

Release Notes

System Software 10.2.10

Inhalt

1	Release 10.2.10 Patch 2	2
1.1	Sicherheitsrelevante Änderungen	2
1.2	Neue Funktionen	2
1.3	Verbesserungen / Fehlerbehebungen	2
2	Release 10.2.10 Patch 1	3
2.1	Fehlerbehebungen	3
3	Release 10.2.10.100	5
3.1	Neue Funktionen	5
3.2	Fehlerbehebungen	6
3.3	Ergänzende Hinweise	8
4	Anhang	8
4.1	Erweiterte Konfiguration von IKEv2-basierten IPSec Peers	8
4.1.1	Festlegung des zu tunnelnden Datenverkehrs	8
4.1.2	Startmodus	9
4.1.3	Eindeutige Rollenverteilung zwischen Client und Server	9

Hinweise

Release Notes beschreiben Neuigkeiten und Änderungen in einem Release für jeweils alle Geräte, für die das Release zur Verfügung steht. Daher können sie Informationen enthalten, die für Ihr Gerät nicht relevant sind. Informieren Sie sich ggf. im Datenblatt Ihres Geräts, welche Funktionen es unterstützt.

Wenn Sie den Webfilter verwenden wollen, müssen Sie mindestens Release 10.2.8 verwenden, da FlashStart eine Serverumstellung vorgenommen hat. Ohne Update funktionieren Suchmaschinenanfragen (z. B. Google) nicht mehr.

1 Release 10.2.10 Patch 2

1.1 Sicherheitsrelevante Änderungen

- **CVE-2022-0778** - Zur Absicherung gegen die in CVE-2022-0778 beschriebenen möglichen Angriffe wurden die von OpenSSL zur Verfügung gestellten Patches in die Systemsoftware integriert.

1.2 Neue Funktionen

- Der DynDNS-Anbieter *ddnss.de* wurde der Liste der vorkonfigurierten Anbieter hinzugefügt.
- In der Konfigurationsoberfläche kann für den Ping-Test, die Host-Überwachung und im Scheduler für den Ereignistyp *Ping-Test* die ausgehende Schnittstelle konfiguriert werden. Insbesondere kann damit die IP-Konnektivität und somit die Funktion von Internetanbindungen ohne erweiterte Routen einfacher und weniger fehlkonfigurationsanfällig überwacht werden. Eine Backup-Internetverbindungen z. B. kann so einfacher zu- und weggeschaltet werden.

1.3 Verbesserungen / Fehlerbehebungen

- **Verbesserungen am WLAN Controller (ER# 1440, 3251)** – Am WLAN Controller wurde eine Reihe von Verbesserungen bei der Konfiguration der verwalteten Access Points - insbesondere bei Verwendung mehrerer Access-Point-Autoprofile für verschiedene IP-Netze - eingeführt.
- **Anzeige fehlerhaft (ER# 2980, 4645, 5477)** - Im Menü Monitoring des WLAN Controllers konnte es zu einer leeren Anzeige und zur Anzeige falscher Zeitangaben, Datendurchsatzwerte und Signalpegelspitzen kommen.
- **Keepalive-Schnittstelle ungewollt aktiviert (ER# 4567)** - In speziellen Konfigurationen, in denen ein Keepalive eine LTE-Schnittstelle beim Ausfall der DSL-Verbindung aktivieren sollte, konnte es vorkommen, dass die LTE-Schnittstelle unnötigerweise aktiviert wurde.
- **Falsche Anzeige an Funktionstasten (ER# 5428)** - Wenn z. B. eine sofortige Rufweiterleitung über ein Tasten-Makro auf eine Funktionstaste gebunden war, aber über eine Tastenprozedur eingeleitet und wieder beendet wurde, war die Anzeige des Status über die Tasten-LED nicht zuverlässig.

Für die Konfiguration der Funktionstasten sollte das Menü **Endgeräte > elmeg Systemtelefone > Systemtelefon | elmeg IP > Bearbeiten > Tasten** verwendet werden. Dies stellt eine korrekte Synchronisation des Status sicher.

