CONFIGURATION GUIDE



# **RUCKUS IoT Controller Configuration Guide**, **1.8.1.0 MR**

**Supporting IoT Controller Release 1.8.1.0** 

Part Number: 800-72981-001 Rev A Publication Date: July 2021

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

© 2021 CommScope, Inc. All rights reserved.

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

### **Export Restrictions**

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

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

### Disclaimer

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

### **Limitation of Liability**

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

### **Trademarks**

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

# Contents

	5
Contacting RUCKUS Customer Services and Support	5
What Support Do I Need?	5
Open a Case	5
Self-Service Resources	
Document Feedback	ϵ
RUCKUS Product Documentation Resources	
Online Training Resources	<i>6</i>
Document Conventions	7
Notes, Cautions, and Safety Warnings	
Command Syntax Conventions	
About This Guide	
Introduction to RUCKUS IoT Controller	
What's New in This Document	
Getting Started	
Before You Begin	
Supported Web Browsers	
Logging In to RUCKUS IoT Controller	
Getting to Know the Dashboard	
Configuring N+1	
Configuring Static Addresses for Primary and Secondary Controllers	
Configuring the N+1 Feature	
Disabling N+1	
Managing IoT Controller System Configuration	
Managing Services	
Enabling Samsung SmartThings	
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 iBeacon 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 (iBeacon, Eddystone and Custom) Activating and Editing the Beacon as a Service Plugin (React Mobile)	
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 Beacon as a Service Plugin (iBeacon, Eddystone and Custom) Activating and Editing the Beacon as a Service Plugin (React Mobile)	
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 Controller Data Stream Plugin	53 58 59 62 64
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 Controller Data Stream Plugin Activating and Editing the Dormakaba 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 Controller Data Stream Plugin Activating and Editing the Dormakaba Plugin Activating and Editing the Telkonet Plugin	53 58 59 62 64 64 66 69
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 Controller Data Stream Plugin Activating and Editing the Dormakaba Plugin Activating and Editing the Telkonet Plugin Activating and Editing the Telkonet Plugin	53 58 59 62 64 64 66 69 71
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 Controller Data Stream Plugin Activating and Editing the Dormakaba Plugin Activating and Editing the Telkonet Plugin Activating and Editing the Soter Plugin Activating and Editing the Soter Plugin	53 58 59 62 64 66 66 69 71 71
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 Controller Data Stream Plugin Activating and Editing the Dormakaba Plugin Activating and Editing the Dormakaba Plugin Activating and Editing the Telkonet Plugin Activating and Editing the Soter Plugin Activating and Editing the Soter Plugin Changing the Password	
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 Controller Data Stream Plugin Activating and Editing the Dormakaba Plugin Activating and Editing the Dormakaba Plugin Activating and Editing the Telkonet Plugin Activating and Editing the Soter Plugin Changing the Password Configuring Virtual Machines Uploading Versions and Patches	53 58 59 62 64 64 66 69 71 71 71 72 72

Backing up Rules	
Uploading the RUCKUS IoT Controller License	
Change the Settings	
Rebooting RUCKUS IoT Controller	
Resetting RUCKUS IoT Controller	
Managing IoT Access Points	81
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 of IoT APs	
Exporting IoT APs to CSV	
Managing Devices	
Devices Overview	
Managing OSRAM Light Bulbs	94
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	105
Rules Engine	
Rules Engine Overview	
Configuring Rules	110
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	
Viewing Events	
Viewing SmartThings Event	

# Preface

•	Contacting RUCKUS Customer Services and Support	5
	Document Feedback	
	RUCKUS Product Documentation Resources	
•	Online Training Resources	6
•	Document Conventions	7
•	Command Syntax Conventions	7

### **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, or go to https://www.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.

## **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.

## **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
bold text	Identifies command names, keywords, and command options.
italic 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].
λ.	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.

# **About This Guide**

# **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 1.8.1.0 MR

Feature	Description	Location	
No new features for this release.	Minor content update	Refer to topics - Backing up Files and Getting to know the Dashboard.	

# **Getting Started**

•	Before You Begin	11
•	Logging In to RUCKUS IoT Controller	. 11
•	Getting to Know the Dashboard	. 15

