CONFIGURATION GUIDE

Ruckus IoT Controller Configuration Guide , 1.1

Supporting IoT Controller Release 1.1

Part Number: 800-72016-001 Rev A
Publication Date: 31 August 2018

Copyright, Trademark and Proprietary Rights Information

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

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

About this Guide

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.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the Ruckus Support Web site at https://support.ruckuswireless.com/contact-us.

Getting Started

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 Browsers

Browser	Version
Google Chrome	63.0
Apple Safari	60.0
Mozilla Firefox	10.1.2 (10603.3.8)

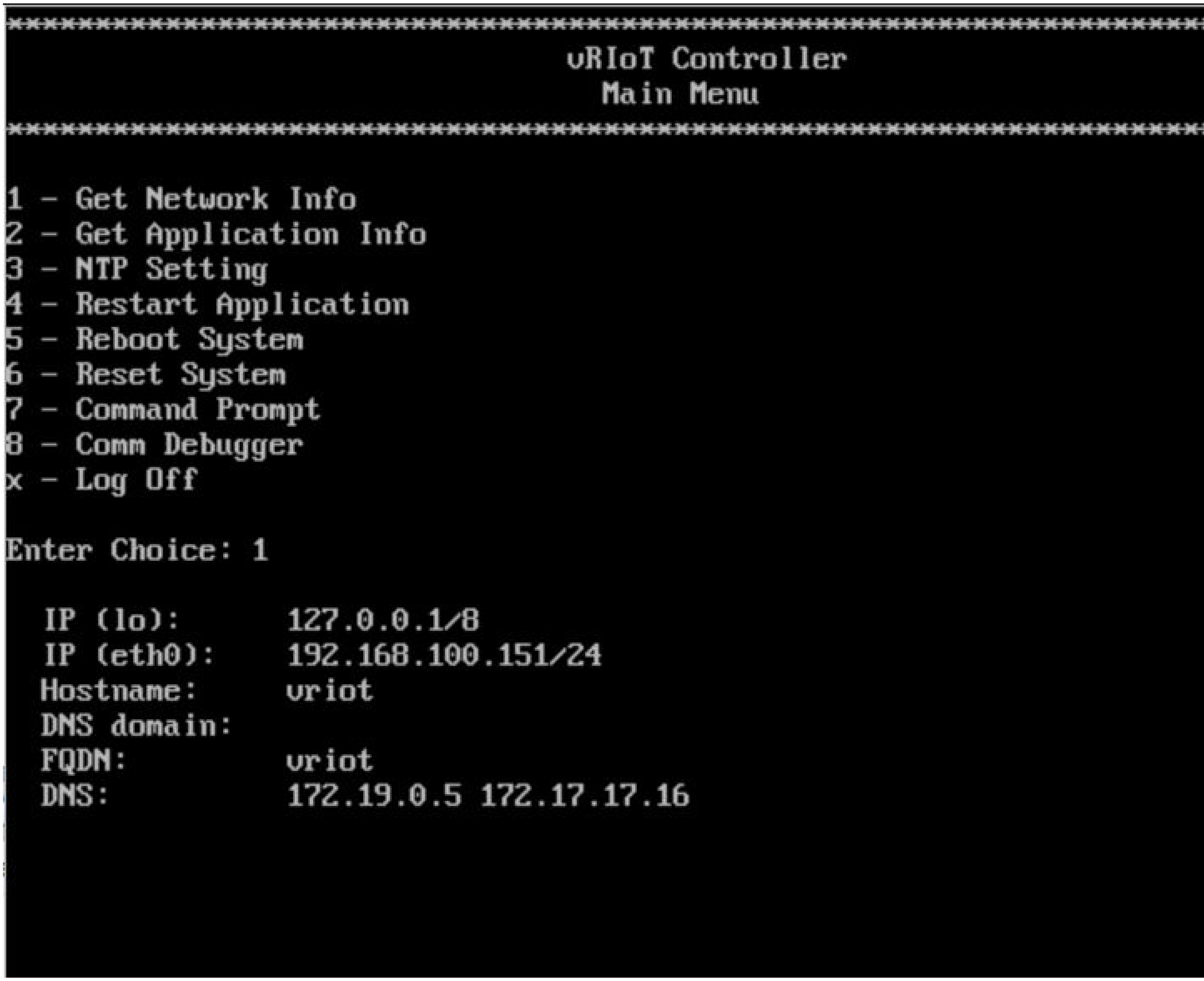
Logging In to Ruckus IoT Controller

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

1. Log in to the console of 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

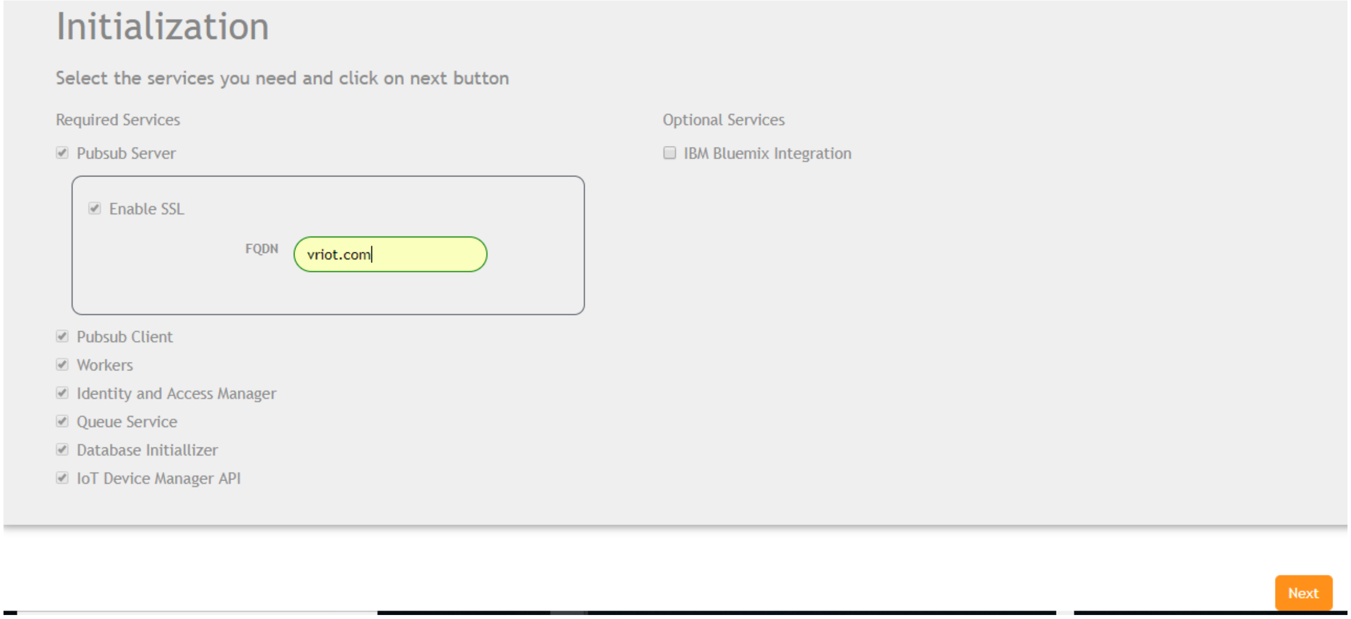


```
****************************************************************************
                              vRIoT Controller
                                Main Menu
****************************************************************************

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

Enter Choice: 1

  IP (lo):       127.0.0.1/8
  IP (eth0):     192.168.100.151/24
  Hostname:      vriot
  DNS domain:
  FQDN:          vriot
  DNS:           172.19.0.5 172.17.17.16
```

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

   The **Initialization** page is displayed.

   FIGURE 2 Initialization Page



Initialization

Select the services you need and click on next button

Required Services

☑ Pubsub Server

☑ Enable SSL

FQDN: vriot.com

☑ Pubsub Client

☑ Workers

☑ Identity and Access Manager

☑ Queue Service

☑ Database Initiallizer

☑ IoT Device Manager API

Optional Services

☐ IBM Bluemix Integration

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

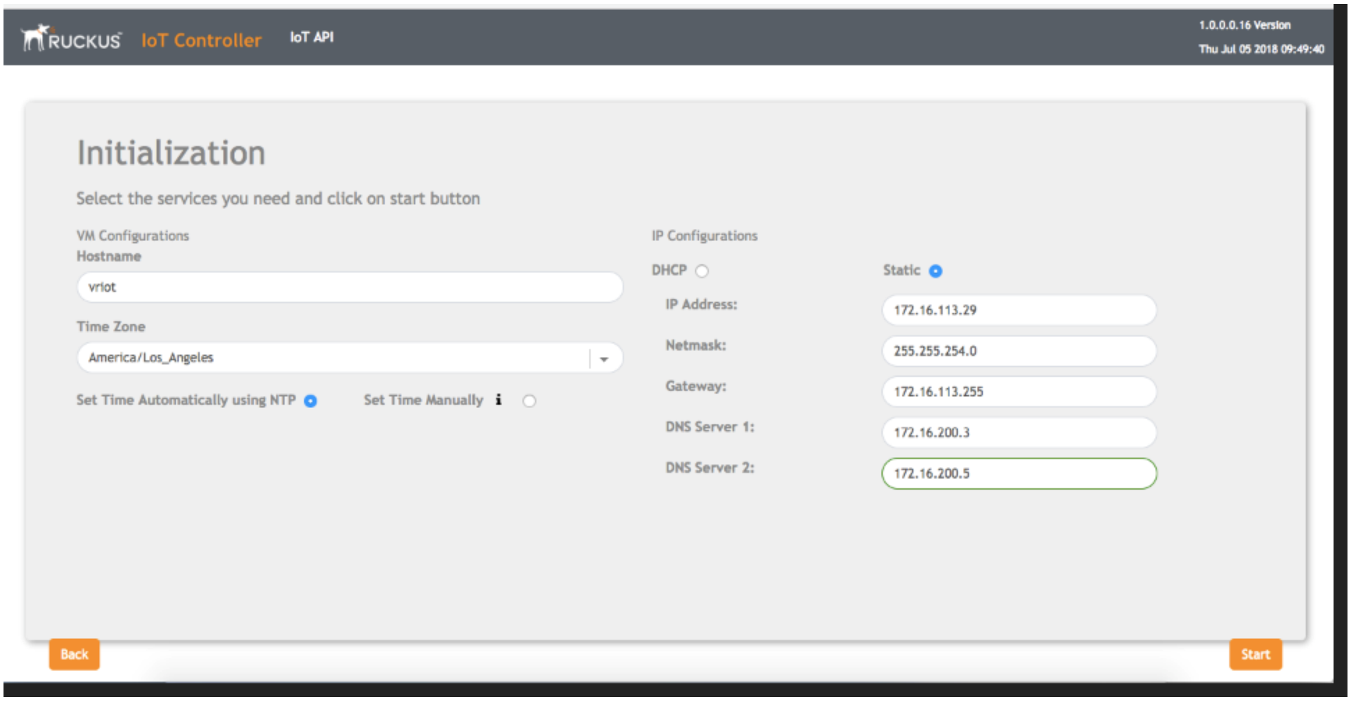
PubSub Server works in SSL mode with mutual authentication, so you must provide a Fully Qualified Domain Name (FQDN) to generate the certificates.

