CONFIGURATION GUIDE



# **RUCKUS IoT Controller** Configuration Guide, 1.7-5.2.1-p2

Supporting IoT Controller Release 1.7-5.2.1-p2

# **Copyright, Trademark and Proprietary Rights Information**

© 2020 CommScope, Inc. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change.

### **Export Restrictions**

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

### Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMSCOPE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

### **Limitation of Liability**

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

### **Trademarks**

ARRIS, the ARRIS logo, COMMSCOPE, RUCKUS, RUCKUS WIRELESS, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

# Contents

Preface	5
Document Conventions	5
Notes, Cautions, and Safety Warnings	
Command Syntax Conventions	
Document Feedback	
RUCKUS Product Documentation Resources	
Online Training Resources	6
Contacting RUCKUS Customer Services and Support	7
What Support Do I Need?	7
Open a Case	
Self-Service Resources	7
About This Guide	9
Introduction to RUCKUS IoT Controller	9
What's New in This Document	9
Getting Started	11
Before You Begin	
Supported Web Browsers	
Logging In to RUCKUS IoT Controller	
Getting to Know the Dashboard	16
Configuring N+1	19
Configuring Static Addresses for Primary and Secondary Controller	
Configuring the N+1 Feature	
Disabling N+1.	
Disabling N+1	
Disabling N+1 Managing IoT Controller System Configuration	
Disabling N+1 Managing IoT Controller System Configuration Managing Services	
Disabling N+1 Managing IoT Controller System Configuration Managing Services Enabling the SmartThings Service	<b>33</b> <b>35</b> 35 36 46
Disabling N+1 Managing IoT Controller System Configuration Managing Services Enabling the SmartThings Service Activating and Editing the Plugins	<b>33</b> <b>35</b> 35 36 46 46
Disabling N+1 Managing IoT Controller System Configuration Managing Services Enabling the SmartThings Service Activating and Editing the Plugins Activating and Editing the Kontakt.io Beacons Plugin	<b>33</b> <b>35</b> 35 36 46 46 46 49
Disabling N+1 Managing IoT Controller System Configuration Managing Services Enabling the SmartThings Service Activating and Editing the Plugins Activating and Editing the Kontakt.io Beacons Plugin Activating and Editing the Assa Abloy Plugin	<b>33</b> <b>35</b> 35 36 46 46 49 50
Disabling N+1 Managing IoT Controller System Configuration Managing Services Enabling the SmartThings Service Activating and Editing the Plugins Activating and Editing the Kontakt.io Beacons Plugin Activating and Editing the Assa Abloy Plugin Activating and Editing the Eddystone Plugin	<b>33</b> <b>35</b> 35 36 46 46 46 49 50 50
Disabling N+1 Managing IoT Controller System Configuration Managing Services Enabling the SmartThings Service Activating and Editing the Plugins Activating and Editing the Kontakt.io Beacons Plugin Activating and Editing the Kontakt.io Beacons Plugin Activating and Editing the Assa Abloy Plugin Activating and Editing the Eddystone Plugin Activating and Editing the iBeacon Plugin	<b>33</b> <b>35</b> 35 36 46 46 46 49 50 50 54 57
Disabling N+1 Managing IoT Controller System Configuration Managing Services Enabling the SmartThings Service Activating and Editing the Plugins Activating and Editing the Kontakt.io Beacons Plugin Activating and Editing the Kontakt.io Beacons Plugin Activating and Editing the Assa Abloy Plugin Activating and Editing the Eddystone Plugin Activating and Editing the Eddystone Plugin Activating and Editing the iBeacon Plugin Activating and Editing the Beacon as a Service Plugin (iBeacon, Eddystone and Custom) Activating and Editing the Beacon as a Service Plugin (React Mobile)	<b>33</b> <b>35</b> 35 36 46 46 46 49 50 50 54 57
Disabling N+1 Managing IoT Controller System Configuration Managing Services Enabling the SmartThings Service Activating and Editing the Plugins Activating and Editing the Kontakt.io Beacons Plugin Activating and Editing the Kontakt.io Beacons Plugin Activating and Editing the Assa Abloy Plugin Activating and Editing the Eddystone Plugin Activating and Editing the Eddystone Plugin Activating and Editing the Beacon Plugin Activating and Editing the Beacon Plugin Activating and Editing the Beacon as a Service Plugin (iBeacon, Eddystone and Custom)	<b>33</b> <b>35</b> <b>35</b> <b>36</b> <b>46</b> <b>46</b> <b>46</b> <b>49</b> <b>50</b> <b>54</b> <b>57</b> <b>62</b> <b>63</b>
Disabling N+1 Managing IoT Controller System Configuration Managing Services Enabling the SmartThings Service Activating and Editing the Plugins Activating and Editing the Kontakt.io Beacons Plugin Activating and Editing the Kontakt.io Beacons Plugin Activating and Editing the Assa Abloy Plugin Activating and Editing the Eddystone Plugin Activating and Editing the Eddystone Plugin Activating and Editing the Beacon Plugin Activating and Editing the Beacon as a Service Plugin (iBeacon, Eddystone and Custom) Activating and Editing the Beacon as a Service Plugin (React Mobile) Activating and Editing the BLE Scan Plugin	<b>33</b> <b>35</b> <b>35</b> <b>36</b> <b>46</b> <b>46</b> <b>46</b> <b>49</b> <b>50</b> <b>50</b> <b>54</b> <b>57</b> <b>62</b> <b>63</b> <b>66</b>
Disabling N+1 Managing IoT Controller System Configuration Managing Services Enabling the SmartThings Service Activating and Editing the Plugins Activating and Editing the Kontakt.io Beacons Plugin Activating and Editing the Kontakt.io Beacons Plugin Activating and Editing the Assa Abloy Plugin Activating and Editing the Eddystone Plugin Activating and Editing the Eddystone Plugin Activating and Editing the Beacon as a Service Plugin (iBeacon, Eddystone and Custom) Activating and Editing the Beacon as a Service Plugin (React Mobile) Activating and Editing the BLE Scan Plugin Activating and Editing the BLE Scan Plugin	<b>33</b> <b>35</b> <b>35</b> <b>36</b> <b>46</b> <b>46</b> <b>46</b> <b>49</b> <b>50</b> <b>50</b> <b>54</b> <b>57</b> <b>62</b> <b>63</b> <b>66</b> <b>68</b>
Disabling N+1 Managing IoT Controller System Configuration Managing Services Enabling the SmartThings Service Activating and Editing the Plugins Activating and Editing the Plugins Activating and Editing the Kontakt.io Beacons Plugin Activating and Editing the Assa Abloy Plugin Activating and Editing the Eddystone Plugin Activating and Editing the Eddystone Plugin Activating and Editing the Beacon Plugin Activating and Editing the Beacon as a Service Plugin (iBeacon, Eddystone and Custom) Activating and Editing the Beacon as a Service Plugin (React Mobile) Activating and Editing the BLE Scan Plugin Activating and Editing the BLE Scan Plugin Activating and Editing the Dormakaba Plugin	<b>33</b> <b>35</b> <b>35</b> <b>36</b> <b>46</b> <b>46</b> <b>49</b> <b>50</b> <b>54</b> <b>50</b> <b>54</b> <b>50</b> <b>54</b> <b>50</b> <b>54</b> <b>62</b> <b>63</b> <b>66</b> <b>68</b> <b>69</b>
Disabling N+1 Managing IoT Controller System Configuration Managing Services Enabling the SmartThings Service Activating and Editing the Plugins Activating and Editing the Kontakt.io Beacons Plugin Activating and Editing the Kontakt.io Beacons Plugin Activating and Editing the Assa Abloy Plugin Activating and Editing the Eddystone Plugin Activating and Editing the Eddystone Plugin Activating and Editing the Beacon Plugin Activating and Editing the Beacon as a Service Plugin (iBeacon, Eddystone and Custom) Activating and Editing the Beacon as a Service Plugin (React Mobile). Activating and Editing the BLE Scan Plugin Activating and Editing the BLE Scan Plugin Activating and Editing the Controller Data Stream Plugin Activating and Editing the Dormakaba Plugin Activating and Editing the Telkonet Plugin	33 35 35 36 46 46 49 50 50 54 54 57 62 63 63 66 68 69 72
Disabling N+1 Managing IoT Controller System Configuration Managing Services Enabling the SmartThings Service Activating and Editing the Plugins Activating and Editing the Vontakt.io Beacons Plugin Activating and Editing the Kontakt.io Beacons Plugin Activating and Editing the Assa Abloy Plugin Activating and Editing the Eddystone Plugin Activating and Editing the Eddystone Plugin Activating and Editing the Beacon Plugin Activating and Editing the Beacon as a Service Plugin (iBeacon, Eddystone and Custom) Activating and Editing the Beacon as a Service Plugin (React Mobile) Activating and Editing the BLE Scan Plugin Activating and Editing the BLE Scan Plugin Activating and Editing the Dormakaba Plugin Activating and Editing the Telkonet Plugin Activating and Editing the Telkonet Plugin Activating and Editing the Telkonet Plugin Activating and Editing the Soter Plugin	33 35 35 36 46 46 46 49 50 50 54 57 62 63 63 66 63 63 67 72 74
Disabling N+1 Managing IoT Controller System Configuration Managing Services Enabling the SmartThings Service Activating and Editing the Plugins Activating and Editing the Kontakt.io Beacons Plugin Activating and Editing the Kontakt.io Beacons Plugin Activating and Editing the Assa Abloy Plugin Activating and Editing the Eddystone Plugin Activating and Editing the Eddystone Plugin Activating and Editing the Beacon Plugin Activating and Editing the Beacon as a Service Plugin (iBeacon, Eddystone and Custom) Activating and Editing the Beacon as a Service Plugin (React Mobile) Activating and Editing the BLE Scan Plugin Activating and Editing the BLE Scan Plugin Activating and Editing the Controller Data Stream Plugin Activating and Editing the Dormakaba Plugin Activating and Editing the Telkonet Plugin Activating and Editing the Soter Plugin Changing the Password	33 35 35 36 46 46 46 49 50 50 50 54 50 50 54 50 50 54 50 50 54 50 50 54 50 50 54 57 62 63 66 66 68 69 72 74 74
Disabling N+1 Managing IoT Controller System Configuration Managing Services. Enabling the SmartThings Service. Activating and Editing the Plugins. Activating and Editing the Kontakt.io Beacons Plugin. Activating and Editing the Kontakt.io Beacons Plugin. Activating and Editing the Assa Abloy Plugin. Activating and Editing the Eddystone Plugin. Activating and Editing the Beacon Plugin. Activating and Editing the Beacon Plugin. Activating and Editing the Beacon as a Service Plugin (iBeacon, Eddystone and Custom). Activating and Editing the Beacon as a Service Plugin (React Mobile). Activating and Editing the BLE Scan Plugin. Activating and Editing the BLE Scan Plugin. Activating and Editing the Dormakaba Plugin. Activating and Editing the Telkonet Plugin. Activating and Editing the Telkonet Plugin. Activating and Editing the Soter Plugin. Changing the Password. Configuring Virtual Machines.	33 35 35 36 46 46 46 49 50 50 50 54 50 50 54 50 50 54 50 50 54 50 50 54 50 50 54 50 50 54 50 50 54 50 50 54 57 62 63 66 66 67 72 74 74 75
Disabling N+1 Managing IoT Controller System Configuration Managing Services Enabling the SmartThings Service Activating and Editing the Plugins Activating and Editing the Kontakt.io Beacons Plugin Activating and Editing the Kontakt.io Beacons Plugin Activating and Editing the Kontakt.io Beacons Plugin Activating and Editing the Eddystone Plugin Activating and Editing the Eddystone Plugin Activating and Editing the Beacon Plugin Activating and Editing the Beacon Plugin Activating and Editing the Beacon as a Service Plugin (iBeacon, Eddystone and Custom) Activating and Editing the Beacon as a Service Plugin (React Mobile) Activating and Editing the BLE Scan Plugin Activating and Editing the Ontroller Data Stream Plugin Activating and Editing the Telkonet Plugin Activating and Editing the Telkonet Plugin Activating and Editing the Soter Plugin Activating and Editing the Soter Plugin Changing the Password Configuring Virtual Machines Uploading Versions and Patches	33 35 35 36 46 46 49 50 50 54 50 54 50 54 50 54 50 54 50 54 50 54 50 54 50 54 57 62 63 63 66 63 64 72 72 74 74 74 75 55

Uploading the RUCKUS for Controller License	Backing up Rules	
Rebooting RUCKUS IoT Controller.         Managing IoT Access Points.         IoT AP Overview.         DHCP Option 43.         RUCKUS Command Line Interface.         USB Power.         Adding an IoT AP.         Editing an IoT AP.         Single IoT Access Point Mode.         Adding Tags to an AP.         Approval O IoT APs.         Exporting IoT APs to CSV.         Managing Devices.         Devices Overview.         Devices Overview.         Devices Overview.         Devices Overview.         Devices Overview.         Discovering Dormakaba Lock.         Blocking an Unblocking Dormakaba Lock.         Blocking the Key Remotely.         Unblocking the Key Remotely.         Rules Engine         Rules Engine Overview.         Configuring Rules.         Configuring I Nota Noveriew. <th>Uploading the RUCKUS IOT Controller License</th> <th></th>	Uploading the RUCKUS IOT Controller License	
Resetting RUCKUS IoT Controller.         Managing IoT Access Points.         IoT AP Overview.         DHCP Option 43.         RUCKUS Command Line Interface.         USB Power.         Adding an IoT AP.         Editing an IoT AP.         Single IoT Access Point Mode.         Adding an IoT AP.         Single IoT Access Point Mode.         Adding Tags to an AP.         Approval of IoT APS.         Exporting IoT APs to CSV.         Managing Devices.         Devices Overview.         Managing Ing the Bulbs.         Managing Dormakaba Lock.         Discovering Dormakaba Lock.         Blocking the Bormakaba Lock.         Blocking the Key Remotely.         Unblocking the Key Remotely.         Rules Engine         Rules Engine Overview.         Configuring Rules.         Rules Engine Overview.         LoRaWAN         LoRaWAN Derview.         LoRaWAN Derview.         LoRaWAN Derview.         LoRaWAN Derview.         Longing In to the LoRa Network         Logging In to the LoRa Network         Logging In to the LoRa Network         Longing In CoReview.         Configuring LoRa Devices	Change the Settings	
Managing IoT Access Points	Rebooting RUCKUS IoT Controller	
IoT AP Overview.         DHCP Option 43.         RUCKUS Command Line Interface.         USB Power.         Adding an IoT AP.         Editing an IoT AP.         Editing an IoT AP.         Editing an IoT AP.         Editing an IoT AP.         Adding Tags to an AP.         Approval of IoT APs.         Exporting IoT APs.         Exporting IoT APs.         Devices.         Devices Overview.         Managing Obstantiation of the state of the st	Resetting RUCKUS IoT Controller	
DHCP Option 43 RUCKUS Command Line Interface USB Power Adding an IoT AP Editing an IoT AP Single IoT Access Point Mode Adding Tags to an AP Approval of IoT APS Exporting IoT APs to CSV <b>Managing Devices.</b> Devices Overview Devices Overview Devices Overview Devices Overview Devices Overview Devices Overview Devices Overview Discovering Dormakaba Lock Blocking and Unblocking Dormakaba Lock Blocking and Unblocking Dormakaba Lock Blocking and Unblocking Dormakaba Lock Blocking the Key Remotely Rules Engine Overview Configuring Rules Rules-Dashboard LoRaWAN LoRaWAN Overview Logging In to the LoRa Network Logging In to the LoRa Network Logging In to the LoRa Network Lorging In Bervices Configuring LoRa Devices Configuring LoRa Devices Configuring LoRa Devices Configuring LoRa Perices Configuring to Semtech LoRa Picocell Gateway as a Router in the LNS <b>Events</b>	Managing IoT Access Points	83
RUCKUS Command Line Interface	IoT AP Overview	83
USB Power Adding an IoT AP. Editing an IoT AP. Single IoT Access Point Mode. Adding Tags to an AP. Approval of IoT APs. Exporting IoT APs to CSV. Managing Devices. Devices Overview. Managing OSRAM Light Bulbs. Managing on Assa Abloy Lock. Managing the Dormakaba Lock. Discovering Dormakaba Lock. Blocking and Unblocking Dormakaba Lock. Blocking the Key Remotely. Unblocking the Key Remotely. Rules Engine. Rules Engine Overview. Configuring Rules. Rules-Dashboard. LoRaWAN LoRaWAN Devriew. Logging in to the LoRa Network Logging in to the LoRa Network LoraWAN Routers. Preparing the Semtech LoRa Picocell Gateway. Configuring LoRa WAN Routers. Preparing the Semtech LoRa Picocell Gateway. Configuring Events.	DHCP Option 43	
Adding an IoT AP Editing an IoT AP		
Editing an IoT AP. Single IoT Access Point Mode. Adding Tags to an AP. Approval of IoT APs. Exporting IoT APs to CSV. Managing Devices. Devices Overview. Managing OSRAM Light Bulbs. Managing the Dormakaba Lock. Managing the Dormakaba Lock. Biocking and Unblocking Dormakaba Lock. Blocking and Unblocking Dormakaba Lock. Blocking and Unblocking Dormakaba Lock. Blocking the Key Remotely. Rules Engine. Rules Engine Overview. Configuring Rules. Rules-Dashboard. LORAWAN LORAWAN Overview. Logging In to the LoRa Network. Logging In to the LoRa Network. Logging In to the LoRa Network. LoRaWAN Routers. Preparing the Semtech LoRa Picocell Gateway Configuring LoRa Devices. Configuring LoRa Decices. Events. Viewing Events.		
Single IoT Access Point Mode	-	
Adding Tags to an AP Approval of IoT APs Exporting IoT APs to CSV Managing Devices Devices Overview Managing OSRAM Light Bulbs. Managing an Assa Abloy Lock. Managing the Dormakaba Locks. Discovering Dormakaba Lock. Blocking and Unblocking Dormakaba Lock. Blocking the Key Remotely. Unblocking the Key Remotely. Rules Engine. Rules Engine Overview. Configuring Rules. Rules-Dashboard. LoRaWAN. LoRaWAN. LoRaWAN Overview. Logging In to the LoRa Network LoRaWAN Routers. Preparing the Semtech LoRa Picocell Gateway as a Router in the LNS. Events. Viewing Events.	Editing an IoT AP	
Approval of IoT APs. Exporting IoT APs to CSV Managing Devices Devices Overview Managing OSRAM Light Bulbs Managing an Assa Abloy Lock. Managing the Dormakaba Locks Discovering Dormakaba Lock. Blocking and Unblocking Dormakaba Lock. Blocking and Unblocking Dormakaba Lock. Blocking the Key Remotely. Unblocking the Key Remotely. Rules Engine. Rules Engine Overview. Configuring Rules. Rules-Dashboard. LoRaWAN LoRaWAN Overview. Logging In to the LoRa Network LoRaWAN Doshboard. Configuring LoRa Devices Configuring LoRa Devices Configuring LoRa Devices Configuring LoRa Devices Configuring LoRa Devices Configuring LoRa Picocell Gateway. Configuring the Semtech LoRa Picocell Gateway as a Router in the LNS.		
Exporting IoT APs to CSV		
Managing Devices Devices Overview Managing OSRAM Light Bulbs Managing an Assa Abloy Lock Managing the Dormakaba Lock Biocking the Tormakaba Lock Biocking and Unblocking Dormakaba Lock Biocking the Key Remotely. Unblocking the Key Remotely. Unblocking the Key Remotely. Unblocking the Key Remotely. Rules Engine Rules Engine Overview Configuring Rules Rules-Dashboard. LORAWAN LoRaWAN Overview Logging In to the LoRa Network LoRaWAN Dashboard Configuring LoRa WAN Routers. Preparing the Semtech LoRa Picocell Gateway Configuring the Semtech LoRa Picocell Gateway as a Router in the LNS. Events	Approval of IoT APs	
Devices Overview	Exporting IoT APs to CSV	
Managing OSRAM Light Bulbs Managing an Assa Abloy Lock Managing the Dormakaba Lock Discovering Dormakaba Lock Blocking and Unblocking Dormakaba Lock Blocking the Key Remotely Unblocking the Key Remotely Rules Engine Rules Engine Overview Configuring Rules Rules-Dashboard. LoRaWAN. LoRaWAN Overview Logging In to the LoRa Network LoRaWAN Dashboard. Configuring LoRa Devices Configuring LoRa Devices Configuring LoRaWAN Routers Preparing the Semtech LoRa Picocell Gateway. Configuring the Semtech LoRa Picocell Gateway as a Router in the LNS Events	Managing Devices	
Managing an Assa Abloy Lock Managing the Dormakaba Locks Discovering Dormakaba Lock Blocking and Unblocking Dormakaba Lock Blocking the Key Remotely Unblocking the Key Remotely Rules Engine. Rules Engine Overview Configuring Rules Rules-Dashboard LoRaWAN LoRaWAN Overview Logging In to the LoRa Network LoRaWAN Derview Configuring LoRa Devices Configuring LoRa Devices Configuring LoRa Devices Configuring LoRa Picocell Gateway Configuring the Semtech LoRa Picocell Gateway as a Router in the LNS Events		
Managing the Dormakaba Lock Discovering Dormakaba Lock	••••	
Discovering Dormakaba Lock	Managing an Assa Abloy Lock	
Blocking and Unblocking Dormakaba Lock Blocking the Key Remotely Unblocking the Key Remotely Rules Engine Overview Configuring Rules Rules-Dashboard. LORAWAN LoRaWAN Overview. Logging In to the LoRa Network LORaWAN Dashboard. Configuring LoRa Devices Configuring LoRa Devices. Configuring LoRa WAN Routers Preparing the Semtech LoRa Picocell Gateway Configuring the Semtech LoRa Picocell Gateway as a Router in the LNS. Events Viewing Events.	• •	
Blocking the Key Remotely Unblocking the Key Remotely Rules Engine Overview Configuring Rules Rules-Dashboard. LORAWAN LORAWAN Overview. Logging In to the LoRa Network LORaWAN Dashboard. Configuring LoRa Devices Configuring LoRa Devices Configuring the Semtech LoRa Picocell Gateway Configuring the Semtech LoRa Picocell Gateway as a Router in the LNS. Events Viewing Events	-	
Unblocking the Key Remotely Rules Engine		
Rules Engine         Rules Engine Overview.         Configuring Rules.         Rules-Dashboard.         LoRaWAN         LoRaWAN Overview.         Logging In to the LoRa Network         LogaWAN Dashboard.         Configuring LoRa Devices         Configuring LoRa Devices         Configuring the Semtech LoRa Picocell Gateway.         Configuring the Semtech LoRa Picocell Gateway as a Router in the LNS.         Events.         Viewing Events.	Blocking the Key Remotely	
Rules Engine Overview	Unblocking the Key Remotely	
Configuring Rules Rules-Dashboard LORaWAN LORaWAN Overview Logging In to the LoRa Network Logging In to the LoRa Network Configuring LoRa Devices Configuring LoRa Devices Configuring LoRaWAN Routers Preparing the Semtech LoRa Picocell Gateway Configuring the Semtech LoRa Picocell Gateway as a Router in the LNS Events	Rules Engine	
Rules-Dashboard LORaWAN LoRaWAN Overview Logging In to the LoRa Network LoRaWAN Dashboard Configuring LoRa Devices Configuring LoRaWAN Routers Preparing the Semtech LoRa Picocell Gateway Configuring the Semtech LoRa Picocell Gateway as a Router in the LNS Events	Rules Engine Overview	
LoRaWAN LoRaWAN Overview Logging In to the LoRa Network LoRaWAN Dashboard Configuring LoRa Devices Configuring LoRaWAN Routers Preparing the Semtech LoRa Picocell Gateway Configuring the Semtech LoRa Picocell Gateway as a Router in the LNS Events	Configuring Rules	
LoRaWAN Overview Logging In to the LoRa Network LoRaWAN Dashboard Configuring LoRa Devices Configuring LoRaWAN Routers Preparing the Semtech LoRa Picocell Gateway Configuring the Semtech LoRa Picocell Gateway as a Router in the LNS Events	Rules-Dashboard	
Logging In to the LoRa Network LoRaWAN Dashboard Configuring LoRa Devices Configuring LoRaWAN Routers. Preparing the Semtech LoRa Picocell Gateway. Configuring the Semtech LoRa Picocell Gateway as a Router in the LNS. Events.	LoRaWAN	
LoRaWAN Dashboard Configuring LoRa Devices Configuring LoRaWAN Routers Preparing the Semtech LoRa Picocell Gateway Configuring the Semtech LoRa Picocell Gateway as a Router in the LNS Events Viewing Events	LoRaWAN Overview	
Configuring LoRa Devices Configuring LoRaWAN Routers Preparing the Semtech LoRa Picocell Gateway Configuring the Semtech LoRa Picocell Gateway as a Router in the LNS Events Viewing Events	Logging In to the LoRa Network	
Configuring LoRaWAN Routers Preparing the Semtech LoRa Picocell Gateway Configuring the Semtech LoRa Picocell Gateway as a Router in the LNS Events Viewing Events	LoRaWAN Dashboard	
Preparing the Semtech LoRa Picocell Gateway Configuring the Semtech LoRa Picocell Gateway as a Router in the LNS Events Viewing Events	Configuring LoRa Devices	
Configuring the Semtech LoRa Picocell Gateway as a Router in the LNS	Configuring LoRaWAN Routers	
Events Viewing Events		
Viewing Events	Configuring the Semtech LoRa Picocell Gateway as a Router in the LNS	
	Events	
Viewing SmartThings Event	Viewing Events	
	Viewing SmartThings Event	

# Preface

•	Document Conventions	5
•	Command Syntax Conventions	5
	Document Feedback	
•	RUCKUS Product Documentation Resources.	e
•	Online Training Resources	6
	Contacting RUCKUS Customer Services and Support	

### **Document Conventions**

The following table lists the text conventions that are used throughout this guide.

