

Ruckus IoT Controller Configuration Guide, 1.4

Supporting IoT Controller Release 1.4

Copyright, Trademark and Proprietary Rights Information

© 2019 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, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, Edgelron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, and ZoneFlex are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Preface.....	5
Document Conventions.....	5
Notes, Cautions, and Warnings.....	5
Command Syntax Conventions.....	6
Document Feedback.....	6
Ruckus Product Documentation Resources.....	6
Online Training Resources.....	7
Contacting Ruckus Customer Services and Support.....	7
What Support Do I Need?.....	7
Open a Case.....	7
Self-Service Resources.....	7
About This Guide.....	9
Introduction to Ruckus IoT Controller.....	9
What's New in This Document.....	9
Getting Started.....	11
Before You Begin.....	11
Supported Web Browsers.....	11
Logging In to Ruckus IoT Controller.....	11
Getting to Know the Dashboard.....	15
Configuring N+1	17
Configuring Static Addresses for Master and Slave.....	17
Configuring the N+1 Feature.....	17
Managing IoT Controller System Configuration.....	33
Managing Services.....	33
Activating and Editing the Plugins.....	34
Activating and Editing the Kontakt.io Beacons Plugin.....	34
Activating and Editing the Eddystone Plugin.....	36
Activating and Editing the iBeacon Plugin.....	40
Activating and Editing the Beacon as a Service Plugin.....	43
Activating and Editing the Controller Data Stream Plugin.....	45
Changing the Password.....	47
Configuring Virtual Machines.....	47
Uploading Versions and Patches.....	48
Uploading an Image.....	48
Uploading a Patch.....	49
Backing Up Files.....	50
Rebooting Ruckus IoT Controller.....	51
Resetting Ruckus IoT Controller.....	52
Managing IoT Access Points.....	55
IoT AP Overview.....	55
DHCP Option 43.....	55
Ruckus Command Line Interface.....	55
USB Power.....	55
Adding an IoT AP.....	57

Editing an IoT AP.....	60
Single IoT Access Point Mode.....	60
Adding Tags to an AP.....	61
Approval of IoT APs.....	63
Managing Devices.....	65
Devices Overview.....	65
Managing OSRAM Light Bulbs.....	67
Managing an Assa Abloy Lock.....	68
Events.....	71
Viewing Events.....	71

Preface

- Document Conventions..... 5
- Command Syntax Conventions..... 6
- Document Feedback..... 6
- Ruckus Product Documentation Resources..... 6
- Online Training Resources..... 7
- Contacting Ruckus Customer Services and Support..... 7

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	<code>device(config)# interface ethernet 1/1/6</code>
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the Start menu, click All Programs .
<i>italics</i>	Publication titles	Refer to the <i>Ruckus Small Cell Release Notes</i> for more information.

Notes, Cautions, and 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.
<i>italic text</i>	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, <i>member[member...]</i> .
\	Indicates a “soft” line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Document Feedback

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

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

When contacting us, include the following information:

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

For example:

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

Ruckus Product Documentation Resources

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

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

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

Online Training Resources

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

Contacting Ruckus Customer Services and Support

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

For product support information and details on contacting the Support Team, go directly to the Ruckus Support Portal using <https://support.ruckuswireless.com>, 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 <https://support.ruckuswireless.com/contact-us> 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>

Preface

Contacting Ruckus Customer Services and Support

- Community Forums—<https://forums.ruckuswireless.com/ruckuswireless/categories>
- Knowledge Base Articles—<https://support.ruckuswireless.com/answers>
- Software Downloads and Release Notes—https://support.ruckuswireless.com/#products_grid
- Security Bulletins—<https://support.ruckuswireless.com/security>

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

About This Guide

- [Introduction to Ruckus IoT Controller](#).....9

Introduction to Ruckus IoT Controller

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

This guide is written 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 Enhancements in Ruckus IoT Controller Release 1.4

Feature	Description	Location
BLE Beacon Visualization	BLE Beacon is seen in the IoT Device tab as any other connected device.	Refer to Devices Overview on page 65
Multi Radio Support per Access Point	Access Point supports internal and external (USB) radios.	Refer to Single IoT Access Point Mode on page 60
Forced Fallback	If the Slave is acting as an Active Slave, and if the Master comes back online, the Forced Fallback feature can be applied, for Master to resume the Active Master role. Active Slave will assume Slave role.	Refer to Configuring N+1 on page 17
Replace Master or Slave	If a Master or Slave goes down to an unrecoverable state, a new IoT Controller can be added (replaced) to the 1+1 cluster, where the new IoT Controller resumes the role of the IoT Controller that was not up and running.	Refer to Configuring N+1 on page 17
Controller Data Stream Connector	Once the connector is enabled, controller parses and packs IoT Device information into JSON format and pushes it to the MQTT Broker.	Refer to Activating and Editing the Controller Data Stream Plugin on page 45
Beacon as a Service Connector	Upon enabling this connector, the mapped IoT APs starts BLE beaconing OTA.	Refer to Activating and Editing the Beacon as a Service Plugin on page 43

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".

Getting Started

Logging In to Ruckus IoT Controller

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

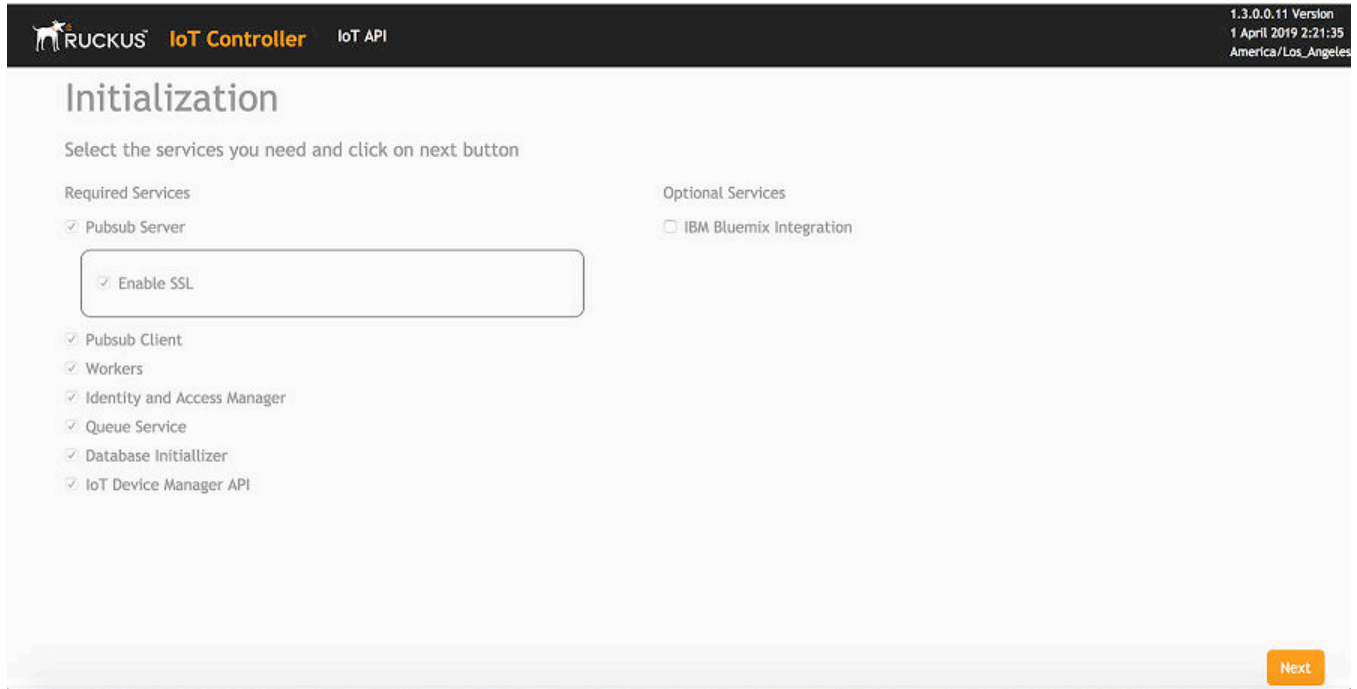
Enter Choice: 1

-----
Network info :
-----
IP (eth0)       : 10.174.112.79/23
Gateway        : 10.174.112.1
Hostname       : 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



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

- Pubsub Server
- Pubsub Client
- Workers
- Identity and Access Manager
- Queue Service
- Database Initializer
- IoT Device Manager API

Pubsub Server works in SSL mode.

Ruckus IoT Controller services are sensitive to time synchronization. If the NTP Sync option is not available (such as in an isolated setup), ensure NTP Sync is disabled in the CLI (Option 3).

Optional services and connectors that can be started include IBM Bluemix Integration. When starting an optional service, additional values must be provided. For example, for IBM Bluemix Integration, the API Key, API Secret, Organization ID, Gateway ID, Gateway Type, and Gateway Token values must be provided.

Getting Started

Logging In to Ruckus IoT Controller

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

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

FIGURE 3 Initialization Page After Accepting Services

1.3.0.0.11 Version
1 April 2019 2:21:48
America/Los_Angeles

Initialization

Select the services you need and click on start button

VM Configurations

Hostname

vriot

Time Zone

America/Los_Angeles

IP Configurations

DHCP Static

Set Time Automatically using NTP Set Time Manually i

NTP Address

Default : ntp.ubuntu.com (Optional)

Back Start

NOTE

The figure shows a DHCP configuration.

5. On the **Ruckus IoT Controller Login** page, enter the username "admin" and password "admin".

FIGURE 4 Ruckus IoT Controller Login Page

RuckusIoT Controller

Username:

Password: Show

Login

You are logged in to the Ruckus IoT Controller.

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

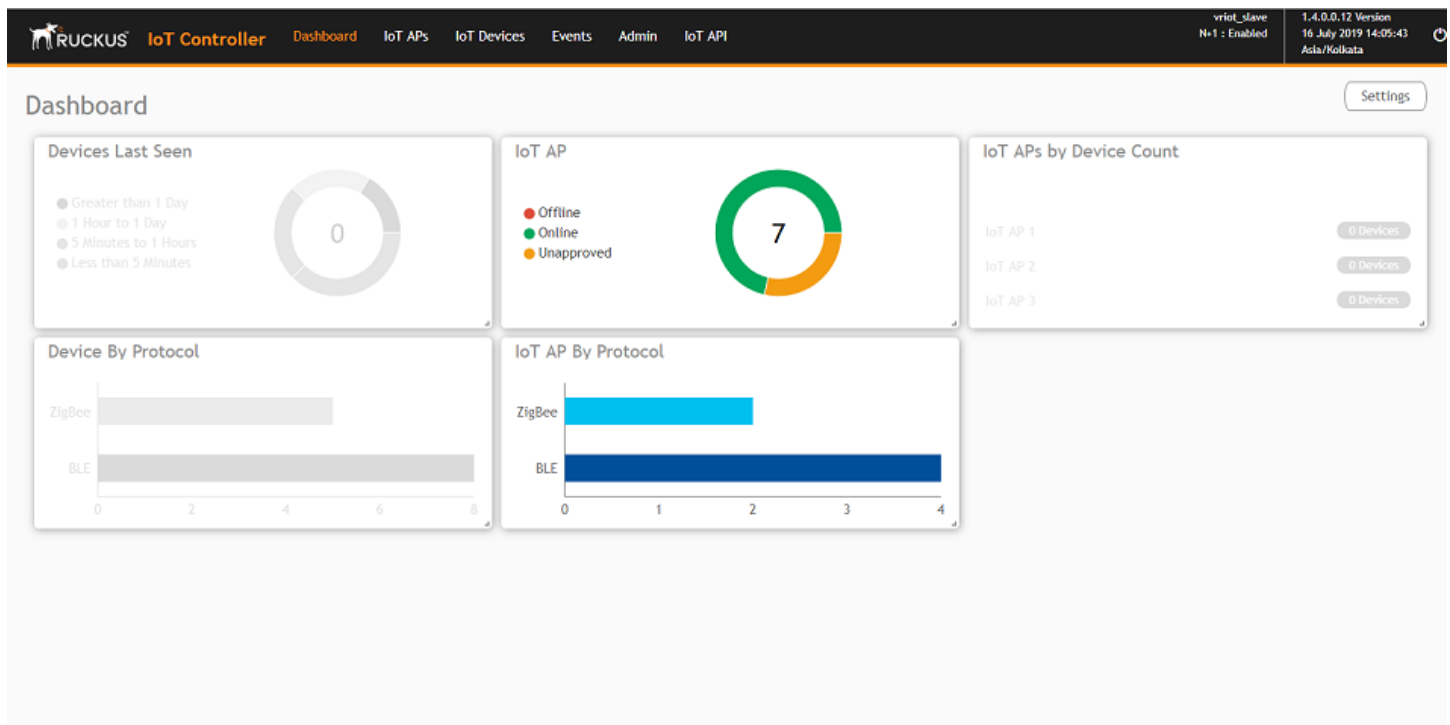


TABLE 4 Dashboard Elements

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

Getting Started

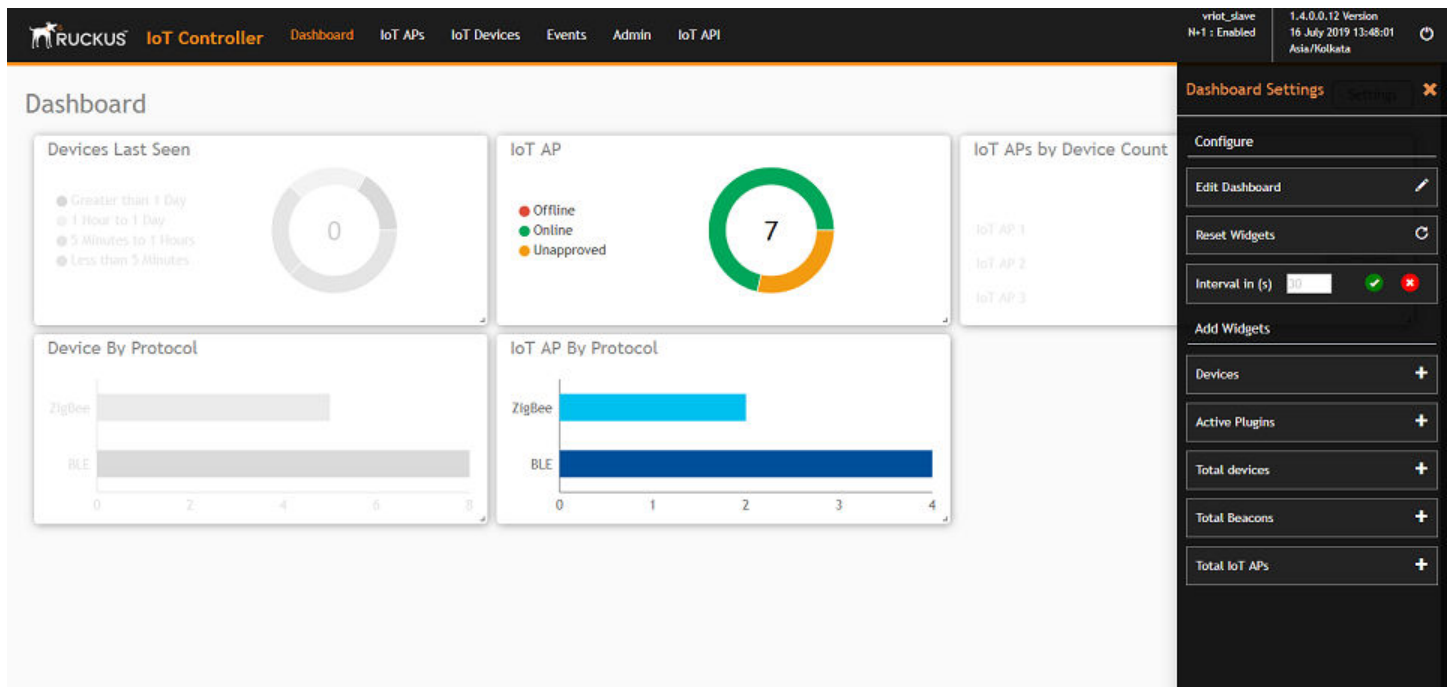
Getting to Know the Dashboard

TABLE 4 Dashboard Elements (continued)



Box Name	Description
Device By Protocol	Shows the total number of devices connected by the protocol being used. Ruckus supports two protocols: BLE and Zigbee.