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



Initialization

Select the services you need and click on start button

VM Configurations

Hostname: vriot

Time Zone: America/Los_Angeles

Set Time Automatically using NTP ● Set Time Manually ○

IP Configurations

DHCP ○ Static ●

IP Address: 172.16.113.29

Netmask: 255.255.254.0

Gateway: 172.16.113.255

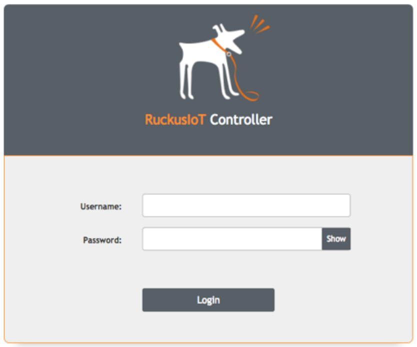
DNS Server 1: 172.16.200.3

DNS Server 2: 172.16.200.5

NOTE
The figure shows a static IP 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 your 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

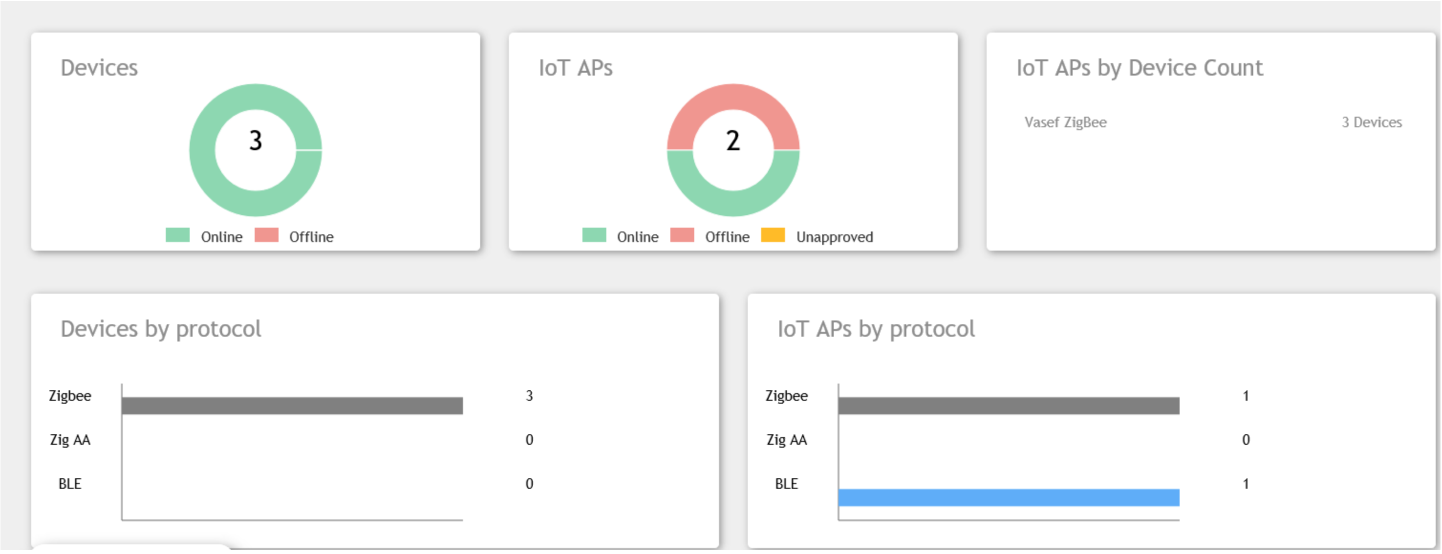


TABLE 3 Dashboard Elements

Box Name	Description
Devices	Shows the status of devices that are connected to the Ruckus IoT Controller.
IoT APs	Shows the status of Access Points that are connected to the Ruckus IoT Controller.
IoT APs by Device Count	Shows the total number of devices connected per Access Point.
Devices by Protocol	Shows the total number of devices connected by the protocol being used. Ruckus supports three protocols: BLE, Zigbee, and Zigbee AA (Assa Abloy).
IoT APs by Protocol	Shows the number of APs running by the protocol being used. Ruckus supports three protocols: BLE, Zigbee, and Zigbee AA (Assa Abloy).

Managing IoT Controller System Configuration

Activating Services

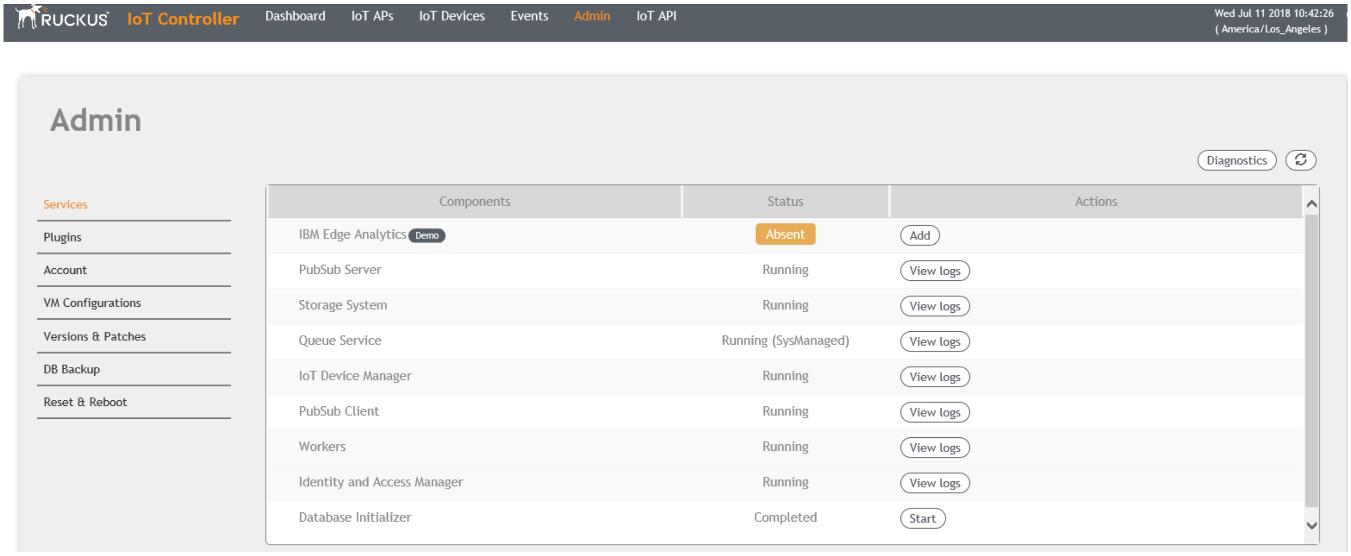
The administrator can restart or manage the mandatory and optional services.

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**.

   Currently running services and their details are displayed.
3. Select a service to edit, restart, or view logs.

FIGURE 6 Services



Components	Status	Actions
IBM Edge Analytics Demo	Absent	Add
PubSub Server	Running	View logs
Storage System	Running	View logs
Queue Service	Running (SysManaged)	View logs
IoT Device Manager	Running	View logs
PubSub Client	Running	View logs
Workers	Running	View logs
Identity and Access Manager	Running	View logs
Database Initializer	Completed	Start

Activating Plugins

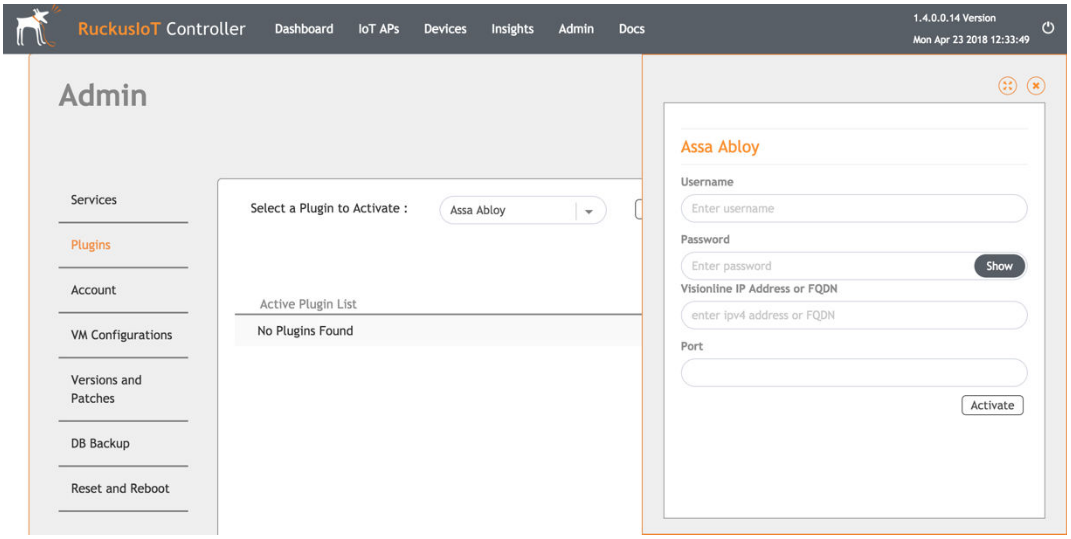
Plugins are the external vendor connectors that can be connected to a vendor infrastructure after the successful activation of a plugin.

Ruckus supports Assa Abloy locks and plugins such as Kontakt.io, iBeacon, and Eddystone .

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**.

FIGURE 7 Plugin Activation



Select a Plugin to Activate : Assa Abloy

Active Plugin List

No Plugins Found

Assa Abloy

Username: Enter username

Password: Enter password

Visionline IP Address or FQDN: enter ipv4 address or FQDN

Port:

3. In the **Select a Plugin to Activate** list, select a plugin.

   The **Active Plugin List** lists the active plugins.
4. Click the active plugin to edit the configuration or deactivate the plugin.

   NOTE
   The figure shows the information for the Assa Abloy plugin. Enter the appropriate information in the **Username**, **Password**, **Visionline IP Address or FQDN** , and **Port** fields and click **Activate**.