#### TABLE 1 Text Conventions

Convention	Description	Example
monospace	Identifies command syntax examples	<pre>device(config)# interface ethernet 1/1/6</pre>
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the <b>Start</b> menu, click <b>All Programs</b> .
italics	Publication titles	Refer to the RUCKUS Small Cell Release Notes for more information.

### Notes, Cautions, and Safety Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

#### NOTE

A NOTE provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

#### ATTENTION

An ATTENTION statement indicates some information that you must read before continuing with the current action or task.



### CAUTION

A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.



### DANGER

A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

## **Command Syntax Conventions**

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
<b>bold</b> text	Identifies command names, keywords, and command options.

#### **Preface** Document Feedback

Convention	Description
<i>italic</i> text	Identifies a variable.
[]	Syntax components displayed within square brackets are optional.
	Default responses to system prompts are enclosed in square brackets.
{x  y  z}	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x y	A vertical bar separates mutually exclusive elements.
<>	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
	Repeat the previous element, for example, member[member].
١	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

### **Document Feedback**

RUCKUS is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to RUCKUS at #Ruckus-Docs@commscope.com.

When contacting us, include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- RUCKUS SmartZone Upgrade Guide, Release 5.0
- Part number: 800-71850-001 Rev A
- Page 7

## **RUCKUS Product Documentation Resources**

Visit the RUCKUS website to locate related documentation for your product and additional RUCKUS resources.

Release Notes and other user documentation are available at https://support.ruckuswireless.com/documents. You can locate the documentation by product or perform a text search. Access to Release Notes requires an active support contract and a RUCKUS Support Portal user account. Other technical documentation content is available without logging in to the RUCKUS Support Portal.

White papers, data sheets, and other product documentation are available at https://www.ruckuswireless.com.

## **Online Training Resources**

To access a variety of online RUCKUS training modules, including free introductory courses to wireless networking essentials, site surveys, and products, visit the RUCKUS Training Portal at https://training.ruckuswireless.com.

# **Contacting RUCKUS Customer Services and Support**

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their RUCKUS products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the RUCKUS Support Portal using https://support.ruckuswireless.com and select Support.

### What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the Open a Case section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the Open a Case section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the Self-Service Resources section.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

### **Open a Case**

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at <a href="https://support.ruckuswireless.com/contact-us">https://support.ruckuswireless.com/contact-us</a> and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

### **Self-Service Resources**

The RUCKUS Support Portal at https://support.ruckuswireless.com offers a number of tools to help you to research and resolve problems with your RUCKUS products, including:

- Technical Documentation—https://support.ruckuswireless.com/documents
- Community Forums—https://forums.ruckuswireless.com/ruckuswireless/categories
- Knowledge Base Articles—https://support.ruckuswireless.com/answers
- Software Downloads and Release Notes—https://support.ruckuswireless.com/#products\_grid
- Security Bulletins—https://support.ruckuswireless.com/security

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at https://support.ruckuswireless.com/ case\_management.

# **About This Guide**

•	Introduction to RUCKUS IoT Controller	9
---	---------------------------------------	---

# **Introduction to RUCKUS IoT Controller**

This document describes the configuration required for setting up the RUCKUS IoT Controller on the network.

This guide is intended for service operators and system administrators who are responsible for managing, configuring, and troubleshooting RUCKUS devices. Consequently, it assumes a basic working knowledge of local area networks, wireless networking, and wireless devices.

#### NOTE

If release notes are shipped with your product and the information there differs from the information in this guide, follow the instructions in the release notes.

### What's New in This Document

TABLE 2 Summary of New Features in RUCKUS IoT Controller Release 1.7-5.2.1-p2

Feature	Description	Location
SmartThings Service	Information on how to connect the Smart Hub dongle to AP to enable the SmarThings service	Refer to Enabling the SmartThings Service on page 36 for more information.

# **Getting Started**

•	Before You Begin	11
•	Logging In to RUCKUS IoT Controller	. 11
•	Getting to Know the Dashboard	16

## **Before You Begin**

The RUCKUS IOT Controller must be installed on a hypervisor.

### **Supported Web Browsers**

The RUCKUS IoT Controller is primarily accessible using a web browser.

TABLE 3 Supported Web Browser Versions

Browser	Version
Google Chrome	63.0 and later
Apple Safari	60.0 and later
Mozilla Firefox	10.1.2 and later

## **Logging In to RUCKUS IoT Controller**

To manage IoT APs and devices, you must first log in to the RUCKUS IoT Controller.

1. Log in to the console of the RUCKUS IoT Controller using the username "admin" and password "admin".

2. Enter **1** in the **Enter Choice** field to get the IP address.

FIGURE 1 RUCKUS IoT Controller Main Menu

<pre>1 - Ethernet N 2 - System Det 3 - NTP Settin 4 - System Ope 5 - N+1 6 - Comm Debug x - Log Off Enter Choice:</pre>	ails g ration ger
Network info :	
IP (eth0) Gateway Hostname DNS domain FQDN DNS	: 10.174.112.79/23 : 10.174.112.1 : vriot :
Set Network(1)	or Exit(x). Select [1/x]:

3. Open a web browser, enter the IP address in the address bar, and press Enter.

The Initialization page is displayed.

FIGURE 2 Initialization Pa	age
----------------------------	-----

Click on next button to continue		
Required Services	Optional Services	
Pubsub Server	Rules Engine	
(	Track Central	
Enable SSL	Samsung SmartThings	
Pubsub Client		
Workers		
Identity and Access Manager		
Queue Service		
Database Initiallizer		
IoT Device Manager API		

The mandatory and optional services are listed on the **Initialization** page. The following services are mandatory:

- Pubsub Server
- Pubsub Client
- Workers
- Identity and Access Manager
- Queue Service
- Database Initializer
- IoT Device Manager API
- Rules Engine
- Track Central
- Samsung SmartThings

Pubsub Server works in SSL mode.

4. Enter the Hostname, Time Zone, and select the IP Configuration (DHCP or Static), and click Next to start all the services in the RUCKUS IoT Controller.

The RUCKUS IoT Controller services are sensitive to time synchronization. If the **NTP Sync** option is not available (such as in an isolated setup), you can select the **Set Time Manually** option to disable NTP sync.

FIGURE 3 Intialization Page After Accepting Services

nitialization						
lick on next button to continue						
M Configurations lostname				IP Configurations		
vriot				DHCP O	Static 🔾	
ime Zone						
America/Los_Angeles			-			
et Time Automatically using NTP 📀	Set Time Manually i	0				
NTP Address	Default : ntp.ubuntu.com	(Optional)				
						_

### NOTE

The figure shows a DHCP configuration.

5. Enter the RUCKUS IoT Controller password in the **New Password** field. Re-enter the password in the **Confirm Password** field. The password must be a least eight characters in length and contain one uppercase letter, one lowercase letter, one digit, and one special character.

#### FIGURE 4 Confirming the Password

RUCKUS IOT Controller	IOT API			1.5.0.0.19 Version 16 December 2019 4:27:28 America/Los_Angeles
Initialization				
Enter new password to continue				
Lines new pussions to continue	New Password	Enter password	Show	
	Confirm Password	Retype password	Show	
Back				Start

6. On the End-user License Agreement page, click Accept to accept the RUCKUS IoT Controller license.

### FIGURE 5 End-user License Agreement

TRUCKUS INT CO	ntroller fat APr	1.5.0.0 Ventoo 16 December 2019 4:27:49 America Lot, Angeles
Initializ	End-user License Agreement	
Enter new page	Ruckus IoT Controller (RIoT Controller) Software License	
	PLEASE READ THIS SOFTWARE LICENSE CAREFULLY. RUCKUS WIRELESS, INC. ("RUCKUS") IS WILLING TO LICENSE THE SOFTWARE TO YOU ("LICENSEE") ONLY ON THE CONDITION THAT THE LICENSE ACCEPTS ALL OF THE FOLLOWING TERMS AND CONDITIONS. IF A USER ACCEPTS THIS LICENSE, OR DOWNLOADS, USES OR INSTALLS THE SOFTWARE, AS AN EMPLOYED OF, OR AS AN AGENT OR CONTRACTOR FOR THE BENEFIT OF, A COMPANY, THAT COMPANY SHALL BE DEEMED THE LICENSEE AND THE USER REPRESENTS THAT IT HAS THE POWER AND AUTHORITY TO ACCEPT THIS AGREEMENT ON BEHALF OF THE COMPANY. BY DOWNLOADING, INSTALLISING THE SOFTWARE, LICENSEE ACKNOWLEDGES THAT IT HAS READ THIS LICENSE AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. IF LICENSEE DOES NOT AGREE TO THE TERMS AND CONDITIONS OF THIS LICENSE, RUCKUS IS UNWILLING TO LICENSE THE SOFTWARE, IN THAT EVENT, LICENSEE MAY NOT DOWNLOAD, USE OR INSTALL THE SOFTWARE AND SHALL BE GIVEN A FULL REFUND OF ANY LICENSE FEES ACTUALLY PAID FOR THE SOFTWARE.	
	1) Definitions "Device" means a single Ruckus access point on Licensee's network. "Documentation" means the published technical manuals, including any updates thereto, relating to the use of the Software made generally available by Ruckus. "Evaluation Term" means the limited period of time following Licensee's initial download of the Software during which Licensee is permitted to use the Software without placing an Order; provided, that the Evaluation Term is subject to early termination as provided in this agreement. "Software" means acopy of a machine executable version of a Ruckus software product that Ruckus makes available to Licensee for download onto equipment owned or controlled by Licensee, and any error corrections, updates or upgrades of such software product that Ruckus makes available to Licensee (or A Ruckus Channel Partner").	

# **Getting to Know the Dashboard**

The **Dashboard**, which is the first page that appears after you log in to the RUCKUS IoT Controller, offers an overall picture and status of the IoT infrastructure. The **Dashboard** shows the total number of IoT devices and IoT APs, the top IoT APs by device count, and the devices and APs by protocol.

### FIGURE 6 RUCKUS IoT Controller Dashboard

RUCKUS IOT Controller Dashboard IoT APs	IoT Devices Events Admin Rules LoRa LNS IoT A	12.3vriot-shriram-15018-QA 1.5.0.0.18 Version pj N+1 : Disabled 16 December 2019 13:59:11 () Asia/Karachi
Dashboard		Settings
Devices Last Seen Pre-Approved Greater than 1 Day 1 Hour to 1 Day 5 Minutes to 1 Hours Less than 5 Minutes	IoT AP Offline Online Unapproved	IoT APs by Device Count R510-Shriram
Device By Protocol	IoT AP By Protocol ZigBee BLE 0 1	

#### TABLE 4 Dashboard Elements

Box Name	Description	
Devices Last seen	Shows the total number of devices last seen.	
IoT APs By Device Count	Shows the total number of devices connected per Access Point.	
Total Devices	Shows the total number of devices.	
Total IoT APs	Shows the total number of Access Points.	
Total Beacons	Shows the total number of Beacons.	
Devices	Shows the status of devices that are connected to the RUCKUS IoT Controller.	
Active Plugins	Shows the plugins that are enabled.	
IOT AP	Shows the status of Access Points that are connected to the RUCKUS IoT Controller.	
IoT AP By Protocol	Shows the number of APs running by the protocol being used.	
	RUCKUS supports two protocols: BLE and Zigbee.	
Device By Protocol	Shows the total number of devices connected by the protocol being used.	
	RUCKUS supports two protocols: BLE and Zigbee.	
Total LNS Hubs	Shows the total number of LoRa Network Server hubs connected to the RUCKUS IoT Controller.	

To set up the Dashboard, click the Settings button. The Dashboard Settings menu is displayed.

#### FIGURE 7 Dashboard Settings

200 - <b>14</b> - 202		123vriot-shriram-15018-QA 1.5.0.0.18 Version
RUCKUS IOT Controller Dashboard IoT APs	IoT Devices Events Admin Rules LoRa LNS IoT AF	N+1 : Disabled 16 December 2019 13:53:30 🕐 Asia/Karachi
		Dashboard Settings
Dashboard		Configure
Devices Last Seen	IoT AP	IoT APs by Device ( Edit Dashboard
Pre-Approved     Greater than 1 Day     1 Hour to 1 Day	• Offline • Online 2 • Unapproved	Reset Widgets C
5 Minutes to 1 Hours     Less than 5 Minutes	• Unapproved	Refresh Interval 🖍
		Add Widgets
Device By Protocol	IoT AP By Protocol	Devices +
	ZigBee	Active Plugins +
BLE	BLE	Total devices +
0 2 4 6 8	0 1	Total Beacons +
		Total IoT APs
		Total LNS Hubs +
		<u> </u>

You can perform the following actions to configure the **Dashboard**.

- To edit the **Dashboard**, click **Edit Dashboard** and either move the position of the tile using the icon or delete the tile using the icon.
- To reset the widgets, click **Reset Widgets** to retrieve the widgets on the **Dashboard**.
- To reset the widget display time, click Refresh Interval to change the display time of the widgets on the Dashboard.

#### NOTE

The default interval is 30 seconds.

The options under Add Widgets allow you to add widgets to the Dashboard. Click + for Devices, Active Plugins, Total devices, Total Beacons, Total IoT APs, and Total LNS Hubs to add widgets to the Dashboard.

# **Configuring N+1**

RUCKUS IOT Controller N+1 high availability (HA) feature ensures high system availability, reliability and scalability of the controller, and also enables load balancing, backup, and failover. To configure an HA cluster, all the hosts in the cluster must have access to the same shared storage, which allows virtual machines (VMs) on a given host to fail over to another host without any downtime in the event of a failure.

Before beginning to use N+1, pay attention to the following prerequisites for configuring the primary and secondary controller:

- The primary and secondary controller must be in the same subnet and reachable.
- The primary and secondary controller must be configured with static IP addresses.
- The primary and secondary controller must be running the same version.
- The primary and secondary controller must have a synchronized date and time.
- The primary and secondary controller must have different host names.
- The secondary controller services must be started for N+1 to work.

## **Configuring Static Addresses for Primary and Secondary Controller**

The static IP addresses of the primary and secondary controller can be configured in two ways.

- 1. From the RUCKUS IoT Controller main menu, select Admin > VM Configurations.
- 2. Set the static address of the primary and secondary controller on the **Initialization** page. Refer to Logging In to RUCKUS IoT Controller on page 11.

## **Configuring the N+1 Feature**

After configuring the static IP addresses for primary and secondary controller, N+1 can be enabled by performing the following steps.

1. Log in to the console of the RUCKUS IoT Controller.

#### 2. Enter **5** in the **Enter Choice** field.

FIGURE 8 RUCKUS IoT Controller Main Menu

\* Ruckus IoT Controller Main Menu 1 - Ethernet Network 2 - System Details 3 - NTP Setting 4 - System Operation 5 - N+1 6 - Comm Debugger x - Log Off Enter Choice: 5 N+1 Status: \_\_\_\_\_ N+1 Mode : Disabled N+1 Configure(l) / Disable(2) / Exit(x) :

3. Enter **1** to continue the configuration.

FIGURE 9 Continuing the Configuration

	N+1 Mode : Di			
	Status:			
2 - S 3 - N 4 - S 5 - N 6 - C x - L	Ethernet Network System Details VTP Setting System Operation V+1 Comm Debugger Log Off r Choice: 5			
****	*****	Mai	T Controller n Menu *********	****
****	******			*****

[N+1 Configure(1) / Disable(2) / Exit(x) :1 Start Primary Controller(1) / Secondary Controller(2) / Exit(x) :

4. To configure the primary controller, enter 1 and type the IP address of the secondary controller in the Enter Secondary Controller IP field.

FIGURE 10 Configuring the Primary Controller

**************************************
MD11 MEUU ***********************************
1 - Ethernet Network 2 - System Details 3 - NTP Setting 4 - System Operation 5 - N+1 6 - Comm Debugger x - Log Off Enter Choice: 5
N+1 Status:
N+1 Mode : Disabled
N+1 Configure(1) / Disable(2) / Exit(x) :1 Start Primary Controller(1) / Secondary Controller(2) / Exit(x) :1
N+1 Configure:
To Configure N+1 ensure following requirements: ************************************

Enter Secondary Controller IP :

5. Type the preferred IP address in the Enter preferred Virtual IP field.

### NOTE

The Preferred Virtual IP should not be same as primary or secondary controller IP.

FIGURE 11 Entering the Preferred Virtual IP Address

*****			******	******	****	****
F		Controller				
	Main	Menu				
*****	******	******	******	******	****	****
1 - Ethernet Network						
2 – System Details						
3 - NTP Setting						
4 - System Operation						
5 - N+1						
6 - Comm Debugger						
x - Log Off						
N+1 Status:			-			
N+1 Mode : Disable	ed					
			-			
N+1 Configure(1) / Disable(2) / E						
Start Primary Controller(1) / Sec	condary Co	ntroller(2) /	Exit(x)	:1		
N+1 Configure:			-			
			-			
To Configure N+1 ensure following			ĸ			
* Primary Controller and Secondar	y Control	ler should be	in same	subnet	and	reachable

Primary Controller and Secondary Controller should be in same submet and reachable.
 Primary Controller and Secondary Controller should be running in same version.
 Primary Controller and Secondary Controller should have synchronized date/time.

Enter Secondary Controller IP :192.168.100.1 Enter preferred Virtual IP :192.168.100.2

6. Enter **Y** to continue with the N+1 configuration.

FIGURE 12 Completing the Primary Controller Configuration

```
Ruckus IoT Controller
                              Main Menu
1 - Ethernet Network
2 - System Details
3 - NTP Setting
4 - System Operation
5 - N+1
6 - Comm Debugger
x - Log Off
[Enter Choice: 5
         _____
N+1 Status:
       N+1 Mode : Disabled
_____
N+1 Configure(1) / Disable(2) / Exit(x) :1
[Start Primary Controller(1) / Secondary Controller(2) / Exit(x) :1
N+1 Configure:
To Configure N+1 ensure following requirements:
* Primary Controller and Secondary Controller should be in same subnet and reachable.
* Primary Controller and Secondary Controller should be configured with static ip address.
* Primary Controller and Secondary Controller should be running in same version.
* Primary Controller and Secondary Controller should have synchronized date/time.
  Enter Secondary Controller IP :10.174.113.177
  Enter preferred Virtual IP :10.174.113.180
  N+1 will stop all services & configurations in Secondary Controller. Enter Y/N to continue : y
       Configuring takes around 5-10 minutes. Please wait
       Primary Controller configuration started..
```

After configuring the primary controller, the configuration of secondary controller begins.

FIGURE 13 Continuing with the Secondary Controller Configuration

```
Ruckus IoT Controller
                                Main Menu
1 - Ethernet Network
2 - System Details
3 - NTP Setting
4 - System Operation
5 - N+1
6 - Comm Debugger
x - Log Off
[Enter Choice: 5
N+1 Status:
                            _____
       N+1 Mode : Disabled
                             _____
N+1 Configure(1) / Disable(2) / Exit(x) :1
[Start Primary Controller(1) / Secondary Controller(2) / Exit(x) :1
              _____
N+1 Configure:
To Configure N+1 ensure following requirements:
*******
* Primary Controller and Secondary Controller should be in same subnet and reachable.
* Primary Controller and Secondary Controller should be configured with static ip address.
* Primary Controller and Secondary Controller should be running in same version.
* Primary Controller and Secondary Controller should have synchronized date/time.
  Enter Secondary Controller IP :10.174.113.177
  Enter preferred Virtual IP :10.174.113.180
  N+1 will stop all services & configurations in Secondary Controller. Enter Y/N to continue : y
       Configuring takes around 5-10 minutes. Please wait
       Primary Controller configuration started..
       Secondary Controller configuration started..
```

FIGURE 14 N+1 Configuration Completed

```
Ruckus IoT Controller
                               Main Menu
1 - Ethernet Network
2 - System Details
3 - NTP Setting
4 - System Operation
5 - N+1
6 - Comm Debugger
x - Log Off
[Enter Choice: 5
            _____
N+1 Status:
      N+1 Mode : Disabled
N+1 Configure(1) / Disable(2) / Exit(x) :1
[Start Primary Controller(1) / Secondary Controller(2) / Exit(x) :1
              _____
N+1 Configure:
             _____
To Configure N+1 ensure following requirements:
* Primary Controller and Secondary Controller should be in same subnet and reachable.
* Primary Controller and Secondary Controller should be configured with static ip address.
* Primary Controller and Secondary Controller should be running in same version.
* Primary Controller and Secondary Controller should have synchronized date/time.
  Enter Secondary Controller IP :10.174.113.177
  Enter preferred Virtual IP :10.174.113.180
  N+1 will stop all services & configurations in Secondary Controller. Enter Y/N to continue : y
       Configuring takes around 5-10 minutes. Please wait
      Primary Controller configuration started..
       Secondary Controller configuration started..
      Configuring N+1 completed...
         _____
```

You have configured N+1 successfully.