To set up the **Dashboard**, click the **Settings** tab. The **Dashboard Settings** window is displayed.

FIGURE 6 Dashboard Settings



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

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

NOTE

The default interval is 30 seconds.

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

Configuring N+1

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

Before beginning to use N+1, pay attention to the following prerequisites for configuring the master and slave:

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

Configuring Static Addresses for Master and Slave

The static IP addresses of the master and slave can be configured in two ways:

- From the Ruckus IoT Controller main menu, select **Admin > VM Configurations**.
- Set the static address of the master and slave 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 master and slave, 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

```
*****
                                Ruckus IoT Controller
                                Main Menu
*****

1 - Ethernet Network
2 - System Details
3 - NTP Setting
4 - System Operation
5 - N+1
6 - Comm Debugger
x - Log Off

Enter Choice: 5

-----
N+1 Status:
-----
                N+1 Mode      : Disabled
-----

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

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

FIGURE 8 Continuing the Configuration

```
*****
                        Ruckus IoT Controller
                        Main Menu
*****

1 - Ethernet Network
2 - System Details
3 - NTP Setting
4 - System Operation
5 - N+1
6 - Comm Debugger
x - Log Off

Enter Choice: 5

-----
N+1 Status:
-----
          N+1 Mode          : Disabled
-----

N+1 Configure(1) / Disable(2) / Exit(x) :1
Start Master(1) / Slave(2) / Exit(x) :█
```

4. To configure the master, enter **1** and type the IP address of the slave in the **Enter Slave IP** field.

FIGURE 9 Configuring the Master

```
*****
                        Ruckus IoT Controller
                        Main Menu
*****

1 - Ethernet Network
2 - System Details
3 - NTP Setting
4 - System Operation
5 - N+1
6 - Comm Debugger
x - Log Off

Enter Choice: 5

-----
N+1 Status:
-----
                N+1 Mode      : Disabled
-----

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

-----
N+1 Configure:
-----
To Configure N+1 ensure following requirements:
*****
* Master and Slave should be in same subnet and reachable.
* Master and Slave should be configured with static ip address.
* Master and Slave should be running in same version.
* Master and Slave should have synchronized date/time.

Enter Slave IP :192.168.100.85█
```

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

NOTE

The Preferred Virtual IP should not be same as master or slave IP.

FIGURE 10 Entering the Preferred Virtual IP Address

```
*****
                        Ruckus IoT Controller
                        Main Menu
*****

1 - Ethernet Network
2 - System Details
3 - NTP Setting
4 - System Operation
5 - N+1
6 - Comm Debugger
x - Log Off

Enter Choice: 5

-----
N+1 Status:
-----
           N+1 Mode       : Disabled
-----

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

-----
N+1 Configure:
-----
To Configure N+1 ensure following requirements:
*****
* Master and Slave should be in same subnet and reachable.
* Master and Slave should be configured with static ip address.
* Master and Slave should be running in same version.
* Master and Slave should have synchronized date/time.

Enter Slave IP :192.168.100.85
Enter preferred Virtual IP :192.168.100.90
```

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

FIGURE 11 Completing the Master Configuration

```
*****
                          Ruckus IoT Controller
                          Main Menu
*****

1 - Ethernet Network
2 - System Details
3 - NTP Setting
4 - System Operation
5 - N+1
6 - Comm Debugger
x - Log Off

Enter Choice: 5

-----
N+1 Status:
-----
          N+1 Mode          : Disabled
-----

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

-----
N+1 Configure:
-----
To Configure N+1 ensure following requirements:
*****
* Master and Slave should be in same subnet and reachable.
* Master and Slave should be configured with static ip address.
* Master and Slave should be running in same version.
* Master and Slave should have synchronized date/time.

Enter Slave IP :192.168.100.85
Enter preferred Virtual IP :192.168.100.90
N+1 will stop all services & configurations in Slave. Enter Y/N to continue : y

          Configuring takes around 5-10 minutes. Please wait
          Master configuration started..
█
```

After the master configuration has completed, the slave configuration begins.

FIGURE 12 Continuing with the Slave Configuration

```
*****
                                Ruckus IoT Controller
                                Main Menu
*****

1 - Ethernet Network
2 - System Details
3 - NTP Setting
4 - System Operation
5 - N+1
6 - Comm Debugger
x - Log Off

Enter Choice: 5

-----
N+1 Status:
-----
                N+1 Mode          : Disabled
-----

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

-----
N+1 Configure:
-----

To Configure N+1 ensure following requirements:
*****
* Master and Slave should be in same subnet and reachable.
* Master and Slave should be configured with static ip address.
* Master and Slave should be running in same version.
* Master and Slave should have synchronized date/time.

Enter Slave IP :192.168.100.85
Enter preferred Virtual IP :192.168.100.90
N+1 will stop all services & configurations in Slave. Enter Y/N to continue : y

        Configuring takes around 5-10 minutes. Please wait
        Master configuration started..
        Slave configuration started..
```

FIGURE 13 N+1 Configuration Completed

```
*****
Ruckus IoT Controller
Main Menu
*****

1 - Ethernet Network
2 - System Details
3 - NTP Setting
4 - System Operation
5 - N+1
6 - Comm Debugger
x - Log Off

Enter Choice: 5

-----
N+1 Status:
-----

      N+1 Mode      : Disabled
-----

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

-----
N+1 Configure:
-----
To Configure N+1 ensure following requirements:
*****
* Master and Slave should be in same subnet and reachable.
* Master and Slave should be configured with static ip address.
* Master and Slave should be running in same version.
* Master and Slave should have synchronized date/time.

Enter Slave IP :192.168.100.85
Enter preferred Virtual IP :192.168.100.90
N+1 will stop all services & configurations in Slave. Enter Y/N to continue : y

      Configuring takes around 5-10 minutes. Please wait
      Master configuration started..
      Slave configuration started..
      Configuring N+1 completed...
-----
```

You have configured N+1 successfully.

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

FIGURE 14 Verifying the IP Address of the Active Master

```
*****
                                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     : 192.168.100.90
      Mode           : Active Master
      My IP          : 192.168.100.81
      Slave IP       : 192.168.100.85
      ConfigSync     : Not Applicable, Controller is Active.
      Node Status    : vriot(2): normal
vriot_active(1): normal
-----

N+1 Configure(1) / Disable(2) / Replace Slave(3) / Exit(x) : █
```

8. To replace the slave , enter 3.

FIGURE 15 Replacing the Slave IP Address

```
*****
                                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     : 192.168.100.90
      Mode           : Active Master
      My IP          : 192.168.100.81
      Slave IP       : 192.168.100.85
      ConfigSync     : Not Applicable, Controller is Active.
      Node Status    : vriot(2): normal
vriot_active(1): normal
-----

N+1 Configure(1) / Disable(2) / Replace Slave(3) / Exit(x) :3
-----
N+1 Replace :
-----
      Enter Slave IP to replace:192.168.100.74█
```

FIGURE 16 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    : 192.168.100.90
Mode          : Active Master
My IP         : 192.168.100.81
Slave IP      : 192.168.100.85
ConfigSync    : Not Applicable, Controller is Active.
Node Status   : vriot(2): normal
vriot_active(1): normal
-----

N+1 Configure(1) / Disable(2) / Replace Slave(3) / Exit(x) :3
-----

N+1 Replace :
-----

Enter Slave IP to replace:192.168.100.89
Deleted nodes
Start replacing slave
Slave configuration started..
Replace node taking more time to start services
Replacing node completed
-----
█
```

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

FIGURE 17 Configuring Forced Fallback

```
*****
                        Ruckus IoT Controller
                        Main Menu
*****

1 - Ethernet Network
2 - System Details
3 - NTP Setting
4 - System Operation
5 - N+1
6 - Comm Debugger
x - Log Off

Enter Choice: 5

-----
N+1 Status:
-----
      N+1 Mode       : Enabled
      Virtual IP     : 192.168.100.90
      Mode           : Master
      My IP          : 192.168.100.81
      Slave IP       : 192.168.100.89
      ConfigSync     : 07/17/2019 03:25:01
      Node Status    : vriot_active(1): normal
vriot_fallback(2): normal
-----

N+1 Configure(1) / Disable(2) / Forced Fallback(3) / Exit(x) :3
-----
N+1 Forced Fallback :
-----
      N+1 will make Master as Active master and Active Slave as Slave.Enter Y/N to continue : y
      Started Fallback
Forced fallback successful
-----
█
```

10. To replace the master, enter 3.

FIGURE 18 Replacing the Master

```
*****
                                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    : 192.168.100.90
      Mode          : Active Slave
      My IP         : 192.168.100.89
      Master IP     : ["192.168.100.81"]
      ConfigSync    : Not Applicable, Controller is Active.
      Node Status   : vriot_active(1): normal
vriot_fallback(2): normal
-----

N+1 Configure(1) / Disable(2) / Replace Master(3) / Exit(x) :3
```

11. Enter the IP address of the master.

FIGURE 19 Continuing with Replacing the Master

```
*****
                                     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     : 192.168.100.90
      Mode           : Active Slave
      My IP          : 192.168.100.89
      Master IP      : ["192.168.100.81"]
      ConfigSync     : Not Applicable, Controller is Active.
      Node Status    : vriot_active(1): normal
vriot_fallback(2): normal
-----

N+1 Configure(1) / Disable(2) / Replace Master(3) / Exit(x) :3
-----
N+1 Replace :
-----
      Enter Master IP to replace:192.168.100.85█
```

Replacing the master has been successfully completed.

FIGURE 20 Completion of Replacing the Master

```
*****
                        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     : 192.168.100.90
      Mode           : Active Slave
      My IP          : 192.168.100.85
      Master IP      : ["192.168.100.81"]
      ConfigSync     : Not Applicable, Controller is Active.
      Node Status    : vriot(2): normal
vriot_active(1): normal
-----

N+1 Configure(1) / Disable(2) / Replace Master(3) / Exit(x) :3
-----

N+1 Replace :
-----

      Enter Master IP to replace:192.168.100.89
Deleted nodes
      Start replacing master
      Slave configuration started..
Slave start failed
Replacing node completed
-----
█
```


Managing IoT Controller System Configuration

- Managing Services..... 33
- Activating and Editing the Plugins..... 34
- Changing the Password..... 47
- Configuring Virtual Machines..... 47
- Uploading Versions and Patches..... 48
- Backing Up Files..... 50
- Rebooting Ruckus IoT Controller..... 51
- Resetting Ruckus IoT Controller..... 52

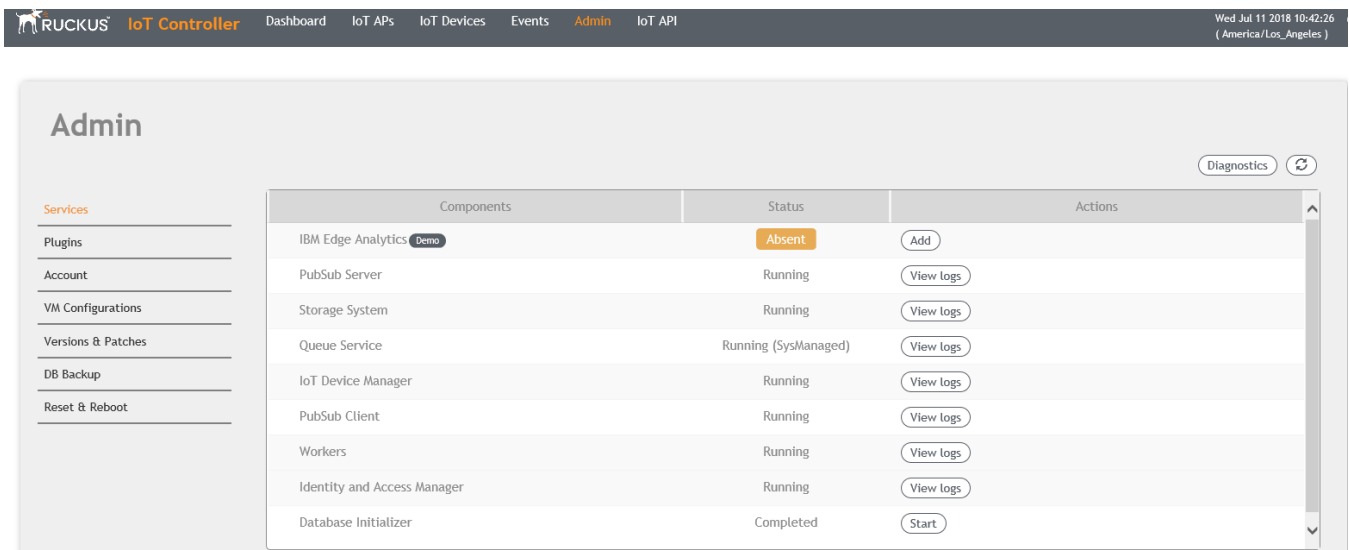
Managing Services

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



The currently running services and their details are displayed.

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

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, and Eddystone.

Activating and Editing the Kontakt.io Beacons Plugin

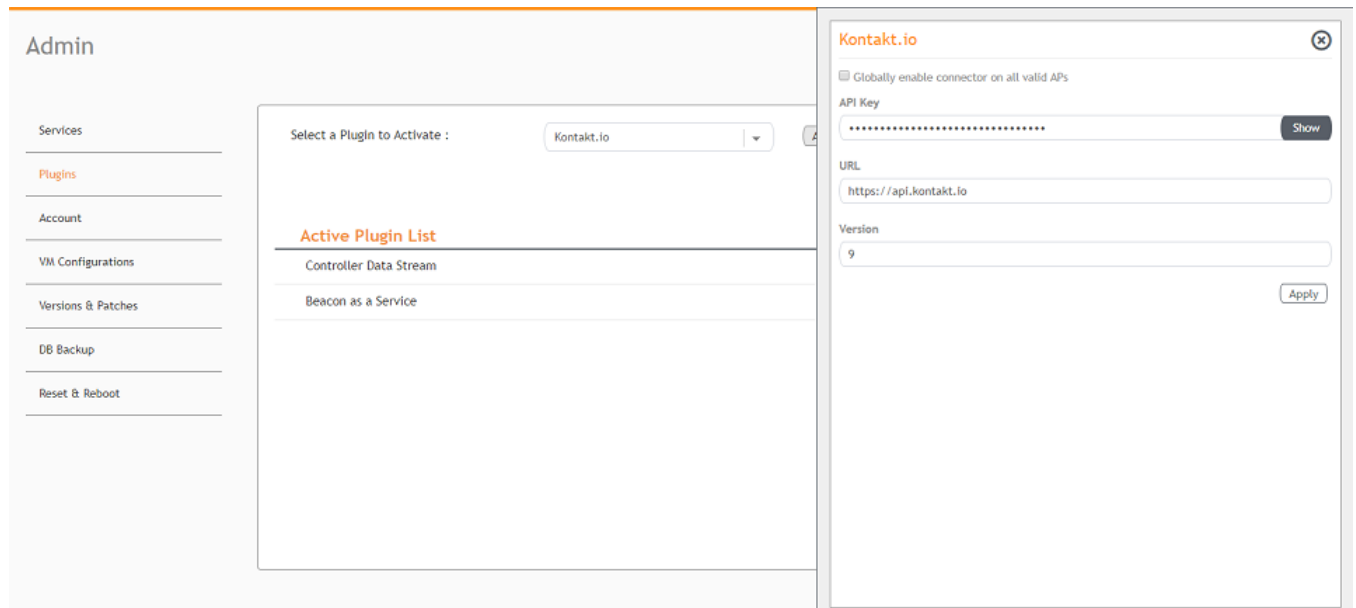
The Ruckus IoT Controller provides support for the Kontakt.io Beacons plugin.

