CONFIGURATION GUIDE

Ruckus IoT Controller Configuration Guide, 1.5.0.1

Supporting IoT Controller Release 1.5.0.1

Part Number: 800-72650-001 Rev A
Publication Date: April 2020

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, COMMSCOPE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

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

Trademarks

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

Contents

Preface

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 Safety Warnings

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

NOTE

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

ATTENTION

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

CAUTION

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

DANGER

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

Command Syntax Conventions

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

Convention	Description
bold text	Identifies command names, keywords, and command options.

Convention	Description
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@commscope.com.

When contacting us, include the following information:

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

For example:

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

RUCKUS Product Documentation Resources

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

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

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

Online Training Resources

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

Contacting RUCKUS Customer Services and Support

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

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

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

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

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

What's New in This Document

TABLE 2 Summary of New Features in Ruckus IoT Controller Release 1.5

Feature	Description	Location
Soter Plugin	Information on how to activate, deactivate, and update a Soter plugin.	Refer to Activating and Editing the Soter Plugin on page 53.
Telkonet Plugin	Information on how to activate, deactivate, and update a Telkonet plugin.	Refer to Activating and Editing the Telkonet Plugin on page 51.
License	The Ruckus IoT Controller is now a licensed product. Information on how to upload licenses.	Refer to Uploading the Ruckus IoT Controller License on page 59.
Rules Engine	The Rules Engine provides a provision to write custom rules using the Node-RED tool.	Refer to Rules Engine Overview on page 80, Configuring Rules on page 80.
LoRaWAN	The Ruckus IoT Controller is now integrated with a LoRa Network Server (LNS) that communicates with LoRa devices and routers. Information on how to configure LoRa devices and routers.	Refer to LoRaWAN Overview on page 83, Configuring LoRa Devices on page 85, Configuring LoRaWAN Routers on page 87.

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 3 Supported Web Browser Versions

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

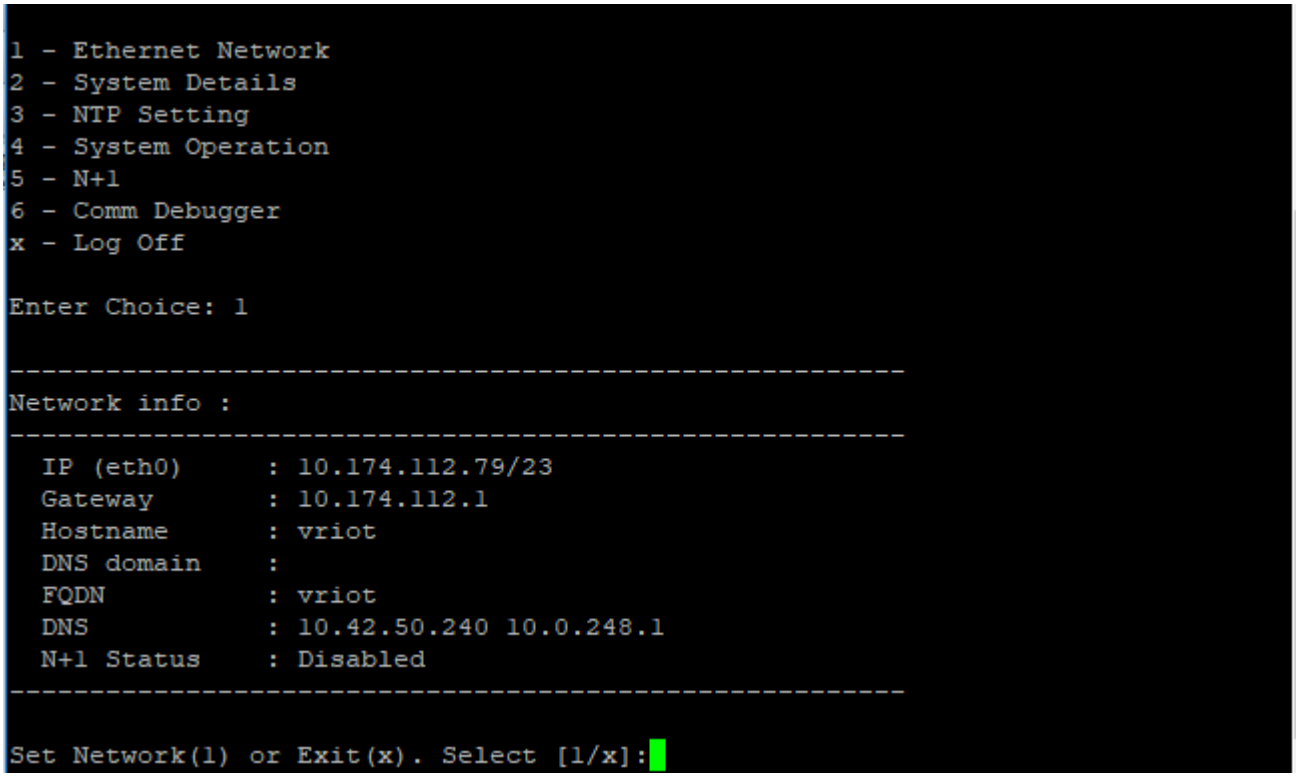
Logging In to Ruckus IoT Controller

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

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

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

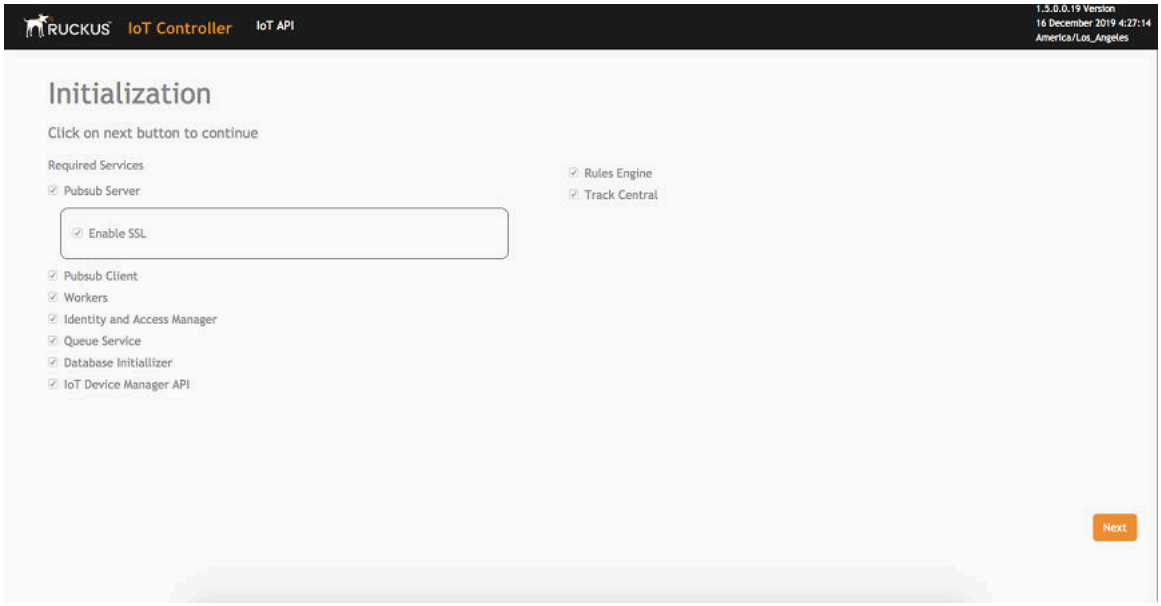
FIGURE 1 Ruckus IoT Controller Main Menu



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:

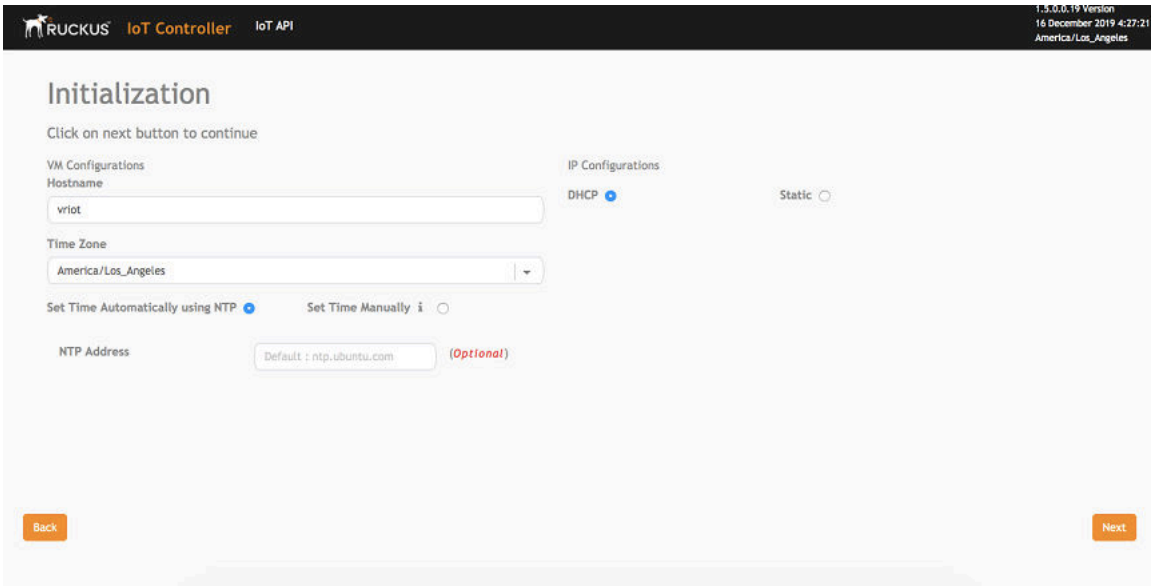
   - Pubsub Server
   - Pubsub Client
   - Workers
   - Identity and Access Manager
   - Queue Service
   - Database Initializer
   - IoT Device Manager API
   - Rules Engine
   - Track Central

   Pubsub Server works in SSL mode.

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

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

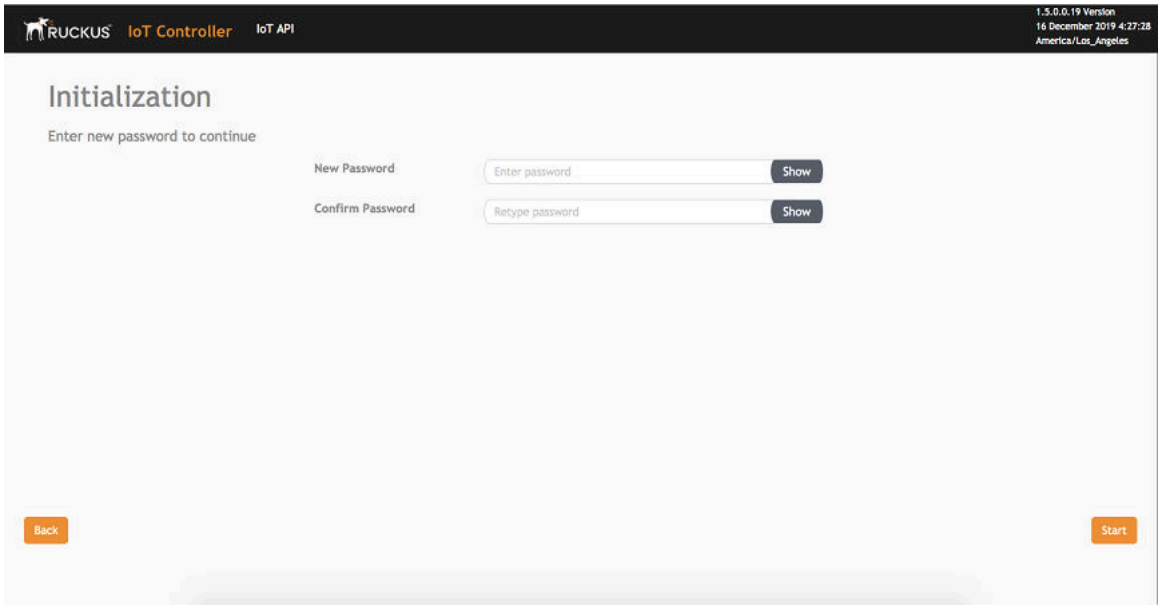
   FIGURE 3 Intialization Page After Accepting Services



NOTE
The figure shows a DHCP configuration.

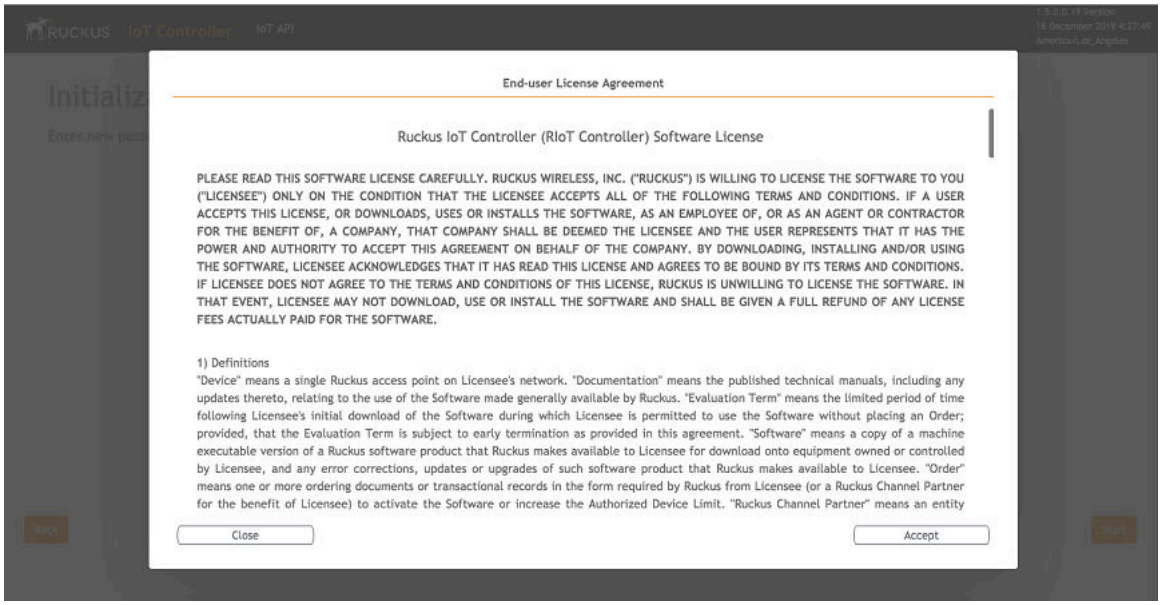
5. Enter the Ruckus IoT Controller password in the **New Password** field. Re-enter the password in the **Confirm Password** field. The password must be a least eight characters in length and contain one uppercase letter, one lowercase letter, one digit, and one special character.

FIGURE 4 Confirming the Password



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

FIGURE 5 End-user License Agreement



Getting to Know the Dashboard

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

FIGURE 6 Ruckus IoT Controller Dashboard

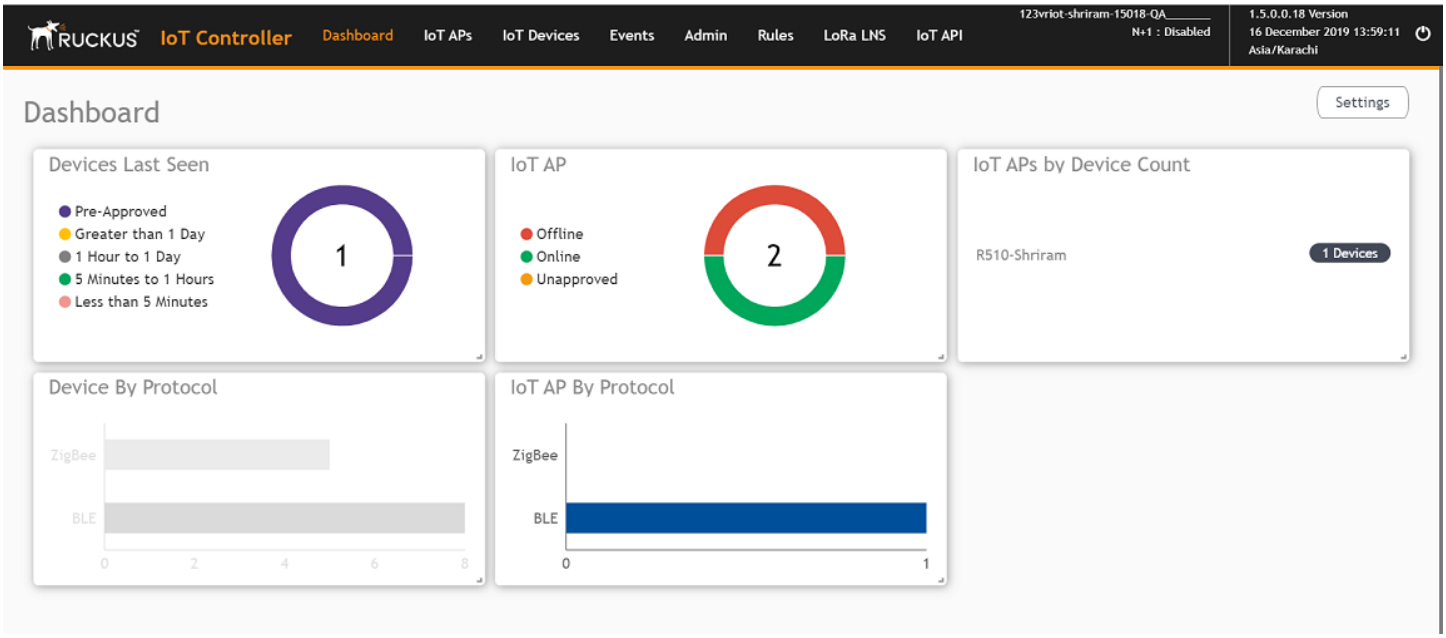
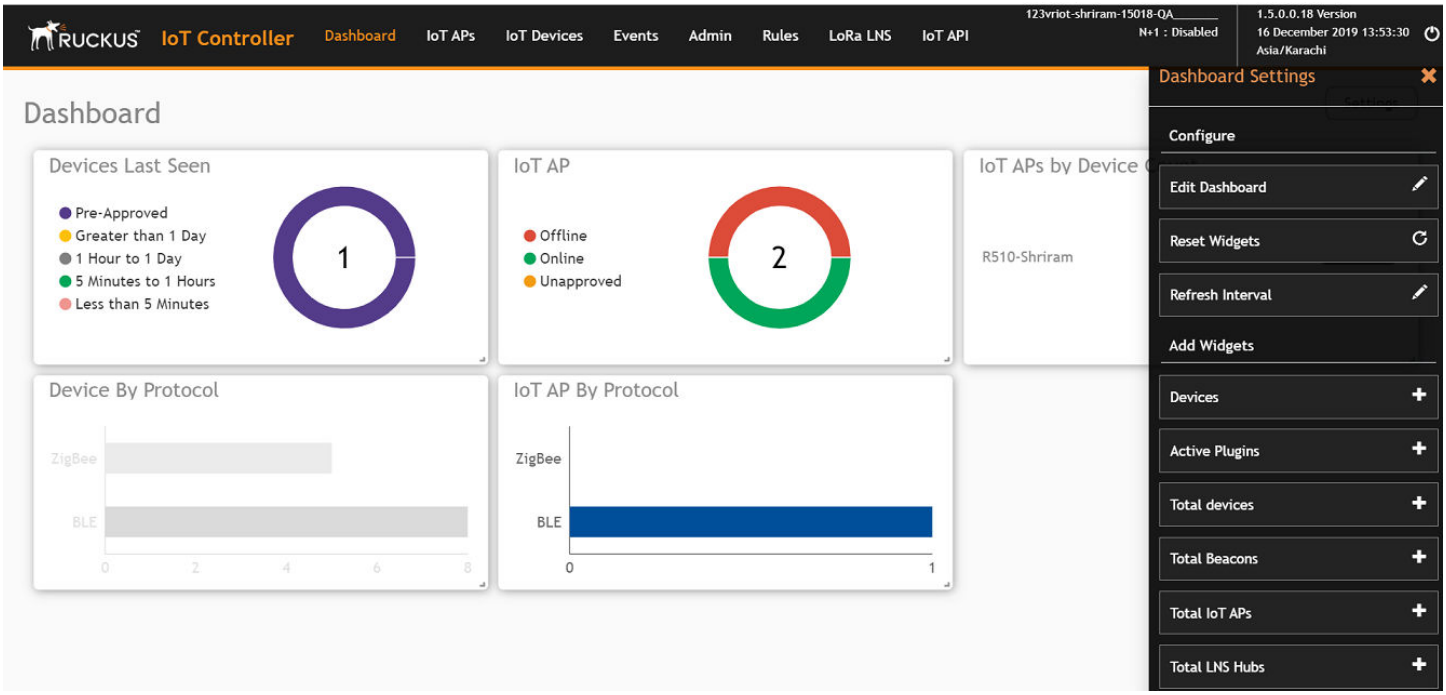


TABLE 4 Dashboard Elements

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

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

FIGURE 7 Dashboard Settings



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

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

> **NOTE**
> The default interval is 30 seconds.

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

Configuring N+1

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

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

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

Configuring Static Addresses for Master and Slave

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

- From the Ruckus IoT Controller main menu, select **Admin** > **VM Configurations**.
- Set the static address of the master and slave on the **Initialization** page. Refer to Logging In to Ruckus IoT Controller on page 11.

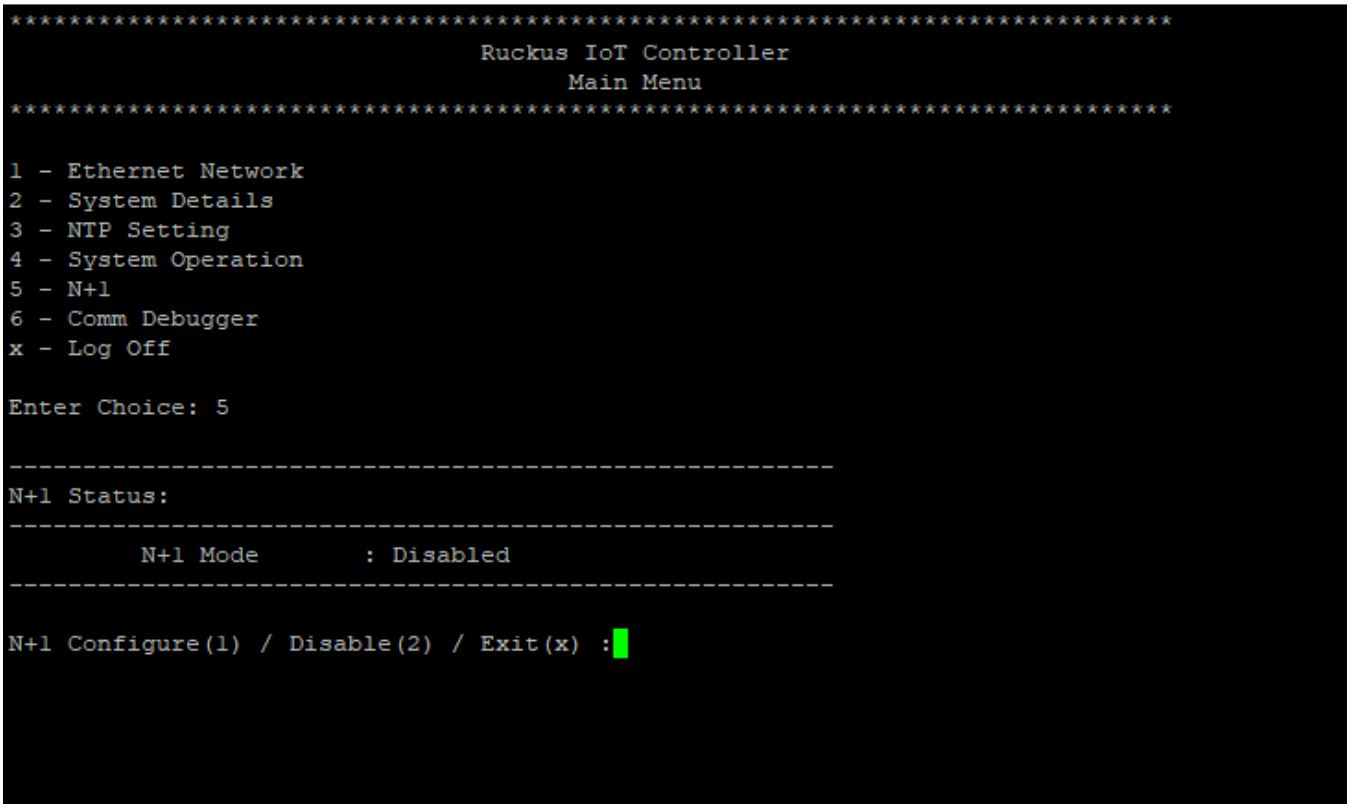
Configuring the N+1 Feature

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

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

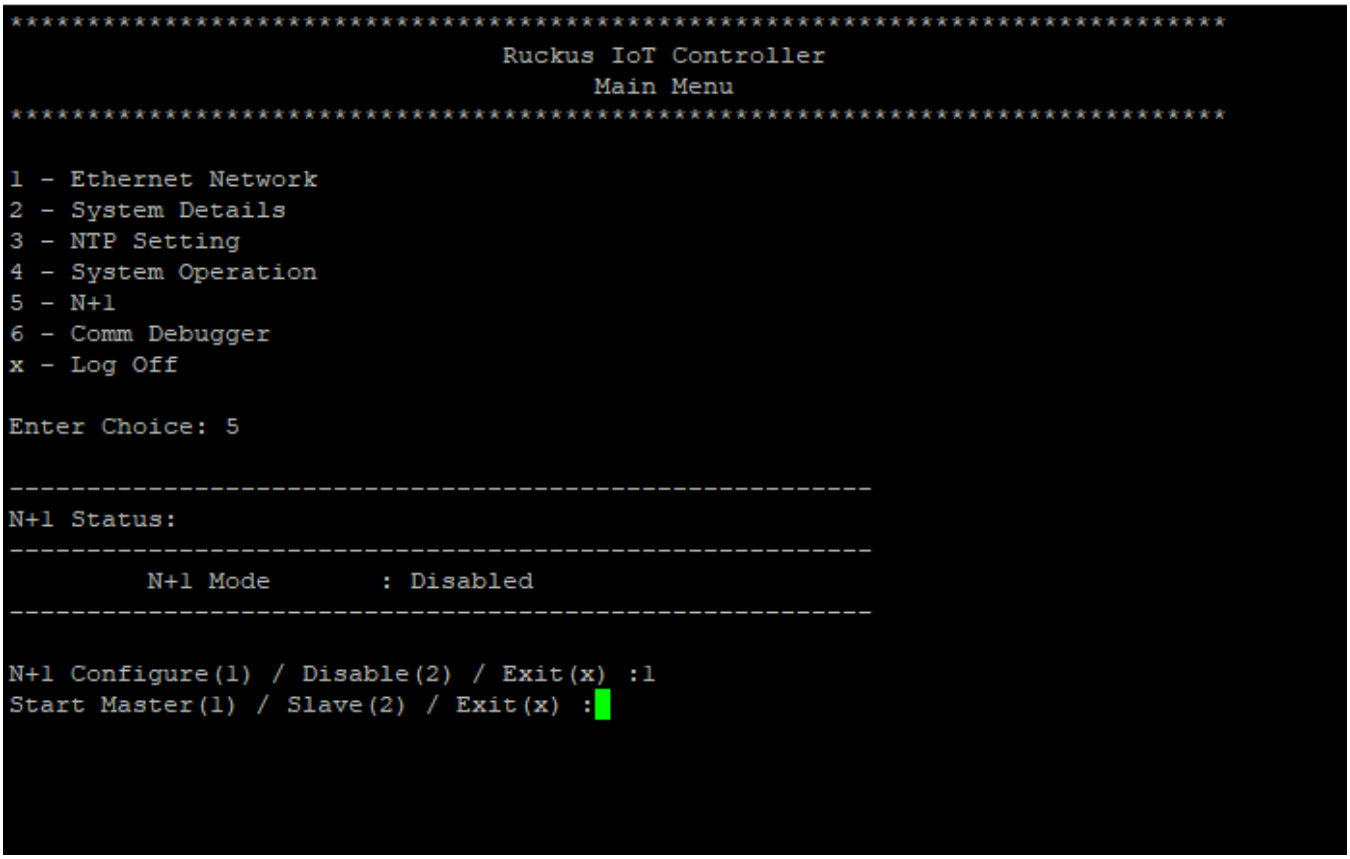
2. Enter **5** in the **Enter Choice** field.

