RELEASE NOTES

RUCKUS IoT 2.2.1.0 MR Release Notes

Supporting IoT Controller Release 2.2.1.0

Part Number: 800-73586-001 Rev B
Publication Date: May 2024

© 2024 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

Revision Number	Summary of changes	Publication date
B	Updating the topic Key Considerations Before Upgrading on page 11	May 2024

Overview

This document provides release information about RUCKUS IoT Suite 2.2.1.0, 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, which is comprised of five elements:

- RUCKUS IoT-ready Access Points (APs)— A device that allows IoT devices to securely connect to the internet and interact with other device.
- 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—An application, deployed in tandem with a RUCKUS SmartZone Controller, that performs connectivity, device, and security management functions behind the scenes for non-Wi-Fi devices. RUCKUS IoT Controller also facilitates cross-solution endpoint communication and provides APIs for northbound integration with IoT cloud services.
- RUCKUS IoT Insights—A cloud-based analytics platform, 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

ATTENTION

Before proceeding with the release activity, ensure you read the section Key Considerations Before Upgrading on page 11.

RUCKUS IoT Suite release 2.2.1.0 MR provides the following updates.

1. BLE Scan and Discovery mode for supporting different BLE Beacons.
   - **BLE Scan Mode** - The BLE Scan mode allows gateways to actively search for other devices, known as advertisers, that are broadcasting their presence or data by querying them for Scan Response packets.

     For more information, refer to *RUCKUS IoT Controller Configuration Guide* for this release.
   - **Discovery Mode** - The Discovery mode allows gateways to scan for various types of beacons based on their discoverability settings.

     For more information, refer to *RUCKUS IoT Controller Configuration Guide* for this release.
2. Stability Fixes - For more details on Stability Fixes, refer to Resolved Issues on page 23.

Key Considerations Before Upgrading

Consider the following factors before proceeding with an upgrade.

- RUCKUS recommends that customers conduct thorough validation and testing of IoT releases within a 90-day trial period before proceeding with any upgrades to their production systems. This ensures that any potential issues or compatibility concerns are identified and addressed before implementation in a live environment.
- The RUCKUS IoT Controller 2.2.1.0 does not support SmartZone Controller releases 7.x.
- The RUCKUS IoT Controller releases after version 2.2.1.0 will not support downgrades.
- To ensure proper database backup/restore functionality from version 1.8.2.0, RUCKUS recommends performing a fresh deployment of version 2.0.1.0.64. After the deployment, restore the 1.8.2.0 database and proceed with upgrades to versions 2.1.1.0 and then to 2.2.1.0.

  NOTE
  Direct migration from version 1.8.2.0 to 2.2.1.0 is not supported. The supported IoT firmware upgrade path is: 1.8.2.0 > 2.0.1.0 > 2.1.1.0 > 2.2.1.0.

- When downgrading a controller from 2.2.1.0 to 2.1.1.0 with APs that have a BLE radio, the radio may become unavailable. To avoid this issue, change the radio mode to any Zigbee mode before downgrading. Once the downgrade is successful, change the radio mode back to BLE.
- Refer to the *RUCKUS IoT Controller Licensing Guide* for guidelines on migrating licenses from Release 1.x to 2.0, 2.0.1, and from Release 2.0 to 2.2.1.
- The process of taking a snapshot of the RUCKUS IoT Controller and deploying it is not supported.

Hardware and Software Support

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

Compatible Hardware:

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

Compatible Software:

- Virtual SmartZone – High Scale (vSZ-H)
- Virtual SmartZone – Essentials (vSZ-E)
- SmartZone 144 (SZ144)
- SmartZone 300 (SZ300)
- 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 (for example, RUCKUS IoT controller, VMware ESXi, Ubuntu Linux server, IP camera VMS, additional IoT VMs or applications), RUCKUS recommends server hardware that meets the following 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 APs	Number of Devices	Type of Device
1500	1500	Assa Abloy Visionline
1500	1500	Dormakaba
500	500	Generic Zigbee
500	500	Vostio
250	250 AP	250 Beacon messages with interval of 1 or 2 seconds
1500	1500 AP	BaaS

NOTE

The combination setup will support only 500 APs and 500 devices (even in case of Assa Abloy and Dormakaba).