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**.

After the plugin is activated, map each IoT AP to a SoftAPID. SoftAPID is a feature of Kontakt.io available from the Kontakt.io system. The SoftAPID (for example, xyz12) must be mapped to an IoT AP using the tag feature. The tag value is `kontakt:softapid`, for example, `kontakt:xyz12`. SoftAPID can be obtained from the Kontakt.io cloud under the **Gateway** tab. After the Kontakt.io plugin has been activated, and the SoftAPID tags are present, beacon management is performed from the Kontakt.io cloud panel and applications.

FIGURE 22 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 then you can activate the plugin for each AP by adding tag. Refer [Adding Tags to an AP](#) on page 61 for more information.

- b) 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.

- c) 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.

- d) Enter the Version number.

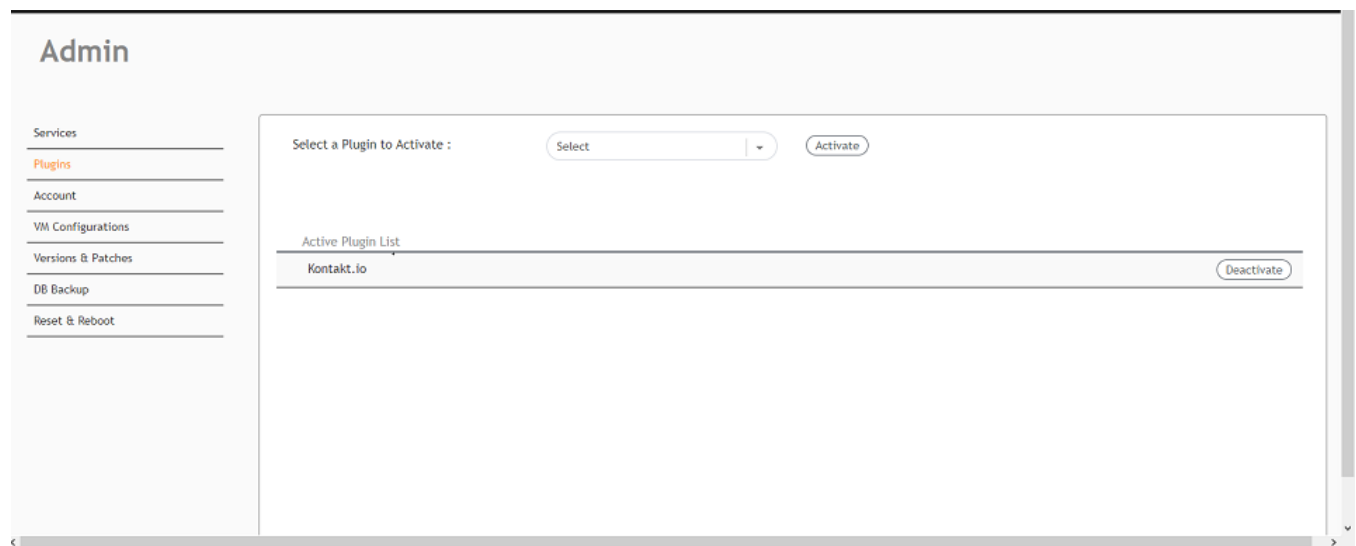
The default version number is 9.

5. Click **Apply**.

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

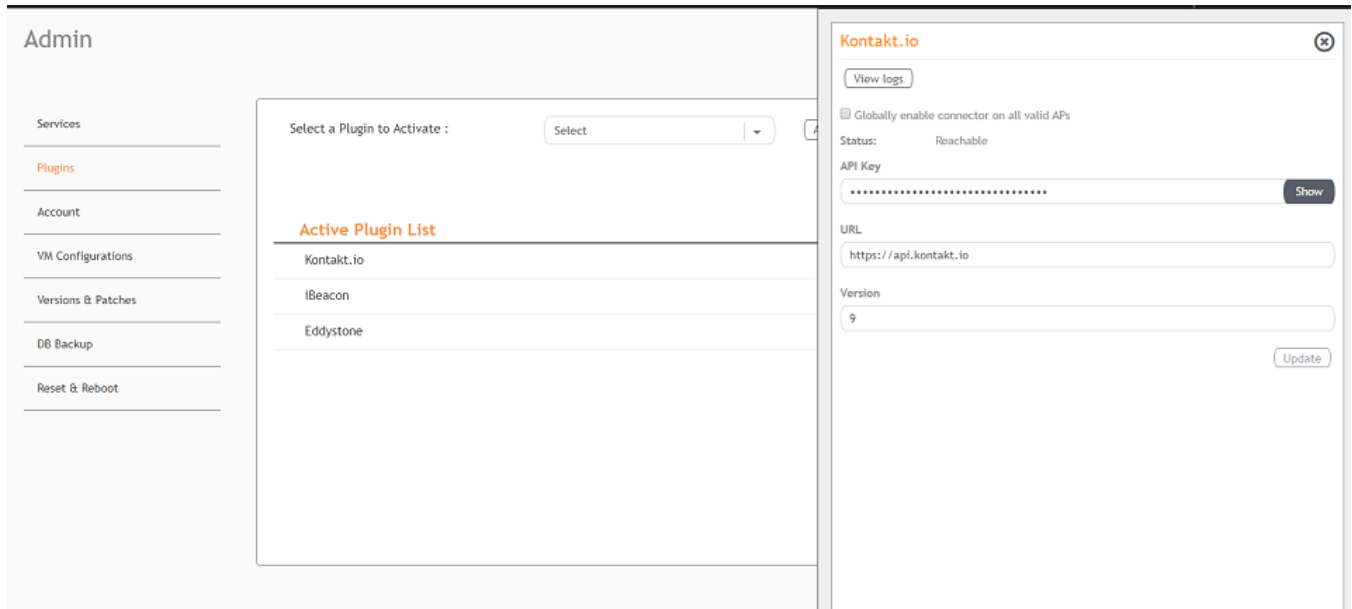
6. To deactivate the Kontakt.io plugin, select it and click **Deactivate**.

FIGURE 23 Deactivating the Kontakt.io Plugin



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

FIGURE 24 Updating the Configuration Parameters



Activating and Editing the Eddystone Plugin

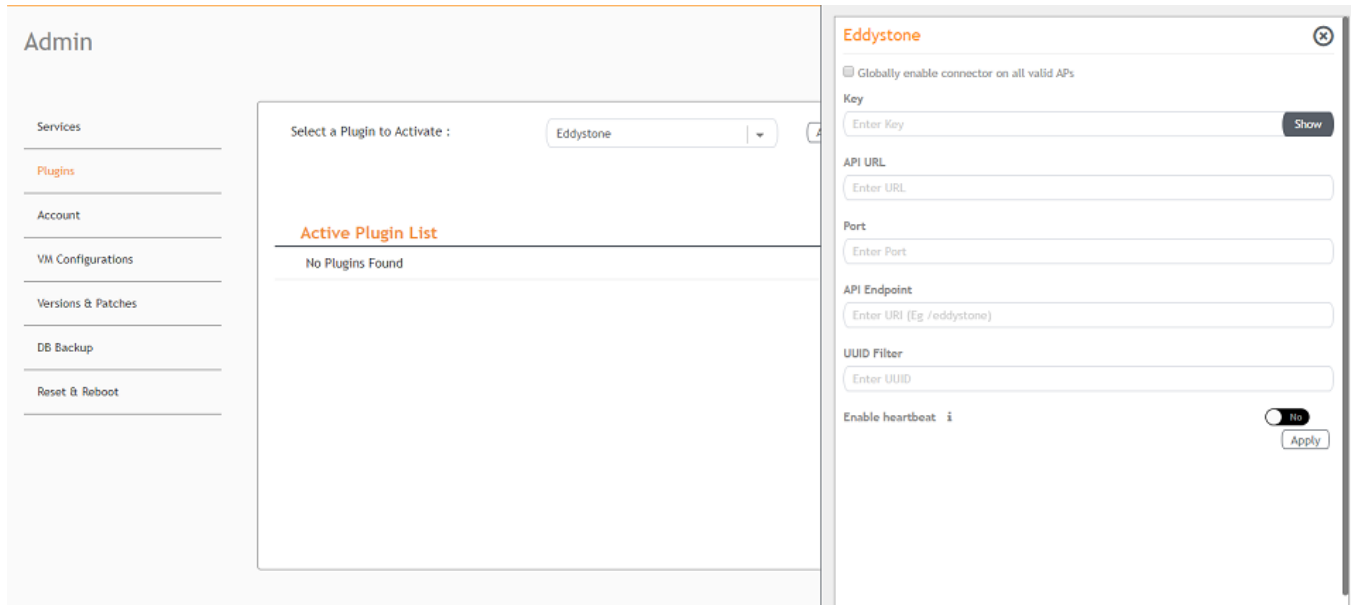
The Ruckus IoT Controller provides support for the Bluetooth Low Energy (BLE) Eddystone plugin. The Ruckus IoT Controller reads the packet from IoT AP, and routes the packets to the BLE beacon vendor cloud services.

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 25 Activating the Eddystone Plugin



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 then you can activate the plugin for each AP by adding tag. Refer [Adding Tags to an AP](#) on page 61 for more information.

- b) Enter the Key.

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

- c) 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.

- d) Enter the Port number.

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

- e) Enter the API Endpoint.

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

- f) Enter the UUID Filter.

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

- g) Enable heartbeat.

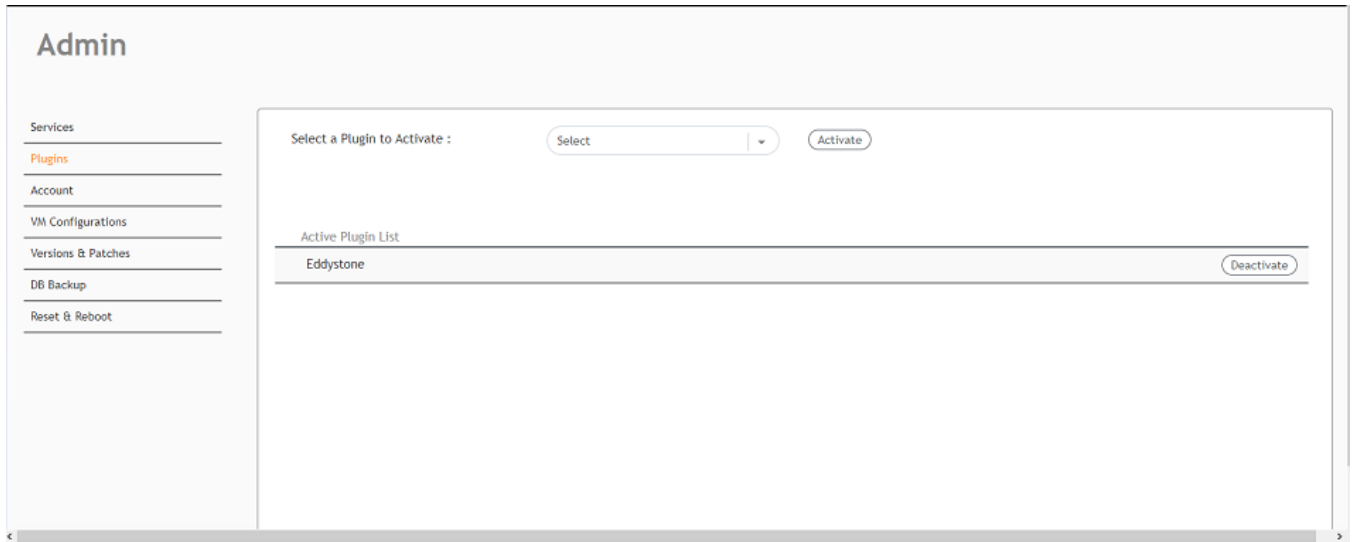
Enabling heartbeat allows the vendor application to receive the IoT AP status, such as online or offline.

5. Click **Apply**.

The Eddystone plugin is added in the **Active Plugin List**.

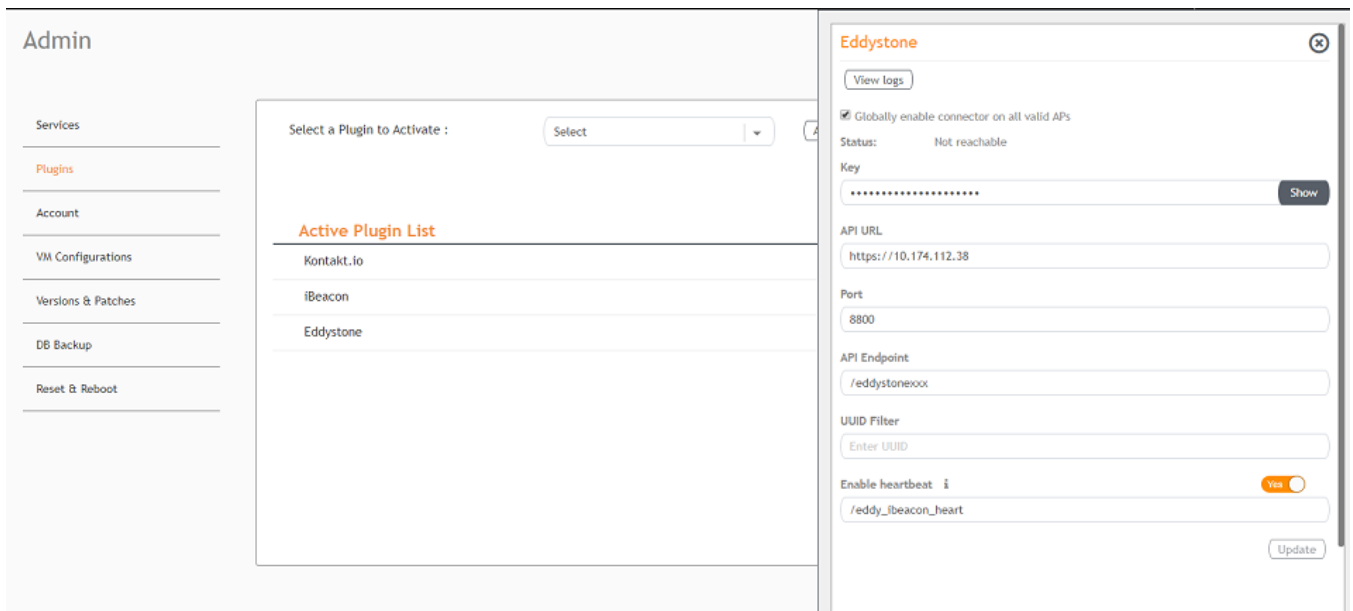
- To deactivate the Eddystone plugin, select it and click **Deactivate**.

