

Release Notes

System Software 10.2.10

Content

1	Release 10.2.10 Patch 2	2
1.1	Safety-relevant changes	2
1.2	New functions	2
1.3	Improvements / error corrections	2
2	Release 10.2.10 Patch 1	3
2.1	Error corrections	3
3	Release 10.2.10.100	5
3.1	New functions	5
3.2	Error corrections	5
3.3	Additional notes	7
4	Appendix	7
4.1	Advanced configuration of IKEv2-based IPSec peers	7
4.1.1	Determination of the data traffic to be tunnelled	7
4.1.2	Start mode	8
4.1.3	Clear distribution of roles between client and server	8

Notes

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

If you want to use the web filter, you must use at least release 10.2.8 because FlashStart has made a server change. Without an update, search engine queries (e.g. Google) no longer work.

1 Release 10.2.10 Patch 2

1.1 Safety-relevant changes

- **CVE-2022-0778** - To protect against the possible attacks described in CVE-2022-0778, the patches provided by OpenSSL have been integrated into the system software.

1.2 New functions

- The DynDNS provider *ddnss.de* was added to the list of preconfigured providers.
- In the configuration interface, the outgoing interface can be configured for the ping test, host monitoring and in the scheduler for the *ping test* event type. This allows IP connectivity and thus the function of Internet connections without extended routes to be monitored more easily and with less susceptibility to misconfiguration. A backup Internet connection, for example, can thus be connected and disconnected more easily.

1.3 Improvements / error corrections

- **Improvements to the WLAN controller (ER# 1440, 3251)** – Improvements for the configuration of managed access points have been made; especially when using multiple access point auto profiles for different IP networks.
- **Display incorrect (ER# 2980, 4645, 5477)** - In the Monitoring menu of the WLAN controller, an empty display and the display of incorrect time information, data throughput values and signal level peaks could occur.
- **Keepalive interface activated unintentionally (ER# 4567)** - In special configurations where a keepalive was supposed to activate an LTE interface when the DSL connection failed, it could happen that the LTE interface was activated unnecessarily.
- **Incorrect display on function keys (ER# 5428, #4538, #3987, #3951, #3117)** - If, for example, an immediate call forwarding was bound to a function key via a key macro, but was initiated and ended again via a key procedure, the status indication via the key LED was not reliable.
In principle, the **Terminals > elmeg system telephones > System telephone | elmeg IP > Edit > Keys** menu should be used to configure the function keys. This ensures correct synchronization of the status.

- **Using incorrect RTP ports (ER# 5720)** - After multiple Early Media dialogs occurred (e.g., due to multiple forwarding), the device sent RTP data to the port of a previous Early Media dialog and did not accept incoming data on the new port.
- **Outbound calls not possible (ER# 5752)** - SIP header handling for CLIR was not compliant with 1TR114. This resulted in outgoing calls not being possible on the Telekom nIMS platform.
- **Calls Aborted (ER# 5830)** - Due to the use of an incorrect TCP port, call setup errors occurred for unencrypted SIP connections over TCP at the Telekom IMS platform.
- **Call forwarding not possible (ER# 5864)** - Call forwarding was not possible due to an incorrect SDP header.
- **Passwords not displayed (ER# 1547)** - Although the setting to display passwords in plain text was enabled on the system, passwords of the configured ISPs were not displayed accordingly.
- **No ringing tone (#5885)** - During operation in media gateway mode, it could happen that no ringing tone was heard in case of call forwarding.
- **IPSec connection disrupted (#3920)** - When monitoring an IPSec peer using Keepalive Monitoring, it could happen that data transmission within the IPSec tunnel was disrupted.
- **Restart (#5296, 5468)** - Unintended restarts could occur when renegotiating the child SA (IPSec SA) of an IPSec connection.
The restarts are now avoided, but it is useful to follow the configuration notes summarized in [Advanced Configuration of IKEv2-based IPSec Peers](#) to ensure seamless renegotiations.
- **Restarts (ER# 5710, 5736)** - Repeated restarts of the device could occur.
- **Unable to connect (ER# 5719)** - There could be problems connecting to numbers on the T-Mobile network.
- **Callback on busy fails (#5704)** - A callback once the other party was no longer busy failed.

