

RUCKUS IoT 2.1.0.0 GA Release Notes

Supporting IoT Controller Release 2.1.0.0

© 2023 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

CommScope and the CommScope logo are registered trademarks of CommScope and/or its affiliates in the U.S. and other countries. For additional trademark information see <https://www.commscope.com/trademarks>. All product names, trademarks, and registered trademarks are the property of their respective owners.

Patent Marking Notice

For applicable patents, see www.cs-pat.com.

Contents

- Document History..... 5**
- Overview..... 7**
- New in This Release..... 9**
- Hardware and Software Support..... 11**
- Release Information..... 13**
 - Supported Upgrade Path..... 15
- Known Issues..... 17**
 - Component: IoT Feature in Access Point with IoT Module I100..... 17
 - Component: RUCKUS IoT Controller 17
- Resolved Issues..... 21**
- Best Practices..... 23**
- Caveats and Limitations..... 25**
 - Caveats..... 25
 - Limitations..... 26
- Supported Devices..... 27**

Document History

Revision Number	Summary of changes	Publication date
A	Initial release notes.	August, 2023

Overview

This document provides release information about RUCKUS IoT Suite 2.1.0.0, a versatile system for managing IoT devices. The RUCKUS IoT Suite is a collection of network hardware, and software infrastructure components that are used to create an IoT access network which is comprised of four elements:

- RUCKUS IoT-ready Access Points (APs)— For this release the following AP models are listed - ready- wall-mount H510, ceiling-mount R510, R610, R710, R720, outdoor models T310, E510, T610, Indoor Access Point R730 (802.11 ax), the Indoor Access Point C110, the LTE access point M510, Indoor Wi-Fi 6 Access Point for Dense Device Environments R650, Indoor Access Point Indoor Wi-Fi 6 Access Point for Ultra-Dense Device Environments R750, Outdoor Wi-Fi 6 Access Point with 2.5Gbps Backhaul T750, High Performance Wi-Fi 6 2x2:2 Indoor Access Point R550, Wall-Mounted Wi-Fi 6 2x2:2 Indoor Access Point H550, Outdoor 2x2:2 2.4/5GHz Wi-Fi 6 access points T350D, Indoor 802.11ax Wi-Fi 6 Access Point R350, Ultra High Performance Wi-Fi 6 8x8:8 with 5.9 Gbps HE80/40 Speeds and Embedded IoT Indoor Access Point R850, Highest capacity tri-band, tri-concurrent Wi-Fi 6E access point (AP) that supports 12 spatial streams (4x4:4 in 6GHz, 4x4:4 in 5GHz, 4x4:4 in 2.4GHz) Access Point R760 and High-Performance Tri-Radio Wi-Fi 6E 2x2:2 with 4.7 Gbps max rate and Embedded IoT Indoor Access Point 560.
- RUCKUS IoT Modules—A device that attaches to a RUCKUS IoT-ready AP and supports standards such as Bluetooth Low Energy (BLE), Zigbee, LoRa and more. The first IoT Module, the I100, supports the 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 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. RUCKUS IoT Controller also facilitates cross-solution endpoint communication and provides APIs for northbound integration with IoT cloud services.
- RUCKUS IoT Insights—A virtual controller, deployed in tandem with the RUCKUS IoT Controller, that performs application-level analysis, control, and logging of RUCKUS IoT events with a focus on an application-level solution.

This document provides a list of release components with their versions , the caveats, limitations, and the known issues.

New in This Release

RUCKUS IoT 2.1.0.0 GA Suite provides the following update.

- Vostio Door Lock Integration
- Scale Improvements
- Stability Fixes

Hardware and Software Support

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

Compatible Hardware:

- H510/R510/T310D and i100 IoT Module
- R610/R710 and i100 IoT Module
- R720 and i100 IoT Module
- R650 Access Point
- R750/T750/T750SE Access Point
- R850 Access Point
- R550/H550 Access Point
- R350/H350/T350D Access Point
- R550 and i100 IoT Module
- R760 Access Point
- R560 Access Point

Compatible Software:

- Virtual SmartZone – High Scale (vSZ-H)
- Virtual SmartZone – Essentials (vSZ-E)
- SmartZone 100 (SZ100)
- RUCKUS IoT Controller (RIoT)

Hardware Requirement

Customers must obtain robust and reliable server hardware that will support a virtualized environment for IoT applications with enough headroom to expand in the future. Each deployment is unique and hardware specifications will need to be adapted to specific needs. For a typical deployment (e.g. RUCKUS IoT controller, VMware ESXi, Ubuntu Linux server, IP camera VMS, additional IoT VMs or applications), we recommend server hardware that meets the below specifications.

