

RUCKUS IoT 1.8.0.0 Release Notes

Supporting IoT Controller Release 1.8.0.0

Copyright, Trademark and Proprietary Rights Information

© 2021 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, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED 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**
- New in This Release..... 4**
 - Changed Behavior..... 4
- Hardware and Software Support..... 5**
- Release Information..... 6**
 - Supported Upgrade Path..... 7
- Known Issues..... 7**
 - Component: IoT feature in Access Point..... 7
 - Component: RUCKUS IoT Controller 8
- Resolved Issues..... 10**
- Best Practices..... 10**
- Caveats and Limitations..... 11**
 - Caveats..... 11
 - Limitations..... 12
- Supported Devices..... 12**

Document History

Revision Number	Summary of changes	Publication date
A	Initial Release Notes	May, 2021

Overview

This document provides release information about RUCKUS IoT Suite 1.8.0.0 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, 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, 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, H550 - Wall-Mounted Wi-Fi 6 2x2:2 Indoor Access Point (AP), and T350D - Outdoor 2x2:2 2.4/5GHz Wi-Fi 6 access points .
- 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. 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 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.

New in This Release

RUCKUS IoT-1.8.0.0 Suite provides the following update:

- H550 and T350D support
- Dorma Kaba https including FQDN support
- Security Vulnerability Fixes
- Beacon As A Service unique UUID per AP
- ZCL write attributes support for 0x000A cluster for Zigbee thermostats
- UI Improvements and Stability Fixes

Changed Behavior

STOP and READ before upgrading

The license will be checked out whenever an AP is approved, and will remain checked out till the time the AP is unapproved or deleted from the controller. The license will continue to be consumed even if the AP goes offline.

Ensure there are sufficient licenses in the controller before upgrade else due to change in the license logic as mentioned above, the controller will redirect to a page wherein AP's have to be unapproved or removed to match the total license available in the system.

IoT Controller Licensing:

IOT controller require following licenses to operate

- RTU
- IOT AP Capacity Licenses
- Support Licenses

KBA: Firmware Upgrade Matrix

<https://support.ruckuswireless.com/articles/000010364>

Hardware and Software Support

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

Compatible Hardware:

- C110 Access Point (C110)
- E510 Access Point (E510)
- H510 Access Point (H510)
- H550 Access Point (H550)
- M510 Access Point (M510)
- R510 Access Point (R510)
- R550 Access Point (R550)
- R610 Access Point (R610)
- R650 Access Point (R650)
- R710 Access Point (R710)
- R720 Access Point (R720)
- R730 Access Point (R730)
- R750 Access Point (R750)
- T310 Access Point (T310)
- T350D Access Point (T350D)
- T610 Access Point (T610)
- T750 Access Point (T750)
- T750SE Access Point (T750SE)
- I100 IoT Module (I100)

Compatible Software:

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

Release Information

Hardware Requirement

RUCKUS recommends the following minimum requirements for IoT Server.

- **CPU:** 4 core i7 or equivalent
- **Memory:** 32 GB
- **Hard Disk:** 1 TB

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: 6.0.0.0.1331
- Control plane software version in the WLAN Controller: 6.0.0.0.1213
- AP firmware version in the WLAN Controller: 6.0.0.0.1594
- IoT Gateway Version: 1.8.0.1.18009
- SmartThings Version: 1.8.0.34.12

RIoT

- RUCKUS IoT Controller version: 1.8.0.0.27
- VMWare ESXi version : 6.5 and later
- KVM Linux virtualizer version: 1:2.5+dfsg-5ubuntu 10.42 and later
- Google Chrome version: 78 and later
- Mozilla Firefox version: 71 and later

3rd Party Integrations

- Assa Abloy
 - Visionline Version: 1.26.0.13
 - Lock Zigbee Version: 3.1.62.1
 - Lock Version: 3.17.37.5
- Samsung SmartThings
 - Hub Software Version: 3.14.1
 - SmartThings Hardware Version: 1.01
- DormaKaba
 - Ambiance Version: 2.6.4.68
 - Lock RT+ version FW version: 06:05.22.20.4
 - Ember Rev: 5.6

TABLE 1 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

TABLE 1 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

Supported Upgrade Path

1.7.1.0.16 > 1.8.0.0.27 [SZ/AP upgrade 5.2.2.0 > 6.0.0.0]

Known Issues

The following are the caveats, limitations and known issues.

Component: IoT feature in Access Point

- 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.

