CONFIGURATION GUIDE

RUCKUS IoT Controller Configuration Guide, 2.2.1.0 MR

Supporting IoT Controller Release 2.2.1.0

Part Number: 800-73587-001 Rev A
Publication Date: April 2024

© 2024 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

CommScope and the CommScope logo are registered trademarks of CommScope and/or its affiliates in the U.S. and other countries. For additional trademark information see https://www.commscope.com/trademarks. All product names, trademarks, and registered trademarks are the property of their respective owners.

Patent Marking Notice

For applicable patents, see www.cs-pat.com.

Contents

Contact Information, Resources, and Conventions **5**
- Document Conventions 5
  - Notes, Cautions, and Safety Warnings 5
- Command Syntax Conventions 6
- Document Feedback 6
- RUCKUS Product Documentation Resources 6
- Online Training Resources 7
- Contacting RUCKUS Customer Services and Support 7
  - What Support Do I Need? 7
  - Open a Case 7
  - Self-Service Resources 7

About This Guide **9**
- Introduction to RUCKUS IoT Controller 9
  - What's New in This Document 9

Getting Started **11**
- Before You Begin 11
  - Supported Web Browsers 11
- Logging In to RUCKUS IoT Controller 11
- Getting to Know the Dashboard 15

Configuring N+1 ..... **19**
- Configuring Static Addresses for Primary and Secondary Controllers 19
- Configuring the N+1 Feature 19

Disabling N+1 ..... **33**

Viewing Counters on the Controller Menu **35**

Managing IoT Controller System Configuration **37**
- Managing Services 37
- Activating the Monitoring Services 38
- Activating and Editing the Plugins 40
  - Activating and Editing the Assa Abloy Plugin 40
  - Activating and Editing the Eddystone Plugin 42
  - Activating and Editing the iBeacon Plugin 46
  - Activating and Editing the Beacon as a Service Plugin (iBeacon, Eddystone and Custom) 49
  - Activating and Editing the Beacon as a Service Plugin (React Mobile) 54
  - Activating and Editing the BLE Scan Plugin 55
  - Activating and Editing the Controller Data Stream Plugin 58
  - Activating and Editing the Dormakaba Plugin 60
  - Activating and Editing the Telkonet Plugin 62
  - Activating and Editing the Soter Plugin 65
  - Activating and Editing the Vostio Plugin 67
  - SALTO Plugin 75
- Changing the Password 84
- Configuring Virtual Machines 85
- Uploading Versions and Patches 86

Uploading an Image ... 86
Uploading a Patch ... 88
Backing Up Files ... 89
Uploading the RUCKUS IoT Controller License ... 90
Change the Settings ... 92
Rebooting RUCKUS IoT Controller ... 95
Resetting RUCKUS IoT Controller ... 96

Managing IoT Access Points ... 97
IoT AP Overview ... 97
DHCP Option 43 ... 97
RUCKUS Command Line Interface ... 98
USB Power ... 98
Gateway Onboarding ... 99
Adding an IoT AP ... 101
Editing an IoT AP ... 103
Single IoT Access Point Mode ... 103
Adding Tags to an AP ... 105
Approval of IoT APs ... 107
Exporting IoT APs to CSV ... 107
Enabling BaaS Major and Minor Number ... 107

Managing Devices ... 111
Devices Overview ... 111
Managing OSRAM Light Bulbs ... 113
Managing an Assa Abloy Lock ... 114
Managing the Dormakaba Locks ... 116
Discovering Dormakaba Lock ... 117
Blocking and Unblocking Dormakaba Lock ... 118
Blocking the Key Remotely ... 122
Unblocking the Key Remotely ... 126
Device Operations for Specific Clusters and Commands ... 129

Events ... 133
Viewing Events ... 133

Contact Information, Resources, and Conventions

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

Document Conventions

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

TABLE 1 Text Conventions

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

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

Document Feedback

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

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

When contacting us, include the following information:

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

For example:

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

RUCKUS Product Documentation Resources

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

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

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

Online Training Resources

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

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.ruckusnetworks.com and select **Support**.

What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at https://support.ruckuswireless.com/contact-us and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

Self-Service Resources

The RUCKUS Support Portal at https://support.ruckuswireless.com offers a number of tools to help you to research and resolve problems with your RUCKUS products, including:

- Technical Documentation—https://support.ruckuswireless.com/documents
- Community Forums—https://community.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.

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 2.2.1.0 MR

Feature	Description	Location
BLE Radio Scan Settings	BLE (Bluetooth Low Energy) Radio Scan Settings refers to the configuration options that control how a BLE radio scans for nearby Bluetooth devices.	Change the Settings on page 92
Single IoT Access Point Mode	Adding two options in the **Radio Info** list.	Single IoT Access Point Mode on page 103

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

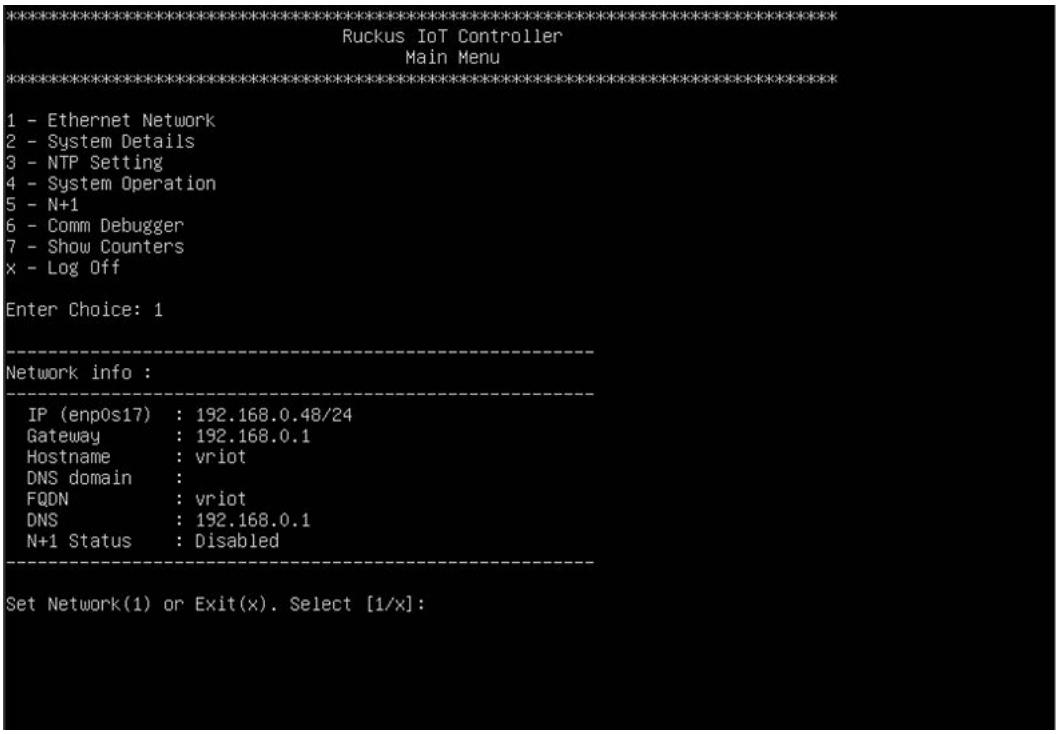
Logging In to RUCKUS IoT Controller

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".

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

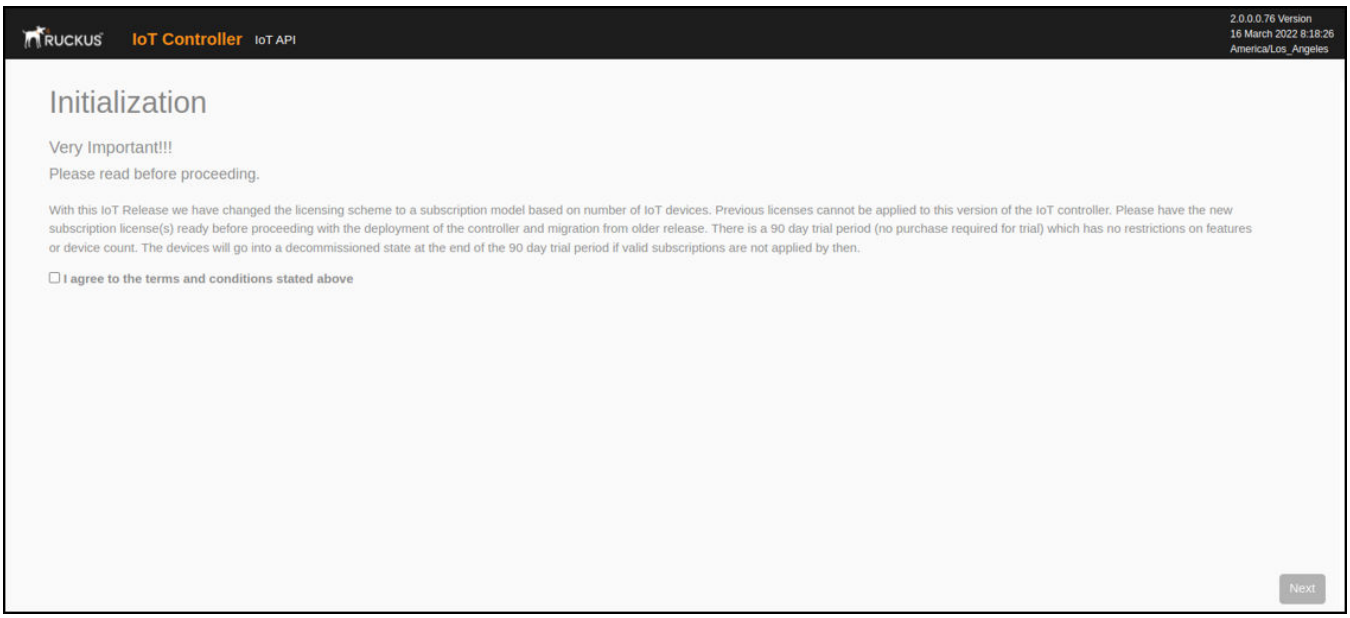
FIGURE 1 RUCKUS IoT Controller Main Menu



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

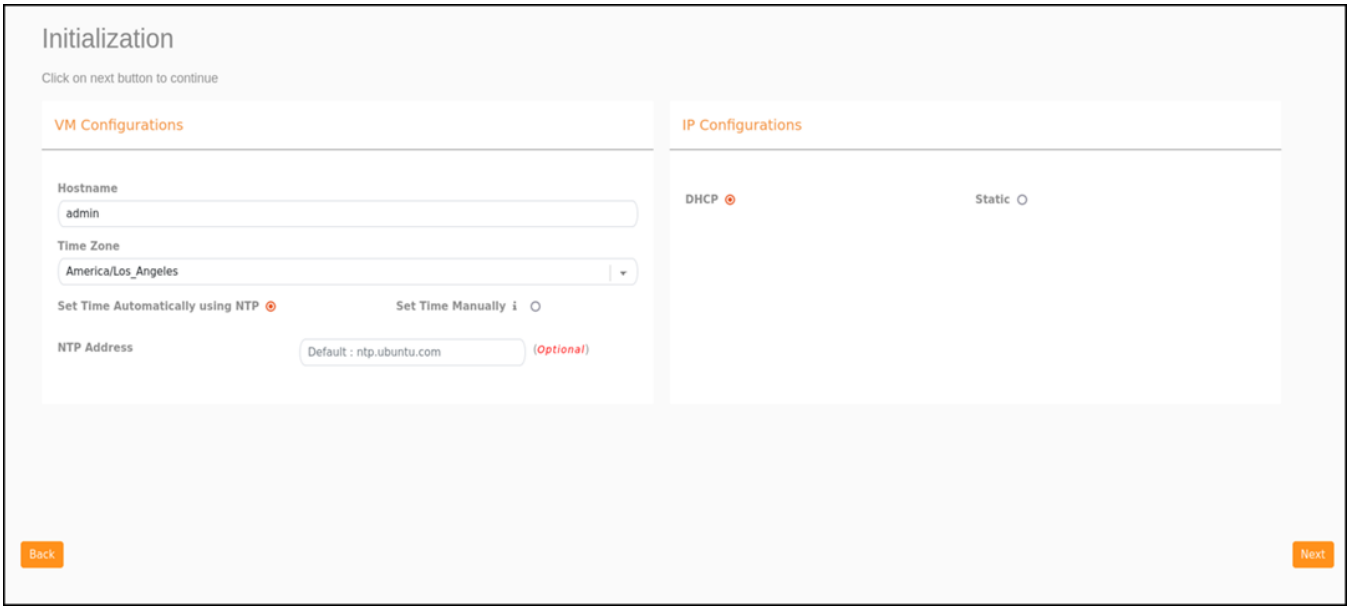
   The **Initialization** page is displayed.

FIGURE 2 Accepting Subscription Based Licensing



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

FIGURE 3 Inital VM and IP Configurations



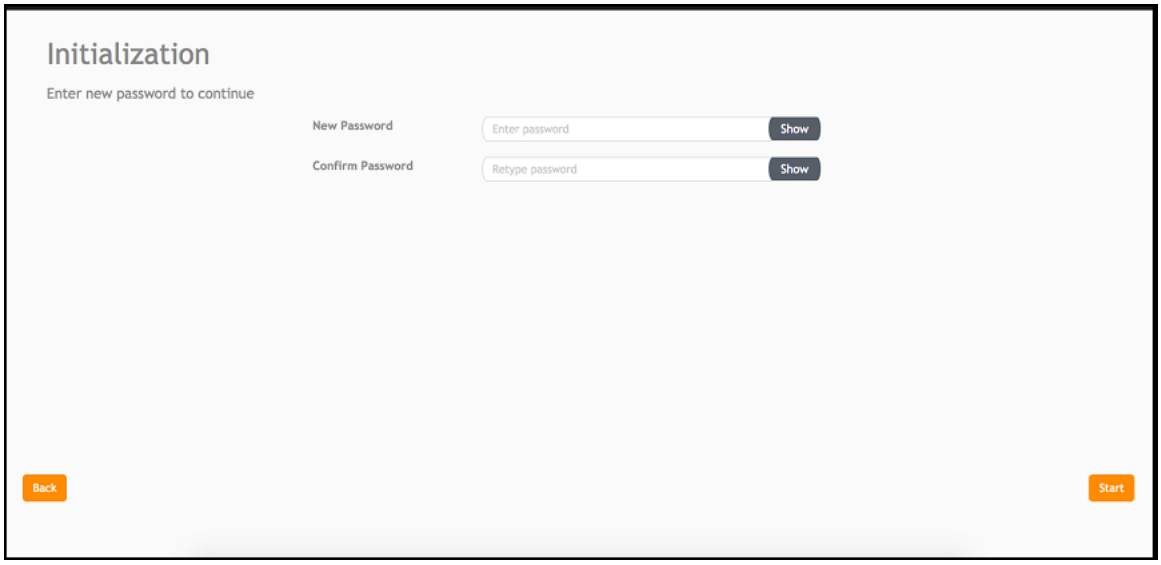
4. Enter the **Hostname**, **Time Zone**, and select the **IP Configuration** (**DHCP** or **Static**), and click **Next** to start all the services in the RUCKUS IoT Controller.

   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.

   NOTE
   Ensure the NTP between the SmartZone, APs and RUCKUS IoT Controller are in sync.

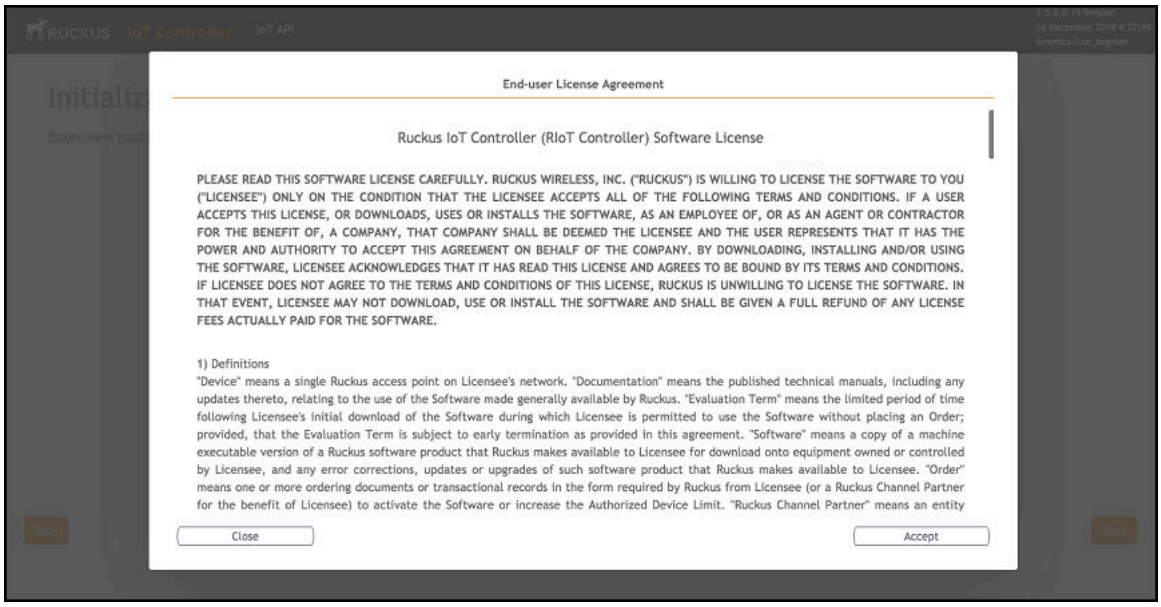
5. Enter the RUCKUS IoT Controller password in the **New Password** field. Re-enter the password in the **Confirm Password** field. The password must be a least eight characters in length and contain one uppercase letter, one lowercase letter, one digit, and one special character. Click **Start**.

   FIGURE 4 Confirming the Password



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

FIGURE 5 End-user License Agreement



Getting to Know the Dashboard

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

FIGURE 6 RUCKUS IoT Controller Dashboard

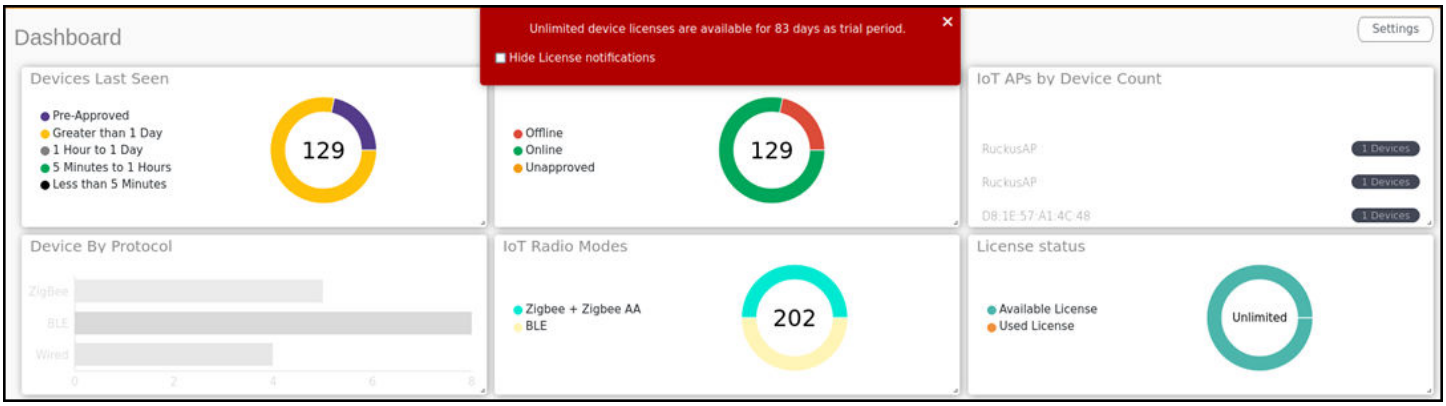


TABLE 4 Dashboard Elements

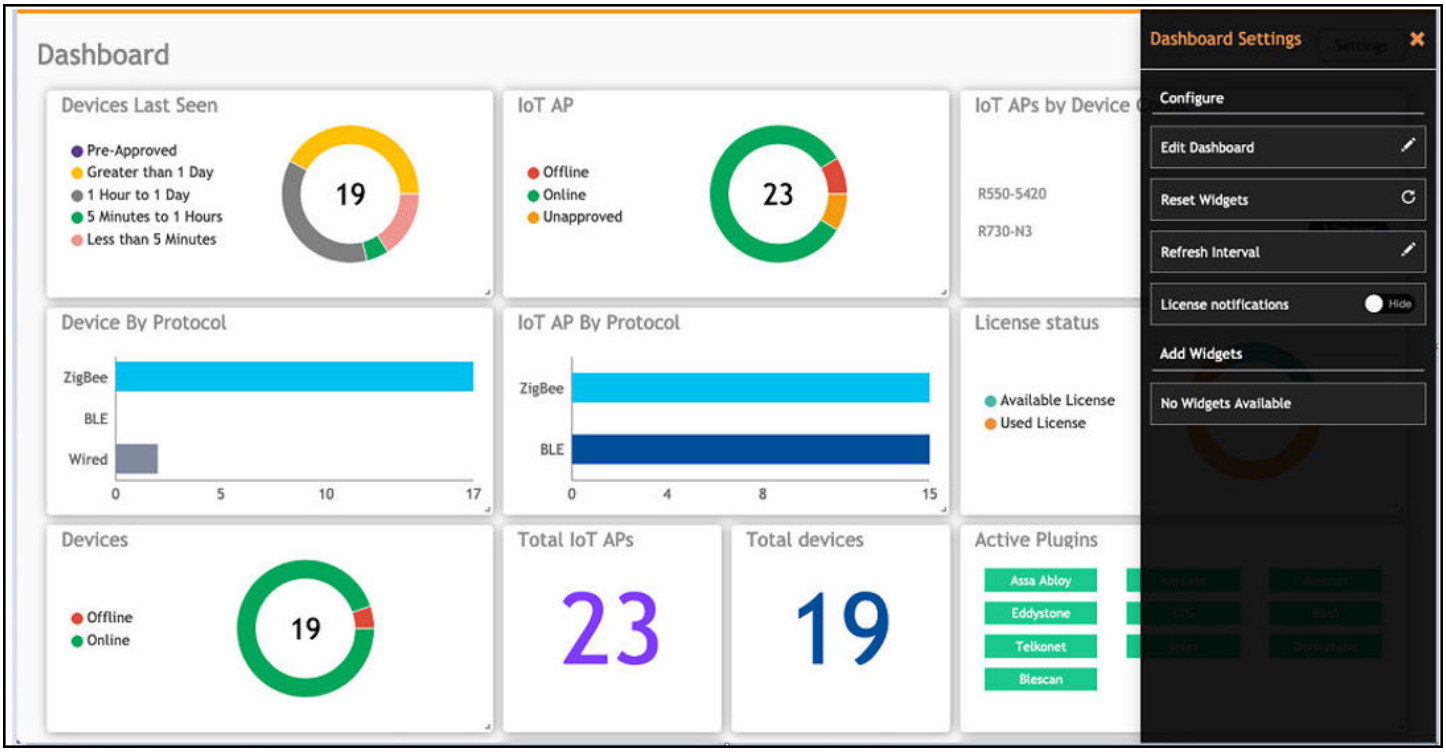
Box Name	Description
Devices Last seen	Shows the total number of devices last seen.

TABLE 4 Dashboard Elements (continued)

Box Name	Description
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 ontroller 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.

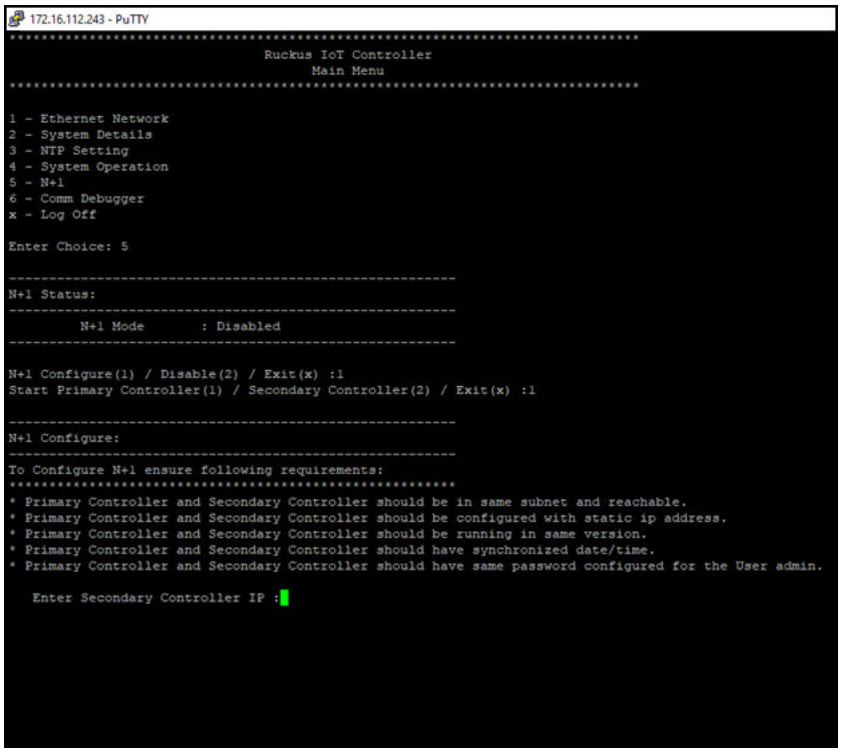
Configuring the N+1 Feature

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.

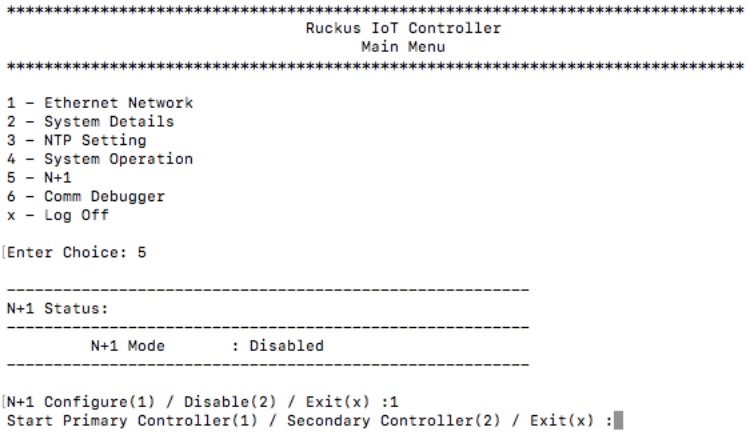
2. Enter **5** in the **Enter Choice** field.

FIGURE 8 RUCKUS IoT Controller Main Menu



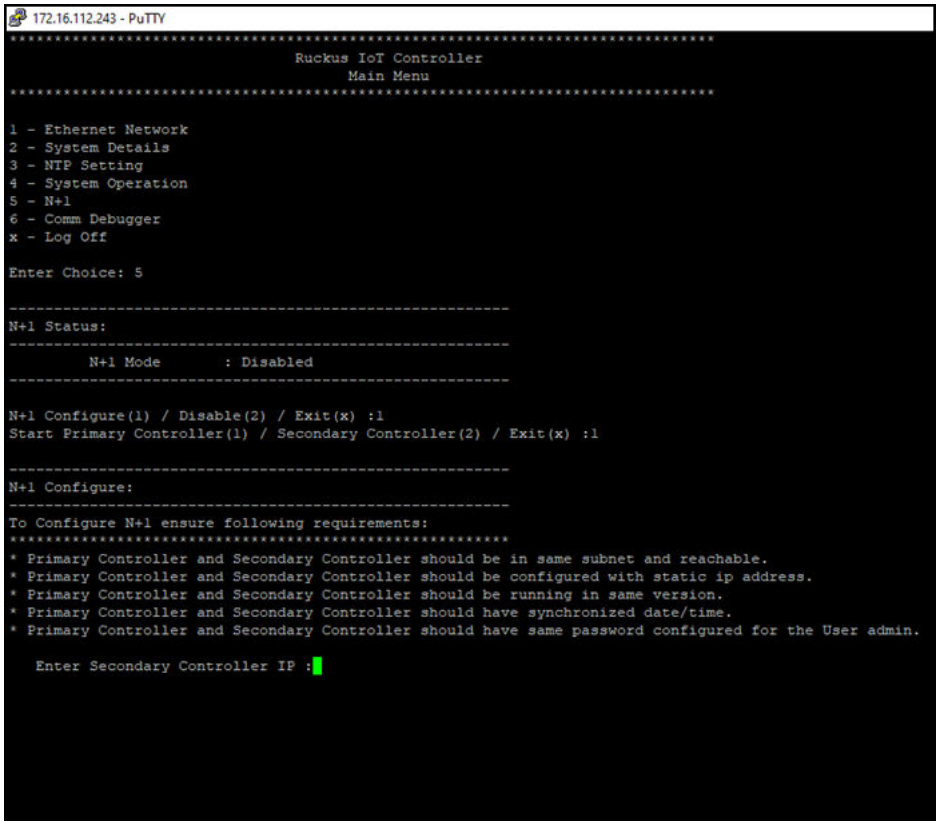
3. Enter **1** to continue the configuration.

FIGURE 9 Continuing the Configuration



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

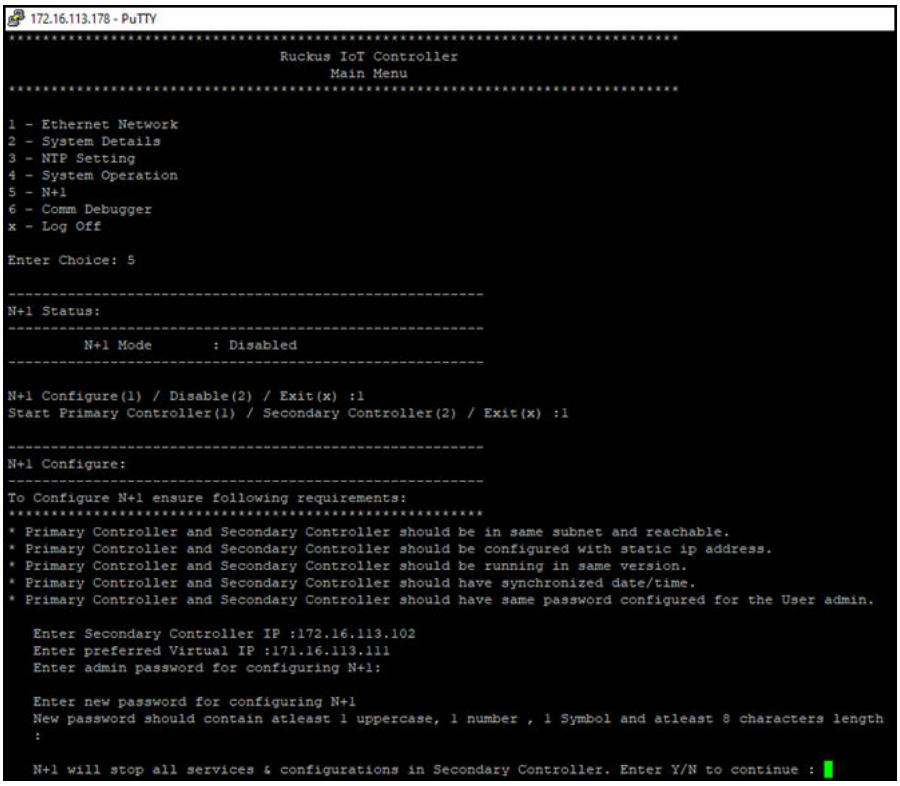
FIGURE 10 Configuring the Primary Controller



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

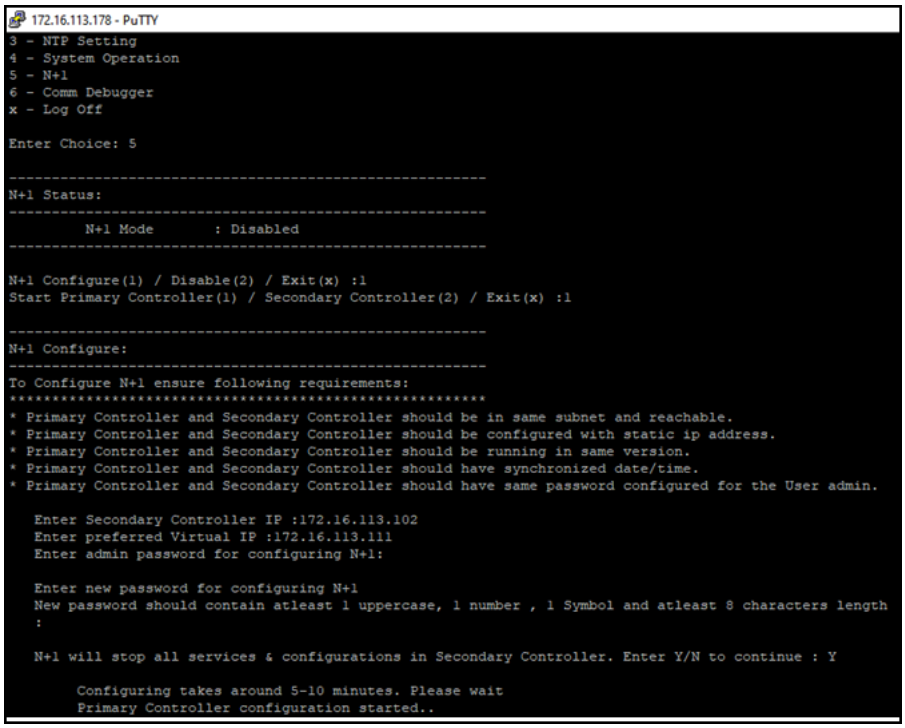
   NOTE
   The preferred virtual IP address must not be the same as the primary or secondary controller IP addresses.

