Release Notes
System Software 10.2.8

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 zwingend das aktuelle Release verwenden, da FlashStart im Mai die Server umstellt. Ohne Update funktionieren die Suchmaschinenanfragen (z. B. Google) nicht mehr.

1 Release 10.2.8.101

1.1 Probleme bei IKEv2-basierten IPSec-Verbindungen

Mit neueren Versionen von Apples Betriebssystemen iOS (aktuell 13.5.1) und macOS (aktuell 10.15.5) kommt es zu Abbrüchen von IKEv2-basierten IPSec-Verbindungen. Das Problem tritt nach dem zunächst erfolgreichen Aufbau einer IPSec-Verbindung von einem Apple Client zu einem bintec-elmeg-Gerät bei der Neuaushandlung des zur Datenverschlüsselung verwendeten Schlüssels, dem sog. „Rekeying“, auf.

Das Problem betrifft nur das Aufrechterhalten einer IPSec-Verbindung und tritt auch während aktiver Nutzung der Verbindung auf. Eine abgebrochene Verbindung kann jederzeit seitens des Clients neu aufgebaut werden. IKEv1-basierte Verbindungen sind nicht betroffen.

Release 10.2.8 Patch 1 behebt einen der zugrunde liegenden Fehler auf Seiten unserer Systemsoftware, kann aber leider die beschriebenen Probleme nicht völlig beheben, da derzeit keine ausreichenden technischen Informationen zu den von Apple vorgenommenen Änderungen vorliegen. Wir untersuchen den Sachverhalt weiterhin und werden ggf. neue Informationen oder Releases veröffentlichen.

Um eine stabilere Verbindung zu ermöglichen bzw. das Auftreten des Problems zu umgehen, können Sie die beiden folgenden Ansätze verfolgen.

1.1.1 Anpassung der Router-Konfiguration

Für iOS-Geräte erzielen Sie die besten Ergebnisse, wenn Sie im für den Peer verwendeten Phase-1-Profil die **DH-Gruppe** auf *5 (1536 Bit)* einstellen und im Phase-2-Profil die Option **PFS-Gruppe verwenden** deaktivieren.

Hinweis:
Achten Sie in allen Fällen darauf, dem entsprechenden Peer die passenden Profile im Menü VPN > IPSec > IPSec-Peers > <Ihr Peer> > Erweiterte Einstellungen zuzuweisen.

Leider ist auch diese Einstellung nicht völlig zuverlässig und führt bei Geräten mit macOS nicht zum Erfolg.

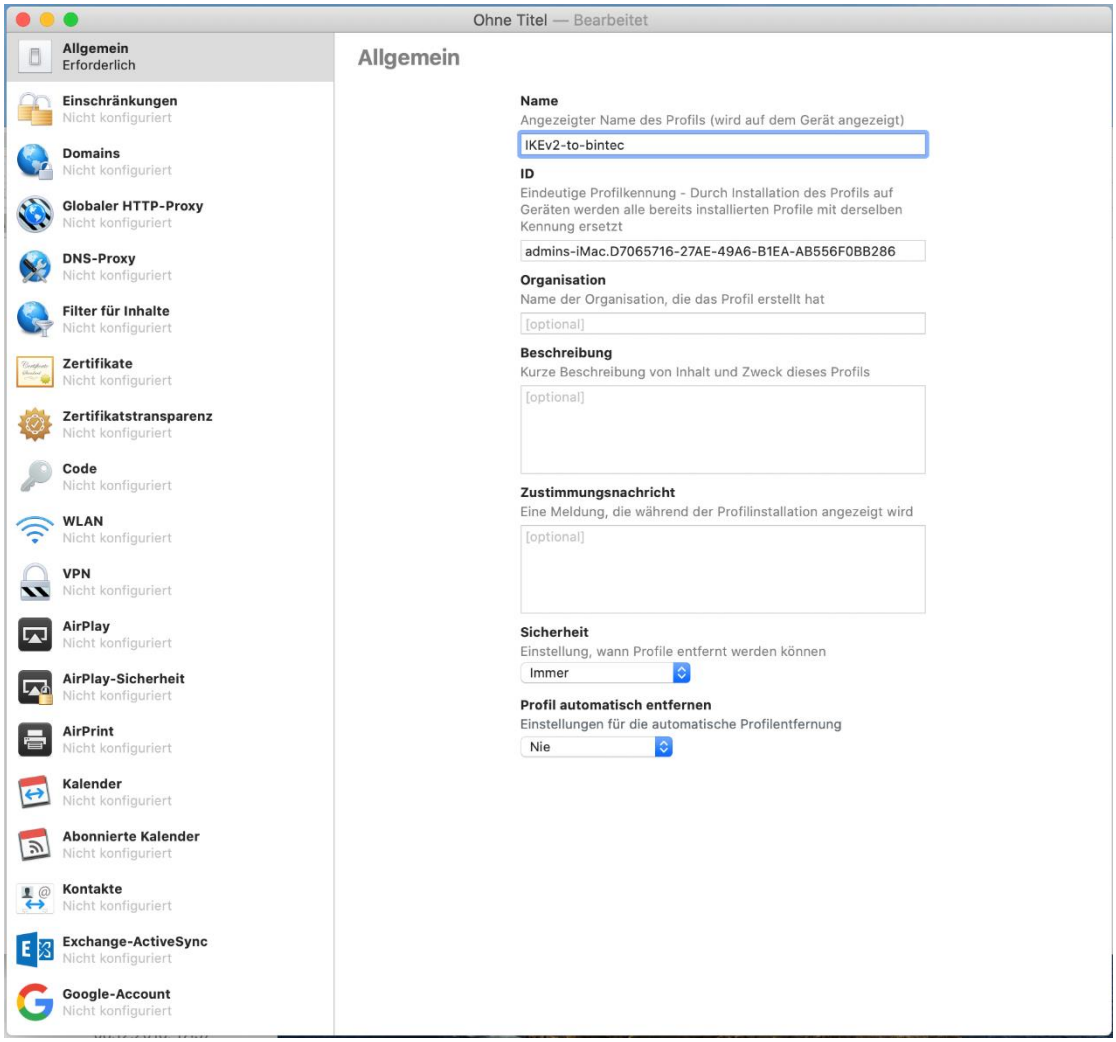
1.1.2 Erweiterte Konfiguration des Apple Clients

