Release Notes
System Software 10.2.9

Content

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 of server changes carried out by FlashStart. Without an update, search engine queries (e.g., Google) no longer work.

1 Release 10.2.9 Patch 3

1.1 Security-relevant changes

- Several security flaws have been discovered under the name **FragAttacks,** which are based on fundamental weaknesses in WLAN standards. Release 10.2.9 Patch 3 is secured against attacks based on these security flaws.

1.2 Changes

- The IPSec implementation has been improved in the area of **IKEv2-based** connections with regard to stability and interoperability. To eliminate any remaining sources of errors as far as possible, refer to the configuration recommendations in the appendix: ***Fehler! Verweisquelle konnte nicht gefunden werden.***.

1.3 Error corrections

- **Restart (# 4218, 4285):** In connection with an IPSec connection with a scheduler configuration, the device could restart.
- **No Internet access via VPN client (# 4400):** Although the IPSec connection was correctly established via a VPN client, it could happen that access to the Internet was not possible if all the client's traffic was sent through the IPSec tunnel.
- **IPSec - Temporarily no data transmission (# 5107):** It could happen that temporary interruptions in data transmission occurred when using IKEv2 in IPSec configurations.
- **Restart (# 5319):** If no peer ID matching the connection request was available on the responder side when establishing an IPSec connection authenticated with RSA certificates, the device could restart on the responder side.
- **SIP connection inactive (# 4378):** If a connection was to be maintained using "SIP OPTIONS" messages, it could happen that this was not successful.

- **Connection not possible (# 5098):** When operating as a media gateway, it could happen that connections were no longer possible under high load when terminal devices were connected to the ISDN port.
- **Restart (# 5199**): When operating as a telephone system, occasional restarts could occur.
- **High system load (#5113):** When operating the device as a WLAN controller, a high system load could occur.

2 Release 10.2.9 Patch 2

2.1 Changes

- **Automatic outside line for consultation:** Previously, it was necessary to dial a leading *0* for a consultation call to an external number even if automatic outside line was configured. For VoIP phones, this behavior has been changed with Release 10.2.9 Patch 2: An automatic outside line access set up for the respective user is carried out when the user starts an eternal consultation.
- **SIP without registration:** When using a SIP connection without registration, problems with incoming calls occurred if the connection was established via an upstream gateway because SIP headers contained an internal IP address. With Release 10.2.9 Patch 2, the public address is transmitted.

2.2 Error corrections

- **Sporadic restarts (# 4957, 4958, 5073):** Sporadic restarts could occur when using IKEv2.

3 Release 10.2.9 Patch 1

3.1 Changes

Version 4 of CloudNetManager is hosted at a new address. Release 10.2.9 Patch 1 uses the new address (https://bintec.cloudnetmanager.com) and updates it in existing installations. The previous CloudNetManager (https://bintec.networkcloudmanager.com) can no longer be used.

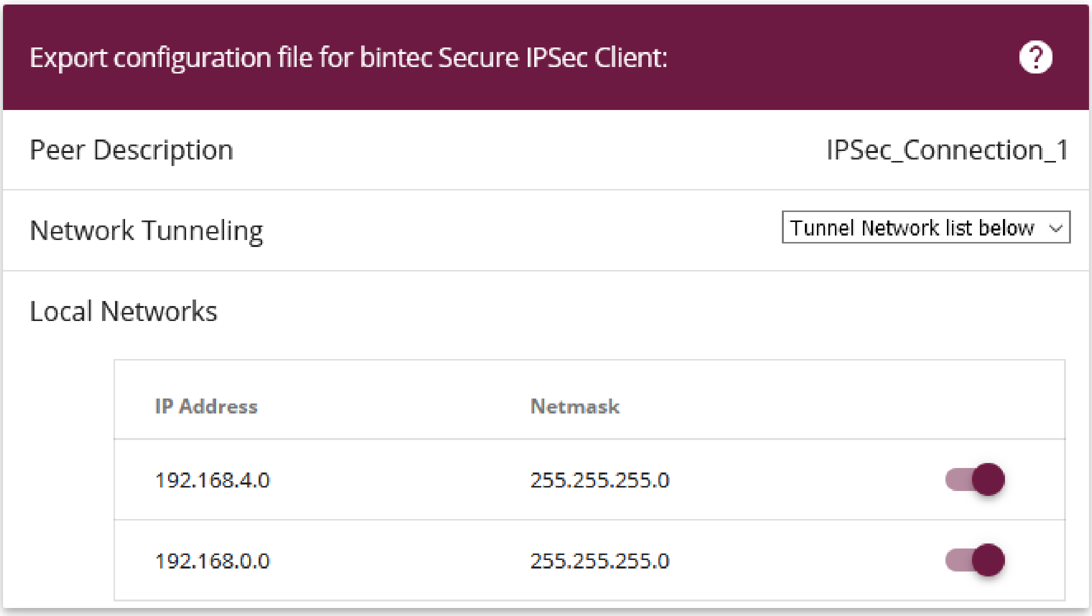
If you intend to use the new CloudNetManager version, make sure you have a user account and the necessary licenses before updating to the new release.