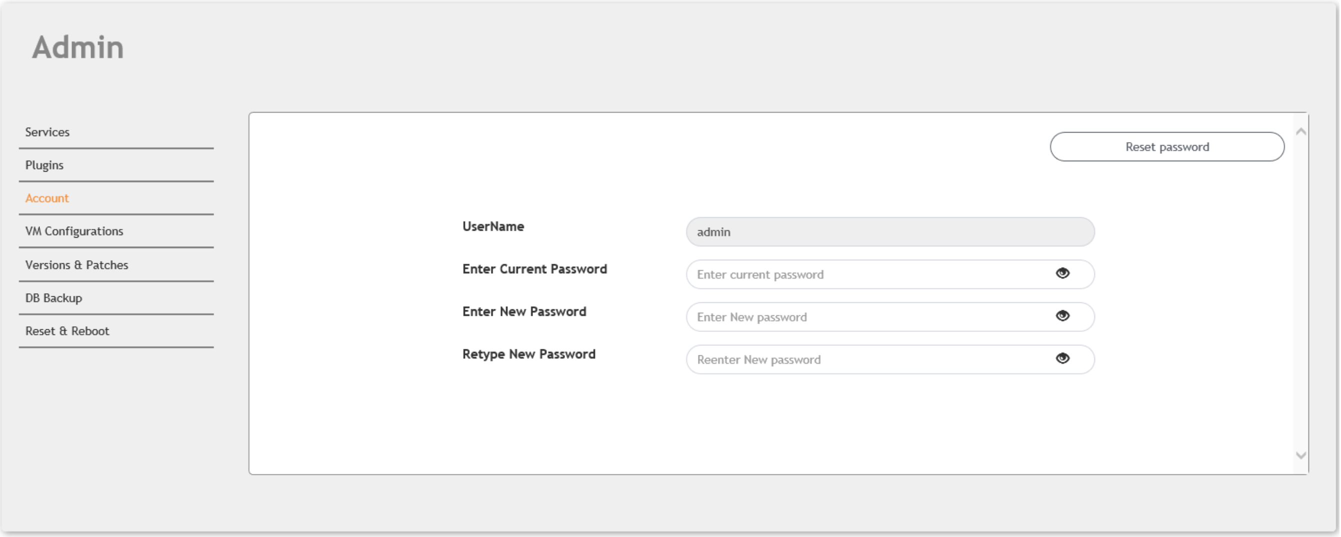
Changing the Password

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 below steps.

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

FIGURE 8 Changing the Password



UserName: admin
Enter Current Password: Enter current password
Enter New Password: Enter New password
Retype New Password: Reenter New password

2. Change the password and click **Reset password**.

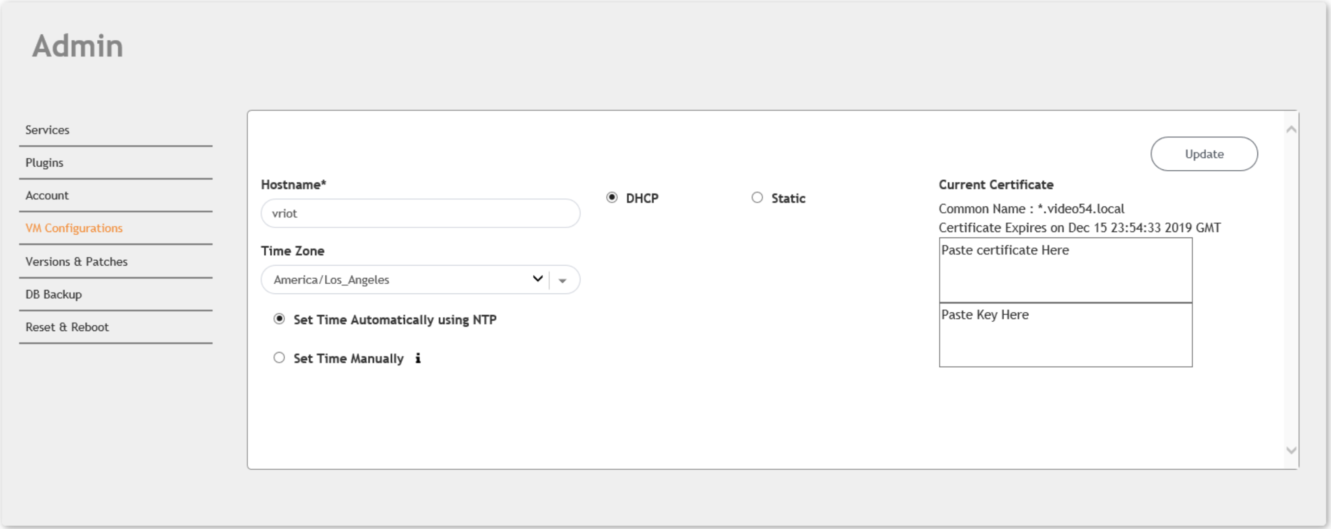
Configuring Virtual Machines

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 9 Configuring Virtual Machine



Hostname*
vriot

Time Zone
America/Los_Angeles

● Set Time Automatically using NTP

○ Set Time Manually

● DHCP ○ Static

Current Certificate
Common Name : *.video54.local
Certificate Expires on Dec 15 23:54:33 2019 GMT

Paste certificate Here

Paste Key Here

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 Tim 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**.

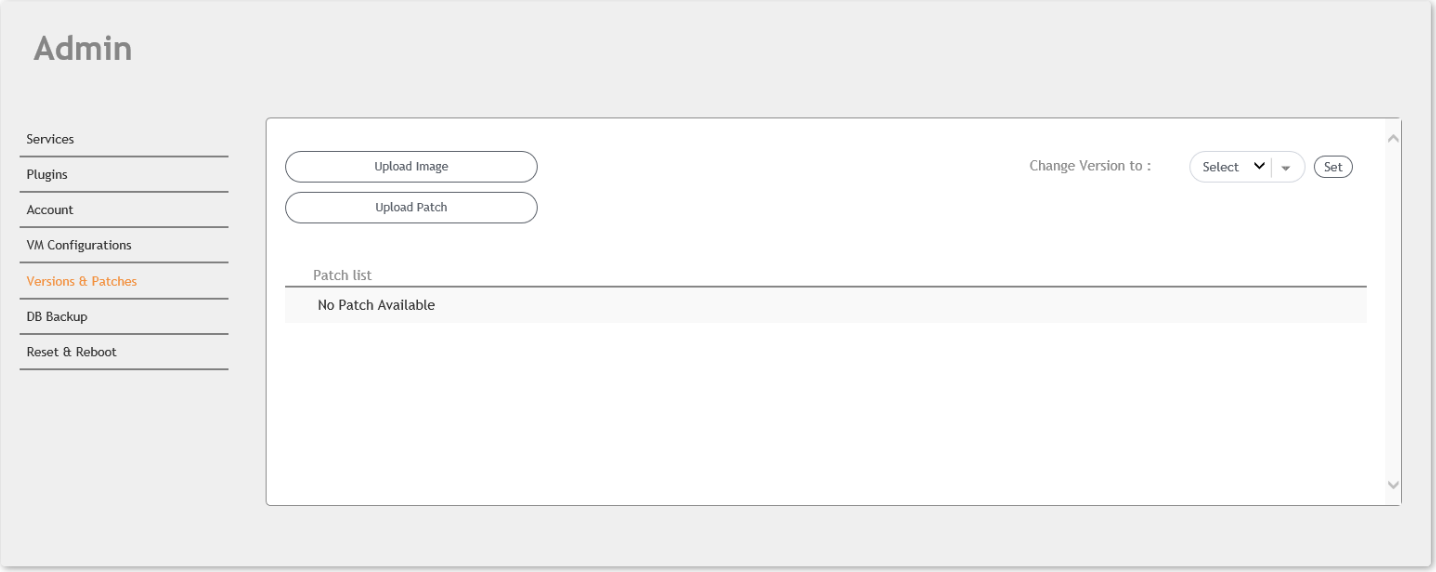
Uploading Versions and Patches

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.

FIGURE 10 Uploading an Image



No Patch Available

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

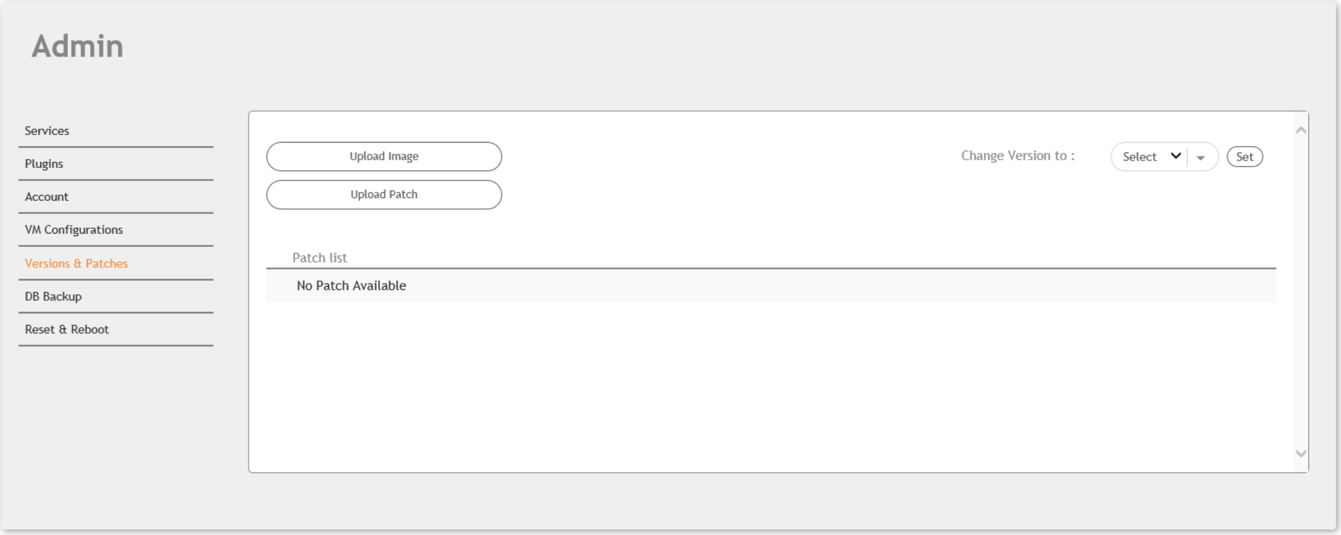
Uploading a Patch

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 11 Uploading a Patch



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

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

   NOTE
   You cannot revert a patch.