- **CPU:** 4 core i7 or equivalent (3.1GHz or Higher)
- **Memory:** 32 GB
- **Hard Disk:** 1 TB

TABLE 1 Supported Capacity for Controller

Number of AP	Number of Devices	Type of Device
1500	1500	Assa Abloy Visionline
1500	1500	DormaKaba
500	500	Generic Zigbee
500	500	Vostio
400	400 AP	400 Beacon messages with interval of 1 or 2 seconds
1500	1500 AP	BaaS

NOTE

The combinational setup will support only 500 AP and 500 devices even in case of Assa Abloy and DormaKaba.

Release Information

- Supported Upgrade Path..... 15

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

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

- WLAN Controller version: 5.2.2.0.1562, 6.1.1.0.967
- AP firmware version in the WLAN Controller: 5.2.2.0.2064, 6.1.1.0.1312
- IoT Gateway Version
5.2.2.0 – 1.9.2.1.10016
6.1.1.0 – 2.1.0.0.20013

RIoT

- RUCKUS IoT Controller version: 2.1.0.0.43
- VMWare ESXi version: 6.5 and later
- KVM Linux virtualizer version: 1:2.5+dfsg-5ubuntu10.42 and later
- Google Chrome version: 78 and later
- Mozilla Firefox version: 71 and later

3rd Party Integrations

- Assa Abloy
- Visionline Version: 1.28.0.67
- Lock Zigbee Version: 3.1.62.1
- Lock Version: 3.17.42.19

Dormakaba

- Ambiance Version: 2.9.0.98
- Lock RT+ version FW version: 02-23-22.4
- Ember Rev: 5.6 build E7

Vostio

- Vostio service tool App version: 2.6.6.0
- Lock Firmware version: 3.59.10.86
- Zigbee Firmware version: 2.7.5

TABLE 2 Release Build Compatibility Matrix

Release	IoT Controller	SZ	AP	Supported AP Models
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

Release Information

TABLE 2 Release Build Compatibility Matrix (continued)

Release	IoT Controller	SZ	AP	Supported AP Models
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
IoT 1.5MR1	1.5.0.0.38	5.1.1.2.15524	5.1.1.2.15524	H510, R510, T310d, E510, R610, R710, R720, T610, R730, C110, M510
IoT 1.5.0.1	1.5.0.1.21	5.2.0.0.699	5.2.0.0.1412 IoT Version : 1.5.0.1.15027	H510, R510, T310d, E510, R610, R650, R710, R720, T610, R730, R750, T750, C110, M510
IoT 1.5.1.0	1.5.1.0.21	5.2.0.0.699	5.2.0.0.1412 IoT Version : 1.5.1.0.15030	H510, R510, T310d, E510, R610, R650, R710, R720, T610, R730, R750, T750, C110, M510
IoT 1.5.1.1	1.5.1.1.22	5.2.0.0.699	5.2.0.0.1412 IoT Version : 1.5.1.0.15030	H510, R510, T310d, E510, R610, R650, R710, R720, T610, R730, R750, T750, C110, M510
IoT 1.6.0.0	1.6.0.0.42	5.2.1.0.515	5.2.1.0.698 IoT Version : 1.6.0.0.16003	H510, R510, T310d, E510, R610, R650, R710, R720, T610, R730, R750, T750, C110, M510
IoT 1.7.0.0	1.7.0.0.22	5.2.1.0.515	5.2.1.0.698 + 5.2.1.0.2011 patch IoT Version : 1.7.0.1.17004 ST Version : 1.7.0.32.12	H510, R510, T310d, E510, R610, R650, R710, R720, T610, R730, R750, T750, C110, M510, R550
IoT 1.7.1.0	1.7.1.0.16	5.2.2.0.317	5.2.2.0.301 IoT Version : 1.7.1.0.17001 ST Version : 1.7.1.34.12	H510, R510, T310d, E510, R610, R650, R710, R720, T610, R730, R750, T750, C110, M510, R550
IoT 1.8.0.0	1.8.0.0.27	6.0.0.0.1331	6.0.0.0.1594 T350D - 6.0.0.0.1610 IoT Version : 1.8.0.1.18009 ST Version : 1.8.0.34.12	H510, R510, T310d, E510, R610, R650, R710, R720, T610, R730, R750, T750, C110, M510, R550, H550, T350D
IoT 1.8.1.0 [MR]	1.8.1.0.16	5.2.2.0.317 6.0.0.0.1331	5.2.2.0.301 IoT Version : 1.8.1.0.18007 6.0.0.0.1594 6.0.0.0.1610 (T350D) IoT Version : 1.8.1.0.18008 ST Version : 1.8.0.34.12	H510, R510, T310d, E510, R610, R650, R710, R720, T610, R730, R750, R850, T750, C110, M510, R550, H550, T350D
IoT 1.8.1.1 [SR]	1.8.1.1.17	5.2.2.0.317	5.2.2.0.301 IoT Version : 1.7.2.0.17009	H510, R510, R550