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



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

FIGURE 11 Completing the Primary Controller Configuration



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

FIGURE 12 Continuing with the Secondary Controller Configuration

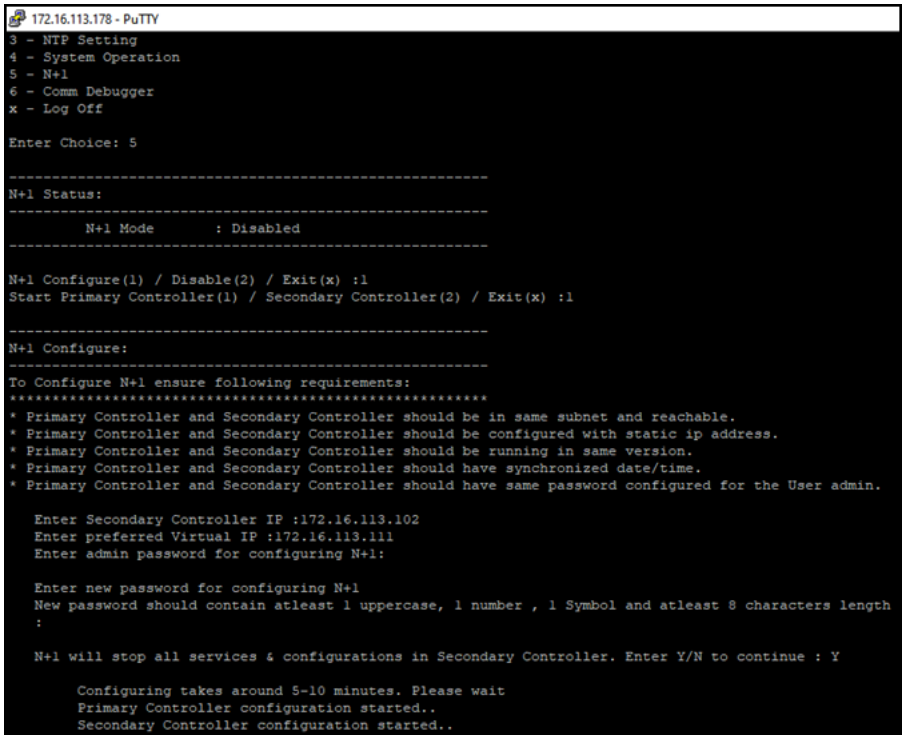
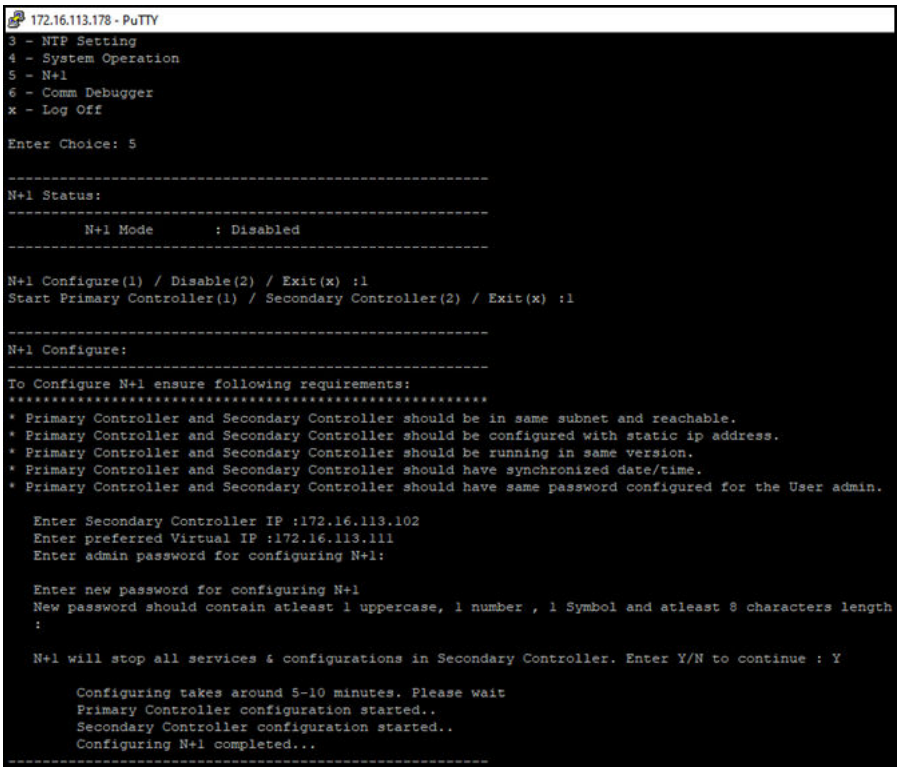


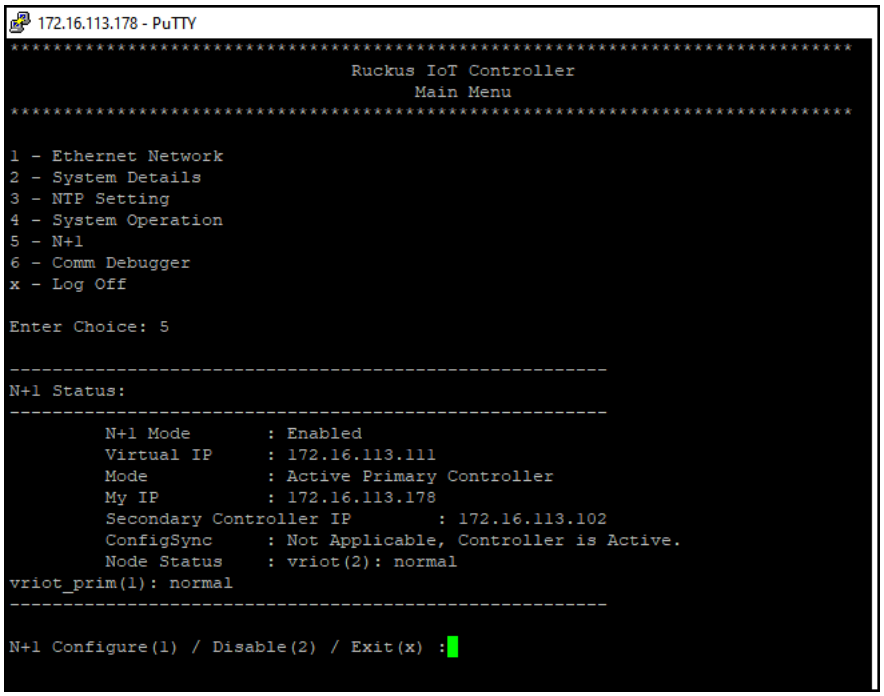
FIGURE 13 N+1 Configuration Completed



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



8. 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

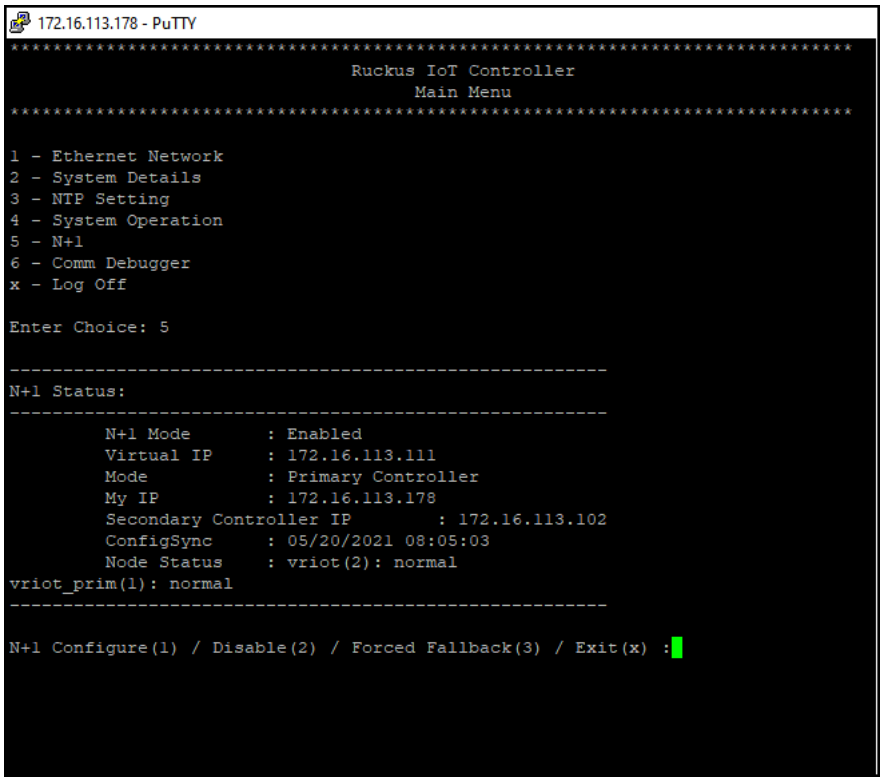
```
*******************************************************************************
                                Ruckus IoT Controller
                                     Main Menu
*******************************************************************************

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
```

