Release Notes
System Software 10.2.9

Inhalt

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 10.2.9 Patch 3

1.1 Sicherheitsrelevante Änderungen

- Unter dem Namen **FragAttacks** ist eine Reihe von Sicherheitsmängeln entdeckt worden, die auf grundlegenden Schwächen der WLAN-Standards beruhen. Release 10.2.9 Patch 3 ist gegen Angriffe auf Basis dieser Sicherheitsmängel abgesichert.

1.2 Änderungen

- Die IPSec-Implementierung ist im Bereich der **IKEv2**-basierten Verbindungen im Bezug auf Stabilität und Interoperabilität verbessert worden. Um ggf. verbleibende Fehlerquellen möglichst auszuschließen, beachten Sie die Empfehlungen zur Konfiguration im Anhang: *Erweiterte Konfiguration von IKEv2-basierten IPSec Peers*.

1.3 Fehlerbehebungen

- **Neustart (# 4218, 4285):** Im Zusammenhang einer IPSec-Verbindung mit einer Scheduler-Konfiguration konnte es zu einem Neustart des Geräts kommen.
- **Kein Internetzugang über VPN Client (# 4400):** Obwohl die IPSec-Verbindung über einen VPN Client korrekt aufgebaut wurde, konnte es vorkommen, dass Zugriff auf das Internet nicht möglich war, wenn der gesamte Datenverkehr des Clients durch den IPSec-Tunnel gesendet wurde.
- **IPSec - Vorübergehend keine Datenübertragung (# 5107):** Es konnte vorkommen, dass bei der Verwendung von IKEv2 in IPSec-Konfigurationen vorrübergehende Unterbrechungen in der Datenübertragung auftraten.
- **Neustart (# 5319):** Wenn beim Aufbau einer mit RSA-Zertifikaten authentisierten IPSec-Verbindung auf der Seite des Responders keine zur Verbindungsanfrage passende Peer ID vorhanden war, konnte es zu einem Neustart des Geräts auf Responder-Seite kommen.

- **SIP-Verbindung inaktiv (# 4378):** Wenn eine Verbindung mithilfe von „SIP OPTIONS“-Nachrichten aufrechterhalten werden sollte, konnte es vorkommen, dass dies nicht erfolgreich war.
- **Verbindung nicht möglich (# 5098):** Im Betrieb als Media Gateway konnte es beim Anschluss von Endgeräten am ISDN-Port vorkommen, dass bei hoher Auslastung keine Verbindungen mehr möglich waren.
- **Neustart (# 5199):** Im Betrieb als Telefonanlage konnte es zu gelegentlichen Neustarts kommen.
- **Hohe Systemlast (#5113):** Es konnte im Betrieb des Geräts als WLAN Controller zu eine hohen Auslastung des Geräts kommen.

2 Release 10.2.9 Patch 2

2.1 Änderungen

- **Automatische Amtsholung bei Rückfrage:** Bisher war es notwendig für eine Rückfrage an eine externe Rufnummer auch dann eine führende *0* zu wählen, wenn eine automatische Amtsholung eingerichtet war. Für VoIP-Telefone ist dieses Verhalten mit Release 10.2.9 Patch 2 geändert worden: Eine ggf. für den Benutzer eingerichtete automatische Amtsholung wird auch bei einer Rückfrage nach extern ausgeführt.
- **SIP ohne Registrierung:** Bei Verwendung einer SIP-Verbindung ohne Registrierung kam es zu Problemen mit eingehenden Rufen, wenn die Verbindung über ein vorgeschaltetes Gateway hergestellt wurde, da SIP Header eine interne IP-Adresse enthielten. Mit Release 10.2.9 Patch 2 wird die öffentliche Adresse übertragen.

2.2 Fehlebehebungen

- **Sporadische Neustarts (# 4957, 4958, 5073):** Bei der Verwendung von IKEv2 konnte es zu sporadischen Neustarts kommen.

3 Release 10.2.9 Patch 1

3.1 Änderungen

Die Version 4 des CloudNetManager wird unter einer neuen Adresse gehostet. Das Release 10.2.9 Patch 1 verwendet die neue Adresse (https://bintec.cloudnetmanager.com) und aktualisiert sie in bestehenden Installationen. Der bisherige CloudNetManager (https://bintec.networkcloudmanager.com) kann nicht mehr genutzt werden.

