Release Notes
System Software 10.2.12 Patch 2

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 FlashStart has made a server change. Without an update, search engine queries (e.g. Google) no longer work.

1 Release 10.2.12 Patch 2

1.1 Security-relevant changes

-

1.2 Improvements / error corrections

- **Corrected syslog message** - In the subsystem PPP the log level for the message 'dispatch item missing' is output as 'DEBUG' instead of 'ERR'.
- **Sporadic reboot (ER#6315)** - Under certain circumstances (SIP registration) and when using user certificates, restarts could occur.
- **Stability (ER#6357)** - Further stability improvement for the be.IP plus in PBX mode.
- **STUN binding requests (ER#6402)** - STUN binding requests are now only sent if NAT is detected on the connection. The SIP "rport" functionality is used for NAT detection.
- **Dropped calls (ER#6304)** - In interaction with the Company Flex connection via a be.IP plus in MGW mode on a PBX, dropped calls could occur.
- **Stability (ER#6356)** - During the initialization of the LTE modem, sporadic system crashes could occur.
- **Missing extended routes** (ER#5816) - In connection with IKEV2 it could happen that extended routes were deleted.
- **New TACACS+ authentication**
  TACACS+ login authentication for SNMP shell is now also performed for the GUI login. For configuration, there must be at least one entry in tacacspServerTable.

  Example:
```
rs353j:httpSessionStatTable> tacacspserverTable

inx Priority(*rw)          Address(rw)           TcpPort(ro)
    Secret(rw)             Timeout(rw)           AdminStatus(-rw)
    OperStatus(ro)         Policy(rw)            EncrMode(rw)
    MultiSession(rw)       PppAuth(rw)           LoginAuth(rw)
    Accounting(rw)         BlockTimeout(rw)      AuthentNoResp(rw)
    AuthentNegResp(rw)     PrivLvlOnLogin(rw)

  0 0                      172.16.96.3           49
    "testing123"           3                     up
    up                     non_authoritative     encrypt
    disabled               disabled              enabled
    disabled               60                    connection_bydefault
    connection_bydefault   5
```

NOTE: Policy = non_authoritative allows recourse to local accounts, for example the 'admin' account.

To map authenticated users via TACACS, one or more specific entries in the biboadmlogintable are required.

Example:

```
rs353j:tacacspServerTable> biboadmlogintable

inx User(*rw)                        Password(rw)
    State(-rw)                       SnmpShellCommand(rw)
    SNMPAccessLevel(rw)              ShellAccessLevel(rw)
    HTTPAccessRights(rw)             ActivityMonAccessLevel(rw)
    ApDiscAccessLevel(rw)            HTTPAccessClass(rw)
    GUIAccessMask(rw)                GUIWriteAccessMask(rw)
    PasswordChangeRequired(rw)       SNMPAccessRightsDefault(rw)
    SNMPAccessRuleFirst(rw)          AccessSelector(rw)
    Usage(rw)

  0 "tacacs_login"
    valid
    no_access                        0
    fci                              0
    0                                user
    0x4                              0x4
    disabled                         no_access
    0                                -1
    selector
```

Weitere Einstellungen:

```
HTTPAccessRights     = fci
Usage                = selector
AccessSelector       = -1 (default)
```

All other settings regarding specific GUI access rights are defined via the biboadmguiAccesstable in conjunction with biboAdmGuiAccessLevelTable entries.

Example:

```
rs353j:biboAdmLoginTable> biboAdmGuiAccessLevelTable

inx BitNr(*rw)              State(-rw)              Description(rw)

  0 2                       valid                   "myprofile"
```

As soon as this functionality is activated, every connection request (GUI access) is redirected to HTTPS via HTTP.

2 Release 10.2.12 Patch 1

2.1 Security-relevant changes

-

2.2 Improvements / error corrections

- **Corrected WLAN client presence announcement in Ethernet LAN (ER#6163) –** On W1001n/Wx003n/Wx003ac series, RSxx3 series and be.IP series with integrated WLAN, the access point announced WLAN client

presence too early in Ethernet LAN (via LLC frames) on association instead after successful authentication of the WLAN client. This could cause sporadic WLAN client IP client connectivity problems, especially on roaming from one AP to another in the same WLAN network.