FIGURE 8 Ruckus IoT Controller Main Menu



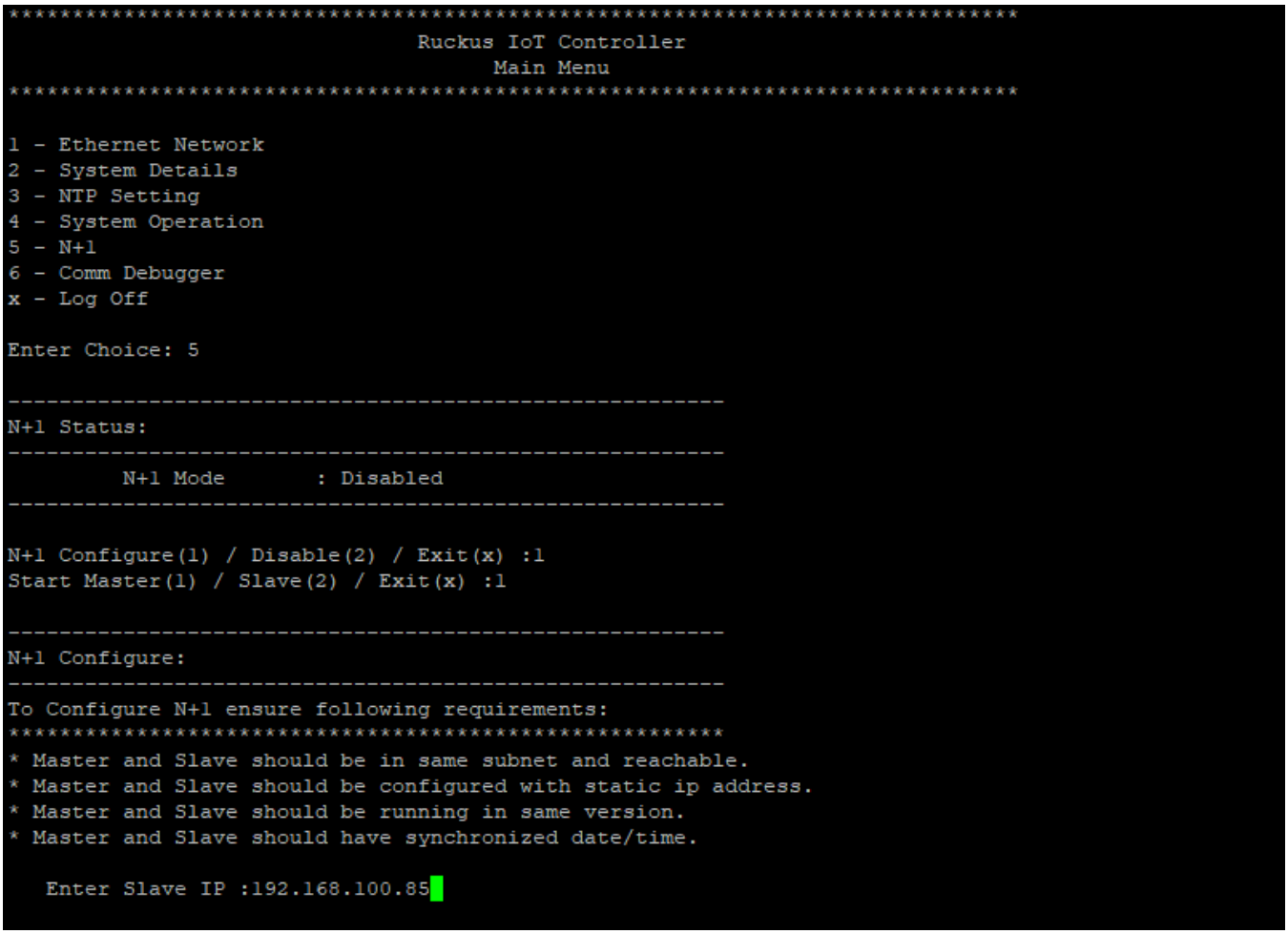
3. Enter **1** to continue the configuration.

FIGURE 9 Continuing the Configuration



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

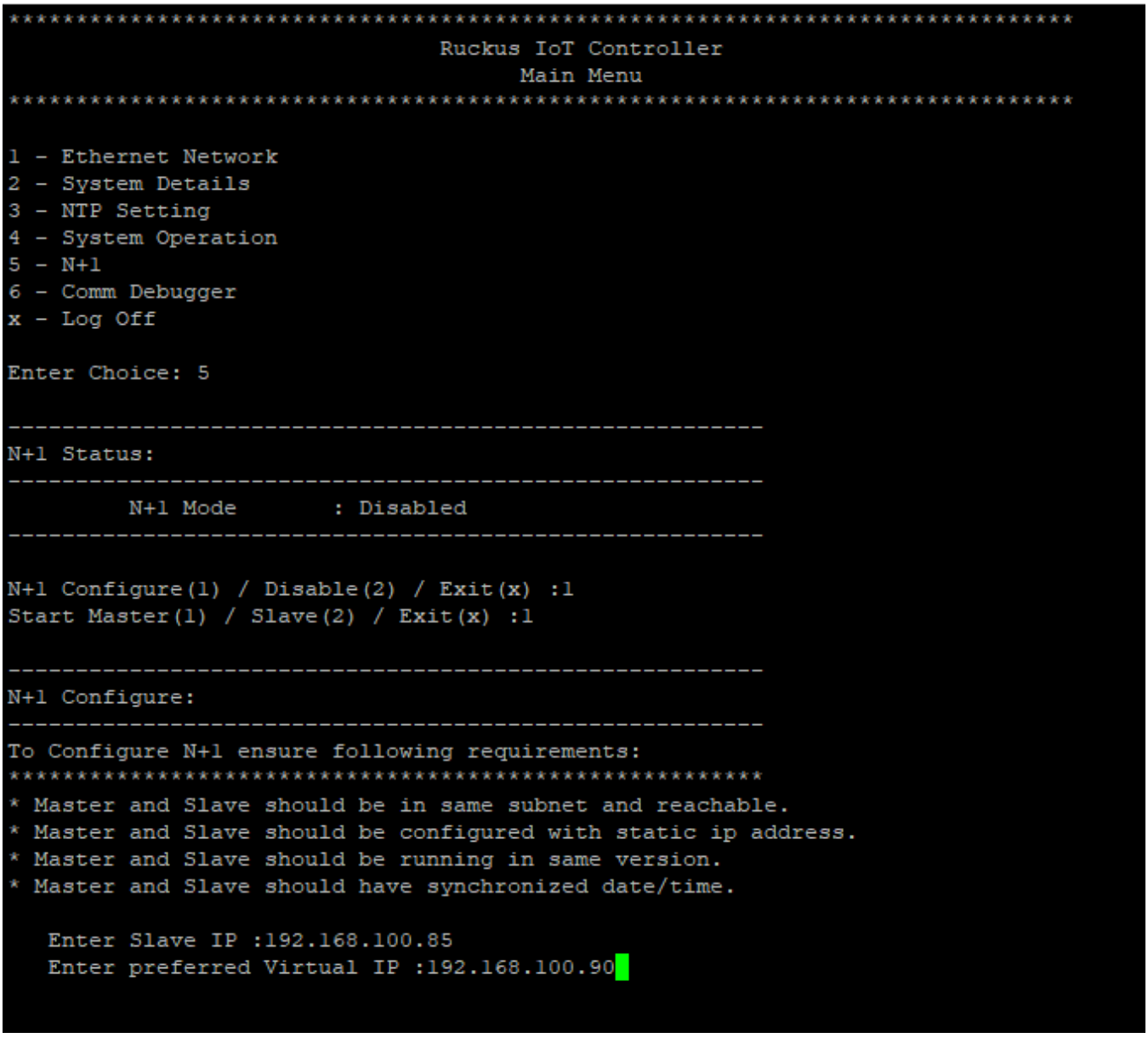
FIGURE 10 Configuring the Master



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

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

FIGURE 11 Entering the Preferred Virtual IP Address



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

FIGURE 12 Completing the Master Configuration

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

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

Enter Choice: 5

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

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

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

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

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

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

FIGURE 13 Continuing with the Slave Configuration

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

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

Enter Choice: 5

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

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

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

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

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

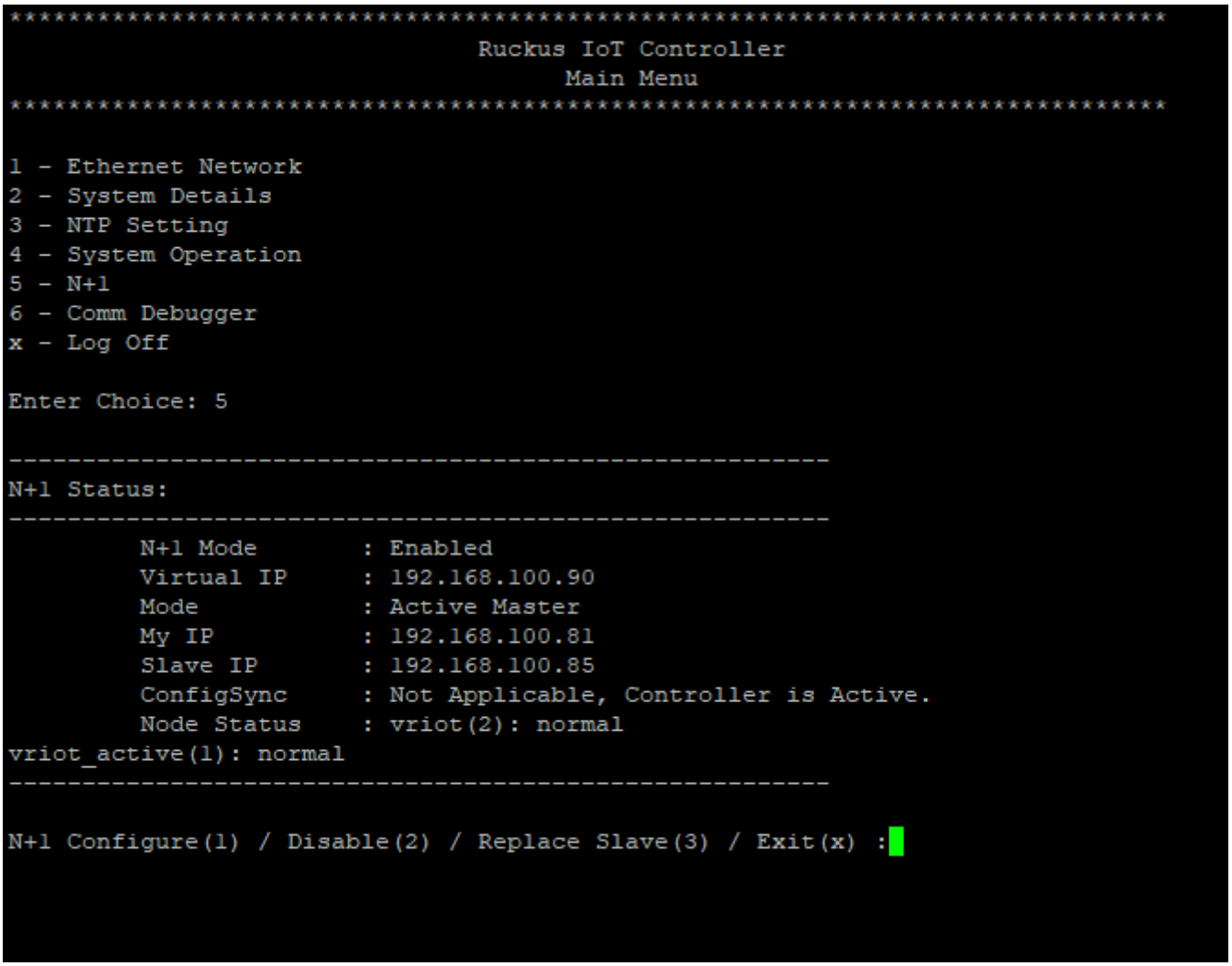
FIGURE 14 N+1 Configuration Completed

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

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

Enter Choice: 5

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

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

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

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

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

You have configured N+1 successfully.

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

FIGURE 15 Verifying the IP Address of the Active Master



8. To replace the slave , enter **3**.

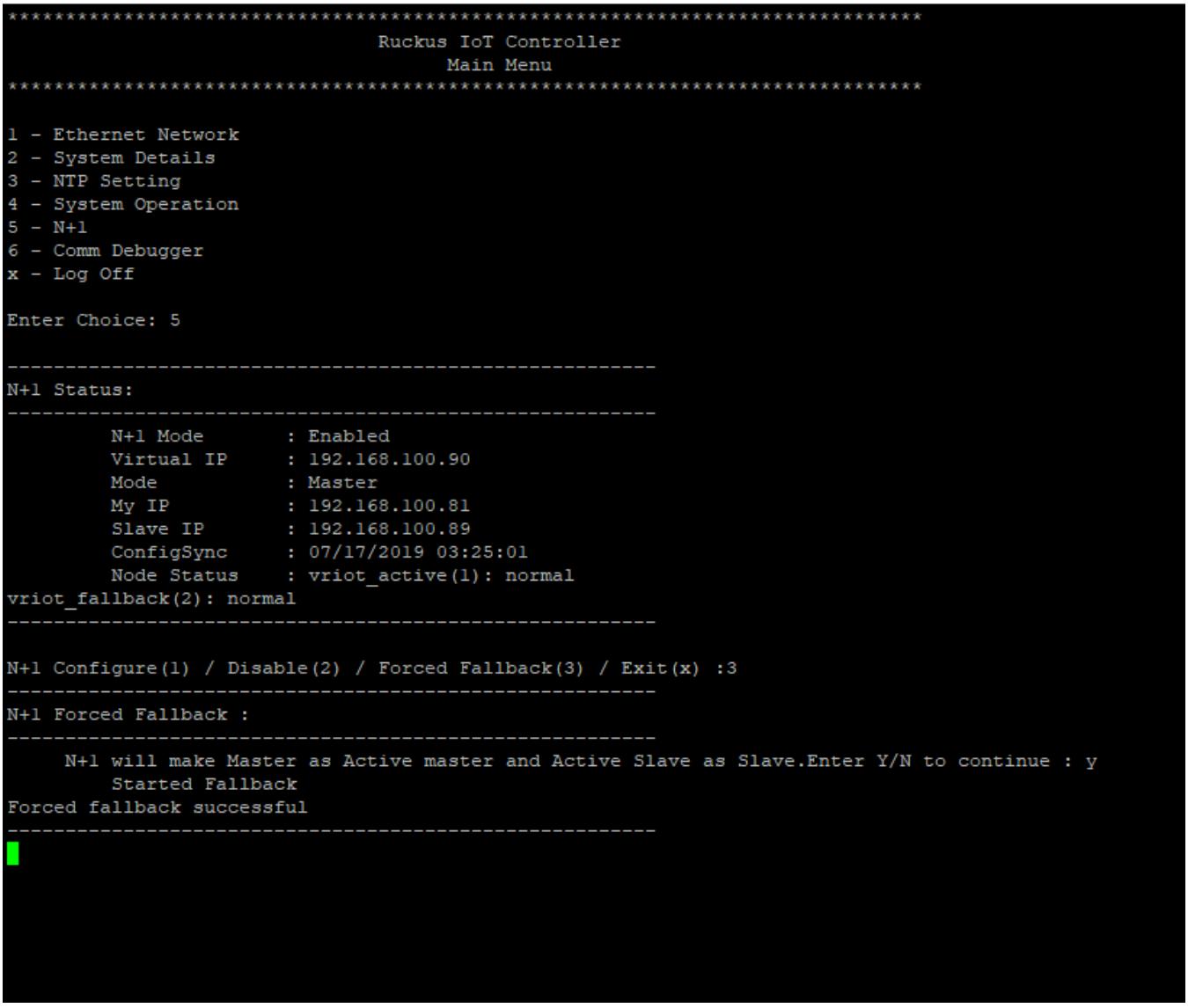
FIGURE 16 Replacing the Slave IP Address

FIGURE 17 Successful Completion of Replacing the Node

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

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

Enter Choice: 5

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

N+1 Configure(1) / Disable(2) / Replace Slave(3) / Exit(x) :3
-------------------------------------------------------
N+1 Replace :
-------------------------------------------------------
   Enter Slave IP to replace:192.168.100.89
Deleted nodes
        Start replacing slave
        Slave configuration started..
Replace node taking more time to start services
Replacing node completed
-------------------------------------------------------
```

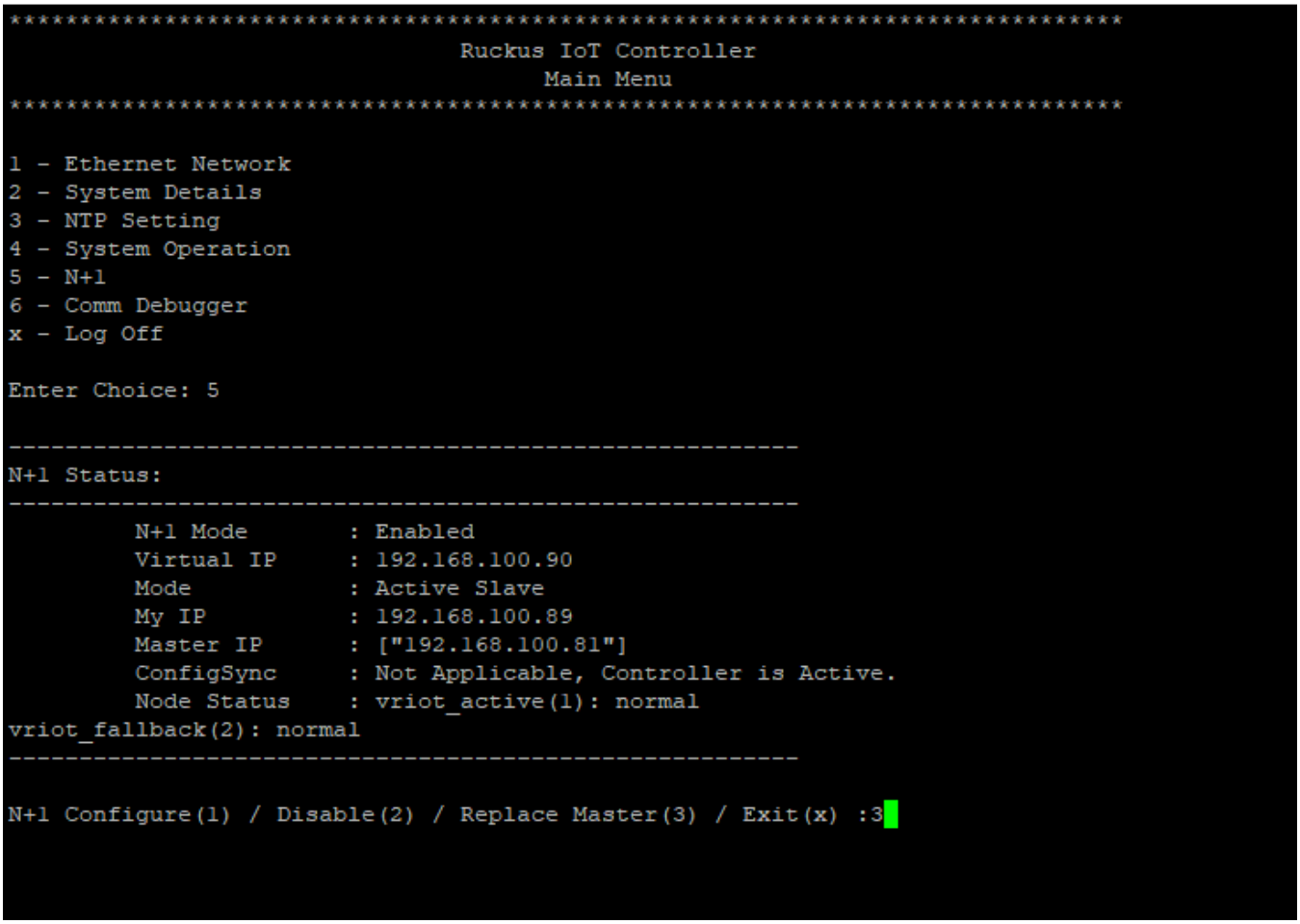
9. To enable Forced Fallback, enter **3** and **y** to continue the configuration.

FIGURE 18 Configuring Forced Fallback



10. To replace the master, enter **3**.

FIGURE 19 Replacing the Master



11. Enter the IP address of the master.

FIGURE 20 Continuing with Replacing the Master

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

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

Enter Choice: 5

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

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

Replacing the master has been successfully completed.

FIGURE 21 Completion of Replacing the Master

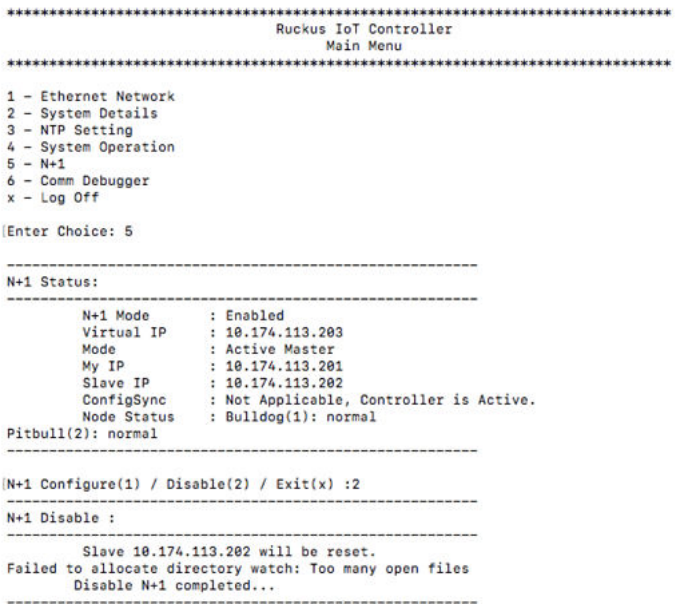
```
*******************************************************************************************
                                Ruckus IoT Controller
                                      Main Menu
*******************************************************************************************

