Release Notes
System Software 3.2.1.3

Content

1 Notes

- *Important*
  In order to install release 3.2.1.3, 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 3.2.1.3 can be installed (otherwise the update to 3.2.1.3 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 in order to be able to install Release 3.2.1.3 afterwards.
  *After the update to Release 3.2.1.3, 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:

- The **maximum number of MAC filter entries** for wireless LAN network clients per wireless LAN network interface is again unlimited in the configuration and is only practically restricted by the free working memory of

the access point. At least *1024* entries are possible depending on the number of configured WLAN networks.

- Deleting and **changing SSIDs** used to take up to 30 seconds and now takes only a few seconds. The response time for configuration changes and page changes within the configuration interface has also been noticeably accelerated.
- The **RSSI threshold** function (accessible on the access point in the **Wireless networks > Advanced settings > Manage lower RSSI threshold** menu or set up via the WLAN controller) is now identical on the **W2022ac** and **W2022ac-ext to** the same function on the **W2044ax** and **W2022ax** access points. The SNR threshold function of software versions 2.4.3.5 and older has thus been replaced.
- The **SIA file** available from the **External Reporting > SIA** menu now contains more comprehensive device diagnostic data in a compressed archive file, including system crash logs and archived logs. This new SIA file is saved by default under a device-specific file name consisting of device type and serial number. In addition, when operating the access point on a WLAN controller, this SIA file can now be uploaded from the WLAN controller to a TFTP server during operation. Direct access to the access point's configuration interface is no longer necessary for this purpose.
- In the **Wireless LAN > WLAN > Radio module settings** menu**,** the configured wireless mode is displayed on the overview page.
- On devices with more than one **Ethernet port**, only the first Ethernet port is active during the device startup process. Further Ethernet ports are activated only after the startup phase.
- When operating on **Cloud Net Manager,** the access point reports the operating states of its WLAN radio modules to the server.
- OSDx-based access points can now record their **internal log** on an external syslog server when operating on a WLAN controller in the same way as BOSS-based access points.
- **ER#5525:** Kernel panics and other low-level system crashes of the access point are now logged in the access point's SIA file for easier troubleshooting by customer support, as are application crashes.

3 Error corrections

- **ER#5664:** When operating on the WLAN controller, some access points in certain configurations "froze" after several weeks and could no longer be accessed via the WLAN controller or the local configuration interface. Affected access points could only be reactivated by a cold start.
- **ER#5531**: The following vulnerabilities have been fixed:
  - CVE-2020-24588
  - CVE-2020-26144
  - CVE-2020-26139
  - CVE-2020-26146.
- **ER#5511:** Under certain circumstances, after the access point found a radar signal, it could stop transmitting until it was restarted, although it 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.

- When operating on a WLAN controller, **MAC filter access lists** configured in the WLAN controller for VSS profiles but **deactivated were** nevertheless rolled out on the access point and were also incorrectly active there.
- If the **MAC filter list** of allowed WLAN clients was modified in the access point during operation, WLAN clients already logged on to the WLAN were not immediately logged off, even though they were no longer allowed in the modified MAC filter list.
- After a runtime of several weeks, it could happen that the access point no longer had **enough RAM** available to perform an update of the system software. In this case, the access point previously had to be restarted before an update. Likewise, the general RAM consumption of the access points has been reduced so that more RAM is available during operation.
- **ER#5472:** When operating on a wireless LAN controller in conjunction with certain user-defined, permanently stored configurations of the access point, the WLAN of the access point could remain disabled after a reboot and subsequent automatic startup by the wireless LAN controller. This error occurred as of system software version 2.4.3.3.
- **ER#5723:** When operating on a WLAN controller, the access point did not report the WLAN clients connected with *OWE* to the WLAN controller for WLAN networks with security mode *OWE transition.* This error has been corrected.
- **ER#5484:** When operating on a Cloud Net Manager, the access point reported incomplete neighbor access point information to the Cloud Net Manager if the access point's system time was incorrect (e.g., due to an incorrectly set time server in the local network router). This error has been corrected.
- **ER#5676:** When operating on a Cloud Net Manager, the Cloud Net Manager server incorrectly reported the error message "Setup internal agent parameters" in its error log after successfully commissioning the access point. This error has been fixed in the access point.
- **ER#5517:** When operating on a WLAN controller, the access point now reports the actual step values it supports for optional transmission power reduction to the WLAN controller.
- **ER#5519:** In the case of neighbor access points in the 2.4GHz band with bandwidth 40MHz, their secondary channel was reported incorrectly to the WLAN controller in some cases. This error has been corrected.
- Neighbor access points with the outdated security mode *WPA* and neighbor access points with the still very rarely encountered, modern security mode *WPA 3 Enterprise CNSA* were not always detected correctly and, when operated on a WLAN controller, were usually reported to the WLAN controller with the **incorrectly detected security mode** *None in* these cases. This error has been corrected.
- During operation on the WLAN controller, the access point temporarily reported an incorrect value for the free RAM on the access point to the WLAN controller during initialization. Similarly, during continuous operation, the **free**

RAM on the access point was reported to the WLAN controller as being slightly too low.

- **ER#5567:** The local IP address of the access point was not communicated to Cloud Net Manager in the system status information.
- **ER#5664:** When operating on the WLAN controller, some access points in certain configurations "froze" after several weeks and could no longer be accessed via the WLAN controller or the local configuration interface. Affected access points could only be reactivated by a cold start.
- **ER#5473:** The local GUI set an outdated default server URL in the **System Management > Global Settings > System** menu when the Cloud Net Manager settings were deleted and recreated.

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.