

RUCKUS IoT Controller Configuration Guide, 2.0.0.0

Supporting IoT Controller Release 2.0.0.0

Copyright, Trademark and Proprietary Rights Information

© 2021 CommScope, Inc. All rights reserved.

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

Export Restrictions

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

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

Disclaimer

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

Limitation of Liability

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

Trademarks

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

Contents

Preface	5
Contacting RUCKUS Customer Services and Support.....	5
What Support Do I Need?.....	5
Open a Case.....	5
Self-Service Resources.....	6
Document Feedback.....	6
RUCKUS Product Documentation Resources.....	6
Online Training Resources.....	6
Document Conventions.....	7
Notes, Cautions, and Safety Warnings.....	7
Command Syntax Conventions.....	7
About This Guide	9
Introduction to RUCKUS IoT Controller.....	9
What's New in This Document.....	9
Getting Started	11
Before You Begin.....	11
Supported Web Browsers.....	11
Logging In to RUCKUS IoT Controller.....	11
Getting to Know the Dashboard.....	15
Configuring N+1	19
Configuring Static Addresses for Primary and Secondary Controllers.....	19
Configuring the N+1 Feature.....	19
Disabling N+1	33
Managing IoT Controller System Configuration	35
Managing Services.....	35
Enabling Samsung SmartThings.....	36
Activating and Editing the Plugins.....	44
Activating and Editing the Kontakt.io Beacons Plugin.....	44
Activating and Editing the Assa Abloy Plugin.....	47
Activating and Editing the Eddystone Plugin.....	48
Activating and Editing the iBeacon Plugin.....	52
Activating and Editing the Beacon as a Service Plugin (iBeacon, Eddystone and Custom).....	55
Activating and Editing the Beacon as a Service Plugin (React Mobile).....	60
Activating and Editing the BLE Scan Plugin.....	61
Activating and Editing the Controller Data Stream Plugin.....	64
Activating and Editing the Dormakaba Plugin.....	66
Activating and Editing the Telkonet Plugin.....	68
Activating and Editing the Soter Plugin.....	71
Changing the Password.....	73
Configuring Virtual Machines.....	73
Uploading Versions and Patches.....	74
Uploading an Image.....	74
Uploading a Patch.....	76
Backing Up Files.....	77

Backing up Rules.....	78
Uploading the RUCKUS IoT Controller License.....	79
Change the Settings.....	81
Rebooting RUCKUS IoT Controller.....	83
Resetting RUCKUS IoT Controller.....	83
Managing IoT Access Points.....	85
IoT AP Overview.....	85
DHCP Option 43.....	85
RUCKUS Command Line Interface.....	86
USB Power.....	86
Adding an IoT AP.....	88
Editing an IoT AP.....	90
Single IoT Access Point Mode.....	91
Adding Tags to an AP.....	92
Approval of IoT APs.....	94
Exporting IoT APs to CSV.....	94
Enabling BaaS Major and Minor Number.....	94
Managing Devices.....	97
Devices Overview.....	97
Managing OSRAM Light Bulbs.....	100
Managing an Assa Abloy Lock.....	101
Managing the Dormakaba Locks.....	102
Discovering Dormakaba Lock.....	103
Blocking and Unblocking Dormakaba Lock.....	104
Blocking the Key Remotely.....	108
Unblocking the Key Remotely.....	112
Device Operations for Specific Clusters and Commands.....	114
Rules Engine.....	117
Rules Engine Overview.....	118
Configuring Rules.....	118
Rules-Dashboard.....	119
Events.....	121
Viewing Events.....	121

Preface

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

Contacting RUCKUS Customer Services and Support

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

For product support information and details on contacting the Support Team, go directly to the RUCKUS Support Portal using <https://support.ruckuswireless.com>, or go to <https://www.commscope.com/ruckus> 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/>
- Knowledge Base Articles—<https://support.ruckuswireless.com/answers>
- Software Downloads and Release Notes—https://support.ruckuswireless.com/#products_grid
- Security Bulletins—<https://support.ruckuswireless.com/security>

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

Document Feedback

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

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

When contacting us, include the following information:

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

For example:

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

RUCKUS Product Documentation Resources

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

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

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

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://commscopeuniversity.myabsorb.com/>. The registration is a two-step process described in this [video](#). You create a CommScope account and then register for, and request access for, CommScope University.

Document Conventions

The following table lists the text conventions that are used throughout this guide.

TABLE 1 Text Conventions

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

Notes, Cautions, and 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.
<i>italic text</i>	Identifies a variable.
[]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{x y z}	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x y	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, <i>member[member...]</i> .
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

About This Guide

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

Introduction to RUCKUS IoT Controller

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

This guide is 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 2.0.0.0 GA

Feature	Description	Location
The support for LoRaWAN is removed.	-	-
Introduction to new license scheme.	Provides support for subscription based model licenses.	Refer to Uploading the RUCKUS IoT Controller License on page 79
Minor updates across the document.	This update includes replacing images wherever required.	-

Getting Started

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

Before You Begin

The RUCKUS IoT Controller must be installed on a hypervisor.

Supported Web Browsers

The RUCKUS IoT Controller is primarily accessible using a web browser.

TABLE 3 Supported Web Browser Versions

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

Logging In to RUCKUS IoT Controller

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

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

Getting Started

Logging In to RUCKUS IoT Controller

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

FIGURE 1 RUCKUS IoT Controller Main Menu

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

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

Enter Choice: 1

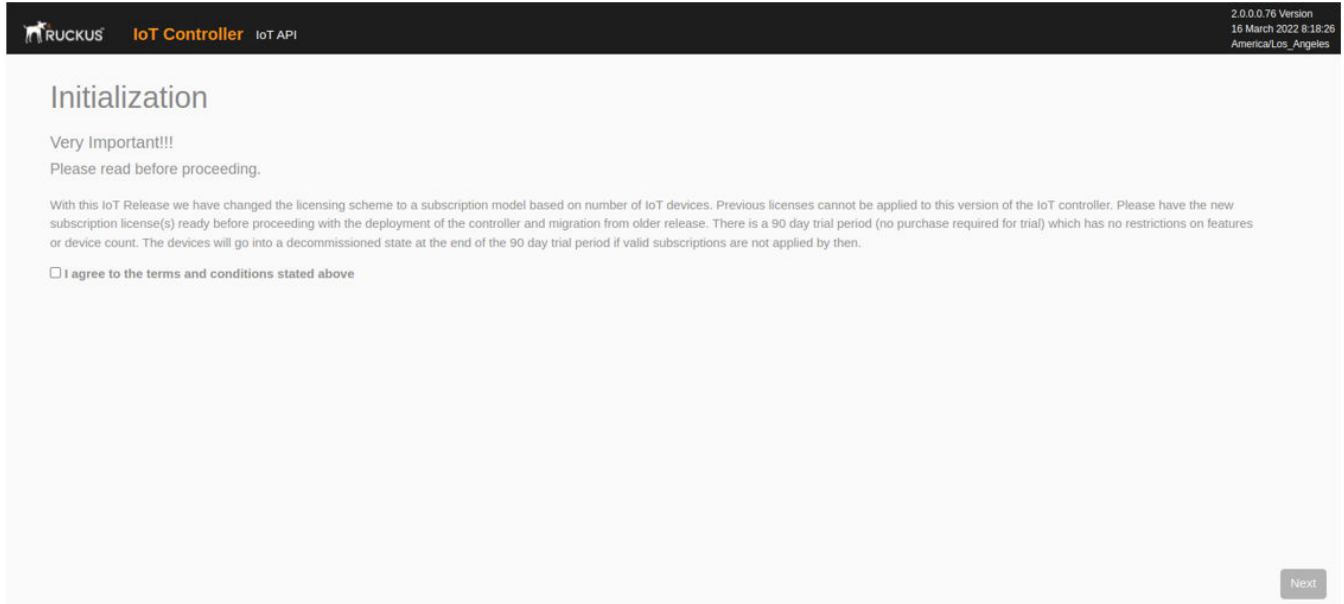
-----
Network info :
-----
IP (enp0s17) : 192.168.0.48/24
Gateway      : 192.168.0.1
Hostname     : vriot
DNS domain   :
FQDN        : vriot
DNS         : 192.168.0.1
N+1 Status  : Disabled
-----

Set Network(1) or Exit(x). Select [1/x]:
```

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

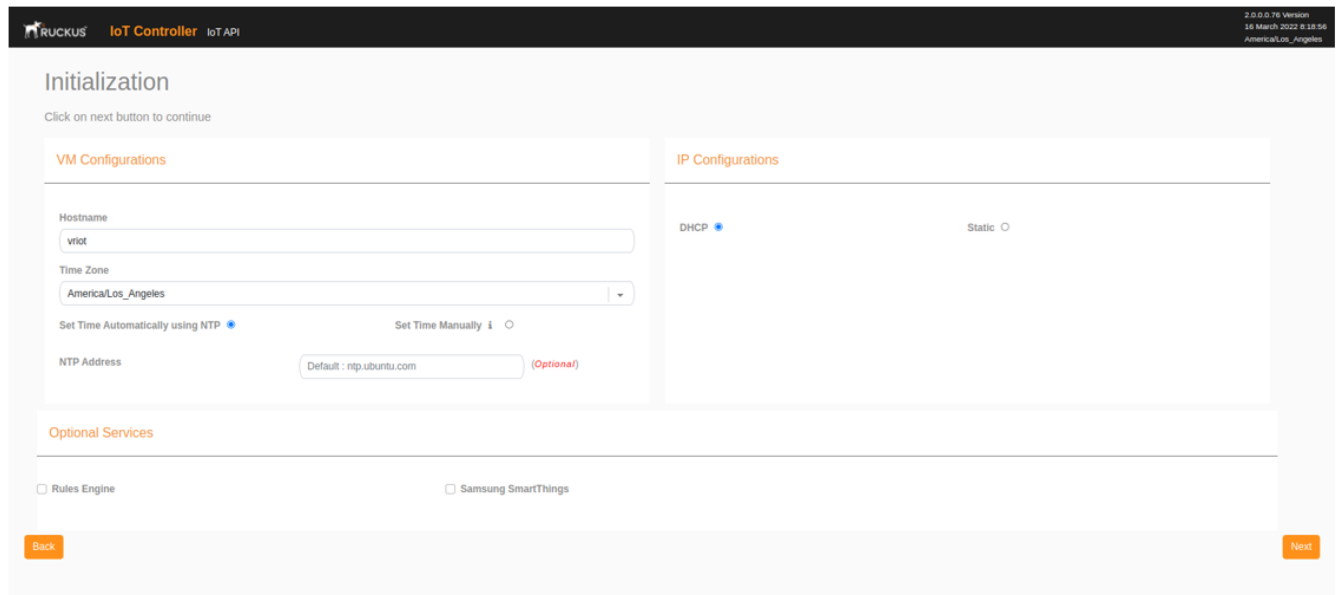
The **Initialization** page is displayed.

FIGURE 2 Accepting Subscription Based Licensing



Select the **I agree to terms and conditions stated above** and click **Next**.

FIGURE 3 Initialization Page



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

- Rules Engine

Getting Started

Logging In to RUCKUS IoT Controller

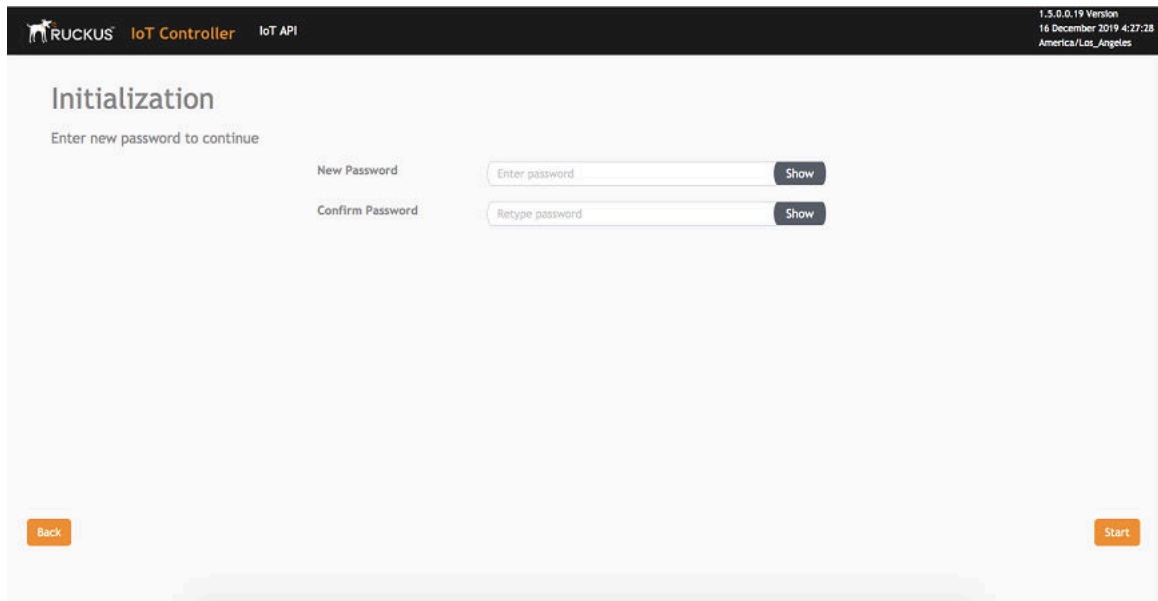
- Smasung SmartThings

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

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

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

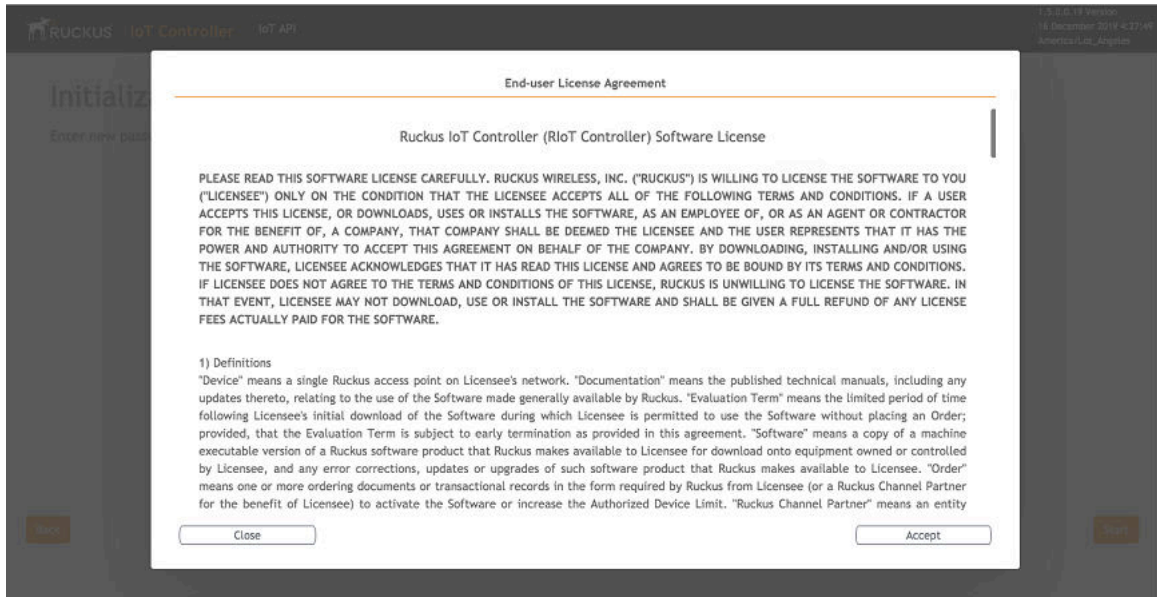
FIGURE 4 Confirming the Password



The screenshot shows the 'Initialization' page of the RUCKUS IoT Controller. The page title is 'Initialization' and the subtitle is 'Enter new password to continue'. There are two input fields: 'New Password' with the placeholder text 'Enter password' and 'Confirm Password' with the placeholder text 'Retype password'. Each input field has a 'Show' button to its right. At the bottom left, there is a 'Back' button, and at the bottom right, there is a 'Start' button. The top navigation bar includes the RUCKUS logo, 'IoT Controller', and 'IoT API'. The top right corner displays version information: '1.5.0.0.19 Version', '16 December 2019 4:27:28', and 'America/Los_Angeles'.

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

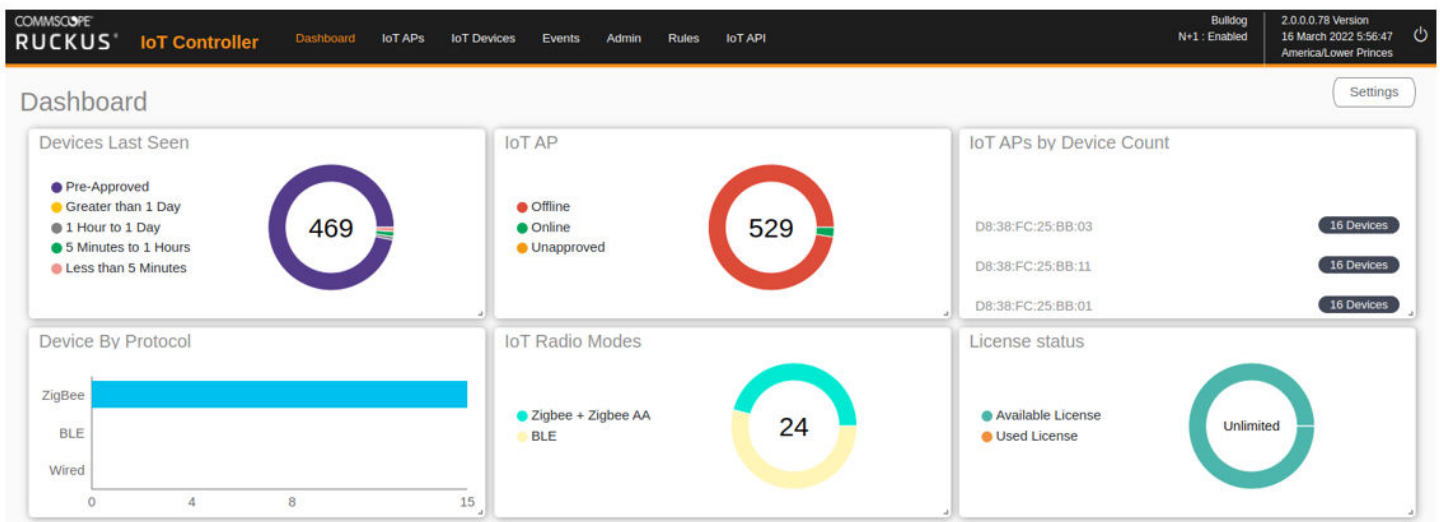
FIGURE 5 End-user License Agreement



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



Getting Started

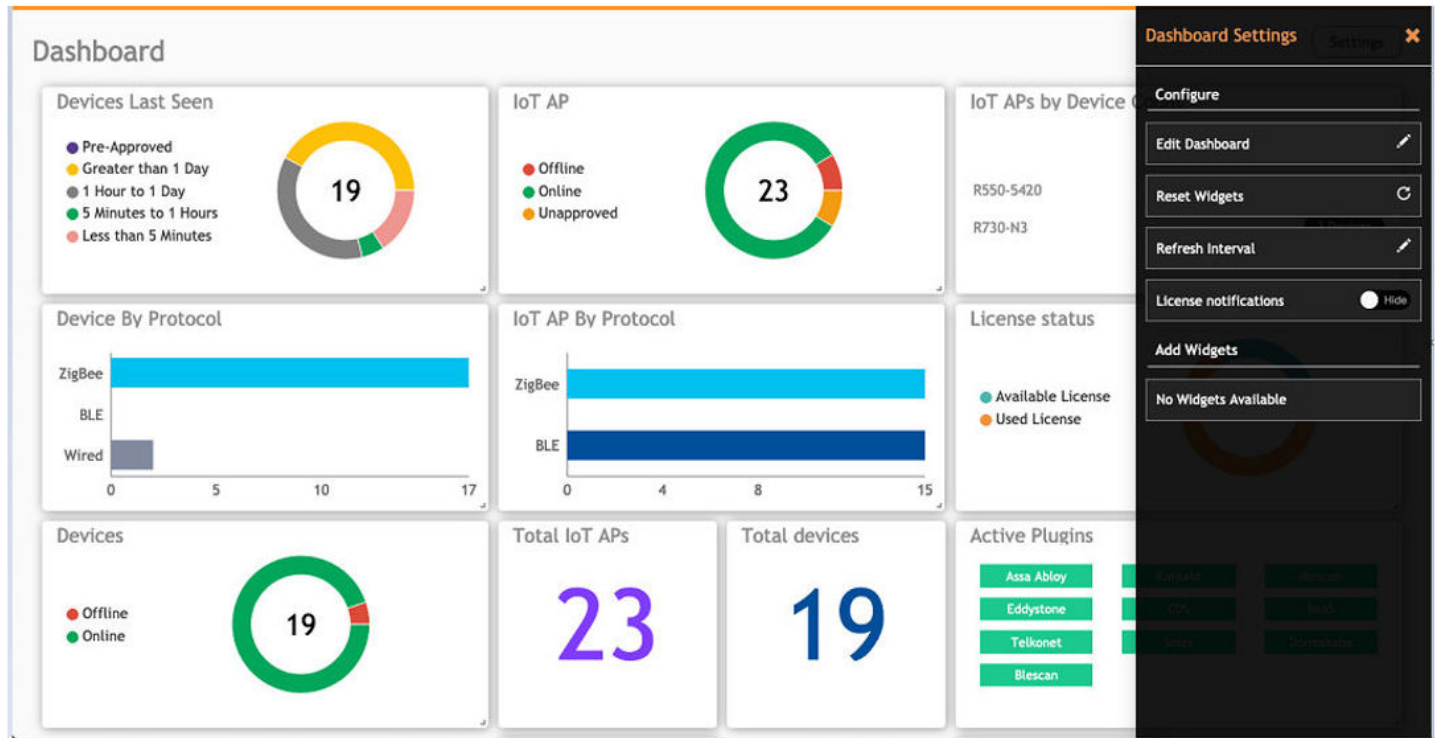
Getting to Know the Dashboard

TABLE 4 Dashboard Elements



Box Name	Description
Devices Last seen	Shows the total number of devices last seen.
IoT APs By Device Count	Shows the total number of devices connected per Access Point.
Total Devices	Shows the total number of devices.
Total IoT APs	Shows the total number of Access Points.
Total Beacons	Shows the total number of Beacons.
Devices	Shows the status of devices that are connected to the RUCKUS IoT Controller.
Devices by Battery Level	Shows the status of devices that are grouped together by battery level.
Active Plugins	Shows the plugins that are enabled.
IoT AP	Shows the status of Access Points that are connected to the RUCKUS IoT Controller.
Device By Protocol	Shows the total number of devices connected by the protocol being used. RUCKUS supports two protocols: BLE and Zigbee.
IoT Radio Modes	Shows the number of APs-Radios running by the protocol being used. RUCKUS supports two protocols: BLE and Zigbee.
License status	Shows the total of number of licenses, and the status of the licenses that are available or used by the RUCKUS IoT Controller.

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

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

Configuring N+1

- [Configuring Static Addresses for Primary and Secondary Controllers.....](#) 19
- [Configuring the N+1 Feature.....](#) 19

RUCKUS IoT Controller N+1 high availability (HA) ensures high system availability, reliability and scalability of the controller, and also enables load balancing, backup, and failover. The hosts must be in the same subnet and must be reachable which allows virtual machines (VMs) on a given host to fail over to another host without any downtime in the event of a failure.

Before beginning to use N+1, pay attention to the following prerequisites for configuring the primary and secondary controllers:

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

Configuring Static Addresses for Primary and Secondary Controllers

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

1. From the RUCKUS IoT Controller main menu, select **Admin > VM Configurations**.
2. Set the static addresses of the primary and secondary controller on the **Initialization** page. Refer to [Logging In to RUCKUS IoT Controller](#) on page 11.

Configuring the N+1 Feature

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

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

Configuring N+1

Configuring the N+1 Feature

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

FIGURE 8 RUCKUS IoT Controller Main Menu

```
172.16.112.243 - PuTTY
*****
Ruckus IoT Controller
Main Menu
*****
1 - Ethernet Network
2 - System Details
3 - NTP Setting
4 - System Operation
5 - N+1
6 - Comm Debugger
x - Log Off

Enter Choice: 5

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

N+1 Configure(1) / Disable(2) / Exit(x) :1
Start Primary Controller(1) / Secondary Controller(2) / Exit(x) :1

-----
N+1 Configure:
-----
To Configure N+1 ensure following requirements:
*****
* Primary Controller and Secondary Controller should be in same subnet and reachable.
* Primary Controller and Secondary Controller should be configured with static ip address.
* Primary Controller and Secondary Controller should be running in same version.
* Primary Controller and Secondary Controller should have synchronized date/time.
* Primary Controller and Secondary Controller should have same password configured for the User admin.

Enter Secondary Controller IP :█
```

3. Enter 1 to continue the configuration.

FIGURE 9 Continuing the Configuration

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

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

Enter Choice: 5

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

N+1 Configure(1) / Disable(2) / Exit(x) :1
Start Primary Controller(1) / Secondary Controller(2) / Exit(x) :█
```

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

FIGURE 10 Configuring the Primary Controller

```
172.16.112.243 - PuTTY
Ruckus IoT Controller
Main Menu
-----
1 - Ethernet Network
2 - System Details
3 - NTP Setting
4 - System Operation
5 - N+1
6 - Comm Debugger
x - Log Off

Enter Choice: 5

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

N+1 Configure(1) / Disable(2) / Exit(x) :1
Start Primary Controller(1) / Secondary Controller(2) / Exit(x) :1

-----
N+1 Configure:
-----
To Configure N+1 ensure following requirements:
-----
* Primary Controller and Secondary Controller should be in same subnet and reachable.
* Primary Controller and Secondary Controller should be configured with static ip address.
* Primary Controller and Secondary Controller should be running in same version.
* Primary Controller and Secondary Controller should have synchronized date/time.
* Primary Controller and Secondary Controller should have same password configured for the User admin.

Enter Secondary Controller IP : █
```

Configuring N+1

Configuring the N+1 Feature

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

NOTE

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

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

```
172.16.113.178 - PuTTY
.....
Ruckus IoT Controller
Main Menu
.....
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 Primary Controller(1) / Secondary Controller(2) / Exit(x) :1
-----
N+1 Configure:
-----
To Configure N+1 ensure following requirements:
*****
* Primary Controller and Secondary Controller should be in same subnet and reachable.
* Primary Controller and Secondary Controller should be configured with static ip address.
* Primary Controller and Secondary Controller should be running in same version.
* Primary Controller and Secondary Controller should have synchronized date/time.
* Primary Controller and Secondary Controller should have same password configured for the User admin.

Enter Secondary Controller IP :172.16.113.102
Enter preferred Virtual IP :171.16.113.111
Enter admin password for configuring N+1:

Enter new password for configuring N+1
New password should contain atleast 1 uppercase, 1 number , 1 Symbol and atleast 8 characters length
:

N+1 will stop all services & configurations in Secondary Controller. Enter Y/N to continue : █
```

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

FIGURE 11 Completing the Primary Controller Configuration

```
172.16.113.178 - PuTTY
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 Primary Controller(1) / Secondary Controller(2) / Exit(x) :1
-----

N+1 Configure:
-----
To Configure N+1 ensure following requirements:
*****
* Primary Controller and Secondary Controller should be in same subnet and reachable.
* Primary Controller and Secondary Controller should be configured with static ip address.
* Primary Controller and Secondary Controller should be running in same version.
* Primary Controller and Secondary Controller should have synchronized date/time.
* Primary Controller and Secondary Controller should have same password configured for the User admin.

Enter Secondary Controller IP :172.16.113.102
Enter preferred Virtual IP :172.16.113.111
Enter admin password for configuring N+1:

Enter new password for configuring N+1
New password should contain atleast 1 uppercase, 1 number , 1 Symbol and atleast 8 characters length
:

N+1 will stop all services & configurations in Secondary Controller. Enter Y/N to continue : Y

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

After configuring the primary controller, the configuration of secondary controller begins.

FIGURE 12 Continuing with the Secondary Controller Configuration

```
172.16.113.178 - PuTTY
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 Primary Controller(1) / Secondary Controller(2) / Exit(x) :1
-----
N+1 Configure:
-----
To Configure N+1 ensure following requirements:
*****
* Primary Controller and Secondary Controller should be in same subnet and reachable.
* Primary Controller and Secondary Controller should be configured with static ip address.
* Primary Controller and Secondary Controller should be running in same version.
* Primary Controller and Secondary Controller should have synchronized date/time.
* Primary Controller and Secondary Controller should have same password configured for the User admin.

Enter Secondary Controller IP :172.16.113.102
Enter preferred Virtual IP :172.16.113.111
Enter admin password for configuring N+1:

Enter new password for configuring N+1
New password should contain atleast 1 uppercase, 1 number , 1 Symbol and atleast 8 characters length
:

N+1 will stop all services & configurations in Secondary Controller. Enter Y/N to continue : Y

Configuring takes around 5-10 minutes. Please wait
Primary Controller configuration started..
Secondary Controller configuration started..
```

FIGURE 13 N+1 Configuration Completed

```
172.16.113.178 - PuTTY
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 Primary Controller(1) / Secondary Controller(2) / Exit(x) :1
-----
N+1 Configure:
-----
To Configure N+1 ensure following requirements:
*****
* Primary Controller and Secondary Controller should be in same subnet and reachable.
* Primary Controller and Secondary Controller should be configured with static ip address.
* Primary Controller and Secondary Controller should be running in same version.
* Primary Controller and Secondary Controller should have synchronized date/time.
* Primary Controller and Secondary Controller should have same password configured for the User admin.

Enter Secondary Controller IP :172.16.113.102
Enter preferred Virtual IP :172.16.113.111
Enter admin password for configuring N+1:

Enter new password for configuring N+1
New password should contain atleast 1 uppercase, 1 number , 1 Symbol and atleast 8 characters length
:

N+1 will stop all services & configurations in Secondary Controller. Enter Y/N to continue : Y

Configuring takes around 5-10 minutes. Please wait
Primary Controller configuration started..
Secondary Controller configuration started..
Configuring N+1 completed...
-----
```


You have configured N+1 successfully.

7. To verify the IP addresses of the primary controller or active primary controller, and the secondary controller or active secondary controller, enter **5** in the **Enter Choice** field.

FIGURE 14 Verifying the IP Address of the Active Primary Controller

```
172.16.113.178 - PuTTY
*****
                        Ruckus IoT Controller
                        Main Menu
*****

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

Enter Choice: 5

-----
N+1 Status:
-----
      N+1 Mode       : Enabled
      Virtual IP     : 172.16.113.111
      Mode           : Active Primary Controller
      My IP          : 172.16.113.178
      Secondary Controller IP : 172.16.113.102
      ConfigSync     : Not Applicable, Controller is Active.
      Node Status    : vriot(2): normal
vriot_prim(1): normal
-----

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

Configuring N+1

Configuring the N+1 Feature

- To replace the secondary controller, enter 3.

NOTE

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

FIGURE 15 Replacing the IP Address of Secondary Controller

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

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

Enter Choice: 5

-----
N+1 Status:
-----
      N+1 Mode       : Enabled
      Virtual IP     : 10.174.113.180
      Mode           : Active Primary Controller
      My IP          : 10.174.113.173
      Secondary Controller IP : 10.174.113.177
      ConfigSync     : Not Applicable, Controller is Active.
      Node Status    : vriot-shriram-151020-esx138(1): normal
vriot-shriram-151020-slave-es138(2): normal(offline)
-----

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

FIGURE 16 Successful Completion of Replacing the Node

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

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

[Enter Choice: 5

-----
N+1 Status:
-----
      N+1 Mode       : Enabled
      Virtual IP     : 10.174.113.180
      Mode           : Active Primary Controller
      My IP          : 10.174.113.173
      Secondary Controller IP      : 10.174.113.177
      ConfigSync     : Not Applicable, Controller is Active.
      Node Status    : vriot-shriram-151020-esx138(1): normal
                    vriot-shriram-151020-slave-es138(2): normal(offline)
-----

[N+1 Configure(1) / Disable(2) / Replace Secondary Controller(3) / Exit(x) :3
-----
N+1 Replace :
-----
[ Enter Secondary Controller IP to replace:10.174.113.172
Deleted nodes
█
```

Configuring N+1

Configuring the N+1 Feature

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

FIGURE 17 Configuring Forced Fallback

```
172.16.113.178 - PuTTY
*****
                        Ruckus IoT Controller
                        Main Menu
*****

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

Enter Choice: 5

-----
N+1 Status:
-----
      N+1 Mode       : Enabled
      Virtual IP     : 172.16.113.111
      Mode           : Primary Controller
      My IP          : 172.16.113.178
      Secondary Controller IP : 172.16.113.102
      ConfigSync     : 05/20/2021 08:05:03
      Node Status    : vriot(2): normal
vriot_prim(1): normal
-----

N+1 Configure(1) / Disable(2) / Forced Fallback(3) / Exit(x) : █
```

10. To replace the primary controller, enter 3.

FIGURE 18 Replacing the Primary Controller

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

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

[Enter Choice: 5

-----
N+1 Status:
-----
      N+1 Mode      : Enabled
      Virtual IP    : 10.174.113.180
      Mode          : Active Secondary Controller
      My IP         : 10.174.113.172
      Primary Controller IP : ["10.174.113.173"]
      ConfigSync    : Not Applicable, Controller is Active.
      Node Status   : vriot-shriram-151020-es15-slave2(2): normal
vriot-shriram-151020-esx138(1): normal(offline)
-----

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

Configuring N+1

Configuring the N+1 Feature

11. Enter the IP address of the primary controller.

FIGURE 19 Continuing with Replacing the Primary Controller

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

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

[Enter Choice: 5

-----
N+1 Status:
-----
      N+1 Mode       : Enabled
      Virtual IP     : 10.174.113.180
      Mode           : Active Secondary Controller
      My IP          : 10.174.113.172
      Primary Controller IP : ["10.174.113.173"]
      ConfigSync     : Not Applicable, Controller is Active.
      Node Status    : vriot-shriram-151020-es15-slave2(2): normal
vriot-shriram-151020-esx138(1): normal(offline)
-----

[N+1 Configure(1) / Disable(2) / Replace Primary Controller(3) / Exit(x) :3
-----
N+1 Replace :
-----
      Enter Primary Controller IP to replace:10.174.113.177
```

Replacing the primary controller has been successfully completed.

