Release Notes
System Software 3.6.1.1

Inhalt

1 Hinweise

*Wichtig: Um das Release 3.6.1.1 zu installieren, ist es notwendig, dass auf dem Access-Point bereits das Release 2.4.3.5 oder höher installiert ist. Access-Points mit älteren Versionen müssen zunächst auf Release 2.4.3.5 aktualisiert werden, bevor das Release 3.6.1.1 eingespielt werden kann (andernfalls bricht das Update auf 3.6.1.1 mit einer Fehlermeldung ab). Falls noch eine sehr alte Version vor 2.4.1.1 installiert ist, müssen diese als Zwischenschritt zunächst auf das Release 2.4.1.1 aktualisiert werden, bevor dann das Release 2.4.3.5 installiert werden kann, um im Anschluss Release 3.6.1.1 installieren zu können. Nach dem Update auf eine Release-Version von 3.2.1.3 oder höher ist ein Downgrade auf eine ältere Version **nicht** mehr möglich, da die minimale Systemsoftwareversion aufgrund eines in Release 3.2.1.3 integrierten Chip-Firmware-Updates angehoben werden musste.*

Diese Version steht nur für **W2022ac** und **W2022ac-ext** zur Verfügung. Bitte beachten Sie, dass die Wi-Fi-6-Access-Points **W2022ax** und **W2044ax** eine gleichlautende Release-Nummerierung verwenden und auch funktional vergleichbar sind. Die Systemsoftware-Dateien sind aber unterschiedlich.

Das Software-Image wird ab sofort auf dem Update-Server in zwei unterschiedlichen Formaten bereitgestellt:

- *.img*: Dateien mit dieser Dateiendung werden wie bisher zur direkten Aktualisierung des Access-Points über die Benutzeroberfläche oder für das Update über den WLAN-Controller verwendet.
- *.tgz*: Dateien mit dieser Dateiendung werden bei der Aktualisierung der Access-Points über den Cloud-Net-Manager (ab Cloud-Net-Manager-Version 5.1.4 benötigt. Dazu muss diese Datei in die Software-Bibliothek des Cloud-Net-Managers geladen werden.

2 Neue Funktionen/Änderungen

- **ER#6071:** Die **WLAN-Datenpriorisierung** erfolgt nun in Übereinstimmung mit RFC 8325 "Mapping Diffserv to IEEE 802.11" und dessen Update RFC 8622 von der Internet Engineering Task Force und **verwendet somit die aktuellen Vorgaben für Wireless Multimedia (WMM) der Wi-Fi Alliance "Wi-Fi QoS Management™ Specification Version 2.0"**. Insbesondere Voice-over-WLAN-Anwendungen profitieren von dieser Änderung und werden nun mit einer höheren korrekten Priorität behandelt. Sprachdaten werden typischerweise im Layer 3 IP-Header entweder mit DSCP-Tag 44 (Voice Admit) oder DSCP-Tag 46 (Expedited Forwarding) gekennzeichnet. Mit dem neuen Mapping werden diese Datenpakete nun im WLAN-Layer 2 korrekt in der WLAN-Prioritätsklasse 6 (Voice) und nicht mehr in der WLAN-Prioritätsklasse 5 (Video) behandelt.
- Bei der Verwaltung von WLAN-Netzwerken mit WPA-Enterprise-Authentifizierung durch einen WLAN-Controller **kann nun ein separater RADIUS-Server für jedes drahtlose Netzwerk auf die APs ausgerollt werden**. Die Möglichkeit, mehrere RADIUS-Server auf einen AP auszurollen, wird für Anwendungsfälle wie die Einrichtung von "eduroam"-WLAN-Netzwerken von Universitäten benötigt. Darüber hinaus kann bei der WPA-Enterprise-Authentifizierung durch einen WLAN-Controller nun ein optionaler RADIUS-Accounting-Server für die Aufzeichnung des WLAN-Benutzerzugriffs auf die APs ausgerollt werden.
  Die Nutzung dieser Funktion erfordert im WLAN-Controller die Systemsoftware Version 10.2.12 Patch 4 oder neuer.
- **Wird** bei der Verwaltung durch einen WLAN-Controller eine **falsche RADIUS-Konfiguration an einen AP ausgerollt, meldet der AP nun hilfreichere Fehlermeldungen** für eine solche Fehlkonfiguration **an den WLAN-Controller zurück**. Wie alle von den APs an den WLAN-Controller gemeldeten Fehlerprotokolle finden Sie diese Fehlermeldungen im WLAN-Controller-Router unter "Monitoring > Internes Protokoll" für das Subsystem "WLC" mit dem Level "Fehler".
- Wenn die APs von einem WLAN-Controller verwaltet werden, kann ein **Werks-Reset über den WLAN-Controller-Router** auf der Seite "Wireless LAN Controller > Wartung" mit der neuen WLAN-Controller-Wartungsaktion "Werkseinstellungen wiederherstellen und neu starten" durchgeführt werden. Diese Funktion ist nützlich, um alte vergessene manuelle Boot-Konfigurationen auf verwalteten APs aus früheren anderen Installationen dieser Geräte zu entfernen und die SIA-Datei der verwalteten APs von alten veralteten Fehlermeldungen zu bereinigen.
  Die Nutzung dieser Funktion erfordert im WLAN-Controller die Systemsoftware Version 10.2.12 Patch 4 oder neuer.
- **WLAN-Controller-Managementdaten (CAPWAP-Protokolldaten) werden nun im Layer-3-IP-Header mit dem DSCP-Tag 48** (CS6 / Network Control) **gekennzeichnet**. Bei der Konfiguration von QoS-Regeln in Netzwerken können CAPWAP-Daten nun einfacher mit einem Filter für dieses DSCP-Tag priorisiert werden. In großen Netzwerken mit viel gleichzeitigem

Benutzerverkehr ist eine QoS-Konfiguration empfehlenswert und hilft, den Verlust der Kontrollverbindung zwischen WLAN-Controller und Access Points zu vermeiden und macht das WLAN-Controller-Netzwerk in diesen Fällen stabiler.