7. To verify the IP addresses of the primary or active primary, and the secondary or active secondary, enter **5** in the **Enter Choice** field.

FIGURE 15 Verifying the IP Address of the Active Primary

Ruckus IoT Controller Main Menu 1 - Ethernet Network 2 - System Details 3 - NTP Setting 4 - System Operation 5 - N+1 6 - Comm Debugger x - Log Off [Enter Choice: 5 \_\_\_\_\_ N+1 Status: \_\_\_\_\_ ------N+1 Mode : Enabled Virtual IP : 10.174.113.180 : Active Primary Controller Mode Mode : Active Primary My IP : 10.174.113.173 Secondary Controller IP : 10.174.113.177 ConfigSync : Not Applicable, Controller is Active. Node Status : vriot-shriram-151020-esx138(1): normal vriot-shriram-151020-slave-es138(2): normal

N+1 Configure(1) / Disable(2) / Exit(x) :

8. To replace the secondary controller , enter **3**.

FIGURE 16 Replacing the IP Address of Secondary Controller

Ruckus IoT Controller Main Menu 1 - Ethernet Network 2 - System Details 3 - NTP Setting 4 - System Operation 5 - N+1 6 - Comm Debugger x - Log Off Enter Choice: 5 \_\_\_\_\_ N+1 Status: N+1 Mode : Enabled Virtual IP : 10.174.113.180 Mode : Active Primary Controller : 10.174.113.173 My IP Secondary Controller IP : 10.174.113.177 ConfigSync : Not Applicable, Controller is Active. Node Status : vriot-shriram-151020-esx138(1): normal vriot-shriram-151020-slave-es138(2): normal(offline)

N+1 Configure(1) / Disable(2) / Replace Secondary Controller(3) / Exit(x) :

FIGURE 17 Successful Completion of Replacing the Node

```
Ruckus IoT Controller
                             Main Menu
*******
1 - Ethernet Network
2 - System Details
3 - NTP Setting
4 - System Operation
5 - N+1
6 - Comm Debugger
x - Log Off
[Enter Choice: 5
            _____
N+1 Status:
            _____
       N+1 Mode : Enabled
Virtual IP : 10.174.113.180
       Mode : Active Primary Controller
My IP : 10.174.113.173
       Secondary Controller IP : 10.174.113.177
       ConfigSync : Not Applicable, Controller is Active.
Node Status : vriot-shriram-151020-esx138(1): normal
vriot-shriram-151020-slave-es138(2): normal(offline)
[N+1 Configure(1) / Disable(2) / Replace Secondary Controller(3) / Exit(x) :3
N+1 Replace :
          Enter Secondary Controller IP to replace:10.174.113.172
Deleted nodes
```

9. To enable Forced Fallback, enter **3** and **y** to continue the configuration.

FIGURE 18 Configuring Forced Fallback

```
Ruckus IoT Controller
                                Main Menu
1 - Ethernet Network
2 - System Details
3 - NTP Setting
4 - System Operation
5 - N+1
6 - Comm Debugger
x - Log Off
Enter Choice: 5
              _____
N+1 Status:
       N+1 Mode : Enabled
Virtual IP : 10.174.113.180
                   : Active Primary Controller
        Mode
                   : 10.174.113.173
        My IP
                                : 10.174.113.177
        Secondary Controller IP
        ConfigSync : Not Applicable, Controller is Active.
        Node Status : vriot-shriram-151020-esx138(1): normal
vriot-shriram-151020-slave-es138(2): normal(offline)
[N+1 Configure(1) / Disable(2) / Replace Secondary Controller(3) / Exit(x) :3
N+1 Replace :
Enter Secondary Controller IP to replace:10.174.113.172
Deleted nodes
       Start replacing Secondary Controller
       Secondary Controller configuration started..
Replace node taking more time to start services
Replacing node completed
```

10. To replace the primary controller, enter3.

FIGURE 19 Replacing the Primary Controller

```
Ruckus IoT Controller
                           Main Menu
1 - Ethernet Network
2 - System Details
3 - NTP Setting
4 - System Operation
5 - N+1
6 - Comm Debugger
x - Log Off
[Enter Choice: 5
          N+1 Status:
          _____
                           _____
      N+1 Mode : Enabled
Virtual IP : 10.174.113.180
      Mode : Active Secondary Controller
My IP : 10.174.113.172
      Primary Controller IP : ["10.174.113.173"]
      ConfigSync : Not Applicable, Controller is Active.
      Node Status : vriot-shriram-151020-es15-slave2(2): normal
vriot-shriram-151020-esx138(1): normal(offline)
```

N+1 Configure(1) / Disable(2) / Replace Primary Controller(3) / Exit(x) :

11. Enter the IP address of the primary controller.

FIGURE 20 Continuing with Replacing the Primary Controller

Ruckus IoT Controller Main Menu 1 - Ethernet Network 2 - System Details 3 - NTP Setting 4 - System Operation 5 - N+1 6 - Comm Debugger x - Log Off Enter Choice: 5 N+1 Status: N+1 Mode : Enabled Virtual IP : 10.174.113.180 : Active Secondary Controller Mode : 10.174.113.172 My IP Primary Controller IP : ["10.174.113.173"] ConfigSync : Not Applicable, Controller is Active. Node Status : vriot-shriram-151020-es15-slave2(2): normal vriot-shriram-151020-esx138(1): normal(offline) [N+1 Configure(1) / Disable(2) / Replace Primary Controller(3) / Exit(x) :3 \_\_\_\_\_ N+1 Replace : \_\_\_\_\_ Enter Primary Controller IP to replace:10.174.113.177

Replacing the primary controller has been successfully completed.

FIGURE 21 Completion of Replacing the Primary Controller

```
Ruckus IoT Controller
                              Main Menu
1 - Ethernet Network
2 - System Details
3 - NTP Setting
4 - System Operation
5 - N+1
6 - Comm Debugger
x - Log Off
[Enter Choice: 5
         _____
N+1 Status:
           _____
                          _____
       N+1 Mode : Enabled
Virtual IP : 10.174.113.180
              : Active Secondary Controller
: 10.174.113.172
       Mode
       My IP
       Primary Controller IP : ["10.174.113.173"]
       ConfigSync : Not Applicable, Controller is Active.
Node Status : vriot-shriram-151020-es15-slave2(2): normal
vriot-shriram-151020-esx138(1): normal(offline)
[N+1 Configure(1) / Disable(2) / Replace Primary Controller(3) / Exit(x) :3
N+1 Replace :
Enter Primary Controller IP to replace:10.174.113.177
      Error: N+1 is already enabled!
Deleted nodes
      Start replacing master
      Secondary Controller configuration started..
Replace node taking more time to start services
Replacing node completed
                     _____
```

# **Disabling N+1**

Complete the following steps to disable N+1 configuration.

- 1. Log in to the console of the Primary controller IP.
- 2. Enter 5 in the Enter Choice field.

FIGURE 22 Disabling the N+1 Configuration

```
Ruckus IoT Controller
                             Main Menu
1 - Ethernet Network
2 - System Details
3 - NTP Setting
4 - System Operation
5 - N+1
6 - Comm Debugger
x - Log Off
Enter Choice: 5
        _____
N+1 Status:
       N+1 Mode : Enabled
Virtual IP : 10.174.113.180
                 : Active Primary Controller
       Mode
                 : 10.174.113.173
       My IP
       Secondary Controller IP
                              : 10.174.113.172
       ConfigSync : Not Applicable, Controller is Active.
       Node Status
                : vriot-shriram-151020-es15-slave1(2): normal
vriot-shriram-151020-esx138(1): normal
[N+1 Configure(1) / Disable(2) / Exit(x) :2
N+1 Disable :
       Secondary Controller 10.174.113.172 will be reset.
      Disable N+1 completed...
```

3. Enter **2** to disable the N+1 configuration.

#### NOTE

After the N+1 configuration is disabled from the active primary controller, the secondary controller resets automatically.

# **Managing IoT Controller System Configuration**

•	Managing Services	35
•	Activating and Editing the Plugins	
•		
•	Configuring Virtual Machines	
•	Uploading Versions and Patches	
•	Backing Up Files	
•	Backing up Rules	
•	Uploading the RUCKUS IoT Controller License	
•	Change the Settings	
•	Rebooting RUCKUS IoT Controller	
•	Resetting RUCKUS IoT Controller	

### **Managing Services**

The administrator can restart or manage the mandatory and optional services.

Complete the following steps to restart or manage the services.

- 1. From the main menu, click Admin.
- 2. In the left navigation pane, click Services.

#### FIGURE 23 Services

### FIGURE 24 Maging Services Page

Admin				
				(Diagnostics) (2
Services	Rules Engine	Stopped	(Start)	
Plugins	PubSub Server	Running	( View logs	
Account	Storage System	Running	( View logs	
VM Configurations	Queue Service	Running (SysManaged)	(View logs)	
Versions & Patches	loT Device Manager	Running	( View logs )	
	PubSub Client	Running	( View logs )	
DB Backup	Workers	Running	View logs	
Rules Backup	Identity and Access Manager	Running	( View logs	
License	Database Initializer	Completed	Start	
Settings	LoKa Network Server	Stopped	Start	
Reset & Reboot	Samsung SmartThings	Stopped	Start	

The currently running services and their details are displayed.

3. Select a service to edit, restart, or view logs.

### **Enabling the SmartThings Service**

You can connect Samsung Smart hub dongle through USB port in RUCKUS AP. Samsung Smart hub dongle has two radios Zigbee and Z-wave. Samsung SmartThings Mobile app will display the configurations, status, info, device list and device status of the Smart hub.

You must perform the following steps to enable Samsung SmartThings service.

1. Click Start to activate the service.

#### NOTE

By default, the SmartThings service is disabled.

#### FIGURE 25 Starting the SmartThings Service

Admin			
			Diagnostics 3
Services	Rules Engine	Stopped	(Start)
Plugins	PubSub Server	Running	(View Logs)
Account	Storage System	Running	(View logs)
VM Configurations	Queue Service	Running (SysManaged)	(View logs)
Versions & Patches	IoT Device Manager	Running	( View logs
DB Backup	PubSub Client	Running	( View logs
Rules Backup	Workers	Running	(View logs)
	Identity and Access Manager	Running	(View logs)
License	Database Initializer	Completed	Start
Settings	LoRa Network Server	Stopped	(Start)
Reset & Reboot	Samsung SmartThings	Running	(View logs) (Stop)

2. Press and hold the reset button for 10 seconds after ST Upgrade Success event is received in the controller Events page.

FIGURE 26 SmartThing Device



### NOTE

To know more about Upgrade event refer to Viewing SmartThings Event on page 124 page.

3. Download SmartThings application and enter the login credentials.

### Managing IoT Controller System Configuration

Managing Services

4. Connect your mobile and AP in the same network or connect the mobile to the SSID of the AP.

FIGURE 27 SmartThings User Interface

My home		
<b>_0</b>	+	
Study >		
Living room >		
📑 The W	eather Ch 4:50 u	

5. After connecting the device to WiFi, a popup will appear, click **ADD Now**.

FIGURE 28 Connecting to WiFi

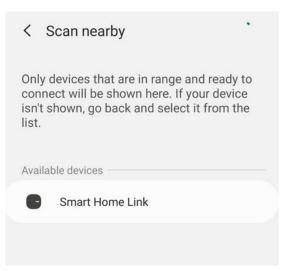
SmartThing	js Hub	) is
SmartThings Lin	ık (0132)	
6		
0.025	•	
- and		
A new device has be Add this device to S		s?
DON'T ADD	LATER	ADD NOW
4	The \ O	Neather Channel

- 6. If the popup fails to appears, perform the following steps.
  - a) Click Devices and select Scan nearby . After few seconds you will get Smart Home Link under available devices.

FIGURE 29 Selecting a Device

< Ac	dd	
What d	o you want to add to this locat	ion?
	Device	
E.	Room	
Q	Voice assistant	0
۲	Scene	
0	Automation	
=	SmartApp	0
-	Member	

FIGURE 30 Scanning the device

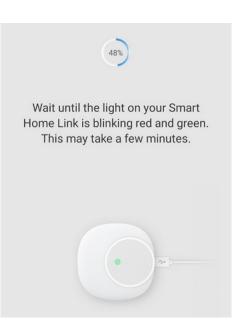


- b) Click the Smart Home Link to continue further.
- c) Select the Location and the Room and wait until the completion is 100 percent.

FIGURE 31 Selecting Location and Room for Hub

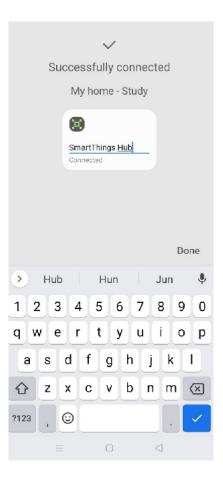
$\overline{\cdots}$	
Select a location and room for Hub.	your
Location	
My home	•
Room	
Study	-

FIGURE 32 Waiting for Completion



d) After connecting successfully, rename your hub as shown below. The Hub name will apear on the Home page.

FIGURE 33 Renaming the Hub Name



### FIGURE 34 Hub Name on the Home page



Managing IoT Controller System Configuration Managing Services

7. Add SmartThings Hub to the APP.

FIGURE 35 Locating the SmartThings Hub

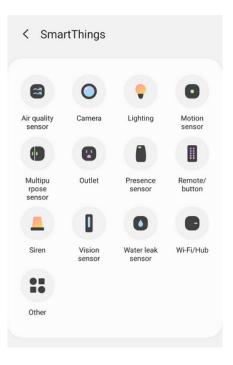
< Add	device		Q
الم الم Scan QF	न १ २ code		nearby
By dev	vice type	By bra	ind
Featured br	rands		
SAMSUNG	SmartThings		
All brands			
ACTOVADE	ADF	ERIA	Acotec Associate for homes
ACTIVAGE	ADF Devices	AduroSmart ERIA	Aeotec
	Ajax Online	arlo	E
AirEx Techno logies	Ajax Online Ltd	Arlo	August Home
AURORA'	6		AXIS

8. Select + icon in the APP and go to devices page to add the device.

### NOTE

Samsung SmartThings hub supports only zigbee/z-wave devices that are listed in add device page.

FIGURE 36 Adding Devices to Hub



9. From the main page, click **IoT APs**.

10. Select an AP from the list. The sidebar on the right side displays the SmarThings information such as SmartThings Hub version, SmartThings Hub Status, SmartThings Dongle Status, SmartThings Hardware Version and SmartThings Serial number.

IoT Access Points						RuckusAP ×	
0 IoT AP Selected	Pre-Approve IoT	APs				IoT AP Approve	(Apply)
[ No Data Available ]	0	Name	MAC ID	IP Address		2	
	0	RuckusAP	94:F6:65:2A:2A:50	192,168,40,49	zic	IoT APs Settings	
						IP 192.168	.40.49
						MAC 94:F6:65	5:24:24:50
						Net Mask 255.255	.255.0
						DNS 192.168	.40.1
						SmartThings version 1.7.0.32	.12
						SmartThings Info	
						SmartThings Hub version	32.12
						SmartThings Dongle status	Detected
						SmartThings Hub status	Stopped
						SmartThings Hardware version	1.01
						SmartThings Serial number	3111000132
Total IoT APs : 1 Export IoT APs	s to CSV					Other Info	Tida

FIGURE 37 SmartThings Info in the Right Pane

## **Activating and Editing the Plugins**

Plugins are the external vendor connectors that can be connected to a vendor infrastructure after the successful activation of a plugin. Ruckus supports Assa Abloy locks and plugins such as Kontakt.io, iBeacon, Eddystone, Beacon as a Service, Controller Data Stream, Telkonet, and Soter.

### Activating and Editing the Kontakt.io Beacons Plugin

The RUCKUS IoT Controller provides support for the Kontakt.io Beacons plugin.

To establish a connection to a vendor infrastructure, the administrator must perform the following steps.

- 1. From the main menu, click Admin.
- 2. In the left navigation pane, click Plugins.

### 3. In the Select a Plugin to Activate list, select the Kontakt.io plugin and click Activate.

### FIGURE 38 Activating the Kontakt.io Plugin

A dura ina			
Admin			Kontakt.io
			Globally enable connector on all valid APs
Services	Select a Plugin to Activate : Kontakt.io	d	Aggregation Interval *
Plugins			API Key *
Account			API Key Show
VM Configurations	Active Plugin List	4	URL•
Versions & Patches	No Plugins Found	_	https://api.kontakt.io
DB Backup			Version •
License			(Apply)
Settings			
Reset & Reboot			
		_	

- 4. After the Kontakt.io plugin is activated, enter the following configuration parameters.
  - a) Select **Globally enable connector on all valid APs** to add all respective IoT APs automatically. Connectors are mapped to IoT AP by adding the connector name tag to the IoT AP.

#### NOTE

If **Globally enable connector on all valid APs** is not selected, you can activate the plugin for each AP by adding a tag. Refer to Adding Tags to an AP on page 90 for more information.

- b) For Aggregation Interval, set the time interval between the two packets.
- c) Enter the API Key.

The RUCKUS IoT Controller posts the beacon messages using the API Key provided. The Vendor application is responsible for authenticating the API Keys.

d) Enter the API URL.

The RUCKUS IoT Controller connects to the vendor/connector URL to send the beacon messages. The URL can be a DNS-resolvable, FQDN-based address.

### NOTE

The plugin supports HTTP and HTTPS modes.

e) Enter the Version number.

The default version number is 9.

5. Click Apply.

The Kontakt.io plugin is added in the Active Plugin List.

6. To deactivate the Kontakt.io plugin, select it and click **Deactivate**.

### FIGURE 39 Deactivating the Kontakt.io Plugin

Admin		
Services Plugins	Setect a Plugin to Activate : Celect	
Account VM Configurations Versions & Patches	Active Plugin List Kontakt.io	(Deactivate)
DB Backup Reset & Reboot		

7. To edit the configuration of the Kontakt.io plugin, select it and click **Update**.

FIGURE 40 Updating the Configuration Parameters

Admin				Kontakt.io View logs	8
Services	Select a Plugin to Activate :	Select 👻	G	Globally enable connector on all valid APs     Status: Reachable	
Plugins				Aggregation Interval *	200 ms
Account	Active Plugin List			API Key •	Show
VM Configurations	Assa Abloy			URL*	Show
Versions & Patches	Kontakt.io			https://api.kontakt.io	
DB Backup	Tile Demo			Version *	
	Trackr Demo			9	
License	iBeacon				Update
Settings	Eddystone				
Reset & Reboot	Controller Data Stream				
	Beacon as a Service				
	Telkonet				

### Activating and Editing the Assa Abloy Plugin

The RUCKUS IoT Controller provides support for the Assa Abloy Door Locks. The RUCKUS IoT Controller reads the packet from the IoT AP and routes the packets to the Visionline Server.

To establish a connection to a vendor infrastructure, the administrator must perform the following steps.

- 1. From the main menu, click Admin.
- 2. In the left navigation pane, click Plugins.
- 3. In the Select a Plugin to Activate list, select the Assa Abloy plugin and click Activate.

### FIGURE 41 Activating the Assa Abloy Plugin

Admin				Assa Abloy 🛞
Services Flagtis Account VN Configurations Virisions & Patches	Select a Plugin to Activate : Active Plugin List	Assa Abloy 🛛 👻	A	- Username •
DB Backup				
Rules Backup				(Apply)
License				
Settings				
Reset & Reboot				

- 4. After the Assa Abloy plugin is activated, enter the following configuration parameters.
  - a) Enter the Username used for connecting to Visionline Server.
  - b) Enter the **Password** used for connecting to Visionline Server.
  - c) Enter the Visionline IP address or FQDN .
  - d) Enter the Port

#### NOTE

By default port number is 443.

#### 5. Click Apply.

The Assa Abloy plugin is added in the Active Plugin List.

Activating and Editing the Plugins

6. To deactivate the Assa Abloy plugin, select it and click **Deactivate**.

FIGURE 42 Deactivating the Assa Abloy Plugin

Admin				
Services	Select a Plugin to Activate :	Dormakaba	• (Activate)	
Plugins				
Account	Active Plugin List			
VM Configurations	Assa Abloy			Deactivate
Versions & Patches				
DB Backup				
Rules Backup				
License				
Settings				
Reset & Reboot				

7. To edit the configuration of the Assa Abloy plugin, select it and click **Update**.

### FIGURE 43 Updating the Configuration Parameters

Admin				Assa Abloy (Bestart ) (Stop) (View logs)
Services Plugins Account	Select a Plugin to Activate :	Cormalaba 🔹	A	II Cabally enable convector on all valid JPs Status: Beachable Utarmane (sym
Account VM Configurations	Active Plugin List Assa Abloy			( ••• Stow Visionline IP Address or PQDN •
Versions & Patches				10.174.112.29 Port * (44)
Rules Backup				Access ID i
License				(Update)
Reset & Reboot				

### Activating and Editing the Eddystone Plugin

The RUCKUS IoT Controller provides support for the Bluetooth Low Energy (BLE) Eddystone plugin. The RUCKUS IoT Controller reads the packet from IoT AP, and routes the packets to the BLE beacon vendor cloud services.

To establish a connection to a vendor infrastructure, the administrator must perform the following steps.

- 1. From the main menu, click Admin.
- 2. In the left navigation pane, click **Plugins**.

### 3. In the Select a Plugin to Activate list, select the Eddystone plugin and click Activate.

### FIGURE 44 Activating the Eddystone Plugin

Eddystone 🛞
Globally enable connector on all valid APs
Aggregation Interval 200 ms
Vendor 1 Vendor 2
Key • Enter Key Show
Enter Key Show
Enter URL
Port
Enter Port
API Endpoint Enter URI (Eg /eddystone)
UUID Filter
Enter UUID
Enable heartbeat i

Activating and Editing the Plugins

- 4. After the Eddystone plugin is activated, enter the following configuration parameters.
  - a) Select **Globally enable connector on all valid APs** to add all respective IoT APs automatically. Connectors are mapped to IoT AP by adding the connector name tag to the IoT AP.