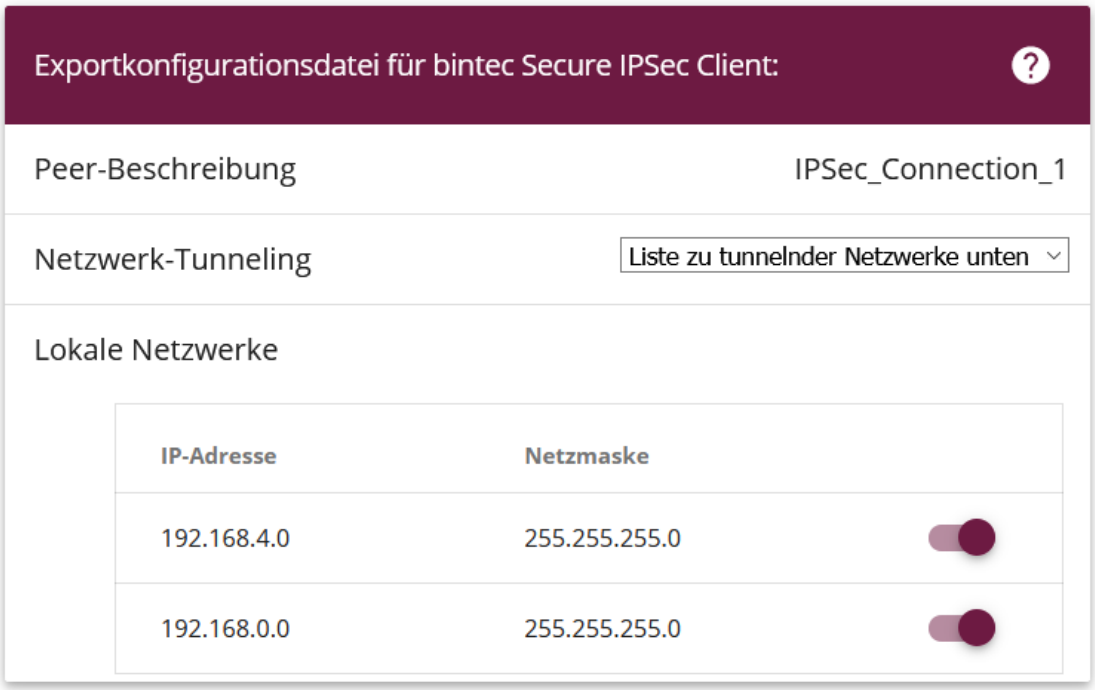
Falls Sie den neuen CloudNetManager Version nutzen möchten, stellen Sie vor dem Einspielen des neuen Release sicher, dass Sie einen Benutzerkonto und die notwendigen Lizenzen haben.

4 Release 10.2.9.100

4.1 Neue Funktionen

4.1.1 Split Tunneling für IPSec Client

Wenn Sie mit dem VPN-Konfigurationsassistenten eine Konfiguration für eine Client-Einwahl erstellen, haben Sie beim Export der Konfiguration für den bintec elmeg Secure Client nun die Möglichkeit, entweder alle oder nur ausgewählte Netzwerke über das VPN zugänglich zu machen:



Split Tunneling wird nicht aktiviert, wenn in der Liste der Netzwerke keine Auswahl getroffen wird.

4.1.2 Unterstützung für W2022ax und W2044ax

Der Wireless LAN Controller unterstützt die kommenden WiFi6 Access Points W2022ax und W2044ax. Der Standard-Kanalplan im 5GHz-Band stellt alle Indoor-Kanäle zur Verfügung (36, 40, 44, 48, 52, 56, 60, 64).

4.1.3 Erweiterte Anzeige

Im Menü **Wireless LAN Controller > Access Point Konfiguration > Bearbeiten** erfolgt eine erweiterte Anzeige der von den Funkmodulen eines Access Points unterstützten Funktionen:

Funkmodul 1 unterstützte Funktionen	Frequenzband: 2,4 GHz or 5 GHz @ ETSI Bandbreite: 20 MHz, 40 MHz (Nur 5 GHz) Drahtloser Modus: 802.11a/b/g/n Spatial Streams: 2x2 Data-Rate Trimming: Nein | WPA 3: Nein

4.1.4 Access Point Steering

Bei der Konfiguration des **Client Steering** im Menü **Wireless LAN Controller > Access Point Konfiguration > Drahtlosenetzwerke > Neu/Bearbeiten** steht die Option **AP Steering** (Access Point Steering) zur Verfügung. Diese veranlasst einen Client mit einer schlechten Verbindung nicht nur das Frequenzband zu wechseln, sondern sich ggf. bei einem anderen Access Point anzumelden, der eine bessere Verbindung zur Verfügung stellen kann.
Diese Funktion setzt die Aktivierung von 802.11k/v voraus.