FIGURE 26 Deactivating the Eddystone Plugin



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

FIGURE 27 Updating the Configuration Parameters



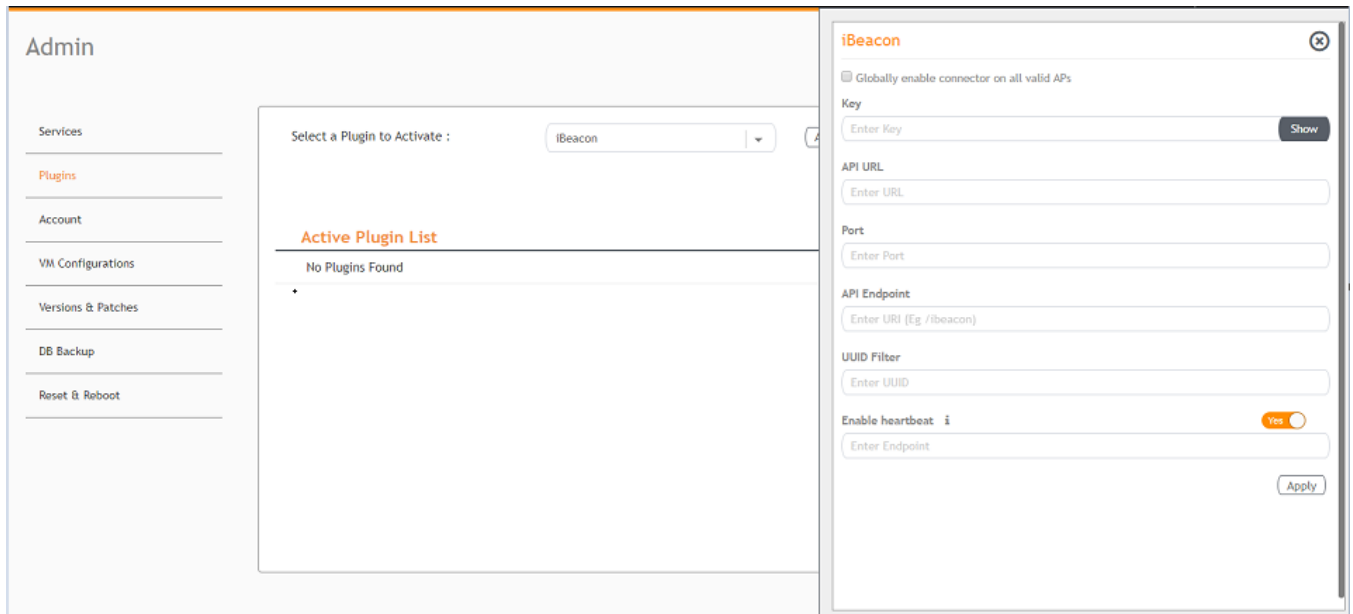
Activating and Editing the iBeacon Plugin

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 28 Activating the iBeacon Plugin



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 then you can activate the plugin for each AP by adding tag. Refer [Adding Tags to an AP](#) on page 61 for more information.

- b) Enter the Key.

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

- c) 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.

- d) Enter the Port number.

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

- e) Enter the API Endpoint.

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

- f) Enter the UUID Filter.

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

- g) Enable heartbeat.

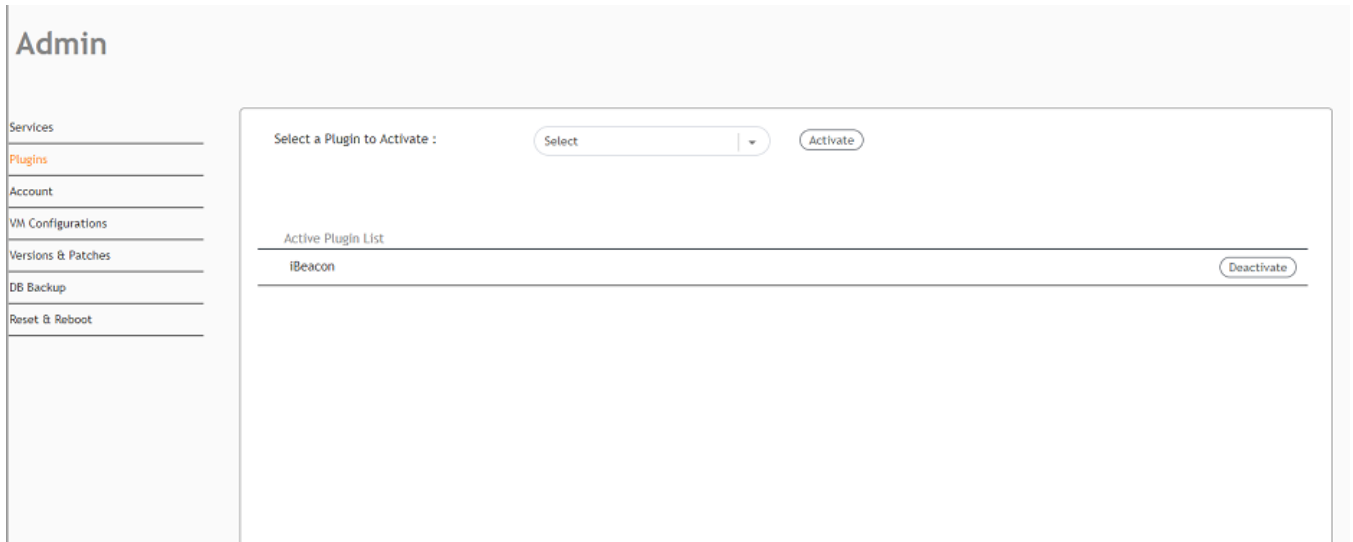
Enabling heartbeat allows the vendor application to receive the IoT AP status, such as online or offline.

5. Click **Apply**.

The iBeacon plugin is added in the **Active Plugin List**.

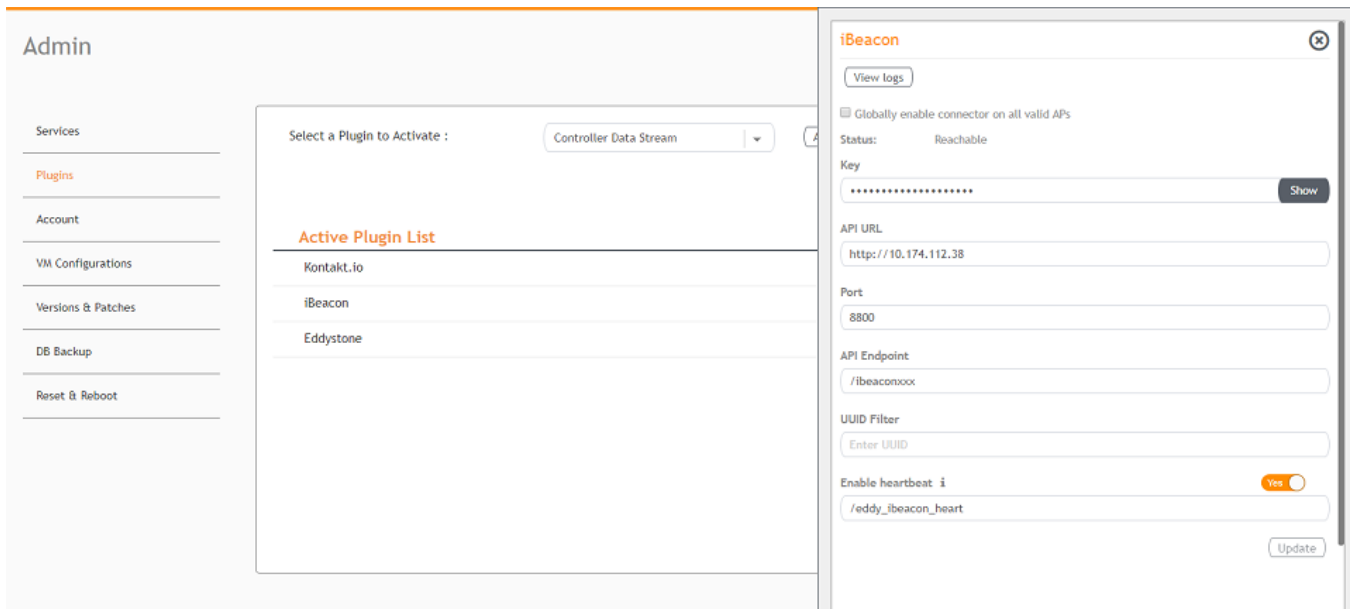
- To deactivate the iBeacon plugin, select it and click **Deactivate**.

FIGURE 29 Deactivating the iBeacon Plugin



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

FIGURE 30 Updating the Configuration Parameters



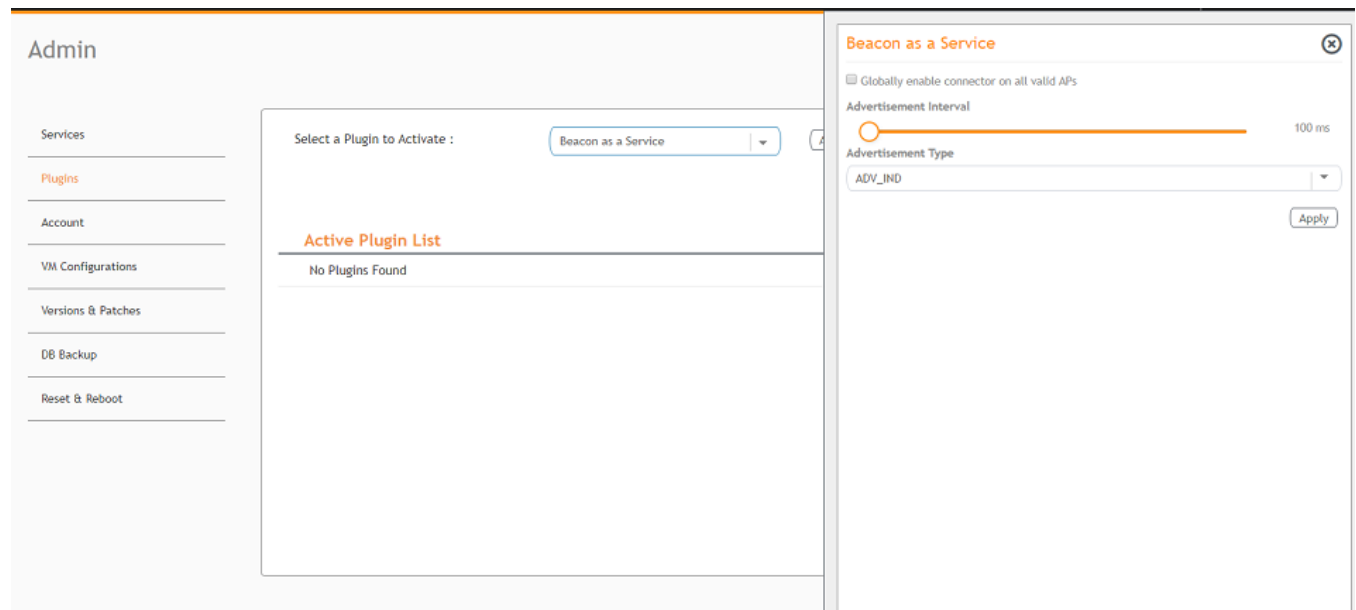
Activating and Editing the Beacon as a Service Plugin

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 31 Activating the Beacon as a Service Plugin



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

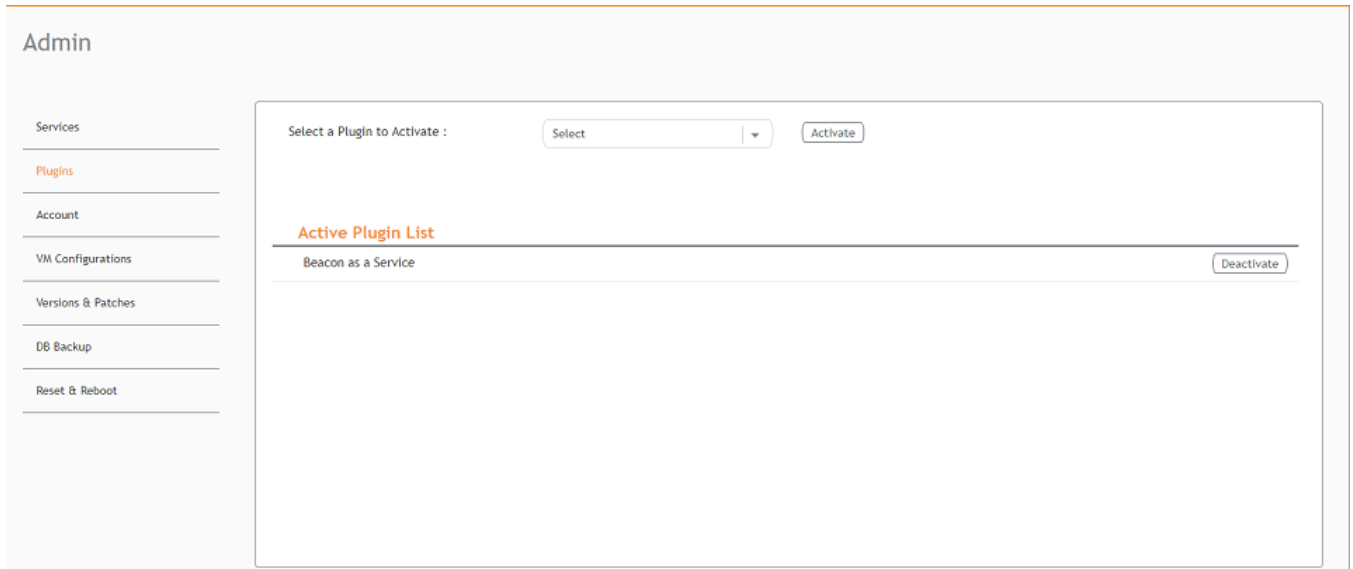
If **Globally enable connector on all valid APs** is not selected then you can activate the plugin for each AP by adding tag. Refer [Adding Tags to an AP](#) on page 61 for more information.

- 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 **Advertisement Type** list, select the type of advertisement.
5. Click **Apply**.

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

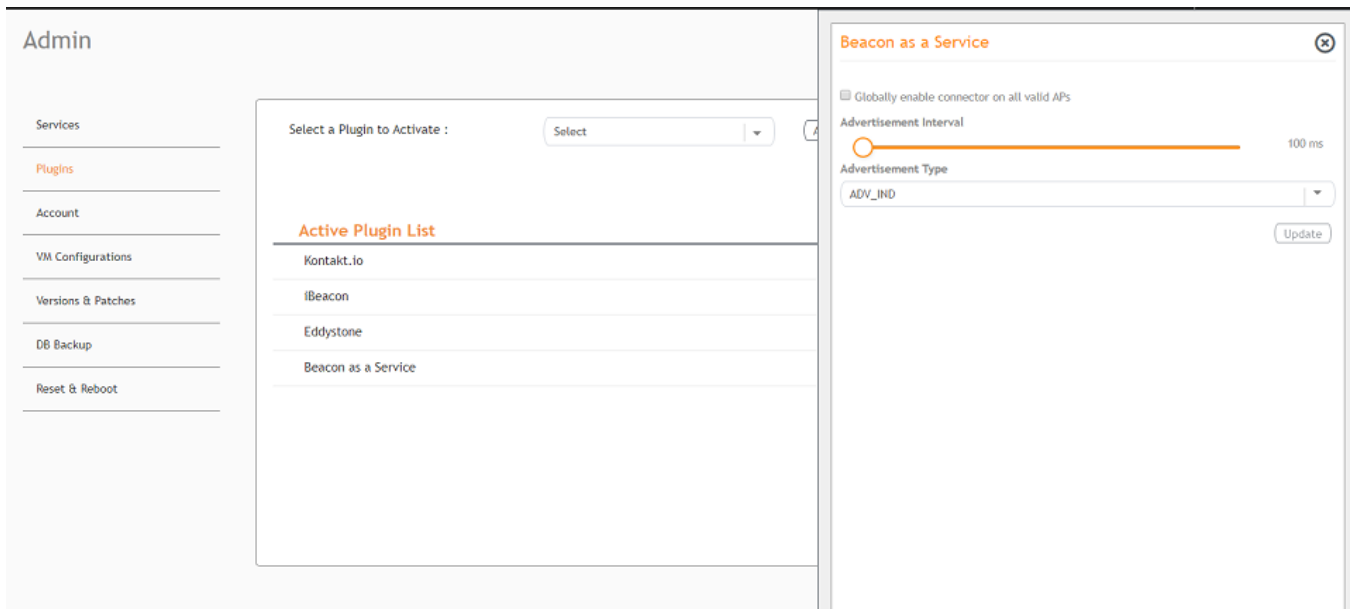
- To deactivate the Beacon as a Service plugin, select it and click **Deactivate**.

