COMMSCOPE®
RUCKUS ®

RUCKUS LTE AP Management Release Notes, 20.03

Supporting Software Release 20.03 Patch 1

Contents

Overview

This release of RUCKUS LTE AP Management includes UI enhancements and defect fixes

LTE AP Management 20.03 Release Notes

New in this Release

Feature List

The following sections lists new features for the LTE AP Management release.

- **LTE Security Gateway**: RUCKUS Clould LTE AP Management now lets you enable or disable IPv6 inside IPv4 tunnel allocation. You can now configure the security gateway in the IPv6, IPv4 or FQDN format.

Supported APs

The following table lists the supported LTE APs in the current release.

TABLE 1 Supported LTE APs

APs	Category	Property
Q410	Indoor	- Plug-in LTE: Low power AP - Stand-alone or plugged with R510/R610 Wi-Fi AP models. **NOTE** Q410 always connects with PoE+ source only. Wi-Fi APs may derive power from "PoE out" port on Q410 when plugged-in. - Single RF Carrier, 2x2 @ 1/2 W EIRP - Ceiling or Wall mount
Q710	Indoor	- High-Capacity LTE - Dual RF Carrier 2x2 @ 1W EIRP - Ceiling or Wall mount
Q910	Outdoor	- Category A LTE - Dual RF Carrier 2x2 @ 1W EIRP - Pole, Wall, or Strand-mount
Q950	Outdoor	- High Power Outdoor - Category B CBSD - Up to 50/100W EIRP achievable with external antennas 4T4R, 200Mbps (40MHz) - Fiber AND Ethernet w/daisy chaining -48VDC

Release Information

This section summarizes product information for the RUCKUS LTE AP Management 20.03 Patch 1 release.

Product Name: RUCKUS LTE AP Management

Release Version: 20.03_LTE Patch 1 (Build 25)

Release available: 29 March 2021

- **Management Service**: Feature enhancements and defect fixes

Server IP Addresses

Service	FQDN	Address	Protocol 1	Protocol 2	Protocol 3	Protocol 4
Qualcomm® Location (XTRA Predicted Satellite Data Service)	xtrapath1.izatcloud.net	Geo	TCP/80 HTTP			
Ruckus SC-Registrar	sc-registrar.ruckuswireless.com	34.211.175.172	ICMP Echo	TCP/443 SSL		
Ruckus SC-Registrar	sc-registrar.ruckuswireless.com	34.212.162.133	ICMP Echo	TCP/443 SSL		
CommScope SAS (STA)	https://stasas.sascms.net:8443	Geo	TCP/443 SSL			
CommScope SAS (Production)	https://cbsd-iot.sascms.net:8443	Geo	TCP/443 SSL			
Federated Wireless SAS	https://sc.federatedwireless.com:443/v1.2	Geo	TCP/443 SSL			
Google SAS (STA)	https://www.google-sas.com/vendor/	Geo	TCP/443 SSL			
Google SAS (Production)	https://sas.goog/v1.2/	Geo	TCP/443 SSL			
Ruckus NTP Server	ntp.cloud.ruckuswireless.com	104.154.107.129	UDP/123 NTP			
Ruckus NTP Server	ntp.cloud.ruckuswireless.com	146.148.32.216	UDP/123 NTP			
Ruckus Cloud HeMS SeGW 1	NA	104.197.44.198	ICMP Echo	UDP/500 IKE	ESP Protocol 50	UDP/4500 NAT-T
Ruckus Cloud HeMS SeGW 2	NA	35.225.228.188	ICMP Echo	UDP/500 IKE	ESP Protocol 50	UDP/4500 NAT-T
Ruckus Cloud HeMS SeGW 3	NA	35.202.152.35	ICMP Echo	UDP/500 IKE	ESP Protocol 50	UDP/4500 NAT-T
Ruckus Cloud HeMS SeGW 4	NA	35.232.65.10	ICMP Echo	UDP/500 IKE	ESP Protocol 50	UDP/4500 NAT-T

NOTE
This list does not contain a DNS server because the AP is using the customer DNS server and therefore doesn't require a special firewall rule.

NOTE
Geo = IP may change depending upon the geo-location. Please type "nslookup <FQDN>" on cmd/ Terminal prompt to detect the exact IP address.

NOTE
This list contains ports for IKE/EXP with or without NAT-T. This list does not contain an EPC SeGW; customer is using private EPC.
Addresses marked "Geo" are using geographic DNS resolution and must be statically configured on the MEC DNS server.