4.1.5 Erweiterte Auswahl an Kanalplänen

Bei der Konfiguration von Access Points über den Wireless LAN Controller steht im Menü **Wireless LAN Controller > Access Point Konfiguration > Funkmodulprofile > Neu/Bearbeiten** eine erweiterte Auswahl an vordefinierten Kanalplänen zur Verfügung:

- *Alle*: Alle Kanäle können bei der Kanalwahl gewählt werden.
- *World Mode* (für Frequenzband = 2,4 GHz, Standardwert): Die automatische Kanalauswahl verwendet nur die überlappungsfreien Kanäle 1, 6, 11.
- *ETSI-Modus* (für Frequenzband = 2,4 GHz): Die automatische Kanalauswahl verwendet nur die überlappungsfreien Kanäle 1, 5, 9, 13.
- *Keine Wetterradarkanäle* (für Frequenzband = 5 GHz, Standardwert): Die Wetterradarkanäle sind von der Kanalwahl ausgeschlossen. Zur Verfügung stehen die Kanäle 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140.
- *Indoors No DFS/TPC* (für Frequenzband = 5 GHz): Diese Kanäle können innerhalb von Gebäuden verwendet werden. DFS (Dynamic Frequency Selection) und TPC (Transmitter Power Control) kommen dabei nicht zum Einsatz. Zur Verfügung stehen die Kanäle 36, 40, 44, 48.
- *Keine Outdoor-Kanäle* (für Frequenzband = 5 GHz): In diesem Kanalplan sind die nur für Indoor-Anwendungen freigegebenen Kanäle 36 bis 64 zusammengefasst. Mit diesem Kanalplan können insbesondere 5GHz-WLAN-fähige Multimedia-Geräte wie Smart TVs optimal in das WLAN-Netz eingebunden werden, die häufig die 5GHz-Outdoor-Kanäle (ab Kanal 100) nicht unterstützen.
- *Benutzerdefiniert*: Wählen Sie die gewünschten Kanäle selbst aus.

4.1.6 Kanalwechsel bei Störungen

Im Menü **Wireless LAN Controller > Access Point Konfiguration > Funkmodulprofile Neu/Bearbeiten > Erweiterte Einstellungen** können Sie nun die Option **Bei Störung Kanal wechseln** aktivieren. Access Points, die von

Funkinterferenzen im ursprünglich ausgewählten Kanal betroffen sind, wechseln dann ggf. den Kanal.

4.1.7 Erweitertes Umgebungs-Monitoring

Dem Umgebungs-Monitoring im Menü **Wireless LAN Controller** wurde das Untermenü **Eigene Access Points** hinzugefügt. Dieses Menü zeigt Informationen über die vom Controller verwalteten Access Points an, wie diese sich gegenseitig "sehen". Dies liefert nützliche Informationen über das von den verwalteten Access Points gebildete Netzwerk und hilft Ihnen bei der Identifizierung potenzieller WLAN-Probleme.

Das Menü enthält Informationen wie den Namen des Access Points, den Kanal, auf dem er arbeitet, seine Signalstärke und wann er von welchem Access Point und auf welchem Kanal zuletzt gesehen wurde.

4.2 Änderungen

- Wenn das interne Funkmodul nicht über den WLAN Controller eingerichtet und verwaltet wird, ist im Menü **WLAN > Verwaltung > Grundeinstellungen** der Regulierungsbereich mit ETSI vorbelegt und kann nicht geändert werden, da bintec-elmeg-Geräte für diesen Bereich zertifiziert sind. Entsprechend stehen für die Option **Region** nur die ETSI-Staaten zur Verfügung.
- Im Menü **Wireless LAN Controller > Controller-Konfiguration** können Sie für den **Regulierungsbereich** zwischen *ETSI* und *Sonstige* wählen. Für die **Region** stehen dann entsprechende Staaten zur Auswahl.
  Diese Information wird in den Beacons übertragen.
- Zur besseren Unterstützung einer WLAN-Konfiguration durch den WLAN Controller ist die **DHCP CAPWAP Option** in den Geräten der be.IP-Serie bereits in der Standardkonfiguration enthalten.
- Es war bisher nicht möglich, im **WLAN-Assistenten** das Frequenzband des integrierten WLAN-Funkmoduls auszuwählen. Wenn ein Gerät nur über ein Modul verfügt, wurde immer das 2,4-GHz-Profil verwendet, und die Einstellung musste ggf. im Menü des WLAN Controller angepasst werden. Diese Möglichkeit besteht nun direkt im Assistenten.