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

FIGURE 17 Configuring Forced Fallback



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) :
```

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.

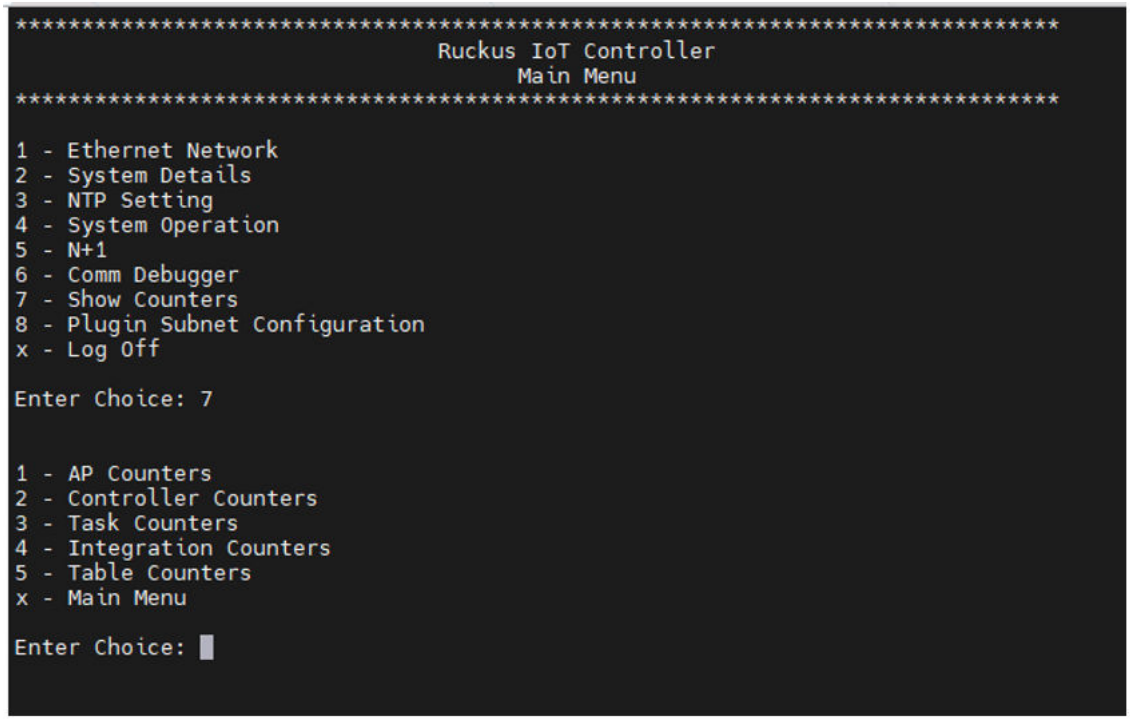
   NOTE
   After the N+1 configuration is disabled from the active primary controller, the secondary controller resets automatically.

Viewing Counters on the Controller Menu

The feature Show Counters allows you to view the information about AP based statics, Controller based statics, and Celery and Beacons Statics etc.

1. Log in to the console of the RUCKUS IoT Controller using the username "admin" and password "admin".
2. Enter **7** in the **Enter Choice** field.

FIGURE 22 Choosing Option 7



The below table lists the counters, and their usages.You can enter the corresponding choice as per your requirement in the choice field at the CLI prompt.

TABLE 5 List of Counters

Counter	Usuage
AP Counters	Displays the inputs for AP based statics such as count of IoT Service Restarts, Dongle swap event, IoT Application Upgrade, and IoT Radio Mode change.
Controller Counters	Displays the Controller Based Statics such as count of AP's added, deleted, Approved orUnapproved, count of devices added or deleted, count of controller Reboot or Upgrade or Downgrade or DB-Backup
Task Counters	Displays the number of celery tasks succeeded or failed.
Integration Counters	Displays the Beacon based Statics such as the number of messages forwarded to each beacon vendor.
Table Counters	Displays the number of documents in the each collection.

3. For example, to view the information about the AP based statics such as count of IoT service restarts, Dongle swap event count, IoT application upgraded count, and IoT Radio Mode change, enter **1** in the **Enter Choice** field and the the Gateway MAC address.

   You must enter the Gateway MAC address for AP Counters, Task Counters and Integration Counters.

Managing IoT Controller System Configuration

- Managing Services....37
- Activating the Monitoring Services....38
- Activating and Editing the Plugins....40
- Changing the Password....84
- Configuring Virtual Machines....85
- Uploading Versions and Patches....86
- Backing Up Files....89
- Uploading the RUCKUS IoT Controller License....90
- Change the Settings....92
- Rebooting RUCKUS IoT Controller....95
- Resetting RUCKUS IoT Controller....96

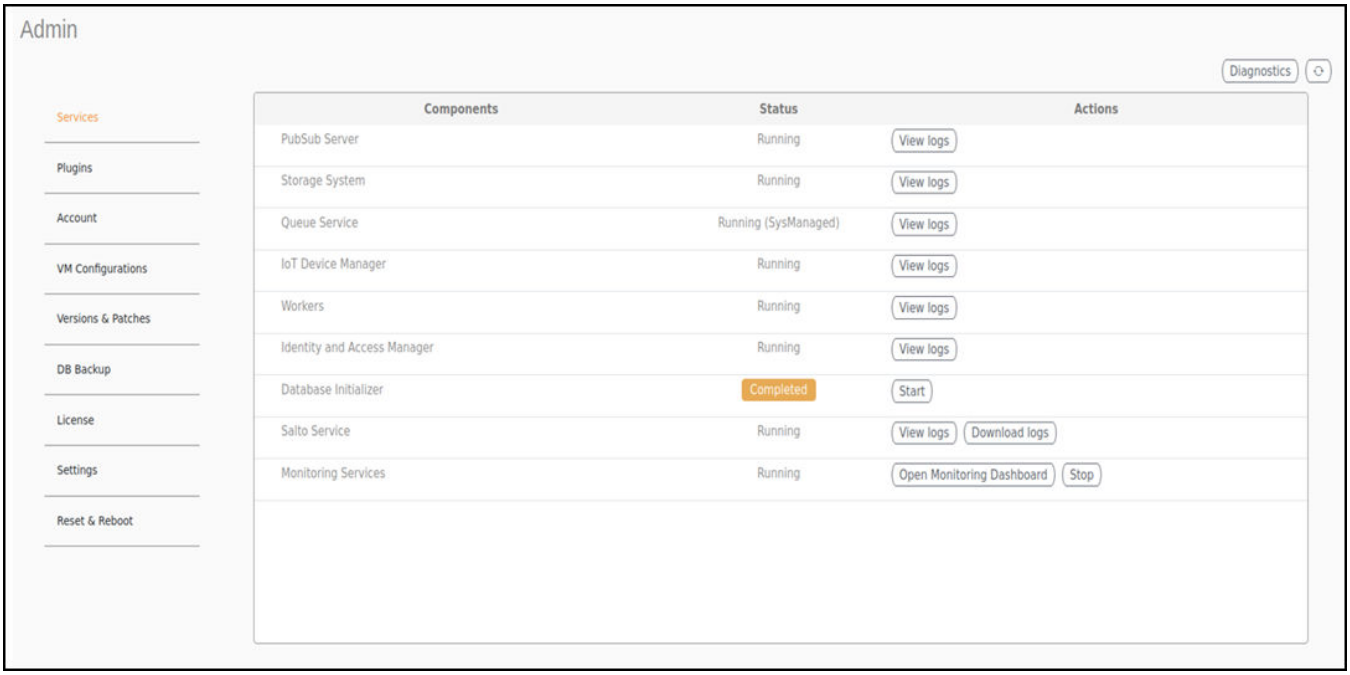
Managing Services

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

Complete the following steps to restart or manage the services.

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

FIGURE 23 Managing Services Page



The currently running services and their details are displayed.

3. Select a service to start or stop.

Activating the Monitoring Services

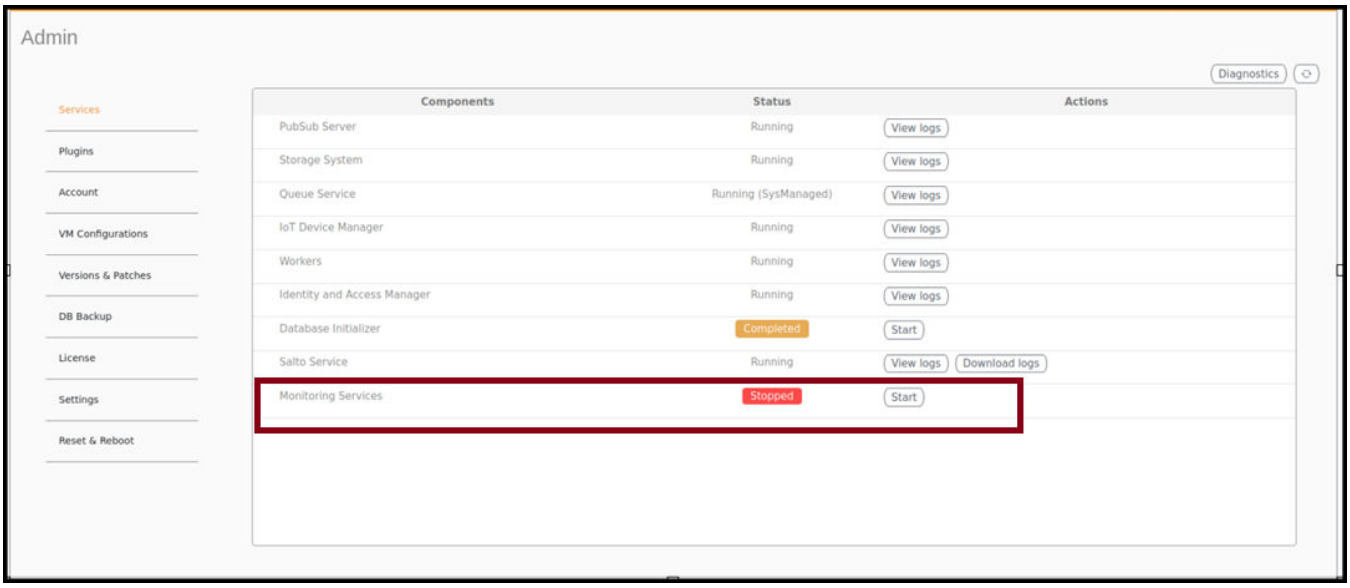
The Monitoring Services collect and store time-series data (metrics) from various targets, enabling you to query, and make analysis based on this data. The multi-dimensional data model has its own query language (PromQL) to communicate. The Monitoring Services assist in monitoring and ensuring the reliablility of system and applications.

To activate the Monitoring Services, the administrator must perform the following steps.

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

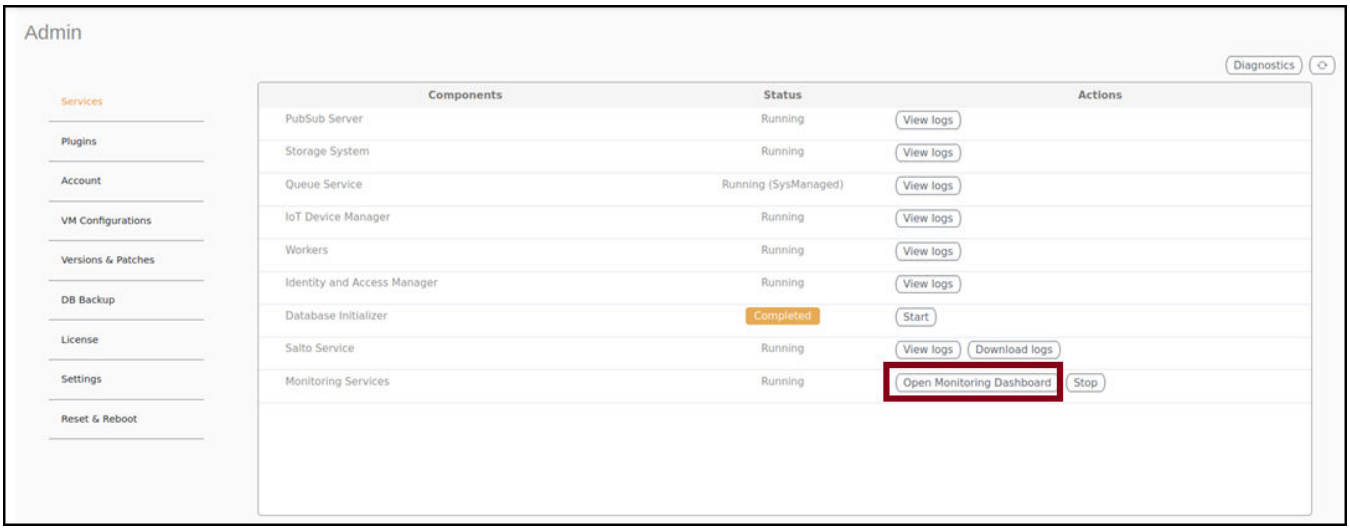
   The currently running services and their details are displayed.
3. Select **Monitoring Services** and click **Start**.

FIGURE 24 Activating the Monitoring Services



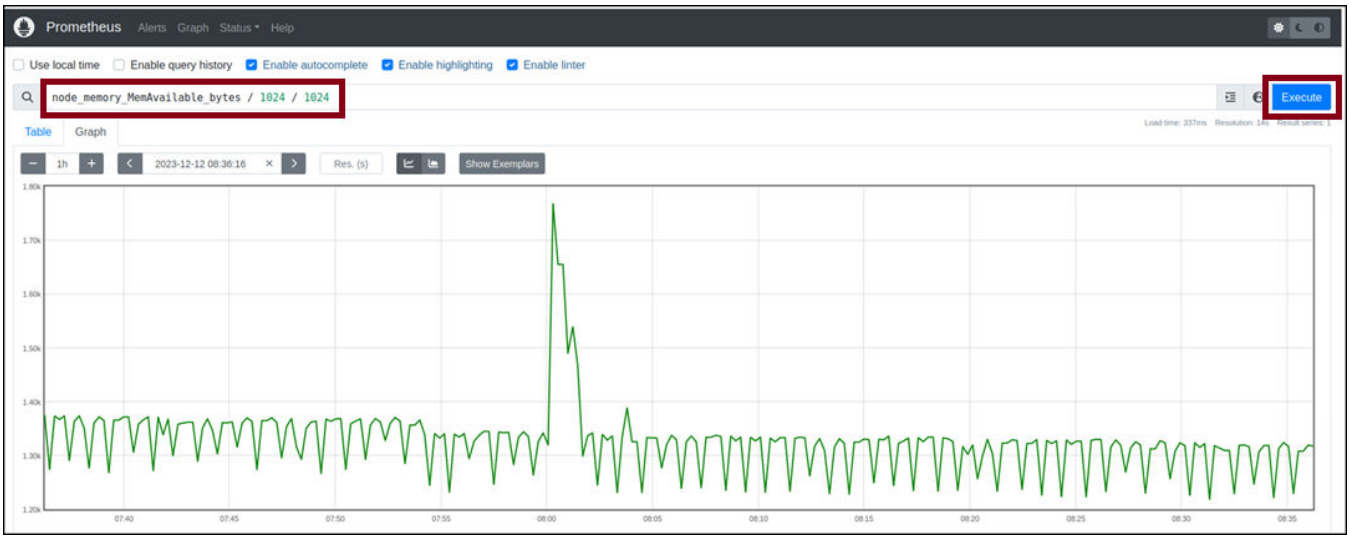
4. Click the **Open Monitoring Dashboard** to open the **Prometheus** Dashboard page.

FIGURE 25 Clicking the Open Monitoring Dashboard



5. Enter the Prometheus query in the **Search** field and click **Execute**.

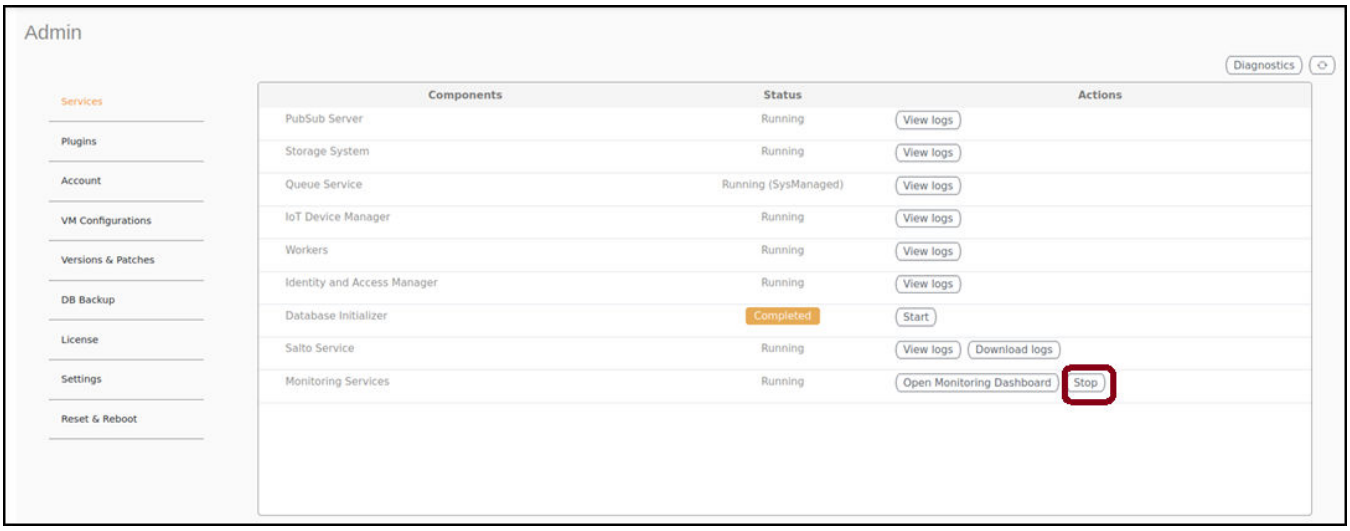
FIGURE 26 The Prometheus Dashboard Page



For example, in the above figure, after entering the Prometheus query **node_memory_MemAvailable_bytes / 1024 / 1024**, the result shows a graph, displaying the available memory in the RUCKUS IoT Controller.

6. To de-activate the Monitoring Services, from the main menu, go to **Admin** > **Services** > **Monitoring Services** and click **Stop**.

FIGURE 27 De-activating the Monitoring Services



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 Assa Abloy Plugin

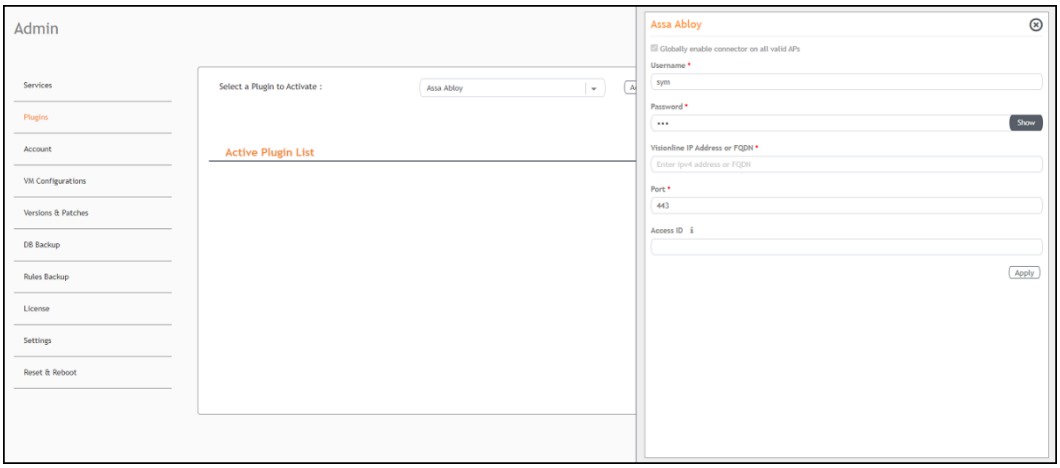
The RUCKUS IoT Controller provides support for the Assa Abloy door locks plugin. The RUCKUS IoT Controller reads the packet from the IoT AP and routes the packets to the Visionline Server.

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 28 Activating the Assa Abloy Plugin

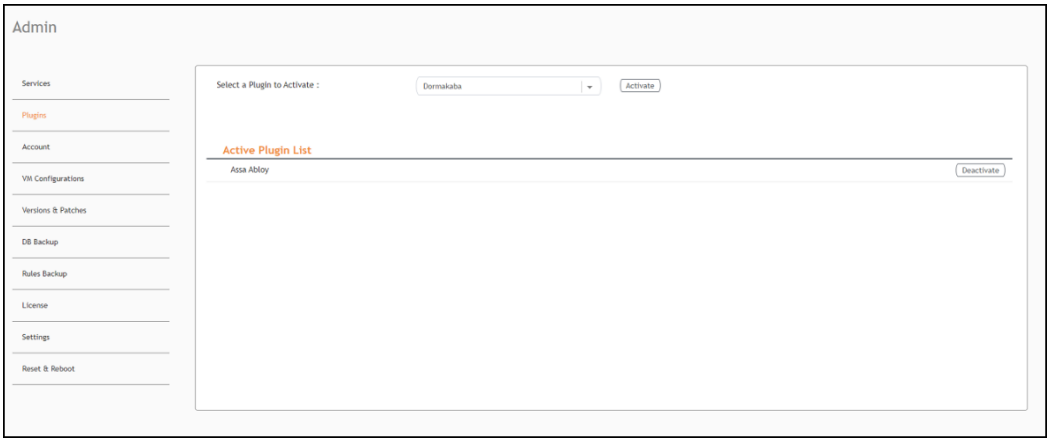


4. After the Assa Abloy plugin is activated, enter the following configuration parameters.
   a) For **Username**, enter the name of the user connecting to the Visionline Server
   b) For **Password**, enter the password of the user connecting to the Visionline Server.
   c) Enter the **Visionline IP address** or **FQDN**.

   NOTE
   By default, the port number is 443.

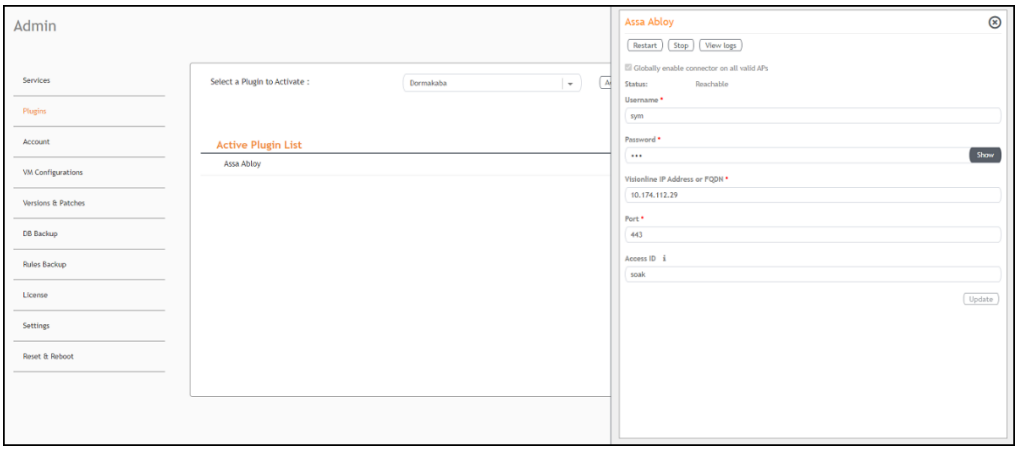
5. Click **Apply**.
   The Assa Abloy plugin is added in the **Active Plugin List**.
6. To deactivate the Assa Abloy plugin, select it and click **Deactivate**.

FIGURE 29 Deactivating the Assa Abloy Plugin



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

FIGURE 30 Updating the Configuration Parameters



Activating and Editing the Eddystone Plugin

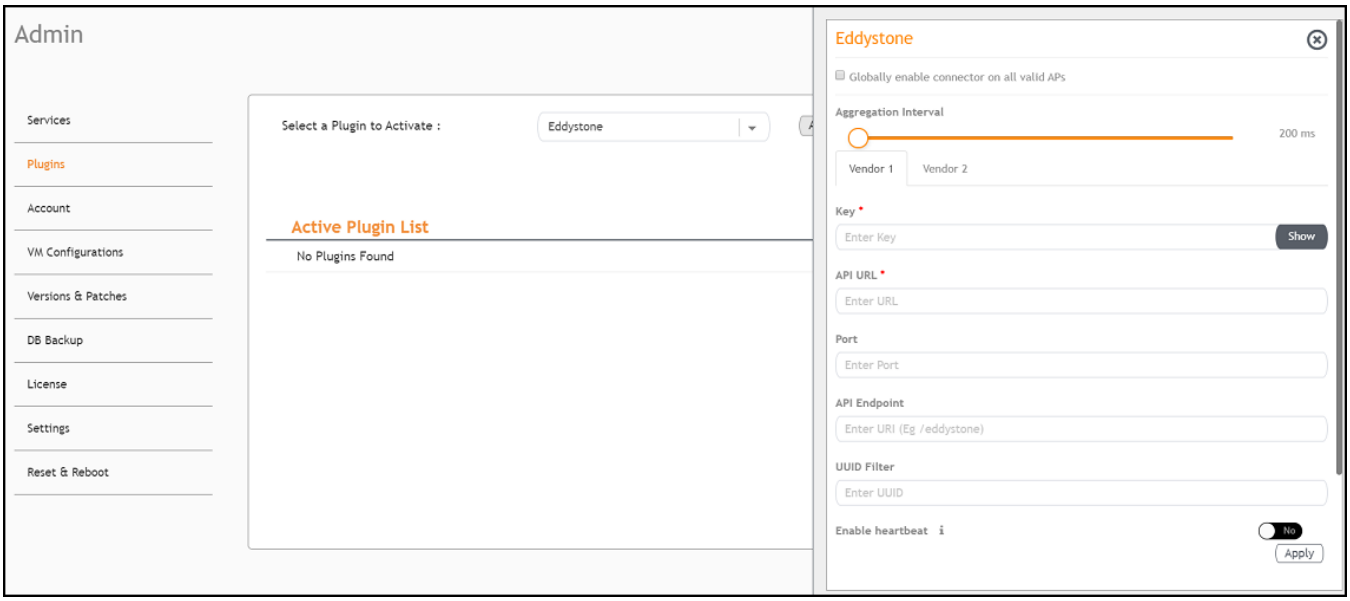
The RUCKUS IoT Controller provides support for the Bluetooth Low Energy (BLE) Eddystone plugin. The RUCKUS IoT Controller reads the packet from IoT AP, and routes the packets to the BLE beacon vendor cloud services.

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 31 Activating the Eddystone Plugin



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

      NOTE
      If **Globally enable connector on all valid APs** is not selected, you can activate the plugin for each AP by adding a tag. Refer to Adding Tags to an AP on page 105 for more information.

