Release Notes
System Software 10.2.8

Content

Notice

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.

If you intend to use the Web Filter, you must use the current release, because FlashStart will change the servers in May. Without an update, search engine queries (e.g. Google) will no longer work.

1 Release 10.2.8.101

1.1 Problems with IKEv2-based IPSec connections

With newer versions of Apple's operating systems iOS (currently 13.5.1) and macOS (currently 10.15.5), IKEv2-based IPSec connections may get terminated. The problem occurs after the initially successful establishment of an IPSec connection from an Apple client to a bintec-elmeg device during the renegotiation of the key used for data encryption, the so-called "rekeying".

The problem only affects the persistence of an IPSec connection and also occurs during active use of the connection. An aborted connection can be reestablished by the client at any time. IKEv1-based connections are not affected.

Release 10.2.8 Patch 1 fixes one of the underlying errors on the side of our system software, but unfortunately cannot completely resolve the described problems, as there is currently no sufficient technical information available about the changes made by Apple. We are continuing to investigate the issue and will release new information or releases as appropriate.

To provide a more stable connection or to avoid the problem, you can make us of the following two approaches.

1.1.1 Adaptation of the router configuration

On iOS devices, for best results, set the **DH group** to *5 (1536 bits)* in the Phase 1 Profile used for the peer, and disable the **Use PFS group** option in the Phase 2 Profile.

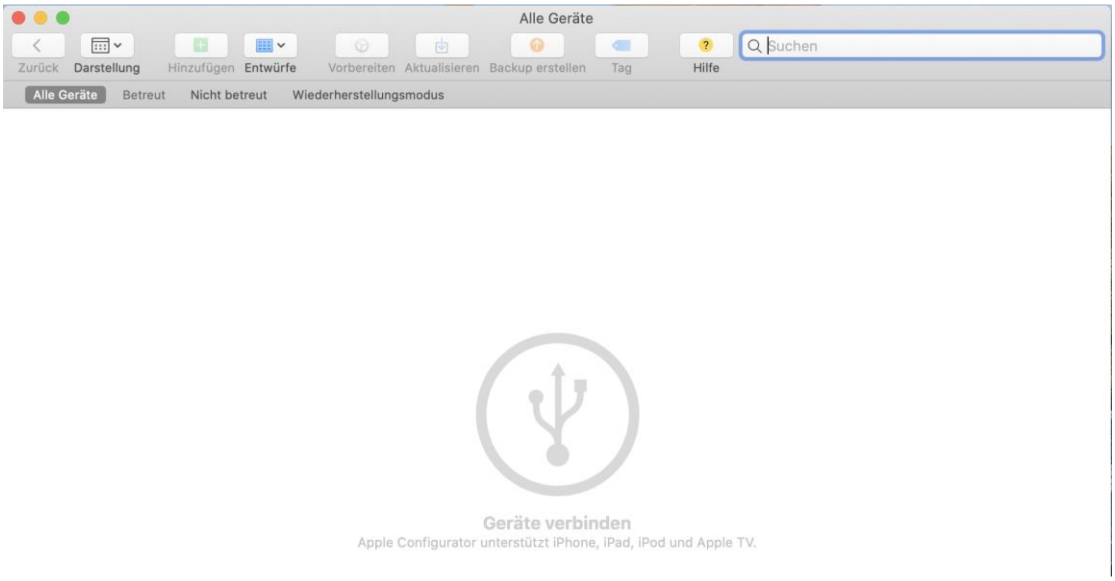
Note:
Make sure to assign the appropriate profiles to the corresponding peer in the menu ***VPN > IPSec > IPSec Peers > <Your Peer> > Advanced Settings****.*
Unfortunately, this setting is not completely reliable and does not work on devices running macOS.

1.1.2 Advanced configuration of the Apple client

With the help of **Apple Configurator 2** it is possible to configure an Apple IPSec client in such a way that rekeying takes place after a long time and therefore does not lead to an aborted connection during this time. You can use this customized configuration directly on a macOS device, but also export it to an iOS device.

