

Ruckus IoT 1.5 Release Notes

Supporting IoT Controller Release 1.5

Copyright, Trademark and Proprietary Rights Information

© 2020 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

Document History	4
Overview	4
Features.....	4
New in This Release	5
Changed Behavior	5
Hardware and Software Support	6
Release Information	6
Known Issues	8
Component: IoT feature in Access Point with IoT Module I100	8
Component: Ruckus IoT Controller.....	8
Limitations.....	9
Best Practices.....	9
Resolved Issues	10
Supported Devices	10

Document History

Revision Number	Summary of changes	Publication date
A	Initial release notes.	January, 2020
B	Added IoT Controller HDD expansion.	January, 2020
C	Added note on Security Advisory.	February, 2020

Overview

This document provides release information about Ruckus IoT Suite 1.5 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), the Indoor Access Point C110, and the LTE access point M510.
- 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-1.5 Suite provides the following update:

- NodeRed Rules Engine
- LoRaWAN Network Server (LNS)
- Telkonet Energy Management Devices Integration
- Soter anti-vaping sensor
- IoT Controller Licensing feature for enabling the controller and a sets of IoT Gateways
- Licensing architecture. RTU and AP capacity licenses can be applied in the IoT controller UI. Initial 'free' option is limited to 5 APs and 90 days beyond which a trial or permanent license must be applied.
- Beacon as a Service extension with more configurability including Generic Beacon
- Multi-vendor generic Beacon reception support for simultaneous connection to multiple cloud back-ends
- Support for Custom beacon in Beacon as a Service feature
- Ruckus SDK for third-party plugin programming for generic BLE devices
- Offlink IoT VLAN for supporting multiple IoT VLANs from one IoT Controller
- KVM virtualization platform support for the IoT Controller
- Compliant with California Senate Bill-327 requirements for information privacy of IoT devices.

New in This Release

Ruckus IoT-1.5 Suite provides the following update:

- NodeRed Rules Engine for automation of various sensors and devices
- LoRaWAN Network Server (LNS) for long range networks
- Telkonet Energy Management Devices Integration
- Soter anti-vaping sensor
- IoT Controller Licensing feature for enabling the controller and a sets of IoT Gateways
- Licensing architecture. RTU and AP capacity licenses can be applied in the IoT controller UI. Initial 'free' option is limited to 5 APs and 90 days beyond which a trial or permanent license must be applied.
- Beacon as a Service extension with more configurability including Generic Beacon
- Multi-vendor generic Beacon reception support for simultaneous connection to multiple cloud back-ends
- Support for Custom beacon in Beacon as a Service feature
- Ruckus SDK for third-party plugin programming for generic BLE devices
- Offlink IoT VLAN for supporting multiple IoT VLANs from one IoT Controller
- KVM virtualization platform support for the IoT Controller
- Compliant with California Senate Bill-327 requirements for information privacy of IoT devices.

Changed Behavior

STOP and READ before upgrading to 1.5

IoT Controller Licensing:

Before upgrading to 1.5 release, please make sure you have bought enough licenses. The licenses should be uploaded to 1.5 controller for uninterrupted services. Please refer the below links on how to get licenses and to contact support.

KBA: Support Activation from Support Portal<https://support.ruckuswireless.com/articles/000008284>

KBA: On how to find serial number of vRIOT controller<https://support.ruckuswireless.com/articles/000010095>

<https://support.ruckuswireless.com/contact-us>

IoT Controller Harddisk Resize:

In 1.5 the default IoT Controller's HDD size is increased to 20GB. In pre-1.5 version the size is just 8GB. So before upgrading to 1.5, customer is expected to increase the HDD to 20GB. Below are the steps and examples.

- Pre-1.5 IoT Controller shut down (power off).
- Resize or Expand the partition to 20GB.
- **VirtualBox:**
 - Go to Vbox installed location and use VBoxManage (cli command tool) to resize. Installed location (HDD) can be acquired from the VBox UI.
 - Execute “VBoxManage modifymedium vriot-1.4.0.0.17.vdi --resize 20480” . In the above command vriot-1.4.0.0.17.vdi, should be replaced with the name of the VDI file of the IoT Controller.
 - Power on VM.
- **VMWare (Workstation or ESX/ESXi):**
 - Go to settings (edit settings) and click on existing HDD.
 - Click on Expand option and set value as 20GB and perform expand.

- Power on VM.
- Bring up 1.4 controller.
- Upload the 1.5 image. In case the free space is less than 3GB, then need to free up space before the upload.
- Perform upgrade as usual.

