

CONNECTED ENTRY RUCKUS AND ASSA ABLOY

ROOM 2023

C.

Configuration & Deployment Guide - Revision 1.0

FEBRUARY 2019

OCKED

Connected Entry: Ruckus and Assa Abloy Deployment & Configuration Guide – Revision 1.0



FEBRUARY 2019

TABLE OF CONTENTS

Intended Audience	. 4
Introduction	. 5
Overview	. 6
Major Subsystems	6
Data Paths	. 7
Versions	8
Design & Installation	. 9
Wi-Fi Infrastructure, Coverage & AP Placement	9
Zigbee Coverage	9
Ruckus loT Ready Infrastructure	9
Ruckus SmartZone Network Controller	9
Ruckus Access Points (APs)	0
Ruckus I100 IoT Module	0
Ruckus IoT Controller	0
Assa Abloy Visionline Server	1
Creating Zigbee function cards for AAGS locks	1
Configuration	12
Ruckus Access Points	12
Ruckus IoT Controller	13
Onboarding & Binding Locks	4
Verification & Troubleshooting	19
Zigbee Sniffer	9
IoT Controller Communications Debugger	20
Visionline Event Logger	20



COPYRIGHT NOTICE AND PROPRIETARY INFORMATION

© 2019 ARRIS Enterprises LLC. 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 ARRIS International plc and/or its affiliates ("ARRIS"). ARRIS reserves the right to revise or change this content from time to time without obligation on the part of ARRIS 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, ARRIS 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. ARRIS 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. ARRIS 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 ARRIS 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 ARRIS, ARRIS AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIES, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF ARRIS 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, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, EdgeIron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, ZoneFlex are trademarks of ARRIS International plc and/ or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access (WPA), the Wi-Fi Protected Setup logo, and WMM are registered trademarks of Wi-Fi Alliance. Wi-Fi Protected Setup[™], Wi-Fi Multimedia[™], and WPA2[™] are trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.



INTENDED AUDIENCE

This document outlines the steps in the deployment and configuration of the Assa Abloy connected smart locks using the Ruckus Networks wireless infrastructure. The document has been written for use by systems engineers. A background in the Ruckus wireless infrastructure as well as the Assa Abloy connected locks is recommended.



INTRODUCTION

Internet of Things (IoT) deployments are often complex and involve products and services at various layers: devices/endpoints, network infrastructure, middleware and platform/services. Market complexity at each layer makes deployments risky and requires extensive integration services. Network silos at each layer necessitate the duplication of equipment and cabling thereby making deployments expensive. Furthermore, such patched together solutions give rise to security vulnerabilities.

Ruckus + Assa Abloy offer an integrated, unified solution for connected, smart door locks. The solution leverages off the Ruckus Wireless Wi-Fi infrastructure and Assa Abloy's leading position in the door-opening marketplace. This integrated approach simplifies device/endpoint onboarding, establishes uniform security protocols and unifies device/endpoint management and policy setting.

This document provides a step-by-step guide to setting up and configuring a connected lock solution using locks provided by Assa Abloy and wireless infrastructure provided by Ruckus.



OVERVIEW

MAJOR SUBSYSTEMS

The Figure below depicts the major system components. Their functionality is summarized in the subsequent table.



Subsystem / Component	Description
SmartZone Network Controller	The Ruckus SmartZone Network Controller simplifies the complexity of scaling and managing Ruckus access points (APs) and switches. All physical (SZ100 / SZ300) and virtual (VSZ-E / VSZ-H) SmartZone appliances support network configuration, monitoring, provisioning, discovery, planning, troubleshooting, performance management, security and reporting. SmartZone network controllers are essential to managing Ruckus loT-ready APs.
Access Points	The Ruckus family of Wi-Fi APs includes a variety of form factors, performance tiers, and price points. Many Ruck- us APs can be upgraded with a Ruckus IoT Module to support IoT services such as Zigbee. Specific models that can be equipped include: H510, R510, T310, E510, R610, T610, R710, R720
loT Controller	The Ruckus IoT Controller is available as a virtual machine and is the management platform for provisioning and on-boarding Ruckus IoT Modules and also provides connectivity to smart lock management platforms such as the Assa Abloy Visionline platform.
Smart Door Lock	Assa Abloy smart door locks are Zigbee capable and communicate with Zigbee enabled Ruckus APs. Using a variety of test cards one can activate various door lock functions. Creation of these test cards is discussed later within this document.
Visionline Server	This Assa Abloy Windows based server is the services and management platform for controlling and setting policy for the smart door locks.
Wi-Fi Devices	Wi-Fi devices such as smartphones, tablets and laptops that connect to the Ruckus wireless infrastructure.
Network	The network that provides connectivity between the various components above.



DATA PATHS

Data is sent between an Assa Abloy Smart Door Lock to the Assa Abloy Visionline Server over the Ruckus wireless infrastructure. The Smart Door Lock connects using Zigbee to a Ruckus I100 IoT Module attached to an upgraded Ruckus IoT-ready AP or to a Ruckus IoT-embedded AP. The Ruckus AP then forwards the data to the Ruckus IoT Controller which then forwards this to the Visionline server, thus completing the data path.

Management data is transmitted between the SmartZone Network Controller and Ruckus APs for onboarding and management of the wireless infrastructure and is not a part of the end-to-end data path.





VERSIONS

The following versions/options are required for the integrated setup.