Proceed as follows to create the configuration:

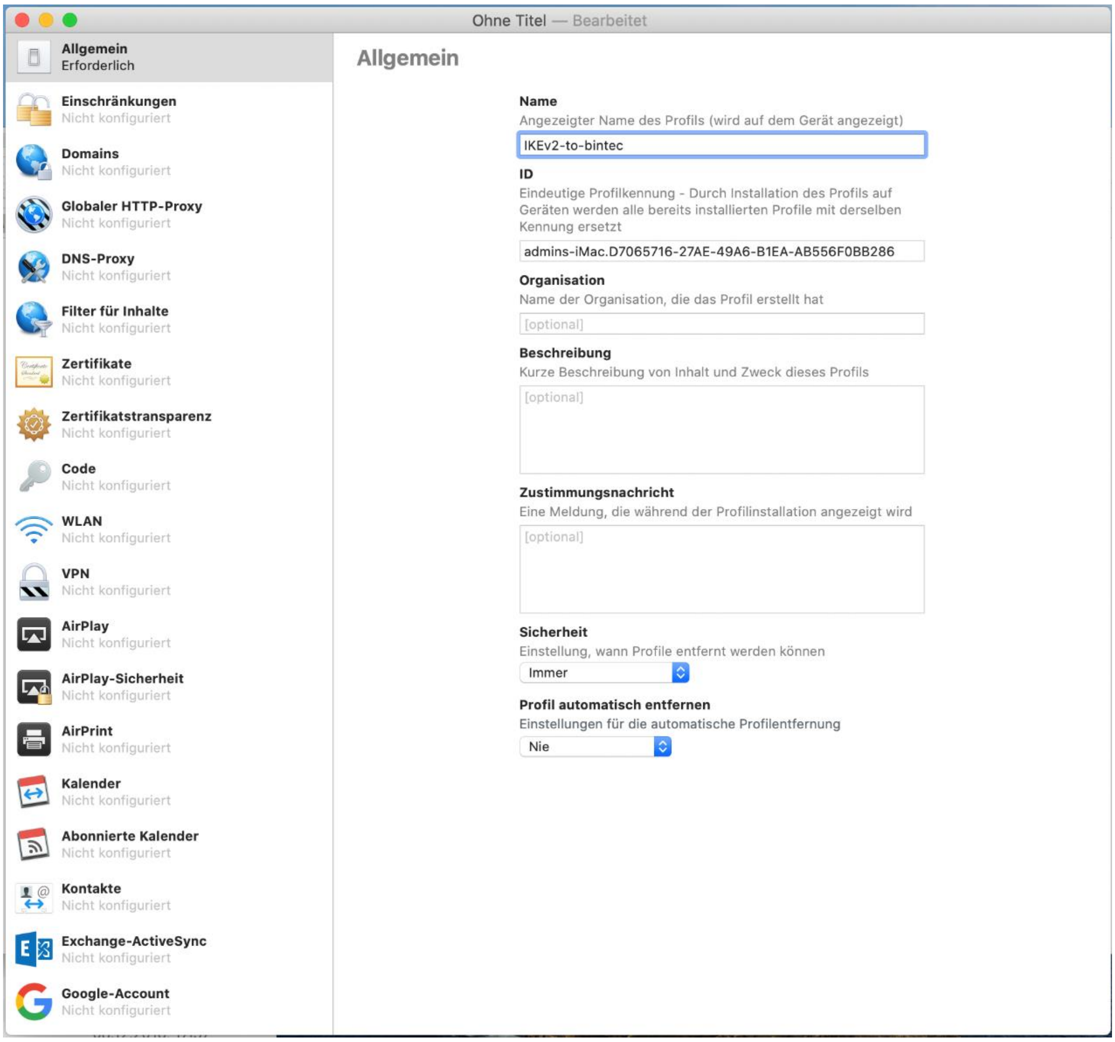
1. Install and open the **Apple Configurator 2**:



Geräte verbinden

Apple Configurator unterstützt iPhone, iPad, iPod und Apple TV.

2. Press **Command + n** to create a new profile. In the window that opens, in the **General** section, enter a name for the profile to be created, in our example *IKEv2-to-bintec*:



Ohne Titel — Bearbeitet

Allgemein

Name
Angezeigter Name des Profils (wird auf dem Gerät angezeigt)
IKEv2-to-bintec

ID
Eindeutige Profilkennung - Durch Installation des Profils auf Geräten werden alle bereits installierten Profile mit derselben Kennung ersetzt
admins-iMac.D7065716-27AE-49A6-B1EA-AB556F0BB286

Organisation
Name der Organisation, die das Profil erstellt hat
[optional]

