CONFIGURATION GUIDE

Ruckus IoT Controller Configuration Guide, 1.3

Supporting IoT Controller Release 1.3

Part Number: 800-72286-001 Rev A
Publication Date: 15 April 2019

Copyright, Trademark and Proprietary Rights Information

© 2019 ARRIS Enterprises LLC. All rights reserved.

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

Export Restrictions

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

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

Disclaimer

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

Limitation of Liability

IN NO EVENT SHALL ARRIS, ARRIS AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, 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 ARRIS HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

ARRIS, the ARRIS logo, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, EdgeIron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, ZoneFlex are trademarks of ARRIS International plc and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access (WPA), the Wi-Fi Protected Setup logo, and WMM are registered trademarks of Wi-Fi Alliance. Wi-Fi Protected Setup™, Wi-Fi Multimedia™, and WPA2™ are trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

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

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 **27**
- Managing Services 27
- Activating and Editing the Plugins 28
  - Activating and Editing the Kontakt.io Beacons Plugin 28
  - Activating and Editing the Eddystone Plugin 30
  - Activating and Editing the iBeacon Plugin 33
- Changing the Password 35
- Configuring Virtual Machines 36
- Uploading Versions and Patches 37
  - Uploading an Image 37
  - Uploading a Patch 38
- Backing Up Files 39
- Rebooting Ruckus IoT Controller 40
- Resetting Ruckus IoT Controller 41

Managing IoT Access Points **43**
- IoT AP Overview 43
  - DHCP Option 43 43
  - Ruckus Command Line Interface 43
- Adding an IoT AP 44
- Editing an IoT AP 47
  - Single IoT Access Point Mode 47
- Approval of IoT APs 48

Managing Devices **49**
Devices Overview 49
Managing OSRAM Light Bulbs 50
Managing an Assa Abloy Lock 51

Events **53**
Viewing Events 53

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	`device(config)# interface ethernet 1/1/6`
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**.
italics	Publication titles	Refer to the *Ruckus Small Cell Release Notes* 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.
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*...].
\	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@arris.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

- 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.

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 2 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

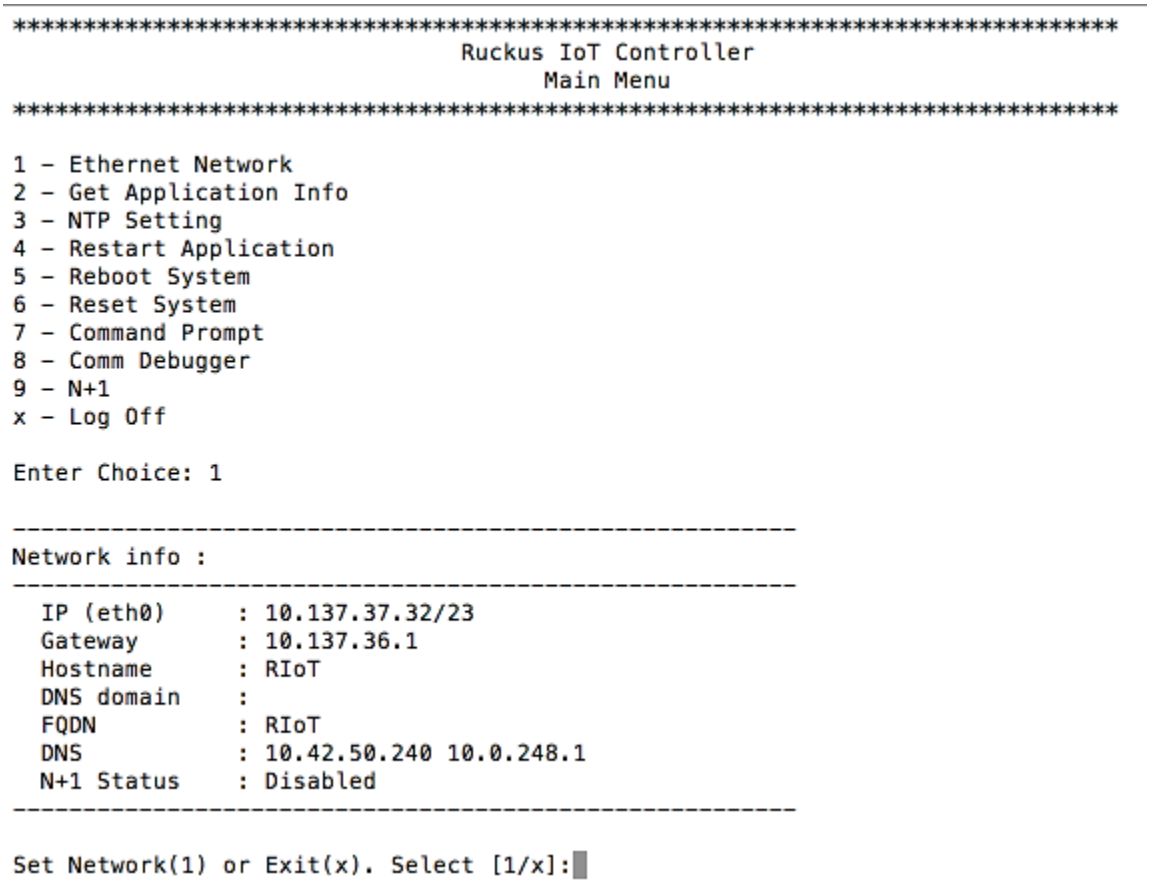
Logging In to Ruckus IoT Controller

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.

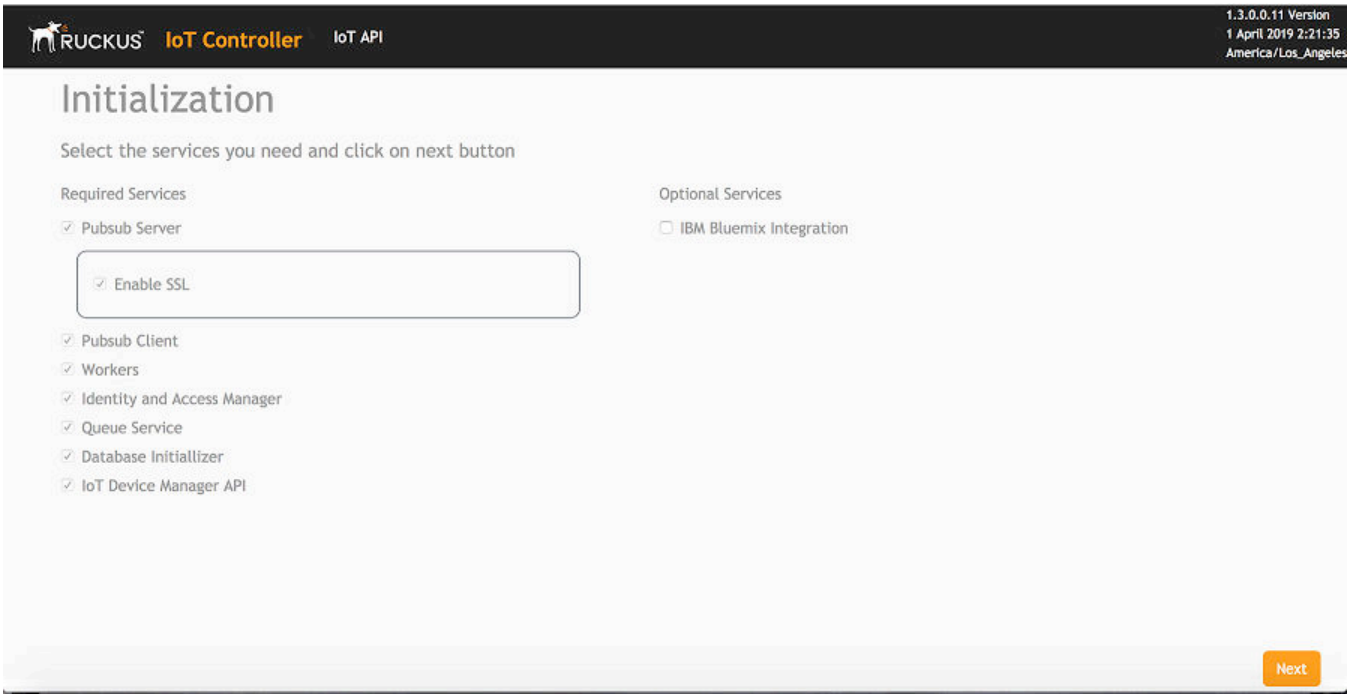
FIGURE 1 Ruckus IoT Controller Main Menu



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

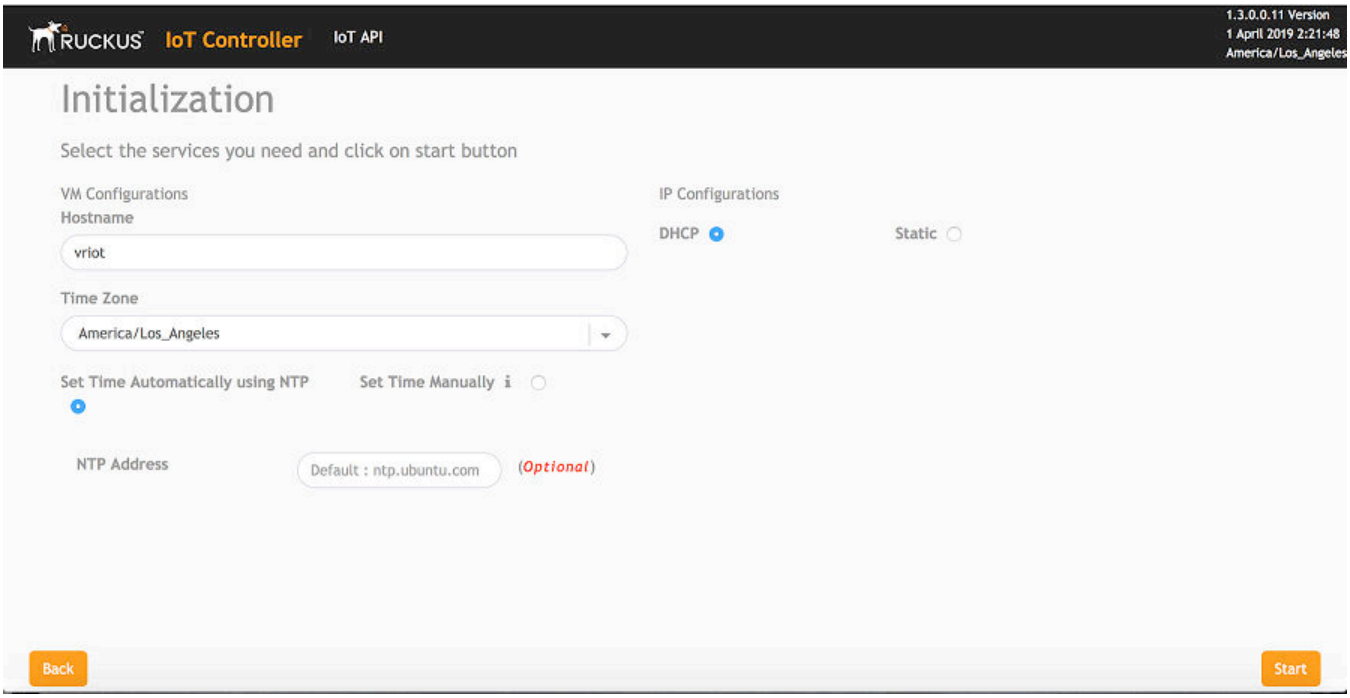
Pubsub Server works in SSL mode.

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.

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.