- **Verwendung falscher RTP-Ports (ER# 5720)** - Nach mehreren erfolgten Early-Media-Dialogen (z. B. durch mehrfache Weiterleitung) sendete die Digitalisierungsbox RTP-Daten an den Port eines früheren Early Media Dialogs und nahm eingehende Daten am neuen Port nicht an.
- **Ausgehende Rufe nicht möglich (ER# 5752)** - Die Behandlung der SIP Header für CLIR war nicht konform zu 1TR114. Dies führte dazu, dass an der nIMS-Plattform der Telekom ausgehende Rufe nicht möglich waren.
- **Rufe abgebrochen (ER# 5830)** - Aufgrund der Verwendung eines falschen TCP-Ports kam es bei unverschlüsselten SIP-Verbindungen über TCP an der IMS-Plattform der Telekom zu Fehlern im Rufaufbau.
- **Anrufweitschaltung nicht möglich (ER# 5864)** - Aufgrund eines falschen SDP Headers war eine Anrufweitschaltung nicht möglich.
- **Passwörter nicht angezeigt (ER# 1547)** – Obwohl die Einstellung zur Klartextanzeige der Passwörter auf dem System aktiviert war, wurden Passwörter der eingerichteten Internetanbieter nicht entsprechend angezeigt.
- **Kein Rufton (#5885, #4538, #3987, #3951, #3117)** – Es konnte vorkommen, dass im Betrieb als Media Gateway im Fall einer Rufweiterleitung keine Rufton zu hören war.
- **IPSec-Verbindung gestört (#3920)** - Bei der Überwachung eines IPSec Peers mittels Keepalive Monitoring konnte es vorkommen, dass die Datenübertragung innerhalb des IPSec-Tunnels gestört wurde.
- **Neustart (#5296, 5468)** - Bei der Neuaushandlung der Child SA (IPSec SA) einer IPSec-Verbindung konnte es zu ungewollten Neustarts kommen. Die Neustarts werden nun vermieden, es ist allerdings sinnvoll, die in [Erweiterte Konfiguration von IKEv2-basierten IPSec Peers](#) zusammengefassten Konfigurationshinweise zu beachten, um reibungslose Neuaushandlungen zu gewährleisten.
- **Neustarts (ER# 5710, 5736)** – Es konnte zu wiederholten Neustarts des Geräts kommen.
- **Verbindung nicht möglich (ER# 5719)** - Es konnte zu Problemen bei der Verbindung zu Nummern im T-Mobile-Netz kommen.
- **Rückruf bei besetzt schlägt fehl (#5704)** - Ein Rückruf, sobald der andere Teilnehmer nicht mehr besetzt war, schlug fehl.

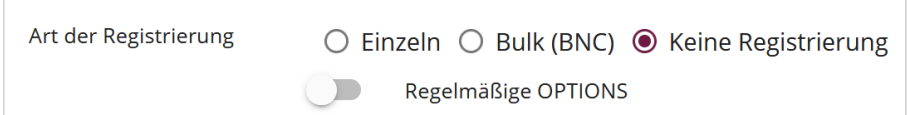
2 Release 10.2.10 Patch 1

2.1 Fehlerbehebungen

- **Telefonie nicht möglich (#5609, 5612, 3957)** – Nach einem Update auf Release 10.2.10 war es nicht mehr möglich, SIP-Anschlüsse, die ohne eine Registrierung arbeiten (z. B. Vodafone-Anschlüsse), zu erreichen.

Um das Problem zu lösen, können Sie in den Einstellungen des Anschlusses die Option **Regelmäßige OPTIONS** aktivieren.