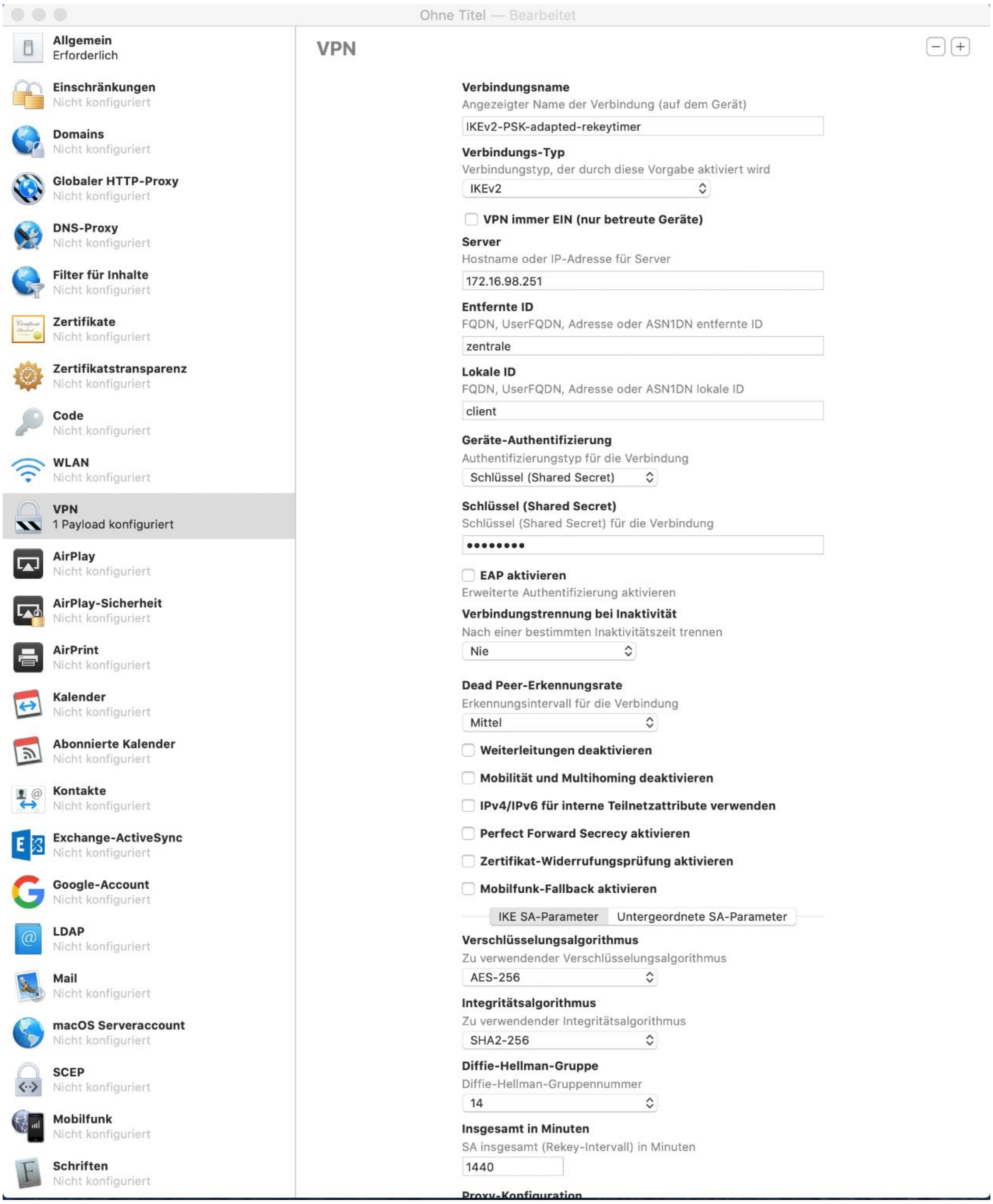
Beschreibung
Kurze Beschreibung von Inhalt und Zweck dieses Profils
[optional]

Zustimmungsnachricht
Eine Meldung, die während der Profilinstallation angezeigt wird
[optional]

Sicherheit
Einstellung, wann Profile entfernt werden können
Immer

Profil automatisch entfernen
Einstellungen für die automatische Profilentfernung
Nie

3. Make the following settings in the VPN section:



VPN

Verbindungsname
Angezeigter Name der Verbindung (auf dem Gerät)
IKEv2-PSK-adapted-rekeytimer

Verbindungs-Typ
Verbindungstyp, der durch diese Vorgabe aktiviert wird
IKEv2

□ **VPN immer EIN (nur betreute Geräte)**

Server
Hostname oder IP-Adresse für Server
172.16.98.251

Entfernte ID
FQDN, UserFQDN, Adresse oder ASN1DN entfernte ID
zentrale

Lokale ID
FQDN, UserFQDN, Adresse oder ASN1DN lokale ID
client

Geräte-Authentifizierung
Authentifizierungstyp für die Verbindung
Schlüssel (Shared Secret)