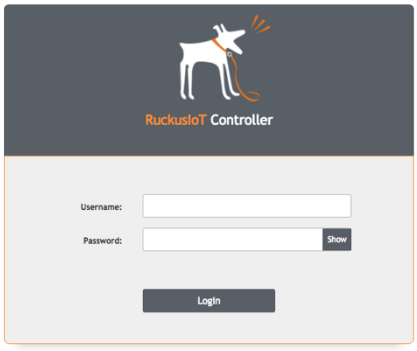
FIGURE 3 Intialization Page After Accepting Services



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



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

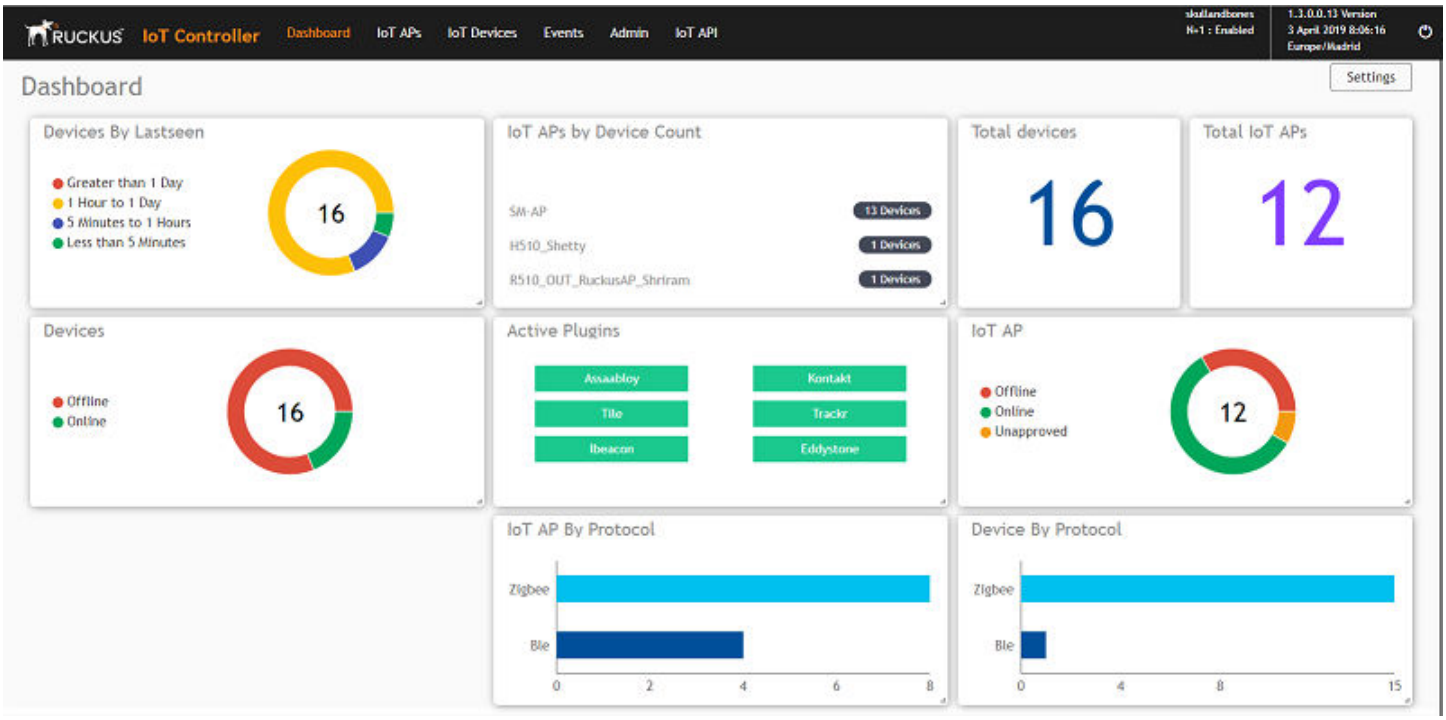


TABLE 3 Dashboard Elements

Box Name	Description
Devices By Lastseen	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 count of total number of devices.
Total IoT APs	Shows the count of total number of Access Points.
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, Zigbee.
Device By Protocol	Shows the total number of devices connected by the protocol being used. Ruckus supports two protocols: BLE, Zigbee.

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 hostnames.
- 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** . Click **Static** to set the master and slave configuration.
- In the Logging In to Ruckus IoT Controller on page 11 section, go to the step 4 Figure 3 on page 14 to set the static address of the master and slave.

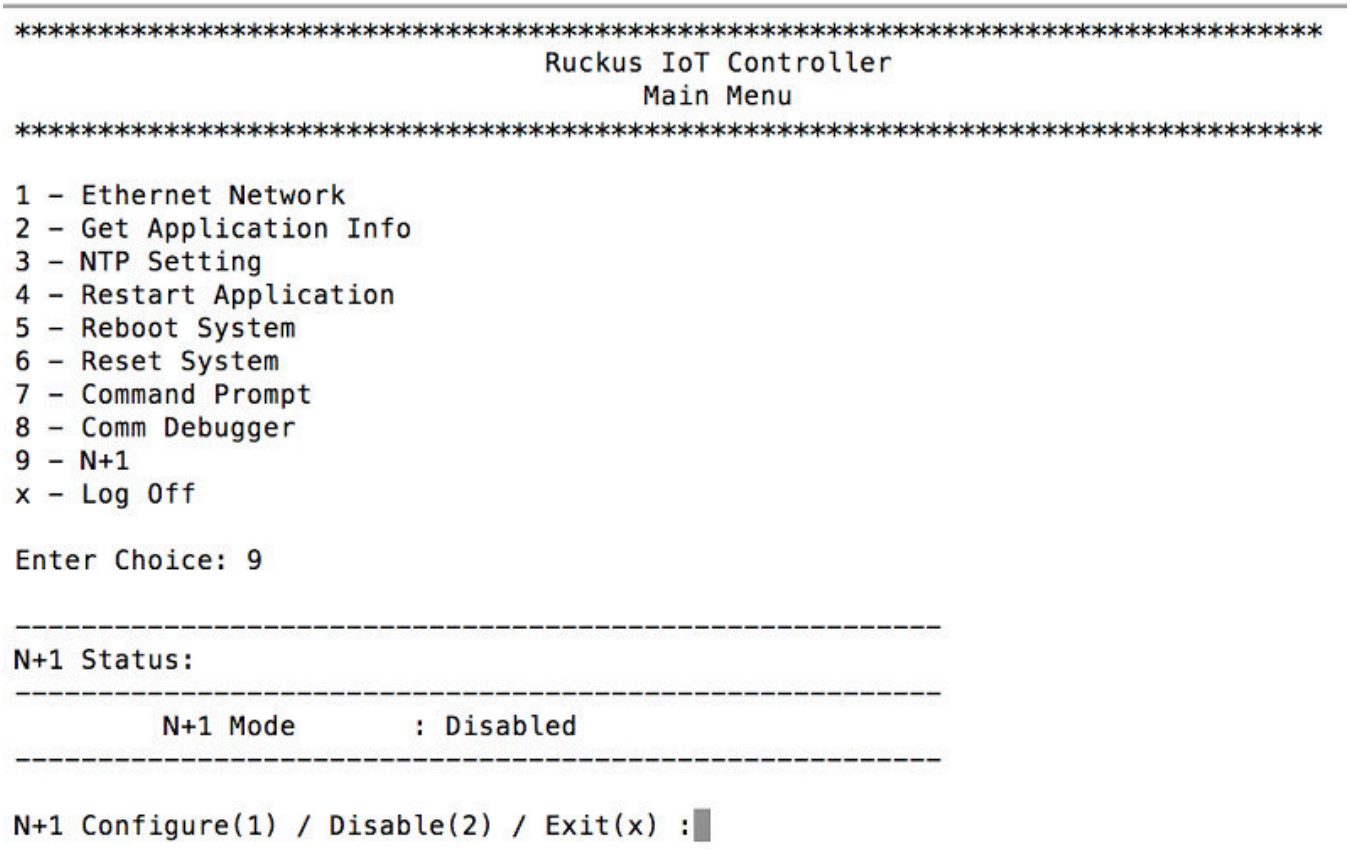
Configuring the N+1 feature

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 **9** in the **Enter Choice** field .

FIGURE 6 Ruckus IoT Controller Main Menu



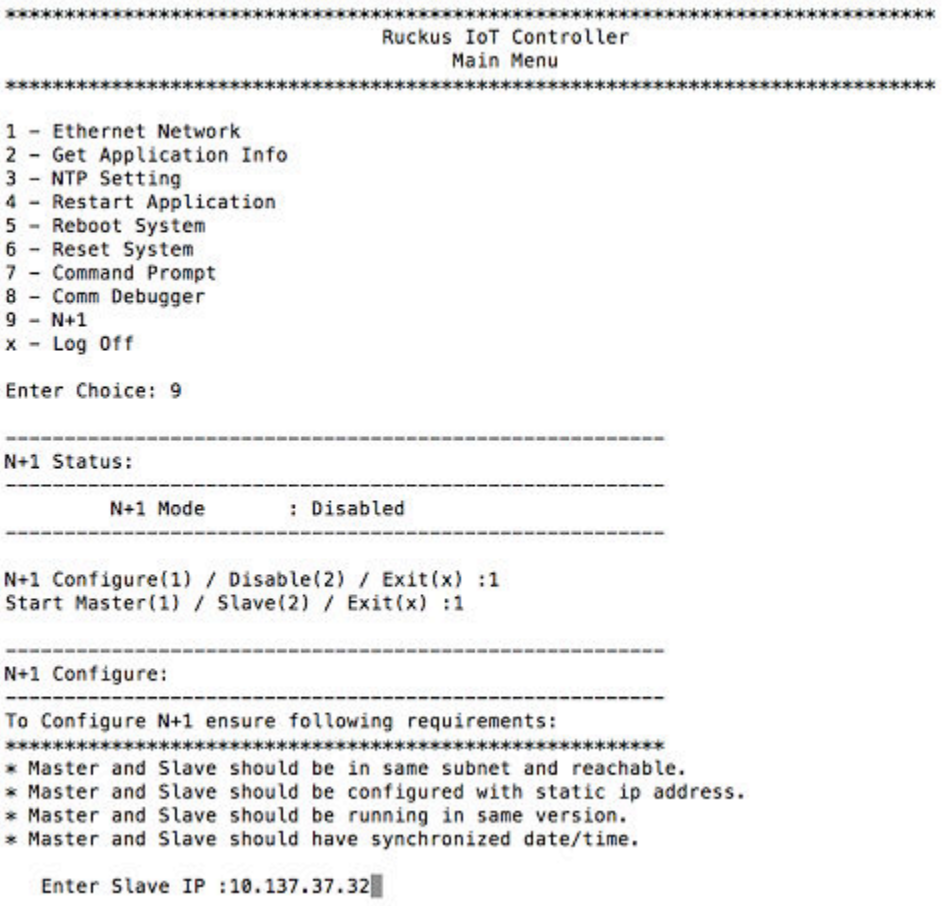
3. Enter **1** to continue the configuration.

FIGURE 7 Continuing the Configuration

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

1 - Ethernet Network
2 - Get Application Info
3 - NTP Setting
4 - Restart Application
5 - Reboot System
6 - Reset System
7 - Command Prompt
8 - Comm Debugger
9 - N+1
x - Log Off

Enter Choice: 9

-------------------------------------------------------
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 the Slave** IP field.

FIGURE 8 Configuring the Master



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

FIGURE 9 Entering the Preferred Virtual IP Address

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

1 - Ethernet Network
2 - Get Application Info
3 - NTP Setting
4 - Restart Application
5 - Reboot System
6 - Reset System
7 - Command Prompt
8 - Comm Debugger
9 - N+1
x - Log Off