2 Release 10.2.10 Patch 1

2.1 Error corrections

- **Telephony not possible (#5609, 5612, 3957)** - After updating to release 10.2.10, it was no longer possible to reach SIP connections that work without a registration (e.g. Vodafone connections).
To solve the problem, you can enable **Periodic OPTIONS** in the connection settings.
 - When operating as a PBX: Go to the **VoIP > Settings > SIP Provider** menu and select the appropriate account. In the **Advanced Settings > Further Settings** menu area, the value *No registration* should be selected for the **Registration Type** option. Here you can activate

Periodic OPTIONS:

Registration type Single Bulk (BNC) No registration

Periodic Options

- When operating as a media gateway: Go to the **VoIP > Settings > SIP Accounts** menu and select the appropriate account. In the **Basic parameters** menu area, the value *No registration* should be selected for the **Registration Type** option. Here you can activate **Periodic OPTIONS:**

Registration type Single Bulk (BNC) No registration

Periodic Options

Your device will then send certain SIP messages (SIP OPTIONS) to the service provider at regular intervals, and the connection will remain active.

- **LTE stick not responding (#5124)** - It could happen that a USB stick connected to the USB port was no longer functional and was only ready for use again after restarting the device.
- **Using the WAN interface for LAN connection (#4165)** - If the WAN Ethernet interface was used as LAN interface, no Internet connection via the internal modem from this LAN was possible.
- **Reboot (#5565)** - Occasional reboots of the device could occur.
- **Incorrect User Agent (#5503)** - Due to an incorrectly created user agent in the SIP message header, there were problems displaying the device on the service provider's SIP platform.
- **Incompatible WLAN security mechanisms (#4248)** - Due to the support of WPA3 and OWE in the WLAN controller, it could happen that the controller specified security settings that are not supported by older access points (WIQ, INY, WNY) (e.g. with WPA3 as the only WPA mode). In this case, it could happen that an access point became active with lower security than the configuration intended, and this error was not detectable. This problem is now avoided: The access point remains inactive and reports an error to the WLAN controller.
- **Missing channel change (#5110)** - When an access point detects a radar signal on the currently used channel, it must change the channel. This was not always the case with access points from the W200x-ac series (WIQ).
- **Channel reallocation fails (#5157)** - If a reallocation of the used radio channel was triggered by the WLAN controller, it was never completed for an access point if it temporarily lost connection to the WLAN controller.
- **Incorrect display of connection duration (#5505)** - Access points of the 802.11n, and 802.11ac series (WIQ, WNY INY) reported an incorrect connection duration to the WLAN controller on first contact, which initially led to an incorrect display in the WLAN controller.
- **Sporadic restarts (#5619)**: Many simultaneous calls could cause the be.IP to restart.

- **No data transfer via IPSec (#5673):** After an interruption of the Internet connection or of the IPSec tunnel, it could happen that no data could be transferred through the tunnel even after it had been reestablished.

3 Release 10.2.10.100

3.1 New functions

- **Support for be.IP plus V. 2** - Release 10.2.10.100 includes many improvements and changes to provide the **be.IP plus V. 2 with** system software optimized in terms of reliability and performance as well as interoperability.
All other products for which the release is available will, of course, also benefit from the improvements especially in the areas of telephony (PBX and MGW) and IPSec (IKEv2).
- **SIP Dual Stack** - SIP connections can be established over both IPv4 and IPV6. The configuration of the function is done by a setting in the MIB: When operating as a *PBX*, set the value of **mpsVoIPConfigIpVersion** to *ipv4_ipv6*; when operating as a media gateway, set the value of **voipSipIpVersion** to *ipv4_ipv6*.
You can make the MIB settings in the GUI if you set the view to *Full Access* and then switch to the **SNMP browser**:



Note

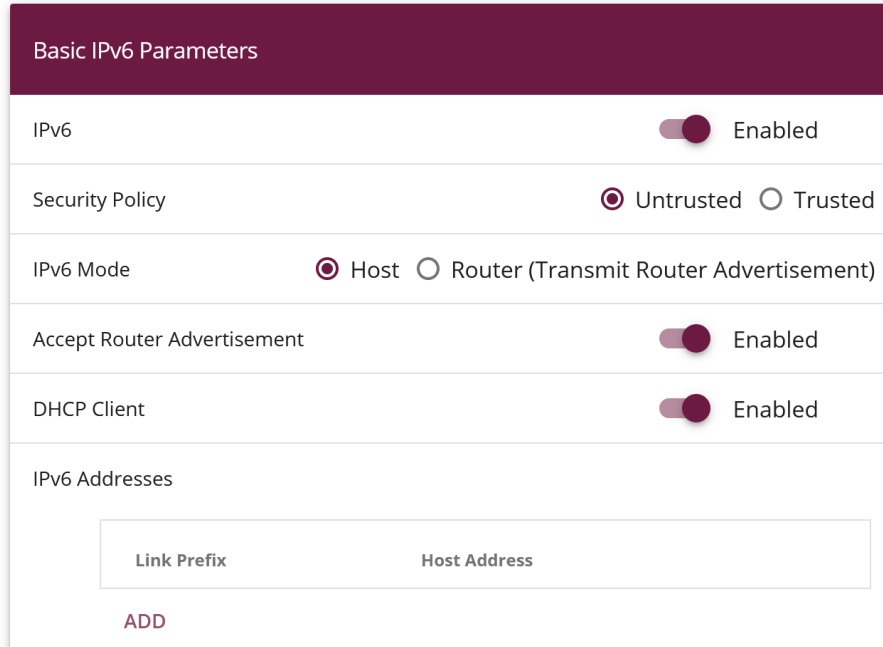
This setting is not covered by the configuration conversion when switching between operation modes. Therefore, adjust it once after a switch if necessary.

3.2 Error corrections

- **No umlauts in DECT solution (#2473):** DECT150 and connected handsets were not able to correctly display umlauts in device names when they were transmitted via provisioning.
- **Busy lamp field display incorrect (#5437, 5462):** After updating the system software to 10.2.9 Patch 3, it could happen that the busy lamp field on a connected phone no longer signaled correctly.
- **Incorrect display on function keys (#5428)** - If, for example, an immediate call forwarding was bound to a function key via a key macro but was initiated and ended again via a key procedure, the display of the status via the key LED was not reliable. The **Terminals > elmeg system phones > System phone | elmeg IP > Edit > Keys** menu should be used to configure the function keys. This ensures correct synchronization of the status.
- **Inoperative configuration (#5451)** - When operating as a PBX, it could happen that the boot configuration of a be.IP became unusable due to an internal process.
- **Internet connections via IPv6 (#5411)** - If an Internet connection was established via IPv6 and DHCP, problems could occur if an IPv6 address was

initially transmitted to the device, but then the execution of SLAAC was signaled. The bintec elmeg device then released the obtained address again. This problem can be prevented with the following settings:

- Make sure that in the **LAN > IP Configuration** menu, the interface over which the connection is established is set up as a DHCPv6 client:



Basic IPv6 Parameters

IPv6 Enabled

Security Policy Untrusted Trusted

IPv6 Mode Host Router (Transmit Router Advertisement)