Hardware and Software Support

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)
- M510 Access Point (M510)
- 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: 5.1.1.2.15524
- Control plane software version in the WLAN Controller: 5.1.1.2.15000
- AP firmware version in the WLAN Controller: 5.1.1.2.15524

RIoT:

- Ruckus IoT Controller version: 1.5.0.0.34
- VMWare ESXi version: 5.5 and later
- VMWare VM Player version: 12 and later
- KVM Linux virtualizer version: 1:2.5+dfsg-5ubuntu10.42 and later

- Oracle VirtualBox version: 5.1.20 and later
- Google Chrome version: 61 and later
- Mozilla Firefox version: 56 and later

SDK:

- Ruckus IoT SDK version: SDK-1.0

TABLE 1 Release Build Compatibility Matrix

Release	IoT Controller	SZ	AP	Supported AP Models
IoT GA 1.0	1.0.0.0.25	3.6.1.2.10051	3.6.1.2.10040	H510, R510, T310d
IoT GA 1.1	1.1.0.0.6	3.6.1.2.12010	3.6.1.2.12007	H510, R510, T310d
IoT GA 1.1MR1	1.1.0.0.6	3.6.1.2.12012	3.6.1.2.12009	H510, R510, T310d
IoT GA 1.2	1.2.0.0.22	3.6.1.2.12535	3.6.1.2.12535	H510, R510, T310d, R610, R710, R720, T610
IoT GA 1.2MR1	1.2.0.0.24	3.6.1.2.12538	3.6.1.2.12538	H510, R510, T310d, R610, R710, R720, T610
IoT GA 1.3	1.3.0.0.14	3.6.1.2.13022	3.6.1.2.13022	H510, R510, T310d, R610, R710, R720, T610
SZ 5.1.1.0	1.2.0.0.24	5.1.1.0.589	5.1.1.0.619	H510, R510, T310d, R610, R710, R720, T610, R730
SZ 5.1.1.0MR1	1.2.0.0.24	5.1.1.0.598	5.1.1.0.624	H510, R510, T310d, R610, R710, R720, T610, R730
SZ 5.1.1.2	1.3.1.0.1	5.1.1.2.14019	5.1.1.2.14019	H510, R510, T310d, R610, R710, R720, T610, R730
SZ 5.1.2	1.3.1.0.1	5.1.2.0.302	5.1.2.0.373	H510, R510, T310d, R610, R710, R720, T610, R730, R750
IoT GA 1.4	1.4.0.0.17	5.1.1.2.15014	5.1.1.2.15014	H510, R510, T310d, R610, R710, R720, T610, R730, C110
IoT 1.5	1.5.0.0.34	5.1.1.2.15524	5.1.1.2.15524	H510, R510, T310d, E510, R610, R710, R720, T610, R730, C110, M510

TABLE 2 IoT Upgrade Support Matrix

Version	GA-1.0	GA-1.1	GA1.1MR1	GA-1.2	GA1.2MR1	GA-1.3	5.1.1.2 (1.3.1.0)	GA-1.4	GA-1.5
GA-1.0	Yes	Yes	Yes	No	No	No	No	No	No
GA-1.1	No	Yes	Yes	Yes	Yes	No	No	No	No
GA1.1MR1	No	No	Yes	Yes	Yes	No	No	No	No
GA-1.2	No	No	No	Yes	Yes	Yes	Yes	No	No
GA1.2MR1	No	No	No	No	Yes	Yes	Yes	No	No
GA-1.3	No	No	No	No	No	Yes	Yes	Yes	No
5.1.1.2 (1.3.1.0)	No	No	No	No	No	No	Yes	Yes	No
GA-1.4	No	No	No	No	No	No	No	Yes	Yes
GA-1.5	No	No	No	No	No	No	No	No	Yes

Fixed Issues:

Known Issues

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

TABLE 3 Fixed Issues

Key	Summary
IOTE- 11	Add KVM Image support for IoT Controller
SEC-232	Upgrade IoT Controller kernel to address CVE-11477 and CVE-11478
IOTC-2726	Mandate change of default password at install of IoT Controller
IOTC-2723	Support for asynchronous BLE alerts from connected sessions.
IOTC-2719	Make Beacon reception aggregation interval configurable.
IOTC-3006	Unprotected APIs in IoT Controller fixed addressing CVE-2020-8005, as described in Ruckus Advisory ID 20200205.

Known Issues

The following are the caveats, limitations and known issues.