Enter Choice: 9

------------------------------------------------------
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 :10.137.37.32
   Enter preferred Virtual IP :10.137.37.33
```

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

FIGURE 10 Completing the Master Configuration

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

1 - Ethernet Network
2 - Get Application Info
3 - NTP Setting
4 - Restart Application
5 - Reboot System
6 - Reset System
7 - Command Prompt
8 - Comm Debugger
9 - N+1
x - Log Off

Enter Choice: 9

-------------------------------------------------------
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 :10.137.37.32
   Enter preferred Virtual IP :10.137.37.33
   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 11 Continuing with the Slave Configuration

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

1 - Ethernet Network
2 - Get Application Info
3 - NTP Setting
4 - Restart Application
5 - Reboot System
6 - Reset System
7 - Command Prompt
8 - Comm Debugger
9 - N+1
x - Log Off

Enter Choice: 9

-------------------------------------------------------
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 :10.137.37.32
   Enter preferred Virtual IP :10.137.37.33
   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 12 N+1 Configuration Completed

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

1 - Ethernet Network
2 - Get Application Info
3 - NTP Setting
4 - Restart Application
5 - Reboot System
6 - Reset System
7 - Command Prompt
8 - Comm Debugger
9 - N+1
x - Log Off

Enter Choice: 9

-------------------------------------------------------
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 :10.137.37.32
   Enter preferred Virtual IP :10.137.37.33
   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 address of **Master**or **Active Master** and **Slave** or **Active Slave**, Enter **9** in the **Enter choice** field.