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

Enter Choice: 5

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

N+1 Configure(1) / Disable(2) / Replace Master(3) / Exit(x) :3
-----------------------------------------------------
N+1 Replace :
-----------------------------------------------------
   Enter Master IP to replace:192.168.100.89
Deleted nodes
        Start replacing master
        Slave configuration started..
Slave start failed
Replacing node completed
-----------------------------------------------------
```

Disabling N+1

Complete the following steps to disable N+1 configuration.

1. Log in to the console of the Master IP.
2. Enter **5** in the **Enter Choice** field.

FIGURE 22 Disabling the N+1 Configuration



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

NOTE

Once the N+1 configuration is disabled from the active master, the slave will automatically reset.

Managing IoT Controller System Configuration

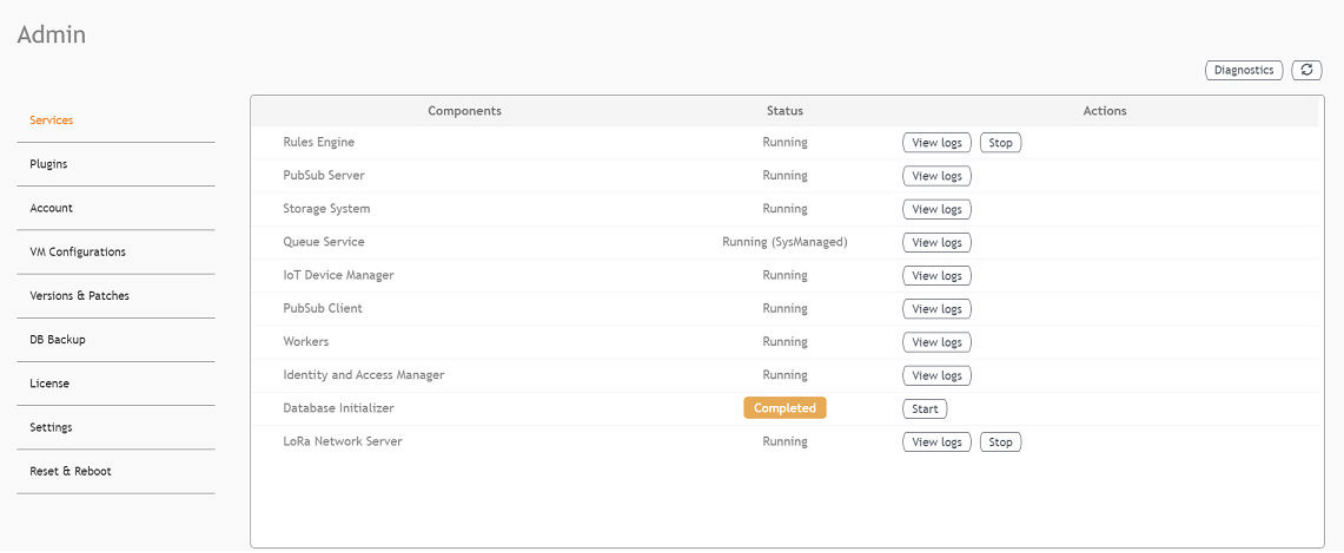
Managing Services

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

Complete the following steps to restart or manage the services.

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

FIGURE 23 Services



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, Eddystone, Beacon as a Service, Controller Data Stream, Telkonet, and Soter.

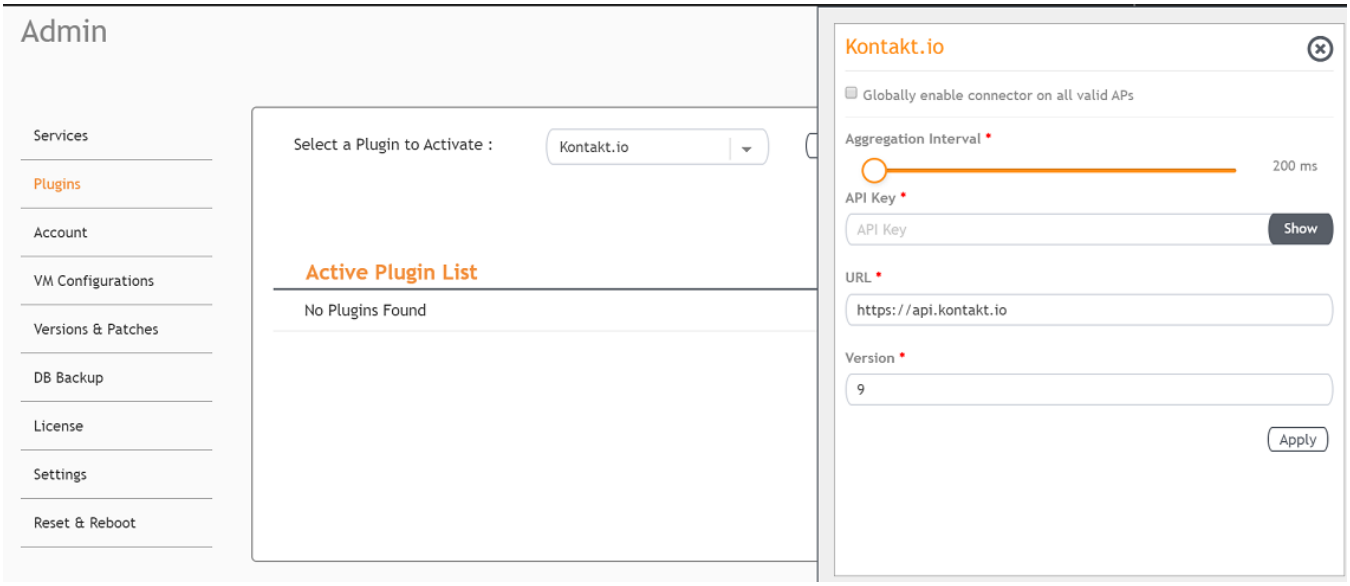
Activating and Editing the Kontakt.io Beacons Plugin

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

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

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

FIGURE 24 Activating the Kontakt.io Plugin



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

      NOTE
      If **Globally enable connector on all valid APs** is not selected, you can activate the plugin for each AP by adding a tag. Refer to Adding Tags to an AP on page 71 for more information.

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

      The Ruckus IoT Controller posts the beacon messages using the API Key provided. The Vendor application is responsible for authenticating the API Keys.
   d) Enter the API URL.

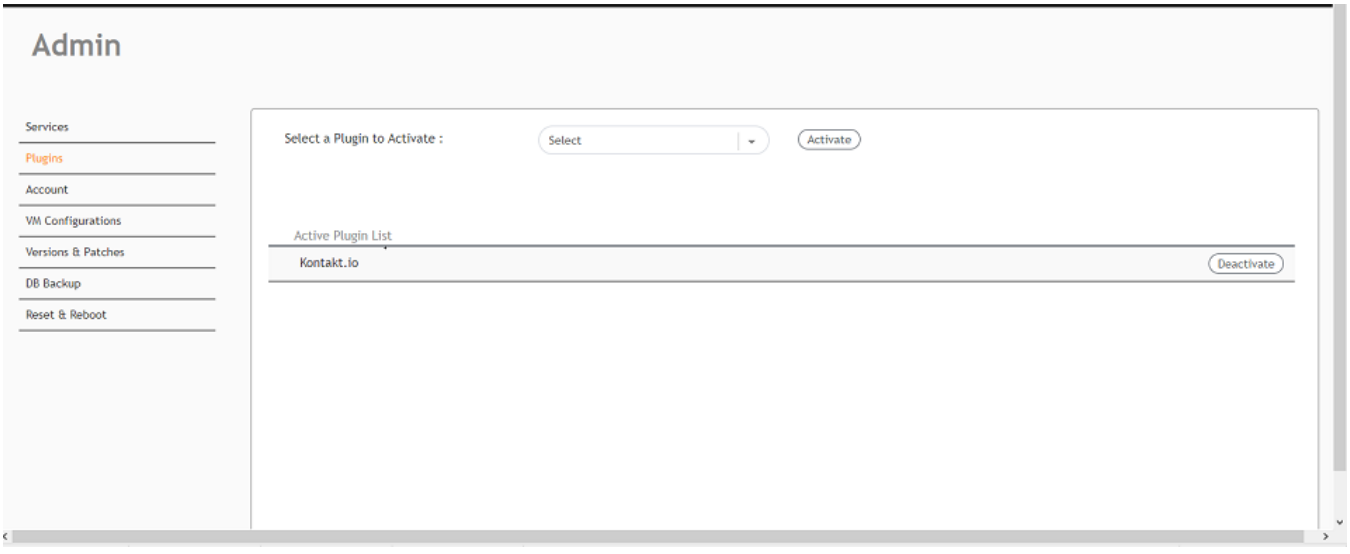
      The Ruckus IoT Controller connects to the vendor/connector URL to send the beacon messages. The URL can be a DNS-resolvable, FQDN-based address.

      NOTE
      The plugin supports HTTP and HTTPS modes.
   e) Enter the Version number.

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

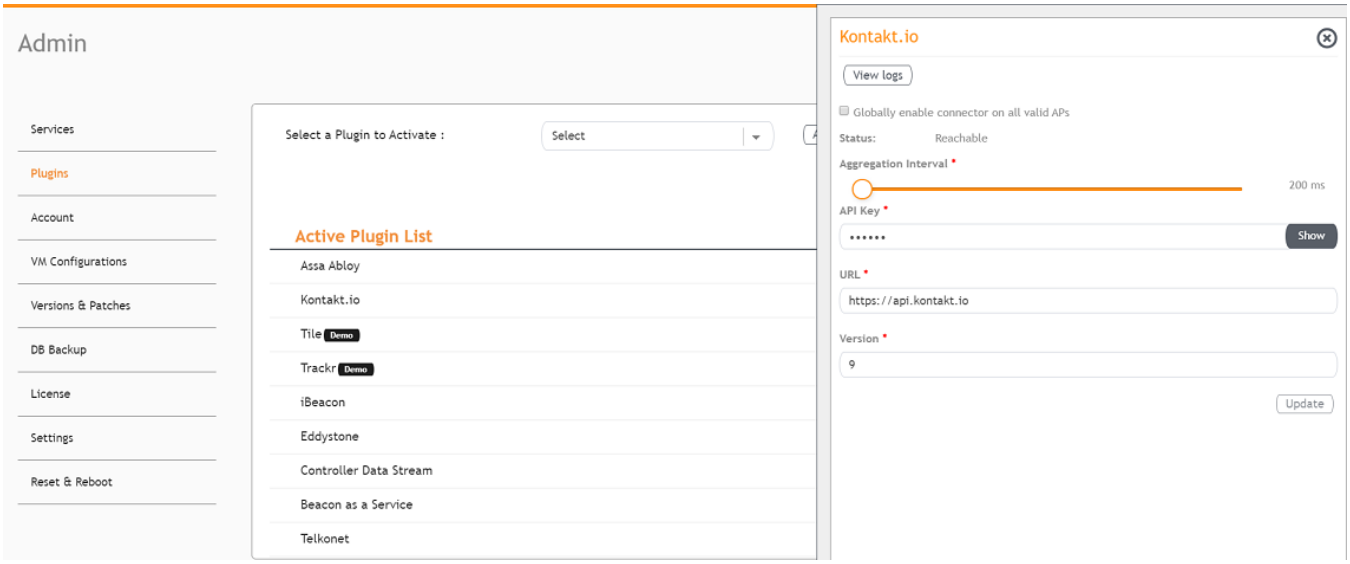
   The Kontakt.io plugin is added in the **Active Plugin List**.
6. To deactivate the Kontakt.io plugin, select it and click **Deactivate**.

FIGURE 25 Deactivating the Kontakt.io Plugin



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

FIGURE 26 Updating the Configuration Parameters



Activating and Editing the Eddystone Plugin

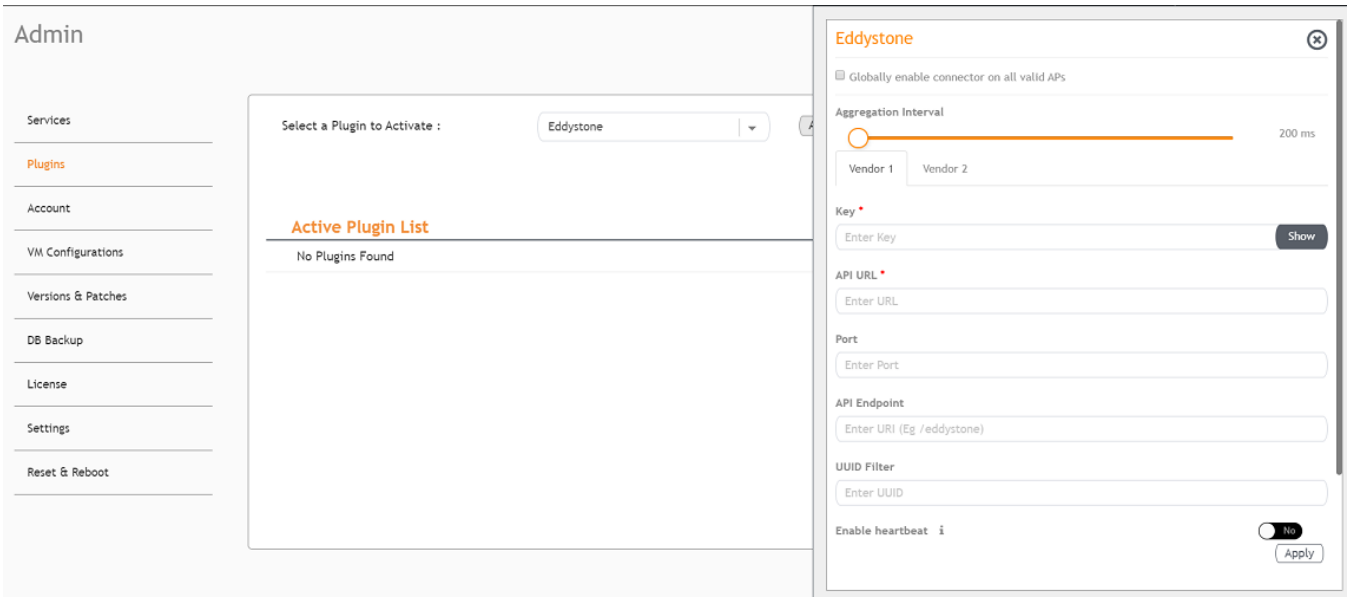
The Ruckus IoT Controller provides support for the Bluetooth Low Energy (BLE) Eddystone plugin. The Ruckus IoT Controller reads the packet from IoT AP, and routes the packets to the BLE beacon vendor cloud services.

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 27 Activating the Eddystone Plugin



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

      NOTE
      If **Globally enable connector on all valid APs** is not selected, you can activate the plugin for each AP by adding a tag. Refer to Adding Tags to an AP on page 71 for more information.

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

      The Ruckus IoT Controller posts the beacon messages using the Key provided. The Vendor application is responsible for authenticating the Keys.
   d) Enter the API URL.

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

      NOTE
      The plugin supports HTTP and HTTPS modes.
   e) Enter the Port number.

      This is the port number on which the vendor/connector web server is running.
   f) Enter the API Endpoint.

      This is the API route where the BLE beacon vendor cloud services receive the beacon payload.
   g) Enter the UUID Filter.

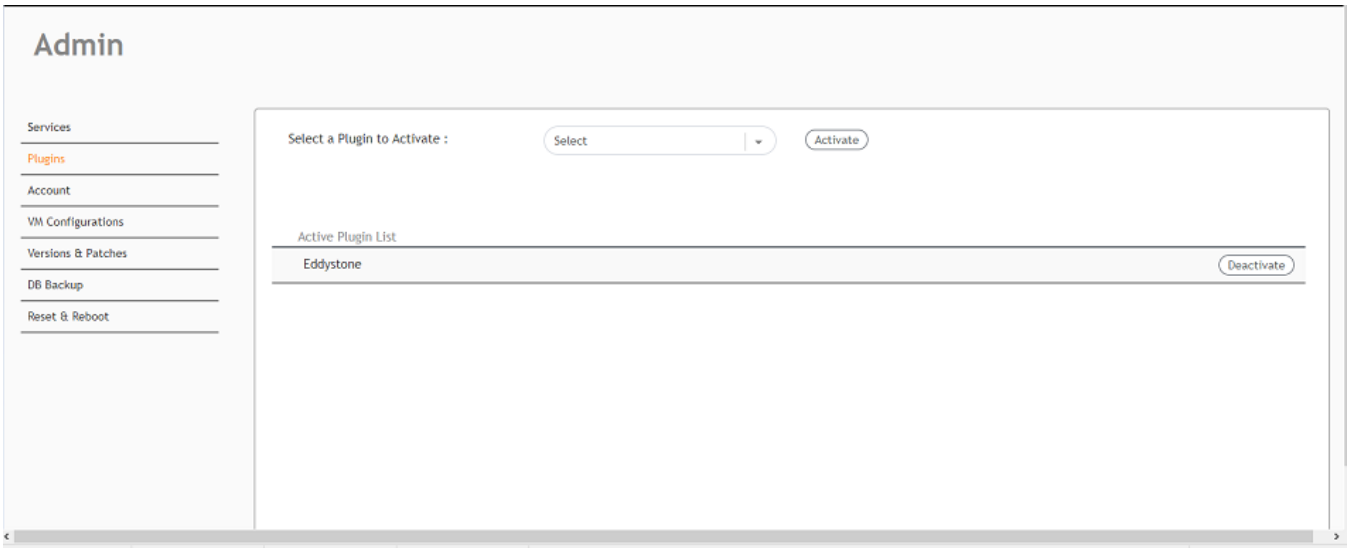