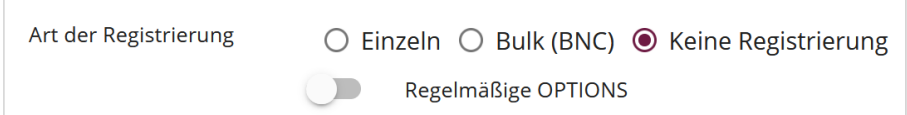
- Im Betrieb als Telefonanlage: Gehen Sie in das Menü **VoIP > Einstellungen > SIP Provider** und wählen Sie das entsprechende Konto aus. Im Menübereich **Erweiterte Einstellungen > Weitere Einstellungen** sollte für die Option **Art der Registrierung** der Wert *Keine Registrierung* ausgewählt sein. Hier können Sie die Option **Regelmäßige OPTIONS** aktivieren:



Art der Registrierung Einzel Bulk (BNC) Keine Registrierung

Regelmäßige OPTIONS

- Im Betrieb als Media Gateway: Gehen Sie in das Menü **VoIP > Einstellungen > SIP-Konten** und wählen Sie das entsprechende Konto aus. Im Menübereich **Basisparameter** sollte für die Option **Art der Registrierung** der Wert *Keine Registrierung* ausgewählt sein. Hier können Sie die Option **Regelmäßige OPTIONS** aktivieren:



Art der Registrierung Einzel Bulk (BNC) Keine Registrierung

Regelmäßige OPTIONS

Ihr Gerät sendet dann in regelmäßigen Abständen bestimmte SIP-Nachrichten (SIP OPTIONS) an den Dienstanbieter, und die Verbindung bleibt aktiv.

- **LTE-Stick reagiert nicht (#5124)** - Es konnte vorkommen, dass ein am USB angeschlossener USB-Stick nicht mehr funktionsfähig war und erst nach einem Neustart des Geräts wieder einsatzbereit war.
- **Nutzung der WAN-Schnittstelle zur LAN-Anbindung (#4165)** – Wenn die WAN-Ethernet-Schnittstelle als LAN-Schnittstelle verwendet wurde, war keine Internetverbindung über das interne Modem aus diesem LAN möglich.
- **Neustart (#5565)** - Es konnte zu gelegentlichen Neustarts des Geräts kommen.
- **Falscher User Agent (#5503)** - Wegen eines falsch erzeugten User Agents im SIP Message Header kam es zu Problemen in der Anzeige des Geräts auf der SIP-Plattform des Dienstanbieters.
- **Inkompatible WLAN Sicherheitsmechanismen (#4248)** – Aufgrund der Unterstützung von WPA3 und OWE im WLAN Controller konnte es vorkommen, dass dieser Sicherheitseinstellungen vorgab, die von älteren Access Points (WIQ, INY, WNY) nicht unterstützt werden (z. B. mit WPA3 als einzigem WPA-Modus). In diesem Fall konnte es vorkommen, dass ein Access Point mit geringerer Sicherheit aktiv wurde, als es die Konfiguration vorsah, und dies nicht erkennbar war. Dieses Problem wird nun vermieden: Der Access Point bleibt inaktiv und meldet einen Fehler an den WLAN Controller.

- **Fehlender Kanalwechsel (#5110)** – Wenn ein Access Point ein Radarsignal auf dem aktuell verwendeten Kanal erkennt, muss er den Kanal wechseln. Dies war bei Access Points der W200x-ac-Reihe (WIQ) nicht immer gegeben.
- **Kanalfestlegung scheitert (#5157)** – Wenn eine Neufestlegung des verwendeten Funkkanals vom WLAN Controller ausgelöst wurde, wurde diese für einen Access Point nie abgeschlossen, wenn dieser vorübergehend die Verbindung zum WLAN Controller verlor.
- **Falsche Anzeige der Verbindungsdauer (#5505)** – Access Points der 802.11n-, und 802.11ac-Serien (WIQ, WNY INY) meldeten dem WLAN Controller beim ersten Kontakt eine falsche Verbindungsdauer, was zunächst zu einer falschen Anzeige im WLAN Controller führte.
- **Sporadische Neustarts (#5619)**: Bei vielen gleichzeitigen Gesprächen konnte es zu einem Neustart der **be.IP** kommen.
- **Kein Datentransfer über IPSec (#5673)**: Nach einer Unterbrechung der Internetverbindung oder des IPSec-Tunnels konnte es vorkommen, dass nach dem Wiederaufbau des Tunnels dennoch keine Daten über die IPSec-Verbindung übertragen werden konnten.

