-bad-1.14.4" under the Library GNU Public License Version 2.0+.

This product includes a library "gobject-introspection-1.54.1" under the Library GNU Public License Version 2.0+.

This product includes a library "gststreamer1.0-plugins-base-1.14.4" under the Library GNU Public License Version 2.0+.

This product includes a library "iptables-1.6.1" under the Library GNU Public License Version 2.0+.

This product includes a library "libgpg-error-1.27" under the Library GNU Public License Version 2.0+.

This product includes a library "gconf-3.2.6" under the Library GNU Public License Version 2.0+.

This product includes a library "gtk+3-3.22.28" under the Library GNU Public License Version 2.0+.

This product includes a library "gtk+-2.24.32" under the Library GNU Public License Version 2.0+.

This product includes a library "gtkmm-2.24.5" under the Library GNU Public License Version 2.0+.

This product includes a library "imx-gst1.0-plugin-4.4.5" under the Library GNU Public License Version 2.0+.

This product includes a library "libexif-0.6.21" under the Library GNU Public License Version 2.0+.

This product includes a library "libcroco-0.6.12" under the Library GNU Public License Version 2.0+.

This product includes a library "gststreamer1.0-rtsp-server-1.14.3" under the Library GNU Public License Version 2.0+.

This product includes a library "libical-2.0.0" under the Library GNU Public License Version 2.0+.

This product includes a library "libgphoto2-2.5.8" under the Library GNU Public License Version 2.0+.

This product includes a library "libnewt-0.52.20" under the Library GNU Public License Version 2.0+.

This product includes a library "libnl-1_3.2.29" under the Library GNU Public License Version 2.0+.

This product includes a library "libsndfile1-1.0.28" under the Library GNU Public License Version 2.0+.

This product includes a library "librsvg-2.40.18" under the Library GNU Public License Version 2.0+.

This product includes a library "networkmanager-1.4.4" under the Library GNU Public License Version 2.0+.

This product includes a library "shared-mime-info-1.8" under the Library GNU Public License Version 2.0+.

This product includes a library "polkit-0.113" under the Library GNU Public License Version 2.0+.

This product includes a library "procps-3.3.12" under the Library GNU Public License Version 2.0+.

This product includes a library "pango-1.40.14" under the Library GNU Public License Version 2.0+.

This product includes a library "linux-imx-4.14.98" under the Library GNU Public License Version 2.0+.

This product includes a library "libusb-compat-1_0.1.5" under the Library GNU Public License Version 2.0+.

This product includes a library "openbox-3.6.1-r2.zip" under the Library GNU Public License Version 2.0+.

This product includes a library "pulseaudio-10.0" under the Library GNU Public License Version 2.0+.

This product includes a library "libtheora-1.1.1-r1.zip" under the Library GNU Public License Version 2.0+.

This product includes a library "speex-1.2.0" under the Library GNU Public License Version 2.0+.

This product includes a library "util-linux-2.32.1" under the Library GNU Public License Version 2.0+.

This product includes a library "systemd-1_234" under the Library GNU Public License Version 2.0+.

This product includes a library "dbus-java-2.7.3" under the Library GNU Public License Version 2.0+.

9.6.10. LGPL-2.0

9.6.11. LGPL

9.6.12. IJG

This software is based in part on the work of the Independent JPEG Group.

9.6.13. FTL

Portions of this software are copyright © 2006 The FreeType Project (www.freetype.org). All rights reserved.

9.6.14. BSD-4-CLAUSE

BSD-4-Clause-UC bind-9.10.5-P3

This product includes software developed by the Internet Systems Consortium.

busybox-1.27.2

This product includes software developed by the Software Freedom Conservancy.