Component	Version
Ruckus SmartZone	3.6.1.2.10051 or higher. Note that the version must be IoT capable. Higher versions (such as 5.0) may not be IoT capable.
Ruckus IoT Controller	1.0 or higher
AAGS Visionline Server	Visionline 1.22.0 or higher. Required Options
	• Online
	Online advance
	Online via generic network infrastructure Zigbee
	# of online rooms
	Web service for callbacks
	Web service for checking and confirming alarms
	Web service for reading network nodes
	Web service for sending open/close commands to doors
AAGS Smart Door Locks	3G and/or 4G RFID lock with Zigbee
	Lock firmware 3.17.36.1 or higher
	Zigbee end node firmware 3.0.60 or higher



DESIGN & INSTALLATION

This section addresses the design and installation considerations pertaining to the various system components.

WI-FI INFRASTRUCTURE, COVERAGE & AP PLACEMENT

The design and installation of the Wi-Fi infrastructure (number and placement of APs, switches, power, etc.) is beyond the scope of this document. There are a number of Design and Best Practice Guides available from Ruckus on how to deploy Wi-Fi in a hospitality environment.

ZIGBEE COVERAGE

The Zigbee coverage requirement is -65 dBm. In most cases, not all APs need to be equipped with the I100 module to provide sufficient Zigbee coverage to the all the door locks in a hospitality environment. In a hotel, APs are deployed to provide in room as well as in-corridor coverage. This typically results in placing APs in the corridors as well as in the room. Equipping the corridor APs with I100 should provide sufficient Zigbee coverage in most cases.

All hospitality sites are different from a RF Coverage perspective and it is recommended that a site survey be performed with a RF Sniffer to ensure that sufficient Zigbee coverage will be obtained at the door locks.

RUCKUS IOT READY INFRASTRUCTURE

As described in the Ruckus IoT Suite Getting Started Guide¹, this consists of installing the following

- 1. Ruckus SmartZone Network Controller
- 2. Ruckus Access Points
- 3. Ruckus I100 IoT Module on the Ruckus AP
- 4. Ruckus IoT Controller

RUCKUS SMARTZONE NETWORK CONTROLLER

The Ruckus SmartZone Network Controller is available as either an appliance (SZ-100) or a virtual controller. The virtual controller is available as an *.ova file and can be installed on the VMWare/ESXi hypervisor. Specifications regarding the minimum requirements for CPU, Memory, Disk, etc. are provided in the Getting Started Guide². This guide also contains detailed installation instructions for various virtualization platforms.

Given below is a brief summary of the relevant steps.

- 1. Download the relevant image (such as *.ova file) and upload to the Hypervisor
- 2. Configure the CPU, RAM, Disk, etc. for the image. This is determined by the number of APs, clients, etc. to be supported and is specified in the Guide mentioned above. Also, delete Network Adapter 2 and 3.
- 3. Launch the image and wait for it to power up on the hypervisor console
- 4. Perform the basic configuration:
 - a. Login in with 'admin' for both username and password
 - b. Enter 'setup' command and press enter
 - c. For example, Enter '1' for Essentials and press enter
 - d. Enter 'Y' and press enter
 - e. Enter '1' for IPv4 and press enter
 - f. Enter '2' for DHCP and press enter
 - g. Note down the assigned IP address to use later for accessing vSZ web UI and enter 'y' for yes to and press enter
 - h. Enter the primary DNS that the IoT Controller uses (refer back to 'Get Network Info' command) and press enter

¹ Ruckus IOT Suite Getting Started Guide

² Ruckus SmartZone Getting Started Guide



- i. Enter secondary DNS if applicable, otherwise leave blank and press enter
- j. Enter Control NAT IP if applicable, otherwise leave blank and press enter
- k. Enter 'restart network' to restart changes made and press enter
- I. Type 'setup' and press enter
- m. Type 'NO' when asked setup network and press enter
- n. Type 'c" to create new cluster and press enter
- o. Enter a cluster name (ie: Vingcard) and press enter
- p. Enter a controller description (ie: vrIoT) and press enter
- q. Type 'y' to confirm settings are correct and press enter
- r. Enter a controller blade name and press enter
- s. Press enter @ system UTC
- t. Press enter @ NTP server
- u. Type 'N' when asked to convert ZoneDirector APs and press enter
- v. Enter a new admin password and press enter, then enter it again and press enter
- w. Enter a CLI enable command password and press enter, then enter it again and press enter
- x. Wait for setup to complete
- 5. Access the instance via https using its IP address and port 8443. The username is admin and the password are the one set above.

RUCKUS ACCESS POINTS (APS)

Deployment of Ruckus APs is beyond the scope of this document. Depending on the AP model number, detailed installation instructions are available from Ruckus.

After the APs have been installed, one needs to ensure that they have been "discovered" by the Ruckus SmartZone Network Controller. Once this discovery has taken place, the controller will automatically upgrade the AP firmware.

RUCKUS I100 IoT MODULE

Detailed instructions for installing the I100 IoT module on the AP are available in the I100 Setup Guide.³

RUCKUS IOT CONTROLLER

The Ruckus IoT Controller is a virtual controller that is available as a *.ova file that can be installed on the VMware ESXi hypervisor. Detailed installation instructions including the CPU, RAM, Disk, etc. requirements are contained in the IoT Controller Installation Guide.⁴

Given below is a summary of the relevant steps for installing this on the VMWare ESXi platform.