FIGURE 20 Successful Completion of Replacing the Primary Controller

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

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

[Enter Choice: 5

-----
N+1 Status:
-----
      N+1 Mode      : Enabled
      Virtual IP    : 10.174.113.180
      Mode          : Active Secondary Controller
      My IP         : 10.174.113.172
      Primary Controller IP : ["10.174.113.173"]
      ConfigSync    : Not Applicable, Controller is Active.
      Node Status   : vriot-shriram-151020-es15-slave2(2): normal
vriot-shriram-151020-esx138(1): normal(offline)
-----

[N+1 Configure(1) / Disable(2) / Replace Primary Controller(3) / Exit(x) :3
-----
N+1 Replace :
-----
[ Enter Primary Controller IP to replace:10.174.113.177
  Error: N+1 is already enabled!
Deleted nodes
  Start replacing master
  Secondary Controller configuration started..
Replace node taking more time to start services
Replacing node completed
-----
█
```


Disabling N+1

Complete the following steps to disable N+1 configuration.

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

FIGURE 21 Disabling the N+1 Configuration

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

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

[Enter Choice: 5

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

      N+1 Mode       : Enabled
      Virtual IP    : 10.174.113.180
      Mode          : Active Primary Controller
      My IP         : 10.174.113.173
      Secondary Controller IP : 10.174.113.172
      ConfigSync    : Not Applicable, Controller is Active.
      Node Status   : vriot-shriram-151020-es15-slave1(2): normal
vriot-shriram-151020-esx138(1): normal
-----

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

N+1 Disable :
-----

      Secondary Controller 10.174.113.172 will be reset.
      Disable N+1 completed...
-----

█
```

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

NOTE

After the N+1 configuration is disabled from the active primary controller, the secondary controller resets automatically.

Managing IoT Controller System Configuration

- Managing Services..... 35
- Activating and Editing the Plugins..... 44
- Changing the Password..... 73
- Configuring Virtual Machines..... 73
- Uploading Versions and Patches..... 74
- Backing Up Files..... 77
- Backing up Rules..... 78
- Uploading the RUCKUS IoT Controller License..... 79
- Change the Settings..... 81
- Rebooting RUCKUS IoT Controller..... 83
- Resetting RUCKUS IoT Controller..... 83

Managing Services

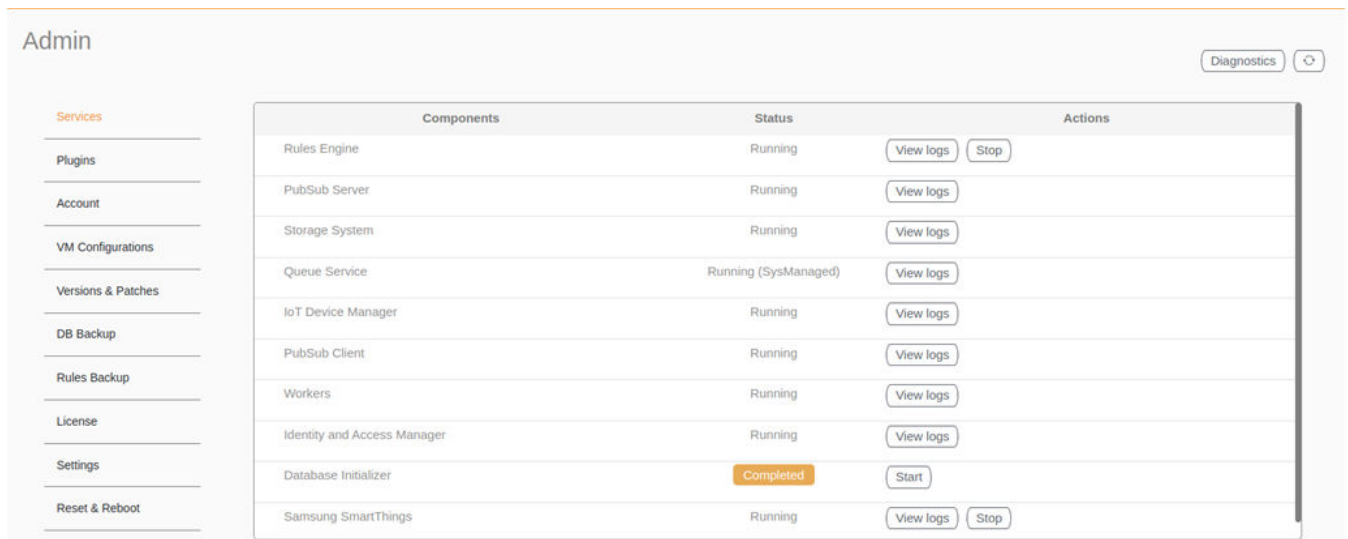
The administrator can restart or manage the mandatory and optional services.

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 22 Services

FIGURE 23 Managing Services Page



The currently running services and their details are displayed.

3. Select a service to start or stop.

Enabling Samsung SmartThings

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


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

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

NOTE

By default SmartThings is disabled.

FIGURE 24 Starting Samsung SmartThings

Components	Status	Actions
Rules Engine	Stopped	Start
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
Samsung SmartThings	Stopped	Start 

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

FIGURE 25 SmartThing Device



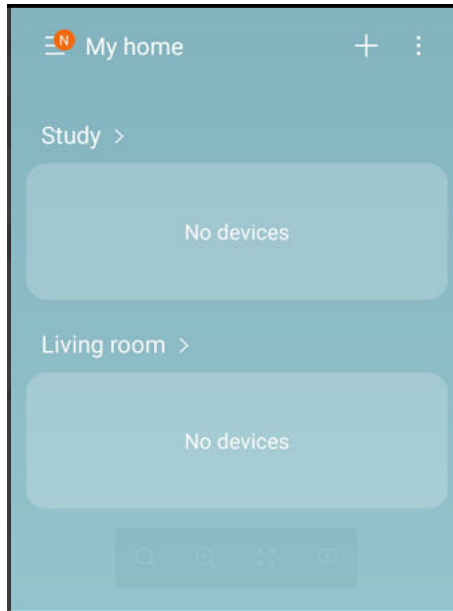
NOTE

For more information on upgrade events, refer [#unique_26](#).

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

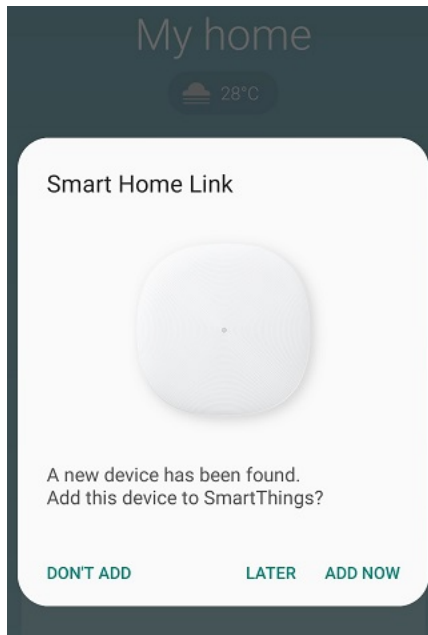
6. Connect your mobile and AP in the same network or connect the mobile to the SSID of the AP.

FIGURE 26 SmartThings User Interface



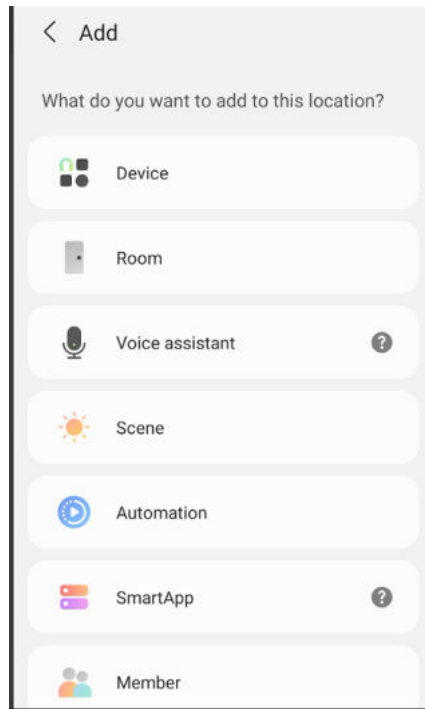
7. After the mobile device connects to Wi-Fi, click **ADD NOW** in the SmartThings device pop-up.

FIGURE 27 Connecting to Wi-Fi



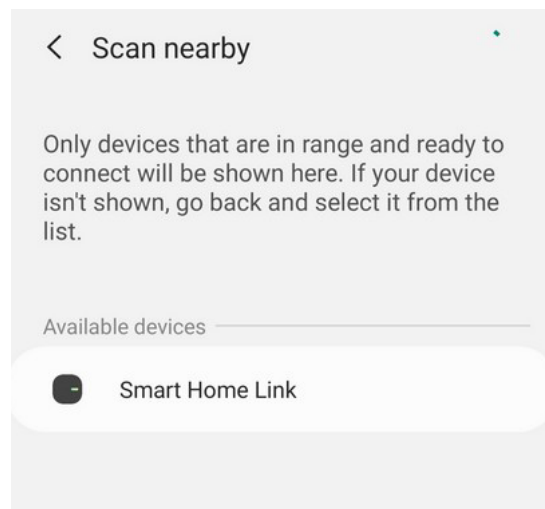
8. If the pop-up does not display, perform the following steps to add your mobile device to SmartThings.
 - a) Click **Device** and select **Scan nearby**.

FIGURE 28 Selecting a Device



The **Smart Home** link is displayed under **Available devices**.

FIGURE 29 Scanning for the device



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

FIGURE 30 Selecting the Location and Room for Your Hub

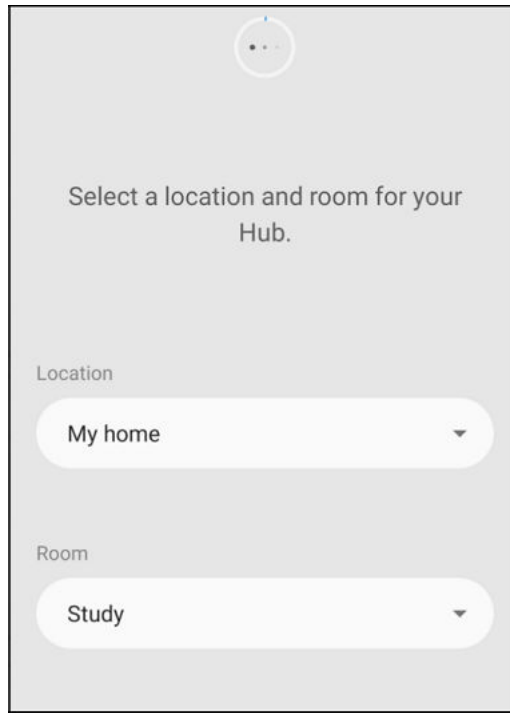
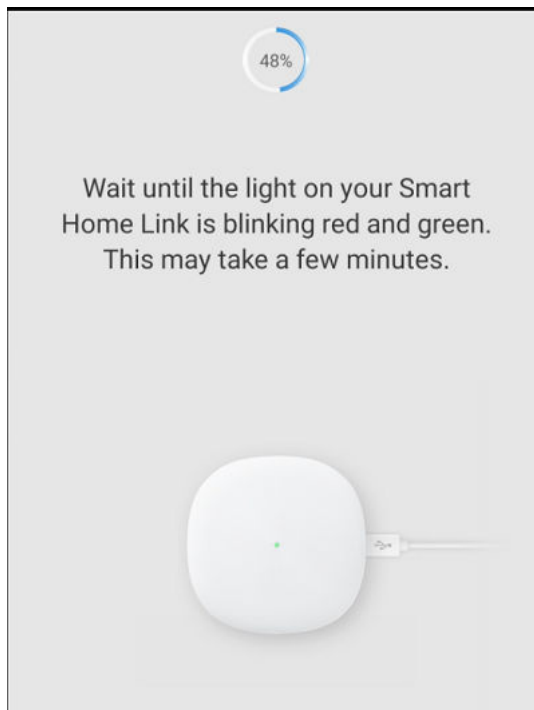


FIGURE 31 Waiting for Successful Connection



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

FIGURE 32 Renaming the Hub

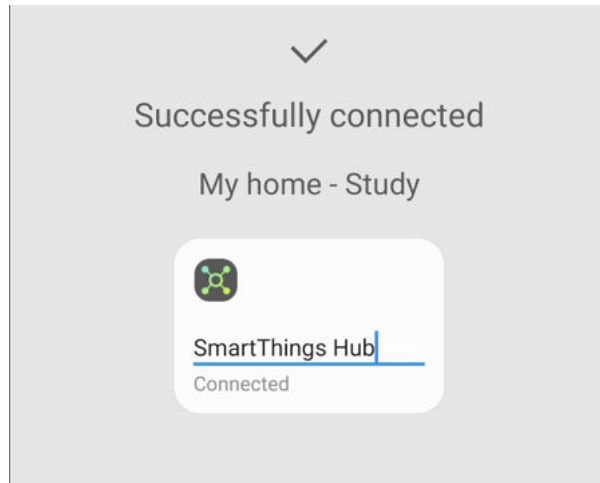
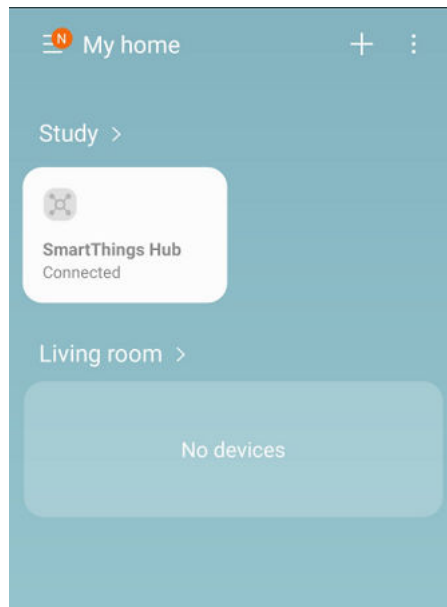
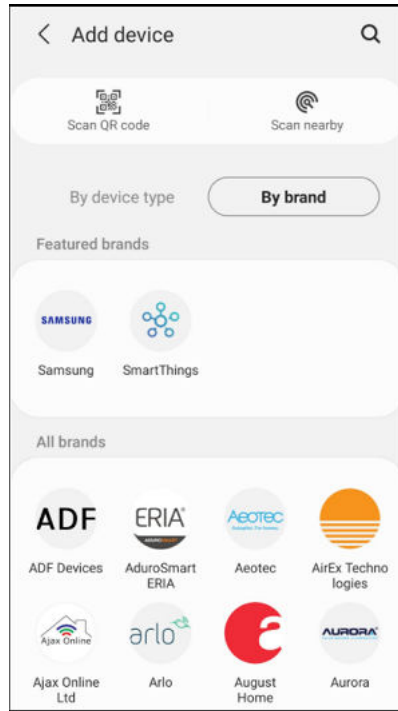


FIGURE 33 Hub Name on the Home Page



9. Add the SmartThings hub to the app.

FIGURE 34 Locating the SmartThings Hub

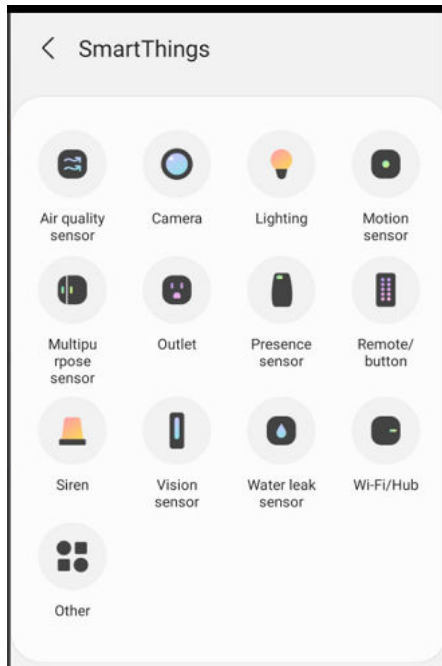


10. Click the + icon in the app and go to the **Devices** page to add the hub.

NOTE

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

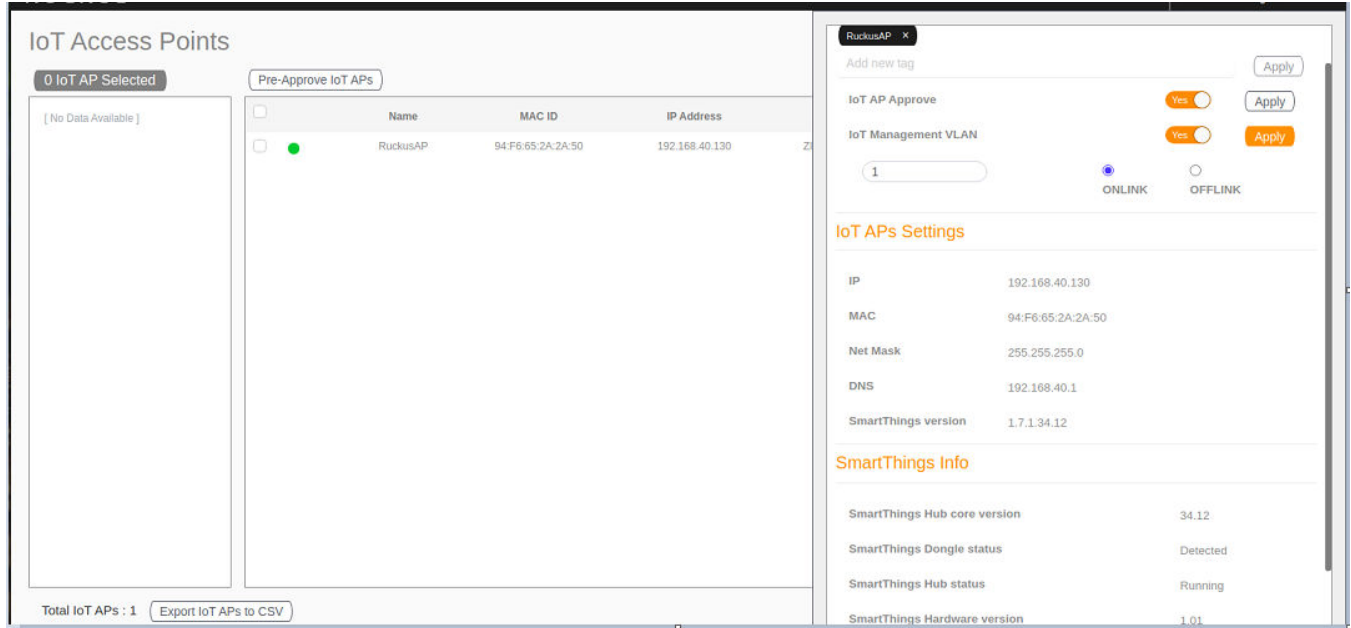
FIGURE 35 Adding Devices to Hub



11. From the main menu, click **IoT APs**.
The IoT Access Points page is displayed.

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

FIGURE 36 SmartThings Information in the Right Pane



Activating and Editing the Plugins

Plugins are the external vendor connectors that can be connected to a vendor infrastructure after the successful activation of a plugin. Ruckus supports Assa Abloy locks and plugins such as Kontakt.io, iBeacon, Eddystone, Beacon as a Service, Controller Data Stream, Telkonet, Soter, BLE Scan, Dormakaba locks.

Activating and Editing the Kontakt.io Beacons Plugin

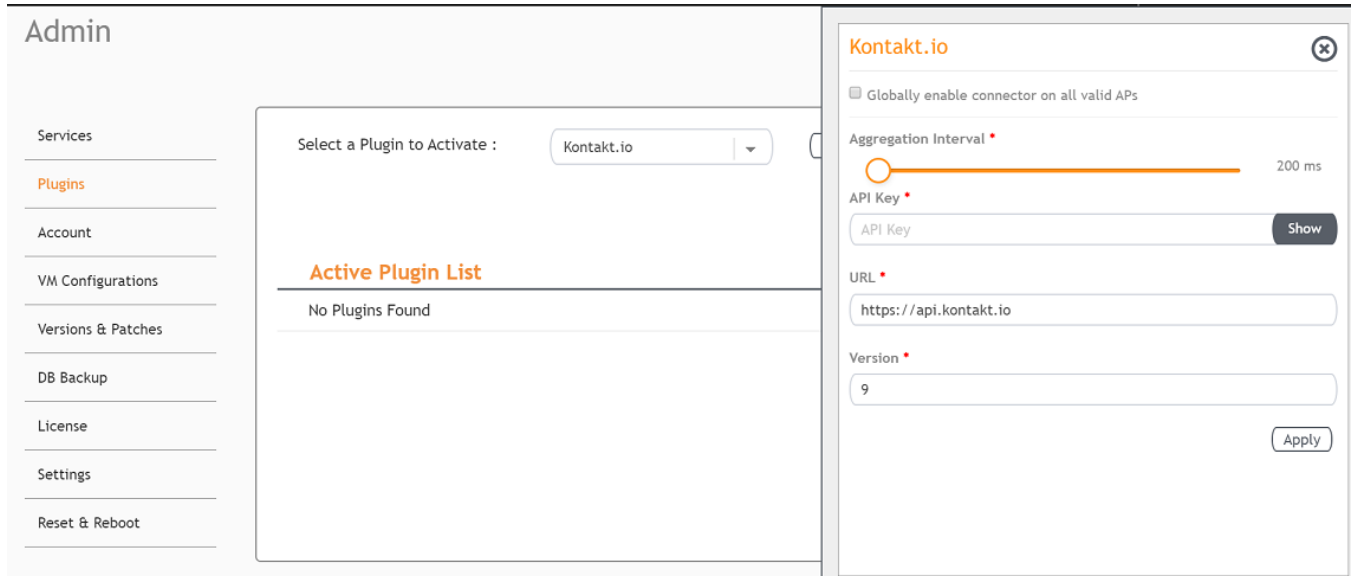
The RUCKUS IoT Controller provides support for the Kontakt.io Beacons plugin.

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 37 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 92 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.

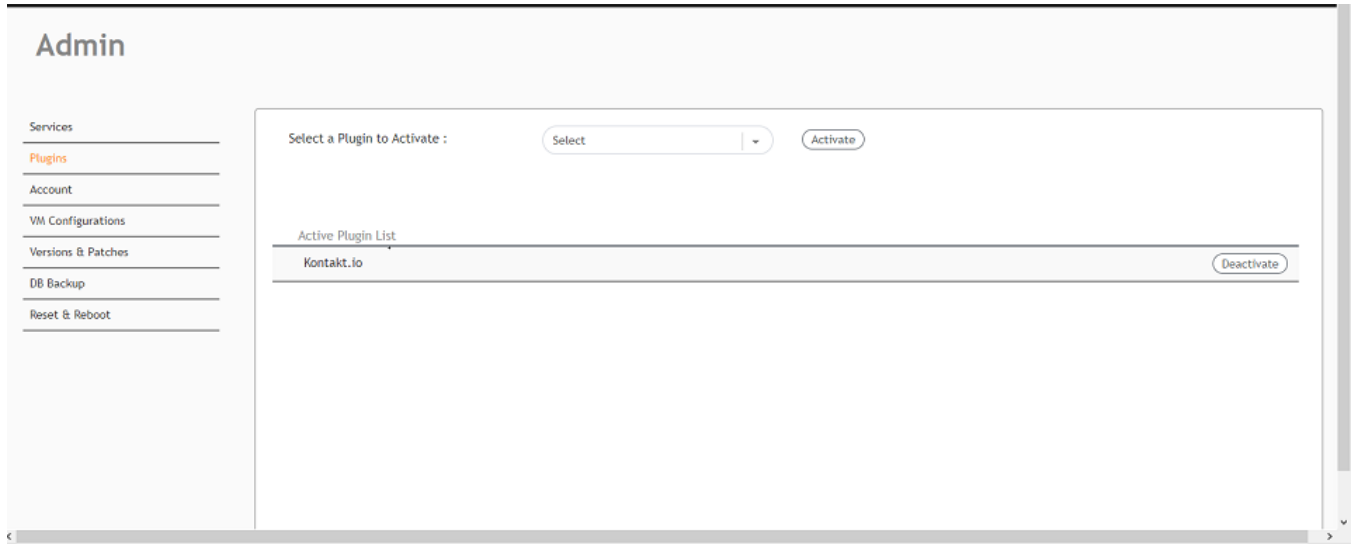
The default version number is 9.

5. Click **Apply**.

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

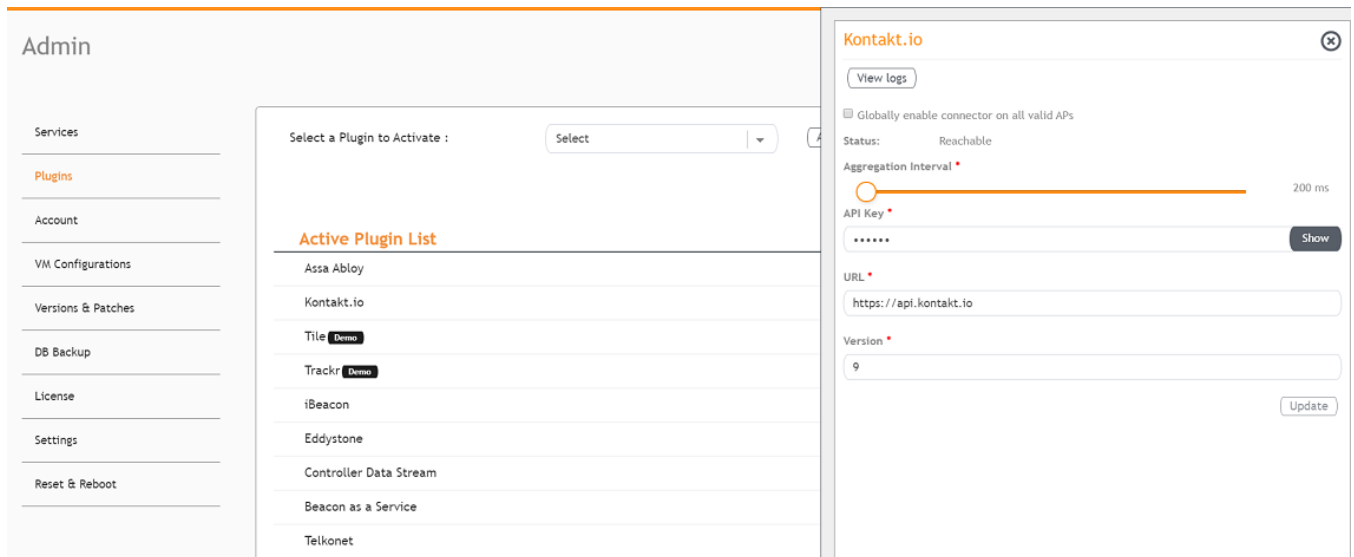
- To deactivate the Kontakt.io plugin, select it and click **Deactivate**.

FIGURE 38 Deactivating the Kontakt.io Plugin



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

FIGURE 39 Updating the Configuration Parameters



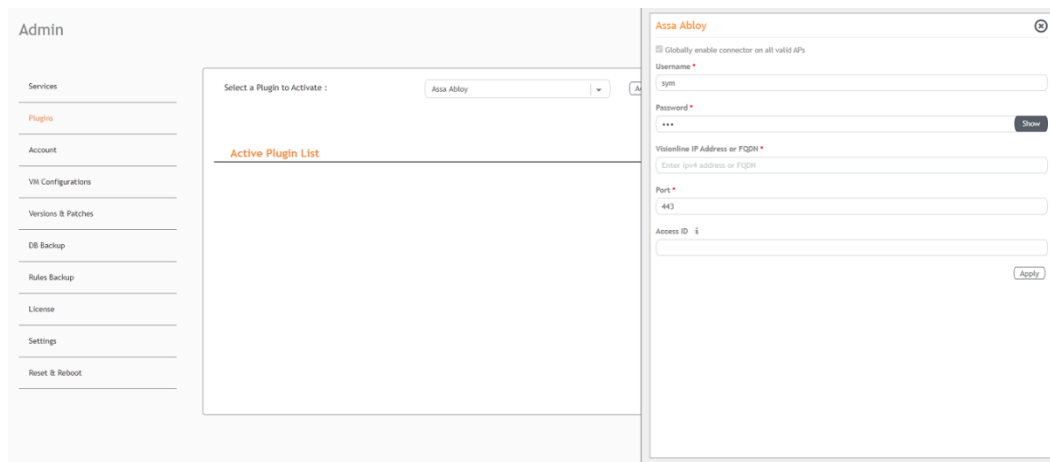
Activating and Editing the Assa Abloy Plugin

The RUCKUS IoT Controller provides support for the Assa Abloy door locks plugin. The RUCKUS IoT Controller reads the packet from the IoT AP and routes the packets to the Visionline Server.

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

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

FIGURE 40 Activating the Assa Abloy Plugin



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

NOTE

If **Globally enable connector on all valid APs** is not selected, you can activate the plugin for each AP by adding a tag. Refer to [Adding Tags to an AP](#) on page 92 for more information.

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

NOTE

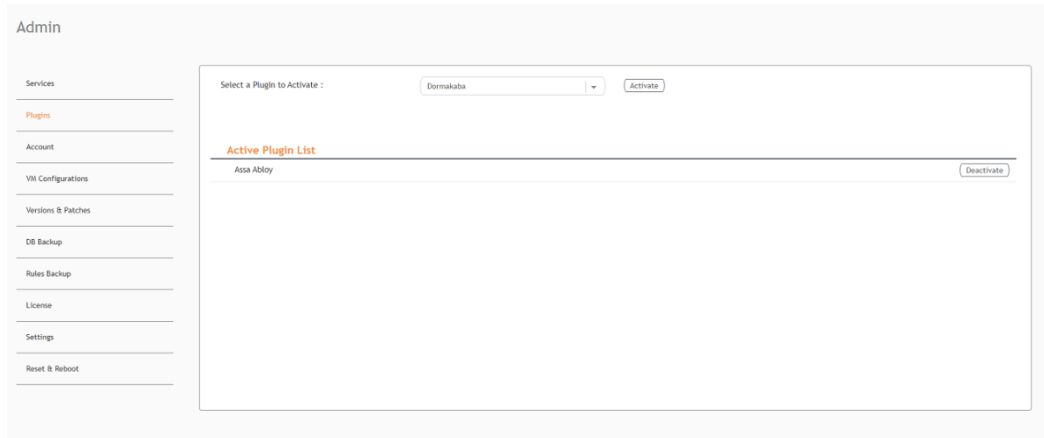
By default, the port number is 443.

5. Click **Apply**.

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

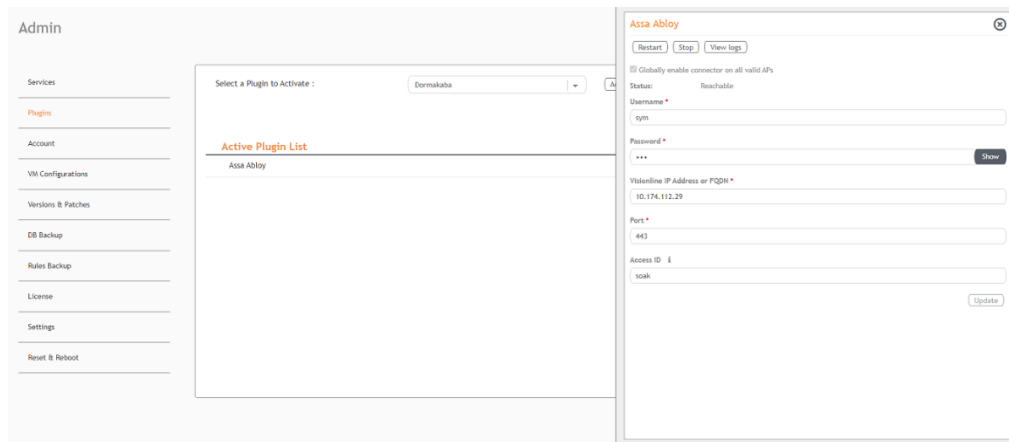
6. To deactivate the Assa Abloy plugin, select it and click **Deactivate**.