Mithilfe des **Apple Configurator 2** ist es möglich, die Konfiguration eines Apple IPSec Client so zu erstellen, dass das Rekeying erst nach langer Zeit erfolgt und daher während dieser Zeit nicht zu einem Abbruch der Verbindung führt. Diese angepasste Konfiguration können Sie direkt auf einem macOS-Gerät einsetzen, aber auch auf ein iOS-Gerät exportieren.

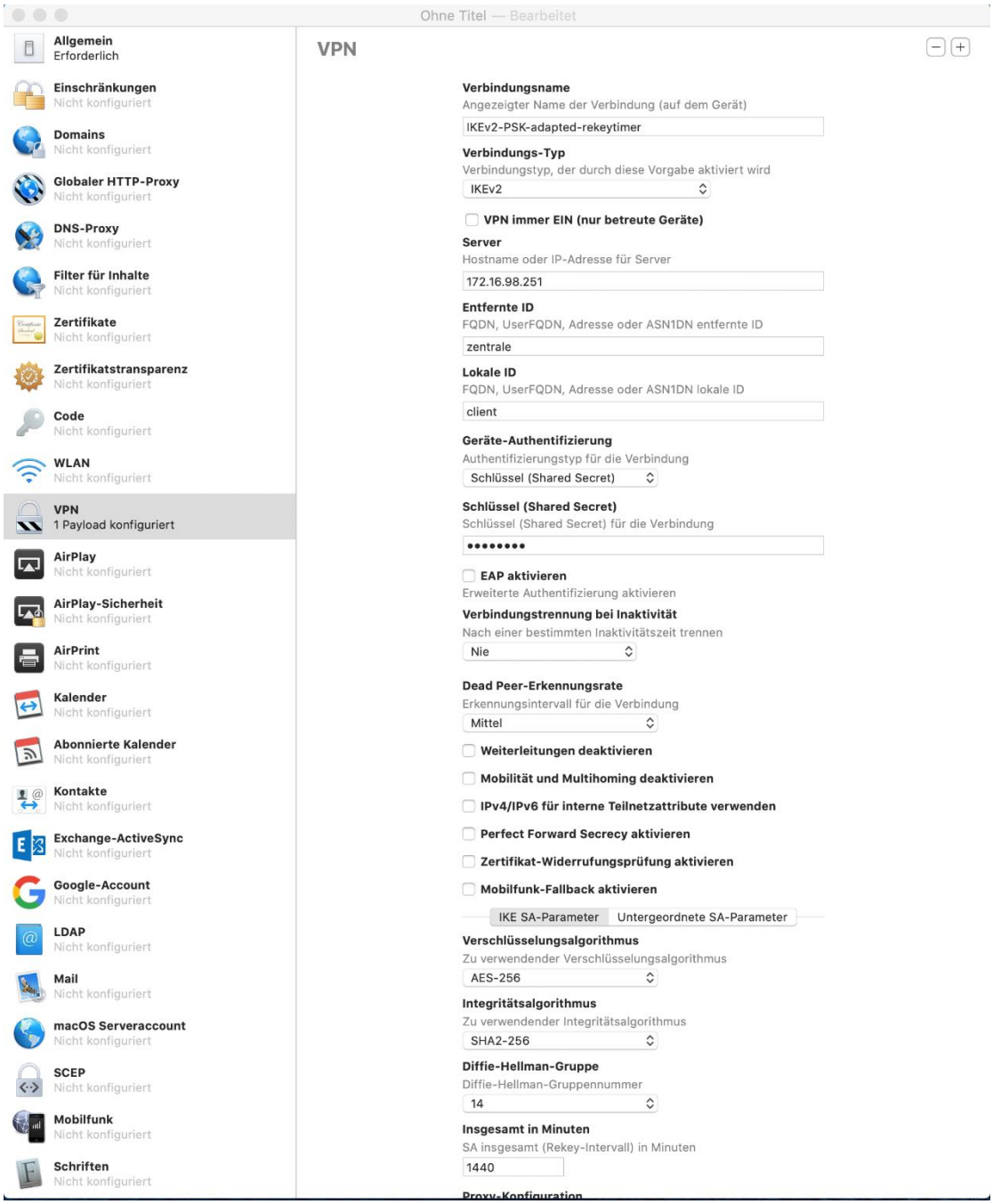
Gehen Sie zum Erstellen der Konfiguration wie folgt vor:

1. Installieren und öffnen Sie den **Apple Configurator 2**:

2. Drücken Sie **Command + n**, um ein neues Profil zu erstellen. In dem sich öffnenden Fenster, vergeben Sie im Abschnitt **Allgemein** einen Namen für das zu erstellende Profil, in unserem Beispiel *IKEv2-to-bintec*:



3. Nehmen Sie im Abschnitt VPN die folgenden Einstellungen vor:

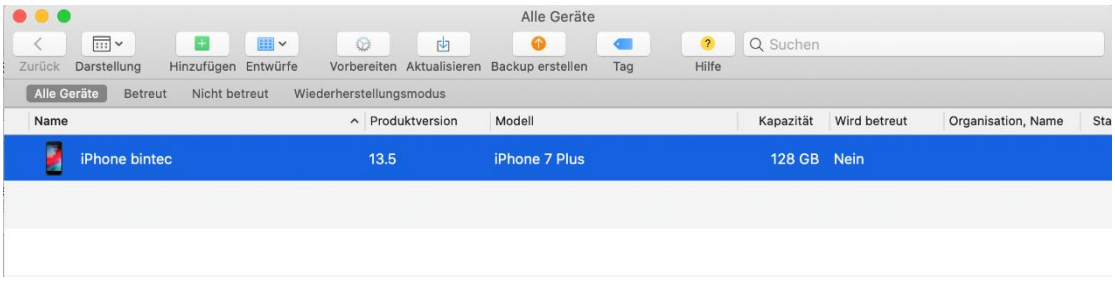


Passen Sie dabei die Einstellungen wie den **Server**, die **Lokale ID** und den **Schlüssel** an Ihre Erfordernisse – wie die Konfiguration des Peers auf Ihrem bintec-elmeg-Gerät – an.
Achten Sie darauf, den Wert für die Option **Insgesamt in Minuten** entsprechend Ihrer Bedürfnisse ggf. hoch zu wählen. Dieser legt fest, wann ein Rekeying stattzufinden hat. In unserem Beispiel ist der Wert auf *1440* Minuten (24 Stunden) gesetzt.

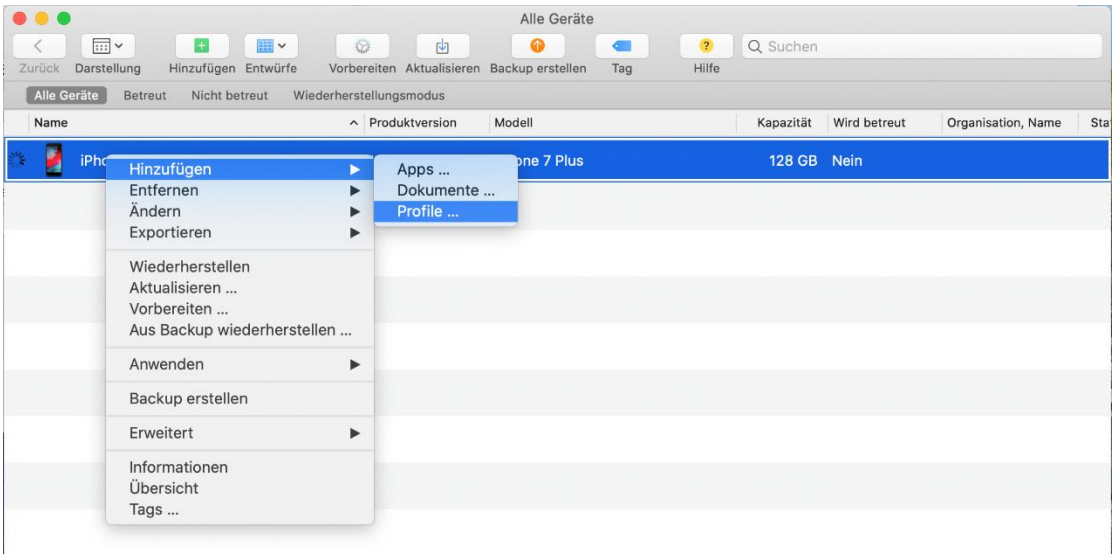
4. Mit der Tastenkombination Command + s können Sie das Profil z. B. im Ordner **Dokumente** speichern und anschließend mit einem Doppelklick auf dem macOS-Gerät aktivieren.