FIGURE 32 Deactivating the Beacon as a Service Plugin



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

FIGURE 33 Updating the Configuration Parameters



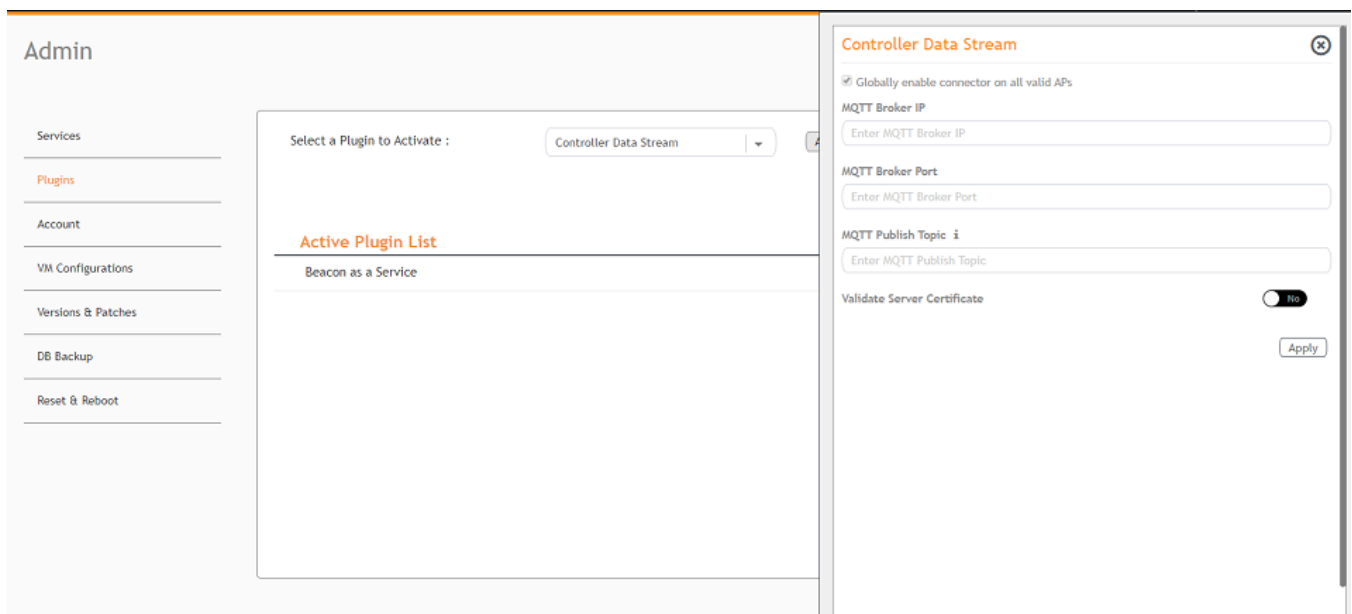
Activating and Editing the Controller Data Stream Plugin

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 34 Activating the Controller Data Stream Plugin



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

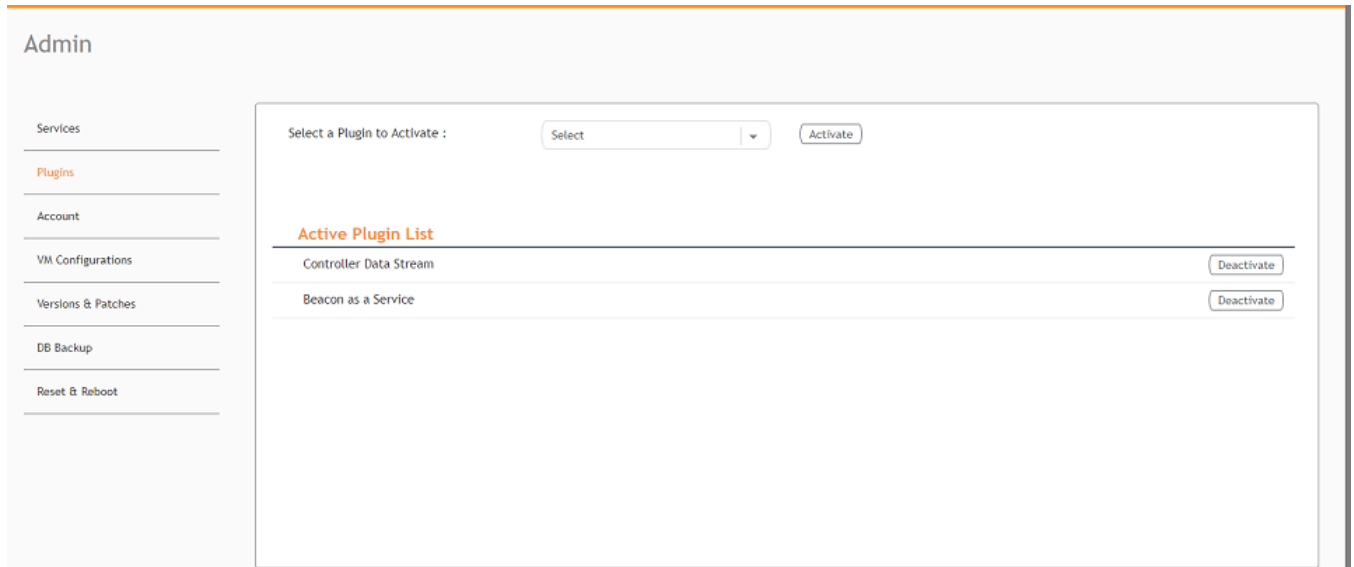
If **Globally enable connector on all valid APs** is not selected then you can activate the plugin for each AP by adding tag. Refer [Adding Tags to an AP](#) on page 61 for more information.

- 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) 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**.

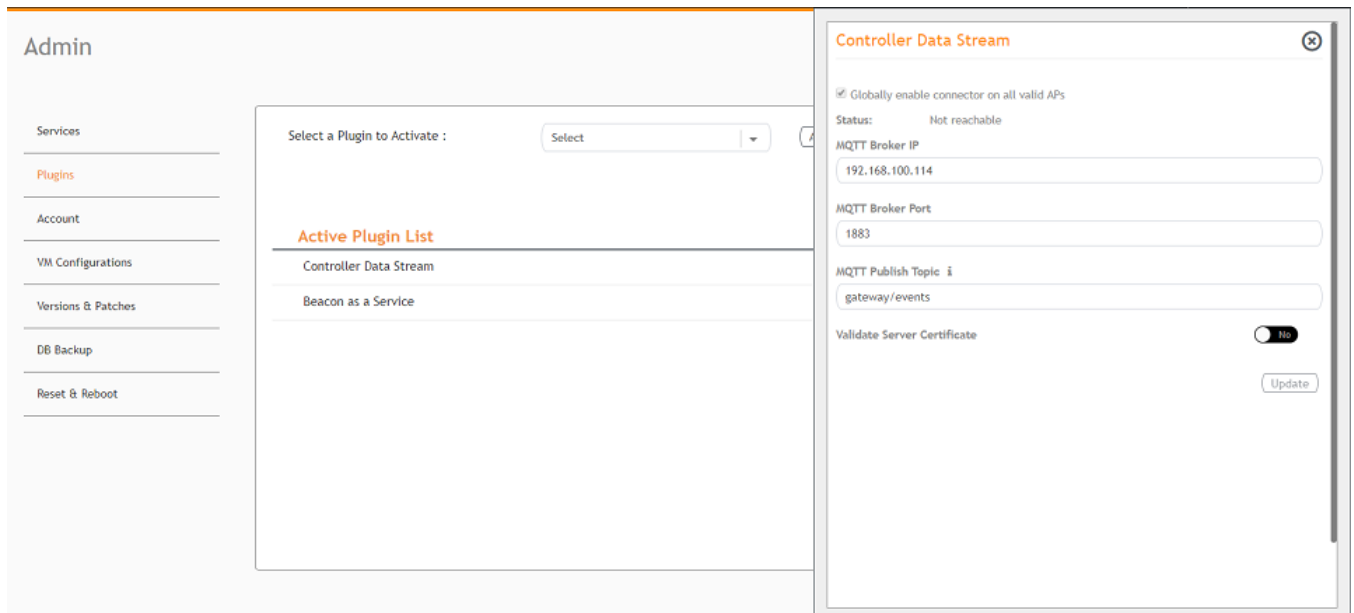
- To deactivate the Controller Data Stream plugin, select it and click **Deactivate**.

FIGURE 35 Deactivating the Controller Data Stream Plugin



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

FIGURE 36 Updating the Configuration Parameters



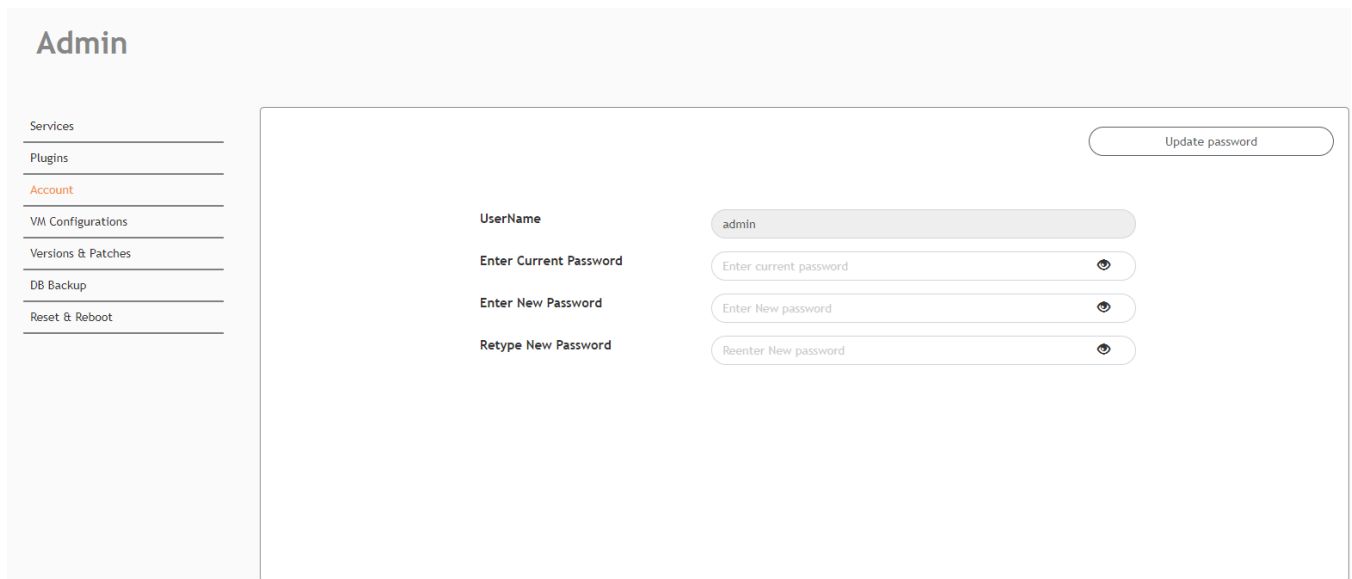
Changing the Password

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 37 Changing the Password



The screenshot shows the 'Admin' interface. On the left is a navigation menu with the following items: Services, Plugins, Account (highlighted in red), VM Configurations, Versions & Patches, DB Backup, and Reset & Reboot. The main content area is titled 'Admin' and contains a form for changing the password. The form includes a 'UserName' field with the value 'admin', and three password fields: 'Enter Current Password', 'Enter New Password', and 'Retype New Password'. Each password field has a toggle icon to show or hide the password. An 'Update password' button is located in the top right corner of the form area.

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 38 Configuring a Virtual Machine

The screenshot shows the 'Admin' interface for configuring a virtual machine. On the left is a navigation menu with 'VM Configurations' selected. The main area contains several configuration sections: 'Hostname*' with a text input 'RIoT'; radio buttons for 'DHCP' (selected) and 'Static'; 'Time Zone' with a dropdown menu set to 'America/Los_Angeles'; radio buttons for 'Set Time Automatically using NTP' (selected) and 'Set Time Manually'; and 'NTP Address' with a text input 'ntp.ubuntu.com' and a red '(Optional)' label. On the right, the 'Current Certificate' section displays 'Common Name : local-mqtt.video54.local' and 'Certificate Expires on Mar 25 16:13:59 2029 GMT', along with two text areas for pasting a certificate and a key, and an 'Update' button.

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.

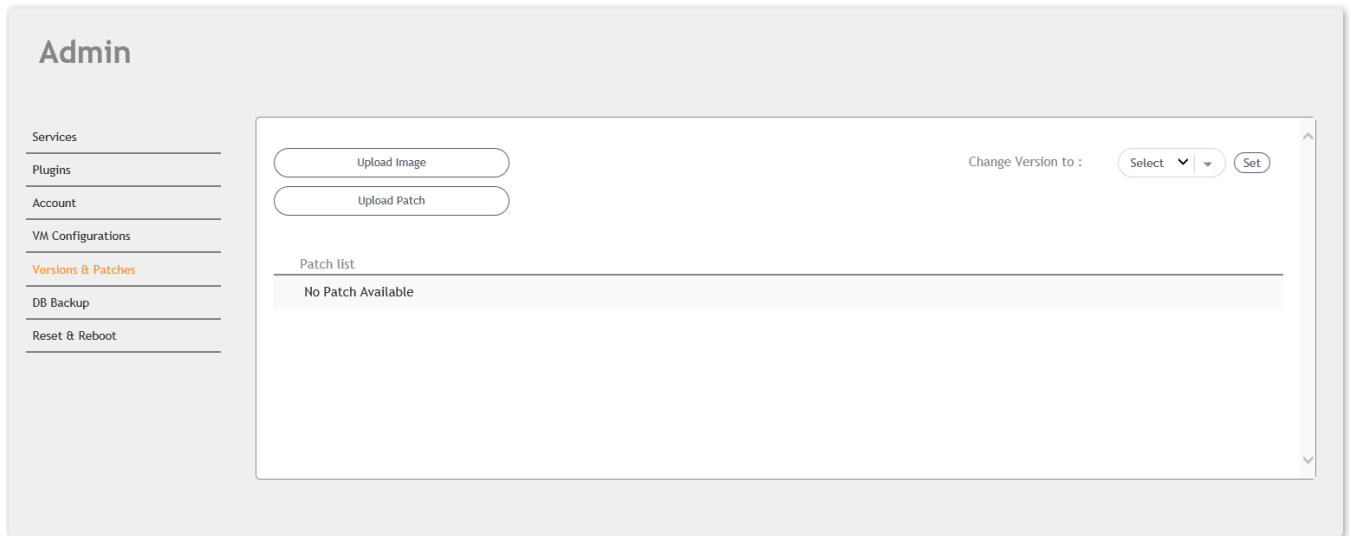
Uploading an Image

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 39 Uploading an Image



3. Click **Upload Image** to upload the upgrade package.
Once uploaded, the new version is listed in the **Change Version to** list.
4. Select the latest version to upgrade and click **Set**.