FIGURE 13 Verifying the IP Address of the Active Master

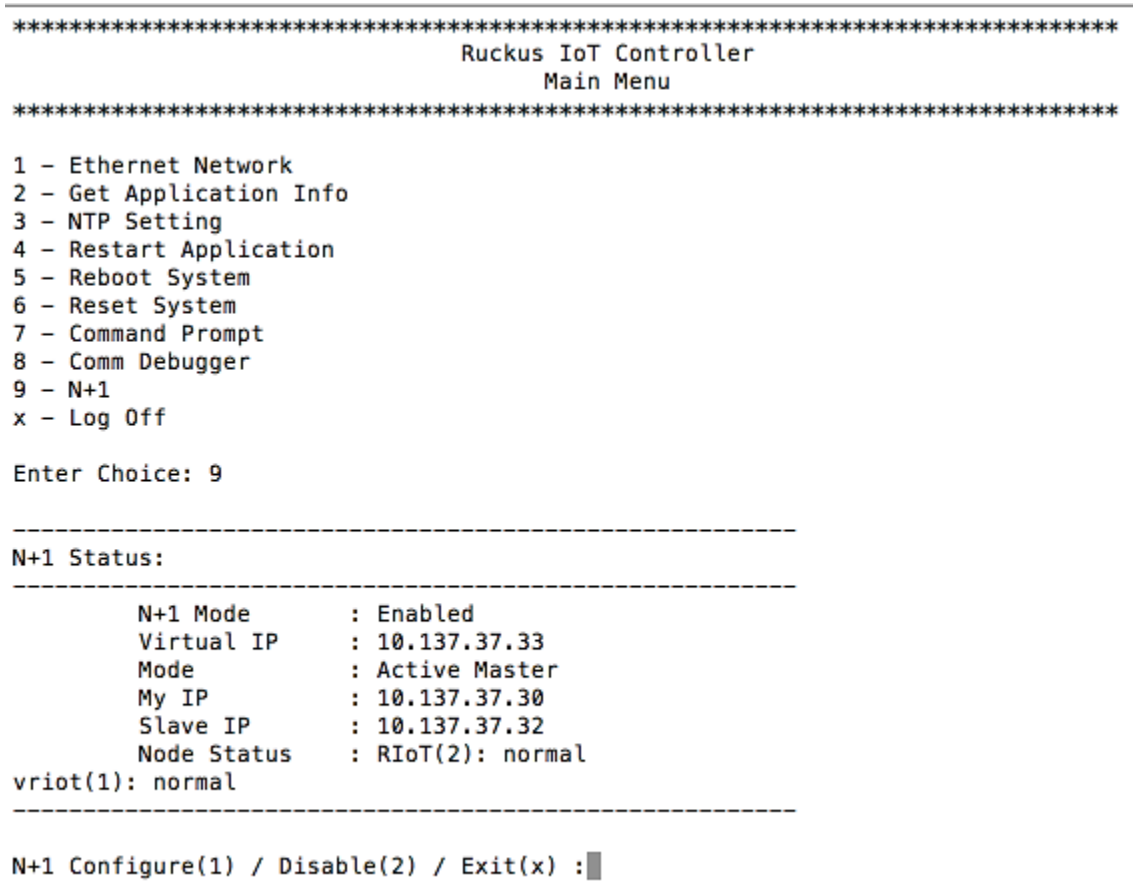


FIGURE 14 Verifying the IP Address of the Slave

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

1 - Ethernet Network
2 - Get Application Info
3 - NTP Setting
4 - Restart Application
5 - Reboot System
6 - Reset System
7 - Command Prompt
8 - Comm Debugger
9 - N+1
x - Log Off

Enter Choice: 9

-------------------------------------------------------
N+1 Status:
-------------------------------------------------------
         N+1 Mode       : Enabled
         Virtual IP     : 10.137.37.33
         Mode           : Slave
         My IP          : 10.137.37.32
         Master IP      : ["10.137.37.30"]
         ConfigSync     : 04/08/2019 12:20:40
         Node Status    : RIoT(2): normal
vriot(1): normal
-------------------------------------------------------

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

Managing IoT Controller System Configuration

- Managing Services....27
- Activating and Editing the Plugins....28
- Changing the Password....35
- Configuring Virtual Machines....36
- Uploading Versions and Patches....37
- Backing Up Files....39
- Rebooting Ruckus IoT Controller....40
- Resetting Ruckus IoT Controller....41

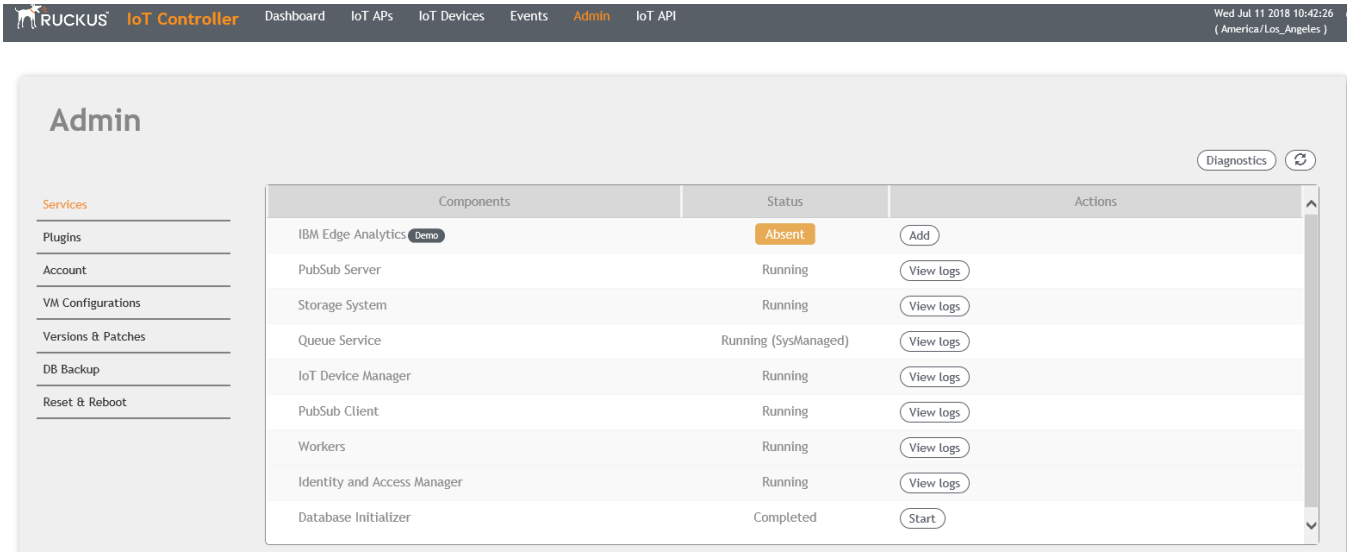
Managing Services

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 15 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

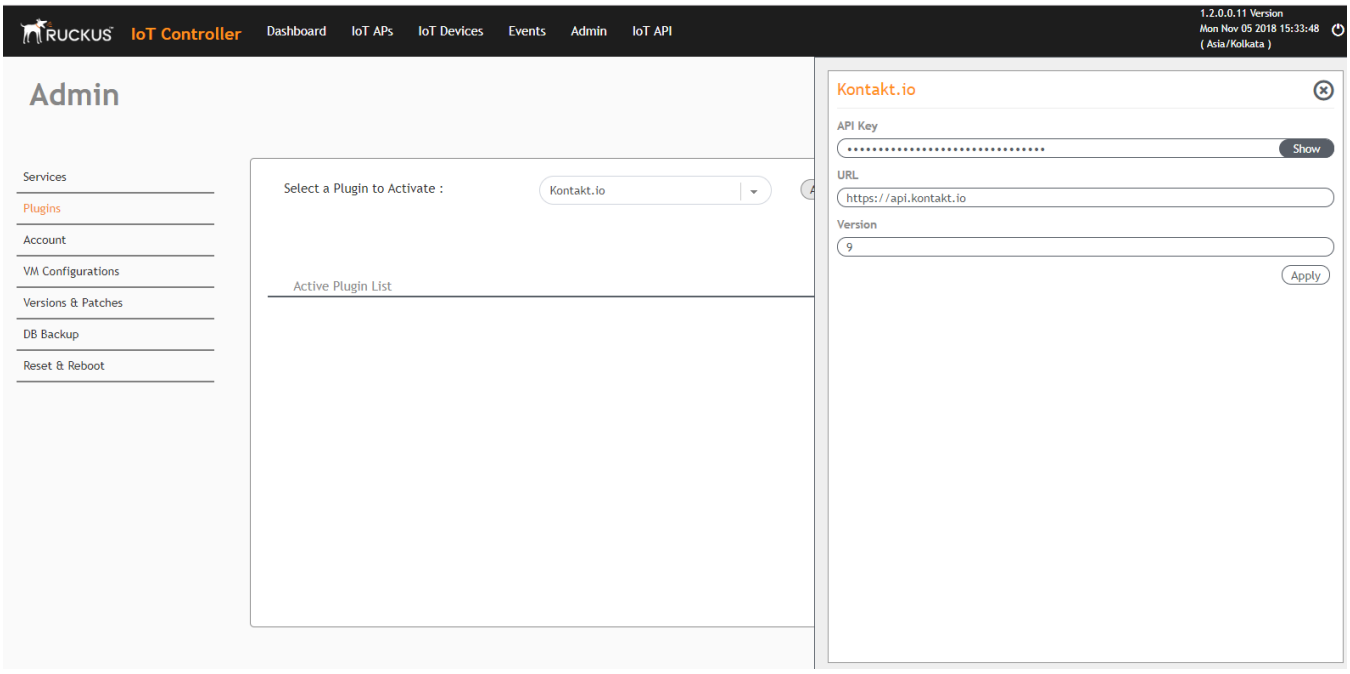
The Ruckus IoT Controller provides support for the Kontakt.io Beacons plugin.

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 16 Activating the Kontakt.io Plugin



4. After the Kontakt.io plugin is activated, enter the following configuration parameters.
   a) 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.

   b) 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.

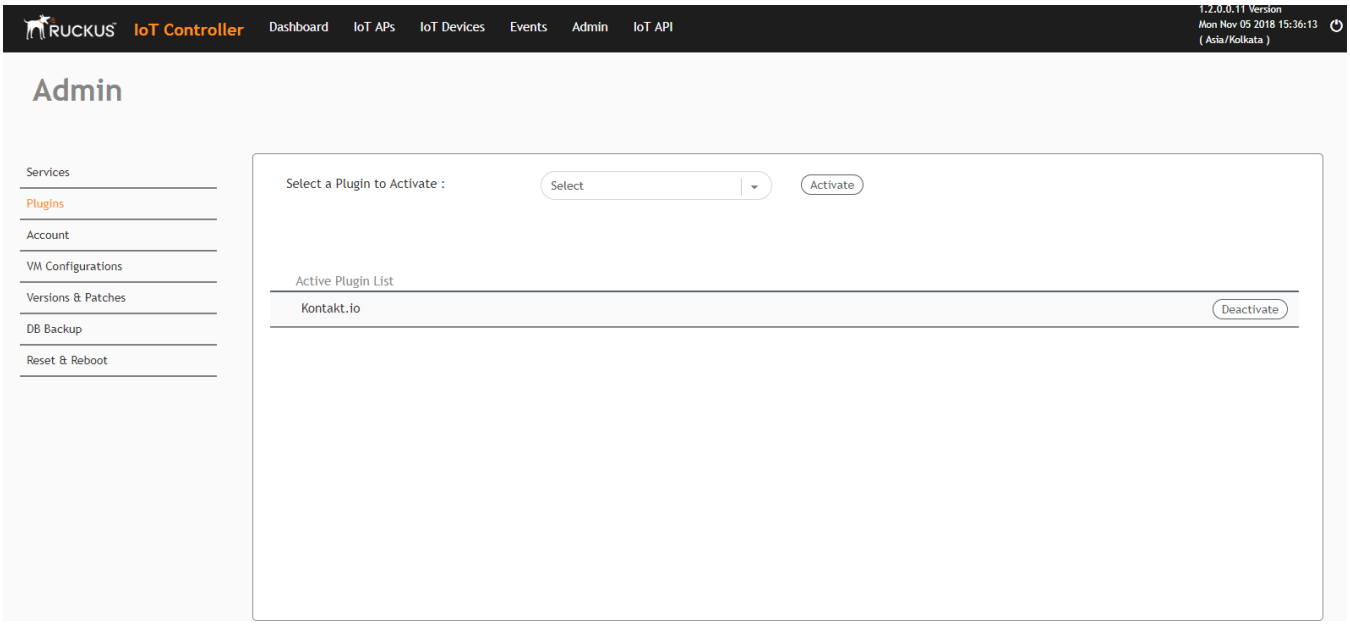