FIGURE 41 Deactivating the Assa Abloy Plugin



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

FIGURE 42 Updating the Configuration Parameters



Activating and Editing the Eddystone Plugin

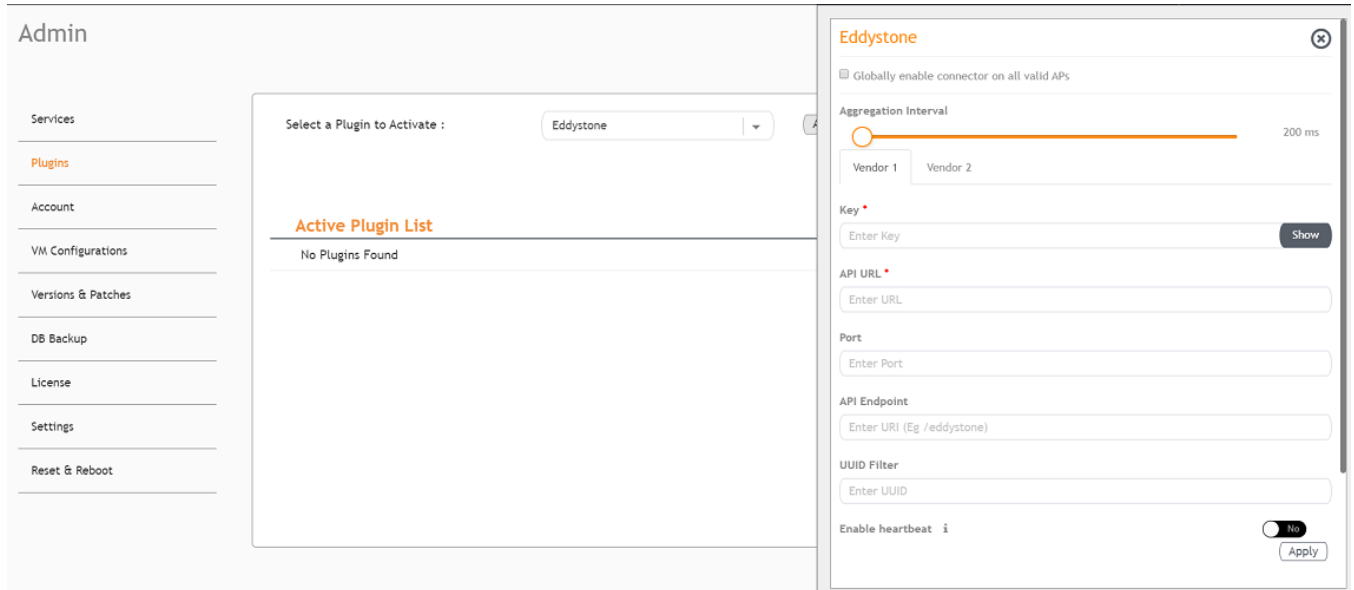
The RUCKUS IoT Controller provides support for the Bluetooth Low Energy (BLE) Eddystone plugin. The RUCKUS IoT Controller reads the packet from IoT AP, and routes the packets to the BLE beacon vendor cloud services.

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 43 Activating the Eddystone Plugin



Managing IoT Controller System Configuration

Activating and Editing the Plugins

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 92 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.

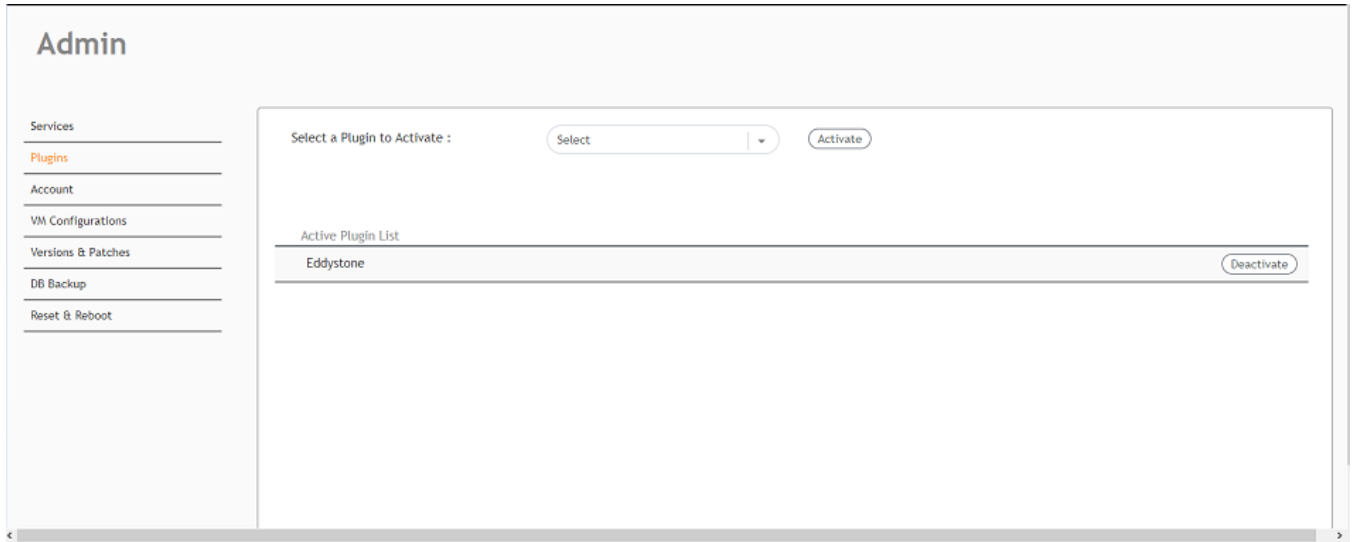
Enabling heartbeat allows the vendor application to receive the IoT AP status, such as online or offline.

5. Click **Apply**.

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

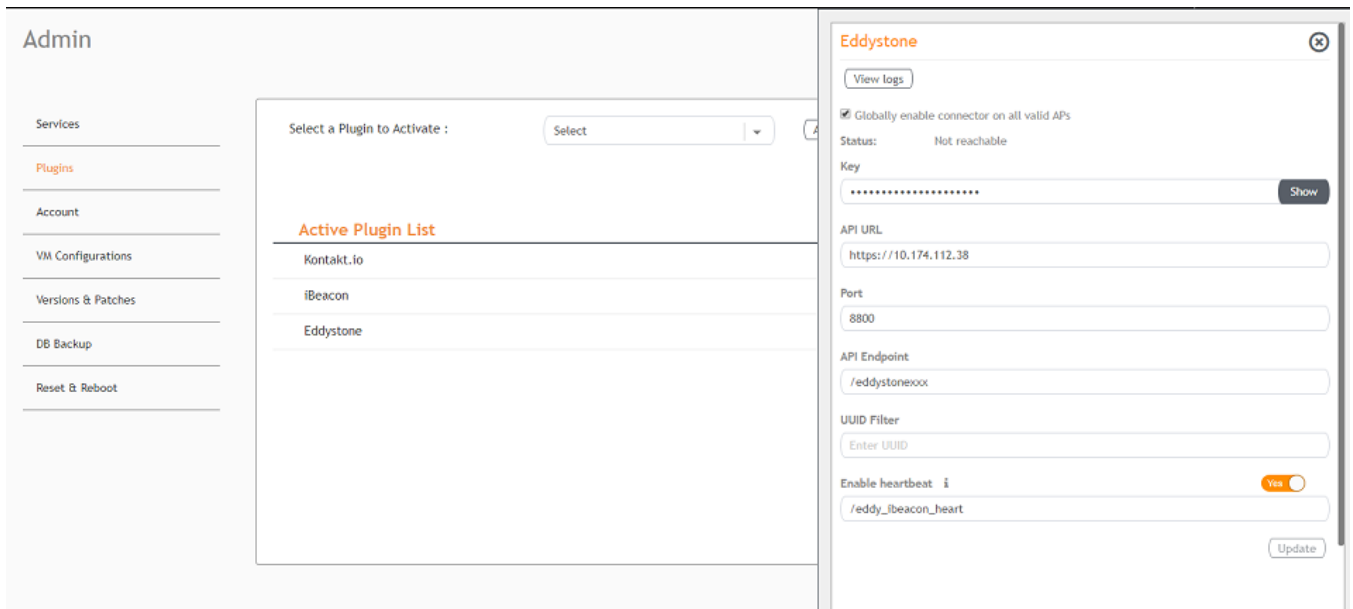
- To deactivate the Eddystone plugin, select it and click **Deactivate**.

FIGURE 44 Deactivating the Eddystone Plugin



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

FIGURE 45 Updating the Configuration Parameters



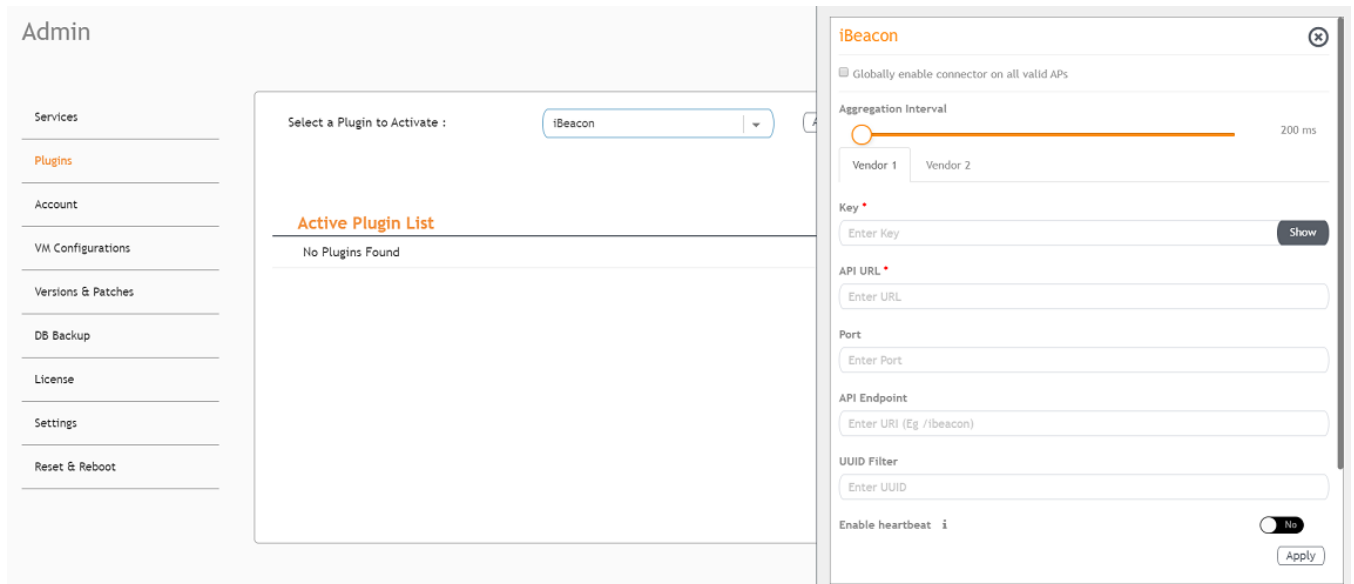
Activating and Editing the iBeacon Plugin

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 46 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 to [Adding Tags to an AP](#) on page 92 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.

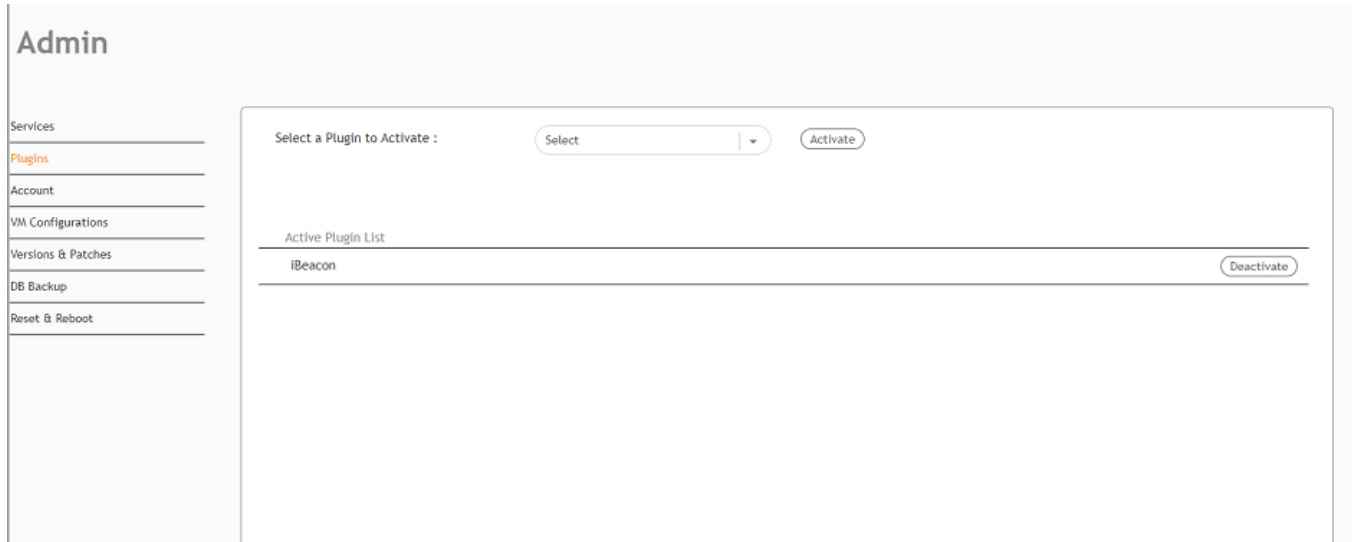
Enabling heartbeat allows the vendor application to receive the IoT AP status, such as online or offline.

5. Click **Apply**.

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

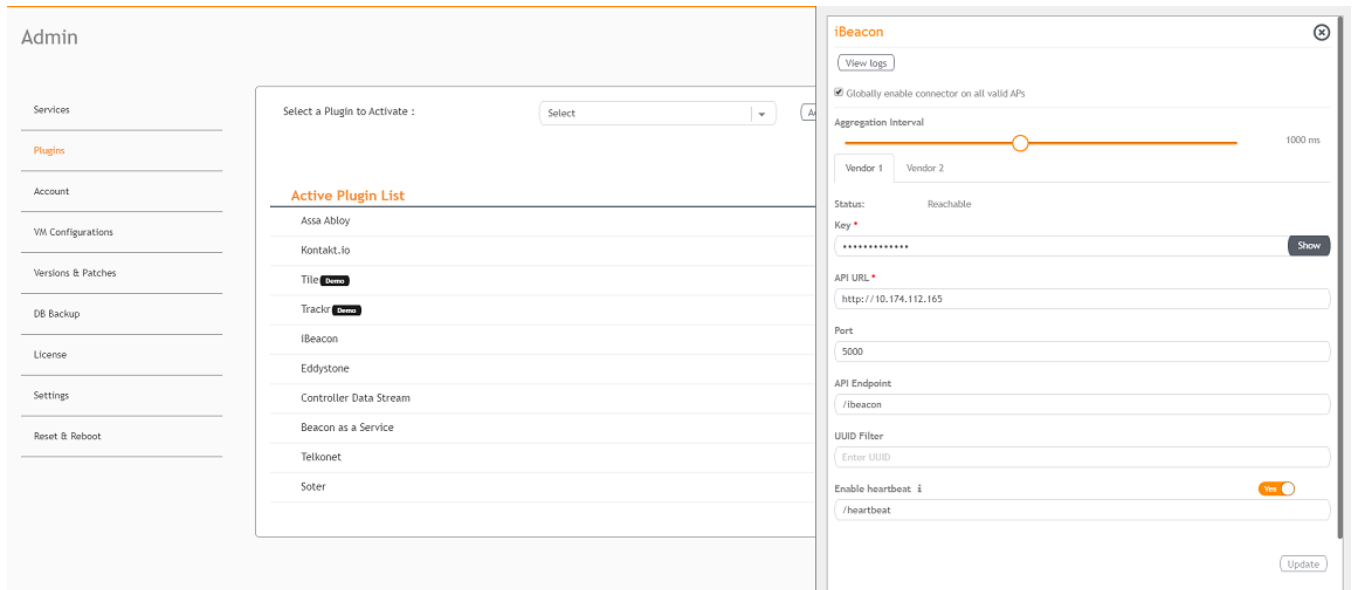
- To deactivate the iBeacon plugin, select it and click **Deactivate**.

FIGURE 47 Deactivating the iBeacon Plugin



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

FIGURE 48 Updating the Configuration Parameters



Activating and Editing the Beacon as a Service Plugin (iBeacon, Eddystone and Custom)

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

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

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

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

FIGURE 49 Activating the Beacon as a Service Plugin (iBeacon)

The screenshot shows the 'Beacon as a Service' configuration window. At the top, there is a title bar with the text 'Beacon as a Service' and a close button. Below the title bar, there is a checkbox labeled 'Globally enable connector on all valid APs' which is checked. Underneath, there is a slider for 'Advertisement Interval' set to 100 ms. Below the slider is a dropdown menu for 'Beacon Type' with 'iBeacon' selected. There are four text input fields: 'UUID' with the value '0047e70a5dc147258799830544ae04f6', 'Major No' with '0102', 'Minor No' with '0000', and 'Tx Power Level @1m' with '0'. An 'Update' button is located at the bottom right of the window.

FIGURE 50 Activating Beacon as a Service (Eddystone)

The screenshot shows the 'Beacon as a Service' configuration window. At the top, there is a title bar with the text 'Beacon as a Service' and a close button. Below the title bar, there is a checkbox labeled 'Globally enable connector on all valid APs' which is checked. Underneath, there is a slider for 'Advertisement Interval' set to 100 ms. Below the slider is a dropdown menu for 'Beacon Type' with 'Eddystone' selected. There are four text input fields: 'Namespace ID' with the value '48d815a81b09b25a41b1', 'Instance ID' with '6b2441d56920', 'URL' with 'http://www.ruckuswireless.com', and 'Tx Power Level @0m' with '0'. An 'Update' button is located at the bottom right of the window.

FIGURE 51 Activating Beacon as Service (Generic)

The screenshot shows the 'Beacon as a Service' configuration window. At the top, there is a checkbox labeled 'Globally enable connector on all valid APs' which is checked. Below it is a slider for 'Advertisement Interval' with a value of 100 ms. The 'Beacon Type' is set to 'Custom Beacon' in a dropdown menu. The 'Vendor type' is set to 'Generic' in another dropdown. There is a text input field containing '03' and an 'Add' button next to it. Below these fields is a table with the following data:

ADV Type	Value	Actions
01	0192	[Edit] [Delete]

An 'Update' button is located at the bottom right of the configuration area.

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

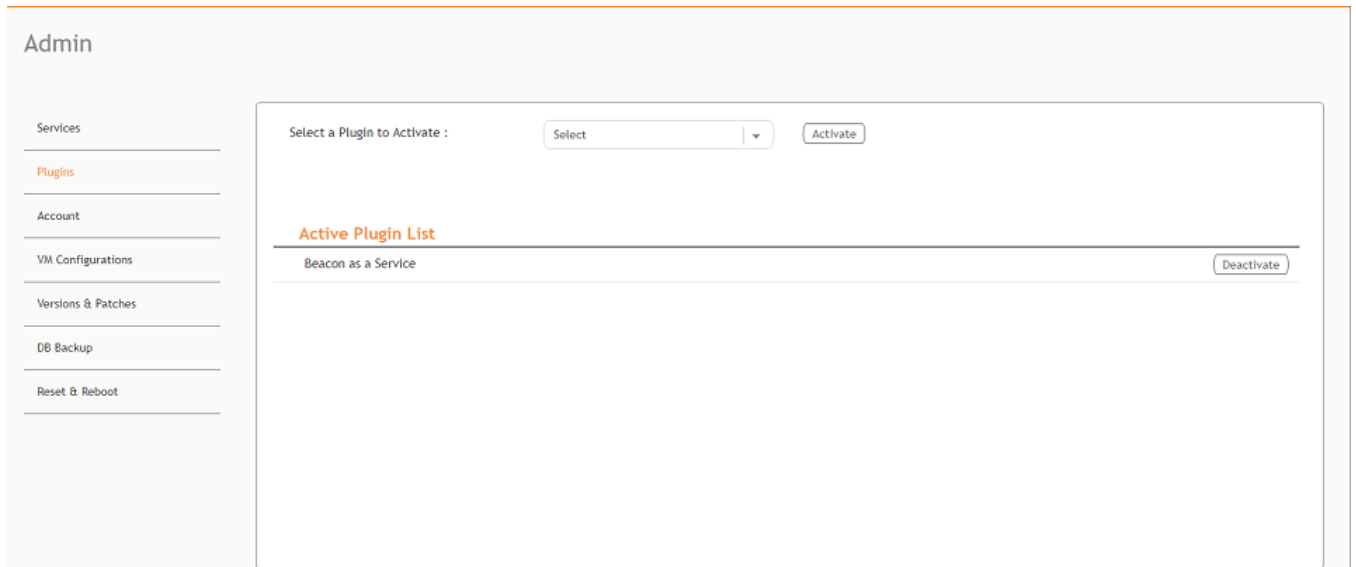
If **Globally enable connector on all valid APs** is not selected, you can activate the plugin for each AP by adding a tag. Refer to [Adding Tags to an AP](#) on page 92 for more information.

- b) In the **Beacon Type** list, select the type of beacon.
 - c) Provide relevant values for given fields based on Beacon Type. For iBeacon, a common 32 characters UUID can be given which will be applied to all APs. If Append AP MAC is checked, Controller will append 12 characters of AP MAC at the end of 20 characters UUID, so that it will be unique for every AP data.
 - d) For **Advertisement Interval**, set the time interval to send the advertisement packets. The advertisement interval ranges from 100 through 1000 milliseconds. The default interval is 100 milliseconds.
5. Click **Apply**.

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

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

FIGURE 52 Deactivating the Beacon as a Service Plugin



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

FIGURE 53 Updating the Configuration Parameters (iBeacon)

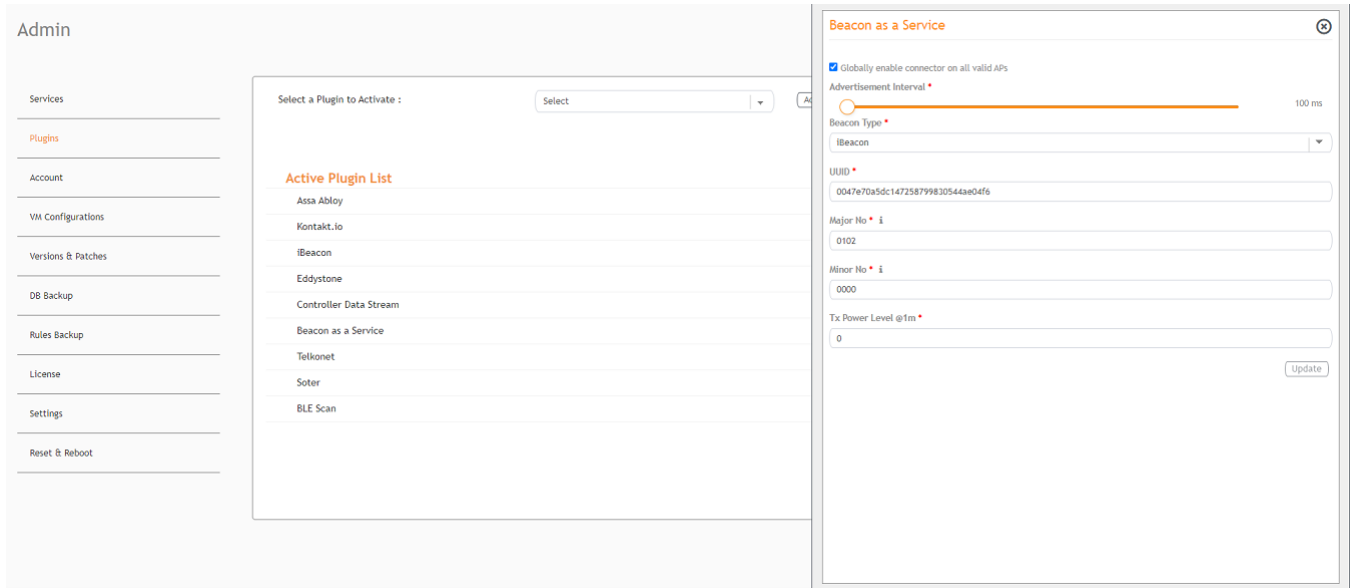


FIGURE 54 Updating Configuration parameters (Eddystone)

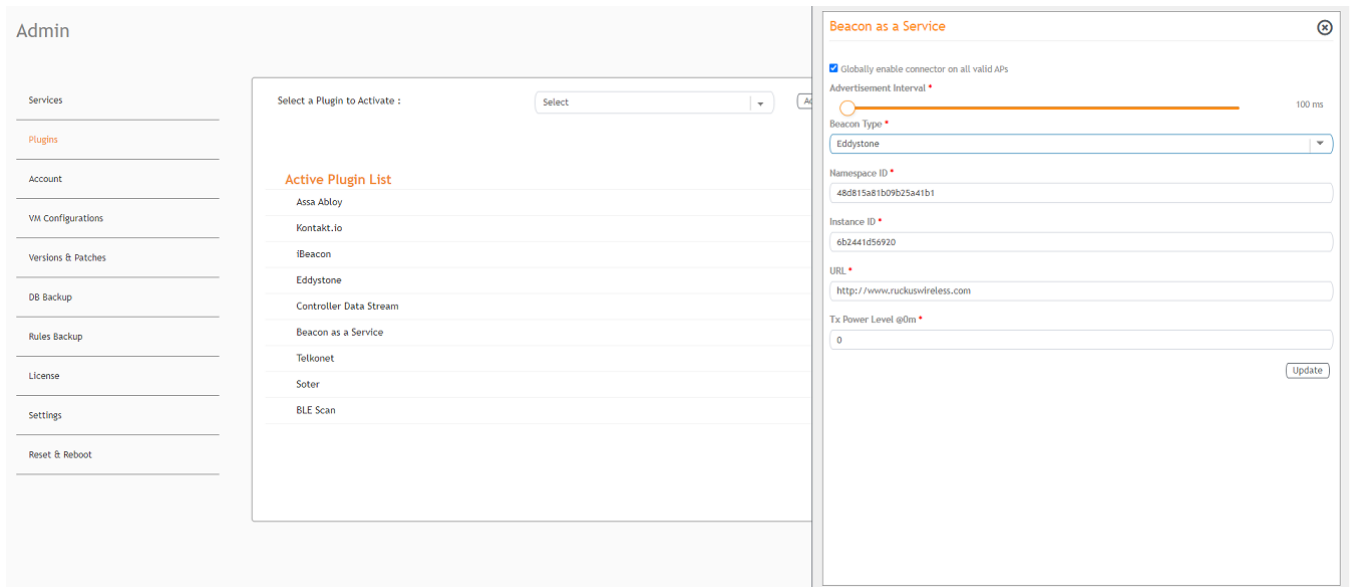
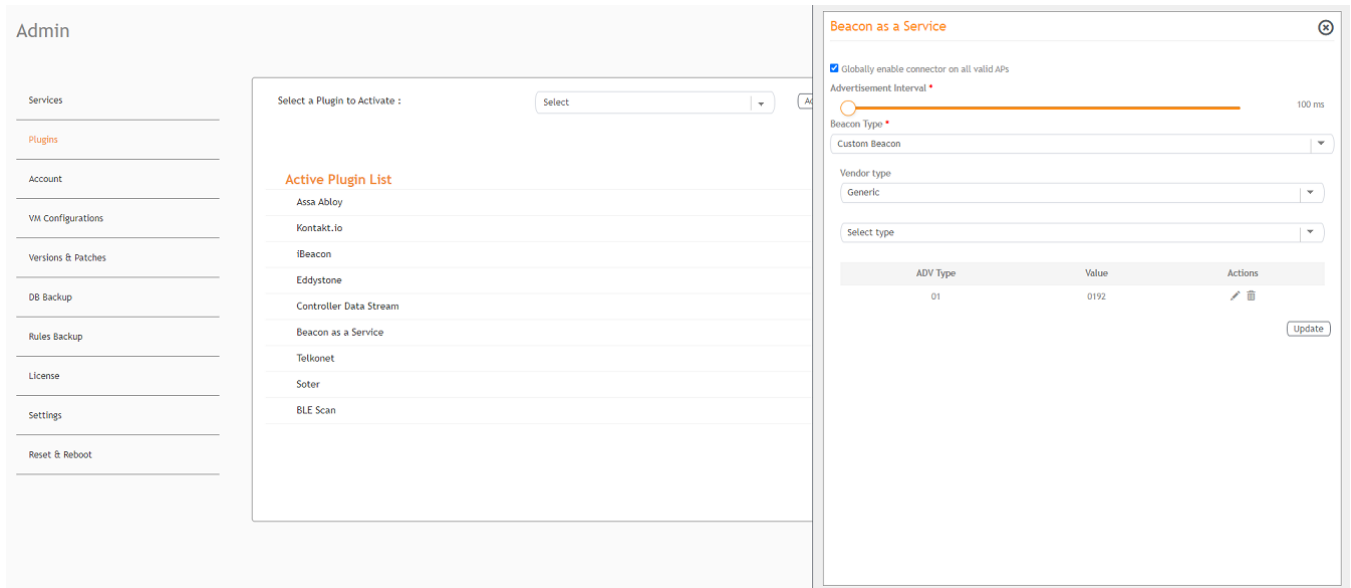


FIGURE 55 Updating Configuration Parameters (Generic)



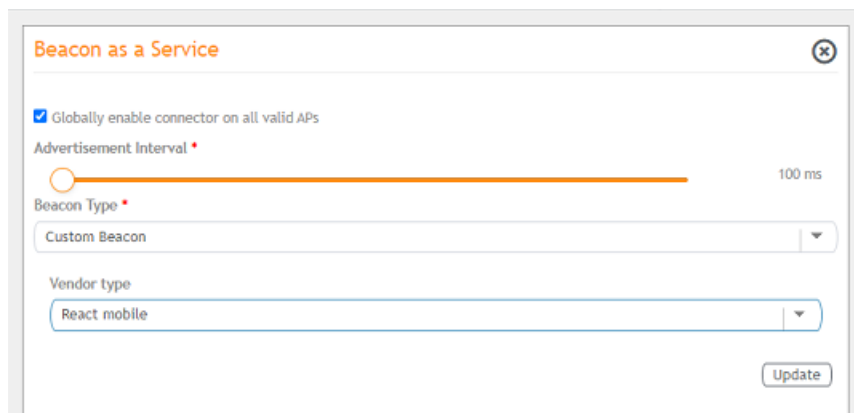
Activating and Editing the Beacon as a Service Plugin (React Mobile)

The RUCKUS IoT Controller provides support for the React Mobile beaconing service. An AP can begin transmitting React Mobile beacons that can be used by the user for various cases, such as wayfinding and pushing.

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

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

FIGURE 56 Activating the Beacon as a Service Plugin



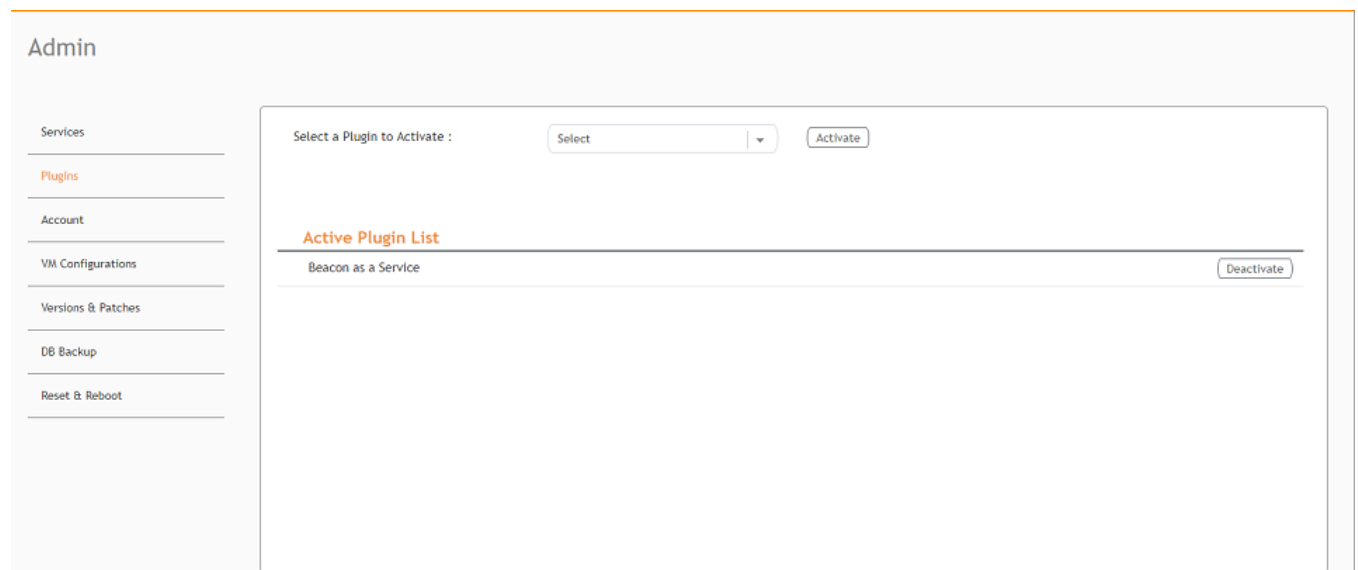
4. After the Beacon as Service plugin is activated, enter the following configuration parameters.
 - a) Select **Globally enable connector on all valid APs** to add all respective IoT APs automatically. Connectors are mapped to IoT AP by adding the connector name tag to the IoT AP.

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 92 for more information.

- b) For **Advertisement Interval**, set the time interval to send the advertisement packets. The advertisement interval ranges from 100 through 1000 milliseconds. The default interval is 100 milliseconds.
 - c) In the **Beacon Type** list, select the type of beacon as Custom.
 - d) In the **Vendor Type** list, select the type as **React Mobile**.
5. Click **Apply**.
The Beacon as a Service plugin is added in the **Active Plugin List**.
6. To deactivate the Beacon as a Service plugin, select it and click **Deactivate**.