Schlüssel (Shared Secret)
Schlüssel (Shared Secret) für die Verbindung
••••••••

□ **EAP aktivieren**
Erweiterte Authentifizierung aktivieren

Verbindungstrennung bei Inaktivität
Nach einer bestimmten Inaktivitätszeit trennen
Nie

Dead Peer-Erkennungsrate
Erkennungsintervall für die Verbindung
Mittel

□ **Weiterleitungen deaktivieren**

□ **Mobilität und Multihoming deaktivieren**

□ **IPv4/IPv6 für interne Teilnetzattribute verwenden**

□ **Perfect Forward Secrecy aktivieren**

□ **Zertifikat-Widerrufungsprüfung aktivieren**

□ **Mobilfunk-Fallback aktivieren**

IKE SA-Parameter | Untergeordnete SA-Parameter

Verschlüsselungsalgorithmus
Zu verwendender Verschlüsselungsalgorithmus
AES-256

Integritätsalgorithmus
Zu verwendender Integritätsalgorithmus
SHA2-256

Diffie-Hellman-Gruppe
Diffie-Hellman-Gruppennummer
14

Insgesamt in Minuten
SA insgesamt (Rekey-Intervall) in Minuten
1440

Proxy-Konfiguration

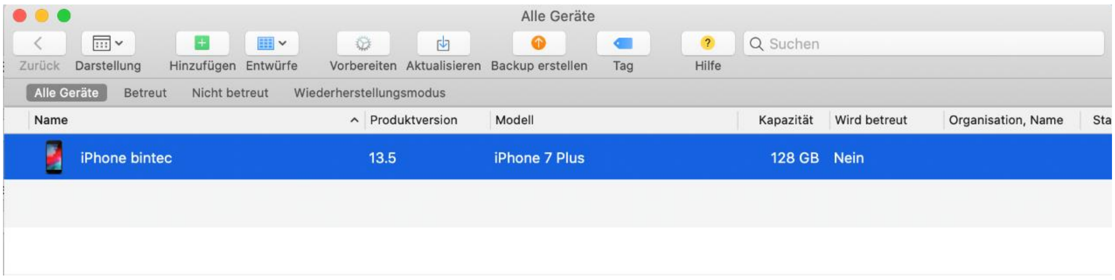
Adjust settings such as the **Server**, the **Local ID** and the **Key** to your requirements - such as the configuration of the peer on your bintec-elmeg device.

Make sure that the value for the **Total in minutes** option is set to a value according to your requirements. This option determines when re-keying is to take place. In our example, the value is set to *1440* minutes (24 hours).

4. With the key combination **Command + s**, you can save the profile to the **Documents** folder, for example, and then activate it on the macOS device by double-clicking it.

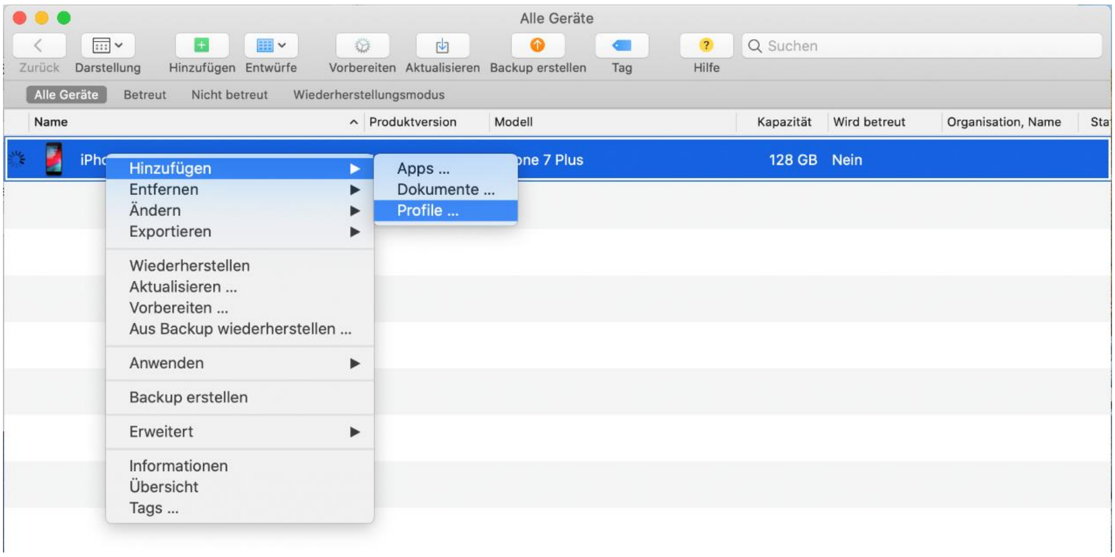
To take advantage of the extended rekeying interval on an iOS device, you can export the created profile. To do this, proceed as follows:

1. Connect the iOS device to the macOS device where the profile is stored. Confirm the device code.

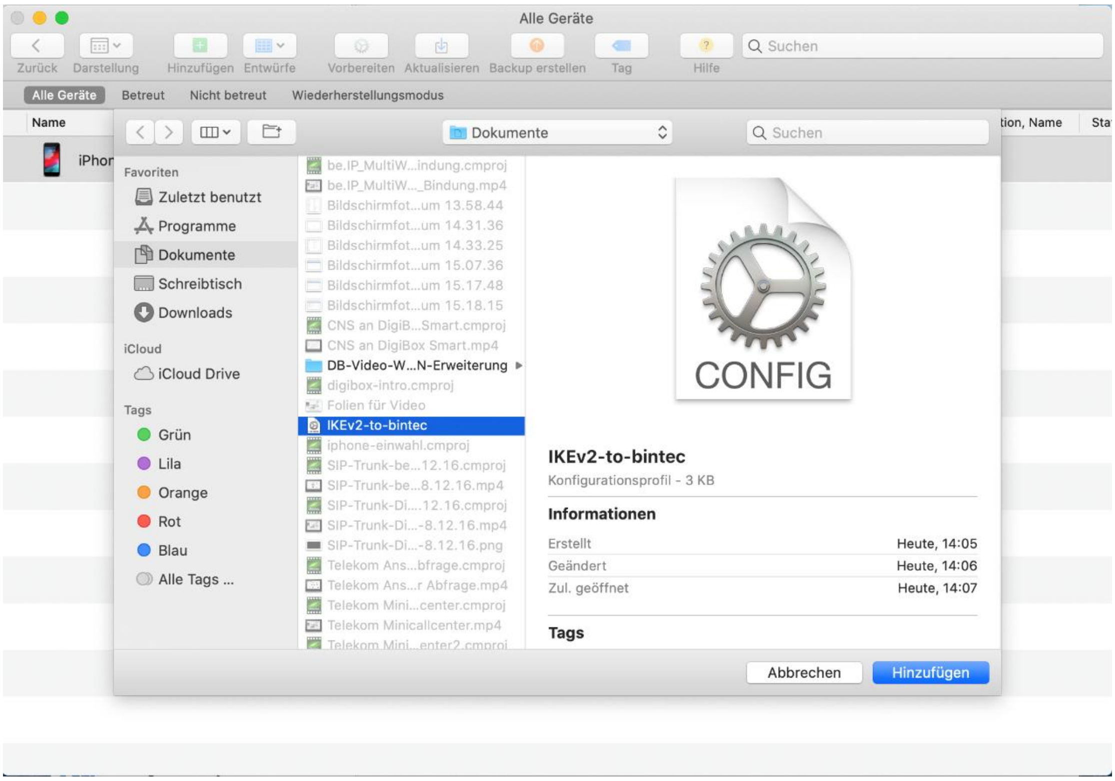


Name	Produktversion	Modell	Kapazität	Wird betreut	Organisation, Name	Sta
iPhone bintec	13.5	iPhone 7 Plus	128 GB	Nein		

2. Switch to the **Add > Profiles** menu with a right mouse click (CTRL click):



3. Transfer the previously created *IKEv2-to-bintec* profile to the iOS device. Follow the instructions on the screen:


Alle Geräte
Zurück
Darstellung
Hinzufügen
Entwürfe
Vorbereiten
Aktualisieren
Backup erstellen
Tag
Hilfe
Suchen
Alle Geräte
Betreut
Nicht betreut
Wiederherstellungsmodus
Name
iPhon
tion, Name
Sta
Dokumente
Suchen
Favoriten
Zuletzt benutzt
Programme
Dokumente
Schreibtisch
Downloads
iCloud
iCloud Drive
Tags
Grün
Lila
Orange
Rot
Blau
Alle Tags ...
be.IP_MultiW...indung.cmproj
be.IP_MultiW..._Bindung.mp4
Bildschirmfot...um 13.58.44
Bildschirmfot...um 14.31.36
Bildschirmfot...um 14.33.25
Bildschirmfot...um 15.07.36
Bildschirmfot...um 15.17.48
Bildschirmfot...um 15.18.15
CNS an DigiB...Smart.cmproj
CNS an DigiBox Smart.mp4
DB-Video-W...N-Erweiterung
digibox-intro.cmproj
Folien für Video
IKEv2-to-bintec
iphone-einwahl.cmproj
SIP-Trunk-be...12.16.cmproj
SIP-Trunk-be...8.12.16.mp4
SIP-Trunk-Di....12.16.cmproj
SIP-Trunk-Di...-8.12.16.mp4
SIP-Trunk-Di...-8.12.16.png
Telekom Ans...bfrage.cmproj
Telekom Ans...r Abfrage.mp4
Telekom Mini...center.cmproj
Telekom Minicallcenter.mp4
Telekom Mini...enter2.cmproj
CONFIG
IKEv2-to-bintec
Konfigurationsprofil - 3 KB
Informationen
Erstellt
Heute, 14:05
Geändert
Heute, 14:06
Zul. geöffnet
Heute, 14:07
Tags
Abbrechen
Hinzufügen