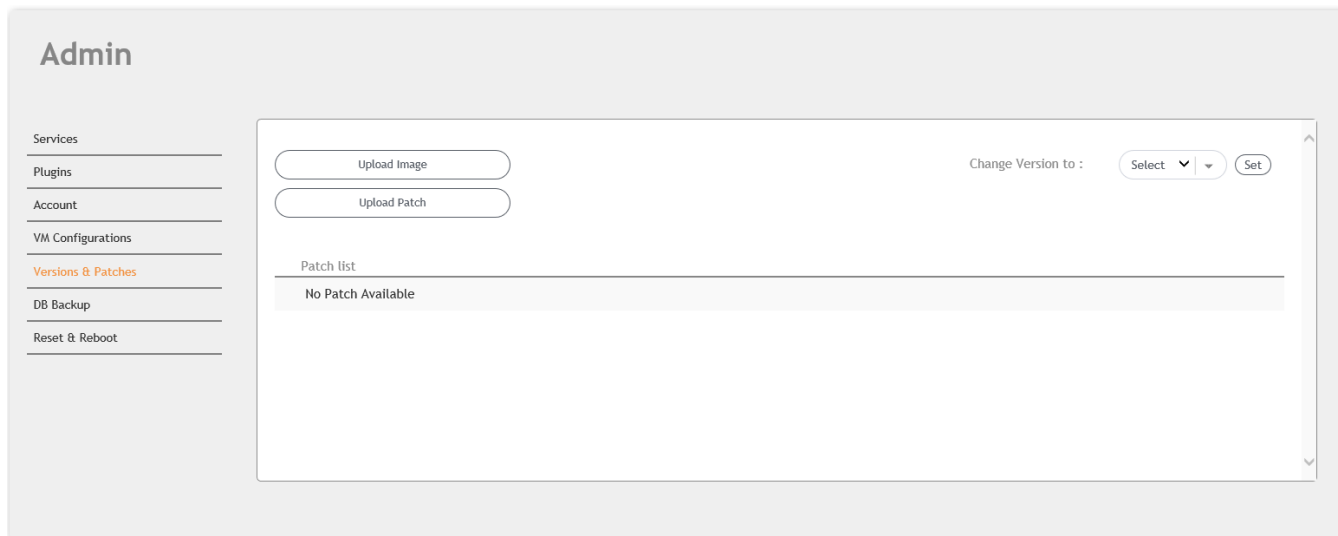
Uploading a Patch

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 40 Uploading a Patch



3. Click **Upload Patch** to upload the patch.

The **Patch list** shows all the applied patches with their statuses and dates.

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 41 Backing Up or Restoring Files



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

NOTE

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

Rebooting Ruckus IoT Controller

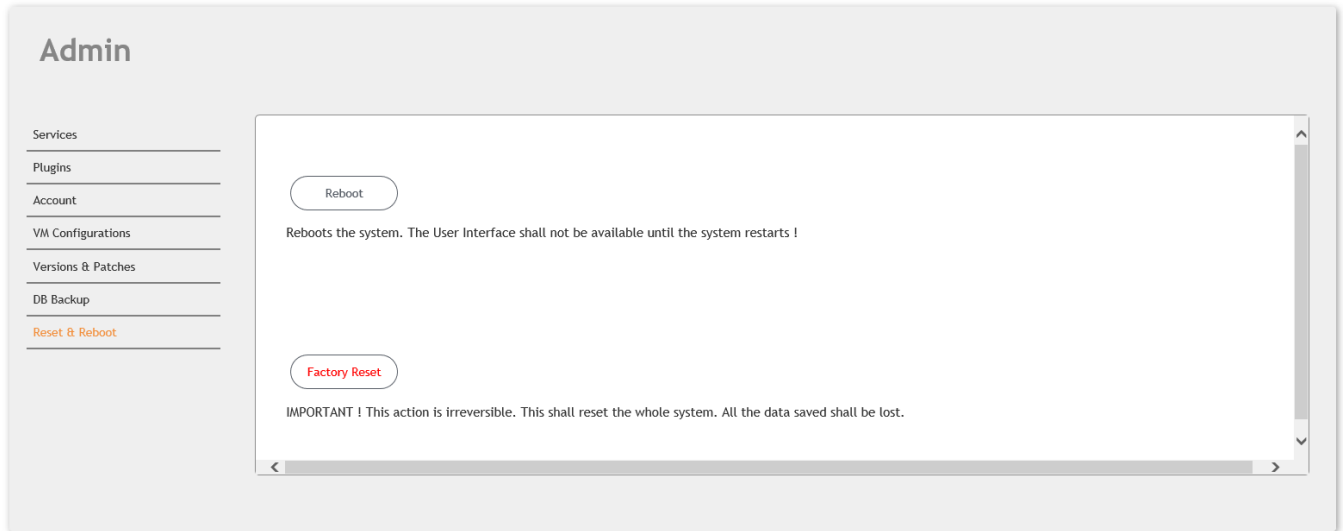
If the Ruckus IoT Controller is experiencing an issue, attempt a reboot to resolve the issue.

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 42 Rebooting Ruckus IoT Controller



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.

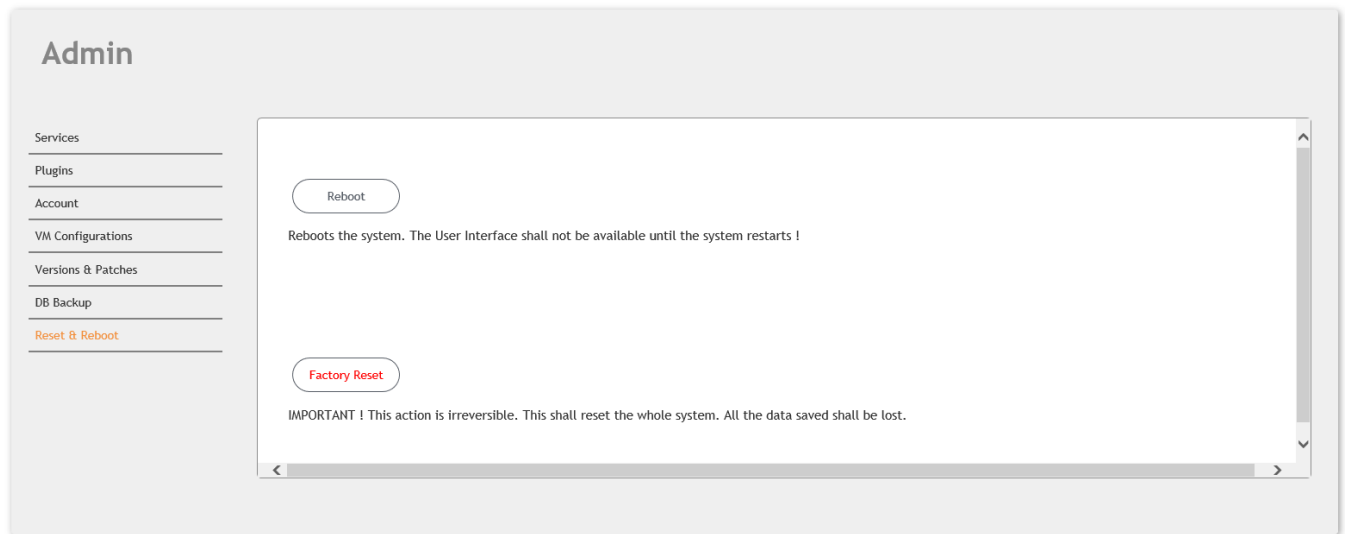


CAUTION
Performing the reset action is irreversible.

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

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

FIGURE 43 Resetting Ruckus IoT Controller



3. Click **Factory Reset**.

Managing IoT Access Points

- IoT AP Overview..... 55
- Adding an IoT AP..... 57
- Editing an IoT AP..... 60
- Adding Tags to an AP..... 61
- Approval of IoT APs..... 63

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 21 and 22. Once the application receives this information, it uses the information to connect to the Ruckus IoT Controller over the Pubsub channel.

NOTE

Configuring a Windows or Linux DHCP server to set up Option 43 is out of scope of this configuration guide.

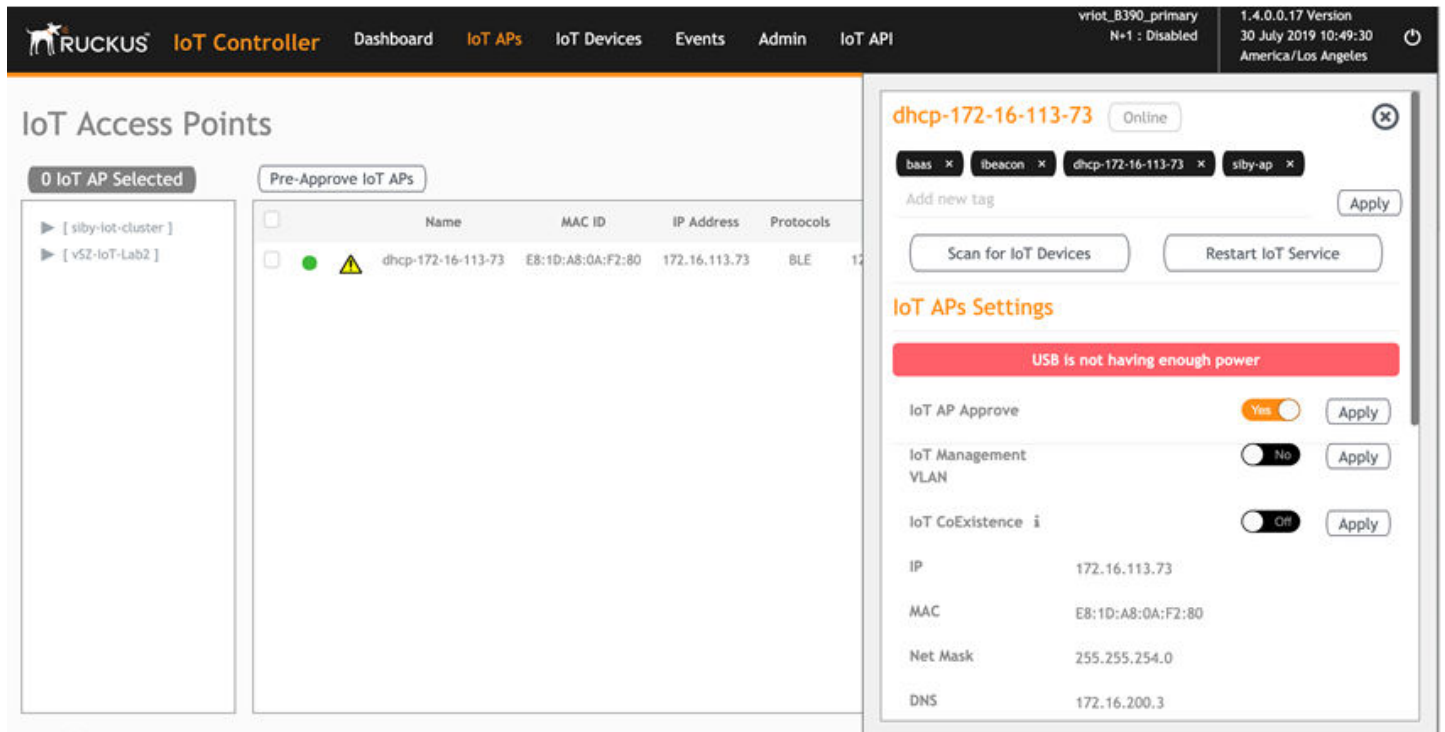
Ruckus Command Line Interface

The `iotg-mqtt-brokerip Ruckus-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 AP page as **USB is not having enough power**.

FIGURE 44 Displaying Shortage of Power



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 45 IoT Access Points Page

The screenshot displays the 'IoT Access Points' management interface. At the top, there is a search bar and a 'Pre-Approve IoT APs' button. Below this, a table lists the configured IoT APs. The table has columns for Name, MAC ID, IP Address, Protocol, Channel, Uptime, and Actions. The 'Actions' column includes search, delete, and a dropdown menu for batch actions. The table shows 12 IoT APs with various statuses (green, red, orange) and configurations.

Name	MAC ID	IP Address	Protocol	Channel	Uptime	Actions	Tags
Karthik-R510-Desk	D8:38:FC:1C:10:90	10.74.136.40	ble	NA	2 days, 0:02:59	[Search] [Delete] [Batch Actions]	[All] [80b] [RuckusIoT0000] [test]
R710	44:1E:98:13:FB:20	192.168.100.37	zigbee_aa	25	5 days, 3:48:52	[Search] [Delete] [Batch Actions]	[All] [44:1E:98:13:FB:20] [RuckusIoT0000] [R710]
R610_Shetty	04:79:C8:04:D9:40	192.168.100.39	ble	NA	NA	[Delete] [Batch Actions]	[All] [04:79:C8:04:D9:40] [80b]
R730	18:7C:08:20:DC:F0	192.168.100.15	zigbee	20	0 days, 0:12:54	[Delete] [Batch Actions]	[All] [18:7C:08:20:DC:F0] [R730]
R510_OUT_RuckusAP_Shriram	EC:8C:A2:37:03:A0	192.168.100.59	zigbee	14	NA	[Delete] [Batch Actions]	[All] [EC:8C:A2:37:03:A0] [R510_OUT_RuckusAP_Shriram]
R510_Shetty	D8:38:FC:1B:FC:D0	192.168.100.77	zigbee	20	NA	[Delete] [Batch Actions]	[All] [D8:38:FC:1B:FC:D0] [RuckusAP]
H510_Shetty	30:87:D9:14:69:00	192.168.100.62	ble	NA	5 days, 3:29:55	[Search] [Delete] [Batch Actions]	[All] [H510_Shetty] [RuckusIoT0000] [30:87:D9:14:69:00]
SW-AP	30:87:D9:15:40:40	192.168.100.58	zigbee	20	2 days, 0:05:36	[Search] [Delete] [Batch Actions]	[All] [SW-AP] [30:87:D9:15:40:40]
H510-RuckusAP-Shriram	0C:F4:D5:1E:97:D0	192.168.100.92	zigbee	19	5 days, 3:49:27	[Search] [Delete] [Batch Actions]	[All] [0C:F4:D5:1E:97:D0] [H510-RuckusAP-Shriram]
R610_AP_Shriram-test	84:79:CB:01:F0:30	192.168.100.54	zigbee_aa	16	5 days, 2:32:23	[Search] [Delete] [Batch Actions]	[All] [R610_AP_Shriram-test] [84:79:CB:01:F0:30]

Total IoT APs : 12

2. Click **Pre-Approve IoT APs**.
The **Pre-Approve IoT APs** page is displayed.

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

FIGURE 46 Adding a Single IoT AP

The screenshot shows a dialog box titled "Pre Approve IoT APs". At the top, there are two tabs: "Single" (which is selected and highlighted in orange) and "Batch". Below the tabs, there is a section for "MAC *" with a text input field containing the value "0E:0D:6F:00:0F:00". Below that is a section for "Tag" with a text input field containing the value "Add new tag". At the bottom of the dialog, there are two buttons: "Cancel" on the left and "Save" on the right.