      The filter allows only the BLE ADV packets with the specified UUID to be passed on to the vendor application.
   h) Enable heartbeat.

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

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

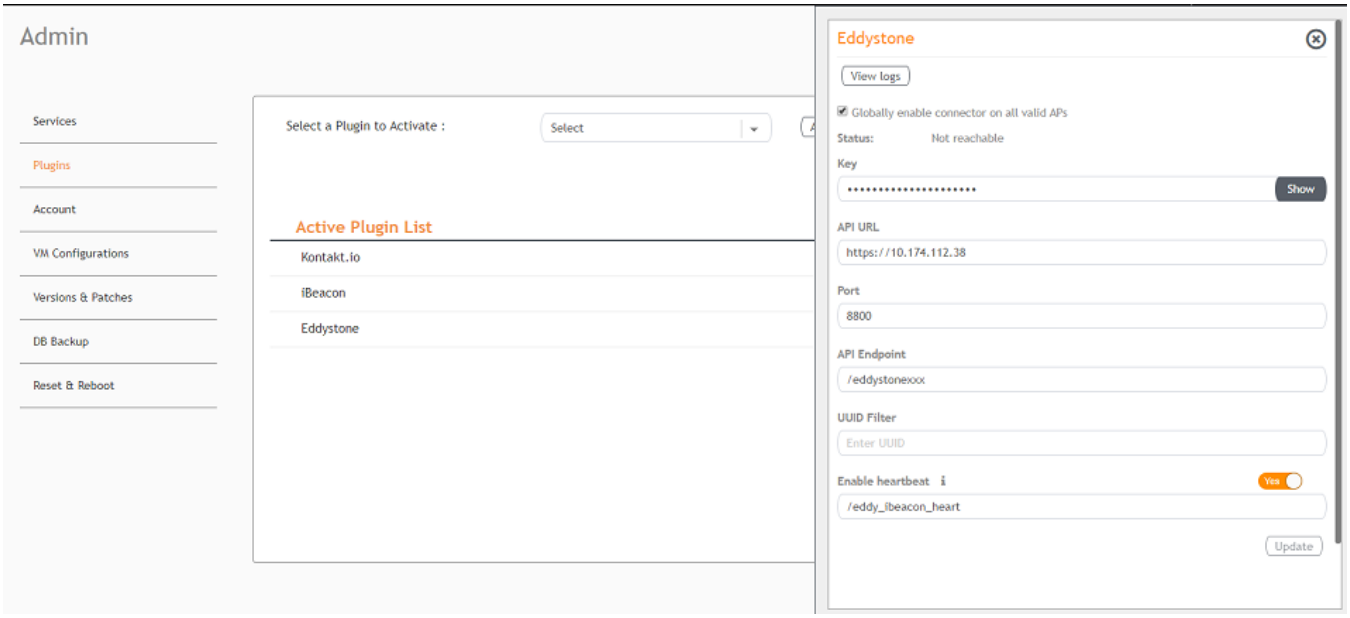
6. To deactivate the Eddystone plugin, select it and click **Deactivate**.

FIGURE 28 Deactivating the Eddystone Plugin



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

FIGURE 29 Updating the Configuration Parameters



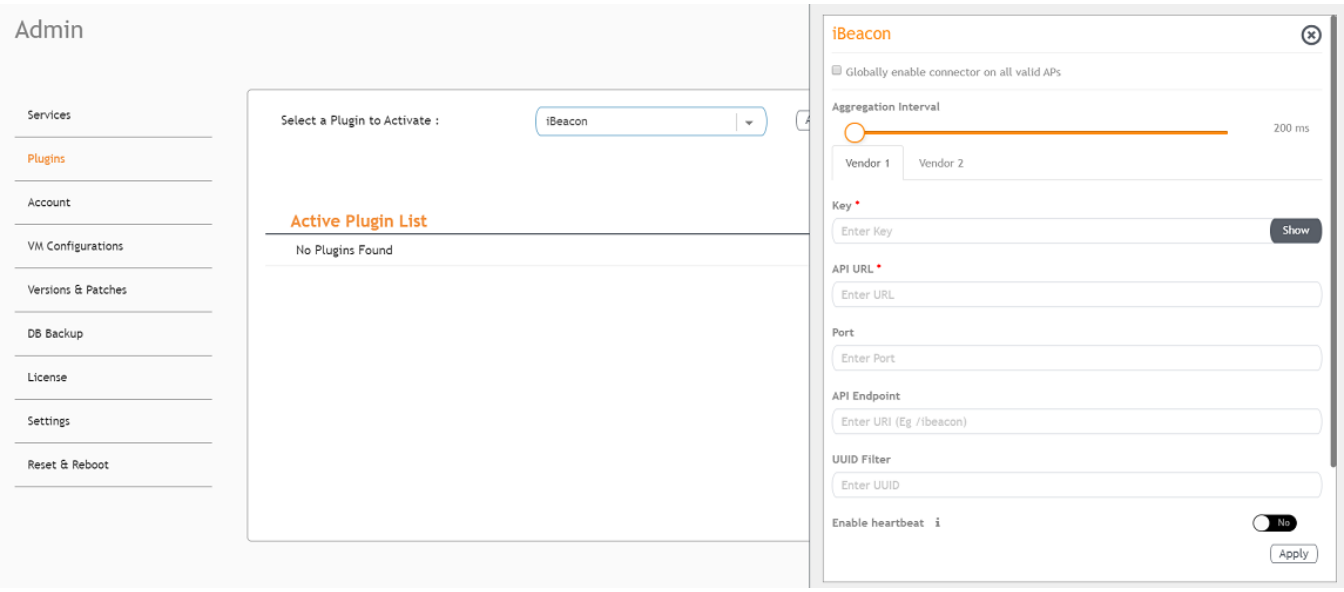
Activating and Editing the iBeacon Plugin

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

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

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

FIGURE 30 Activating the iBeacon Plugin



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

      NOTE
      If **Globally enable connector on all valid APs** is not selected, you can activate the plugin for each AP by adding a tag. Refer toAdding Tags to an AP on page 71 for more information.

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

      The Ruckus IoT Controller posts the beacon messages using the Key provided. The Vendor application is responsible for authenticating the Keys.
   d) Enter the API URL.

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

      NOTE
      The plugin supports HTTP and HTTPS modes.
   e) Enter the Port number.

      This is the port number on which the vendor/connector web server is running.
   f) Enter the API Endpoint.

      This is the API route where the BLE beacon vendor cloud services receive the beacon payload.
   g) Enter the UUID Filter.

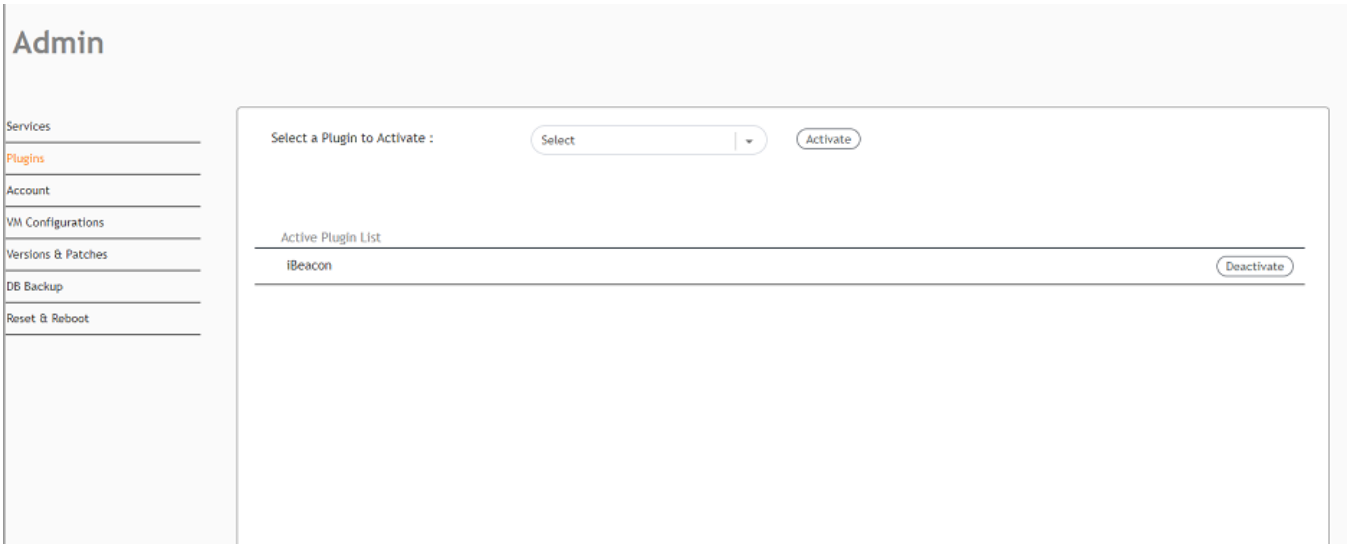
      The filter allows only the BLE ADV packets with the specified UUID to be passed on to the vendor application.
   h) Enable heartbeat.

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

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

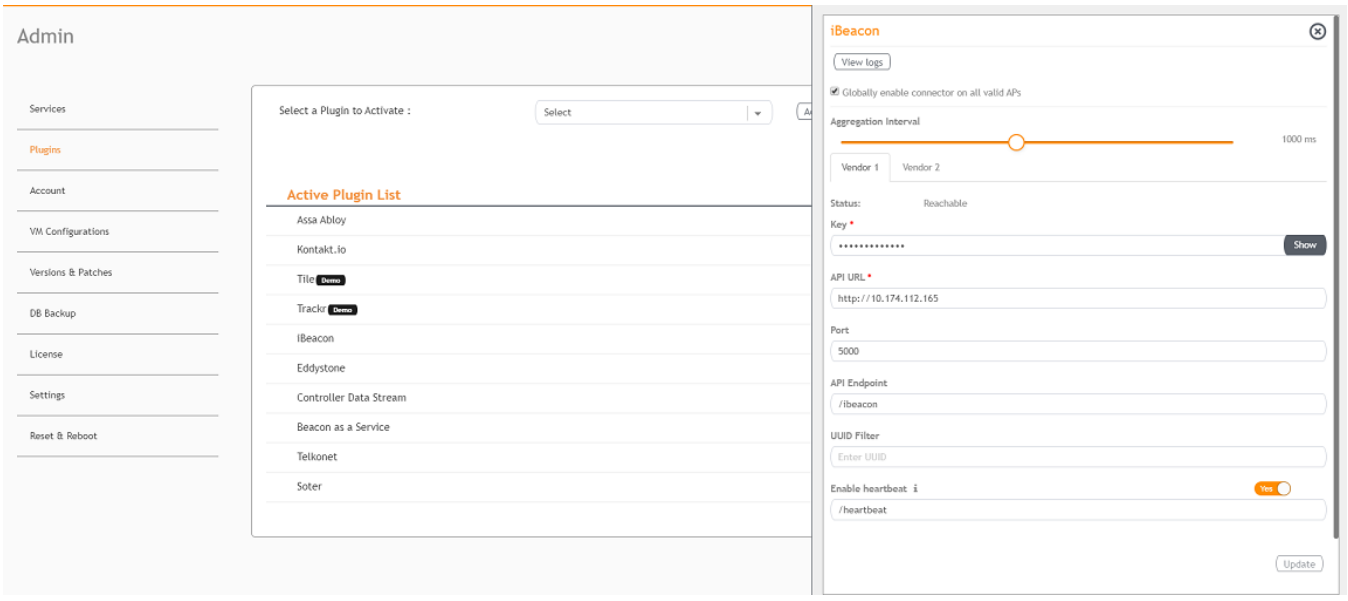
6. To deactivate the iBeacon plugin, select it and click **Deactivate**.

FIGURE 31 Deactivating the iBeacon Plugin



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

FIGURE 32 Updating the Configuration Parameters



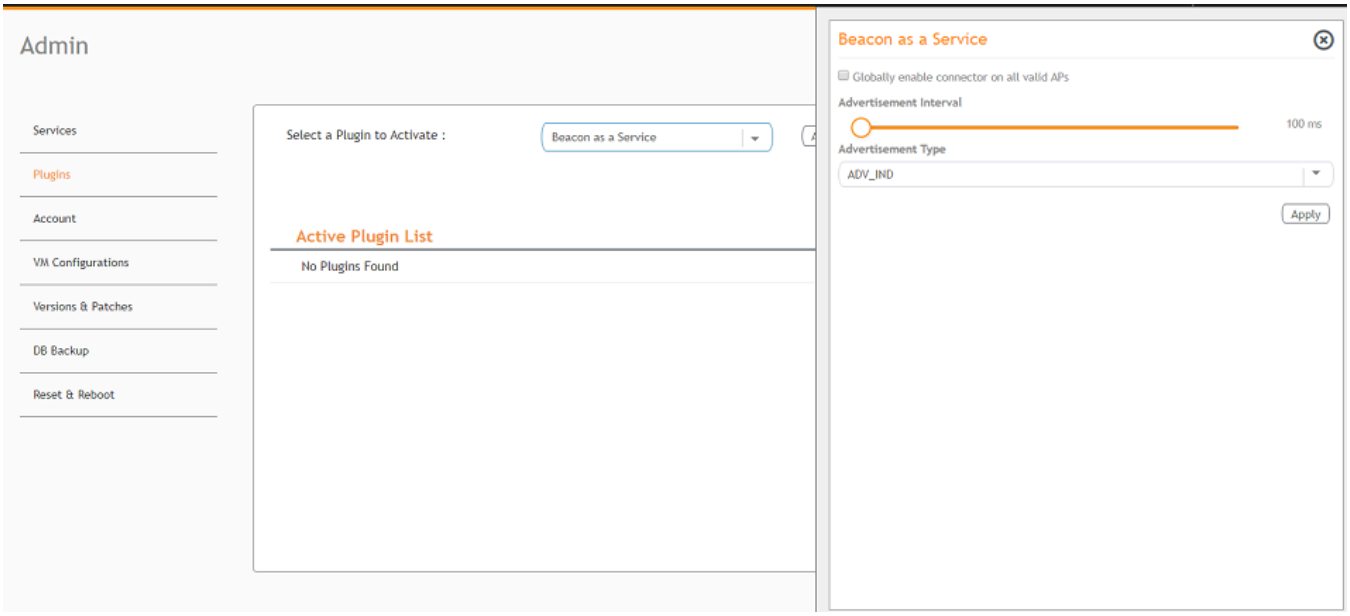
Activating and Editing the Beacon as a Service Plugin

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

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

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

FIGURE 33 Activating the Beacon as a Service Plugin



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

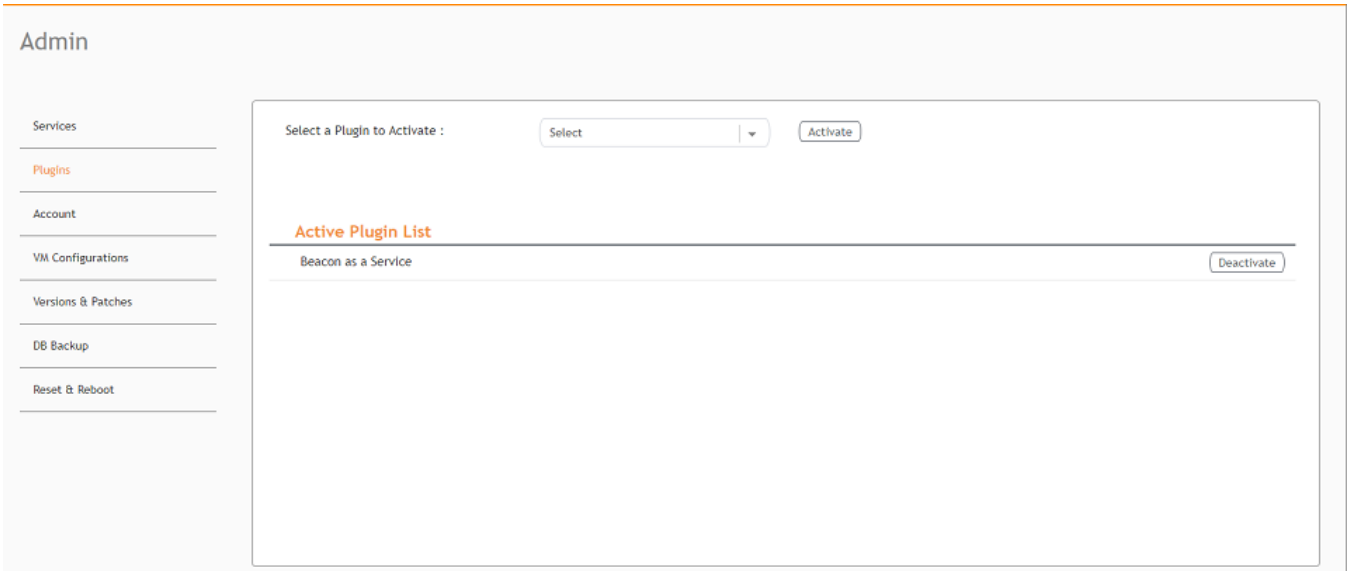
      NOTE
      If **Globally enable connector on all valid APs** is not selected, you can activate the plugin for each AP by adding a tag. Refer to Adding Tags to an AP on page 71 for more information.

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

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

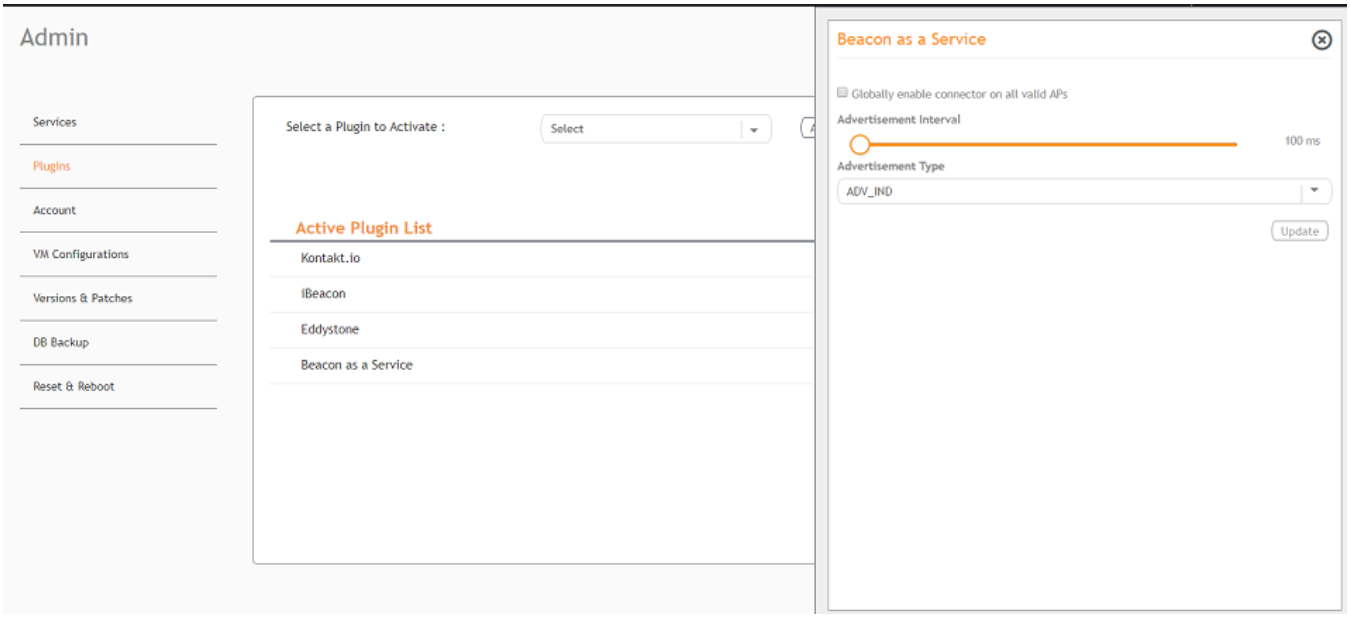
6. To deactivate the Beacon as a Service plugin, select it and click **Deactivate**.

FIGURE 34 Deactivating the Beacon as a Service Plugin



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

FIGURE 35 Updating the Configuration Parameters



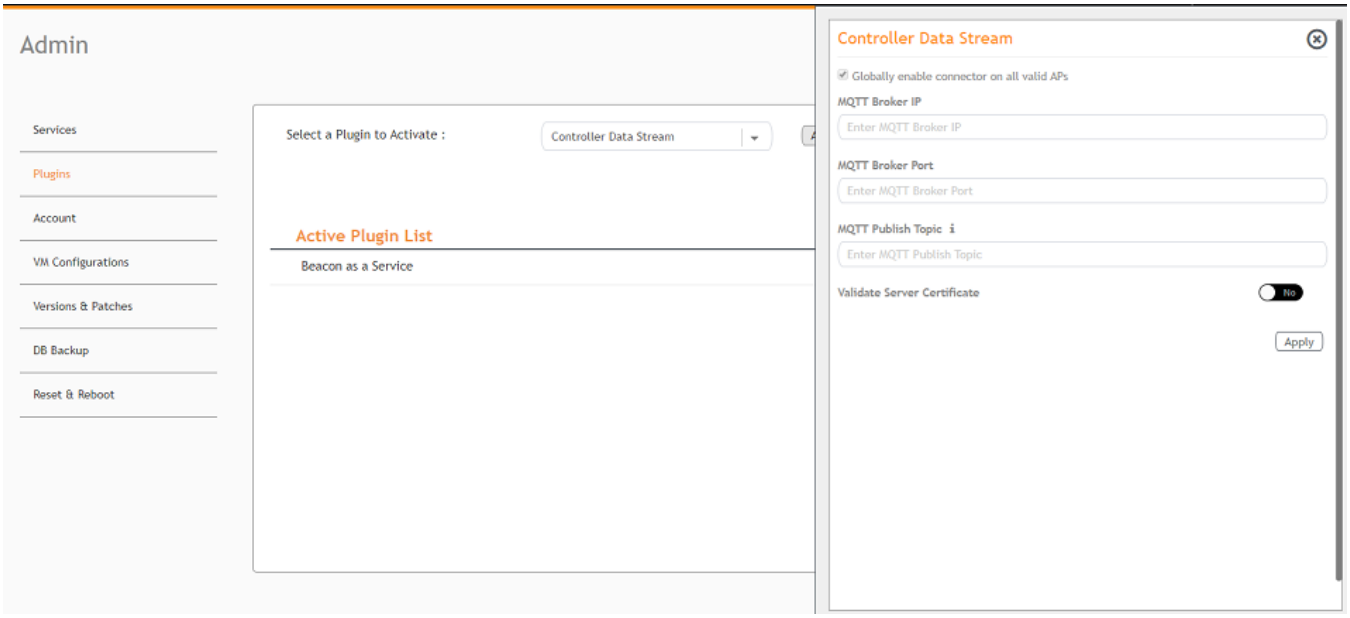
Activating and Editing the Controller Data Stream Plugin

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

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

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

FIGURE 36 Activating the Controller Data Stream Plugin



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

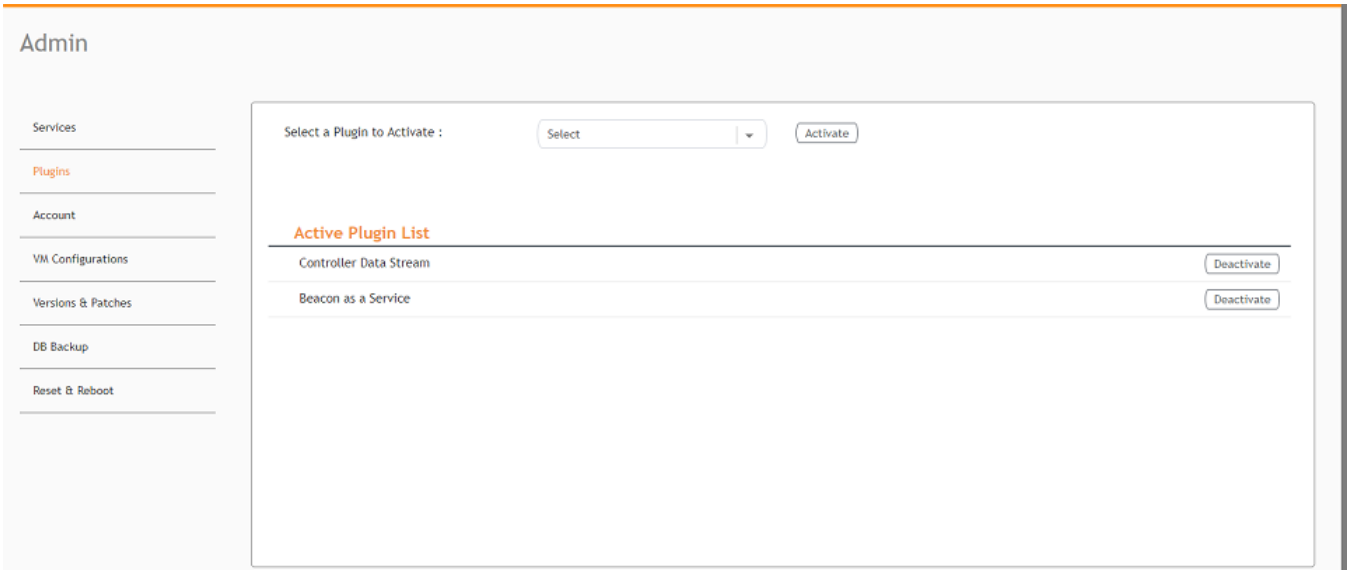
      NOTE
      If **Globally enable connector on all valid APs** is not selected then you can activate the plugin for each AP by adding tag. Refer Adding Tags to an AP on page 71 for more information.

   b) In **MQTT Broker IP**, enter the IP address of your MQTT broker.
   c) In **MQTT Broker Port**, enter the network port to which you want to connect.