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

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

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

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

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

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

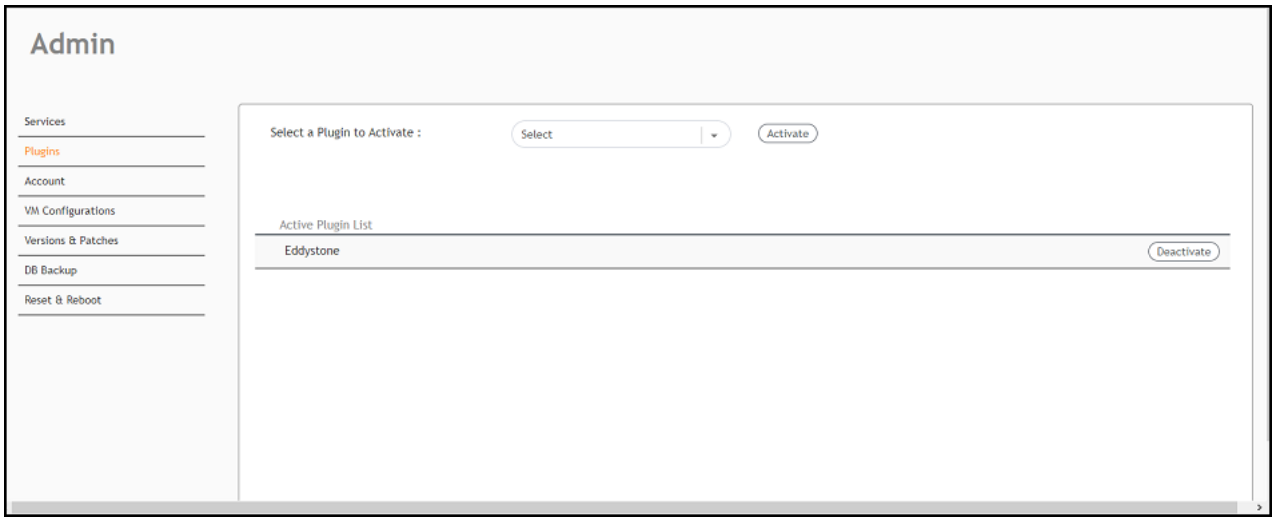
      The filter allows only the BLE ADV packets with the specified UUID to be passed on to the vendor application.
   h) Enable heartbeat.

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

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

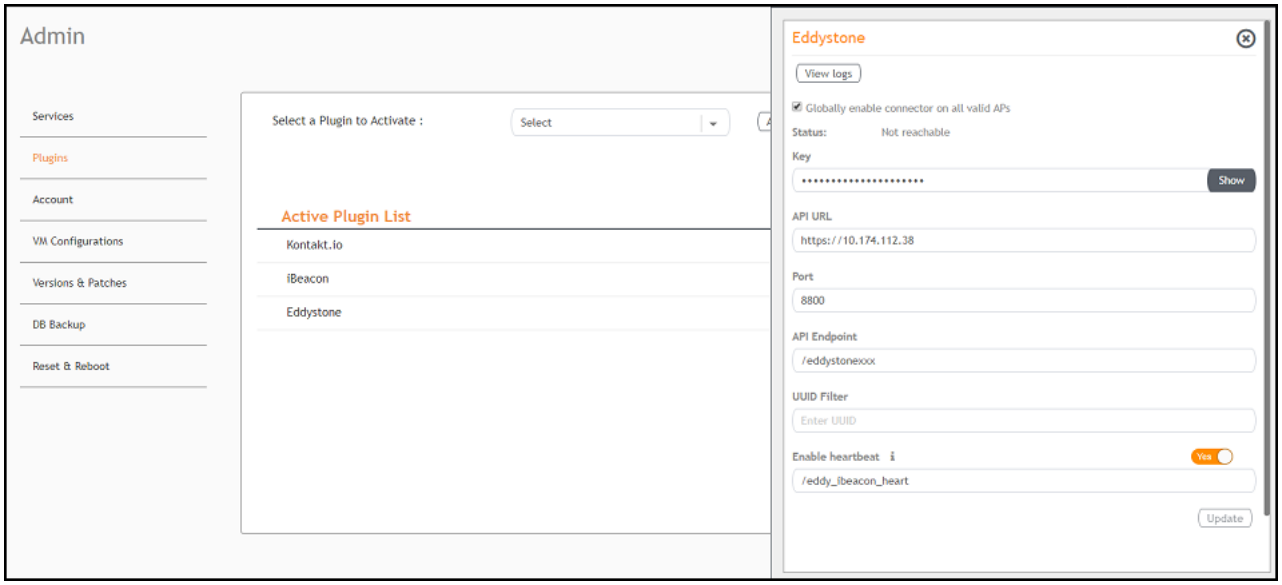
6. To deactivate the Eddystone plugin, select it and click **Deactivate**.

FIGURE 32 Deactivating the Eddystone Plugin



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

FIGURE 33 Updating the Configuration Parameters



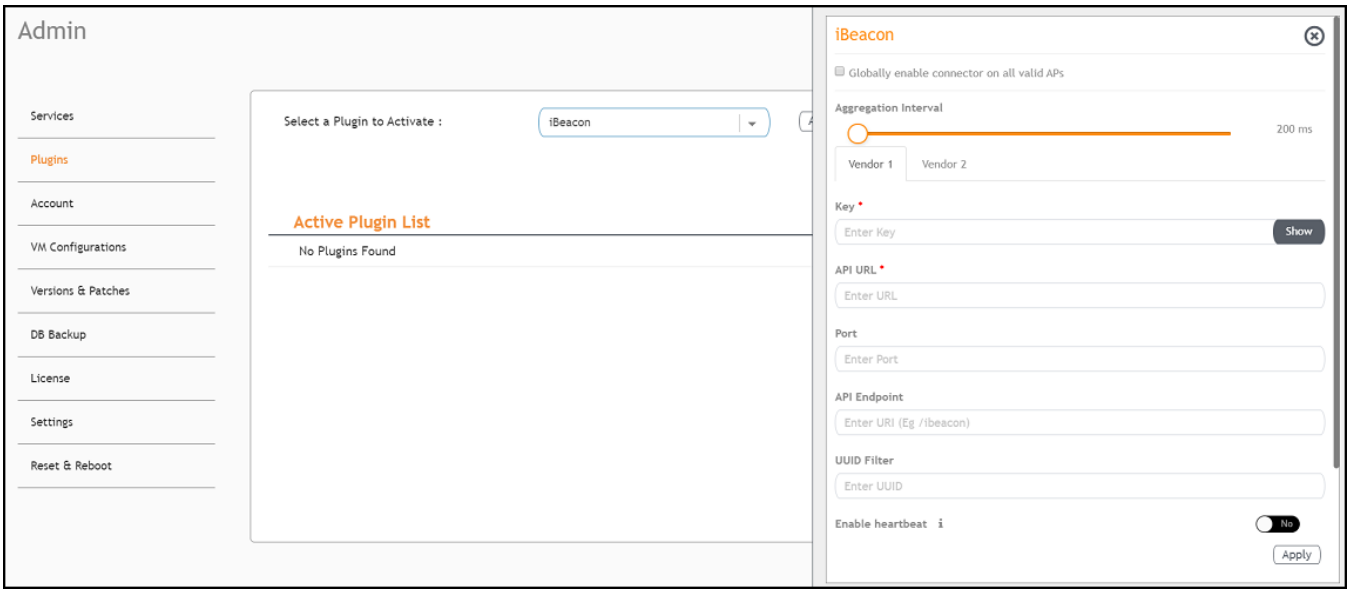
Activating and Editing the iBeacon Plugin

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 34 Activating the iBeacon Plugin



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

      NOTE
      If **Globally enable connector on all valid APs** is not selected, you can activate the plugin for each AP by adding a tag. Refer toAdding Tags to an AP on page 105 for more information.

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

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

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

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

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

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

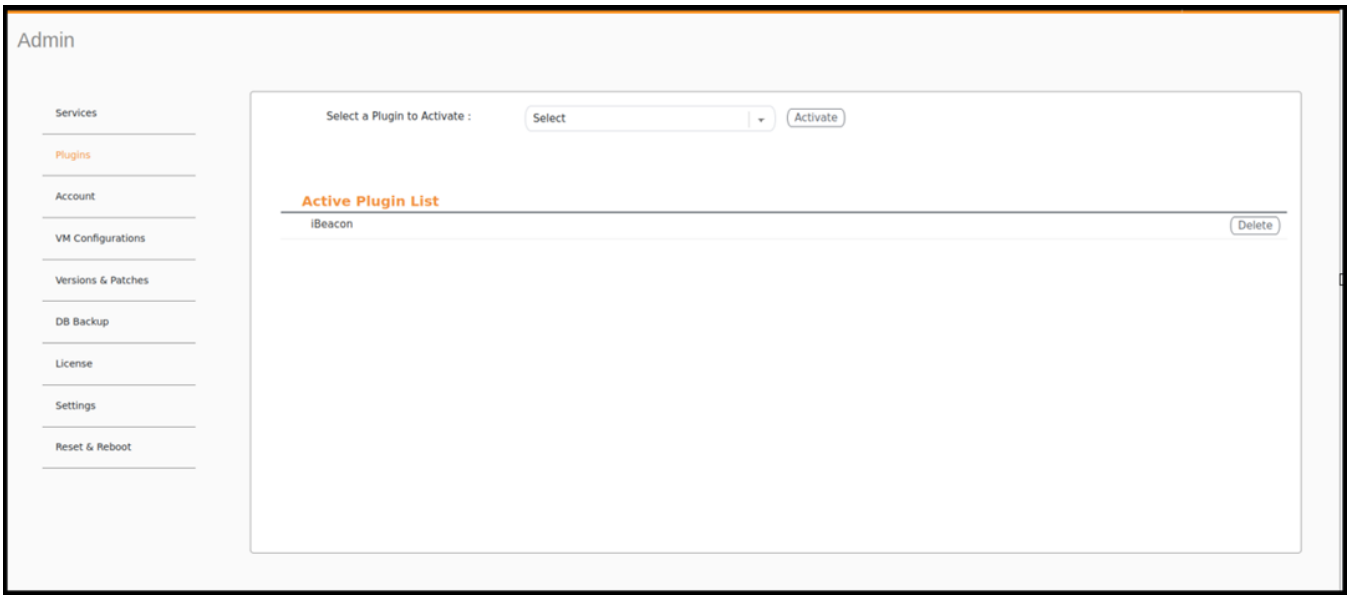
      The filter allows only the BLE ADV packets with the specified UUID to be passed on to the vendor application.
   h) Enable heartbeat.

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

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

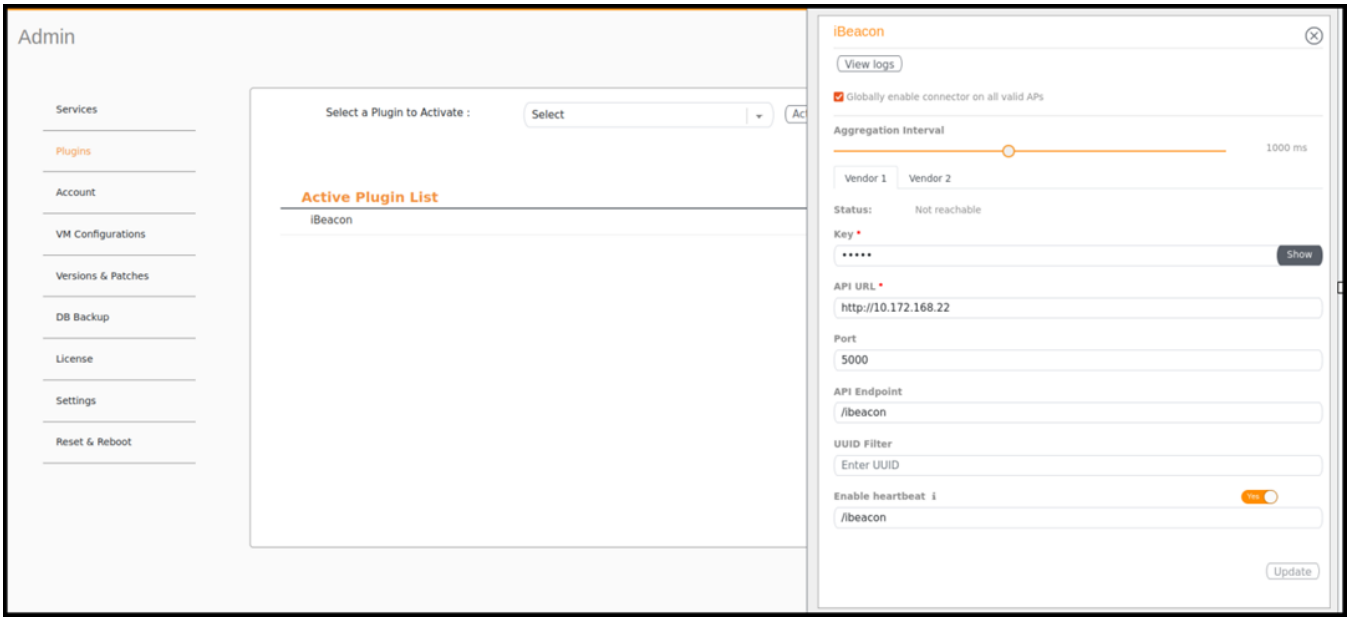
6. To deactivate the iBeacon plugin, select it and click **Deactivate**.

FIGURE 35 Deactivating the iBeacon Plugin



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

FIGURE 36 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 37 Activating the Beacon as a Service Plugin (iBeacon)

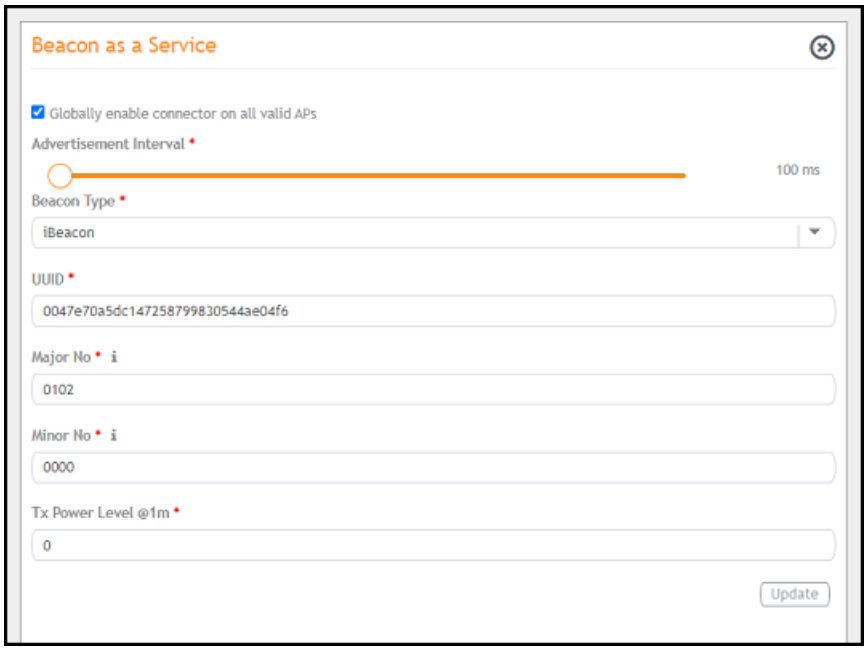


FIGURE 38 Activating Beacon as a Service (Eddystone)

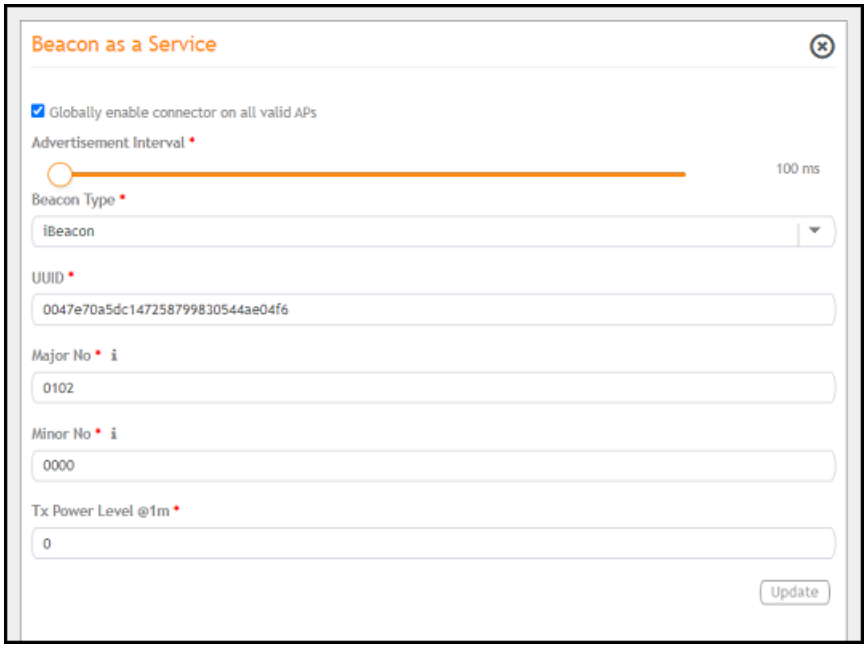
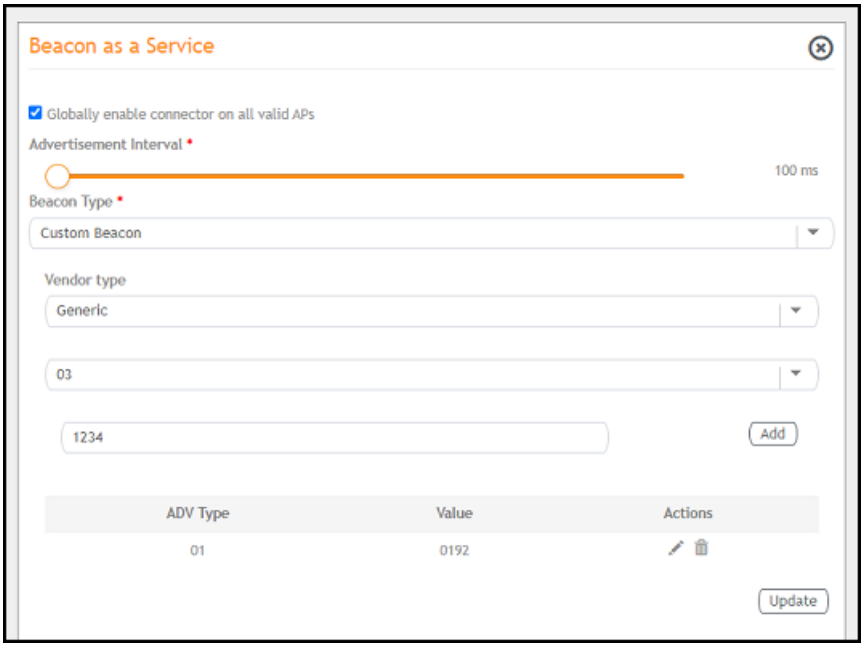


FIGURE 39 Activating Beacon as Service (Generic)



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.

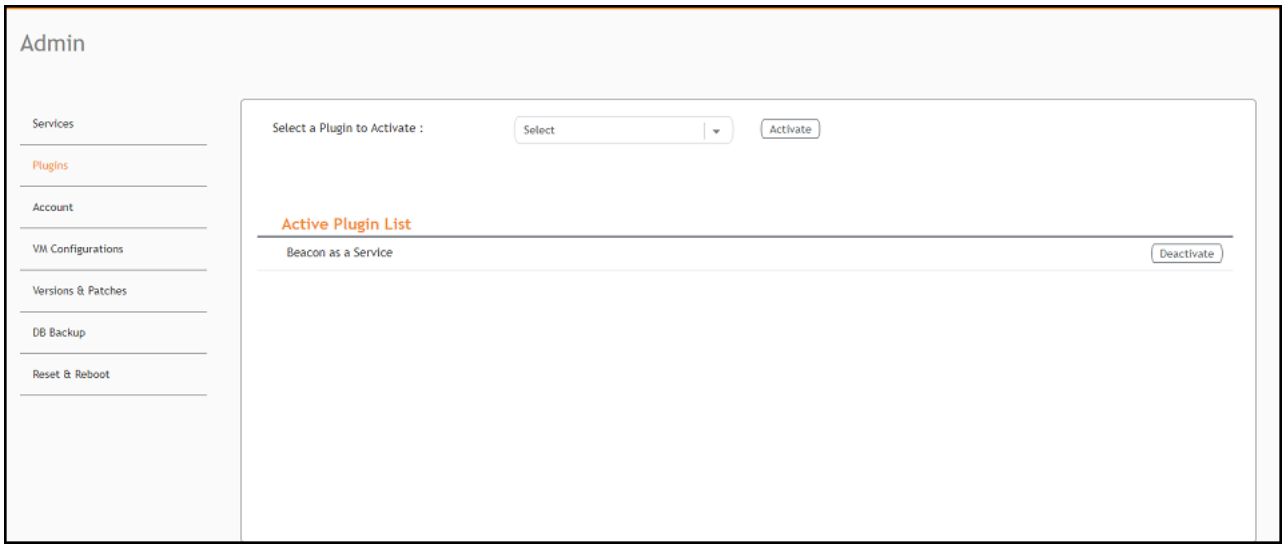
      NOTE
      If **Globally enable connector on all valid APs** is not selected, you can activate the plugin for each AP by adding a tag. Refer to Adding Tags to an AP on page 105 for more information.

   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**.

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

FIGURE 40 Deactivating the Beacon as a Service Plugin



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

FIGURE 41 Updating the Configuration Parameters (iBeacon)

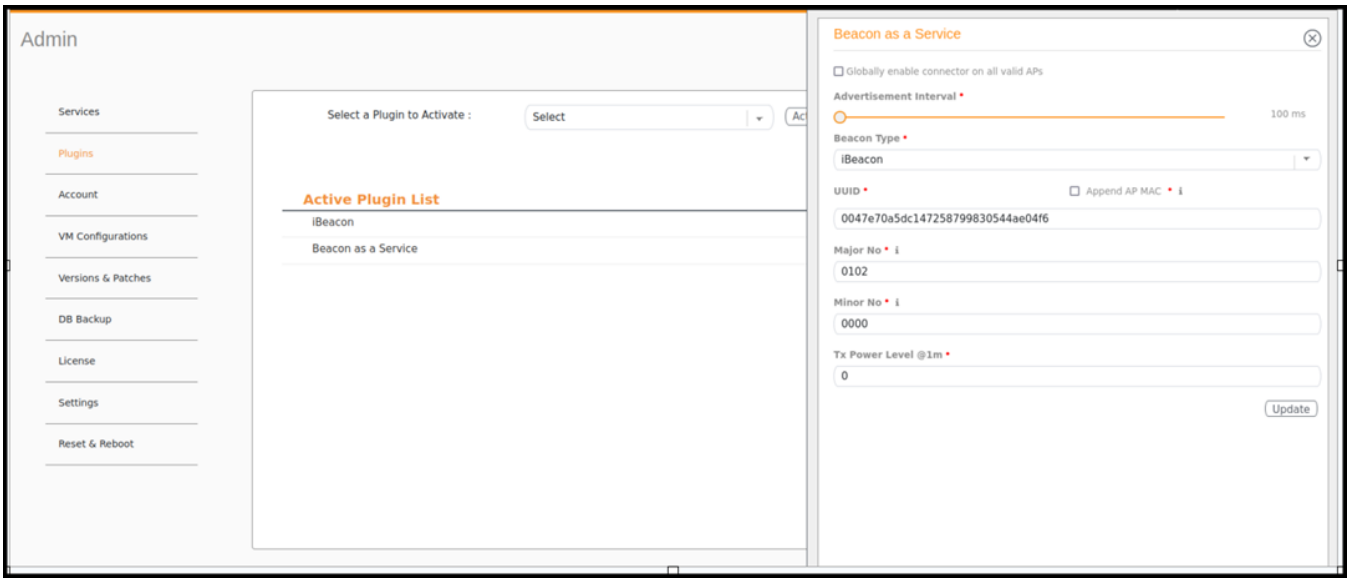


FIGURE 42 Updating Configuration parameters (Eddystone)

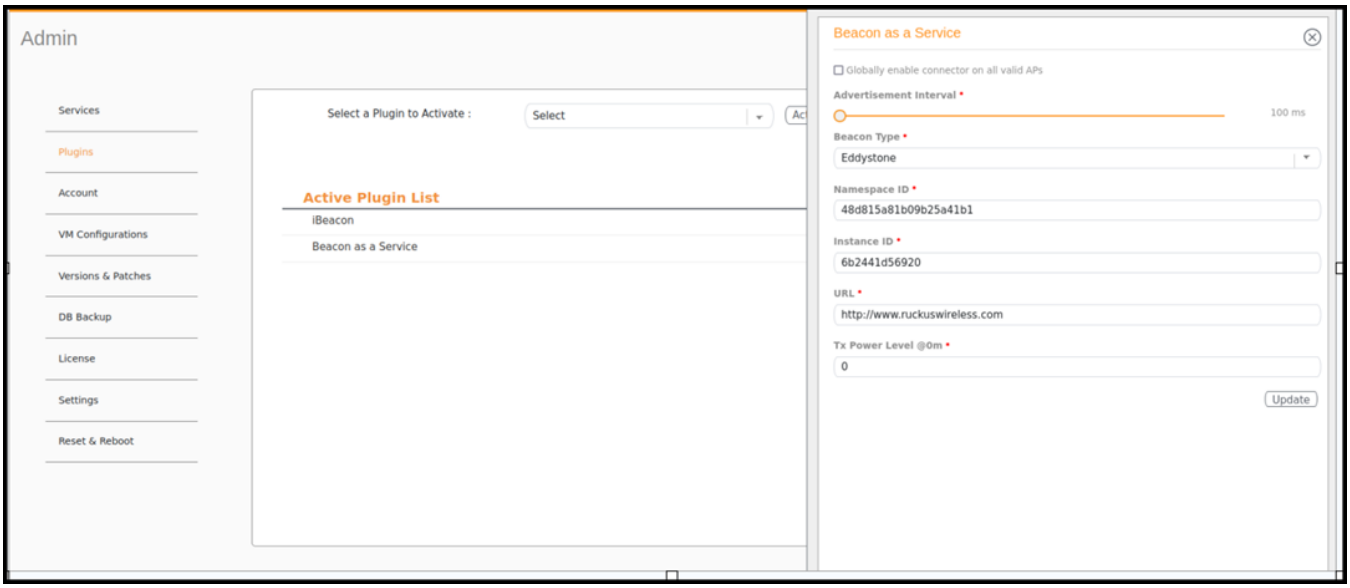
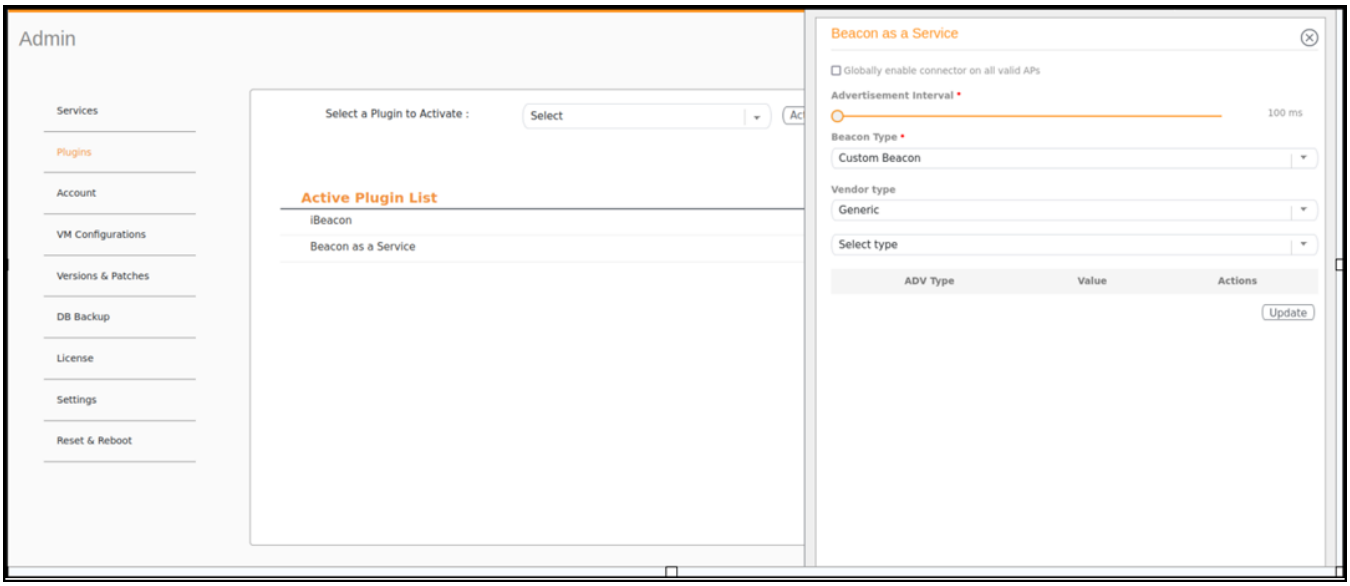


FIGURE 43 Updating Configuration Parameters (Generic)



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 44 Activating the Beacon as a Service Plugin

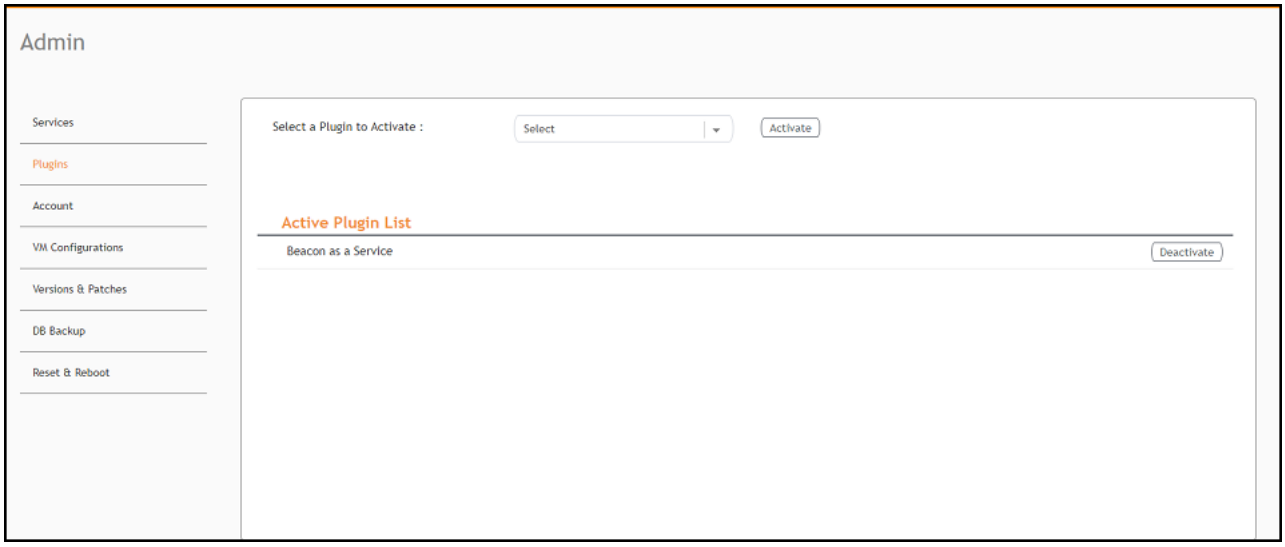
4. After the Beacon as Service plugin is activated, enter the following configuration parameters.
   a) Select **Globally enable connector on all valid APs** to add all respective IoT APs automatically. Connectors are mapped to IoT AP by adding the connector name tag to the IoT AP.

      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 105 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 45 Deactivating the Beacon as a Service Plugin



Activating and Editing the BLE Scan Plugin

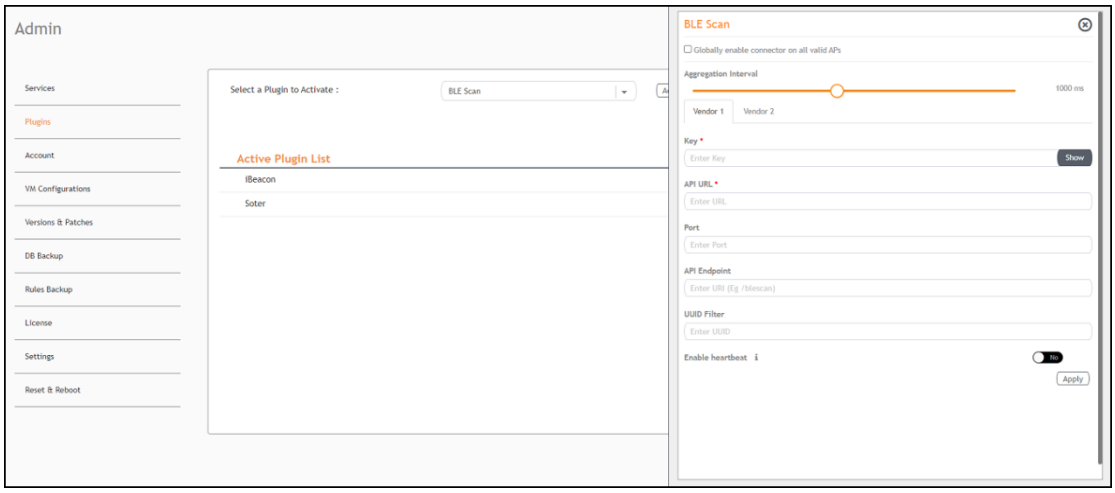
The RUCKUS IoT Controller provides support for the Bluetooth Low Energy (BLE) BLE Scan Plugin . The RUCKUS IoT Controller reads the packet from the IoT AP and routes the packets to the BLE beacon vendor cloud services.

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 46 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 105 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.

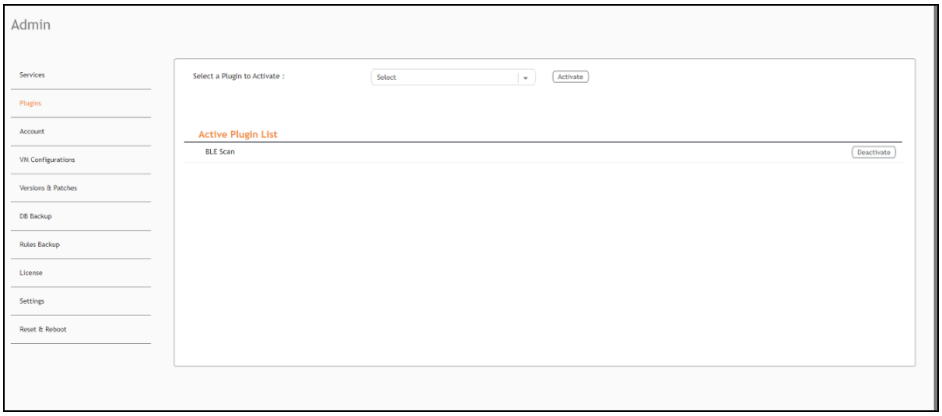
      Enabling heartbeat allows the vendor application to receive the IoT AP status, such as online or offline.

5. Click **Apply**.

   The BLE Scan plugin is added in the **Active Plugin List**.

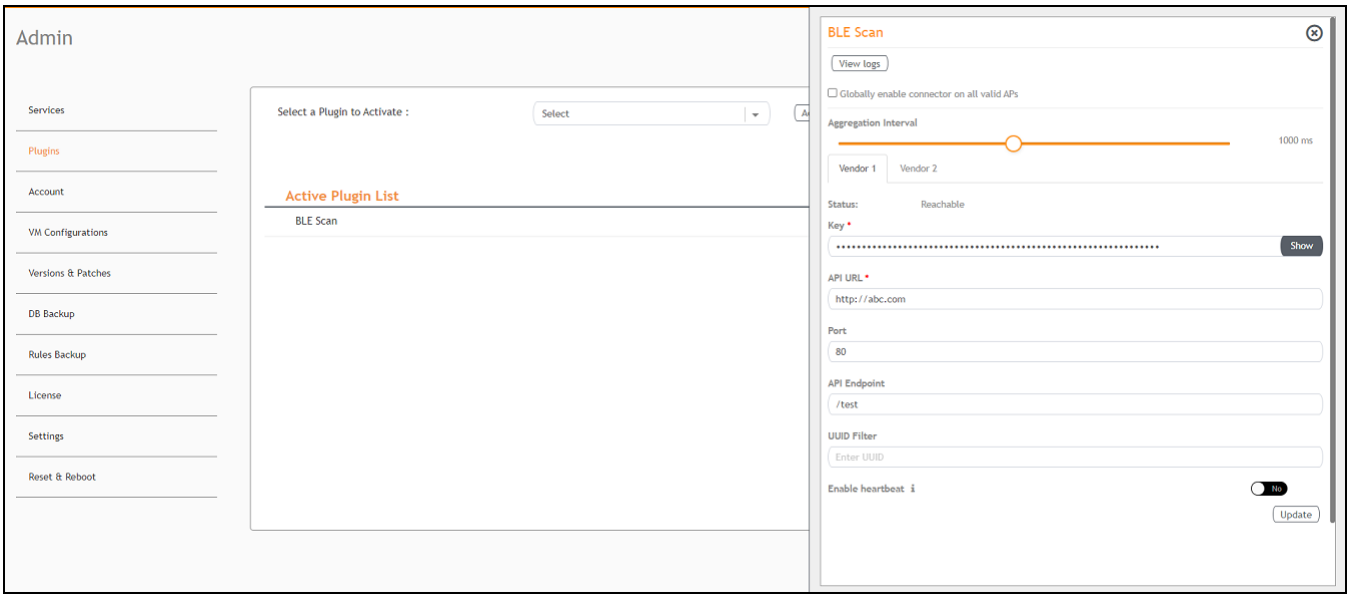
6. To deactivate the BLE Scan plugin, select it and click **Deactivate**.

FIGURE 47 Deactivating the BLE Scan Plugin



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

FIGURE 48 Updating the Configuration Parameters



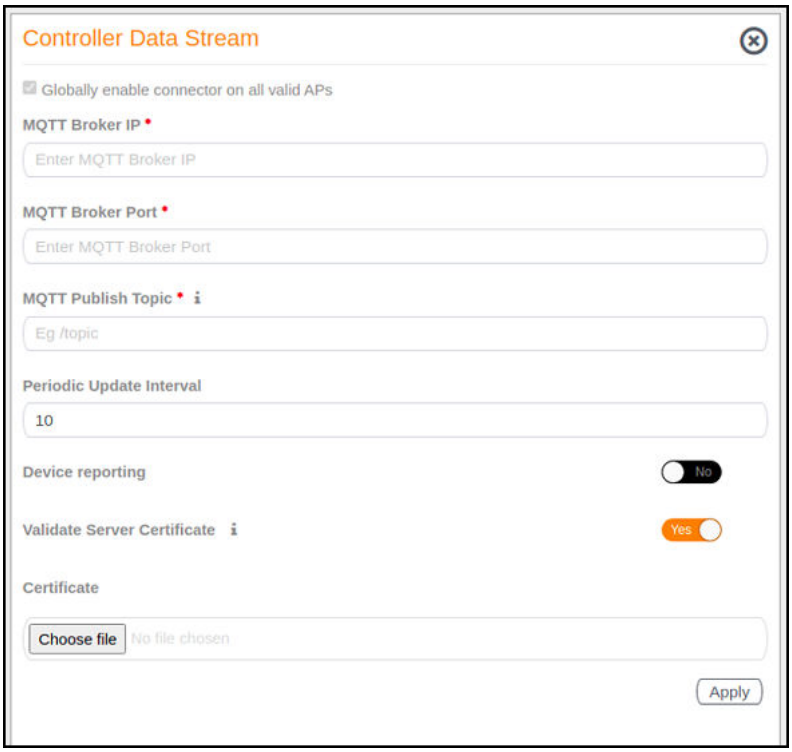
Activating and Editing the Controller Data Stream Plugin

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 49 Activating the Controller Data Stream Plugin

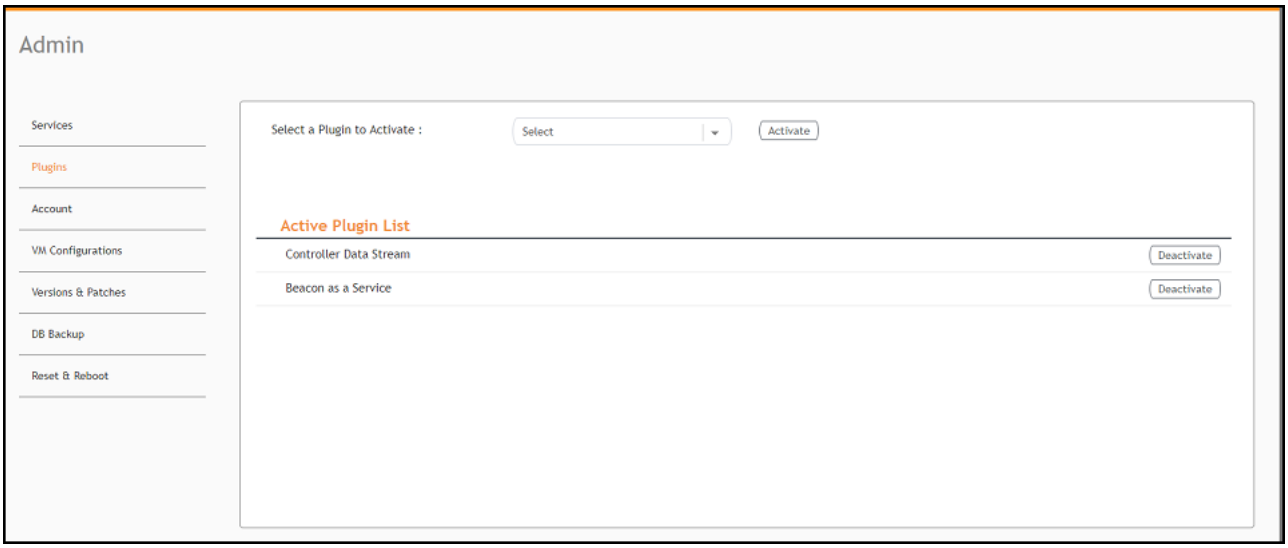


4. After the Controller Data Stream plugin is activated, enter the following configuration parameters.
   a) In **MQTT Broker IP**, enter the IP address of your MQTT broker.
   b) In **MQTT Broker Port**, enter the network port to which you want to connect.
   c) In **MQTT Publish Topic**, enter the 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.
   d) In **Periodic Update Interval** enter the interval to receive MQTT Publish.
   e) Enable **Device Reporting** and enter the topic endpoint which will publish message whenever a device change event is received.
   f) 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**.

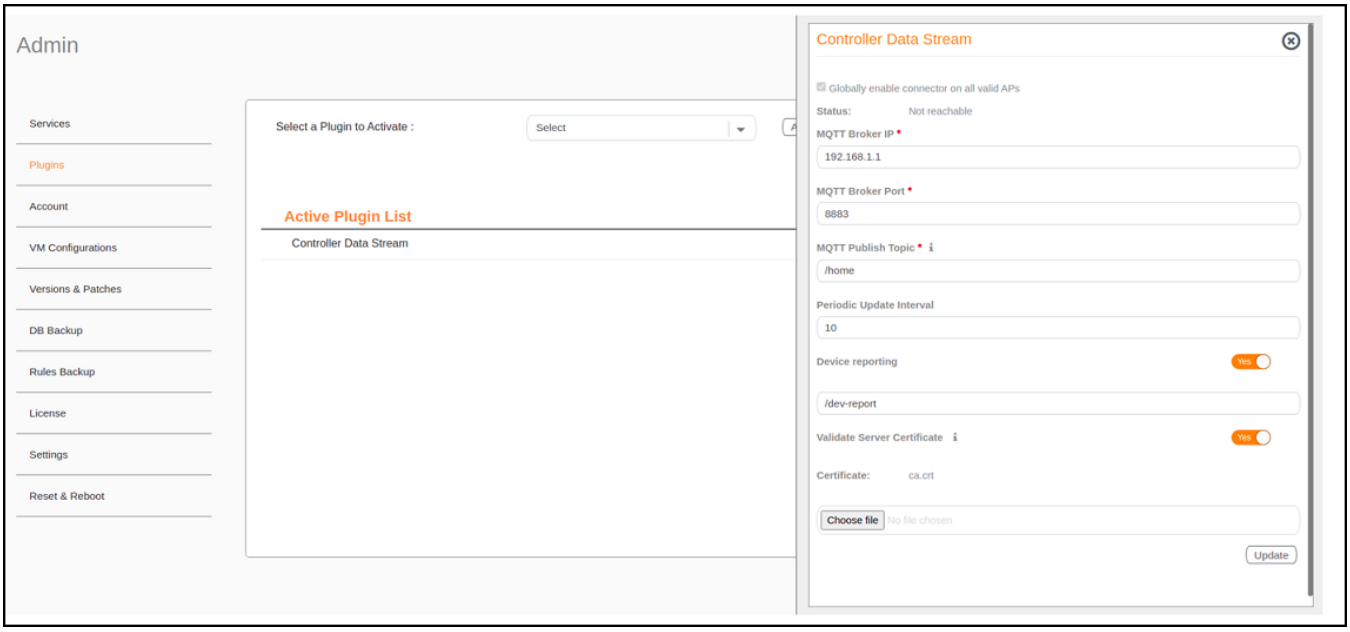
6. To deactivate the Controller Data Stream plugin, select it and click **Deactivate**.

FIGURE 50 Deactivating the Controller Data Stream Plugin