TABLE 2 Release Build Compatibility Matrix (continued)

Release	IoT Controller	SZ	AP	Supported AP Models
IoT 1.8.2.0 [MR]	1.8.2.0.44	<ul style="list-style-type: none"> 5.2.2.0.317 6.0.0.0.1331 	5.2.2.0.2016 IoT Version : 1.8.2.0.18013 6.0.0.0.1594 6.0.0.0.1610 (T350D) 6.0.0.0.3073 (R350) IoT Version : 1.8.2.0.18010 ST Version : 1.8.1.34.12	H510,R510,T310d,E510,R610,R650,R710,R720,T610,R730,R750,T750,C110,M510,R550,H550,T350D, R350, R850.
IoT 2.0.0.0	2.0.0.0.82	<ul style="list-style-type: none"> 5.2.2.0.317 6.1.0.0.935 	5.2.2.0.2016 IoT Version : 1.9.2.0.10001 ST Version: 1.8.1.34.12 6.1.0.0.1595 IoT Version : 2.0.0.0.20037 ST Version: 2.0.0.34.12	H510, R510, T310d, E510, R610, R650, R710, R720, T610, R730, R750, T750, C110, M510, R550, H550, T350D, R350, R850, T750SE, H350.
IoT 2.0.0.2	2.0.0.2.43	6.1.0.0.935	6.1.0.2.18 IoT Version : 2.0.0.2.28	R650, R730, R750, T750, R550, H550, T350D, R350, R850, T750SE, H350
IoT 2.1.0.0	2.1.0.0.43	<ul style="list-style-type: none"> 5.2.2.0.1562 6.1.0.0.935 	5.2.2.0.2064 IoT Version : 1.9.2.1.10016 6.1.1.0.1312 IoT Version : 2.1.0.0.20013	H510, R510, T310d, E510, R610, R650, R710, R720, T610, R730, R750, T750, C110, M510, R550, H550, T350D, R350, R850, T750SE, H350, R760, R560

Supported Upgrade Path

2.0.1.0.64 -> 2.1.0.0.43

NOTE

Any migration from 1.8 has to go through 2.0.1 MR and upgrade to 2.1. Refer to *RUCKUS IoT Controller Migration guide, 2.0.1.0 MR* for more details.

Known Issues

The following are the caveats, limitations and known issues.