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 47 Adding a Batch of IoT APs

The screenshot shows a web interface for adding IoT APs. At the top, there is a section titled "Pre Approve IoT APs" with two tabs: "Single" and "Batch". The "Batch" tab is selected and highlighted in orange. Below the tabs, there is a button labeled "Download CSV Template". Underneath that is a file selection area with a "Choose File" button and the text "No file chosen". At the bottom of the interface, there are two buttons: "Cancel" on the left and "Upload" on the right.

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

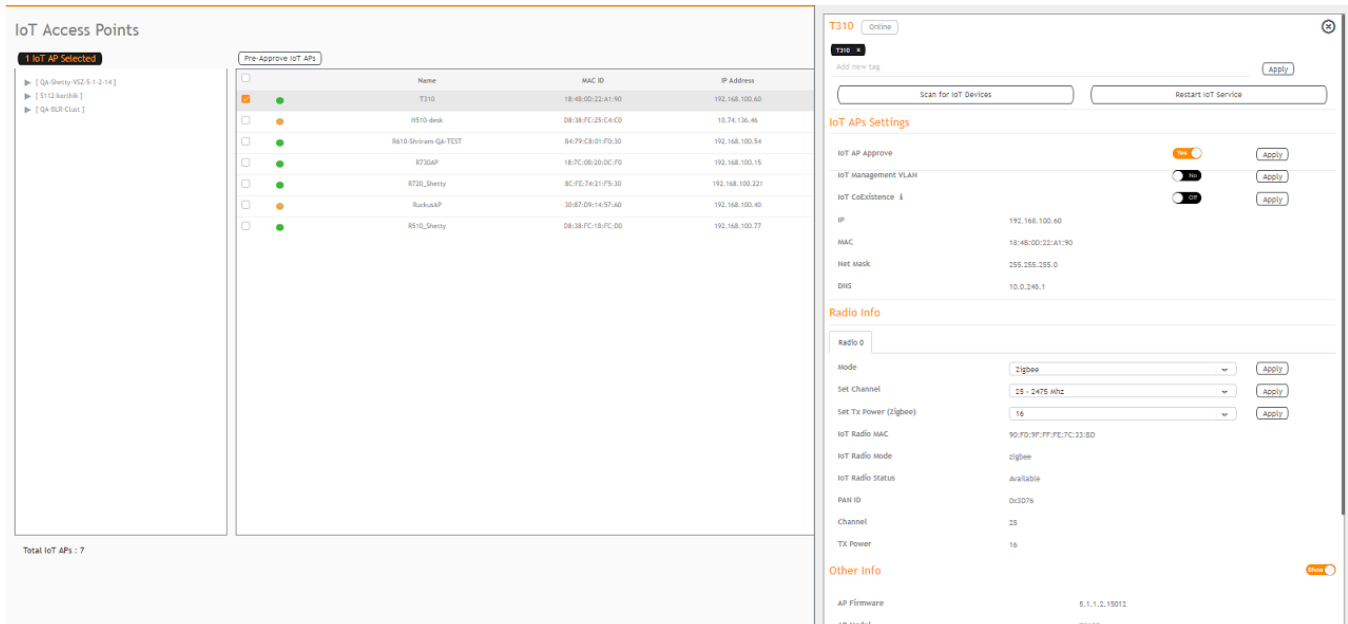
You can use Single IoT Access Point Mode to edit a single IoT AP.

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.

- Click an IoT AP to edit.

FIGURE 48 Single IoT AP Mode



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**
- **Enable 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.

Adding Tags to an AP

The AP tags are a way of grouping APs together by applying an identifying tag. If the **Globally enable connector on all valid APs** is disabled then perform the following to activate the plugin on the AP.

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

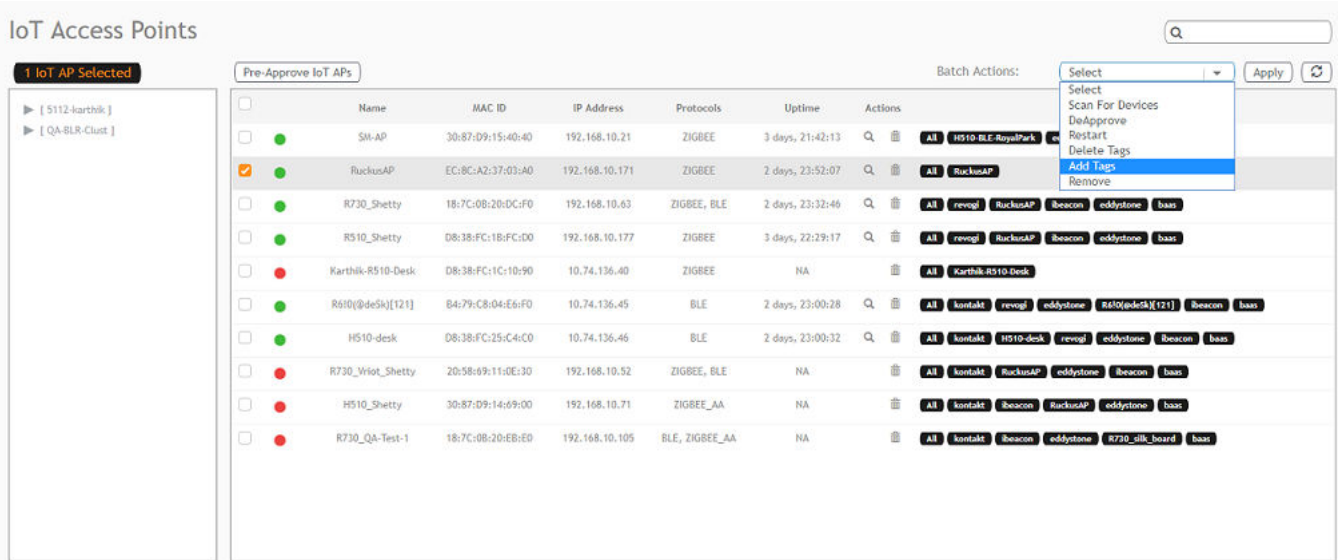
A list of IoT APs is displayed.

2. Select an IoT AP.

NOTE

You can select one or more APs to add tags.

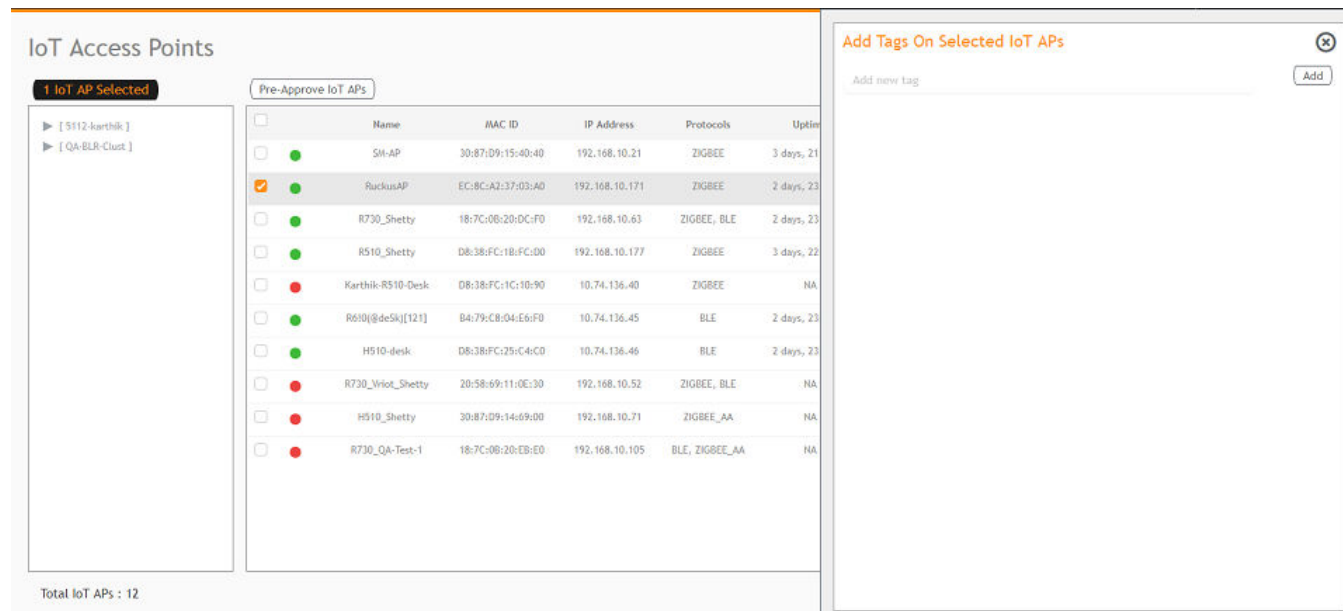
FIGURE 49 Selecting an AP to Add Tag



3. Select **Add Tags** from the drop-down list.

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

FIGURE 50 Adding Tag



To activate the following plugin you must label them using the respective tag name.

TABLE 5 Activating the Plugin by Adding Tag Name

Plugin	Tag Name
Kontakt	kontakt
iBeacon	ibeacon
Beacon as a Service	baas
Eddystone	eddytone
Revogi Bulb	revogi

Approval of IoT APs

The IoT APs must be approved by the administrator. The Ruckus 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).

Managing Devices

- [Devices Overview](#).....65
- [Managing OSRAM Light Bulbs](#)..... 67
- [Managing an Assa Abloy Lock](#).....68

Devices Overview

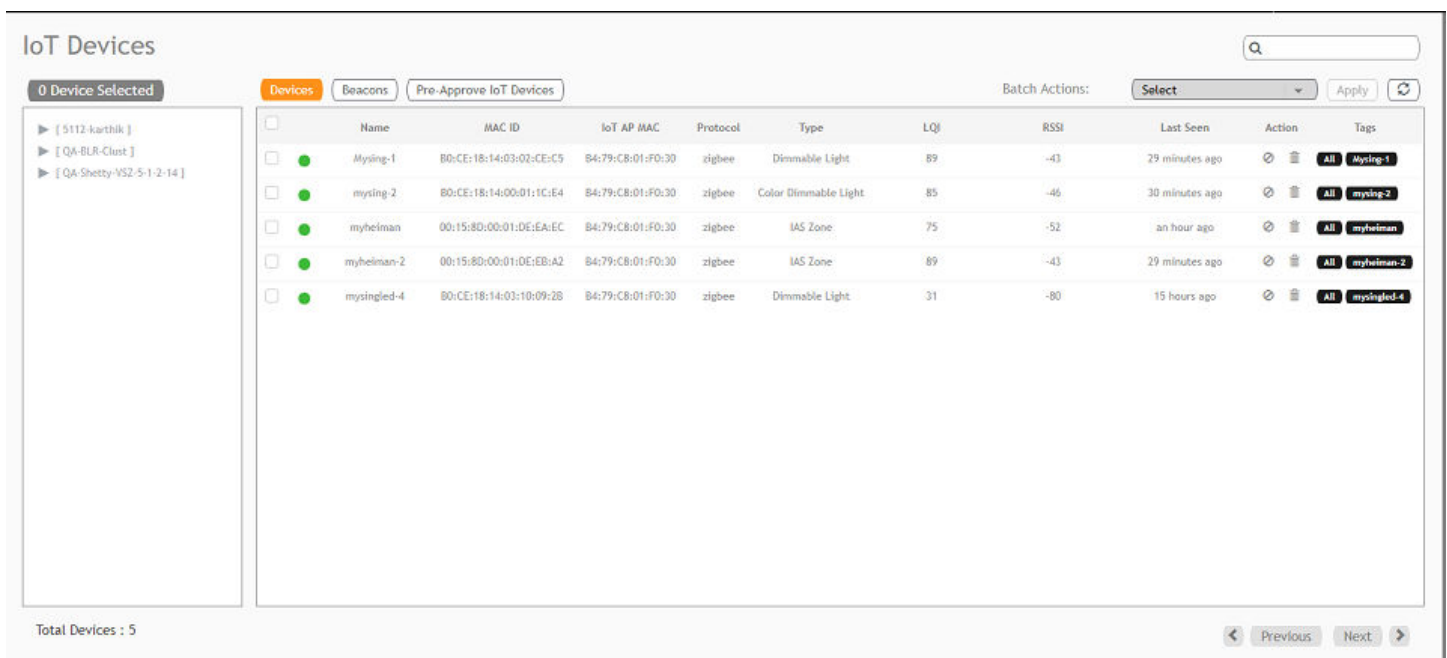
The Ruckus IoT Controller requires explicit user approval of devices. Only an approved device can be allowed into the IoT infrastructure.

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:

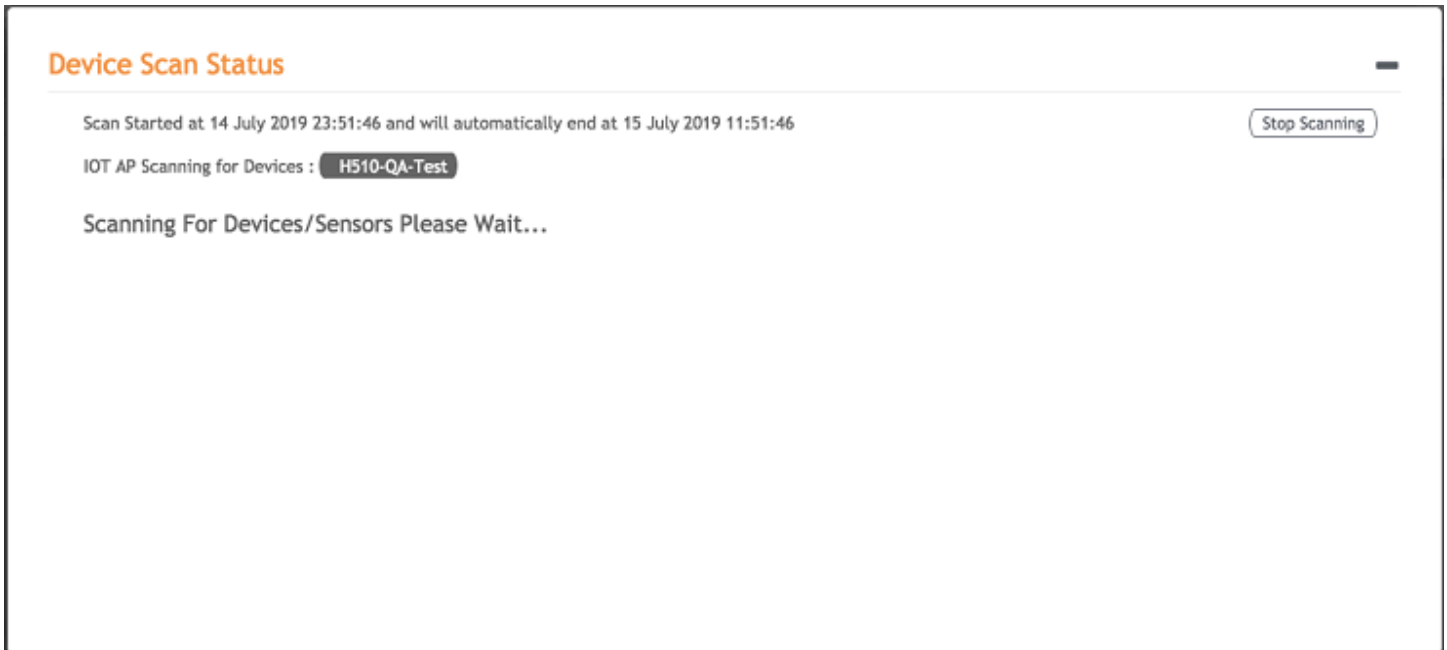
- A list of devices
- The operations on devices (such as remove, blacklist, and device-specific operations)