- 1. Download the *.ova image and upload to the ESXi server
- 2. Verify that the instance has 2 vCPUs, 2 GB RAM and 8GB disk
- 3. Power up the instance and access it via the console. Credentials are admin/admin
- 4. Enter 1 to get the IP address of the virtual machine
- 5. Access the instance via a Web browser. Both http and https are supported
- 6. In the initialization page, select all the services and also specify the FQDN for this instance
- 7. Confirm the configuration information and click Start
- 8. The IoT Controller page is now displayed. Credentials are admin/admin

³ Ruckus I100 IoT Module Quick Setup Guide

⁴ Ruckus IOT Controller, Software Installation Guide



ASSA ABLOY VISIONLINE SERVER

This is a Windows based server. After installation, its IP Address/FQDN as well as the login credentials should be noted.

CREATING ZIGBEE FUNCTION CARDS FOR AAGS LOCKS

These exercise various door lock functions and are required for the binding process as well as for verification and troubleshooting. They can be created using the Visionline server as follows:

- 1. You will need 2 x 4K Mifare keys (Staff keys)
 - a. Set sub product Zigbee key
 - b. Start discovery in Zigbee
- 2. Visionline operator who has access to login and create Zigbee setup cards
- 3. In the Navigation window to the left, scroll down to SETUP CARDS
- 4. Select ZIGBEE CONFIGURATION
- 5. Click the '...' button to select the user the key is being issued for
- 6. Set the number of days you want this key to be valid for
- 7. Under type, select **SET SUB PRODUCT ZIGBEE**
- 8. Click 'Make card' button
- 9. Repeat steps 3-8 with the exception of step 7, select START DISCOVERY IN ZIGBEE



CONFIGURATION

This section outlines the configuration steps for each subsystem.

RUCKUS ACCESS POINTS

The access point needs to be provisioned with an IoT controller IP address. This can be done either using DHCP Option 43 or using AP CLI.

DHCP OPTION

The DHCP server could be run on ICX switch or any server. This section presents an example configuration for ICX switch. Please note the use of option 43, sub-codes 6 for vSZ controller IP and 21 (hex 15) for the IoT controller IP.

```
ip dhcp-server pool group1
excluded-address 172.16.101.254
lease 1 0 0
network 172.16.101.0 255.255.255.0
option 3 ip 172.16.101.254
option 6 ip 8.8.8.8
option 43 hex 060e3137322e31362e3230302e323030150e3137322e31362e3230302e313030
deploy
```

AP CLI

- 1. Log into the AP via ssh (Terminal on MAC or Putty on a PC)
- 2. Credentials are those listed in the SmartZone Controller (Access Points->AP->Configure->AP Configuration->AP Admin Logon)
- 3. Enter the following commands

```
set IoTg-mqtt-brokerip <IoT Controller IP>
set IoTg-mqtt-ssl 1
set IoTg-mqtt-port 8883
set IoTg-enable 1
```

As shown below, the AP will now appear in the IoT Controller "IoT APs" screen. Repeat the above for all APs.





UCKUS IoT Contr	oller	Dashboard	INT APS INT Devices	Events Adm	in IoTAPI			1.1.0. Thu N (Ame	0.6 Versio ov 15 2018 rica/Los_A
0 IoT ACCESS	Poi	Approve IoT APs)		Batch Actions:		lect	Q (Apply	0
► (+52-6-R07-Sandbox		Status	Name	MAC ID	IP Address	Protocol	Channel	Uptime	
► [v52-6-8007]	0	Online	RuckusAP	34:8F:27:26:4A:90	192.168.46.106	ZIGBEE	16	27 days, 3:36:39	(Scan
	0	Offline	H510-Zigbee-Futurecom	44:10:98:04:80:60	192.168.40.50	ZIGBEE	25	0 days, 2:54:26	Scan
	0	Offline	R510-TALHEIDA-LATAM-BR	EC:8C:A2:11:ED:F0	10.111.111.150	NA	NA.	3 days, 10:02:05	(Scan
	0	Offline	H510-BLE-Futurecom	44:1E:98:04:EF:C0	10.73.133.230	BLE	NA,	0 days, 12:07:52	Scan
	0	Online	R510 IoT	34:8F:27:25:56:A0	10.10.6.79	BLE	NA	16 days, 1:14:08	Scan
	0	Offline	R510-Saul	EC:58:EA:00:13:70	136.170.209.205	BLE	NA	0 days, 4:48:46	Scan
	0	Unapproved	RuckusAP	E8:10:A8:01:86:E0	192.168.23.136	NA	NA ·	15 days, 3:40:44	(Scan

RUCKUS IOT CONTROLLER

Assa Abloy Plugin

As shown below, the Assa Abloy plugin needs to be activated in the IoT Controller. The IP address and credentials for the Visionline Server are obtained after its installation.

RUCKUS INT Cor	itroller Dashboard IoT	APs IoT Devices	Events	Admin	Iot Api	1.1.0.0.6 Version Wed Sep 19 2018 15:52:37 ((America/Onicago)
Admin Services Plagins Account VM Configurations VM Configurations UN Configurations DB Backup Reset & Reboot	Select a Plugin to Activate : Active Plugin List	Assa Abloy	•		Assa Abloy Juername sym assword 10.243.2.194 bert 443	Show 30N (Activate



ONBOARDING & BINDING LOCKS

There are two methods of onboarding and binding the locks: (a) Keycard method and (b) Lock Service 3G method. These are detailed below.