## **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

```
1 - Ethernet Network
2 - System Details
3 - NTP Setting
4 - System Operation
5 - N+1
6 - Comm Debugger
x - Log Off
Enter Choice: 1
   _____
Network info :
      _____
                             _____
 IP (eth0) : 10.174.112.79/23
Gateway : 10.174.112.1
 Gateway : 10
Gateway : vriot
 DNS domain
 FQDN
            : vriot
 DNS
            : 10.42.50.240 10.0.248.1
 N+1 Status : Disabled
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 Page

Initialization					
VM Configurations			IP Configurations		
Hostname vriot. Time Zone		)	рнср 🖲	Static O	
America/Santiago	Set Time Manually i •				
Optional Services					
C Rules Engine	Track Central			Samsung SmartThings	

The following optional services are listed on the Initialization page.

- Rules Engine
- Track Central
- Smasung SmartThings
- 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 **Set Time Automatically using NTP** option is not available (such as in an isolated setup), you can select the **Set Time Manually** option to disable NTP sync.

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. Click **Start**.

#### FIGURE 3 Confirming the Password

RUCKUS IoT Controller IoT A	PI			1.5.0.0.19 Version 16 December 2019 4:27:28 America/Los_Angeles
Initialization				
1.2	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.

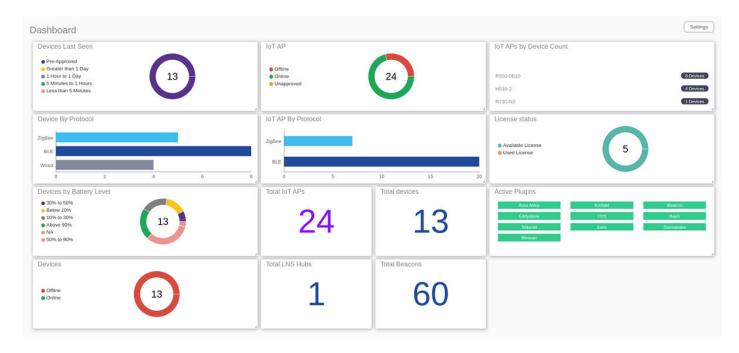
#### FIGURE 4 End-user License Agreement

ializ	End-user License Agreement	
re para	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 EMPLOYEE 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, INSTALLING AND/OR USING THE SOFTWARE, LICENSEE ACKNOWLEDGES THAT IT HAS READ THIS LICENSE AND AGREES TO BE DOUND 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 a copy 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 for the benefit of Licensee) to activate the Software or increase the Authorized Device Limit. "Ruckus Channel Partner" means an entity	
	Close	Start

## **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 5 RUCKUS IoT Controller Dashboard



#### 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.
Devices by Battery Level	Shows the status of devices that are grouped together by battery level.
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.

### Getting Started

Getting to Know the Dashboard

#### TABLE 4 Dashboard Elements (continued)

Box Name	Description	
	Shows the total of number of licenses, and the status of the licenses that are available or used by the RUCKUS IoT Controller.	

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

#### FIGURE 6 Dashboard Settings

ashboard			Dashboard Settings
Devices Last Seen	IOT AP	IoT APs by Device	Configure
Pre-Approved     Greater than 1 Day	• Offline		Edit Dashboard
1 Hour to 1 Day     5 Minutes to 1 Hours	Online     Unapproved	R550-5420	Reset Widgets
e Less than 5 Minutes		R730-N3	Refresh Interval
Device By Protocol	IoT AP By Protocol	License status	License notifications
ZigBee		_	Add Widgets
BLE	ZigBee	<ul> <li>Available License</li> <li>Used License</li> </ul>	No Widgets Available
Wired	BLE		
0 5 10	17 0 4 8	15	
Devices	Total IoT APs Total devices	Active Plugins	
	22 40	Assa Abloy Eddystone	Nontale Incession
• Offline • Online 19	23 19	Telkonet	Soter:
		Blescan	

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, License Status, Total Beacons, Total IoT APs, and Total LNS Hubs to add widgets to the Dashboard.

Ш

# **Configuring N+1**

RUCKUS IoT Controller N+1 high availability (HA) 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 controllers:

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

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

The static IP addresses of the primary and secondary controllers can be configured in two ways:

- 1. From the RUCKUS IoT Controller main menu, select Admin > VM Configurations.
- 2. Set the static addresses 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.

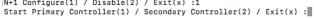
FIGURE 7 RUCKUS IOT Controller Main Menu

🚰 172.16.112.243 - PuTTY
******
Ruckus IoT Controller
Main Menu
* * * * * * * * * * * * * * * * * * * *
<pre>1 - Ethernet Network 2 - System Details 3 - NTP Setting 4 - System Operation 5 - N+1 6 - Comm Debugger x - Log Off</pre>
Enter Choice: 5
Enter Choice: 5
N+1 Status:
N+1 Mode : Disabled
<pre>8+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. * Primary Controller and Secondary Controller should have same password configured for the User admin. Enter Secondary Controller IP :

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

FIGURE 8 Continuing the Configuration

*****	******
	Ruckus IoT Controller
	Main Menu
*****	***************************************
<ol> <li>Ethernet Network</li> <li>System Details</li> <li>NTP Setting</li> <li>System Operation</li> <li>N+1</li> <li>Comm Debugger</li> <li>Log Off</li> </ol>	
Enter Choice: 5	
N+1 Status:	
N+1 Mode : Disa	
[N+1 Configure(1) / Disable(2)	/ Exit(x) :1



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

FIGURE 9 Configuring the Primary Controller

# 172.16.112.243 - PuTTY
******************
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>
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.
* Primary Controller and Secondary Controller should have same password configured for the User admin.
Party Garage days Garage 10 and 10
Enter Secondary Controller IP :

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

#### NOTE

The preferred virtual IP address must not be the same as the primary or secondary controller IP addresses.

Enter the admin password and type a preferred N+1 password

₽ 172.16.113.178 - PuTTY
Ruckus IoT Controller Main Menu
<pre>1 - Ethernet Network 2 - System Details 3 - NTP Setting 4 - System Operation 5 - N+1 6 - Comm Debugger x - Log Off</pre>
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:
<ul> <li>Primary Controller and Secondary Controller should be in same subnet and reachable.</li> <li>Primary Controller and Secondary Controller should be configured with static ip address.</li> </ul>
<ul> <li>Primary Controller and Secondary Controller should be configured with static 1p address.</li> <li>Primary Controller and Secondary Controller should be running in same version.</li> </ul>
* Primary Controller and Secondary Controller should have synchronized date/time. * Primary Controller and Secondary Controller should have same password configured for the User admin.
- Filmary controller and Secondary controller should have same password configured for the user admin.
Enter Secondary Controller IP :172.16.113.102 Enter preferred Virtual IP :171.16.113.111 Enter admin password for configuring N+1:
Enter new password for configuring N+1 New password should contain atleast 1 uppercase, 1 number , 1 Symbol and atleast 8 characters length :
N+1 will stop all services & configurations in Secondary Controller, Enter Y/N to continue :

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

FIGURE 10 Completing the Primary Controller Configuration

₽ 172.16.113.178 - PuTTY
<ul> <li>a NTP Setting</li> <li>4 - System Operation</li> <li>5 - N+1</li> <li>6 - Comm Debugger</li> <li>* - Log Off</li> </ul>
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 configured with static ip address. * 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. * Primary Controller and Secondary Controller should have synchronized date/time. * Primary Controller and Secondary Controller should have same password configured for the User admin. Enter Secondary Controller IP :172.16.113.110 Enter preferred Virtual IP :172.16.113.111 Enter admin password for configuring N+1: Enter new password for configuring N+1 New password should contain atleast 1 uppercase, 1 number , 1 Symbol and atleast 8 characters length
: 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 11 Continuing with the Secondary Controller Configuration

172.16.113.178 - PuTTY
<ul> <li>NTP Setting</li> <li>System Operation</li> <li>N+1</li> <li>Comm Debugger</li> <li>Log Off</li> </ul>
inter Choice: 5
+1 Status:
N+1 Mode : Disabled
H1 Configure(1) / Disable(2) / Exit(x) :1 tart Primary Controller(1) / Secondary Controller(2) / Exit(x) :1
+1 Configure:
o 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. Primary Controller and Secondary Controller should have same password configured for the User admin.
Enter Secondary Controller IP :172.16.113.102 Enter preferred Virtual IP :172.16.113.111 Enter admin password for configuring N+1:
Enter new password for configuring N+1 New password should contain atleast 1 uppercase, 1 number , 1 Symbol and atleast 8 characters length :
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 12 N+1 Configuration Completed

μ₽ 172.16.113.178 - PuTTY
3 - NTP Setting
4 - System Operation
5 - N+1 6 - Comm Debugger
c - comm bebugger x - Log Off
Enter Choice: 5
N+1 Status:
N+1 Mode : Disabled
N+1 Configure(1) / Disable(2) / Exit(x) :1
<pre>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.
<ul> <li>* Primary Controller and Secondary Controller should have synchronized date/time.</li> <li>* Primary Controller and Secondary Controller should have same password configured for the User admin.</li> </ul>
crammel concretes and occument concretes proved note sume baconers contraduce for one core amazin
Enter Secondary Controller IP :172.16.113.102
Enter preferred Virtual IP :172.16.113.111 Enter admin password for configuring N+1:
Enter admin password for configuring wit:
Enter new password for configuring N+1
New password should contain atleast 1 uppercase, 1 number , 1 Symbol and atleast 8 characters length
:
N+1 will stop all services & configurations in Secondary Controller. Enter $\rm Y/N$ 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 controller or active primary controller, and the secondary controller or active secondary controller, enter **5** in the **Enter Choice** field.

FIGURE 13 Verifying the IP Address of the Active Primary Controller