      NOTE
      The plugin supports HTTP and HTTPS modes.

   c) Enter the Version number.

      The default version number is 9.
5. Click **Apply**.

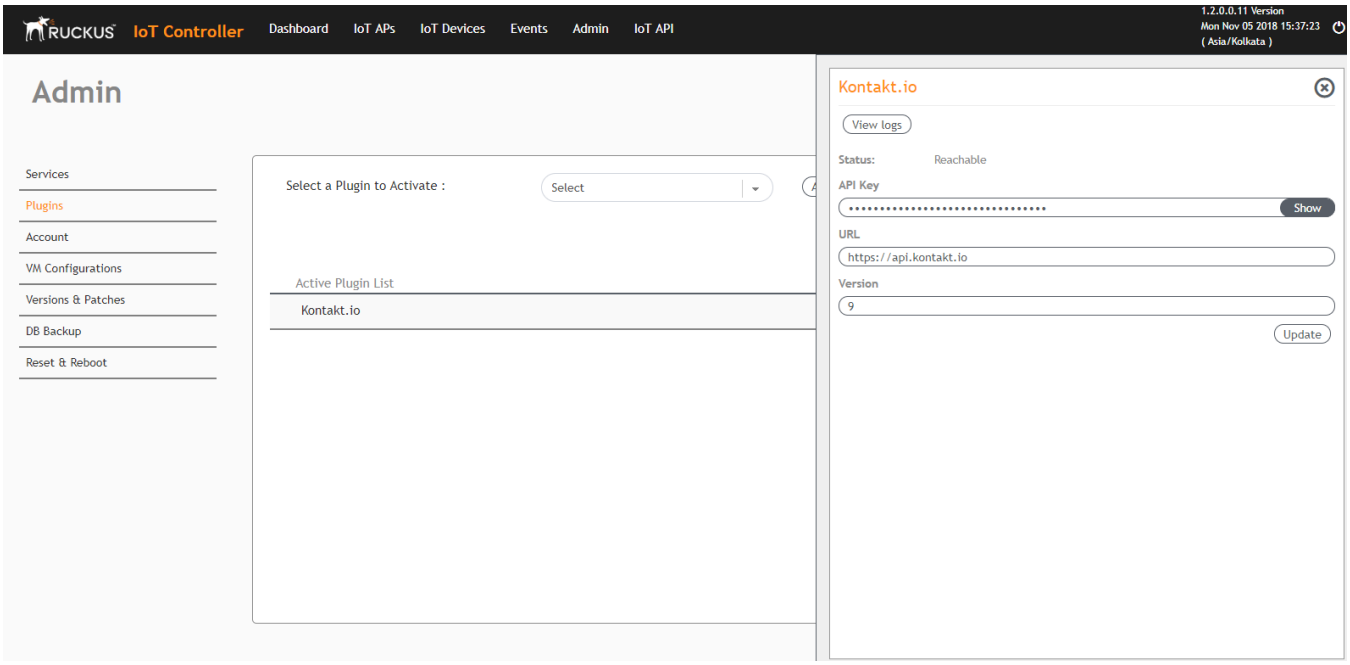
   The Kontakt.io plugin is added in the **Active Plugin List**.
6. To deactivate the Kontakt.io plugin, select it and click **Deactivate**.

FIGURE 17 Deactivating the Kontakt.io Plugin



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

FIGURE 18 Updating the Configuration Parameters



Activating and Editing the Eddystone Plugin

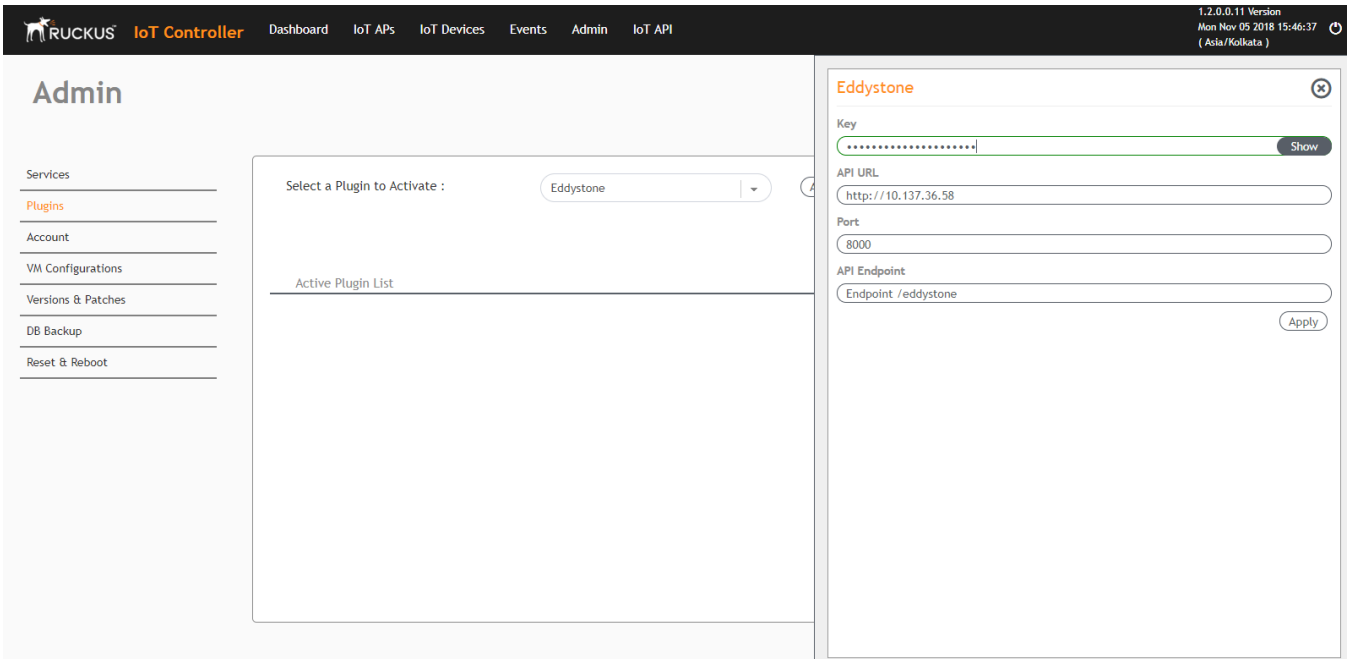
The Ruckus IoT Controller provides support for the Bluetooth Low Energy (BLE) Eddystone plugin. The Ruckus IoT Controller reads the packet from IoT AP, and routes the packets to the BLE beacon vendor cloud services.

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 19 Activating the Eddystone Plugin



4. After the Eddystone plugin is activated, enter the following configuration parameters.
   a) Enter the Key.

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

   b) 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.

   c) Enter the Port number.

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

   d) Enter the API Endpoint.

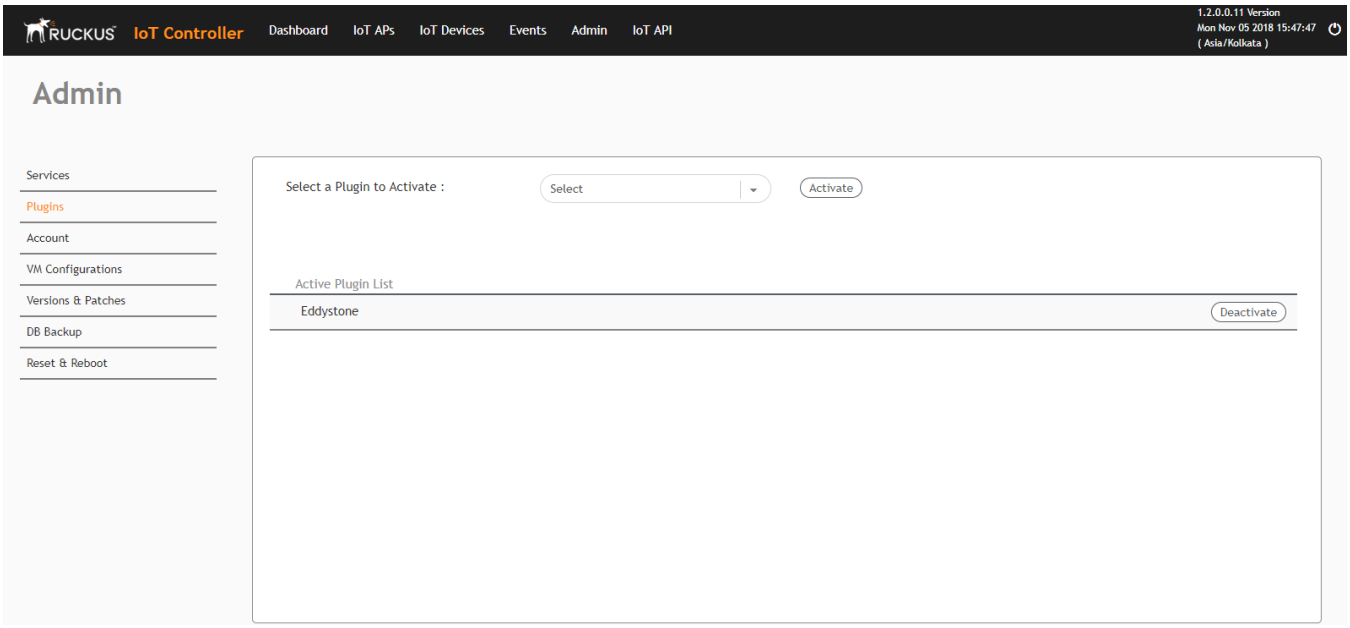
      This is the API route where the BLE beacon vendor cloud services receive the beacon payload.

5. Click **Apply**.

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

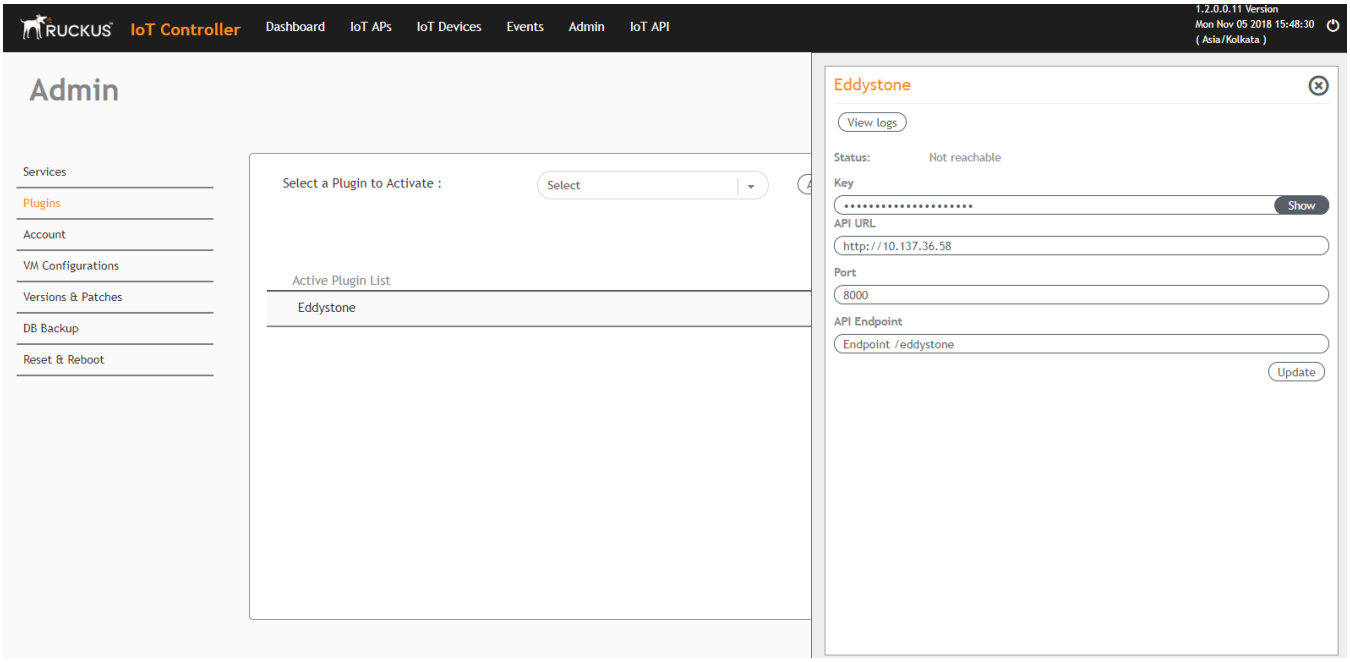
6. To deactivate the Eddystone plugin, select it and click **Deactivate**.

FIGURE 20 Deactivating Eddystone Plugin



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

FIGURE 21 Updating the Configuration Parameters



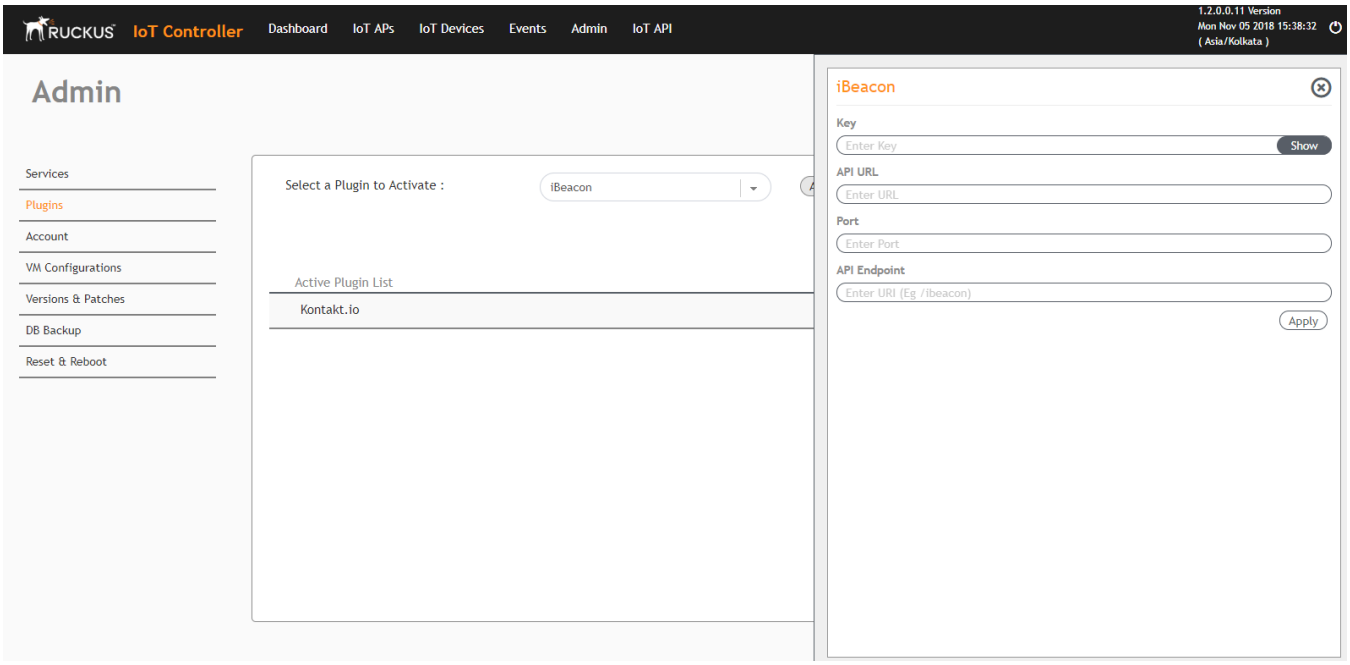
Activating and Editing the iBeacon Plugin

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 and click **Activate**.