KeyCard Method (Preferred)

- 1. On the Ruckus IoT Controller, Go to the IoT APs module
- 2. All APs previously provisioned should now appear here and awaiting approval
- 3. Check the box next to the APs, select APPROVE in the batch action drop down, and then click APPLY
- 4. A pop confirmation of the approval should appear
- 5. Repeat for each AP

RUCKUS	IoT Controller	Dash	board loT A	Ps loT	Devices	Events	Admin	IoT API						1.1.0.0.6 Version Wed Sep 19 2018 (America/Chicage	15:04:49 >)	C
																ĥ
IoT A	Access Po	ints	5										۹			
1 IoT AP Se	elected	Pre	Approve IoT APs							Batcl	n Actions:	Approve		(Apply)	2	
► [Vingca	ard]		Status	Name	MAC	ID	IP Address	Protocol	Channel	Uptime		Actions		Tags		
			Unapproved	RuckusAP	E8:1D:A8:0	0B:9B:20	10.243.2.201	NA	NA	0 days, 0:04:06	Scan	Restart IoT Service	Remove	All RuckusAP E8:1D:A	3:06	
			Suc	cess								×				
			IoT /	Ps App	roved Su	uccesfu	ully	oint	ts							

- 6. Double click on an AP to open the properties
- 7. Change the MODE to ZIGBEE(AAGS) and click apply
- 8. A popup confirmation of the changes will appear
- 9. Once the AP comes back up, it's ready to bind with a lock
- 10. Repeat for all APs

tuckusAP onto	ne	8
CR-10-AB-08-98-20 ×	Rachard +	
Add new tag		
Scan for IoT De	vices Restart IoT	Service
IoT APs Setting		
IoT AP Approve	-	Apply)
Mode	(Zigbee(AA) v	Apply
IP	10.243.5.229	
MAC	E8:10:A8:08:98:20	
Net Mask	255.255.254.0	
DNS	10.243.5.68	
IoT Module MAC	90:F0:9F:FF:FE:7C:33:97	
IoT Module Mode	zigbee_aa	
Advanced Mode		(Internet)
	_	



11. Click Scan for IoT Devices button and a pop-up window will appear that shows it's scanning

Scan Started at 9/10/2018 107 AP Scanning for Device	, 12:32:19 PM and will automatica n: RuckusAP	lly end at 9/11/2018, 12	::32:19 AM	Stop Scarvi
Name *	Hanufacturer Name	MAC Address	INT AP MAC	Actions
	No Devic	es/Sensors Found		

- 12. DEVICE SCAN STATUS should pop up indicating IoT is actively scanning
- 13. Create a Zigbee function keycard. (refer to "Creating Zigbee function cards for AAGS locks" section)
- 14. A device should now appear in list
- **15.** Enter the preferred name, such as the room number, under the NAME field and click ACCEPT. Once the device has been accepted, it will no longer appear in the scan window.
- 16. Repeat steps 13-15 for any other locks that are to be connected to this AP
- 17. Once complete, click STOP SCANNIG and repeat all steps above for the next AP

Dev	vice Scan Status				~
	Scan Started at 9/10/2018 IOT AP Scanning for Device	. 12:32:19 PH and will autom is : RuckusAP	atically end at 9/11/2018, 12	2:32:19 AM	(Stop Scanning)
	Name *	Manufacturer Name	MAC Address	IOT AP MAC	Actions
		No D	evices/Sensors Found		
				art markets many	where the
Scanning For D	Devices 📀			Advanced Marke	1999 II.
Scanning For C	Devices 💽			intraction man	
Scanning For C	Devices () atus	II automatically end at 9/21/20	715, 11:32-18 PM	int matche man	ana an
Scanning For D CCE Scan State an Started at 9/2 T AP Scanning for	Devices O atus 11/2018, 11:33:18 AM and wi r Devices : RuckusAP	II automatically end at 9/21/20	718, 11:32:18 PM	is Produkt man	Stop Scanning
Scanning For I CCE Scan State an Started at 9/2 T AP Scanning for Nan	Devices O atus ti/2018, 11:33:18 AM and wi r Devices : RuckusAP me *	II automatically end at 9/21/20 Manufacturer Name	718, 11:32:18 PM MAC Address	in Transformer and the second standard	Step Scanning Actions



- 18. Go to the IoT DEVICE module at the top of the window
- 19. All accepted locks should now appear in this list
- 20. Perform end to end testing to confirm lock events are posting to Visionline and you're able to send online commands to the lock

oT Devices									۹.		
0 Device Selected	Pre	- Approve IoT Device	0				Batch Actions:	(Select	•	(Apply)	0
► (Vegard)		IoT Device Name	IsT Device MAC	INT AP MAC	Protocol	Type	Last Seen	Actions		Tags	
	0	101	00:17:74:01:06:01:33:80	E8:10:A8:08:3E:60	tigbee_aa	AA_LOCK	2 minutes ago	(Remove) (Blacklist)	00		

Lock Service 3G Method

This method requires authorized users of Lock Service 3G.

- 1. On the Ruckus IoT Controller, Go to the IoT APs module
- 2. All APs previously provisioned should now appear here and awaiting approval
- 3. Check the box next to the APs, select APPROVE in the batch action drop down, and then click APPLY
- 4. A pop confirmation of the approval should appear
- 5. Repeat for each AP

RUCKUS	IoT Controller	Dash	board loT A	Ps loT (Devices Events	Admin	IoT API				1.1.0.0.6 Version Wed Sep 19 2018 15:04:49 (America/Chicago)	O
IOT A	Access Poi	nts	Approve IoT APs						Batch	Q.	(Apply) (2)	
► [Vingca	ard]		Status Unapproved	Name RuckusAP	MAC ID E8:1D:A8:0B:9B:20	IP Address 10.243.2.201	Protocol	Channel NA	Uptime 0 days, 0:04:06	Actions Scan (Restart IoT Service) Remove)	Tags Al) (RackusAP) (E8:10:A8:0)	



