

Ruckus IoT 1.4 Release Notes

Supporting IoT Controller Release 1.4

Copyright, Trademark and Proprietary Rights Information

© 2019 CommScope, Inc. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change.

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMSCOPE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

ARRIS, the ARRIS logo, CommScope, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, Edgelron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, and ZoneFlex are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Overview	4
Features.....	4
Hardware and Software Compatibility	4
Release Information	5
Caveats, Limitations, and Known Issues	6
Component: IoT feature in Access Point with IoT Module I100	6
Component: Ruckus IoT Controller.....	6
Limitations.....	6
Best Practices.....	7
Supported Devices	7

Overview

This document provides release information about Ruckus IoT Suite 1.4 a versatile system for managing IoT devices. The Ruckus IoT Suite is a collection of network hardware and software infrastructure components used to create an IoT access network that is comprised of four elements:

- Ruckus IoT-ready Access Points (APs)— in addition to the wall-mount H510, the ceiling-mount R510, the outdoor model T310, the ceiling-mount R610, R710, and R720, the outdoor models E510, and T610 as of this release the following additional AP models are now IoT-ready: Indoor Access Point R730 (802.11 ax) and Indoor Access Point C110
- Ruckus IoT Modules—A NEW device that attaches to a Ruckus IoT-ready AP and supports standards such as Bluetooth Low Energy (BLE), Zigbee, LoRa and more. Our first IoT Module, the I100, will support BLE or Zigbee within the same enclosure.
- Ruckus SmartZone Controller—existing WLAN controller, which provides basic networking information for both the WLAN and the IoT access network.
- Ruckus IoT Controller—A NEW virtual controller, deployed in tandem with a Ruckus SmartZone Controller, that performs connectivity, device, and security management functions behind the scenes for non-WiFi devices. Our IoT Controller also facilitates cross-solution endpoint communication and provides APIs for northbound integration with IoT cloud services.

This document provides a list of the release components, their versions, a link to documentation, as well as caveats, limitations, and known issues in this release.

Features

Ruckus IoT-1.4 Suite provides the following update:

- Multi-Mode Radio Support in R730 (1-Zigbee and 1-BLE only supported)
- Gateway as a Beacon
- BLE Visualization
- AA Operator Key support
- Statistics Push (MQTT Based)
- Connector Gateway Mapping (connector enable/disable on per Gateway basis)
- Connector Gateway Heartbeat
- iBeacon and Eddystone Vendor UUID Filtering
- N+1 Enhancement (Master/Slave replacement and Force Fallback)

Hardware and Software Compatibility

This release is compatible with the following controller and access point hardware and software.

Compatible Hardware:

- C110 Access Point (C110)
- H510 Access Point (H510)
- R510 Access Point (R510)
- R610 Access Point (R610)
- R710 Access Point (R710)

- R720 Access Point (R720)
- T310 Access Point (T310)
- E510 Access Point (E510)
- T610 Access Point (T610)
- R730 Access Point (R730)
- I100 IoT Module (I100)

Compatible Software:

- Virtual SmartZone High Scale (vSZ-H)
- Virtual SmartZone Essentials (vSZ-E)
- SmartZone 100 (sz-100)
- Ruckus IoT Controller (RIoT)

Release Information

This section lists the version of each component in this release.

vSCG (vSZ-H and vSZ-E), and SZ-100:

- WLAN Controller version: 5.1.1.2.15014
- Control plane software version in the WLAN Controller: 5.1.1.2.15000
- AP firmware version in the WLAN Controller: 5.1.1.2.15014

RIoT:

- Ruckus IoT Controller version: 1.4.0.0.17
- VMWare ESXi version: 5.5 and later
- VMWare VM Player version: 12 and later
- Oracle VirtualBox version: 5.1.20 and later
- Google Chrome version: 61 and later
- Mozilla Firefox version: 56 and later

Fixed Issues:

The following ER and Field issues are fixed for this release:

TABLE 1 Fixed Issues

Key	Summary
IOTE-39	IOTE-32 Dashboard changes for Connector Gateway Heartbeat
IOTE-37	CLI should provide an option to go back to the main menu.
IOTE-27	VRIoT shell access via sesame
IOTE-25	Assaabloys visionline connector to support webclient based authentication
IOTE-13	IoT Controller WebUI enhancement to show BLE devices
ER-7432	IOT-1.3.0.0.14- GUI would not update the AP IP address.

Caveats, Limitations, and Known Issues

The following are the caveats, limitations and known issues.

Component: IoT feature in Access Point with IoT Module I100

- IOTC-2434 - Some Zigbee Devices does not report the current value of the attributes.
Workaround - Try to manually query from the UI. Not guaranteed to work as it is device specific.
- IOTC-2679 - Gateway: Able to execute rkscli commands even though internal(for H510)/External(R730) interfaces not available
Workaround - None
- IOTC-2597 - Controller:Factory default AP tx power shows as 6 not setting to max value
Workaround - Manually set the tx-power to max from the UI

Component: Ruckus IoT Controller

- IOTC-2655 - device gets NOT PERMITTED if controller has upgraded to 1.4 and AP is in 1.3
Workaround - upgrade AP first and then controller
- IOTC-2673 - after downgrading from 1.4 to 1.3 N+1 process is not running and both master and slave are not active
Workaround - Disable N+1 and reconfigure
- IOTC-2666 - All Gateways are getting selected when Tag based filter is applied.
Workaround - Do not select using the select all checkbox instead select individually
- IOTC-2590 - Using the search box in the controller UI to search for specific beacons is not functional. An HTTP 400 not found error will be seen
Workaround - None
- IOTC-2434 - Move to level Reported values are not updated for SLV Zigbee bulb in Device Information field.
IOTC-2338 - Osram bulbs doesn't report attribute changes for operation commands (Color, Hue and Level)
Workaround - press the refresh button next to the attribute to send the read command. Some devices may not respond
- IOTC-2703 - after upgrade from 1.3.0.0.14 to 1.4.0.0.16 total beacons widget is not available for adding to dashboard
Workaround - reset the dash board and add the widgets back to the dashboard
- IOTC-2733 - Unable to disable the BLE plugins for the offline AP even though the plugin tags gets removed
Workaround - Once the AP is online add the removed tags and remove it to disable the plugin in the AP
- IOTC-2734 - CDS configured with verify certificate enabled will not work after N+1 failover
Workaround - Edit the plugin and copy paste the certificate and save.