This product includes software developed by the University of California, Berkeley and its contributors.

curl-7.66.0

This product includes software developed by Daniel Stenberg <daniel@haxx.se>.

e2fsprogs-1.43.8

This product includes software developed by Theodore Ts'o <tytso@mit.edu>.

file-5.31

This product includes software developed by Ian F. Darwin.

iputils-s20151218

This product includes software developed by Alexey Kuznetsov and YOSHIFUJI Hideaki.

kbd-2.0.4

This product includes software developed by Alexey Gladkov <gladkov.alexey@gmail.com>.

libarchive-3.3.2

This product includes software developed by Tim Kientzle.

libpcap-1.8.1

This product includes software developed by the TCPdump Group.

libtheora-1.1.1

This product includes software developed by the Xiph.org Foundation.

libxfont2-2.0.1

This product includes software developed by the X.Org Foundation.

linux-imx-4.14.98

This product includes software developed by Linus Torvalds.

ncurses-6.0+20170715

This product includes software developed by the Free Software Foundation, Inc.

nss-3.35

This product includes software developed by the Mozilla Foundation.

shadow-4.2.1

This product includes software developed by the Debian Project.

tcpdump-4.9.2

This product includes software developed by the TCPdump Group.

tiff-4.0.9

This product includes software developed by the company Silicon Graphics International.

This product includes software developed by the University of California, Berkeley and its contributors.

util-linux-2.32.1

This product includes software developed by the company Red Hat Limited.

9.6.15. APACHE-2.0

tslib

```CopyrightNotice.txt```

\*\*\*\*\*

Copyright (c) Microsoft Corporation. All rights reserved. Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at <http://www.apache.org/licenses/LICENSE-2.0> THIS CODE IS PROVIDED ON AN \*AS IS\* BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OR CONDITIONS OF TITLE, FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY OR NON-INFRINGEMENT.

See the Apache Version 2.0 License for specific language governing permissions and limitations under the License.

\*\*\*\*\*

**typescript**

```CopyrightNotice.txt```

Copyright (c) Microsoft Corporation. All rights reserved. Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at <http://www.apache.org/licenses/LICENSE-2.0> THIS CODE IS PROVIDED ON AN *AS IS* BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OR CONDITIONS OF TITLE, FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY OR NON-INFRINGEMENT.

See the Apache Version 2.0 License for specific language governing permissions and limitations under the License.

apache-mime4j-0.6

Apache JAMES Mime4j

Copyright 2004-2009 The Apache Software Foundation.

This product includes software developed at

The Apache Software Foundation (<http://www.apache.org/>).

classmate-1.1.0

Java ClassMate library was originally written by Tatu Saloranta (tatu.saloranta@iki.fi)

Other developers who have contributed code are:

* Brian Langel

commons-codec-1.10

Apache Commons Codec

Copyright 2002-2014 The Apache Software Foundation

This product includes software developed at

The Apache Software Foundation (<http://www.apache.org/>).

`src/test/org/apache/commons/codec/language/DoubleMetaphoneTest.java` contains test data from <http://aspell.net/test/orig/batch0.tab>.

Copyright (C) 2002 Kevin Atkinson (kevina@gnu.org)

=====

The content of package `org.apache.commons.codec.language.bm` has been translated from the original php source code available at <http://stevemorse.org/phoneticinfo.htm> with permission from the original authors.

Original source copyright:

Copyright (c) 2008 Alexander Beider & Stephen P. Morse.

commons-compress-1.12

Apache Commons Compress

Copyright 2002-2016 The Apache Software Foundation

This product includes software developed at

The Apache Software Foundation (<http://www.apache.org/>).

The files in the package `org.apache.commons.compress.archivers.sevenz` were derived from the LZMA SDK, version 9.20 (C/ and CPP/7zip/), which has been placed in the public domain:

"LZMA SDK is placed in the public domain." (<http://www.7-zip.org/sdk.html>)

commons-email-1.5

Apache Commons Email

Copyright 2001-2017 The Apache Software Foundation

This product includes software developed at

The Apache Software Foundation (<http://www.apache.org/>).

commons-io-2.5

Apache Commons IO

Copyright 2002-2016 The Apache Software Foundation

This product includes software developed at

The Apache Software Foundation (<http://www.apache.org/>).

commons-lang3-3.2.2

Apache Commons Lang

Copyright 2001-2014 The Apache Software Foundation

This product includes software developed at

The Apache Software Foundation (<http://www.apache.org/>).