FIGURE 22 Activating iBeacon Plugin



4. After the iBeacon plugin is activated, enter the following configuration parameters.
   a) Enter the Key.

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

   b) 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.

   c) Enter the Port number.

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

   d) Enter the API Endpoint.

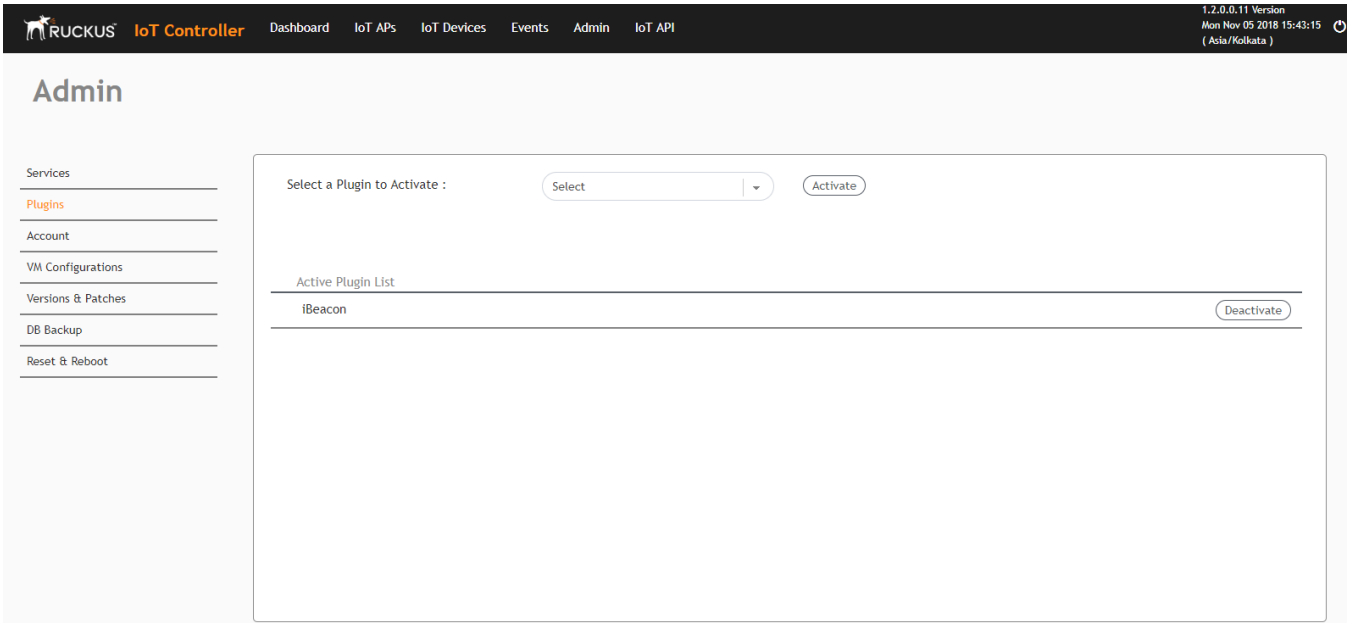
      This is the API route where the BLE beacon vendor cloud services receive the beacon payload.

5. Click **Apply**.

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

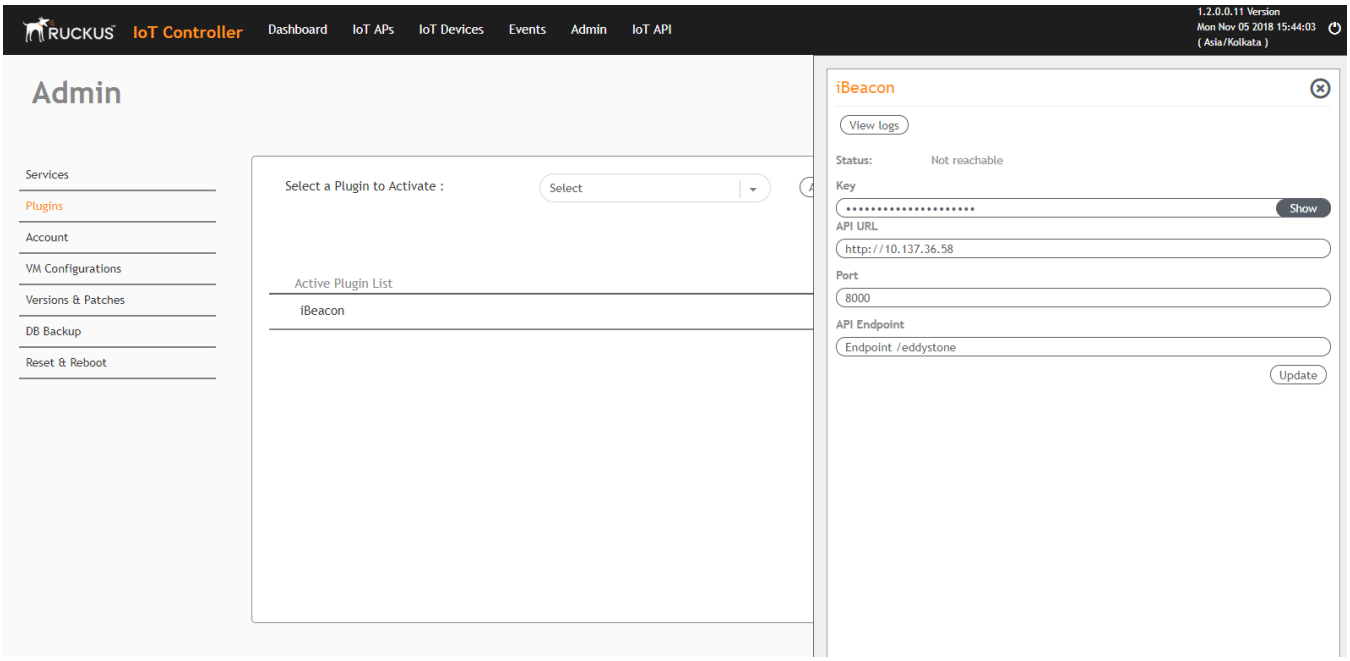
6. To deactivate the iBeacon plugin, select it and click **Deactivate**.

FIGURE 23 Deactivating the iBeacon Plugin



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

FIGURE 24 Updating the Configuration Parameters



Changing the Password

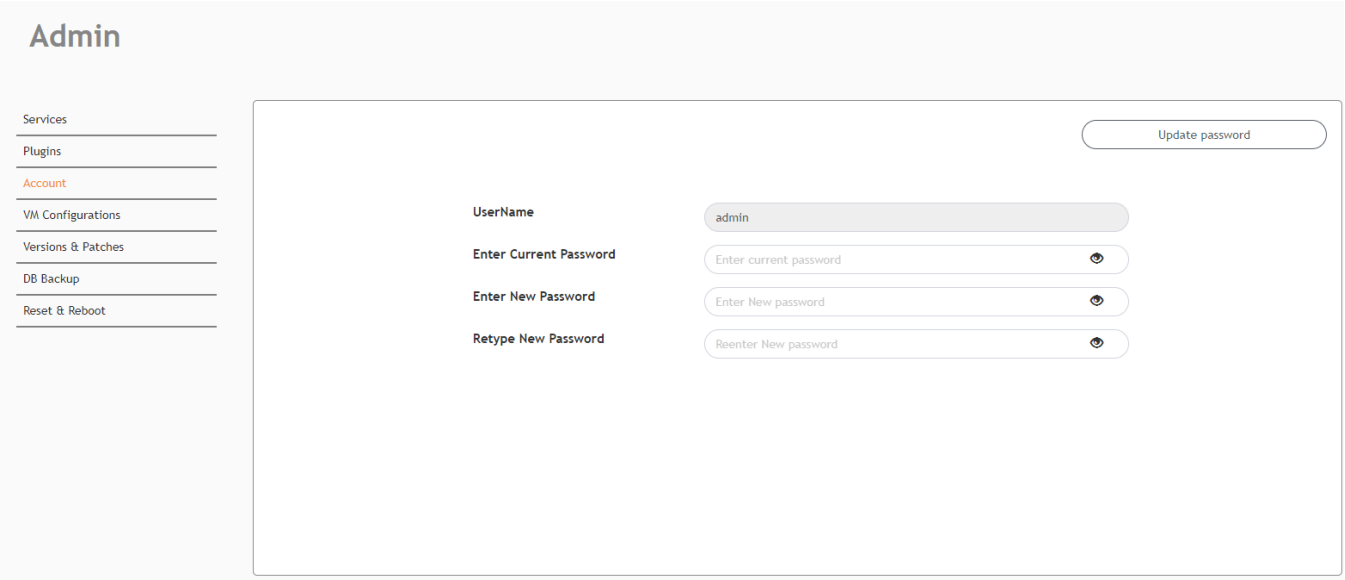
A single administrator is responsible for creating a Ruckus IoT Controller account. This administrator manages system operations.

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 25 Changing the Password



3. Change the password and click **Update password**.

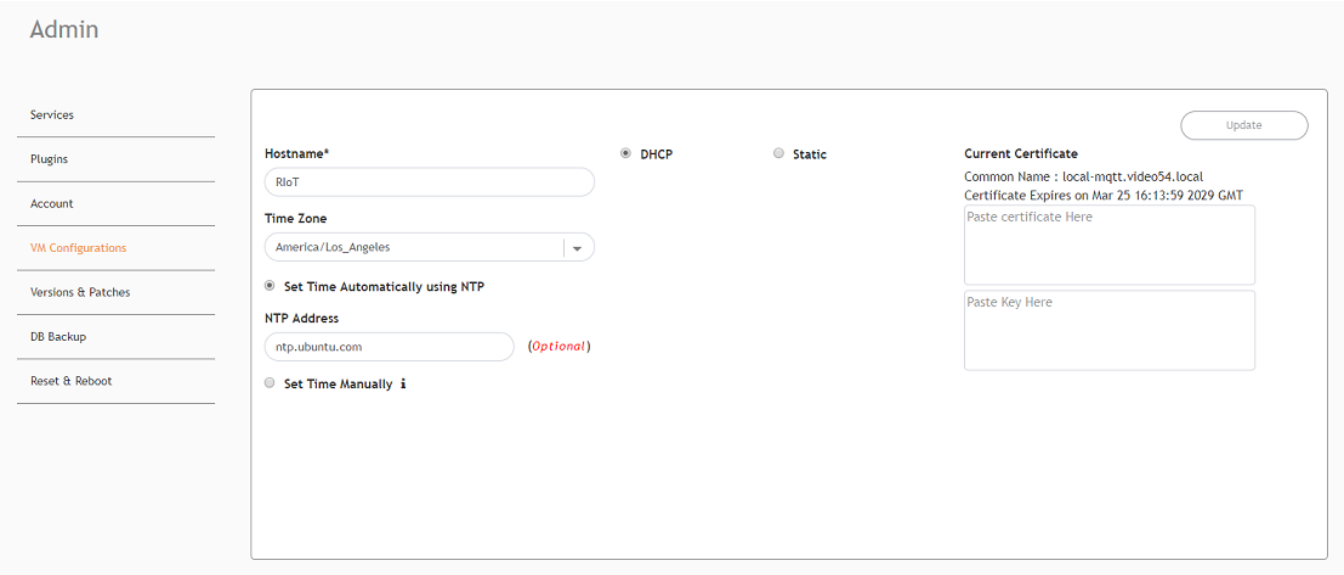
Configuring Virtual Machines

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 26 Configuring a Virtual Machine



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.

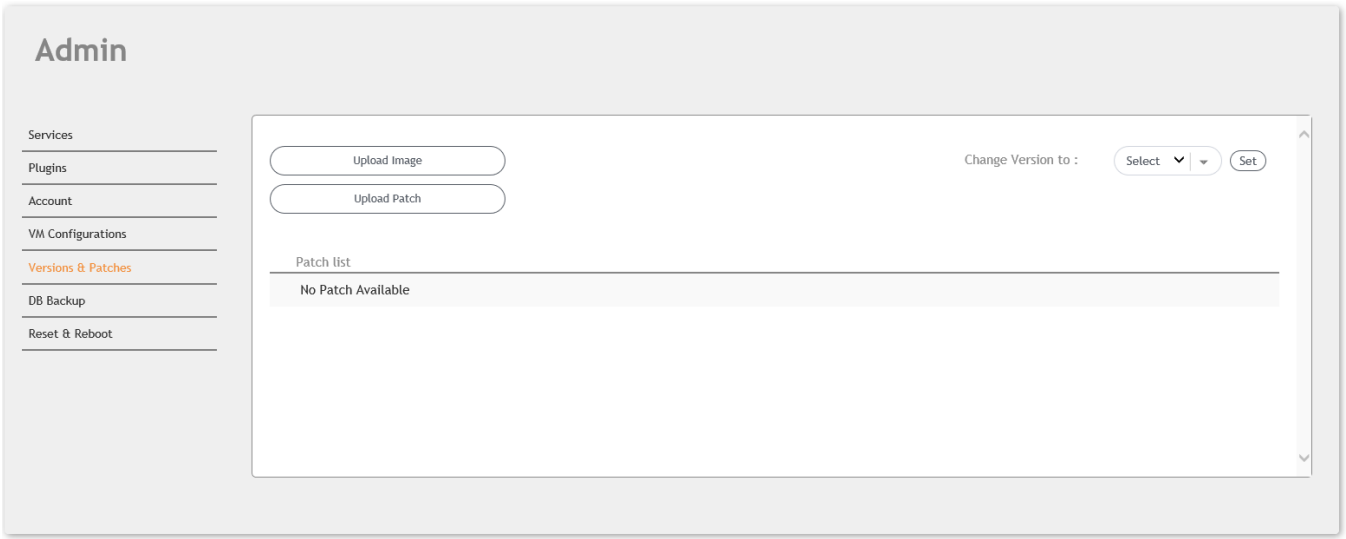
Uploading an Image

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 27 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**.

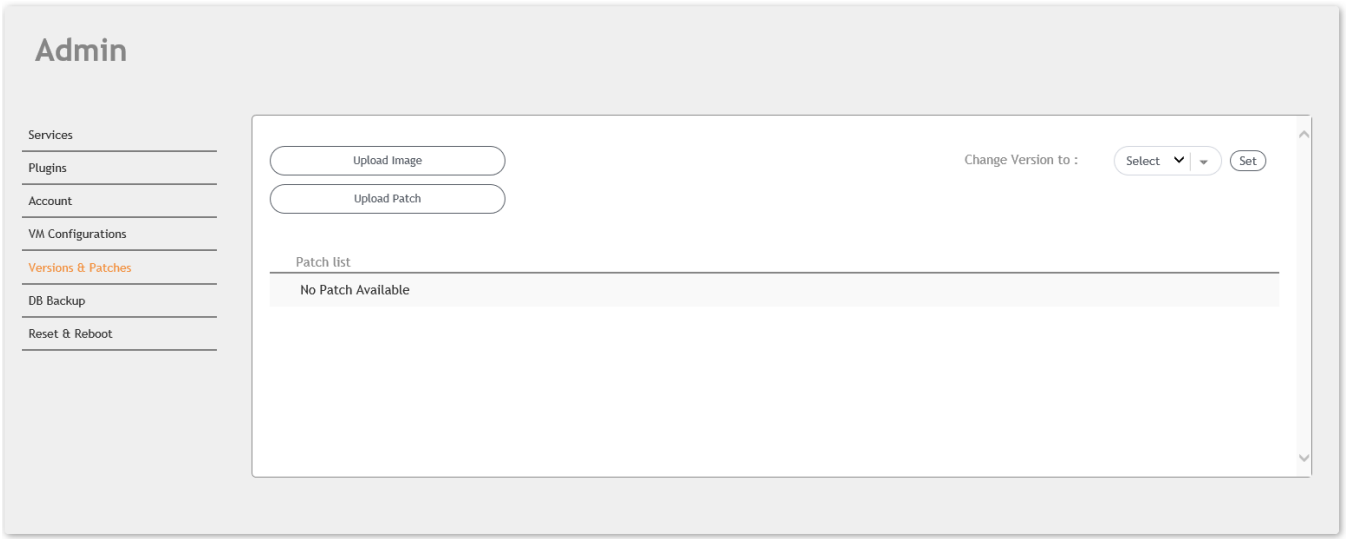
Uploading a Patch

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 28 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 29 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

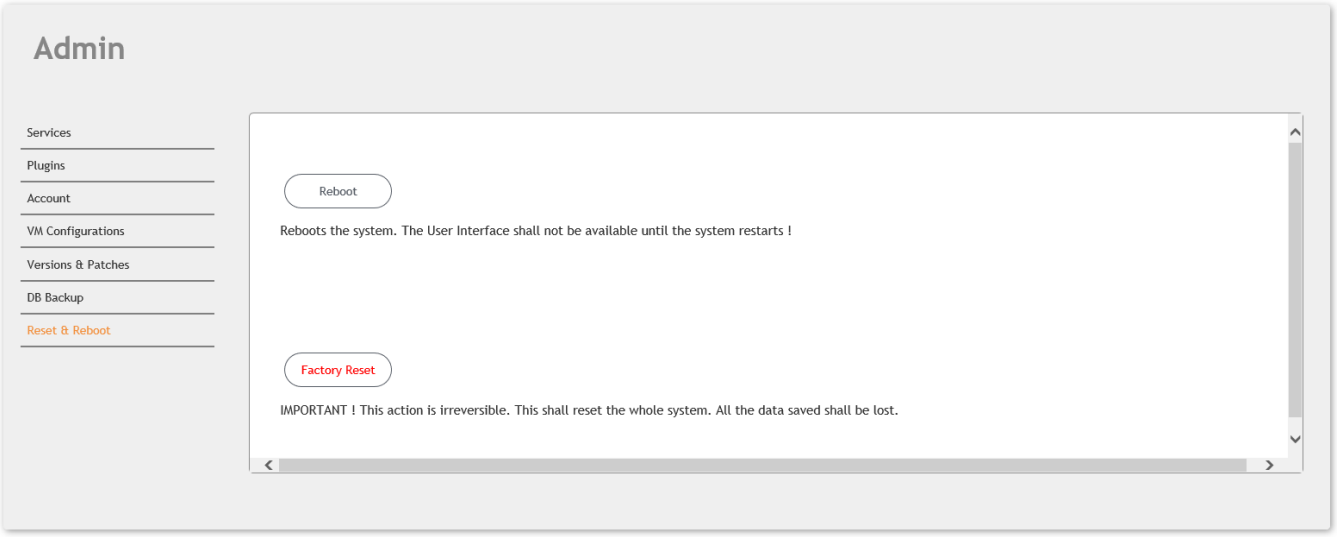