Known Issues

Component: RUCKUS IoT Controller

- IOTC-3159 - Factory resetting the T750 AP disables the IOT
Workaround - PoE power setting to AT, BT5, BT7 will enable IoT process automatically.
- IOTC-3557 - Zigbee_DK mode allows generic zigbee devices to connect but no attributes or commands are listed.
Workaround - None.
- IOTC-3807 - Wlan channel conflict is not detected and channel does not change when co-ex is enabled in both IoT radios.
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-4036 - Downgrading from 5.2.2 to 5.2 rksiot process is not starting
Workaround - Upgrade the AP back to 5.2.2 and then do a set factory on the AP. After that downgrade the AP back to 5.2.
- IOTC-4238 - nRF connect APP does not show the beacon from AP if append MAC is checked.
Workaround - Use a different APP or use another Ruckus IoT Gateway with ibeacon plugin enabled.
- IOTC-4249 - BLE stack didn't come up on R510 AP if the MQTT connection lost for sometime and connects back later.
Workaround - Restart the IoT service from the UI.

Component: RUCKUS IoT Controller

- 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-2971 - After initial configuration of the controller the UI will remain stuck in the EULA page in Firefox Browser.
Workaround - Refresh the page in the browser.
- IOTC-2980 - Connection lost message seen on switching from rules dashboard to rules configuration.
Workaround - None (property of node-red design).
- 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.
- IOTC-3078 - Total LNS count is displaying blank in dashboard page in firefox browser..
Workaround - Go to Admin tab, stop the LoRa Network Server and start it again.
- IOTC-3080 - Blacklisted devices are part of total device count in the dashboard.
Workaround - None
- IOTC-3540 - Telkonet: setting static ip from controller shell does causing telkonet plugin not to run.
Workaround - Deactivate and activate the plugin.
- IOTC- 3646- Activate/Deactivate of Plugin logs the user out when deployed in Virtualbox or VMplayer.
Workaround - None.
- IOTC-3650 - Restoring a db backup from a N+1 controller on a standalone controller enables N+1
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-3705 - No logs shown in UI for BLE scan on clicking on View Logs.
Workaround- None.
- IOTC-3731 - Node-Red Deploy Icons are not correctly displayed when node-red config screen is opened in a new window.
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-3804 -Activating Dormakaba plugin with wrong/not reachable IP address throws Operation failed error.
Workaround - None.
- IOTC-3871- Device Attribute fails to show in IoT controller.
Workaround - Query the specific cluster/attribute using API call.
- IOTC-4082/IOTC-4039 -Not able to set Tx power as 8 for the internal radio of R650/T350D AP in BLE mode.
Workaround - None.
- IOTC-4093- Ruckus IOT Controller: LoRaLNS iframe page doesn't load properly in the IOT controller.
Workaround - Open the LoRA page in a seperate window by going to "https://<controller IP>:7008/index.html" -> accept the risk then the LoRA opens in the iframe.
- IOTC-4108 - LoRa service is automatically started after upgrade from 1.7.1 to .1.8 even if service was stopped in 1.7.1.
Workaround - Stop the service from Admin Page.
- IOTC-4109- After temp license expiry license count is not reduced even though alert says expired.
Workaround - Wait for 5 mins for license mismatch page to load.
- IOTC-4232 - Starting of pairing ON from Ambiance if left open, within 10-15 minutes the status change to pairing OFF even if pairing is still ON.
Workaround - None .
- IOTC-4255 - Status reporting and control is lost during the N+1 upgrade and it prompts the user to login once the secondary becomes active.
Workaround - None .
- IOTC-4256 - AP MQTT connection is lost to the broker after the secondary controller restarts and it recovers only after the primary controller comes up after upgrade.
Workaround - None .
- IOTC-4258 - Trying to add hostname with hyphen at the end ignores the entire hostname.
Workaround - None .
- IOTC-4275 - From IoT controller UI, cannot disable IoT management VLAN in Samsung Smartthings dongle connected AP.
Workaround - Login to AP and set the IoT VLAN to disaable from RKSCLI .
- IOTC-4277 - Error message of not enough license is not visible and is shown in the background on adding pre-approved AP's.
Workaround - None.
- IOTC-4280 - UI incorrectly display Append AP MAC as unchecked even if the functionality is unique UUID per AP.
Workaround - None
- IOTC-4281 - UI displays 0x000A attribute values incorrectly.
Workaround - Use API calls to get device attrbiute values.

Resolved Issues

- IOTC-4283 - Unable to remove/deactivate the Vendor2 alone for multi vendor plugin after activating the plugin with both Vendor-1 and Vendor-2.

Workaround - Deactivate the plugin and activate with only vendor 1 data.

- IOTC-4285 - Trying to write negative value through API for cluster 0x000A attribute 0x0002 returns API error.

Workaround - None.

- IOTC-4291 - Pre-approve device not accepting space in name while it is accepted in scan window and edit device.