4.3 Fehlerkorrekturen

- **ER# 4905:** Es war nicht möglich, die letzte einem Funkmodul zugeordnete SSID zu löschen, auch wenn diese nicht benötigt wurde.
- **ER# 4832:** Ein DECT160 wurde im GUI nach der Einbindung als DECT210 angezeigt.
- **ER# 4787:** Bei der Verwendung von PPTP mit MPPE konnte es zu einem Neustart des Geräts kommen.
- **ER# 4869:** Beim Betrieb einer be.IP als Media Gateway konnte es vorkommen, dass Rufweiterleitungen oder T.38-Faxverbindungen fehlschlugen.
- **ER# 3743:** Es konnte vorkommen, dass beim IKEv2 Child SA Rekeying die bestehenden SAs nicht vollständig abgebaut wurden und es so zu nicht funktionsfähigen IPSec-Verbindungen kam.

- **ER# 4596:** Bei der Verwendung von LISP konnte es vorkommen, dass Verbindungen bei einer Statusänderung von Schnittstellen nicht mehr funktionsfähig waren.
- **ER# 4835:** Es konnte zu Neustarts des Geräts bei der Aktivierung von IPsec-Verbindungen kommen.
- **ER# 1478:** Ein SNMP Walk von der Windows Power Shell aus konnte zu einem Blockieren des Geräts führen und einen Neustart erforderlich machen.
- **ER# 4594:** Aufgrund einer falschen Berechnung der an der WAN-Schnittstelle verfügbaren Bandbreite konnte es vorkommen, dass eingehende Rufe abgewiesen wurden.
- **ER# 4665:** Einige Access Points und Router meldeten dem WLAN Controller im Umgebungs-Monitoring Access Points mit WPA2-Enterprise-Verschlüsselung fälschlicherweise als ungesichert.
- **ER# 4689:** Nach einer Unterbrechung der Internetverbindung konnte es unter Umständen sehr lange dauern, bis eine bestehende IPSec-Verbindung wiederhergestellt werden konnte.
- **ER# 2050, 3371, 4416, 4439, 4889:** Es konnte zu sporadischen Neustarts und gelegentlich auch zu einem „Boot Loop“ kommen, bei dem das Gerät kontinuierlich neu startete.
- **ER# 4283:** Wenn ein IPSec Multi Peer für die Einwahl in ein Zielnetzwerk verwendet wurde, so wurde an zwei sich verbindenden Clients die gleiche IP-Adresse vergeben, wenn diese in ihren jeweiligen lokalen Netzwerken die gleiche interne IP-Adresse hatten.
- **ER# 4295:** Wenn der WLAN Controller aktiv war und Kontrolle über die VLAN-Einstellungen der Bridge-Schnittstelle hatte, waren weitere, im Menü **LAN > IP-Konfiguration** angelegte VLANs nicht funktionsfähig.
- **ER# 3419:** Es konnte vorkommen, dass es nicht möglich war dem System ein Telefon hinzuzufügen, wenn eine VPN-Verbindung aktiv war. Der Vorgang schlug mit der Meldung „Globaler Fehler / Der Wert muss größer oder gleich...“ fehl.
- **ER# 4056:** Bei der Freigabe von Anruflisten und Telefonbuch konnte es zu Problemen kommen. Unter bestimmten Umständen mussten diese Listen mehrmals freigegeben werden.

4.4 Bekannte Einschränkungen

- Der Access Point W2003ac akzeptiert lediglich Verbindungen von 47 Clients, auch wenn die Option **Hard Limit** höher eingestellt ist.

