RELEASE NOTES

RUCKUS LTE AP Release Notes SC 04.02.00

Part Number: 800-72813-001 RevA
Publication Date: December 2020

Contents

About this Release

This document provides release information for Ruckus LTE AP Release SC 04.02.0000 including information on new features, resolved issues, and unresolved issues.

Supported Hardware

Ruckus LTE AP Release SC 04.02.00 supports the following Access Point models:

P01-Q910-US02
P01-Q950-US02
P01-Q710-US02
P01-Q410-US01

NOTE

Legacy Access Points P01-Q910-US00 and P01-Q710-US00 are also supported, but without Carrier Aggregation (CA) capabilities.

New in this Release

List of features introduced in Ruckus LTE AP Release SC 04.02.00:

- **CMPv2 Certificate Enrollment Enhancements:** As part of the 4.2 release, AP supports below features for CMPv2 enrollment:
  - Support for FQDN for CMP server as well as Root CA repository.
  - IPv6 support: CMPv2 enrollment using an IPv6 CMP server as well as IPv6 Root CA repository.
  - HTTPS connection capability with CMPv2 server.
- **Secure Boot :** As part of the 4.2 release, AP supports authentication of images as part of secure boot. The authentication of the image is performed in two stages:

  1. At the time of bootup.
  2. At the time of software download.

  The following images of AP shall be signed and is authenticated as part of boot-up process and also at the time of software download:
  - boot.img
  - sbl1.mbn
  - emmc_apps.mbn
  - tz.mbn

  In addition to above two procedures, the authenticity of images and prevention from any malicious image to be written on RSC will be ensured via sector locking of eMMC flash.
- **ELKPI enhancements:** As part of the 4.2 release, AP shall read Offending App file present in halt event of AP from previous crash and send it as a part of cumulative reports to ELKPI. This value shall be displayed in ELKPI dashboards. On Prem DMS Support: As a part of this feature AP has been integrated with DMS and the following features supported on AP:
  - CMPv2 certificate enrollment with IPv4 CMP server
  - Macro Hand Over
  - MOCN
  - Supported alarms
  - Log Upload
- **Security Audit:** As part of this feature third party software packages were upgraded.
- **3rd Party Security Vulnerabilities:** A review of the third party packages has found multiple CVEs.

  The summary of upgrades is listed in the table below:

TABLE 1 Third Party Security Vulnerabilities

Software	Old Version	New Version
openssl	1.0.2j	1.0.2u
Python	2.7.9	2.7.18
Libssh2	1.2.4	1.9.0
Libevent	2.0.21	2.1.11
NTP	4.2.8p7	4.2.8p14
DNSMasq	2.70	2.81
ISC BIND	9.10.2-P2	9.11.19
ISC DHCP	4.1.2	4.1-ESV-R16
Libcurl	7.55.0	7.70.0
Strongswan	5.3.5	5.8.4

- **Macro Handover:** The LTE inter frequency neighbours configuration (EARFCN, Bandwidth, CIO) support from cloud is now available on Ruckus LTE AP SC 4.2.

  This feature describes about the mobility of UEs to inter-frequency neighbors. The inter-frequency neighbors can be Macro EnodeB or Home EnodeB types and at the same time inter-frequency neighbors can be in same band (intra-band) or different band (inter-band). The neighbor cells shall be configured statically through OAM configuration or dynamically through report CGI from UEs.

  As per the 3GPP specification inter-frequency neighbors are broadcasted in SIB5 for idle mode UEs and configured by RRC connection reconfiguration message for connected mode UEs and based-on events in measurement report from UE, handover in initiated from source RSC to target RSC. The target RSC can be a HomeEnodeB or Macro EnodeB type.

  The feature functionality added includes:

  – Configuration of Inter-frequency neighbor carriers from Cloud/CLI.
  – Handling of UE based neighbors (ANR) based on measurement report with report CGI.
  – Handling of X2 ENB Configuration Update message for EARFCN change of X2 neighbor cell.
  – Updating the neighbor table based on neighbor inactivity.