3 Release 10.2.10.100

3.1 Neue Funktionen

- **Unterstützung der be.IP plus V. 2** – Release 10.2.10.100 umfasst eine große Anzahl von Verbesserungen und Änderungen, um der **be.IP plus V. 2** eine im Hinblick auf Zuverlässigkeit und Leistung sowie Interoperabilität optimierte Systemsoftware zur Verfügung zu stellen. Alle anderen Produkte, für die das Release zur Verfügung steht, profitieren natürlich ebenfalls von den Verbesserungen vor allem in den Bereichen Telefonie (PBX und MGW) und IPSec (IKEv2).
- **SIP Dual Stack** – SIP-Verbindungen können sowohl über IPv4 als auch über IPV6 aufgebaut werden. Die Konfiguration der Funktion erfolgt über eine Einstellung in der MIB: Im Betrieb als Telefonanlage setzen Sie den Wert von **mppsVoIPConfigIpVersion** auf *ipv4_ipv6*; im Betrieb als Media Gateway den von **voipSipIpVersion** auf *ipv4_ipv6*. Sie können die MIB-Einstellungen im GUI vornehmen, wenn Sie die Ansicht auf *Vollzugriff* einstellen und dann in den **SNMP-Browser** wechseln:



Hinweis

Diese Einstellung wird nicht von der Konvertierung der Konfiguration beim Wechsel zwischen den Betriebsarten erfasst. Passen Sie sie daher ggf. nach einem Wechsel einmalig an.

3.2 Fehlerbehebungen

- **Keine Umlaute in DECT-Lösung (#2473):** DECT150 und angeschlossene Handsets waren nicht in der Lage Umlaute in den Gerätenamen korrekt darzustellen, wenn diese über die Provisionierung übermittelt wurden.
- **Anzeige im Besetztlampenfeld falsch (#5437, 5462):** Nach einem Update der Systemsoftware auf 10.2.9 Patch 3 konnte es vorkommen, dass das Besetztlampenfeld and einem angeschlossenen Telefon nicht mehr korrekt signalisierte.
- **Falsche Anzeige an Funktionstasten (#5428)** – Wenn z. B. eine sofortige Rufweiterleitung über ein Tasten-Makro auf eine Funktionstaste gebunden war, aber über eine Tastenprozedur eingeleitet und wieder beendet wurde, war die Anzeige des Status über die Tasten-LED nicht zuverlässig. Für die Konfiguration der Funktionstasten sollte das Menü **Endgeräte > elmeg Systemtelefone > Systemtelefon | elmeg IP > Bearbeiten > Tasten** verwendet werden. Dies stellt eine korrekte Synchronisation des Status sicher.
- **Nicht funktionsfähige Konfiguration (#5451)** – Im Betrieb als Telefonanlage konnte es vorkommen, dass die Boot-Konfiguration einer be.IP durch einen internen Vorgang unbrauchbar wurde.
- **Internetanschlüsse über IPv6 (#5411)** – Wenn ein Internetanschluss über IPv6 und DHCP aufgebaut wurde, konnte es zu Problemen kommen, wenn dem Gerät zunächst eine IPv6-Adresse übermittelt wurde, dann aber die Ausführung von SLAAC signalisiert wurde. Das bintec-elmeg-Gerät gab die bezogene Adresse dann wieder frei.
Dieses Problem lässt sich mit folgenden Einstellungen verhindern:
 - Stellen Sie sicher, dass im Menü **LAN > IP-Konfiguration** die Schnittstelle, über die die Verbindung aufgebaut wird, als DHCPv6

Client eingerichtet ist:

Grundlegende IPv6-Parameter

IPv6	<input checked="" type="checkbox"/> Aktiviert
Sicherheitsrichtlinie	<input checked="" type="radio"/> Nicht Vertrauenswürdig <input type="radio"/> Vertrauenswürdig
IPv6-Modus	<input checked="" type="radio"/> Host <input type="radio"/> Router (Router-Advertisement übermitteln)
Router Advertisement annehmen	<input checked="" type="checkbox"/> Aktiviert
DHCP-Client	<input checked="" type="checkbox"/> Aktiviert
IPv6-Adressen	
Link-Präfix	Host-Adresse
HINZUFÜGEN	