Backing Up Files

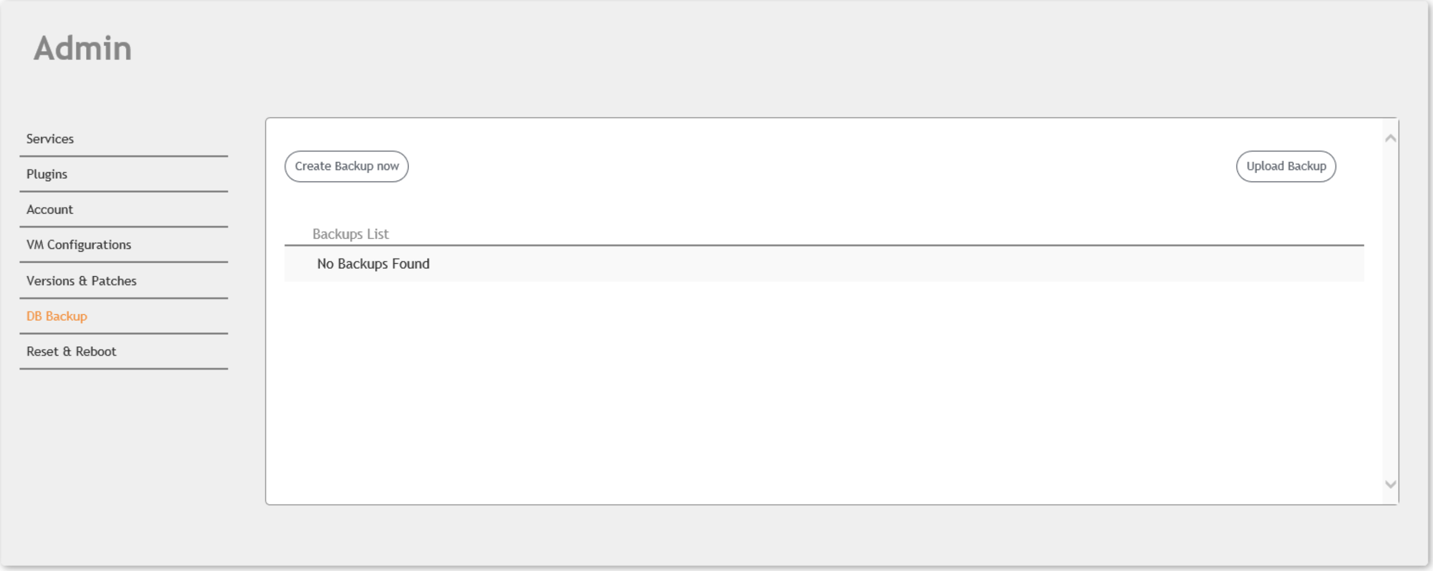
The Ruckus IoT Controller allows you to back up and restore the configuration and data files. You can restore an existing configuration file on the Ruckus IoT Controller from which it is originated, or restore a configuration file from a different Ruckus IoT Controller. Backed up files are in the tar.gz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

To perform a backup manually, click **Create Backup now**.

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.

Backup files can be downloaded and re-uploaded by selecting **Upload Backup**.

FIGURE 12 Backing Up or Restoring Files



No Backups Found

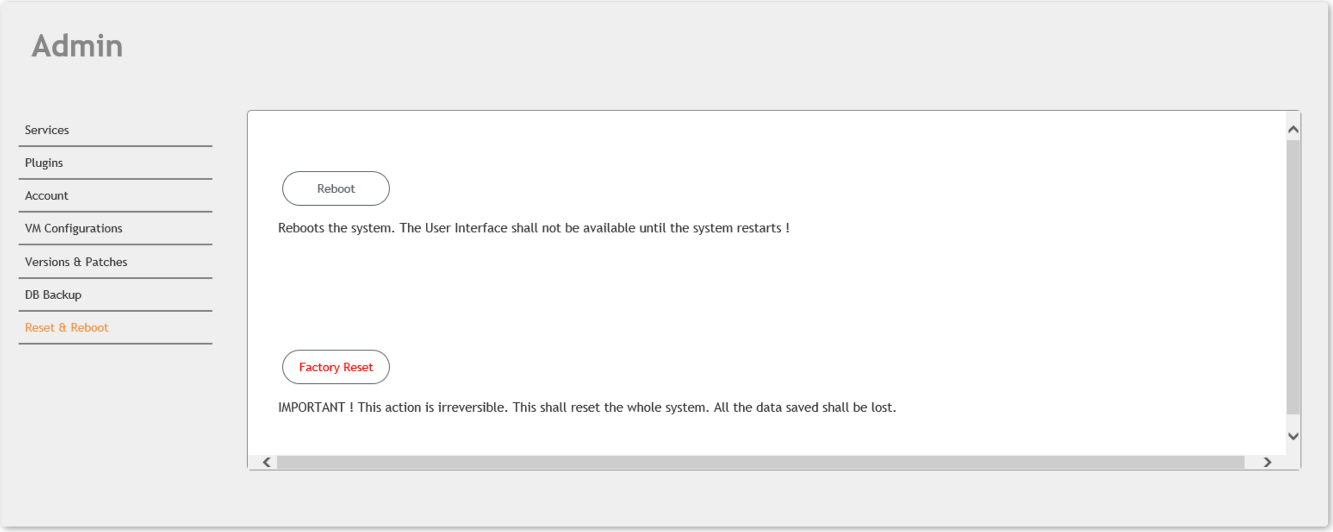
Rebooting Ruckus IoT Controller

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 **menu** , click **Admin**.
2. In the left navigation pane, click **Reset and Reboot**.

FIGURE 13 Rebooting Ruckus IoT Controller



Reboots the system. The User Interface shall not be available until the system restarts !

IMPORTANT ! This action is irreversible. This shall reset the whole system. All the data saved shall be lost.

3. Click **Reboot**.

Resetting Ruckus IoT Controller

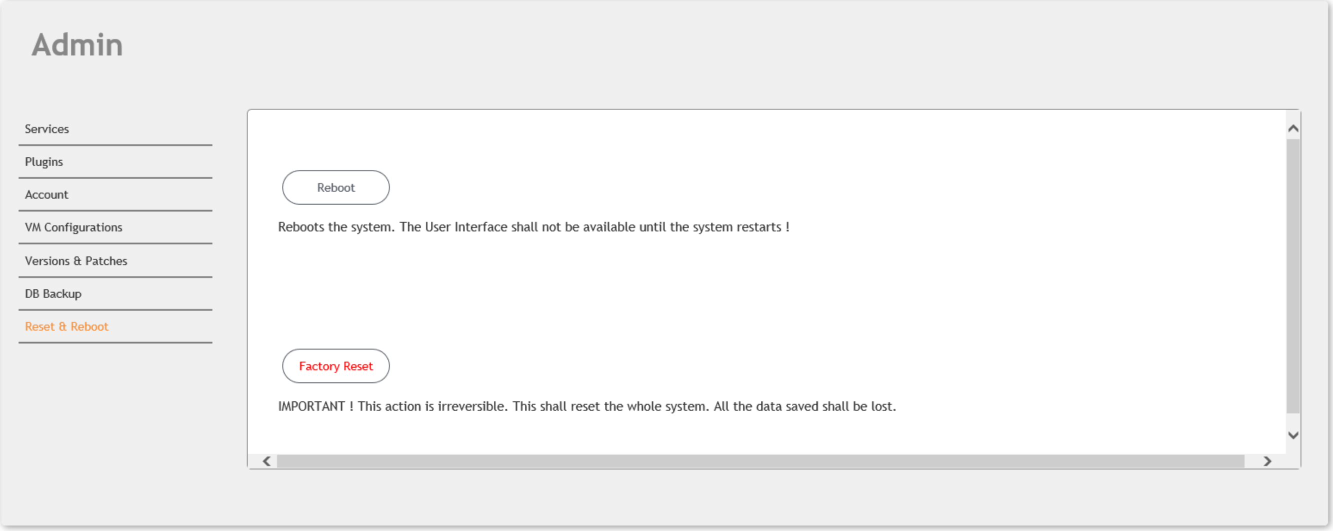
To remove all of the settings that are configured on the Ruckus IoT Controller, reset it to the factory default settings.

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

CAUTION
Performing a reset removes all of the settings that are configured.

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

   FIGURE 14 Resetting Ruckus IoT Controller



Reboots the system. The User Interface shall not be available until the system restarts !

IMPORTANT ! This action is irreversible. This shall reset the whole system. All the data saved shall be lost.

3. Click **Factory Reset**.

Managing IoT Access Points

IoT AP Overview

SmartZone (SZ) holds the IoT AP firmware. You must make sure the IoT Access Point 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 aRuckus 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

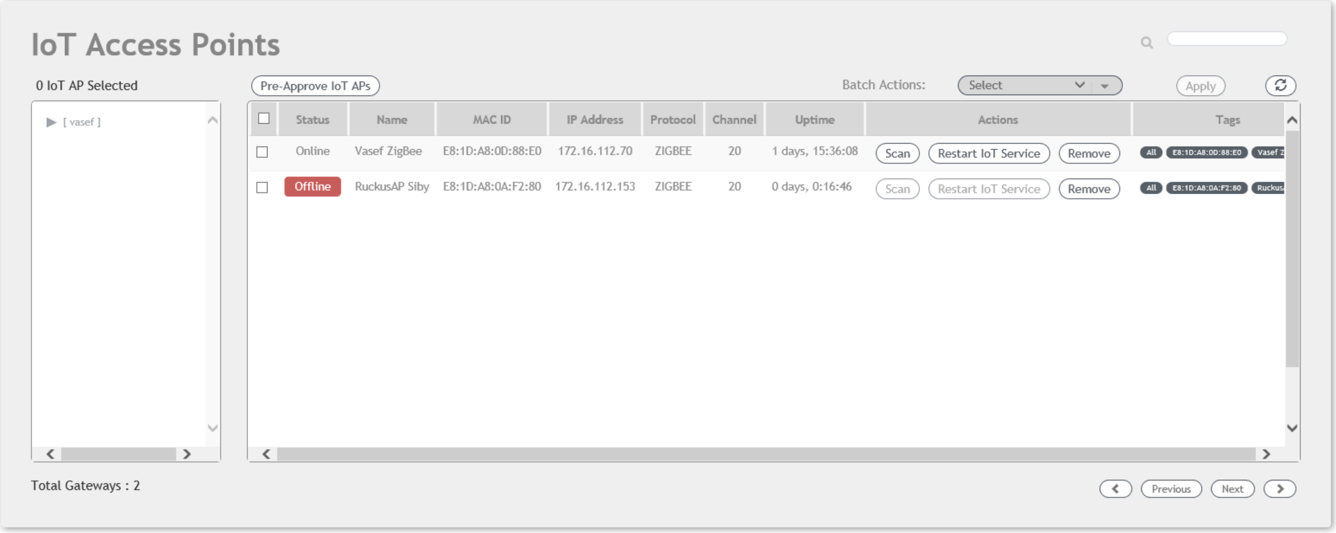
The administrator can add an IoT AP to the Ruckus IoT Controller to manage IoT devices.

Complete the following steps to add an IoT AP to Ruckus IoT Controller.

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

   The **IoT Access Point** page is displayed.