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

FIGURE 51 Updating the Configuration Parameters



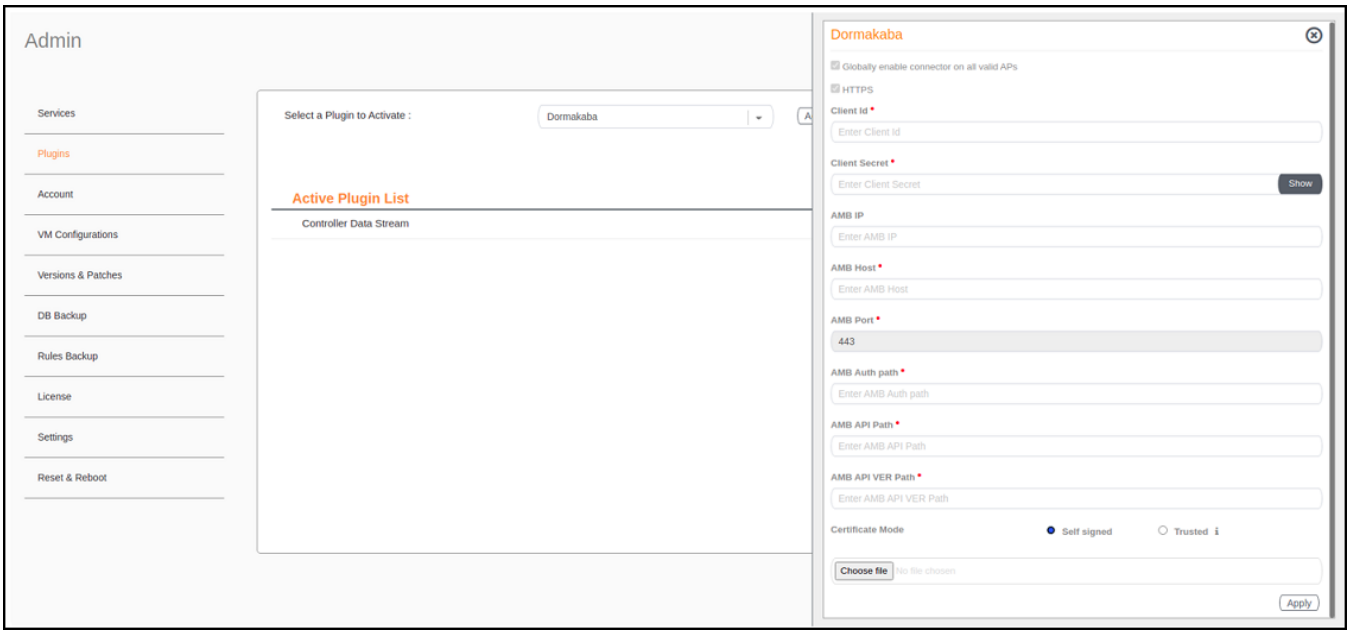
Activating and Editing the Dormakaba Plugin

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 52 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.

      NOTE
      The Client ID must not be configured as "admin" while activating the Dormakaba plugin.

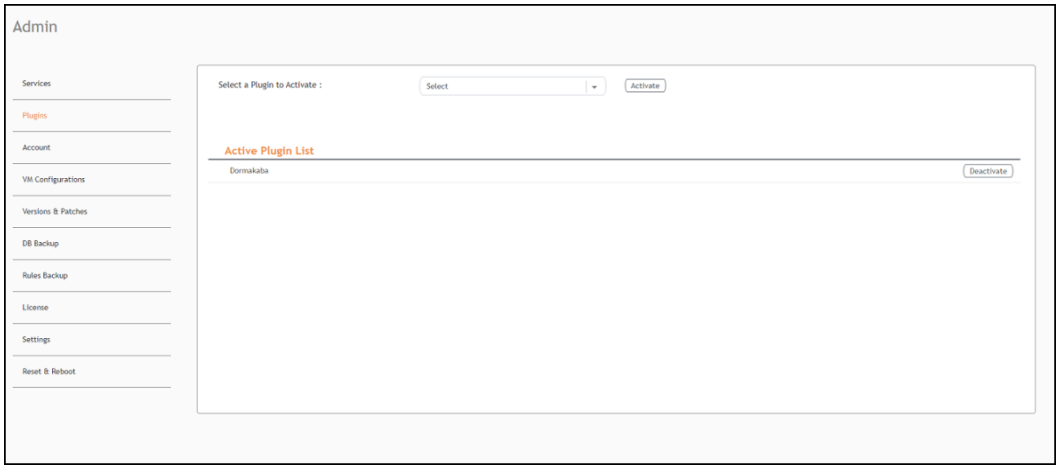
   b) Enter the **Client Secret** used for connecting to Ambiance Server.
   c) Enter the **Ambiance IP Address** .
   d) Enter the **Ambiance Host**.

      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**.

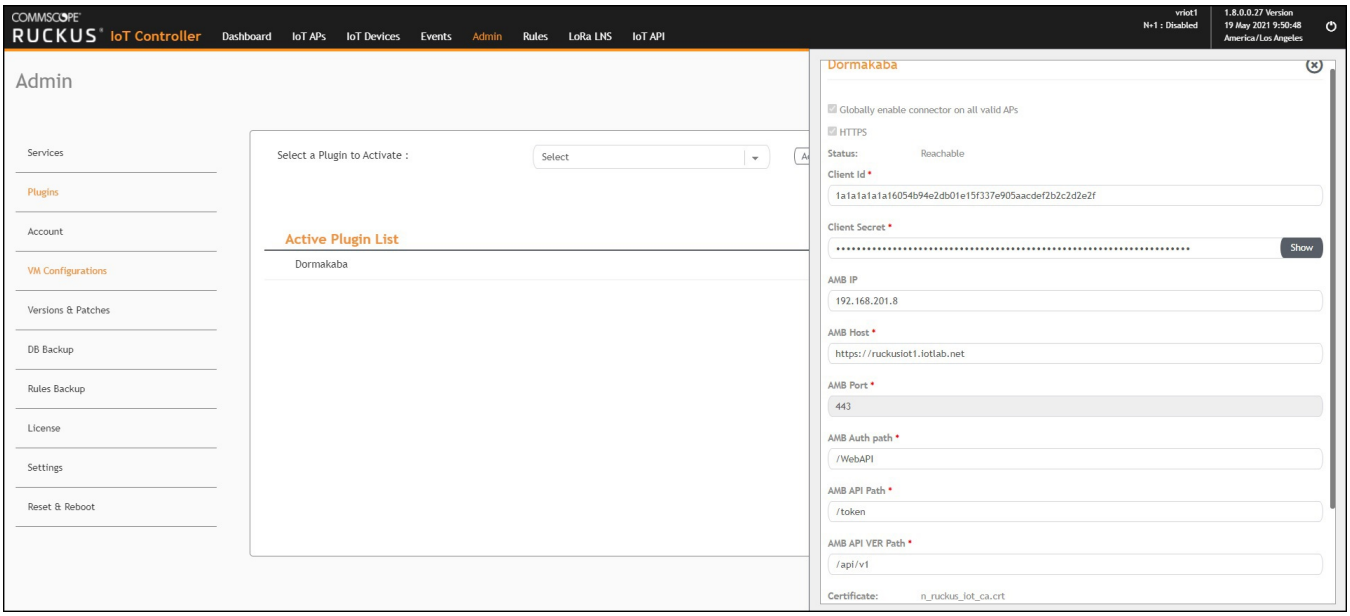
   The Dormakaba plugin is added in the **Active Plugin List**.
6. To deactivate the Dormakaba plugin, select it and click **Deactivate**.

FIGURE 53 Deactivating the Dormakaba Plugin



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

FIGURE 54 Updating the Configuration Parameters



Activating and Editing the Telkonet Plugin

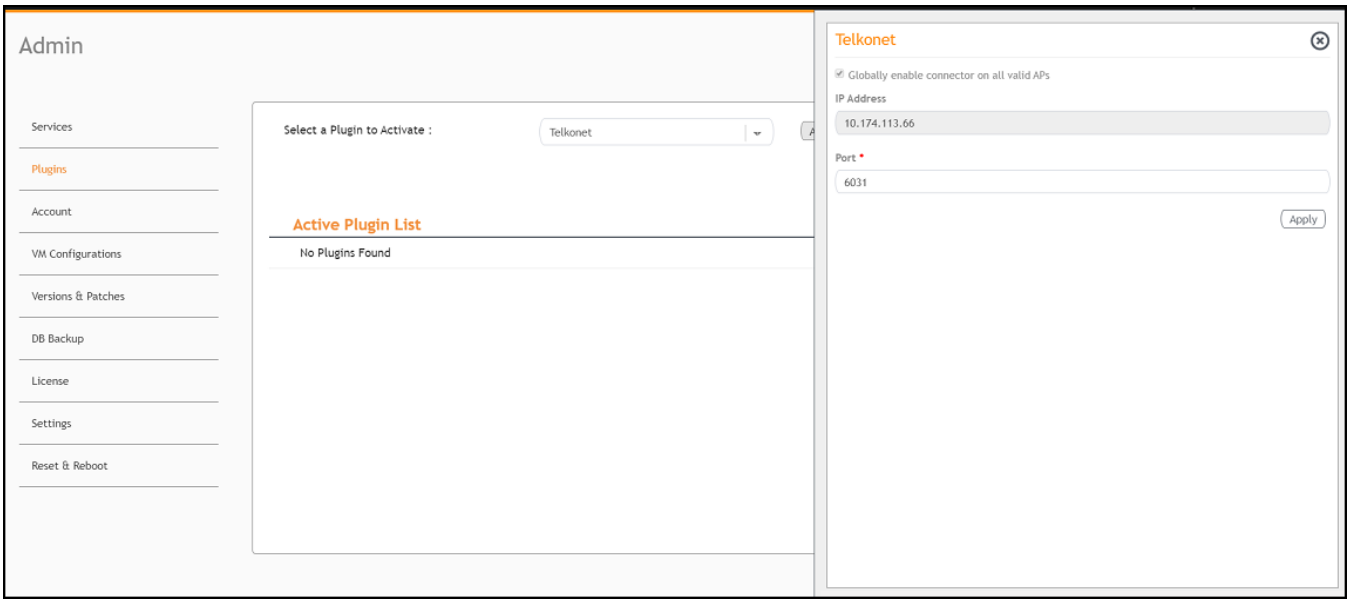
The RUCKUS IoT Controller provides support for the Telkonet devices and their respective MQTT APIs.

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 55 Activating the Telkonet Plugin



4. After the Telkonet plugin is activated, enter the following configuration parameters.
   a) Enter the IP Address.

      This is the IP address of the Telkonet controller.

   b) Enter the Port number.

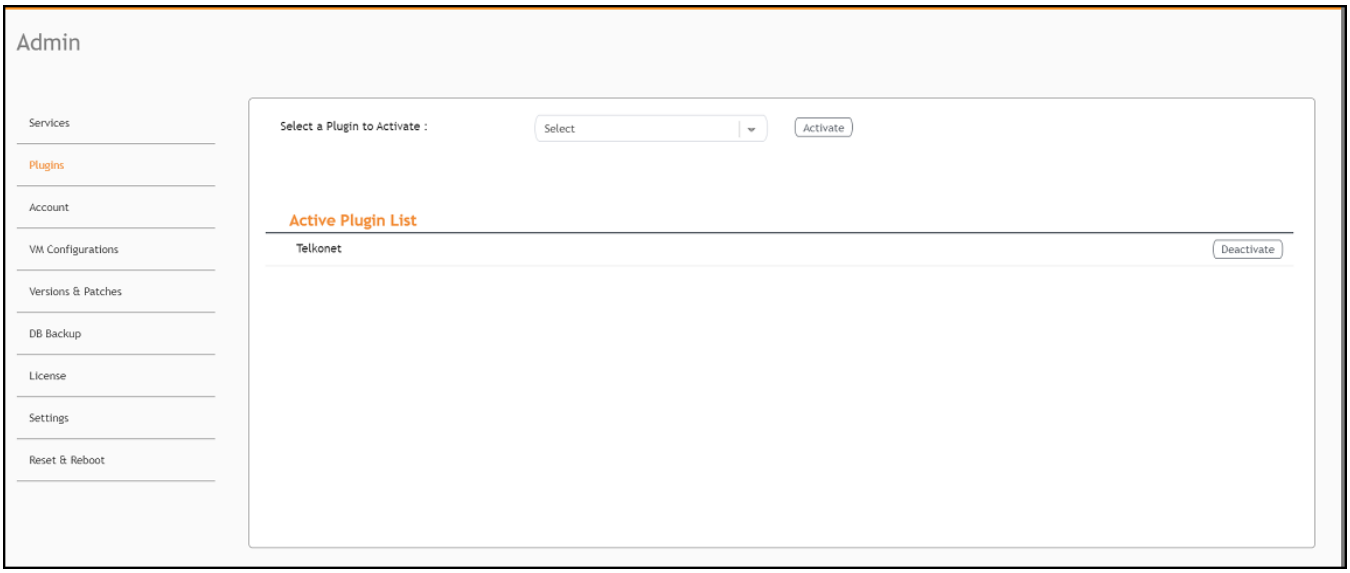
      This is the port number on which the vendor/connector web server is running.

5. Click **Apply**.

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

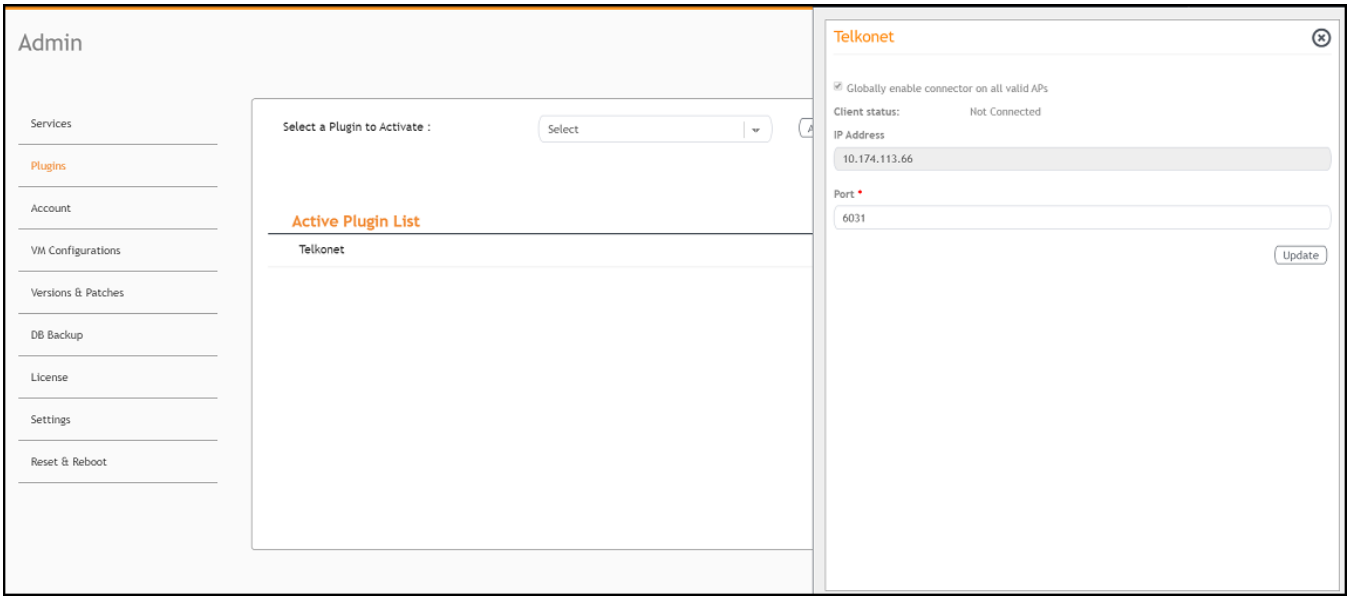
6. To deactivate the Telkonet plugin, select it and click **Deactivate**.

FIGURE 56 Deactivating the Telkonet Plugin



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

FIGURE 57 Updating the Configuration Parameters



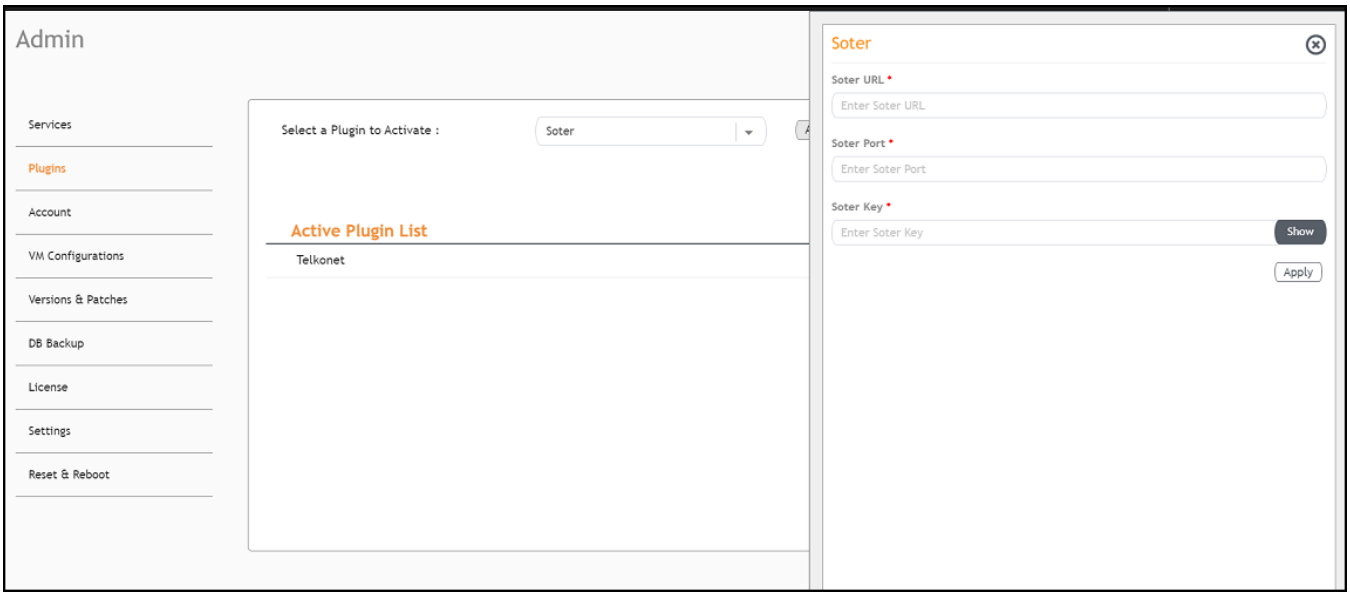
Activating and Editing the Soter Plugin

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 58 Activating the Soter Plugin



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

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

   b) Enter the Port number.

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

      NOTE
      The default MQTT port is 8883.

   c) Enter the Key.

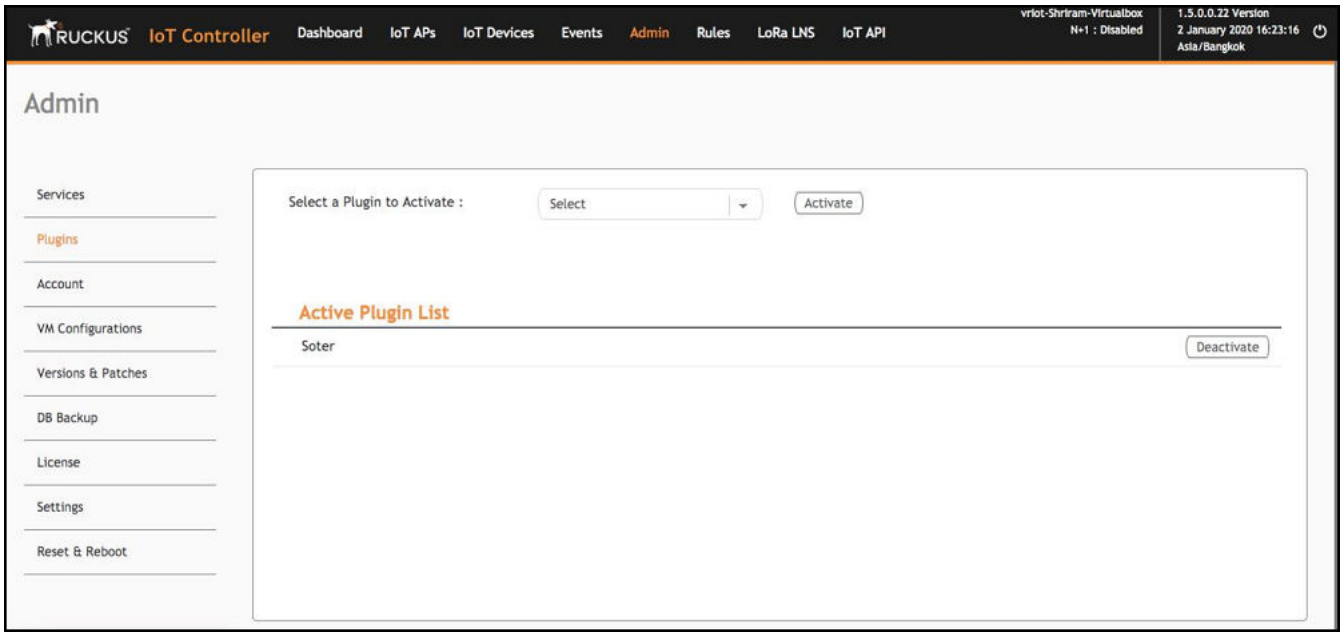
      The Vendor application is responsible for authenticating the Keys.

5. Click **Apply**.

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

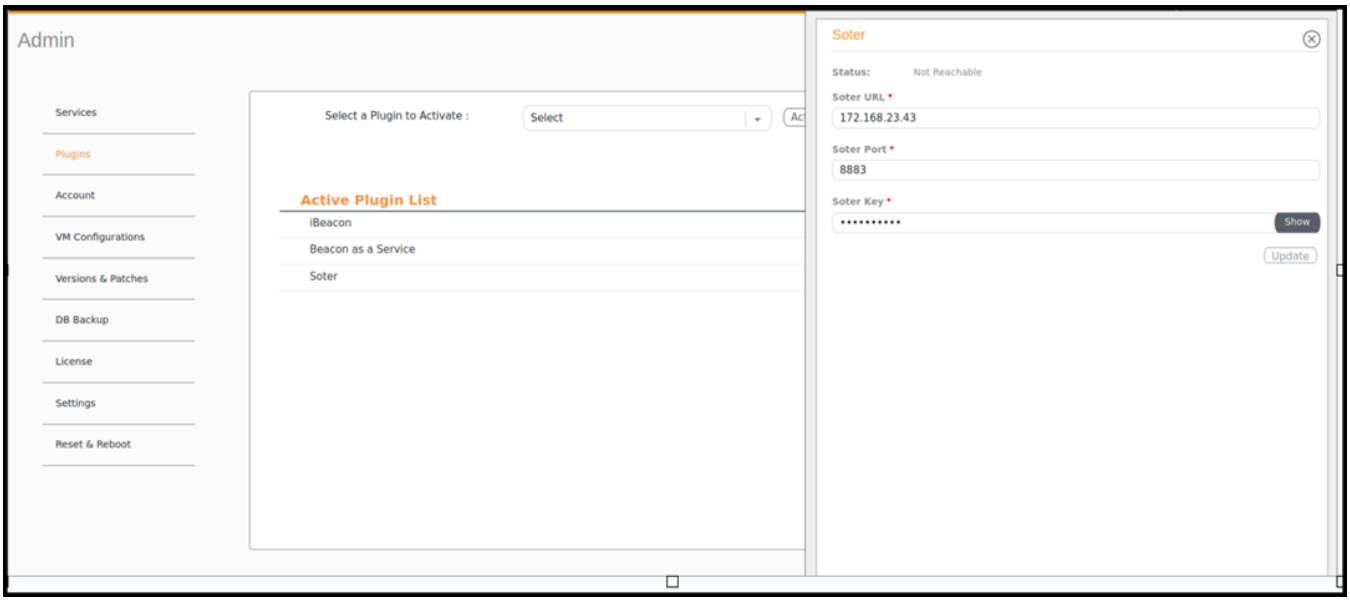
6. To deactivate the Soter plugin, select it and click **Deactivate**.

FIGURE 59 Deactivating the Soter Plugin



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

FIGURE 60 Updating the Configuration Parameters



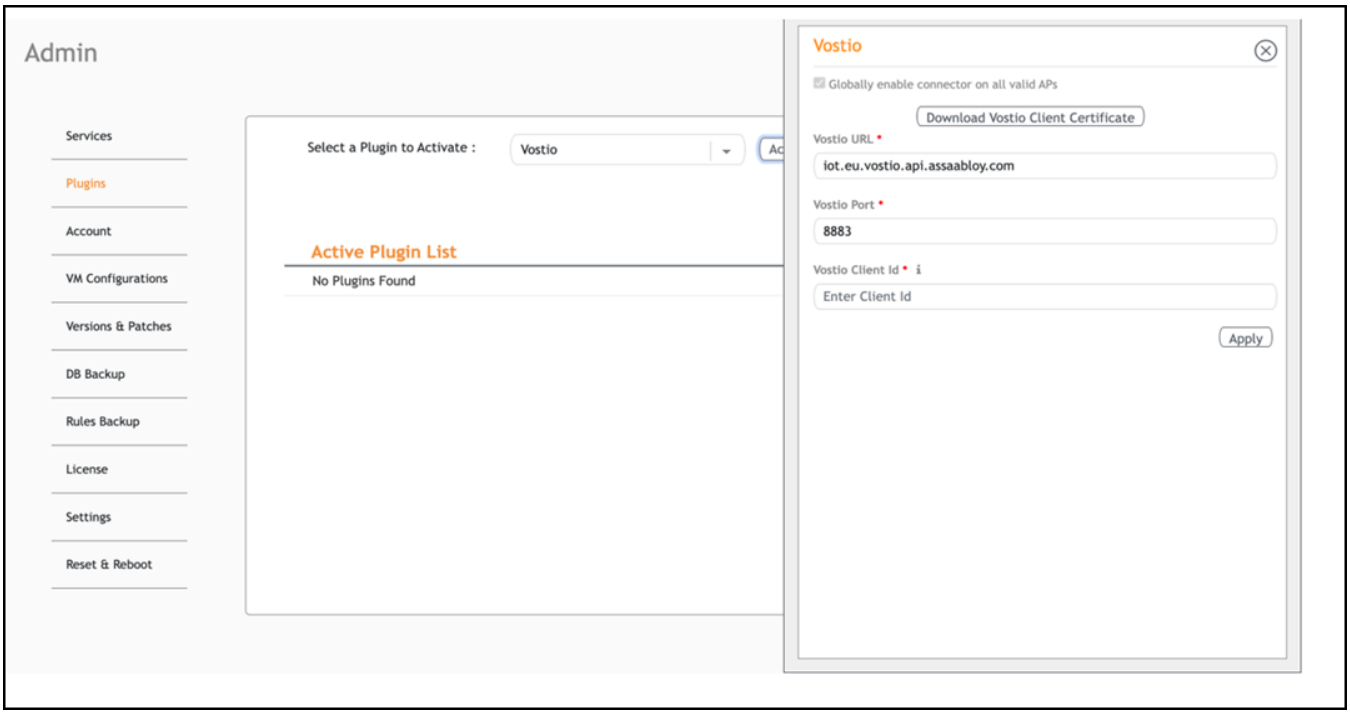
Activating and Editing the Vostio Plugin

The RUCKUS IoT Controller supports the Vostio plugin. The RUCKUS IoT Controller communicates with Vostio Assa Abloy cloud and executes the operations issued from the Vostio cloud.

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. From the **Select a Plugin to Activate** list, select a **Vostio** plugin and click **Activate**.

FIGURE 61 Activating the Vostio Plugin



4. After the Vostio plugin is activated, enter the following configuration parameters.
   a) Enable **Globally enable connector on all valid APs** to add IoT APs. The connectors are mapped to the IoT AP by adding the connector name tag to the 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 105 for more information.

   b) Click **Download Vostio Client Certificate** to generate and download the Vostio client certificate.
   c) In **Vostio URL** field, enter the URL for vostio.

      NOTE
      By default, the vostio URL is set to Vostio URL endpoint.

   d) In **Vostio Port** field, enter the port number.

      NOTE
      By default, the port number is 8883.

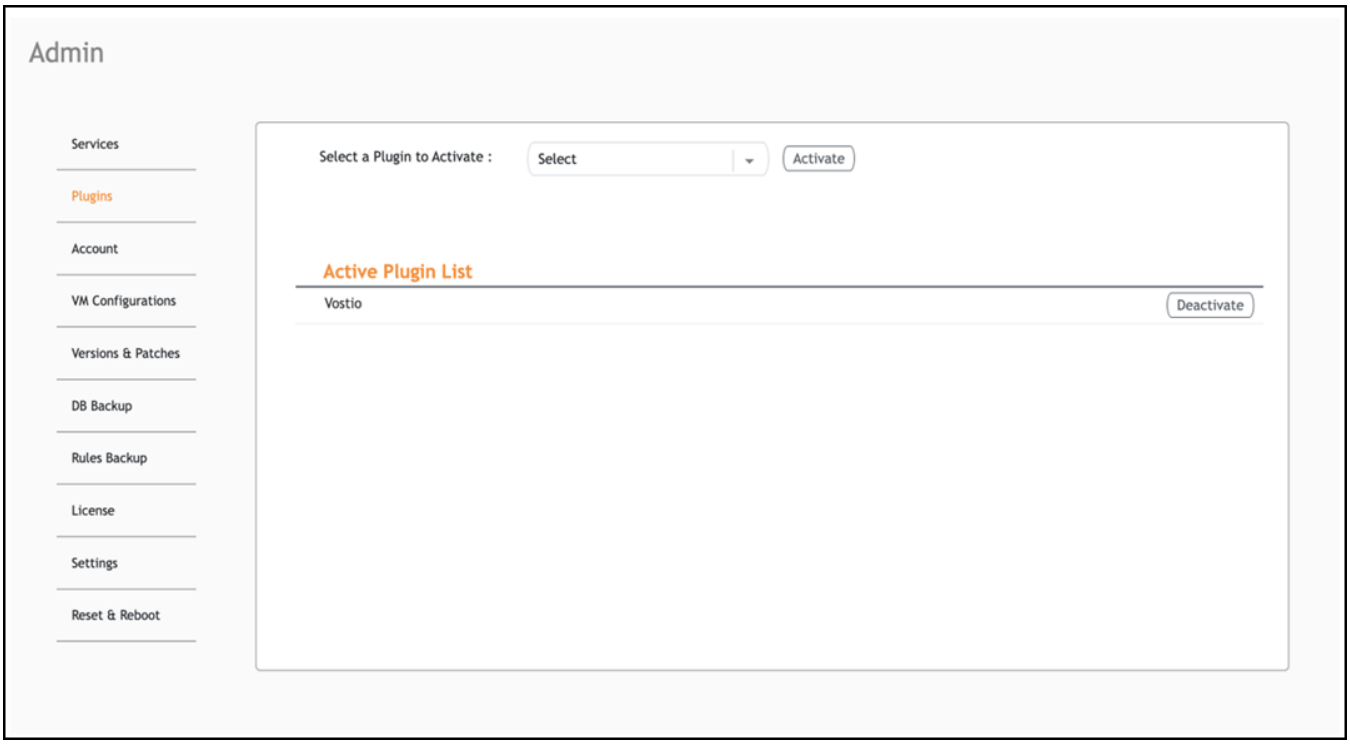
   e) In **Vostio Client Id** field, enter the network ID.

      NOTE
      Refer to Getting the Network ID from Vostio Cloud Platform on page 71 to retrieve the Network ID.

5. Click **Apply**. The Vostio plugin is added in the **Active Plugin List**.

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

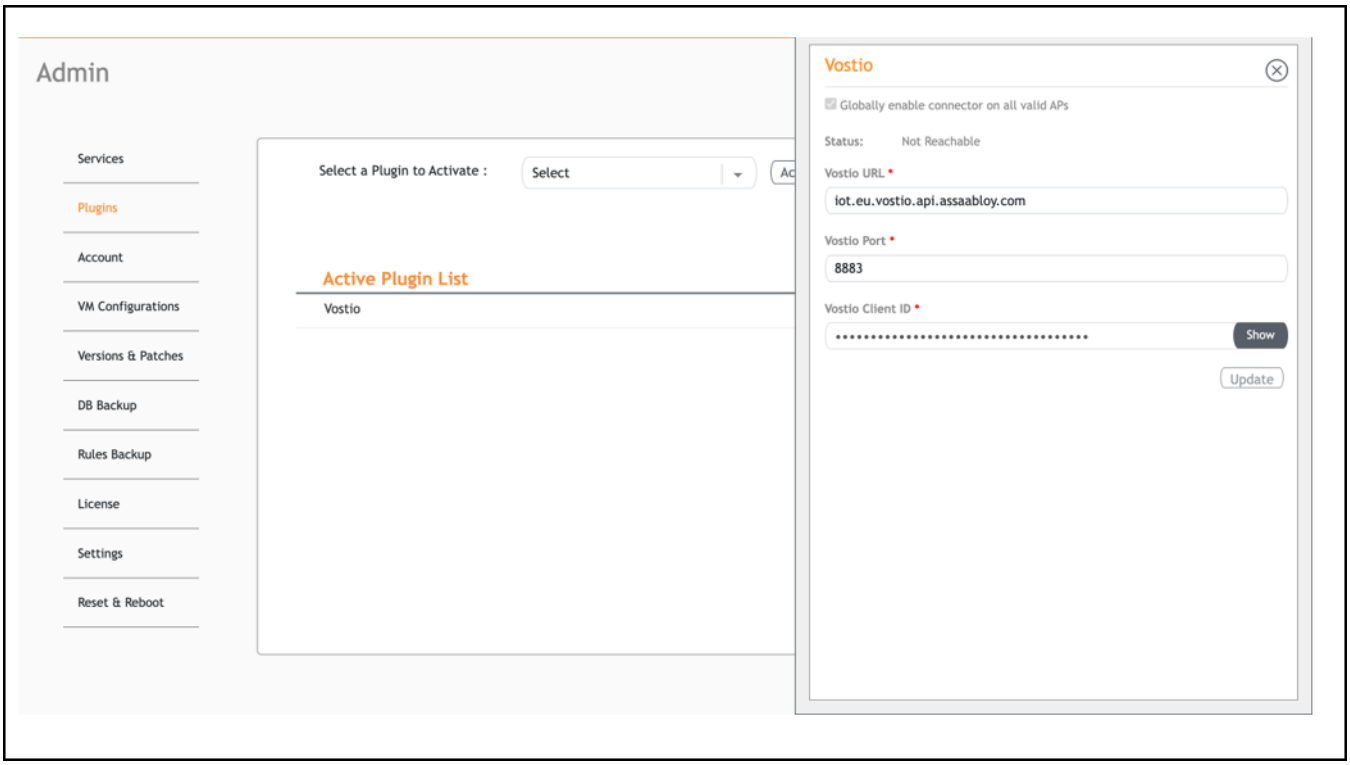
FIGURE 62 Deactivating the Vostio Plugin



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

NOTE
The **Vostio Client Id** field cannot be edited. You can edit **Vostio URL** and **Vostio Port** fields.

FIGURE 63 Updating the Fields in Vostio Plugin



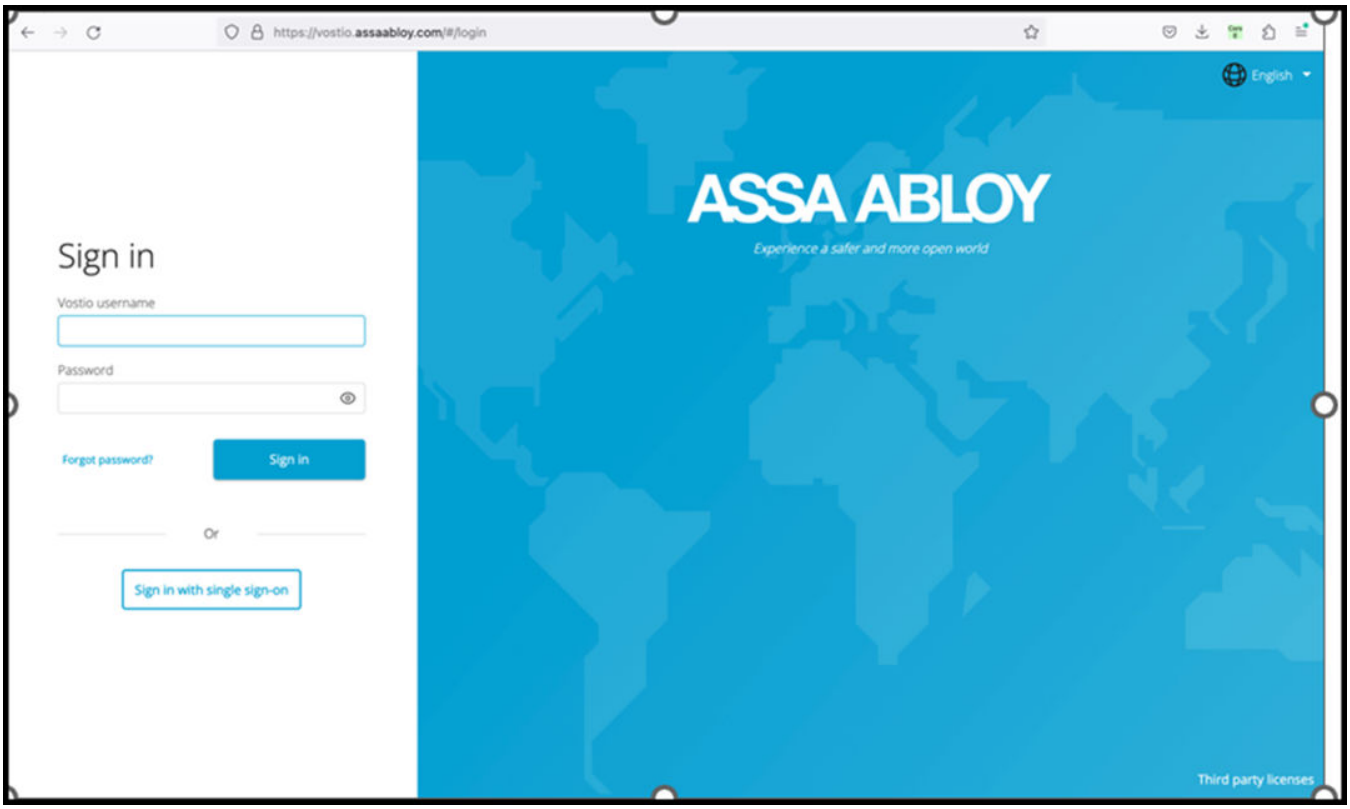
Getting the Network ID from Vostio Cloud Platform

Perform the following steps to obtain the network ID.

1. Open a web browser and type the url https://vostio.assaabloy.com/#/login.

   The **ASSA ABLOY** Sign in page is displayed.

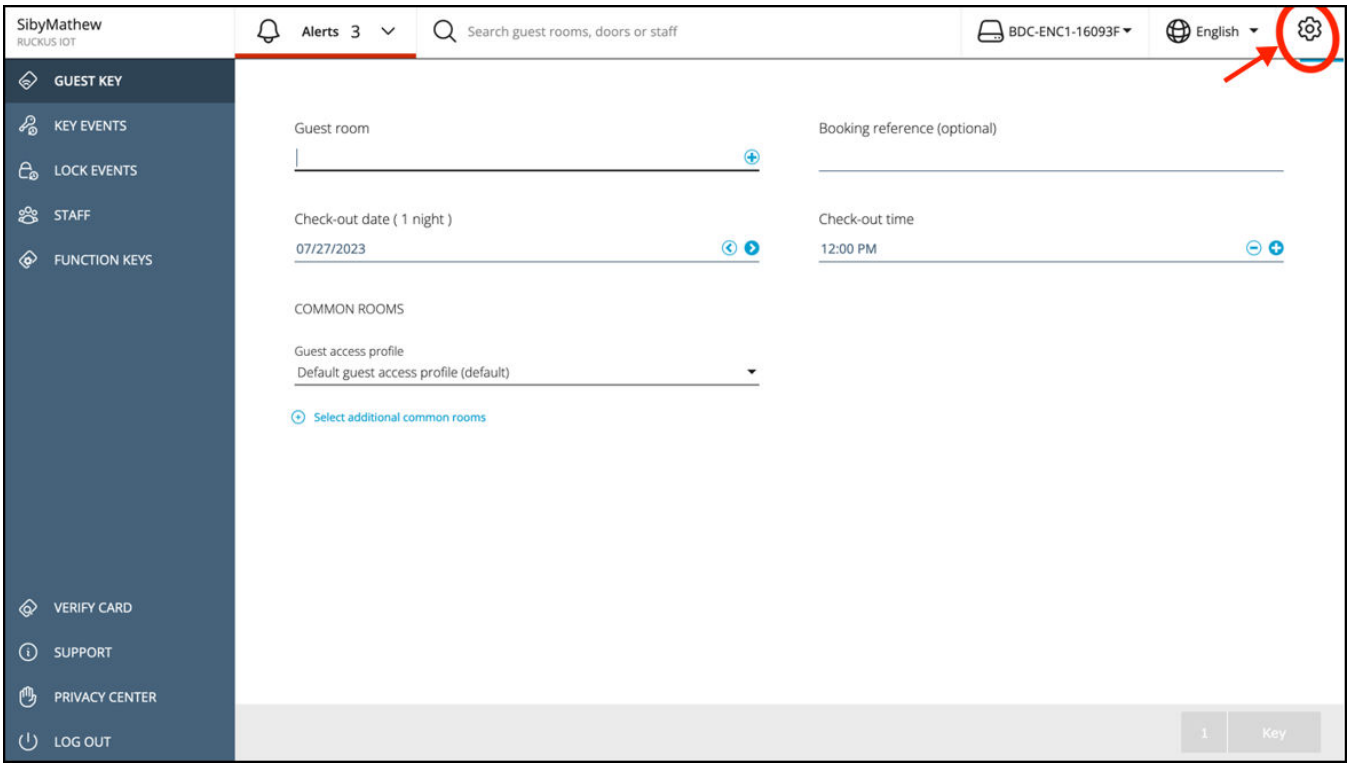
   FIGURE 64 ASSA ABLOY Sign In Page



2. Enter the Vostio username and password. Click **Sign in**.

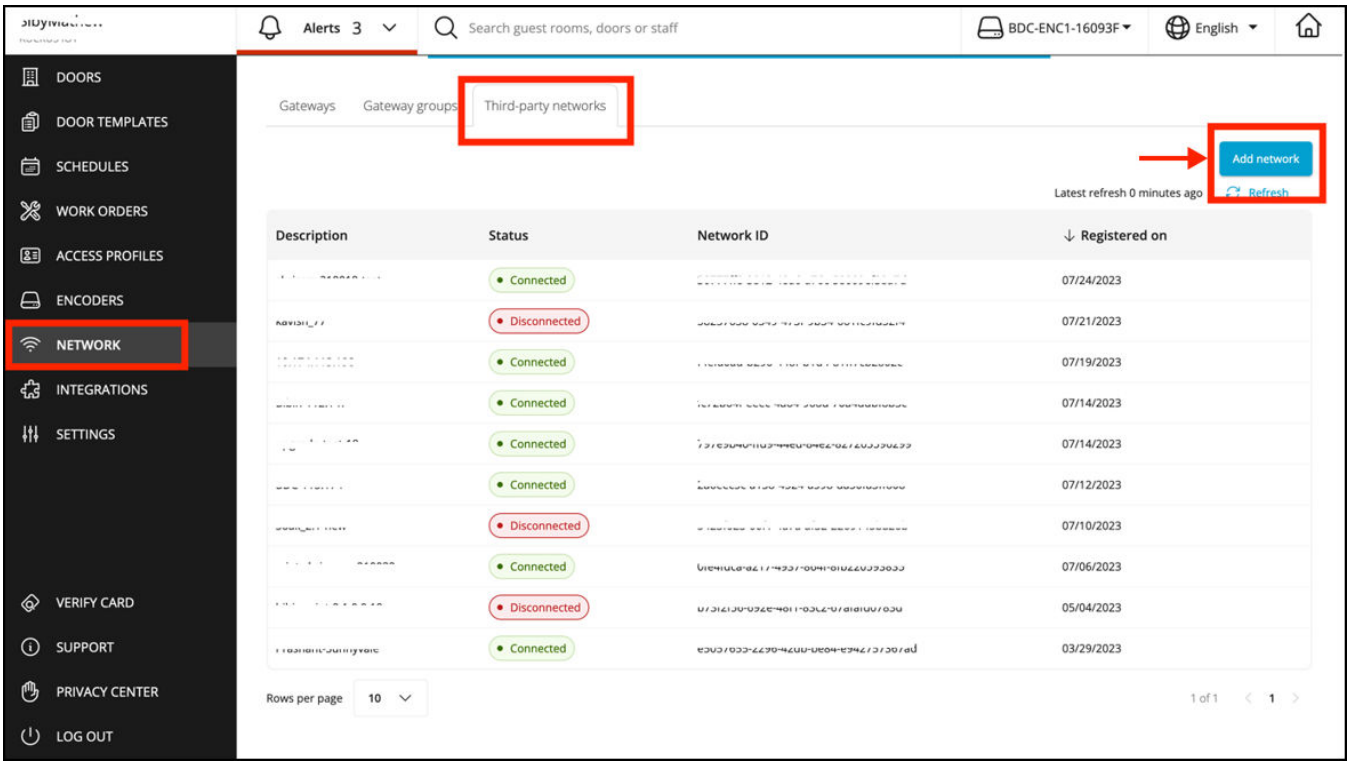
3. Click the **Settings** icon in the top right corner.

FIGURE 65 Settings Page



4. From the left navigation pane, select the **NETWORK** tab and click **Third -party networks**.

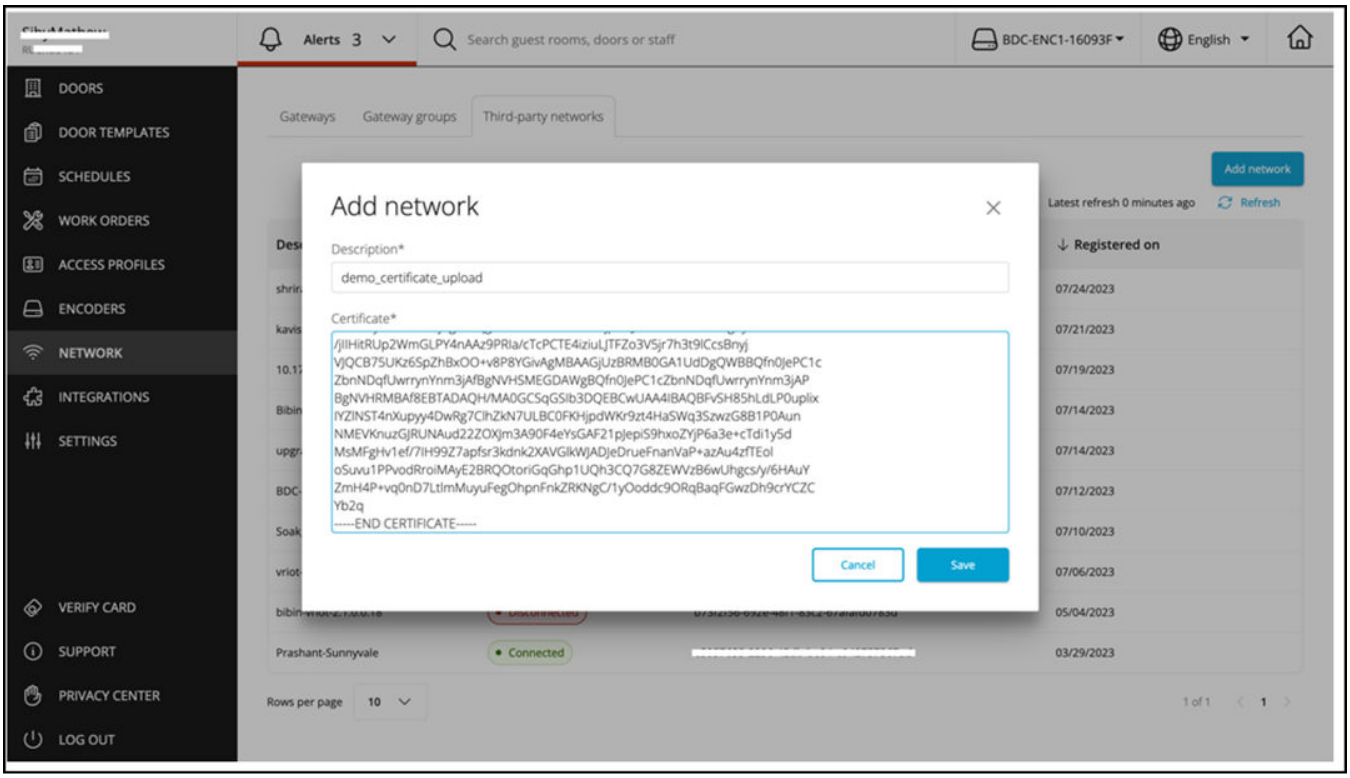
FIGURE 66 Selecting the Network Tab



5. Click **Add network** to add the details of the certificate in the **Add network** page.

   In the **Description** field, enter the name for the certificate. Copy the content of the certificate into the **Certificate** field, and click **Save**. You can view the certificate under the **Third-party networks** tab.

   FIGURE 67 Adding Network Details

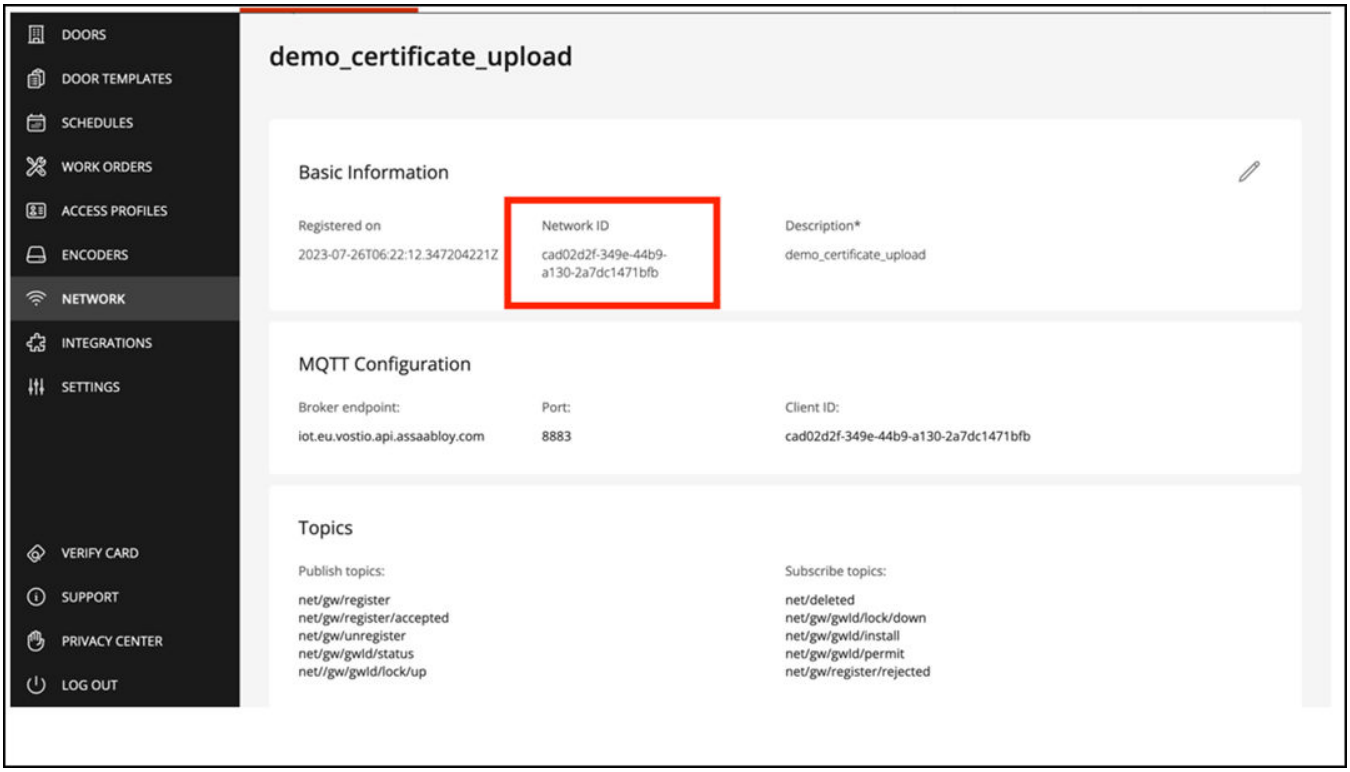


NOTE

Refer to step 4(b) Activating and Editing the Vostio Plugin on page 67 for downloading the Vostio Client certificate.

6. Click the uploaded certificate in **Description** column.Under **Basic Information** view the certificate details and capture the value of network ID in **Network ID** column.