Um den Vorteil des verlängerten Rekeying-Intervalls auch auf einem iOS-Gerät nutzen zu können, können Sie das erstellte Profil exportieren. Gehen Sie dazu folgendermaßen vor:

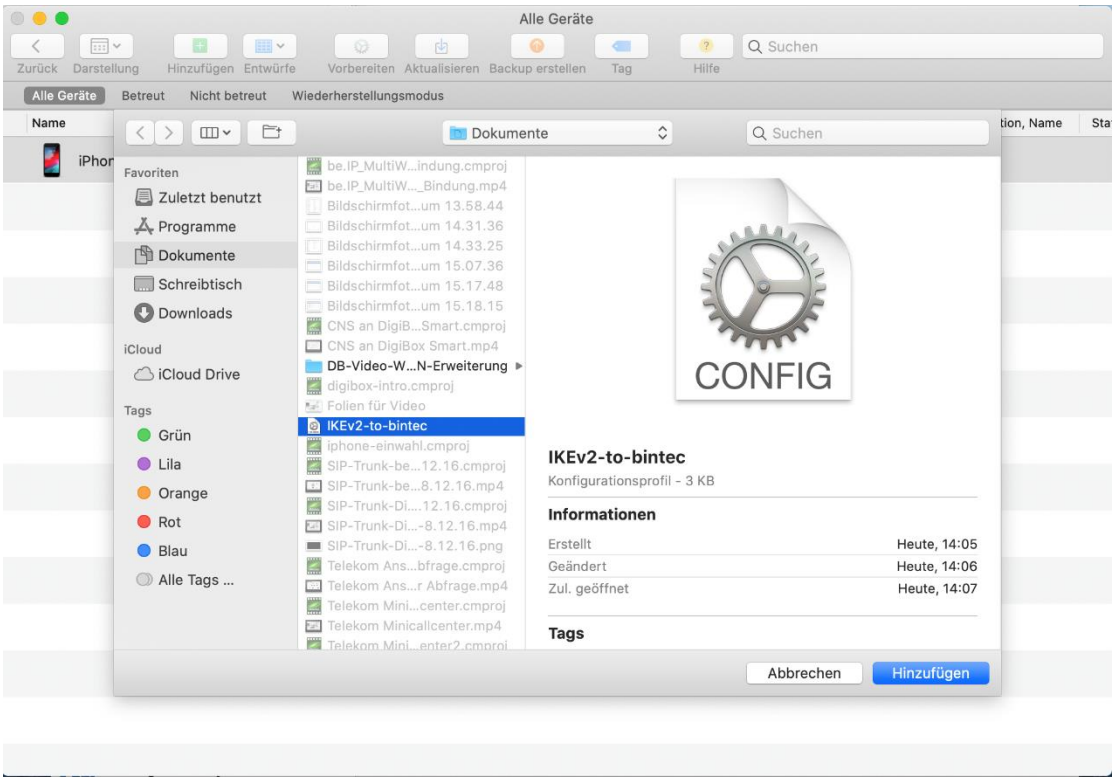
1. Verbinden Sie das iOS-Gerät mit dem macOS-Gerät, auf dem das Profil gespeichert ist. Bestätigen Sie den Geräte-Code.