- 6. Double click on an AP to open the properties
- 7. Change the MODE to ZIGBEE(AAGS) and click apply
- 8. A popup confirmation of the changes will appear
- 9. Once the AP comes back up, it's ready to bind with a lock
- 10. Repeat for all APs



11. Click Scan for IoT Devices button and a pop-up window will appear that shows it's scanning



- 12. Connect Service PC to the lock
- Under CONFIGURE LOCK, select 'Set sub product Zigbee' and press 'Set'
 a. LCU LED should respond with single green flash
- 14. Under CONFIGURE LOCK, select 'Start discovery in Zigbee' and press 'Set'
- a. LCU LED should respond with a quick green flutter
- 15. Disconnect Service PC from lock



- 16. Present a valid guest key to the lock to operate it
- 17. A device should appear when the IoT AP found the lock
- 18. Enter the room number/name under the IoT Device Name field
- 19. Click on the ALLOW
- 20. This lock should now appear under the IoT Devices module

RUCKUS INT Con	troller	Dushboard	IoT APs IoT Devices	Events Adm	in loTA	м			1.1.0.0.6 Version Tue Sep 11 2018 16:31 (America/Oscago)
IOT Device 0 Device Selected	es @	e-Approve IoT Devic	e)		B	atch ctions:	Select	Q.	1997) (Ö)
► (vigord)		IoT Device Name	IoT Device MAC	INT AP MAC	Protocol	Type	Last Seen	Action	
		101	00.17.7A.01.06.05.C8.5E	E8:10:A8:08:98:20	tigbee, as	AA_LOCK	In 5 hours	(Remove) (Backlist)

- 21. Check Visionline Sysmon to confirm if lock events are populating
- 22. Perform Visionline any online lock commands to confirm functionality



VERIFICATION & TROUBLESHOOTING

Overall system operation can be verified by making sure that any action on the lock (such as open/close, use of various test cards, etc.) is reflected in the Visionline Server. Conversely, any control action (such as door open/close) initiated in the Visionline Server should be reflected in a corresponding action in the chosen lock.

The following troubleshooting tools can be used to verify communications on the various segments of the Smart Door Lock to Visionline Server path.

ZIGBEE SNIFFER

Recommended Zigbee Sniffer S/W and hardware modules:

Software:

- Ubiqua Protocol Analyzer: https://www.ubilogix.com/ubiqua/ (Software license/subscription required)
- TI SmartRF Packet Sniffer: <u>http://www.ti.com/tool/PACKET-SNIFFER</u> (Free & provides Wireshark integration)

USB Capture Device:

• TI CC 2531 USB Module: http://www.ti.com/tool/cc2531emk

*Please refer SmartRF documentation for all the supported capture devices

This can be used to examine the door lock to AP communications over Zigbee.

Padat RX P	Time (es) +44715 +4125095 10	Frame control field Type Sec Pod Ack.reg Hill_compr DD 0 0 0 0 0	Sequence number 1x23 (x7777	Dest. Address Caffff	Reactor request 10 PCS						
Radar RX 10	Time (us) =4087 =4129182 28	Frame control field Type Dec Phd. Ack.reg 248_compr 308 0 0 0 0 0	Bequence number (a1) (a15k)	Address dations	Superframe specification 80 80 F. CAP BLE Courd Associ 15 15 15 0 1 0	GFS Relds Les. Promits 0 0	Descion payload 00 20 84 30 83 36 83 49 88 45 31 77 77 77 11	Pak_Prof P.Ve	Beauton Payload (MNK La r Biz_Cap Dev.Depth 0x1 0x0	per Decoded) Dev. Cop. Rat., HARSD Col. Dath (Concernment)	TX Offset (ryshols) (arrent
Public RE 11	Fame (ut) +23110 +4052292 28	Frame control field Type Sec Pnd Ack.reg Bidl_compar Bidl 0 0 0 0	Sequence number 0x04 0x1411	Source Address Calloco	Superframe specification 80 50 F. CAP BLE Court Assoc 15 15 15 0 1 0	GPS fields Les Permit 0 0	Beacton payboad 00 20 84 42 89 23 C0 5F CE 7C 04 FF FF FF 61	Dis Dest 1.76	Beacce Payload (MIN La r RLr_Cep Dev.Depth Cal Dati	per Decoded) Dev. Cep. East. FMIIID Cell. December 2018/FC128/F42	TROTANT [systels] (arterer 37 OF
Pada RX 12	Time (us) +29755 +6776042 28	Frame control field Type Bec Pod Ack.reg Hill_compr 309 0 0 0 0 0	tengenter number 1x11 (x1214	Address Cuttoto	Superframe specification NO BO F. GAP NLE Court Assoc 15 15 15 0 3 0	GTS fields Les Permits 0 0	Beaution payload 00 20 84 37 87 08 78 12 17 07 15 77 87 87 00	Stat Front F.Ve	Beauton Payload (MIK La r Pitr_Cap Dev. Depth 0x1 0x0	per Decoded) Dev. Cap. Kan., RAKID Cac	TR Offset (symbols) (wreterner 15 OF
Padat RX 13	Time (uk) +1639 +4080481 28	Frame control field Type Dec Phil Ack.reg 350_compr 308 0 0 0 0 0	Sequence number 0x15 (x2075	Source Address Califold	Superframe specification BO BO F.CAP BLE Cover Associ 15 15 18 1 1	GPS Relde Les Person	Pending addr Delete CallAM CallED Exec CallEDEL2E3285000E	CADOFFFC4T/FIGA	Bearon paylo	M LG PCS Sength/ 44 K35	
Puebe RE 16	*1647 Lengt +1647 103	frame control field Type Sec Ptd Ack.reg Hill_compt 3111 0 0 1 1	Sequence number Dx24 0x8127	Beat. Address Calif.20	Source LG PCS Address LG PCS DeECLS 207 EDS						
Radar RX 15	Time (uk) =8215 =4191545 20	Frame control field Type fee Pod Ack.reg Hill_compr 308 0 0 0 0 0	Bequetor Boards mandper 1x10 Date18	Source Address failtes	Superframe specification 80 80 F.CAP BLE Courd Associ 15 15 15 0 1 0	GTS fields Les Prenist 0 0	Descise payload 00 20 84 12 20 17 22 34 34 91 50 97 97 97 11	Pik_Prof F.Ve Del Del	Beacon Payload (MNK La r Pir_Cap Dev.Depth 0x1 0x0	per Decoded) Dev. Cap. Ean. HANID Cal. EanCF194AAD2170012	TX Offset (symbols) (serverser) 15 OF
Public RX 16	Firme (u4) +52003 =4545144 20	Frame control field Type Sec Phd Ack.reg 352_compr 3CH 0 0 0 0	Sequence number Dalit Dalit	Source Address Calloco	Superframe specification 80 SO F. CAP BLE Courd Associ 15 15 15 0 1 1	GPS fields Sen Primits 0 0	Beaccon payload 00 20 54 54 51 57 59 CL 12 74 5C CB 77 FT FT 51	Star Prof. P.Ve	Beacon Payload (MINK La r Biz_Cap Dev.Depth 0x1 0x0	per Decoded) Dev. Cap. East. Statico Cacl. DarDocretocaescrost	TR OTHER [ryshrils] CHITTEET 114 OF
Public RX 17	Time (us) Lengt	Frame control field Type Sec Pod Ack.reg Hill_compr CHD 0 0 1	Sequence Dest. number PEB 0x20 Ox6014	Deat. Address Cattoos	Source Source PES Address (Lt. court Pt	Association required	100 PCS			