FIGURE 57 Deactivating the Beacon as a Service Plugin



Activating and Editing the BLE Scan Plugin

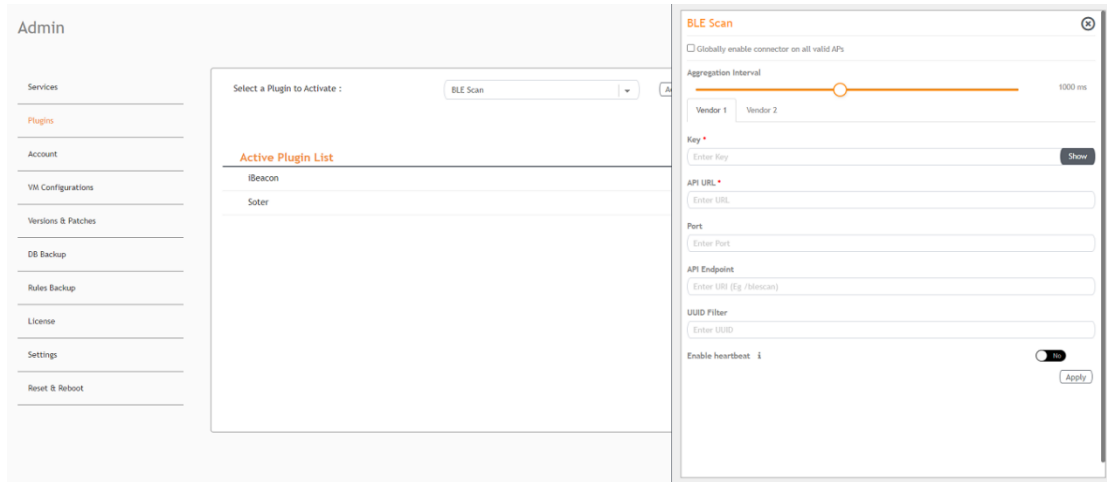
The RUCKUS IoT Controller provides support for the Bluetooth Low Energy (BLE) BLE Scan Plugin . The RUCKUS IoT Controller reads the packet from the IoT AP and routes the packets to the BLE beacon vendor cloud services.

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

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

3. In the **Select a Plugin to Activate** list, select the BLE Scan plugin and click **Activate**.

FIGURE 58 Activating the BLE Scan Plugin



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

NOTE

If **Globally enable connector on all valid APs** is not selected, you can activate the plugin for each AP by adding a tag. Refer to [Adding Tags to an AP](#) on page 92 for more information.

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

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

- d) Enter the API URL.

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

NOTE

The plugin supports HTTP and HTTPS modes.

- e) Enter the Port number.

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

- f) Enter the API Endpoint.

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

- g) Enter the UUID Filter.

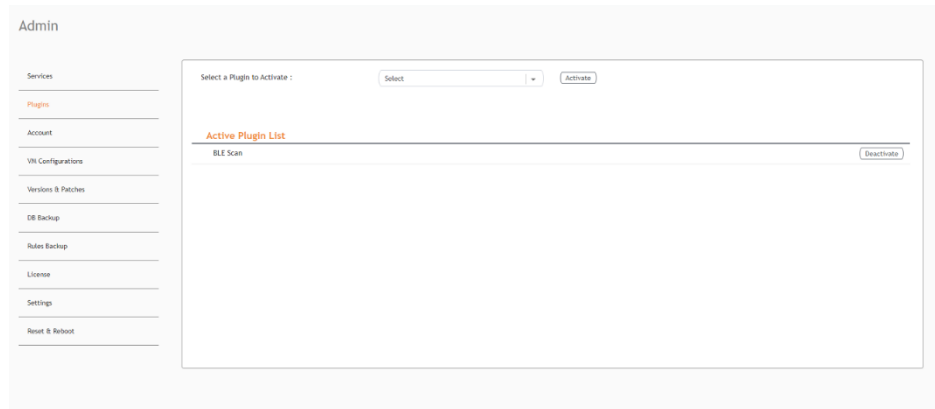
The filter allows only the BLE ADV packets with the specified UUID to be passed on to the vendor application.

- h) Enable heartbeat.

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

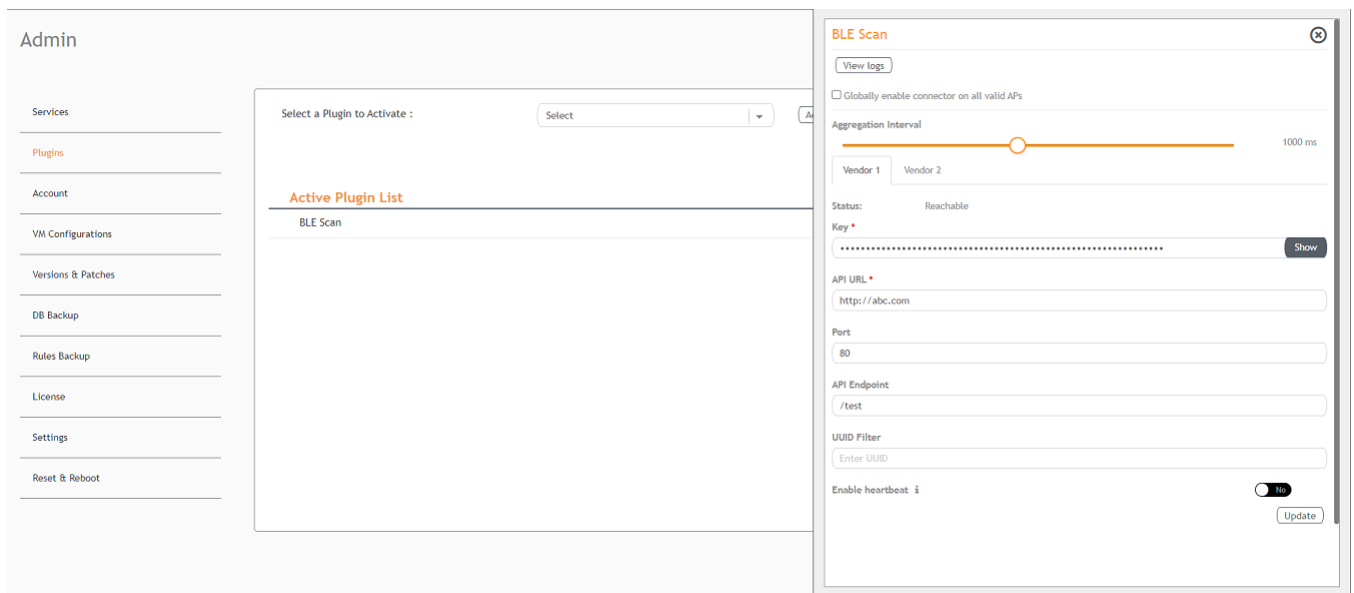
5. Click **Apply**.
The BLE Scan plugin is added in the **Active Plugin List**.
6. To deactivate the BLE Scan plugin, select it and click **Deactivate**.

FIGURE 59 Deactivating the BLE Scan Plugin



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

FIGURE 60 Updating the Configuration Parameters



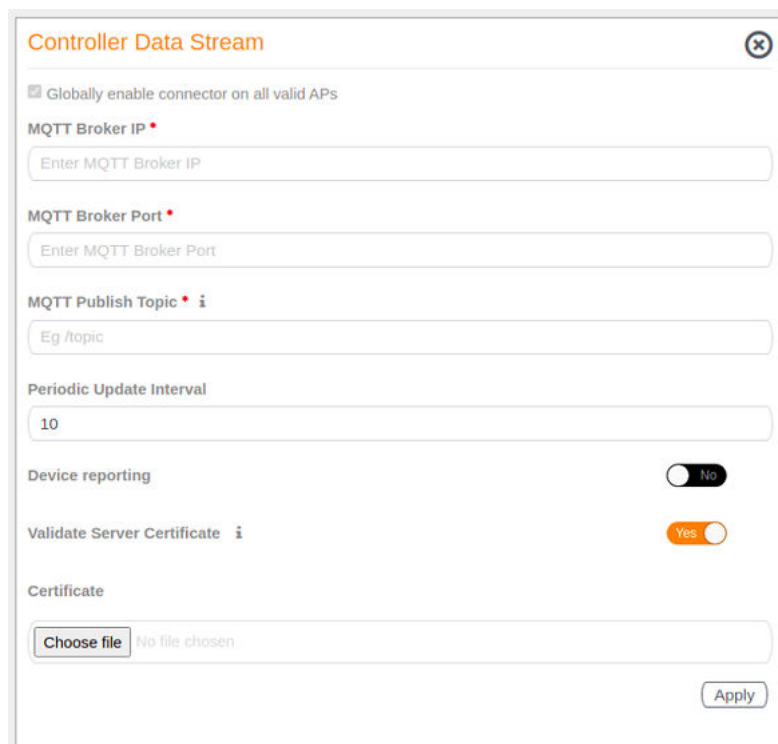
Activating and Editing the Controller Data Stream Plugin

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 61 Activating the Controller Data Stream Plugin



The screenshot shows the configuration page for the Controller Data Stream plugin. The page title is "Controller Data Stream" with a close button in the top right corner. Below the title, there is a checkbox labeled "Globally enable connector on all valid APs". The main configuration area includes several input fields: "MQTT Broker IP" with a placeholder "Enter MQTT Broker IP", "MQTT Broker Port" with a placeholder "Enter MQTT Broker Port", and "MQTT Publish Topic" with a placeholder "Eg /topic" and an information icon. Below these is a "Periodic Update Interval" field with the value "10". There are two toggle switches: "Device reporting" is currently turned off (No), and "Validate Server Certificate" is currently turned on (Yes). At the bottom, there is a "Certificate" section with a "Choose file" button and the text "No file chosen". An "Apply" button is located in the bottom right corner.

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

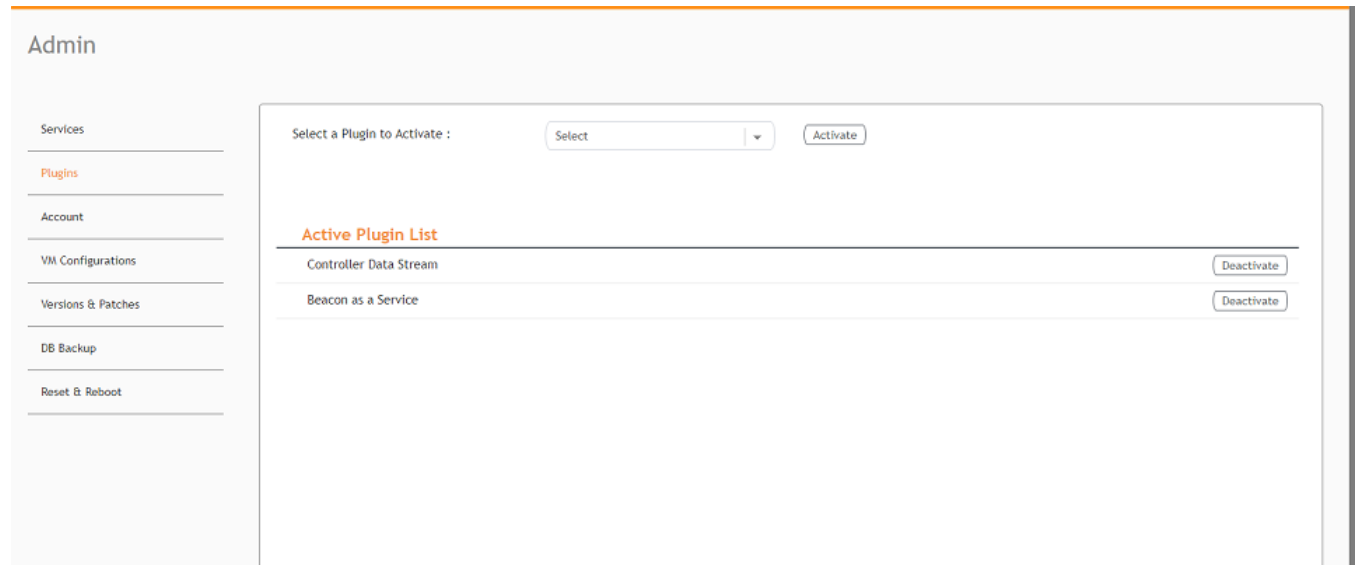
If **Globally enable connector on all valid APs** is not selected then you can activate the plugin for each AP by adding tag. Refer [Adding Tags to an AP](#) on page 92 for more information.

- b) In **MQTT Broker IP**, enter the IP address of your MQTT broker.
 - c) In **MQTT Broker Port**, enter the network port to which you want to connect.
 - d) In **MQTT Publish Topic**, enter the topic name as a simple string that is hierarchically structured with forward slashes (/) as delimiters. An MQTT client can publish messages as soon as it connects to a broker.
 - e) In **Periodic Update Interval** enter the interval to receive MQTT Publish.
 - f) Enable **Device Reporting** and enter the topic endpoint which will publish message whenever a device change event is received.
 - g) Enable **Validate Server Certificate** to secure the connection with SSL.
5. Click **Apply**.

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

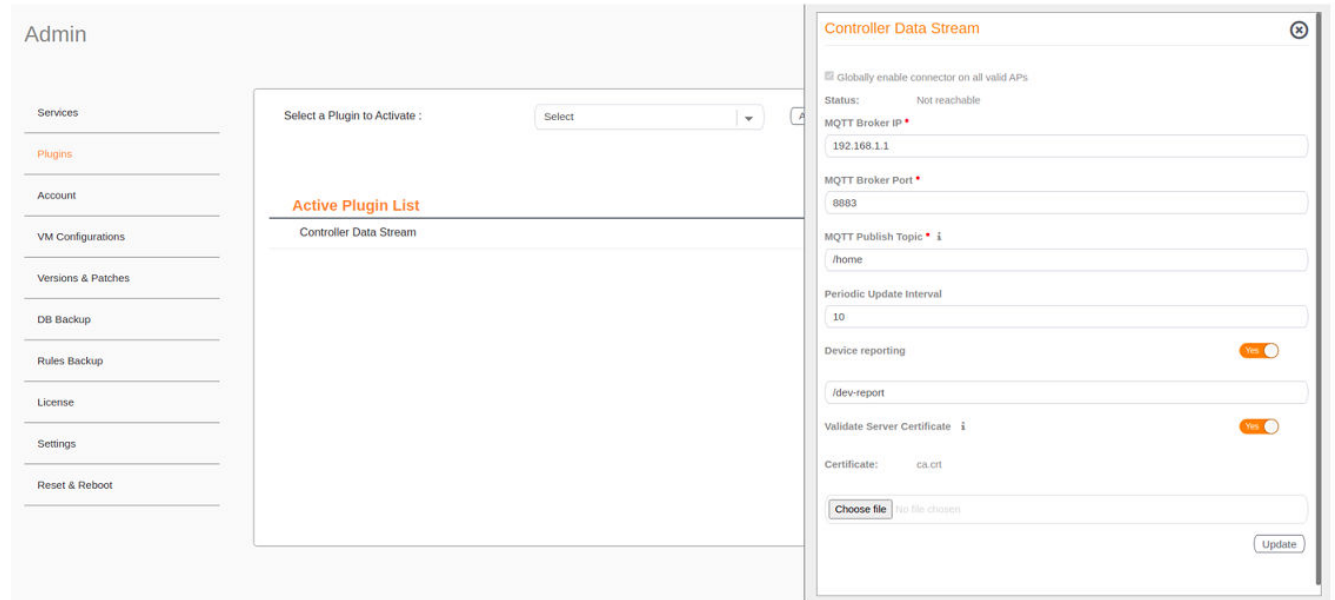
6. To deactivate the Controller Data Stream plugin, select it and click **Deactivate**.

FIGURE 62 Deactivating the Controller Data Stream Plugin



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

FIGURE 63 Updating the Configuration Parameters



Activating and Editing the Dormakaba Plugin

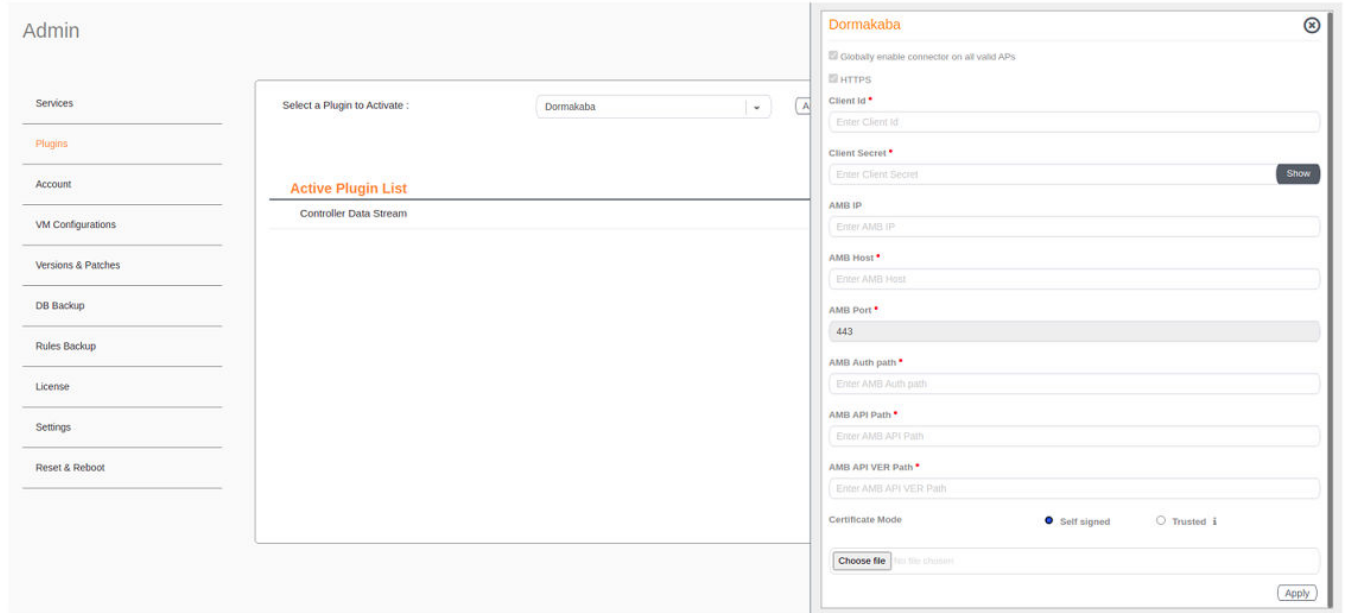
The RUCKUS IoT Controller provides support for for the Dormakaba Door Locks. The RUCKUS IoT Controller reads the packet from the IoT AP and routes the packets to the Ambiance Server.

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

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

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

FIGURE 64 Activating the Dormakaba Plugin



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

NOTE

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

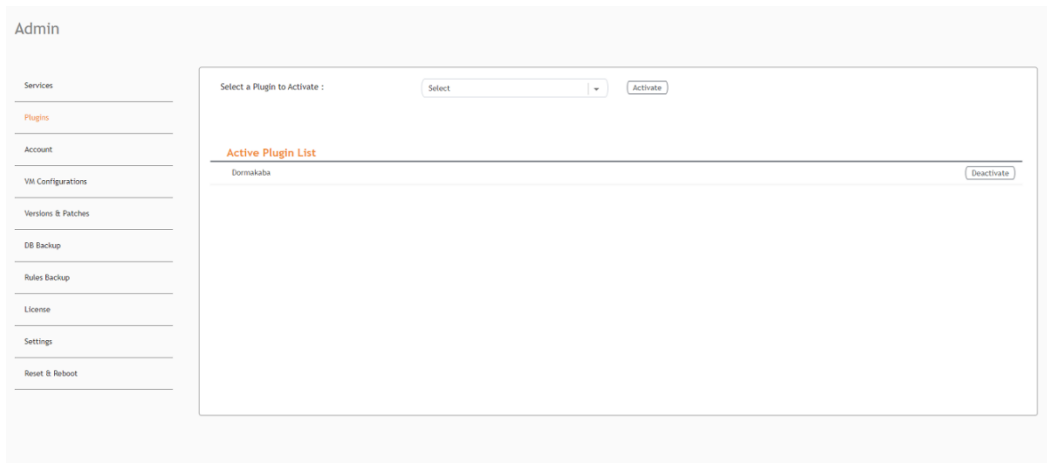
- e) Enter the **Ambiance Port**.
 - f) Enter the **Ambiance Auth Path**.
 - g) Enter the **Ambiance API Path**.
 - h) Enter the **Ambiance API VER Path**.
 - i) Select the **Certificate Mode**.
 - j) Click **Choose file**.
5. Click **Apply**.
The Dormakaba plugin is added in the **Active Plugin List**.

Managing IoT Controller System Configuration

Activating and Editing the Plugins

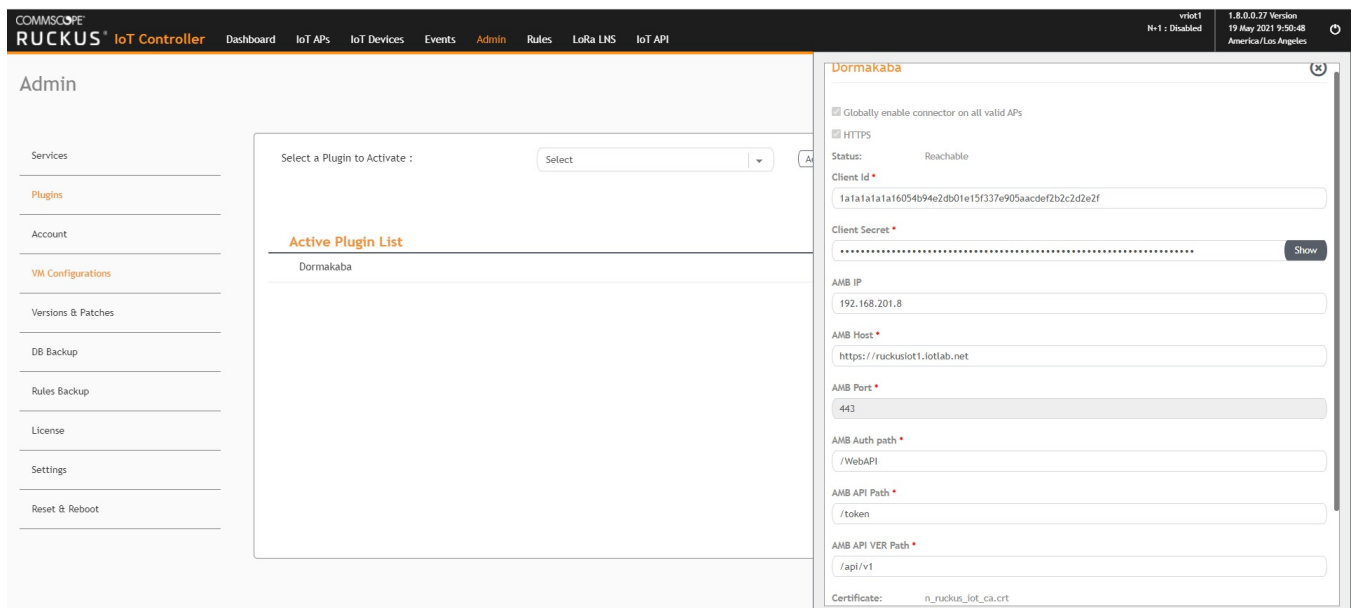
6. To deactivate the Dormakaba plugin, select it and click **Deactivate**.

FIGURE 65 Deactivating the Dormakaba Plugin



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

FIGURE 66 Updating the Configuration Parameters



Activating and Editing the Telkonet Plugin

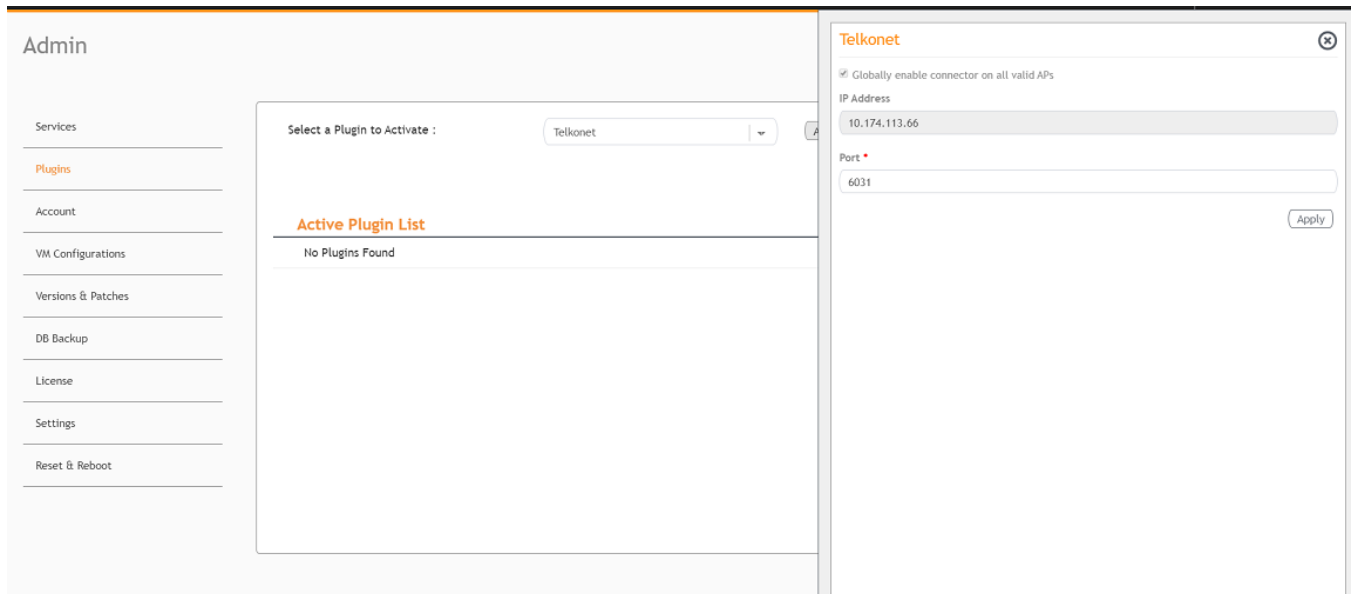
The RUCKUS IoT Controller provides support for the Telkonet devices and their respective MQTT APIs.

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 67 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.

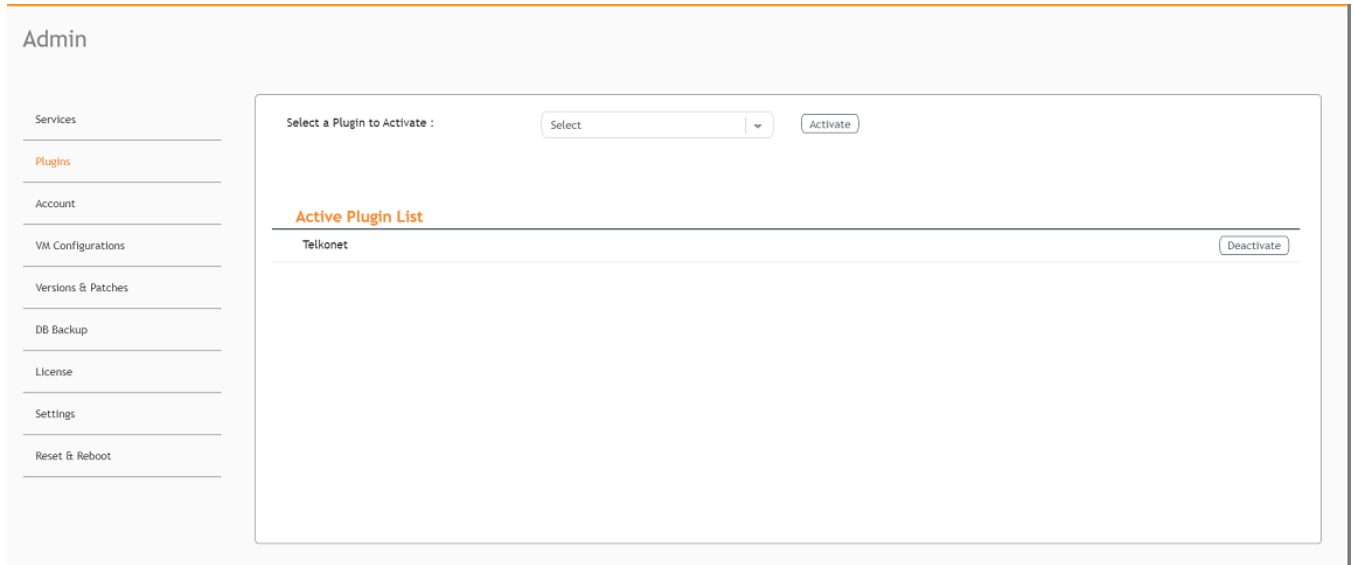
NOTE

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 92 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**.

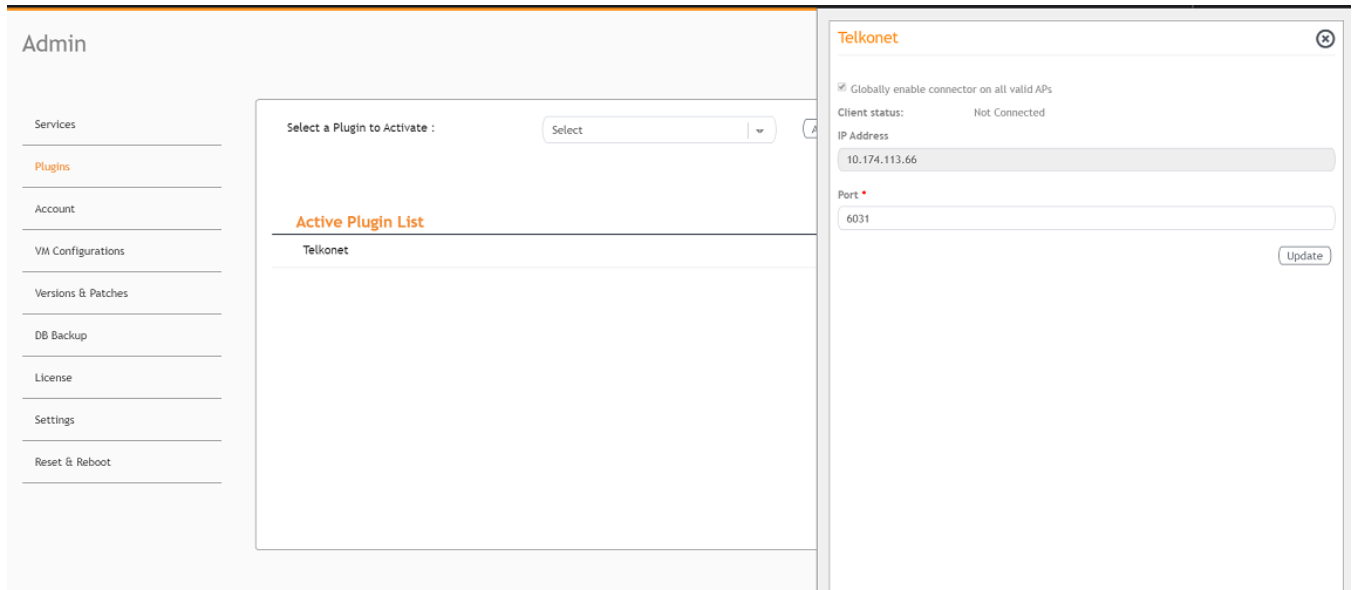
- To deactivate the Telkonet plugin, select it and click **Deactivate**.

FIGURE 68 Deactivating the Telkonet Plugin



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

FIGURE 69 Updating the Configuration Parameters



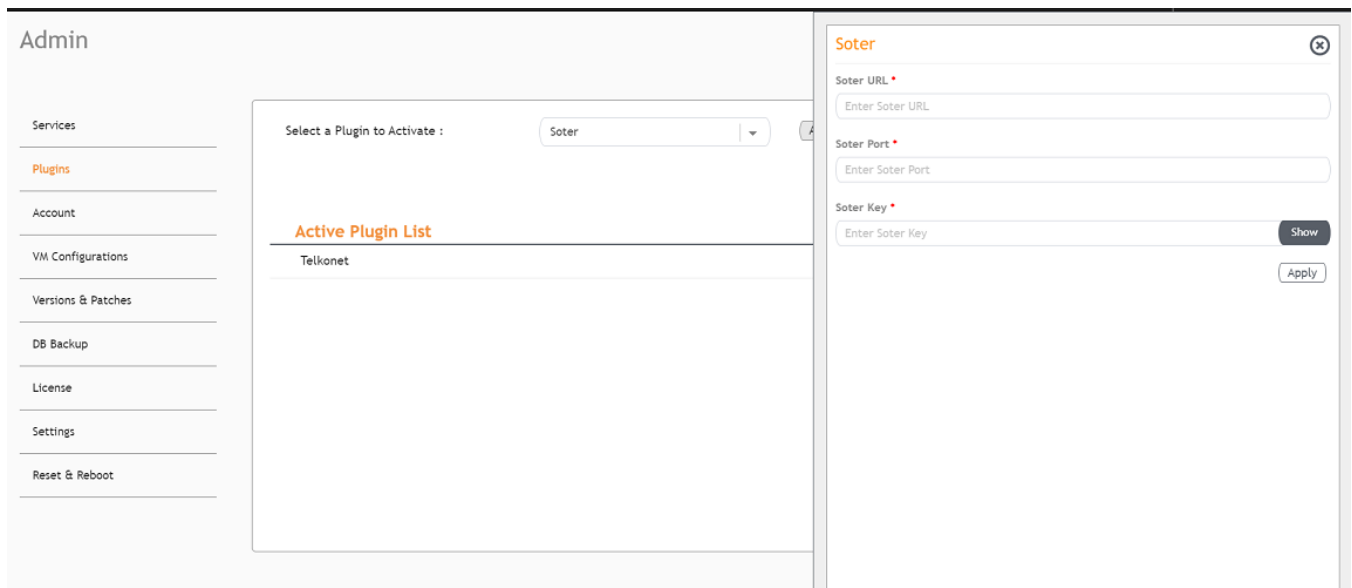
Activating and Editing the Soter Plugin

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 70 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.