FIGURE 68 Capturing the Network ID



NOTE
The value of the network ID is used as the Vostio client ID for RUCKUS IoT Controller.

SALTO Plugin

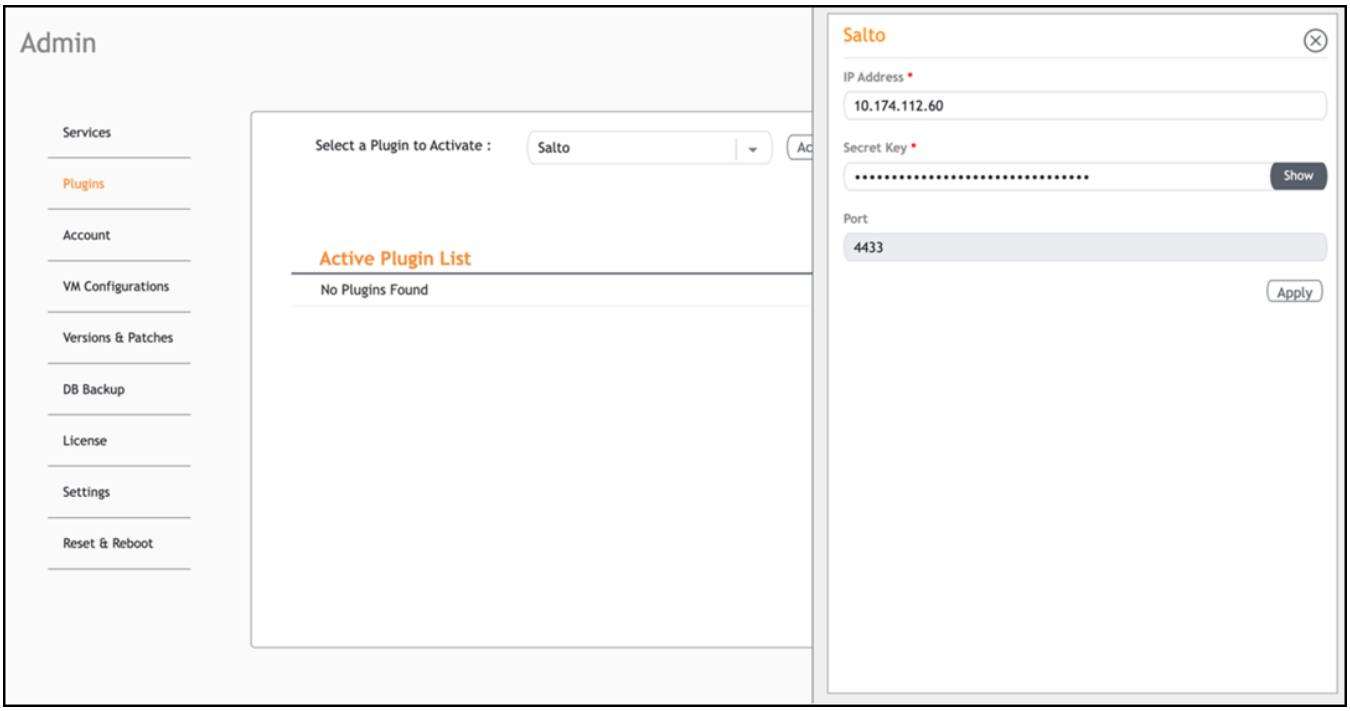
The SALTO App operating within the RUCKUS IoT Controller communicates with SALTO space solutions, and onboards SALTO locks to the gateway through gateway and lock internal communication.

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 Salto plugin and click **Activate**.

   FIGURE 69 Selecting Salto PLugin from the list



4. After the Salto plugin is activated, enter the following configuration parameters.
   a) Enter the **IP Address** of the Salto Space for which you want the RUCKUS IoT Controller to be configured.
   b) Enter the **Security Key** which is generated from the Salto Space.

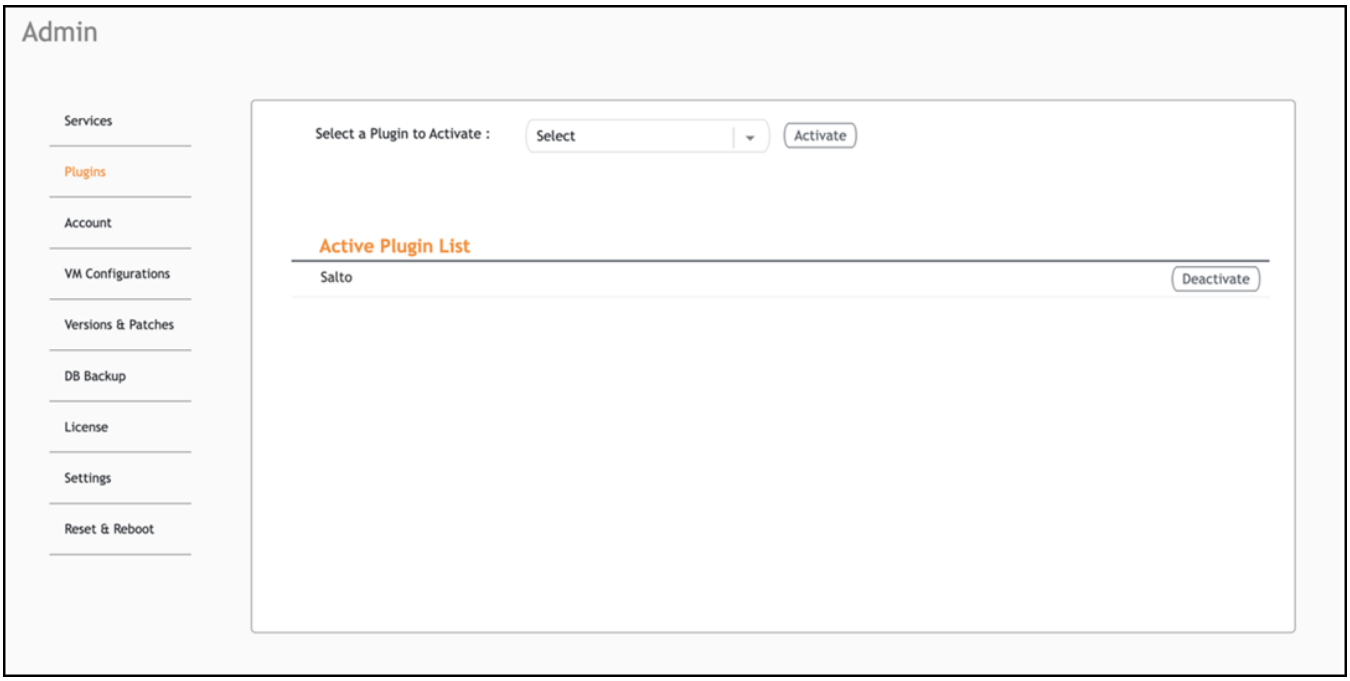
      NOTE
      Refer to Adding Controller to the SALTO Space on page 79 to generate the Secret Key.

   c) The **Port** is pre-configured with the port number 4433, and this value cannot be altered.
5. Click **Apply**.

   The Salto plugin is added in the **Active Plugin List**. After activating the plugin, navigate to the Salto Space and perform its Initialization. Refer to Adding Controller to the SALTO Space on page 79 to perform Initialization.

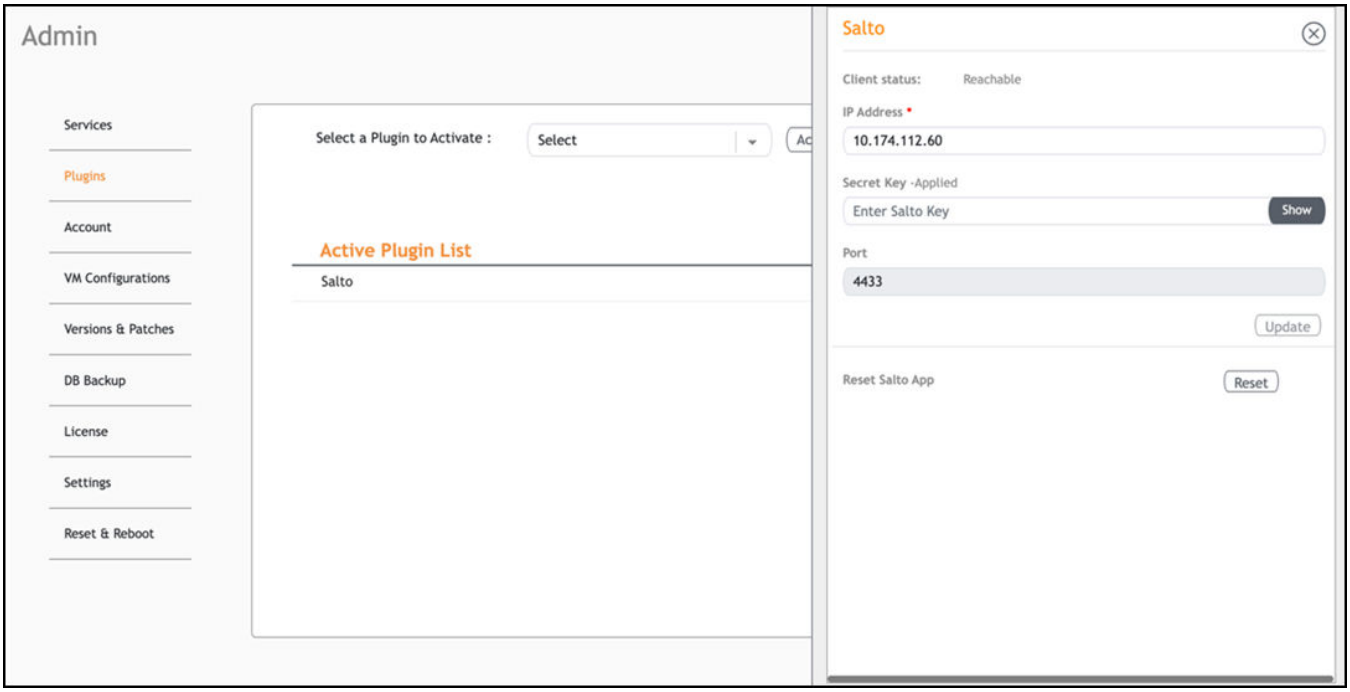
6. To deactivate the Salto plugin, select it and click **Deactivate**.

FIGURE 70 Dectivating the Plugin



7. To edit the configuration of the Salto plugin, click **Reset** adjacent to Reset Salto App. This clears the entry in the **Secret Key** field and closes the Salto plugin side bar.

   FIGURE 71 Updating the Configuration



8. Select the Salto plugin from the **Active Plugin List** and repeat step 4 to enter the new configuration parameters. Cick **Update**. After successfully updating the plugin initlaize the Secret Key. Refer to Adding Controller to the SALTO Space on page 79 to perform Initialization.

Adding Controller to the SALTO Space

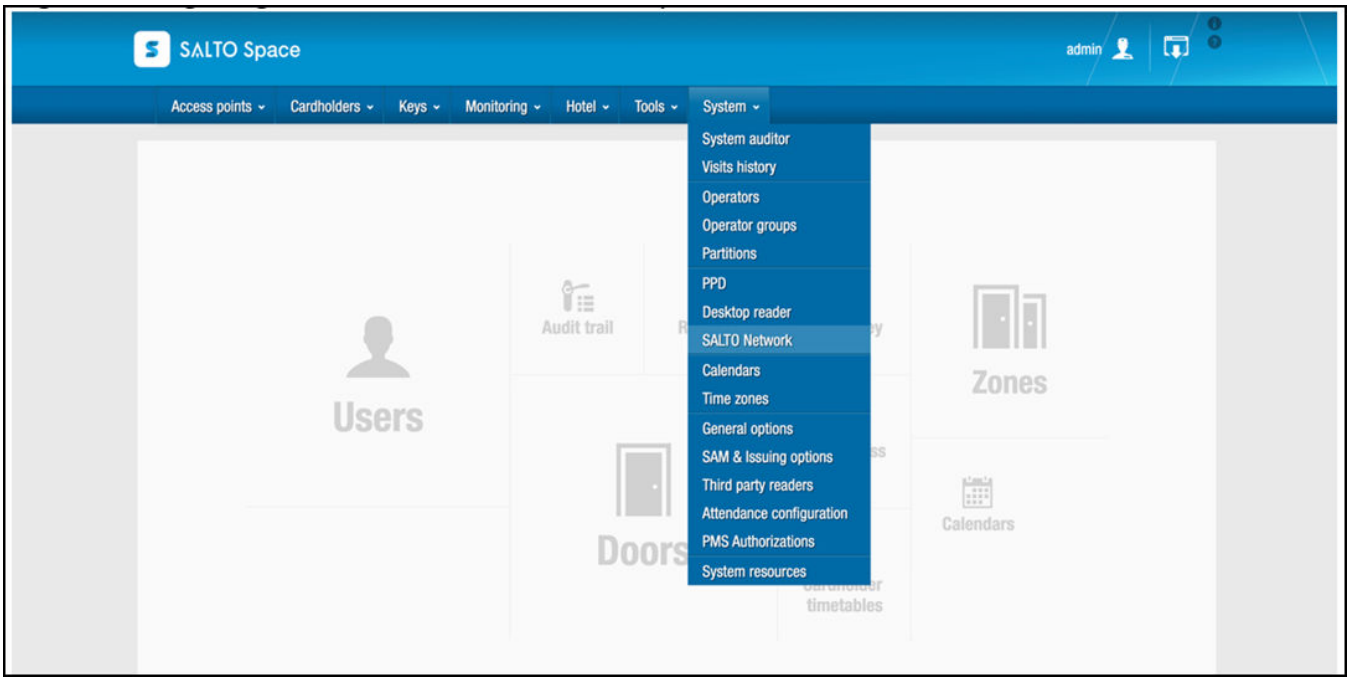
SALTO Space is an on-premise management platform that allows you to manage RUCKUS IoT controller, IoT gateways and SALTO locks. Generating the Secret Key and Initialization of the Secret Key are the crucial steps in authentication of the RUCKUS IoT Controller in the SALTO Space network.

Following are the steps to generate the Secret Key and Initializing the key.

1. Log in to the SALTO Space with valid credentials. Click **Enter**.

   The **SALTO Space** page is displayed.

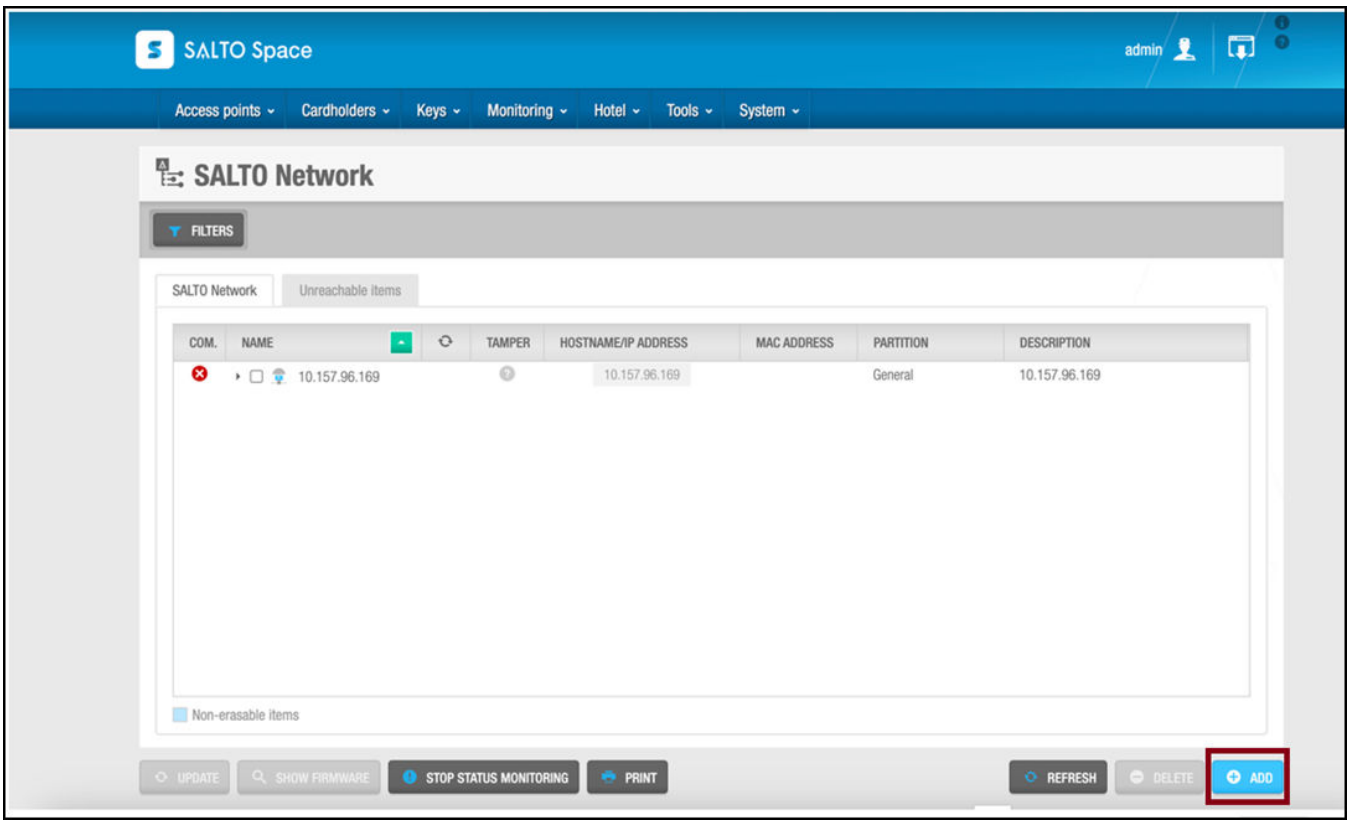
   FIGURE 72 SALTO Space Dashboard



2. On the menu, click **System** and select **SALTO Network** from the list.

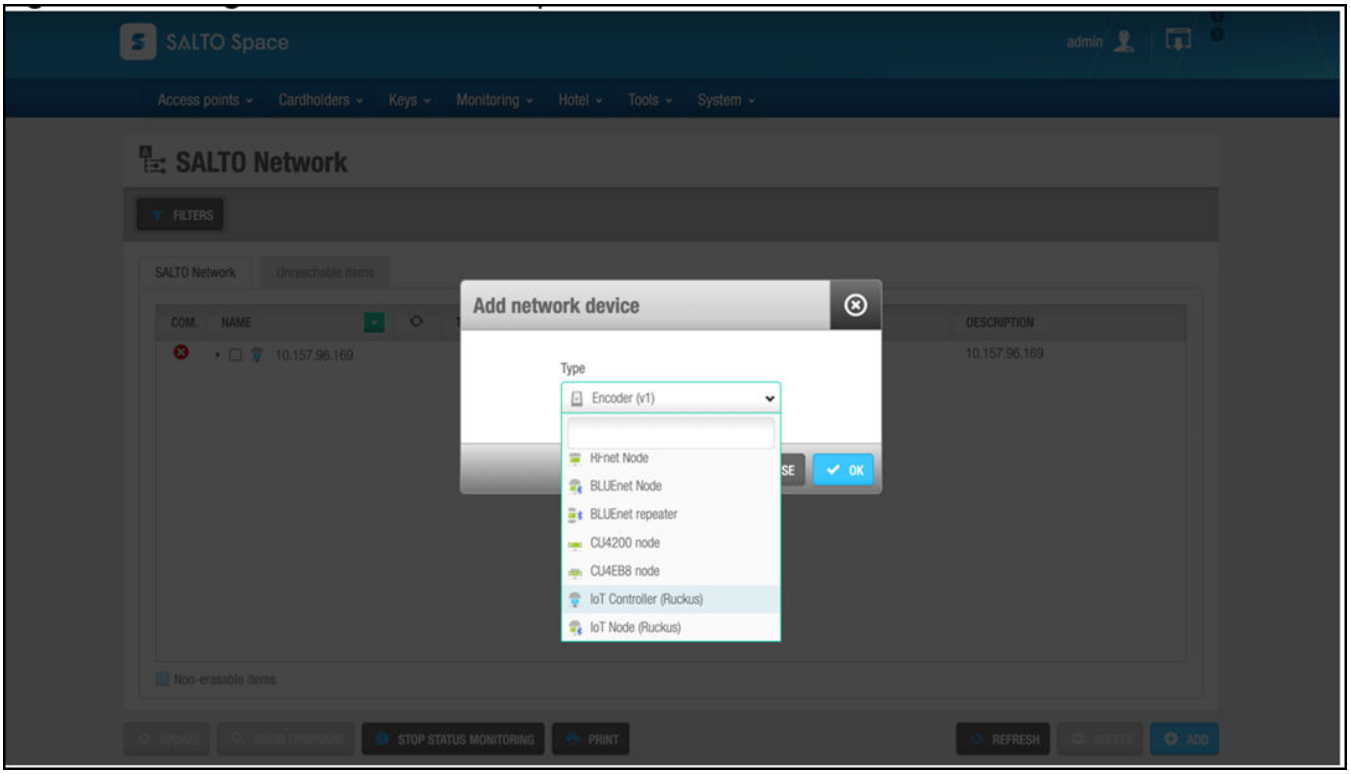
   The **SALTO Network** page is displayed.

   FIGURE 73 SALTO Network Page



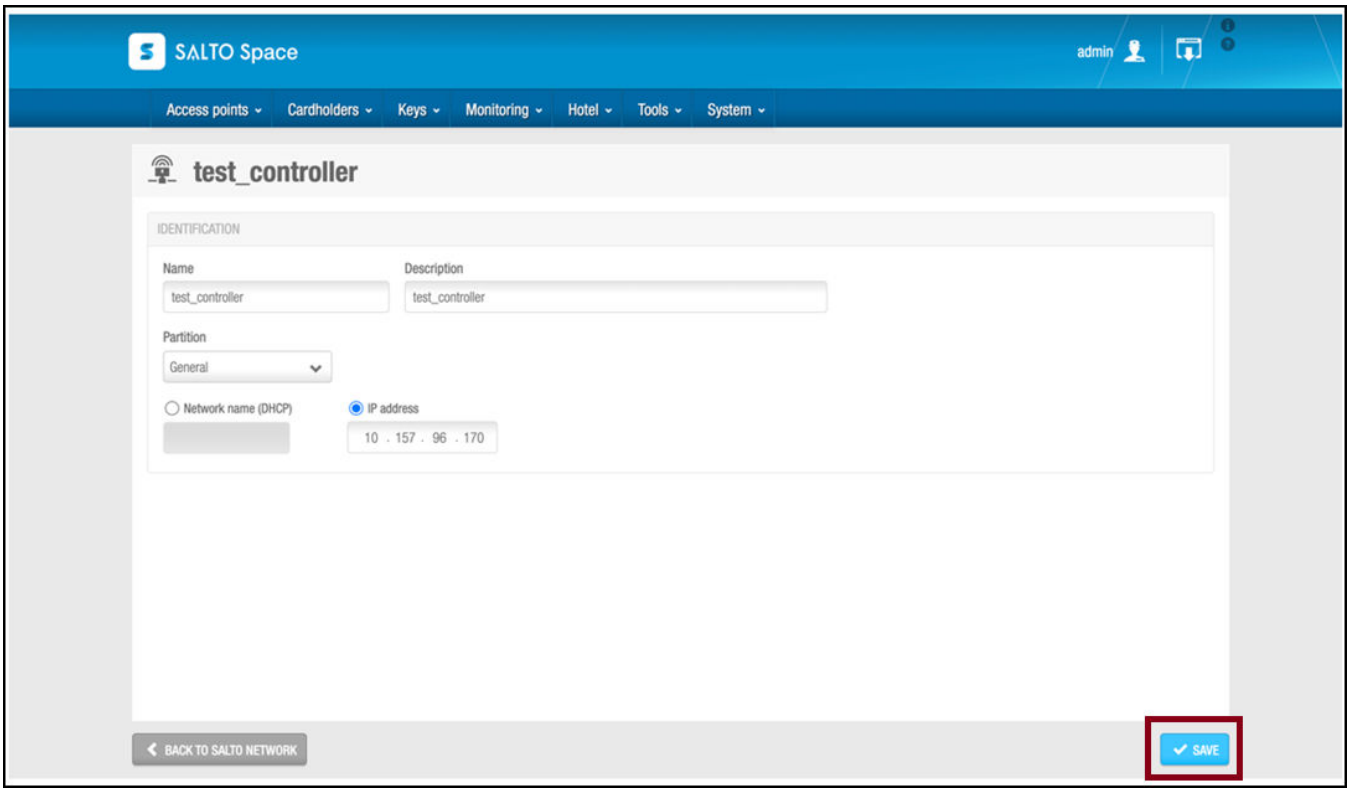
3. Click **ADD**. The **Add network device** pop-up page is displayed. Select the **IoT Controller (Ruckus)** from the **Type** list and click **OK**. The **IDENTIFICATION** page is displayed.

FIGURE 74 Selecting the IoT Controller from the list



4. Configure the following parameters on the **IoT Controller (Ruckus)** page.
   a) **Name**: Enter the name for the controller.
   b) **Description**: Enter the description for the controller.
   c) **Partition**: Select **General** from the list. By defalut the Partition selected is **General**.
   d) **IP address**: Enter the RUCKUS IoT Controller IP address.

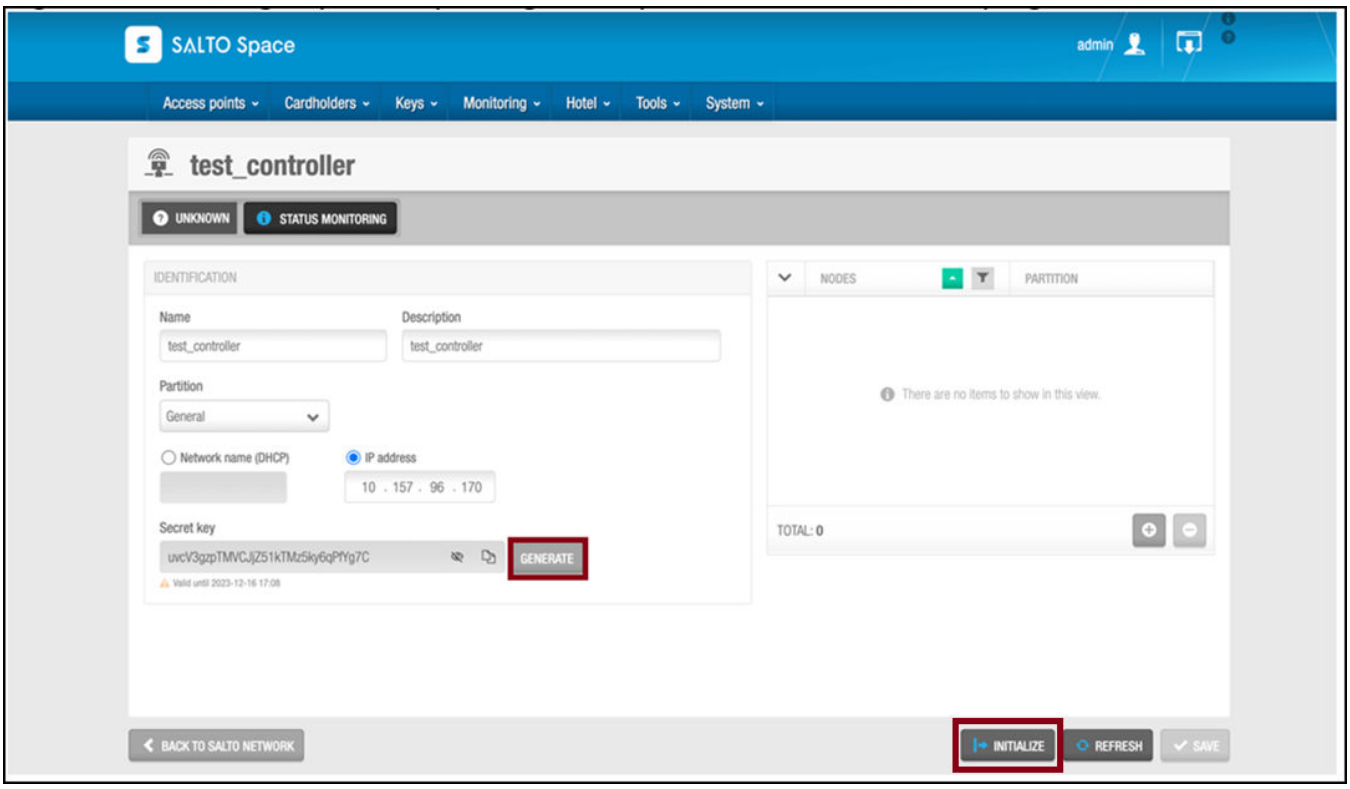
FIGURE 75 Configuring the IoT Controller Parameters



5. Click **Save** to save the RUCKUS IoT Controller information.

   The **IDENTIFICATION** page is displayed

   FIGURE 76 Clicking Generate and Initialize buttons



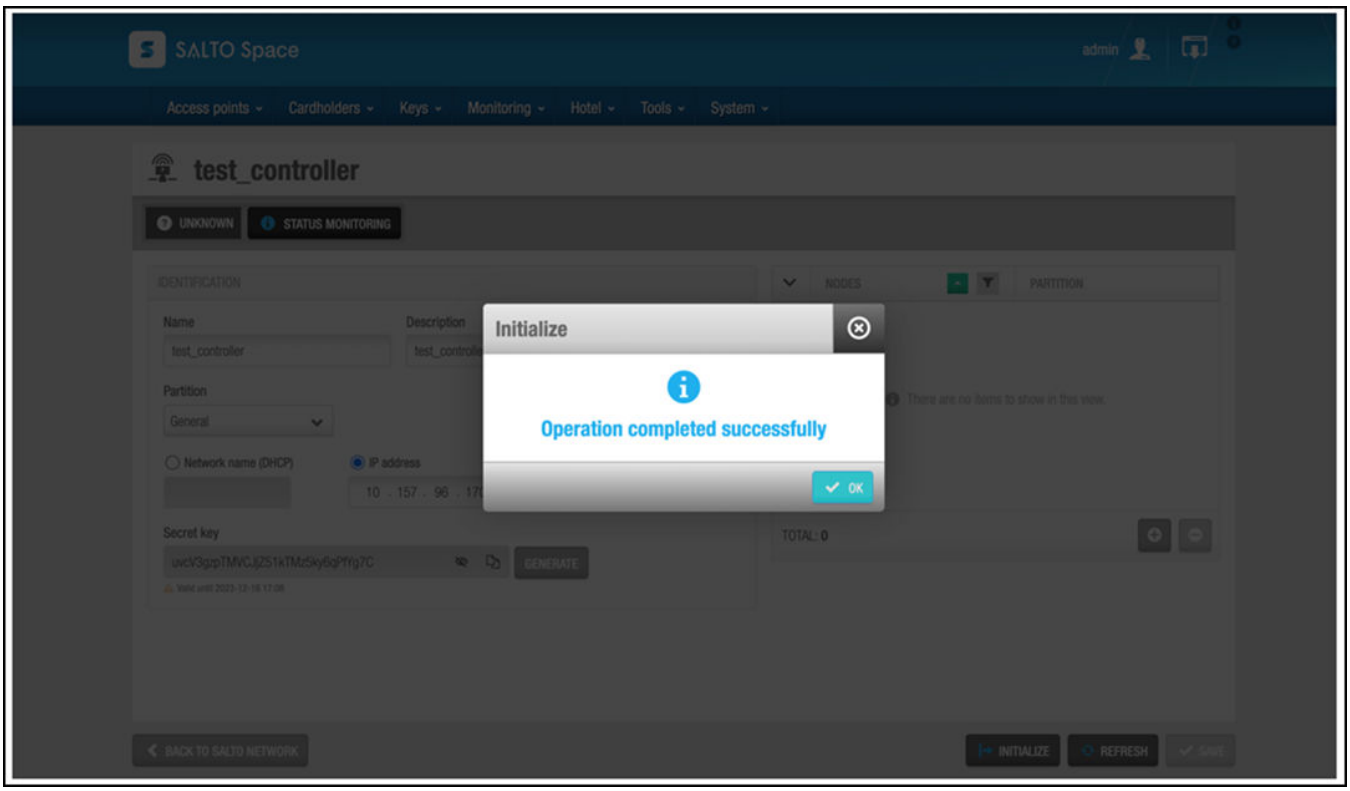
6. Click **Generate** to generate the Secret key. Click the **Copy** icon to copy the Secret Key.

   NOTE
   The Secret key is used for activating the SALTO plugin.

7. Click **Initialize** to initialize the Secret key.

   The **IoT Controller (Ruckus)** is successfully connected with SALTO Space network.

   FIGURE 77 Successful Completion



Changing the Password

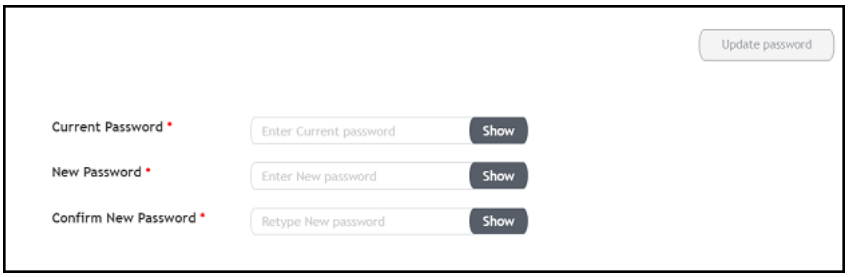
A single administrator is responsible for creating a RUCKUS IoT Controller account. This administrator manages system operations.

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 78 Changing the Password



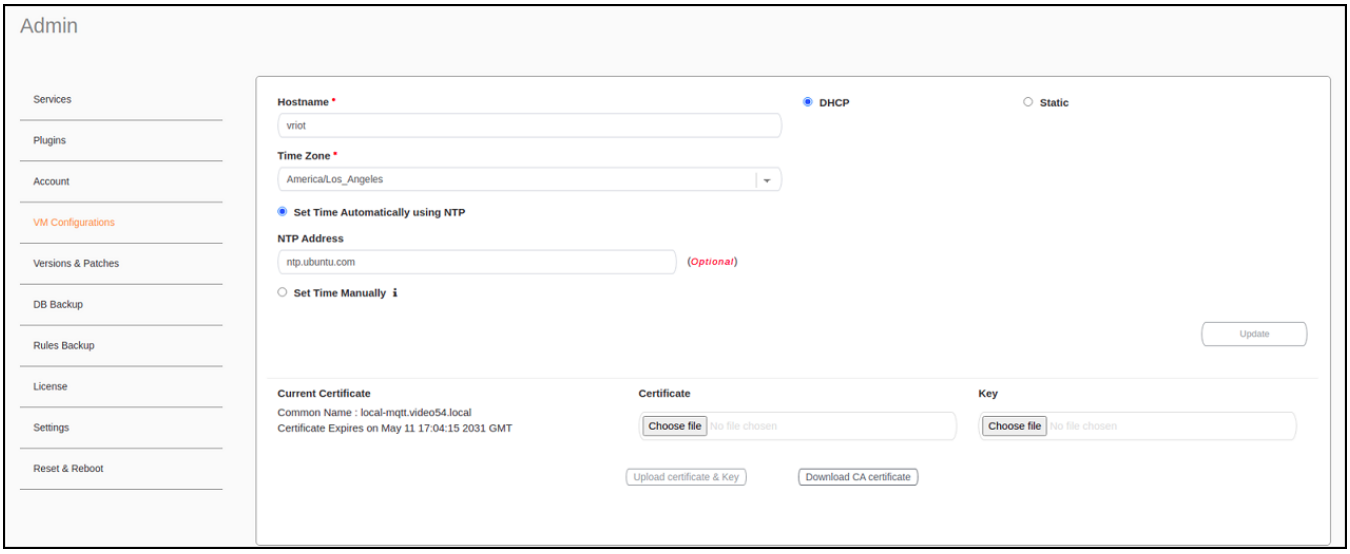
3. Change the password and click **Update password**.

Configuring Virtual Machines

Complete the following steps to configure a virtual machine (VM).

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

FIGURE 79 Configuring a Virtual Machine



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

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

4. Click **Update**.

Uploading Versions and Patches

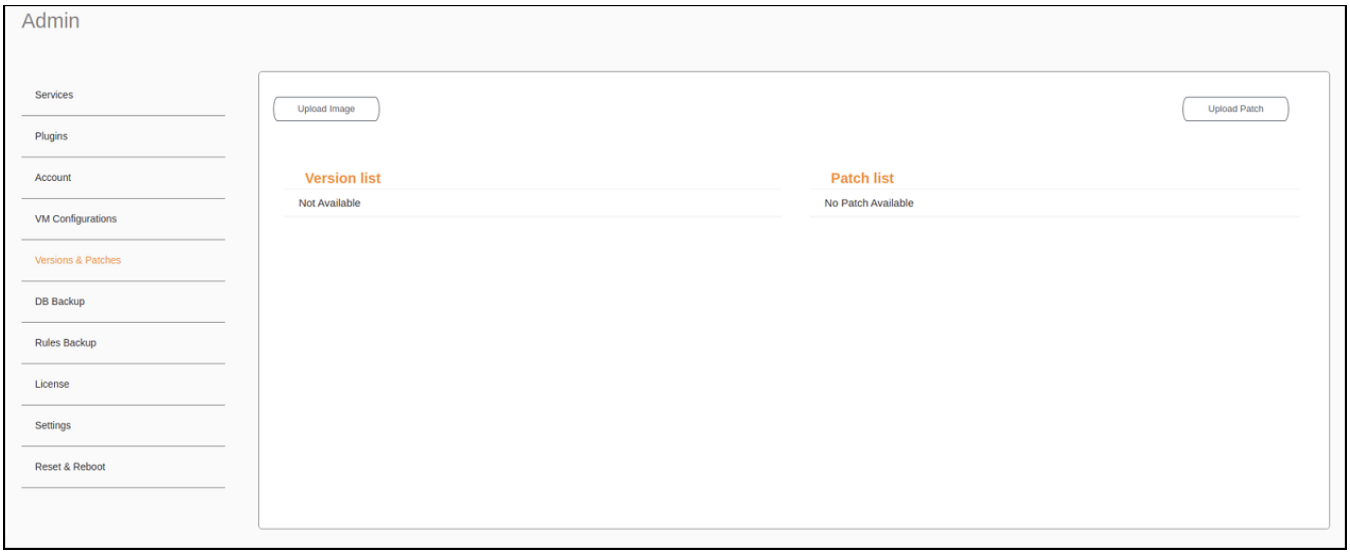
RUCKUS frequently releases updates to RUCKUS IoT Controller. The administrator normally receives any updates about new and updated software by email.

Uploading an Image

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

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

FIGURE 80 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 81 Initating the Upgrade Process

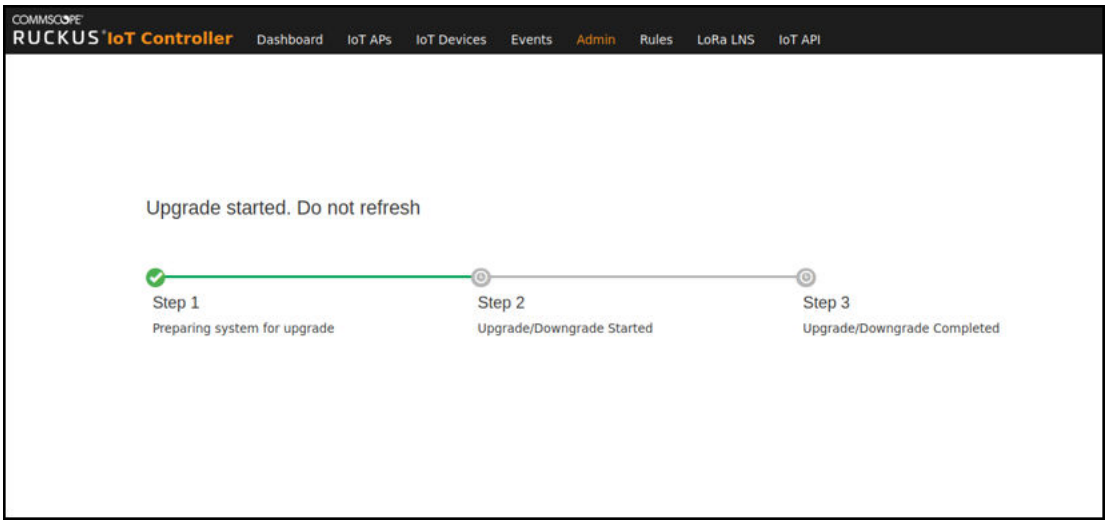
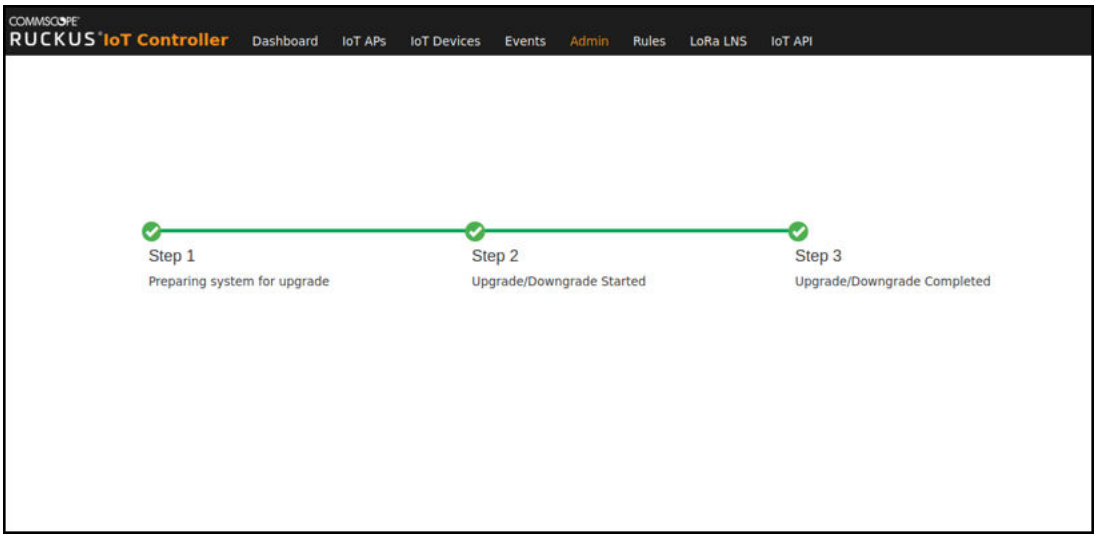


FIGURE 82 Completing the Upgrade Process



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 83 N+1 Upgrade Started

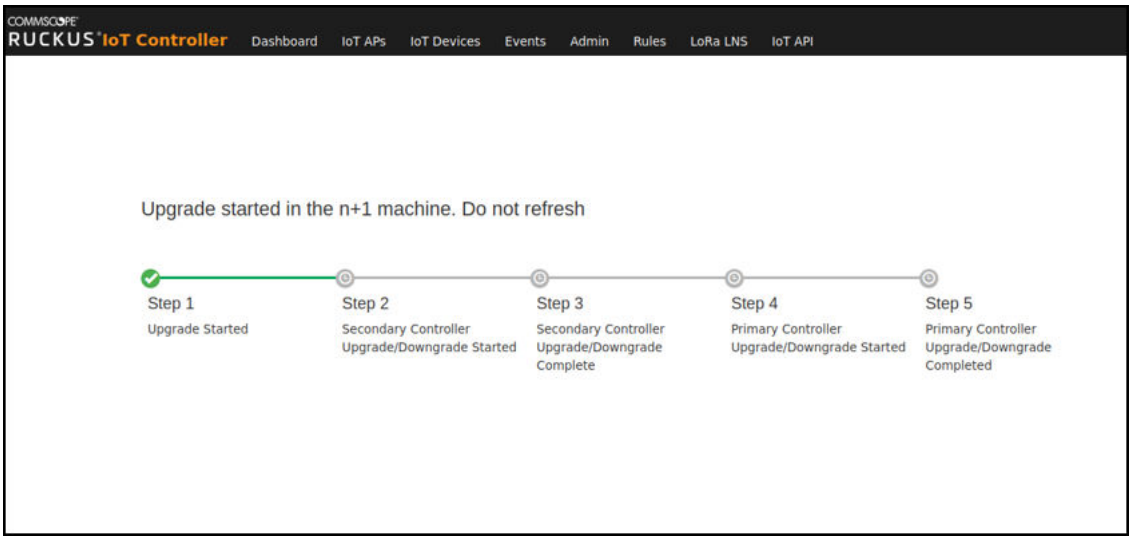
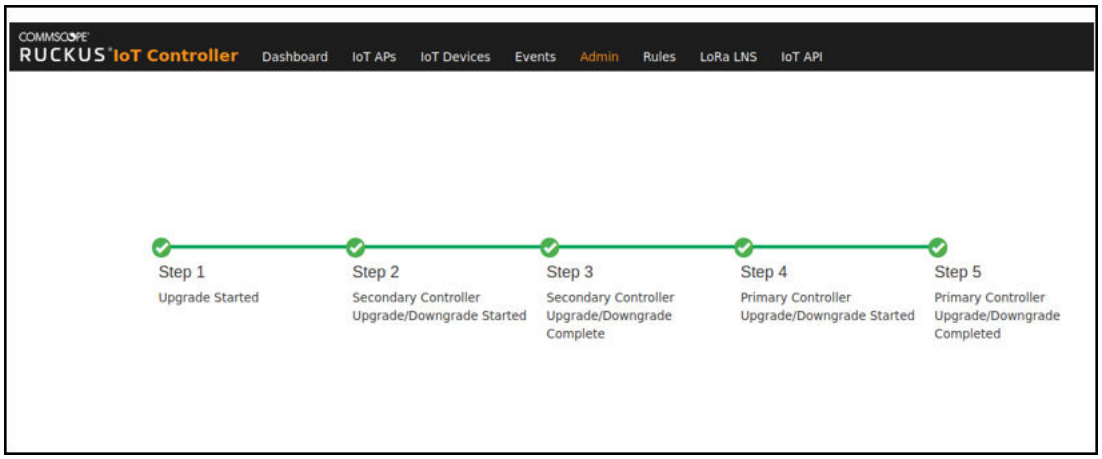


FIGURE 84 N+1 Upgrade Completed



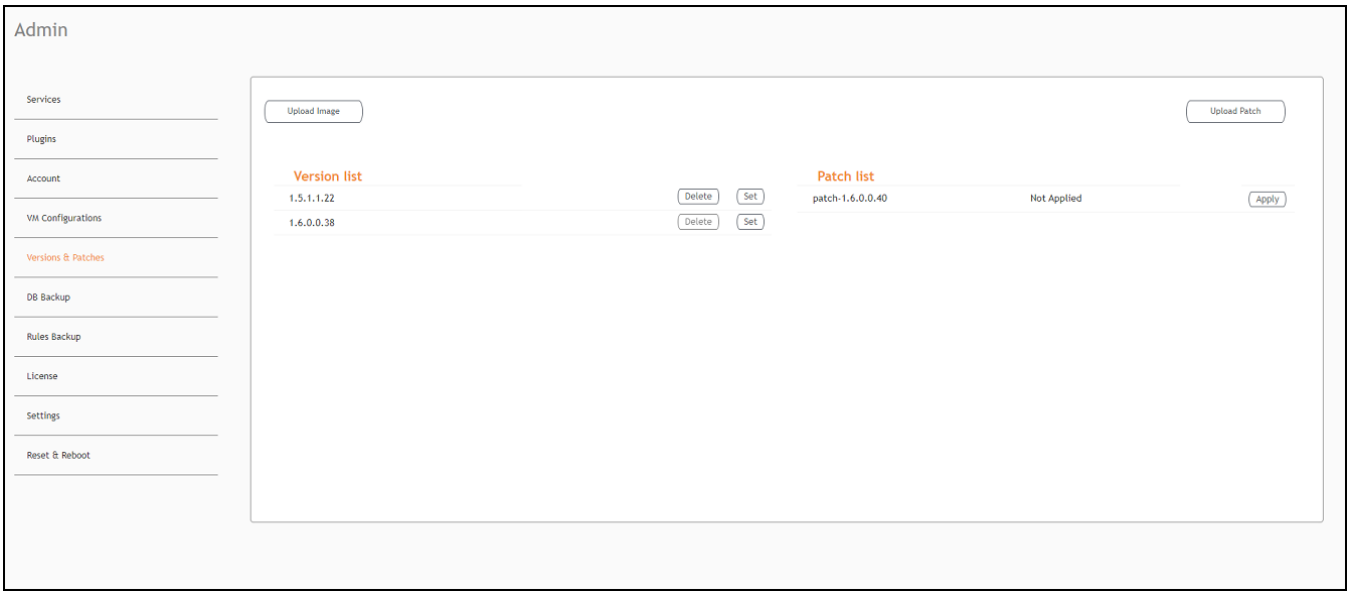
Uploading a Patch

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 85 Uploading a Patch



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

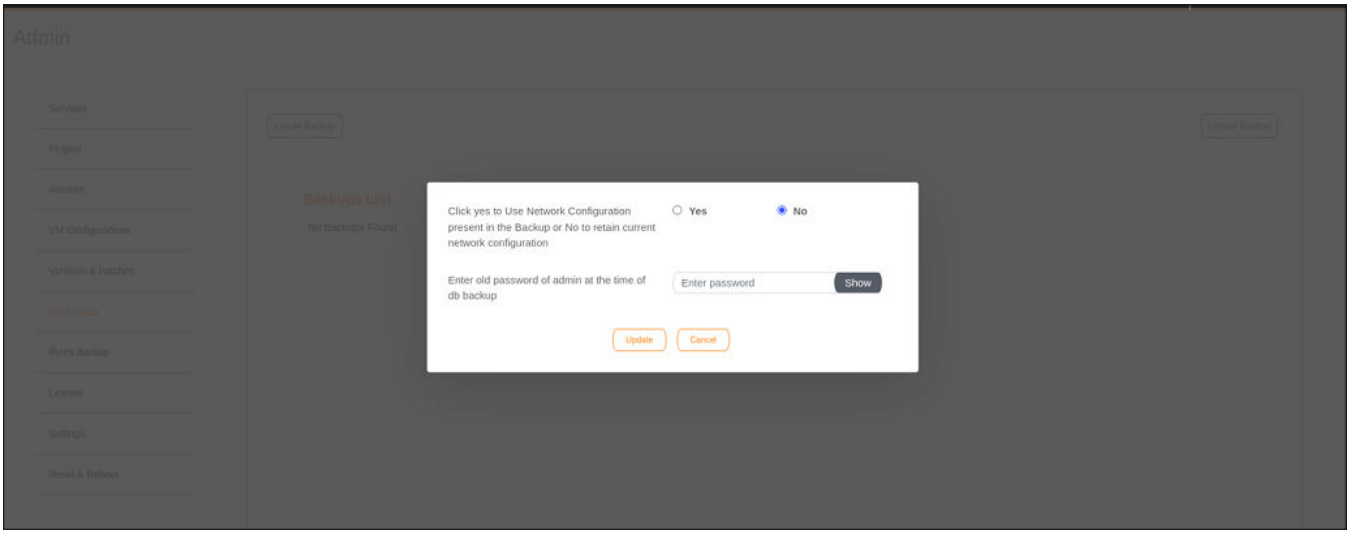
ATTENTION
You cannot revert a patch.

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 86 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 the below message , so you can select either static or dynamic network configuration present in the backup file.