### NOTE

If **Globally enable connector on all valid APs** is not selected, you can activate the plugin for each AP by adding a tag. Refer to Adding Tags to an AP on page 90 for more information.

- b) For Aggregation Interval, set the time interval between the two packets.
- c) Enter the Key.

The RUCKUS IoT Controller posts the beacon messages using the Key provided. The Vendor application is responsible for authenticating the Keys.

d) Enter the API URL.

The RUCKUS IoT Controller connects to the vendor/connector URL to send the beacon messages. The URL can be a DNS-resolvable, FQDN-based address.

### NOTE

The plugin supports HTTP and HTTPS modes.

e) Enter the Port number.

This is the port number on which the vendor/connector web server is running.

f) Enter the API Endpoint.

This is the API route where the BLE beacon vendor cloud services receive the beacon payload.

g) Enter the UUID Filter.

The filter allows only the BLE ADV packets with the specified UUID to be passed on to the vendor application.

h) Enable heartbeat.

Enabling heartbeat allows the vendor application to receive the IoT AP status, such as online or offline.

5. Click Apply.

The Eddystone plugin is added in the Active Plugin List.

6. To deactivate the Eddystone plugin, select it and click **Deactivate**.

### FIGURE 45 Deactivating the Eddystone Plugin

Admin		
Services Plugins Account	Select a Plugin to Activate : Select	
VM Configurations Versions & Patches DB Backup Reset & Reboot	Active Plugin List Eddystone	Deactivate
Neser & Neudol		
¢		

7. To edit the configuration of the Eddystone plugin, select it and click **Update**.

FIGURE 46 Updating the Configuration Parameters

Admin				Eddystone View logs	8
Services Plugins	Select a Plugin to Activate :	Select 🔍	Ø	Globally enable connector on all valid APs     Status: Not reachable     Key	
Account	Active Plugin List			API URL	Show
VM Configurations	Kontakt.io			https://10.174.112.38	
Versions & Patches	iBeacon			Port 8800	
DB Backup	Eddystone			API Endpoint	
Reset & Reboot				/eddystonexox	
				UUID Filter	
				Enter UUID	
				Enable heartbeat i	Yes
				/eddy_ibeacon_heart	
					(Update)

### Activating and Editing the iBeacon Plugin

The RUCKUS IoT Controller provides support for the Bluetooth Low Energy (BLE) iBeacon plugin. The RUCKUS IoT Controller reads the packet from the IoT AP, and routes the packets to the BLE beacon vendor cloud services.

To establish a connection to a vendor infrastructure, the administrator must perform the following steps.

- 1. From the main menu, click **Admin**.
- 2. In the left navigation pane, click Plugins.
- 3. In the Select a Plugin to Activate list, select the iBeacon plugin and click Activate.

FIGURE 47 Activating the iBeacon Plugin

Admin			iBeaco	n	8
Services Plugins	Select a Plugin to Activate :	(IBeacon   +)		iy enable connector on all valid APs ion Interval	200 ms
Account	Active Plugin List		Key •	0/	Show
VM Configurations Versions & Patches	No Plugins Found		API URL		
DB Backup			Port Enter P	ort	
License			API Endp	pint RI (Eg /ibeacon)	
Reset & Reboot			UUID Filt	er	
				oud eartbeat i	No
					Apply

- 4. After the iBeacon plugin is activated, enter the following configuration parameters.
  - a) Select **Globally enable connector on all valid APs** to add all respective IoT APs automatically. Connectors are mapped to IoT AP by adding the connector name tag to the IoT AP.

### NOTE

If **Globally enable connector on all valid APs** is not selected, you can activate the plugin for each AP by adding a tag. Refer toAdding Tags to an AP on page 90 for more information.

- b) For Aggregation Interval, set the time interval between two packets.
- c) Enter the Key.

The RUCKUS IoT Controller posts the beacon messages using the Key provided. The Vendor application is responsible for authenticating the Keys.

d) Enter the API URL.

The RUCKUS IoT Controller connects to the vendor/connector URL to send the beacon messages. The URL can be a DNS-resolvable, FQDN-based address.

### NOTE

The plugin supports HTTP and HTTPS modes.

e) Enter the Port number.

This is the port number on which the vendor/connector web server is running.

f) Enter the API Endpoint.

This is the API route where the BLE beacon vendor cloud services receive the beacon payload.

g) Enter the UUID Filter.

The filter allows only the BLE ADV packets with the specified UUID to be passed on to the vendor application.

h) Enable heartbeat.

Enabling heartbeat allows the vendor application to receive the IoT AP status, such as online or offline.

5. Click Apply.

The iBeacon plugin is added in the Active Plugin List.

Activating and Editing the Plugins

6. To deactivate the iBeacon plugin, select it and click **Deactivate**.

### FIGURE 48 Deactivating the iBeacon Plugin

Admin				
Services	Select a Plugin to Activate :	Select	(Activate)	
Plugins		Select	<ul> <li>Activate</li> </ul>	
Account				
VM Configurations	Active Plugin List			
Versions & Patches	iBeacon			(Deactivate)
DB Backup				
Reset & Reboot				

7. To edit the configuration of the iBeacon plugin, select it and click **Update**.

FIGURE 49 Updating the Configuration Parameters

			_		
Admin				IBeacon (View logs)	8
Services Plugins Account	Select a Plugin to Activate : Active Plugin List	Select v	(A	C Globally enable connector on all valid APs  Aggregation Interval  Vendor 1 Vendor 2	000 ms
VM Configurations	Assa Abloy			Status: Reachable Key *	Show
Versions & Patches	Kontakt.io Tile Beno			API URL * http://10.174.112.165	511041
DB Backup	Trackr			Port	
License	IBeacon			5000	$\square$
	Eddystone			API Endpoint	
Settings	Controller Data Stream			( /ibeacon	
Reset & Reboot	Beacon as a Service			UUID Filter	
	Telkonet			Enter UUID	
	Soter			Enable heartbeat i	)
				/heartbeat	
				U	Jpdate )

# Activating and Editing the Beacon as a Service Plugin (iBeacon, Eddystone and Custom)

The RUCKUS IoT Controller provides support for the Bluetooth Low Energy (BLE) beaconing service. An AP can begin transmitting BLE beacons (iBeacons) that can be used by the user for various cases, such as wayfinding and pushing.

To establish a connection to a vendor infrastructure, the administrator must perform the following steps.

- 1. From the main menu, click **Admin**.
- 2. In the left navigation pane, click **Plugins**.

Activating and Editing the Plugins

3. In the Select a Plugin to Activate list, select the Beacon as a Service plugin and click Activate.

FIGURE 50 Activating the Beacon as a Service Plugin (iBeacon)

Beacon as a Service	8
Globally enable connector on all valid APs	
Advertisement Interval •	
Beacon Type •	100 ms
iBeacon	Ŧ
UUID •	
0047e70a5dc147258799830544ae04f6	
Major No * i	
0102	
Minor No * i	
0000	
Tx Power Level @1m *	
0	
	Update

FIGURE 51 Activating Beacon as a Service (Eddystone)

Beacon as a Service	۲
Globally enable connector on all valid APs	
Advertisement Interval *	
0	100 ms
Beacon Type •	
Eddystone	Ψ
Namespace ID •	
48d815a81b09b25a41b1	
Instance ID •	
6b2441d56920	
URL•	
http://www.ruckuswireless.com	
Tx Power Level @0m *	
0	
	(
	Update

FIGURE 52 Activating Beacon as Service (Generic)

Beacon as a Service			6
Globally enable connector on all valid APs			
dvertisement Interval *			
0			100 ms
eacon Type *			
Custom Beacon			*
Vendor type			
Generic			
03			-
1234			Add
ADV Type	Value	Actions	
01	0192	/ 11	
			Update

- 4. After the Beacon as Service plugin is activated, enter the following configuration parameters.
  - a) Select **Globally enable connector on all valid APs** to add all respective IoT APs automatically. Connectors are mapped to IoT AP by adding the connector name tag to the IoT AP.

### NOTE

If **Globally enable connector on all valid APs** is not selected, you can activate the plugin for each AP by adding a tag. Refer to Adding Tags to an AP on page 90 for more information.

- b) In the **Beacon Type** list, select the type of beacon.
- c) After selecting the type of Beacon, in the **Advertisement Type** list, select the type of advertisement.
- d) For **Advertisement Interval**, set the time interval to send the advertisement packets. The advertisement interval ranges from 100 through 1000 milliseconds. The default interval is 100 milliseconds.
- 5. Click Apply.

The Beacon as a Service plugin is added in the Active Plugin List.

6. To deactivate the Beacon as a Service plugin, select it and click **Deactivate**.

FIGURE 53 Deactivating the Beacon as a Service Plugin

Admin		
Services	Select a Plugin to Activate : Activate	
Plugins		
Account	Active Plugin List	
VM Configurations	Beacon as a Service	(Deactivate )
Versions & Patches		
DB Backup		
Reset & Reboot		

7. To edit the configuration of the Beacon as a Service plugin, select it and click **Update**.

Admin Beacon as a Service 8 Globally enable connector on all valid APs Advertisement Interval • Services Select a Plugin to Activate : A Select -100 ms  $\bigcirc$ Beacon Type • Plugins iBeacon Ψ UUID • Account Active Plugin List 0047e70a5dc147258799830544ae04f6 Assa Abloy VM Configurations Major No • i Kontakt.io 0102 iBeacon Versions & Patches Minor No \* i Eddystone 0000 DB Backup Controller Data Stream Tx Power Level @1m • Beacon as a Service Rules Backup 0 Telkonet License Soter BLE Scan Settings Reset & Reboot

FIGURE 54 Updating the Configuration Parameters (iBeacon)

### FIGURE 55 Updating Configuration parameters (Eddystone)

Admin				Beacon as a Service ③
Services Plugins	Select a Plugin to Activate :	Select v	(A4	Clobally enable connector on all valid APs  Advertisement Interval *      Beacon Type *      Eddystone      V
Account	Active Plugin List			Namespace ID * 466815a81b09b25a41b1
VM Configurations	Assa Abloy Kontakt.io			Instance ID •
Versions & Patches	iBeacon			6b2441d56920 URL *
DB Backup	Eddystone Controller Data Stream		-	http://www.ruckuswireless.com
Rules Backup	Beacon as a Service			Tx Power Level @0m* 0
License	Soter		_	(Update)
Settings	BLE Scan			
Reset & Reboot				

Activating and Editing the Plugins

### FIGURE 56 Updating Configuration Parameters (Generic)

Admin					Beacon as a Service		۲
Services Plugins	Select a Plugin to Activate :	Select	<u>+</u> ) (	Ac	Cidebally enable connector on all valid APs Advertisement Interval • Beacon Type • Custom Beacon		100 ms
Account	Active Plugin List			_	Vendor type Generic		
VM Configurations	Assa Abloy Kontakt.io				Select type		•
Versions & Patches	iBeacon				ADV Type	Value	Actions
DB Backup	Eddystone Controller Data Stream				01	0192	/ 8
Rules Backup	Beacon as a Service						Update
License	Soter						
Settings	BLE Scan						
Reset & Reboot							

### Activating and Editing the Beacon as a Service Plugin (React Mobile)

The RUCKUS IoT Controller provides support for the React Mobile beaconing service. An AP can begin transmitting BLE beacons (React) that can be used by the user for various cases, such as wayfinding and pushing.

To establish a connection to a vendor infrastructure, the administrator must perform the following steps.

- 1. From the main menu, click Admin.
- 2. In the left navigation pane, click **Plugins**.
- 3. In the Select a Plugin to Activate list, select the Beacon as a Service plugin and click Activate.

FIGURE 57 Activating Beacon as a Service (React Mobile)

Beacon as a Service	8
Globally enable connector on all valid APs	
Advertisement Interval *	
0	100 ms
Beacon Type •	
Custom Beacon	· · · · · · · · · · · · · · · · · · ·
Vendor type	
React mobile	· · · )
	Update

- 4. After the Beacon as Service plugin is activated, enter the following configuration parameters.
  - a) Select **Globally enable connector on all valid APs** to add all respective IoT APs automatically. Connectors are mapped to IoT AP by adding the connector name tag to the IoT AP.

### NOTE

If **Globally enable connector on all valid APs** is not selected, you can activate the plugin for each AP by adding a tag. Refer to Adding Tags to an AP on page 90 for more information.

- b) For Advertisement Interval, set the time interval to send the advertisement packets. The advertisement interval ranges from 100 through 1000 milliseconds. The default interval is 100 milliseconds.
- c) In the **Beacon Type** list, select the type of beacon as **Custom**.
- d) After selecting the type of Beacon, in the Vendor Type list, select the type as React Mobile.
- 5. Click Apply.

The Beacon as a Service plugin is added in the Active Plugin List.

6. To deactivate the Beacon as a Service plugin, select it and click **Deactivate**.

#### FIGURE 58 Deactivating the Beacon as a Service Plugin

Admin				
Services	Select a Plugin to Activate :	Select	• Activate	
Plugins				
Account	Active Plugin List			
VM Configurations	Beacon as a Service			Deactivate
Versions & Patches				
DB Backup				
Reset & Reboot				

### Activating and Editing the BLE Scan Plugin

The RUCKUS IoT Controller provides support for the Bluetooth Low Energy (BLE) BLE Scan Plugin . The RUCKUS IoT Controller reads the packet from the IoT AP and routes the packets to the BLE beacon vendor cloud services.

To establish a connection to a vendor infrastructure, the administrator must perform the following steps.

- 1. From the main menu, click Admin.
- 2. In the left navigation pane, click Plugins.

3. In the Select a Plugin to Activate list, select the BLE Scan plugin and click Activate.

Admin				BLE Scan	8
Services Plugins	Select a Plugin to Activate :	BLE Scan 🛛 👻	A	Vendor 1 Vendor 2	1000 ms
Account	Active Plugin List			Key • Enter Key	Show
VM Configurations	IBeacon			API URL*	
Versions & Patches	SOLEY			Port	
DB Backup				Enter Port	
Rules Backup				API Endpoint (Enter UBI (Eg /blescan)	
License				UUD Filter	
Settings				Enable heartbeat i	No
Reset & Reboot					Apply

- 4. After the BLE Scan plugin is activated, enter the following configuration parameters.
  - a) Select **Globally enable connector on all valid APs** to add all respective IoT APs automatically. Connectors are mapped to IoT AP by adding the connector name tag to the IoT AP.

#### NOTE

If **Globally enable connector on all valid APs** is not selected, you can activate the plugin for each AP by adding a tag. Refer to Adding Tags to an AP on page 90 for more information.

- b) For Aggregation Interval, set the time interval between the two packets.
- c) Enter the Key.

The RUCKUS IoT Controller posts the beacon messages using the Key provided. The Vendor application is responsible for authenticating the Keys.

d) Enter the API URL.

The RUCKUS IoT Controller connects to the vendor/connector URL to send the beacon messages. The URL can be a DNS-resolvable, FQDN-based address.

### NOTE

The plugin supports HTTP and HTTPS modes.

e) Enter the Port number.

This is the port number on which the vendor/connector web server is running.

f) Enter the API Endpoint.

This is the API route where the BLE beacon vendor cloud services receive the beacon payload.

g) Enter the UUID Filter.

The filter allows only the BLE ADV packets with the specified UUID to be passed on to the vendor application.

h) Enable heartbeat.

Enabling heartbeat allows the vendor application to receive the IoT AP status, such as online or offline.

### 5. Click Apply.

The BLE Scan plugin is added in the Active Plugin List.

6. To deactivate the BLE Scan plugin, select it and click **Deactivate**.

### FIGURE 60 Deactivating the BLE Scan Plugin

Services	Select a Plugin to Activate :	Select	* (Activate	
Plugins				
Account	Active Plugin List			
VN. Configurations	BLE Scan			Deactivate
Versions & Patches				
D6 Backup				
Rules Backup				
license				
lettings				
Reset & Reboot				

7. To edit the configuration of the BLE Scan plugin, select it and click **Update**.

### FIGURE 61 Updating the Configuration Parameters

Admin				BLE Scan            View logs
Services	Select a Plugin to Activate :	Select 🔍	A	Globally enable connector on all valid APs  Aggregation Interval  1000 ms
Account	Active Plugin List			Vendor 1 Vendor 2 Status: Reachable
VM Configurations	BLE Scan		_	Key *
Versions & Patches				API URL•
DB Backup				http://abc.com Port
Rules Backup				80
License				API Endpoint /test
Settings				UUID Filter
Reset & Reboot				(Enter UUD
				Enable heartbeat i

### Activating and Editing the Controller Data Stream Plugin

The RUCKUS IoT Controller provides support for the Controller Data Stream plugin. The Controller Data Stream is a Message Queue Telemetry Transport (MQTT) data stream. When it is enabled, it sends IoT device-related details to the third-party MQTT endpoint (MQTT Broker). The device data stream is sent to third-party every 300 seconds.

To establish a connection to a vendor infrastructure, the administrator must perform the following steps.

- 1. From the main menu, click **Admin**.
- 2. In the left navigation pane, click **Plugins**.
- 3. In the Select a Plugin to Activate list, select the Controller Data Stream plugin and click Activate.

FIGURE 62 Activating the Controller Data Stream Plugin

Controller Data Stream	$\otimes$
Globally enable connector on all valid APs	
MQTT Broker IP •	
Enter MQTT Broker IP	
MQTT Broker Port •	
Enter MQTT Broker Port	
MQTT Publish Topic * i	
Eg /topic	
Periodic Update Interval	
10	
Device reporting	No
Validate Server Certificate	No
	Apply

- 4. After the Controller Data Stream plugin is activated, enter the following configuration parameters.
  - a) Select **Globally enable connector on all valid APs** to add all respective IoT APs automatically. Connectors are mapped to IoT AP by adding the connector name tag to the IoT AP.

### NOTE

If **Globally enable connector on all valid APs** is not selected then you can activate the plugin for each AP by adding tag. Refer Adding Tags to an AP on page 90 for more information.

- b) In MQTT Broker IP, enter the IP address of your MQTT broker.
- c) In MQTT Broker Port, enter the network port to which you want to connect.
- d) In **MQTT Publish Topic**, enter the topic name as a simple string that is hierarchically structured with forward slashes (/) as delimiters. An MQTT client can publish messages as soon as it connects to a broker.
- e) In **Periodic Update Interval** enter the interval to receive MQTT Publish.
- f) Enable Device Reporting and enter the topic endpoint which will publish message whenever a device change event is received.
- g) Enable Validate Server Certificate to secure the connection with SSL.

### 5. Click Apply.

The Controller Data Stream plugin is added in the Active Plugin List.

6. To deactivate the Controller Data Stream plugin, select it and click **Deactivate**.

### FIGURE 63 Deactivating the Controller Data Stream Plugin

Admin		
Services	Select a Plugin to Activate : Select 🗸 🗸	
Plugins		
Account	Active Plugin List	
VM Configurations	Controller Data Stream	Deactivate
Versions & Patches	Beacon as a Service	Deactivate
DB Backup		
Reset & Reboot		

7. To edit the configuration of the Controller Data Stream, select it and click **Update**.

FIGURE 64 Updating the Configuration Parameters

Admin				Controller Data Stream	⊗
	[			Globally enable connector on all valid APs     Status: Reachable	
Services	Select a Plugin to Activate :	Select 🗸 🗸	A	MQTT Broker IP •	
Plugins				192.168.29.200 MOTT Broker Port •	]
Account	Active Plugin List			8883	
VM Configurations	Assa Abloy			MQTT Publish Topic • i	
vw.comgurations	Kontakt.io			/home	
Versions & Patches	iBeacon			Periodic Update Interval	
	Eddystone			10	
DB Backup	Controller Data Stream			Device reporting	D
Rules Backup	Beacon as a Service			/dev-report	
	Telkonet			Validate Server Certificate	
License	Soter				
Settings	BLE Scan				Update
Reset & Reboot					
	L		-		

### Activating and Editing the Dormakaba Plugin

The RUCKUS IoT Controller provides support for for the Dormakaba Door Locks. The RUCKUS IoT Controller reads the packet from the IoT AP and routes the packets to the Ambiance Server.

To establish a connection to a vendor infrastructure, the administrator must perform the following steps.

- 1. From the main menu, click Admin.
- 2. In the left navigation pane, click Plugins.
- 3. In the Select a Plugin to Activate list, select the Dormakaba plugin and click Activate.

### FIGURE 65 Activating the Dormakaba Plugin

Admin				Dormakaba   Citobally enable connector on all valid APs
Services	Select a Plugin to Activate :	Dormakaba 👻	Ā	AllB Username •      (Enter AllB Username  AllB Password •
Plugins				Enter AMB password Show
Account	Active Plugin List			AMB IP
VM Configurations				Enter ANB IP ANB Host *
Versions & Patches				Enter AMB Host
DB Backup				AMB Port*  Enter Port
Rules Backup				AMB Auth path
License				AMB API Path •
Settings				Enter AMB API Path
Reset & Reboot				ANE API VER Path * Enter ANB API VER Path
				(Apply)

- 4. After the Dormakaba plugin is activated, enter the following configuration parameters.
  - a) Enter the Ambiance Username used for connecting to Ambiance Server.
  - b) Enter the Ambiance Password used for connecting to Ambiance Server.
  - c) Enter the Ambiance IP Address .
  - d) Enter the Ambiance Host.

#### NOTE

The URL for Host is http://Ambiance IP Address

- e) Enter the Ambiance Port.
- f) Enter the Ambiance Auth Path.
- g) Enter the Ambiance API Path.
- h) Enter the Ambiance API VER Path.
- 5. Click Apply.

The Dormakaba plugin is added in the Active Plugin List.

#### 6. To deactivate the Dormakaba plugin, select it and click **Deactivate**.

### FIGURE 66 Deactivating the Dormakaba Plugin

Admin				
Services	Select a Plugin to Activate :	Select	· Activate	
Plugins				
Account	Active Plugin List			
VM Configurations	Dormakaba			Deactivate
Versions & Patches				
DB Backup				
Rules Backup				
License				
Settings				
Reset & Reboot				

7. To edit the configuration of the Dormakaba plugin, select it and click **Update**.

### FIGURE 67 Updating the Configuration Parameters

Admin				Dormakaba
				Globally enable connector on all valid APs
			-	AMB Username *
Services	Select a Plugin to Activate :	Select v	A	Admin01
Plugins				AMB Password •
				Show
Account	Active Plugin List			AM8 IP
	Dormakaba			10.174.113.240
VM Configurations				AMB Host *
Versions & Patches				http://10.174.113.240
				AMB Port *
DB Backup				80
Rules Backup				AMB Auth path
nates backup				(/auth
License				AMB API Path •
				( /apl
Settings				AMB API VER Path *
Reset & Reboot				(/ver
				Update
			_	-

### Activating and Editing the Telkonet Plugin

The RUCKUS IoT Controller provides support for the Telkonet devices and their respective MQTT APIs.

To establish a connection to a vendor infrastructure, the administrator must perform the following steps.

- 1. From the main menu, click Admin.
- 2. In the left navigation pane, click **Plugins**.