Workaround - Add device without space in the name and then edit the device if space is required.

Resolved Issues

The following issues are resolved for this release

TABLE 2 Resolved Issues

Key	Summary
IOTC-4048/IOTC-3894	Ibeacon Vendor-2 plugin status is incorrectly detected, and packets are forwarded.
IOTC-4044	Yale lock time attribute is shown in Hex value.
ER-10013	[Sumitomo Fudosan Villa Fontaine Co., Ltd] IOT 1.5.0.0.34 : N+1 disabled on the Master after power cycle "Error: Slave is already configured by this master"
ER-10011	[RUCKUS NETWORKS INC]-vRIOT-1.7.1.0.16- R650 Failed to join IOT Controller- OpenSSL Error: error:14089086:SSL routines:ssl3_get_client_certificate:certificate verify failed.
ER-9987	[Sonifi Solutions]- [Sheraton Lincoln Harbor] vRIOT-1.5.0 21 IoT APs randomly go offline.
ER-9842	NEXT GENERATION VOICE : IOT 1.7.1.0.16 : IOT devices are offline after the upgrade.

Best Practices

Following is the list of best practices

- 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 primary and secondary 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 primary option in N+1 only after making sure primary is not reachable from secondary.
- 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.

- After deleting a device from the controller wait for 20 seconds before trying to onboard the deleted device again.
- For IAS Zone devices to remove the device from the controller and re-onboard, delete the device from the controller before doing a factory reset of the end device. If it's a new device remove the battery and then put the battery and onboard

Caveats and Limitations

Caveats

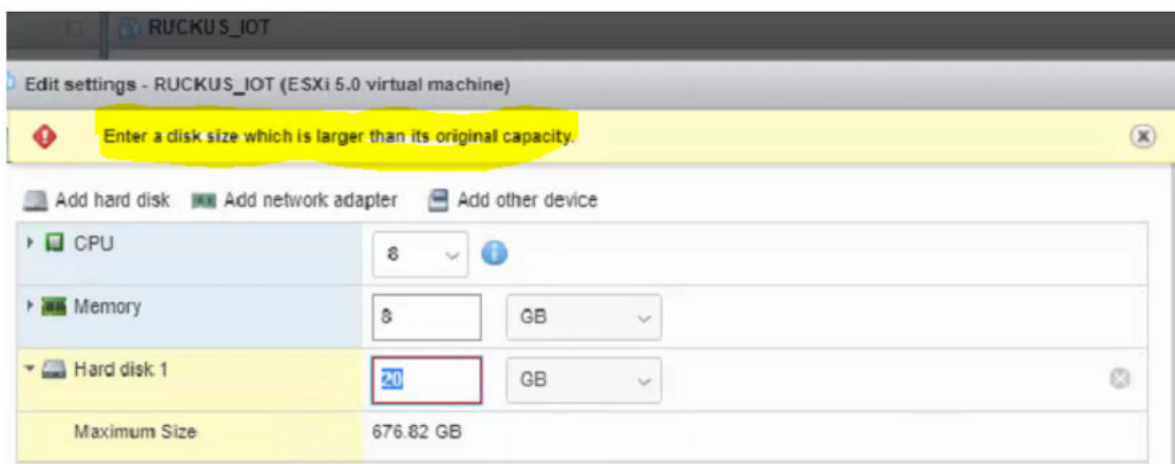
- The admin password cannot be retrieved once lost.
- RUCKUS recommends to back up the database at regular intervals.
- Disk Space must re-size from 8GB to exactly 20GB (less than or greater than 20GB will cause failure) starting from 1.5 Release onwards and exactly 20GB should be allocated during deployment.

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.

Supported Devices

Limitations

Workaround - It is recommended bulk scan to onboard IOT devices, this may result into IOT devices connecting to the far AP's and result into low RSSI/LQI.

Limitations

- 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 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.
- Snapshot and deploy of IoT controller snapshot 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.

Device	Type	Mode	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	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

TABLE 3 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	LIGHTIFY A19 RGBW
Multipurpose Sensor	Sensor	Zigbee	SmartThings	Samjin	
Button	Sensor	Zigbee	SmartThings	Samjin	
Motion	Sensor	Zigbee	SmartThings	Samjin	

Supported Devices

TABLE 3 Supported Devices tested with SmartThings (continued)

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
Water Leak Sensor	Sensor	Zigbee	SmartThings	Samjin	
Smart Plug	Sensor	Zigbee	SmartThings	Samjin	
Bulb	Bulb	Zigbee	Aduro SMART ERIA		

TABLE 4 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

COMMScope®
RUCKUS®

© 2021 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
<https://www.commscope.com>