   d) In **MQTT Publish Topic**, enter the topic name as a simple string that is hierarchically structured with forward slashes (/) as delimiters. An MQTT client can publish messages as soon as it connects to a broker.
   e) Enable **Validate Server Certificate** to secure the connection with SSL.
5. Click **Apply**.

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

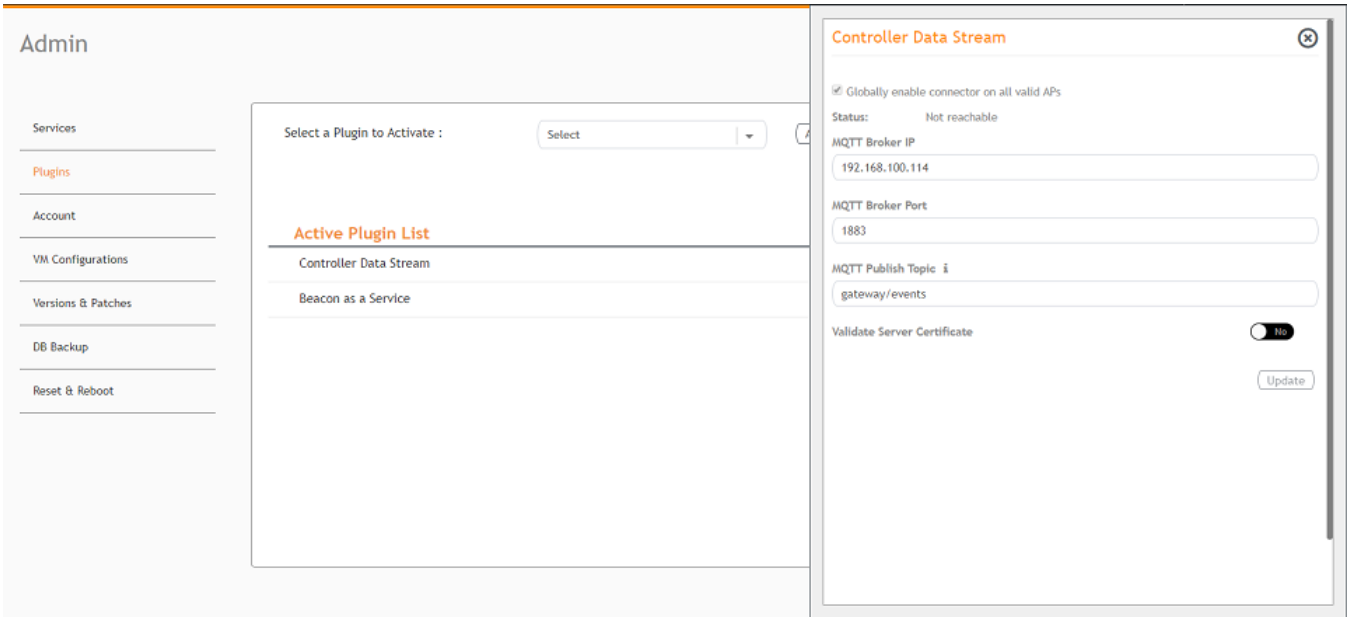
6. To deactivate the Controller Data Stream plugin, select it and click **Deactivate**.

FIGURE 37 Deactivating the Controller Data Stream Plugin



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

FIGURE 38 Updating the Configuration Parameters



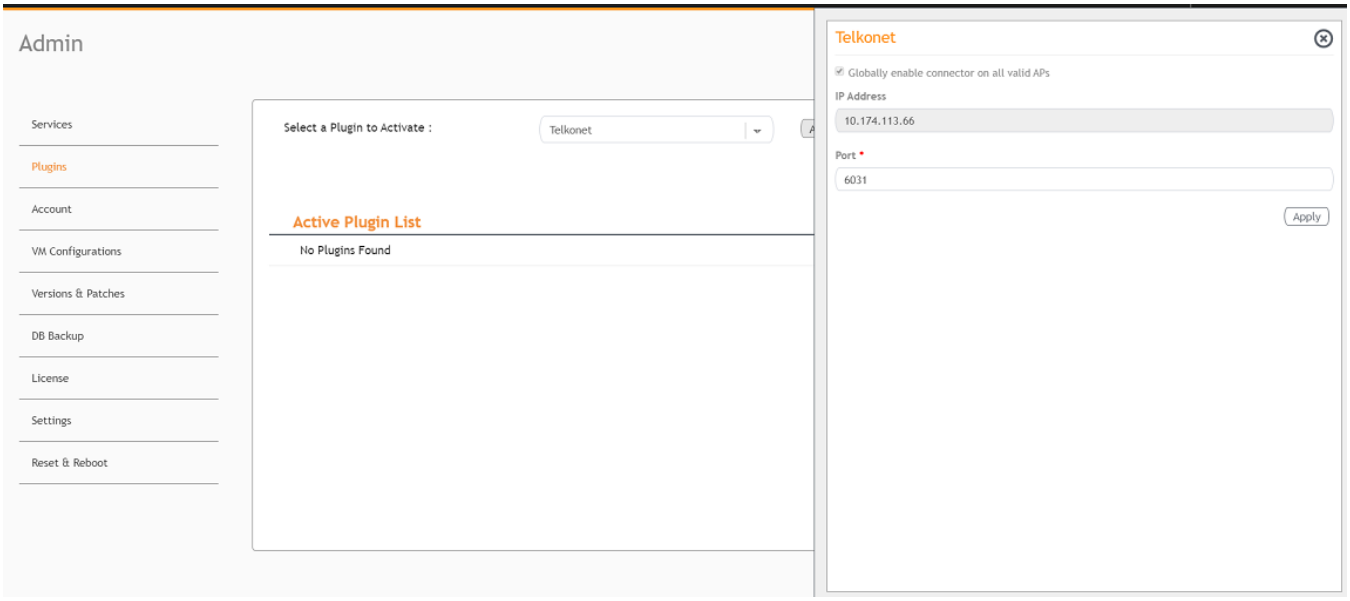
Activating and Editing the Telkonet Plugin

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

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

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

FIGURE 39 Activating the Telkonet Plugin



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

      NOTE
      If **Globally enable connector on all valid APs** is not selected, you can activate the plugin for each AP by adding a tag. Refer to Adding Tags to an AP on page 71 for more information.

   b) Enter the IP Address.

      This is the IP address of the Telkonet controller.

   c) Enter the Port number.

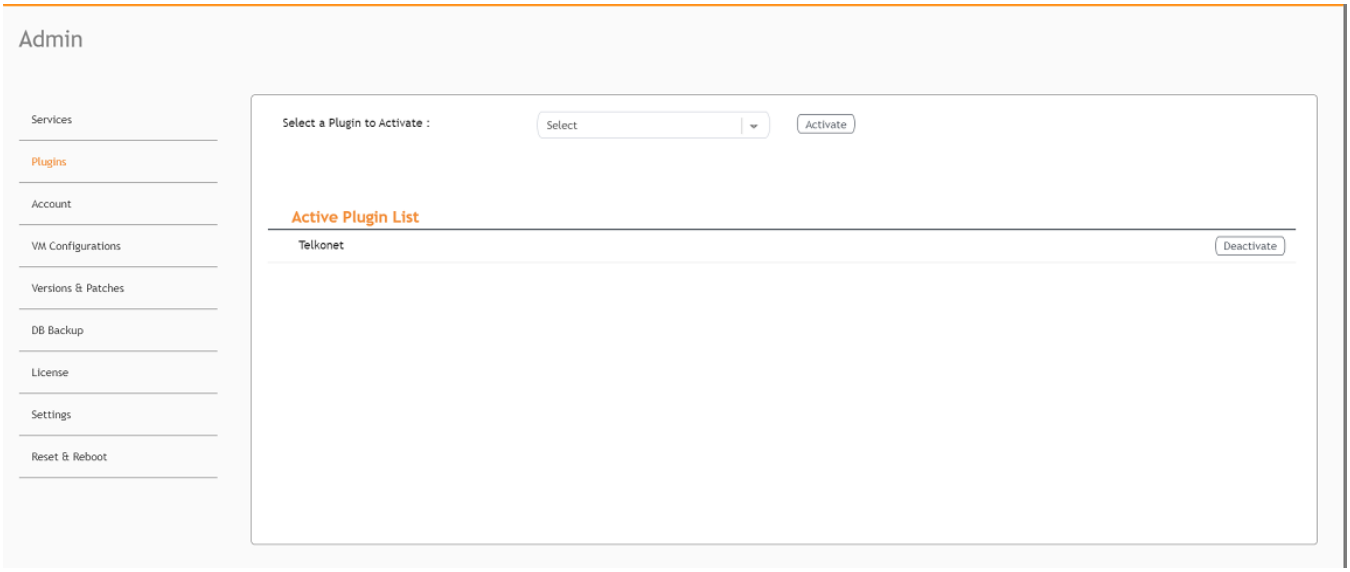
      This is the port number on which the vendor/connector web server is running.

5. Click **Apply**.

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

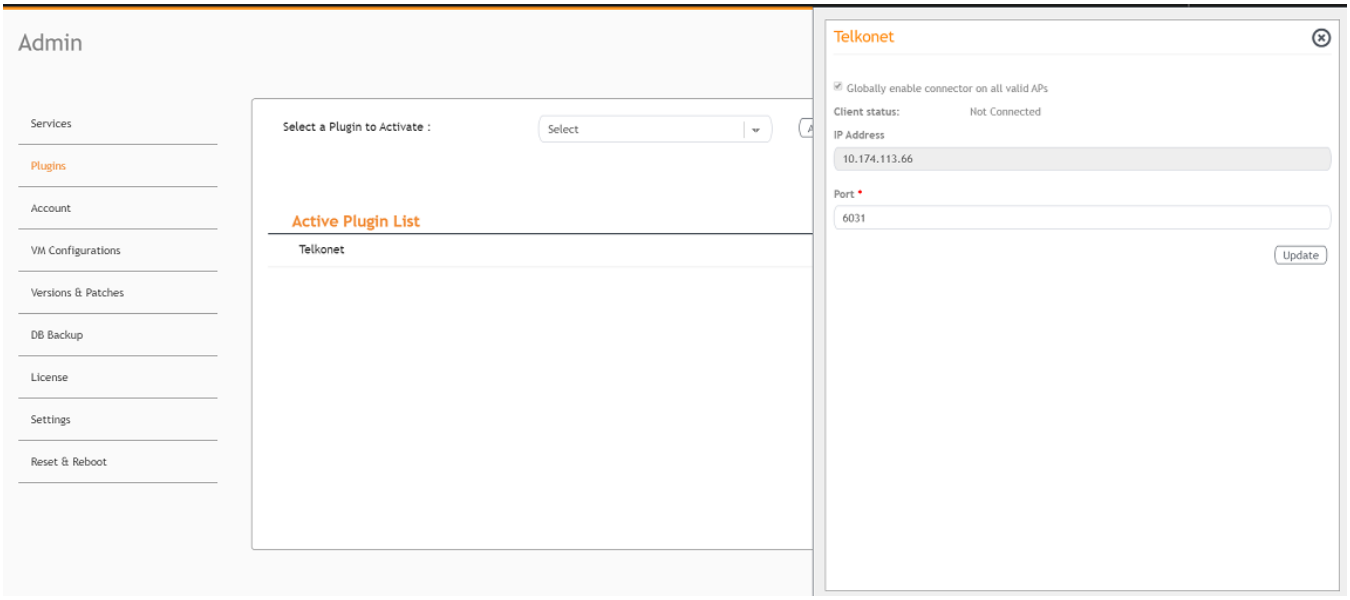
6. To deactivate the Telkonet plugin, select it and click **Deactivate**.

FIGURE 40 Deactivating the Telkonet Plugin



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

FIGURE 41 Updating the Configuration Parameters



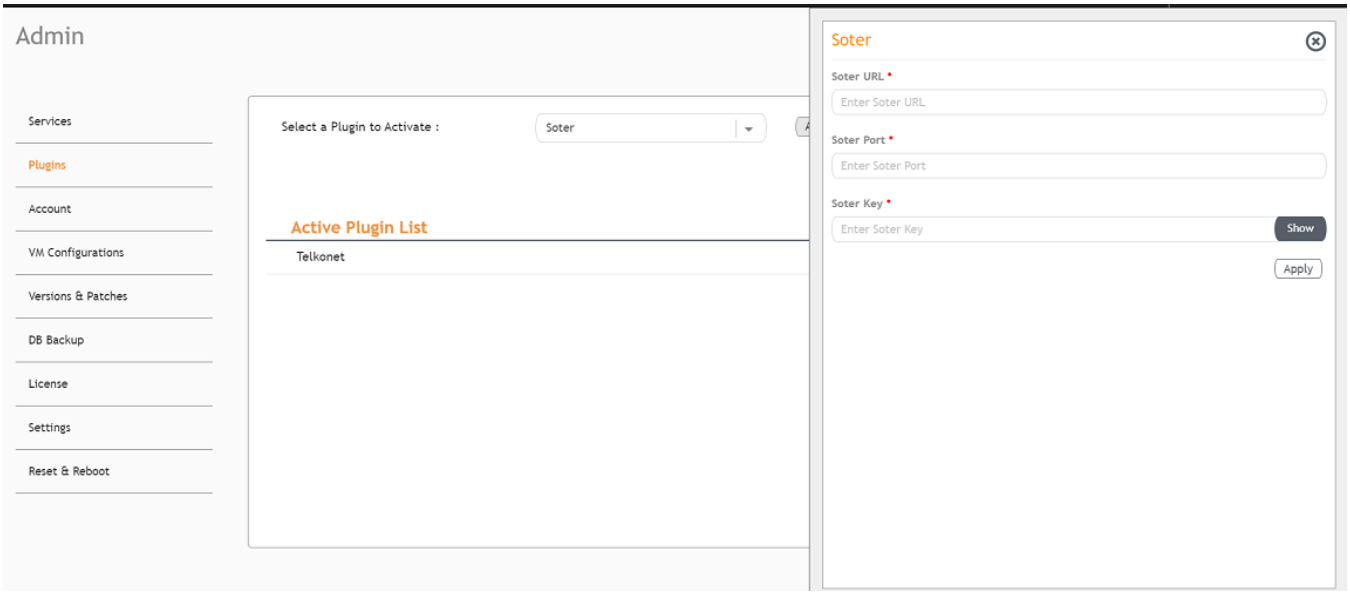
Activating and Editing the Soter Plugin

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

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

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

FIGURE 42 Activating the Soter Plugin



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

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

   b) Enter the Port number.

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

      NOTE
      The default MQTT port is 8883.

   c) Enter the Key.

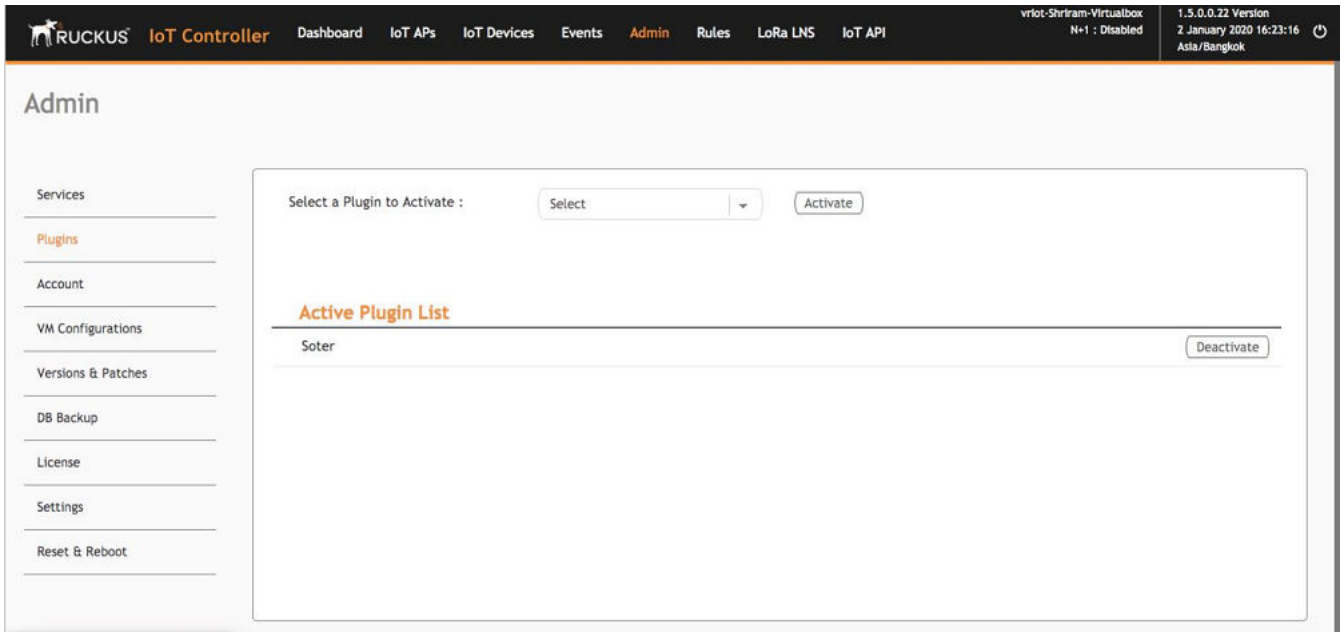
      The Vendor application is responsible for authenticating the Keys.

5. Click **Apply**.

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

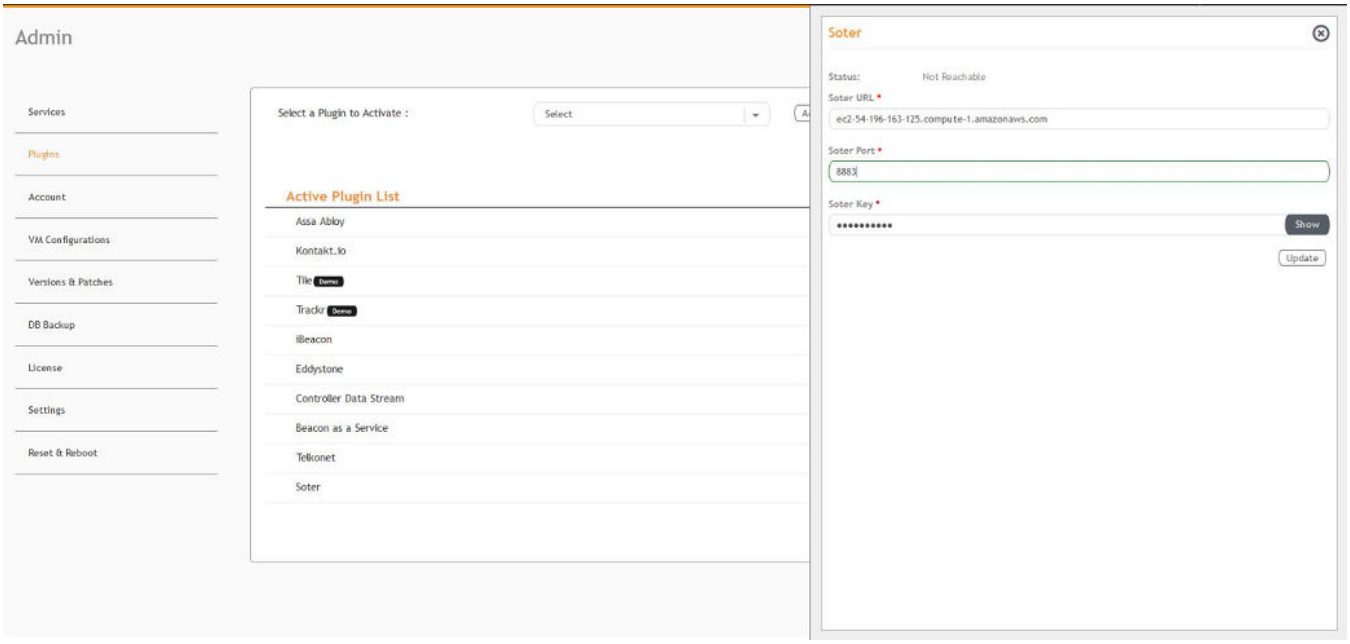
6. To deactivate the Soter plugin, select it and click **Deactivate**.

FIGURE 43 Deactivating the Soter Plugin



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

FIGURE 44 Updating the Configuration Parameters



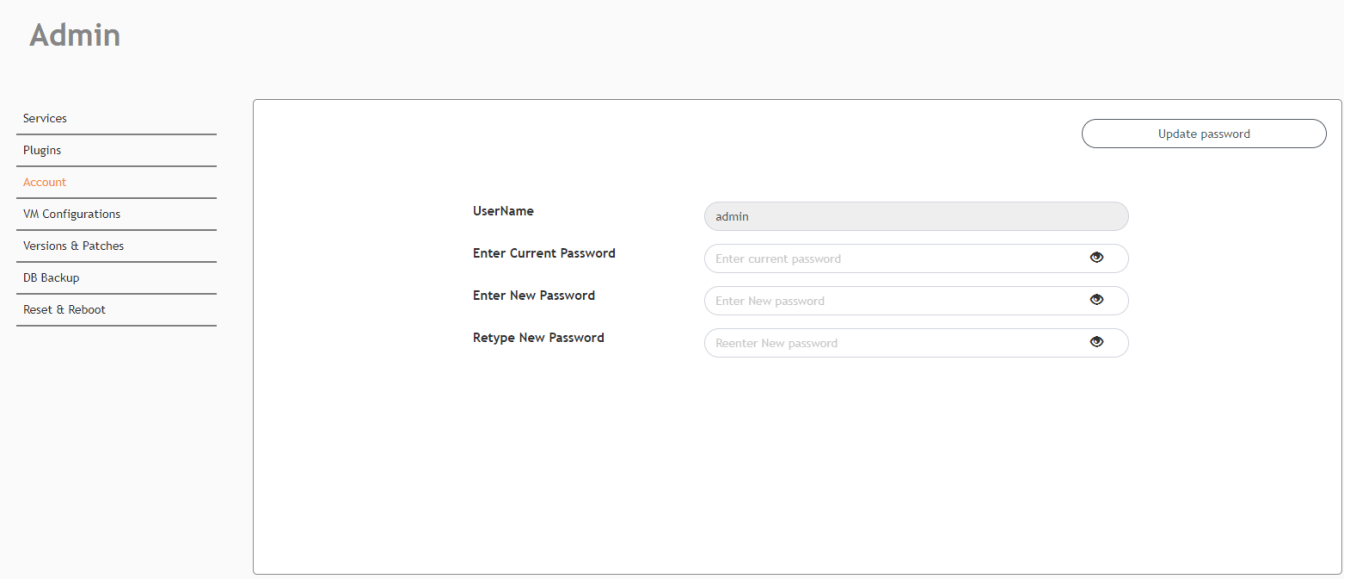
Changing the Password

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 45 Changing the Password



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

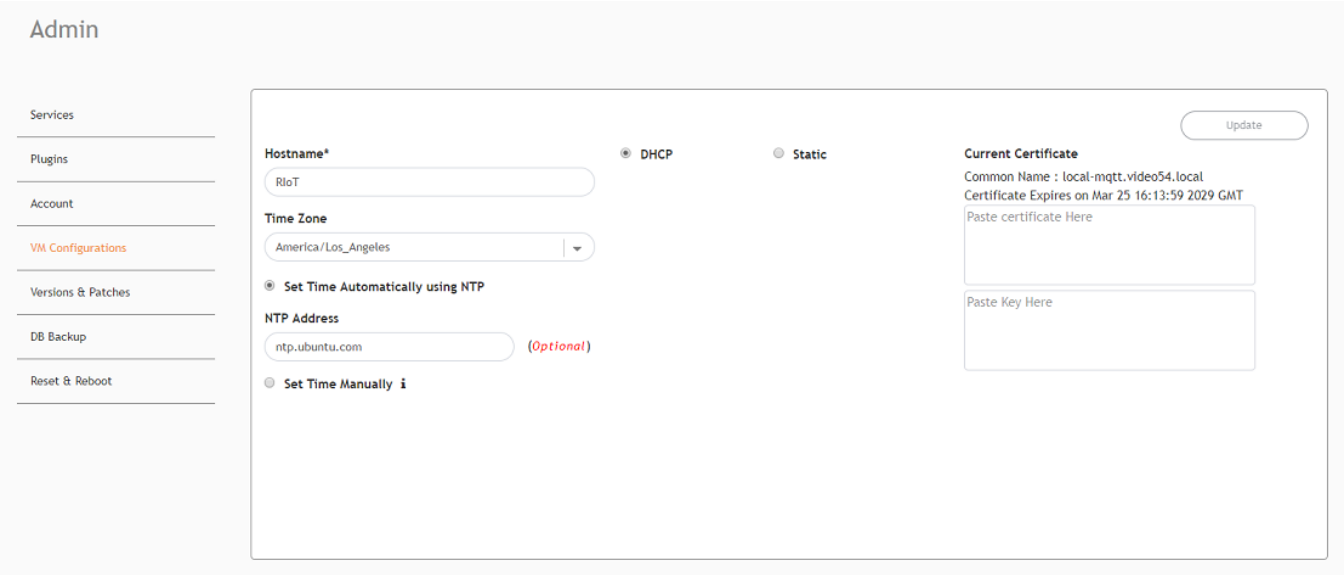
Configuring Virtual Machines

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 46 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.

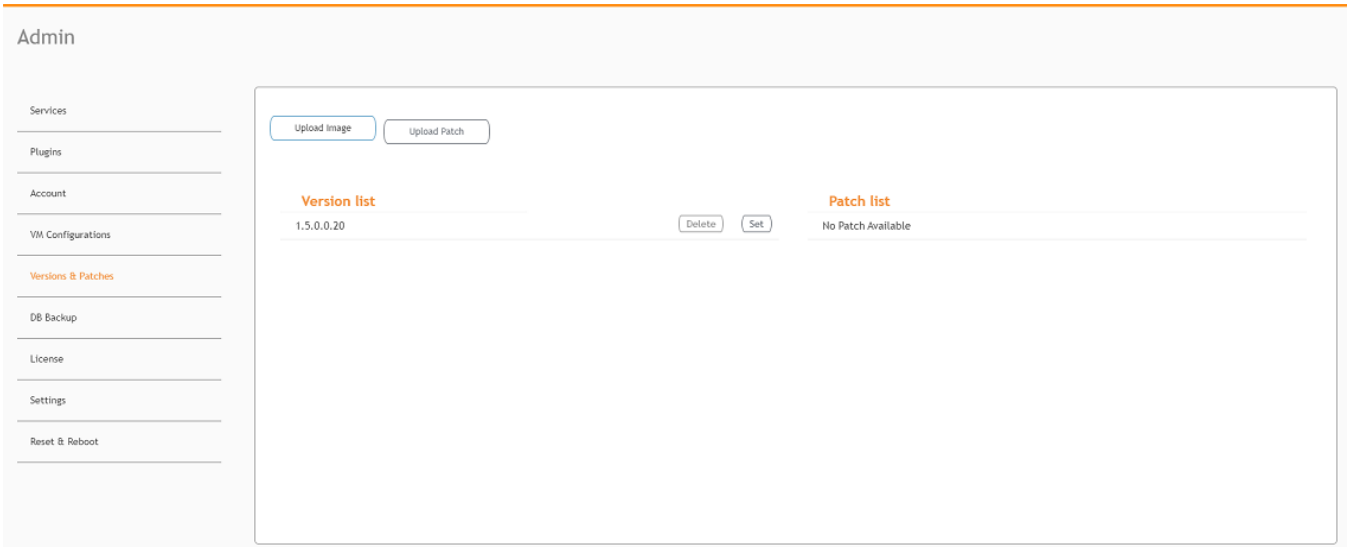
Uploading an Image

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 47 Uploading an Image



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

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

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

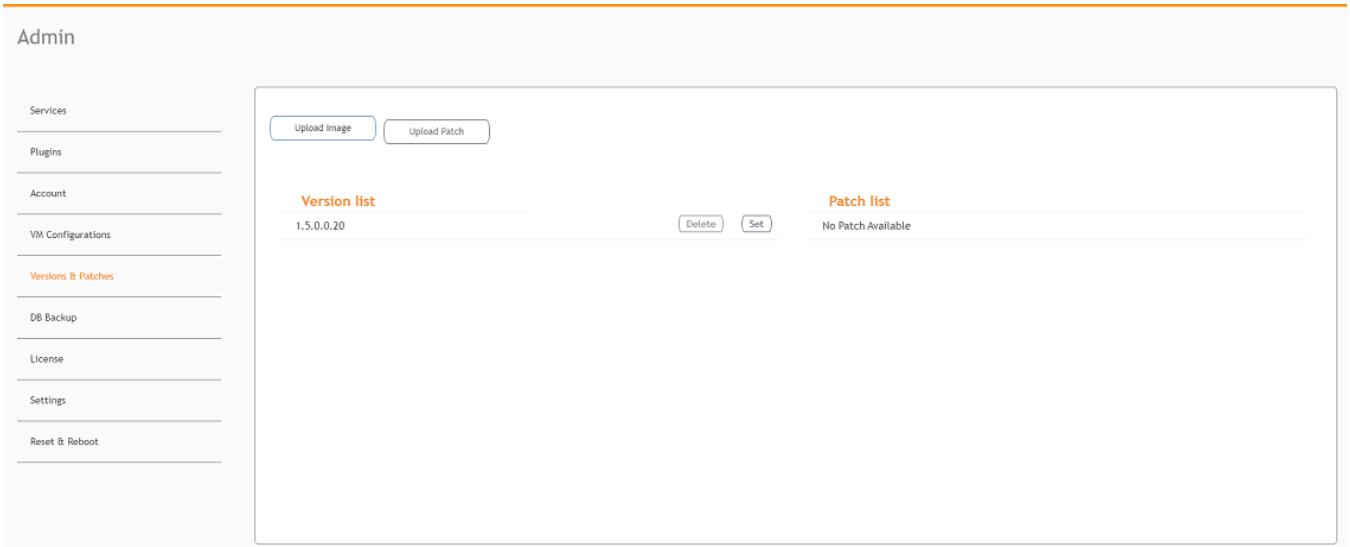
Uploading a Patch

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

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

2. In the left navigation pane, click **Versions & Patches**.

FIGURE 48 Uploading a Patch



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

ATTENTION
You cannot revert a patch.

Backing Up Files

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

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

FIGURE 49 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.

Uploading the Ruckus IoT Controller License

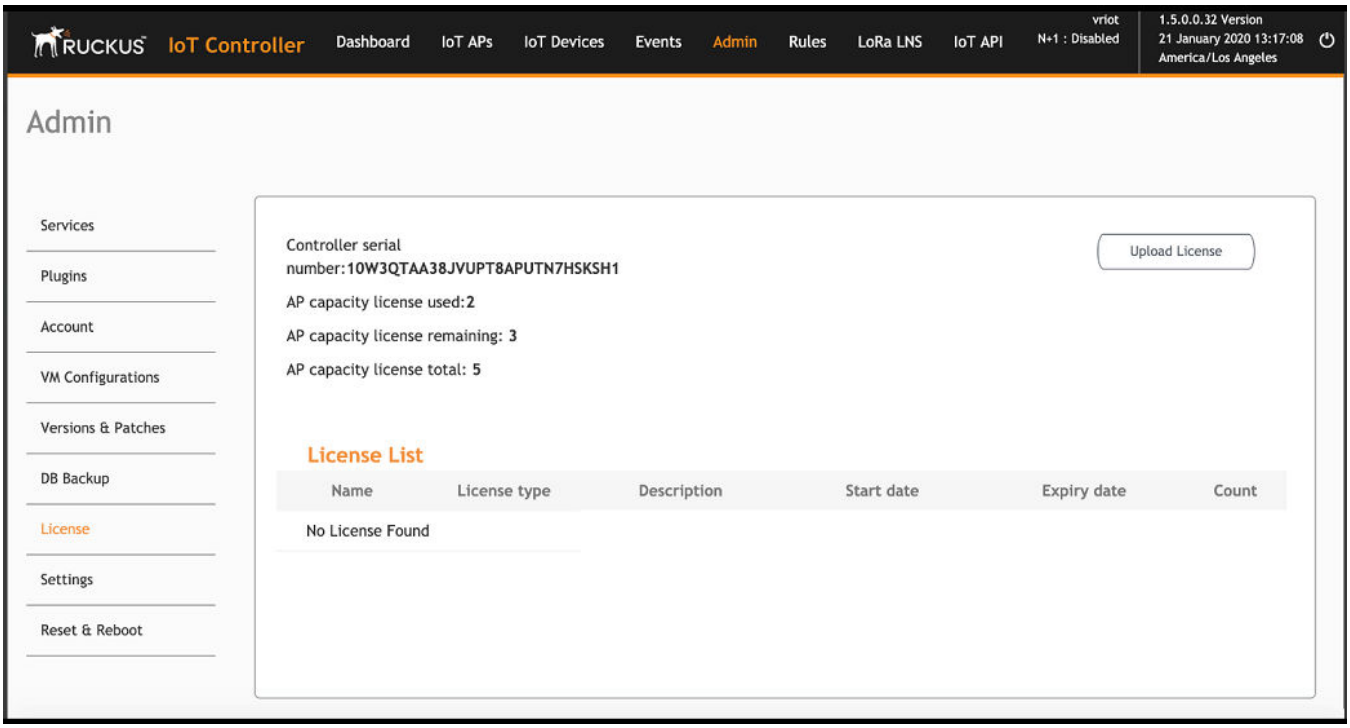
To obtain and activate the license, refer to "Activating a License" in the *Ruckus IoT ControllerSoftware Installation Guide*.