- **Fix of occasional permanent WLAN outages after radar event (ER#654, ER#3349) –** Under certain circumstances at W1001n/Wx003n/Wx003ac series, RSxx3 series and be.IP series with integrated WLAN it could happen in WLAN 5GHz operation on DFS channels (all 5GHz channels starting from channel 52) after detecting a radar signal or other interference that the WLAN stopped transmitting permanently until the device was restarted. This happened even in case the access point could have switched to a free channel without a radar signal, or the legal waiting period of 30 minutes had expired. The error was not detectable via the WLAN controller, but only on-site, since the access point incorrectly reported to the WLAN controller that the radio module was in operation.

- **Fix of IPv6 address assignment via DHCPv6 (ER#5971) -** In DHCPv6 client at non-rapid-commit case the IANA and IAPD section (received from DHCPv6 solicit message) were not copied into the subsequent DHCPv6 request message. This caused IPv6 connectivity problems on some ISP such as "Deutsche Glasfaser".

- **Do not bind additional DHCP options in IP/MAC binding (ER#6205) -** In GUI menu **Local Services > DHCP Server > IP/MAC Binding** a **static IP/MAC binding** did bind (invisibly to the user) additional to the IP/MAC binding further DHCP options (DNS server, default gateway etc.) to the DHCP client MAC address. This caused network problems for these DHCP clients in case **DHCP options** were changed later in **DHCP server**.
  Please note: Existing IP/MAC bindings will not be automatically converted on update. After Firmware update please remove and add them again in GUI to correct these entries.

- **Fix for multiple DynDNS accounts on the same interface (ER#5411) -** Under certain circumstances (especially at fiber-optic uplinks), on device reboot multiple **DynDNS accounts** per interface did not work. In case of error only the first DynDNS account worked, further accounts failed on IP update.

- **Fix on adding a new VoIP phone in PBX configuration (ER#3419) -** Under certain circumstances (especially when a VPN connection was existing) creating a new VoIP telephone failed with an error message in GUI menu **Assistants > Telephony > Terminals > NEW**.

- **PBX fix for early media on SIP forking (ER#6044) -** After receiving multiple ringing messages from provider (SIP Forking) early media ring tone was not always forwarded to the internal SIP client, instead in these cases only the local ring tone was audible for the caller.

- **Corrected VoIP message sanitize check in PBX (ER#6292) -** Under certain circumstances a RTCP Goodbye message in a call was erroneously forwarded from WAN to LAN.

- **Send RTP idle tone on forwarding an incoming call from remote (ER#6148) -** Under certain circumstances on calling from an external number (especially from T-Mobile network) to the PBX, e.g. the **Follow me** function in

the PBX did not work when it was configured to forward the call to an external destination as well.

- **Fixed DNS decoding problem in PBX (ER#6276) -** Voicemail e-mail delivery to "smtp.office365.com" (and possibly some others) failed due to a DNS decoding error.
- **Fix of small memory leak in DNS resolver (ER#4418) -** Under certain circumstances the DNS resolver had a memory leak as it sometimes did not free again the RAM of obsolete ipDnsDynamicTable entries.

3 Release 10.2.12

3.1 Security-relevant changes

- Changes have been made to protect against so-called cross domain injections (see https://xdi-attack.net).