Component: IoT Feature in Access Point with IoT Module I100

- IOTC-6713 - AP once connected to 2.1 controller will not connect to a 2.0.1.0 controller
Workaround - Rebooting the AP will make the AP connect to 2.0.1.0 controller.
- IOTC-6163 - AP's with Internal Radio throwing USB low power warning.
Workaround - None
- IOTC-3809 - Enabling channelfly co-ex fails to change channels.
Workaround - After enabling channelfly disable and enable co-ex on the radio.
- IOTC-3807 - Wlan channel conflict is not detected and channel does not change when co-ex is enabled in both radios
Workaround - None.
- IOTC-3557 - Zigbee_DK mode allows generic zigbee devices to connect by no attributes or commands are listed
Workaround - None.
- IOTC-3159 - Factory resetting the T750 AP disables the IOT
Workaround - Setting correct power level automatically enables the IoT process.
- IOTC-1832 - In Dense BLE beacon deployments (more than 800 beacons seen by single AP) the beacon packets are dropped and would experience longer latency to reach the endpoint.
Workaround - None

Component: RUCKUS IoT Controller

- IOTC-6602 - After Factory reset controller UI does not come up.
Workaround - Bring up a new controller and use DB restore instead of Factory Reset.
- IOTC-6565 - Blacklisting a device is throwing Error
Workaround - Refreshing the page shows Device is blacklisted.
- IOTC-6487 - Active SSH connections are not terminated on disabling the SSH from UI.
Workaround - None.
- IOTC-6314 - Vostio: Many times GW status is displayed incorrectly in Vostio Portal.
Workaround - Refresh the screen on Vostio cloud portal.
- IOTC-6116 - UI gets stuck in the upgrade progress screen (no close button) if controller rebooted during upgrade.
Workaround - None
- IOTC-6112 - vRIOT login page do not auto redirect to https when controller is behind NAT

Known Issues

Component: RUCKUS IoT Controller

Workaround - Use <https://controllerIP/refUI/#/Login>

- IOTC-5939 - In Ambiance server it takes 25 minutes for a Gateway to go from "deactivated" state to "pairing OFF" state which leads to lock not being able to get onboarded

Workaround - Send Pairing ON from Ambiance server for the Gateway.

- IOTC- 5733- License count mismatch after Bulk deletion of devices.

Workaround - The mismatch will go away when license check happens which is maximum interval of 5 minutes.

- IOTC-5448 - Success message is not shown while restoring DB Backup from standalone controller to another N+1 enabled controller with network configuration as 'NO'.

Workaround - None

- IOTC-5434 - DB restore failed after N+1 failover if password contains '\$' symbol.

Workaround - Avoid '\$' symbol in password.

- IOTC-5428 - Device name with more than 24 characters is shown with MAC address appended to the name in IOT APs page.

Workaround - None.

- IOTC-5366 - Sudden Power outage could cause controller to become inaccessible since service keeps continuously restarting.

Workaround - None (Redeploy controller)

- IOTC-3871 - Device Attribute fails to show in IoT controller.

Workaround - Query the specific cluster/attribute using API call.

- IOTC-3804 - Activating Dormakaba plugin with wrong/not reachable IP address throws Operation failed error

Workaround - None.

- IOTC-3765 -When Ambiance Server is set to European date format, date shows up nana/nana/.

Workaround - Set the date in US format in the Ambiance Server.

- IOTC-3760 - Ambiance UI shows Door is Unlatch under Metric though Door is latched

Workaround - None. Contact Dormakaba.

- IOTC-3719 - MQTT Push events sent even with no state/device change/Action

Workaround - None

- IOTC-3674 - Zone_ID of IAS devices may be displayed as 255 for some devices

Workaround - Triggering an event from the device sometimes sets the correct Zone_ID.

- 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 primary IP and secondary IP .

- ER-11709 - When there is a dongle swap the older radio is made unavailable and the new dongle comes up as another radio hence displaying 2 radios in the UI.

Workaround - User has to delete the AP and let it rediscover again.

- ER-11818 - Search Filters accuracy isn't correct

Workaround - None.

- ER-11817 - NTP drift caused Gateways to disconnect from the controller and continuously try to connect leading to a burst of messages queueing up.

Workaround - None.

- ER-11816 - Deleting a device may not immediately delete and may show up in UI.

Workaround - Wait for some time. This could be because of controller may be processing other data and the delete command could be queued up.

- ER-12520 - Using admin credentials to enable DormaKaba plugin causes controller to lose its licenses and Serial No. information.

Workaround - Do not use Admin credentials but use the Client ID and Client Key provided by DormaKaba.