This product includes software from the Spring Framework, under the Apache License 2.0 (see: `StringUtils.containsWhitespace()`)

commons-logging-1.2

Apache Commons Logging

Copyright 2003-2014 The Apache Software Foundation

This product includes software developed at

The Apache Software Foundation (<http://www.apache.org/>).

cxf-core-3.2.6

Apache CXF

Copyright 2006-2018 The Apache Software Foundation

This product includes software developed at

The Apache Software Foundation (<http://www.apache.org/>).

cxf-rt-bindings-soap-3.2.6

Apache CXF

Copyright 2006-2018 The Apache Software Foundation

This product includes software developed at

The Apache Software Foundation (<http://www.apache.org/>).

cxf-rt-bindings-xml-3.2.6

Apache CXF

Copyright 2006-2018 The Apache Software Foundation

This product includes software developed at

The Apache Software Foundation (<http://www.apache.org/>).

cxf-rt-databinding-jaxb-3.2.6

Apache CXF

Copyright 2006-2018 The Apache Software Foundation

This product includes software developed at

The Apache Software Foundation (<http://www.apache.org/>).

cxf-rt-frontend-jaxws-3.2.6

Apache CXF

Copyright 2006-2018 The Apache Software Foundation

This product includes software developed at

The Apache Software Foundation (<http://www.apache.org/>).

Java classes (source and binary) under `org.apache.cxf.jaxws.javaee` are generated from schema available here: (http://java.sun.com/xml/ns/javaee/javaee_5.xsd)

cxf-rt-frontend-simple-3.2.6

Apache CXF

Copyright 2006-2018 The Apache Software Foundation

This product includes software developed at

The Apache Software Foundation (<http://www.apache.org/>).

cxf-rt-transports-http-3.2.6

Apache CXF

Copyright 2006-2018 The Apache Software Foundation

This product includes software developed at

The Apache Software Foundation (<http://www.apache.org/>).

This project includes Public Suffix List copied from

https://publicsuffix.org/list/effective_tld_names.dat

licensed under the terms of the Mozilla Public License, v. 2.0

Full license text: <<http://mozilla.org/MPL/2.0/>>

cxf-rt-transports-http-undertow-3.2.6

Apache CXF

Copyright 2006-2018 The Apache Software Foundation

This product includes software developed at

The Apache Software Foundation (<http://www.apache.org/>).

cxf-rt-ws-addr-3.2.6

Apache CXF

Copyright 2006-2018 The Apache Software Foundation

This product includes software developed at

The Apache Software Foundation (<http://www.apache.org/>).

cxf-rt-ws-policy-3.2.6

Apache CXF

Copyright 2006-2018 The Apache Software Foundation

This product includes software developed at

The Apache Software Foundation (<http://www.apache.org/>).

This product includes software Copyright University of Southampton IT Innovation Centre, 2009

(<http://www.it-innovation.soton.ac.uk>).

cxf-rt-wsdl-3.2.6

Apache CXF

Copyright 2006-2018 The Apache Software Foundation

This product includes software developed at

The Apache Software Foundation (<http://www.apache.org/>).

httpasyncclient-4.1.4

Apache HttpAsyncClient

Copyright 2010-2018 The Apache Software Foundation

This product includes software developed at

The Apache Software Foundation (<http://www.apache.org/>).

httpclient-4.5.6

Apache HttpClient

Copyright 1999-2018 The Apache Software Foundation

This product includes software developed at

The Apache Software Foundation (<http://www.apache.org/>).

httpcore-4.4.10

Apache HttpCore

Copyright 2005-2018 The Apache Software Foundation

This product includes software developed at

The Apache Software Foundation (<http://www.apache.org/>).