```
Use Network Configuration Present in Backup
```

Uploading the RUCKUS IoT Controller License

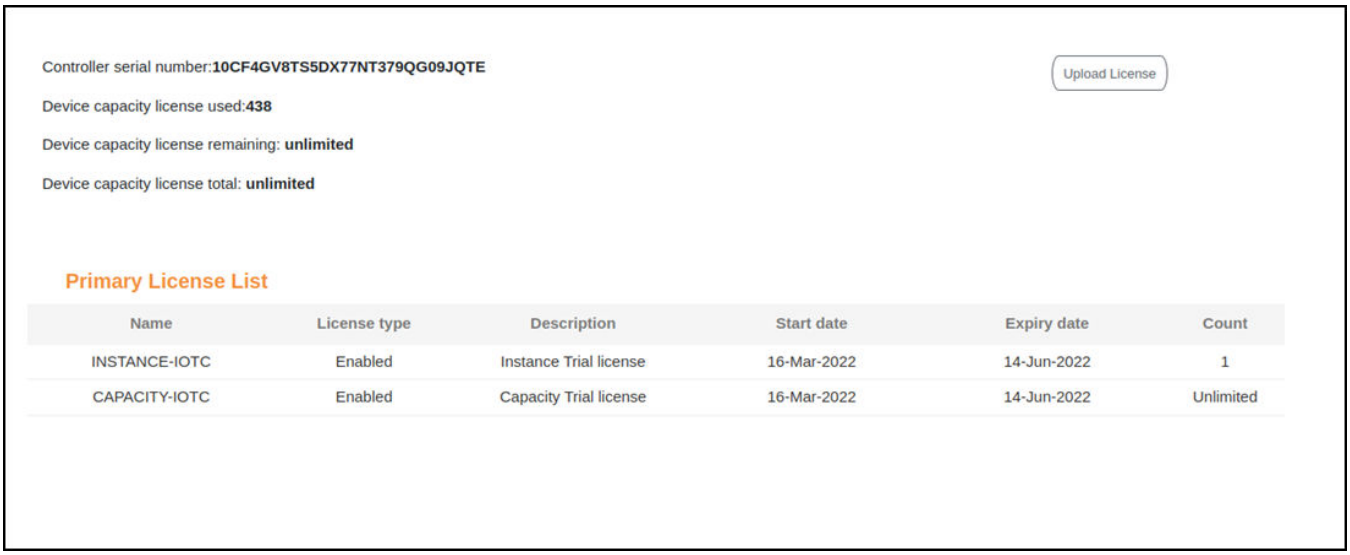
To obtain and activate the license, refer to "Activating a License" in the *RUCKUS IoT Controller Software Installation Guide*.

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

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

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

FIGURE 87 Uploading a License



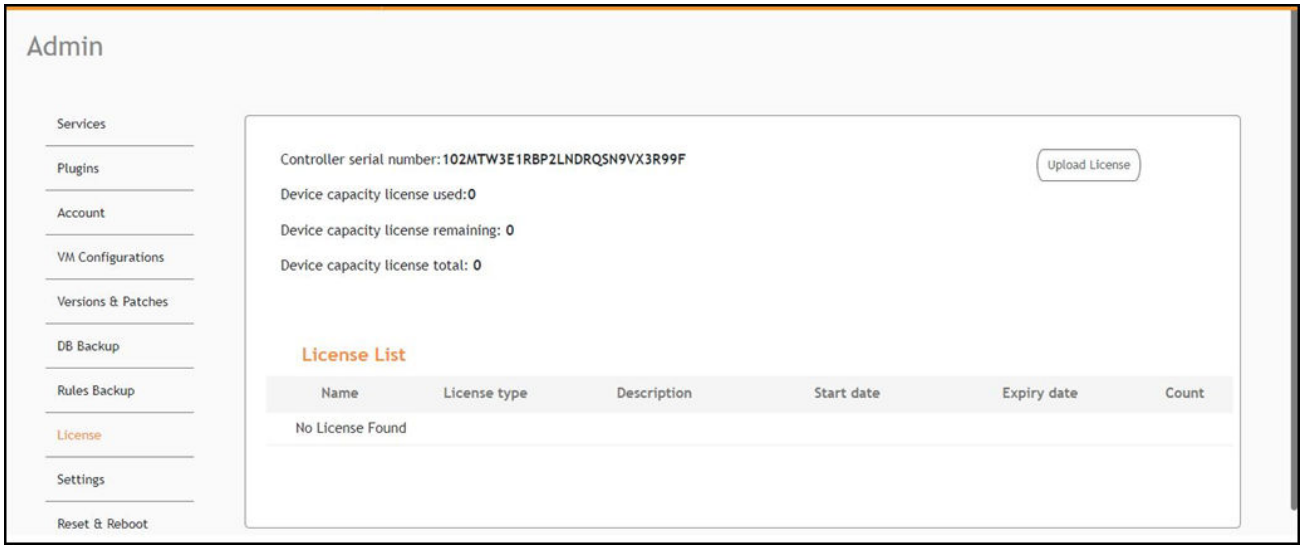
3. Click **Upload License** to upload the license. The License check-out means consuming a device capacity license, and License check-in means forfeiting a device capacity license. The License check-out happens when Device gets added. The License check-in happens when Device is deleted.

   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**.

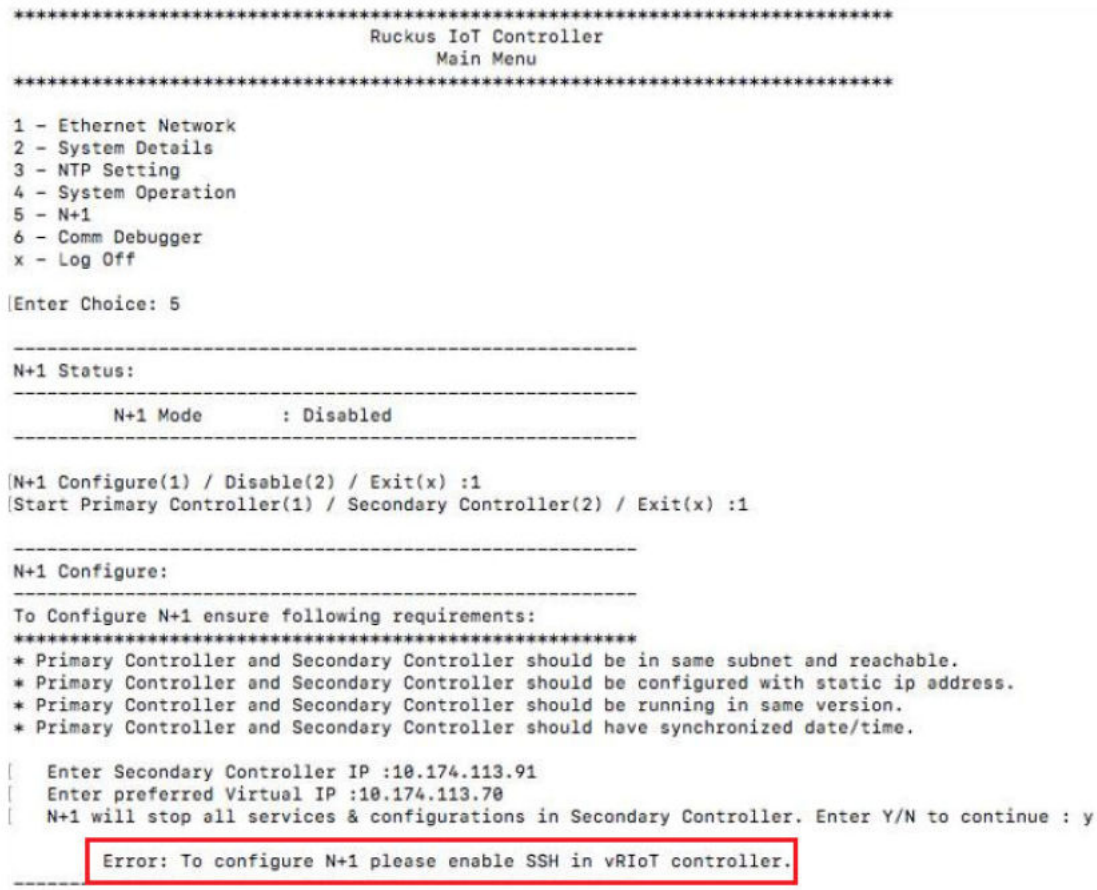
2. In the left navigation pane, click **Settings**.

FIGURE 88 Settings Page

3. Enable **SSH**.

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

   FIGURE 89 Showing Error on Disabling SSH



4. The **Log Level Settings** consists of the below list items. By deafault, select **INFO** and click **Apply**.
   - DEBUG - To debug a problem in IoT controller, relatively detailed tracing used by application developers for troubleshooting. Logs a message with level DEBUG on this logger.
   - INFO - Informational messages that might make sense to end users and system administrators and highlight the progress of the application. Logs a message with level INFO on this logger.
   - WARNING - Warning logs indicate that an unexpected event has occurred in an application that may disrupt or delay other processes. Logs a message with level WARNING on this logger.
   - ERROR - Error events of considerable importance that will prevent normal program execution but might still allow the application to continue running. Logs a message with level ERROR on this logger.

5. The **BLE Radio Scan Settings** consists of the **Scan Mode** and **Discovery Mode**. The BLE Scan mode allows gateways to actively search for and communicate with nearby BLE devices by querying them for Scan Response packets.The Discovery mode of gateways enables to scan for different types of beacons based on the discoverability settings.

   Discoverable - In this mode, gateways will only scan for beacons that have the discoverable field enabled. This means that only beacons explicitly configured to be discoverable will be detected during the scanning process.

   Not-Discoverable - In this mode, gateways will scan for all beacons regardless of their discoverability settings. This includes both beacons with the discoverable field enabled and those with it disabled.

   NOTE

   - By default, **Passive** and **Discoverable** modes are set.
   - You can configure the **Scan Mode** to operate in **Active** mode. In the Active mode, gateways send scan requests and expect a SCAN_RSP packet in response to each broadcasted packet.
   - The **Not-Discoverable** discovery mode is not supported in R730, R750, T750, R850, T750SE, R650 APs and the I100 IoT Module.

6. Click **Apply** to apply the settings.

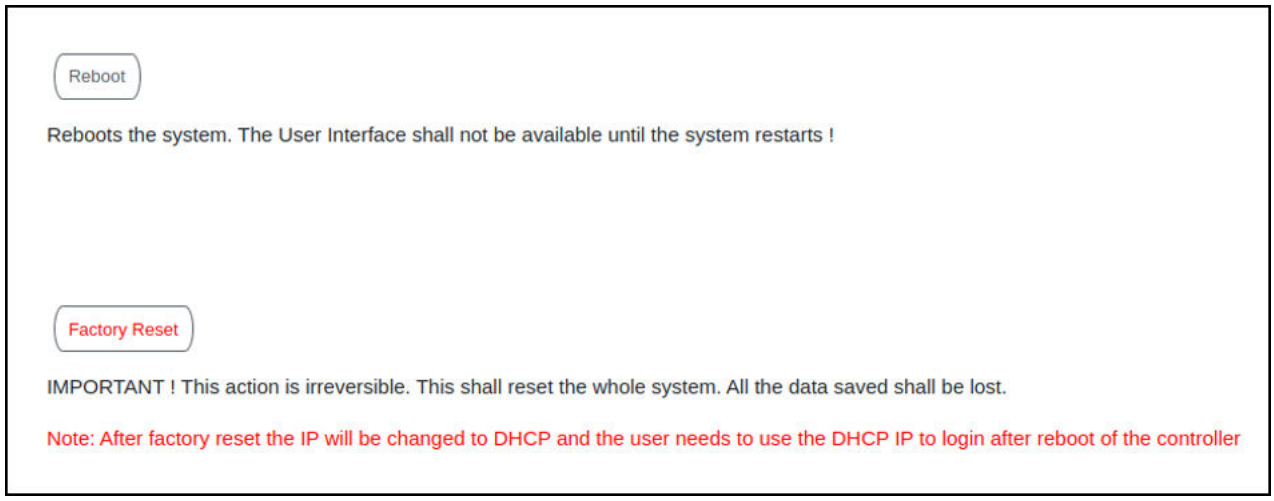
Rebooting RUCKUS IoT Controller

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 90 Rebooting RUCKUS IoT Controller



3. Click **Reboot**.

Resetting RUCKUS IoT Controller

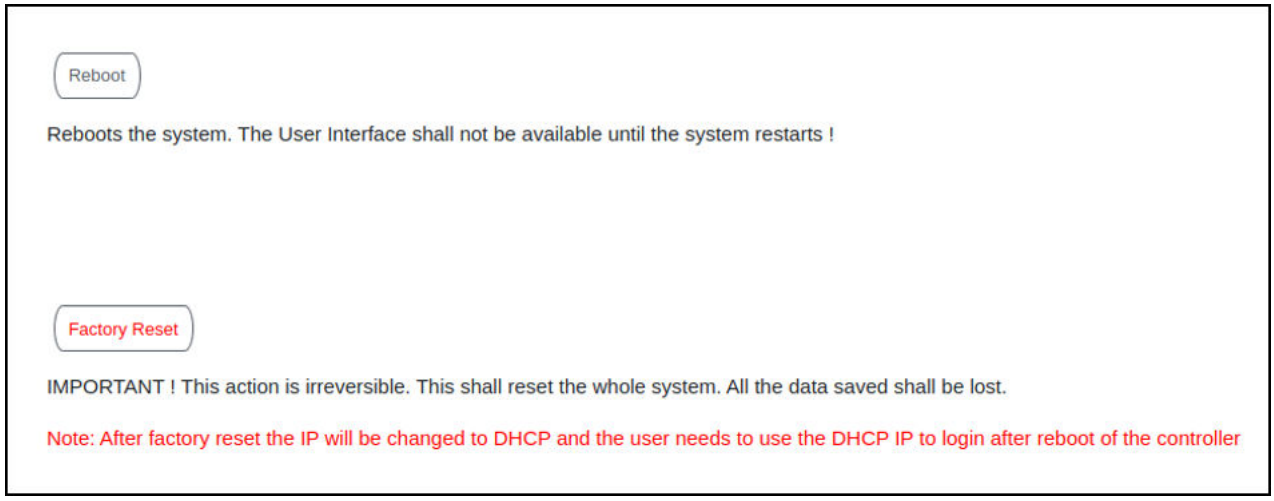
To remove all of the settings that are configured on the RUCKUS IoT Controller, reset it to the factory default settings.

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 91 Resetting RUCKUS IoT Controller



3. Click **Factory Reset**.

Managing IoT Access Points

- IoT AP Overview 97
- Gateway Onboarding 99
- Adding an IoT AP 101
- Editing an IoT AP 103
- Adding Tags to an AP 105
- Approval of IoT APs 107
- Exporting IoT APs to CSV 107

IoT AP Overview

SmartZone (SZ) holds the IoT AP firmware. You must make sure the IoT Access Point (AP) connects to SZ and downloads the appropriate IoT firmware. An IoT AP discovers SZ using discovery methods such as DHCP Option 43, Domain Name System (DNS), and Access Point Registry (APR) modes.

The RUCKUS IoT Controller displays the IoT AP hierarchy (Domain, Zone, Group) information, which is derived from the IoT AP and SmartZone connection. Therefore, it is important to ensure that the IoT AP is running the latest appropriate IoT firmware.

An IoT Access Point discovers the RUCKUS IoT Controller by using Option 43 or the RUCKUS Command Line Interface (RKSCLI). RKSCLI mode is not encouraged, and must be used only if a DHCP server is not present.

DHCP Option 43

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

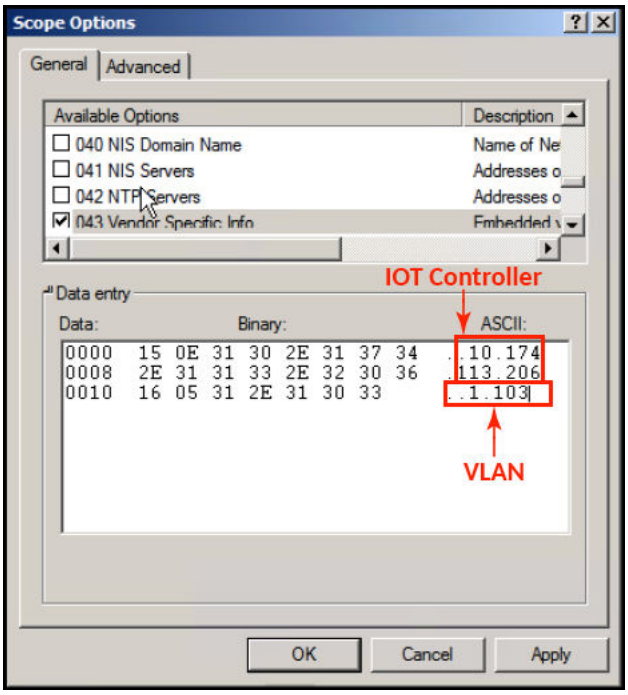
- Suboption 21: Used to configure a RUCKUS IoT Controller IPv4 address or FQDN (mandatory)
- Suboption 22: Used to set the control VLAN for IoT Control/Data traffic (optional)

Option 43 supports both binary and ASCII formats. The IoT Access Point bootup process checks for Option 43 and suboptions 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.

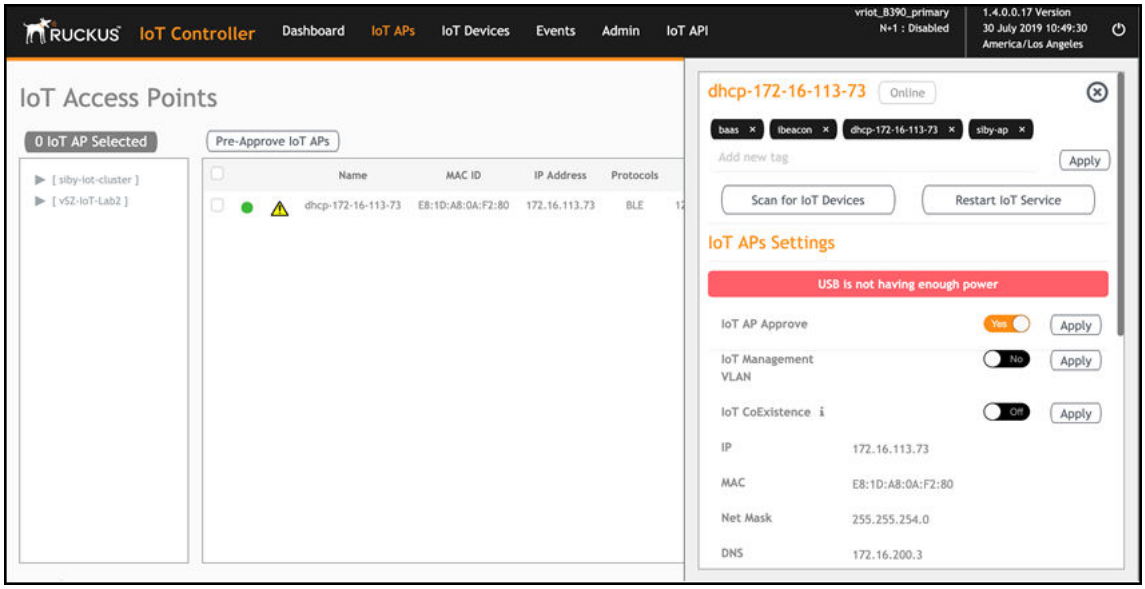
RUCKUS Command Line Interface

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

USB Power

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

FIGURE 92 Displaying a Shortage of USB Power



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

Gateway Onboarding

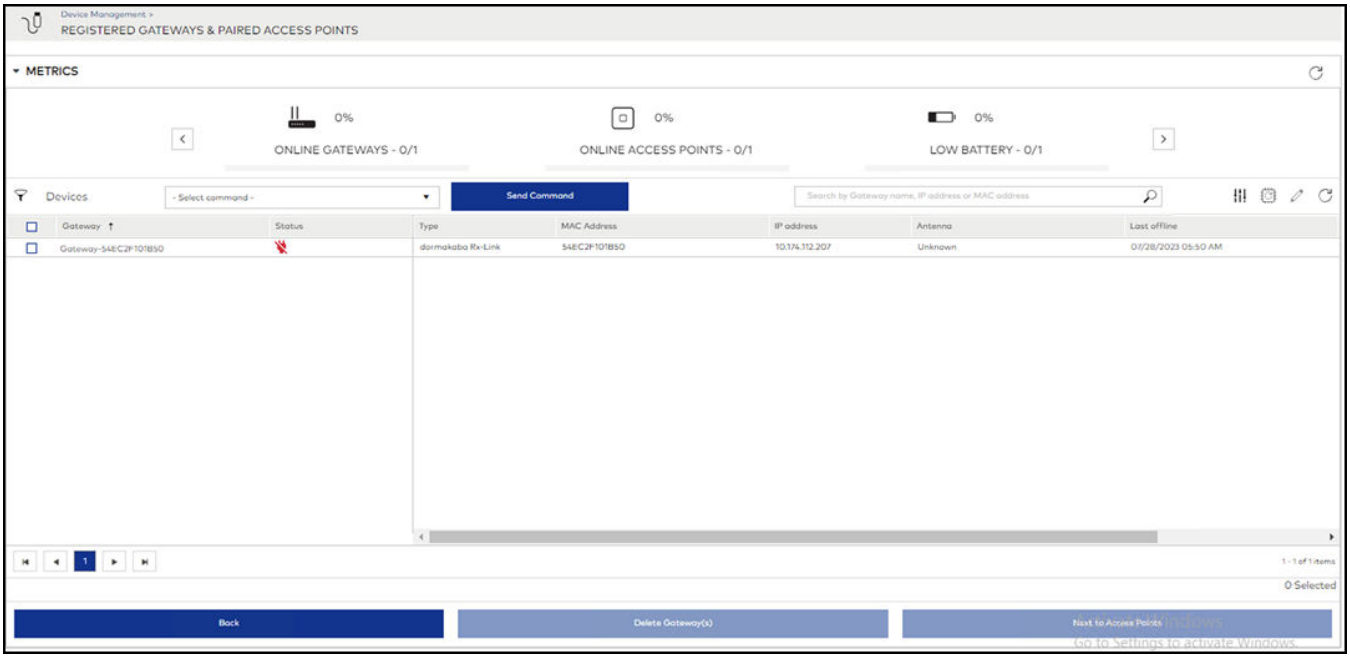
Gateway Onbarding can done by performing following steps.

1. Log into AP console and set IoT Controller using the command **set iotg-mqtt-brokerip <iot controller ip address>**
2. Approve the AP
3. Configure ZigBee(DK) mode by performing below substeps.
   a) Click AP, w window will open.
   b) Select the radio that need to configure mode.
   c) For mode, from drop down list, select “ZigBee(DK).
   d) Click **Apply**

   The ZigBee_DK protocol has been configured successfully.

4. After Configuring ZigBee_DK successfully, login to Ambiance Server and go to "**Device Management**", and click **Registered Gateways and Paired Access Points**.

FIGURE 93 Showing Registered Gateways and Paired Access Points



Adding an IoT AP

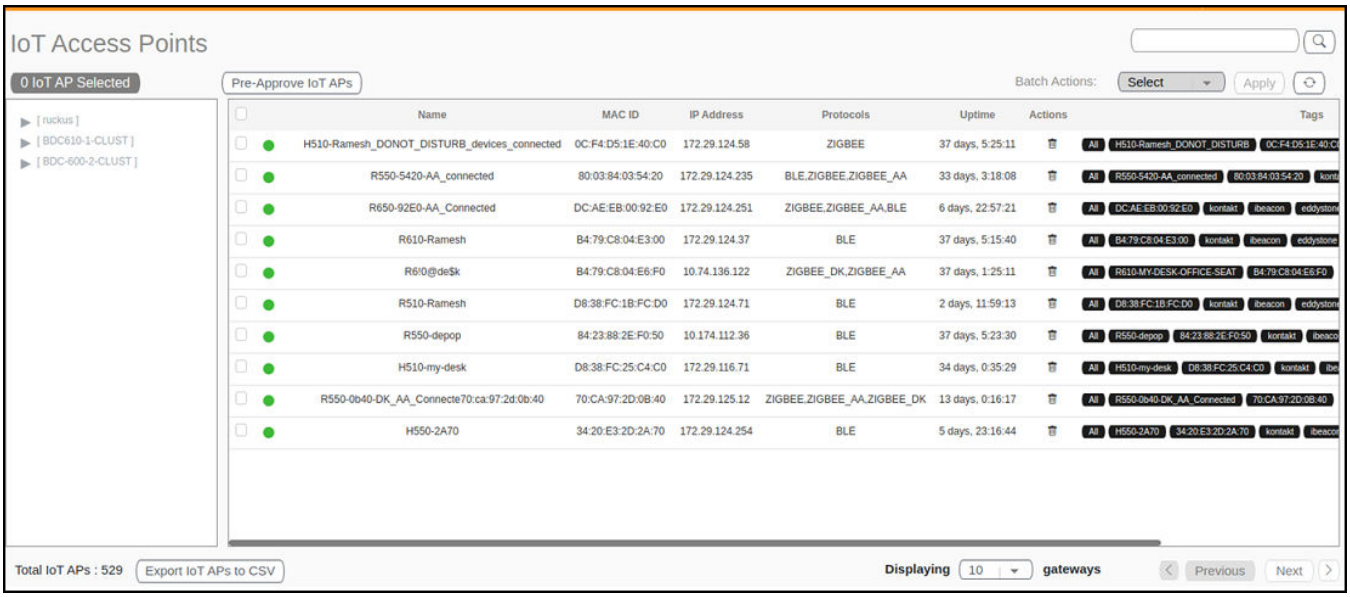
The administrator can add an IoT AP to the RUCKUS IoT Controller to manage IoT devices.

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 94 IoT Access Points Page

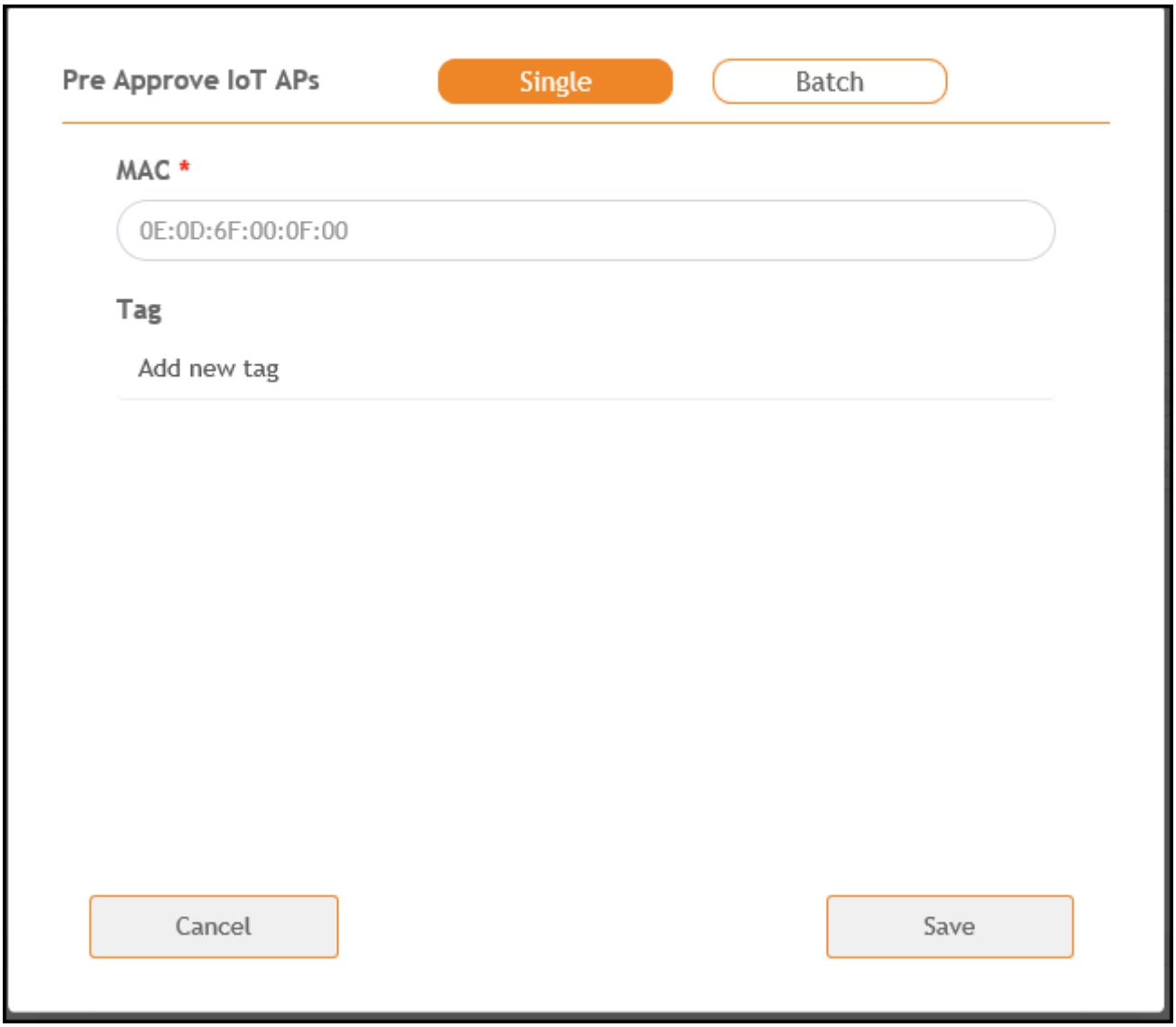