Release Information

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

Virtual SmartZone and SmartZone (vSZ-H, vSZ-E, SZ-100, SZ-144, and SZ300)

- WLAN Controller version: 5.2.2.0.1563, 6.1.2.0.441
- AP firmware version in the WLAN Controller: 5.2.2.0.2122, 6.1.2.0.1309
- IoT Gateway Version

  1.9.2.2.11000 (applicable to vSZ/SZ firmware version 5.2.2.0)

  2.2.1.0.20013 (applicable to vSZ/SZ firmware version 6.1.2.0)

RIoT

- RUCKUS IoT Controller version: 2.2.1.0.25
- 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: 2.7.6
- Lock Firmware version: 3.59.10.90
- Zigbee Firmware version: 2.10.14

SALTO

- Lock Model – Ælement Fusion
- Lock Firmware version – AB.10, Control-01-38, HW Rev-00
- PPD Firmware version – 02.22
- SALTO Space version – 6.8.4.0

TABLE 2 Release Build Compatibility Matrix

Release	IoT Controller	SZ/vSZ Controller	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	5.2.2.0.2016 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	• 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 2.0.1.0	2.0.1.0.64	• 5.2.2.0.1562 • 6.1.0.0.935	5.2.2.0.2064 IoT Version : 1.9.2.0.11010 ST Version: 1.8.1.34.12 6.1.0.0.1595/6.2.0.103.513/6.1.0.0.9210 (R760) IoT Version : 2.0.1.0.20015 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, R760
IoT 2.1.0.0	2.1.0.0.43	• 5.2.2.0.1562 • 6.1.1.0.959	5.2.2.0.2122 IoT Version : 1.9.2.1.10016 6.1.1.0.1322 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
IoT 2.1.1.0	2.1.0.0.43	• 5.2.2.0.1562 • 6.1.1.0.959	5.2.2.0.2122 IoT Version : 1.9.2.1.10016 6.1.1.0.1322 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
IoT 2.2.0.0	2.2.0.0.28	• 5.2.2.0.1562 • 6.1.2.0.354	5.2.2.0.2064 IoT Version : 1.9.2.2.10011 6.1.2.0.850 IoT Version: 2.2.0.0.20009	H510, R510, T310d, E510, R610, R650, R710, R720, T610, R730, R750, T750, C110, M510, R550, H550, T350D, R350, R850, T750SE, H350, R760, R560
IoT 2.2.1.0	2.2.1.0.25	• 5.2.2.0.1563 • 6.1.2.0.441	5.2.2.0.2122 IoT Version : 1.9.2.2.11000 6.1.2.0.1309 IoT Version: 2.2.1.0.20013	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

2.1.1.0.2 -> 2.2.1.0.25

2.2.0.0.28 -> 2.2.1.0.25

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- 7589 - Upgrade from 2.1.1 -> 2.2.1 -> Delete Plugin -> 2.1.1 -> have to activate plugin twice to enable it.

  Workaround - Activate the Plugin twice.
- IOTC- 7579 - Gateway commissioning info not sent to Ambiance while changing the mode to Zigbee_DK if the AP has already received the Dormakaba configuration.

  Workaround - None
- IOTC- 7530 - Gateway commissioning info not sent to Ambiance while doing a mode change from any other radio to Zigbee_DK.

  Workaround - Update the DK plugin to send commissioning message for all APs.
- IOTC- 7516 - After upgrade from unsupported version to 2.2.1, the APs go into firmware mismatch state even though the controller stays in the current version.

  Workaround - Follow the upgrade path to get to 2.2.1. Path - 2.0.0.0.82 -> 2.0.1.0.64 -> 2.1.1.0.2 -> 2.2.1.0.25
- IOTC-7441 - Replaced Secondary controller doesn't become active after performing failover from primary controller.

  Workaround - None

- IOTC-7394 - Node status of the secondary controller is not shown in RAS of primary controller after replacing the secondary controller.

  Workaround - None
- IOTC-7178 - After Trial License expiry no error message is displayed. controller will navigate to license page and no other navigation is allowed.

  Workaround - Upload a Valid license .
- IOTC- 7392 - Node status for the other controller (Primary or secondary) not shown in RAS after replacing the primary controller.

  Workaround - None.
- IOTC- 7191 - Controller UI becomes inaccessible in very corner cases.

  Workaround - Restart services from controller shell or reboot the controller.
- IOTC- 7190 - Deleting and onboarding a Dormakaba lock between different AP might cause Last seen value to be shown incorrectly.

  Workaround - None.
- IOTC-7155 - Sometimes Dormakaba lock is not shown in ambiance server but get onboarded to IOT controller

  Workaround - Delete the lock from the controller and re-onboard the lock.
- IOTC-7032 - Upgrading controller from 2.0.1.2 to 2.2.0.0 causes Salto locks to become offline in the Salto Space

  Workaround - Reset the Salto plugin from the side panel -> Deactivate the Salto plugin -> Login to the Salto Space and goto System-Salto Network -> Select the Controller and reset the controller -> Generate the secret key and enable the Salto plugin from the controller -> Initialize the VRIOT controller from the Salto Space.
- IOTC-6487 - Active SSH connections are not terminated on disabling the SSH from UI

  Workaround - None
- IOTC-6379 - After failover Gateway and locks are not coming online on the Space

  Workaround - None. N+1 is not supported.
- IOTC-6361 - Salto Key is missing on DB restore setup

  Workaround - None: DB backup/restore is not supported
- IOTC-6169 - Salto: Radio's LQI, RSSI and Last Seen Values are not displayed or incorrectly displayed.