3. In the Select a Plugin to Activate list, select the Telkonet plugin and click Activate.

### FIGURE 68 Activating the Telkonet Plugin

Admin				Clobally enable connector on all valid APs P Address	$\otimes$
Services	Select a Plugin to Activate :	Telkonet 👻	A	10.174.113.66	
Plugins				Port • 6031	
Account	Active Plugin List				Apply
VM Configurations	No Plugins Found				
Versions & Patches					
DB Backup					
License					
Settings					
Reset & Reboot					
			_		

- 4. After the Telkonet plugin is activated, enter the following configuration parameters.
  - a) Select **Globally enable connector on all valid APs** to add all respective IoT APs automatically. Connectors are mapped to IoT AP by adding the connector name tag to the IoT AP.

### NOTE

If **Globally enable connector on all valid APs** is not selected, you can activate the plugin for each AP by adding a tag. Refer to Adding Tags to an AP on page 90 for more information.

b) Enter the IP Address.

This is the IP address of the Telkonet controller.

c) Enter the Port number.

This is the port number on which the vendor/connector web server is running.

5. Click Apply.

The Telkonet plugin is added in the Active Plugin List.

6. To deactivate the Telkonet plugin, select it and click **Deactivate**.

### FIGURE 69 Deactivating the Telkonet Plugin

Admin			
Services	Select a Plugin to Activate :	Select 🛛 👻 🗍 Activate	
Plugins			
Account	Active Plugin List		
VM Configurations	Telkonet		Deactivate
Versions & Patches			
DB Backup			
License			
Settings			
Reset & Reboot			

7. To edit the configuration of the Telkonet plugin, select it and click **Update**.

FIGURE 70 Updating the Configuration Parameters

Admin				Telkonet	$\otimes$
Services Plugins Account	Select a Plugin to Activate : Active Plugin List	Select v	Ø	Client status: Not Connected D Address 10.174.113.66 Port • 6031	
VM Configurations	Telkonet				pdate
Versions & Patches					
DB Backup					
License					
Settings					
Reset & Reboot					

### Activating and Editing the Soter Plugin

The RUCKUS IoT Controller provides support for the Soter plugin. The Soter Sensor must have IoT Controller MQTT Broker details for the Soter Sensor MQTT Client to connect and transmit data.

To establish a connection to a vendor infrastructure, the administrator must perform the following steps.

- 1. From the main menu, click Admin.
- 2. In the left navigation pane, click Plugins.
- 3. In the Select a Plugin to Activate list, select the Soter plugin and click Activate.

FIGURE 71 Activating the Soter Plugin

Admin				Soter 🙁
Services Plugins	Select a Plugin to Activate :	〔Soter	7	Soter URL • (Enter Soter URL ) Soter Port • Enter Soter Port
Account	Active Plugin List			Soter Key • Enter Soter Key Show
VM Configurations Versions & Patches	Telkonet			(Apply)
DB Backup License				
Settings Reset & Reboot				

- 4. After the Soter plugin is activated, enter the following configuration parameters.
  - a) Enter the Soter URL.

This URL is used to establish the MQTT connection between the controller and the Soter server.

b) Enter the Port number.

This is the port number on which the MQTT server is running.

### NOTE

The default MQTT port is 8883.

c) Enter the Key.

The Vendor application is responsible for authenticating the Keys.

5. Click Apply.

The Soter plugin is added in the Active Plugin List.

6. To deactivate the Soter plugin, select it and click **Deactivate**.

FIGURE 72 Deactivating the Soter Plugin

RUCKUS IoT Conti	oller Dashboard IoT APs IoT Devices Events Admin Rules LoRa LNS IoT A	vriot-Shriram-Virtualbox 1.5.0.0.22 Version Apj N+1 : Disabled 2 January 2020 16:23:16 (*) Asia/Bangkok
Admin		
Services	Select a Plugin to Activate : Select Activate	
Plugins		
Account	Anthree Principal Content	
VM Configurations	Active Plugin List Soter	Deactivate
Versions & Patches		( black days
DB Backup		
License		
Settings		
Reset & Reboot		

7. To edit the configuration of the Soter plugin, select it and click **Update**.

FIGURE 73 Updating the Configuration Parameters

Admin				Soter	8
Services Plugins	Select a Plugin to Activate :	Select	A	Status: Not Reachable Soter URL • e2-54-196-163-125.compute-1.amazonaws.com Soter Port • (5883)	)
Account	Active Plugin List			Soter Key*	)
VM Configurations	Assa Abloy Kontakt.lo			(********	Show
Versions & Patches	Tile (terro				(Update)
DB Backup	Trackr (Dense)				
License	iBeacon Eddystone				
Settings	Controller Data Stream				
Reset & Reboot	Beacon as a Service				
2	Soter				

## **Changing the Password**

A single administrator is responsible for creating a RUCKUS IoT Controller account. This administrator manages system operations.

To change the password, the administrator must perform the following steps.

- 1. From the main menu, click Admin.
- 2. In the left navigation pane, click Account.

FIGURE 74 Changing the Password

			Update passw
Current Password *			
Current Password	Enter Current password	Show	
New Password *	Enter New password	Show	

3. Change the password and click Update password.

## **Configuring Virtual Machines**

Complete the following steps to configure a virtual machine (VM).

- 1. From the main menu, click Admin.
- 2. In the left navigation pane, click VM Configurations.

FIGURE 75 Configuring a Virtual Machine

				Update
Hostname *	DHCP	Static	Current Certificate	
Primaryyy	IP Address:	10.174.113.204	Common Name : local-mqtt.video54.local Certificate Expires on Apr 18 14:35:35 2030 GMT	
Time Zone *	Netmask:	255.255.254.0	Paste certificate Here	
Asla/Tokyo 👻	Gateway:	10.174.112.1		
Set Time Automatically using NTP NTP Address	DNS Server 1:	10.10.10.10	Paste Key Here	
ntp.ubuntu.com (Optional)	DNS Server 2:	10.10.10.106		
Set Time Manually i				

- 3. Complete the configuration information.
  - a) In the **Hostname** field, enter the host name.
  - b) In the Time Zone list, select the time zone.
  - c) Select Set Time Automatically using NTP or Set Time Manually to set the time.
  - d) Click **DHCP** or **Static** to set the RUCKUS IoT Controller configuration.

#### NOTE

The RUCKUS IoT Controller is configured with a self-signed certificate, but a proper (CA-signed) certificate can be added to the system.

4. Click Update.

### **Uploading Versions and Patches**

RUCKUS frequently releases updates to RUCKUS IoT Controller. The administrator normally receives any updates about new and updated software by email.

### **Uploading an Image**

RUCKUS sends periodic notifications by email regarding new versions of the RUCKUS IoT Controller.

- 1. From the main menu, click Admin.
- 2. In the left navigation pane, click Version & Patches.

#### FIGURE 76 Uploading an Image

Admin				
Services	Upload Image Upload Patch			
Plugins				
Account	Version list		Patch list	
VM Configurations	1.5.1.1.22	Delete Set	No Patch Available	
Versions & Patches	1.6.0.0.38	(Service) (Ser		
DB Backup				
Rules Backup				
License				
Settings				
Reset & Reboot				

3. Click **Upload Image** to upload the upgrade package.

Once uploaded, the new version is listed in the Version list.

4. Select the latest version to upgrade and click Set. To remove a version, select it and click Delete.

### **Uploading a Patch**

Patches to the software can be downloaded from the RUCKUS Support portal.

- 1. From the main menu, click **Admin**.
- 2. In the left navigation pane, click Versions & Patches.

FIGURE 77 Uploading a Patch

Admin					
Services	Upload Image				Upload Patch
Plugins					
Account	Version list	(Delete) (Set)	Patch list patch-1.6.0.0.40	Not Applied	(Apply)
VM Configurations	1.6.0.0.38	(Delete) (Set			
Versions & Patches					
DB Backup					
Rules Backup					
License					
Settings					
Reset & Reboot					

3. Click Upload Patch to upload the patch.

ATTENTION

You cannot revert a patch.

### **Backing Up Files**

The RUCKUS IoT Controller allows you to back up and restore the configuration and data files. You can restore an existing configuration file on the RUCKUS IoT Controller from which it originated, or restore a configuration file from a different RUCKUS IoT Controller. Backed up files are in the tar.gz format.

- 1. From the main menu, click Admin.
- 2. In the left navigation pane, click **DB Backup**.

#### FIGURE 78 Backing Up or Restoring Files

Create Backup	(Upload Backup
Backups List	
No Backups Found	

- 3. Click Create Backup now to perform a backup manually.
- 4. Click Upload Backup to download and re-upload the backup files.

#### NOTE

The RUCKUS IoT Controller maintains the backups of the last five configuration files. Upon completing the backup, the network settings are reset to DHCP.

### **Backing up Rules**

The RUCKUS IoT Controller allows you to back up and restore the static files, and node-red flows. You can restore an existing flow or file on the RUCKUS IoT Controller from which it originated, or restore a from a different RUCKUS IoT Controller. Backed up files are in the tar.gz format.

- 1. From the main menu, click Admin.
- 2. In the left navigation pane, click Rules Backup.

FIGURE 79 Backing Up or Restoring Rules

ull Backup 👻 Create Rules Backup	Upload Rules Backup
ull Backup Tows Backup tatic Files Backup RUIES BacKupS List	
VRIOT_Rules_Full_2020-04-17-06-07-53_GMT.tar.gz	(Download) (Restore) (Delete
VRIOT_Rules_Flows_Only_2020-04-17-06-08-00_GMT.tar.gz	(Download) (Restore) (Delete
VRIOT_Rules_Static_Only_2020-04-17-06-08-06_GMT.tar.gz	(Download) (Restore) (Delete

#### Managing IoT Controller System Configuration

Uploading the RUCKUS IoT Controller License

- 3. Select either of the following from the drop-down, and click Create Rules Backup.
  - Full Backup: It is the back up of statics files and nodal flows.
  - Flows Backup: It is the back up of nodal flows.
  - Static Files Backup: It is the back up of static files.
- 4. Click Upload Rules Backup to upload back up.

A dialog-box appears as below, click **Confirm**.

FIGURE 80 Confirming Upload of Backup File

Confirm
On uploading the backup file, Rules Engine will perform implicit restore and reboot.
Confirm

5. Click Download to download the backup, Restore to restore the backup, and Delete to delete the backup.

### **Uploading the RUCKUS IoT Controller License**

To obtain and activate the license, refer to "Activating a License" in the RUCKUS IoT Controller Software Installation Guide.

Complete the following steps to upload a license for the RUCKUS IoT Controller.

1. From the main menu, click Admin.

2. In the left navigation pane, click **License**.

#### FIGURE 81 Uploading a License

Controller serial number:10N AP capacity license used:11	IUH24GD5M6CC37W57AUD	01C1XDK			Upload License
AP capacity license remaining	g: 9				
AP capacity license total: 20					
License List					
Name	License type	Description	Start date	Expiry date	Count
INSTANCE-IOTC	Enabled	Permanent License	31-oct-2019	permanent	1
CAPACITY-AP-IOTC	Enabled	Permanent License	31-oct-2019	permanent	20

3. Click Upload License to upload the license.

The Upload License page displays the following information:

- Controller serial number : Displays the number of the RUCKUS IoT Controller serial number which can be used to activate the license.
- AP capacity license used: Displays the number of licenses used by APs.
- AP capacity licenses remaining: Displays the number of unused licenses by APs.
- AP capacity license total : By default, the total number of licenses is 5. If you need an additional license, you must generate a license. To generate a license, refer to "Activating a License" in the *RUCKUS IoT Controller Software Installation Guide*.
- License List: Lists the details of the license, such as Name, License Type, Description, Start date, Expiry date and count.

### **Change the Settings**

N+1 Configuration and Hot Upgrade can be performed only when SSH is enabled.

1. From the main menu, click Admin.

#### 2. In the left navigation pane, click **Settings**.

#### FIGURE 82 Settings Page

SSH	Enable	(Apply)
N+1 and Hot Upgrade feature will not	be available if SSH is disab	led

3. Enable SSH.

#### NOTE

If SSH is disabled, the N+1 configuration cannot be established and the following error is observed.

FIGURE 83 Showing Error on Disabling SSH

*****
Ruckus IoT Controller
Main Menu
***************************************
1 - Ethernet Network
2 - System Details
3 - NTP Setting
4 - System Operation
5 - N+1
6 - Comm Debugger
x - Log Off
Enter Choice: 5
N+1 Status:
N+1 Mode : Disabled
<pre>(N+1 Configure(1) / Disable(2) / Exit(x) :1 (Start Primary Controller(1) / Secondary Controller(2) / Exit(x) :1</pre>
N+1 Configure:
To Configure N+1 ensure following requirements:
******
* Primary Controller and Secondary Controller should be in same subnet and reachable.
* Primary Controller and Secondary Controller should be configured with static ip address.
* Primary Controller and Secondary Controller should be running in same version.
* Primary Controller and Secondary Controller should have synchronized date/time.
Enter Secondary Controller IP :10.174.113.91
Enter preferred Virtual IP :10.174.113.70
N+1 will stop all services & configurations in Secondary Controller. Enter Y/N to continue : y
Error: To configure N+1 please enable SSH in vRIoT controller.

## **Rebooting RUCKUS IoT Controller**

If the RUCKUS IoT Controller is experiencing an issue, attempt a reboot to resolve the issue.

Complete the following steps to reboot the RUCKUS IoT Controller.

- 1. From the main menu, click Admin.
- 2. In the left navigation pane, click **Reset & Reboot**.

FIGURE 84 Rebooting RUCKUS IoT Controller

Reboot	
Reboots the system. The	User Interface shall not be available until the system restarts !
(Factory Reset	is irreversible. This shall reset the whole system. All the data saved shall be lost.

3. Click Reboot.

### **Resetting RUCKUS IoT Controller**

To remove all of the settings that are configured on the RUCKUS IoT Controller, reset it to the factory default settings.

Complete the following steps to reset the RUCKUS IoT Controller to its factory default settings.



CAUTION Performing the reset action is irreversible.

1. From the main menu, click Admin.

2. In the left navigation pane, click Reset & Reboot.

FIGURE 85 Resetting RUCKUS IoT Controller

Reboot	
Reboots the system. The User Interface shall not be available until the system restarts !	
Factory Reset	
IMPORTANT ! This action is irreversible. This shall reset the whole system. All the data saved shall be lost.	

3. Click Factory Reset.

# **Managing IoT Access Points**

•	IoT AP Overview	. 83
	Adding an IoT AP	
	Editing an IoT AP	
	Adding Tags to an AP	
	Approval of IoT APs	
	Exporting IoT APs to CSV	

### **IoT AP Overview**

SmartZone (SZ) holds the IoT AP firmware. You must make sure the IoT Access Point (AP) connects to SZ and downloads the appropriate IoT firmware. An IoT AP discovers SZ using discovery methods such as DHCP Option 43, Domain Name System (DNS), and Access Point Registry (APR) modes.

The RUCKUS IoT Controller displays the IoT AP hierarchy (Domain, Zone, Group) information, which is derived from the IoT AP and SmartZone connection. Therefore, it is important to ensure that the IoT AP is running the latest appropriate IoT firmware.

An IoT Access Point discovers the RUCKUS IoT Controller by using Option 43 or the RUCKUS Command Line Interface (RKSCLI). RKSCLI mode is not encouraged, and must be used only if a DHCP server is not present.

### **DHCP Option 43**

The IoT Access Point supports Option 43 with the following suboptions:

- Suboption 21: Used to configure a RUCKUS IoT Controller IPv4 address or FQDN (mandatory)
- Suboption 22: Used to set the control VLAN for IoT Control/Data traffic (optional)

Option 43 supports both binary and ASCII formats. The IoT Access Point bootup process checks for Option 43 and suboptions 06, 21 and 22. Once the application receives this information, it uses the information to connect to the controller over the Pubsub channel.

You can use the DHCP Option 43 sub-option code 06 to set the SCG/vSZ/SZ IP address in the format SubCode /Length/ (Value In Hex). For example : If the IP address is 10.24.123.4, then the hex string is as follows 06 0b 31302e32342e3132332e34.

The DHCP Option 43 sub-option code 21 and 22 is used to set the RUCKUS IoT Controller IP address.

For Example, Windows DHCP Configuration with Sub-option 21 and 22:

cope Opti General		:d									?
Availab	e Optior	IS							[	)escrip	tion 🔺
040	VIS Don	nain N	ame						1	lame o	of Ne
041 NIS Servers											ses o
042 NTP Servers     Addresses o											
<b>№</b> 043	/endor !	Specifi	ic Inf	'n					F	mbed	ded 🗸 🖵
•											▶
"Data er Data:	try —		E	Binary	r:					Cor ASCII:	ntroller
0000	2Ē	31	31 31 31	30 33 2E	2E 2E 31	31 32 30	37 30 33	34 36	11	0.17 3.20 .103	16
								VL	AN		
					ОК		1	Car	ncel		Apply

Linux DHCP option 43, sub option 21 configuration is as follows:

- option RKUS.scg-address "192.168.0.3"
- option RKUS.riot-address "192.168.0.2";

dhcp\_opt43 configuration subopt 22- "vlan\_mode.vlan\_id"

- #option RKUS.iotvlan-address "0.4" -enables onlink VLAN
- #option RKUS.iotvlan-address "1.4" -enables offlink VLAN
- Offlink VLAN configuration is used when the IOT Gateway/AP and IOT controller are in different networks.
- Onlink VLAN configuration is used when the IOT Gateway/AP and IOT controller are in same network.

### **RUCKUS Command Line Interface**

The set iotg-mqtt-brokeripRUCKUS-IoT-Controller-IP-address command can be used to discover the RUCKUS IoT Controller.

### **USB** Power

If an AP does not have enough USB power, it is displayed in the IoT APs page with the following message: USB is not having enough power.

#### FIGURE 86 Displaying a Shortage of USB Power

RUCKUS INT C		Dashboard IoT AP	s IoT Devices	Events	Admin	IOT API	dhcp-172-16-113-73 Ontine	30 July 2019 10:49:30 America/Los Angeles
IoT AP Selected	Pre-Approv	ve IoT APs					baas × ibeacon × dhcp-172-16-113-73 >	
[ siby-lot-cluster ]	0	Name	MAC ID	IP Address	Protocols		Add new tag	Apply
[vSZ-loT-Lab2]	0.0	dhcp-172-16-113-73	E8:1D:A8:0A:F2:80	172.16.113.73	BLE	12	Scan for IoT Devices	Restart IoT Service
							IoT APs Settings	
								Mana and
							USB is not having enoug	h power
							IoT AP Approve	Yes Apply
							loT Management VLAN	No Apply
							IoT CoExistence i	C Off Apply
							IP 172.16.113.73	
							MAC E8:1D:A8:0A:F2:80	6
							Net Mask 255.255.254.0	
							DNS 172.16.200.3	

#### NOTE

If there is a shortage in USB power, you must contact the customer support team for more details.

# Adding an IoT AP

The administrator can add an IoT AP to the RUCKUS IoT Controller to manage IoT devices.

Complete the following steps to add an IoT AP to the controller.

1. From the main menu, click **IoT APs**.

The IoT Access Points page is displayed.

#### FIGURE 87 IoT Access Points Page

0 IoT AP Selected	(Pre-Ap	prove IoT APs					Ba	tch Ad	tions	Select - Apply
[chaos]		Name	MAC ID	IP Address	Protocol	Channel	Uptime	Act	ions	Tags
<ul> <li>[ 13-QA-VSZ ]</li> <li>[ VRIOTQA-CLST ]</li> </ul>		Karthik-R510-Desk	D8:38:FC:1C:10:90	10.74.136.40	ble	NA	2 days, 0:02:59	Q	Û	All and kentakt:Ruduz80000 (test
▶ [QA-V5Z-5-1-460]		R710	44:1E:98:13:FB:20	192.168.100.37	zigbee_aa	25	5 days, 3:48:52	Q	Û	All (4412-96-1575-20) (kentakterachusztocoz) (2710)
		R610_Shetty	B4:79:C8:04:D9:40	192.168.100.39	ble	NA	NA		Û	(4) (H.77:CE:04.59:49) (dds)
		R730	18:7C:08:20:DC:F0	192.168.100.15	zigbee	20	0 days, 0:12:54		î	(41) (18/7C08:20.0C/F0) (8730)
		R510_OUT_RuckusAP_Shriram	EC:8C:A2:37:03:A0	192.168.100.59	zigbee	14	NA		Û	All BCISCIA2:37:03:A0 R510_00T_BudiusAP_Shiftam
		R510_Shetty	D8:38:FC:18:FC:D0	192.168.100.77	zigbee	20	NA		Û	(41) D8:38:7C-18:7C:00 RadiasAP
		H510_Shetty	30:87:D9:14:69:00	192.168.100.62	ble	NA	5 days, 3:29:55	Q	î	40 H510_Shetty (kontakt:Ruckas800001 (30:87:07:14:68:00
		SM-AP	30:87:D9:15:40:40	192.168.100.58	zigbee	20	2 days, 0:05:36	Q	Û	(AL) (548-AP) (32,877,095,152,402,40)
		H510-RuckusAP-Shriram	0C:F4:D5:1E:97:D0	192.168.100.92	zigbee	19	5 days, 3:49:27	Q	<b>B</b>	All 00:194105:10:97.00 (H510-Backson-Shriram)
		R610_AP_Shriram-test	84:79:C8:01:F0:30	192.168.100.54	zigbee_aa	16	5 days, 2:32:23	Q	Î	(41) 8610_AP_Shrinam-test 84.795.08.01:78:30

#### 2. Click Pre-Approve IoT APs.

The Pre-Approve IoT APs page is displayed.

3. To add a single IoT AP, click **Single**.

FIGURE	88	Adding	а	Single	IoT	AP
INCOME	00	/ uumb	u	Single	101	<i>/</i> · · ·

MAC *		
0E:0D:6F:00:0F:00		
Tag		
Add new tag		

4. Enter the MAC address of the IoT AP and click **Save**.

The IoT AP is now added to the IoT AP list.

#### NOTE

To add multiple IoT APs, click **Batch** and download the CSV template. Enter the required details in the CSV template and click **Upload**.

FIGURE 89 Adding a Batch of IoT APs

Pre Approve IoT APs Single Ba	itch
Download CSV Template	
Choose File No file chosen	
Cancel	Upload

### **Editing an IoT AP**

The administrator can edit an IoT AP to change its settings and name. Edits can be made on a single IoT AP or on IoT APs in bulk.

### Single IoT Access Point Mode

You can use Single IoT Access Point Mode to edit a single IoT AP.

Complete the following steps to edit a single IoT AP.

1. From the main menu, click IoT APs.

A list of selected IoT APs is displayed.