How Do I Get Support?

For product support information and details on contacting the RUCKUS Customer Services and the Support Team, go to the RUCKUS Support portal: https://support.ruckuswireless.com, or https://www.ruckuswireless.com and select **Support**.

Upgrading AP Software

This topic provides information on upgrading the AP to secure SmallCell 4.3 default build or above and also downgrading the AP from secure SmallCell 4.3 default build or above.

Follow these steps to upgrade the AP software.

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

1. Directly upgrade AP to SC4.3 default build or above.

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

2. Directly upgrade AP to SC4.3 default build or above.

Downgrading AP Software

Follow these steps to downgrade the AP software.

Case 1: Base build on AP is SmallCell 4.3

1. Directly downgrade AP to any other SC 4.3 patch build or default build.

Case 2: Base build on AP is any SC 4.3 patch build or default build to lower builds (SC4.0, SC3.0, SC2.4, and so on)

2. Downgrade the AP software to SC 4.2 intermediate (build 14).

3. Downgrade the AP software to lower builds.

Determining Software Upgrade or Downgrade

Use this table to determine software upgrade and downgrade.

Base Build	Destination Build	Actions
SC4.3 Default build	SC4.3 Patch build	Upgrade
SC4.1 or above	SC4.3 Default build or above	Upgrade
Build lower than SC4.1 (SC4.0, SC3.0, SC2.4, and so on.)	SC4.3 Default build or above	Upgrade
SC4.3 Patch build	SC4.3 Default build	Downgrade
SC4.3 Patch build	4.2 build 14	Downgrade
SC4.3 Default build	Build lower than SC4.2 build 14 (SC4.2, SC4.1, SC4.0, SC3.0, SC2.4, and so on)	Downgrade AP to SC4.2 intermediate (build 14) and then downgrade AP to lower builds.

Issues and Fixes

Resolved Issues

The following table provides information on the known issues in the current release.

Resolved Issues	Description
LTE-7261	Cell_Type GPV failure (AP returns invalid parameter name).
LTE-7286	GPV failure occurs while changing the cell type if the AP model builds are different in SKUs.
LTE-7289	Wrong EARFCN bandwidth dropdown value while configuring MACRO EARFCN.
LTE-7284	AP initiated IKE for EPC even when the CMP enrollment got failed after factory upgrade.
LTE-7303	SAS shows negative numbers for SAS availability.
LTE-7306	Cloud SeGW should not assign low range 10 Net addresses.
CBRSE-341	The venue LTE settings screen is blank.

Open Issues

Following is a list of unresolved issues in this release.

Open Issues	Description
LTE-5165	An unexpected technical error access denied appears while navigating for the AP view.
LTE-6127	In certain corner cases, the available ECGI count shows lower than expected.
LTE-6504	Not removing invalid e-mail addresses causes Amazon to lock our account
LTE-6981	Invalid date is displayed for alarms.
LTE-7141	CMP re- enrollment should not be initiated on updating crypto parameters from Cloud, and on AP reboot.
LTE-7146	Throughput is not getting updated on the Cloud.
LTE-7159:	A customer inherits the privileges from the superuser account instead of the customer account.
LTE-7160	The delete AP operation fails (error - the configuration database is locked).
LTE-7163	AP is not operational after a software downgrade.
LTE-7171	Cloud is sending the venue level LED parameter during changing any venue level parameter or software upgrade and downgrade causing the AP level LED OFF state change to ON.
LTE-7173	GPV is failing when adding AP.
LTE-7178	Errors when adding AP/Factory Reset AP and not become operational.
LTE-7181	Adding PLMN ID and re-ordering PLMN IDs fails with Error Code 9003.

Limitations

Band Change

> **NOTE**
> We are changing the default AP configuration to Band 48 (CBRS Band). You can check the band of operation for your AP by clicking on **AP** -> **AP Properties** -> **More**.
> If your Venue was previously customized to operate on Band 42/43, and you want to continue to do so, do get in touch with your Ruckus Representative for help, or open a support case.

Adding AP After Deletion

Following the deletion of AP from a Venue, you must wait for a few minutes before adding back to the Venue to prevent a scenario where the delete operation is not completed prior to the add operation.

CBSD- SAS Communication

The AP registration with SAS cycle (CPAS) may take up to 24 hours; thus, grant may not be available for up to 24 hours.

COMMSCOPE®
RUCKUS®