Release Notes
System Software 10.2.4

Content

Release Notes describe news and changes in a release for each of the devices for which the release is available. Therefore, they may contain information that is not relevant to your device. If necessary, refer to the data sheet of your device to find out which functions it supports.

1   Release 10.2.4.101 (Patch 1)

1.1   New Features

1.1.1   VoSIP / MediaSec

MediaSec is a method of negotiating the mechanisms by which the voice data transmitted between your bintec elmeg system and a SIP server can be protected against access by third parties. To secure all aspects of VoIP communication, both the connection via the Internet and the actual voice data should be encrypted. The connection between your system and the server is therefore encrypted by means of TLS, the transmitted data by means of SRTP. MediaSec regulates the protection of the transmitted data between the SIP server and your system.

For seamless support, automatic negotiation of the transport protocol is mandatory. Fixed transport protocol settings (UDP and TCP) may cause problems during registration. Additionally, the use of SRTP must be allowed.
Your VoIP provider must support MediaSec.

PBX Mode

Configuration is carried out in the menu **VoIP > Settings > SIP-Provider**.

To support MediaSec, the following settings must be made or verified:

- **Registrar: Transport Protocol** =
    - *Automatic* for dynamic activation of MediaSec (RECOMMENDED!) or
    - *TLS* for static activation (without fallback to UDP/TCP)
- **Advanced Settings > Codec Settings**:
    - **SRTP** = *active*
    - **MediaSec** = *active*.

MGW Mode

Configuration is carried out in the menu **VoIP > Settings > SIP Accounts**.

To support MediaSec, the following settings must be made or verified:

- **Basic Parameters: Protocol**
    - *Automatic* for dynamic activation of MediaSec (RECOMMENDED!) or
    - *TLS* for static activation (without fallback to UDP/TCP)
- **Advanced Settings > Options:**

- o **RTP** = *active*
- o **MediaSec** = *active*.

1.2 Error corrections

- **VoSIP Support**: Release 10.2.4.101 (Patch 1) supports VoSIP (Voice over Secure IP), i.e. encrypted IP telephony.
- **IP Routing – Extended routes display (# 666)**: Displaying extended IPv4 routes in the overview did not provide identifying individual routes simply.
- **LTE – Internet access not functional (#1544)**: For devices without hardware reset of the LTE module, a reset changed the module status to *down,* but the module was not reset.
- **IPv6 – Packet loss (#1604)**: When routing fragmented IPv6 packets, it could happen that associated packets were collected but then discarded.
- **IPSec – Connection aborted (# 1630, 1844)**: After rekeying, a previously functional IPSec connection was aborted.
- **Ethernet – Switch configuration (# 1787):** Under **Physical Interfaces > Ethernet Ports,** no connection was established with **Configured Speed / Mode** = *Fixed 1000 mbps / Full Duplex*.
- **VoIP – SIP registration failed (#1885)**: The SIP registration of a HiPath 3000 v9 failed because of a header problem in the REGISTER request.
- **SIP – Certificate problem (# 1920)**: The SIP trunk TLS registration was not functional when **Check TLS certificate** was active.
- **Telephony - SIP Forking (# 1979):** SIP forking was not supported, so it could happen that outgoing calls were missing the ringing tone.
- **IPSec - Rekeying Fails (# 2107):** As a rule, rekeying of phase 2 is triggered by the initiator of an IPSec connection. If the initiator does not initiate rekeying at the end of the phase 2 SA lifetime, the responder must trigger it. In this case, it could happen that the negotiation failed, and no data could be transmitted.
- **VoIP – Connection aborted (# 2034)**: It could happen that VoIP connections were aborted when calling a team with *Automatic Call Pick-up with MoH.*
- **IPSec - Data transfer aborted (# 2062)**: After about 13 minutes the data transfer of an Apple iPhone 8 via IPSec IKEv2 connection was aborted.
- **FAX – Sporadic panic (#2074)**: Problems between session and timer sporadically caused a panic.
- **PBX – Memory problems (# 2166)**: Never-endling transactions caused memory problems.
- **Telephony – Route selection not possible (# 2173)**: Under **Call Routing > Automatic Route Selection > Interface / Provider > New** no route for external calls was available when **Routing Modus** = *Route*.
- **VoIP – Wrong file dependency (# 2198, media gateway only)**: The system software contained wrong file dependencies for the VoIP location.
- **SIP - One-way voice connection (# 1569, Media Gateway only):** In conjunction with a Netphone Cloud there could be one-way voice connections.

- **SIP - Wrong SIP Error used (# 1611, Media Gateway only):** If a fax was sent via T.38, but the receiver did not support T.38, the device answered with a SIP 415 instead of the required SIP 488.
- **SIP DTMF (# n / a, Media Gateway only):** Transmission of DTMF failed if the recipient supported DTMF inband only.

1.3 Known restrictions

- **SIP – Ring tone distorted (#2234):** With SRTP encrypted connections it can happen that the ring tone of an outgoing call is distorted.
- **SIP – Error in the RTP stream (#2229 – PBX mode):** It can happen that there are errors in the transmission of Music on Hold during connections encrypted with TLS+SRTP.

2 Release 10.2.4.100

2.1 New Features

Support for elmeg T600: Release 10.2.4 supports the key extension **elmeg T600** for **IP620** and **IP630** IP phones. The following key functions can be configured in the configuration interface of your be.IP in PBX mode:

- Dial Key
- Dial Key (DTMF)
- Extension Key (User)
- Macro Function

The MSN selection key and, as well as Park and Retrieve, are only available on the telephone as key functions. The configuration is done in the menu **Terminals > elmeg System Phones > elmeg IP > Edit**.

More information about the T600 can be found at http://www.bintec-elmeg.com/produkte/all-ip/telefone/t600 .

2.2 Changes

- **IP - DHCP metric configurable:** It is now possible to assign a metric for the routes received by an interface via DHCP. This may be necessary when configuring backup connections to ensure a clean switch to the backup and back again.
- **Scheduler - additional expressions available:** Additional variables are now available for use in the scheduler:
  - SL is replaced by the value of the MIB variable sysLocation
  - SC by the variable sysContact
  - N by the variable sysName.

2.3 Error Corrections

- **IPSec - IPSec Client configuration not exportable (# 1846):** It could happen that the export of the configuration file of an IPSec peer for the IPSec client failed.

- **GUI - Incomplete Display (# 889):** Under **System Administration > Status > SIP Provider** only five phone numbers were displayed.

- **WLAN Controller - Cumbersome input (# 1314**): To create a WLAN controller auto-profile that applies to slave access points with any IP address, it was necessary to enter *0.0.0.0 / 0.0.0.0.* This has been replaced by a simple switch.

- **NFON - SIP profile not correct (# 2061):** The SIP profile used in the configuration of an NFON account was incorrect.

- **Telephony – Volume setting not stored (# 1809):** If the headset volume had been set to more than "3" on **S560**, this was not stored correctly on the **be.IP**. upon provisioning (e.g. after a disconnect) the setting was not transmitted correctly to the phone.
  The correction must also be included in the system software of the telephone. An updated version will be available from the download section of **S560**.

- **Swyx - Fax Encoding Fails (# 1681):** On devices with an Audiocodes DSP, there were errors in fax encoding. No fax connection could be established via this DSP.

- **ISDN - Clearmode not functional (# 1664):** On devices with an Audiocodes DSP, it was not possible to let communicate ISDN devices via Clearmode according to RFC4040.