httpcore-nio-4.4.10

Apache HttpCore NIO

Copyright 2005-2018 The Apache Software Foundation

This product includes software developed at

The Apache Software Foundation (<http://www.apache.org/>).

jackson-core-2.9.10

jackson-databind-2.9.10

jackson-jaxrs-json-provider-2.9.10

jackson-module-afterburner-2.9.10

jackson-module-jaxb-annotations-2.9.10

jackson-module-kotlin-2.9.10

Jackson JSON processor

Jackson is a high-performance, Free/Open Source JSON processing library. It was originally written by Tatu Saloranta (tatu.saloranta@iki.fi), and has been in development since 2007. It is currently developed by a community of developers, as well as supported commercially by FasterXML.com.

Licensing

Jackson core and extension components may be licensed under different licenses. To find the details that apply to this artifact see the accompanying LICENSE file. For more information, including possible other licensing options, contact FasterXML.com (<http://fasterxml.com>).

Credits

A list of contributors may be found from CREDITS file, which is included in some artifacts (usually source distributions); but is always available from the source code management (SCM) system project uses.

neethi-3.1.1

Apache Neethi

Copyright 2004-2018 The Apache Software Foundation

This product includes software developed at The Apache Software Foundation (<http://www.apache.org/>).

This product is tested with testcases developed at W3C under the license: <http://www.w3.org/Consortium/Legal/2002/copyright-documents-20021231> The source distribution of this product includes those testcases.

xmlschema-core-2.2.3

Apache WebServices - XmlSchema

Copyright 2004-2018 The Apache Software Foundation

This product includes software developed at

The Apache Software Foundation (<http://www.apache.org/>).

Portions Copyright 2006 International Business Machines Corp. Portions Copyright (C) World Wide Web Consortium 2006, 2007 and licensed under the three-part BSD license.

9.6.16. APACHE-1.1

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

10. LIST OF FIGURES

Fig. 1	Boot view "Preparing App".....	18
Fig. 2	Boot view "Initializing".....	18
Fig. 3	Boot view "Starting App".....	19
Fig. 4	Indoor - Format "Small".....	20
Fig. 5	Indoor - Format "Large".....	21
Fig. 6	Indoor - Keypad.....	22
Fig. 7	Indoor - Contacts.....	23
Fig. 8	Indoor - Recent.....	24
Fig. 9	Indoor - Format "Large".....	25
Fig. 10	Indoor - Format "Small".....	25
Fig. 11	Indoor - Format "Small (Image or Text)".....	26
Fig. 12	Indoor - 1 button, format "Large".....	26
Fig. 13	Frame "1 Button".....	27
Fig. 14	Frame "2 Buttons (1/2, 1/2)".....	28
Fig. 15	Frame "3 Buttons (1/3, 1/3, 1/3)".....	28
Fig. 16	Frame "3 Buttons (1/2, 1/4, 1/4)".....	29
Fig. 17	Frame "3 Buttons (2/3, 1/6, 1/6)".....	29
Fig. 18	Frame "4 Buttons (1/2, 1/6, 1/6, 1/6)".....	30
Fig. 19	Frame "4 Buttons (1/4, 1/4, 1/4, 1/4)".....	30
Fig. 20	Frame "5 Buttons (1/5, 1/5, 1/5, 1/5, 1/5)".....	31
Fig. 21	Customised visualisation.....	32
Fig. 22	Contact management.....	33
Fig. 23	Contact Management - Directory.....	34
Fig. 24	Outgoing Call - Type "Standard" with pictograms.....	35
Fig. 25	Outgoing Call - Type "Standard" without pictograms.....	36
Fig. 26	Outgoing Call - Type "Emergency" with pictograms.....	36
Fig. 27	Outgoing Call - Type "Emergency" without pictograms.....	37
Fig. 28	Incoming Call - with pictograms.....	38
Fig. 29	Incoming Call - with call control buttons.....	38
Fig. 30	In Call - Type "Standard" with pictograms.....	40
Fig. 31	In Call - Type "Standard" without pictograms.....	40
Fig. 32	In Call - Type "Emergency" with pictograms.....	41
Fig. 33	In Call - Type "Standard" without pictograms.....	41
Fig. 34	In Call - Keypad.....	43
Fig. 35	In Call - Audio devices.....	44
Fig. 36	Call ended.....	45
Fig. 37	Search - Layout "Indoor".....	46
Fig. 38	Search - Layout "Door".....	46
Fig. 39	Search - Layout "Contact Management".....	47
Fig. 40	PIN code.....	48
Fig. 41	Shuffled keypad numbers for code input.....	49
Fig. 42	User actions.....	50
Fig. 43	Confirmation dialogue.....	51
Fig. 44	Settings.....	52
Fig. 45	Settings - Audio.....	53
Fig. 46	Settings - Display "Adaptive".....	54
Fig. 47	Settings - Display "Manually".....	54
Fig. 48	Settings - Language.....	56
Fig. 49	Settings - System Information.....	57
Fig. 50	Settings - System Information - Network State.....	58
Fig. 51	Settings - System Information - SIP Servers.....	59
Fig. 52	Settings - System Information - Device Information.....	60
Fig. 53	Settings - System Information - Privacy.....	61
Fig. 54	Web interface can be accessed.....	62
Fig. 55	Web interface cannot be accessed.....	62
Fig. 56	Privacy.....	62
Fig. 57	Menu bar.....	63
Fig. 58	Change notice	64
Fig. 59	Confirmation notice.....	65
Fig. 60	Error message.....	65
Fig. 61	Activities and action sequences.....	65
Fig. 62	Landing page.....	66