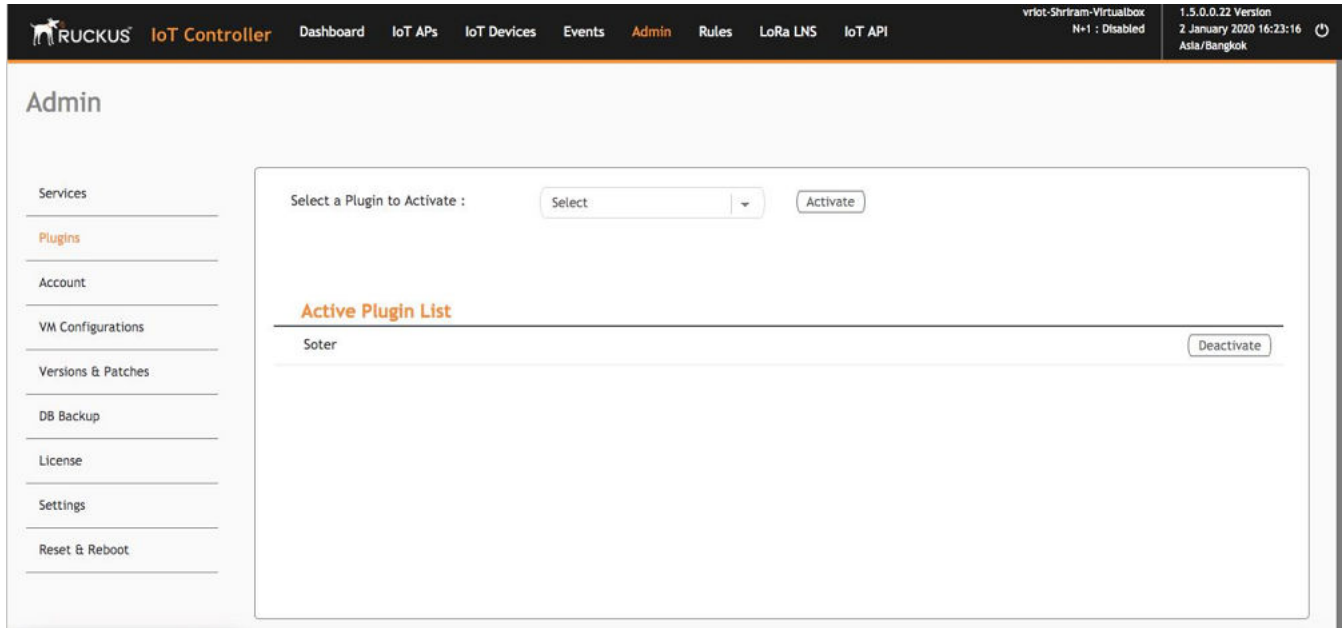
- c) Enter the Key.

The Vendor application is responsible for authenticating the Keys.
5. Click **Apply**.

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

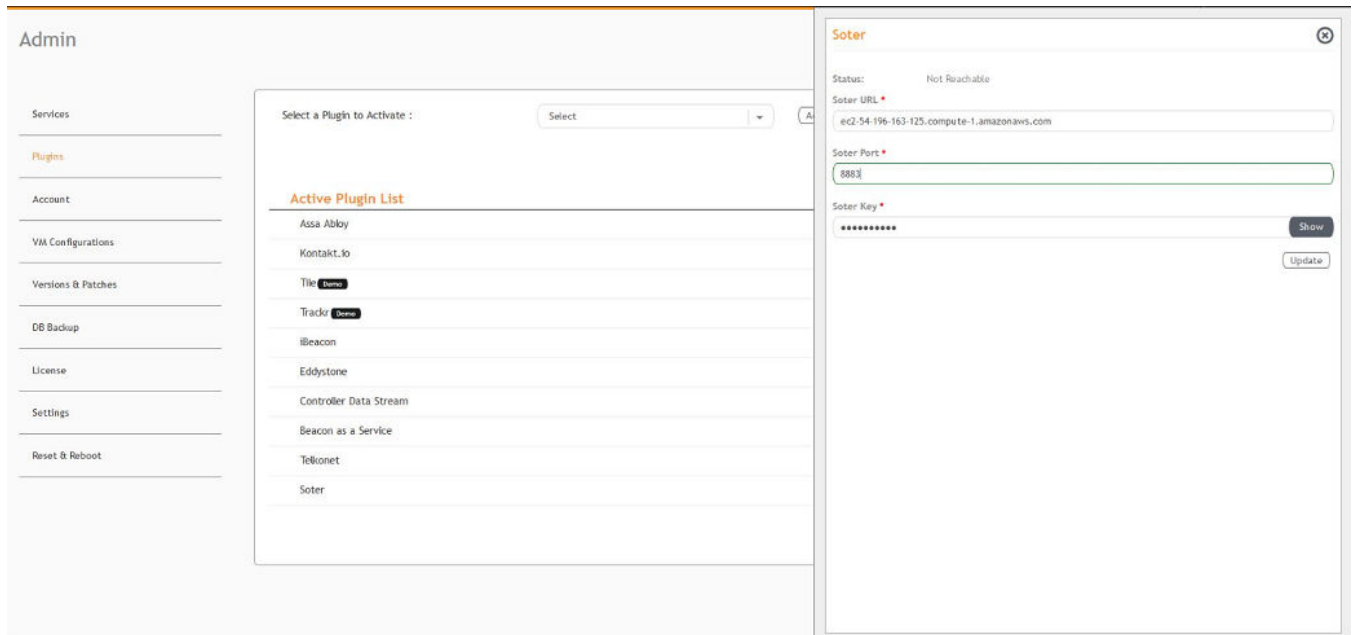
- To deactivate the Soter plugin, select it and click **Deactivate**.

FIGURE 71 Deactivating the Soter Plugin



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

FIGURE 72 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 73 Changing the Password

The screenshot shows a web form for changing a password. At the top right is an "Update password" button. Below it are three input fields, each with a "Show" button to toggle visibility: "Current Password" (placeholder: "Enter Current password"), "New Password" (placeholder: "Enter New password"), and "Confirm New Password" (placeholder: "Retype New 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 74 Configuring a Virtual Machine

The screenshot shows the "Admin" page with a left navigation menu. The "VM Configurations" option is highlighted. The main content area contains configuration fields for a virtual machine. The "Hostname" field is set to "vriot". The "Time Zone" is set to "America/Los_Angeles". The "NTP Address" is set to "ntp.ubuntu.com" (marked as optional). The "Set Time Automatically using NTP" radio button is selected. Below these fields are "Certificate" and "Key" sections, each with a "Choose file" button and a "No file chosen" message. At the bottom are "Upload certificate & Key" and "Download CA certificate" buttons. An "Update" button is located at the bottom right of the configuration area.

Managing IoT Controller System Configuration

Uploading Versions and Patches

3. Complete the configuration information.
 - a) In the **Hostname** field, enter the host name.
 - b) In the **Time Zone** list, select the time zone.
 - c) Select **Set Time Automatically using NTP** or **Set Time Manually** to set the time.
 - d) Click **DHCP** or **Static** to set the RUCKUS IoT Controller configuration.

NOTE

The RUCKUS IoT Controller is configured with a self-signed certificate, but a proper (CA-signed) certificate can be added to the system.

4. Click **Update**.

Uploading Versions and Patches

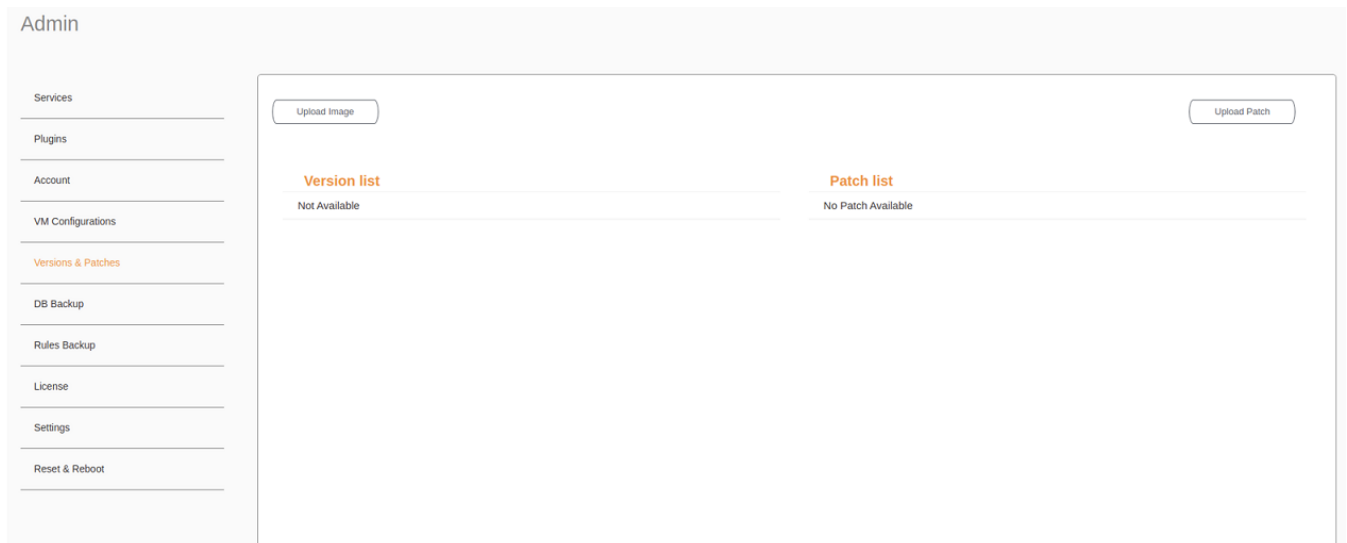
RUCKUS frequently releases updates to RUCKUS IoT Controller. The administrator normally receives any updates about new and updated software by email.

Uploading an Image

RUCKUS sends periodic notifications by email regarding new versions of the RUCKUS IoT Controller.

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

FIGURE 75 Uploading an Image



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

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**.

FIGURE 76 Initiating the Upgrade Process

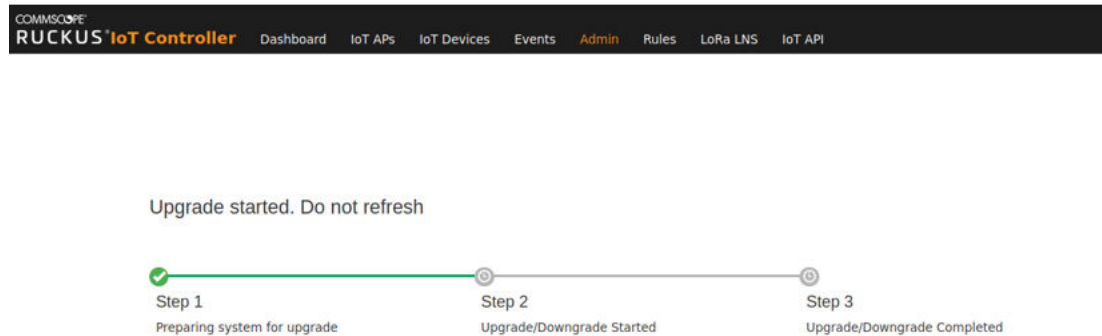
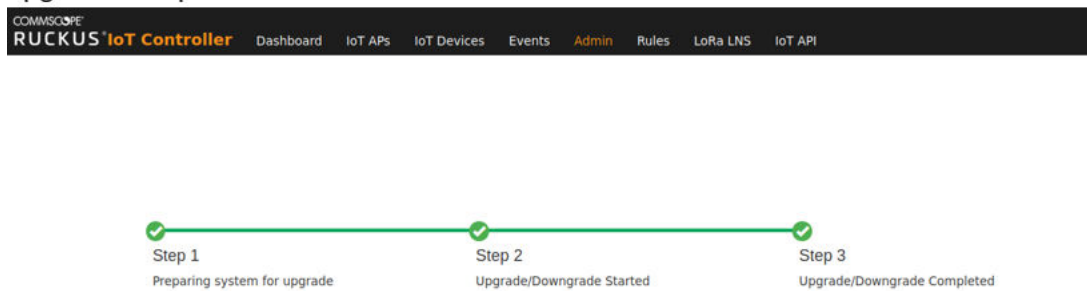


FIGURE 77 Completing the Upgrade Process



Upgrade N+1 RUCKUS IoT Controller

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

3. From the version list select the latest version to upgrade and click **Set**.

FIGURE 78 N+1 Upgrade Started

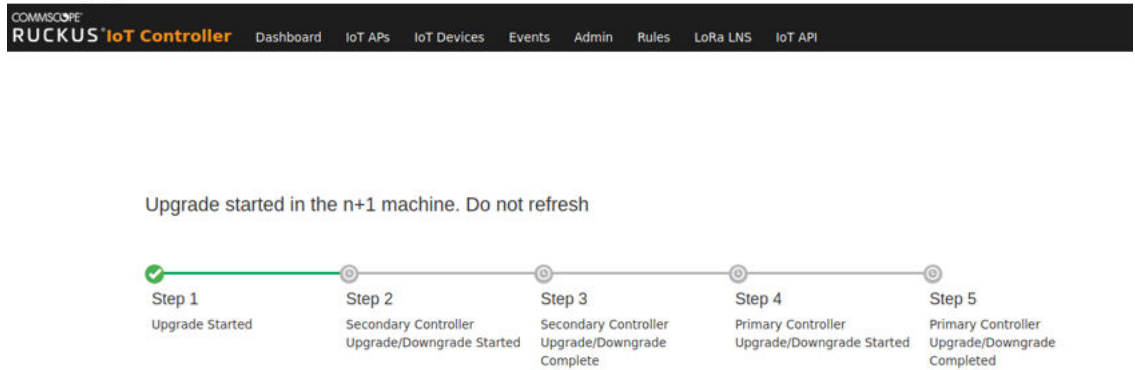
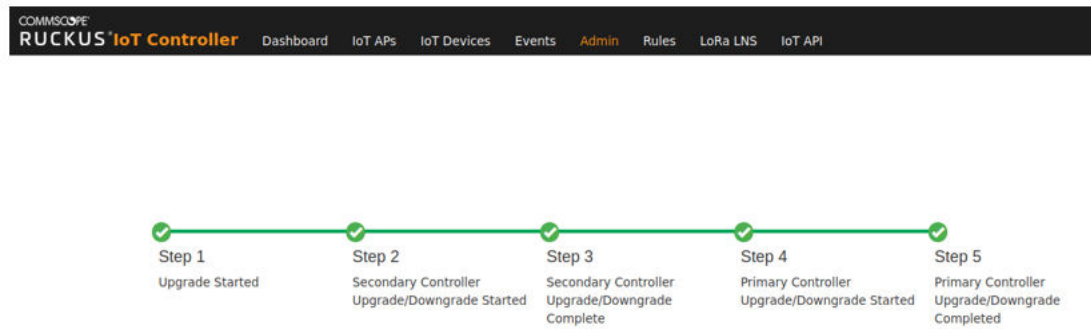


FIGURE 79 N+1 Upgrade Completed



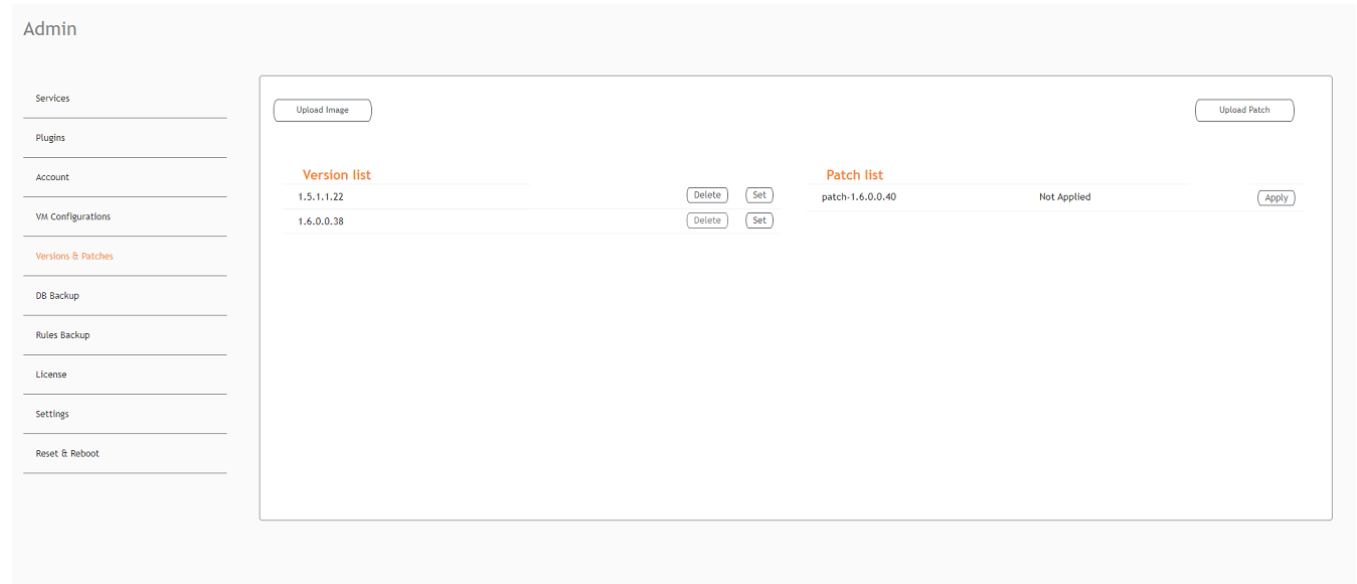
Uploading a Patch

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 80 Uploading a Patch



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

ATTENTION

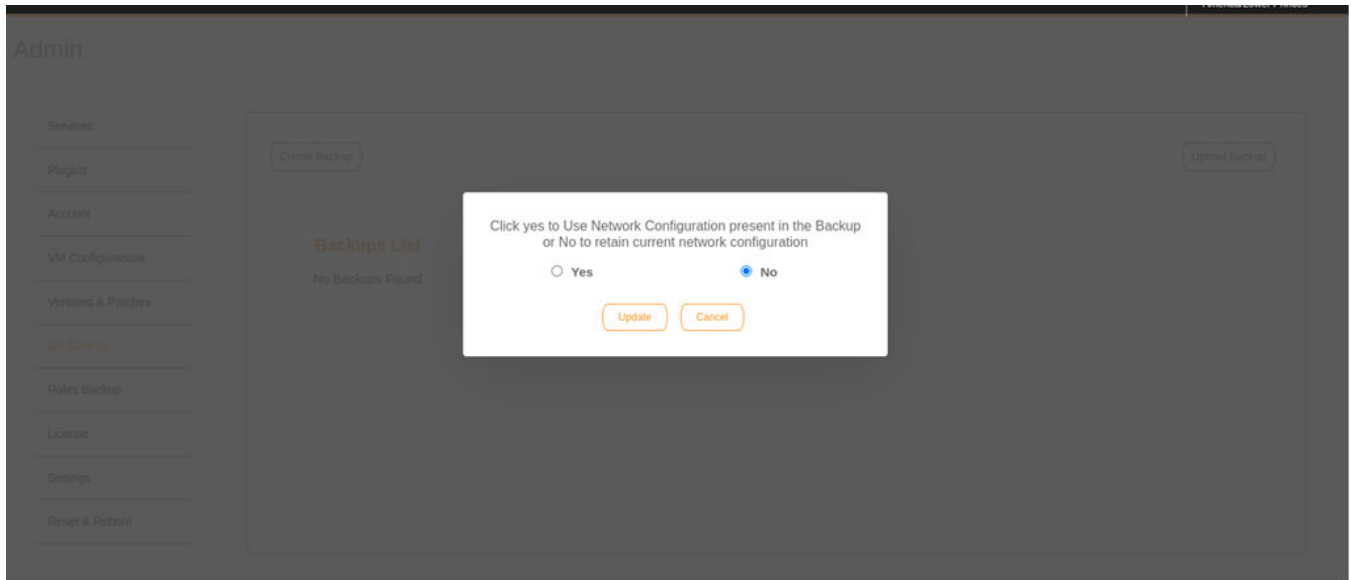
You cannot revert a patch.

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 81 Backing Up or Restoring Files



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

NOTE

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

Use Network Configuration Present in Backup , so you can select either static or dynamic network configuration present in the backup file.

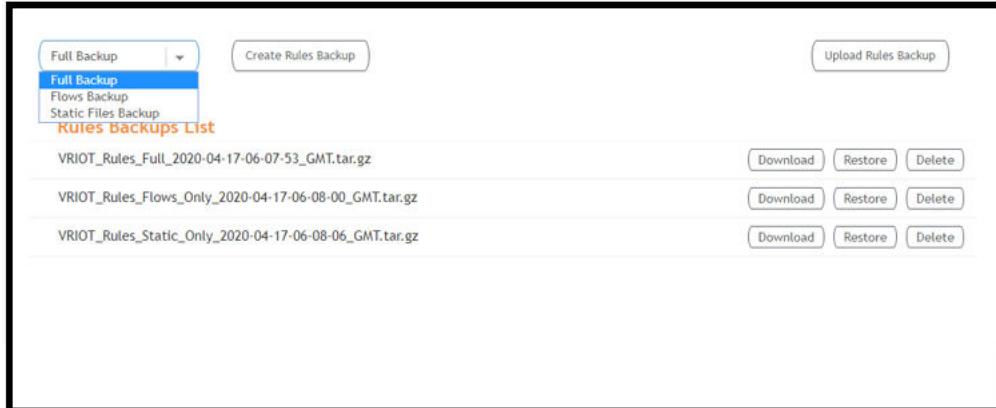
Backing up Rules

The RUCKUS IoT Controller allows you to back up and restore the static files, and node-red flows. You can restore an existing flow or file on the RUCKUS IoT Controller from which it originated, or restore a from a different RUCKUS IoT Controller. Backed up files are in the tar.gz format.

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

- In the left navigation pane, click **Rules Backup**.

FIGURE 82 Backing Up or Restoring Rules



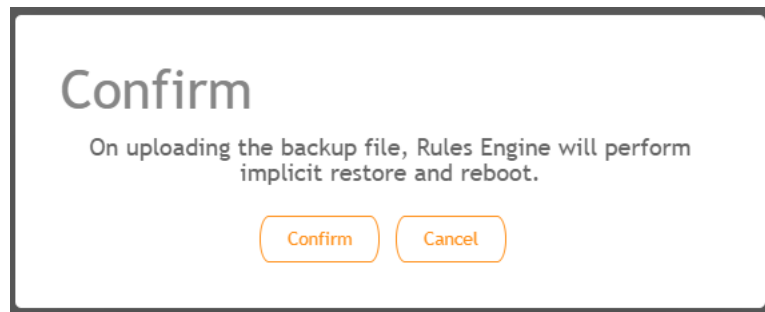
- Select either of the following from the drop-down, and click **Create Rules Backup**.

- **Full Backup**: It is the back up of statics files and nodal flows.
- **Flows Backup**: It is the back up of nodal flows.
- **Static Files Backup**: It is the back up of static files.

- Click **Upload Rules Backup** to upload back up.

A dialog-box appears as below, click **Confirm**.

FIGURE 83 Confirming Upload of Backup File



- Click **Download** to download the backup, **Restore** to restore the backup, and **Delete** to delete the backup.

Uploading the RUCKUS IoT Controller License

To obtain and activate the license, refer to "Activating a License" in the *RUCKUS IoT Controller Software Installation Guide*.

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

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

Managing IoT Controller System Configuration

Uploading the RUCKUS IoT Controller License

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

FIGURE 84 Uploading a License

Controller serial number: **10CF4GV8TS5DX77NT379QG09JQTE**

Upload License

Device capacity license used: **438**

Device capacity license remaining: **unlimited**

Device capacity license total: **unlimited**

Primary License List

Name	License type	Description	Start date	Expiry date	Count
INSTANCE-IOTC	Enabled	Instance Trial license	16-Mar-2022	14-Jun-2022	1
CAPACITY-IOTC	Enabled	Capacity Trial license	16-Mar-2022	14-Jun-2022	Unlimited

3. Click **Upload License** to upload the license. The License check-out means consuming a device capacity license, and License check-in means forfeiting a device capacity license. The License check-out happens when Device gets added. The License check-in happens when Device is deleted.

NOTE

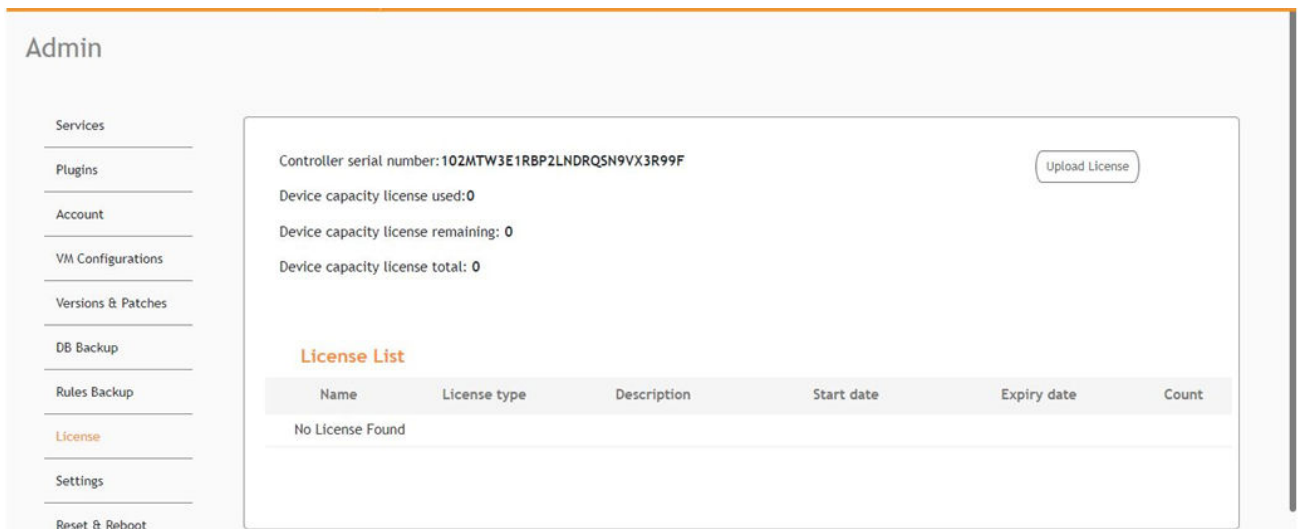
In N+1 configuration, for the secondary controller the license capacity is unlimited for 30 days.

The Upload License page displays the following information:

- **Controller serial number** : Displays the number of the RUCKUS IoT Controller serial number which can be used to activate the license.
- **Device capacity license used:** Displays the number of licenses used by Devices.

NOTE

If no core license is uploaded after expiry of trial then the GUI is redirected to a warning message as below, and access to the controller comes to a halt until you upload the new license.



- **Device capacity licenses remaining:** Displays the number of unused licenses by Devices.
- **Device capacity license total** : It is the total capacity available for the device. It will appear only when the user uploads the device capacity license. To generate a license, refer to "Activating a License" in the *RUCKUS IoT Controller Software Installation Guide*.
- **License List:** Lists the details of the license, such as **Name**, **License Type**, **Description**, **Start date**, **Expiry date** and **count**.

Change the Settings

N+1 Configuration and Hot Upgrade can be performed only when SSH is enabled.

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

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

FIGURE 85 Settings Page



- Enable **SSH**.

NOTE

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

FIGURE 86 Showing Error on Disabling SSH

```
*****
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 Primary Controller(1) / Secondary Controller(2) / Exit(x) :1

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

Enter Secondary Controller IP :10.174.113.91
Enter preferred Virtual IP :10.174.113.70
N+1 will stop all services & configurations in Secondary Controller. Enter Y/N to continue : y

Error: To configure N+1 please enable SSH in vRIoT controller.
```

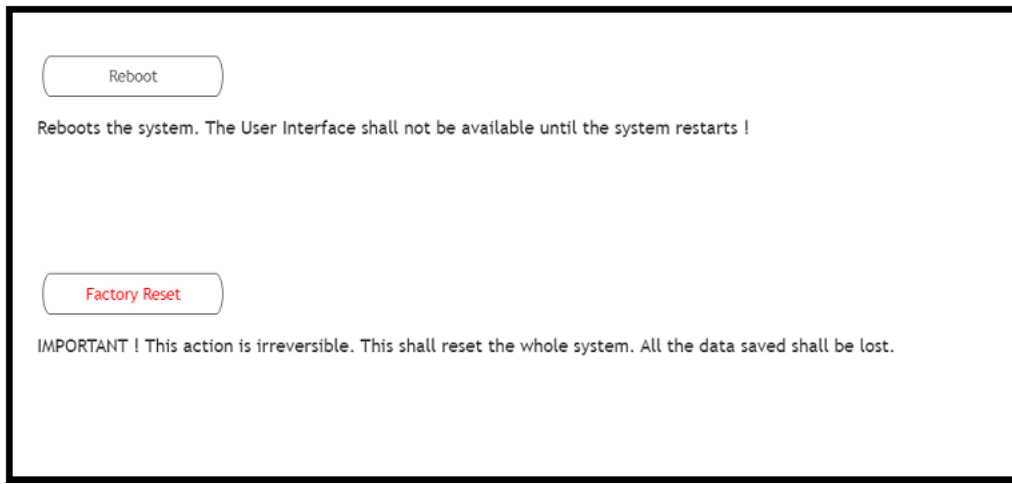
Rebooting RUCKUS IoT Controller

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

Complete the following steps to reboot the RUCKUS IoT Controller.

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

FIGURE 87 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.



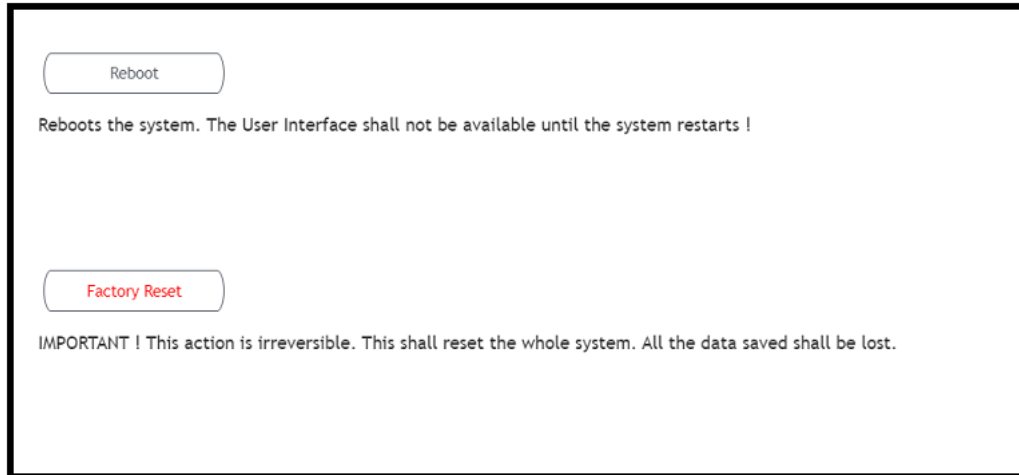
CAUTION

Performing the reset action is irreversible.

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

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

FIGURE 88 Resetting RUCKUS IoT Controller



3. Click **Factory Reset**.

Managing IoT Access Points

- IoT AP Overview..... 85
- Adding an IoT AP..... 88
- Editing an IoT AP..... 90
- Adding Tags to an AP..... 92
- Approval of IoT APs..... 94
- Exporting IoT APs to CSV..... 94

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 (RKSLI). RKSLI mode is not encouraged, and must be used only if a DHCP server is not present.

DHCP Option 43

The IoT Access Point supports Option 43 with the following suboptions:

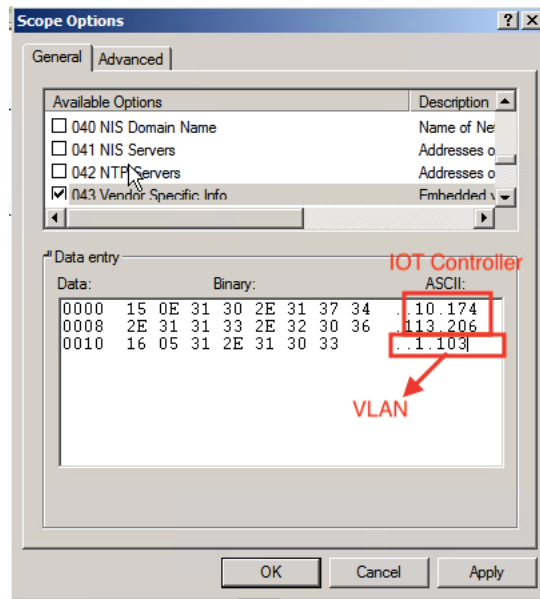
- Suboption 21: Used to configure a RUCKUS IoT Controller IPv4 address or FQDN (mandatory)
- Suboption 22: Used to set the control VLAN for IoT Control/Data traffic (optional)

Option 43 supports both binary and ASCII formats. The IoT Access Point bootup process checks for Option 43 and suboptions 06, 21 and 22. Once the application receives this information, it uses the information to connect to the controller over the Pubsub channel.

You can use the DHCP Option 43 sub-option code 06 to set the SCG/vSZ/SZ IP address in the format SubCode /Length/ (Value In Hex). For example : If the IP address is 10.24.123.4, then the hex string is as follows 06 0b 31302e32342e3132332e34.

The DHCP Option 43 sub-option code 21 and 22 is used to set the RUCKUS IoT Controller IP address.

For Example, Windows DHCP Configuration with Sub-option 21 and 22:



Linux DHCP option 43, sub option 21 configuration is as follows:

- option RKUS.scg-address "192.168.0.3"
- option RKUS.riot-address "192.168.0.2";

dhcp_opt43 configuration subopt 22- "vlan_mode.vlan_id"

- #option RKUS.iotvlan-address "0.4" -enables onlink VLAN
- #option RKUS.iotvlan-address "1.4" -enables offlink VLAN
- Offlink VLAN configuration is used when the IOT Gateway/AP and IOT controller are in different networks.
- Onlink VLAN configuration is used when the IOT Gateway/AP and IOT controller are in same network.

RUCKUS Command Line Interface

The `set iotg-mqtt-brokeripRUCKUS-IoT-Controller-IP-address` command can be used to discover the RUCKUS IoT Controller.

USB Power

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

FIGURE 89 Displaying a Shortage of USB Power

The screenshot shows the RUCKUS IoT Controller web interface. The top navigation bar includes 'Dashboard', 'IoT APs', 'IoT Devices', 'Events', 'Admin', and 'IoT API'. The user is logged in as 'vriot_B390_primary' with 'N+1 : Disabled'. The version is '1.4.0.0.17' and the location is 'America/Los Angeles'.