4 Release 10.2.9.100

4.1 New features

4.1.1 Split Tunneling for IPSec Client

If you use the VPN configuration wizard to create the configuration for a client dial-in, you now have the option of making either all or only selected networks accessible via the VPN when exporting the configuration for the bintec elmeg Secure Client:



Export configuration file for bintec Secure IPSec Client:

Peer Description	IPSec_Connection_1
Network Tunneling	Tunnel Network list below
Local Networks	

IP Address	Netmask	
192.168.4.0	255.255.255.0	●
192.168.0.0	255.255.255.0	●

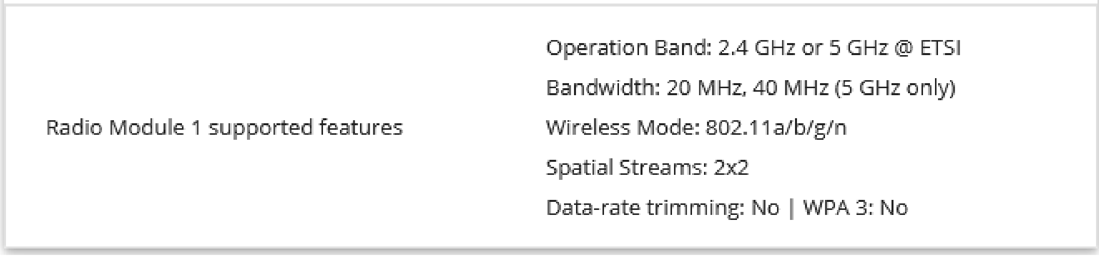
Split tunneling is not enabled if no selection is made in the list of networks.

4.1.2 Support for W2022ax and W2044ax

The wireless LAN controller supports the upcoming WiFi6 access points W2022ax and W2044ax. The default channel plan in the 5GHz band provides all indoor channels (36, 40, 44, 48, 52, 56, 60, 64).

4.1.3 Advanced display

In the **Wireless LAN Controller > Access Point Configuration > Edit** menu, there is an extended display of the functions supported by the radio modules of an access point:



Radio Module 1 supported features	Operation Band: 2.4 GHz or 5 GHz @ ETSI Bandwidth: 20 MHz, 40 MHz (5 GHz only) Wireless Mode: 802.11a/b/g/n Spatial Streams: 2x2 Data-rate trimming: No | WPA 3: No

4.1.4 Access Point Steering

When configuring **Client Steering** in the **Wireless LAN Controller > Access Point Configuration > Wireless Networks > New/Edit** menu**,** the option **AP Steering** (Access Point Steering) is available. This causes a client with a poor connection to not only change frequency bands, but also to register with another access point that can provide a better connection, if necessary.
This function requires the activation of 802.11k/v.

4.1.5 Extended selection of channel plans

When configuring access points via the wireless LAN controller, an extended selection of predefined channel plans is available in the Wireless **LAN Controller > Access Point Configuration > Radio Profiles > New/Edit** menu:

- *All*: All channels can be selected during channel selection.
- *World Mode* (for frequency band = 2.4 GHz, default value): The automatic channel selection uses only the non-overlapping channels 1, 6, 11.
- *ETSI mode* (for frequency band = 2.4 GHz): Automatic channel selection uses only the non-overlapping channels 1, 5, 9, 13.
- *No weather radar channels* (for frequency band = 5 GHz, default value): The weather radar channels are excluded from the channel selection. Available channels are 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140.
- *Indoors No DFS/TPC* (for frequency band = 5 GHz): These channels can be used inside buildings. DFS (Dynamic Frequency Selection) and TPC (Transmitter Power Control) are not used. Channels 36, 40, 44, 48 are available.
- *No outdoor channels* (for frequency band = 5 GHz): This channel plan combines channels 36 to 64, which are specified for indoor applications only. This channel plan can be used to optimally integrate 5GHz WLAN-capable multimedia devices, such as smart TVs, into the WLAN network, which often do not support the 5GHz outdoor channels (channel 100 and higher).
- *User defined*: Select the desired channels yourself.