Fig. 63	Overview - Device Information.....	66
Fig. 64	Device states.....	67
Fig. 65	Overview - Symphony Cloud Platform Information.....	67
Fig. 66	Overview.....	69
Fig. 67	Overview - Device Information.....	70
Fig. 68	Device states.....	70
Fig. 69	Overview - Symphony Cloud Platform Information.....	71
Fig. 70	Overview - Network State.....	72
Fig. 71	Overview - ONVIF.....	72
Fig. 72	Overview - SIP Servers.....	73
Fig. 73	General.....	74
Fig. 74	General - General	75
Fig. 75	General - DNSv4 Server	75
Fig. 76	General - DNSv6 Server	76
Fig. 77	General - 802.1X Authentication "Disabled".....	76
Fig. 78	General - 802.1X-Authentication „EAP-MD5“.....	77
Fig. 79	General - 802.1X Authentication „EAP-TLS“	77
Fig. 80	General - IEEE 802.1Q (VLAN)	78
Fig. 81	Allgemein - Quality of Service	78
Fig. 82	IPv4.....	79
Fig. 83	IPv4 - IPv4 „Disabled“	79
Fig. 84	IPv4 - IPv4 „DHCP“	80
Fig. 85	IPv4 - IPv4 „Manual“	80
Fig. 86	IPv4 - NAT	81
Fig. 87	IPv6 "Link-local only".....	82
Fig. 88	IPv6 „Automatic“	82
Fig. 89	IPv6 „Manual“	83
Fig. 90	Advanced Services.....	84
Fig. 91	Advanced Services - Symphony Cloud Platform Settings.....	84
Fig. 92	Advanced Services - SSH-Server.....	85
Fig. 93	Advanced Services - Set-UP Tool Settings.....	85
Fig. 94	Advanced Services - API Security.....	85
Fig. 95	TLS.....	86
Fig. 96	TLS - Server Certificates.....	86
Fig. 97	Web browser "Not secure".....	86
Fig. 98	Web browser "Secure".....	87
Fig. 99	TLS - Client CA Certificates.....	87
Fig. 100	ONVIF.....	88
Fig. 101	ONVIF - ONVIF Configuration	89
Fig. 102	ONVIF - ONVIF User.....	90
Fig. 103	ONVIF - ONVIF Information	90
Fig. 104	SIP.....	91
Fig. 105	SIP - SIP Settings.....	92
Fig. 106	SIP - SIP-Server.....	94
Fig. 107	Call Settings.....	96
Fig. 108	Call Settings - In Call.....	97
Fig. 109	Call Settings - Incoming Call.....	97
Fig. 110	Call Settings - Outgoing Call.....	98
Fig. 111	Advanced Options.....	99
Fig. 112	Advanced options - Registrarless.....	99
Fig. 113	Advanced Options - SIP-Server	100
Fig. 114	Certificates.....	101
Fig. 115	Certificates - SIP Certificates.....	101
Fig. 116	Certificates - SIP CA Certificates.....	102
Fig. 117	Device.....	103
Fig. 118	Device states.....	67
Fig. 119	Create a new layout.....	104
Fig. 120	Edit Layout Name.....	105
Fig. 121	Device - All - General.....	105
Fig. 122	Device - All - Display Settings.....	106
Fig. 123	Device - All - Pictograms.....	107
Fig. 124	Device - Idle - General.....	108
Fig. 125	Background image too wide (left) and too high (right).....	109
Fig. 126	Device - Idle - Customized Visualization.....	110
Fig. 127	Device - Idle - Buttons for the layouts "Indoor" and "Door".....	111
Fig. 128	Device - Idle - Buttons for the layouts "Indoor", "Door" and "Frame".....	111