4. You can then use the imported profile to establish an IPSec connection.

1.2 Error corrections / workarounds

- **IPSec - connection abort (#4286):** Due to an *informative request* not answered by bintec-elmeg devices, IPSec connections could be interrupted.
- **DS Lite - Source IP address not retrievable (#3397):** An IPv4 source address could not be obtained on DS Lite connections. This caused problems when sending messages from the voice mail system.

2 Release 10.2.8.100

2.1 New features

2.1.1 WLAN - encryption standard WPA3

- With this release the Wireless LAN Controller supports the encryption standard **WPA3** for W2022ac access points running system software 2.4.1.1 or higher. Older bintec access points and the internal WLAN do not support WPA 3. WPA 3 serves to improve security in WLAN networks. In the menu **Wireless LAN > WLAN > Wireless Networks (VSS) > New** in the **Security Settings** section, you will **find** new options. The options **Security Mode** = *OWE* and **Security Mode** = *OWE Transition* are suitable for open networks. OWE (Opportunistic Wireless Encryption) only works with WPA3 enabled clients that have OWE implemented. The data transfer between access point

and client is encrypted.
OWE-Transition is suitable for networks that are to be used by WPA3-capable clients, but also by older, non-WPA3-capable clients. For clients that support WPA3, the data transfer between access point and client is encrypted, for all others it is unencrypted.
With **Security Mode** = *WPA-PSK* or **Security Mode** = *WPA-Enterprise,* you can set **WPA Mode** = *WPA3* for WPA3-enabled clients or select **WPA Mode** = *WPA2 and* WPA3 to use WPA2 and WPA3-enabled clients on the same network.

- The following menus have been changed to support configuration of these options:
  - Wizards -> WLAN
  - Wireless LAN Controller -> Wizard
  - Wireless LAN Controller -> Slave AP Configuration -> Slave Access Points
  - Wireless LAN Controller -> Slave AP Configuration -> Wireless Networks (VSS)
- In the menu **Wireless LAN Controller > Controller Configuration > Slave AP Auto Profile > Edit,** you will find a note that WPAv3 profiles are not available on all access points.

2.1.2 WLAN standard 802.11r/k/v

- The Wireless LAN Controller supports the WLAN standards 802.11r/k/v for W2022ac access points running system software 2.4.1.1 or higher:
  - **Fast BSS Transition (802.11r)**
    802.11r (Fast BSS Transition, FT) is a mechanism that allows a WLAN client to restore an existing WPA encryption faster when changing access points than it would do with full authentication. The 802.11r protocol shortens this process and thus the interruption of data traffic when switching to another access point. 802.11r is supported with WPA2-PSK, WPA3-SAE, WPA2-Enterprise and WPA3-Enterprise. 802.11r is not supported by all **bintec** access points.
  - **Management of radio resources (802.11k)**
    When 802.11k is activated, WLAN clients send information about their functionality (2.4/5GHz support, ...) and information about other access points in the environment to their current access point.
    This information enables the access point to find the best roaming options for the client.
    802.11k is not supported by all **bintec** access points.
  - **Network supported roaming (802.11v)**
    The access point regularly sends information to a connected WLAN client about neighboring access points that are eligible for roaming. This information enables the WLAN client to make better roaming decisions. 802.11r is not supported by all **bintec** access points.

2.1.3 Dual Stack Lite - AFTR

- In the menu **WAN > Internet + Dial-up > Dual Stack Lite > New,** the IP address of the AFTR (Address Family Transition Router) can not only be entered as a static address - as before - but also obtained via DHCP.

2.1.4 Wireless LAN Controller - Monitoring

In the **Wireless LAN Controller > Monitoring > Active Clients** menu, additional information about the used radio band and channel is added to the overview.