If the Ruckus IoT Controller is experiencing an issue, attempt a reboot to resolve the issue.

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 30 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.

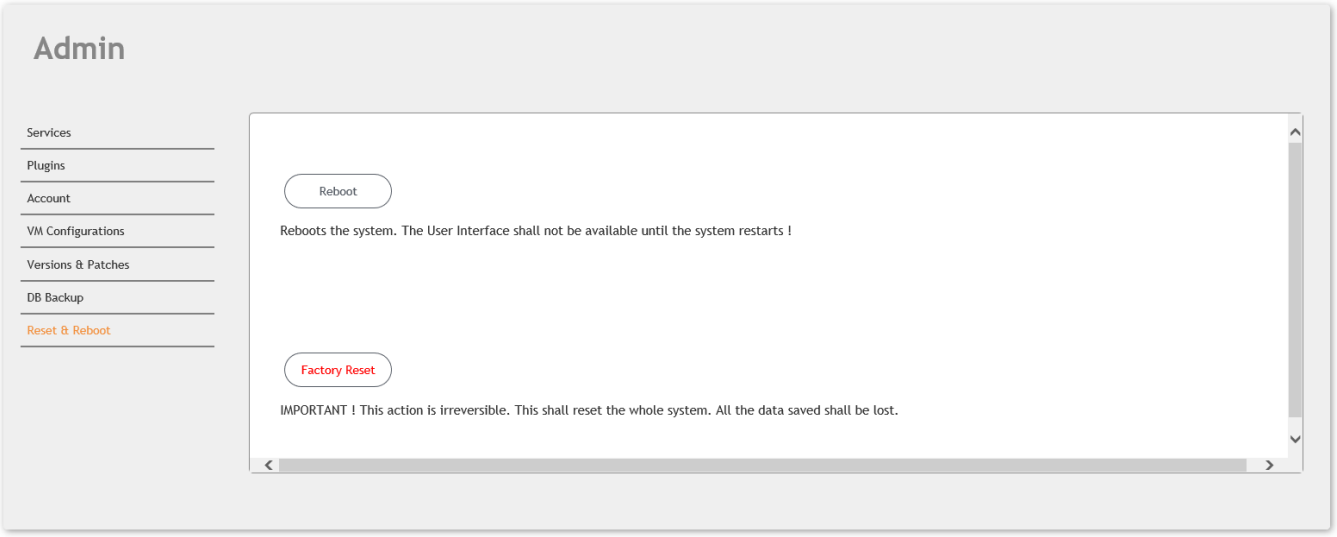
Complete the following steps to reset the Ruckus IoT Controller to its factory default settings.

CAUTION
Performing the reset action is irreversible.

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

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

FIGURE 31 Resetting Ruckus IoT Controller



3. Click **Factory Reset**.

Managing IoT Access Points

- IoT AP Overview....43
- Adding an IoT AP.... 44
- Editing an IoT AP....47
- Approval of IoT APs.... 48

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.

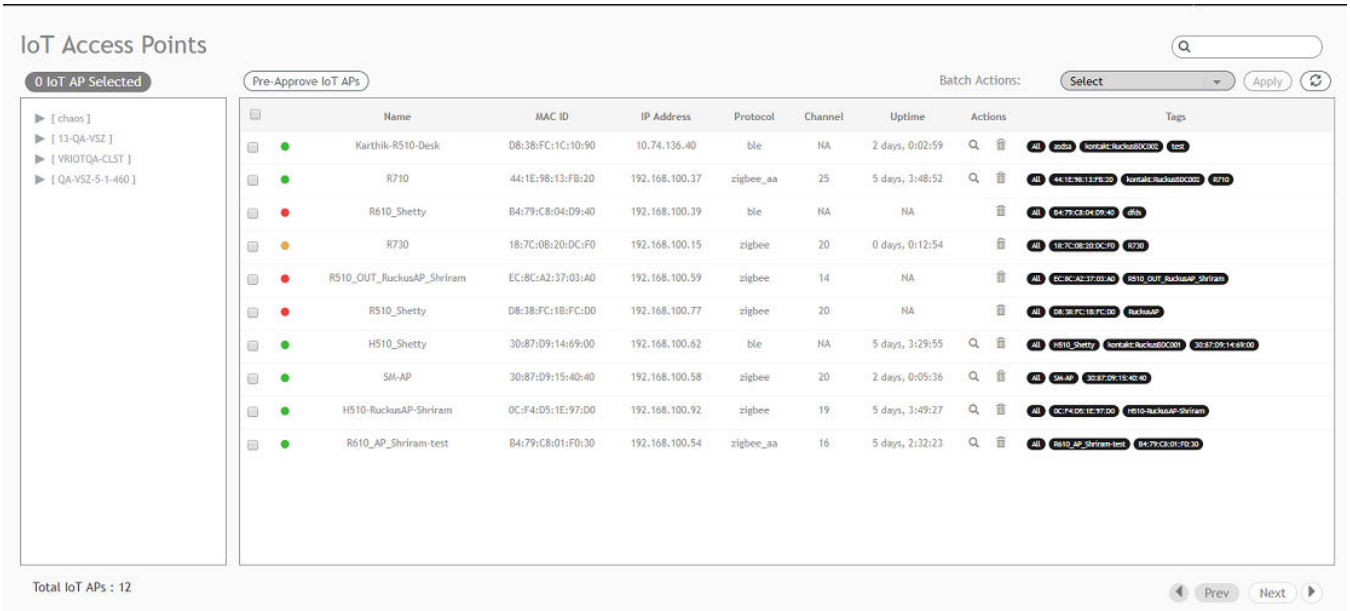
Adding an IoT AP

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.

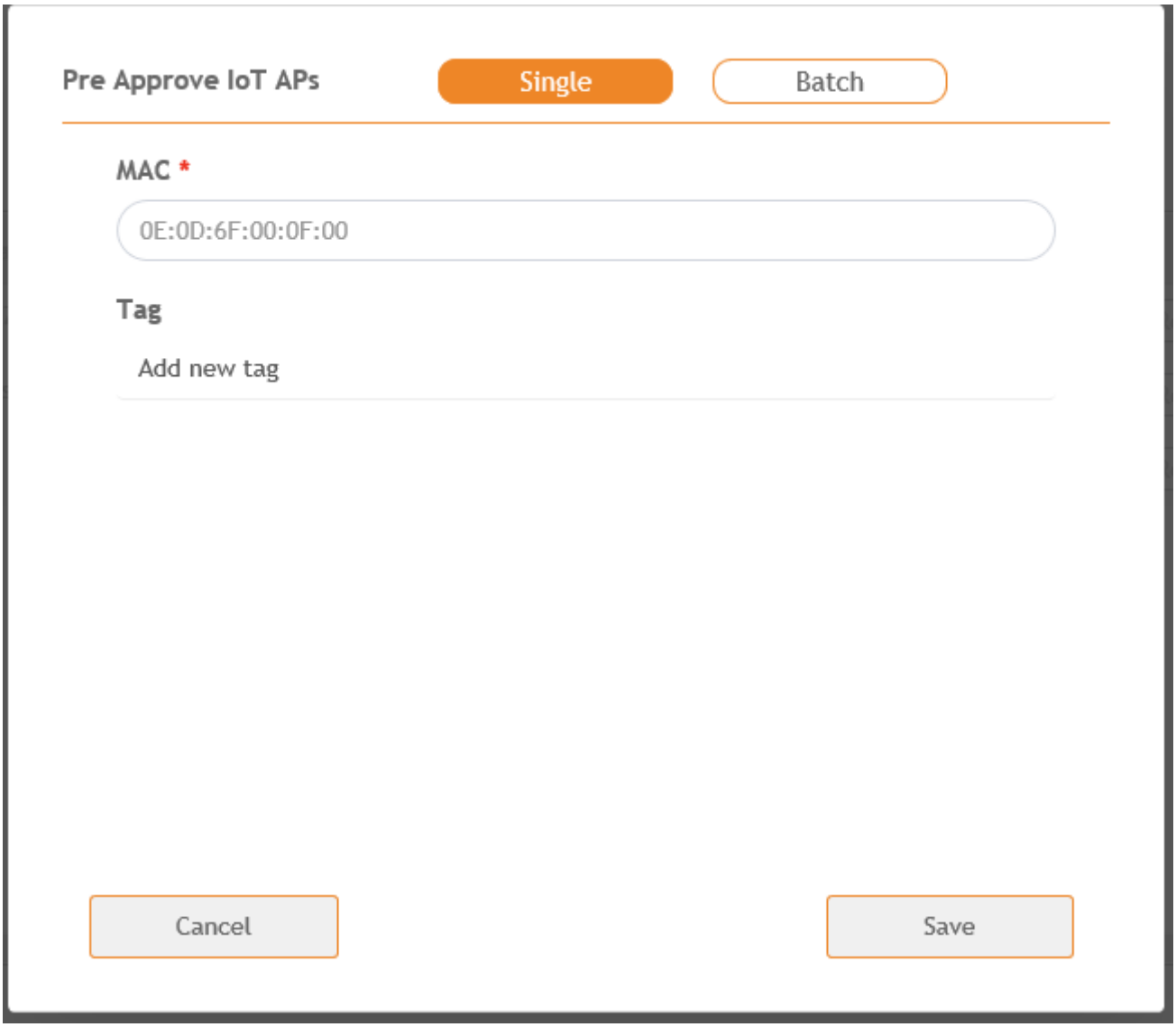
   FIGURE 32 IoT Access Points Page



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

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

FIGURE 33 Adding a Single IoT AP

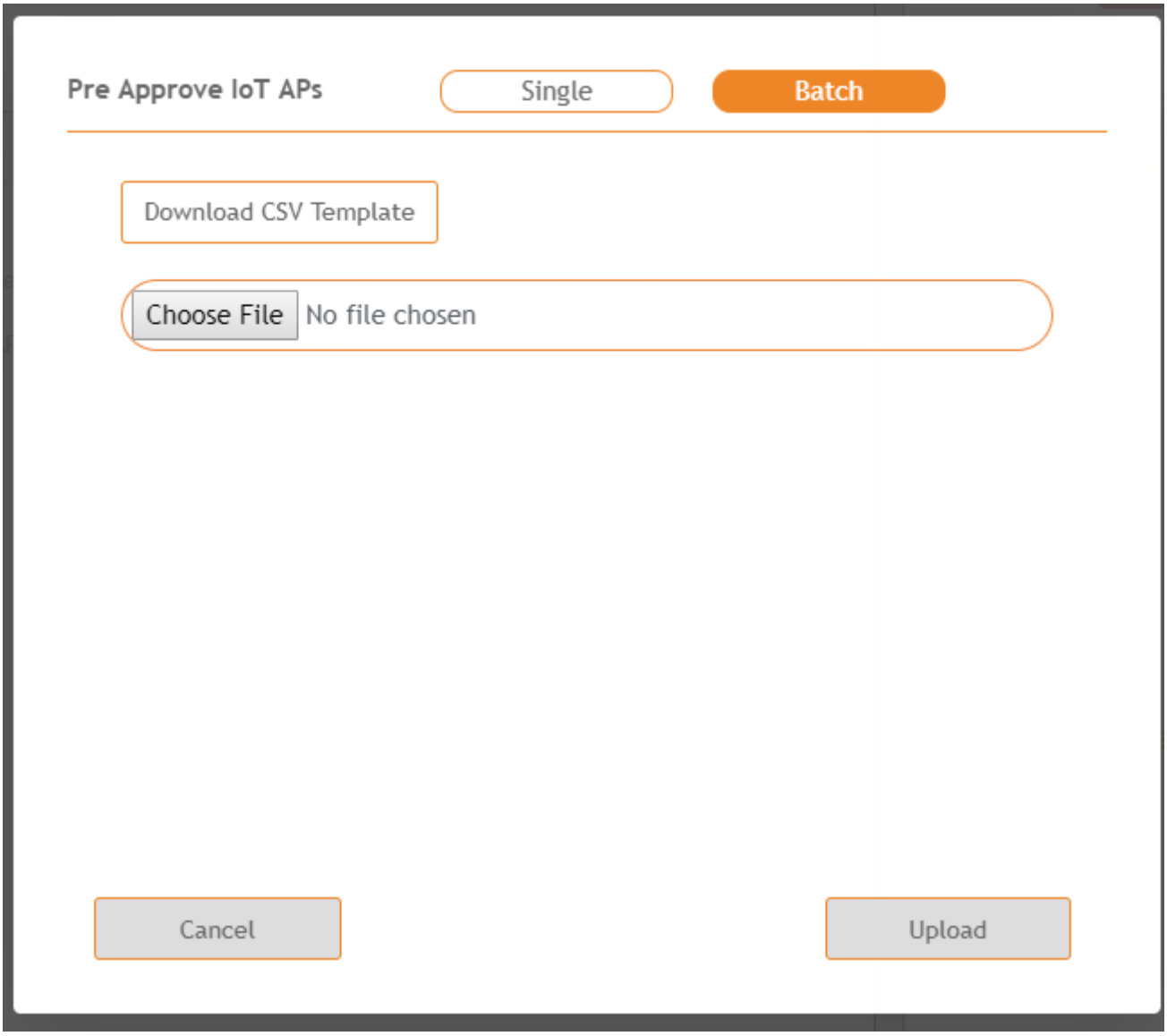


4. Enter the MAC address of the IoT AP and click **Save**.

   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 34 Adding a Batch of IoT APs



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

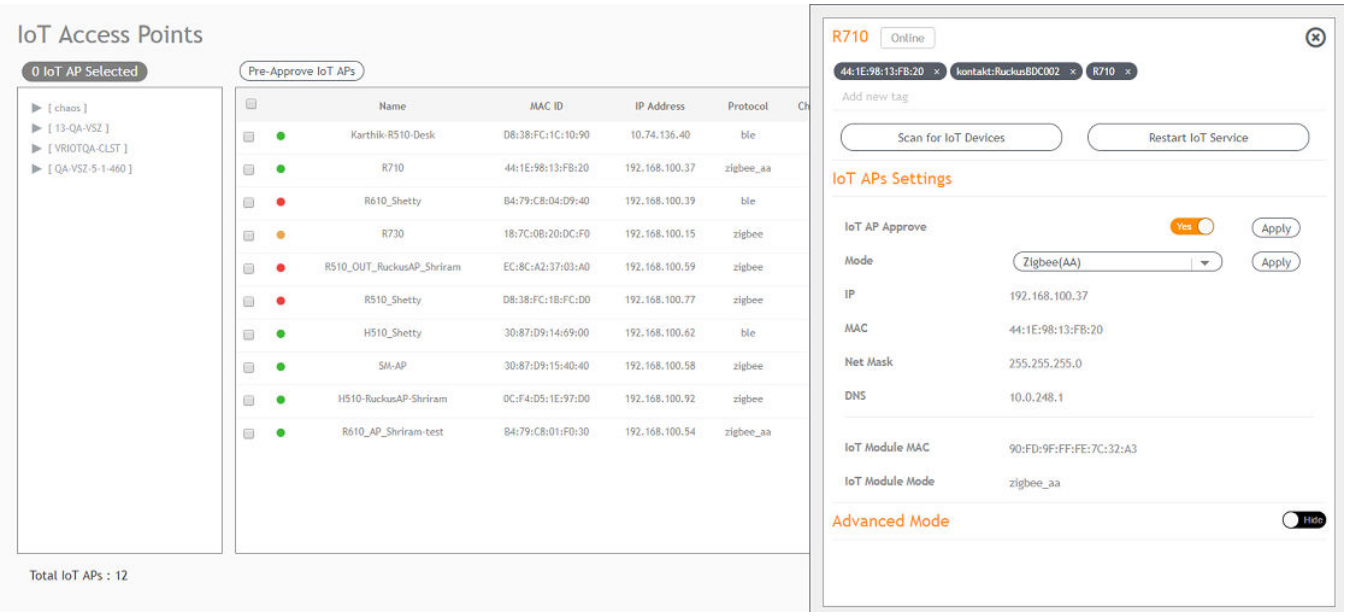
You can use Single IoT Access Point Mode to edit a single IoT AP.

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 35 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.

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.....49
- Managing OSRAM Light Bulbs..... 50
- Managing an Assa Abloy Lock.....51

Devices Overview

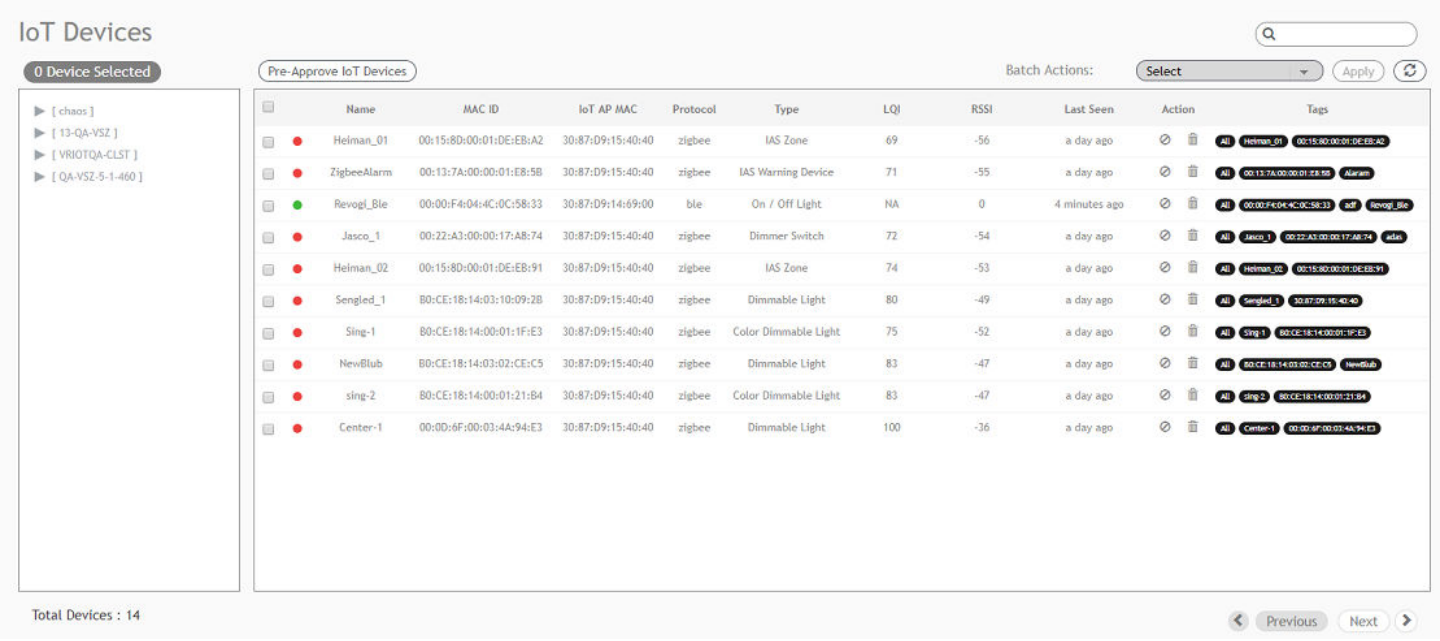
The Ruckus IoT Controller requires explicit user approval of devices. Only an approved device can be allowed into the IoT infrastructure.