3.2 Improvements / error corrections

- **Expanded WLAN Controller license limits** - For all BOSS based be.IP devices, the number of maximum manageable Access Points has been increased to 48. For BOSS based RSxx3 devices, the number of maximum manageable Access Points has been increased to 72. Additionally, the number of freely manageable Access Points (i.e., without the need to purchase extra licenses) has been increased for all supported BOSS based devices (RXL series, RSxx3 series, be.IP series, Rxxx2 series, W1001n/Wx003n/Wx003ac series) to 6 Access Points.
- **Factory default Radio Profiles optimized for Wi-Fi 6 APs (#5592)** - In factory default settings, the Radio Profiles are now optimized for Wi-Fi 6 Access Points (W2044ax and W2022ax) and have wireless mode 802.11ax and 4 spatial streams enabled by default.
  As always, if a Bintec Access Point does not support these settings, it automatically selects a setting that is closest to the transmitted configuration. Furthermore, the factory default channel plan in the 2.4GHz radio profile has been changed from *World Mode* (1, 6, 11) to *ETSI Mode* (1, 5, 9, 13) to provide optimal performance in the crowded 2.4GHz frequency band in Europe. In the 5GHz band, the factory default channel plan has been changed for all devices except be.IP series from the *No outdoor channels* plan to the wider *No weather radar channels* plan.
  Keep in mind that many Smart TV WLAN clients and some other older WLAN clients with 5GHz support, support the No outdoor channels *plan at maximum.*
  Saved WLAN Controller configurations will not be altered on update by these changes to the factory default settings.
- **Improvements in WLAN Controller GUI** - Numerous improvements have been made in the areas of access point management and monitoring:
  - o **Improved WLAN network overview and more encryption methods selectable in WLC assistant** - In GUI menu **Assistants > WLAN (WLC)** the **WLAN Networks** overview page now displays the overall

state of all managed Access Points, the number of connected WLAN clients to all managed WLAN networks, and the configured security of each WLAN network. In the edit page of this assistant more encryption methods can be selected (in addition to *Inactive* and *WPA 2 PSK, OWE Transition*, *OWE*, *WPA 2 and WPA 3 PSK*, *WPA 3 PSK* have been added).
Encryption methods with OWE and WPA 3 are only supported by OSDx based Access Points.

- o **Occasionally missing radio and VSS profile assignment after initial WLAN setup via WLC assistant (#4660)** - On initial setup of the WLAN Controller via the GUI menu **Assistants > WLAN (WLC),** it could happen that some discovered Access Points were not correctly managed. In case of this error, these Access Points did either have no Radio profile and no VSS profile assigned, or they had each VSS profile assigned twice on each radio module.

- o **Improved and enhanced General settings page** - In the GUI menu **Wireless LAN Controller > Controller Configuration > General,** the available settings have been rearranged for better clarity and have been extended with more advanced settings:
The option **Managed AP location** has been renamed to **Managed APs connection timeouts** in the advanced settings section, and the available values have been renamed from *Local (LAN)* and *Remote (WAN)* to *Tight* and *Relaxed* and extended with a *Custom* scheme. All values have a detailed description about their respective effect. Moreover, in the advanced settings section the options **WLAN Controller debug level**, **Update Interval for statistics of managed APs**, **Keep old reports of Neighbor APs**, and **AP management initialization** can be configured. Previously, these new settings were available via SNMP shell only.

- o **Autoprofiles now can be enabled and disabled** - In the overview page of the menu **Wireless LAN Controller > Controller Configuration > AP Autoprofile,** individual autoprofile entries now can be enabled and disabled via the new **Action** column
This setting - as everything in the autoprofile settings - only applies to newly discovered Access Points and not to already managed ones.

- o **"Default Radius Server" for WPA Enterprise networks made configurable** – For WPA Enterprise VSS profiles, the **Default Radius Server** for each entry can be selected in the menus **Wireless LAN Controller > Controller Configuration > AP Autoprofile > edit** and **Wireless LAN Controller > AP Configuration > Access Points > edit.** It can, therefore, be corrected in case the reference is missing in an entry. So far, it was not possible to roll out a working WPA Enterprise network via Autoprofiles, and, on the **Access Point** page, these settings were handled in the background by the GUI. It could then happen that an incorrect WPA Enterprise configuration could not be detected.
In case you are using WPA Enterprise secured VSS profiles, make

sure that all configured Autoprofiles and Access Points are referencing your configured Default Radius Server, and add the reference if it is not present there.

o **New Security Mode *WPA 3 Enterprise CNSA* for high-security WLAN networks** - The **Security Mode** *WPA 3 Enterprise CNSA* has been added to the GUI menu **Wireless LAN Controller > AP Configuration > Wireless Networks (VSS) > edit**. *WPA 3 Enterprise CNSA* is an advanced WPA 3 Enterprise mode for high-security environments.