Resolved Issues

The following issues are resolved for this release

TABLE 3 Resolved Issues

Key	Summary
IOTC-6022	Gateways in 6.1 will stay in firmware mismatch state for extended period of time and IoT radio's will not come up.
IOTC-5948	N+1 upgrade will not be successful when upgrading from 2.0.0.0 to 2.1.0.0
IOTC-5931	Timezone doesn't change on a setup if admin password is changed after Db restore.
IOTC-5926	Changing the log level in Admin-Settings page gives an "Operation Failed" error.
IOTC-5925	Setpoint Raise/Lower by 1 unit functionality does not work for Thermostat.
IOTC-5922	Gateway commissioning message not sent to Ambiance server after deactivating and activating DK plugin on a DB restored setup.
IOTC-5870	License notification flag still says that premium license is expired even after installing license for 3 additional years.
IOTC-5864	BAAS beacon data are not updated with the baas major/minor number applied from the batch action.
IOTC-5836	A duplicate entry is created under the Patch list for each patch apply operation in VRIOT
IOTC-5748	After Factory Reset the screen remain static and there is no indication if the controller is being factory reset.
IOTC-5478	Invalid error is thrown in UI while trying to set channel for Multi-radio AP in Multi-pan(radio1) using batch action.
IOTC-5473	No APs and devices are shown in the IOT controller due to high CPU utilization after a day of soaking
IOTC-5472	Not able to delete bulk number of devices due to 504 gateway time-out.
IOTC-5469	Restoring 1.8.2 db-backup lists controller-gateway in the IoT-AP table on clicking refresh multiple times.
IOTC-5461	There is not alert message displayed when there are only less than or equal to 10 days for license expiry.
IOTC-5460	N+1 CLI takes almost 25 secs to complete .
IOTC-5408	Restoring 1.8.2 db backup TOTAL LNS Widget is not removed from Dashboard
IOTC-5399	Decommissioned device doesn't come online after adding Premium license on top of BASE+CAPACITY licenses.
IOTC-5386	Failed to view services logs on clicking view logs button.
IOTC-5309	Zigbee device is joining to AP with wrong install code
IOTC-5155	IOT process keeps restarting every time when DHCP option 43 for VLAN settings without any changes
IOTC-4678	IoT Radio widget will not update unless AP is reboot or factory set.
IOTC-3731	Node-Red Deploy Icons are not correctly displayed when node-red config screen is opened in a new window
IOTC-3080	Blacklisted devices are part of total device count in the dashboard.
ER-12503	IOT Controller UI login 302 redirect to HTTP
ER-12717	Controller UI is not displaying connected AP's due to an exception.
ER-12270	Not able to change radio mode from BLE to Zigbee DK after DB restore.
ER-12209	Dormakaba Plugin Cannot be activated with a Trusted CA Cert
ER-12143	IOT process keeps restarting everytime when DHCP option 43 settings are received
ER-12022	REST API Call is not returning information about all connected devices.
ER-11885	vRIOT UI prompts a License Warning for the Support and Grace Period Expiration
ER-11868	Events tab events filter not able to enter values.
ER-11843	vRIOT Mosquitto-ap.log aren't rotating
ER-11719	C110 IOT process cannot be started

Best Practices

Following is the list of best practices

- Recommended Periodic interval of 120 seconds in Controller Data Stream Plugin. Lesser values could lead to system instability.
- 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.

Caveats and Limitations

Caveats

- The db backup size is reduced to 132kb.
- The admin password cannot be retrieved once lost.
- RUCKUS recommends to back up the database at regular intervals. For example, when there are changes in the network.
- Disk Space must re-size from 8GB to exactly 20GB (less than or greater than 20GB will cause failure) starting from 1.5 Release onwards and exactly 20GB should be allocated during deployment.

NOTE

However, reducing the HDD size is more complicated than increasing it.

You receive the following error while decreasing the HDD size on the VMware.

FIGURE 1 Error Message when HDD size is Reduced



The HDD shrinking for a VM requires expertise an editing *.vmdk. To shrink the disk size, you can refer to https://www.vmware.com/support/ws5/doc/ws_disk_shrink.html or <https://kb.vmware.com/s/article/1002019>. An alternative mechanism is to take config backup of existing vRIOT instance, install a fresh instance of vRIOT of the same version as the config backup, and allocate the recommended HDD/CPU/memory resources. After the new instance is up, you can shutdown the existing instance to avoid any conflicts. You can then upload the configuration backup to it and upgrade the vRIOT to the desired version firmware.

