RELEASE NOTES

RUCKUS IoT 1.8.2.0 MR Release Notes

Supporting IoT Controller Release 1.8.2.0

Part Number: 800-73058-001 Rev A
Publication Date: October 2021

Copyright, Trademark and Proprietary Rights Information

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

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

Overview

This document provides release information about RUCKUS IoT Suite 1.8.2.0 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)— As of this release the following AP models are now IoT 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 62x2:2 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 and Ultra High Performance Wi-Fi 6 8x8:8 with 5.9 Gbps HE80/40 Speeds and Embedded IoT Indoor Access Point R850.
- 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-1.8.2.0 MR Suite provides the following update:

- Support for 5.2.2.0 and 6.0.0.0 SZ versions
- UI Improvements and Stability Fixes
- Security Vulnerability Fixes
- Support for private zigbee attributes (cluster 201 – attribute 1E and cluster 204 – attribute 2) for thermostat (Radius One)
- Support to write attributes for cluster id 0x0201, 0x0204
- Support for AP R350

Changed Behavior

STOP and READ before ugrading

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

Firmware compatibility Matrix of Ruckus IOT controller and v/SZ

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)
- R850 Access Point (R850)
- R350 Access Point (R350)
- 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)

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
- **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: 5.2.2.0.317, 6.0.0.0.1331
- Control plane software version in the WLAN Controller: 5.2.2.0.126, 6.0.0.0.1213
- AP firmware version in the WLAN Controller: 5.2.2.0.301, 6.0.0.0.1594, 6.0.0.0.1610 (T350D), 6.0.0.0.3073 (R350)
- IoT Gateway Version

  5.2.2.0 - 1.8.2.0.18013

  6.0.0.0 – 1.8.2.0.18010
- SmartThings Version: 1.8.1.34.12

RIoT

- RUCKUS IoT Controller version: 1.8.2.0.44
- 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: 1.26.0.13
  - Lock Zigbee Version: 3.1.62.1
  - Lock Version: 3.17.37.5
- Smart Things
  - Hub Software Version: 3.14.1
  - SmartThings Hardware Version: 1.01
- DormaKaba
  - Ambiance Version: 2.6.9.9
  - 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
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 1 Release Build Compatibility Matrix (continued)

Release	IoT Controller	SZ	AP	Supported AP Models
IoT 1.8.2.0 [MR]	1.8.2.0.44	• 5.2.2.0.317 • 6.0.0.0.1331	5.2.2.0.301 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.

Supported Upgrade Path

1.8.1.0.16 -> 1.8.2.0.44

NOTE
1.8.2.0 IoT controller supports both 5.2.2.0 and 6.0.0.0.

Known Issues

The following are the caveats, limitations and known issues.

Component: IoT Feature in Access Point with IoT Module I100

- IOTC-4249 - BLE stack didn't come up on R510 AP if the MQTT connection lost for an interval and connects back.

  Workaround - Restart the IoT service from the UI.
- 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-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-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-4876 - During activation of DK plugin controller may get into a condition where AP and devices keep going online/offline.

  Workaround - Deactivate and Activate the DormaKaba plugin.
- IOTC-4857 - Hovering over the more icon in AP scan window shows the APs details extending beyond the window limit.

  Workaround - None.
- IOTC-4839 - Need to enter login credentials twice for first time after upgrade from 1.8.1.0 to 1.8.2.0.

  Workaround - None
- IOTC-4464 - If the AA lock is turn off (remove one battery) for few minutes, lock goes offline observed with internal radio AP's.

  Workaround - Need to reonboard the AA lock using the initial AA lock onboarding process.
- IOTC-4300 - Dormakaba: GW and lock connection are not persistent when IoT controller is rebooted.

Workaround -Reinitiate connection from Ambiance server to the controller

- IOTC-4290 - After AP factory reset, plugin external dongle (zigbee mode) AP comes up with Zigbee/Zigbee mode

  Workaround - Change one of the radio mode to BLE as Zigbee/Zigbee mode is not supported
- 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-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- 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-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-4039 - Not able to set Tx power as 8 for the internal radio of R650/T350D AP in BLE mode.

  Workaround - None.
- 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-3731 - Node-Red Deploy Icons are not correctly displayed when node-red config screen is opened in a new window.

  Workaround - None
- IOTC-3719 - MQTT Push events sent even with no state/device change/Action

  Workaround - None
- IOTC-3705 - No logs shown in UI for BLE scan on clicking on View Logs.