   FIGURE 15 IoT Access Point Page

   IoT Access Points

   0 IoT AP Selected

   Batch Actions: Select

□	Status	Name	MAC ID	IP Address	Protocol	Channel	Uptime	Actions	Tags
□	Online	Vasef ZigBee	E8:1D:A8:0D:88:E0	172.16.112.70	ZIGBEE	20	1 days, 15:36:08	Scan Restart IoT Service Remove	All E8:1D:A8:0D:88:E0 Vasef Z
□	Offline	RuckusAP Siby	E8:1D:A8:0A:F2:80	172.16.112.153	ZIGBEE	20	0 days, 0:16:46	Scan Restart IoT Service Remove	All E8:1D:A8:0A:F2:80 Ruckus

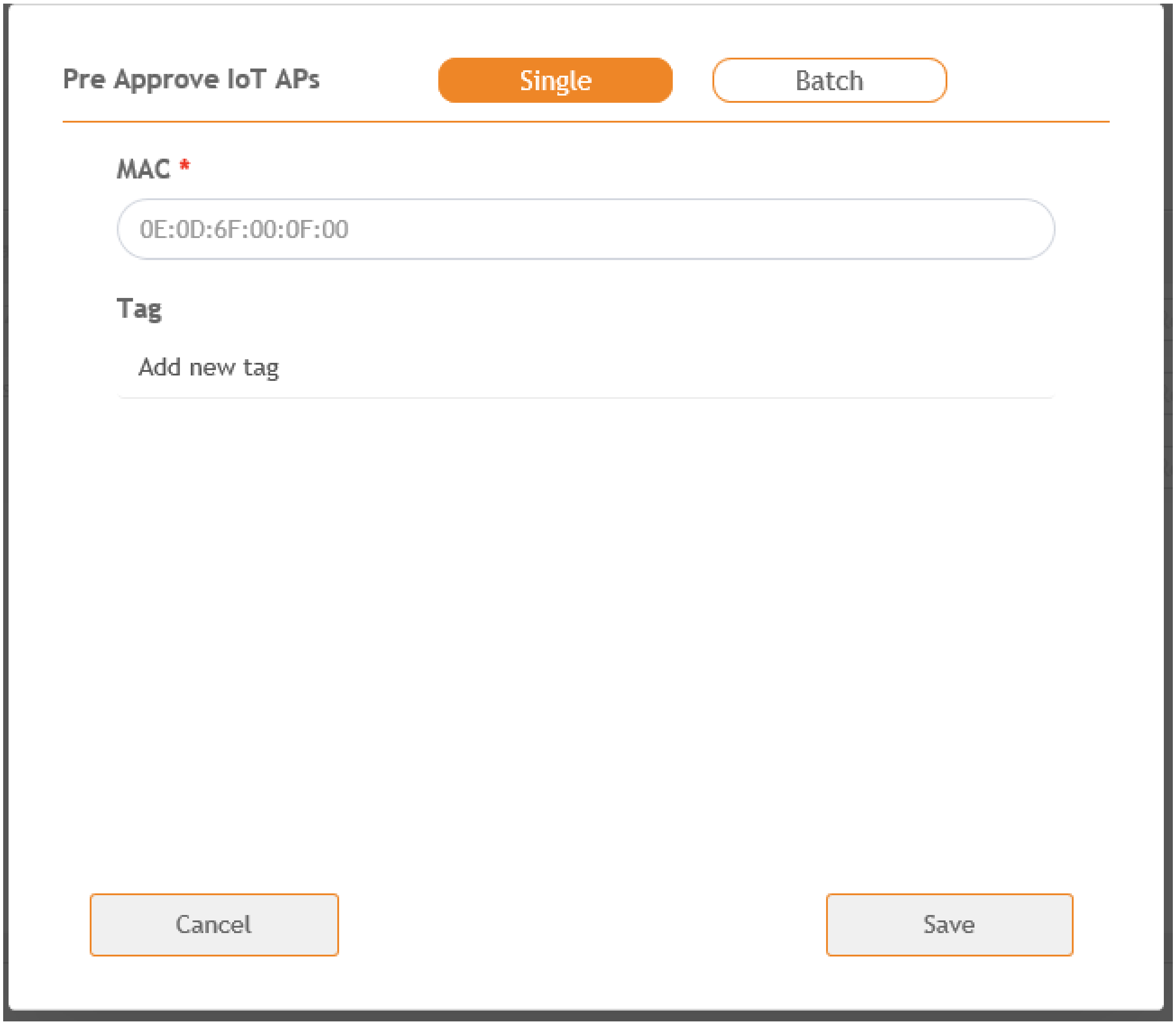
   Total Gateways : 2

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

   The **Pre-Approve IoT AP** page is displayed.

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

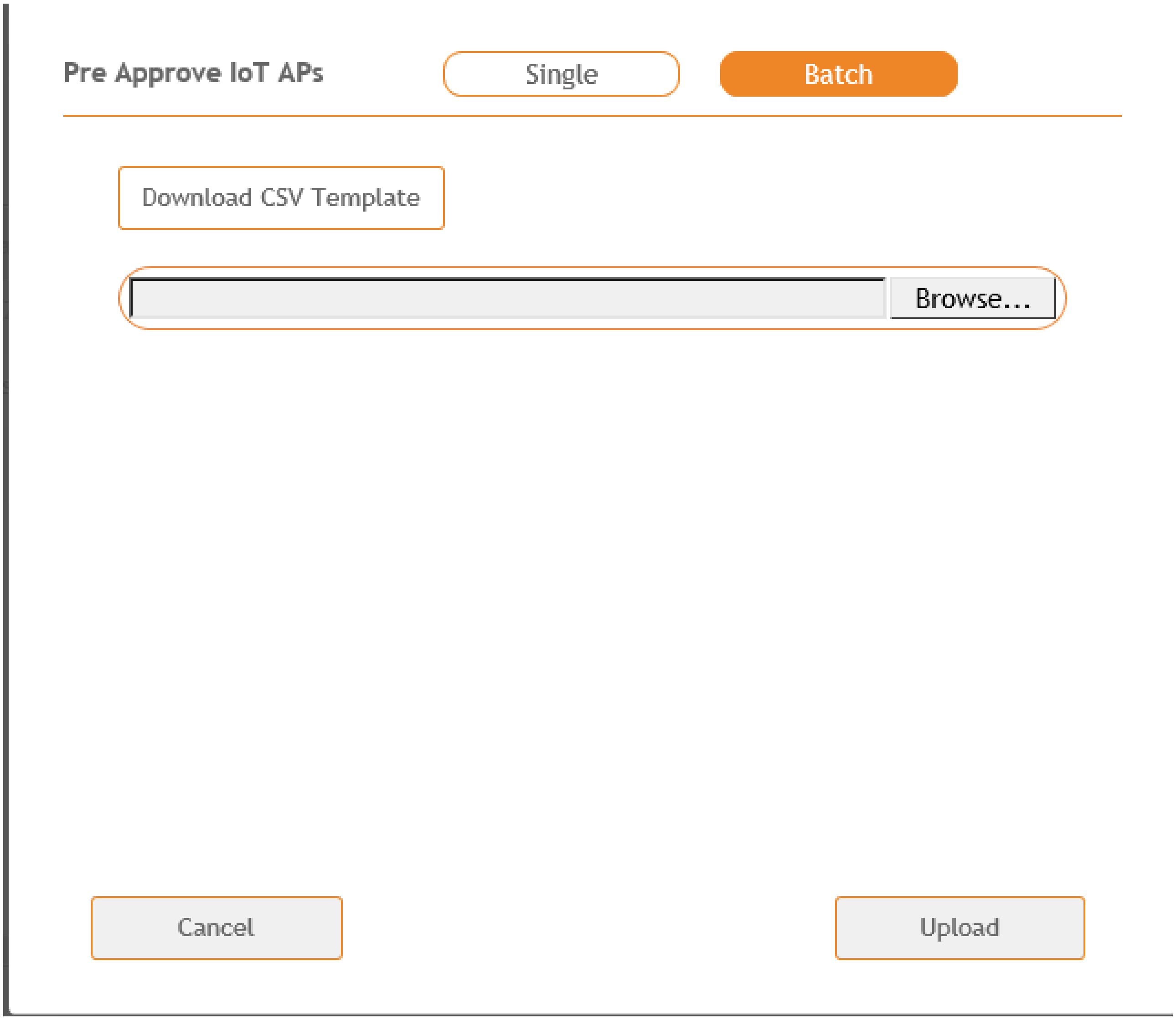
FIGURE 16 Adding a Single IoT AP



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 17 Adding a Batch of IoT APs



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

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

5. Approve the selected IoT AP.

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.

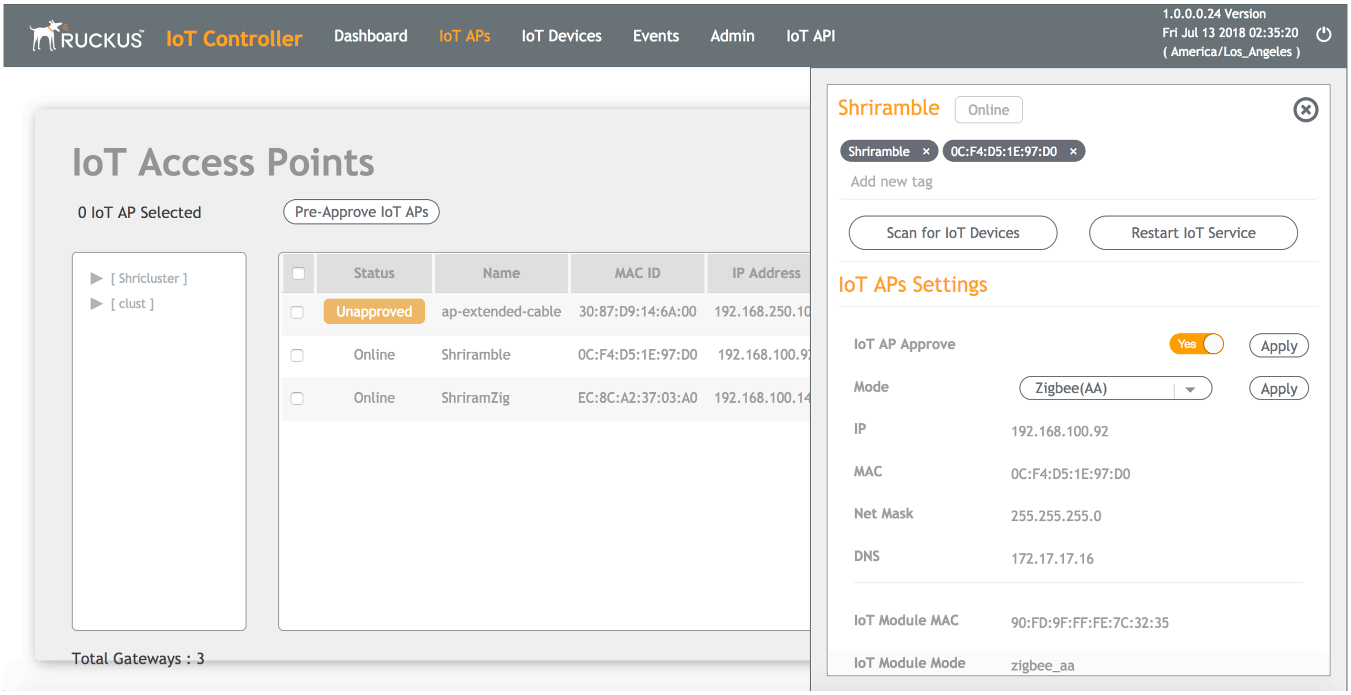
Complete the following steps to edit a single IoT AP.