The Wi-Fi Alliance calls this security mode *WPA3-Enterprise with 192-bit mode,* and it is a totally different security mode than the common **WPA3-Enterprise** despite the similar naming. **WPA 3 Enterprise CNSA** requires WLAN clients to support SHA384 for key hashing, AES-GCMP-256 for encryption, Protected Management Frames (802.11w), authentication with EAP-TLS using Elliptic Curve Diffie-Hellman (ECDH) exchange, the Elliptic Curve Digital Signature Algorithm (ECDSA) using a 384-bit elliptic curve, and finally a Radius server, which provides and enforces this form of authentication. Currently, only few WLAN client devices support this high-security mode. In contrast, the basic **WPA3-Enterprise** mode only enforces a minimum of AES-CCMP-128 encryption and Protected Management Frames over **WPA2-Enterprise** mode.

WPA 3 Enterprise CNSA is supported only by OSDx based Access Points running system software version 2.4.1.1 or higher.

o **Improved WLAN Controller monitoring overview** - The dashboard in the menu **Wireless LAN Controller > Monitoring > WLAN Controller** has been rearranged for better clarity, and the **Overview** box has been expanded with statistics of the operational states of **Radio modules**, **Wireless networks** and **Active Clients** of all managed Access Points.

o **New Radio Modules monitoring page** - The menu **Wireless LAN Controller > Monitoring > Access Points** has been split into the pages **Access Points** and **Radio Modules,** which show more relevant information.

The new **Access Points** page no does not contain radio module information any longer, but now additionally displays the **CPU Usage**, **Memory Usage** and **ETH Link Speed** of each managed Access Point, which is useful for troubleshooting and locating Ethernet cable and Ethernet switch port issues within the network.

The new **Radio Modules** page shows all radio modules of managed Access Points. In addition to all previously available radio module information it shows **Channel Utilization**, the number of **Radar Detections**, connected **Clients**, a **DL Bytes** and **UL Bytes** counter and the radio module **Status**. These statistics help monitor and troubleshooting the WLAN radio status for each managed Access Point more closely than before.

Channel Utilization is reported by all OSDx based Access Points and

by 802.11ac capable BOSS APs (e.g., W2003ac), but not by BOSS Access Points supporting 802.11n at maximum (e.g., W1001n or the internal radio of be.IP Plus).

- o **Display used Security Mode for Active Clients (#4259)** - The **Security Mode** actually used by connected WLAN clients is now displayed in the menu **Wireless LAN Controller > Monitoring > Active Clients**. This information is helpful in WLAN networks where multiple security settings are available in order to identify which security setting is used by which WLAN client. So, e.g., in a *WPA 2 and WPA 3* mixed mode WLAN network, you can now see which connected clients support WPA 3 and which require WPA 2.
  This new field is reported only by OSDx based Access Points running system software version 3.2.1.1 or higher.

- o **Wrong number dimension used for throughput graph in Active Clients detail page (#4139)** - In the menu **Wireless LAN Controller > Monitoring > Active Clients > Details,** the number dimension of the throughput graph is now dynamically adapted according to the current throughput data rate of the WLAN client.

- o **More clear and consistent data direction text labels in WLAN Controller monitoring pages** - In all WLAN Controller monitoring pages, the Bytes counter and throughput graph labels for both directions have been changed from **Tx (Transmit) Rx (Receive)** to **DL (Downlink)** and **UL (Uplink)**. In a WLAN Controller context, **Tx** and **Rx** caused confusion, as they depend on the perspective - either the one of a managed Access Point or the one of the Active Client.