🛃 172.16.1	13.178 - PuTTY	
******	*******	****************
		Ruckus IoT Controller
		Main Menu
******	********	************
1 - Ethe	rnet Network	
2 - Syst	em Details	
3 - NTP	Setting	
4 - Syst	em Operation	
5 - N+1		
6 - Comm	Debugger	
x - Log	Off	
Enter Ch	oice: 5	
N+1 Stat		
	N+1 Mode	
		: 172.16.113.111
		: Active Primary Controller
		: 172.16.113.178
		troller IP : 172.16.113.102
		: Not Applicable, Controller is Active.
		: vriot(2): normal
wrigt pr	im(1): normal	
viiot_pi		
N+1 Conf	igure(1) / Dis	able(2) / Exit(x) :
Inter Com	.rgure(r) / Dro	

8. To replace the secondary controller, enter 3.

#### NOTE

While replacing the node, both controller should have same admin password and user needs to enter the password while replacing the node.

FIGURE 14 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
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) :

FIGURE 15 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** to continue the configuration.

FIGURE 16 Configuring Forced Fallback

뤋 172.16.113.178 - PuTTY	
******	***************************************
	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	
	: 172.16.113.111
	: Primary Controller
	: 172.16.113.178
_	troller IP : 172.16.113.102
ConfigSync	: 05/20/2021 08:05:03
Node Status	: vriot(2): normal
vriot prim(l): normal	
N+1 Configure(1) / Dis	able(2) / Forced Fallback(3) / Exit(x) :
···· · ····· · ···· · · · · · · · · ·	

10. To replace the primary controller, enter 3.

FIGURE 17 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 18 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 Mode : Active Secondar 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) :3 N+1 Replace : \_\_\_\_\_ Enter Primary Controller IP to replace:10.174.113.177

Replacing the primary controller has been successfully completed.

FIGURE 19 Successful 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
       Mode
       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) :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 20 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	.33
	Activating and Editing the Plugins	
•	Changing the Password	. 71
	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 21 Services

#### FIGURE 22 Managing Services Page

Admin				
				(Diagnostics)
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 start or stop.

### **Enabling Samsung SmartThings**

You can connect the Samsung Smart Hub dongle through the USB port in RUCKUS AP. The Samsung Smart Hub dongle has two radios: Zigbee and Z-Wave. The Samsung SmartThings mobile app displays the configurations, status, information, device list, and device status of the Samsung Smart Hub.

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

- 1. From the main menu, click Admin.
- 2. In the left navigation pane, click **Services**.
- 3. Click **Start** to activate the service.

#### NOTE

By default SmartThings is disabled.

#### FIGURE 23 Starting Samsung SmartThings

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	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)

4. After receiving an Upgrade Success message for the ST Upgrade event on the IoT Controller Events page, press and hold the reset button on the Smart Hub for 10 seconds.

FIGURE 24 SmartThing Device



#### **NOTE** For more information on upgrade events, refer Viewing SmartThings Event on page 122.

5. Download the SmartThings app and enter your login credentials.

#### Managing IoT Controller System Configuration

Managing Services

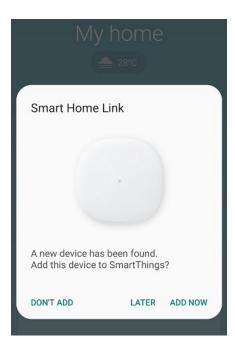
6. Connect your mobile and AP in the same network or connect the mobile to the SSID of the AP.

FIGURE 25 SmartThings User Interface

🗐 My home	+							
Study >								
Living room >								

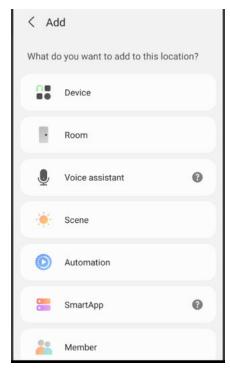
7. After the mobile device connects to Wi-Fi, click **ADD NOW** in the SmartThings device pop-up.

FIGURE 26 Connecting to Wi-Fi



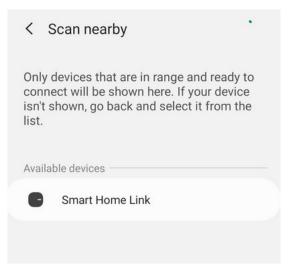
- 8. If the pop-up does not display, perform the following steps to add your mobile device to SmartThings.
  - a) Click Device and select Scan nearby.

FIGURE 27 Selecting a Device



The Smart Home link is displayed under Available devices.

FIGURE 28 Scanning for the device

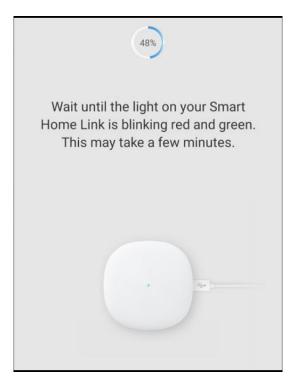


- b) Click Smart Home Link.
- c) Select the location and room for your hub and wait for your device to connect successfully.

FIGURE 29 Selecting the Location and Room for Your Hub

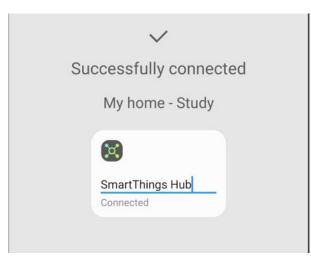
Select a location and room for Hub.	your	
Location		
My home	*	
Room		
Study	*	

FIGURE 30 Waiting for Successful Connection



d) After the hub connects successfully, rename your hub. The hub name will be displayed on the home page.

FIGURE 31 Renaming the Hub



#### FIGURE 32 Hub Name on the Home Page

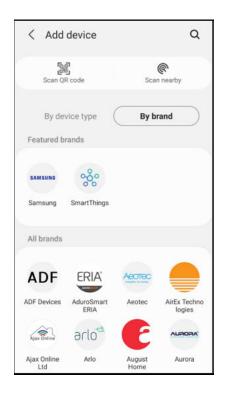
🔊 My home	+	
Study >		
SmartThings Hub Connected		
Living room >		

#### Managing IoT Controller System Configuration

Managing Services

9. Add the SmartThings hub to the app.

FIGURE 33 Locating the SmartThings Hub

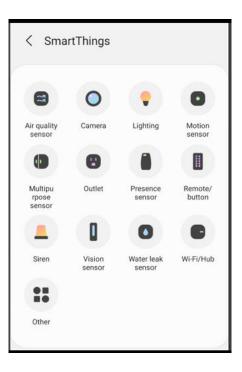


10. Click the + icon in the app and go to the **Devices** page to add the hub.

#### NOTE

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

FIGURE 34 Adding Devices to Hub



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

The IoT Access Points page is displayed.

12. Select an AP from the list. The sidebar on the right displays the SmartThings information for the selected AP, such as the hub version, dongle status, hub status, hardware version, and serial number.

FIGURE 35 SmartThings Information in the Right Pane

IoT Access Poin	ts					RuckusAP X				
0 IoT AP Selected	Pre-Approve I	oT APs				Add new tag				Apply
[ No Data Available ]		Name	MAC ID	IP Address		IoT AP Approve				Apply )
1.100	0	RuckusAP	94:F6:65:2A:2A:50	192.168.40.130	ZI	IoT Management VLA	N		Yes 🜔	Apply
						(1		ONLINK	O	
						IoT APs Settings				
						IP	192.168.40.130	0		
						MAC	94:F6:65:2A:2/	1:50		
						Net Mask	255.255.255.0			
						DNS	192.168.40.1			
						SmartThings version	1.7.1.34.12			
						SmartThings Info	ľ.			
						SmartThings Hub co	e version		34.12	
						SmartThings Dongle	status		Detected	
						SmartThings Hub sta	tus		Running	
Total IoT APs : 1 Export Io	T APs to CSV					SmartThings Hardwa	re version		1.01	

# **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, Soter, BLE Scan, Dormakaba locks, and React Mobile.

### 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.

Admin			Kontakt.io	×
			Globally enable connector on all valid APs	
Services	Select a Plugin to Activate : Kontakt.io	d	Aggregation Interval •	
Plugins			200 m	15
Account			API Key Show	~
VM Configurations	Active Plugin List		URL •	
Versions & Patches	No Plugins Found		https://api.kontakt.io	
DB Backup			Version • 9	
License				y)
Settings				_
Reset & Reboot				
		-		

#### FIGURE 36 Activating the Kontakt.io Plugin

- 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 88 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 37 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 38 Updating the Configuration Parameters

Admin				Kontakt.io	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*	
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 plugin. 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 39 Activating the Assa Abloy Plugin

Admin				Assa Abloy ③ © Globally enable connector on all valid APs Username •
Services	Select a Plugin to Activate :	Assa Abloy 📃 💌	A	
Plugins				Password •
Account	Active Plugin List			Visionline IP Address or FQDN * Enter Ip+4 address or FQDN
VM Configurations				Port*
Versions & Patches				(443 Access ID i
DB Backup				
Rules Backup				(Apply)
License				
Settings				
Reset & Reboot				
			_	

- 4. After the Assa Abloy 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 the 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 88 for more information.

- b) For Username, enter the name of the user connecting to the Visionline Server
- c) For **Password**, enter the password of the user connecting to the Visionline Server.
- d) Enter the Visionline IP address or FQDN.

#### NOTE

By default, the port number is 443.

#### 5. Click Apply.

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

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

FIGURE 40 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				
D8 Backup				
Rutes Backup				
License				
Settings				
Reset & Reboot				

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

#### FIGURE 41 Updating the Configuration Parameters

Admin				Assa Abloy Restart (Stop) (View logs)	8
Services	Select a Plugin to Activate :	Dormakaba 🛛 👻	A	III Globally enable connector on all valid APs Status: Reachable Username *	
Plugins				sym	
Account	Active Plugin List			Password •	אוכו
VM Configurations	Assa Abloy		-	*** Visionline IP Address or PQDN *	
Versions & Patches				10.174.112.29 Port *	
DB Backup				43	
Rules Backup				Access ID i soak	
License				Upd	ate
Settings					
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 42 Activating the Eddystone Plugin

Admin			Eddy	stone	$\otimes$
			Glob	ally enable connector on all valid APs	
Services	Select a Plugin to Activate :	Eddystone v	Aggreg	ation Interval	200 ms
Plugins			Vend	or 1 Vendor 2	
Account	Active Plugin List		Key •		
VM Configurations	No Plugins Found		Enter API UR		Show
Versions & Patches			Enter		
DB Backup			Port		
License			API En		/
Settings				URI (Eg /eddystone)	
Reset & Reboot			UUID F	lter	
				heartbeat i (	No (Apply)
					( Child

- 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 88 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 43 Deactivating the Eddystone Plugin

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

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

FIGURE 44 Updating the Configuration Parameters

Admin				Eddystone View logs	8