Limitations

- N+1 can be disabled (from Master) even when Slave is not reachable. When Slave comes back online, need to delete and create a new Slave controller.
- N+1 Auto Fallback is not supported (If Master is back online, Slave will run as Active Slave)

- Database backup and restore is not supported across major releases.
- Gateway supporting multi-mode causes IoT by AP protocol count to go wrong as each mode is considered as a separate AP
- IoT co-ex feature is not supported on multi-mode Gateway (R730)

Best Practices

- Both IoT Controller and vSZ/AP need to be upgraded to their release versions of 1.4.0/5.1.1.2 together and upgrade only from the release versions of 1.3, or with vSZ/AP from 3.6.1.0 and above is supported.
- Upgrade is supported only on +1. In case of lower version eg. 1.2 then controller needs to be upgraded to 1.3 and then to 1.4
- Time and Timezone should be properly set in Ruckus IoT Controller.
- N+1 works on Virtual IP mode. For successful failover AP MQTT Broker should be configured for Virtual IP.
- N+1 Configuration Sync happens every 5 minutes. If a configuration change and failover happened within the 5 minutes window, new configuration will be lost.
- In N+1 mode make sure Master and Slave have the same admin credentials (password).
- The IoT Controller (4vCPU) at max supports upto 400 packets/second and any load above this could lead to controller instability. Capacity planning needs to be taken care of during deployment so as not to exceed the limit.
- Use the Replace master option in N+1 only after making sure master is not reachable from slave
- For information on clusters, refer to this externally available Zigbee Alliance Zigbee Cluster Library 6 document at <http://www.zigbee.org/~zigbeeor/wp-content/uploads/2014/10/07-5123-06-zigbee-cluster-library-specification.pdf>.

Supported Devices

This section documents the supported IoT end devices. Multiple other devices may work with this release but they have not been validated.

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
Vingcard Signature	Lock	Zigbee	Assa-Abloy	AA_LOCK	
Vingcard Essence	Lock	Zigbee	Assa-Abloy	AA_LOCK	
Yale YRD220/240 TSDB Display Lock	Lock	Zigbee	Assa-Abloy	Yale	YRD220/240 TSDB
Yale YRD210 Push Button Lock	Lock	Zigbee	Assa-Abloy	Yale	YRD210 Push
Smartcode 916	Lock	Zigbee	Kwikset	Kwikset	SMARTCODE_DEADBOLT_10T
Smartcode 910 (450201)	Lock	Zigbee	Kwikset	Kwikset	
Lightify (RGB) Model 73674	Bulb	Zigbee	Osram	OSRAM	LIGHTIFY A19 RGBW
Lightify Model 73693	Bulb	Zigbee	Osram	OSRAM	LIGHTIFY A19 Tunable White45856
Lightify Model 73824	Bulb	Zigbee	Osram	OSRAM	
Element Color Plus	Bulb	Zigbee	Sengled	sengled	E11-N1EA
Bulb - LED	Bulb	Zigbee	Sengled	sengled	Z01-A19NAE26
E11-G13	Bulb	Zigbee	Sengled	sengled	E11-G13
Lux	Bulb	Zigbee	Philips	Philips	LWB004

Supported Devices

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
SLV E27 Lamp Valetto (Zigbee 3.0)	Bulb	Zigbee 3.0	SLV		
GE Smart Dimmer	Switch	Zigbee	GE	Jasco Products	45857
GE Smart Switch	Switch	Zigbee	GE	Jasco Products	45856
Smart Plug	Plug	Zigbee	Centralite	Centralite	4257050-ZHAC
Zen Thermostat	Thermostat	Zigbee	Zen Within	Zen Within	Zen-01
ZBALRM	Alarm	Zigbee	Smartenit		Model #1021 A
Temp, Humidity Sensor	Sensor	Zigbee	Heiman	HEIMAN	HT-N
Gas detector	Sensor	Zigbee	Heiman	HEIMAN	GASSensor-N
Contact Sensor/Door Sensor	Sensor	Zigbee	Centralite	Centralite	3300-G
3-Series Motion Sensor	Sensor	Zigbee	Centralite	Centralite	3305-G
Temperature Sensor	Sensor	Zigbee	Centralite	Centralite	3310-G
Revogi Lamp	Bulb	BLE	Revogi	Revogi	
Panic Button	Beacon	BLE	TraknProtect		
Tray Beacon	Beacon	BLE	TraknProtect		
Asset Beacon	Beacon	BLE	TraknProtect		
Card Beacon	Beacon	BLE	TraknProtect		
Card Tag	Beacon	BLE	Kontakt.io		CT18-3
Beacon Pro	Beacon	BLE	Kontakt.io		BP16-3
Asset Tag	Beacon	BLE	Kontakt.io		S18-3



© 2019 CommScope, Inc. All rights reserved.
Ruckus Wireless, Inc., a wholly owned subsidiary of CommScope, Inc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com