Release Notes
System Software 2.2.1.1

Content

1 Release 2.2.1.1

1.1 Note
This version is only available for the W2022ac / W2022ac-ext devices.

1.2 New Features

- **WPA3:** The WPA3 encryption standard serves to improve the security of WLAN networks. There are new settings in the section **Security Settings** of the **Wireless LAN > WLAN > Wireless Networks (VSS) > New** menu. The settings **Security Mode** = *OWE-Transition* and **Security Mode** = *OWE* are used to create open networks.
  OWE (Opportunistic Wireless Encryption) only works with WPA3 enabled clients that have OWE implemented. Data transfer between the access point and the 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 data transfer between the access point and the client is encrypted, but it remains unencrypted for all others.
  With **Security Mode** = *WPA-PSK* or **Security Mode** = *WPA-Enterprise*, you can select **WPA Mode** = *WPA3* for WPA3 capable clients or **WPA Mode** = *WPA2 and WPA3* for WPA2 and WPA3 capable clients in the same network.

- **SNR Threshold:** The SNR Threshold parameter allows you to define a limit value for signal-to-noise ratio when communicating with a client. If an access point "sees" that one of its clients falls below this signal-to-noise ratio for longer than the tolerance time specified, it disconnects the client from the network. This forces the client to look for a new access point, i.e. to check which access point provides the best signal and connect to it.
  You can enable **SNR Threshold Management** under **Wireless LAN > WLAN > Wireless Networks (VSS) > New/Edit > Advanced Settings**.

- **Data Rate Trimming:** With Release 2.2.1.1, the Data Rate Trimming function is available. In order to display the function, under **Wireless LAN > WLAN > Radio Settings > Edit** the parameter **Operation Mode** must be set to *Access Point*.
  Data Rate Trimming allows you to optimize the performance of your WLAN. You can block low transfer rates and enforce the use of higher rates.
  When the use of low data rates is inhibited (so-called data rate trimming), the client is caused to connect to another access point more quickly as the distance to its current access point grows. The client must use the data rates specified for it. In the **Wireless LAN > WLAN > Wireless Networks (VSS) > New / Edit > Advanced Settings** menu, you can configure the rates to be supported using the **Data Rate Trimming** option. Depending on the selected frequency band, various predefined data rate profiles are available.

- **Max. number of clients - soft limit:** Select the **Wireless LAN > WLAN > Wireless Networks (VSS) > New** menu to limit the number of connected devices under **Client load balancing**.
  To avoid a radio module being used to its maximum capacity you can set

a "soft" restriction on the number of connected clients under **Max. number of clients – soft limit**. If this number is reached, new connection requests are initially rejected. If the client cannot find another wireless network and, therefore, repeats its request, the connection is accepted. Requests are definitively rejected only when the **Max. number of clients - hard limit** is reached.

- **Static gateway address and static DNS:** In the **Local Services > DNS** menu, you can enter fixed values for **Gateway Address** and **DNS**. This is useful, for example, if you want to download software from the company server and do not use DHCP or for data exchange with **be.SDx**.

- **Configurable Default Route:** In the **Networking > Routes > IPv4 Route Configuration > New** menu, you can configure a default route with the **Route Type** = *Default Route via Gateway* setting. Furthermore, you can configure network routes and host routes with **Route Type** = *Network Route via Gateway* and **Route Type** = *Host Route via Gateway*.

1.3 Changes

- -

1.4 Error corrections

- **Data frames – Count not correct (#3103):** If a **W2022ac** was connected to multiple devices via the same WLAN, it could happen that only the frames of the first device were counted correctly. *0* frames were displayed for the other devices.

- **Radio module – background scanning (#3102, #3101):** For a **W2022ac**, background scanning did not work.

- **Radio module – no neighbor APs (#3007):** Despite the radio module being active, no neighboring APs were displayed for the 2.4 GHz frequency band. After saving the configuration and rebooting the device, the neighbor access points were displayed correctly.

- **Channel selection (#3004):** The automatic channel selection did not work correctly; it did not select the optimum channel.

- **Radio module – Scanning incomplete (#2938):** With band steering enabled, not all channels were found in the 5 GHz band with automatic channel selection.

- **Radio module – background scanning (#2799):** During background scanning, packet loss occurred.

- **Security Updates:** Numerous security updates have been implemented.

1.5 Known restrictions

- The WLAN controller of the BOSS-based products (**be.IP**, **RS series**, **RXL**) currently does not support the newly added security functions WPA3 and OWE of **W2022ac**.

- It is not possible to downgrade to a previous software version or to overwrite version 2.2.1.1 with the same version. The attempt leads to a deadlock of the device, which must be corrected with a manual restart.