IoT CONTROLLER COMMUNICATIONS DEBUGGER

Option 8 on the IoT controller invokes the Comm Debugger, which can be used to examine AP to IoT Controller communications.

login as: admin admin@10.34.7.72's password: Last login: Thu Sep 27 11:07:42 2018 from 10.34.2.152
vRioT Controller Main Menu
1 - Get Network Info 2 - Get Application Info 3 - NTP Setting 4 - Restart Application 5 - Rebot System 6 - Reset System 7 - Command Prompt 8 - Comm Debugger x - Log Off Enter Choice: 8 Gateway MAC:18:48:DD:06:A8:C0 Exclude topic/gateway/events Press Cit'+c to get Main menu.
<pre>sudo password for root: Client initiated successfully. Initiating broker connection. Connection with broker successful. Subscribed to Topic: (qos: 0, 'topic': 'controller/#) controller/gateway/commands ("commands": "DEVICE_JOIN", 'value": "ON")], "gateway_euid": "18:48:0D:06:AB:C0"} gateway/evice/authentication ("gateway_euid": 18:48:0D:06:AB:C0", 'network_id":0, 'device_euid": "00:17:7A:01:06:06:8E:C4", 'device_name": "AA_LOCK", "device_serial": "111111111", "connection_state": 1} gateway/evice/authentication ("gateway_euid": 18:48:0D:06:AB:C0", 'network_id":0, 'device_euid": "00:17:7A:01:06:06:8D:FC", 'device_name": "AA_LOCK", "device_serial": "111111111", "connection_state": 1} gateway/euid": 18:48:0D:06:AB:C0", 'network_id":0, 'device_euid": "00:17:7A:01:06:06:8D:FC", "device_name": "AA_LOCK", "device_serial": "11111111", "connection_state": 1} gateway/euid": 18:48:0D:06:AB:C0", 'network_id":0, 'device_euid": "00:17:7A:01:06:06:8D:FC", "device_name": "AA_LOCK", "device_serial": "11111111", "connection_state": 1} commands: ["device_euid": "00:17:7A:01:06:06:8D:FC", "command": "PERMITTED"]}, 'gateway_euid": "18:48:0D:06:AB:C0"} controller/gateway/commands ("commands": ["device_euid": "00:17:7A:01:06:06:8D:FC", "command": "PERMITTED"]}, 'gateway_euid": "18:48:0D:06:AB:C0"} gateway/skd, data ("gateway_euid": "18:48:D0:06:AB:C0", "network_id": 1629", "vendor_code": "0xF1F2, 0", "device_euid": "00:17:7A:01:06:06:8E:04", "device_type": "AA_LOCK", "function_id": "0x01", "attributes": ["attribute": "AA_TUNNEL_DATA", "value": "6e e6 f5 cc fb f0 72 b9 d8 31 dc e4 d2 85 0c 41 05 62?]]) gateway.euid:: "18:48:DD:06:AB:C0", "network_id": "1629", "vendor_code": "0xF1F2, 0", "device_euid:: "00:17:7A:01:06:06:8D:C0", "network_id": "1629", "vendor_co</pre>

VISIONLINE EVENT LOGGER

The Event Log on the Visionline Server can be examined to analyze events as seen by the server.