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

   A list of selected IoT APs is displayed.

2. Click an IoT AP to edit.

FIGURE 18 Single IoT AP Mode



☐	Status	Name	MAC ID	IP Address
☐	Unapproved	ap-extended-cable	30:87:D9:14:6A:00	192.168.250.10
☐	Online	Shriramble	0C:F4:D5:1E:97:D0	192.168.100.9
☐	Online	ShriramZig	EC:8C:A2:37:03:A0	192.168.100.14

IoT AP Approve	Yes
Mode	Zigbee(AA)
IP	192.168.100.92
MAC	0C:F4:D5:1E:97:D0
Net Mask	255.255.255.0
DNS	172.17.17.16
IoT Module MAC	90:FD:9F:FF:FE:7C:32:35
IoT Module Mode	zigbee_aa

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**

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

Bulk AP Mode

You can use Bulk AP Mode to edit more than one IoT AP.

Complete the following steps to edit a batch of IoT APs.

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

   A list of selected IoT APs is displayed.

2. Select the IoT APs to edit.

   Administrator can edit the following in bulk options.

   - **Scan Devices**
   - **Set Channnel**
   - **Set Tx Power**
   - **DeApprove**
   - **Restart**
   - **Remove AP**
3. Select the options and click **Apply**.

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

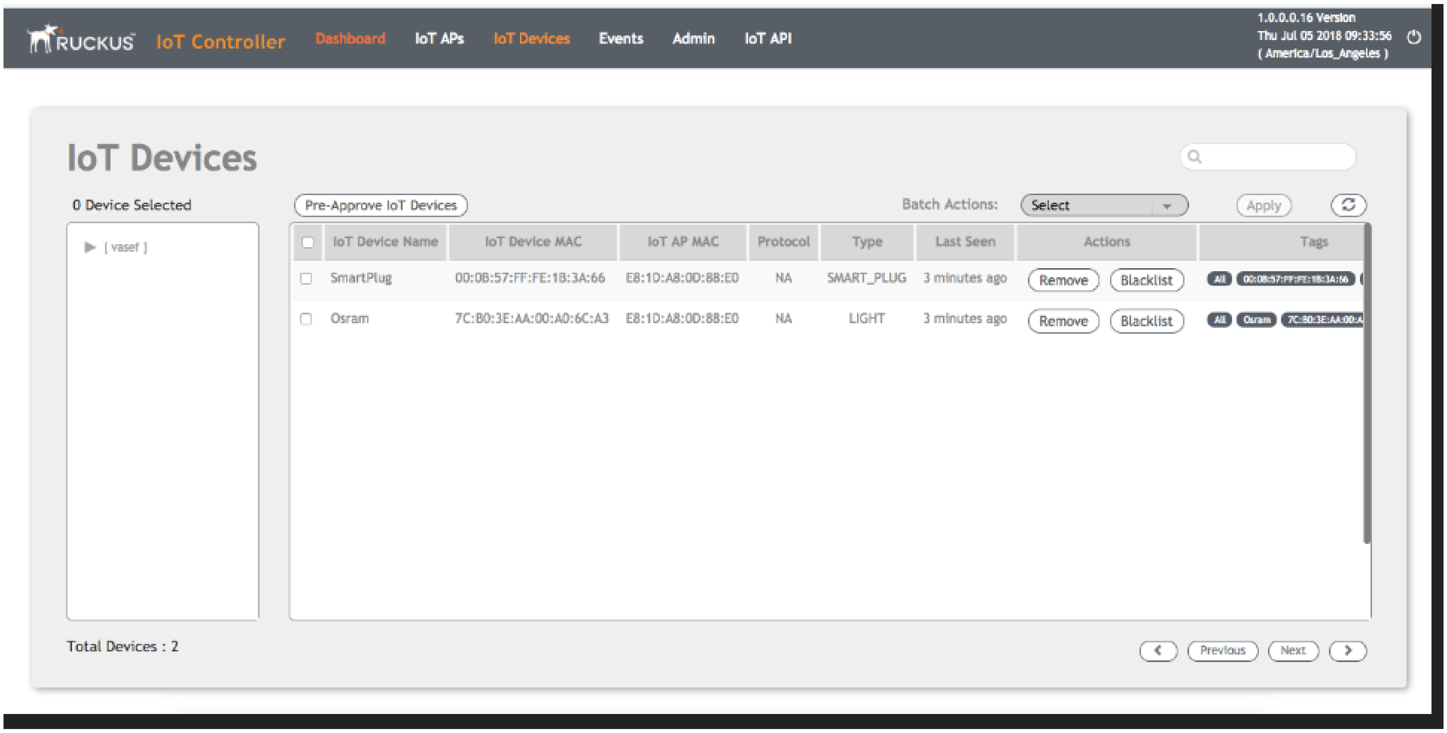
The Ruckus IoT Controller requires explicit user approval of devices. Only an approved device can be allowed into the IoT infrastructure.

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).

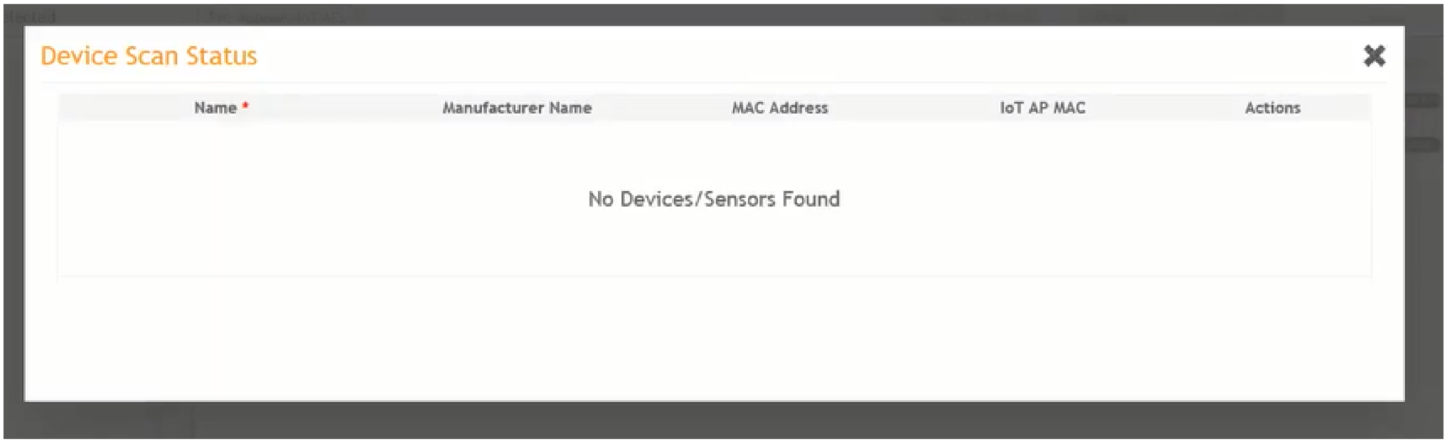
FIGURE 19 IoT Devices Page



□	IoT Device Name	IoT Device MAC	IoT AP MAC	Protocol	Type	Last Seen	Actions	Tags
□	SmartPlug	00:0B:57:FF:FE:1B:3A:66	E8:1D:A8:0D:88:E0	NA	SMART_PLUG	3 minutes ago	Remove Blacklist	All 00:0B:57:FF:FE:1B:3A:66
□	Osram	7C:B0:3E:AA:00:A0:6C:A3	E8:1D:A8:0D:88:E0	NA	LIGHT	3 minutes ago	Remove Blacklist	All Osram 7C:B0:3E:AA:00:A

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 20 Device Discovery Dialog Box



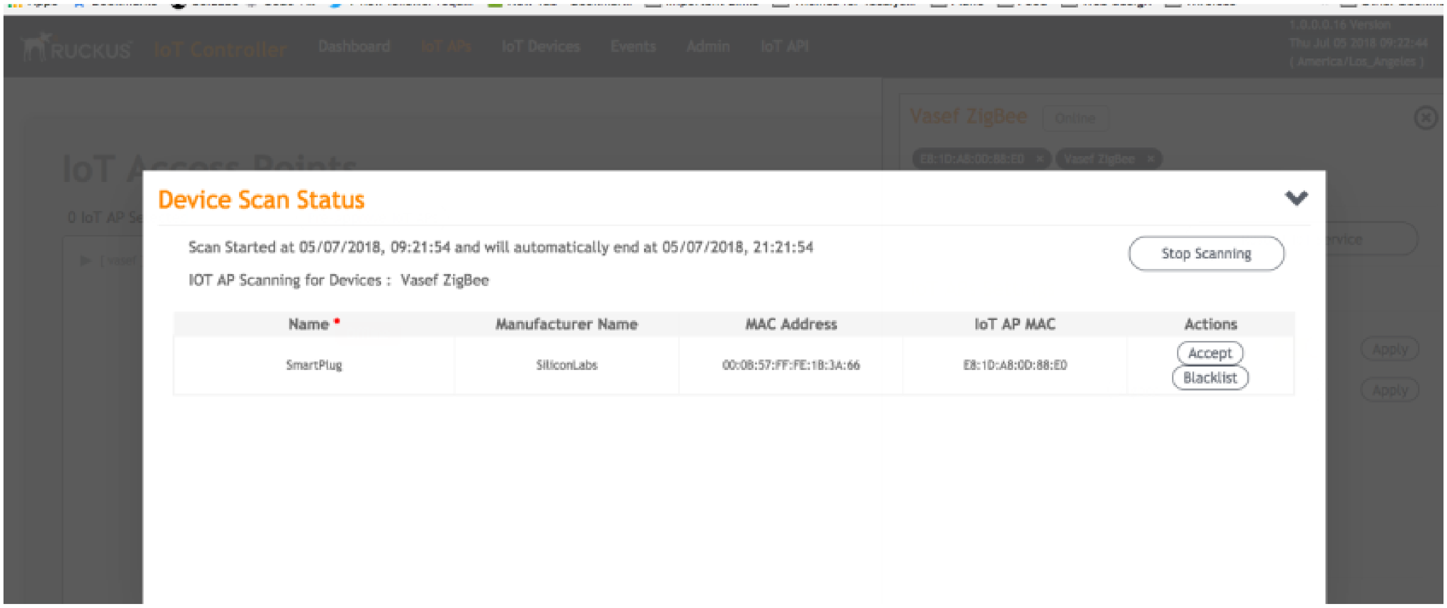
Device Scan Status

Name *	Manufacturer Name	MAC Address	IoT AP MAC	Actions

No Devices/Sensors Found

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 21 Adding Device After Discovery