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

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

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

FIGURE 50 Uploading a License



3. Click **Upload License** to upload the license.

   The Upload License page displays the following information:

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

Change the Settings

You can upgrade an AP firmware image without a full upgrade through normal or patch upgrades.

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

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

FIGURE 51 Settings Page

Rebooting Ruckus IoT Controller

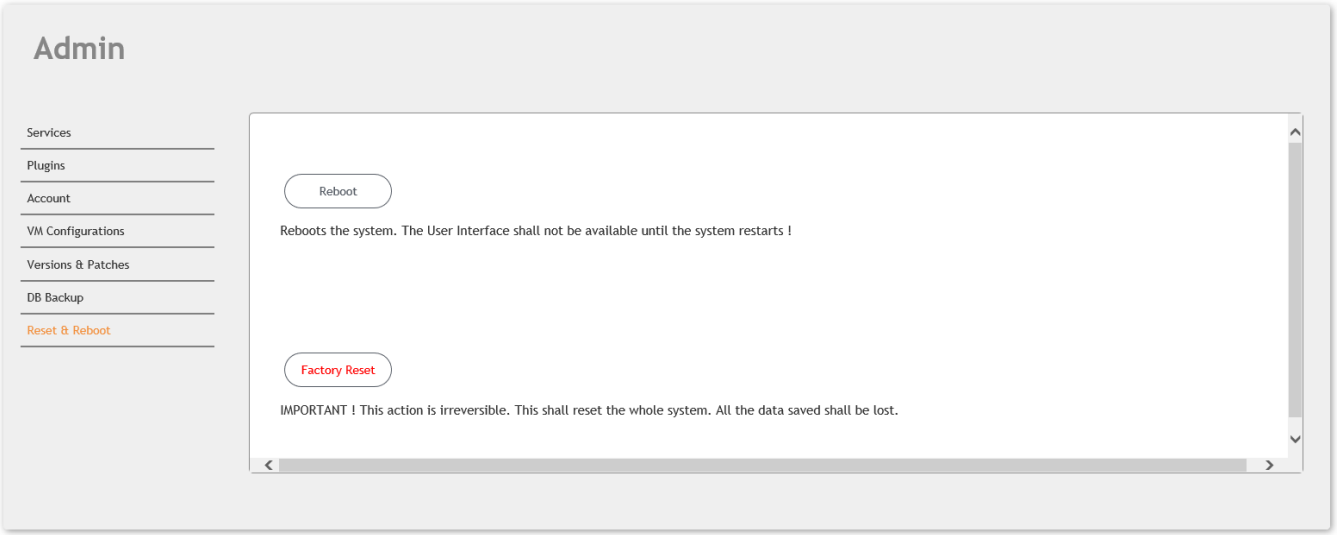
If the Ruckus IoT Controller is experiencing an issue, attempt a reboot to resolve the issue.

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 52 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.

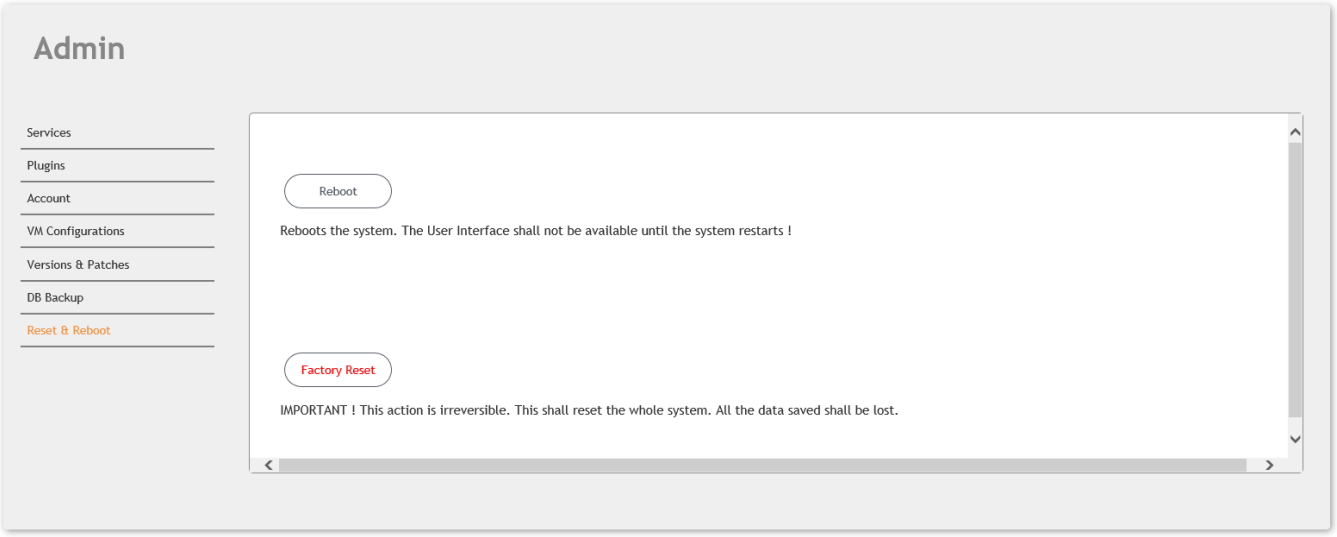
Complete the following steps to reset the Ruckus IoT Controller to its factory default settings.

CAUTION
Performing the reset action is irreversible.

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

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

FIGURE 53 Resetting Ruckus IoT Controller



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 (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.

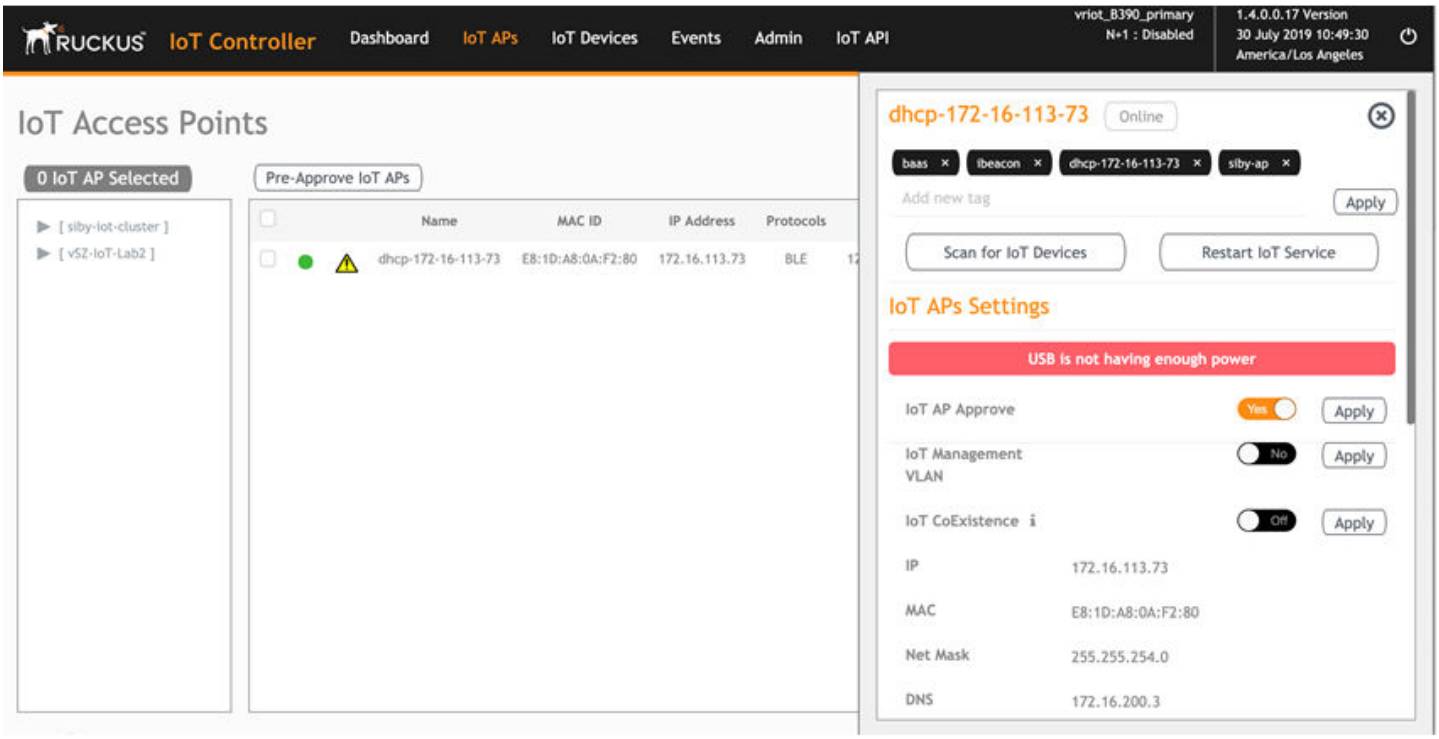
Ruckus Command Line Interface

The **set iotg-mqtt-brokerip** *Ruckus-IoT-Controller-IP-address* command can be used to discover the Ruckus IoT Controller.

USB Power

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

FIGURE 54 Displaying a Shortage of USB Power



NOTE

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

Adding an IoT AP

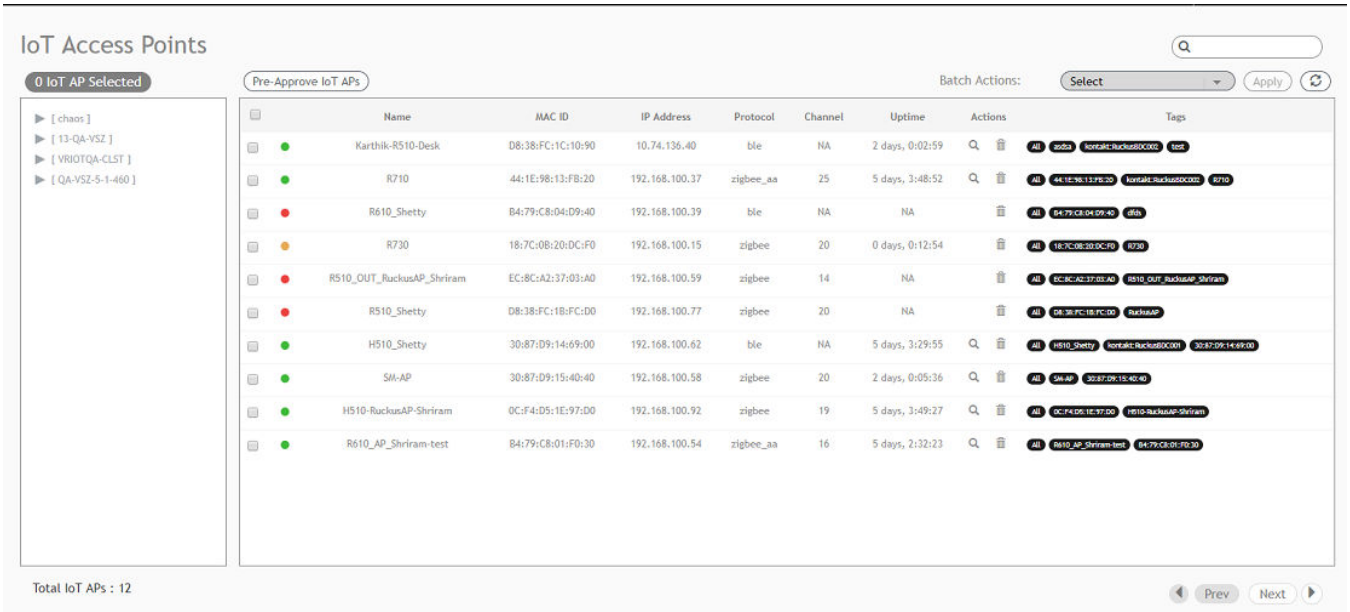
The administrator can add an IoT AP to the Ruckus IoT Controller to manage IoT devices.

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

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

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

   FIGURE 55 IoT Access Points Page

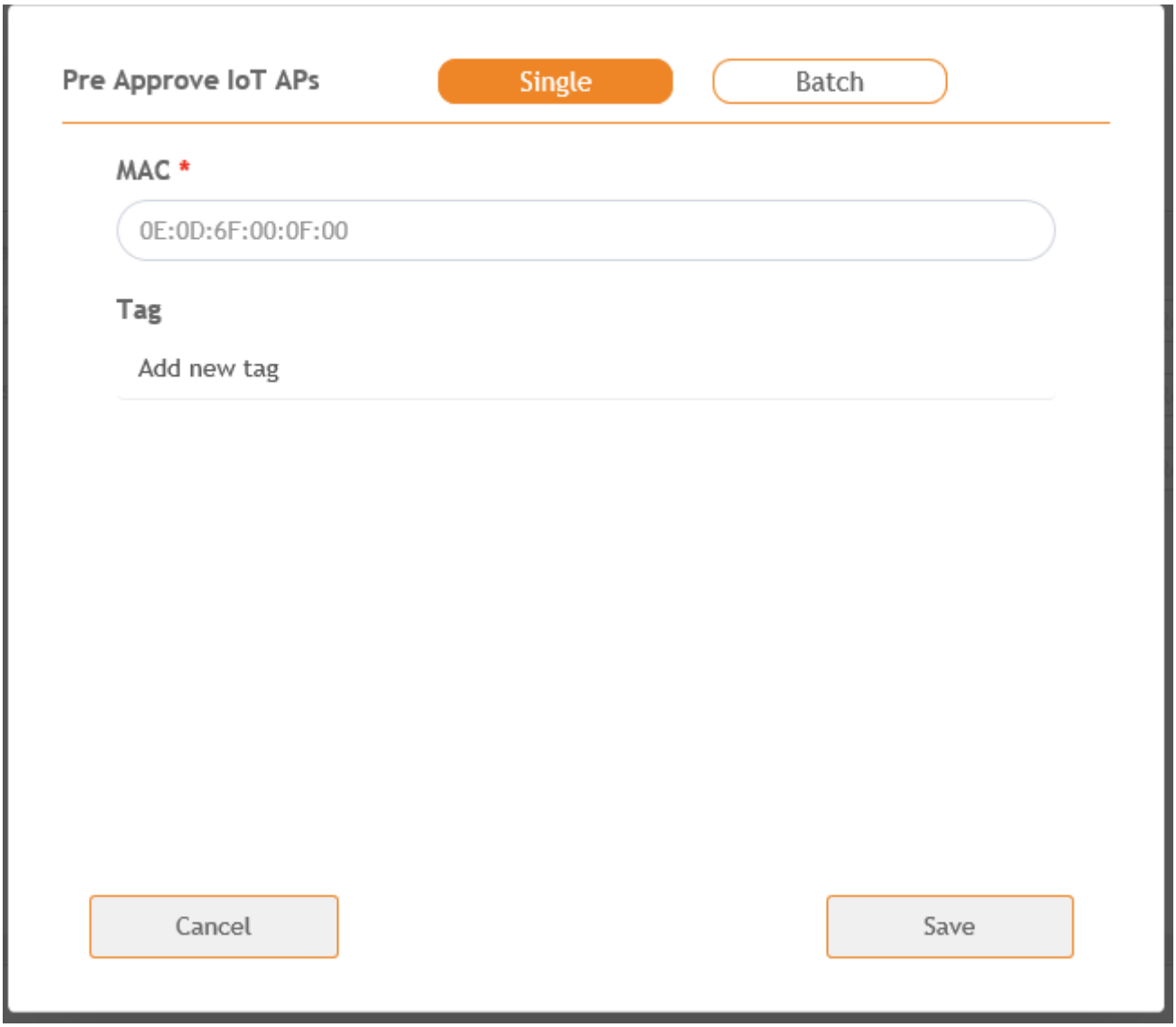


2. Click **Pre-Approve IoT APs**.

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

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

FIGURE 56 Adding a Single IoT AP

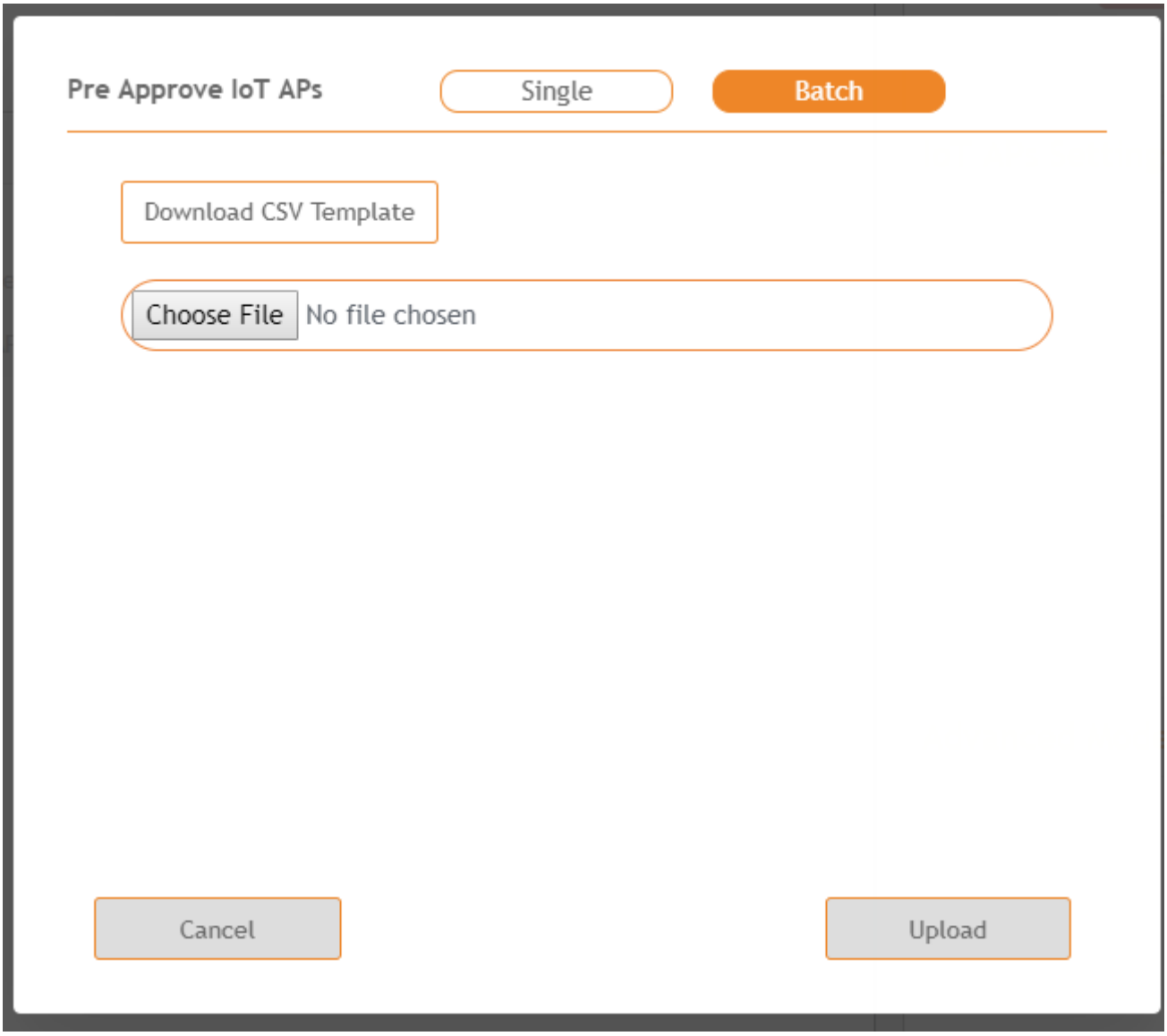


4. Enter the MAC address of the IoT AP and click **Save**.

   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 57 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.

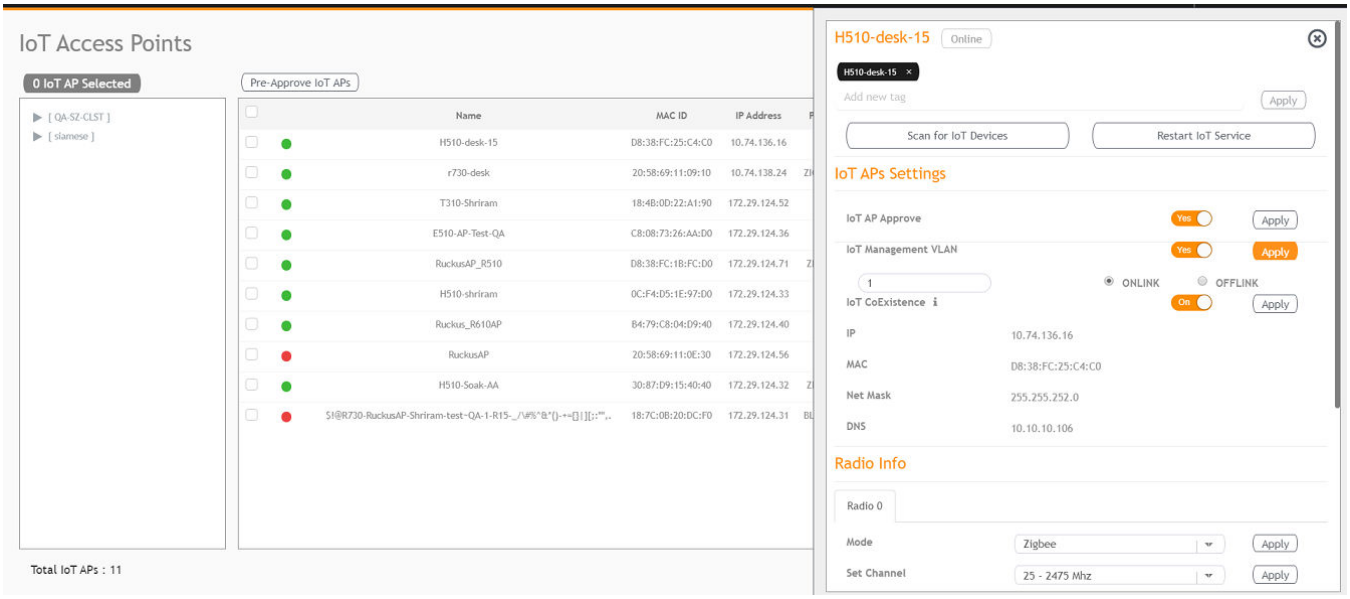
Complete the following steps to edit a single IoT AP.

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

   A list of selected IoT APs is displayed.

2. Click an IoT AP to edit.

FIGURE 58 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**
- **IoT Management VLAN**
- **AP Firmware**
- **AP Model**

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

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

Adding Tags to an AP

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

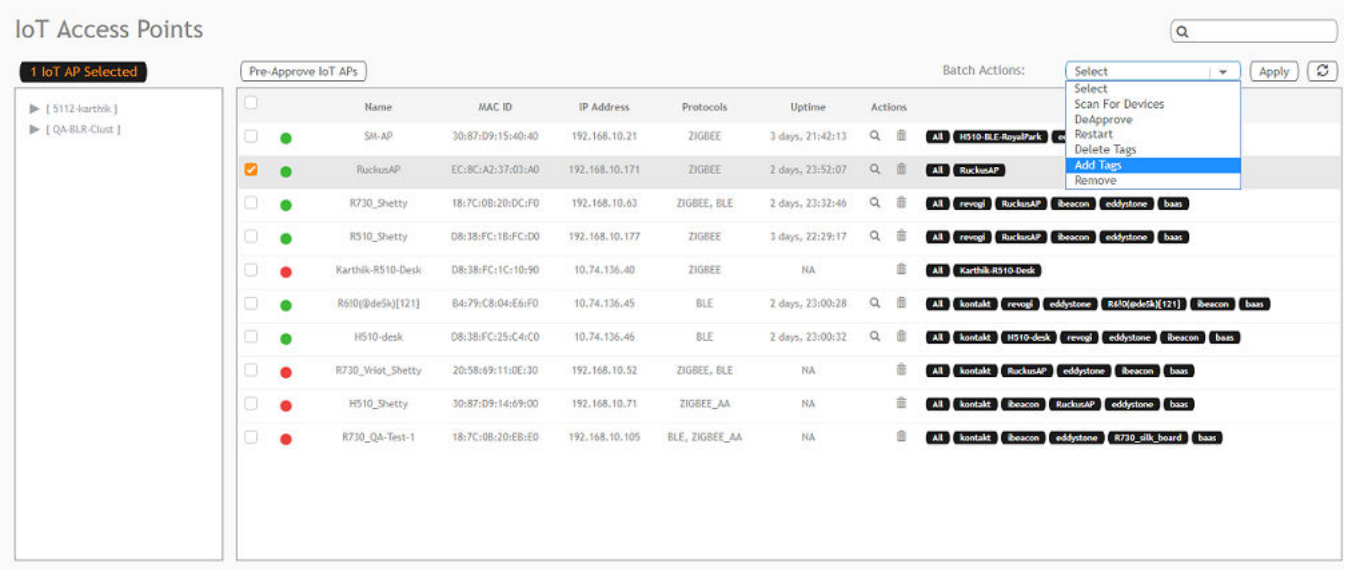
1. From the main menu, click **IoT APs**.

   A list of IoT APs is displayed.

2. Select an IoT AP.

   NOTE
   You can select one or more APs to add tags.

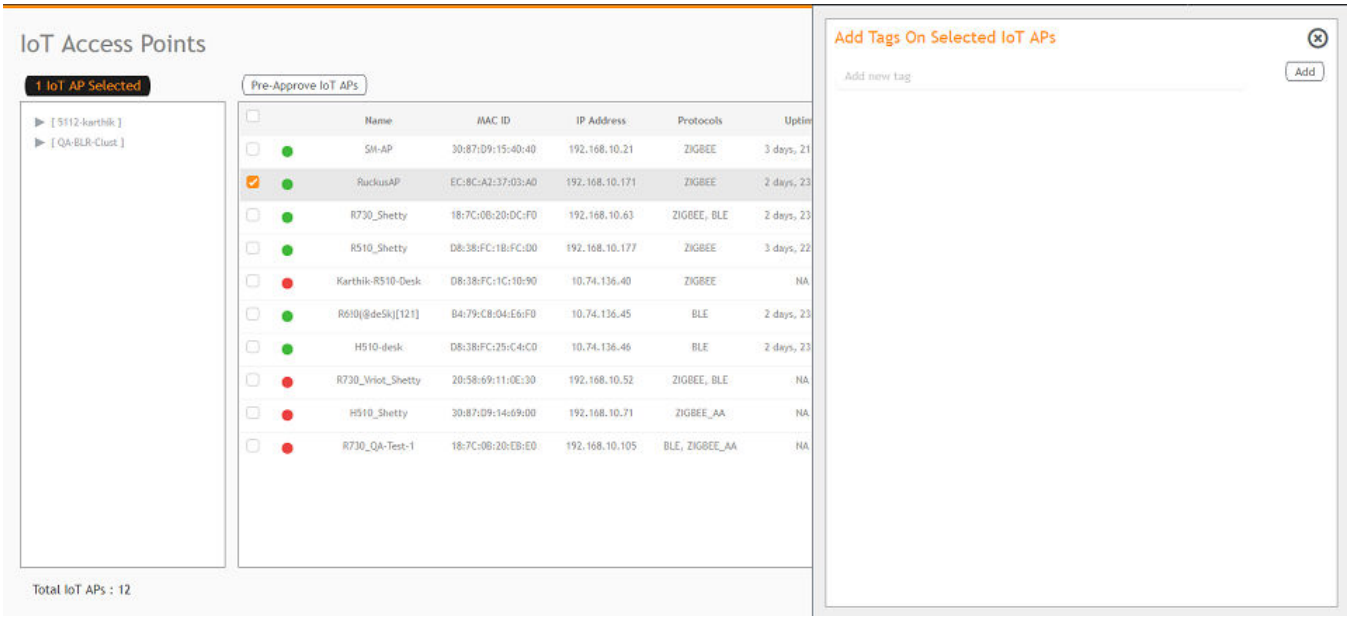
   FIGURE 59 Selecting an AP to Add Tags



3. Select **Add Tags** from the **Batch Actions** list.

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

FIGURE 60 Adding a Tag



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

TABLE 5 Plugins and Corresponding Tag Names

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

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

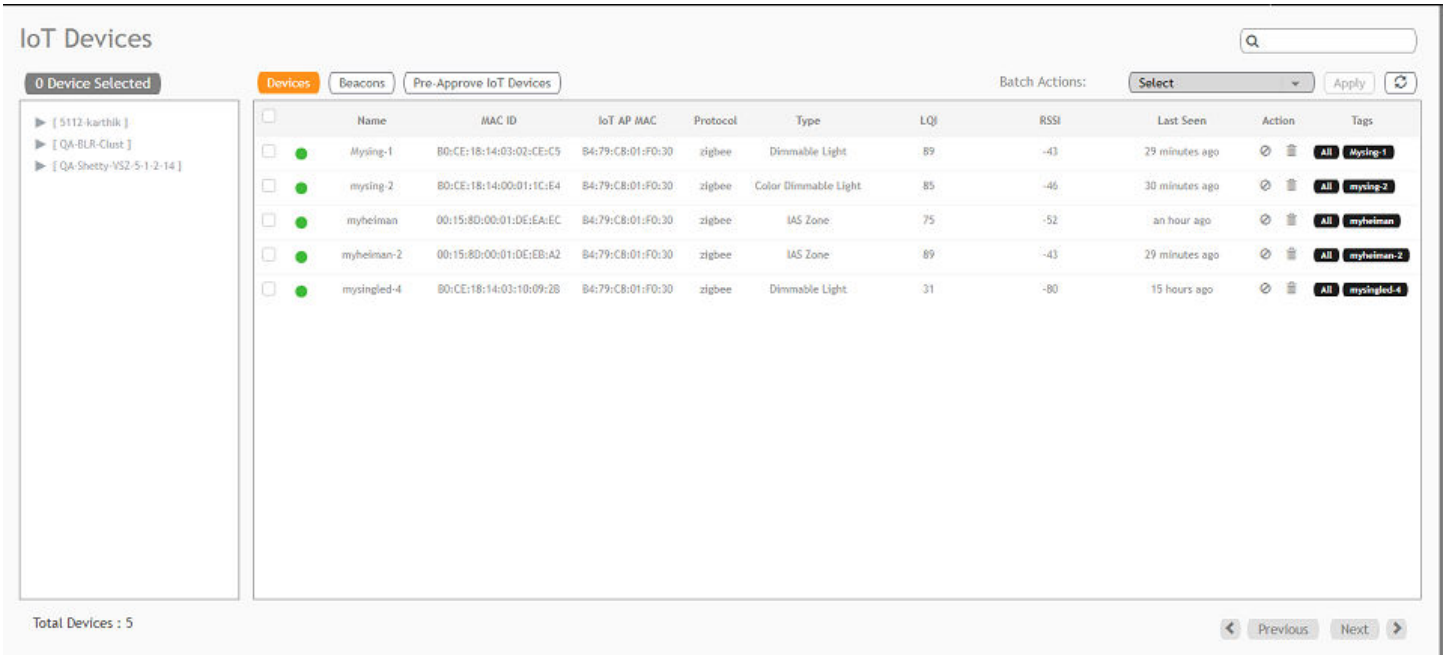
The Ruckus IoT Controller requires explicit user approval of devices. Only an approved device can be allowed into the IoT infrastructure.

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

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

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

FIGURE 61 IoT Devices Page

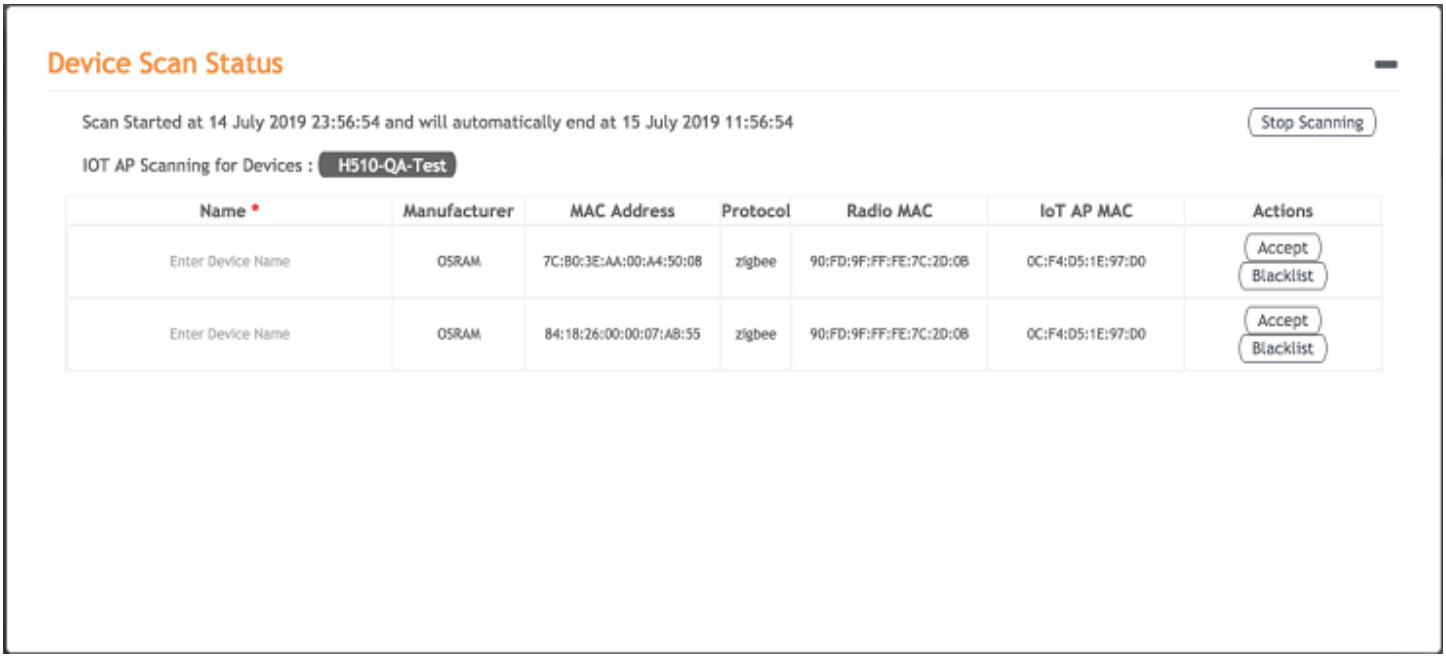