Services Plugins	Select a Plugin to Activate :	Select v (	2	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 Eddystone			Port 8800	
DB Backup				API Endpoint	
Reset & Reboot				/eddystonexox UUID Filter	
				Enter UUID	
				Enable heartbeat i /eddy_fbeacon_heart	Yes
					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 45 Activating the iBeacon Plugin

Admin			iBe	eacon	⊗
			G	Globally enable connector on all valid APs	
Services	Select a Plugin to Activate :	(iBeacon   👻	Aggr	regation Interval	200 ms
Plugins			Ve	Vendor 1 Vendor 2	
Account	Active Plugin List		Key		
VM Configurations	No Plugins Found			url.•	Show
Versions & Patches				nter URL	
DB Backup			Port		
License				nter Port	
Settings				nter URI (Eg /ibeacon)	
Reset & Reboot				D Filter	
				Iter UUID	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 88 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.

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

#### FIGURE 46 Deactivating the iBeacon Plugin

Admin		
Services	Select a Plugin to Activate : Select (Activate)	
Plugins		
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 47 Updating the Configuration Parameters

Admin				iBeacon 🛞
				View logs
Services	Colorbo Olucio de Labierte e		_	Clobally enable connector on all valid APs
Services	Select a Plugin to Activate :	Select 👻	(A	Aggregation Interval
Plugins				1000 ms
				Vendor 1 Vendor 2
Account	Active Plugin List			Status: Reachable
VM Configurations	Assa Abloy			Key *
	Kontakt.io			Show
Versions & Patches				API URL *
	Tile Denno			http://10.174.112.165
DB Backup	Trackr Demo			
	íBeacon			Port
License	Eddystone			
Settings	Controller Data Stream			API Endpoint
Jerrings	Controller Data Stream			( /ibeacon
Reset & Reboot	Beacon as a Service			UUID Filter
	Telkonet			(Enter UUID
	Soter			Enable heartbeat i
				/heartbeat
				(Update)

# 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**.

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

FIGURE 48 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	Ψ
UUID •	
0047e70a5dc147258799830544ae04f6	
Major No • i	
0102	
Minor No • i	
0000	
Tx Power Level @1m •	
0	
	Update

FIGURE 49 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 50 Activating Beacon as Service (Generic)

leacon as a Service			(
Globally enable connector on all valid APs			
dvertisement Interval *			
0			100 ms
eacon Type •			
Custom Beacon			· · · · ·
Vendor type			
Generic			
Generic			
03			•
1234			Add
ADV Type	Value	Actions	
01	0192	/ î	
			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 88 for more information.

- b) In the **Beacon Type** list, select the type of beacon.
- c) Provide relevant values for given fields based on Beacon Type. For iBeacon, a common 32 characters UUID can be given which will be applied to all APs. If Append AP MAC is checked, Controller will append 12 characters of AP MAC at the end of 20 characters UUID, so that it will be unique for every AP data.
- 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 51 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 AP 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 Strean Tx Power Level @1m • Beacon as a Service Rules Backup 0 Telkonet License Soter BLE Scan Settings Reset & Reboot

FIGURE 52 Updating the Configuration Parameters (iBeacon)

#### FIGURE 53 Updating Configuration parameters (Eddystone)

Admin				Beacon as a Service            Seacon as a Service
Services	Select a Plugin to Activate :	(Select   v)	A	Globally enable connector on all valid APs     Advertisement Interval *     Bescon Type *     Eddystone     v
Account	Active Plugin List			Namespace ID * 486815a81b09b25a41b1
VM Configurations	Assa Abloy Kontakt.io			Instance ID • 6b2441d5920
Versions & Patches	iBeacon Eddystone			URL •
DB Backup	Controller Data Stream			http://www.ruckuswireless.com
Rules Backup	Beacon as a Service Telkonet		_	( o
License	Soter			(Update)
Settings	BLE Scan		-	
Reset & Reboot				

FIGURE 54 Updating Configuration Parameters (Generic)

Admin				Beaco	on as a Service		8
Services Plugins	Select a Plugin to Activate :	(Select v)	(A	Advertis Beacon	ally enable connector on all valid APs sement Interval • Type • m Beacon		100 ms
Account	Active Plugin List			Vendo	or type heric		
VM Configurations	Assa Abloy Kontakt.io			Sele	ect type		· · · · · · · · · · · · · · · · · · ·
Versions & Patches	iBeacon				ADV Type	Value	Actions
DB Backup	Eddystone Controller Data Stream				01	0192	× 1
Rules Backup	Beacon as a Service						Update
License	Telkonet		_				
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 React Mobile beacons 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 55 Activating the Beacon as a Service Plugin

Beacon as a Service	8
Globally enable connector on all valid APs	
Advertisement Interval •	
Beacon Type •	100 ms
Custom Beacon	· · · · · · · · · · · · · · · · · · ·
Vendor type	
React mobile	<b>v</b>
	(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 88 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) 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 56 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.

<b>FIGURE 57</b> Activating the BLE Scan Plugin
---

Admin				BLE Scan (S) Globally enable connector on all valid APs
Services Plugins	Select a Plugin to Activate :	BLE Scan	• A	Aggregation Interval 0000 ms
Account	Active Plugin List			Key • Enter Key Show
VM Configurations	1Beacon Soter			API URL.
Versions & Patches				Port
DB Backup				Enter Port API Endpoint
Rules Backup				(Enter URI (Eg /blescan)
License				UUID Filter (Enter UUID )
Settings				Enable heartbeat i
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 88 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 58 Deactivating the BLE Scan Plugin

Admin				
Services	Select a Plugin to Activate :	Select	* Activate	
Plugins				
Account	Active Plugin List			
VN Configurations	BLE Scan			Deactivate
Versions & Patches				
D8 Backup				
Rules Backup				
License				
Settings				
Reset & Reboot				

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

#### FIGURE 59 Updating the Configuration Parameters

Admin				BLE Scan (View logs)
Services	Select a Plugin to Activate :	Select 🗸	A	Aggregation Interval
Plugins				Vendor 1 Vendor 2
Account	Active Plugin List		_	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				Enable heartbeat i
				Update

### 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 60 Activating the Controller Data Stream Plugin

Controller Data Stream	8
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	Yes
Certificate	
Choose file No file chosen	
	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 88 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 61 Deactivating the Controller Data Stream Plugin

Admin		
Services	Select a Plugin to Activate : Celect 🖌	
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 62 Updating the Configuration Parameters

Admin				Controller Data Stream	۲
Services Plugins Account	Select a Plugin to Activate :	Select	(A	MQTT Broker Port •	
Providin	Active Plugin List			8883	
VM Configurations	Controller Data Stream			MQTT Publish Topic * i	
Versions & Patches				/home Periodic Update Interval	
DB Backup				10	
Rules Backup				Device reporting	Yes 🔘
License				/dev-report	)
Settings				Validate Server Certificate i Certificate: ca.crt	Yes
Reset & Reboot				Choose file his file chosen	
			_		(Update)

### 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 63 Activating the Dormakaba Plugin

Admin					Dormakaba
					Globally enable connector on all valid APs  III HTTPS
Services	Select a Plugin to Activate :	Dormakaba	•	(A	Citent Id
Plugins					Client Secret
Account	Active Plugin List				Enter Client Secret Show
VM Configurations	Controller Data Stream				AMB IP Enter AMB IP
Versions & Patches					AMB Host •
DB Backup					Enter AMB Hest
Rules Backup					443
License					AMB Auth path   Enter AMB Auth path
Settings					AMB API Path •
Reset & Reboot					Exter AMB API YER Path
					Enter AMB API VER Path
					Certificate Mode • Self signed O Trusted i
					Choose file Ites the chasteri
					(Apply)

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

#### NOTE

The URL for Host is https://exmaple.test.net.

- e) Enter the Ambiance Port.
- f) Enter the Ambiance Auth Path.
- g) Enter the Ambiance API Path.
- h) Enter the Ambiance API VER Path.
- i) Select the **Certificate Mode**.
- j) Click Choose file.
- 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 64 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 65 Updating the Configuration Parameters

COMMSCOPE				vriot1 N+1 : Disabled	1.8.0.0.27 Version 19 May 2021 9:50:48
RUCKUS <sup>®</sup> IoT Controller	Dashboard IoT APs IoT Devices Events	Admin Rules LoRa LNS IoT API			America/Los Angeles
Admin				Dormakaba	(%)
Services	Select a Plugin to Activate :	Select	- A	Status: Reachable Client Id *	
Plugins				1a1a1a1a1a16054b94e2db01e15f337e905aacdef2b2c2d2e2f	
Account	Active Plugin List			Client Secret *	Show
VM Configurations	Dormakaba			AMB IP	
Versions & Patches				192.168.201.8	
DB Backup				AMB Host * https://ruckusiot1.iotlab.net	
Rules Backup				AMB Port *	
License				AMB Auth path *	
Settings				(/WebAPI	
Reset & Reboot				AMB API Path • /token	
				AMB API VER Path •	
				/api/v1	
				Certificate: n_ruckus_lot_ca.crt	

### 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 66 Activating the Telkonet Plugin

Admin				Telkonet
Services	Select a Plugin to Activate :	Telkonet 🛛	A	
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 88 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 67 Deactivating the Telkonet Plugin

Admin		
Services	Select a Plugin to Activate : Select	<ul> <li>Activate</li> </ul>
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 68 Updating the Configuration Parameters

Admin				Telkonet	$\otimes$
Services Plugins	Select a Plugin to Activate :	Select v (	ē	Clobally enable connector on all valid APs Client status: Not Connected IP Address 10.174.113.66	