Fig. 129	Device - Idle - Buttons for the layout "Frame".....	112
Fig. 130	Device - In Call - General.....	115
Fig. 131	Device - Incoming Call - General.....	115
Fig. 132	Device - Outgoing Call - General.....	116
Fig. 133	Audio.....	117
Fig. 134	Volume.....	118
Fig. 135	Volume.....	118
Fig. 136	Volume with connected EB3E2A-AUD.....	119
Fig. 137	Audio Devices.....	120
Fig. 138	Audio Devices.....	120
Fig. 139	Audio Devices with EB3E2A-AUD.....	121
Fig. 140	Audio Optimisation.....	123
Fig. 141	Advanced Audio Settings.....	124
Fig. 142	Loudspeaker/Microphone Surveillance.....	126
Fig. 143	Audio Monitoring	127
Fig. 144	Sound Pressure Level.....	128
Fig. 145	Video.....	129
Fig. 146	Motion detection.....	130
Fig. 147	Advertising.....	131
Fig. 148	Advertising - Advertising Mode.....	131
Fig. 149	Advertising - Advertisements.....	133
Fig. 150	IOs	134
Fig. 151	Activity.....	135
Fig. 152	Activity - Activities.....	135
Fig. 153	Activity - Add Activity.....	136
Fig. 154	Activity - Editing an activity.....	137
Fig. 155	Action Sequences.....	141
Fig. 156	Action Sequence - Add Action Sequence.....	141
Fig. 157	Action Sequence - Edit Action Sequence.....	142
Fig. 158	Action Sequences - Edit Action Sequence.....	142
Fig. 159	Action Sequence - Time Sequence.....	143
Fig. 160	Action Sequences - Actions.....	144
Fig. 161	Contacts.....	147
Fig. 162	Import contacts via a CSV file.....	148
Fig. 163	Contacts - Edit contacts.....	149
Fig. 164	Contacts - Add Call Buttons.....	150
Fig. 165	Contact Management.....	150
Fig. 166	Contact Management - Sticky Buttons and Directory Buttons.....	151
Fig. 167	Contact Management - Directory.....	152
Fig. 168	Contact Management - Buttons.....	153
Fig. 169	Contact Management - Button Configuration.....	153
Fig. 170	Contact Management - Edit contact.....	154
Fig. 171	Audio Files.....	156
Fig. 172	Audio File - Edit Audio File.....	157
Fig. 173	Snapshots.....	157
Fig. 174	Images.....	158
Fig. 175	Images.....	159
Fig. 176	System.....	160
Fig. 177	System - System	161
Fig. 178	System - Language and Region.....	162
Fig. 179	System - Time and Date.....	163
Fig. 180	System - Email Configuration.....	163
Fig. 181	System - Keypad.....	164
Fig. 182	Backup	164
Fig. 183	Backup - Backup.....	165
Fig. 184	Backup - Backup Storage.....	165
Fig. 185	User Management.....	166
Fig. 186	User Management - Users.....	166
Fig. 187	User Management - Profile.....	167
Fig. 188	User Management - Profile - Profile.....	168
Fig. 189	User management - Profile - passwords.....	169
Fig. 190	User Management - Profile - API-Token	170
Fig. 191	User Management - Profile - edit API-Token.....	171
Fig. 192	User Management - Profile - ONVIF User Level.....	172