2. Click an IoT AP to edit.

#### FIGURE 90 Single IoT AP Mode

IoT AP Selected	Pre-Approve	e loT APs					ibeacon × baas × eddystor	e × kontakt × R730-Shriram ×	
[ga16-clust-qa]	Ö	Name	MAC ID	IP Address	Protocols	Up	Add new tag		(Apply)
[ jackjack ] [ ga151-clust ]		RuckusAP	30:87:D9:14:6A:00	172.29.116.56	BLE	3 days	IoT APs Settings		
[Burst-const]		R610(@deSk)[121]	84:79:C8:04:E6:F0	10,74,136,230	BLE	3 days	IP	172.29.124.31	
		H510-desk-15	D8:38:FC:25:C4:C0	10.74.136.16	ZIGBEE	3 days			
		R730-Shriram	18:7C:08:20:DC:F0	172.29.124.31	BLE, ZIGBEE		MAC	18:7C:0B:20:DC:F0	
	0	RuckusAP	B4:79:C8:04:D9:40	172.29.124.40	ZIGBEE	3 days	Net Mask	255.255.252.0	
							DNS	10.10.10.106	
		T310-Shriram	18:48:0D:22:A1:90	172.29.124.52	ZIGBEE_AA	2 days	loT version	1.5.1.0.15029	
		R730-Manoj	18:7C:08:20:EB:E0	172.29.116.28	BLE, ZIGBEE		1.10.112		
		R750-Shriram	84:79:C8:3E:72:00	172.29.124.34	BLE, ZIGBEE	2 days	Radio Info		
		H510-Shriram	0C:F4:D5:1E:97:D0	172.29,124.215	ZIGBEE		Radio 0 Radio 1		
		R510-Shriram	EC:8C:A2:37:03:A0	172.29.124.35	BLE	0 days	Mode	BLE	Apply )
							Set Tx Power (BLE)	10	Apply)
							loT Radio MAC	00:0D:6F:FF:FE:8B:88:AF	(1444)
							IoT Radio Mode	ble	

Existing information displays, and the following options can be edited:

- Add New Tag
- Scan for IoT Devices
- Restart IoT Service
- IoT AP Approve
- Mode (Zigbee, BLE, Zigbee Assa Abloy)
- IoT Coexistence
- Set Channel
- Set TxPower
- IoT Management VLAN
- AP Firmware
- AP Model

In addition, the status of the IoT AP module is available, such as network information, IoT AP module information, and properties.

- 3. Click IoT Management VLAN to configure the VLAN mode.
- 4. Select **ONLINK** to configure the VLAN within the same network.
- 5. Select **OFFLINK** to configure the VLAN within different network or different region.

# Adding Tags to an AP

The AP tags are a way of grouping APs together by applying identifying tags. If the **Globally enable connector on all valid APs** is disabled when activating a plugin, complete the following steps to add tags to an AP to activate a plugin on the AP.

1. From the main menu, click **IoT APs**.

A list of IoT APs is displayed.

2. Select an IoT AP.

#### NOTE

You can select one or more APs to add tags.

#### FIGURE 91 Selecting an AP to Add Tags

1 IoT AP Selected	Pre-Approv	ve loT APs							Batch Actions:	Select		Apply	) (2
▶ [ 5112-karthik ]		Name	MAC ID	IP Address	Protocols	Uptime	Acti	ons		<ul> <li>Select</li> <li>Scan For Devices</li> <li>DeApprove</li> </ul>			
[QA-SLR-Clust]		SM-AP	30:87:D9:15:40:40	192,168,10,21	ZIGBEE	3 days, 21:42:13	٩	8	All H510-BLE-RoyalPark				
	<b>2</b> •	RuckusAP	EC:8C:A2:37:03:A0	192,168.10,171	ZIGBEE	2 days, 23:52:07	٩	â	All RuckusAP	Add Tags Remove			
		R730_Shetty	18:7C:0B:20:DC:F0	192.168.10.63	ZIGBEE, BLE	2 days, 23:32:46	Q	ŵ	All revogi RuckusAP	beacon eddystone baas			
		R510_Shetty	D8:38:FC:18:FC:D0	192.168.10.177	ZIGBEE	3 days, 22:29:17	Q	ŵ	All revogi RuckasAP	ibeacon eddystone baas			
		Karthik-R510-Desk	D8:38:FC:1C:10:90	10.74.136.40	ZIGBEE	NA		曲	All Karthik-R510-Desk				
		R610(@deSk)[121]	84:79:C8:04:E6:F0	10.74.136.45	BLE	2 days, 23:00:28	Q	8	All kontakt revogi ed	klystone R610(øde5k)[121]	beacon	baas	
		H510-desk	D8:38:FC:25:C4:C0	10.74.136.46	BLE	2 days, 23:00:32	Q	ŵ	All kontakt H510-desk	revogi eddystone ibeacor	baas		
		R730_Wriot_Shetty	20:58:69:11:0E:30	192,168,10.52	ZIGBEE, BLE	NA		ŵ	All kontakt RuckusAP	eddystone (ibeacon ) baas			
		H510_Shetty	30:87:D9:14:69:00	192,168,10,71	ZIGBEE_AA	NA		亩	All kontakt Beacon	RuckusAP eddystone baas			
		R730_QA-Test-1	18:7C:0B:20:EB:E0	192.168.10.105	BLE, ZIGBEE_AA	NA		畲	All kontakt (Beacon)	oddystone ( R730_silk_board )	baas		

3. Select Add Tags from the Batch Actions list.

4. Click Apply. The Add Tags on Selected IoT APs page is displayed. Enter the tag name in the field Add new tag field and click Add.

#### FIGURE 92 Adding a Tag

IoT AP Selected	(Pre-Appr	ove IoT APs					Add new tag	A
[5112-karthik]		Name	MAC ID	IP Address	Protocols	Uptin		
[QA-BLR-Clust]	0.	SM-AP	30:87:09:15:40:40	192.168.10.21	ZIGBEE	3 days, 21		
	2 .	RuckusAP	EC:8C:A2:37:03:A0	192.168.10.171	ZIGBEE	2 days, 23		
	0 •	R730_Shetty	18:7C:08:20:DC:F0	192,168,10.63	ZIGBEE, BLE	Z days, 23		
		R510_Shetty	D8:38:FC:18:FC:00	192.168.10.177	ZIGBEE	3 days, 22		
	0 .	Karthik-R510-Desk	D8:38:FC:1C:10:90	10.74.136.40	ZIGBEE	NA		
	0.	R610(@deSk)[121]	B4:79:C8:04:E6:F0	10.74.136.45	BLE	2 days, 23		
	0 .	H510-desk	D8:38:FC:25:C4:C0	10.74.136.46	BLE	2 days, 23		
	0.	R730_Wriot_Shetty	20:58:69:11:0E:30	192.168.10.52	ZIGBEE, BLE	NA		
	0.	H510_Shetty	30:87:09:14:69:00	192,168,10,71	ZIGBEE_AA	NA		
	0 .	R730_QA-Test-1	18:7C:08:20:EB:E0	192.168.10.105	BLE, ZIGBEE_AA	NA		

To activate a plugin, you must label the plugin with the respective tag name. The following table lists the plugins and corresponding tag names.

#### TABLE 5 Plugins and Corresponding Tag Names

Plugin	Tag Name
Kontakt.io Beacons	kontakt
iBeacon	ibeacon
Beacon as a Service	baas
Eddystone	eddystone
BLE Scan	blescan

# **Approval of IoT APs**

The IoT APs must be approved by the administrator. The RUCKUS I100 IoT Module is activated only for approved APs. There is an option to disapprove a previously approved AP. This operation can be performed on a single AP (using Single IoT Access Point Mode) or on multiple APs (using Bulk AP Mode).

### **Exporting IoT APs to CSV**

You can export IoT APs to CSV by clicking **Export IoT APs to CSV**, which allows to download all the APs in the IoT APs page, and the corresponding information into a CSV format file that can be saved.

T Access Points										۹ (	
IoT AP Selected	Pre-Approve IoT	Φ <u>5</u>						Batch Actions:	Select	*	Apply (
No Data Jewiable ]	0	Name	MAC ID	IP Address	Protocols	Uptime	Actions		Tags		
	•	RuckusAP	20:58:69:11:09:10	192.168.29.154	BLE, ZIGGEE	t days, 5:17:00	Q 🗊	(Al) (Buttour) (konski) (beston) (e	ddystane baas blescan		
tal IoT APs : Export IoT APs to	CSV )							isplaying 10 + gr	Revenue.	< Previous	Next

# **Managing Devices**

•	Devices Overview	. 93
•	Managing OSRAM Light Bulbs	. 96
•	Managing an Assa Abloy Lock	
•	Managing the Dormakaba Locks	. 98

### **Devices Overview**

The RUCKUS IoT Controller requires explicit user approval of devices. Only an approved device can be allowed into the IoT infrastructure.

To add devices to the RUCKUS IoT Controller or to view the beacons for an AP, from the main menu, click IoT Devices.

The **IoT Devices** page shows the following items:

- A list of devices
- The operations on devices (such as remove, blacklist, and device-specific operations)

#### FIGURE 93 IoT Devices Page

13

Device Selected	Devices	Beacons ) ( Pre-Appro	ve IoT Devices					Batch Actions:	Select		Apply (
is Data Available ]	0	Name	MAC ID	IOT AP MAC	Protocol	Type	LQI	R551	Last Seen	Action	Tags
		Telko PIRD1	001031000011100037110	20:58:69:11:09:10	zigbee	IAS Zone	66	-58	5 minutes ago	0 8	All Telko-Pil
	0 •	Telko-Pi802	00:0A/80:00:11:00:30:4E	20:58:69:11:09:10	zigbee	145 Zone	63	-60	8 minutes ago	Ø	AE Telto P
	0.	Telko Pill03	0010430000111001331F3	20(58:69:11:09:10	rigbee	LAS Zone	n	-54	5 minutes ago	0 1	AE Telto-PS
	•	ST-Button	18:60:97:90:01:08:43:20	20:58:69:11:09:10	zigbee	IAS Zone	72	-54	10 minutes ago	Ø	AE ST-Bette
	0 •	ST-water	28:60:97:00:01:08:08:24	20:58:69:11:09:10	righer	IAS Zone	50	-62	6 minutes ago	0 1	All Stwate
		ST-Pilk	28160197100101106148:17	20:58:69:11:09:10	zigbee	1AS Zone	77	-51	5 minutes ago	0 8	AL STOR
	0.	Telko-Door	00104180100110100150136	20:58:69:11:09:10	zigbee	LAS Zone	45	-71	3 hours ago	0 8	All Telto-De
		eria-motion	00:15:80:00:01:A6:09:34	20:58:69:11:09:10	zigber	IAS Zone	36	-77	23 minutes ago	ØB	All Ceria-ma
tal Devices : 8 Export IoT Devic	es to CSV )						Disp	aying (10 + d	evices	< Previou	s Next

The device scan operation must be performed to start the device discovery process on the gateway. Upon starting device discovery, a dialog box is displayed, as shown in the following figure.

#### FIGURE 94 Device Discovery Dialog Box

Scan Started at 14 July 2019 23:51:46 and will automatically end at 15 July 2019 11:51	1:46	Stop Scanning
IOT AP Scanning for Devices : H510-QA-Test		
Scanning For Devices/Sensors Please Wait		

A device gets added to the RUCKUS IoT Controller through Discover IoT Devices operations. If a device is pre-approved, the discovered device automatically joins the list of discovered devices. If the discovered device is not pre-approved, then you must select **Accept** or **Blacklist**. If the device is accepted, it joins the list of discovered devices.

#### FIGURE 95 Adding Device After Discovery

Scan Started at 14 July 2019 23:56:54 and will automatically end at 15 July 2019 11:56:54 IOT AP Scanning for Devices : H510-QA-Test									
Name *	Manufacturer	MAC Address	Protocol	Radio MAC	IoT AP MAC	Actions			
Enter Device Name	05RAM	7C:80:3E:AA:00:A4:50:08	zigbee	90:FD:9F:FF:FE:7C:2D:08	0C:F4:D5:1E:97:D0	(Accept) (Blacklist)			
Enter Device Name	OSRAM	84:18:26:00:00:07:AB:55	zigbee	90:FD:9F:FF:FE:7C:2D:08	0C:F4:D5:1E:97:D0	(Accept ) (Blacklist			

The Beacons page shows the list of beacons for the selected AP.

#### FIGURE 96 Beacons Page

	(Devices) Beacons				
► [ QA-BLR-Clust ]	IoT AP	Beacon Info			
	0C:F4:D5:1E:97:D0	Vendor ID : 0x004C ( 4 Latitude : 0 Longitude : 0	15)		
		Device MAC	Last Seen	RSSI	Data
		00:00:2C:B4:3A:1A:22:BE	a few seconds ago	-81	02011A0BFF4C000906032C00000000
		00:00:2C:84:3A:1A:22:BE	a few seconds ago	-83	02011A0BFF4C000906032C00000000
		00:00:D5:7C:FF:20:F8:93	a few seconds ago	-72	0201061AFF4C000215F7826DA64FA24E9880248C5B71E0893E897E0083
		00:00:C5:D5:A5:C8:6C:B1	a few seconds ago	-78	0201061AFF4C000215F7826DA64FA24E9880248C5871E0893E6D608F43
		00:00:F8:DA:65:7E:5F:9D	a few seconds ago	-76	0201061AFF4C000215F7826DA64FA24E9880248C5B71E0893E42C5A64F
		00:00:F1:83:5D:72:C9:33	a few seconds ago	-65	0201061AFF4C000215F7826DA64FA24E9880248C5871E0893E17BF0E0F
		00:00:F1:83:5D:72:C9:33	a few seconds ago	-64	0201061AFF4C000215F7826DA64FA24E9880248C5871E0893E17BF0E0F
		00:00:F1:83:5D:72:C9:33	a few seconds ago	-61	0201061AFF4C000215F7826DA64FA24E9880248C5871E0893E178F0E0F
		00:00:F7:85:E7:B5:18:16	a few seconds ago	-78	0201061AFF4C000215F7826DA64FA24E9880248C5B71E0893E2F870E08
		00:00:FE:0A:A0:AC:80:DA	a few seconds ago	-64	0201061AFF4C000215F7826DA64FA24E988024BC5B71E0893EEC13910F
		00:00:FE:0A:A0:AC:80:DA	a few seconds ago	-59	0201061AFF4C000215F7826DA64FA24E9880248C5871E0893EEC13910F
		00.00.05.01.10.16.00.01	a far an an a far a second	10	

The **Export IoT Devices to CSV** will allow to download all the Devices in the IoT devices page and corresponding information into a CSV format file which can be saved.

#### FIGURE 97 Exporting IoT Devices to CSV

Design of the second	Devi	-	acons) (Pre-Approv	a lat conduct )						Batch Actions:	Select	1	Apply
Device Selected	DOVI	66	acons Pre-Approv	e tot bevices j	24022114					batch Actions:	Select		• Apply
No Dute Available 1	0		Name	MAC ID	IoT AP MAC	Protocol	Туре	LQI		RSSI	Last Seen	Acti	
	0	•	Telko-P1R01	00x04r80x00r11x00r37r10	20158:69:11:09:10	zigbee	1AS Zone	65		-58	5 minutes ago	0	all Telks
	0	•	Telko-PiR02	00:0A:80:00:11:00:30:4E	20:58:69:11:09:10	righee	IAS Zone	63		-60	é minutes ago	0	ii Al Tella
	0	•	Tetko-PIR03	00:04:00:00:11:00:33:F3	20158:09111:09110	rigbee	t45 Zone	72		-54	5 minutes ago	0	
	0	•	ST-Button	28:60:97:00:01:08:43:20	20:58:69:11:09:10	ziptee	145 Zone	72		-54	10 minutes ago	ø	Ê (Al) 5746
	0	•	ST-water	28:40:97:00:01:08:06:24	20158:69:11:09:10	zigter	IAS Zone	53		-63	6 minutes ago	0	
	0		ST-PIR	28:60:97:00:01:06:A8:17	20:58:69:11:09:10	zigbee	IAS Zone	77		-51	5 minutes ago	0	-
	0		Telko Door	00:04:30:00:10:00:90:18	20:58:69:11:09:10	ziptee	UAS Zone	45		-71	3 hours age	0	E All Telks
	0		eria-motion	00:15:50:00:01:46:09:34	20:58:69:11:09:10	zigber	145 Zone	36		-77	23 minutes ago	0	11 AII (miat
tal Devices : Export IoT Devic	es to CSV								Displaying	(10 + ) device	5	¢ Prev	ious Next

# **Managing OSRAM Light Bulbs**

To discover OSRAM light bulbs, complete the following operations.

- 1. Ensure that the bulb is in the OFF state.
- 2. Switch on the power for five seconds.
- 3. Switch off the power for two seconds.
- 4. Repeat steps 2 and 3 five times.
- 5. Switch on the power.

The OSRAM light bulb on the Reset/Initiate discovery blinks blue, green, and red, and then the light bulb remains on.

FIGURE 98 Managing OSRAM Light Bulb

> [QA-Cluster]       IoT Device Name       IoT Device NAC       IoT AP MAC       Protocol       Type         > [Test-upgrade]       aasf       00:08:57:FF:EE:18:38:64       0C:F4:D5:1E:3C:40       zigbee       Smart plug       7C:B0:3E:AA:00:A4:5E:69 × (4 × A         > s1       00:13:7A:00:00:01:E8:58       0C:F4:D5:1C:52:50       zigbee       IAS Warning Devic       Add new tag	[ QA-Cluster]       ioT Device Name       ioT Device MAC       ioT AP MAC       Protocol       Type         [ assf       00:08:57:FF:E1:B:38:64       0C:F4:D5:1C:52:50       zigbee       Smart plug       Add new tag         [ s1       00:15:80:00:01:DE:E4:E0       0C:F4:D5:1C:52:50       zigbee       Color Dimmable Lig         [ s2       00:05:6F:00:D5:24:20:CE       0C:F4:D5:1C:52:50       zigbee       Color Dimmable Lig         [ yale       00:00:6F:00:D5:24:20:CE       0C:F4:D5:1C:52:50       zigbee       Smart plug         Level Control       255         Basic       255         Basic       0C:Color Control       255         Basic       0C:Color Control       0C:RAM         Color Control       0C:rentX       54         PimarySY       0	Apply	١)	Osram	IoT Device Name					-Approve IoT Devices	Pre-	Device Selected
aast       00:00:03/FF:FE:15:35:04       00:F4:D5:1E:32:50       zigbee       SMART plug         is1       00:13:7A:00:00:01:E8:58       0C:F4:D5:1C:52:50       zigbee       LAS Varning Devic         is2       00:15:80:00:01:DE:EA:EC       0C:F4:D5:1C:52:50       zigbee       Color Dimmable Lig         iyale       00:00:6F:00:05:24:20:CE       0C:F4:D5:1C:52:50       zigbee       Smart plug         Level Control       CurrentLevel       255         Basic       ZCL Version       1 (Version)         PowerSource       Mains (single phase) (1)         Manufacturer Name       00SRAM         Color Control       CurrentX       54         CurrentX       54         PrimarySY       0	aast 0000037FFFFE1033894 0C1F41031E32C40 2ggee Smart pug   i s1 001337A0000011E838 0C1F410511C52250 zigbee IAS Varning Devic   i s2 0015153000011E1EAEC 0C1F410511C52250 zigbee Color Dimmable Lig   i yale 00:00:6F:00:05:24:20:CE 0C:F4:05:1C:52:50 zigbee Smart pug   i yale 00:00:6F:00:05:24:20:CE i yale Smart pug   i yale 00:00:6F:00:05:24:20:CE yale Smart pug   i<	) (Apply)	:D5:1C:52:50- RuckusAP   🗸 🔪	0C:F4:D5:1C:52	IoT AP	Туре	Protocol	IoT AP MAC	IoT Device MAC	IoT Device Name		▶ [ QA-Cluster ]
s2 00:15:80:00:01:DE:EA:EC 0C:F4:D5:1C:52:50 zigbee IAS Zone   o Osram 7C:80:3E:AA:00:A4:5E:69 0C:F4:D5:1C:52:50 zigbee Color Dimmable Lig   o yale 00:0D:6F:00:05:24:20:CE 0C:F4:D5:1C:52:50 zigbee Smart plug   Level Control 255   Basic 255   Basic 255   Basic 255   DowerSource Mains (single phase) (1)   Manufacturer Name 005RAM   Color Control CurrentX   CurrentX 54   PrimarySY 0	S2 00:15:80:00:01:DE:EA:EC 0C:F4:D5:1C:52:50 zigbee Color Dimmable Lis oram 7C:80:3E:A4:00:A4:5E:69 0C:F4:D5:1C:52:50 zigbee Color Dimmable Lis organe 00:00:6F:00:05:24:20:CE 0C:F4:D5:1C:52:50 zigbee Smart plus Backlist Device: Device Information Level Control CurrentLevel 255 Basic Color Control Color Control Color Control CourrentX 641 PrimarySY 0 PrimaryAX 0 CurrentY 22			s4 ×	7C:B0:3E:AA:00:A4:5E:69 ×	Smart plug	zigbee	0C:F4:D5:1E:3C:40	00:0B:57:FF:FE:1B:3B:64	aasf		[Test-upgrade]
Image: Control       Control         Image: Control       CurrentLevel         Image: Control       Control         Image: Control       CurrentLevel         Image: Control       CurrentX         Image: Control       CurrentX <td>Image: Control       Control         Image: Control       Color Control</td> <td></td> <td></td> <td></td> <td>Add new tag</td> <td>IAS Warning Devic</td> <td>zigbee</td> <td>0C:F4:D5:1C:52:50</td> <td>00:13:7A:00:00:01:E8:5B</td> <td>s1</td> <td></td> <td></td>	Image: Control       Control         Image: Control       Color Control				Add new tag	IAS Warning Devic	zigbee	0C:F4:D5:1C:52:50	00:13:7A:00:00:01:E8:5B	s1		
Image: Soram       7C:80:3E:AA:00:A4:5E:69       0C:F4:D5:1C:52:50       zigbee       Color Dimmable Lig         Image: Soram       00:0D:6F:00:05:24:20:CE       0C:F4:D5:1C:52:50       zigbee       Smart plug       Device Information         Image: Soram       Viewer Soram       Viewer Soram       255         Basic       ZCL Version       1(Version)         Power Source       Mains (single phase) (1)         Manufacturer Name       OSRAM         Color Control       CurrentX         CurrentX       54         PrimarySY       0	yale 00:00:6F:00:05:24:20:CE 0C:F4:D5:1C:52:50 zigbee Smart plug   Level Control 255   Basic ZCL Version 1(Version)   PowerSource Mains (single pha Manufacturer Name OSRAM   Color Control CorrentX 54A   PrimarySY 0 PrimarySY 0   PrimarySY 0 PrimarySY 0   PrimaryAX 0 CurrentY 22	(Apply)	Off		Blacklist Device:	IAS Zone	zigbee	0C:F4:D5:1C:52:50	00:15:8D:00:01:DE:EA:EC	s2		
Juc       Outpoint noncont montanes in pope       Inter page         Level Control       CurrentLevel       255         Basic       ZCL Version       1(Version)         PowerSource       Mains (single phase) (1)         Manufacturer Name       OSRAM         Color Control       CurrentX       54         PrimarySY       0	Juc       Outputs totable contribution ingene interprete         Level Control       255         Basic       Imagene interprete         ZCL Version       1(Version)         PowerSource       Mains (single pha Manufacturer Name)       OSRAM         Color Control       Imagene interprete       0         PrimarySY       0       0         PrimarySY       0       0         CurrentY       22       1					Color Dimmable Lig	zigbee	0C:F4:D5:1C:52:50	7C:B0:3E:AA:00:A4:5E:69	Osram		
CurrentLevel 25   Basic 7.00   ZCL Version 1(Version)   PowerSource Mains (single phase) (1)   Manufacturer Name □OSRAM   Color Control 1000000000000000000000000000000000000	CurrentLevel 255   Basic 1/(vrsion)   CLVersion 1/(vrsion)   PowerSource Mains (single phane)   Manufacturer Name 0   Color Control 1   CurrentX 54   Primary5Y 0   Primary4X 0   CurrentY 22				Device Information	Smart plug	zigbee	0C:F4:D5:1C:52:50	00:0D:6F:00:05:24:20:CE	yale		
Basic       ZCL Version     1(Version)       PowerSource     Mains (single phase) (1)       Manufacturer Name     □OSRAM       Color Control     CurrentX       CurrentX     54       Primary5Y     0	Basic       I/(Version)         ZCL Version       1/(Version)         PowerSource       Mains (single phanistraturer Name)         Color Control       Color Control         CurrentX       54         PrimarySY       0         QurrentY       22	-			Level Control							
ZCL Version     1(Version)       PowerSource     Mains (single phase) (1)       Manufacturer Name     □OSRAM       Color Control     CurrentX       CurrentX     54       Primary5Y     0	ZCL Version       1(Version)         PowerSource       Mains (single phanolitic)         Manufacturer Name       □OSRAM         Color Control       CurrentX         Primary5Y       0         Primary4X       0         CurrentY       22		255		CurrentLevel							
PowerSource Mains (single phase) (1) Manufacturer Name □OSRAM Color Control CurrentX 54 Primary5Y 0	PowerSource Mains (single pha Manufacturer Name □OSRAM Color Control CurrentX 54 Primary5Y 0 Primary4X 0 CurrentY 22	-			Basic							
Manufacturer Name     □OSRAM       Color Control     □CurrentX       CurrentX     54       Primary5Y     0	Anufacturer Name CosrAM Color Control CurrentX 54 Primary5Y 0 Primary4X 0 CurrentY 22		1(Version)		ZCL Version							
Color Control       CurrentX     54       Primary5Y     0	Color Control CurrentX 5 0 Primary5Y 0 CurrentY 22	e) (1)	Mains (single phase) ( 1		PowerSource							
CurrentX         54           Primary5Y         0	CurrentX 54 Primary5Y 0 Primary4X 0 CurrentY 22		□ OSRAM		Manufacturer Name							
Primary5Y 0	Primary5Y 0 Primary4X 0 CurrentY 22	-			Color Control							
	Primary4X 0 CurrentY 22		54		CurrentX							
Primary4X 0	CurrentY 22		0		Primary5Y							
			0		Primary4X							
CurrentY 22	Puppank ab matter 201		22		CurrentY							
	tal Devices : 5 Primary1X 23471		23471		Primary1X							tal Devices : 5