- o **Neighbor AP monitoring improvements and bug fixes (#5515, #5524)** - The fields **Radio Fingerprint** and Access Point **Type** have been added to the menu **Wireless LAN Controller > Neighbor Monitoring > Neighbor APs**. Filtering of the display of all fields has been added, and by default the neighbor Access Point entries are sorted by their **Radio Fingerprint** for a better overview of the WLAN neighborhood.

  All entries with the same **Radio Fingerprint** very likely are caused by the same Neighbor Access Point radio. This allows identifying multiple SSIDs created by the same neighbor and which neighbor SSIDs belong together, and it allows determining the true number of neighbor Access Points.

  The **Type** field shows if the neighbor is running in Access Point, Mesh or in Ad hoc mode

  Mesh neighbors are recognized only by OSDx based Access Points running system software version 3.2.1.2 or higher, BOSS based Access Points still recognize mesh neighbor Access Points as Ad hoc types and do not see the Mesh ID.

  Especially mesh neighbors can cause a high channel utilization on the channels they use as they are the backbone connection in this kind of WLAN networks.

  The new fields allow easier identification of WLAN throughput

performance bottlenecks caused by WLAN neighbors.

Moreover, the **Channel** field has been enhanced to always display the actual wireless mode and bandwidth of the neighbor Access Point in a short notation and the name of the wireless mode in a tool tip

OSDx based Access Points need to run system software version 3.2.1.1 or higher, BOSS based Access Points need to run system software version 10.2.10 Patch 1 or higher to report the wireless mode of neighbor APs.

- o **Rogue AP monitoring page -** The missing **APPLY** button for accepted known rogue APs has been added to the menu **Wireless LAN Controller > Neighbor Monitoring > Rogue APs**.
- o **Firmware Maintenance page bug fixes** - The action **Save configuration with state information** has been renamed to **Get support information data** in the menu **Wireless LAN Controller > Maintenance**, and the handling of the URL input field has been fixed so that the protocol prefix is not added twice if the URL is specified with the protocol prefix.
- o **When accessing some WLC menus, GUI writes "NCI Alert" messages into Syslog (#4859)** - This issue has been fixed.
- o **New predefined e-mail alert event** - The new event *Managed AP setup error* has been added to the menu **External Reporting > Alert Service > Alert Recipient > edit/new**. This predefined e-mail alert sends all configuration error messages reported by the managed Access Point. This alert simplifies the detection and correction of user configuration errors, especially when incomplete or incompatible wireless settings are applied - an error that cannot be prevented by the user interface.