2.2 Changes

- **DNS - Bailiwick Check customizable (#3780):** Due to a strict Bailiwick check, it could happen that the secure search function in the web filter was not working. With the MIB variable **ipDnsCheckBailiwick** the behavior can now be adjusted.
- **MGW- Numbering Plan Information changed (#3942):** To avoid problems with Avaya PBXs, the Numbering Plan Information (NPI) parameter has been changed from *unknown* to *ISDN numbering plan.*
- **WLAN client mode:** In bintec access points of the recent n-series (W1001n, W1003n etc.) and bintec routers of the RS series, the roaming behavior has been considerably accelerated when operating the device in WLAN client mode.
- **WAN - DSLite (#4205):** In the menu **WAN > Internet + Dial-up > Dual Stack Lite > New** the parameters AFTR in **AFTR Mode** and **AFTR Gateway** in **Static AFTR** have been renamed.
- **Wireless LAN Controller - WPA Mode (#4186, 4244):** In the menus **Wireless LAN Controller > Slave AP Configuration > Wireless Networks (VSS)** and **Wireless LAN Controller > Wizard > Step 3 > Edit,** the selectable values for the parameters **Security Mode** and **WPA Mode** in the respective drop-down list were sorted by encryption strength.
- **Bintec Secure IPSec Client:** All bintec devices are using a unified version of the Bintec Secure IPSec Client.

2.3 Error corrections

- **Wireless LAN Controller - Wireless Networks (VSS) displayed incorrectly (#2864):** If a WTP was disabled in the **Wireless LAN Controller > Slave AP Configuration** menu, **the Wireless LAN Controller > Monitoring > Wireless Networks (VSS)** menu still displayed "Activated, channel scan is running. Please wait...".
- **VoIP - Problem with RelAix MSN Account (#4064):** A single number MSN of the provider RelAix configured as MSN SIP account with a single MSN did not work.
- **IPSec - Tunnel problems (#3743):** When using IPSec with IKEv2, under certain circumstances, using an Enigmatec router as remote IPSec gateway could cause the tunnel to get blocked.

- **IPSec - Problems with certificates (#3882, 4157):** When using IPSec, the creation of a tunnel using certificates failed because the digital signature could not be verified although it was valid.
- **IPSec - connection failed (#3920):** With high payload, connections were occasionally aborted.
- **PPPoE - Wrong speed (#3873):** When connecting PPPoE via a virtual interface, the uplink always had the default speed of 128K.
- **Voice Mail - Incomplete Recording (#3869):** At connections of the provider HFO, it could happen that messages to a voice mail box were recorded incompletely.
- **DHCP - Renew process did not work correctly (#3555):** If DHCP client mode was used on two interfaces, the renewal process did not work correctly, the distributed IP address disappeared for a short time.
- **CoS - Problem with IP640 (#3527):** Class-of-Service rules could be circumvented with service codes on the elmeg IP640. Using a service code via a function key on an elmeg IP640, for example, it was possible to switch to night mode although this was prohibited by a class-of-service rule.
- **PPTP, L2TP - Menus displayed in GUI by mistake (#3526):** The PPTP and L2TP menus were displayed in the GUI although they were not part of the functionality of the devices.
- **Authentication - RADIUS (#3472):** In the menu **System Management > Remote Authentication > RADIUS > New > Advanced Settings** the parameter **Reload Interval** was incorrectly displayed in seconds instead of minutes and the parameter input box was missing.
- **MGW - CallRouting (#3433):** Calls were not possible in MGW mode because no default call number was set after initial setup. When converting from PBX to MGW, the default phone number will now be converted.
- **Telephony - Call forwarding aborted (#3425):** If a call was to be forwarded to a mobile phone in the Telekom network, the call was aborted.
- **Telephony – Error at Deutschen Telefon connections (#3411):** At single number connections of Deutsche Telefon, it could happen that incoming calls were not possible.
- **Dual Stack Lite - IPv4 did not work (#3868):** With Dual Stack Lite with 1&1 or M-net IPv6 worked, but IPv4 did not.
- **Telephony - Call shown as anonymous (#3189):** Incoming calls from a mobile phone with Telekom One Number were unintentionally shown with suppressed number.
- **Telephony - Problem during call setup (#1903):** If an Invite without SDP was used during session setup, problems occurred.
- **Wireless LAN Controller - Performance Issues (#1780):** If a wireless LAN controller was managing many access points, high CPU utilization could occur. After some time, network communication became slower and slower until WLAN stopped working.
- **WLAN - Security Problem (#4048):** Under certain circumstances, it was possible to send unencrypted ARP requests into the LAN of an access point

with the help of a script and thus impair the LAN performance. This security problem has been fixed