Accept Router Advertisement Enabled

DHCP Client Enabled

IPv6 Addresses

Link Prefix Host Address

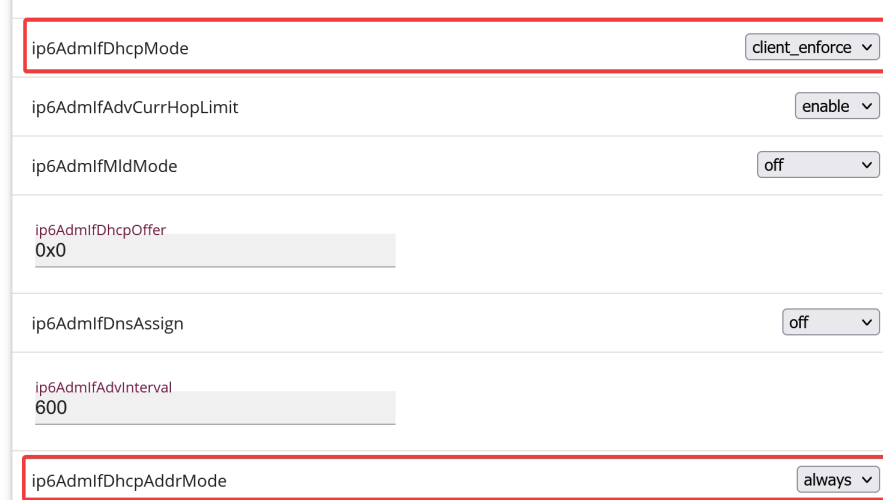
ADD

- Check that a dynamic prefix is created in the **Network > General IPv6 Prefixes** menu.
- Then switch to the SNMP browser:



be.IP plus bintec elmeg LANGUAGE VIEW Standard Standard SNMP Browser

- In the **ip6AdmIfTable** for the corresponding interface, set the value for **ip6AdmIfDhcpMode** to *client_enforce* and for **ip6AdmIfDhcpAddrMode** to *always*:



ip6AdmIfDhcpMode client_enforce

ip6AdmIfAdvCurrHopLimit enable

ip6AdmIfMldMode off

ip6AdmIfDhcpOffer 0x0

ip6AdmIfDnsAssign off

ip6AdmIfAdvInterval 600

ip6AdmIfDhcpAddrMode always

3.3 Additional notes

- Some connections, e.g., a Telekom CompanyFlex SIP Trunk, can only be configured in the **VoIP** menu of the *Expert* or *Full Access View*. If one of these connections has been created, it must not be changed via the assistants, as this would render the configuration non-functional.

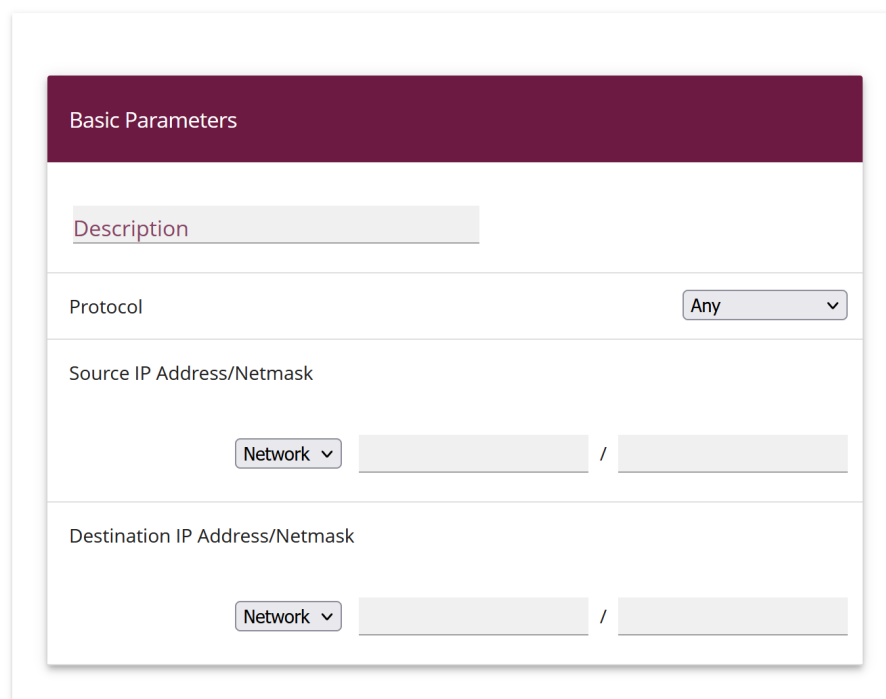
4 Appendix

4.1 Advanced configuration of IKEv2-based IPSec peers

To ensure that the negotiation of connection parameters works without errors for IPSec connections based on IKEv2, it is recommended to configure the connection as described below.