Account	Active Plugin List			Port • (6031	
VM Configurations	Telkonet				Update
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 69 Activating the Soter Plugin

Admin				Soter	⊗
				Soter URL •	
Services	Select a Plugin to Activate :	Soter v	4	Enter Soter URL Soter Port •	
Plugins				Enter Soter Port	
Account	Antice Divers Link			Soter Key •	
VM Configurations	Active Plugin List			Enter Soter Key Sh	
Versions & Patches					9
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 70 Deactivating the Soter Plugin

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

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

FIGURE 71 Updating the Configuration Parameters

Admin				Soter	8
Services Plugins	Select a Plugin to Activate :	Select	· · · (A	Status: Not Reachable Seter URL * e2.54:196-163-125.compute-1.amazonaws.com Seter Pert *	
Account	Active Plugin List			( 8883) Soter Key •	)
VM Configurations	Assa Abloy Kontakt.io				Show
Versions & Patches	Tile Domo				(Update)
DB Backup	Tracky Dense				
License	Eddystone				
Settings	Controller Data Stream				
Reset & Reboot	Beacon as a Service Telkonet				
	Soter				
	7L				

# **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 72 Changing the Password

			Update passw
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 73 Configuring a Virtual Machine

Services	Hostname *		DHCP	○ Static	
Plugins	vriot				
ccount	America/Los_Angeles	<b>•</b> )			
/M Configurations	Set Time Automatically using NTP NTP Address				
ersions & Patches	ntp.ubuntu.com	(Optional)			
B Backup	○ Set Time Manually i				
ules Backup					Update
cense	Current Certificate	Certificate		Кеу	
ttings	Common Name : local-mqtt.video54.local Certificate Expires on May 11 17:04:15 2031 GMT	Choose file No file chosen		Choose file No file chosen	
eset & Reboot		Upload certificate & Key	Download CA certificate		

**Uploading Versions and Patches** 

- 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 74 Uploading an Image

Admin			
Services	Upload Image		Upload Patch
Plugins			
Account	Version list	Patch list	
VM Configurations	Not Available	No Patch Available	
Versions & Patches			
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 75 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	pater-rototot-to	Hoc Applied	
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 76 Backing Up or Restoring Files

0			
Admin			
Seren			
Actor .	Barchupes Lint. Vacti del anni 2022 de 14 23 42 34 datta	4	
with Contrigon rationals	VIIICI_08_sim_2021-07-14-03-23-0	Use Network Configuration Present in Backup	
, Veneral Editions		Yes  Vo  Vo  Vo  Vo  Vo  Vo  Vo  Vo  Vo  Vo	
Arte Bacture			
ime			
- Skelingel			
And Added			

- 3. Click Create Backup now to perform a backup manually.
- 4. Click Download to download the backup files.
- 5. Click Upload Backup to upload and restore a DB backup file.

### NOTE

The RUCKUS IoT Controller maintains the backups of the last five configuration files. While uploading or restoring database backup file, a dialogue box appears with a message

Use Network Configuration Present in Backup

, so you can select either static or dynamic network configuration present in the backup file.

## **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 77 Backing Up or Restoring Rules

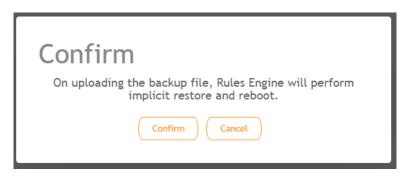
Full Backup v Create Rules Backup	(Upload Rules Backup
Full Backup Flows Backup Static Files Backup Kules Backups List	
VRIOT_Rules_Full_2020-04-17-06-07-53_GMT.tar.gz	(Download) (Restore) (Delete
VRIOT_Rules_Flows_Only_2020-04-17-06-08-00_GMT.tar.gz	(Download) (Restore) (Delete
VRIOT_Rules_Static_Only_2020-04-17-06-08-06_GMT.tar.gz	(Download) (Restore) (Delete

- 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 78 Confirming Upload of Backup File



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 79 Uploading a License

Controller serial number:101 AP capacity license used:11 AP capacity license remainin AP capacity license total: 20	g: 9	1C1XDK			Upload License
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 License check-out means consuming an AP capacity license, and License check-in means forfeiting an AP capacity license. The License check-out happens when AP is approved. The License check-in happens when AP is deleted or unapproved.

### NOTE

In N+1 configuration, for secondary controller the license capacity is unlimited for 30 days.

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.

### NOTE

If the number of approved APs are greater than total number of licenses available in the controller, then the GUI is redirected to a warning message as below, and access to the controller comes to an halt until you unapprove or delete the APs to match the license count. The mismatch usually occurs due to DB restore, after upgrade or N+1 failover or fallback.

-									Bate	ch Actions: (	Select	- Apply (S
0			Approved	Name	MAC ID	IP Address	Protocols	Uptime	Actions			Tags
0	•	⚠	ж	R730-N3	1C:3A:60:28:7F:10	10.174.113.126	NA	NA	Î	All ( R730-N3		
0			×	R650-N1	DC:AE:EB:00:91:E0	10.174.112.220	NA	7 days, 20:45:44	Î	All ( R650-N1		
	•		1	R720-QA-Test	8C:FE:74:21:F5:30	172.29.124.62	BLE	0 days, 16:49:20	÷	All R720-QA-Test	kontakt R	eacon (eddystone baas bies
	•		-	T310-Shriram	18:48:00:22:A1:90	172.29.124.52	ZIGBEE_AA	0 days, 16:48:50	<b>B</b>	All T310-Shrivam		
O	•		-	H510-my-desk	D8:38:FC:25:C4:C0	10.74.136.152	NA	5 days, 9:16:57	8	All H510-my-desk	)	
0	•		1	R550-0640	70:CA:97:20:08:40	10,174,113,135	BLE	6 days, 11:23:55	8	All R550-0640	kontakt (ibea	con eddystone baas blesca
0	•		1	R610(@deSk)[121]	B4:79:C8:04:E6:F0	10.74.136.153	BLE	6 days, 11:23:35	8	All R6!0(sde5k)[1	t1] kontakt	(ibeacon) eddystone (baas)
	•		-	E510-Shriram	C8:08:73:26:AA:D0	172.29.124.36	ZIGBEE	0 days, 16:48:49	8	All ES10-Shriram	(	
0	•		×	R650-Praveen	20:58:69:38:87:10	10.174.112.66	NA	NA		All R650-Praveen	)	
0	•		1	H510-VLAN	30:87:D9:14:57:AD	0.0.0.0	ZIGBEE, Z-WAVE	0 days, 16:48:48	B	All HS10-VLAN		
	•	⚠	ж	RuckusAP	34:20:E3:2D:23:90	10.174.113.84	NA	NA	8	All RuckusAP		
0	•		~	R650-N5	DC:AE:EB:00:97:60	10.174.113.176	NA	NA	8	All R650-N5		
					•     ×     R720-H3       •     ×     R650-H1       •     ×     R650-H1       •     ·     R720-QA-Test       •     ·     T310-Shriram       •     ·     H510-my-desk       •     ·     R550-0b-k0       •     ·     R510(@desk)[121]       •     ·     R650-Pravecon       •     ×     R650-Pravecon       •     ×     R650-Pravecon       •     ×     R650-Pravecon       •     ×     RackuzAP	▶         R730-N3         1C:3A:60i28:77:10           ▶         R650-N1         DC:AE:EB:00:91:ED           ▶         R720-QA-Test         BC:FE:74:21:F5:30           ▶         ✓         R720-QA-Test         BC:FE:74:21:F5:30           ▶         ✓         R730-N3         16:38:FC:25:C4:C0           ▶         ✓         T310-Shriram         18:48:00:22:A1:90           ▶         ✓         H510-my-desk         D8:138:FC:25:C4:C0           ▶         ✓         R550-0b-40         70:CA:97:20:08:40           ▶         ✓         R510[BideSA][121]         B4:79:CB:04:E6:F0           ▶         ✓         R510_Shriram         C8:08:71:26:A4:D0           ▶         ✓         R550-Praveen         20:58:69:138:B7:10           ▶         ✓         H510-VLAH         30:87:09:14:57:AD           ▶         ▲         Rackar&P         34:20:E1:20:23:90	▲         X         R730-N3         1C13At660:28:7F:10         10.174.113.126           ▲         X         R650-N1         DC1AE:EB:00:91:E0         10.174.112.220           ▲         X         R650-N1         DC1AE:EB:00:91:E0         10.174.112.220           ●         ✓         R720-QA-Test         8C1FE:74:21:F5:30         172.29.124.62           ●         ✓         T310-Shriram         18:48:00:22:A1:90         172.29.124.52           ●         ✓         H510-my-desk         B8:38:FC:25:C4:C0         10.74.136.152           ●         ✓         R560-0b:40         70:CA:97:20:08:40         10.174.113.155           ●         ✓         R560-0b:40         70:CA:97:20:08:40         10.174.113.155           ●         ✓         R560-Pravecen         20:58:69:38:400         172.39.124.36           ●         ▲         R650-Pravecen         20:58:69:38:87:10         10.174.112.66           ●         ▲         R650-Pravecen         20:58:69:38:87:10         10.174.112.66           ●         ▲         R650-Pravecen         20:58:69:38:87:10         10.174.112.66           ●         ▲         R650-Pravecen         20:58:69:38:87:10         10.174.113.184           ●         ▲         Ruck	Image: Constraint of the second s	Image: State Sta	Image: State of the state	Image: State of the state	Image: State Sta

- 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 80 Settings Page



3. Enable SSH.

### NOTE

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

FIGURE 81 Showing Error on Disabling SSH

******	*****
Ruckus IoT Cont	roller
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 Control</pre>	
N+1 Configure:	
To Configure N+1 ensure following requirements:	
**************************************	nould be in same subnet and reachable. nould be configured with static ip address. nould be running in same version.
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 S	SH 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 82 Rebooting 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 **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 83 Resetting RUCKUS IoT Controller

Reboot	
Reboots the system	. The User Interface shall not be available until the system restarts !
Factory Reset	
IMPORTANT ! This a	

3. Click Factory Reset.

# **Managing IoT Access Points**

•	IoT AP Overview	81
	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:

General	Advance	ed								
Availat	ole Option	ns						[	)escrip	tion 🔺
040	NIS Dor	main N	ame					1	lame o	f Ne
041	NIS Ser	vers						F	ddres	ses o
	NTPSe							F	ddres	ses o
I ∩43	Vendor	Specifi	c: Info	5				F	mbed	led 🗸 👻