Device Scan Status

Scan Started at 05/07/2018, 09:21:54 and will automatically end at 05/07/2018, 21:21:54

IOT AP Scanning for Devices : Vasef ZigBee

Name *	Manufacturer Name	MAC Address	IoT AP MAC	Actions
SmartPlug	SiliconLabs	00:08:57:FF:FE:1B:3A:66	E8:1D:A8:0D:88:E0	Accept Blacklist

Managing OSRAM Light Bulbs

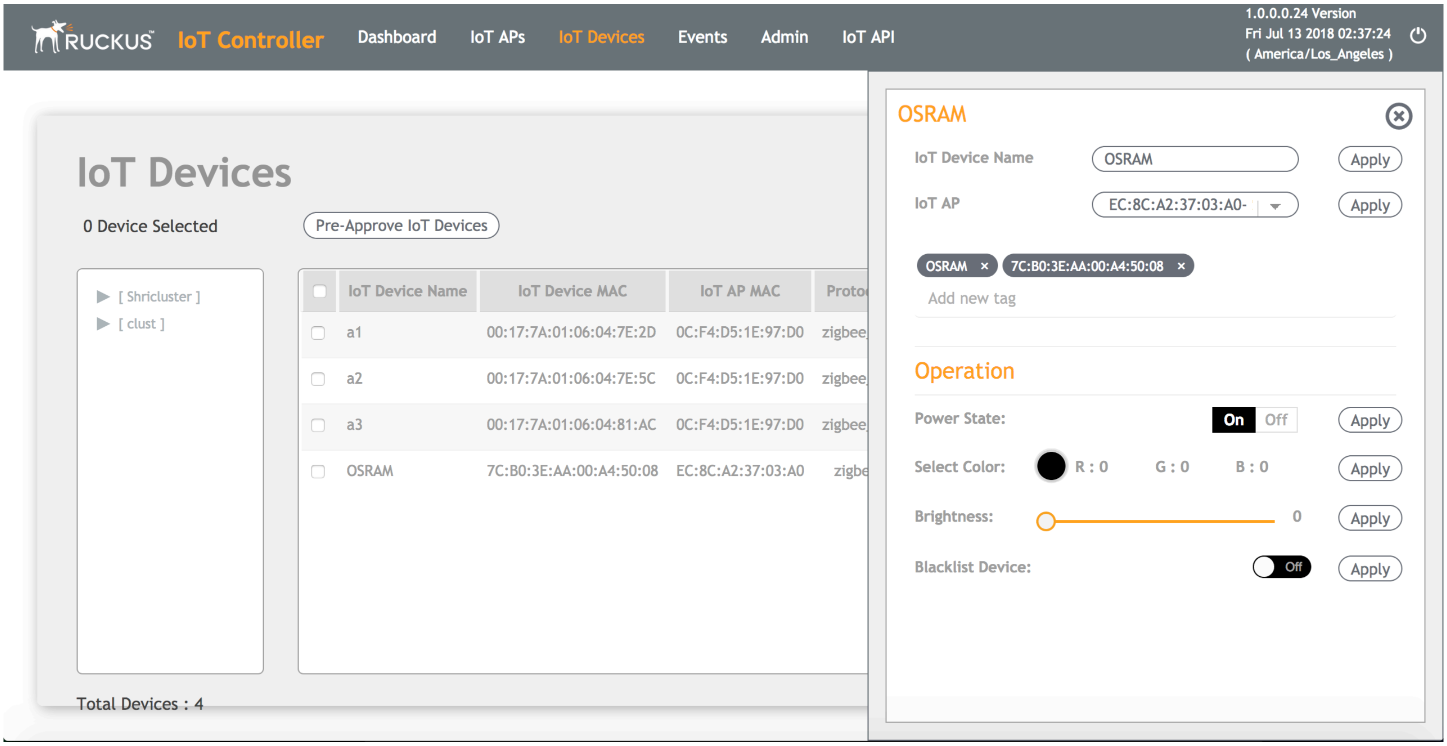
To discover OSRAM bulbs, complete the following operations.

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 for five times.
5. Switch on the power.

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

FIGURE 22 OSRAM Light Bulb



□	IoT Device Name	IoT Device MAC	IoT AP MAC	Proto
□	a1	00:17:7A:01:06:04:7E:2D	0C:F4:D5:1E:97:D0	zigbee
□	a2	00:17:7A:01:06:04:7E:5C	0C:F4:D5:1E:97:D0	zigbee
□	a3	00:17:7A:01:06:04:81:AC	0C:F4:D5:1E:97:D0	zigbee
□	OSRAM	7C:B0:3E:AA:00:A4:50:08	EC:8C:A2:37:03:A0	zigbe

IoT Device Name: OSRAM

IoT AP: EC:8C:A2:37:03:A0-

Tags: OSRAM ×, 7C:B0:3E:AA:00:A4:50:08 ×

Power State: On Off

Select Color: ● R : 0 G : 0 B : 0

Brightness: 0

Blacklist Device: Off

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, as the discovered device type is light bulb.

Managing 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.

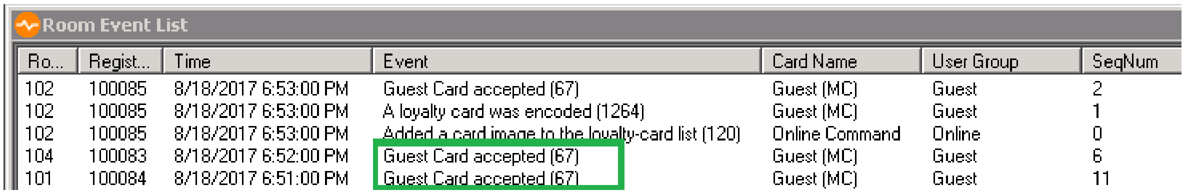
1. Swipe the AA Lock Discover Card across the lock.
2. Ensure that the LED blinks green.
3. Add the lock to the Ruckus IoT Controller (if it is not already pre-approved).

Assa Abloy locks are operated 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 23 Visionline Server Event Log



Room Event List

Ro...	Regist...	Time	Event	Card Name	User Group	SeqNum
102	100085	8/18/2017 6:53:00 PM	Guest Card accepted (67)	Guest (MC)	Guest	2
102	100085	8/18/2017 6:53:00 PM	A loyalty card was encoded (1264)	Guest (MC)	Guest	1
102	100085	8/18/2017 6:53:00 PM	Added a card image to the 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

Plugins

Supporting the Kontakt.io Beacons Plugin

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

Before you begin using the plugin, ensure the following steps are completed.

1. Activate the Kontakt.io Beacon plugin.

   For more information on how to activate a plugin, refer to Activating Plugins on page 18.

   After the plugin is activated, map each IoT AP to a SoftAPID. SoftAPID is a feature of Kontakt.io and the user can get it from the Kontakt.io system. The SoftAPID (for example xyz12) should be mapped to an IoT AP, using the tag feature. Tag value should be kontakt:softapid>, for example, kontakt:xyz12. SoftAPID can be obtained from the cloud Kontakt.io 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.
2. Enter the following configuring 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 vendor/connector URL to send the beacon messages. The URL can be a DNS-resovable, FQDN-based address.

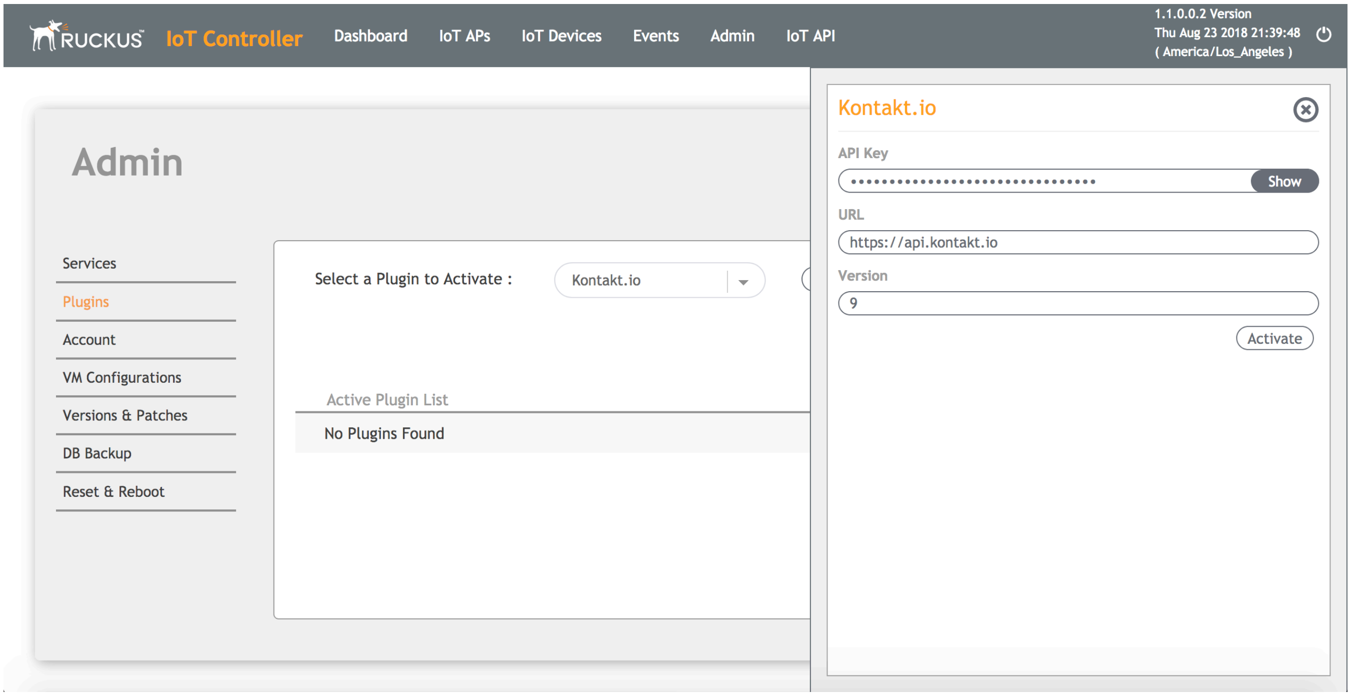
      NOTE
      The plugin supports HTTP and HTTPS modes.

   c) Enter the **Version** number.

      The default version number is 9.