Component: IoT feature in Access Point with IoT Module I100

- IOTC-2691-Ruckus IOT Controller: Three network interfaces are shown for the R730 AP while connecting the AP to old Controller
Workaround - None

Component: Ruckus IoT Controller

- IOTC-3087/IOTC-3005-In a DB restored controller license alert and second license upload will not work
Workaround - None.
- IOTC-3078-Total LNS count is displaying blank in dashboard page in firefox browser
Workaround - None.
- IOTC-3075-Only the first 10 APs is shown in the Beacons (IoT Devices) page irrespective of AP being BLE or Zigbee
Workaround - Filter via tree view but even in that the first 10 only will be shown
- IOTC-3069-In a N+1 setup traffic going from controller to cloud will not use Virtual IP in the packet
Workaround - configure firewall to allow traffic to pass from master IP and Slave IP
- IOTC-3067-N+1 configuration failed if Master and Slave have same hostname is upper and lower case
Workaround -Configure different names for Master and Slave
- IOTC-3060-Telkonet EcoCentral status display down for all end devices even when device is an operational
Workaround - None
- IOTC-3012-Presence of wired device on the controller causes count mismatch on number of devices between Devices Last seen widget and Devices by Protocol widget in the Dashboard
Workaround - None
- IOTC-2980-connection lost message seen on switching from rules dashboard to rules configuration
Workaround - None (property of node-red design)
- IOTC-2868-Clicking on LoRa tab in Firefox browser gives Potential Security Issue page

Workaround - Right-click the lock icon at the top left corner of the iframe, then navigate This Frame->Show Only This Frame, then you see the “Advanced”->“Accept the Risk and Continue” button. Click it.After that hit “back” twice and refresh

- IOTC-2948 - Time mismatch is seen between the actual time and the time shown in Controller.

Workaround - None

- IOTC-2693-On downgrading from 1.5 to 1.4, track_central_service and node_red_service should not display/running

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

- IOTC-2711-Concurrent ZigBee-ZigBee or BLE-BLE on dual-radio platform is not supported

Workaround - None.

Limitations

- 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 1.5.0/5.1.1.2 together and upgrade only from the release versions of 1.4, 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. 1.3 then controller needs to be upgraded to 1.4 and then to 1.5
- 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).
- It is recommended to install IoT controller in a host (hypervisor/KVM/virtualbox/VMplayer) which has 60% CPU and 60% MEM free
- The IoT Controller (4vCPU) at max supports upto 400 BLE beacon 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>.
- Onboarding of Telkonet devices and device report propagation to the Telkonet cloud takes a long time as the Telkonet system update periods can typically be 10-30 minutes.
- When setting up offlink VLAN, routing must be correct, otherwise access points may stay over reboot in unreachable state and require reset of the VLAN state via CLI access over ssh.
- When maintaining logged in REST API session state in Rules Engine flows, refresh period should be the same as with UI, 8 hours.

Resolved Issues

NOTE

A number of additional issues have been resolved internal to the product.

- IOTC-2879 Samsung Smarthings Water leak detector not working
- IOTC-2455 MinMeasuredValue in Temp sensor shows 645.36 degree celsius
- IOTC-2701 CDS-enabling validate certificate and pasting the certificate still gives error "Please Fill Certificate"
- 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
- IOTC-2838 pan mismatch detected on every reboot of AP (H510). pan rpm key getting updated for p1 instead of p2
- IOTC-2738 when iBeacon or Kontakt.io connector is ON, AP loses connection to vRIoT.
- IOTC-2814 Coex option in controller not displaying with one radio active and second radio in-active
- IOTC-2848 Login prompt displaying on rules configuration page
- IOTC-2538 Gateway: Dongle mode change is aborted when the DHCP Option 43 is triggered during mode change and process repeats continuously
- IOTC-2676 RIOT Controller: iBeacon plugin shows stale old data while activating the plugin second time
- IOTC-2525 Zigbee channel change didn't happen after bringing up the WLAN with overlapping wifi channel
- IOTC-2590 Smart Zone tree-view and beacon filtering not working and getting HTTP 400 not found.

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
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

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
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
Multipurpose Sensor	Sensor	Zigbee	Smart things	Samjin	
Button	Sensor	Zigbee	Smart things	Samjin	
Motion Sensor	Sensor	Zigbee	Smart things	Samjin	
Water Leak Sensor	Sensor	Zigbee	Smart things	Samjin	
Motion Sensor	Sensor	Zigbee	Aduro SMART ERIA	ADUROLIGHT	
Smart Plug	Plug	Zigbee	Smart Things	Samjin	
Bulb	Bulb	Zigbee	Aduro SMART ERIA		
Bulb	Bulb	Zigbee	Cree		BA19-08027OMF-12CE26-1C100
Smart Plug	Plug	Zigbee	INNR		
Smart Blinds	Blinds	Zigbee	Axis Gear		
Occupancy Sensor	Sensor	Zigbee	Telkonet		
Door Sensor	Sensor	Zigbee	Telkonet		
Thermostat	Thermostat	Zigbee	Telkonet		
Picocell	Gateway	LoRa	Semtech		
Mini Hub/ Basic station	Gateway	LoRa	TABS		
Door Sensor	Sensor	LoRa	TABS		
Occupancy Sensor	Sensor	LoRa	TABS		
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
Vape/Sound Sensor	Sensor	Wired	Soter		FlySense