Fig. 193	User Management - Profile - Roles.....	172
Fig. 194	User Management - Allowed Action Sequences.....	172
Fig. 195	User Management - Roles	173
Fig. 196	User Management - edit Role.....	174
Fig. 197	Codecs	175
Fig. 198	Codecs - Audio Codecs	176
Fig. 199	Codecs - Video Codecs	177
Fig. 200	Logging	177
Fig. 201	Logging - SystemLog.....	178
Fig. 202	Logging - Trace	178
Fig. 203	Logging - Eventlog	179
Fig. 204	Logging - General.....	179
Fig. 205	SNMP.....	180
Fig. 206	Remote Control.....	181
Fig. 207	Available actions - Change Audio Device.....	182
Fig. 208	Available actions - Play Audio File.....	182
Fig. 209	Available actions - Output.....	183
Fig. 210	Available actions - Change Display Brightness.....	183
Fig. 211	Available actions - Change Display Mode.....	184
Fig. 212	Available actions - Send DTMF Tone.....	184
Fig. 213	Available actions - Send Email.....	185
Fig. 214	Available actions - Cancel Call.....	185
Fig. 215	Available actions - On Hold.....	185
Fig. 216	Available actions - HTTP Client Action.....	186
Fig. 217	Available actions - Disconnect IP Secure Connector.....	187
Fig. 218	Available actions - Chain Call.....	187
Fig. 219	Available actions - Change Volume.....	188
Fig. 220	Available actions - Change Layout.....	188
Fig. 221	Available actions - Set LED.....	188
Fig. 222	Available actions - Mute Microphone.....	189
Fig. 223	Available actions - Parallel Call.....	189
Fig. 224	Available actions - Switch Pictogram.....	190
Fig. 225	Available actions - Call.....	191
Fig. 226	Available actions - Answer Call.....	191
Fig. 227	Available actions - Mute Ringing Tone.....	192
Fig. 228	Available actions - Snapshot.....	192
Fig. 229	Available actions - Play Info Message at the Remote Station.....	192
Fig. 230	Available actions - Delayed Action.....	193
Fig. 231	Available actions - Switch Video.....	193
Fig. 232	Available actions - Interrupt Advertisement.....	194
Fig. 233	Available actions - Change Advertising Mode.....	194
Fig. 234	Available actions - Show View.....	194
Fig. 235	Upload Window.....	195
Fig. 236	Videostream.....	196
Fig. 237	Standbild.....	198
Fig. 238	ONVIF Configuration.....	200
Fig. 239	Configure action.....	200
Fig. 240	Add Activity and Action Sequence - Add Activity.....	201
Fig. 241	Add Activity and Action Sequence - Add Activity.....	201
Fig. 242	Add Activity and Action Sequence - Add Activity.....	201
Fig. 243	Add Activity and Action Sequence - Name the Action Sequence.....	202
Fig. 244	Add Activity and Action Sequence - Edit Action Sequence.....	202
Fig. 245	Add Activity and Action Sequence - Edit Action Sequence.....	202
Fig. 246	Loudspeaker Microphone Surveillance - Add Activity.....	203
Fig. 247	Loudspeaker-Microphone Surveillance - Edit Activity	203
Fig. 248	Loudspeaker-Microphone-Surveillance - Add Action Sequence.....	203
Fig. 249	Loudspeaker-microphone surveillance - Name action sequence.....	204
Fig. 250	Loudspeaker-Microphone-Surveillance - Edit Action Sequence.....	204
Fig. 251	Loudspeaker-Microphone-Surveillance - Edit Action Sequence	205
Fig. 252	Loudspeaker-Microphone-Surveillance - Add Activity	206
Fig. 253	Loudspeaker-Microphone-Surveillance - Edit Activity	206
Fig. 254	Loudspeaker-Microphone-Surveillance - Add Action Sequence.....	206
Fig. 255	Loudspeaker-Microphone-Surveillance - Edit Action Sequence.....	206
Fig. 256	Loudspeaker-microphone surveillance - Edit Action Sequence.....	207
Fig. 257	Loudspeaker-Microphone-Surveillance - Edit Loudspeaker-Microphone-Surveillance.....	208
Fig. 258	Loudspeaker-Microphone-Surveillance - Delete Action Sequences.....	208