3. Click **Activate**.

FIGURE 24 Configuring Parameters for the Kontakt.io Plugin



Select a Plugin to Activate : Kontakt.io

API Key: ••••••••••••••••••••••••••••••••

URL: https://api.kontakt.io

Version: 9

Supporting the iBeacon Plugin

The Ruckus IoT Controller provides supports 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.

Before you begin using the plugin to send iBeacon BLE packets, ensure the following steps are completed.

1. Activate the iBeacon plugin.

NOTE
For more information on how to activate a plugin, refer to Activating Plugins on page 18.

2. After the 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**.

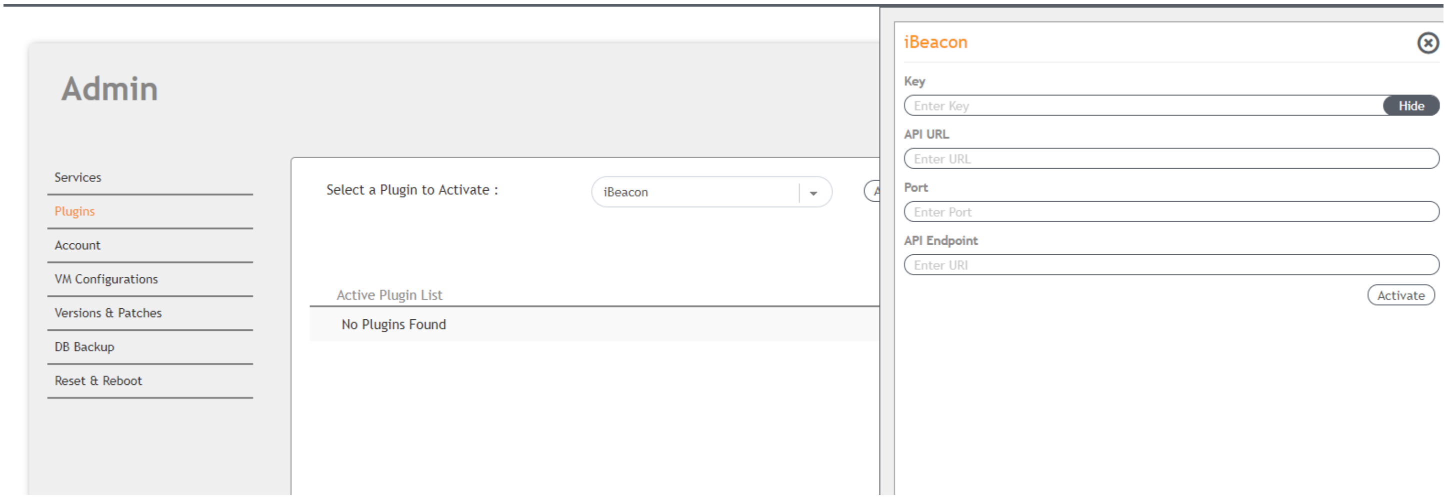
      The Ruckus IoT Controller connects to vendor/connector URL to send the beacon messages. The URL can be a DNS-resovable, FQDN-based address.

      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.
3. Click **Activate**.

FIGURE 25 Configuring Parameters for the iBeacon Plugin



Supporting the Eddystone Plugin

The Ruckus IoT Controller provides supports 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.

Before you begin using the plugin to send Eddystone BLE packets, ensure the following steps are completed.

1. Activate the Eddystone plugin.

   NOTE
   For more information on how to activate a plugin, refer to Activating Plugins on page 18.

2. After the 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**.

      Ruckus IoT Controller connects to 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.

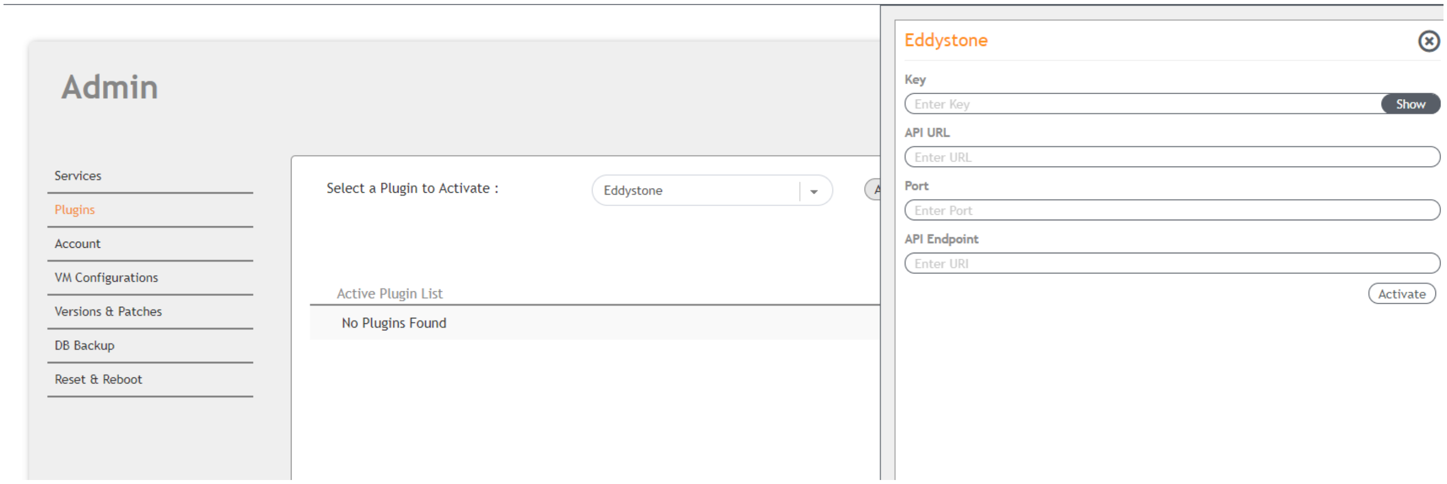
      This is the port number on which the vendor/connector web server is running.

   d) Enter the **API Endpoint**.

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

3. Click **Activate**.

FIGURE 26 Configuring Parameters for the Eddystone Plugin



Events

Viewing Events

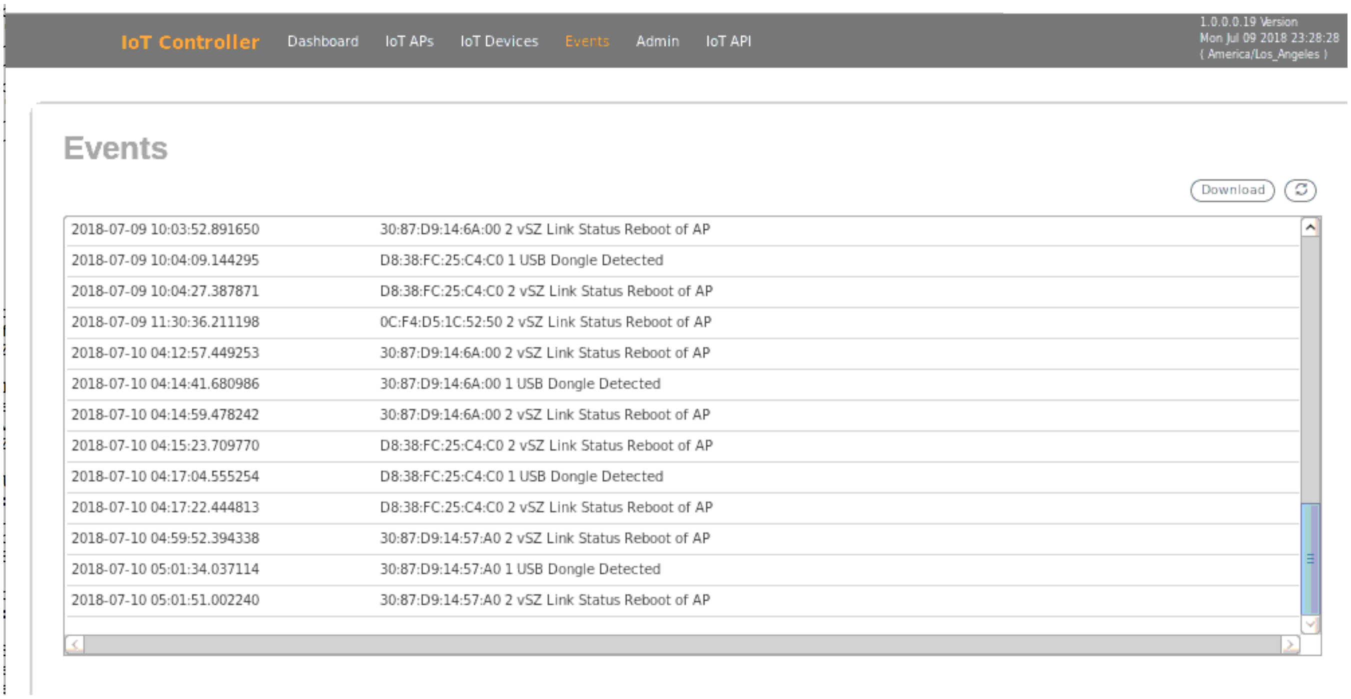
An event is an occurrence or the detection of certain conditions in and around the Ruckus IoT Module. An AP rebooting, detection of a Ruckus IoT Module, module undetection, and module swap are all examples of events.

Complete the following to view events.

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

   The **Events** page is displayed.

   FIGURE 27 Events



```
2018-07-09 10:03:52.891650    30:87:D9:14:6A:00 2 vSZ Link Status Reboot of AP
2018-07-09 10:04:09.144295    D8:38:FC:25:C4:C0 1 USB Dongle Detected
2018-07-09 10:04:27.387871    D8:38:FC:25:C4:C0 2 vSZ Link Status Reboot of AP
2018-07-09 11:30:36.211198    0C:F4:D5:1C:52:50 2 vSZ Link Status Reboot of AP
2018-07-10 04:12:57.449253    30:87:D9:14:6A:00 2 vSZ Link Status Reboot of AP
2018-07-10 04:14:41.680986    30:87:D9:14:6A:00 1 USB Dongle Detected
2018-07-10 04:14:59.478242    30:87:D9:14:6A:00 2 vSZ Link Status Reboot of AP
2018-07-10 04:15:23.709770    D8:38:FC:25:C4:C0 2 vSZ Link Status Reboot of AP
2018-07-10 04:17:04.555254    D8:38:FC:25:C4:C0 1 USB Dongle Detected
2018-07-10 04:17:22.444813    D8:38:FC:25:C4:C0 2 vSZ Link Status Reboot of AP
2018-07-10 04:59:52.394338    30:87:D9:14:57:A0 2 vSZ Link Status Reboot of AP
2018-07-10 05:01:34.037114    30:87:D9:14:57:A0 1 USB Dongle Detected
2018-07-10 05:01:51.002240    30:87:D9:14:57:A0 2 vSZ Link Status Reboot of AP
```

2. Click **Download**.

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

RUCKUS™
an ARRIS company

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