4.1.6 Channel change in case of interference

In the **Wireless LAN Controller > Access Point Configuration > Radio Profiles > New/Edit > Advanced Settings** menu**,** you can now activate the option **Switch Channel on Jammer**. Access points that are affected by radio interference in the originally selected channel will then change channel if necessary.

4.1.7 Advanced neighbor monitoring

The **Own Access Points** submenu has been added to the **Neighbor Monitoring** in the **Wireless LAN Controller** menu**.** This menu displays information about how access points managed by the controller "see" each other. This provides useful information about the network formed by the managed access points and helps you identify potential WLAN problems.

The menu contains information such as the name of the access point, the channel it is operating on, its signal strength and when it was last seen by which access point and on which channel.

4.2 Changes

- If the internal radio module is not set up and managed via the WLAN controller, the regulatory domain in the menu **WLAN > Administration > Basic Settings** is preset with *ETSI* and cannot be changed because bintec elmeg devices are certified for this area. Accordingly, only the ETSI countries are available for the **Region** option.
- In the menu **Wireless LAN Controller > Controller Configuration**, you can select between *ETSI* and *Other* for the **Regulatory Domain**. For **Region**, corresponding states are then available for selection.
This information is transmitted in the beacons.
- For better support of a WLAN configuration by the WLAN controller, the **DHCP CAPWAP** option is already included in the standard configuration of the be.IP series devices.
- It was previously not possible to select the frequency band of the integrated WLAN radio module in the **WLAN wizard**. If a device only has one module, the 2.4 GHz profile was always used, and the setting had to be adjusted in the WLAN controller menu if necessary. This option is now available directly in the wizard.

4.3 Error corrections

- **ER# 4905:** It was not possible to delete the last SSID assigned to a radio module, even if it was not needed.
- **ER# 4832:** A DECT160 was displayed in the GUI as DECT210 after integration.
- **ER# 4787:** When using PPTP with MPPE, the device could reboot.
- **ER# 4869:** When operating a be.IP as a media gateway, call forwarding or T.38 fax connections could fail.
- **ER# 3743:** It could happen that during IKEv2 child SA rekeying, the existing SAs were not completely removed, resulting in non-functional IPSec connections.
- **ER# 4596:** When using LISP, connections could become inoperable when the status of interfaces changed.
- **ER# 4835:** Device reboots could occur when activating IPsec connections.
- **ER# 1478:** An SNMP walk from the Windows Power Shell could cause the device to lock up and require a reboot.
- **ER# 4594:** Due to an incorrect calculation of the bandwidth available at the WAN interface, incoming calls could be rejected.
- **ER# 4665:** Some access points and routers incorrectly reported access points with WPA2-Enterprise encryption as unsecured to the WLAN controller in the neighbor monitoring.
- **ER# 4689:** After an Internet connection interruption, it could take a long time to re-establish an existing IPSec connection.

- **ER# 2050, 3371, 4416, 4439, 4889:** Sporadic reboots could occur, as well as an occasional "boot loop" where the device rebooted continuously.
- **ER# 4283:** If an IPSec Multi Peer was used to dial into a destination network, the same IP address was assigned to two connecting clients if they had the same internal IP address on their respective local networks.
- **ER# 4295:** When the WLAN controller was active and had control over the bridge interface VLAN settings, other VLANs created in the **LAN > IP Configuration** menu were not functional.
- **ER# 3419:** It could happen that it was not possible to add a phone to the system when a VPN connection was active. The operation failed with the message "Global error / The value must be greater than or equal to.... ".
- **ER# 4056:** Problems could occur when sharing call lists or a phone book. Under certain circumstances, these lists had to be shared several times.

4.4 Known limitations

- The W2003ac access point only accepts connections from 47 clients, even if the **Hard Limit** option is set higher.