- Kontrollieren Sie, dass im Menü **Netzwerk > Allgemeine IPv6-Präfixe** ein dynamischer Präfix angelegt ist.
- Wechseln Sie dann in dem SNMP-Browser:

be.IP plus

SPRACHE ANSICHT Standard

Standard
SNMP-Browser

- Stellen Sie in der **ip6AdmIfTable** für die entsprechende Schnittstelle den Wert für **ip6AdmIfDhcpMode** auf *client_enforce* und für **ip6AdmIfDhcpAddrMode** auf:

ip6AdmIfDhcpMode	client_enforce <input type="text"/>
ip6AdmIfAdvCurrHopLimit	enable <input type="text"/>
ip6AdmIfMldMode	off <input type="text"/>
ip6AdmIfDhcpOffer 0x0	
ip6AdmIfDnsAssign	off <input type="text"/>
ip6AdmIfAdvInterval 600	
ip6AdmIfDhcpAddrMode	always <input type="text"/>

3.3 Ergänzende Hinweise

- Die Einrichtung einiger Anschlüsse, z. B. eines Telekom CompanyFlex SIP-Trunk, ist nur in der **Ansicht Experte** oder **Vollzugriff** im Menü **VoIP** möglich. Ist einer dieser Anschlüsse angelegt, darf er nicht über die Assistenten verändert werden, da die Konfiguration dadurch nicht mehr funktionsfähig wäre.

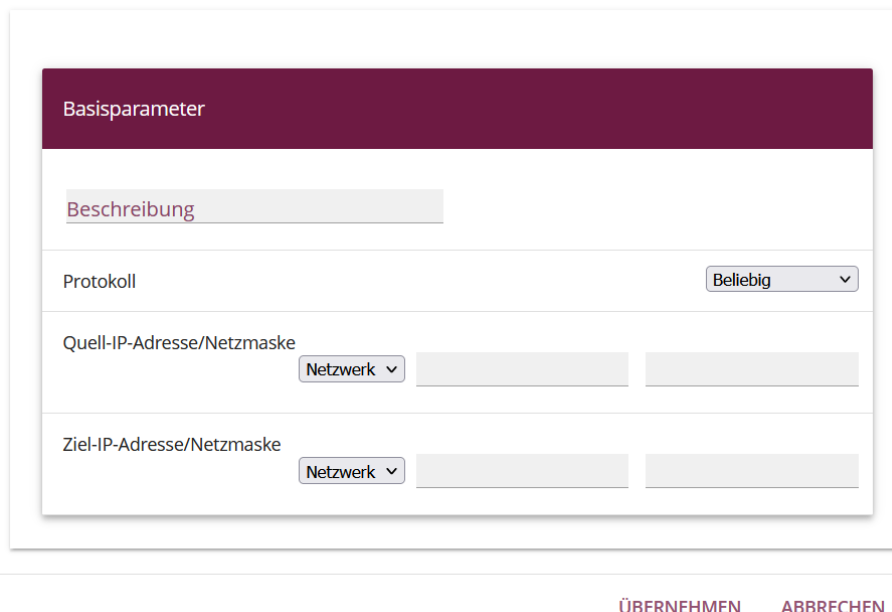
4 Anhang

4.1 Erweiterte Konfiguration von IKEv2-basierten IPSec Peers

Um sicherzustellen, dass bei auf IKEv2 basierenden IPSec-Verbindungen die Aushandlung Verbindungsparameter fehlerfrei funktioniert, empfiehlt es sich die im Folgenden beschriebenen Einstellungen vorzunehmen.