•										
Data e الم	entry —					 		ют	Cor	ntrolle
Data:			Bi	nary	r:			_	ASCII:	_
000 000 001	8 2E	31	31	30 33 2E		37 30 33		. 11	0.17 3.20 .103	6
							VL.	AN		

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 84 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 85 IoT Access Points Page

IoT AP Selected	(Pre-A	pprove IoT APs					Ba	tch Ac	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	(Al) (2022) (kentakt:Ruchet20000) (tex)
► [ QA-VSZ-5-1-460 ]		• R710	44:1E:98:13:FB:20	192.168.100.37	zigbee_aa	25	5 days, 3:48:52	Q	Û	(AI) (4418-585137523) (konskesadaszocoz) (270)
	•	R610_Shetty	B4:79:C8:04:D9:40	192.168.100.39	ble	NA	NA		Û	(21) (5+775CR(04109:40) (dds)
		e R730	18:7C:0B:20:DC:F0	192.168.100.15	zigbee	20	0 days, 0:12:54		î	All 16:7C08:20:0C:F0 (8730)
		R510_OUT_RuckusAP_Shriram	EC:8C:A2:37:03:A0	192.168.100.59	zigbee	14	NA		Û	All EC:8C:A2:37:03:A0 BS10_0UT_BudusAP_Shriram
		R510_Shetty	D8:38:FC:18:FC:D0	192.168.100.77	zigbee	20	NA		Û	(41) DI: 32 PC-18 PC-18
		H510_Shetty	30:87:D9:14:69:00	192.168.100.62	ble	NA	5 days, 3:29:55	Q	î	All H510_Shetty (kontakt:Rucks800.001) (30:87:09:14:69:00)
		SM-AP	30:87:D9:15:40:40	192.168.100.58	zigbee	20	2 days, 0:05:36	Q	Û	AL SHAP 3237.07.15.40.40
		H510-RuckusAP-Shriram	0C:F4:D5:1E:97:D0	192.168.100.92	zigbee	19	5 days, 3:49:27	Q	Ē	All 00:14 05:16:37:00 (HS10-RackasAP-Shrivan)
		R610_AP_Shriram-test	84:79:C8:01:F0:30	192.168.100.54	zigbee_aa	16	5 days, 2:32:23	Q	Û	(4) 8610_4P_Shrinam-test 64:7%CR: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	86 Adding	a Single	IoT AP
TIGONE	oo / waanig	u singic	10170

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 87 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 88 Single IoT AP Mode

IoT AP Selected	Pre-Approve	lot APs					ibeacon × baas × eddystone	× kontakt × R730-Shriram ×	
[ga16-clust-qa]	0	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		
[Busicense]		R610(@de5k)[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	Z/GBEE	3 days	Net Mask	255.255.252.0	
		T310-Shriram	18:48:00:22:A1:90	172.29.124.52	ZIGBEE_AA	2 days	DNS	10.10.10.106	
		R730-Manoj	18:7C:08:20:EB:E0	172.29.116.28	BLE, ZIGBEE		loT version	1.5.1.0.15029	
						_	Radio Info		
	•	R750-Shriram	84:79:C8:3E:72:00	172.29.124.34	BLE, ZIGBEE	2 days			
		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)
							IoT Radio MAC	00:0D:6F:FF:FE:88:88:AF	
							IoT Radio Mode	ble	
							iot hadio mode	bie	

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 89 Selecting an AP to Add Tags

I S112-karth&;       Name       MAC ID       IP Address       Protocols       Uptime       Actions       Scin For Devices DeApprove         [ QA&BLR-Clust ]       SM: AP       30:87:07:15:40:40       192.168.10.21       2168EE       3 days, 21:42:13       Q       I       ALI Instabutes       Deapprove         [ QA&BLR-Clust ]       RuckinAP       E0:80:A237:03:A0       192.168.10.21       2168EE       3 days, 21:42:13       Q       III       ALI Instabutes       Delete Tags       Add Tags         [ Q & RIT20_Shetty       18:7C:08:2A:37:03:A0       192.168.10.777       ZIGBEE       2 days, 22:32:40       Q       III       ALI reversition dedukes       Restore       Restore       Restore       Add Tags         [ Q & RIT20_Shetty       18:7C:08:2A:05:F0       192.168.10.177       ZIGBEE       2 days, 22:32:40       Q       III       ALI reversition dedukes       Restore       State       2 days, 22:39:17       Q       III       ALI reversition dedukes       Restore       State       2 days, 22:39:17       Q       IIII       ALI reversition dedukes       Restore       State       2 days, 22:39:17       Q       IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	1 IoT AP Selected	Pre-Approv	ve IoT APs							Batch Actions:	Select	( ¥ )	Apply	) (2
	▶ [ 5112-karthik ]		Name	MAC ID	IP Address	Protocols	Uptime	Acti	ions		Scan For Devices			
Image: Constraint of the second se	▶ [QA-8LR-Clust]		SM-AP	30:87:D9:15:40:40	192,168,10,21	ZIGBEE	3 days, 21:42:13	٩	8	All HS10-BLE-RoyalPark	Restart			
R510_Shetty       D8:38:FC:1Eh:FC:D0       192:468.10.177       ZIGEEE       3 days, 22:29:17       Q iff       Al renegi Rackadd Redox Riddystore Radio         Attribuic R510_Desk       D8:38:FC:1Eh:FC:D0       10.74.156.40       ZIGEEE       NA       iff       Al renegi Rackadd Redox Riddystore Radio       Radio         R510_ModeSk)[121]       B4:79:C8:04:E6:F0       10.74.156.40       BLE       2 days, 23:00:28       Q       iff       Al kontakt R510 Desk       Radio       Rad		•	RuckusAP	EC:8C:A2:37:03:A0	192,168,10,171	ZIGBEE	2 days, 23:52:07	Q	ŵ	All RuckusAP	Add Tags			
Image: Section of the section of th			R730_Shetty	18:7C:0B:20:DC:F0	192.168.10.63	ZIGBEE, BLE	2 days, 23:32:46	٩	ŵ	All revogi RuckusAP	ibeacon eddystone baas	)		
•       R510(0de5k)[121]       B4:79:C8:04-E6:F0       10.74.136.45       BLE       2 days, 23:00:28       Q       II       AI       kontakt       (rever)       C6dystore       E8400de65k](121]       Bencon       Lass         •       H510-desk       D8:38:FC:25:C4:C0       10.74.136.45       BLE       2 days, 23:00:32       Q       II       AI       kontakt       (rever)       C6dystore       Rescon       Lass         •       R730_Wiot_Shetty       20:58:d9:11:0E:30       192.168.10.52       Z106EE, BLE       NA       III       AI       Kontakt       K		• •	R510_Shetty	D8:38:FC:18:FC:D0	192.168.10.177	ZIGBEE	3 days, 22:29:17	Q	ŵ	All revogi RuckarAP	ibeacon eddystone baas	)		
Image: State in the state			Karthik-R510-Desk	D8:38:FC:1C:10:90	10.74.136.40	ZIGBEE	NA		畲	All Karthik-R510-Deck				
•       R730_Viriot_Shetty       20:58:69:11:0E:30       192.168.10.52       ZIGBEE, BLE       NA       If       A1       Kontakt       RactusAP       eddystone       Beecon       Ibast         •       H510_Shetty       30:87:09:14:69:00       192.168.10.71       ZIGBEE_AA       NA       If       A1       Kontakt       RactusAP       eddystone       Ibast			R610(@deSk)[121]	B4:79:C8:04:E6:F0	10.74.136.45	BLE	2 days, 23:00:28	Q	<sup>®</sup>	All kontakt revogi es	ddystone R610(@deSk)[121]	ibeacon	baas	
H510_Shetty         30:87:07:14:67:00         192.168.10.71         ZIGSEE_AA         NA         Image: Comparison of the co			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 ibea	on baas		
			R730_Wriot_Shetty	20:58:69:11:0E:30	192,168,10.52	ZIGBEE, BLE	NA		8	All kontakt RuckusAP	eddystone ibeacon baa	3		
			H510_Shetty	30:87:09:14:69:00	192,168,10.71	ZIGBEE_AA	NA		畲	All kontakt ibeacon	RuckusAP ddystone baa	3		
R730_QA-Test-1 18:7C:08:20:E8:E0 192.168.10.105 ELE, ZIGEEE_AA NA II kontakt Basson eddpatans (R720_tilk_board bass)			R730_QA-Test-1	18:7C:0B:20:EB:E0	192.168.10.105	BLE, ZIGBEE_AA	NA		ß	All kontakt ibeacon	eddystone 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 90 Adding a Tag

oT AP Selected	(Pre-Appr	ove IoT APs					Add new tag	(
[5112-karthik]		Name	MAC ID	IP Address	Protocols	Uptin		
QA-BLR-Clust ]	0.	SM-AP	30:87:D9:15:40:40	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	2 days, 23		
	0.	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	Pre-Approve IoT A	Ps						Batch Actions:	Select	Q (
No Data Juwilable ]		Name	HAC ID	IP Address	Protocols	Uptime	Actions	and the second	Tap	3.1(34)
	•	RuckusAP	20:58:69:11:09:10	192.148.29.154	BLE, ZIGGEE	1 days, 5:17:00	Q 🏦	All (Buckusser bostahl Beacon e	ilynone) (Las) (Liesan)	
tal IoT APs : Export IoT APs to CS	<u>v</u> )						D	isplaying 10 + ga	teways	< Previous Nex

# **Managing Devices**

•	Devices Overview	91
•	Managing OSRAM Light Bulbs	. 94
•	Managing an Assa Abloy Lock	95
•	Managing the Dormakaba Locks	96

## **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 91 IoT Devices Page

Device Selected	Devices	Beacons Pre-Appro	ve IoT Devices					Batch Actions:	Select		Apply 3
No Date Available ]	0	Name	HAC ID	IOT AP MAC	Protocol	Type	rði	R55i	Last Seen	Action	Tags
		Telko PiRD1	0010A:80:00111:00:37:10	20:58:69:11:09:10	zigben	IAS Zone	66	-58	5 minutes ago	0 8	Al Telko-Piki
	0 •	Telko-PiR02	00:0A/80:00:11:00:30:4E	20158169111109110	zigbee	LAS Zone	63	-60	5 minutes ago	Ø Î	AE Telko Pilo
	0 .	Telko-Pilli03	00104(30)00111(00:33:F3	20158169111109110	rigbee	IAS Zone	$\overline{n}$	-54	5 minutes ago	0 1	AR Tello-Par
	•	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	Al ST-Button
	0 .	ST-water	28:50:97:00:01:08:06:24	20:58:69:11:09:10	zigbee	145 Zone	55	-62	6 minutes ago	0 1	Al ST-water
		ST-Pill	28160197100101106148117	20:58:69:11:09:10	zigbee	145 Zone	77	-51	5 minutes ago	0 8	AE STOR
	0 .	Telko Door	00104180100110100150136	20:50:69:11:09:10	zigben	145 Zone	45	-71	3 hours ago	0 11	AE Telto-Dos
	0.	eria-motion	00115180:001011A6109134	20:58:69:11:09:10	zigber	145 Zone	36	-17	23 minutes ago	Ø	All eria-mot
tal Devices : 8 Export IoT Devic	es to CSV )						Dispi	aying (10 + d	evices	< Previous	Next

The device scan operation must be performed to start the device discovery process on the gateway.

### NOTE

It is important that the IoT devices are scanned and onboarded to the nearest AP for good RSSI/LQI. For more information about RSSI/LQI for reliable connection, refer to https://support.ruckuswireless.com/articles/000011687.

Upon starting device discovery, a dialog box is displayed, as shown in the following figure.

### FIGURE 92 Device Discovery Dialog Box

Scan Started at 14 July 2019 23:51:46 and will automatic	ally end at 15 July 2019 11:51:46	(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 93 Adding Device After Discovery

an Started at 14 July 2019 23:56:54 and will automatically end at 15 July 2019 11:56:54										
Name *	Manufacturer	MAC Address	Protocol	Radio MAC	IoT AP MAC	Actions				
Enter Device Name	OSRAM.	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:0B	0C:F4:D5:1E:97:D0	(Accept ) (Blacklist				

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

### FIGURE 94 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	0201061AFF4C000215F7826DA64FA24E9880248C5871E0893E6D6D8F43				
		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	0201061AFF4C000215F7826DA64FA24E9880248C5871E0893E178F0E0F				