2. Wechseln Sie mit einem rechten Mausklick (CTRL-Klick) in das Menü **Hinzufügen > Profile**:



3. Übertragen Sie das zuvor erstellte Profil *IKEv2-to-bintec* auf das iOS-Gerät. Folgen Sie den Anweisungen auf dem Bildschirm:



4. Im Anschluss können Sie das importierte Profil zum Aufbau einer IPSec-Verbindung nutzen.

1.2 Fehlerkorrekturen / Workarounds

- **IPSec – Verbindungsabbruch (#4286):** Aufgrund einer von bintec-elmeg-Geräten nicht beantworteten *Informational Request* konnte es zum Abbruch von IPSec-Verbindungen kommen.
- **DS Lite – Quell-IP-Adresse nicht abrufbar (#3397):** An DS-Lite-Anschlüssen konnte keine IPv4-Quelladresse ermittelt werden. Daraufhin kam es zu Problemen beim Versenden von Nachrichten des Voice Mail Systems.

2 Release 10.2.8.100

2.1 Neue Funktionen

2.1.1 WLAN - Verschlüsselungsstandard WPA3

- Mit dem Release wird der Verschlüsselungsstandard **WPA3** im Wireless LAN Controller in Verbindung mit **bintec W2022ac** Access Points ab Firmware 2.4.1.1 unterstützt. Ältere bintec APs und das interne WLAN der bintec Router unterstützen WPA3 nicht.
  WPA3 dient dazu, die Sicherheit in WLAN-Netzen zu verbessern. Im Menü **Wireless LAN > WLAN > Drahtlosnetzwerke (VSS) > Neu** im Bereich

Sicherheitseinstellungen finden Sie neue Einstellmöglichkeiten. Die Einstellungen **Sicherheitsmodus** = *OWE* und **Sicherheitsmodus** = *OWE-Transition* sind für offene Netze geeignet.
OWE (Opportunistic Wireless Encryption) funktioniert ausschließlich mit WPA3-fähigen Clients, bei denen OWE implementiert ist. Die Datenübertragung zwischen Access Point und Client ist verschlüsselt.
OWE-Transition bietet sich für Netze an, die von WPA3-fähigen Clients, aber auch von älteren, nicht WPA3-fähigen, Clients genutzt werden sollen. Bei Clients, die WPA3 unterstützen, erfolgt die Datenübertragung zwischen Access Point und Client verschlüsselt, bei allen anderen unverschlüsselt.
Mit **Sicherheitsmodus** = *WPA-PSK* oder **Sicherheitsmodus** = *WPA-Enterprise* können Sie **WPA-Modus** = *WPA3* für WPA3-fähige Clients einstellen oder **WPA-Modus** = *WPA2 und* WPA3 wählen, um WPA2- und WPA3-fähige Clients im selben Netz zu verwenden.

- Folgende Menüs sind betroffen:
  Assistenten -> WLAN
  Wireless LAN Controller -> Wizard
  Wireless LAN Controller -> Slave-AP-Konfiguration -> Slave Access Points
  Wireless LAN Controller -> Slave-AP-Konfiguration -> Drahtlosnetzwerke (VSS)
- Im Menü **Wireless LAN Controller > Controller-Konfiguration > Slave-AP-Autoprofil > Bearbeiten** finden Sie einen Hinweis, dass WPAv3-Profile nicht auf allen Access Points verfügbar sind.

2.1.2 WLAN Standard 802.11r/k/v

- Im Wireless LAN Controller werden die WLAN-Standards 802.11r/k/v in Verbindung mit den bintec W2022ac Access Points ab Firmware 2.4.1.1 unterstützt:
  - **Schneller BSS-Übergang (802.11r)**
    802.11r (Fast BSS Transition, FT) ist ein Mechanismus, mit dem ein WLAN Client beim Wechseln des Access Points eine bestehende WPA Verschlüsselung schneller wiederherstellen kann, als dies bei einer vollständigen Authentifizierung der Fall wäre. Mit Hilfe des 802.11r-Protokolls wird dieser Vorgang und somit die Unterbrechung des Datenverkehrs beim Wechsel zu einem anderen Access Point verkürzt. 802.11r wird bei WPA2-PSK, WPA3-SAE, WPA2-Enterprise und WPA3-Enterprise unterstützt. 802.11r wird nicht von allen bintec Access Points unterstützt.
  - **Verwaltung der Funkressourcen (802.11k)**
    Bei aktivierten 802.11k senden WLAN Clients dem Access Point Informationen über ihre Funktionalität (2,4/5GHz Support, ….) und Informationen über weitere Access Points in der Umgebung.
    Diese Informationen helfen dem Access Point die besten Roaming-Möglichkeiten für den Client zu finden. 802.11k wird nicht von allen bintec Access Points unterstützt.

- **Netzwerkunterstütztes Roaming (802.11v)**
  Der Access Point sendet einem verbundenen WLAN Client regelmäßig Informationen über weitere Access Points in der Umgebung die für ein Roaming in Frage kommen.
  Diese Informationen helfen dem WLAN Client bessere Roaming-Entscheidungen zu treffen. 802.11r wird nicht von allen bintec Access Points unterstützt.