5 Anhang

5.1 Erweiterte Konfiguration von IKEv2-basierten IPSec Peers

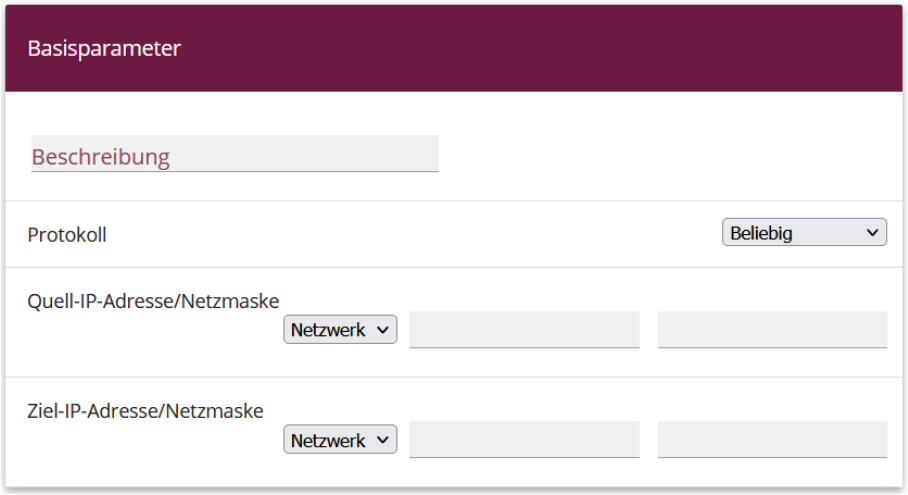
Release 10.2.9 Patch 3 beseitigt eine Ursache möglicher Probleme bei der Aushandlung IKEv2-basierter IPSec-Verbindungen. Bisher bestimmt ausschließlich die im IPSec Peer konfigurierte Route, welche IP-Daten über die IPSec-Verbindung übertragen werden. Dieser auf Routen basierende Ansatz zur Bestimmung der bei

der IPSec-Aushandlung auszutauschenden sogenannten Traffic-Selektoren ist häufig zu unscharf und führt daher unter Umständen zu Stabilitäts- und Interoperabilitätsproblemen.

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

5.1.1 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 **Internet & Netzwerk > VPN > IPSec > IPSec-Peers > Bearbeiten > Zusätzlicher Filter des IPv4-Datenverkehrs** eine Eingrenzung des Ziel- und des Quellnetzes vornehmen:

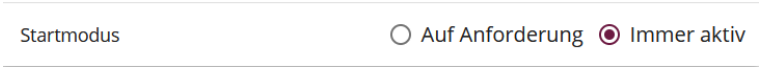


Stellen Sie in diesem Menü sicher, dass die über den Tunnel verbundenen Netze alle IP-Adressen umfassen, die Zugriff auf das entfernte Netzwerk haben sollen, und ebenso alle Adressen, die dort erreicht werden sollen.

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

5.1.2 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 **Internet & Netzwerk > VPN > IPSec > IPSec-Peers > Bearbeiten > Erweiterte IPSec-Optionen** auf den Wert *Immer aktiv* zu setzen, um einen eindeutigen Zustand der IPSec-Schnittstelle zu gewährleisten:



5.1.3 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-

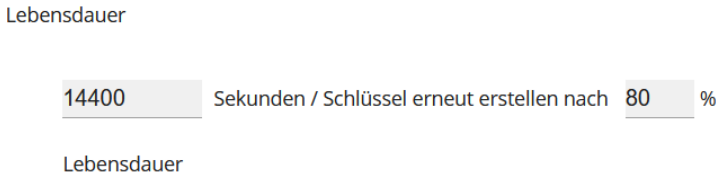
Rolle) achten. Dies ist sowohl für den anfänglichen Verbindungsaufbau als auch für die periodische Neuaushandlung der IPSec-Verbindung wichtig.

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.

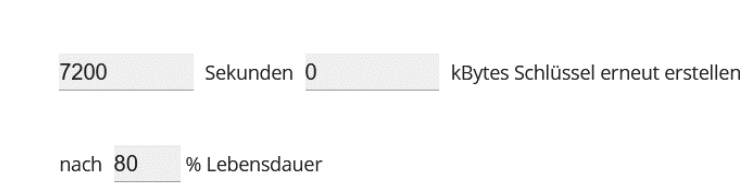
Aufgrund der asymmetrischen Konfiguration der Lebensdauer und der damit verbundenen klaren Rollenverteilung können Sie Kollisionen bei der sich periodisch wiederholenden Neuaushandlung der IPSec-Verbindung vermeiden.

Sie finden die Einstellungen in folgenden Menüs:

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

  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**

  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!