4.1.1 Determination of the data traffic to be tunnelled

It is useful to specify the traffic that should be sent over the tunnel as precisely as possible. To do this, you can narrow down the destination and source networks in the **VPN > IPSec > IPSec peers > Edit > Additional filter of IPv4 traffic** menu:



APPLY CANCEL

In this menu, make sure that the networks connected via the tunnel include all IP addresses that should have access to the remote network, and likewise all addresses that should be reached there.

These settings are always useful, regardless of whether the *On demand* or *Always on Start Mode* is selected in the **Advanced IPSec Options** section.

4.1.2 Start mode

For IPSec connections that must be permanently active and for which the bintec elmeg router initiates the connection, it is recommended to set the **Start Mode** of the peer in the menu **VPN > IPSec > IPSec Peers > Edit > Advanced settings** to *Always on* value to ensure a unambiguous state of the IPSec interface.

4.1.3 Clear distribution of roles between client and server

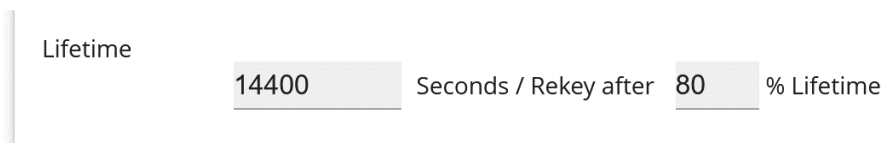
When configuring an IPSec connection, you should always ensure that the roles of the two IPSec connection partners are clearly assigned (initiator or responder role). This is important both for the initial connection setup and for the periodic renegotiation of the IPSec connection.

Therefore, when configuring the **Lifetime** in the Phase 1 and Phase 2 profiles, make sure that the set value on the initiator side is shorter than on the responder side. For example, you can set two-thirds of the responder's phase 1 lifetime for the initiator's phase 1 lifetime. Proceed in the same way for the phase 2 lifetime.

Due to the asymmetric configuration of the lifetime and the associated clear distribution of roles, you can avoid collisions during the periodically repeated renegotiation of the IPSec connection.

You can find the settings in the following menus:

- **Internet & Network > VPN > IPSec > Phase-1-Profiles > Edit**

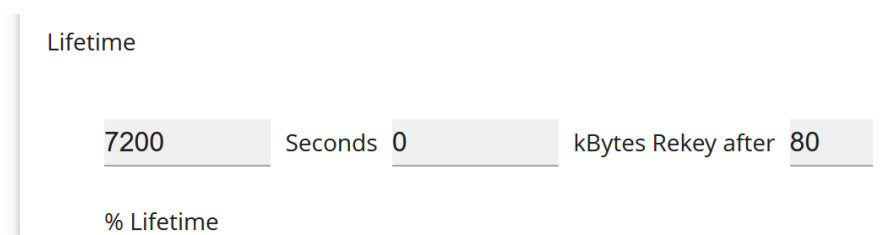


The screenshot shows the configuration for Phase-1-Profiles. It features a 'Lifetime' label followed by a text input field containing '14400', the text 'Seconds / Rekey after', another text input field containing '80', and the text '% Lifetime'.

Set the values so that the validity of the Phase 1 parameters is shorter on the dialing client than on the server.

Make sure that you select the profile here that the peer in question actually uses!

- **Internet & Network > VPN > IPSec > Phase-2-Profiles > Edit**



The screenshot shows the configuration for Phase-2-Profiles. It features a 'Lifetime' label followed by a text input field containing '7200', the text 'Seconds', a text input field containing '0', the text 'kBytes Rekey after', a text input field containing '80', and the text '% Lifetime'.

Set the values so that the validity of the Phase 2 parameters is shorter on the dialing client than on the server.

Make sure that you select the profile here that the peer in question actually uses!

The validity of phase 1 should clearly exceed that of phase 2!