After clicking the device, the right pane is displayed. In this pane, you can edit device configurations and device operations. To change device configurations, set the device name in the **IoT Device Name** field, select an AP association from the **IoT AP** list, select the device tag from the **Add new tag** list, and set the device blacklist from the **BlackList Device** list. Device operations depend on the device selected.

#### NOTE

In the preceding figure, the device operations are on/off, color, and brightness, because the discovered device type is an OSRAM light bulb.

# Managing an Assa Abloy Lock

Assa Abloy locks cannot be controlled using the RUCKUS IoT Controller. To discover an Assa Abloy lock and to add it in the RUCKUS IoT Controller, perform the following steps.

- 1. Swipe the AA Lock Discover Card across the lock.
- 2. Ensure that the LED blinks green.
- 3. Add the lock to the RUCKUS IoT Controller (if it is not already pre-approved).

Assa Abloy locks operate using the Visionline server. To establish the initial connection (after adding the lock) between an Assa Abloy lock and the Visionline server, perform the following steps.

- 1. Swipe the card (guest or staff card) in front of the lock.
- 2. Verify the event log from the Visionline Server Event Log to ensure that the connection is established.

#### NOTE

For more information, refer to the Visionline documentation for instructions on installing Visionline.

#### FIGURE 99 Visionline Server Event Log

1 R

~Roo	om Event I	.ist				
Ro	Regist	Time	Event	Card Name	User Group	SeqNum
102	100085	8/18/2017 6:53:00 PM	Guest Card accepted (67)	Guest (MC)	Guest	2
102	100085	8/18/2017 6:53:00 PM	A loyalty card was encoded (1264)	Guest (MC)	Guest	1
102	100085	8/18/2017 6:53:00 PM	Added a card image to the lovalty-card list (120)	Online Command	Online	0
104	100083	8/18/2017 6:52:00 PM	Guest Card accepted (67)	Guest (MC)	Guest	6
101	100084	8/18/2017 6:51:00 PM	Guest Card accepted (67)	Guest (MC)	Guest	11

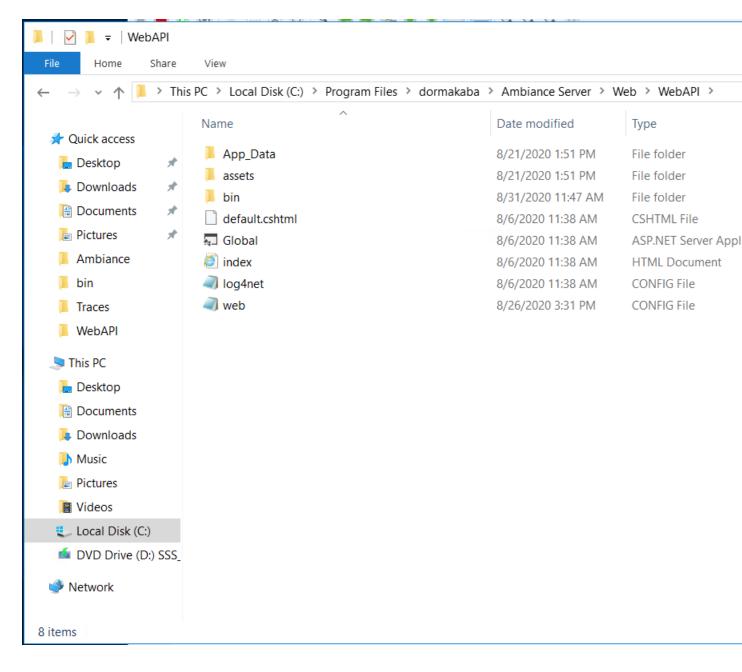
## **Managing the Dormakaba Locks**

The communication between Ambiance Server and RUCKUS IoT Controller takes place through API Endpoints.

You must configure the IP adddress of the controller by performing the following steps.

1. In the Ambiance Server, go to C:\Program Files\dormakaba\Ambiance Server\Web\WebAPI\web.config file and open the web.config file in notepad.

FIGURE 100 Locating the web config file



2. From the row, HubGatewayServiceUri value="http://10.74.136.127/", select the IP address of the controller.

FIGURE 101 Finding the IP Address

```
web - Notepad
File Edit Format View Help
    <add key="PmsRestApiURL" value="http://localhost:45226/" />
    <add key="PMSRestAPIUser" value="admin01" />
    <add key="PMSRestAPIKey" value="admin@01" />
    <add key="timeout" value="3600000" />
    <add key="ConnectionToRabbitMQRetrialCount" value="1" />
    <add key="ConnectionToRabbitMQRetrialDelayInSeconds" value="20" />
    <add key="DependencyServerRetryDelaySeconds" value="2" />
    <add key="DependencyServerRetryCount" value="5" />
    <!--Rest EndPoint URI TODO Move to syssetting-->
    <add key="HubGatewayServiceUri"
                                        value="http://192.168.0.2/" />
    <!--Log and Tracing Settings-->
    <add key="enableTracing" value="false" />
    <add key="loganet.Internal.Debug" value="false" />
<add key="logConfigFile" value="%katimavik_root%\log4net.config" />
<add key="ClientInstallationPackageLocation" value="C:\Program Files\dormakaba\Ambiance Server\Web\Ambiance Client.exe" />
<add key="ClientInstallationPackageName" value="Ambiance_Client.exe" />
<add key="ClientInstallationConfigPackageLocation" value="C:\Program Files\dormakaba\Ambiance Server\Web\serverURL.config" />
<add key="ClientInstallationConfigPackageName" value="serverURL.config" />
  </appSettings>
  <system.web>
    <trace enabled="false" pageOutput="false" requestLimit="40" localOnly="false" />
    <compilation debug="true" targetFramework="4.6.2" />
<httpRuntime maxRequestLength="1048576" targetFramework="4.5" />
  </system.web>
  <runtime>
    <ThrowUnobservedTaskExceptions enabled="false" />
    <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
       <dependentAssembly>
         <assemblyIdentity name="System.Net.Http" publicKeyToken="B03F5F7F11D50A3A" culture="neutral"/>
        <bindingRedirect oldVersion="0.0.0.0-4.2.0.0" newVersion="4.0.0.0"/>
```

### **Discovering Dormakaba Lock**

Dormakaba locks cannot be controlled using the RUCKUS IoT Controller. To discover a Dormakaba lock and to add it in the controller, perform the following steps.

- 1. Select the Gateway and start a Device Scan from Ambiance UI.
  - A scan window appears in the UI.
- 2. Swipe the DormaKaba Pairing Card across the lock.
- 3. Ensure that the LED blinks.

Dormakaba Lock details will show in the Scan Window of the contrroller.

- 4. Add the lock to the Ruckus IoT Controller (if it is not already pre-approved).
- 5. Go to Device Management page, select the Gateway, click on Next to Access Points in the Ambiance UI.

You can now verify if the lock has established its communication with Ambiance Server.

### **Blocking and Unblocking Dormakaba Lock**

Dormakaba locks operate using the Ambiance server. Complete the steps below to onboard lock.

1. Login to the Ambiance Server. The default username and password is Admin01 and Admin@01.

#### FIGURE 102 Login into Dormakaba Plugin

dormakaba 🚧	Select an application	÷				O prashant shah
	Guest Reg	istration	Reports		Staff Managen	
	Staff Keys	Property Builder	Device Management	System Keys	Access Management	Programming & Auditing
	O I TRP		J		Π	
			<	>		

#### 2. Click Device Management.

#### FIGURE 103 Selecting Device Management

Ambiance <sup>™</sup> - Device Manageme: × +		- 🗆 X
← → C () localhost/deviceMgr.html#!/		९ ☆ 🛛 :
dormakaba 🚧 🛛 Device Management 🗸 🗸	Proshort shah 🗸 🛃	्र ? 🗅
Device Management > SELECT A DEVICE TYPE		
Device Management		
Encoders Configure encoders to encode and read keys		
Gateway Configuration Configure gateways for online communication		
Registered Gateways & Paired Access Points Manage registered gateways and paired access points		
	Please select an option.	

3. Click Register Gateways & Paired Access Points.

FIGURE 104 Selecting Register Gateways and Paired Access points

Marka Ambiance™ - Device M	Managemer × +						-	
$\leftrightarrow$ $\rightarrow$ $\bigcirc$ $\bigcirc$ loc	alhost/deviceMgr.html#	#!/					Q \$	0:
dormakaba 🚧	Device Management	~				Proshant shah	t) ∞ ;	
	oont > D GATEWAYS & PAIRED	ACCESS POINTS						
▼ METRICS								C
٢.	ONLINE GATE		ONLINE	) 12.5% ACCESS POINTS - 1/8	LOW	0% / BATTERY - 0/8	>	
√ Gateways	Pairing ON	•	Send Command		Search by Gateway name, IP address or N	AC address	III ©	0 C
Gateway †		Status	Туре	MAC Address	IP Address	Antenna		Lost
Gateway-8CFE74		<u>.</u>	dormakaba Gateway	8CFE741071A0	192.168.0.4	Pairing OFF		10/
Gateway-B479C8 Gateway-C803F5		¥ ¥	dormakaba Gateway dormakaba Gateway	B479C81E60C0 C803F5109440	192.168.0.2	Pairing OFF Pairing OFF		10/
Gateway-C80873		¥.	dormakaba Gateway	C8087318B840	192.168.0.2	Pairing OFF		10/1
			4					•
H 4 1 F	H						1	- 4 of 4 items
								1 Selected
	Back to device selection			Delete Gateway(s)		Next to access points		
© 2020 - Ambiance™ - 2.4.1.3	1						10/12/202	0 12:05 PM

- 4. From the Gateways, select a gateway, and from the pull down select Pairing ON and click Send Command to start the gateway in scanning mode.
- 5. Swipe RF Pairing key card.

The LED pattern blinks green LED once, and amber colour LED thrice.

- 6. Lock will appear in IoT Controller's Scan Window, give name to the Lock and click Accept.
- 7. Select the same Gateway, from pull down menu and select Pairing OFF, and click Send Command to stop pairing.

8. Click Device manager > Registered Gateways & Access Points, and select the Access point.

FIGURE 105 Displaying the Lock

Markance™ - Dev	ice Managemer × +						- 0	$\times$
← → C (0)	localhost/deviceMgr.html#!/						Q ☆ 9	:
dormakaba	Device Management V				Proshont shah	•	ध्य ?	ב
	gement > RED GATEWAYS & PAIRED ACCESS POINTS							
* METRICS							C	ļ
٢	ONLINE GATEWAYS - 4/4		12.5% CCESS POINTS - 1/8		LOW BATTERY - 0/8		>	
Access Point	s -Select command-	Send Command		Search by Access Po	pint nome	ز		C
Access Point		Lock profile	Gateway		Building	Floor		
105	•	RTNFC	Gateway-8CFE741071A0		Ruckus Wireless Networks	FLOOR1		
H 4 1 )	· M	4					1 - 1 of 1 it	• tems
							0 Selec	ted
		Bac	k to gateway selection					
© 2020 - Ambiance™ - 2	4.1.3						10/12/2020 12:10	PM

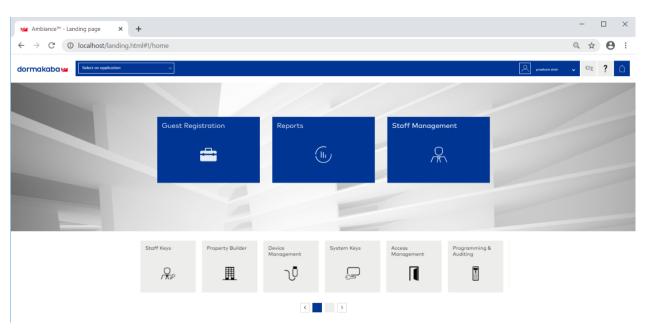
9. To confirm the lock connection, select the sage gateway, and click **Next to Access Point**.

### **Blocking the Key Remotely**

Perform the below steps to block the key remotely.

1. Go to Dormakaba Homepage.

#### FIGURE 106 Dormakaba Homepage



#### 2. Click System Keys.

#### FIGURE 107 Selecting the System Keys

C ③ localhost/systemKeys.html#!/		९ 🕁 😝
ormakaba		🔎 producer skalt 🗸 🛃 ?
Syntam Kays > SELECT A KEY TYPE		
Key Types		
Block Keys Temporarily disable all keys with a specific credential		
Cancel Keys Permanently disable a specific key		
Diagnestic Kays Callect data from lacks for troubleshooting		
Electronic Lockout Toggie Keys Disabluśnaśka ofi non-Emergency Keys		
Falsafe Keys Malio guest backup keys		
<b>hibit Keys</b> Permaniently disable all activa guest keys		
Latch Keys Disoble possoge mode in locks		
Nimary Program Kays Perform advanced operations on locks	Please select a key type.	
Reservence Keys Reservchronize a specific key		
Secondary Program Keys Neprogram a Primary Program Key		
Special Function Keys Perform system-level operations on locks		
foggle Latch/Unlatch Keys Disable/kinable possage mode		
Inblock Keys Re-enable keys that were previously blocked		

#### 3. Click Block Keys.

FIGURE 108 Selecting the Block Keys

🕍 Ambiance <sup>™</sup> - System Keys 🗙 🕂		- 🗆 ×
← → C () localhost/systemKeys.html#l/		९ ☆ 🛛 🗄
dormakabaw		🗵 e 🛃 e 🕹 🤋 🙆
ELECTAKEV TYPE		
No Yanz		
Disable gewage made in tade.  Primary Program Kaya Perform obvinced operations on tades	Please select o key type.	
Nergenoli krys Ritorichowa salanifik kry Senoday Phagan Krys Dipulgalani Artina, Trigani Kry		
Special Function Kays Pur farm system lead operations on lacks		
Toggle Late/United: Keys Diseblu/institut pressge model		
Unblock Keys Re-articles keys that were previously blocked		
Unidata Kies Endele passage mude in locka		

#### 4. Click Next to credential.

FIGURE 109 Clicking the option Next to credential

🕍 Ambiance™ - System Keys 🛛 🗙 🕂		- 🗆 ×
$\leftrightarrow$ $\rightarrow$ C ( ) localhost/systemKeys.html#!/functionKeys-main		ବ 🕁 😝 :
dormakaba		🔎 prashara talah 🗸 🏊 📍 🗋
Sime Block Keys > KEY INFO		
Key Info	Summary	
Key expiration	Key Info	
10/13/2020 01:14 PM	Key tope: Block Keys Key expiration: 10/13/2020 01:14 PM	
	Credential	
	Key Holder	
Back Next to Credentials	Make Keys	Block Køys Remotely
© 2020 - Ambiance** - 2.4.1.3		10/12/2020 01:14 PM

5. From the list, select Guest to block a Guest room.

FIGURE 110 Selecting Guest from the drop-down list

O localhost/system	Keys.html#!/func	tionKeys	-keyLis	t			Q & (
ormakaba						proshows shish	• 👌 ?
CREDENTIAL							
Electronic Lockout Toggle	•	0	ρ	Summary			
Ek Select Credential Class				Key Info			
Electronic Lockout Toggle Emergency				Key type:	Block Keys		
Grand Master				Key expiration:	10/13/2020 01:14 PM		
Guest							
Inhibit				Credential			
Limited Use Stoff							
Moster Toggle Latch/Unlatch				Key Holder			
Toggle Latch/Unistan							

6. Select a guest room number from the drop-down list to block the key.

FIGURE 111 Selecting the Guest Room Number

dormakaba 🚧				Prosibont shah v	۵ ؟
CREDENTIAL					
Guest	• \$ P	Summary			
104	Room104, Prashant104 10/09/2020 To 10/29/2020	Key Info			
105	105, Guest105 10/02/2020 To 10/17/2020 106, Guest106 10/05/2020 To 10/20/2020	Key type: Key expiration:	Block Keys 10/13/2020 01:14 PM		
	10/03/2020 10 10/20/2020	Credential			
		Guest Room access: Check-In: Check-Out: Guest(s):	Guest 105 10/02/02020 10:37 AM 10/17/0220 11:00 AM 105, Guest105		
		Key Holder			
Sort By 🎝 Name					
Back to Key Info	Next to Key Holder		Make Keys	Block Keys Remotely	

#### 7. Click Block Key Remotely.

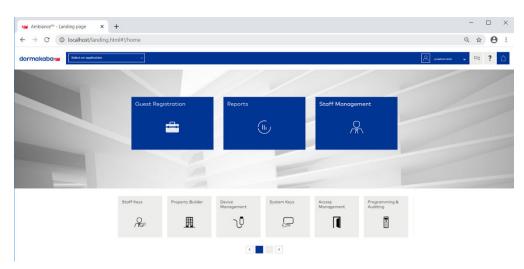
After you click **Block Key Remotely**, the LEDs will glow in the following pattern - one solid red LED, six green, and yellow LED together.

### **Unblocking the Key Remotely**

Perform the below steps to unblock the keys remotely.

1. Go to the Dormakaba Homepage.

#### FIGURE 112 Dormakaba Homepage



#### 2. Click System Keys.

#### FIGURE 113 Selecting the Unblock Keys

Markan Ambiance <sup>w</sup> - System Keys X +		- 0	×
← → C ③ localhost/systemKeys.html#!/		९ ☆ €	<b>9</b> ()
dormakabawa		R	?
Select a key type			
Key Types Black Keys Importing deable at lays with a specific credential			
Cancel Keys Premanently disable a specific key			
Dispontit Kyp Cohect data from tacks for traviblesheating			
Bischneis Lockent Toggie Keys Disobis/mable all non-Emergency Keys			
Folio/e Keys Militio gavest backupi keys			
Inhibit Keys Personnently deable of octive guest keys			
Latah Keya Disabit promoge index in looks. Primary Program Keya			
Voluny Yrdyden Key Perform Solarde aperations on lydis Resequence Keys	Pinoan salect o livy type.		
Resynchronize a specific key			
Secondary Peogram Kay Telapogoan o Intracy Troopan Kay Secold Function Kay			
Perform system feed operations on locks			
Taggle Lutch/Libitch Keys Disuble/enable possoge molo			
Unblock Klys IN-intollie keys that were previously blocked			
Unloth Keys Enable passage mode in locks			

Managing Devices Managing the Dormakaba Locks

#### 3. Click Next to Credntial.

FIGURE 114 Clicking the option Next to Credential

🚧 Ambiance™ - System Keys 🛛 🗙 🕂		
$ ightarrow$ C ( $ ilde{O}$ localhost/systemKeys.html#!/functionKeys-main		९ 🕁 😫
ormakaba 🛩		R producet shah 🗸 🚵 ?
Block Keys > KEY INFO		
Key Info	Summary	
Key expiration	Key Info	
10/13/2020 01:14 PM	Key type: Block Keys Key expiration: 10/13/2020 01:14 PM	
	Credential	
	Key Holder	
Back Next to Credentials	Molee Keys	Block Keys Remotely
Bock Next to Credentials	Moler Keys	Block Keys Remotely

4. From the list select **Guest** to unblock a guest room.

FIGURE 115 Selecting Guest from the drop-down list

Mmbiance™ - System Keys × +					-		×
← → C () localhost/systemKeys.html#!/fun	ctionKeys-keyL	ist			Q ☆	θ	:
dormakaba 🚧				Proshort shah	• 🐣	?	ב
CREDENTIAL							
Electronic Lockout Toggle      El Select Credencial Class Electronic Lockout Toggle	۹ \$	Summary Key Info					
Emergency Grand Master Guest		Key type: Key expiration:	Block Keys 10/13/2020 01:14 PM				
Inhibit Limited Use Staff Master		Credential Key Holder					
Toggle Latch/Unlatch							

5. Select a guest room number to unblock.

### 6. Click Unblock Key Remotely.

After you click **Unblock Key Remotely**, the LEDs will glow in the following pattern - one solid red LED, six green, and yellow LED together.