2.1.3 Dual Stack Lite – AFTR

- Im Menü **WAN > Internet + Einwählen > Dual Stack Lite > Neu** kann die IP-Adresse des AFTR (Address Family Transition Router) nicht nur – wie bisher – als statische Adresse eingegeben sondern auch über DHCP bezogen werden.

2.1.4 Wireless LAN Controller - Monitoring

- Im Menü **Wireless LAN Controller > Monitoring > Aktive Clients** werden in der Übersicht zusätzlich Informationen über das verwendete Band und den Kanal hinzugefügt.

2.2 Änderungen

- **DNS - Bailiwick Check anpassbar (# 3780):** Aufgrund eines strikten Bailiwick Checks konnte es vorkommen, dass die Funktion der sicheren Suche im Webfilter nicht funktionsfähig war. Über die MIB-Variable **ipDnsCheckBailiwick** lässt sich das Verhalten nun anpassen.
- **MGW- Numbering Plan Information geändert (#3942):** Um Probleme mit Avaya Telefonanlagen zu vermeinden, wurde der Parameter Numbering Plan Information (NPI) von *unknown* auf *ISDN numbering plan* geändert.
- **WLAN-Client-Modus (#4048):** In bintec Access Points der neueren n-Serie (W1001n, W1003n usw.) und bintec Routern der RS-Serie wurde für den Betrieb des Geräts im WLAN-Client-Modus das Roaming-Verhalten erheblich beschleunigt.
- **WAN – DSLite (#4205):** Im Menü **WAN > Internet + Einwählen > Dual Stack Lite > Neu** wurden die Parameter **AFTR** in **AFTR-Modus** und **AFTR Gateway** in **Statischer AFTR** umbenannt.
- **Wireless LAN Controller – WPA-Modus (#4186, 4244):** In den Menüs **Wireless LAN Controller > Slave-AP-Konfiguration > Drahtlosnetzwerke (VSS)** und **Wireless LAN Controller > Wizard > Schritt 3 > Bearbeiten** wurden bei den Parametern **Sicherheitsmodus** und **WPA-Modus** in der jeweiligen Dropdown-Liste die wählbaren Werte nach Verschlüsselungsstärke sortiert.
- **Bintec Secure IPSec Client:** In allen bintec Geräten wird ein einheitlicher Bintec Secure IPSec Client verwendet.

2.3 Fehlerkorrekturen

- **Wireless LAN Controller - Drahtlosnetzwerke (VSS) fehlerhaft angezeigt (#2864):** Wenn im Menü **Wireless LAN Controller > Slave-AP-Konfiguration** ein WTP deaktiviert wurde, wurde im Menü **Wireless LAN**

Controller > Monitoring > Drahtlosnetzwerke (VSS) für das entsprechende VSS trotzdem „Activated, channel scan is running. Please wait…“ angezeigt.

- **VoIP - Problem mit RelAix MSN Account (#4064):** Ein Einzelrufnummernanschluss MSN des Anbieters RelAix konfiguriert als MSN SIP Account mit einer einzigen MSN funktionierte nicht.
- **IPSec - Tunnelprobleme (#3743):** Bei Verwendung von IPSec mit IKEv2 konnte es unter bestimmten Umständen bei Verwendung eines Enigmatec Routers als Remote IPSec Gateway zur Blockierung des Tunnels kommen.
- **IPSec - Probleme mit Zertifikaten (#3882, 4157):** Bei Verwendung von IPSec misslang der Aufbau eines Tunnels beim Einsatz von Zertifikaten, da die digitale Signatur nicht verifiziert werden konnte, obwohl sie gültig war.
- **IPSec - Verbindung fehlerhaft (#3920):** Bei hoher Nutzlast konnte es zu einem Abbruch der Verbindung kommen.
- **PPPoE - Falsche Geschwindigkeit (#3873):** Bei einer PPPoE-Verbindung über eine virtuelle Schnittstelle hatte der Uplink immer die Standardgeschwindigkeit von 128K.
- **Voice Mail - Unvollständige Aufzeichnung (# 3869):** An Anschlüssen des Anbieters HFO konnte es dazu kommen, dass Nachrichten an eine Voice Mail Box nur unvollständig aufgezeichnet wurden.
- **DHCP - Renew-Prozess funktionierte nicht korrekt (#3555):** Wenn der DHCP-Client-Modus auf zwei Schnittstellen verwendet wurde, funktionierte der Renew-Prozess nicht korrekt, die IP-Adresse war kurzzeitig verschwunden.
- **CoS - Problem mit IP640 (#3527):** Class-of-Service-Regeln konnten mit Service Codes am elmeg IP640 umgangen werden. Mit einem Service Code über eine Funktionstaste an einem elmeg IP640 konnte z. B. in den Nachtmodus geschaltet werden, obwohl dies über eine Class-of-Service-Regel verboten war.
- **PPTP, L2TP – Menüs im GUI versehentlich angezeigt (#3526):** Die Menüs PPTP und L2TP wurden im GUI angezeigt, obwohl sie nicht Bestandteil des Funktionsumfangs der Geräte waren.
- **Authentifizierung – RADIUS (#3472):** Im Menü **Systemverwaltung > Remote Authentifizierung > RADIUS > Neu > Erweiterte Einstellungen** wurde der Parameter **Neulade-Intervall** fälschlicherweise in Sekunden statt in Minuten angezeigt und es fehlte der Parameterbereich.
- **MGW - CallRouting (#3433):** Im MGW-Modus war Telefonieren nicht möglich, weil nach der Inbetriebnahme keine Standard-Rufnummer gesetzt war. Bei Konvertierung von PBX nach MGW wird künftig auch die Standard-Rufnummer konvertiert.
- **Telefonie – Rufweiterleitung abgebrochen (#3425):** Wenn ein Ruf an ein Mobiltelefon im Netz der Telekom weitergeleitet werden sollte, brach der Ruf ab.
- **Telefonie – Fehler an Anschlüssen der Deutschen Telefon (#3411):** An Einzelanschlüssen der Deutschen Telefon konnte es dazu kommen, dass eingehende Rufe nicht möglich waren.