		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	0201061AFF4C000215F7826DA64FA24E988024BC5B71E0893E2F870E08				
		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				
		00.00.05.01.10.10.00.01			0104042 10010000000000000000000000000000				

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 95 Exporting IoT Devices to CSV

Γ Devices									•	a (	
Device Selected	Devices	Beacons Pre-Appro	e tot Devices					Batch Actions:	Select	w.	Apply)
[ No Date Available ]	0	Name	MAC ID	INT AP MAC	Protocol	Type	LQI	R351	Last Seen	Action	Tags
	•	Telko-P1R01	00x0Ac80x00:11x00x37x10	20158:69:11:09:10	zigbee	IAS Zone	65	-50	5 minutes ago	0 8	All Telko-P
	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	ØÎ	all Telko-r
	0 •	Tetko-PIRD3	00:04:80:00:11:00:33:F3	20158:09111:09190	righee	tAS Zone	72	-54	5 minutes ago	0 1	All Telko-P
	•	ST-Button	28:60:97:00:01:08:43:20	20:58:69:11:09:10	riptee	145 Zone	72	-54	10 minutes ago	Ø 🗊	All ST-BAR
	0 •	STiwater	38:60:97:00:01:08:08:24	20150:69:11:09:10	zigter	IAS Zone	58	-63	6 minutes aga	0 11	All ST-wate
	0.	ST-PIR	28:60:97:00:01:06:AB:17	20:58:69:11:09:10	zigbee	IAS Zohe	77	-51	5 minutes ago	Ø 11	All 57-PM
	•	Telko-Door	00:04:80:00:10:00:90:78	20158-69111:09110	ziptee	UAS Zone	45	-71	3 hours age	0 1	All Telko-1
	•	eria-motion	00:15:60:00:01:46:C9:34	20:58:69:11:09:10	zigbee	185 Zpoe	54	-17	23 minutes ago	© îi	All orla-m
tal Devices : Export IoT Devices to	• CSV )							Displaying 10 + de	evices	Previous	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 96 Managing OSRAM Light Bulb

Device Selected	Pre-Approve IoT De	vices				loT Device Name	Osram	Apply (
▶ [ QA-Cluster ]	IoT Device N	ame IoT Device MAC	IoT AP MAC	Protocol	Туре	IoT AP	0C:F4:D5:1C:52:50- RuckusAP   ▼	Apply
[Test-upgrade]	aasf	00:0B:57:FF:FE:1B:3B:64	0C:F4:D5:1E:3C:40	zigbee	Smart plug	7C:B0:3E:AA:00:A4:5E:69 ×	s4 ×	
	🔲 s1	00:13:7A:00:00:01:E8:5B	0C:F4:D5:1C:52:50	zigbee	IAS Warning Devic	Add new tag		
	s2	00:15:8D:00:01:DE:EA:EC	0C:F4:D5:1C:52:50	zigbee	IAS Zone	Blacklist Device:	Off	(Apply)
	☑ Osram	7C:B0:3E:AA:00:A4:5E:69	0C:F4:D5:1C:52:50	zigbee	Color Dimmable Lig			
	🔲 yale	00:0D:6F:00:05:24:20:CE	0C:F4:D5:1C:52:50	zigbee	Smart plug	Device Information		
						Level Control		_
						CurrentLevel	255	
						Basic		-
						ZCL Version	1(Version)	
						PowerSource	Mains (single phase) ( 1	)
						Manufacturer Name	□OSRAM	
						Color Control		-
						CurrentX	54	
						Primary5Y	0	
						Primary4X	0	
						CurrentY	22	

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 97 Visionline Server Event Log

1 R

~Roo	∽Room Event List							
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		

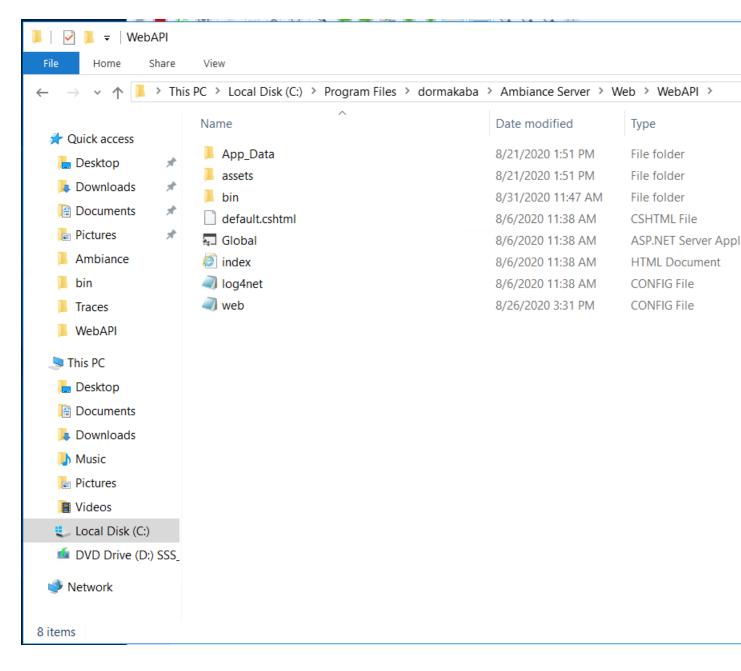
## **Managing the Dormakaba Locks**

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 98 Locating the web config file



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

FIGURE 99 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="ConnectionToRabbitMORetrialDelayInSeconds" 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="803F5F7F11D50A3A" 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 100 Login into Dormakaba Plugin

dormakaba 🚧	Select an application	~				O prashant shah
	Guest Reg	istration	Reports	Ĩ.,	Staff Managerr	
						-
	Staff Keys	Property Builder	Device Management	System Keys	Access Management	Programming & Auditing
			<	>		

### 2. Click Device Management.

### FIGURE 101 Selecting Device Management

Multiple Ambiance™ - Device Managemer × +		- C	) X
$\leftrightarrow$ $\rightarrow$ C ( ) localhost/deviceMgr.html#!/		Q 🕁	<b>e</b> :
dormakaba 🞽 🛛 Device Management 🗸 🗸	product shah 🗸 🛂	्द ?	$\mathbf{\hat{\Box}}$
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 102 Selecting Register Gateways and Paired Access points

Marka Ambiance™ - Device M	Managemer × +						-	
← → C (0 loc	calhost/deviceMgr.html#	#!/					Q \$	0
dormakaba 🚧	Device Management	×				Prashant shah V	t) ∞ ;	? 🗅
	nent > 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 M	AC address	III ©	0 C
🖃 Gateway 🕇		Status	Туре	MAC Address	IP Address	Antenna		Lost
Gateway-8CFE74		0	dormakaba Gateway	8CFE741071A0	192.168.0.4	Pairing OFF		10/
Gateway-B479C8			dormakaba Gateway dormakaba Gateway	8479C81E60C0 C803F5109440	192.168.0.2	Pairing OFF Pairing OFF		10/
Gateway-C803F5		¥ ¥	dormakaba Gateway	C80873188840	192.168.0.2	Pairing OFF		10/1
			4					•
H 4 1 F	H							- 4 of 4 items 1 Selected
	Back to device selection			Delete Gateway(s)		Next to access points		- Selected
© 2020 - Ambiance <sup>14</sup> - 2.4.1.3							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 103 Displaying the Lock

🛛 🖌 Ar	mbiance™ - Device №	Managemer × +						-	
← →	C O loca	alhost/deviceMgr.html#!/						ର 🕁	<b>0</b> :
dorn	nakaba 🚧	Device Management V				Proshant shah	<b>↓</b>	িব	?
J	Device Manageme REGISTERED	nt > GATEWAYS & PAIRED ACCESS POINTS							
▼ ME	ETRICS								C
	٢	ONLINE GATEWAYS - 4/4	ONLINE A	12.5% CCESS POINTS - 1/8		LOW BATTERY - 0/8		>	
Ŷ	Access Points	-Select command-	Send Command		Search by Access P	ioint nome		P	lii C
	Access Point 🕇	Status	Lock profile	Gateway		Building	Floor		
	105	•	RTNFC	Gateway-8CFE741071A0		Ruckus Wireless Networks	FLOOR1		
Id	<b>1 F</b>	ы	4						▶ 1-1 of 1 items
									0 Selected
			Back	to gateway selection					
© 2020	0 - Ambiance <sup>14</sup> - 2.4.1.3							10/12/2	020 12:10 PM

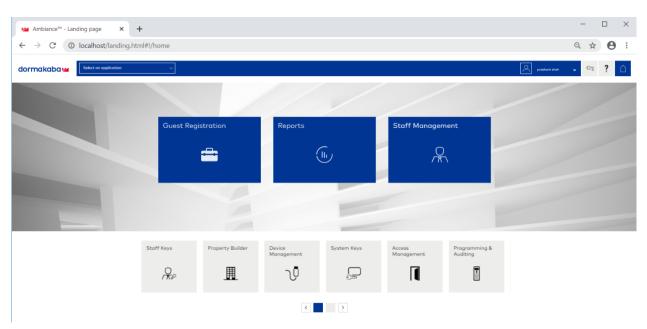
9. To confirm the lock connection, select the sage gateway, and click **Next to Access Point**.

## **Blocking the Key Remotely**

Perform the below steps to block the key remotely.

1. Go to Dormakaba Homepage.

### FIGURE 104 Dormakaba Homepage



### 2. Click System Keys.

### FIGURE 105 Selecting the System Keys

← → ♂ ③ localhost/systemKeys.html#!/		Q & <b>0</b>
C U localnost/systemkeys.html#!/		U H O
ormakaba 😖		🛛 provhore skale 🗸 🕹 💡
Set SetLect a Key type		
Key Types		
Black Keys Temporarily disable all keys with a specific credential		
Concel Keys Permanently disable a specific key		
Diagnestic Keys Collect data from locks for troubleshooting		
Electronic Lockovt Toggie Keys Disabilylanable ull non-Emergency Keys		
Folisafe Keys Make guest bookup keys		
Inhibit Keys Permaniently disable all active guest keys		
Latch Keys Disoble possage mode in locks		
Primary Program Keys Perform advanced operations on locks	Please select a key type.	
Resequence Keys Resynchronize a specific key		
Secondary Program Kays Naprogram a Primary Program Kay		
Special Function Keys Perform system-level operations on locks		
Toggle Latch/Unistch Kays Disable/enable possage mode		
Jebiock Keys Re-enable keys that were previously blacked		
Unlatch Keys Ecolis passage mode in locks		

### 3. Click Block Keys.

FIGURE 106 Selecting the Block Keys

🖬 Ambiance <sup>™</sup> - System Keys 🗙 🕂	- 0	×
← → C ② localhost/systemKeys.html#l/	Q 🖈 😝	()
dormakabaw	🗵 🕞 🔁 ?	۵
ELECT A KEY TYPE		
Terr Type : Terr Type Type Type Type Type Type Type Type		
Primming databa databa guest keys     Lateh Keys     Lateh Keys     District generation in locks.     Primary physical Keys     Primary physical Keys     Primary physical digetabations on locks.	Press and it for type.	
Palagunoi Repi Republicanta sandfa key Secolary Program Repi Diporgeni at Tarting In Signar Rey		
Special Function Keys Per furm system head operations on lacks		
Toggie Late/Alviet/Novs Disable/web/e possoge mode		
Unblack Keys Min-analish keys that were previously blacked		
Unletzh Keys E-robie passage mode in locka		

### 4. Click Next to credential.

FIGURE 107 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	Block Keys > KEY INFO	
Key Info	Summary	
Key expiration	Key Info	
	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 108 Selecting Guest from the drop-down list

🚧 Ambiance™ - System Keys 🛛 🗙 🕂							-	
← → C ③ localhost/systemKeys	.html#!/functionKey	s-keyList					@, ☆	Θ
dormakaba 🚧						Proshort sheh	• 🕹	? û
Ellock Keys > Key Info > CREDENTIAL								
Electronic Lockout Toggle	• 0	P	Summary					
El Select Credential Class			Key Info					
Electronic Lockout Toggle Emergency								
Grand Master			Key type: Key expiration:	Block Keys 10/13/2020 01:14 PM				
Guest								
Inhibit			Credential					
Limited Use Stoff								
Moster			Key Holder					
Toggle Latch/Unlatch								

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

FIGURE 109 Selecting the Guest Room Number

dormakaba 🚧				Proshant shah	• 🐣 ? 🗅
CREDENTIAL					
Guest	• \$ P	Summary			
104	Room104, Prashant104 10/09/2020 To 10/29/2020	Key Info			
105 106	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 10/02/2020 10:37 AM 10/17/2020 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.

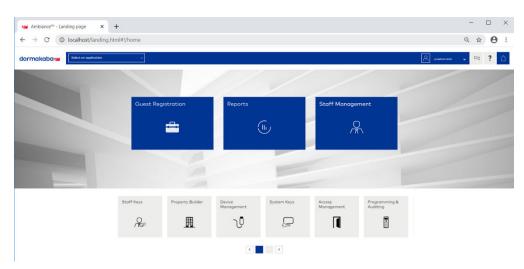
After you click Block Key Remotely, the LEDs will glow in the following pattern - one solid red LED, six green, and yellow LED together.

## **Unblocking the Key Remotely**

Perform the below steps to unblock the keys remotely.

1. Go to the Dormakaba Homepage.

### FIGURE 110 Dormakaba Homepage



### 2. Click System Keys.

### FIGURE 111 Selecting the Unblock Keys

🚧 Ambiance <sup>w</sup> - System Keys 🗙 🕂	- 🗆 X
← → C ③ localhost/systemKeys.html#!/	९ 🖈 😝 🗄
dormakaba	A 😣 ? 🗅
Select a Key Type	
KeyTypes	
Block Kays Temporonly disable all keys with a specific credential	
Canol Kaya Pensanetty disable a specific key	
Diagnostic Keys Collect data from Lecia for troublesheating	
Electronic Lockost Toggle Klys Disblor/mable of non-Emergancy Klys	
Fallade Keys Male guest backup keys	
<b>Inhibit Keys</b> Permanently deable all active guest keys	
Latuh Kaya Disolite possoge mijele ih lacks	
Primary Program Kaya Perform advanced operations on looks	Please select a key type.
Resequence Keys Resynchronise a specific key	
Secondary Program Keya Reprogram a Primary Program Key	
Special Function Keys Perform system level operations on locks	