4.1.1 Festlegung des zu tunnelnden Datenverkehrs

Es ist sinnvoll, den Datenverkehr, der tatsächlich über den Tunnel gesendet werden soll, möglichst präzise festzulegen. Dazu können Sie im Menü **VPN > IPSec > IPSec-Peers > Bearbeiten > Zusätzlicher Filter des IPv4-Datenverkehrs** eine Eingrenzung des Ziel- und des Quellnetzes vornehmen:



The screenshot shows a configuration window titled "Basisparameter". It contains the following fields:

- Beschreibung**: A text input field.
- Protokoll**: A dropdown menu currently showing "Beliebig".
- Quell-IP-Adresse/Netzmaske**: A section with a "Netzwerk" dropdown menu and two adjacent text input fields.
- Ziel-IP-Adresse/Netzmaske**: A section with a "Netzwerk" dropdown menu and two adjacent text input fields.

At the bottom right of the window, there are two buttons: "ÜBERNEHMEN" and "ABBRECHEN".

Stellen Sie in diesem Menü sicher, dass die über den Tunnel verbundenen Netze alle IP-Adressen umfassen, die Zugriff auf das entfernte Netzwerk haben sollen, und ebenso alle Adressen, die dort erreicht werden sollen.

Diese Einstellungen sind immer sinnvoll, unabhängig davon, ob im Abschnitt **Erweiterte IPSec-Optionen** der **Startmodus** *Auf Anforderung* oder *Immer aktiv* ausgewählt ist.

4.1.2 Startmodus

Bei IPSec-Verbindungen, die dauerhaft aktiv sein müssen und bei denen der bintec-elmeg-Router die Verbindung initiiert, empfiehlt es sich, den **Startmodus** des Peers im Menü **VPN > IPSec > IPSec-Peers > Bearbeiten > Erweiterte Einstellungen** auf den Wert *Immer aktiv* zu setzen, um einen eindeutigen Zustand der IPSec-Schnittstelle zu gewährleisten:

4.1.3 Eindeutige Rollenverteilung zwischen Client und Server

Bei der Konfiguration einer IPSec-Verbindung sollten Sie stets auf eine klare Rollenverteilung der beiden IPSec-Verbindungspartner (Initiator- oder Responder-Rolle) achten. Dies ist sowohl für den anfänglichen Verbindungsaufbau als auch für die periodische Neuaushandlung der IPSec-Verbindung wichtig.

Achten Sie daher bei der Konfiguration der **Lebensdauer** im Phase-1- und im Phase-2-Profil darauf, dass der eingestellte Wert auf Initiator-Seite kürzer ist als auf Responder-Seite. So können Sie z. B. für die Phase-1-Lebensdauer des Initiators zwei Drittel der Phase-1-Lebensdauer des Responders einstellen. Verfahren Sie ebenso für die Phase-2-Lebensdauer.

Aufgrund der asymmetrischen Konfiguration der Lebensdauer und der damit verbundenen klaren Rollenverteilung können Sie Kollisionen bei der sich periodisch wiederholenden Neuaushandlung der IPSec-Verbindung vermeiden.

Sie finden die Einstellungen in folgenden Menüs:

- **Internet & Netzwerk > VPN > IPSec > Phase-1-Profile > Bearbeiten**

Lebensdauer

14400 Sekunden / Schlüssel erneut erstellen nach 80

% Lebensdauer

Stellen Sie die Werte so ein, dass die Gültigkeit der Phase-1-Parameter auf dem sich einwählenden Client kürzer ist als auf dem Server.

Achten Sie darauf, dass Sie hier das Profil auswählen, das der betreffende Peer auch tatsächlich verwendet!

- **Internet & Netzwerk > VPN > IPSec > Phase-2-Profile > Bearbeiten**

Lebensdauer

7200 Sekunden 0 kBytes Schlüssel erneut

erstellen nach 80 % Lebensdauer

Stellen Sie die Werte so ein, dass die Gültigkeit der Phase-2-Parameter auf

dem sich einwählenden Client kürzer ist als auf dem Server.

Achten Sie darauf, dass Sie hier das Profil auswählen, das der betreffende Peer auch tatsächlich verwendet!

Die Gültigkeit der Phase 1 sollte die der Phase 2 deutlich übersteigen!