- RUCKUS IOT platform is not FIPS compliance and if the AP's have FIPS certificate, it would not join the IOT controller. MQTT logs will throw an OpenSSL Error: error:14089086:SSL routines:ssl3_get_client_certificate:certificate verify failed.
- IoT APs will randomly go offline if we override the MQTT IP using AP CLI script from the vSZ.

Workaround - Do not push MQTT Broker IP to the AP's which already have established MQTT session with the IP controller

- AP Search filter does not work with the AP IP address.
- **ER-9842**- IOT 1.7.1.0.16- IOT devices would disconnect from the IOT controller if their RSSI/LQI is low.

Workaround - It is NOT recommended bulk scan to onboard IoT devices.

Limitations

- PAN0 cannot be set to Zigbee_AA if PAN1 is already set to Zigbee_AA. To set PAN0 to Zigbee_AA set PAN1 to Deactivated.
- DB backup taken from pre-2.1.0.0 controller cannot be restored on 2.1.0.0 controller.
- UEI Thermostat on changing the cooling setpoint causes the Heat setpoint value to change. This is a Vendor Implementation Design.
- IoT controller does not retain set values of UEI Thermostat upon the AP reboot. This is handled in vendor software.
- NTP drift will cause Gateways to disconnect from the controller and continuously try to connect leading to a burst of messages queueing up and controller not being able to process messages.
- MQTT connection will not be established when the vlan mode is offlink but the controller is in same subnet
- AP and Phone having the ST APP should be in the same subnet to detect and add the dongle.
- Pushing VLAN from option43 or RKSCLI will cause the AP to keep disconnecting from MQTT.
- Hot plugging of dongle is not supported. Reboot of AP is required in case dongle is plugged out and plugged in.
- Concurrent ZigBee-ZigBee, ZigbeeAA-ZigbeeAA, ZigbeeDK-Zigbee-DK on dual-radio platform is not supported.
- Broker IP is set to Unconfigured if controller is not reachable for 24Hrs. Broker IP has to be reconfigured either manually through RKSCLI or DHCP Option-43.
- N+1 Auto Fallback is not supported (If primary is back online, secondary will run as active secondary).
- 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.
- Uploading a new temporary license after the previous temporary license has expired is not supported.

Supported Devices

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

TABLE 4 Bulbs

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
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		
Bulb	Bulb	Zigbee	Aduro SMART ERIA		
Bulb	Bulb	Zigbee	Cree		BA19-08027OMF-12CE26-1C100
Hue	Bulb	Zigbee	Philips	Hue White	840 Lumens

TABLE 5 Locks

Device	Type	Model	Manufacturer	Basic Name	Basic Model
Vingcard Signature	Lock	Zigbee	Assa-Abloy	AA_LOCK	
Vingcard Essence	Lock	Zigbee	Assa-Abloy	AA_LOCK	
RT+	Lock	Zigbee	Dormakaba	Dormakaba	79PS01011ER-626
Yale YRD220/240 TSDB Display	Lock	Zigbee	Assa-Abloy	Yale	Yale YRD220/240 TSDB
Yale YRD210 Push Button	Lock	Zigbee	Assa-Abloy	Yale	YRD210 Push
Smartcode 916	Lock	Zigbee	Kwikset	Kwikset	SMARTCODE_DEADBOLT_10T
Smartcode 910 (450201)	Lock	Zigbee	Kwikset	Kwikset	

TABLE 6 SWITCHES/PLUGS/THERMOSTAT/ALARM/BLINDS

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
GE Smart Dimmer	Switch	Zigbee	GE	Jasco Products	45857
GE Smart Dimmer	Switch	Zigbee	GE	Jasco Products	45856
Smart Plug	Plug	Zigbee	Centralite	Centralite	
Smart Plug	Plug	Zigbee	Smart things	Samjin	
Smart Plug	Plug	Zigbee	INNR		
Zen Thermostat	Thermostat	Zigbee	Zen Within	Zen Within	Zen-01
Ecolnsight Plus	Thermostat	Zigbee	Telkonet	Telkonet	
ZBALRM	Alarm	Zigbee	Smartenit		Model #1021 A
Smart Blinds	Blinds	Zigbee	Axis Gear		
UEI Thermostat	Thermostat	Zigbee	UEI		TBH300ZBSN