- **Der Sicherheitsmodus "WPA 3 Enterprise CNSA" wurde in der lokalen AP-GUI** im Menü "Wireless LAN > WLAN > Drahtlosnetzwerke (VSS) > Bearbeiten" **hinzugefügt**. Zuvor war er nur über den WLAN-Controller konfigurierbar.
- **Der AP zeigt nun in der lokalen GUI** im Menü "Systemverwaltung > Status" in den "Systeminformationen" an, **welche (Fern-) Konfigurationsanwendung (WLAN-Controller, Cloud Net Manager / be.WLAN oder Lokale Konfiguration) den AP gerade verwaltet** und den aktuellen Betriebsstatus dieser Konfigurationsanwendung. Diese Statusinformationen sind nützlich, um wesentliche Konflikte und Fehler der Konfigurationsanwendung zu klären.
- Die Liste der MAC Address Organizationally Unique Identifiers wurde in der lokalen GUI aktualisiert.

3 Fehlerbeseitigungen

- **ER#6487:** Sporadisch konnten sich WLAN-Clients nach mehreren Tagen oder sogar Wochen Betriebszeit auf dem W2022ac-AP zwar noch mit dem WLAN-Netzwerk verbinden, bekamen aber keine IP-Adresse mehr per DHCP von einem DHCP-Server im LAN und konnten somit das WLAN auf diesem AP nicht mehr nutzen, bis der betroffene AP neu gestartet wurde.
  Hinweis: Sollten Sie dieses Problem wider Erwarten auch mit OSDx-Version 3.6.1.1 beobachten, deaktivieren Sie bitte den "Wiederkehrenden Hintergrund-Scan", da der Fehler mit der Vorgängerversion OSDx 3.2.1.5 nur auftrat, wenn dieses Feature aktiviert war:
  - Falls Sie Ihren AP über die lokale GUI konfiguriert haben, deaktivieren Sie den "Wiederkehrenden Hintergrund-Scan" im AP GUI Menü "Wireless LAN > WLAN > Einstellungen Funkmodul > Bearbeiten" für beide WLAN-Radios.
  - Falls Sie den WLAN-Controller verwenden, deaktivieren Sie den "Wiederkehrenden Hintergrund-Scan" über den WLAN-Controller-Router im GUI-Menü "Wireless LAN Controller > Access-Point-Konfiguration > Funkmodulprofile > Bearbeiten" für alle bestehenden Funkmodulprofile (in den Standardeinstellungen zwei).
- **ER#6460:** Die **lokale GUI-Anmeldung schlug fehl**, wenn Sie ein **Admin-Passwort mit einem Nicht-ASCII-Zeichen** festgelegt hatten.
- **ER#6461: Manuelle Zeiteinstellung über die lokale GUI** im Menü "Systemverwaltung > Globale Einstellungen > Datum und Uhrzeit" **schlug fehl**.
- **ER#6537:** Bei der Verwaltung des APs mit be.WLAN hat der **CNM-Dienst falsche Standardwerte für den RSSI-Schwellwert konfiguriert**.
- **Verschiedene seltene Abstürze von Systemdiensten und Kernel-Panics** (mit einer Häufigkeit von etwa einem Absturz pro Gerät und Monat) **wurden behoben**.

- Im internen AP-Systemprotokoll wurden mehrere störende Protokollmeldungen über erkannte Nachbar-Access Points entfernt.
- Die Erzeugung von SIA-Dateien scheitert nicht mehr an unerwarteten Verzeichnisstrukturen im Coredump-Bereich und kann den Flash-Speicher des AP nicht mehr füllen.
- Mit OSDx-Firmware-Versionen 3.2.1.x **aktualisierten W2022ac-Access-Points ein altes Systemdatum (z.B. 1. Januar 1970) beim Systemstart nicht mehr mindestens auf den Kompilierzeitpunkt des Firmware-Images** und behielten somit das alte Datum bei, falls der AP das aktuelle Datum nicht anderweitig (z.B. per NTP) erhielt. Dieses Problem konnte zu Problemen mit falschen alten Systemdaten führen, wenn ein solcher AP über be.WLAN verwaltet wurde, da die Zertifikatsüberprüfung intern (für den Benutzer nicht sichtbar) mit der Begründung "Zertifikat ist noch nicht gültig" fehlschlug.

4 Bekannte Probleme

- Die Einstellungen **AP-Steering** und **Verwaltung der Funkressourcen (802.11k)** sind in der Konfigurationsoberfläche enthalten, haben aber im vorliegenden Release keine Funktion.