The main section is titled 'IoT Access Points'. On the left, there are two clusters: '[sibly-iot-cluster]' and '[vSZ-iot-Lab2]'. The 'Pre-Approve IoT APs' section contains a table with the following data:

Name	MAC ID	IP Address	Protocols
dhcp-172-16-113-73	E8:1D:A8:0A:F2:80	172.16.113.73	BLE

The right-hand panel shows the configuration for 'dhcp-172-16-113-73', which is 'Online'. It includes tags: 'baas', 'ibeacon', 'dhcp-172-16-113-73', and 'sibly-ap'. Below the tags, there are buttons for 'Scan for IoT Devices' and 'Restart IoT Service'. The 'IoT APs Settings' section features a red warning banner: 'USB is not having enough power'. The settings are as follows:

- IoT AP Approve: Yes (toggle on) [Apply]
- IoT Management VLAN: No (toggle off) [Apply]
- IoT CoExistence: Off (toggle off) [Apply]
- IP: 172.16.113.73
- MAC: E8:1D:A8:0A:F2:80
- Net Mask: 255.255.254.0
- DNS: 172.16.200.3

NOTE

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

Adding an IoT AP

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

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

1. From the main menu, click **IoT APs**.
The **IoT Access Points** page is displayed.

FIGURE 90 IoT Access Points Page

The screenshot displays the 'IoT Access Points' management interface. On the left, there is a tree view showing the network structure with folders for '[nactus]', '[BDC610-1-CLUST]', and '[BDC-600-2-CLUST]'. The main area is titled 'Pre-Approve IoT APs' and contains a table of IoT APs. The table has columns for Name, MAC ID, IP Address, Protocols, Uptime, Actions, and Tags. The 'Batch Actions' dropdown is set to 'Select'. At the bottom, it shows 'Total IoT APs : 529', an 'Export IoT APs to CSV' button, and a 'Displaying 10 gateways' section with 'Previous' and 'Next' navigation buttons.

Name	MAC ID	IP Address	Protocols	Uptime	Actions	Tags
H510-Ramesh_DONOT_DISTURB_devices_connected	0C:F4:D5:1E:40:C0	172.29.124.58	ZIGBEE	37 days, 5:25:11	[trash]	All H510-Ramesh_DONOT_DISTURB_0C:F4:D5:1E:40:C0
R550-5420-AA_connected	80:03:84:03:54:20	172.29.124.235	BLE,ZIGBEE,ZIGBEE_AA	33 days, 3:18:08	[trash]	All R550-5420-AA_connected_80:03:84:03:54:20
R650-92E0-AA_Connected	DC:AE:EB:00:92:E0	172.29.124.251	ZIGBEE,ZIGBEE_AA,BLE	6 days, 22:57:21	[trash]	All DC:AE:EB:00:92:E0_kontakt_ibeacon_eddystat
R610-Ramesh	B4:79:C8:04:E3:00	172.29.124.37	BLE	37 days, 5:15:40	[trash]	All B4:79:C8:04:E3:00_kontakt_ibeacon_eddystat
R610@de\$K	B4:79:C8:04:E6:F0	10.74.136.122	ZIGBEE_DK,ZIGBEE_AA	37 days, 1:25:11	[trash]	All R610-MY_DESK_OFFICE_SEAT_B4:79:C8:04:E6:F0
R510-Ramesh	D8:38:FC:1B:FC:D0	172.29.124.71	BLE	2 days, 11:59:13	[trash]	All D8:38:FC:1B:FC:D0_kontakt_ibeacon_eddystat
R550-depop	84:23:88:2E:F0:50	10.174.112.36	BLE	37 days, 5:23:30	[trash]	All R550-depop_84:23:88:2E:F0:50_kontakt_ibeacon
H510-my-desk	D8:38:FC:25:C4:C0	172.29.116.71	BLE	34 days, 0:35:29	[trash]	All H510-my-desk_D8:38:FC:25:C4:C0_kontakt_ibeacon
R550-0b40-DK_AA_Connecte70.ca:97:2d:0b:40	70:CA:97:2D:0B:40	172.29.125.12	ZIGBEE,ZIGBEE_AA,ZIGBEE_DK	13 days, 0:16:17	[trash]	All R550-0b40-DK_AA_Connected_70:CA:97:2D:0B:40
H550-2A70	34:20:E3:2D:2A:70	172.29.124.254	BLE	5 days, 23:16:44	[trash]	All H550-2A70_34:20:E3:2D:2A:70_kontakt_ibeacon

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

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

FIGURE 91 Adding a Single IoT AP

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

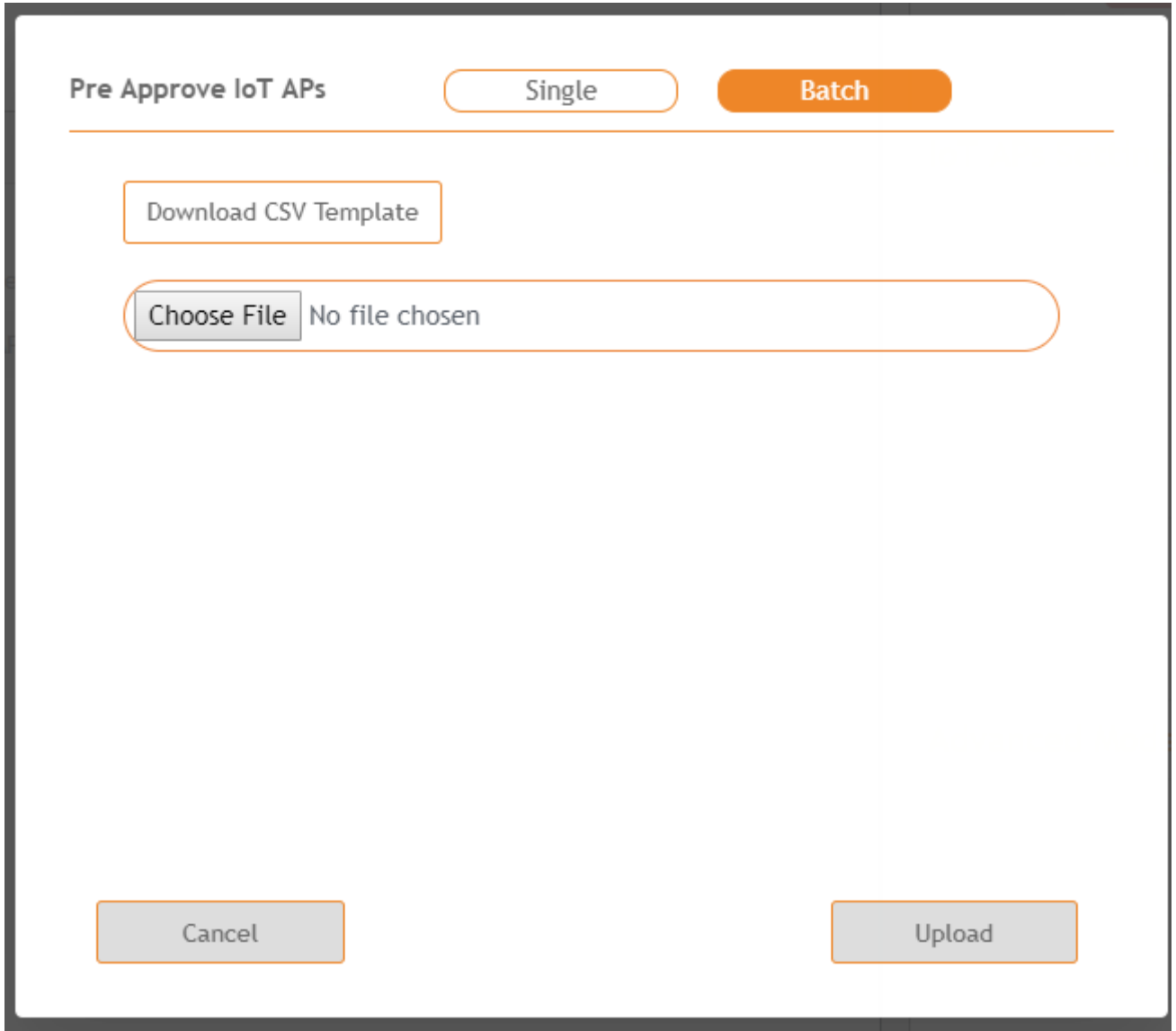
4. Enter the MAC address of the IoT AP and click **Save**.

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 92 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.

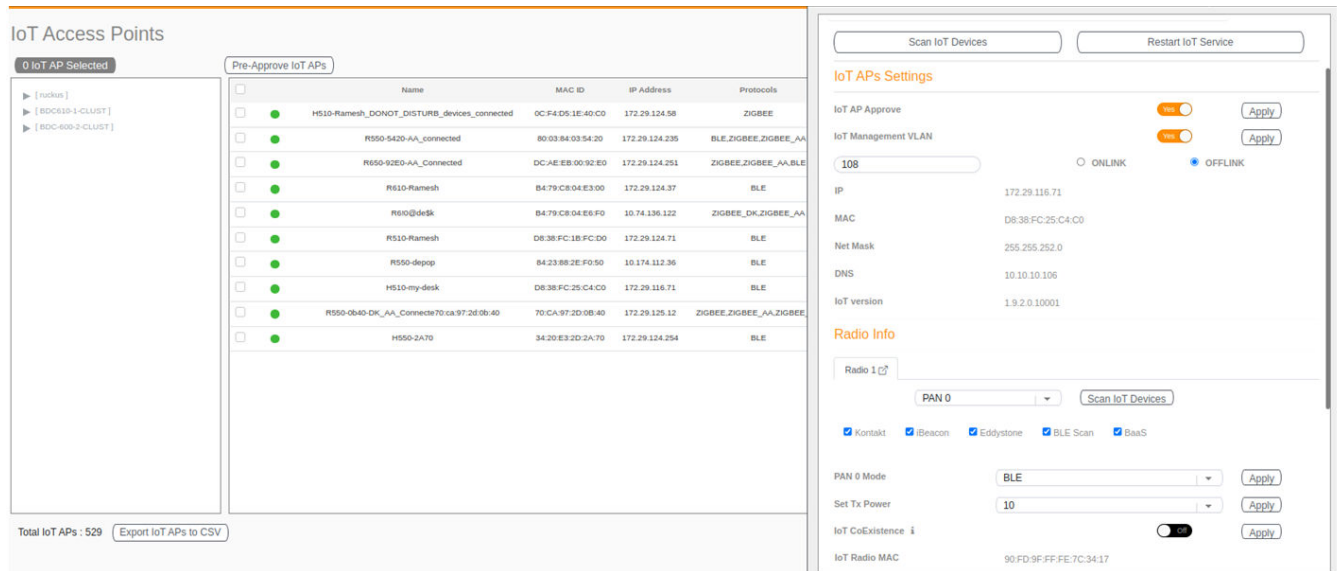
Single IoT Access Point Mode

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 93 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, Zigbee DK)
- 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

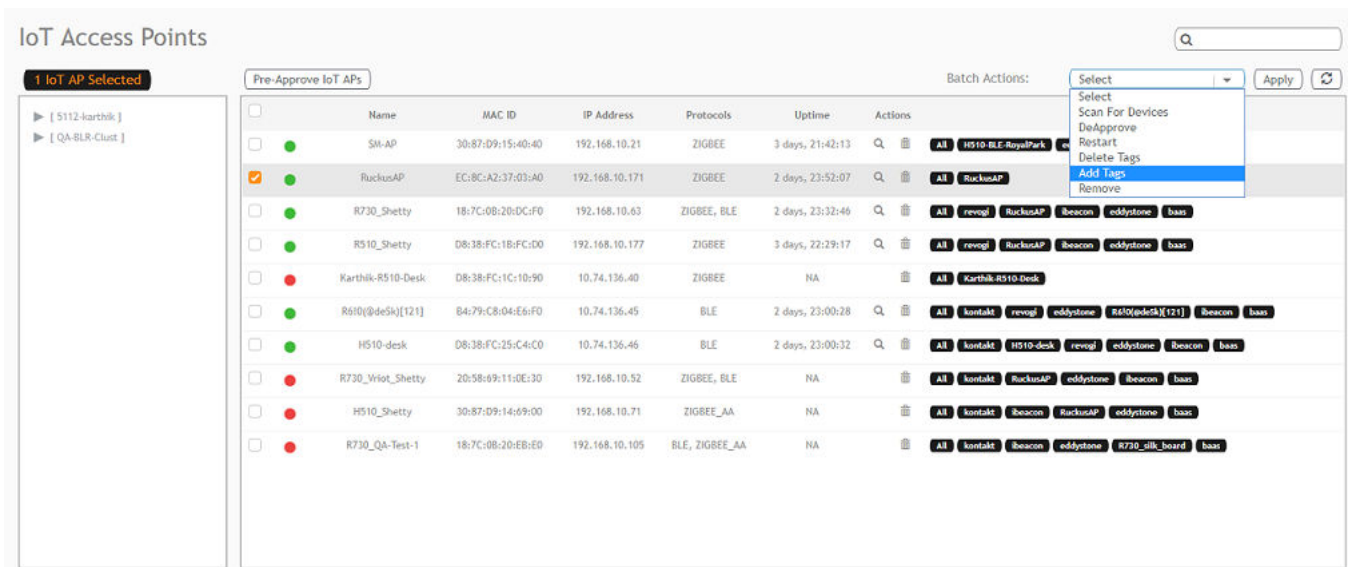
The AP tags are a way of grouping APs together by applying identifying tags. If the **Globally enable connector on all valid APs** is disabled when activating a plugin, complete the following steps to add tags to an AP to activate a plugin on the AP.

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.

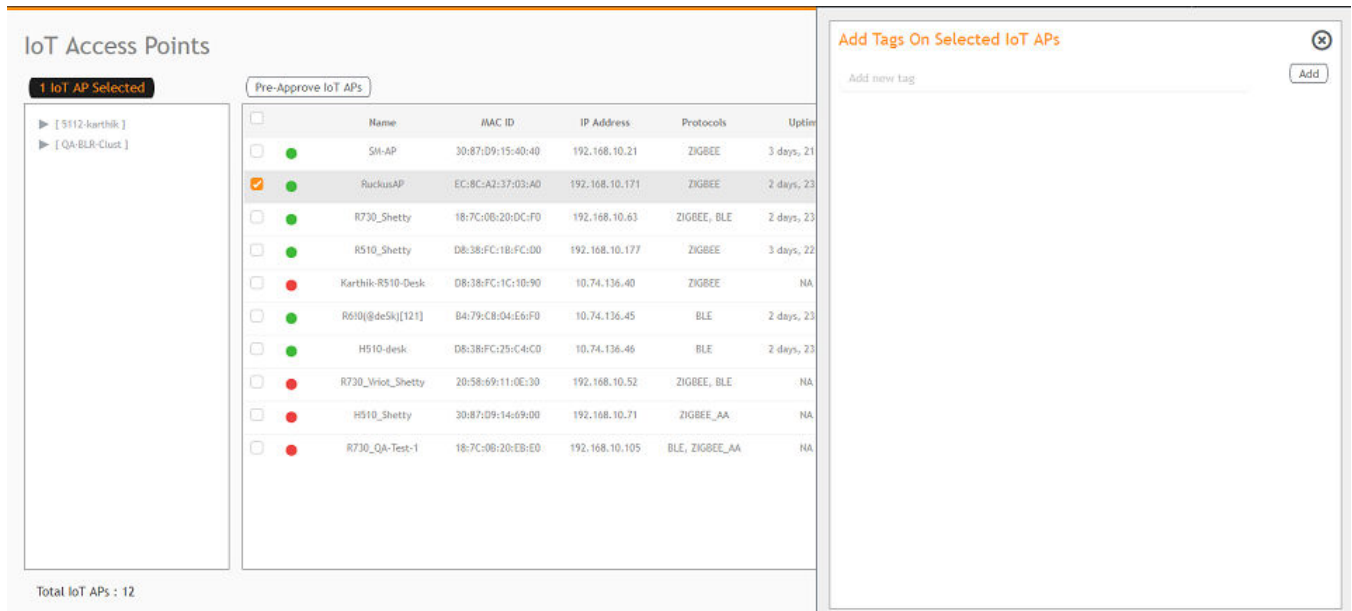
FIGURE 94 Selecting an AP to Add Tags



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

- 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 95 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

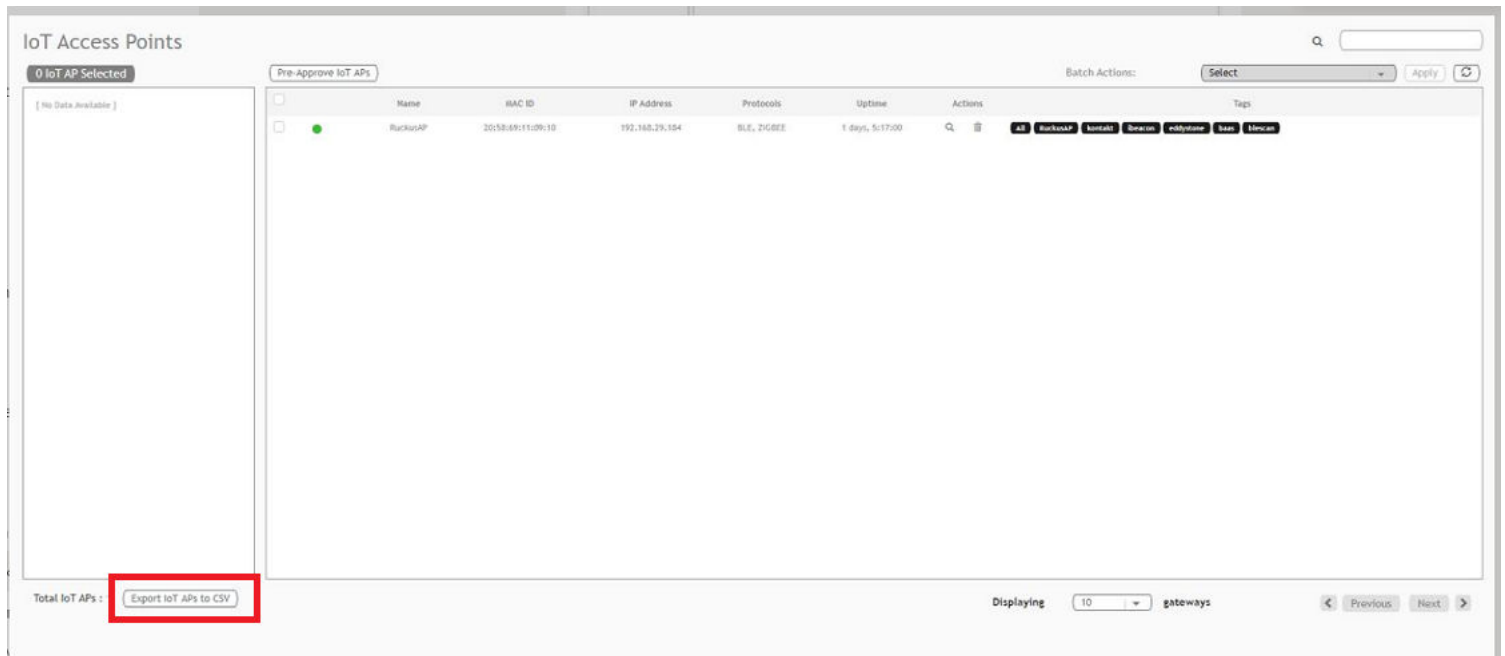
Plugin	Tag Name
Kontakt.io Beacons	kontakt
iBeacon	ibeacon
Beacon as a Service	baas
Eddystone	eddstone
BLE Scan	blescan

Approval of IoT APs

The IoT APs must be approved by the administrator. The RUCKUS I100 IoT Module is activated only for approved APs. There is an option to disapprove a previously approved AP. This operation can be performed on a single AP (using Single IoT Access Point Mode) or on multiple APs (using Bulk AP Mode).

Exporting IoT APs to CSV

You can export IoT APs to CSV by clicking **Export IoT APs to CSV**, which allows to download all the APs in the IoT APs page, and the corresponding information into a CSV format file that can be saved.



Enabling BaaS Major and Minor Number

BaaS is enabled only when the BaaS plugin is activated.

Complete the following steps to enable BaaS Major and Minor Number.

1. From the main menu, click IoT APs.
A list of selected IoT APs is displayed.

2. Click an IoT AP, and update the fields **BAAS iBeacon Major No** and **BAAS iBeacon Minor No** in AP sidebar.

NOTE

You can update a single IoT AP.

The screenshot displays the IoT Controller interface. On the left, a table titled 'Pre-Approve IoT APs' contains one entry:

	Name	MAC ID	IP Address
<input type="checkbox"/>	RuckusAP	0C:F4:D5:1E:22:10	192.168.20.10

On the right, the 'Radio Info' sidebar for 'Radio 0' is shown. It includes the following settings:

- Kontakt
- iBeacon
- Eddystone
- BLE Scan
- BaaS
- Custom BaaS Major Minor No: Yes
- Baas iBeacon Major No:
- Baas iBeacon Minor No:
- Mode: BLE
- Set Tx Power (BLE): 10
- IoT CoExistence: On
- IoT Radio MAC: 90:FD:9F:FF:FE:0C:89:CB
- IoT Radio Mode: ble
- IoT Radio Status: Available
- PAN ID: 0xFFFF
- Channel: NA

3. Select **Batch BaaS operation** from the **Batch Actions** list.

NOTE

You can select one or more APs to add tags.

- To update for more than single IoT AP, update **Baas iBeacon Major No** and **Baas iBeacon Minor No** from sidebar.

FIGURE 96 Updating Baas Major and Minor Number for Multiple IoT APs

The screenshot displays the IoT AP management interface. On the left, a table lists IoT APs with columns for Name, MAC ID, IP Address, and Protocol. The 'H510' AP is selected. On the right, the 'BaaS plugin Batch operations' sidebar is open, showing a 'Custom BaaS Major Minor No' toggle set to 'Yes' and an 'Apply' button. Below the toggle are input fields for 'Baas iBeacon Major No' and 'Baas iBeacon Minor No'.

<input type="checkbox"/>	Name	MAC ID	IP Address	Protocol
<input type="checkbox"/>	R650-Shriram-qa-test	B4:79:C8:3E:75:40	172.29.124.182	NA
<input type="checkbox"/>	R750-Shriram-qa-test	B4:79:C8:3E:72:00	172.29.116.68	NA
<input checked="" type="checkbox"/>	H510	0C:F4:D5:1E:97:D0	172.29.124.215	BLE
<input type="checkbox"/>	R610-Shriram	B4:79:C8:01:F0:30	172.29.124.39	NA
<input type="checkbox"/>	H510-2-SHRIRAM	30:87:D9:14:69:00	172.29.102.22	ZIGBE

BaaS plugin Batch operations

Custom BaaS Major Minor No Yes No

Baas iBeacon Major No

Baas iBeacon Minor No

Managing Devices

- Devices Overview..... 97
- Managing OSRAM Light Bulbs..... 100
- Managing an Assa Abloy Lock..... 101
- Managing the Dormakaba Locks..... 102
- Device Operations for Specific Clusters and Commands..... 114

Devices Overview

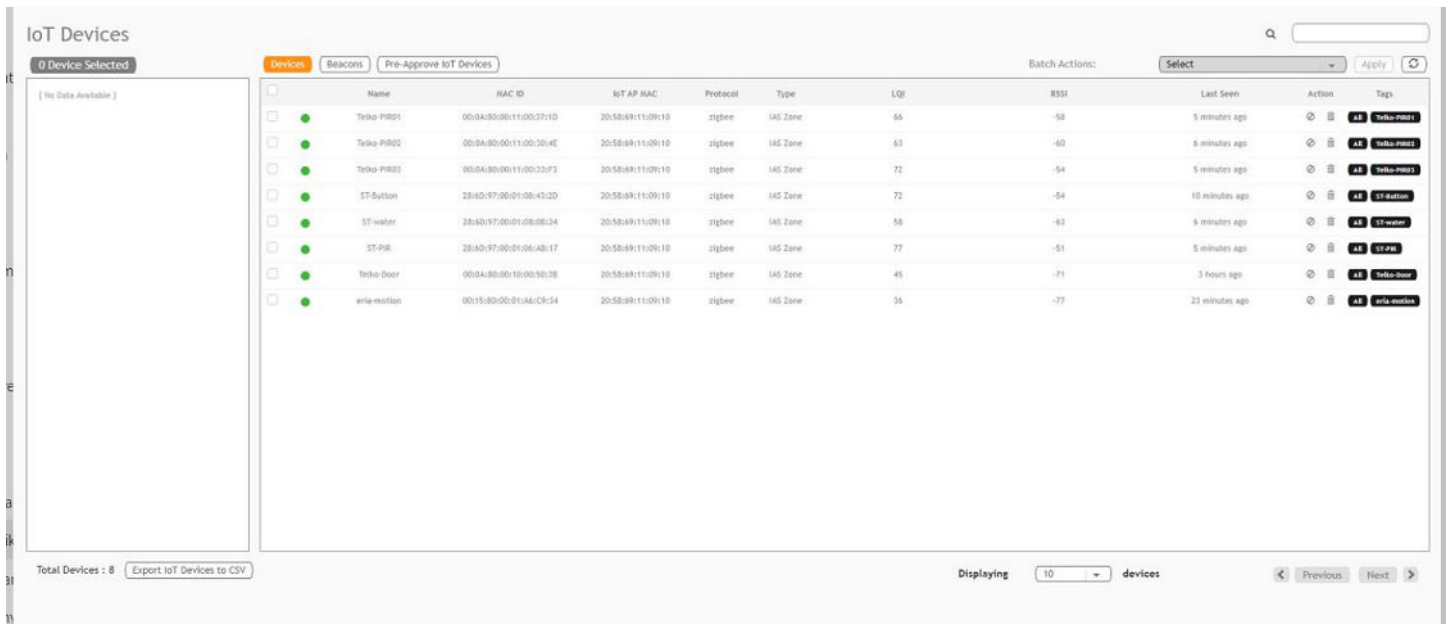
The RUCKUS IoT Controller requires explicit user approval of devices. Only an approved device can be allowed into the IoT infrastructure.

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 97 IoT Devices Page



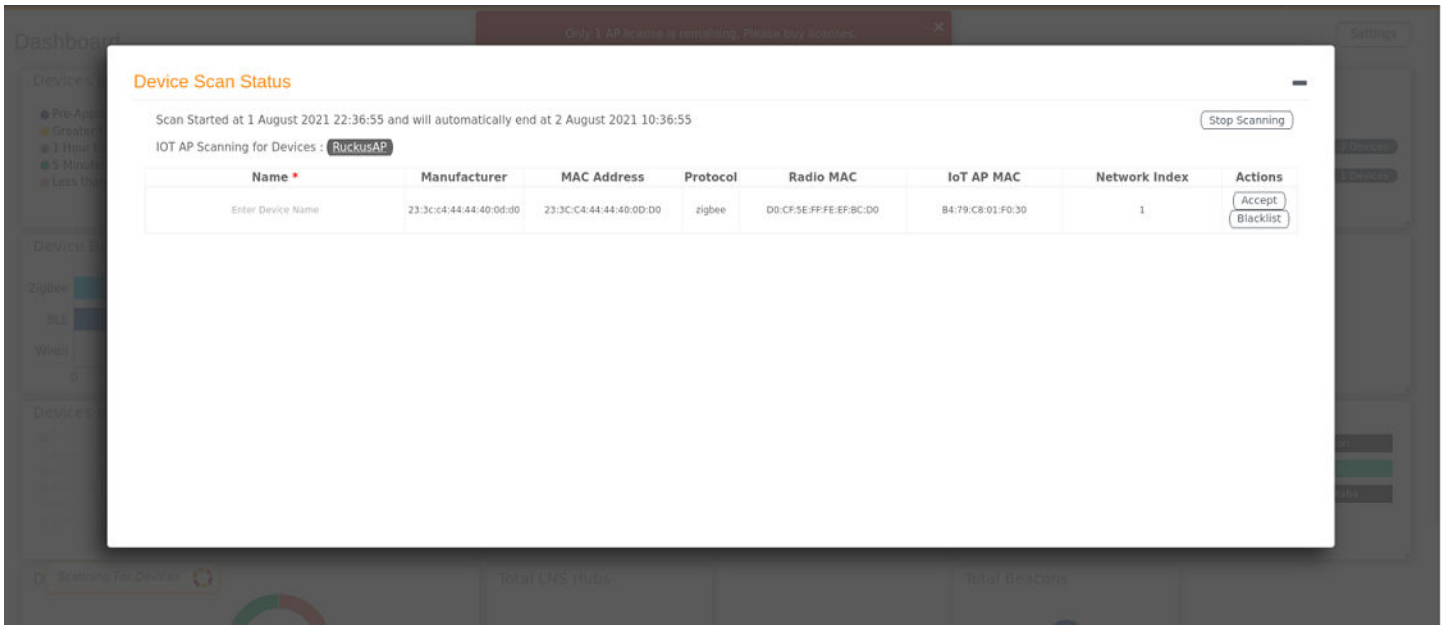
The device scan operation must be performed to start the device discovery process on the gateway.

NOTE

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

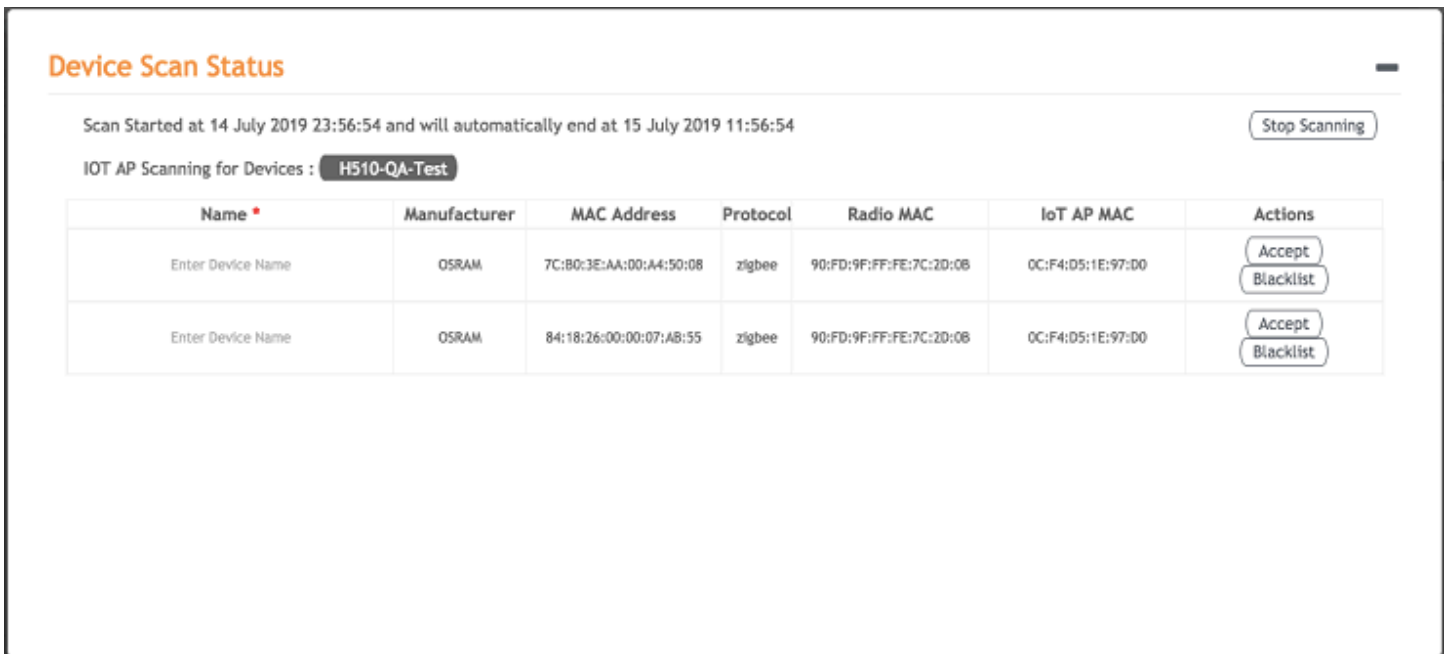
Upon starting device discovery, a dialog box is displayed, as shown in the following figure.

FIGURE 98 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 99 Adding Device After Discovery



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

FIGURE 100 Beacons Page

IoT Devices

Devices **Beacons**

IoT AP
0C:F4:D5:1E:97:D0

Beacon Info

Vendor ID : 0x004C (45)
Latitude : 0 Longitude : 0

Device MAC	Last Seen	RSSI	Data
00:00:2C:B4:3A:1A:22:BE	a few seconds ago	-81	02011A0BFF4C000906032C00000000
00:00:2C:B4:3A:1A:22:BE	a few seconds ago	-83	02011A0BFF4C000906032C00000000
00:00:D5:7C:FF:20:F8:93	a few seconds ago	-72	0201061AFF4C000215F7826DA64FA24E988024BC5B71E0893E897E0D83B3
00:00:C5:D5:A5:CB:6C:81	a few seconds ago	-78	0201061AFF4C000215F7826DA64FA24E988024BC5B71E0893E6D06F43B3
00:00:F8:DA:65:7E:5F:9D	a few seconds ago	-76	0201061AFF4C000215F7826DA64FA24E988024BC5B71E0893E42C5A64FB3
00:00:F1:83:5D:72:C9:33	a few seconds ago	-65	0201061AFF4C000215F7826DA64FA24E988024BC5B71E0893E17BF0E0FB3
00:00:F1:83:5D:72:C9:33	a few seconds ago	-64	0201061AFF4C000215F7826DA64FA24E988024BC5B71E0893E17BF0E0FB3
00:00:F1:83:5D:72:C9:33	a few seconds ago	-61	0201061AFF4C000215F7826DA64FA24E988024BC5B71E0893E17BF0E0FB3
00:00:F7:85:E7:B5:18:16	a few seconds ago	-78	0201061AFF4C000215F7826DA64FA24E988024BC5B71E0893E2F870E08B3
00:00:FE:0A:A0:AC:80:DA	a few seconds ago	-64	0201061AFF4C000215F7826DA64FA24E988024BC5B71E0893EEC13910FB3
00:00:FE:0A:A0:AC:80:DA	a few seconds ago	-59	0201061AFF4C000215F7826DA64FA24E988024BC5B71E0893EEC13910FB3

Total Beacons : 62

Previous Next

The **Export IoT Devices to CSV** will allow to download all the Devices in the IoT devices page and corresponding information into a CSV format file which can be saved.