  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-3650 -Restoring a db backup from a N+1 controller on a standalone controller enables N+1.

  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-3080- Blacklisted devices are part of total device count in the dashboard.

  Workaround - None.
- 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-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-2980 - Connection lost message seen on switching from rules dashboard to rules configuration..

  Workaround - None (property of node-red design).

- IOTC-2971 - After initial configuration of the controller the UI will remain stuck in the EULA page in Firefox.

  Workaround - Refresh the page in the browser.

- 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.

Resolved Issues

The following issues are resolved for this release

TABLE 2 Resolved Issues

Key	Summary
IOTC-4491	Device by battery level widget-> count of device and in doughnut is mismatched since NA value is not populated.
IOTC-4459	Append AP MAC checkbox remains unchecked while upgrading the setup from 1.8.0.0 to 1.8.1.0 build
IOTC-3705	No logs shown in UI for BLE scan on clicking on View Logs
IOTC-3540	Telkonet: Setting static ip from controller shell does causing telkonet plugin not to run
ER-10714	vRIOT-1.7.1.0.16- Commands triggered from Visionline are sent as Broadcast by vRIOT when Target Door Lock is down.
ER-10645	AP stops handling the incoming beacon packets when it detects a beacon with Extended ADV (BT-5.x).
ER-10626/ ER-10620	Resolved an issue where vRIOT Throws a "License Parser Tool Error" when we upload License file.

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 (hypervisior/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

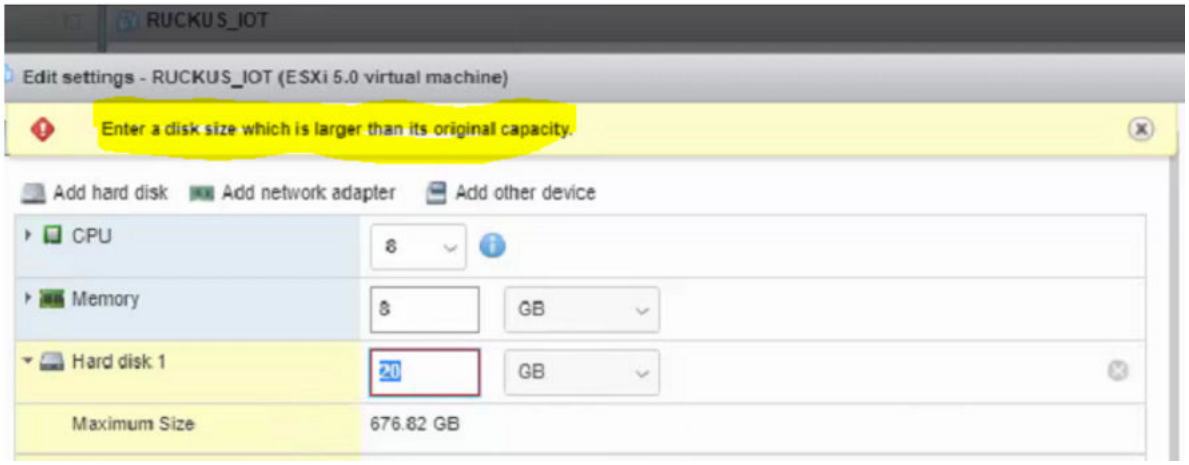
Caveats

- 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.

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

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.
- HTTPS Communication is not supported between Ambiance (DormaKaba) and IoT Controller.
- 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 seperate 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 3 Bulbs

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
Lightify (RGB) Model 73674	Bulb	Zigbee	Osram	OSRAM	LIGHTFY 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 Valeto (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 4 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 5 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
EcoInsight Plus	Thermostat	Zigbee	Telkonet	Telkonet	
ZBALRM	Alarm	Zigbee	Smartenit		Model #1021 A
Smart Blinds	Blinds	Zigbee	Axis Gear		

TABLE 6 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

TABLE 7 LoRa

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
Picocell	Gateway	LoRa	Semtech		
Mini Hub/ Basic station	Gateway	LoRa	TABS		
Door Sensor	Sensor	LoRa	TABS		
Occupancy Sensor	Sensor	LoRa	TABS		

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

TABLE 8 BLE (continued)

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
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	SmarThings	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

COMMSCOPE®
RUCKUS®

350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com