- **S1AP Cell Type support :**
  – Macro eNB support for SKU Q950.
  – Adding ECGI records to the Administration page with choice of either used by “Macro eNB” or “Home eNB”.
  – Configuring PCI range to be used by Home eNB on the Network configuration page.

- **PWS feature enhancement:** CBSD supports the following PWS-functionalities:
  – PWS restart indication procedure.
  – PWS failure indication procedure.
  – WarningAreaCoordinates support in WriteReplaceWarning procedure.

Resolved Issues

Resolved Issues	Description
AZ-4134	lte_oam crashed while setting EARFCN for interfreq carrier through CLI and several other issues.
AZ-2811	Inter-freq ANR & HO on the basis of UE measurement don't happen if neighbor is not already added through NL.
AZ-4239	Default values are not configuring on AP while adding interfreq carrier and neighborListLteCell.
AZ-4332	Handover preparation got triggered for scell of nbr AP.
AZ-4769	False alarm for certificate expired raised when iHems FQDN resolution failed.
AZ-4794	Grant suspension alarm (Alarm id - 135)not cleared even after grant authorized.
CBRSE-230	Kuhana-Fi 4.0 Crash LTE_OAM & SOMC.
CBRSE-255	SOMC CRASH on Q710 running 04.00.01.03.
CBRSE-303	Clients not connecting to the AP though AR is not enabled.
CBRSE-267	4.0.1 crash in locmgr.
CBRSE-295	Comast Q710s crash with SOMC running 04.01.00.
CBRSE-332	Clients not able to do data session with samsung galaxy S10 SM-G973U.

Known Issues

Known Issues	Description
AZ-5134	Neighbor addition did not happen when UE has sent the CGI report and the PCI range is overlapping.
AZ-5148	SIB decoding failure during NL scan for AP with TDD-6 configuration.
AZ-5219	ReportCGI for band-66 neighbor failed with iPhone11 and iPhone12 (UE is sending empty CGI report).
AZ-5221	In SPV from cloud Cell-Identity received, but "CELL_TYPE" was missing.
AZ-5104	[Q950] No HB is initiated after LTE AP(already granted) is reboot from cloud.

Upgrading AP Software

This topic provides information on upgrading the AP to secure SmallCell 4.2 default build (15 onwards) or above.

Case 1: Base build on AP is SmallCell 4.1 or above:

1. Directly upgrade AP to SC4.2 default build (build 15) or above.

Case 2: Base build on AP is lower than SmallCell 4.1 (SC4.0, SC3.0, SC2.4, and so on).

1. Upgrade AP to SC4.2 intermediate (build 14).
2. Post this, upgrade AP to secure SC4.2 default build (build 15) or above.

Downgrading AP Software

This topic provides information on downgrading the AP to secure SmallCell 4.2 default build (15 onwards) or above.

Case 1: Base build on AP is SmallCell 4.2 patch build or above or default build (build 15):

1. Directly downgrade AP to any other SC 4.2 patch build or default build (build 15).

Case 2: Base build on AP is any SC 4.2 patch build or default build (build 15) to lower builds (SC4.0, SC3.0, SC2.4, etc):

1. Downgrade AP to SC4.2 intermediate (build 14).
2. Post this, downgrade AP to lower builds.

Determining Software Upgrade or Downgrade

Use this table to determine software upgrade and downgrade.

Base Build	Destination Build	Actions
SC 4.2 Default Build	SC 4.2 Patch Build	Upgrade
SC 4.1 or above	SC 4.2 Default Build (build 15) or above	Upgrade
Build lower than SC4.1 (SC 4.0, SC 3.0, SC 2.4, and so on.)	SC 4.2 Default Build (build 15) or above	Upgrade AP to SC4.2 intermediate (build 14) and then upgrade AP to secure SC4.2 default build (build 15) or above
SC 4.2 Patch Build	SC 4.2 Default Build	Downgrade
SC 4.2 Default Build	Build lower than SC 4.2 (SC 4.1, SC 4.0, SC 3.0, SC 2.4, and so on)	Downgrade AP to SC4.2 intermediate (build 14) and then downgrade AP to lower builds.

COMMSCOPE®
RUCKUS®

350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com