FIGURE 51 IoT Devices Page



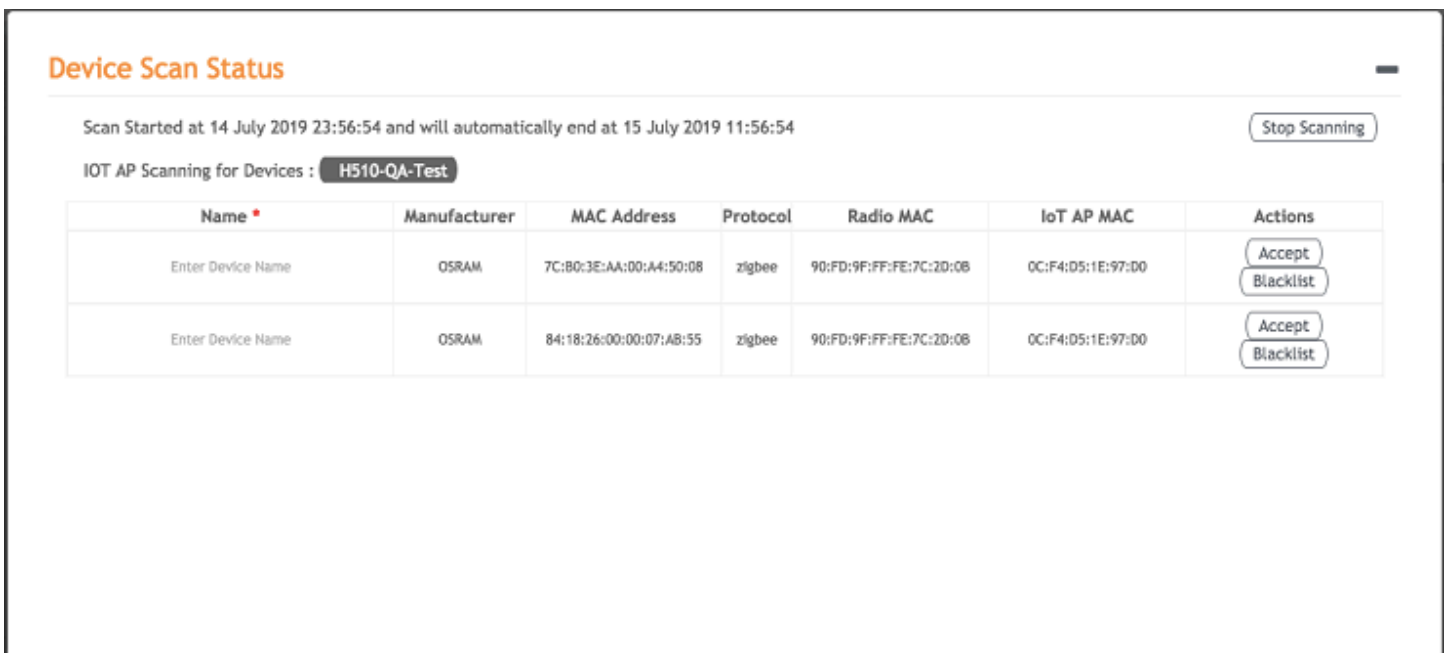
The device scan operation must be performed to start the device discovery process on the gateway. Upon starting device discovery, a dialog box is displayed, as shown in the following figure.

FIGURE 52 Device Discovery Dialog Box



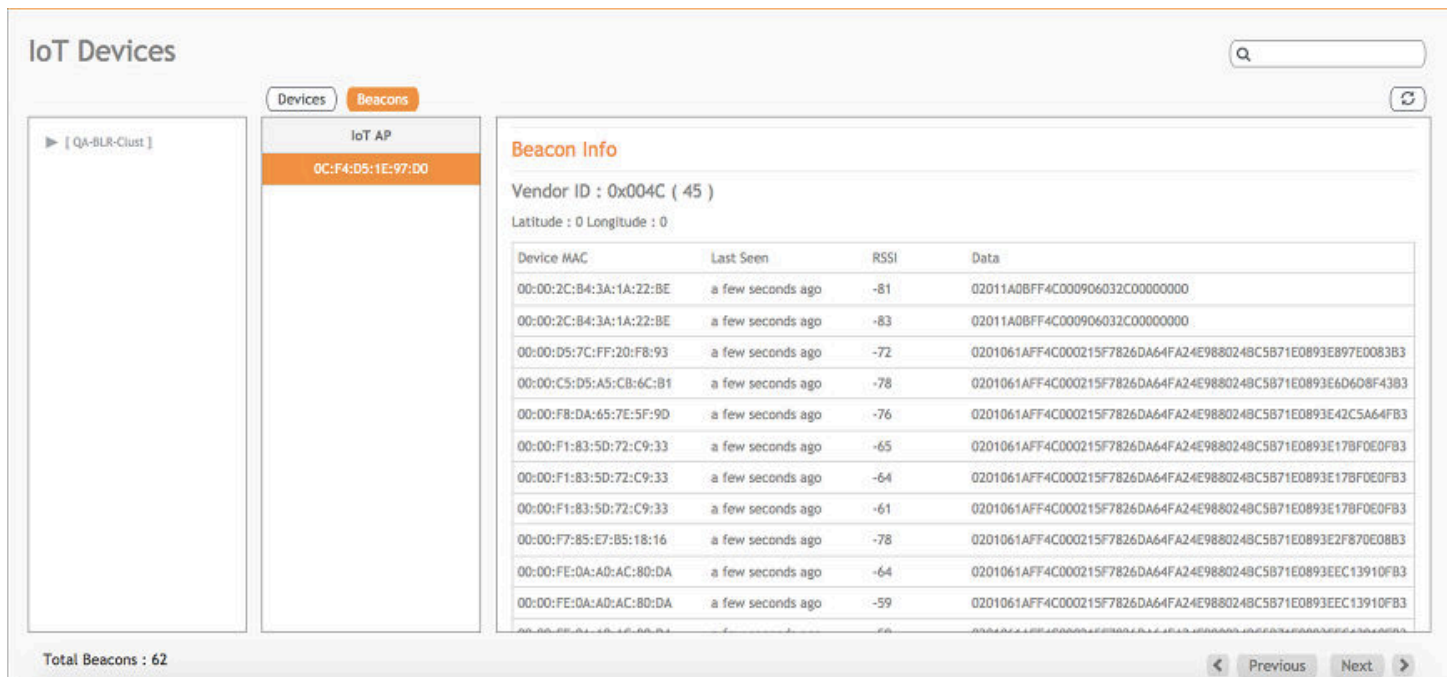
A device gets added to the Ruckus IoT Controller through Discover IoT Devices operations. If a device is pre-approved, the discovered device automatically joins the list of discovered devices. If the discovered device is not pre-approved, then you must select **Accept** or **Blacklist**. If the device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

FIGURE 53 Adding Device After Discovery



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

FIGURE 54 Beacons Page



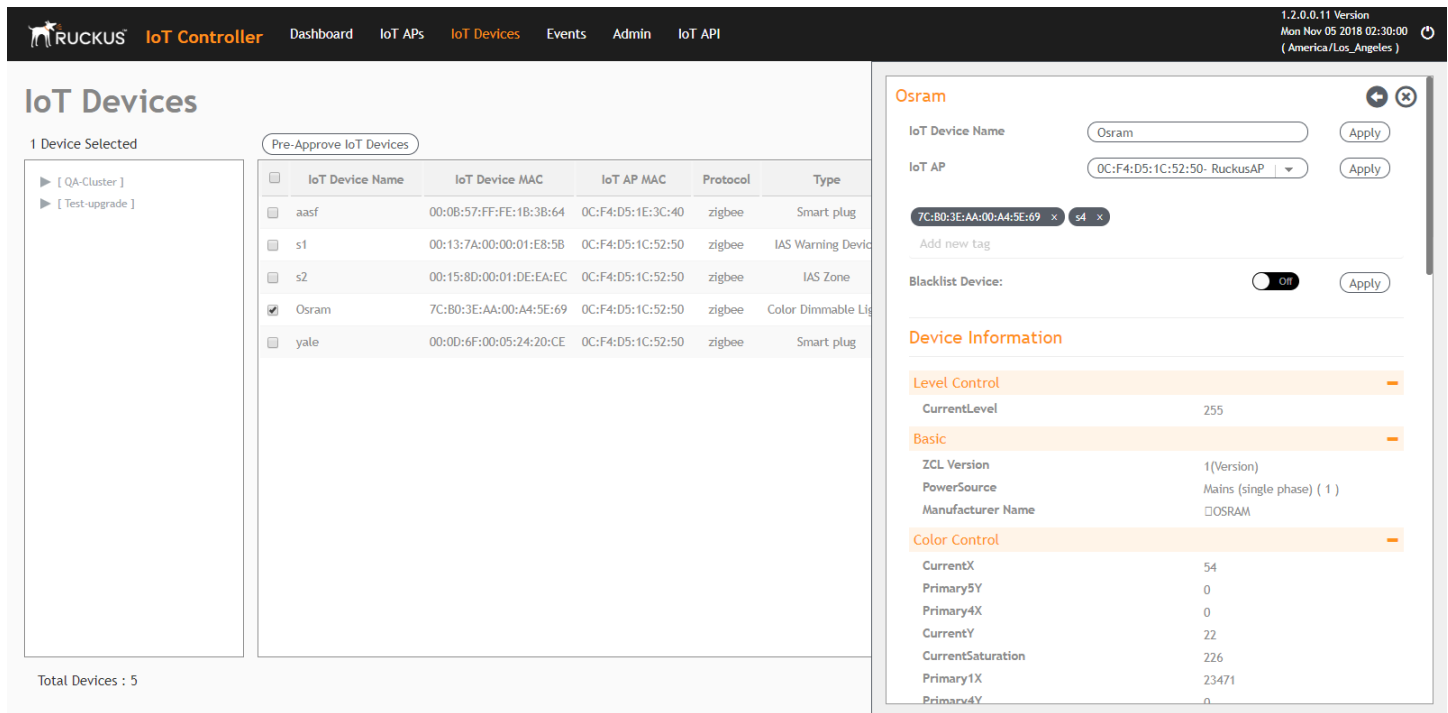
Managing OSRAM Light Bulbs

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 55 Managing OSRAM Light Bulb



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).

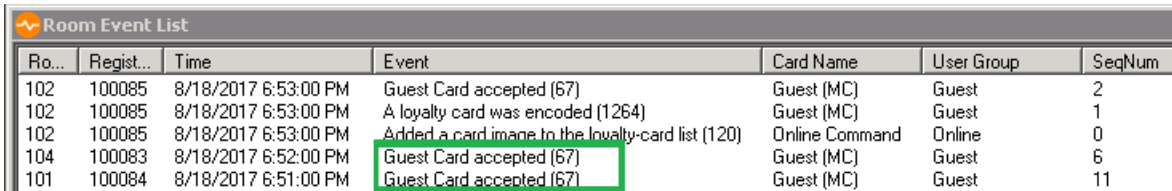
Assa Abloy locks operate using the Visionline server. To establish the initial connection (after adding the lock) between an Assa Abloy lock and the Visionline server, perform the following steps.

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 56 Visionline Server Event Log



The screenshot shows a window titled "Room Event List" with a table of event logs. The table has seven columns: "Ro...", "Regist...", "Time", "Event", "Card Name", "User Group", and "SeqNum". The data rows are as follows:

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 loyalty-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

Events

- Viewing Events..... 71

Viewing Events

An event is an occurrence or the detection of certain conditions in and around the Ruckus IoT Module. An AP rebooting, detection of a Ruckus 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 57 Events Page

Time	AP MAC	ID	Event	Message
2019-07-17 05:42:18.855107	B4:79:C8:01:F0:30	5	Radio Message Delivery Failed	B0:CE:18:14:03:02:CE:C5 is not responding for command 'On00'
2019-07-17 05:42:18.380511	B4:79:C8:01:F0:30	5	Radio Message Delivery Failed	B0:CE:18:14:03:02:CE:C5 is not responding for command 'Move to Hue(direction 2,3)'
2019-07-17 05:42:17.861363	B4:79:C8:01:F0:30	5	Radio Message Delivery Failed	B0:CE:18:14:03:02:CE:C5 is not responding for command 'Add Scene'
2019-07-17 05:41:59.066870	B4:79:C8:01:F0:30	5	Radio Message Delivery Failed	B0:CE:18:14:00:01:1C:E4 is not responding for command 'Move to Hue(direction 2,3)'
2019-07-17 05:41:58.560641	B4:79:C8:01:F0:30	5	Radio Message Delivery Failed	B0:CE:18:14:00:01:1C:E4 is not responding for command 'Move to Hue(direction 2,3)'
2019-07-17 05:41:58.073009	B4:79:C8:01:F0:30	5	Radio Message Delivery Failed	B0:CE:18:14:00:01:1C:E4 is not responding for command 'Move to Hue(direction 2,3)'
2019-07-17 05:41:57.554897	B4:79:C8:01:F0:30	5	Radio Message Delivery Failed	B0:CE:18:14:00:01:1C:E4 is not responding for command 'Move to level'
2019-07-17 05:41:57.048804	B4:79:C8:01:F0:30	5	Radio Message Delivery Failed	B0:CE:18:14:00:01:1C:E4 is not responding for command 'On'
2019-07-17 05:41:56.541556	B4:79:C8:01:F0:30	5	Radio Message Delivery Failed	B0:CE:18:14:00:01:1C:E4 is not responding for command 'Add Scene'
2019-07-17 05:41:56.050397	B4:79:C8:01:F0:30	5	Radio Message Delivery Failed	B0:CE:18:14:00:01:1C:E4 is not responding for command 'Identify'
2019-07-17 05:36:18.844241	B4:79:C8:01:F0:30	5	Radio Message Delivery Failed	B0:CE:18:14:03:02:CE:C5 is not responding for command 'On00'
2019-07-17 05:36:18.365948	B4:79:C8:01:F0:30	5	Radio Message Delivery Failed	B0:CE:18:14:03:02:CE:C5 is not responding for command 'Move to Hue(direction 2,3)'
2019-07-17 05:36:17.850956	B4:79:C8:01:F0:30	5	Radio Message Delivery Failed	B0:CE:18:14:03:02:CE:C5 is not responding for command 'Add Scene'
2019-07-17 05:36:07.691108	B4:79:C8:01:F0:30	5	Radio Message Delivery Failed	B0:CE:18:14:00:01:1C:E4 is not responding for command 'Move to Hue(direction 2,3)'
2019-07-17 05:36:07.653421	B4:79:C8:01:F0:30	5	Radio Message Delivery Failed	B0:CE:18:14:00:01:1C:E4 is not responding for command 'Move to Hue(direction 2,3)'
2019-07-17 05:35:58.082789	B4:79:C8:01:F0:30	5	Radio Message Delivery Failed	B0:CE:18:14:00:01:1C:E4 is not responding for command 'Move to Hue(direction 2,3)'
2019-07-17 05:35:57.568188	B4:79:C8:01:F0:30	5	Radio Message Delivery Failed	B0:CE:18:14:00:01:1C:E4 is not responding for command 'Move to level'

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.



© 2019 CommScope, Inc. All rights reserved.
Ruckus Wireless, Inc., a wholly owned subsidiary of CommScope, Inc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com