- **Dual Stack Lite - IPv4 funktionierte nicht (#3868):** Bei Dual Stack Lite mit 1&1 oder M-net funktionierte IPv6, IPv4 jedoch nicht.
- **Telefonie - Anruf als anonym angezeigt (#3189):** Eingehende Rufe von einem Mobiltelefon mit Telekom One Number wurden ungewollt mit unterdrückter Rufnummer angezeigt.
- **Telefonie – Problem beim Rufaufbau (#1903):** Wenn beim Aufbau einer Session ein Invite ohne SDP verwendet wurde, kam es zu Problemen.
- **Wireless LAN Controller - Performance-Probleme (#1780):** Wenn ein Wireless LAN Controller viele Access Points verwaltete, konnte es zu hoher Auslastung der CPU kommen. Nach einiger Zeit wurde die Netzwerkkommunikation immer langsamer bis das WLAN nicht mehr funktionierte.
- **WLAN – Sicherheitsproblem (#4048):** Unter bestimmten Umständen war es möglich, mit Hilfe eines Scripts unverschlüsselte ARP Requests in das LAN eines Access Points zu senden und damit die Performance des LAN zu reduzieren. Dieses Sicherheitsproblem wurde behoben.
- **Telefonie - Zweite MSN nicht erreichbar (#4002):** Wenn bei Konfiguration mehrerer MSNs die erste MSN in Betrieb war, war die zweite MSN nicht erreichbar.
- **MGW – Rufabbruch (#4065):** Bei Geräten mit ISDN konnte es zu Rufabbrüchen kommen.
- **Firewall – Fehlerhafte Anzeige (#3985):** In den Menüs **Firewall > Richtlinien > IPv4-Filterregeln** und **Firewall > Richtlinien > IPv6-Filterregeln** wurden fälschlicherweise leere Klammern angezeigt. Im Syslog wurden NCI-Alert-Fehlermeldungen angezeigt.
- **Wireless LAN Controller - Probleme beim Sicherheitsmodus (#4189, 4190, 4222):** Im Menü **Wireless LAN Controller > Slave-AP-Konfiguration > Drahtlosnetzwerke > Neu** konnte es bei den Sicherheitseinstellungen bei bestimmten Parameterkombinationen zu falschen Voreinstellungen kommen.
- **Wireless LAN Controller - Probleme beim Sicherheitsmodus (#4187):** Wenn bei einem Drahtlosnetzwerk der **Sicherheitsmodus** von *WPA-PSK* auf *WPA Enterprise* geändert wurde, wurde das PSK nicht gelöscht.
- **DSLite – Fehlfunktion (#4206):** Wenn eine statische AFTR-Adresse mit Leerzeichen eingetragen wurde, kam es zu Fehlfunktionen von DSLite.
- **Wireless LAN Controller – Funkmodulprofile nicht gefiltert (#4250):** Im Menü **Wireless LAN Controller > Slave-AP-Konfiguration > Slave Access Points > Bearbeiten** wurden in der Dropdown-Liste **Aktives Funkmodulprofil** mehr Profile angezeigt als die Modulkapazitäten zur Verfügung stellen, d.h. zum Beispiel für Funkmodulprofil 1 ist nur *2.4 GHZ Radio Profile* verfügbar**,** es wurde aber auch *5 GHz Radio Profile* angezeigt.
- **Wireless LAN Controller – Falsche Voreinstellung beim zweiten Funkmodul (#4252):):** Im Menü **Wireless LAN Controller > Slave-AP-Konfiguration > Slave Access Points > Neu** war die Voreinstellung für das zweite Funkmodul *2.4 GHz Radio Profile* statt *5 GHz Radio Profile*.
- **Wireless LAN Controller - Falsche Voreinstellung beim Sicherheitsmodus (#4256):** Im Menü **Wireless LAN Controller > Slave-AP-**