- **Telephony - Second MSN not reachable (#4002):** If the first MSN was in use when multiple MSNs were configured, the second MSN was not reachable.
- **MGW - Call Abort (#4065):** Devices with ISDN could experience aborted calls.
- **Firewall - Incorrect Display (#3985):** In the menus **Firewall > Policies > IPv4 Filter Rules and Firewall > Policies > IPv6 Filter Rules** empty brackets were displayed incorrectly**.** NCI alert error messages were displayed in the syslog.
- **Wireless LAN Controller - Security Mode Problems (#4189, 4190, 4222):** In the menu **Wireless LAN Controller > Slave AP Configuration > Wireless Networks > New**, the security settings for certain parameter combinations could be set incorrectly.
- **Wireless LAN Controller - Security Mode Problems (#4187):** If the security mode of a wireless network was changed from *WPA-PSK* to *WPA Enterprise*, the PSK was not deleted.
- **DSLite - Malfunction (#4206):** If a static AFTR address was entered with spaces, DSLite malfunctioned.
- **Wireless LAN Controller - Radio Module Profiles not filtered (#4250):** In the menu **Wireless LAN Controller > Slave AP Configuration > Slave Access Points > Edit** in the drop down list **Active Radio Module Profile** more profiles were displayed than the module capacities made available, i.e. for example for radio module profile 1 only the *2.4 GHZ Radio Profile* is available, but the *5 GHz Radio Profile* was also displayed.
- **Wireless LAN Controller - Wrong default setting on the second wireless module (#4252):):** In the menu **Wireless LAN Controller > Slave AP Configuration > Slave Access Points > New** the default setting for the second radio module was the *2.4 GHz* Radio *Profile* instead of the *5 GHz Radio Profile.*
- **Wireless LAN Controller - Wrong default setting for security mode (#4256):** In the menu **Wireless LAN Controller > Slave AP Configuration > Wireless Networks (VSS) > New** the value *Inactive* was wrongly preselected for **Security Mode**.
- **Wireless LAN Controller - VSS profiles double (#4197):** In the menu **Wireless LAN Controller > Wizard** in **Step 4** on the **Edit** page, the VSS profiles were assigned twice to the detected access point.
- **PBX - Problems with SIP provider envia TEL (#4208):** When using an Avaya PBX and the SIP provider envia TEL, one-way voice connections occurred sporadically.
- **VPN - be.IP Secure Client (#4006, 3711):** In the menu **VPN > be.IP Secure Cient** an outdated image, an outdated logo and a misleading description were displayed. The link to the Client was not correct.
- **Wireless LAN Controller - Wrong defaults for wlcWlanIfProfileTable (#4255):** Parameters in the MIB table **wlcWlanIfProfileTable** were incorrectly

set. Among other things, this resulted in access points being disabled by default.

- **Wireless LAN Controller - Wrong radio module profiles (#4267):** In the menu **Wireless LAN Controller > Slave AP Configuration > Radio Module Profiles > New,** profiles were created with the setting *Indoor/Outdoor* instead of *Indoor* or *Outdoor*.
- **Wireless LAN Controller - Slave AP Configuration (#4250, 4272):** In the menus **Wireless LAN Controller > Slave AP Configuration > Slave Access Points > Edit** and **Wireless LAN Controller > Wizard, radio module**, profiles could be selected for which the respective radio module was not suitable.
- **Wireless LAN Controller- Invalid Configuration (DEV:CI 28026):** If the menu **Wireless LAN Controller > Slave AP Configuration > Slave Access Points > Edit** menu was exited without selecting a wireless network profile, an invalid configuration was created.
- **Wireless LAN Controller - Channel Definition (#4257):** In the menu **Wireless LAN Controller > Slave AP Configuration > Slave Access Points,** a new channel selection could be triggered by clicking on **Start**, but the displayed screen did not change and no message was shown that the scan was running.

2.4 Known Issues

- **Wireless LAN Controller - Problems with BOSS-based access points and WPA3 (#4248):** BOSS-based access points do not support WPA3. When a WPA3-enabled wireless network profile is rolled out on a BOSS-based access point, the wireless LAN controller typically displays a warning message and does not roll out the incompatible configuration. Under certain circumstances, when attempting to roll out a WPA3-enabled wireless network on an incompatible BOSS access point, this warning will not be displayed, and the incompatible configuration will be rolled out on the access point. As a result, unexpected and unsafe settings may occur on this access point.