  Workaround - None.
- IOTC-6243- Salto tag should be added to the AP whenever a Salto lock is added to the controller.

  Workaround - None
- IOTC-6185 - Delete option of Salto locks from the controller is allowed which is not a valid use case..

  Workaround - None. Do not delete the lock as it will not auto populate again on the controller
- 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

  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 Paring ON from Ambiance server for the Gateway.

- 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.

Resolved Issues

The following issues are resolved in this release.

TABLE 3 Resolved Issues

Key	Summary
ER-13401	Location packet missing after upgrade from 2.0 to 2.2.
ER-13396	BLE radio does not come up when AP connected to 1.8.2 controller is connected directly to 2.2 without intermediate upgrade.
IOTC-7308	zclcapability API failing without passing pin as params in payload.

Best Practices

Following is the list of best practices to be followed to maximize the benefits of the new release, and to minimize the potential challenges or risks.

- The recommended periodic interval for the Controller Data Stream Plugin is 120 seconds. It is important to adhere to this interval as using lesser values could potentially lead to system instability.
- It is crucial to ensure that the time and timezone are accurately set in the RUCKUS IoT Controller. This ensures that all time-based functions and features operate correctly and that logs and events are timestamped accurately.
- To ensure successful failover in N+1 mode, it is necessary to configure the AP MQTT Broker for the Virtual IP. This allows for seamless transition and uninterrupted communication between the Access Points (APs) and the IoT Controller in the event of a failover.

Caveats and Limitations

Caveats

- The backup database size is reduced to 132kb.
- The admin password cannot be retrieved once lost.
- RUCKUS recommends to back up the database at regular intervals.
- The RUCKUS IoT platform is not FIPS compliant and if an AP has 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 you override the MQTT IP using AP CLI script from the vSZ.

  Workaround - Do not push MQTT Broker IP to the APs 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 to bulk scan to onboard IoT devices.

Limitations

- Do not use admin credentials for activating the Dormakaba plugin.
- In a SALTO Setup, N+1 is not supported.
- In a SALTO Setup, database backup/restore is not supported.
- 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.
- Database backup taken from a pre-2.2.0.0 controller cannot be restored on a 2.2.0.0 controller.
- Database backup and restore is not supported across major releases.
- N+1 Auto Fallback is not supported (if primary is back online, secondary will run as active secondary).
- UEI Thermostat: 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 the 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 unplugged and then plugged in.
- Concurrent ZigBee-ZigBee, ZigbeeAA-ZigbeeAA, ZigbeeDK-ZigbeeDK 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.
- 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.

- Snapshot and deploy of IoT controller snapshot is not supported.

Supported Devices

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

TABLE 4 Bulb

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 5 Lock

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	
Ælement Fusion	Lock	BLE	Salto	Salto Lock	FwNum 0141 (v01.20)

TABLE 6 SWITCH/PLUG/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	SmartThings	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 SWITCH/PLUG/THERMOSTAT/ALARM/BLINDS (continued)

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
UEI Thermostat	Thermostat	Zigbee	UEI		TBH300ZBSN

TABLE 7 Sensor Devices

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	SmartThings	SAMJIN	IM6001-MPP01
Water Leak Sensor	Sensor	Zigbee	SmartThings	SAMJIN	IM6001-WLP01
Motion Sensor	Sensor	Zigbee	SmartThings	SAMJIN	IM6001-MTP01
Button	Sensor	Zigbee	SmartThings	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 Bluetooth Low Energy (BLE) Devices

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 Device not QA tested but supported

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
VingCard Sigma	Lock	Zigbee	Assa Abloy	AA_LOCK	Sigma
VingCard Alpha	Lock	Zigbee	Assa Abloy	AA_LOCK	Alpha
VingCard Classic	Lock	Zigbee	Assa Abloy	AA_LOCK	Classic
VingCard Allure	Lock	Zigbee	Assa Abloy	AA_LOCK	Allure
Ælement	Lock	BLE	Salto	Salto	FwNum 0135 (v03.21)
XS4 One	Lock	BLE	Salto	Salto	FwNum 0134 (v01.80
XS4 Original+	Lock	BLE	Salto	Salto	FwNum 0174 (v01.10)
NEO	Lock	BLE	Salto	Salto	FwNum 0158 (v01.20

© 2024 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com