To add devices to the Ruckus IoT Controller, from the main menu, click **IoT Devices**.

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

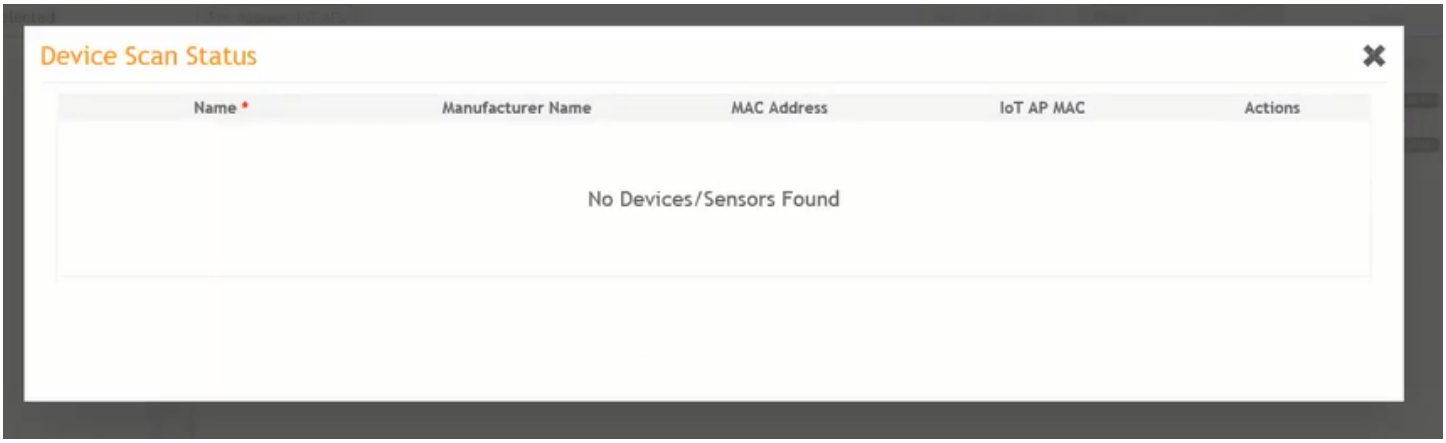
- A list of devices
- The operations on devices (such as remove, blacklist, and device-specific operations)

FIGURE 36 IoT Devices Page



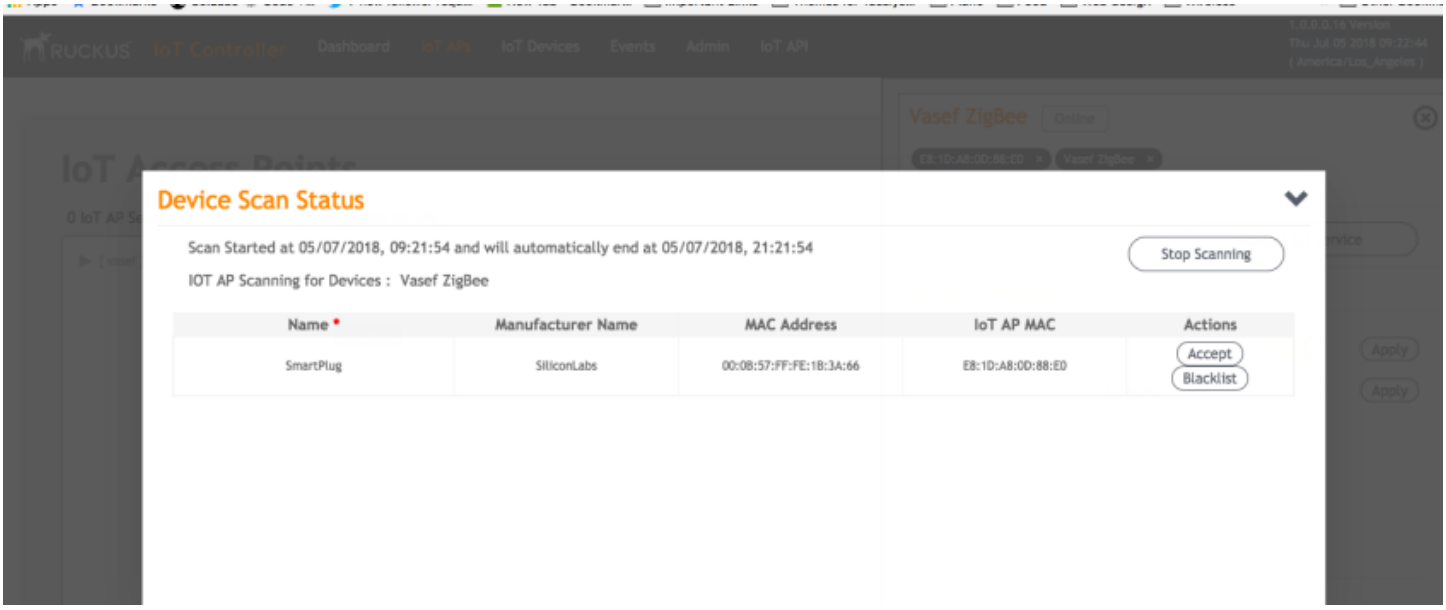
The device scan operation must be performed to start the device discovery process on the gateway. Upon starting device discovery, a dialog box is displayed, as shown in the following figure.

FIGURE 37 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 38 Adding Device After Discovery



Managing OSRAM Light Bulbs

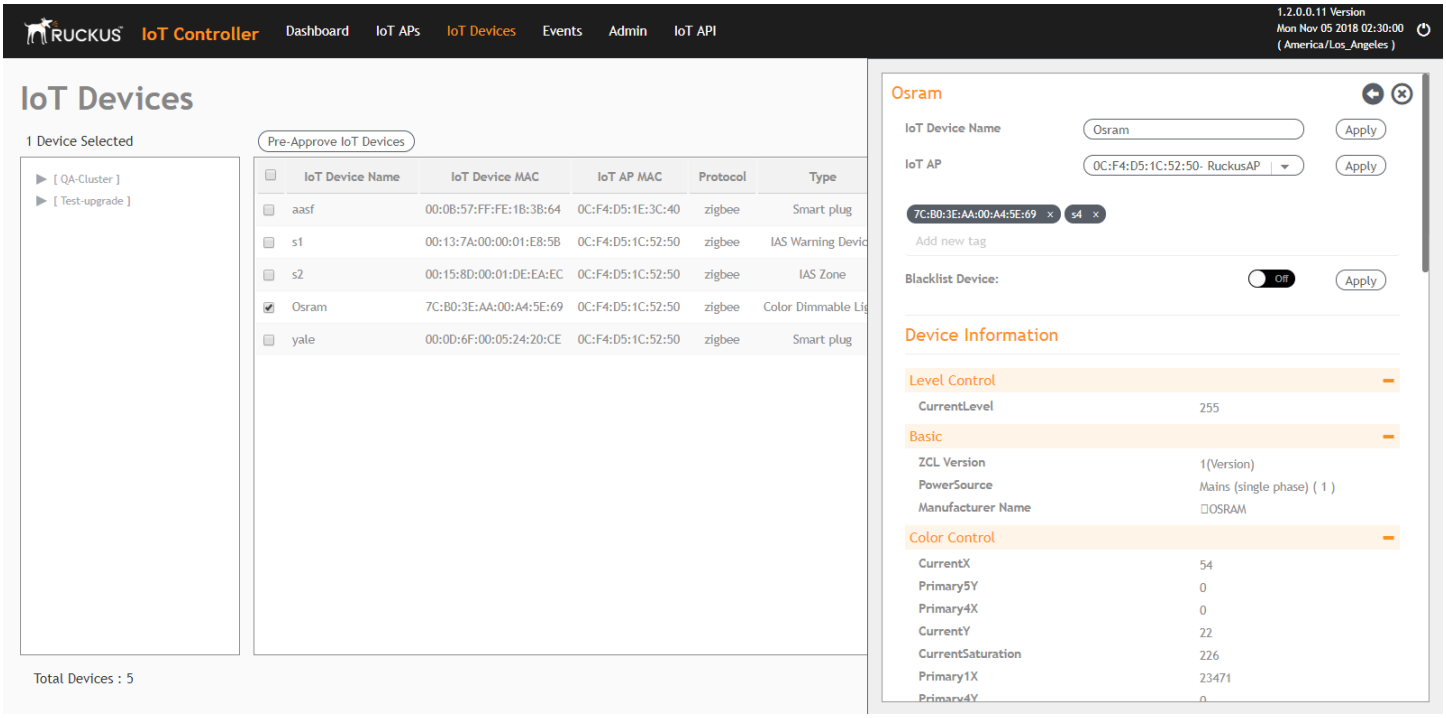
To discover OSRAM light bulbs, complete the following operations.

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 39 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.

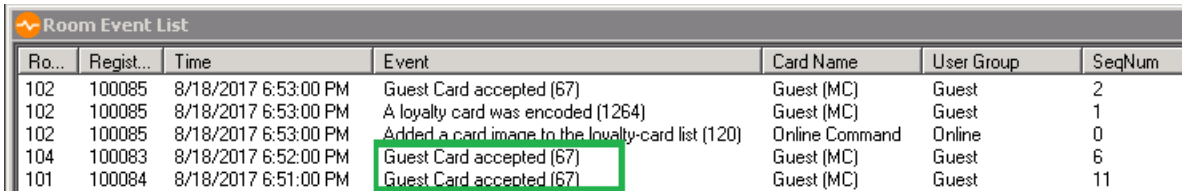
1. Swipe the AA Lock Discover Card across the lock.
2. Ensure that the LED blinks green.
3. Add the lock to the Ruckus IoT Controller (if it is not already pre-approved).

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 40 Visionline Server Event Log



Events

- Viewing Events..... 53

Viewing Events

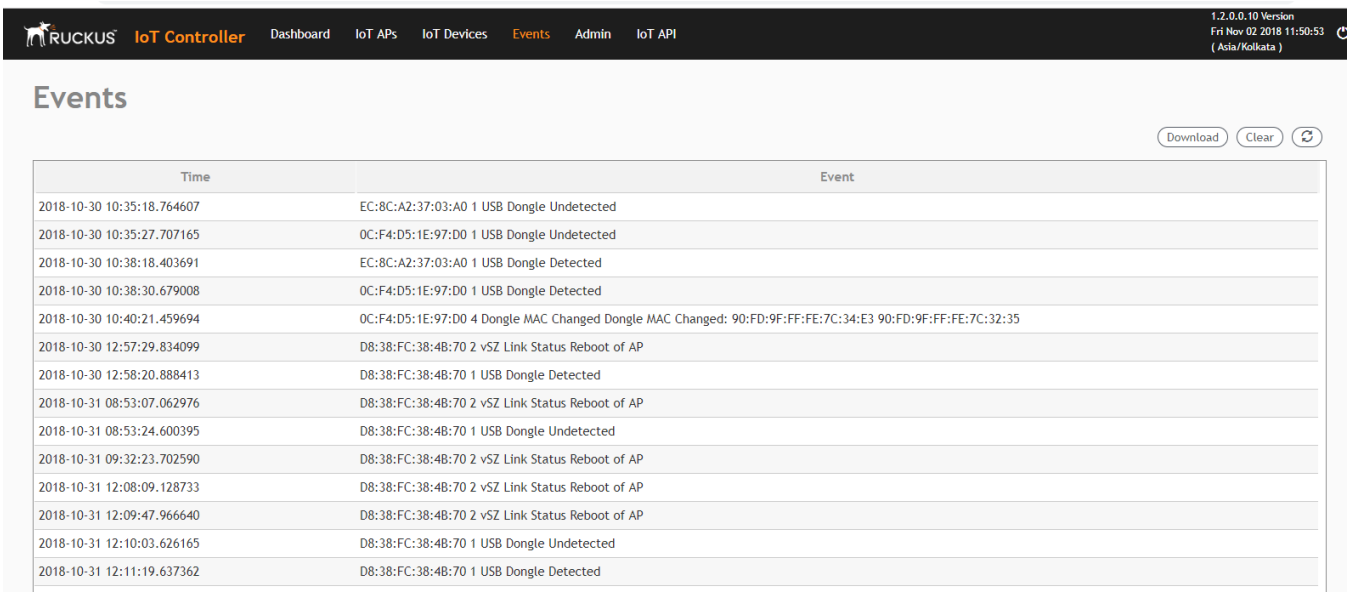
An event is an occurrence or the detection of certain conditions in and around the Ruckus IoT Module. An AP rebooting, detection of a Ruckus IoT Module, module undetection, and module swap are all examples of events.

Complete the following steps to view events.

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

   The **Events** page is displayed.

   FIGURE 41 Events Page



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 ARRIS Enterprises LLC. All rights reserved.
Ruckus Wireless, Inc., a wholly owned subsidiary of ARRIS International plc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com