FIGURE 101 Exporting IoT Devices to CSV

IoT Devices

0 Device Selected

Devices **Beacons** Pre-Approve IoT Devices

Batch Actions: Select Apply

Name	MAC ID	IoT AP MAC	Protocol	Type	LQI	RSSI	Last Seen	Action	Tags
Telko-P801	00:0A:80:00:11:00:37:10	20:5B:69:11:09:10	zigbee	IAS Zone	66	-58	5 minutes ago	⊗	telko-p801
Telko-P802	00:0A:80:00:11:00:30:4E	20:5B:69:11:09:10	zigbee	IAS Zone	63	-60	6 minutes ago	⊗	telko-p802
Telko-P803	00:0A:80:00:11:00:33:F3	20:5B:69:11:09:10	zigbee	IAS Zone	72	-54	5 minutes ago	⊗	telko-p803
ST-button	28:60:97:00:01:08:43:2D	20:5B:69:11:09:10	zigbee	IAS Zone	72	-54	10 minutes ago	⊗	st-button
ST-water	28:60:97:00:01:08:06:24	20:5B:69:11:09:10	zigbee	IAS Zone	58	-63	6 minutes ago	⊗	st-water
ST-PIR	28:60:97:00:01:06:A0:17	20:5B:69:11:09:10	zigbee	IAS Zone	77	-51	5 minutes ago	⊗	st-pir
Telko-Door	00:0A:80:00:10:00:50:38	20:5B:69:11:09:10	zigbee	IAS Zone	45	-71	3 hours ago	⊗	telko-door
erie-motion	00:15:80:00:01:A0:C9:34	20:5B:69:11:09:10	zigbee	IAS Zone	56	-77	23 minutes ago	⊗	erie-motion

Total Devices : **Export IoT Devices to CSV**

Displaying 10 devices

Previous Next

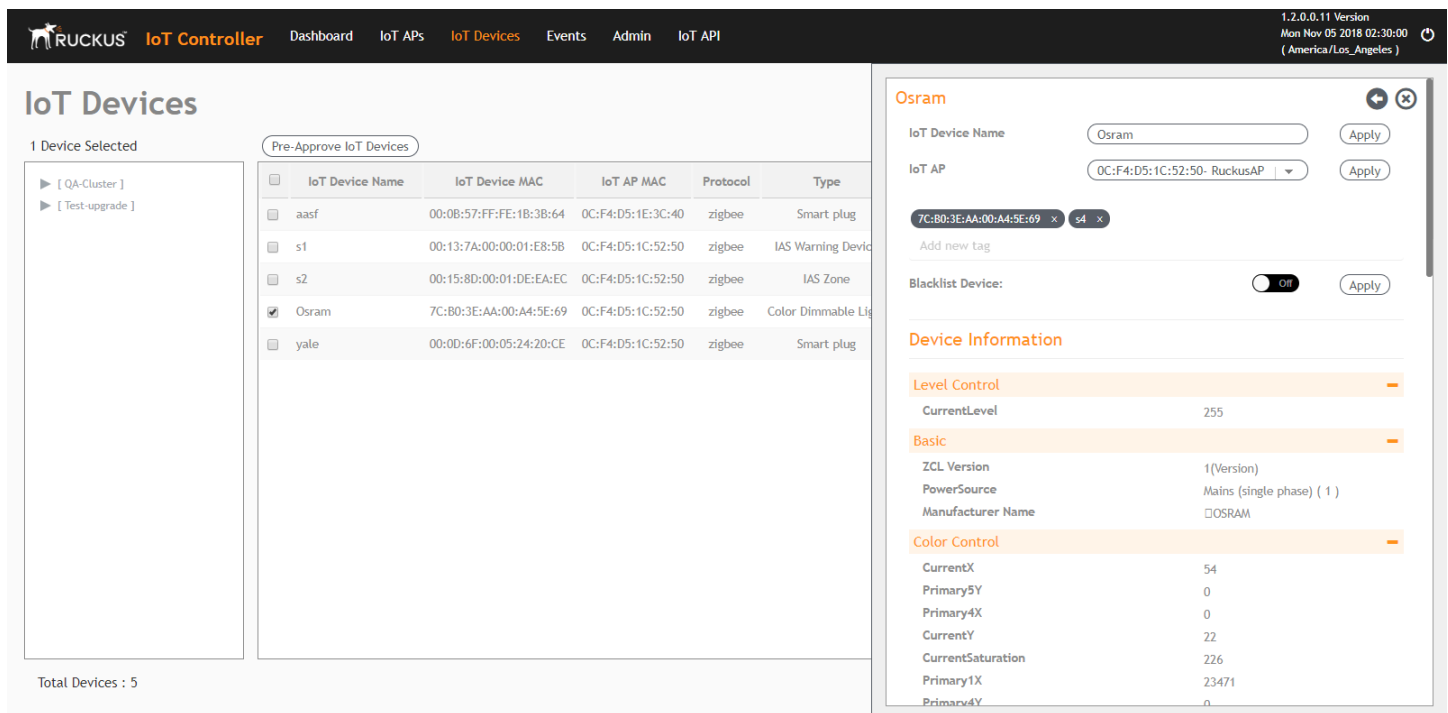
Managing OSRAM Light Bulbs

To discover OSRAM light bulbs, complete the following operations.

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

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

FIGURE 102 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 103 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

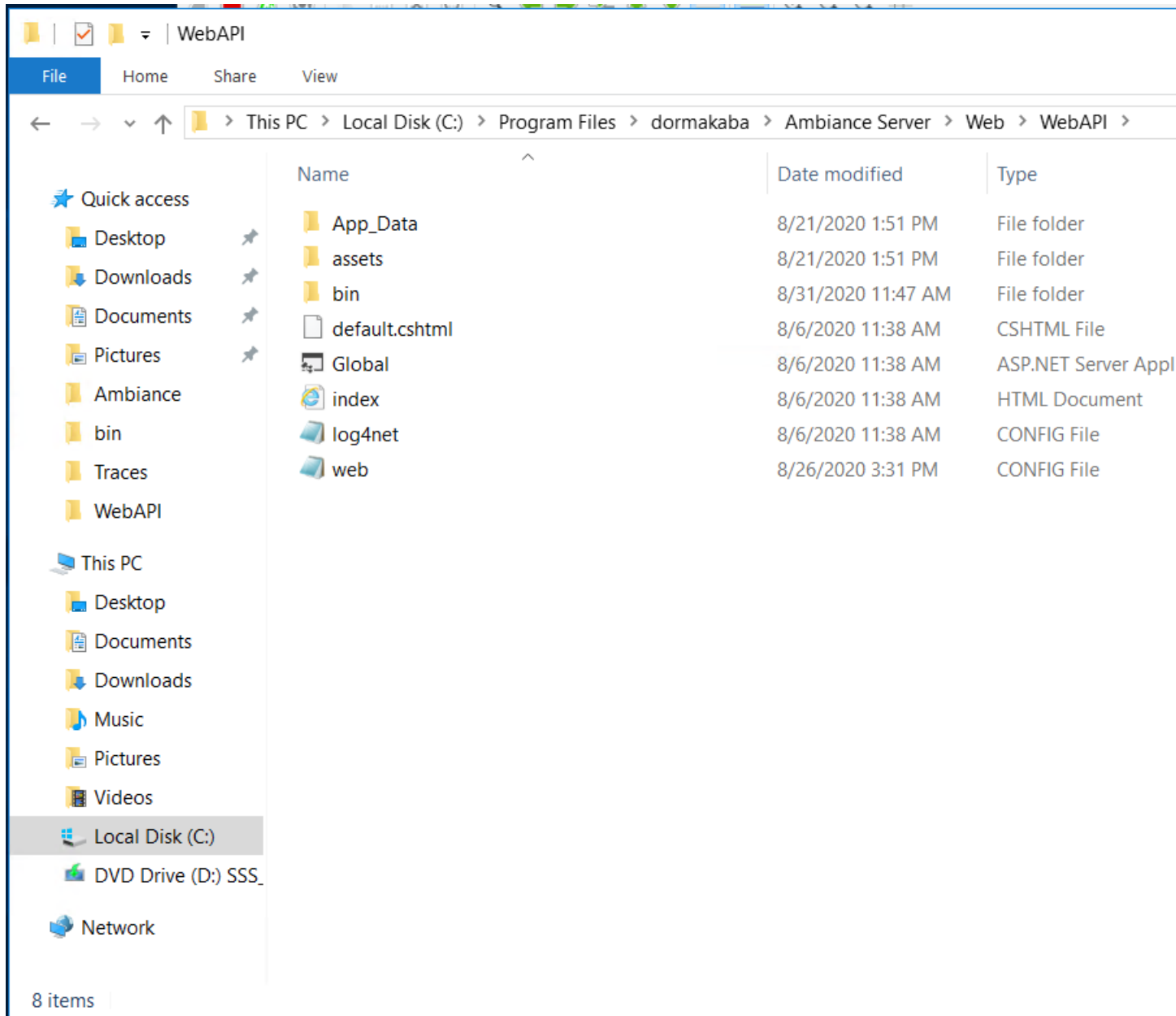
Managing the Dormakaba Locks

The communication between Ambiance Server and RUCKUS IoT Controller takes place through API Endpoints.

You must configure the IP address of the controller by performing the following steps.

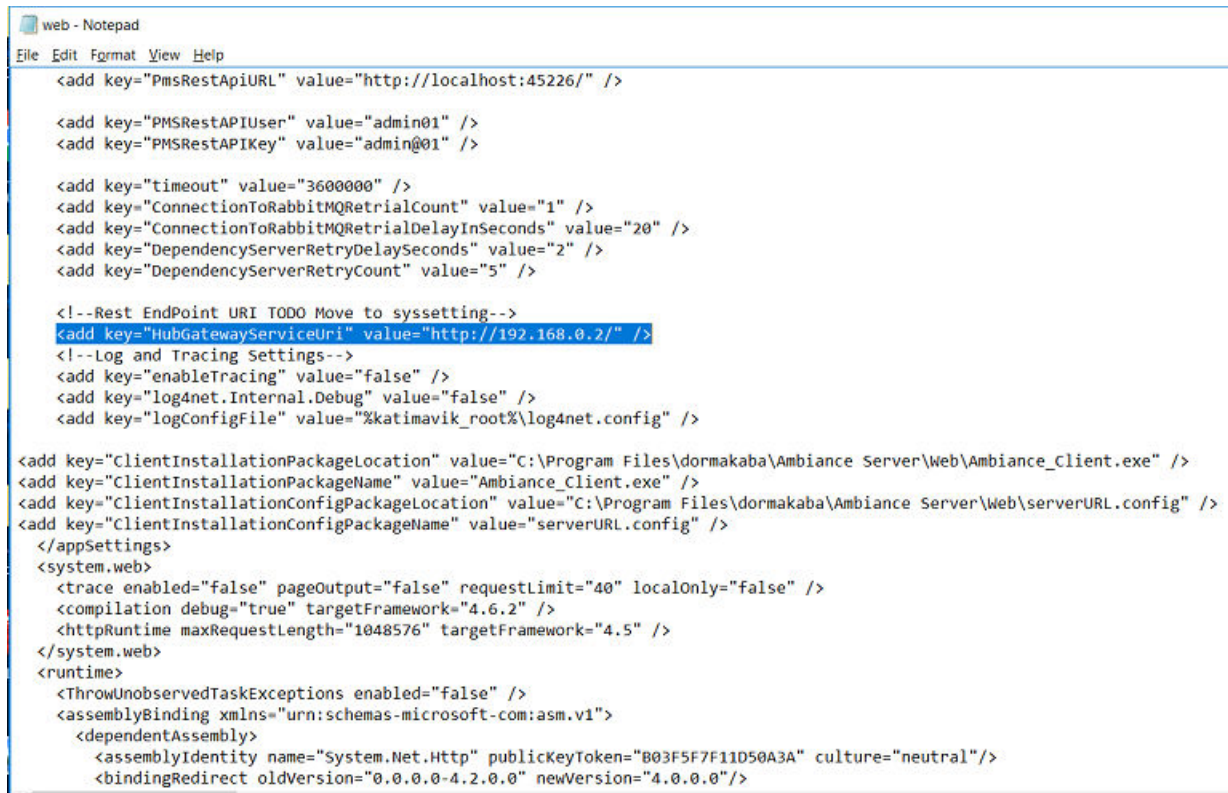
1. In the Ambiance Server, go to `C:\Program Files\dormakaba\Ambiance Server\Web\WebAPI\web.config` file and open the web.config file in notepad.

FIGURE 104 Locating the web config file



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

FIGURE 105 Finding the IP Address



```
web - Notepad
File Edit Format View Help
<add key="PmsRestApiURL" value="http://localhost:45226/" />

<add key="PMSRestAPIUser" value="admin01" />
<add key="PMSRestAPIKey" value="admin@01" />

<add key="timeout" value="3600000" />
<add key="ConnectionToRabbitMQRetrialCount" value="1" />
<add key="ConnectionToRabbitMQRetrialDelayInSeconds" value="20" />
<add key="DependencyServerRetryDelaySeconds" value="2" />
<add key="DependencyServerRetryCount" value="5" />

<!--Rest EndPoint URI TODO Move to syssetting-->
<add key="HubGatewayServiceUri" value="http://192.168.0.2/" />
<!--Log and Tracing Settings-->
<add key="enableTracing" value="false" />
<add key="log4net.Internal.Debug" value="false" />
<add key="logConfigFile" value="%katimavik_root%\log4net.config" />

<add key="ClientInstallationPackageLocation" value="C:\Program Files\dormakaba\Ambiance Server\Web\Ambiance_Client.exe" />
<add key="ClientInstallationPackageName" value="Ambiance_Client.exe" />
<add key="ClientInstallationConfigPackageLocation" value="C:\Program Files\dormakaba\Ambiance Server\Web\serverURL.config" />
<add key="ClientInstallationConfigPackageName" value="serverURL.config" />
</appSettings>
<system.web>
  <trace enabled="false" pageOutput="false" requestLimit="40" localOnly="false" />
  <compilation debug="true" targetFramework="4.6.2" />
  <httpRuntime maxRequestLength="1048576" targetFramework="4.5" />
</system.web>
<runtime>
  <ThrowUnobservedTaskExceptions enabled="false" />
  <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
    <dependentAssembly>
      <assemblyIdentity name="System.Net.Http" publicKeyToken="B03F5F7F11D50A3A" culture="neutral"/>
      <bindingRedirect oldVersion="0.0.0.0-4.2.0.0" newVersion="4.0.0.0"/>
    </dependentAssembly>
  </assemblyBinding>
</runtime>
```

Discovering Dormakaba Lock

Dormakaba locks cannot be controlled using the RUCKUS IoT Controller. To discover a Dormakaba lock and to add it in the controller, perform the following steps.

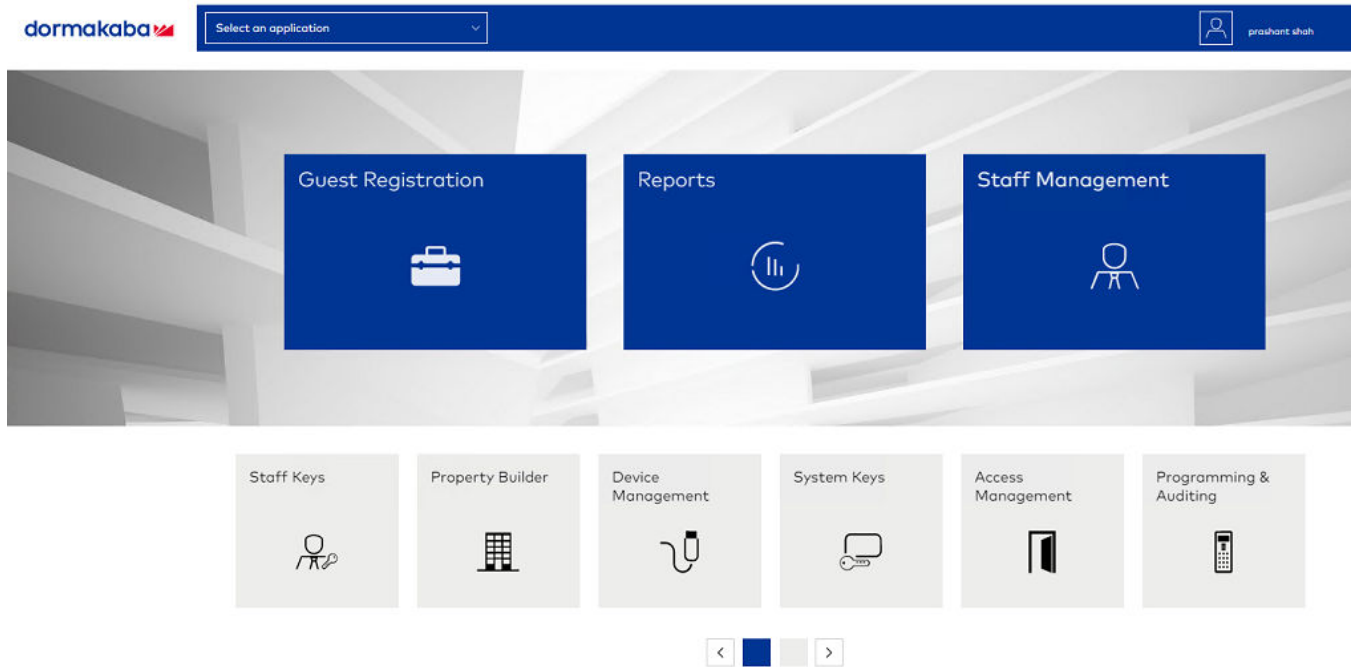
- Select the Gateway and start a Device Scan from Ambiance UI.
A scan window appears in the UI.
- Swipe the Dormakaba Pairing Card across the lock.
- Ensure that the LED blinks.
Dormakaba Lock details will show in the Scan Window of the controller.
- Add the lock to the Ruckus IoT Controller (if it is not already pre-approved).
- Go to **Device Management** page, select the **Gateway**, click on **Next** to Access Points in the Ambiance UI.
You can now verify if the lock has established its communication with Ambiance Server.

Blocking and Unblocking Dormakaba Lock

Dormakaba locks operate using the Ambiance server. Complete the steps below to onboard lock.

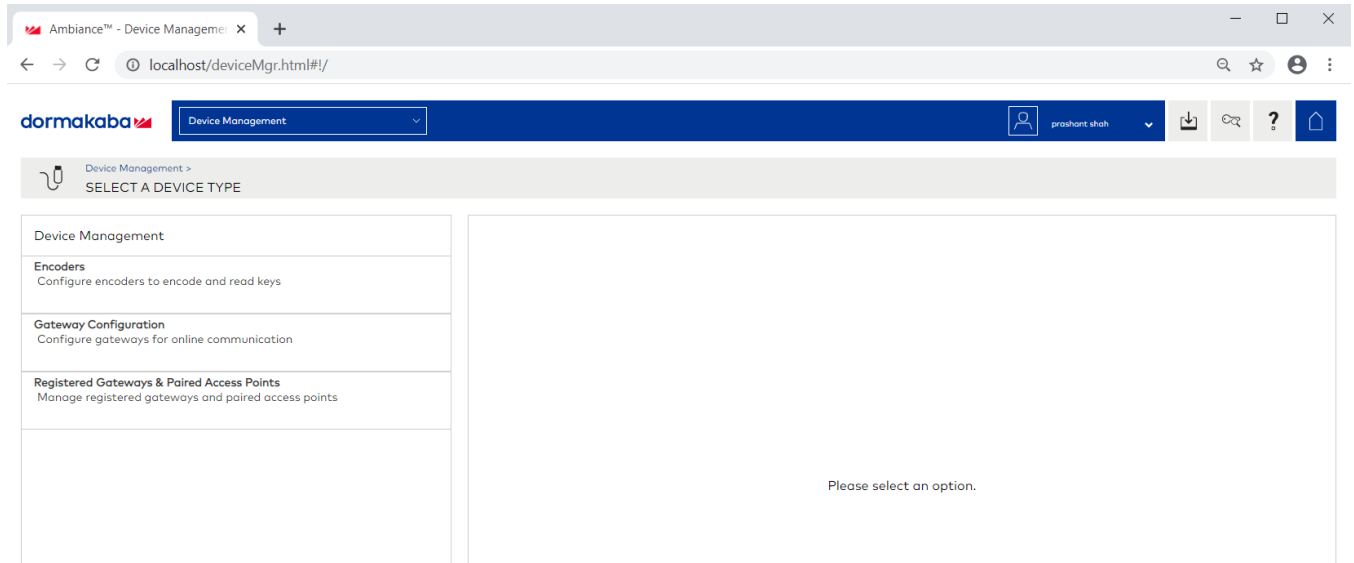
1. Login to the Ambiance Server. The default username and password is **Admin01** and **Admin@01**.

FIGURE 106 Login into Dormakaba Plugin



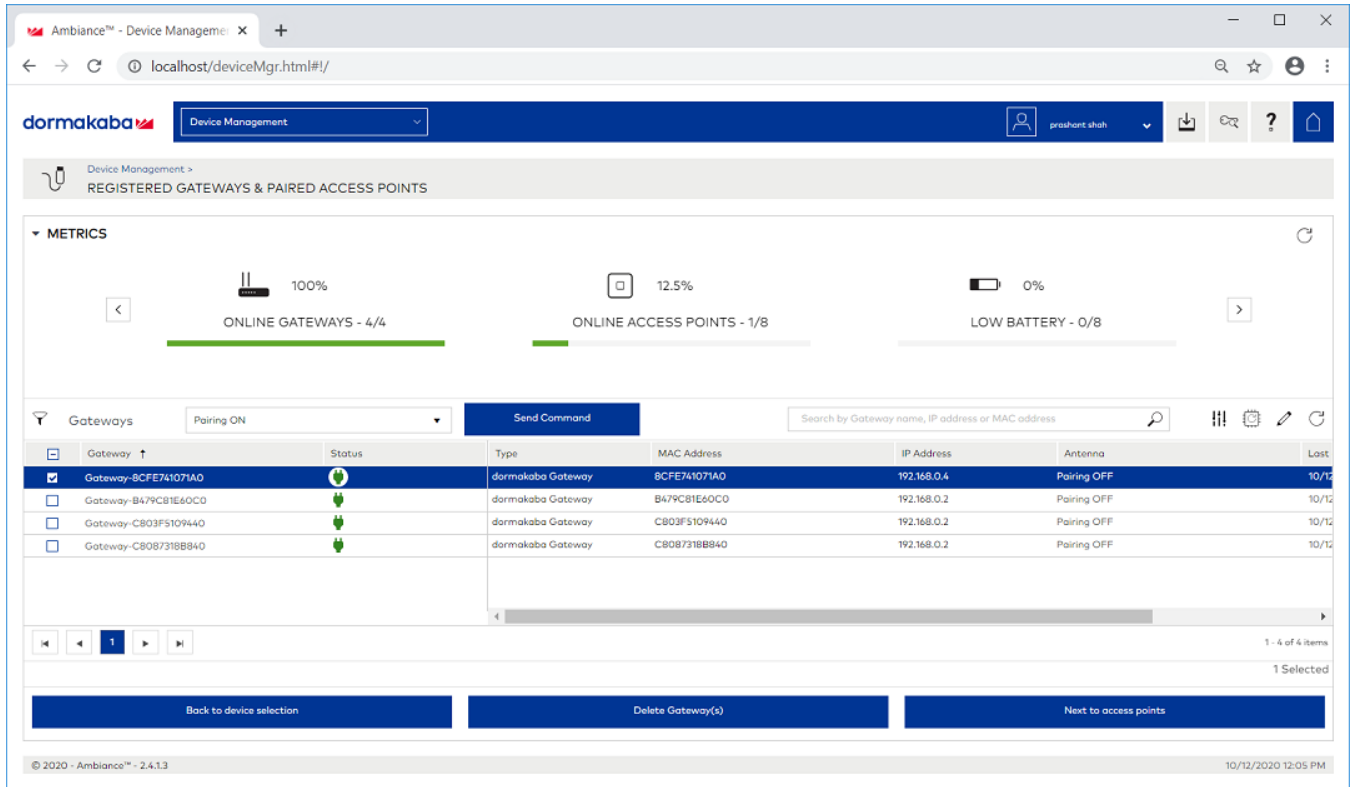
2. Click **Device Management**.

FIGURE 107 Selecting Device Management



3. Click **Register Gateways & Paired Access Points**.

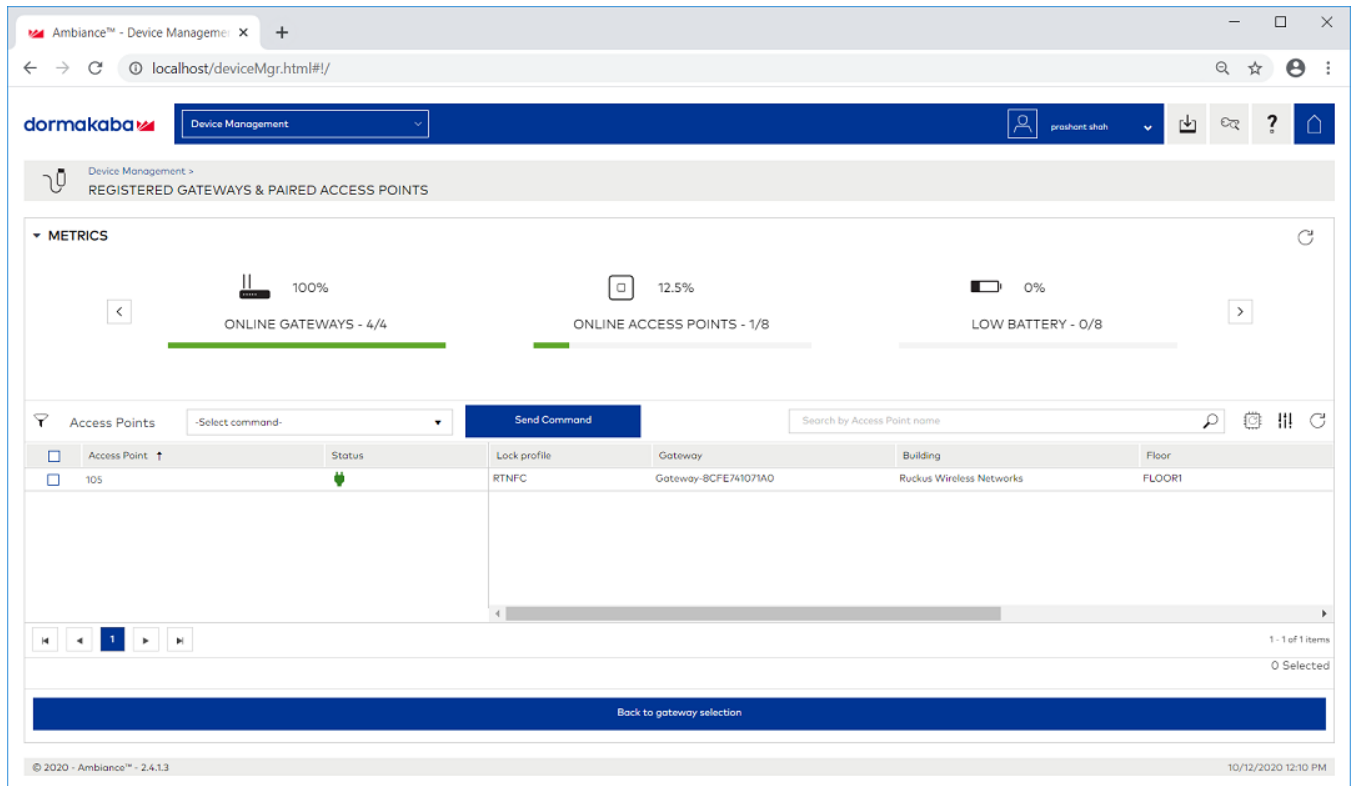
FIGURE 108 Selecting Register Gateways and Paired Access points



4. From the **Gateways**, select a gateway, and from the pull down select **Pairing ON** and click **Send Command** to start the gateway in scanning mode.
5. Swipe RF Pairing key card.
The LED pattern blinks green LED once, and amber colour LED thrice.
6. Lock will appear in IoT Controller's **Scan Window**, give name to the Lock and click **Accept**.
7. Select the same **Gateway**, from pull down menu and select **Pairing OFF**, and click **Send Command** to stop pairing.

8. Click **Device manager > Registered Gateways & Access Points**, and select the Access point.

FIGURE 109 Displaying the Lock



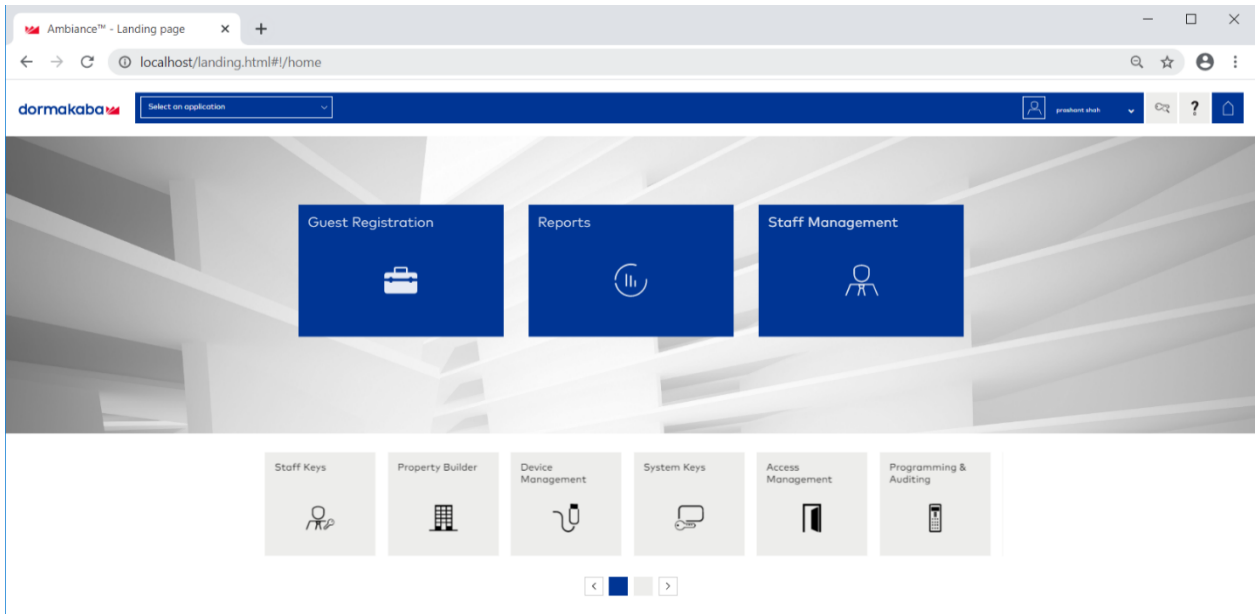
9. To confirm the lock connection, select the sage gateway, and click **Next to Access Point**.

Blocking the Key Remotely

Perform the below steps to block the key remotely.

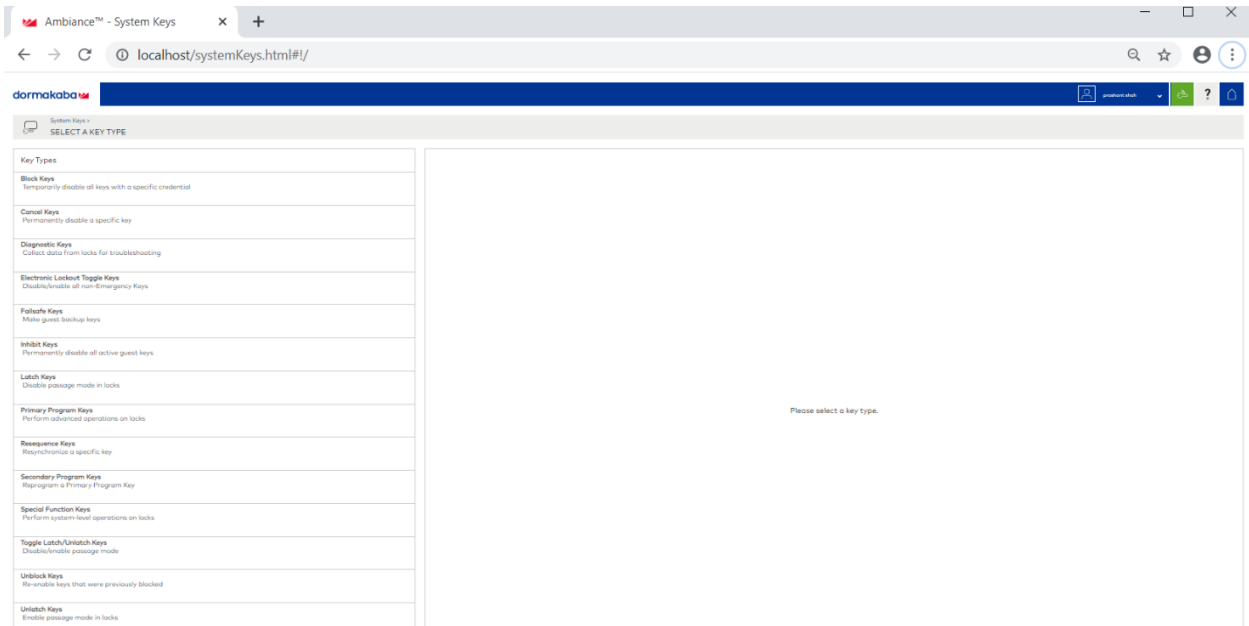
1. Go to Dormakaba Homepage.