5 Appendix

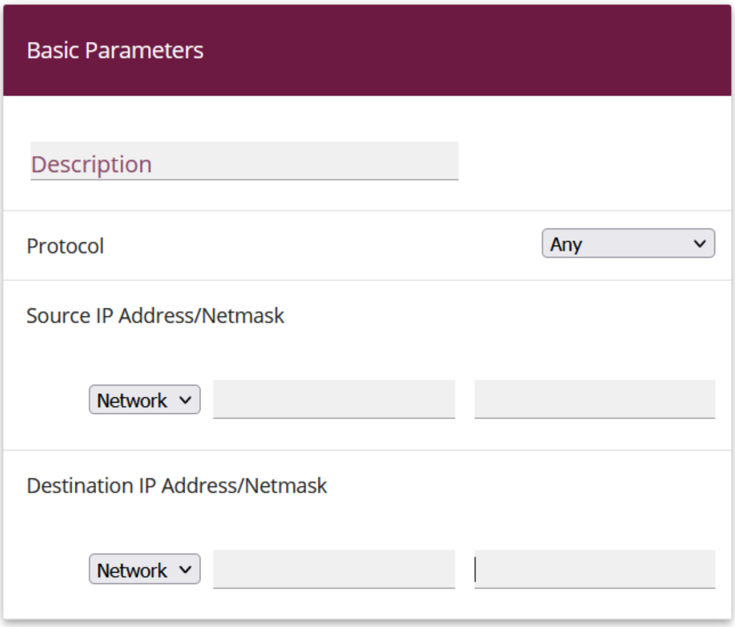
5.1 Advanced configuration of IKEv2-based IPSec peers

Release 10.2.9 Patch 3 removes a cause of potential problems when negotiating IKEv2-based IPSec connections. Previously, only the route configured in the IPSec peer determined which IP data was transmitted over the IPSec connection. This route-based approach to determining the so-called traffic selectors to be exchanged during IPSec negotiation is often too fuzzy and therefore may lead to stability and interoperability problems.

To ensure that traffic selector negotiation works correctly for IKEv2-based IPSec connections, it is recommended that you make the settings described below.

5.1.1 Determination of the data traffic to be tunneled

It makes sense to specify the traffic that is actually to be sent via the tunnel as precisely as possible. To do this, you can narrow down the destination and source networks in the **Internet & Network > VPN > IPSec > IPSec Peers > Edit > Additional filter of IPv4 traffic menu:**



Basic Parameters

Description

Protocol: Any

Source IP Address/Netmask: Network

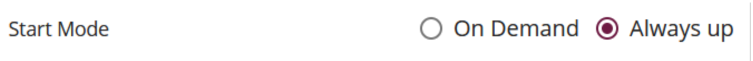
Destination IP Address/Netmask: Network

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 up* **Start Mode** is selected in the **Advanced IPSec Options** section.

5.1.2 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 to the value *Always up* in the **Internet & Network > VPN > IPSec > IPSec Peers > Edit > Advanced IPSec Options** menu to ensure a definite state of the IPSec interface:



Start Mode ○ On Demand ● Always up

5.1.3 Clear distribution of roles between client and server

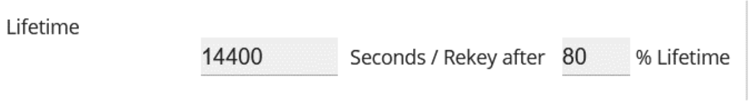
When configuring an IPSec connection, you should always ensure that the roles of the two IPSec connection partners are clearly assigned (initiator or responder role). This is important both for the initial connection establishment and for the periodic renegotiation of the IPSec connection.

Therefore, when configuring the **Lifetime** in the Phase 1 and Phase 2 profiles, make sure that the 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 periodical renegotiation of the IPSec connection.

You can find the settings in the following menus:

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

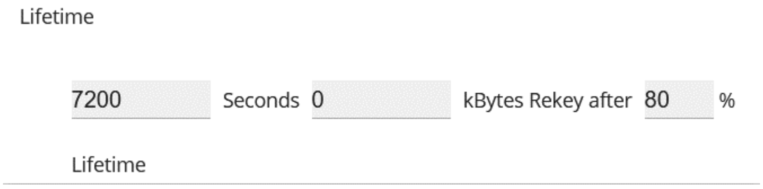
  

  Lifetime

  14400 Seconds / Rekey after 80 % Lifetime

  Set the values so that the validity of the Phase 1 parameters is shorter on the connecting 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**

  Lifetime

  7200 Seconds 0 kBytes Rekey after 80 %

  Lifetime

  Set the values so that the validity of the Phase 2 parameters is shorter on the connecting 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!