Fig. 259	Interrupt Advertisement - Add new Action Sequence.....	209
Fig. 260	Interrupt Advertisement - Edit Action.....	209
Fig. 261	Interrupt Advertisement - Add new Action Sequence.....	209
Fig. 262	Interrupt Advertisement - Name action sequence.....	210
Fig. 263	Interrupt Advertisement - Edit Action Sequence.....	210
Fig. 264	Interrupt Advertisement - Edit Action Sequence.....	210
Fig. 265	Configure Motion Detection.....	211
Fig. 266	Import Backup.....	211
Fig. 267	Import settings.....	212
Fig. 268	Accessing the web interface.....	215
Fig. 269	Changing the password.....	215
Fig. 270	Updating via USB stick.....	217
Fig. 271	ID5 DKGM or ID5 DKHSGM - Configure Audio Devices.....	225
Fig. 272	ID5 DKGM or ID5 DKHSGM - Activate the "Push-to-Talk" Pictogram.....	226
Fig. 273	ID5 DKGM or ID5 DKHSGM - Activate the "In Conversation" Pictogram.....	227
Fig. 274	ID5 DKGM or ID5 DKHSGM - Edit Action Sequence	227
Fig. 275	ID5 DKGM or ID5 DKHSGM - Edit Action Sequence	227
Fig. 276	ID5 DKGM or ID5 DKHSGM - Edit Action Sequence.....	228
Fig. 277	ID5 DKGM or ID5 DKHSGM - Edit Action Sequence	228
Fig. 278	ID5 DKGM or ID5 DKHSGM - Configure VirtuoSIS.....	229
Fig. 279	ID5 DKGM or ID5 DKHSGM - Configure VirtuoSIS.....	229
Fig. 280	ID5 DKGM or ID5 DKHSGM - Configure VirtuoSIS.....	230
Fig. 281	ID5 DKGM or ID5 DKHSGM - Configure VirtuoSIS.....	230
Fig. 282	Configuring device remote control - Adding an activity.....	232
Fig. 283	Configuring device remote control - Editing an activity.....	233
Fig. 284	Configuring device remote control - Adding an action sequence.....	233
Fig. 285	Configuring device remote control - Naming an action sequence.....	233
Fig. 286	Configuring device remote control - Editing an action sequence.....	233
Fig. 287	Configuring device remote control - Editing an action sequence.....	234

11. **LIST OF TABLES**

Tab. 1.	UDP ports and services.....	11
Tab. 2.	TCP ports and services.....	11
Tab. 3.	Other ports and services.....	12
Tab. 4.	Overview.....	224



commend

www.commend.com