# **Rules Engine**

•	Rules Engine Overview	112
•	Configuring Rules	112
•	Rules-Dashboard	113

### **Rules Engine Overview**

The RUCKUS IoT Controller provides a provision to write custom rules using the Node-RED tool. The Rules Engine provides a browser-based Node-RED editor that makes design flows using the wide range of nodes in the palette. These nodes can be deployed at runtime in a single click.

### **Configuring Rules**

The RUCKUS IoT Controller allows you to configure a rule or design a flow for an AP or device by using a wide range of the nodes in the palette of Node-RED editor.

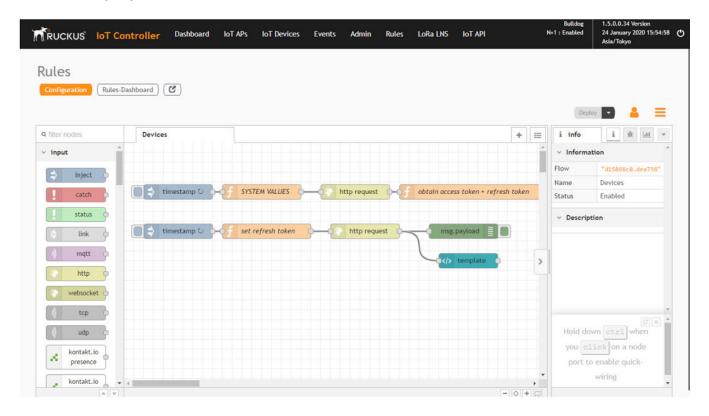
Complete the following steps to configure a rule.

1. From the main menu, click Rules > Configuration.

#### NOTE

To create the rules, refer to https://nodered.org/docs/.

FIGURE 116 Configuring a Rule



#### 2. Click the http request node.

FIGURE 117 Editing the HTTP Request Node

RUCKUS IOT Co	ntroller Dashboard IoT APs I	oT Devices Events Admin R	ules LoRa LNS IoT API	vriot-master N+1 : Enabled	1.5.0.0.12 Version 18 November 2019 22:46:5 America/Los Angeles
					lay 💽 🔒 🚍
a fliter nodes	Devices	Edit http request node		# debug	i i in
<ul> <li>input</li> </ul>		Delete	Cancel Done		T all nodes
🗧 inject 👌		© Properties		11/19/2019, 12:13:41 PM msg.payload : string[58]	node: 440b435c.9925dc
catch b	timestamp O SYSTEM	Append msg.payload as query stri	ng parameters	"{"detail":"Authen credentials were n	
status		☑ Enable secure (SSL/TLS) connection			
Link o	timestamp O	TLS Configuration TLS configur	ration •		
matt		Use authentication			
		A Type basic authentic	ation		
http		& Usernane admin			
websocket		Password			
tcp 👌					
dudp o		Use proxy			
kontakt.io		← Return a UTF-8 string	•		
resence		Name Name			

Enter the login credentials, such as username and password, in the Username and Password fields, respectively.

3. Click Deploy.

The workflow is ready to be deployed.

### **Rules-Dashboard**

The Rules-Dashboard displays the configured rules.

1. From the main menu, click Rules > Rules-Dashboard.

FIGURE 118 Rules-Dashboard

Name	MAC ID	IOT AP MAC	Protocol	Туре	LQI	RSSI	Last Se
Sample	00:00:00:00:00:00	20:58:69:38:88:F0	NA	Simple Sensor	0	0	0
20:58:69:38:88:F0	20:58:69:38:88:22	20:58:69:38:88:F0	NA	Simple Sensor	0	0	0
20:58:69:38:88:11	20:58:69:3B:B8:11	20:58:69:38:88:F0	NA	Simple Sensor	0	0	0

The Rules-Dashboard lists the configured devices.

2. Click 🙆 .

A browser opens with the Rules-Dashboard page.

- 3. Click File-Manager.
  - A File-Manager page opens
- 4. Click Upload Files.

#### FIGURE 119 Uploading Files in the File Manager

Туре	Name	Size	Last modified time	Path	Action
1	naveen	4 KB	30 January 2020 9:24:15	/VRIOT/backend/node-red-static/naveen	8
1	pradham	4 KB	30 January 2020 9:24:42	/VRIOT/backend/node-red-static/pradham	畲
2	test	4 KB	30 January 2020 9:42:24	/VRIOT/backend/node-red-static/test	Ô
<b>1</b>	images	4 KB	3 February 2020 10:40:04	/VRIOT/backend/node-red-static/images	畲
lii -	testfile	0 Bytes	30 January 2020 8:56:12	/VRIOT/backend/node-red-static/testfile	Û
1	images1	4 KB	4 February 2020 8:55:35	/VRIOT/backend/node-red-static/images1	Û
<b>1</b>	raj	4 KB	3 February 2020 10:32:09	/VRIOT/backend/node-red-static/raj	Û
1	raaga	4 KB	3 February 2020 12:21:00	/VRIOT/backend/node-red-static/raaga	Û
-	akhil	4 KB	30 January 2020 9:31:43	/VRIOT/backend/node-red-static/akhil	畲

### NOTE

The following file-formats are supported to upload the file.

- HTML
- CSS
- PNG
- JPEG
- GIF

# **LoRaWAN**

•	LoRaWAN Overview	. 115
•	Logging In to the LoRa Network	. 115
	LoRaWAN Dashboard	
•	Configuring LoRa Devices	. 117
	Configuring LoRaWAN Routers	

### **LoRaWAN Overview**

LoRa is a wireless technology used for IoT applications. LoRaWAN can be provisioned using the LoRa Network Server (LNS) that is embedded in the RUCKUS IoT Controller. The RUCKUS IoT LNS is able to communicate with LoRa routers, end devices, and as well as with LoRa application servers through its northbound interfaces.

### Logging In to the LoRa Network

LoRaWAN is a media access control (MAC) protocol for wide area networks. It is designed to allow low-powered devices to communicate with Internet-connected applications over long-range wireless connections.

Complete the following steps to access the LoRa network.

1. From the main menu, click LoRa LNS.

The LoRaWAN login page is displayed.

FIGURE 120 Logging In to the LoRaWAN

LoRaWAN			
TrackNet			<b>^</b>
	Enter your user login Enter your password	0	
	SUBMIT		

2. Enter the login credentials and click Submit.

### NOTE

The login credentials for the LoRaWAN network and the RUCKUS IoT Controller are the same.

### **LoRaWAN Dashboard**

The LoRaWAN dashboard provides the count of routers and devices connected to the LoRa Network Server (LNS) of the RUCKUS IoT Controller. It also displays the messages related to network traffic.

#### FIGURE 121 LoRaWAN Dashboard

=	Overview				Admir		<u>-</u> c	0
3	admin/TrackNet	Â						
۲	Overview						-	
	Management A		1.				L	Ra
	Kouthers 3	MANADEMENT		ANAGEMENT	_	MFBSAGES INSPECT		
	Users	Downloads:						
	Credentials Events	API specification: APIspec.	C					
	Alaming Logs	Notifications:	0					
	Paraers	No pending not fication.						
•	Messages A	• Version History:						

1. Header Panel

3. Navigation Bar

2. Main Control Panel

The following table describes the components of the LoRaWAN dashboard.

TABLE 6 Identifying the Various Components of the LoRaWAN Dashboard

Name	Components
Header Panel	Consists of the following components:
	Help icon
	Refresh icon
	Name of the user

TABLE 6 Identifying the Various Components of the LoRaWAN Dashboard (continued)

Name	Components
Main Content Panel	<ul> <li>Consists of the following components:         <ul> <li>Devices: Displays the count of LoRa devices connected to the LNS.</li> <li>NOTE</li></ul></li></ul>

### **Configuring LoRa Devices**

Before you add LoRa devices to the Lora Network Server (LNS), you must provision the device.



to provision the device.

FIGURE 122 Configuring LoRa Devices

On the **Devices** page, click

1.

≡	Devices					Admin		- C	?
SESSIONS	PROVISIONING	FINDER	0						
Ξ	Ĉ	হ	EUI	Q 00-01-00-00	-00-00-00 🔕				
0	۰	۵	0			15 # of Ro	← Add	Column	*
🔲 EUI 🛧			Туре	Version	DevAddr	Class	FCntUp	Last Uptime	
00-01-00-0	00-00-00-00		ABP	1.0	8253E	A	57	19-12-18-12:31:20	
					< 1 >				

The following example shows the configuration of the device Semtech TBDW100 Door/Window Sensor device. Different devices have different ways to configure the gateway to communicate with the LNS of the Ruckus IoT Controller.

FIGURE 123 Provisioning the Device

D	evices					
Ē	۴۹	Q F	L fi		Q 58	- <u>۵</u> Ռ-Ր. Ք-ՈՌ-ՈՌ-1Ո-
Device EUI 0C-1F-1A-	32-54-FF-F8-60					•
EUI () or	EUI range (#cn	t).	Owner			
ΟΤΑΑ			🔲 De	rivation		
Add OTAA or	ABP device.		Derive ke	ys from specified set	cret,	
1.1		- A		✓ EU863		
LoRaWAN Ve Join EUI 00-02-00-0	rsion 00-00-00-00-01	Device class		Region		
Network Key 97704E16		0CC598E802C1[	)			
App Key (Hex 94C692E9		BD4EA46E11CF	С			

- 2. Enter values for the device parameters. (Refer to the previous figure for an example.)
  - **Device EUI**: The MAC ID of the device.
  - **Owner**: Select the one who is provisioned from the list.
  - Derivation: Select the check box to derive keys from a specified secret.
  - Region: Must be U.S. or block0 (from menu).
  - LoRaWAN Version: The version number of the LoRaWAN.
  - Device class: Must be A, B, or C.
  - Join EUI: A group indicator with no actual configuration-enforcing meaning, though in a product there are conventions to follow.
  - **Network Key**: Enter the network key provided by the manufacturer.
  - App Key: Enter the application key provided by the manufacturer.
- 3. Click Add. The device is added to the LNS.

#### FIGURE 124 Device Joining the LNS

RUCKUS	IoT Contro	ller Dasht	board IoT AP	i loT Devices Evi	ents Admin Rukes	LoRa LNS IoT API			vrkit N=T : Disabled	cf73.1.5-Integrations.3146 We 4 October 2079 17:08:54 America/Los Angeles
RaWAN	4									
=	Devices							Admin	- c	0
ESSIONS P	PROVISIONING	FINDER	0							
۲	۵	٩	EUI	Q	58-40-CB-00-00-10-81-09	0				
0	٥	۰	0					15 # of flows	Add Column	
EU +				Type	Vertical	Desidate	Clare	FCettap	Last Optime	
58-A0-C8-00	00 10 81 09			OTAA	(10)	140.5719	Α.		19-10-04-15-36-26	
EUI: Dwmet: Type: Wersien: State: State: Nwk Key: App Key: Joie EUI: NwkSKeyUp: NwkSKeyUp: NwkSKeyUp: Devkddr: Devkddr:	C\$309FC4C9FF 00-02-03-03-00-00 38582C97E6A8 608F000895FE	2307A32A4D2D4 E09418FD7EC54	11618EDC IO3C8630 IOF192F3							

#### NOTE

When the FCntUp variable receives a packet, the state changes from ProV to ALIVE.

### **Configuring LoRaWAN Routers**

To add a router to the LoRa Network Server (LNS), you must provision the router.

Complete the following steps to configure the Semtech LoRa Picocell Gateway to communicate with the LoRa Network Server (LNS) in the Ruckus IoT Controller.

#### NOTE

Different routers have different ways of provisioning the gateway.

### **Preparing the Semtech LoRa Picocell Gateway**

- 1. Load PicoGW\_UI\_Release\_V1.0.3.4 and run Setup.
- 2. In the **Properties\_UI** dialog box, address the following options:
  - Select the Use a cloud network check box.
  - Click Get Gateway Unique.
  - Select the Use custom gateway ID check box.
  - Copy the ID to the copy buffer to use later in the process.
  - Change the Server address to the IP address of the TrackCentral LNS.
  - Set Port up and Port down to 1680.
  - For Tx lut, select Tx\_Lut\_15 and set the Rf power to 30 dBm (to allow the end device to join the ACK TX).

FIGURE 125 Configuring the LoRa Picocell Gateway

	k									
Server Addu	ns.eu.iot.se	emtech	n.clot 🗸	Po	rt200	000		Use a d	cloud netv	vork
ateway pro	perties									
D 353	30322E00	6300	Use cus	tom ga	tewa	y ID	$\checkmark$	Get G	lateway U	
Server addre	ess 192.16	8.0.2	Keepaliv	e interv	a10	\$	s	Forward	crc valid	true
Port up	1680	\$	Stat int	erval	30	\$	s	Forward	crc error	false
Port down	1680	\$	Push tir	neout	100	•	ms	Forward	crc disable	efalse
Radio Receive en:	Radio_ s	~	Chan Enable	Chan_				Tx lut Pa gain	Tx_Lut_C	
Туре	SX125		Radio	Radio				Mix gain	5	
Frequency	902.7	MH	IF	-400	\$	KHZ		Rf power	9	dBn
	-164 🗅	dB	BW	1250	1~	Hz		Dig gain	3	3
Rssi offset		uD								
	true 🗘	UD								
Rssi offset		MH						Selector	onfiguratio	on to

3. Select the Global Conf option, and launch the packet forwarder by selecting **Show packet forwarder console**.

FIGURE 126 Starting Packet Forwarder

PacketForwarder_UI	658-7768 🔒 🖬 Stop Share	
Global Conf Options Open Log Folder About	-	
Stor Packet Forwarder     Stor Packet Forwarder     Start saving received pack     Packet Filter     Frequency     MHz     Device address     CRC Valid	Csv delimiter	×
Channel       Image: Packet Forwarder for Windows         CR       Image:	Deplay parameters  Show packet forwarder console  Show hal b: continuous console  Show hal b: test console  Show pat b: test console  Show conf selector at starting	Gateway mode Start in DFU mode Device selection Selected device SEMTECH ProcOW Virtual ComPort (COM5) Charge device
# CR_COX: 0.00%, CRC_FAIL: 0.00%, CRC_GAIL: 0.00%         # PF packets forwarded: 0 (0 bytes)         # PUSH_DATA datagrams sent: 0 (0 bytes)         # PUSH_DATA datagrams sent: 0 (0 bytes)         # PUSH_DATA datagrams sent: 0 (0 bytes)         # PUSH_DATA acknowledged: 0.00%         ### [ODWSTREAM] ###         # PULL_DATA sent: 3 (0.00% acknowledged)         # PULL_RESP(onse) datagrams recaived: 0 (0 bytes)         # Romb       # Romk         Romb       Rook         Romb       Rook         ### [IDT] ###         #### [IDT] ###         #### [IDT] ###         #### [IDT] ###     <	` 11", "rxnb":0, "rxok":0, "rxfw":0,	'ackr":θ.θ,"dwnb":θ,"txnb":θ}}

### **Configuring the Semtech LoRa Picocell Gateway as a Router in the LNS**

Complete the following steps to configure the Semetech LoRa Picocell Gateway as a router in the LoRa Network Server (LNS).

1. On the **Routers** page, click

Ð

to configure the router.

- a) In the **Owner** field, enter the name of the owner.
- b) In the MAC address field, enter the MAC address or router ID by adding a colon between every four characters.
- c) In the Router name field, enter the name of the router.
- d) In the **Region** field, select a region from the list.

#### FIGURE 127 Configuring the Router

RUCKUS IOT Controller	Dashboard IoT APs IoT Devices	Events Admin Rules	LoRa LNS IOT API	
LoRaWAN				
				Admin
ROUTER-TABLE ROUTER-MAP				
Search	Q <b>A A</b>	8° 🖌	* 0	15
Router ID	Name/::1	Ŧ		
Crouter-1:	Owner ID 3535:3032:2E00;6300	Nar Te:	e st Router PicoCell	
	MAC address or router ID. Address or Lat,Lon Q, 0,0	Rou	ier name.	Ŧ
	US902/block0	▼ pki	wd	Ŧ
	Region	Han	lware specification	
	RxDelay		1DRoff	
	Delay for RX1/2. ADD CLOSE	Dat.	rate offset for RX1.	

LoRaWAN Configuring LoRaWAN Routers

2. Click ADD.

The router is added to the LNS.

FIGURE 128 Adding the Router to the LNS

4	oT Controller	Dashbi	oard Io1	APs loT	Devices	Events Admi	n Rules	LoRa LNS Io	T API		vriot N+1 : Disabled		itegrations.3134 2019 16:04:50 25 Angeles	versio
oRaWAN														
≡ R	outers								Adm	nin		с	?	
Search		Q	0	0	1	Q0	ý.	0	0	15	<ul> <li>Add Column</li> </ul>		*	
			-				-			# of Rows				- 1
Router ID						Name				Connected	Region			
router-1:						IsAlive System	n Health			ê	EU863			1
router-3535:30	32:2e00:6300					TestRouter				÷	US902/block	:0		
ROUTER-INFO RID: Router ID: Name: Connected: Owner: Region: GPS Location: MAC Address: GPS Location: Firmware: Firmware: #Dpw: #Down:	ROUNDTRIP-TIMES 38340236498541210 router-35353032280 TestRouter T owner-1 US902/block0 0,0000,0000 30/322E00.63/0 udp://192.168.0.32.52 Protocol Version 2 0 0	00 0:6300	IT-HISTORY	PACKET-R	ATES									
Last Uptime: Last Dntime: Last Connect:	69-12-31-16:00:00 69-12-31-16:00:00 69-12-31-16:00:00													

## **Events**

•	Viewing Events	123
•	Viewing SmartThings Event	. 124

### **Viewing Events**

An event is an occurrence or the detection of certain conditions in and around the RUCKUS I100 IoT Module. An AP rebooting, detection of a RUCKUS I100 IoT Module, module undetection, and module swap are all examples of events.

Complete the following steps to view events.

1. From the main menu, click **Events**.

The Events page is displayed.

#### FIGURE 129 Events Page

					(Download) (Clear)
Time	AP MAC	ID	Event	Message	
2020-10-14 06:51:30.895026	18:4B:0D:22:A1:90	5	Radio Message Delivery Failed	00:17:7A:01:06:03:EA:07 is not responding for command '0x00AA'	
2020-10-14 06:24:37.472023	B4:79:C8:3E:75:40	5	Radio Message Delivery Failed	0xFFFD is not responding for command '0x00FF'	
2020-10-14 05:34:27.287314	B4:79:C8:3E:75:40	5	Radio Message Delivery Failed	0xFFFD is not responding for command '0x00FF'	
2020-10-14 03:25:00.686952	C8:08:73:26:AA:D0	5	Radio Message Delivery Failed	00:0A:80:00:10:00:3D:04 is not responding for command '0x0000'	
2020-10-14 03:25:00.675017	C8:08:73:26:AA:D0	5	Radio Message Delivery Failed	00:0A:80:00:10:00:3D:04 is not responding for command '0x0000'	
2020-10-14 03:25:00.663326	C8:08:73:26:AA:D0	5	Radio Message Delivery Failed	00:0A:80:00:10:00:3D:04 is not responding for command '0x0000'	
2020-10-14 03:25:00.651257	C8:08:73:26:AA:D0	5	Radio Message Delivery Failed	00:0A:80:00:10:00:3D:04 is not responding for command '0x0000'	
2020-10-14 03:25:00.640624	C8:08:73:26:AA:D0	5	Radio Message Delivery Failed	00:0A:80:00:10:00:3D:04 is not responding for command '0x0000'	
2020-10-14 03:25:00.628133	C8:08:73:26:AA:D0	5	Radio Message Delivery Failed	00:0A:80:00:10:00:3D:04 is not responding for command '0x0000'	
2020-10-14 03:25:00.615276	C8:08:73:26:AA:D0	5	Radio Message Delivery Failed	00:0A:80:00:10:00:3D:04 is not responding for command '0x0000'	
2020-10-14 03:25:00.602752	C8:08:73:26:AA:D0	5	Radio Message Delivery Failed	00:0A:80:00:10:00:3D:04 is not responding for command '0x0000'	
2020-10-14 03:25:00.589194	C8:08:73:26:AA:D0	5	Radio Message Delivery Failed	00:0A:80:00:10:00:3D:04 is not responding for command '0x0000'	
2020-10-14 03:25:00.575277	C8:08:73:26:AA:D0	5	Radio Message Delivery Failed	00:0A:80:00:10:00:3D:04 is not responding for command '0x0000'	
2020-10-14 03:25:00.550865	C8:08:73:26:AA:D0	5	Radio Message Delivery Failed	00:0A:80:00:10:00:3D:04 is not responding for command '0x0000'	
2020-10-14 00:53:29.808857	B4:79:C8:3E:75:40	5	Radio Message Delivery Failed	0xFFFD is not responding for command '0x00FF'	

#### 2. Click Download to download the event logs file.

The event logs file contains the time of the event occurrence, its MAC address, and event name.

3. Click **Clear** to clear the log file.

## **Viewing SmartThings Event**

The Events page shows the SmartThings events from AP.

Complete the following steps to view events.

1. From the main menu, click Events.

The Events page is displayed.

#### FIGURE 130 Event page for Smartthings

Time	AP MAC	ID	Event	Message
20-12-15 07:43:49.999590	94:F6:65:2A:2A:50	200	ST Upgrade	Upgrade Success
20-12-15 07:43:49.951628	94:F6:65:2A:2A:50	200	ST Upgrade	Upgrade Success
20-12-15 07:41:37.561340	94:F6:65:2A:2A:50	6	Upgrade	Controller version 1.7.0.0.20 supports AP st firmware version 1.7.0.32.12, Gateway 94:F6:85:2A:2A:50 is in st firmware version 0 - Send upgrade.
20-12-15 07:41:37.151674	94:F6:65:2A:2A:50	6	Upgrade	Controller version 1.7.0.0.20 supports AP st firmware version 1.7.0.32.12, Gateway 94:F6:65:2A:2A:50 is in st firmware version 0 - Send upgrade.
20-12-15 07:41:17.499438	94:F6:65:2A:2A:50	6	Upgrade	Controller version 1.7.0.0.20 supports AP st firmware version 1.7.0.32.12, Gateway 94:F6:65:2A:2A:50 is in st firmware version 0 - Send upgrade.
20-12-15 07:41:17.064761	94:F6:65:2A:2A:50	6	Upgrade	Controller version 1.7.0.0.20 supports AP st firmware version 1.7.0.32.12, Gateway 94:F6:65:2A:2A:50 is in st firmware version 0 - Send upgrade.

2. Click **Download** to download the event logs file.

The event logs file contains the time of the event occurrence, its MAC address, and event name.

3. Click **Clear** to clear the log file.



© 2020 CommScope, Inc. All rights reserved. 350 West Java Dr., Sunnyvale, CA 94089 USA https://www.commscope.com