- **DHCP server ignored some special DHCP requests (#6110)** - The internal DHCP server wrongly ignored client DHCP requests to IP unicast (to the IP address of the DHCP server) with destination Ethernet Broadcast address (FF:FF:FF:FF:FF:FF).
- **Error in DHCP Relay (#6036) -** Unicast Replies were not fully RFC compliant, which could cause problems with responses to DHCP requests.
- **Call termination (#6111) -** It could happen that a call termination was triggered by the platform when calls were already in progress on a Telekom connection.
- **Calls Failed (#6060) -** Incoming calls were occasionally dropped immediately after signaling.
- **No ringing tone (#6048, 6048, 5885, 4538, 3987, 3951, 3117) -** It could happen that no ringing tone was heard, e.g., in case of call forwarding.
- **GUI prevents the configuration of more than 25 VLAN interfaces (ER#5322)** - The limit has been removed in GUI. Now more than 25 VLAN interfaces can be created.
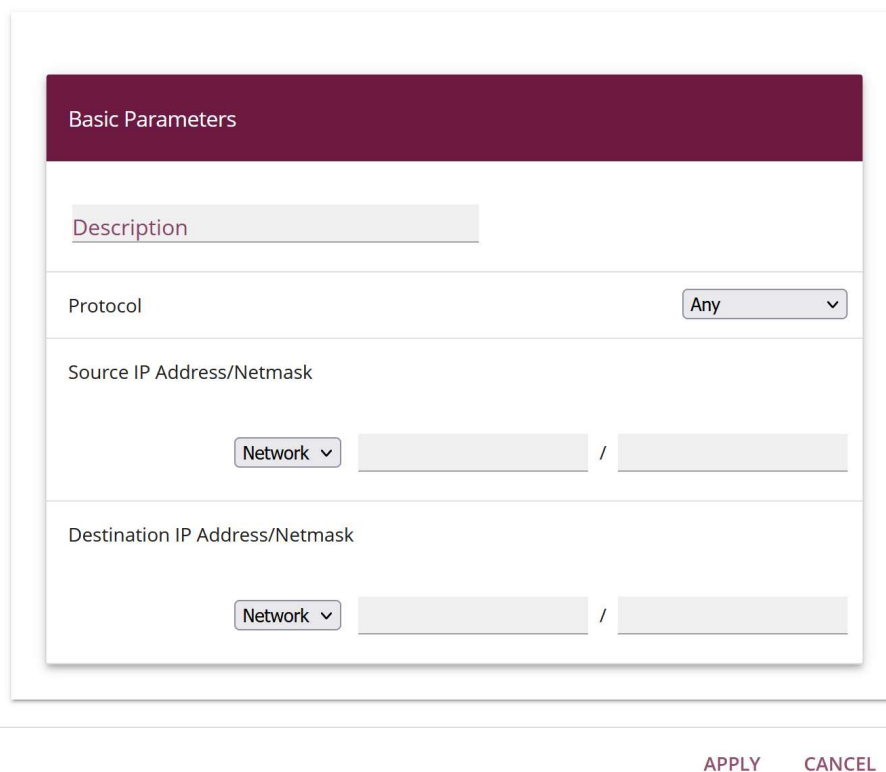
4 Appendix

4.1 Advanced configuration of IKEv2-based IPSec peers

To ensure that the negotiation of connection parameters works without errors for IPSec connections based on IKEv2, it is recommended to configure the connection as described below.

4.1.1 Determination of the data traffic to be tunneled

It is useful to specify the traffic that should be sent over the tunnel as precisely as possible. To do this, you can narrow down the destination and source networks in the **VPN > IPSec > IPSec peers > Edit > Additional filter of IPv4 traffic menu:**

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

4.1.2 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 in the menu **VPN > IPSec > IPSec Peers > Edit > Advanced settings** to *Always on* value to ensure an unambiguous state of the IPSec interface.

4.1.3 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).
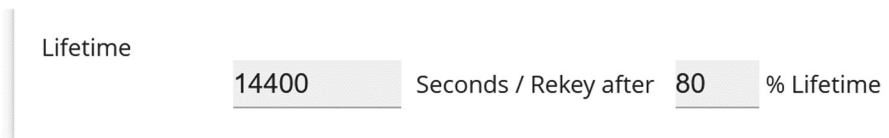
This is important both for the initial connection setup and for the periodic renegotiation of the IPSec connection.

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

You can find the settings in the following menus:

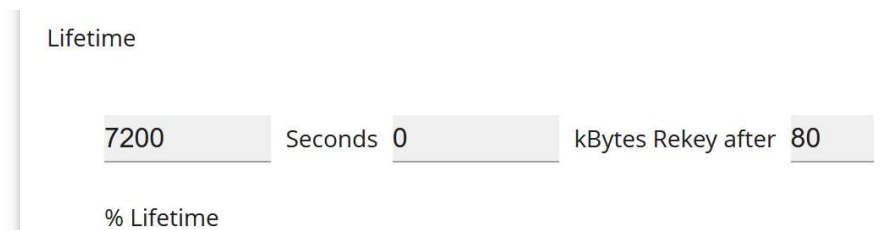- **Internet & Network > VPN > IPSec > Phase-1-Profiles > Edit**

Lifetime

14400 Seconds / Rekey after 80 % Lifetime

Set the values so that the validity of the Phase 1 parameters is shorter on the dialing 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 dialing 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!