Toggle Latch/Unlatch Keys Disobili/insble possoge modo	
Leblock Keys Re-anable keys that were previously blocked	
Unidath Kaya Einable passoge mode in locks	

Managing Devices Managing the Dormakaba Locks

### 3. Click Next to Credntial.

FIGURE 112 Clicking the option Next to Credential

🚄 Ambiance™ - System Keys 🛛 🗙 🕂		- 0
ightarrow C ( ) localhost/systemKeys.html#!/functionKeys-main		९ 🖈 😫
ormakaba		R prastant sheh 🗸 😂 ? [
Block Keys > KEY INFO		
Key Info	Summary	
Key expiration	Key Info	
10/13/2020 01:14 PM	Key type:         Block Keys           Key explication:         10/13/2020 01;14 PM	
	Credential	
	Key Holder	
Back Next to Credentials	Moke Keys	Block Keys Remotely
Book Next to Credentials	MolerKeys	Block Keys Remotely

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

FIGURE 113 Selecting Guest from the drop-down list

🚧 Ambiance™ - System Keys 🗙 🕂					-		$\times$
← → C () localhost/systemKeys.html#!/fun	nctionKeys-keyLis	t			@ ☆	θ	:
dormakaba				Proshont shah	•	?	$\hat{\Box}$
Block Keys > Key Info > CREDENTIAL							
Ettrovic Lackout Toggle Et Solitet Createral Class Energies/y Clarad Matar Uses Uses Uses Uses Uses United Use Steff Matar Toggle Lateh/Unlatch		Summary Key Infe Key type: Key expiration: Credential Key Holder	Block Keya 10/11/2020 OTSH PM				

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	110
•	Configuring Rules	110
•	Rules-Dashboard	111

## **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.

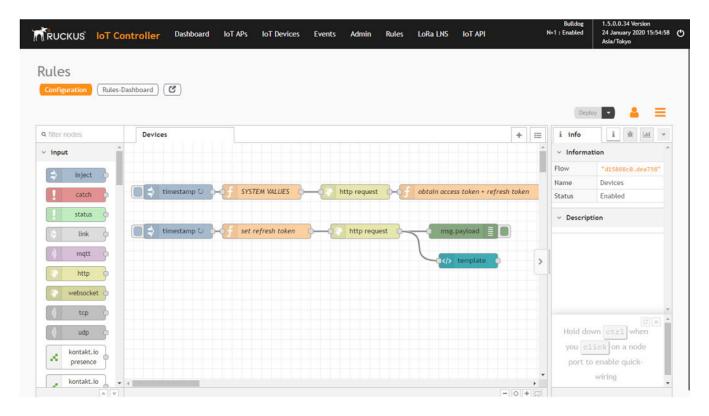
Complete the following steps to configure a rule.

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

#### NOTE

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

FIGURE 114 Configuring a Rule



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

FIGURE 115 Editing the HTTP Request Node

RUCKUS IoT Co				Dep	America/Los Angeles
a filter nodes	Devices	Edit http request node		⊕ debug	i 🕸 🔝 👻
~ input		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 SYSTE	Append msg.payload as query string param	neters *	"{"detail":"Authen credentials were n	
status				cresentials were n	oc provided. 7
Link 0	timestamp O - f set re	TLS Configuration TLS configuration	• •		
matt		✓ Use authentication			
http		Type basic authentication	· ·		
		admin			
websocket		Password			
tcp D		Use proxy			
udp		Return     a UTF-8 string			
kontakt.io					
kontakt.lo		Return     a UTF-8 string     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 116 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 117 Uploading Files in the File Manager

Туре	Name	Size	Last modified time	Path	Actions
1	naveen	4 KB	30 January 2020 9:24:15	/VRIOT/backend/node-red-static/naveen	Û
<b>1</b>	pradham	4 KB	30 January 2020 9:24:42	/VRIOT/backend/node-red-static/pradham	û
<b>m</b>	test	4 KB	30 January 2020 9:42:24	/VRIOT/backend/node-red-static/test	û
<b>m</b>	images	4 KB	3 February 2020 10:40:04	/VRIOT/backend/node-red-static/images	û
là	testfile	0 Bytes	30 January 2020 8:56:12	/VRIOT/backend/node-red-static/testfile	Û
<b>m</b>	images1	4 KB	4 February 2020 8:55:35	/VRIOT/backend/node-red-static/images1	Û
<b>m</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	節

#### NOTE

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

- HTML
- CSS
- PNG
- JPEG
- GIF

# **LoRaWAN**

•	LoRaWAN Overview	113
•	Logging In to the LoRa Network	113
•	LoRaWAN Dashboard	114
•	Configuring LoRa Devices	115
•	Configuring LoRaWAN Routers	. 117

### **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 118 Logging In to the LoRaWAN

LoRaWAN			
TrackNet			*
	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 119 LoRaWAN Dashboard

=	Overview			•	Adm	in .	<u>- c</u>	0
3	admin/TrackNet	<b>^</b>						
•	Ocurview						. 🗢	
	Management ^		0				L	Ra
	outlers 3	MANADEMENT		MANABEMENT		MFBRAGEB INSPECT		
	Usens Credentials	Downloads: API specification: APIspee.		~				
	Events Alarming Logs	Notifications:		0				
	Parsers	No pending hot fication.						
9	Messages A	<ul> <li>Version History:</li> </ul>						

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 120 Configuring LoRa Devices

On the **Devices** page, click

1.

≡	Devices					Admin		- C	?
SESSIONS	PROVISIONING	FINDER	0						
Ξ	Ċ	হ	EUI	Q 00-01-00-00-	-00-00-00 🛞				
0	۰	٠	0			15 # of Ro		l Column	*
🗆 EVI 🛧			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 121 Provisioning the Device

D	evices					
Ē	۴۹	Q F	LII		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 122 Device Joining the LNS

RUCKUS	IoT Contro	oller Dasht	xoard IoT APs	IoT Devices Events	Admin Rules	LoRa LNS IoT API			N+T : Disabled	cf73.1.5-lokegratikam.3146 Wer 4 October 2019 17:08:54 America/Los Angeles
	Devices							Admin	- c	Ø
essions r	PROVISIONING	FINDER	0							
۲	۵	٩	EUI	Q (11	49-08-00-00-10-81-09					
<b>0</b>	0	٥	0	Tow	Vertica	Desidade	Class	15 # of Nova FCritica	Add Column     Lair Option	•
58-40-CB-00	00 10 81 09			OTAA	1.1	1805719	A		19-10-04-15-26-26	
EUI: Dwnar: Type: Version: State: Nwk Key: App Key: Join EUI: Nwk SKeyOwn: AppSkey: Dev&ddr: Dev&ddr: Dev&ddr:	C\$329FC4C99F 00-02-03-00-00 38582C97E6AF 608F000895F	12307A32A4D2D4 109418FD7EC54	1618EDC D308630 0F192F3							

#### 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 123 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 prop	perties									
D 353	30322E00	6300	Use cus	tom ga	tewa	y ID	$\checkmark$	Get G	lateway U	
Server addre	ss 192.16	8.0.2	Keepaliv	e interv	a10	\$ :	5	Forward	crc valid	true
Port up	1680	\$	Stat inte	erval	30	\$	s	Forward	crc error	false
Port down	1680	\$	Push tin	neout	100	•	ms	Forward	crc disable	efalse
Radio	Radio_		Chan	Chan	Mul	~		Tx lut	Tx_Lut_0	) ~
Receive ena	able true	\$	Enable	dtrue				Pa gain	0	
	SX125		Radio	Radio	<u>    (      </u>	-		Mix gain	5	3
Туре	UNILU								-	dBn
Type Frequency	902.71	MH:	IF	-400	÷	KHz		Rf power	9	dBu
		MH: dB	IF BW	- <b>400</b> 1250	leal	KH2 HZ		Rf power Dig gain	9 3	
Frequency	902.71	2000 B	12		leal			The second second second		
Frequency Rssi offset	902.71 -164	2000 B	12		leal			Dig gain		

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

FIGURE 124 Starting Packet Forwarder

PacketForwarder_UI	658-7768 🔒 🖬 Stop Share	
Gkobal Conf     Options     Open Log Folder     About       Image: Start Forwarder     Start Saving received pack       Packet Filter       Frequency     MHz     Device address       Channel     Image: Packet Forwarder for Windows	Options_UI Cov extract options Cov delimiter Display parameters	- C X
CR INFO: downstream port is configured to "1680" INFO: downstream keep-alive interval is configured INFO: statistics display interval is configured INFO: upstream PUSH_DATA time-out is configured INFO: packets received with a valid CRC will be Packet Detains INFO: packets received with a CRC error will NOT Potocol Version PINFO: [main] concentrator started, packets can no INFO: host/sx1301 time offset=(1570141069s:33377 Expocted packets INFO: bost/sx1301 time offset=(1570141069s:33377 Expocted packets received by concentrators of the INFO: bost/sx1301 time offset=(1570141069s:33377 Expocted packets received by concentrators: 0	Show packet forwarder console Show hal br continuous console Show hal br test console Show pit br test console Show conf selector at starting	Start in DFU mode Device selection Selected device SEMTECH ProcOW Virtual ComPort (COM5) Charge device
# CRC_OX: 0.00%, CRC_FAIL: 0.00%, OR_CC: 0.00%         # FP packets forwarded: 0 (0 bytes)         # PUSH_DATA datagrams sent: 0 (0 bytes)         # PUSH_DATA acknowledged: 0.00%         ## PULL_DATA acknowledged: 0.00%         ## PULL_DATA sent: 3 (0.00% acknowledged)         # PULL_DATA sent: 3 (0.00% acknowledged)         # PULL_RESP(onsol datagrams received: 0 (0 bytes)         # Romb       # Rr packets sent to concentrator: 0 (0 bytes)         # Romb       Romk         ### [JIT] ###         # GPS sync is disabled         #### END #####         JSON up: {"stat":{"time":"2019-10-03 22:18:42 GW         WARNING: [up] ack server connection error : 106	` 17", "rxnb":0, "rxok":0, "rxfw":0, "	OK 'ackr":0.0,"dwnb":0,"txnb":0}}

### **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 125 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 126 Adding the Router to the LNS

RUCKUS	loT Controller	Dashbo	oard Io1	APs loT	Devices	Events Admir	ı Rules	LoRa LNS Io1	ГАРІ		vriot N+1 : Disabled	1 30	la, 1.5-Integrations.313- ctober 2019 16:04:50 erica/Los Angeles	4 Versk
oRaWAN														
≡ R	outers								Adm	in	-	с	?	
Search		Q	0	0	1	00	ý.	0	0	15	Add Column		*	
										# of Rows				- 1
Router ID						Name			0	Connected	Region			
router-1:						IsAlive System	Health		0	ê	EU863			1
router-3535:30	32:2e00:6300					TestRouter				÷	US902/bloc	:k0		
ROUTER-INFO RID: Router ID: Name: Connected: Owner: Region: GPS Location: MAC Address: Connection: Firmware: #Up: #Down: Last Uptime:	ROUNDTRIP-TIMES 383402364965412100 router-355320322400 TestRouter TestRouter TestRouter TestRouter 1059022/block0 0.0000,0000 0.03222200,63.00 udp//192.168.0.3252 Protocol Version 2 0 69-1231-16.00.00 69-1231-16.00.00	0	IT-HISTORY SPinn	PACKET-R	ATES									
Last Dntime:														

## **Events**

•	Viewing Events	121
•	Viewing SmartThings Event	122

### **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 127 Events Page

					(Download) (Clear)
Time	AP MAC	ID	Event	Message	
2020-10-14 06:51:30.895026	18:48:0D: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 128 Event page for Smartthings

Time	AP MAC	ID	Event	Message
020-12-15 07:43:49.999590	94:F6:65:2A:2A:50	200	ST Upgrade	Upgrade Success
020-12-15 07:43:49.951628	94:F6:65:2A:2A:50	200	ST Upgrade	Upgrade Success
020-12-15 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:F6:65:2A:2A:50 is in st firmware version 0 - Send upgrade.
020-12-15 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.
020-12-15 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.
020-12-15 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.



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