The device scan operation must be performed to start the device discovery process on the gateway. Upon starting device discovery, a dialog box is displayed, as shown in the following figure.

FIGURE 62 Device Discovery Dialog Box

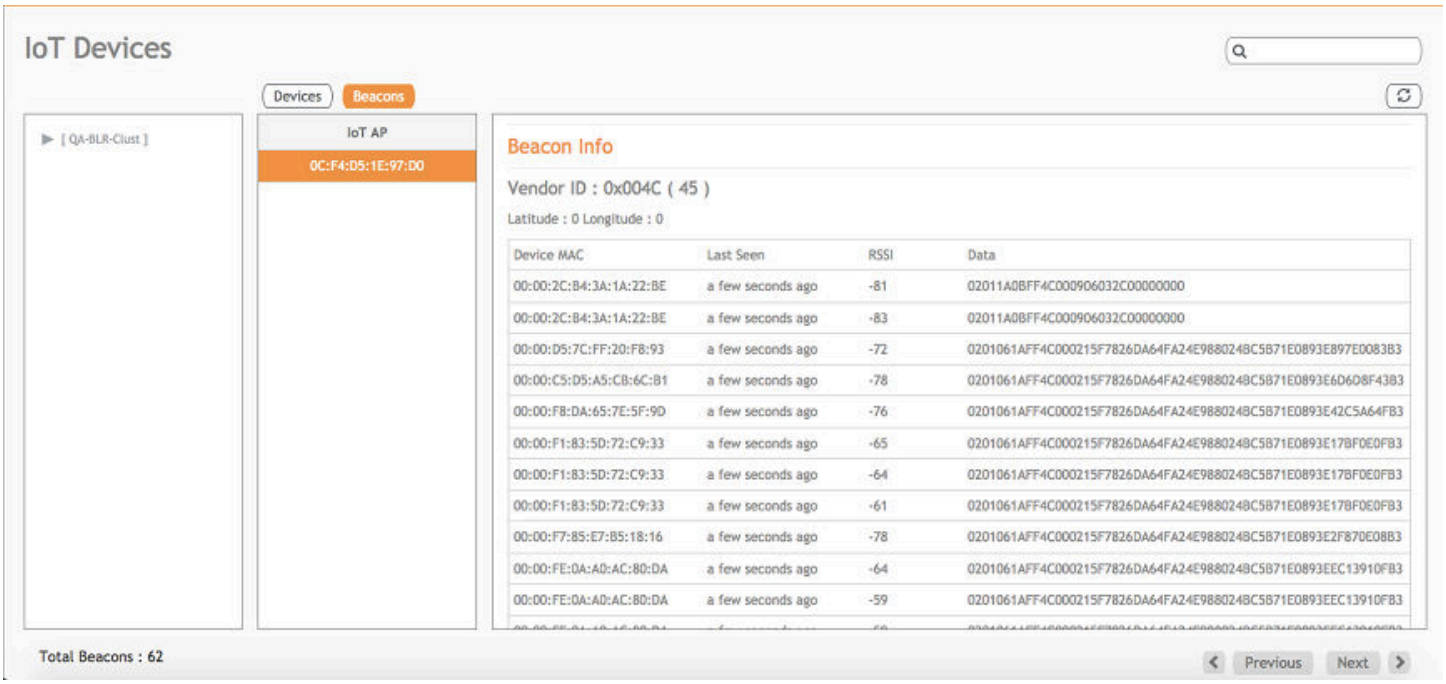
A device gets added to the Ruckus IoT Controller through Discover IoT Devices operations. If a device is pre-approved, the discovered device automatically joins the list of discovered devices. If the discovered device is not pre-approved, then you must select **Accept** or **Blacklist**. If the device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

FIGURE 63 Adding Device After Discovery



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

FIGURE 64 Beacons Page



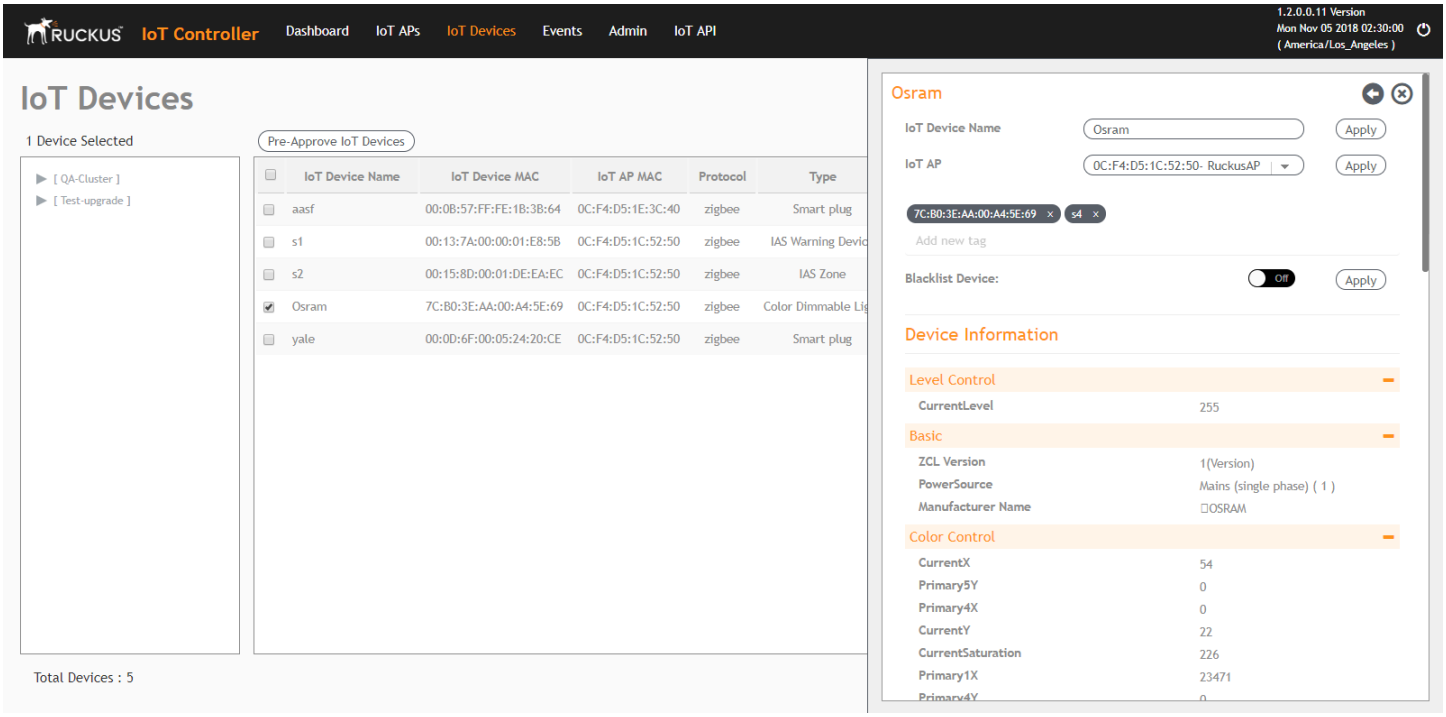
Managing OSRAM Light Bulbs

To discover OSRAM light bulbs, complete the following operations.

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

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

FIGURE 65 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.

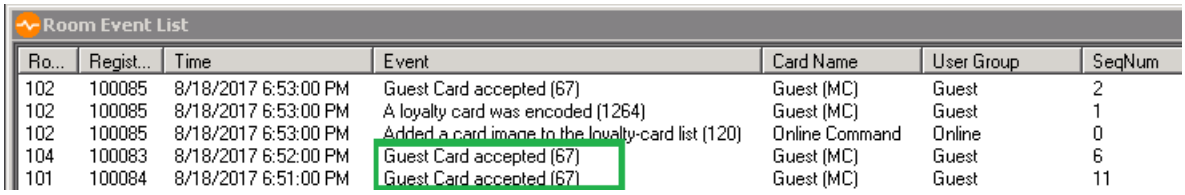
1. Swipe the AA Lock Discover Card across the lock.
2. Ensure that the LED blinks green.
3. Add the lock to the Ruckus IoT Controller (if it is not already pre-approved).

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 66 Visionline Server Event Log



Rules Engine

Rules Engine Overview

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

Configuring Rules

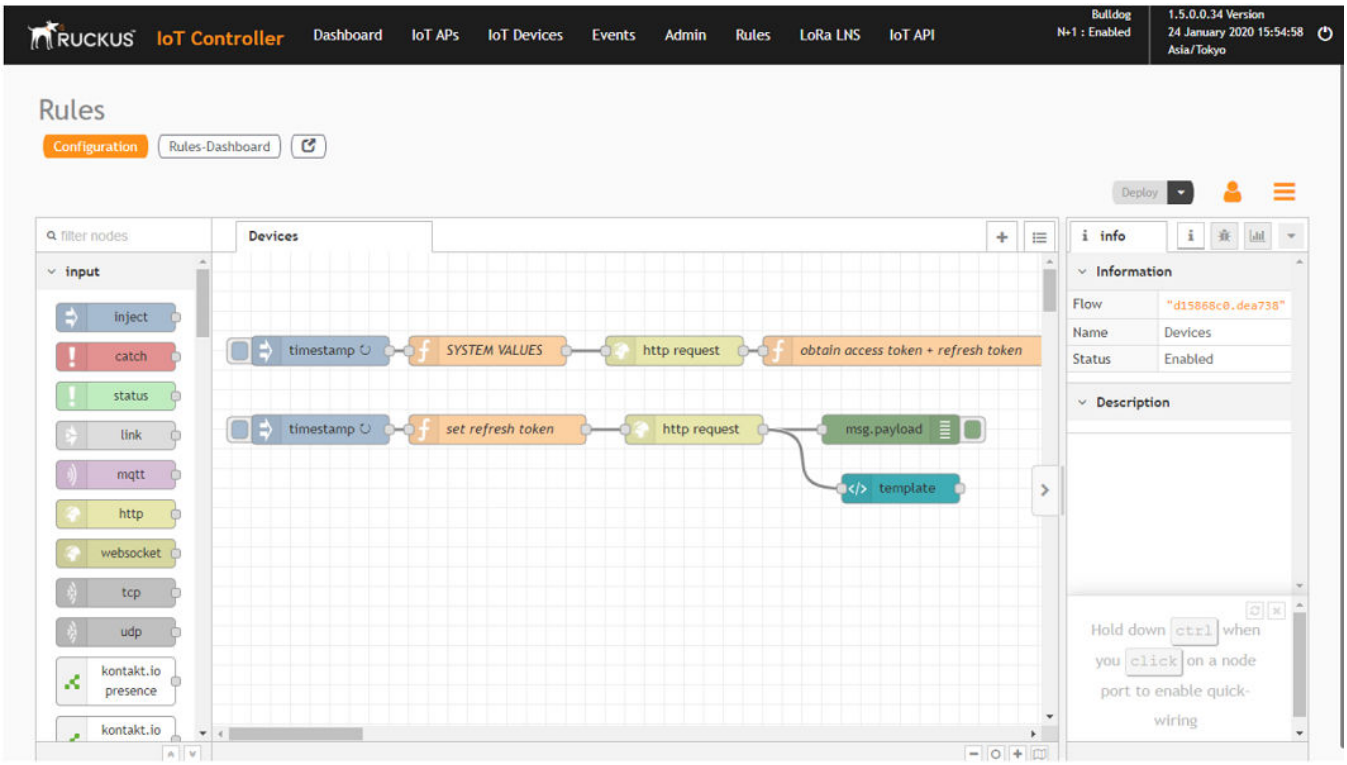
The Ruckus IoT Controller allows you to configure a rule or design a flow for an AP or device by using a wide range of the nodes in the palette of Node-RED editor.

Complete the following steps to configure a rule.

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

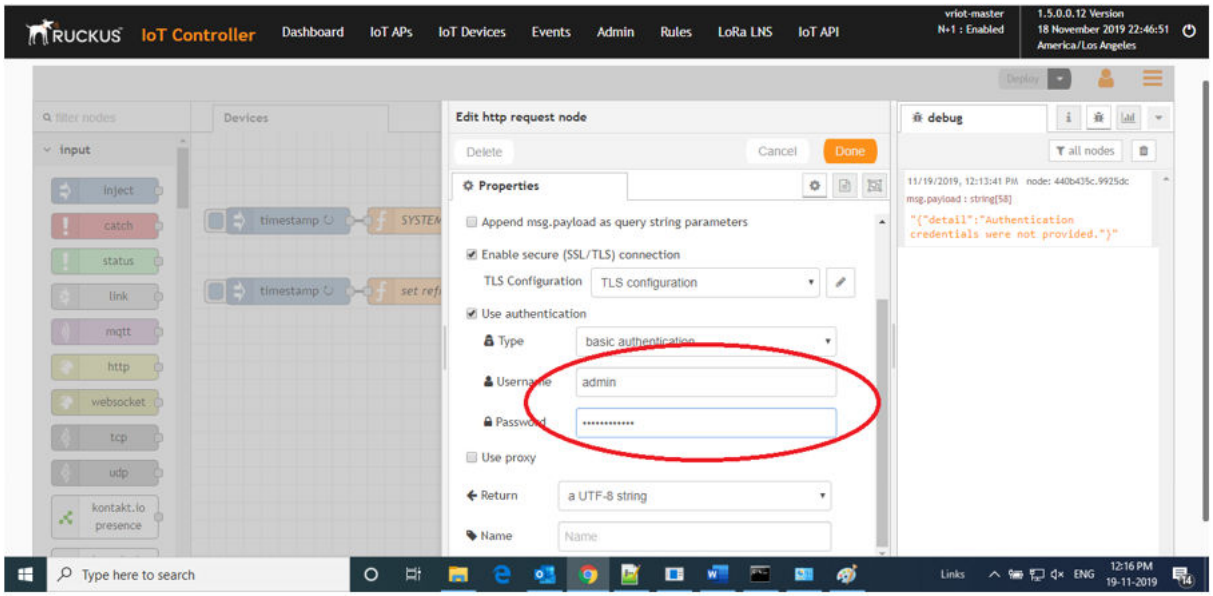
   NOTE
   To create the rules, refer to https://nodered.org/docs/.

FIGURE 67 Configuring a Rule



2. Click the **http request** node.

FIGURE 68 Editing the HTTP Request Node



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

3. Click **Deploy**.

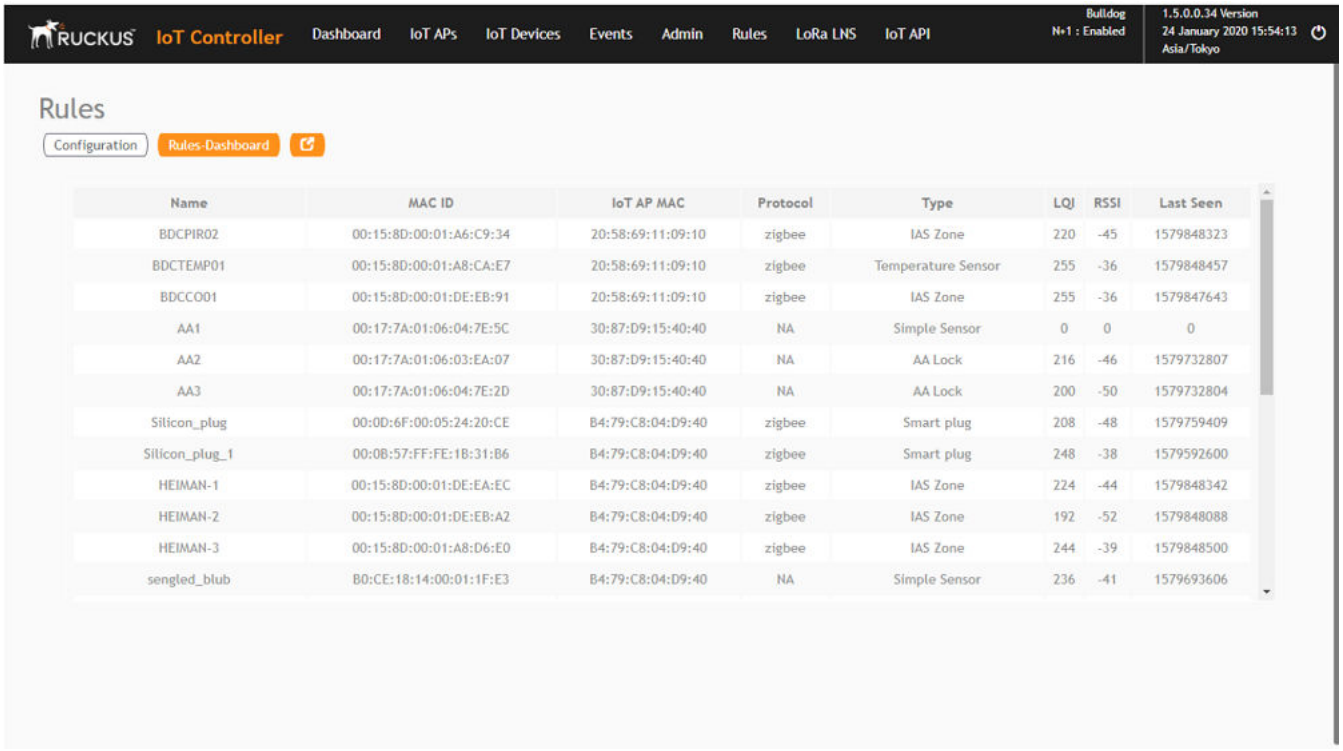
The workflow is ready to be deployed.

Rules-Dashboard

The **Rules-Dashboard** displays the configured rules.

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

   FIGURE 69 Rules-Dashboard



Name	MAC ID	IoT AP MAC	Protocol	Type	LQI	RSSI	Last Seen
BDCPIR02	00:15:8D:00:01:A6:C9:34	20:58:69:11:09:10	zigbee	IAS Zone	220	-45	1579848323
BDCTEMP01	00:15:8D:00:01:A8:CA:E7	20:58:69:11:09:10	zigbee	Temperature Sensor	255	-36	1579848457
BDCCO01	00:15:8D:00:01:DE:EB:91	20:58:69:11:09:10	zigbee	IAS Zone	255	-36	1579847643
AA1	00:17:7A:01:06:04:7E:5C	30:87:D9:15:40:40	NA	Simple Sensor	0	0	0
AA2	00:17:7A:01:06:03:EA:07	30:87:D9:15:40:40	NA	AA Lock	216	-46	1579732807
AA3	00:17:7A:01:06:04:7E:2D	30:87:D9:15:40:40	NA	AA Lock	200	-50	1579732804
Silicon_plug	00:0D:6F:00:05:24:20:CE	B4:79:C8:04:D9:40	zigbee	Smart plug	208	-48	1579759409
Silicon_plug_1	00:0B:57:FF:FE:1B:31:B6	B4:79:C8:04:D9:40	zigbee	Smart plug	248	-38	1579592600
HEIMAN-1	00:15:8D:00:01:DE:EA:EC	B4:79:C8:04:D9:40	zigbee	IAS Zone	224	-44	1579848342
HEIMAN-2	00:15:8D:00:01:DE:EB:A2	B4:79:C8:04:D9:40	zigbee	IAS Zone	192	-52	1579848088
HEIMAN-3	00:15:8D:00:01:A8:D6:E0	B4:79:C8:04:D9:40	zigbee	IAS Zone	244	-39	1579848500
sengled_blub	B0:CE:18:14:00:01:1F:E3	B4:79:C8:04:D9:40	NA	Simple Sensor	236	-41	1579693606

   The **Rules-Dashboard** lists the configured devices.

2. Click  .

   A browser opens with the **Rules-Dashboard** page.

LoRaWAN

LoRaWAN Overview

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

Logging In to the LoRa Network

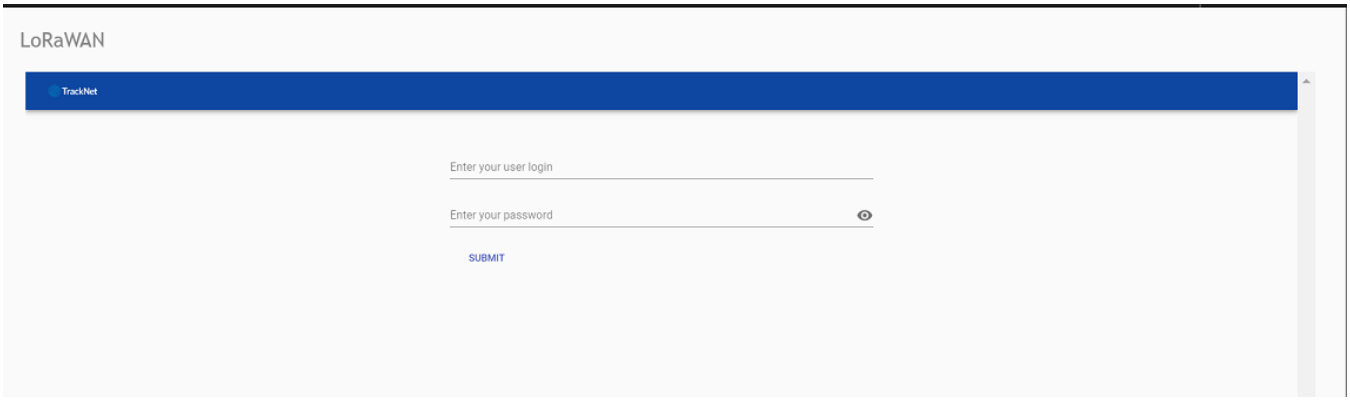
LoRaWAN is a media access control (MAC) protocol for wide area networks. It is designed to allow low-powered devices to communicate with Internet-connected applications over long-range wireless connections.

Complete the following steps to access the LoRa network.

1. From the main menu, click **LoRa LNS**.

   The LoRaWAN login page is displayed.

   FIGURE 70 Logging In to the LoRaWAN



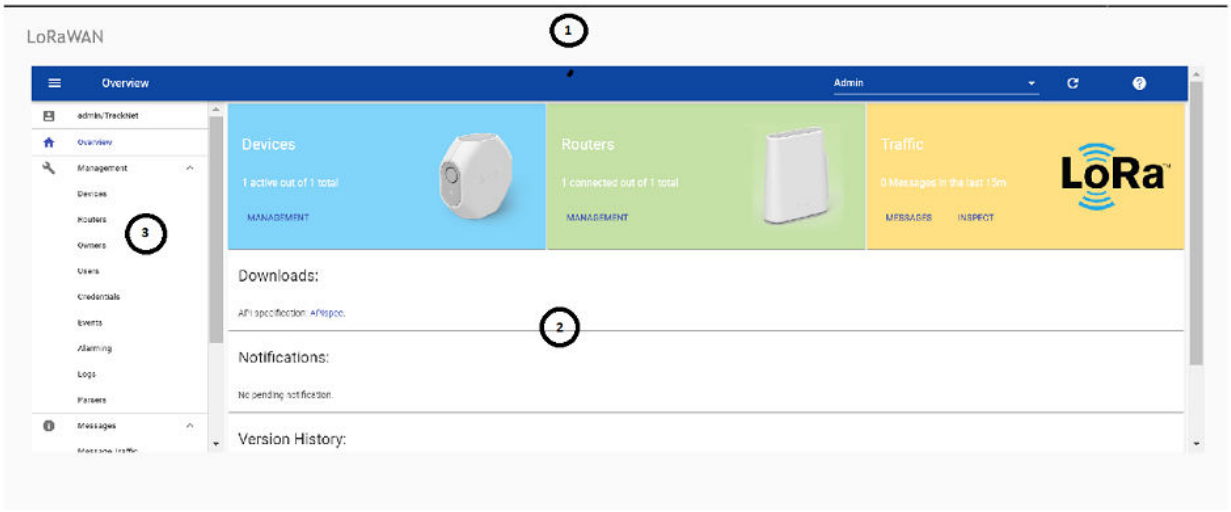
2. Enter the login credentials and click **Submit**.