Registration Nu.	Command	Bhriswers	Last Transmission	Succeeded	Cancelled	Buffered	Constant and some	
514	Set time	89	9/27/2018 4:07	No	No	Yes		
13	Ping	1	9/26/2018 4:03	No	No	Yes		
12	Ping	0	9/25/2018 4:03	No	Yes	Yes		
11	Ping	0	9/24/2018 4 03	No	Yes	Yes		
10	Ping	0	9/23/2018 4:03	No	Yes	Yes		
09	Ping	0	9/22/2018 4 03	No	Yes	Yes		
16	Ping	0	9/21/2018 4:03	No	Ver	Ver		
17	Ping	0	9/20/2018 4 03	No	Yes	Ves		
6	Ping	0	3/19/2018 4:03	No	Ves	Yes		
15	Ping	0	9/18/2018 4:02	No	Ver	Ver		
04	Ping	0	9/17/2018 4 02	No	Yes	Yes		
13	Ping	0	9/16/2018 4:02	No	Yes	Ves		
8-10-	Dina	0	9./1E /2010 4.00		Ver	Ves		
12	ring	U	3713771184117	Nen				
02	Ping	0	9/14/2018 4:02	No	Vet	Ver		
902 901 Room Event L	Ping Pinn htt	0	9/14/2018 4:02 9/13/2018 4:02 9/13/2018 4:02	No No Nn	Yes Yes	Yes Yes Yes		
12 11 Room Event L som	Ping Pinn ist Registration Nu.	0 n Time	9/14/2018 4:02 9/13/2018 4:02 9/13/2018 4:02	No No	Yes Yes	Yes Yes Yes	User Group	SeqN
02 01 Room Event L som 2	Ping Pinn ist Registration Nu 0	0 0 1 1 1 1 1 1 2/27/2018 102	9/13/2018 4 02 9/13/2018 4 02 9/13/2018 4 02 Event	No No No	Yes Yes	Yes Yes Card Name Docr Unit Internal	User Group	SegNi 14
A2 21 Room Event L 20 2	Prog Prive Ist Registration Nu 0	0 0 1 1 1 1 1 1 1 1 1 1 1 1 1	S/15/2016 4:02 S/13/2018 4:02 S/13/2018 4:02 Event The door is left opp The door is left opp	No No Nn m too long (316) (313)	Yes Yes Yes	Yes Yes Card Name Door Unit Internal Door Unit Internal	User Group n/a n/a	SegN 14 8
20 71 Room Event L 20 0 0 0	Ping Pinn Registration Nu. 0 0	0 0 1 1 1 1 1 1 1 1 1 1 1 1 1	S/13/2018 4 02 S/13/2018 4 02 S/13/2018 4 02 Event The door is left op The door is opened The door is opened	No No Nn en too long (316) (313) d hom the inside (3	Yes Yes Yes 17]	Yes Yes Card Name Door Unit Internal Door Unit Internal Door Unit Internal	User Group n/a n/a	SeqN 14 8 7
00 00 Room Event L 00 0 0 0	ring Pring Ist Registration Nu 0 0 0 0	0 0 1 1 1 1 1 1 1 1 1 1 1 1 1	S/14/2018 4 02 S/13/2018 4 02 S/13/2018 4 02 Event The door is left ope The door is closed The door is opened The door is closed	No No No In too long (316) (313) d hom the inside (3 (313)	Yes Yes Yes 17)	Yes Yes Card Name Door Unit Internal Door Unit Internal Door Unit Internal	User Group n/a n/a n/a	SeqN 14 8 7 6
22 27 28 20 20 20 20 20 20 20 20 20 20 20 20 20	Prog Pron ist Registration Nu. 0 0 0 0 0	0 0 1 3/27/2018 102. 3/27/2018 102. 3/27/2018 102. 3/27/2018 102.	Briszons 402 9/14/2018 402 9/13/2018 4 (02 Event The door is left ope The door is closed The door is closed The door is closed The door is closed The door is closed	No No No en too kong (316) (313) d hom the inside (3 (313) (313)	Yes Yes Yes 17)	Yes Yes Card Name Door Unit Internal Door Unit Internal Door Unit Internal Door Unit Internal	User Group n/a n/a n/a n/a	SegN 14 8 7 6 5
00 00 00 00 00 00 00 00 00 00	Ping Pinn Registration Nu. 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 1 9/27/2018 102. 9/27/2018 102. 9/27/2018 102. 9/27/2018 102. 9/27/2018 102.	Event Event The door is left ope The door is left ope The door is closed The door is openet The door is openet The door is openet Guest Cad accept	No No No (313) (313) (313) (313) (313) (313) (312) to (312) to (312) to (312) to (312)	Yes Yes 17)	Yes Yes Card Name Door Unit Internal Door Unit Internal Door Unit Internal Door Unit Internal Guest (MC)	User Group rv/a rv/a rv/a rv/a rv/a Guest	SeqN 14 8 7 6 5 4
Room Event L som 2 0 0 0 0 7	Ping Pinn Ist Registration Nu. 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 1 3/27/2018 102 3/27/2018 102 3/27/2018 102 3/27/2018 102 3/27/2018 102 3/27/2018 102 3/27/2018 102	Briszons 402 9/14/2018 402 9/13/2018 410 Event The door is left ope The door is closed The door is closed	No No No (313) d from the inside (3 (313) d (312) ted (57) d (312)	Yes Yes Yes 17)	Yes Yes Card Name Door Unit Internal Door Unit Internal Door Unit Internal Door Unit Internal Door Unit Internal Guest (MC) Door Unit Internal	User Group n/a n/a n/a n/a Guest n/a	SeqN 14 8 7 6 5 4 0
22 71 100 800m Event L 90 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9	Ping Pinn ist Registration Nu. 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 1 9/27/2018 102 9/27/2018 102 9/27/2018 102 9/27/2018 102 9/27/2018 102 9/27/2018 102 9/27/2018 102 9/27/2018 102	Event Event The door is left ope The door is left ope The door is opened Substance Staft card accept The door is opened Substance Staft card accept	No No Nn in too long (316) (313) d hom the inside (3 (313) d (312) ted (57) d (312) d (512) d (512)	Yes Yes 77	Ves Yes Card Name Door Unit Internal Door Unit Internal Door Unit Internal Door Unit Internal Guest (MC) Door Unit Internal Statt (SC)	User Group n/a n/a n/a n/a Guest n/a ENGINEERING	SeqN 14 8 7 6 5 4 0 15
Room Event L son 2 0 0 0 7 7 1	Ping Ping Registration Nu. 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 1 1 Time 9/27/2018 102. 9/27/2018 102. 9/27/2018 102. 9/27/2018 102. 9/27/2018 102. 9/27/2018 102. 9/27/2018 102. 9/27/2018 102. 9/27/2018 102.	Event Event Event The door is left op The door is left op The door is closed The door is openet The door is openet Guett Cad accept The door is openet Suett Cad accept The door is openet Suett Cad accept The door is openet The door is openet Suett Cad accept The door is openet Staff cad accept The door is openet	No No No in too long (316) (313) d from the inside (3 (312) d (312) d (312) d (312) d (312) d (312) d (313)	1465 Yes Yes 17)	Ves Yes Card Name Door Unit Internal Door Unit Internal Door Unit Internal Door Unit Internal Guest (MC) Door Unit Internal Statt (SC) Door Unit Internal	User Group n/a n/a n/a n/a Guest n/a ENGINEERING n/a	SegN 14 8 7 6 5 4 0 15 9
122 01 2000 Event L 2000 2 0 0 0 0 7 7 7 1 1	Ping Ping Registration Nu. 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 1 9/27/2018 10.2 9/27/2018 10.2 9/27/2018 10.2 9/27/2018 10.2 9/27/2018 10.2 9/27/2018 10.2 9/27/2018 10.2 9/27/2018 10.2 9/27/2018 10.2	ST 13/2018 4 (2) ST 14/2018 4 (2) ST 13/2018 4 (2)	No No No (313) (313) (313) (313) (313) (4(312) (4(312) (4(312) (4(312))) (4	Yes Yes Yes 17]	Card Name Card Name Cord Name Door Unit Internal Door Unit Internal Door Unit Internal Door Unit Internal Guest (MC) Door Unit Internal Guest (MC) Door Unit Internal Statt (SC) Door Unit Internal Door Un	User Group n/a n/a n/a n/a Guest n/a ENGINEERING n/a	Section 14 8 7 6 5 4 0 15 9 8
02 01 00 00 02 00 00 00 00 00 01 11 10 00 00	Ping Ping Registration Nu. 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 0 1 9/27/2018 102. 9/27/2018 102. 9/27/2018 102. 9/27/2018 102. 9/27/2018 102. 9/27/2018 102. 9/27/2018 102. 9/27/2018 102. 9/27/2018 102. 9/27/2018 102.	Event Event Event Event The door is left ope The door is left ope The door is opened The door is closed The door is closed	No No No 1000 long [316] [313] (313] (313] (313) (312) (313) (313) d lon the inside [3] (313)	17) 17)	Ves Yes Card Name Door Unit Internal Door Unit Internal Door Unit Internal Door Unit Internal Door Unit Internal Guest (MC) Door Unit Internal Statt (SC) Door Unit Internal Door Unit Internal Door Unit Internal Door Unit Internal Door Unit Internal	User Group n/a n/a n/a n/a Guest n/a ENGINE ERING n/a n/a n/a	5eqN 14 8 7 6 5 4 0 15 9 8 3