FIGURE 110 Dormakaba Homepage



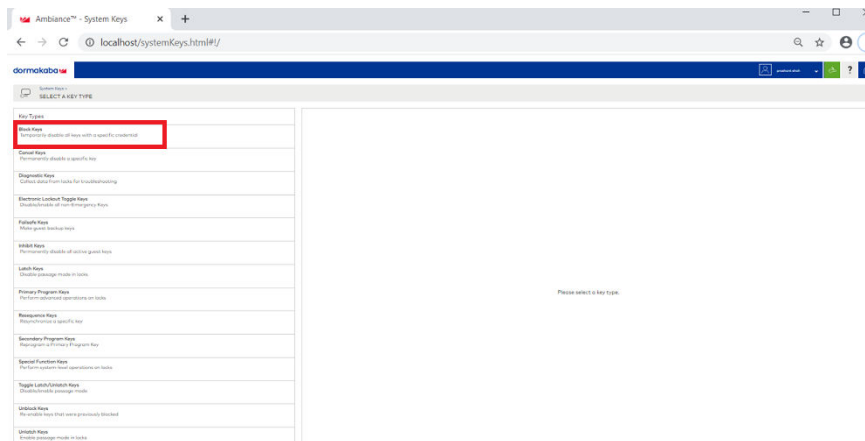
2. Click **System Keys**.

FIGURE 111 Selecting the System Keys



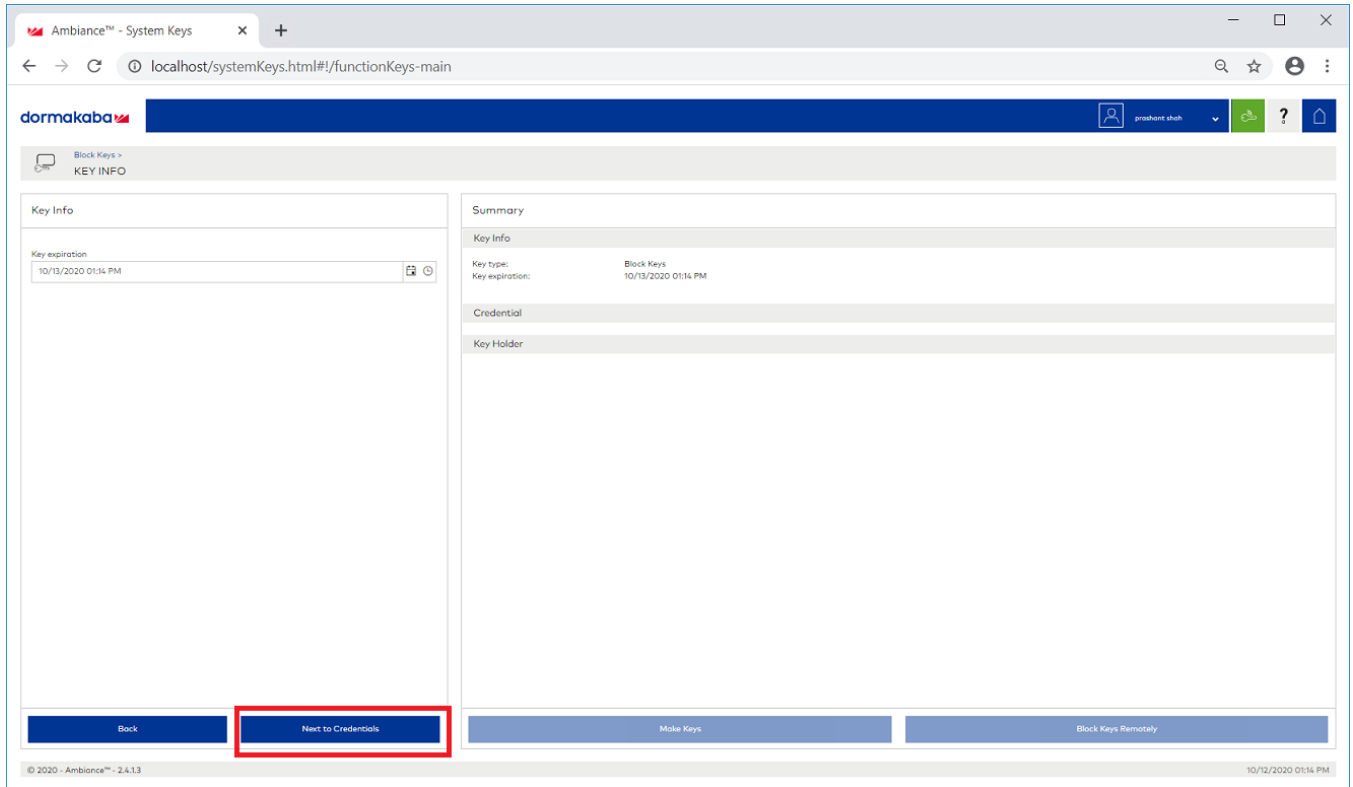
3. Click **Block Keys**.

FIGURE 112 Selecting the Block Keys



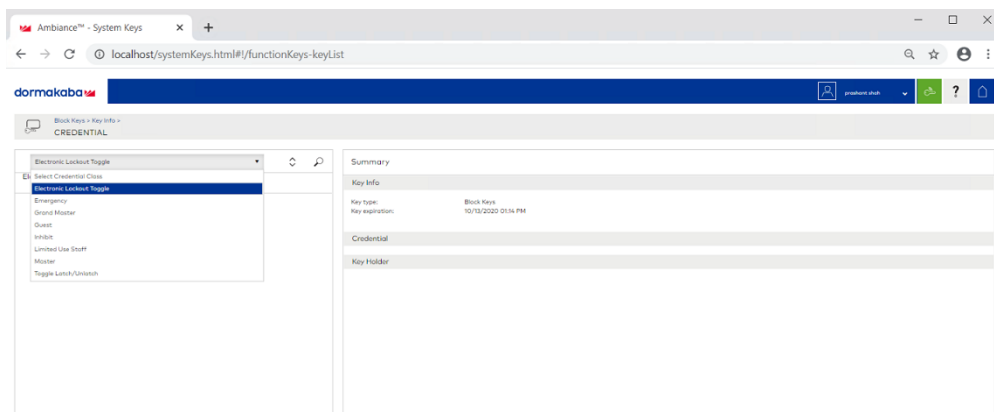
4. Click **Next to credential**.

FIGURE 113 Clicking the option Next to credential



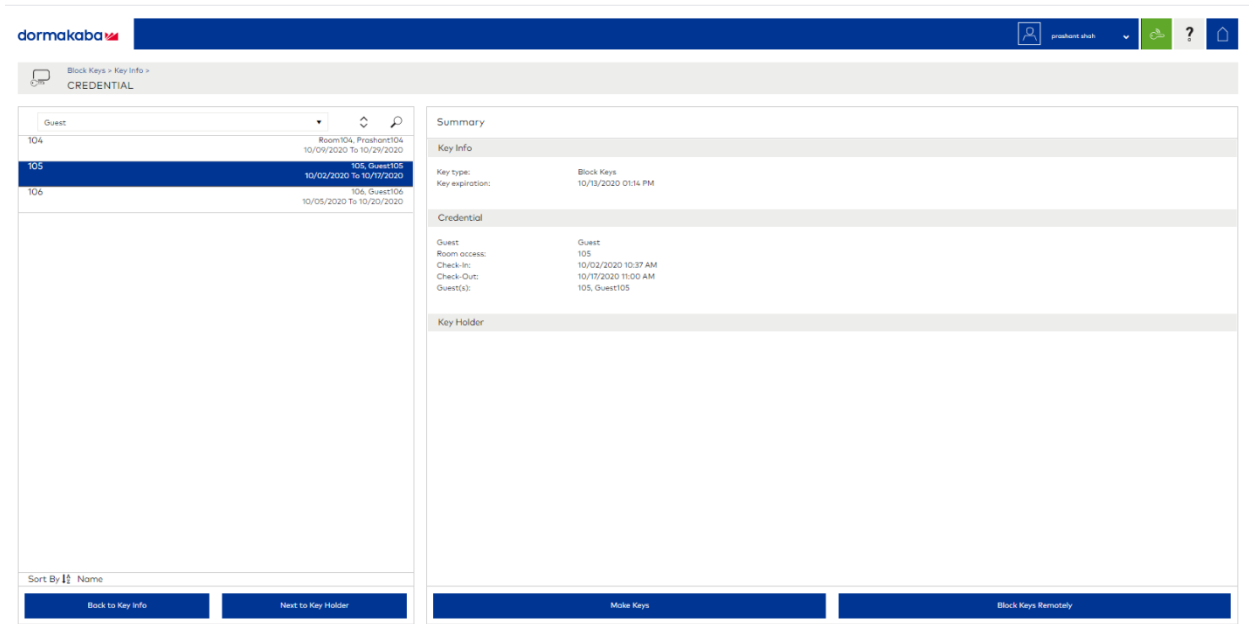
5. From the list, select **Guest** to block a **Guest** room.

FIGURE 114 Selecting Guest from the drop-down list



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

FIGURE 115 Selecting the Guest Room Number



7. Click **Block Key Remotely**.

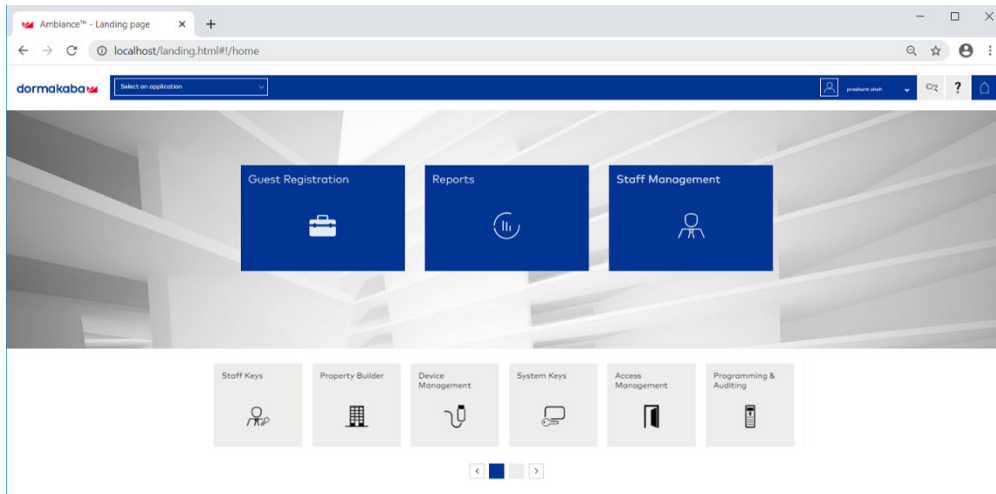
After you click **Block Key Remotely**, the LEDs will glow in the following pattern - one solid red LED, six green, and yellow LED together.

Unblocking the Key Remotely

Perform the below steps to unblock the keys remotely.

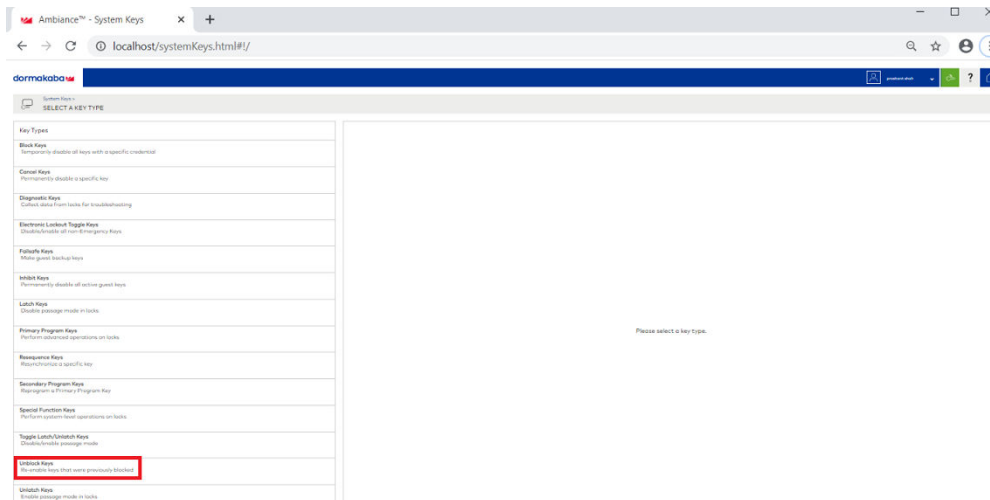
1. Go to the Dormakaba Homepage.

FIGURE 116 Dormakaba Homepage



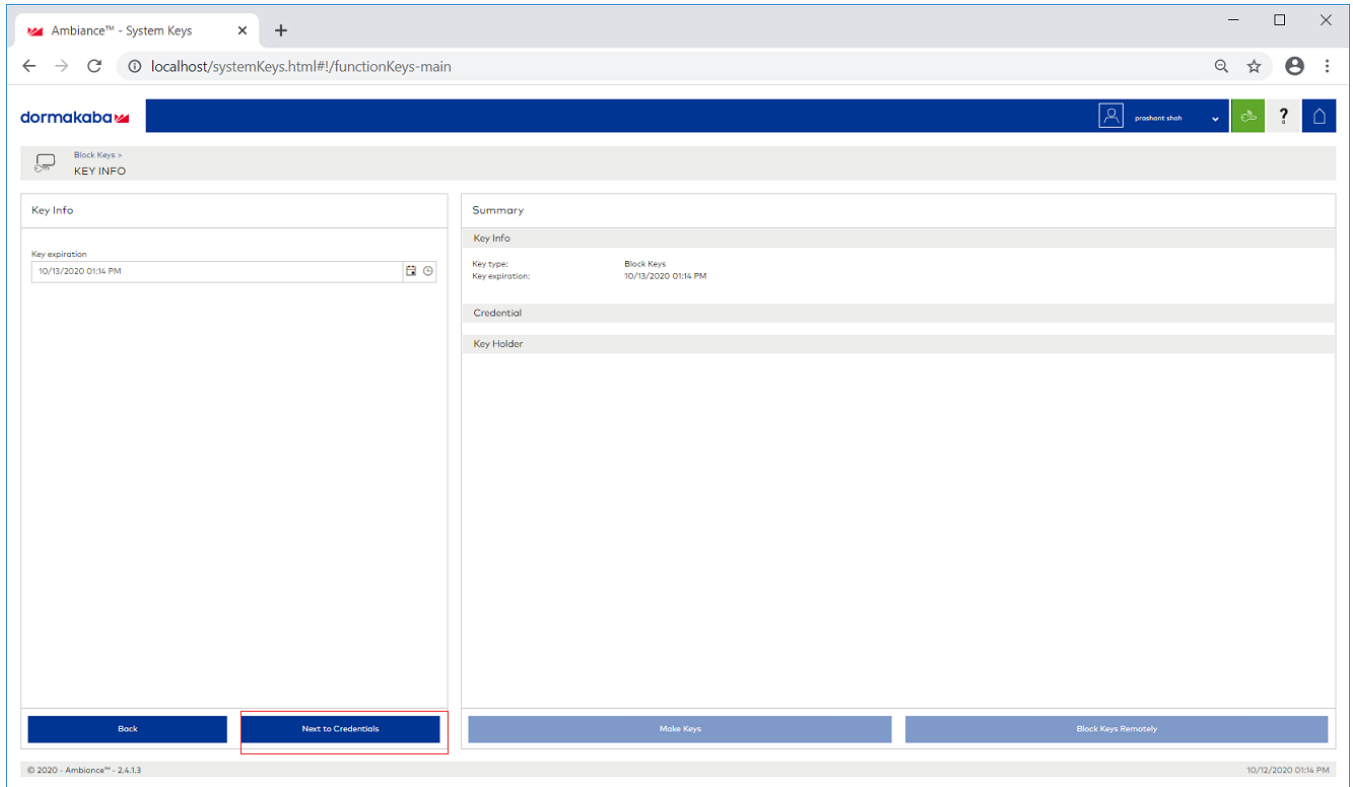
2. Click **System Keys**.

FIGURE 117 Selecting the Unblock Keys



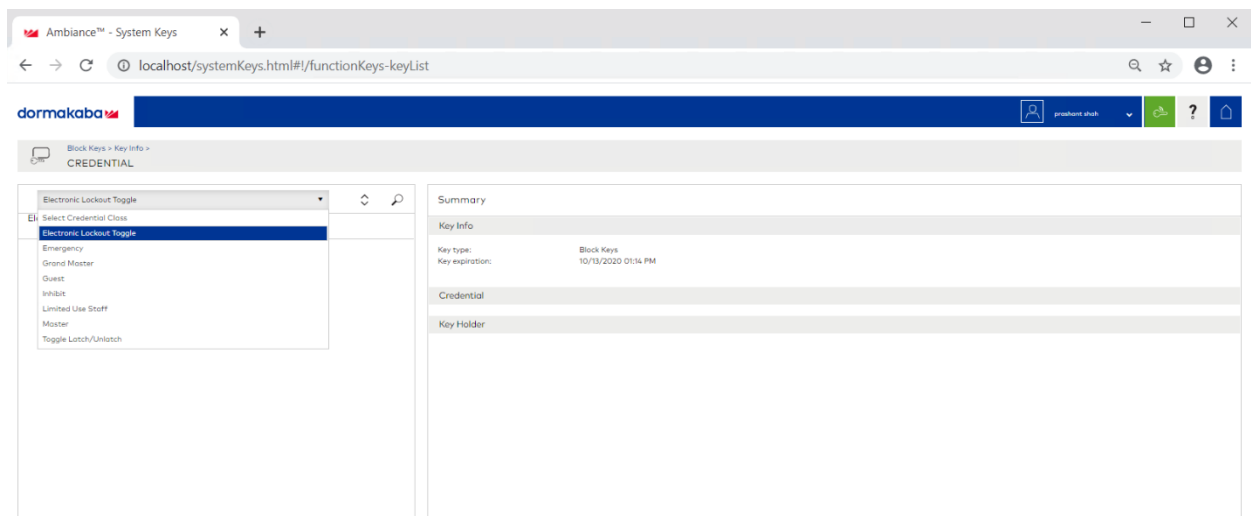
3. Click **Next to Credential**.

FIGURE 118 Clicking the option Next to Credential



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

FIGURE 119 Selecting Guest from the drop-down list



Managing Devices

Device Operations for Specific Clusters and Commands

5. Select a guest room number to unblock.
6. Click **Unblock Key Remotely**.

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

Device Operations for Specific Clusters and Commands

To configure the values for Thermostat complete the following steps.

1. From the main menu, go to **IoT Devices > Devices**.

2. Select a thermostat, and configure the various operations such as **SystemMode**, **Local Temperature Calibration**, **Max Cool Setpoint Limit**, **Max Heat Setpoint Limit**, **Min Cool Setpoint Limit**, **Min Heat Setpoint Limit**, **Occupied Cooling Setpoint**, **Occupied Heating Setpoint**, **Unoccupied Cooling Setpoint**, **Unoccupied Heating Setpoint**, **FanMode**, and **KeypadLockout** in the sidebar.

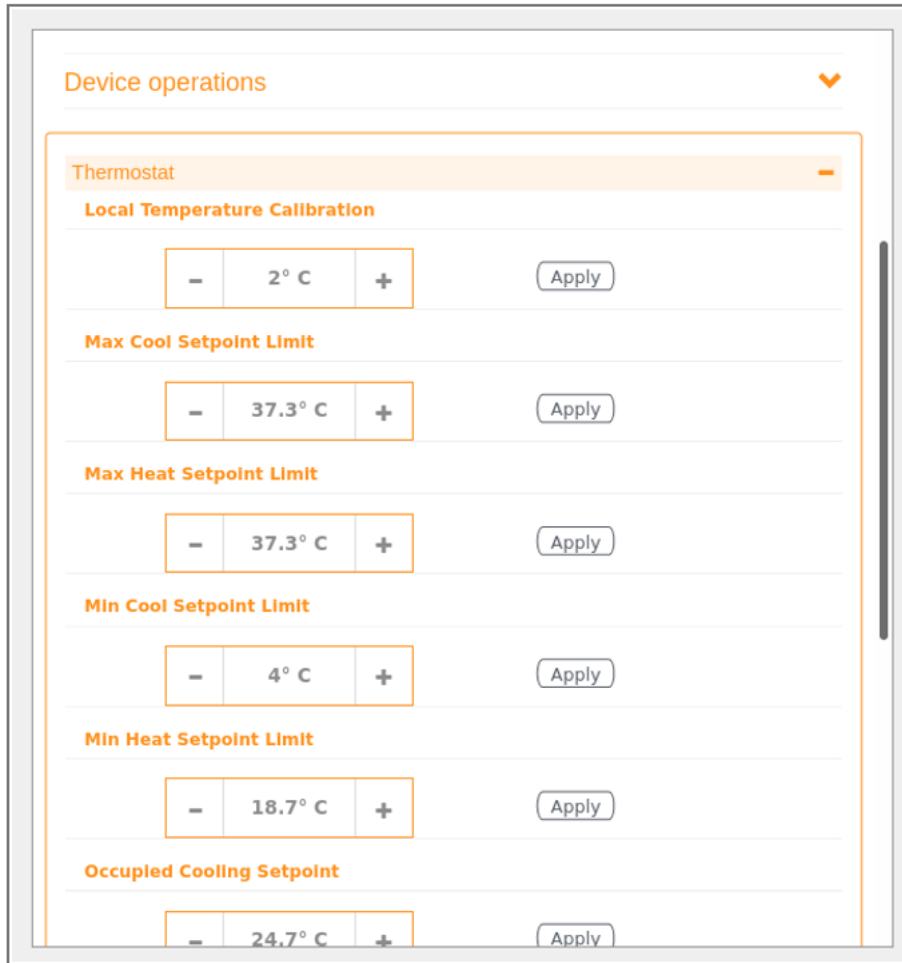


FIGURE 120 Thermostat User Interface Configuration and Fan Control Cluster operations

Managing Devices

Device Operations for Specific Clusters and Commands

The screenshot displays a configuration interface for a thermostat. It features several sections with adjustable settings:

- Temperature Setpoint:** A control bar with a minus sign, a value of 18.7° C, and a plus sign, followed by an "Apply" button.
- Occupied Cooling Setpoint:** A section header followed by a control bar with a minus sign, a value of 24.7° C, and a plus sign, followed by an "Apply" button.
- Occupied Heating Setpoint:** A section header followed by a control bar with a minus sign, a value of 19.4° C, and a plus sign, followed by an "Apply" button.
- System Mode:** A section header followed by a dropdown menu currently set to "Heat" and an "Apply" button.
- Thermostat User Interface Configuration:** A section header with a minus sign on the right.
- Keypad Lockout:** A section header followed by a dropdown menu currently set to "No lockout" and an "Apply" button.
- Fan Control:** A section header with a minus sign on the right.
- Fan Mode:** A section header followed by a dropdown menu currently set to "On" and an "Apply" button.

Rules Engine

- Rules Engine Overview..... 118
- Configuring Rules..... 118
- Rules-Dashboard..... 119

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.

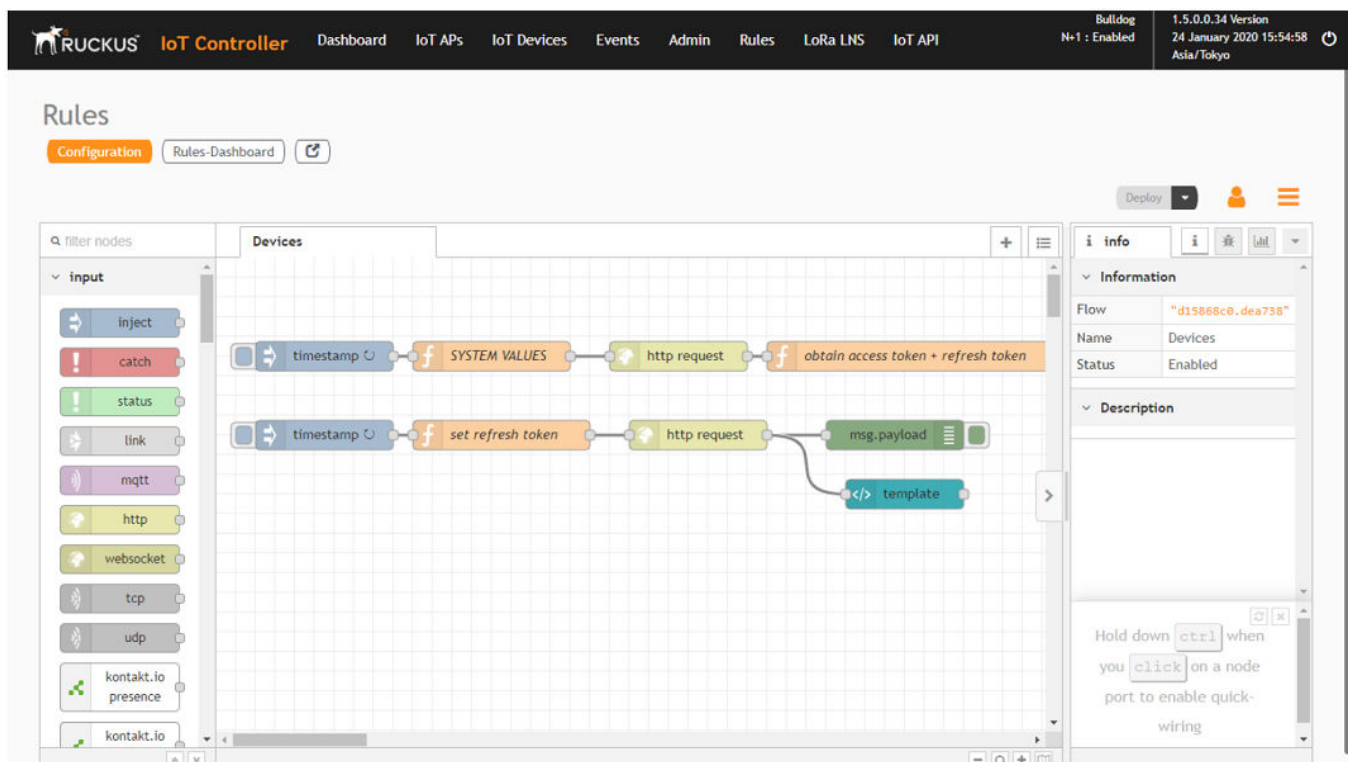
Complete the following steps to configure a rule.

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

NOTE

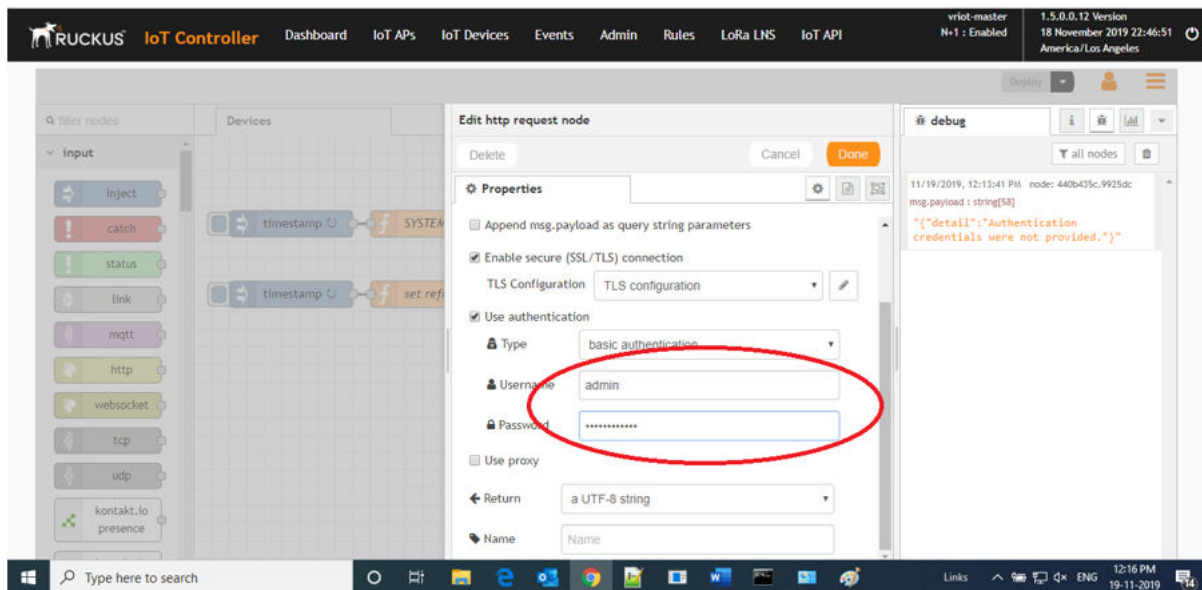
To create the rules, refer to <https://nodered.org/docs/>.

FIGURE 121 Configuring a Rule



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

FIGURE 122 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 123 Rules-Dashboard

Name	MAC ID	IoT AP MAC	Protocol	Type	LQI	RSSI	Last Seen
Sample	00:00:00:00:00:00	20:58:69:38:B8:F0	NA	Simple Sensor	0	0	0
20:58:69:38:B8:F0	20:58:69:38:B8:22	20:58:69:38:B8:F0	NA	Simple Sensor	0	0	0
20:58:69:38:B8:11	20:58:69:38:B8:11	20:58:69:38:B8:F0	NA	Simple Sensor	0	0	0

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


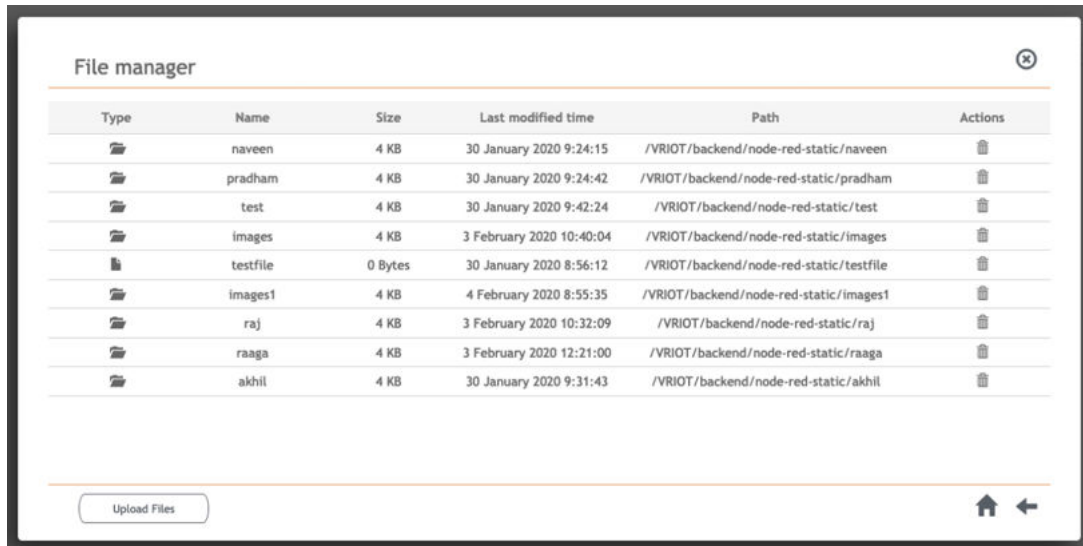
2. Click  .
A browser opens with the **Rules-Dashboard** page.
3. Click File-Manager.
A File-Manager page opens
4. Click **Upload Files**.

FIGURE 124 Uploading Files in the File Manager



NOTE

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

- HTML
- CSS
- PNG
- JPEG
- GIF

Events

- Viewing Events..... 121

Viewing Events

An event is an occurrence or the detection of certain conditions in and around the RUCKUS I100 IoT Module. An AP rebooting, detection of a RUCKUS I100 IoT Module, module undetection, and module swap are all examples of events.

To view the Events, from the main menu, click **Events** tab, the **Events** page is displayed as below.

FIGURE 125 Events Page

Log level	Token	Log message
INFO	994809e4a50a11ecac4fe9b3d2d4c6aa	Publish for Controller Data Stream
INFO	994809e4a50a11ecac4fe9b3d2d4c6aa	Periodic reporting interval configured
INFO	994809e4a50a11ecac4fe9b3d2d4c6aa	Publish payload on CDS endpoint
INFO	eff9ba6ea4fa11ecac49e9b3d2d4c6aa	smarththing service is running..
INFO		Device not registered : {device_euid: 'dc:a6:32:1f:6d:73', type: 'ping', value: 'device4.2.1'}
INFO		Soter Message from sensor.. b[{"device_euid":"dc:a6:32:1f:6d:73","type":"ping","value":"device4.2.1"}]
INFO		Soter Message from sensor.. soter/ruckus/iot/pipeline
INFO	994809e4a50a11ecac4fe9b3d2d4c6aa	Publish for Controller Data Stream
INFO	994809e4a50a11ecac4fe9b3d2d4c6aa	Periodic reporting interval configured
INFO	994809e4a50a11ecac4fe9b3d2d4c6aa	Publish payload on CDS endpoint
INFO	994809e4a50a11ecac4fe9b3d2d4c6aa	Publish for Controller Data Stream
INFO	994809e4a50a11ecac4fe9b3d2d4c6aa	Periodic reporting interval configured
INFO	994809e4a50a11ecac4fe9b3d2d4c6aa	Publish payload on CDS endpoint
INFO	eff9ba6ea4fa11ecac49e9b3d2d4c6aa	smarththing service is running..
INFO	994809e4a50a11ecac4fe9b3d2d4c6aa	Publish for Controller Data Stream
INFO	994809e4a50a11ecac4fe9b3d2d4c6aa	Periodic reporting interval configured