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

LoRaWAN Dashboard

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

FIGURE 71 LoRaWAN Dashboard



1. Header Panel
2. Main Control Panel
3. Navigation Bar

The following table describes the components of the LoRaWAN dashboard.

TABLE 6 Identifying the Various Components of the LoRaWAN Dashboard

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

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

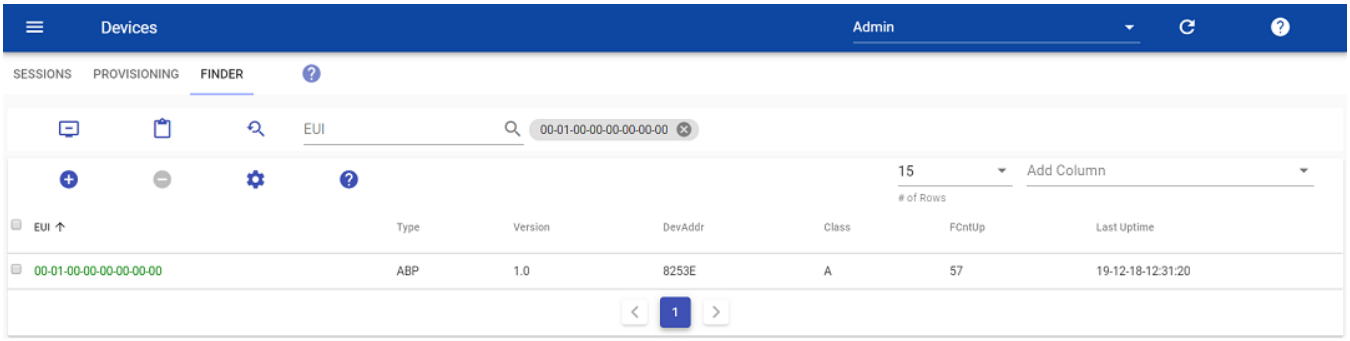
Name	Components
Main Content Panel	Consists of the following components: • Devices: Displays the count of LoRa devices connected to the LNS. **NOTE** If you click **Management** , the **Devices** page is displayed with more information about the devices. • Routers: Displays the count of LoRa routers connected to LNS. If you click **Management**, the **Routers** page is displayed with more information about the routers. • Traffic: Displays the traffic in the network. **NOTE** If you click **Message**, the **Message traffic** page is displayed. If you click **Inspect**, the **Watchboard** page is displayed. • Downloads: Allows you to download API specification files. • Notifications: Displays the notifications. • Version History: Displays the version history of LoRa Network Server (LNS).

Configuring LoRa Devices

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

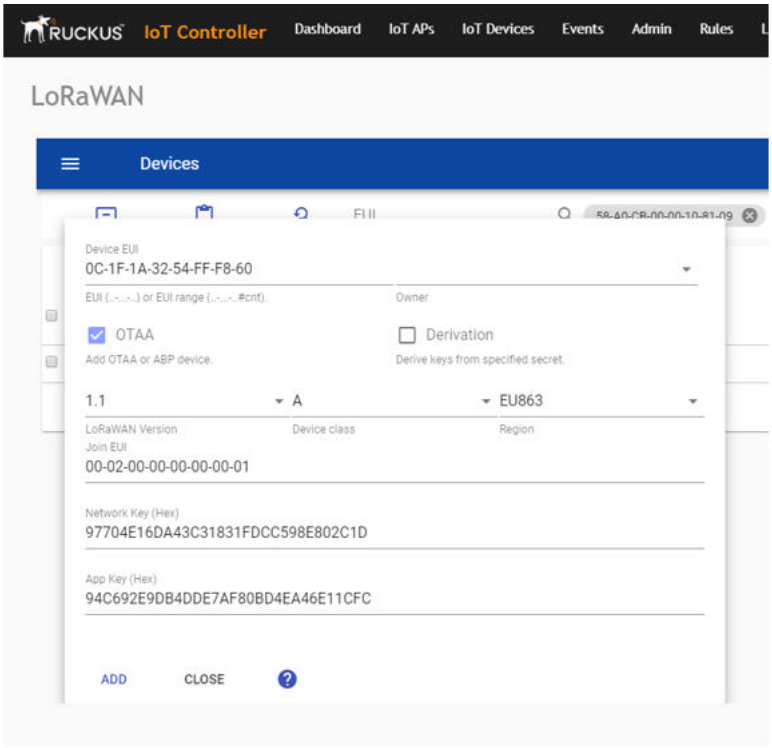
1. On the **Devices** page, click  to provision the device.

FIGURE 72 Configuring LoRa Devices



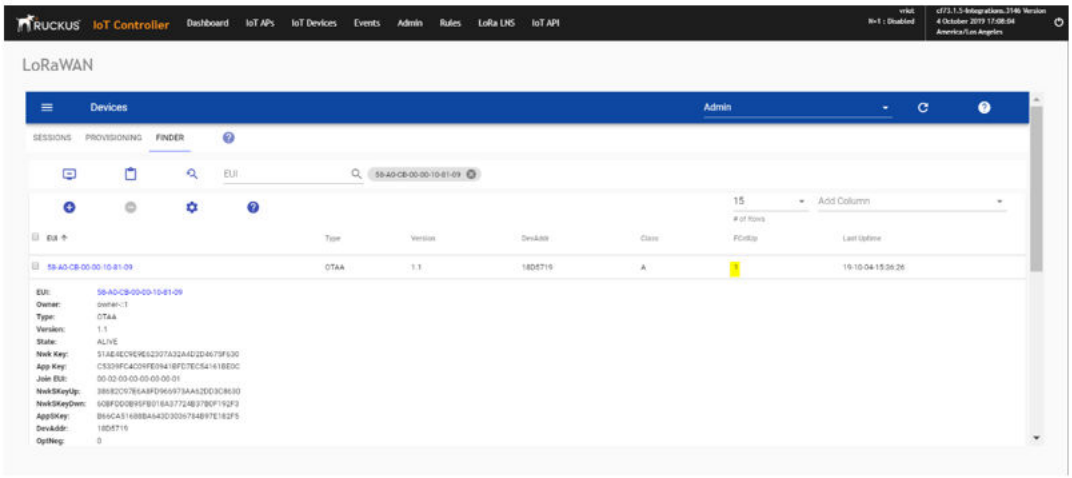
The following example shows the configuration of the device Semtech TBDW100 Door/Window Sensor device. Different devices have different ways to configure the gateway to communicate with the LNS of the Ruckus IoT Controller.

FIGURE 73 Provisioning the Device



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

FIGURE 74 Device Joining the LNS



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

Configuring LoRaWAN Routers

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

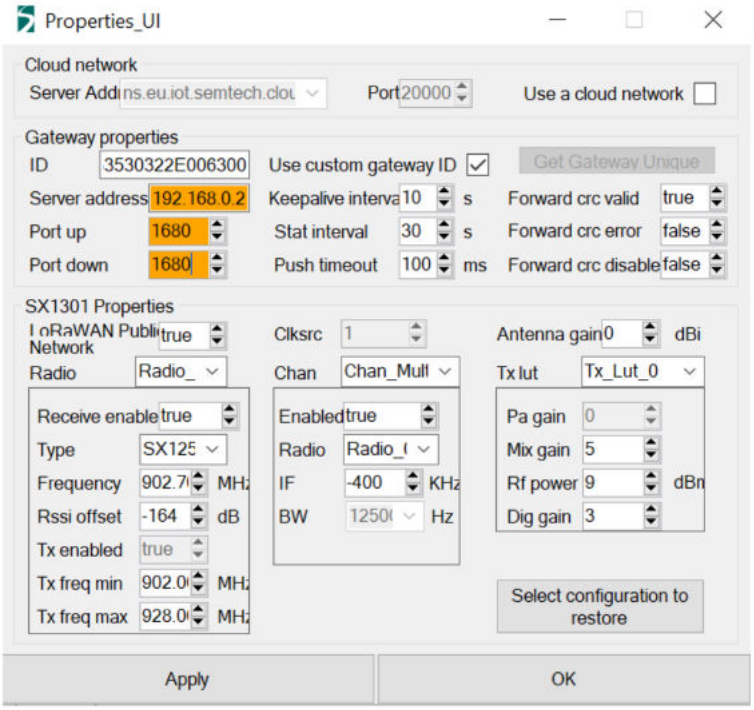
Complete the following steps to configure the Semtech LoRa Picocell Gateway to communicate with the LoRa Network Server (LNS) in the Ruckus IoT Controller.

NOTE
Different routers have different ways of provisioning the gateway.

Preparing the Semtech LoRa Picocell Gateway

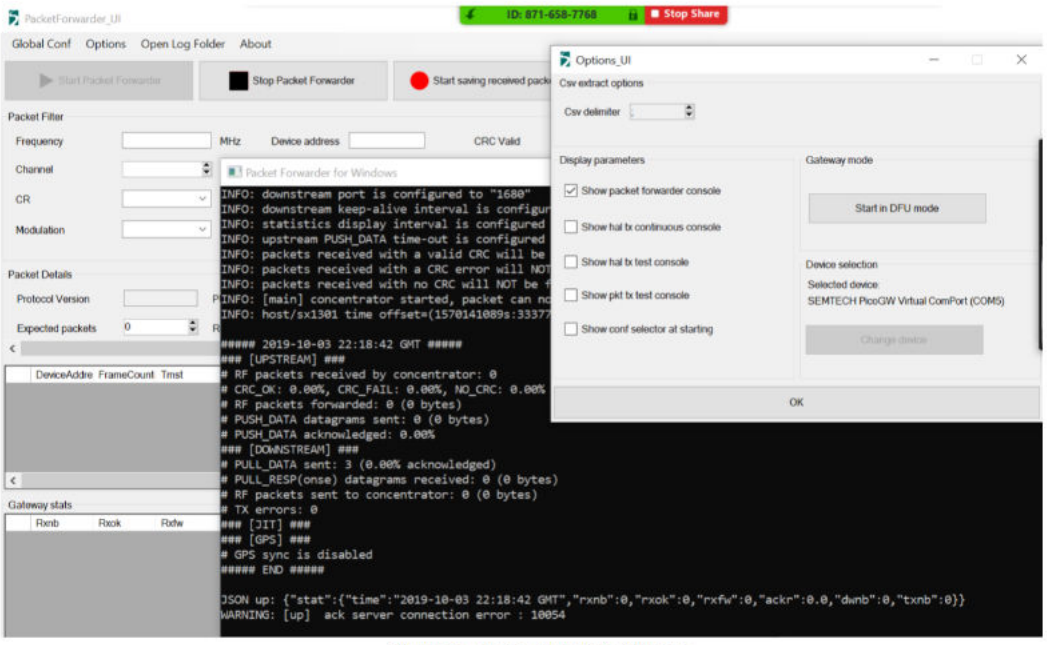
1. Load PicoGW_UI_Release_V1.0.3.4 and run **Setup**.
2. In the **Properties_UI** dialog box, address the following options:
   - Select the **Use a cloud network** check box.
   - Click **Get Gateway Unique**.
   - Select the **Use custom gateway ID** check box.
   - Copy the ID to the copy buffer to use later in the process.
   - Change the **Server address** to the IP address of the TrackCentral LNS.
   - Set **Port up** and **Port down** to **1680**.
   - For **Tx lut**, select **Tx_Lut_15** and set the **Rf power** to **30** dBm (to allow the end device to join the ACK TX).

FIGURE 75 Configuring the LoRa Picocell Gateway



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

FIGURE 76 Starting Packet Forwarder

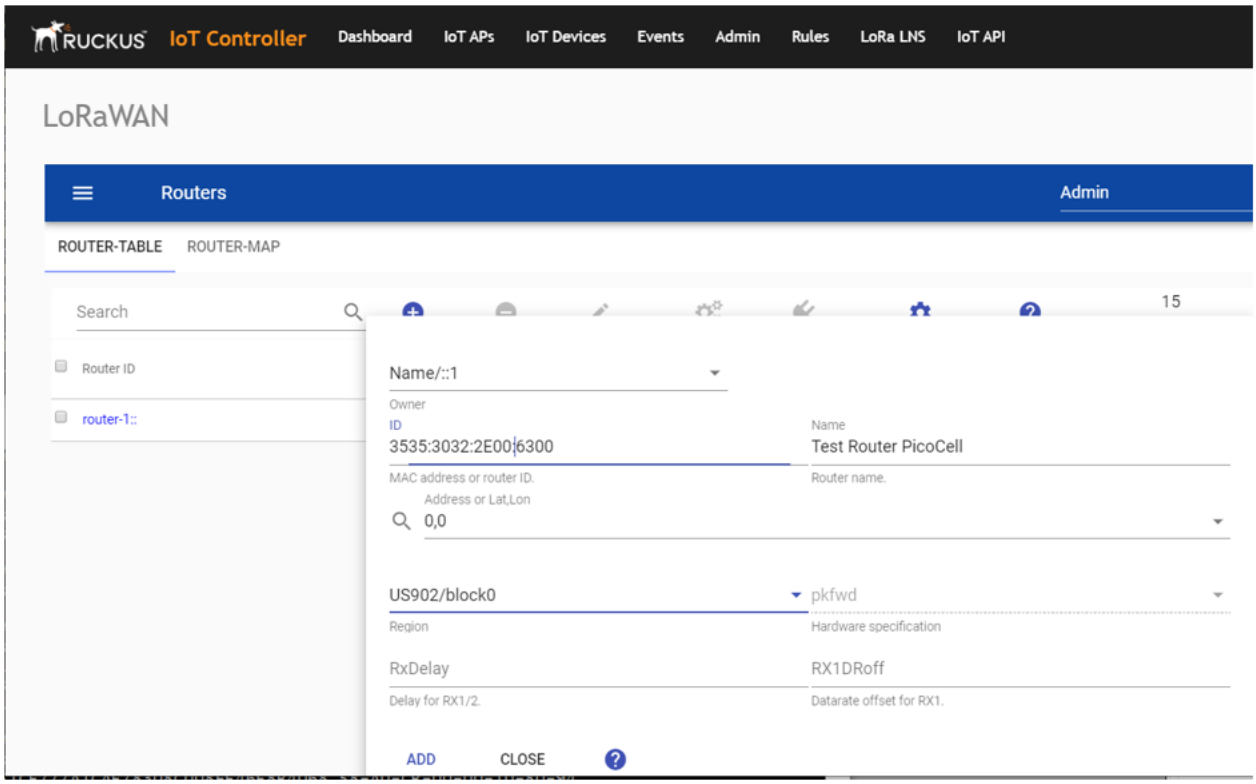


Configuring the Semtech LoRa Picocell Gateway as a Router in the LNS

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

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

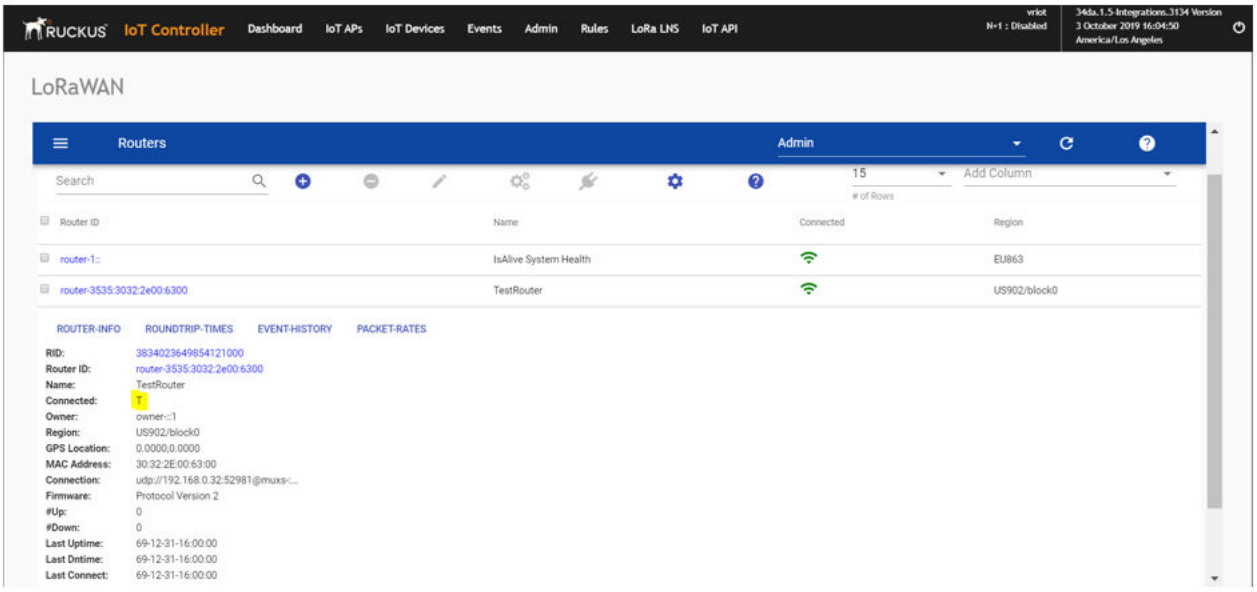
FIGURE 77 Configuring the Router



2. Click **ADD**.

   The router is added to the LNS.

   FIGURE 78 Adding the Router to the LNS



Events

Viewing Events

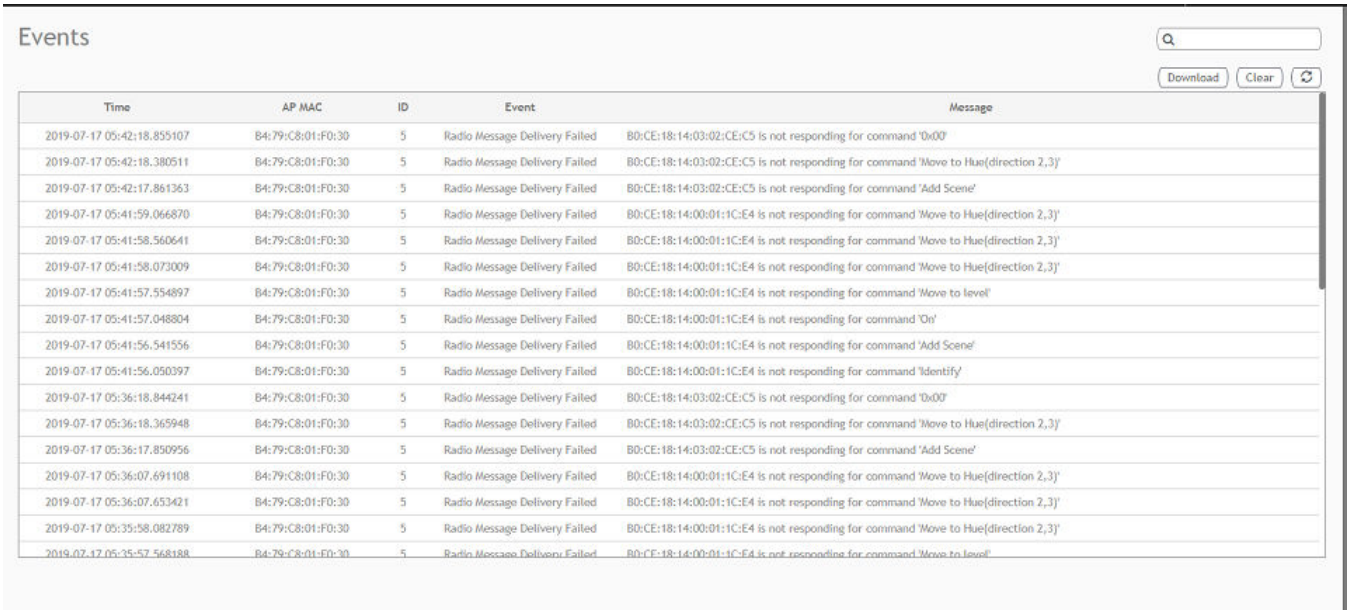
An event is an occurrence or the detection of certain conditions in and around the Ruckus IoT Module. An AP rebooting, detection of a Ruckus IoT Module, module undetection, and module swap are all examples of events.

Complete the following steps to view events.

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

   The **Events** page is displayed.

   FIGURE 79 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.

COMMSCOPE®
RUCKUS®

350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com