About Ruckus Networks

Ruckus Networks enables organizations of all sizes to deliver great connectivity experiences. Ruckus delivers secure access networks to delight users while easing the IT burden, affordably. Organizations turn to Ruckus to make their networks simpler to manage and to better meet their users' expectations. For more information, visit www.ruckuswireless.com.

© ARRIS Enterprises LLC. All rights reserved. The Ruckus, Ruckus Wireless, Ruckus logo, Big Dog design, BeamFlex, ChannelFly, Xclaim, ZoneFlex and OPENG trademarks are registered in the U.S. and other countries. Ruckus Networks, MediaFlex, FlexMaster, ZoneDirector, SpeedFlex, SmartCast, SmartCell, and Dynamic PSK are Ruckus trademarks worldwide. Other names and brands mentioned in this document or website may be claimed as the property of others.

Ruckus Networks | 350 West | ava Drive | Sunnyvale, CA 94089 USA | T: (650) 265-4200 | F: (408) 738-2065 ruckuswireless.com

About ARRIS

ARRIS International plc (NASDAQ: ARRS) is powering a smart, connected world. The company's leading hardware, software and services transform the way that people and businesses stay informed, entertained and connected. For more information, visit www.arris.com.

For the latest ARRIS news:

Check out our blog: ARRIS EVERYWHERE

Follow us on Twitter: @ARRIS

© 2019 ARRIS Enterprises LLC. All rights reserved. ARRIS, the ARRIS logo, Ruckus, Ruckus Wireless, the Ruckus logo, and the Big Dog design are trademarks of ARRIS International plc and/or its affiliates. All other trademarks are the property of their respective owners.