Supported Devices

TABLE 7 Sensors

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
Garage Door Tilt Sensor	Sensor	Zigbee	NYCE	NYCE	NCZ-3014-HA
Curtain Motion Sensor	Sensor	Zigbee	NYCE	NYCE	NCZ-3045-HA
Door / Window Sensor	Sensor	Zigbee	NYCE	NYCE	NCZ-3011-HA
Temperature and Humidity Sensor	Sensor	Zigbee	Aqara	LUMI	WSDCGQ11LM
Motion Sensor	Sensor	Zigbee	Aqara	LUMI	RTCGQ11LM
ERIA Smart Door/ Window Sensor	Sensor	Zigbee	AduroSMART ERIA	ADUROLIGHT	81822
ERIA Smart Motion Sensor	Sensor	Zigbee	AduroSMART ERIA	ADUROLIGHT	81823
Multipurpose Sensor	Sensor	Zigbee	Smart things	Samjin	IM6001-MPP01
Button	Sensor	Zigbee	Smart things	Samjin	IM6001-WLP01
Motion Sensor	Sensor	Zigbee	Smart things	Samjin	IM6001-MTP01
Water Leak Sensor	Sensor	Zigbee	Smart things	Samjin	IM6001-BTP01
EcoSense Plus	Sensor	Zigbee	Telkonet	Telkonet	SS6205-W
EcoContact Plus	Sensor	Zigbee	Telkonet		SS6255-W
Temp, Humidity Sensor	Sensor	Zigbee	Heiman	HEIMAN	HS1HT-N
Gas detector	Sensor	Zigbee	Heiman	HEIMAN	HS3CG
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
3-Series Micro Door Sensor	Sensor	Zigbee	Centralite	Centralite	3323-G
Door Sensor	Sensor	Zigbee	Ecolink	Ecolink	4655BC0-R
Temp & Humidity Sensor	Sensor	Zigbee	Sonoff	Sonoff	SNZB-02
Celling Motion Sensor	Sensor	Zigbee	NYCE	NYCE	NCZ-3043-HA
Ecolink Flood Detection Sensor	Sensor	Zigbee	Ecolink	Ecolink	FLZB1-ECO

TABLE 8 BLE

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
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

TABLE 9 Wired

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
Vape/Sound Sensor	Sensor	Wired	Soter	-	FlySense

TABLE 10 Supported Devices tested with SmartThings

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
Yale YRD220/240 TSDB Display	Lock	Zigbee	Assa-Abloy	Yale	YRD220/240 TSDB
Lightify (RGB) Model 73674	Bulb	Zigbee	Osram	OSRAM	LIGHTFY A19 RGBW
Multipurpose Sensor	Sensor	Zigbee	SmartThings	Samjin	
Button	Sensor	Zigbee	SmartThings	Samjin	
Motion Sensor	Sensor	Zigbee	SmartThings	Samjin	
Water Leak Sensor	Sensor	Zigbee	SmartThings	Samjin	
Smart Plug	Sensor	Zigbee	SmartThings	Samjin	
Bulb	Bulb	Zigbee	Aduro SMART ERIA		
AEOTEC Multi Sensor	Sensor	Zwave	AEOTEC	AEOTEC	ZW 100-A
Hue Hub	Hub	Wired	Philips	Philips	3241312018A

TABLE 11 Device not QA tested but supported

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
Vingcard	Sigma	Lock	Zigbee	Assa-Abloy	AA_LOCK
Vingcard	Alpha	Lock	Zigbee	Assa-Abloy	AA_LOCK
Vingcard	Classic		Zigbee	Assa-Abloy	AA_LOCK
Vingcard	Allure		Zigbee	Assa-Abloy	AA_LOCK



© 2023 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
<https://www.commscope.com>