Release Notes
System Software 3.6.1.1

Content

1 Notes

Important: To install release 3.6.1.1, it is necessary that release 2.4.3.5 or higher is already installed on the access point. Access points with older versions must first be updated to release 2.4.3.5 before release 3.6.1.1 can be installed (otherwise the update to 3.6.1.1 aborts with an error message). If a very old version prior to 2.4.1.1 is still installed, these must first be updated to Release 2.4.1.1 as an intermediate step before Release 2.4.3.5 can then be installed to be able to install Release 3.6.1.1 afterwards. After the update to a release version of 3.2.1.3 or higher, a downgrade to an older version is ***no longer*** *possible because the minimum system software version had to be raised due to a chip firmware update integrated in Release 3.2.1.3.*

This version is only available for **W2022ac** and the **W2022ac-ext.** Please note that the Wi-Fi 6 access points **W2022ax** and **W2044ax** use the same release numbering and are also functionally comparable. However, the system software files are different.

The software image is now provided on the update server in two different formats:

- *.img*: Files with this file extension are used as before for updating the access point directly via the user interface or for updating via the WLAN controller.
- *.tgz*: Files with this file extension are required when updating the access points via Cloud Net Manager (Cloud Net Manager version 5.1.4 or higher). For this purpose, this file must be loaded into the Cloud Net Manager software library.

2 New features/changes

- **ER#6071: WLAN data prioritization** is now performed in compliance to RFC 8325 “Mapping Diffserv to IEEE 802.11” and its update RFC 8622 from Internet Engineering Task Force and thus **uses the state-of-the-art defaults for Wireless Multimedia (WMM) from Wi-Fi Alliance “Wi-Fi QoS Management™ Specification Version 2.0”**. Especially Voice over WLAN applications benefit from this change and are handled now with a higher correct priority. Voice data typically are tagged in Layer 3 IP header either with DSCP tag 44 (Voice Admit) or DSCP tag 46 (Expedited Forwarding). With the new mapping these data packets are now handled correctly in WLAN Layer 2 in WLAN priority class 6 (Voice) and not any longer in WLAN priority class 5 (Video).

- When managed by a WLAN Controller on WLAN networks with WPA Enterprise authentication a **separate RADIUS server for each wireless network can be rolled out to the APs now**. The ability to roll out multiple RADIUS servers to an AP is needed for use cases such as setup of “eduroam” WLAN networks from universities. Furthermore, when managed by a WLAN Controller on WPA Enterprise authentication an optional RADIUS accounting server for accounting of WLAN user access can be rolled out to the APs now.
  The use of this function requires system software version 10.2.12 Patch 4 or newer in the WLAN Controller.
- When managed by a WLAN Controller in case a **wrong RADIUS configuration** is rolled out to an AP **the AP now reports more helpful error messages for such a misconfiguration back to the WLAN Controller**. Like all error log messages reported by the APs to the WLAN Controller these error messages can be found in the WLAN Controller router under “Monitoring > Internal log” for the “WLC” subsystem with the “Error” level.
- When managed by a WLAN Controller **a factory reset can be performed on the APs via the WLAN Controller router** at “Wireless LAN Controller > Maintenance” page with the new WLAN Controller maintenance action “Restore factory defaults and reboot” now. This function is useful to remove old forgotten manual boot configurations on managed APs from previous other installations of these devices and to clean up the SIA file of managed APs from old obsolete error messages.
  The use of this function requires system software version 10.2.12 Patch 4 or newer in the WLAN Controller.
- **WLAN Controller management data (CAPWAP protocol data) is now tagged in Layer 3 IP header with DSCP tag 48** (CS6 / Network Control). When configuring QoS policies in networks CAPWAP data now can be prioritized easier with a match for this DSCP tag. In large networks with lots of concurrent user traffic a QoS configuration is recommended and will help to avoid losing control connection between WLAN Controller and Access Points and thus will make the WLAN Controller network more stable in these cases.
- The Security Mode **"WPA 3 Enterprise CNSA" has been added to the local AP GUI** in menu "Wireless LAN > WLAN > Wireless Networks (VSS) > edit" now. Previously it was only configurable via WLAN Controller.
- **The AP now displays in local GUI** in menu “System Management > Status” in the “System Information” **which (remote) configuration application (WLAN Controller, Cloud Net Manager / be.WLAN or Local Configuration) is currently managing the AP** and the current operational status of this configuration application. This status information is useful for clarifying essential configuration application conflicts and errors.
- The list of MAC Address Organizationally Unique Identifiers has been updated in local GUI.

3 Error corrections

- **ER#6487: Sporadically** after several days or even weeks of uptime on W2022ac AP **WLAN clients were still able to connect to the WLAN network but did not get any longer an IP address via DHCP from a DHCP server** in LAN and thus were not able any longer to the use WLAN on that AP until the affected AP was rebooted.
  Hint: In the unexpected case you observe this problem even with OSDx version 3.6.1.1 please disable “Cyclic Background Scanning” as the error was happening with the previous release OSDx 3.2.1.5 only in case this feature was enabled:
  - In case you configured your AP via the local GUI disable “Cyclic Background Scanning” in AP GUI menu “Wireless LAN > WLAN > Radio Settings > edit” for both WLAN radios.
  - In case you are using the WLAN Controller disable “Cyclic Background Scanning” via the WLAN Controller router in GUI menu “Wireless LAN Controller > AP Configuration > Radio Profiles > edit” for all existing radio profile (in default settings two).
- **ER#6460: Local GUI login failed** if you had set an admin password **with a non-ASCII character**.
- **ER#6461: Manual time setting via local GUI** in menu “System Management > Global Settings > Date and Time” **failed**.
- **ER#6537:** When managing the AP with be.WLAN **the CNM service configured wrong default values for RSSI threshold**.
- Various **rare system service crashes and kernel panics** (with a frequency of about one crash per device and month) **have been fixed**.
- In internal AP system log several undesired log messages on detected neighbour access points were removed.
- SIA file generation does not fail any longer on unexpected directory structure in coredump section and cannot fill up the AP flash memory any longer.
- With OSDx firmware versions 3.2.1.x **W2022ac access points did not update any longer an old system date (such as 1. January 1970) at least to firmware image compile time on system startup** and thus kept that old date in case the AP did not get the current date otherwise (such as NTP). This issue could cause problems with wrong old system dates when managing such an AP via be.WLAN due to certificate validation check which failed internally (not visible to the user) with “certificate is not valid yet” reason.

4 Known issues

- **The AP Steering** and **Radio Resource Management (802.11k)** settings are included in the configuration interface but have no function in this release.