Konfiguration > Drahtlosnetzwerke (VSS) > Neu war unter **Sicherheitsmodus** fälschlicherweise der Wert *Inaktiv* voreingestellt.

- **Wireless LAN Controller - VSS-Profile doppelt (#4197):** Im Menü **Wireless LAN Controller > Wizard** wurden im **Schritt 4** auf der Seite **Bearbeiten** die VSS-Profile den gefundenen Access Point doppelt zugewiesen.
- **Wireless LAN Controller – Verweis nicht korrekt (#4188):** Im Menü **Wireless LAN Controller > Slave-AP-Konfiguration > Drahtlosnetzwerke (VSS)** wurde auf ein englisches Dokument verwiesen, obwohl das Dokument in deutscher Sprache verfügbar ist.
- **PBX – Probleme mit SIP Provider envia TEL (#4208):** Bei Verwendung einer Avaya Telefonanlage und dem SIP Provider envia TEL kam es sporadisch zu einseitigen Sprachverbindungen.
- **VPN – be.IP Secure Client (#4006, 3711):** Im Menü **VPN > be.IP Secure Cient** wurden ein veraltetes Bild, ein veraltetes Logo sowie eine missverständliche Beschreibung angezeigt. Der Link zum Cient war nicht korrekt.
- **Wireless LAN Controller – Falsche Voreinstellungen bei wlcWlanIfProfileTable (#4255):** In der MIB-Tabelle **wlcWlanIfProfileTable** waren Parameter falsch voreingestellt. Das führte unter anderem dazu, dass Access Points standardmäßig ausgeschaltet waren.
- **Wireless LAN Controller – Falsche Funkmodulprofile (#4267):** Im Menü **Wireless LAN Controller > Slave-AP-Konfiguration > Funkmodulprofile > Neu** wurden die Profile statt mit der Einstellung *Indoor* oder *Outdoor* mit der Einstellung *Indoor/Outdoor* erzeugt.
- **Wireless LAN Controller - Slave-AP-Konfiguration (#4250, 4272):** In den Menüs **Wireless LAN Controller > Slave-AP-Konfiguration > Slave Access Points > Bearbeiten** und **Wireless LAN Controller > Wizard** konnten Funkmodulprofile ausgewählt werden, für die das jeweilige Funkmodul nicht geeignet waren.
- **Wireless LAN Controller- Ungültige Konfiguration (DEV:CI 28026):** Wenn im Menü **Wireless LAN Controller > Slave-AP-Konfiguration > Slave Access Points > Bearbeiten** die Seite verlassen wurde ohne ein Drahtlosnetzwerk-Profil zu wählen, wurde eine ungültige Konfiguration erzeugt.
- **Wireless LAN Controller – Kanalfestlegung (#4257):** Im Menü **Wireless LAN Controller > Slave-AP-Konfiguration > Slave Access Points** war eine **Neue Kanalfestlegung** durch Klicken auf **Start** zwar auslösbar, aber der Benutzer war unter Umständen irritiert, weil sich die Anzeige auf dem Bildschirm nicht änderte und keine Meldung angezeigt wurde, dass der Scan läuft.

2.4 Bekannte Probleme

- **Wireless LAN Controller - Probleme mit BOSS-basierten Access Points und WPA3 (#4248):** BOSS-basierte Access Points unterstützen kein WPA3. Wenn ein WPA3-fähiges Drahtlosnetzwerkprofil auf einem BOSS-basierten Access Point ausgerollt wird, zeigt der Wireless LAN Controller in der Regel

einen Warnhinweis an und rollt die inkompatible Konfiguration nicht aus. Unter bestimmten Umständen wird beim Versuch ein WPA3-fähiges Drahtlosnetzwerk auf einem inkompatiblen BOSS Access Point auszurollen dieser Warnhinweis nicht angezeigt, sondern die inkompatible Konfiguration wird auf dem Access Point ausgerollt. In Folge dessen kann es bei diesem Access Point zu unerwarteten und unsicheren Einstellungen kommen.