2. Click **Pre-Approve IoT APs**.

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

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

FIGURE 95 Adding a Single IoT AP

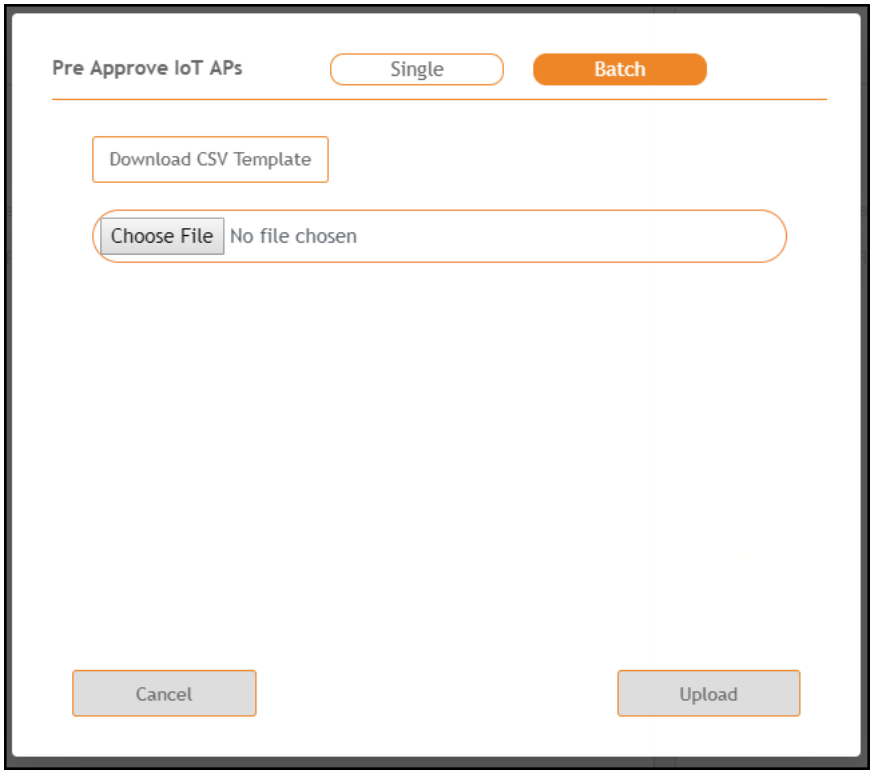


4. Enter the MAC address of the IoT AP and click **Save**.

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

   NOTE
   To add multiple IoT APs, click **Batch** and download the CSV template. Enter the required details in the CSV template and click **Upload**.

FIGURE 96 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.

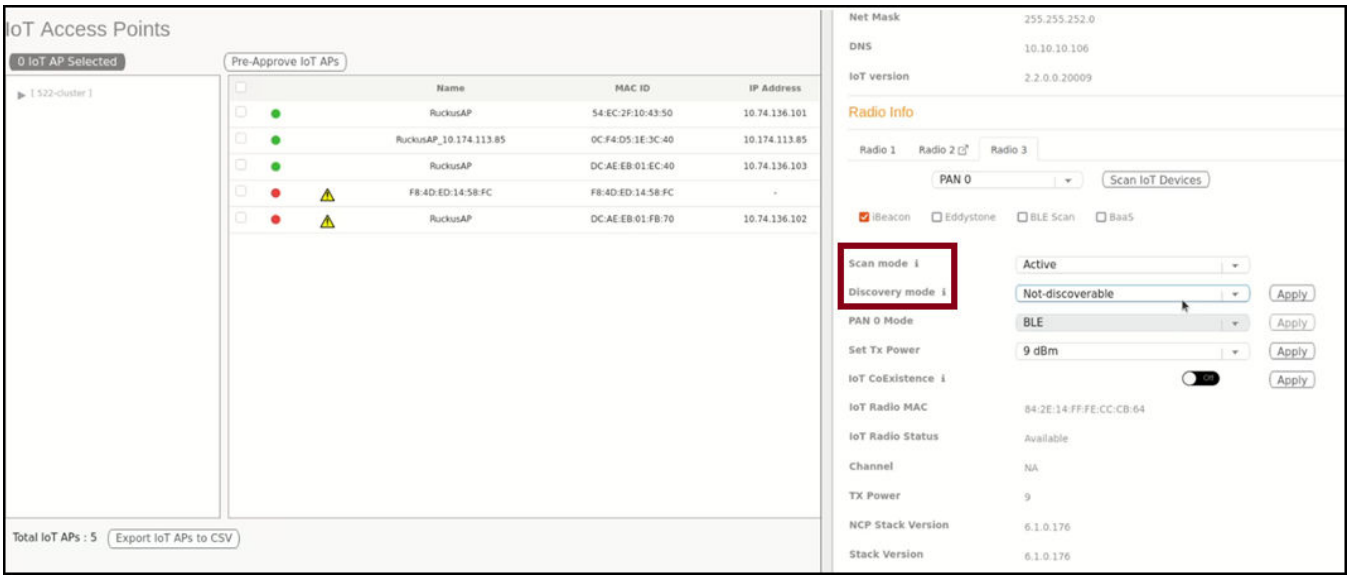
Complete the following steps to edit a single IoT AP.

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

   A list of selected IoT APs is displayed.

2. Click an IoT AP to edit.

FIGURE 97 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)
- **Scan mode**
- **Discovery mode**
- **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.

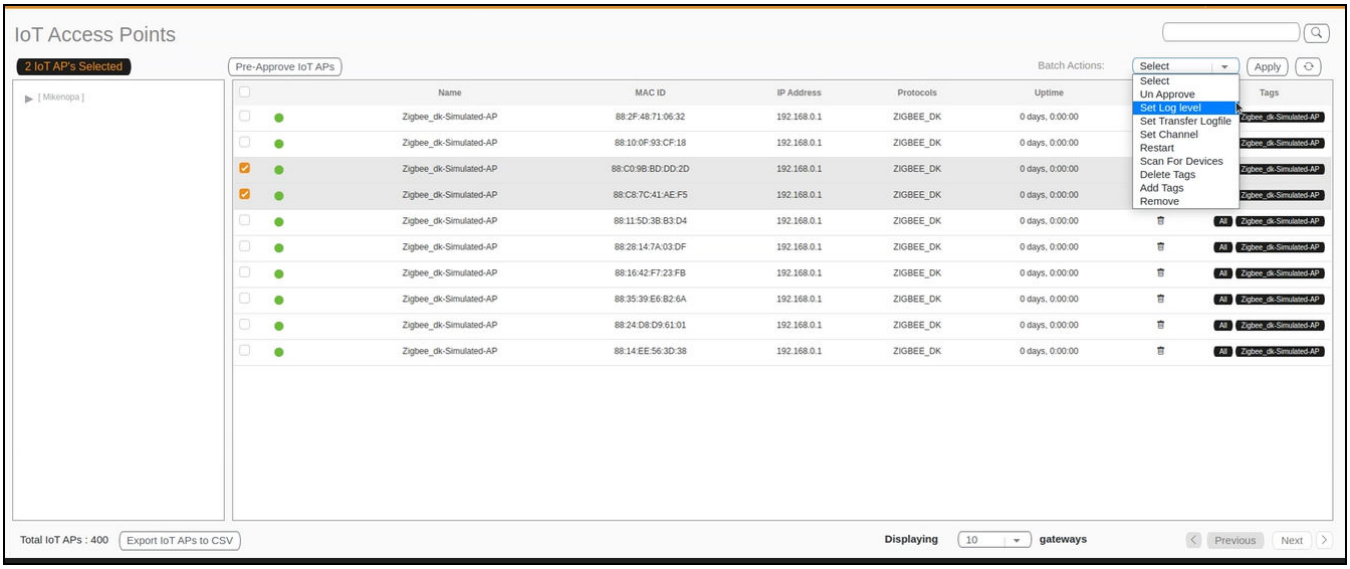
1. From the main menu, click **IoT APs**.

   A list of IoT APs is displayed.

2. Select an IoT AP. You can select single or multiple AP(s) and perform batch actions as below.

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

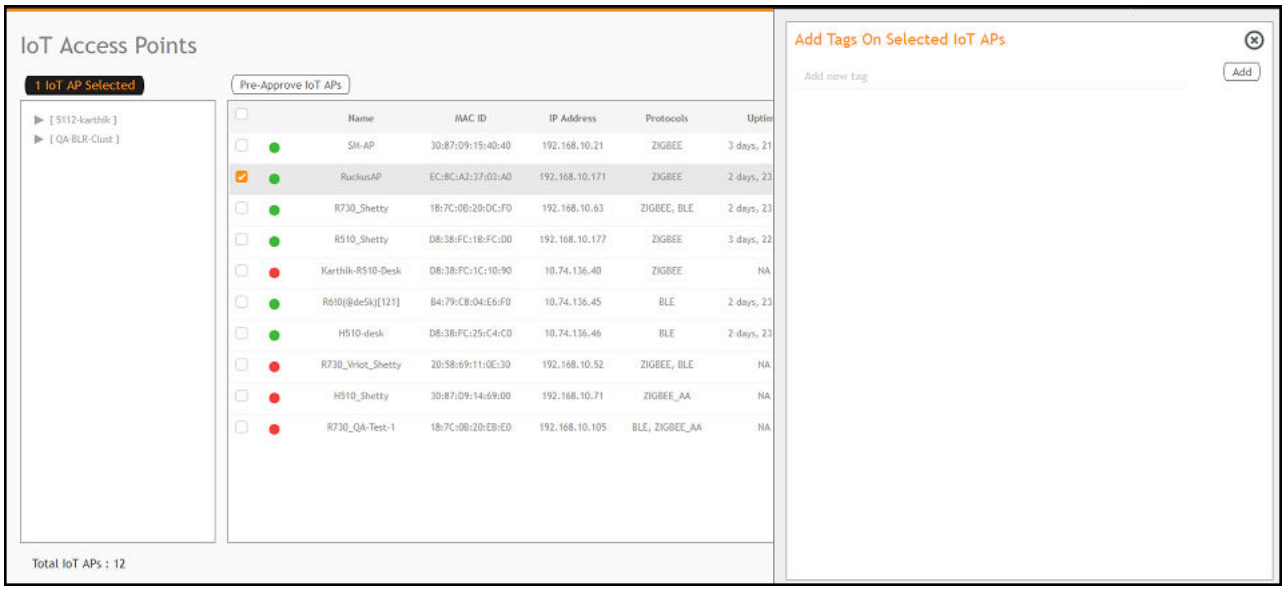
   FIGURE 98 Selecting an AP to Add Tags



3. The **Batch Actions** list contains the options listed below. Select **Add Tags** from the list.
   - Un Approve - To Unapprove the selected approved AP(s)
   - Set Log level - Setting log level for selected AP(s)
   - Set Transfer Logfile - Enable or Disable AP logs transfer from AP to controller for selected AP(s)
   - Restart - Restart selected AP(s)
   - Scan For Devices - Scan for selected AP(s)
   - Delete Tags - Delete Tags for selected AP(s)
   - Add Tags - Add Tags for selected AP(s)
   - Remove - Remove selected AP(s)
   - BaaS operations - Change BaaS operations for selected AP(s)

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

FIGURE 99 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 6 Plugins and Corresponding Tag Names

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

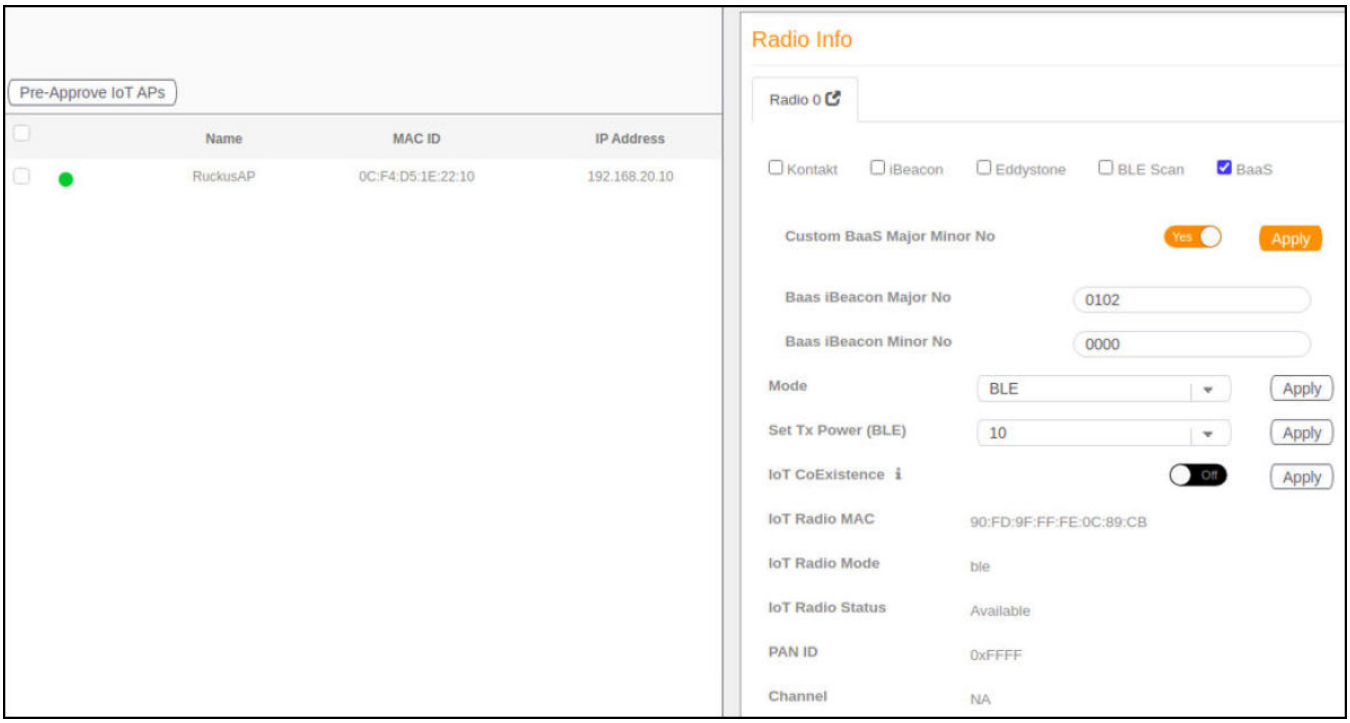
Complete the following steps to enable BaaS Major and Minor Number.

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.

   FIGURE 100 Enabling Baas Major and Minor number



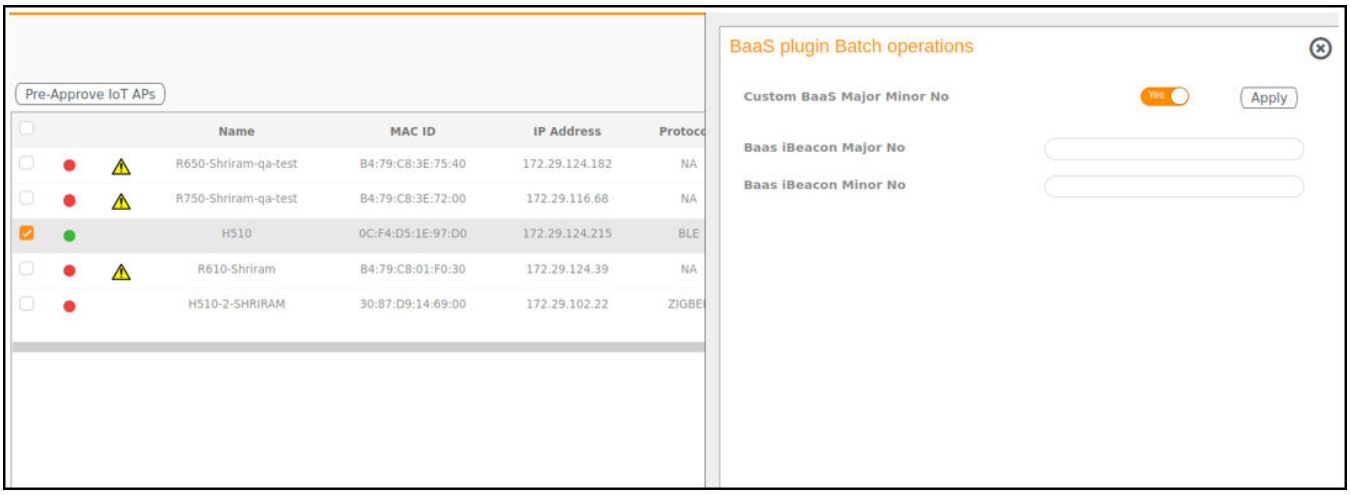
   NOTE
   You can update a single IoT AP.

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

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

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

FIGURE 101 Updating Baas Major and Minor Number for Multiple IoT APs



Managing Devices

- Devices Overview..... 111
- Managing OSRAM Light Bulbs..... 113
- Managing an Assa Abloy Lock..... 114
- Managing the Dormakaba Locks..... 116
- Device Operations for Specific Clusters and Commands..... 129

Devices Overview

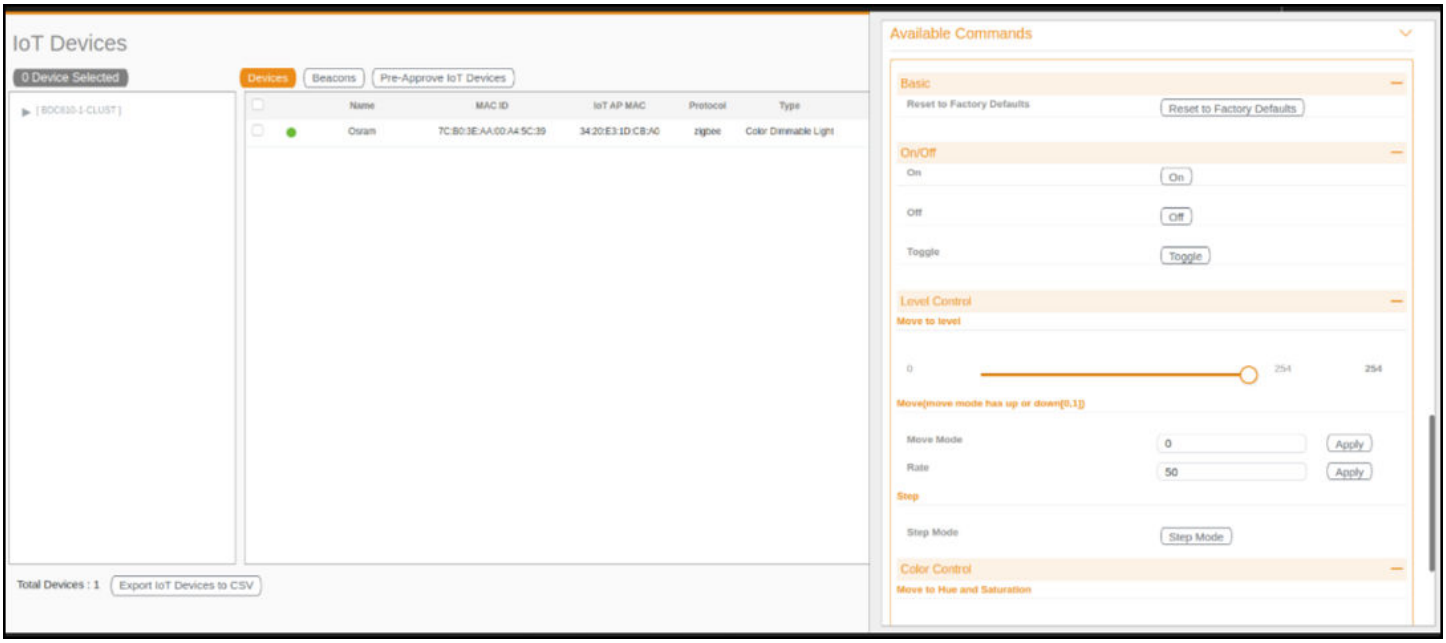
The RUCKUS IoT Controller requires explicit user approval of devices. Only an approved device can be allowed into the IoT infrastructure.

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 102 IoT Devices Page

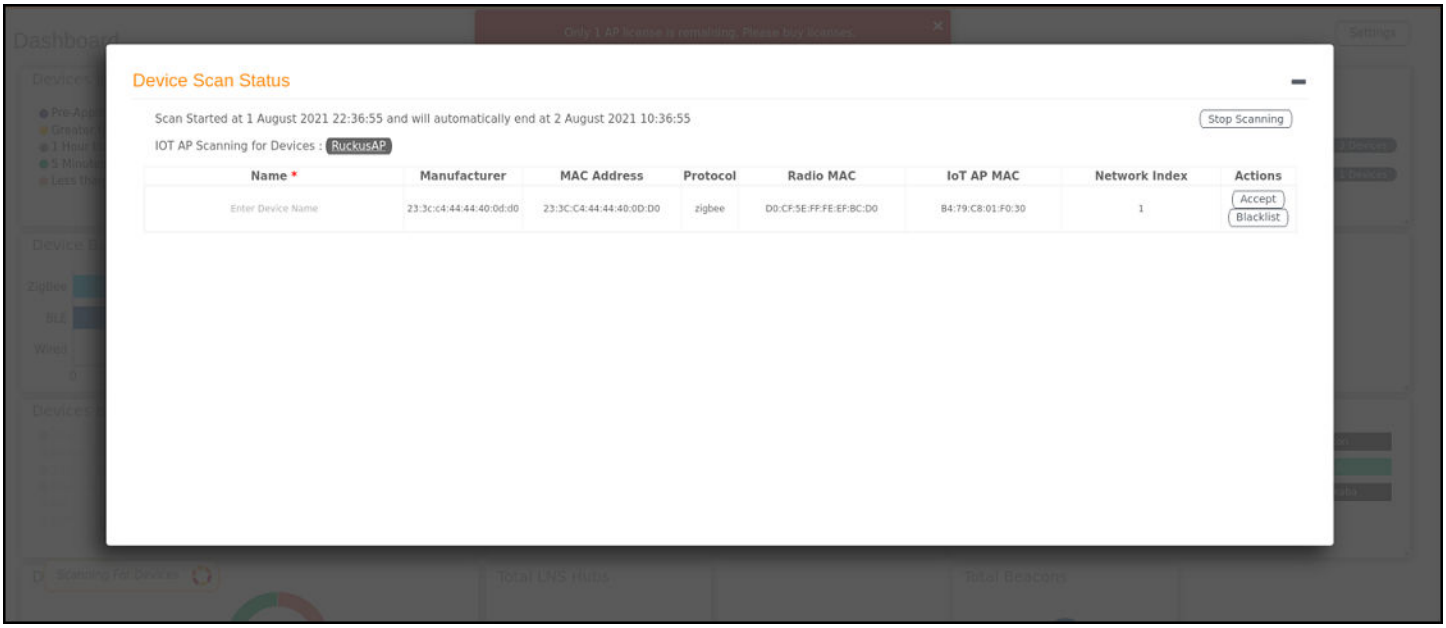


The device scan operation must be performed to start the device discovery process on the gateway.

> **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.

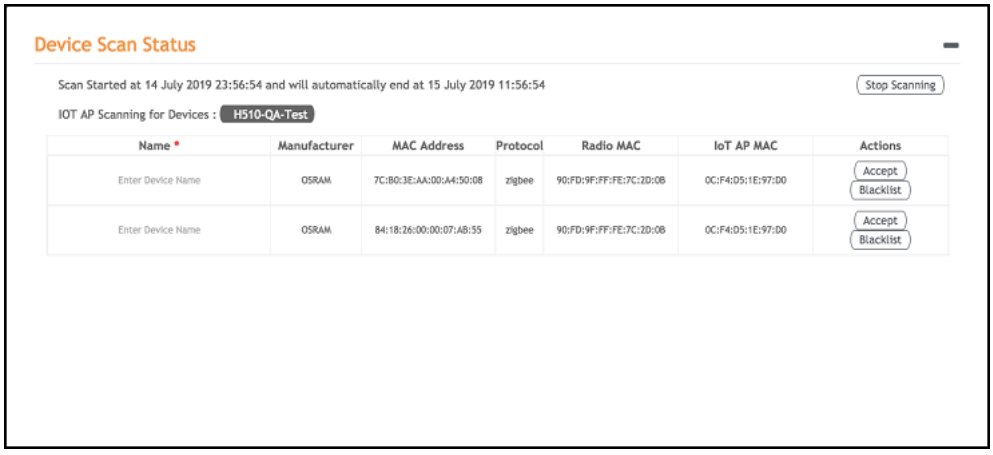
Upon starting device discovery, a dialog box is displayed, as shown in the following figure.

FIGURE 103 Device Discovery Dialog Box



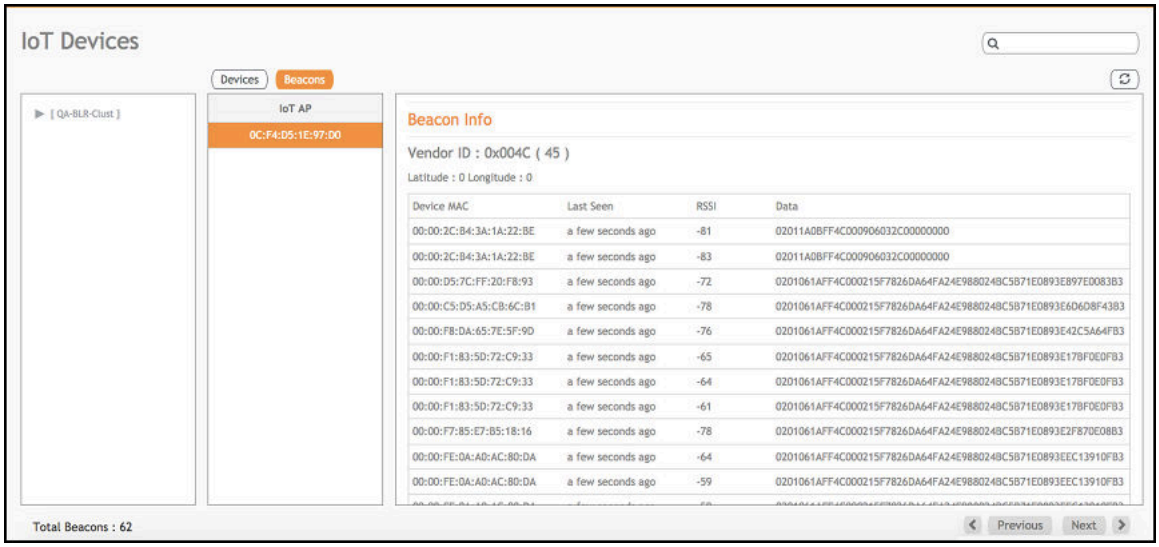
A device gets added to the RUCKUS IoT Controller through Discover IoT Devices operations. If a device is pre-approved, the discovered device automatically joins the list of discovered devices. If the discovered device is not pre-approved, then you must select **Accept** or **Blacklist**. If the device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

FIGURE 104 Adding Device After Discovery



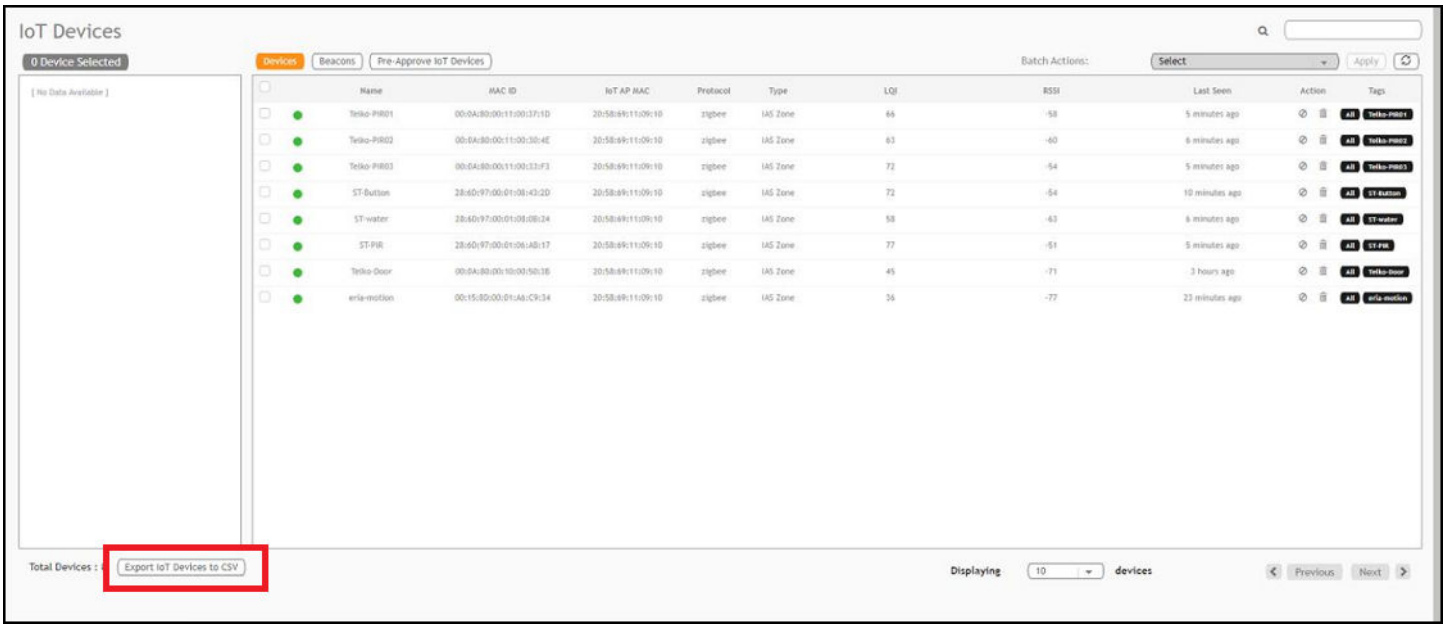
The **Beacons** page shows the list of beacons for the selected AP.

FIGURE 105 Beacons Page



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 106 Exporting IoT Devices to CSV



Managing OSRAM Light Bulbs

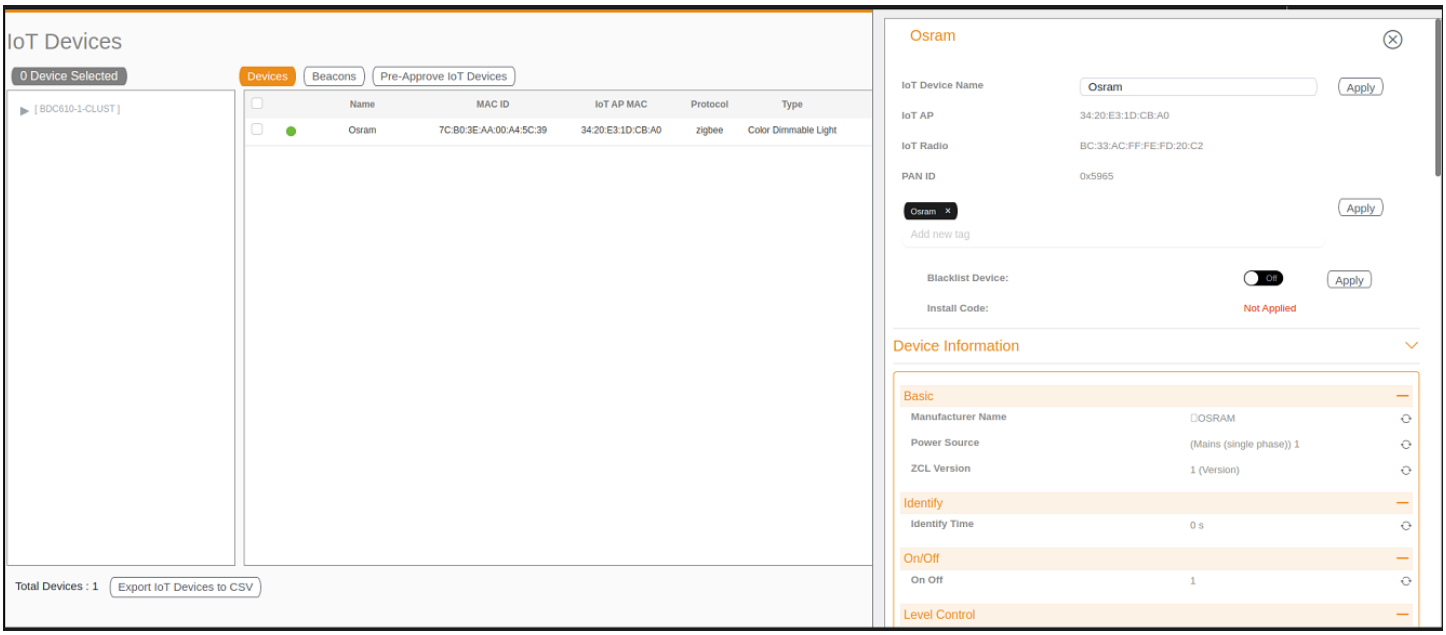
To discover OSRAM light bulbs, complete the following operations.

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 107 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.

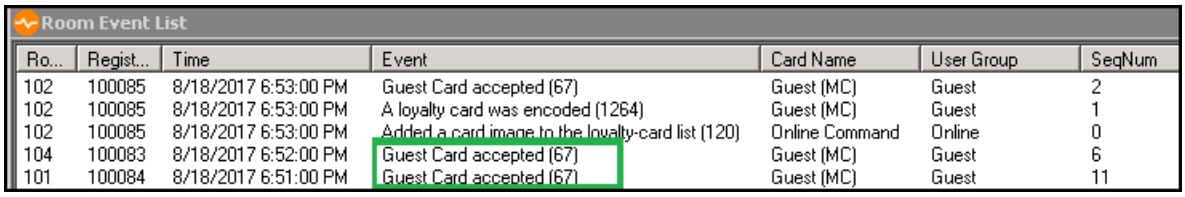
1. Swipe the AA Lock Discover Card across the lock.
2. Ensure that the LED blinks green.
3. Add the lock to the RUCKUS IoT Controller (if it is not already pre-approved).

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 108 Visionline Server Event Log



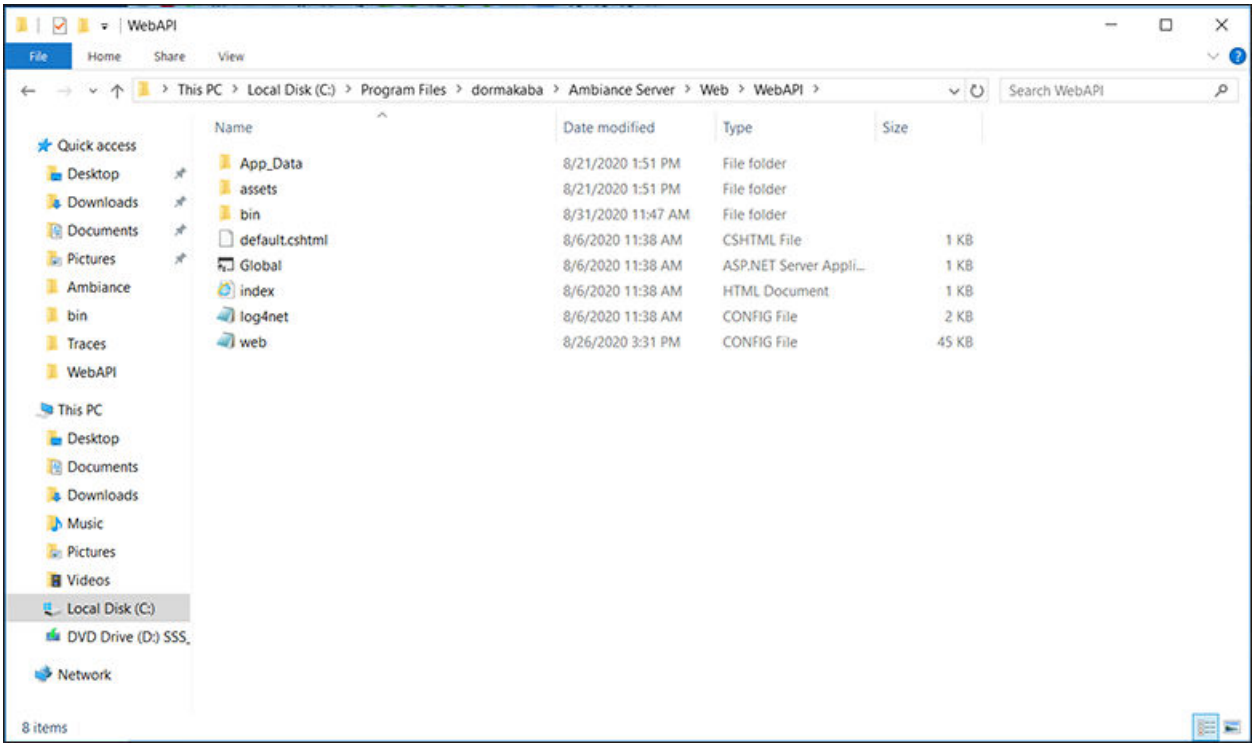
Managing the Dormakaba Locks

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

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

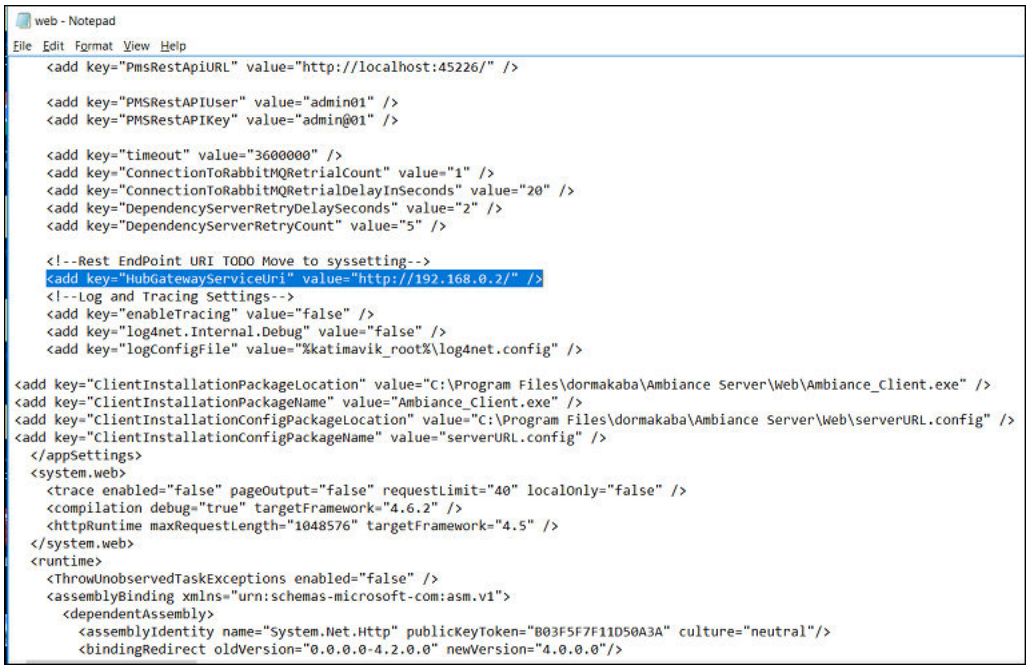
1. In the Ambiance Server, go to `C:\Program Files\dormakaba\Ambiance Server\Web\WebAPI\web.config file` and open the web.config file in notepad.

   FIGURE 109 Locating the web config file



2. From the row, **HubGatewayServiceUri** value="http://192.168.0.2/", select the IP address of the controller.

FIGURE 110 Finding the IP Address



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.

1. Select the Gateway and start a Device Scan from Ambiance UI.

   A scan window appears in the UI.
2. Swipe the DormaKaba Pairing Card across the lock.
3. Ensure that the LED blinks.

   Dormakaba Lock details will show in the Scan Window of the contrroller.
4. Add the lock to the Ruckus IoT Controller (if it is not already pre-approved).
5. Go to **Device Management** page, select the **Gateway**, click on **Next** to Access Points in the Ambiance UI.

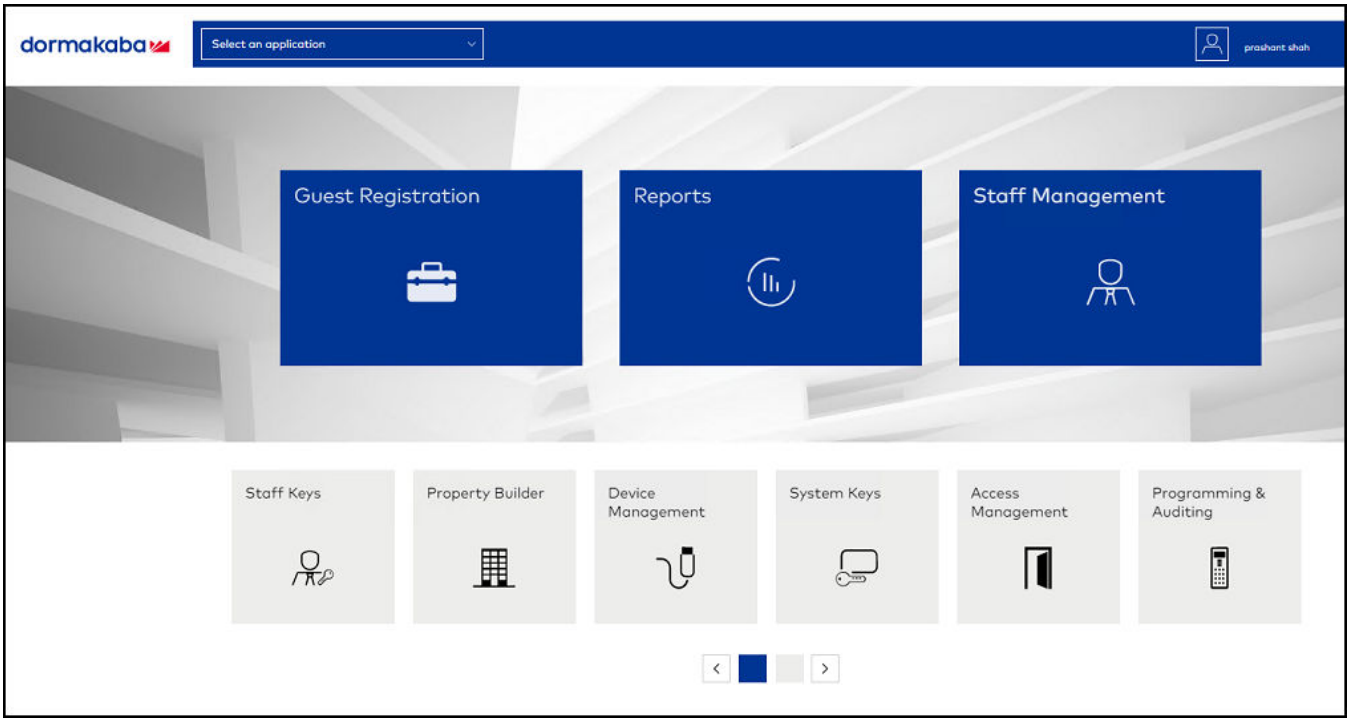
   You can now verify if the lock has established its communication with Ambiance Server.

Blocking and Unblocking Dormakaba Lock

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

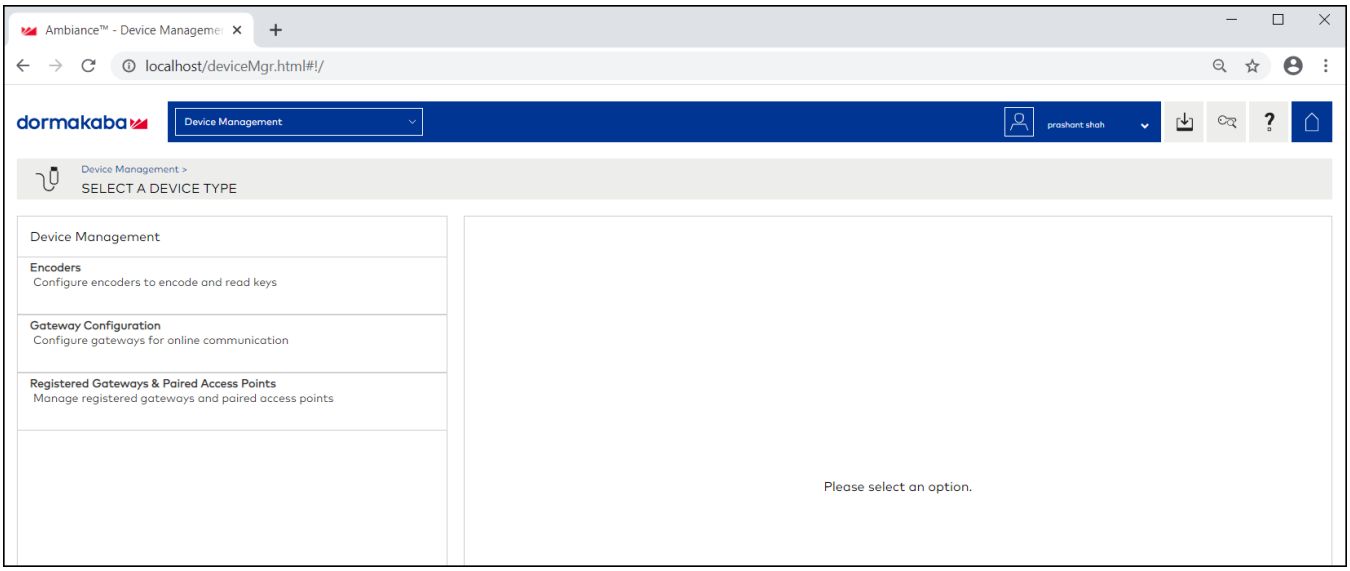
1. Login to the Ambiance Server. The default username and password is **Admin01** and **Admin@01**.

FIGURE 111 Login into Dormakaba Plugin



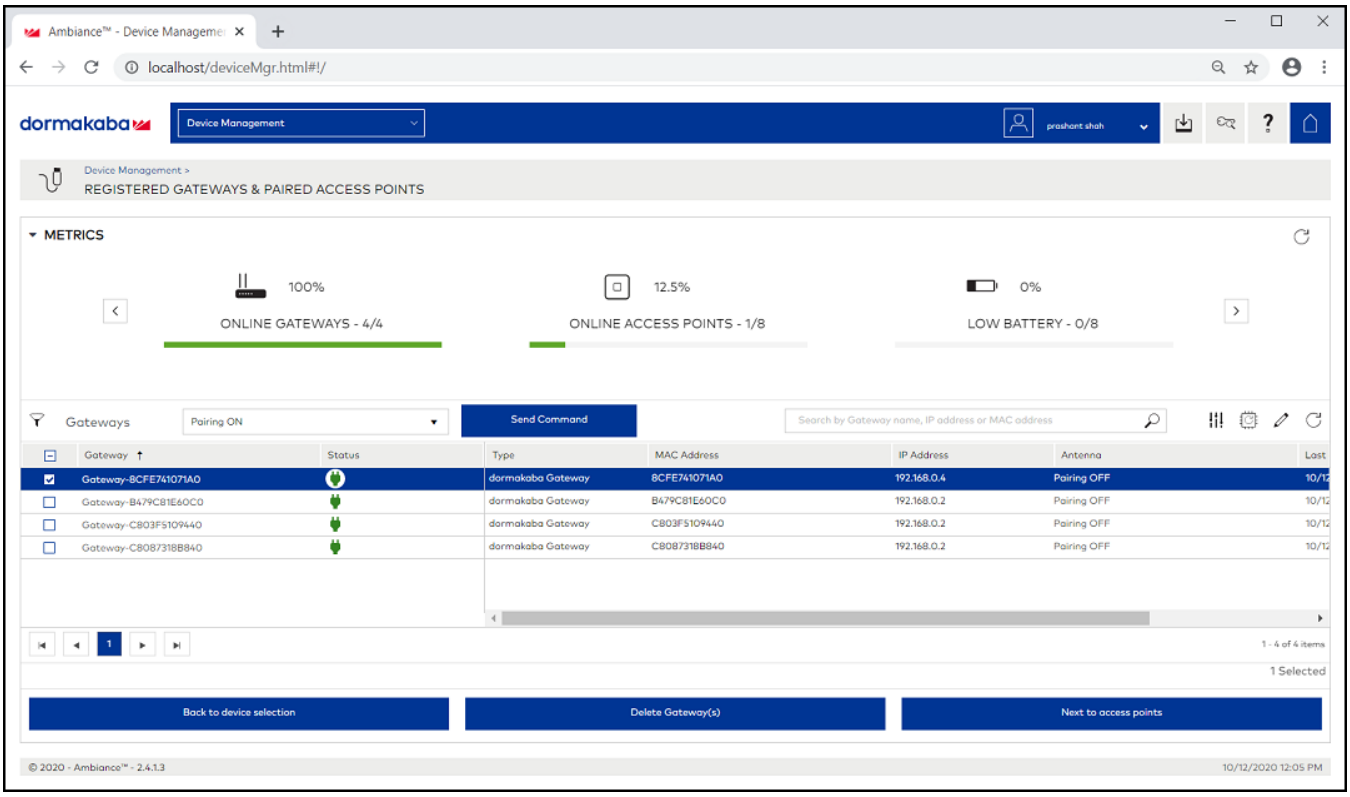
2. Click **Device Management**.

FIGURE 112 Selecting Device Management



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

FIGURE 113 Selecting Register Gateways and Paired Access points

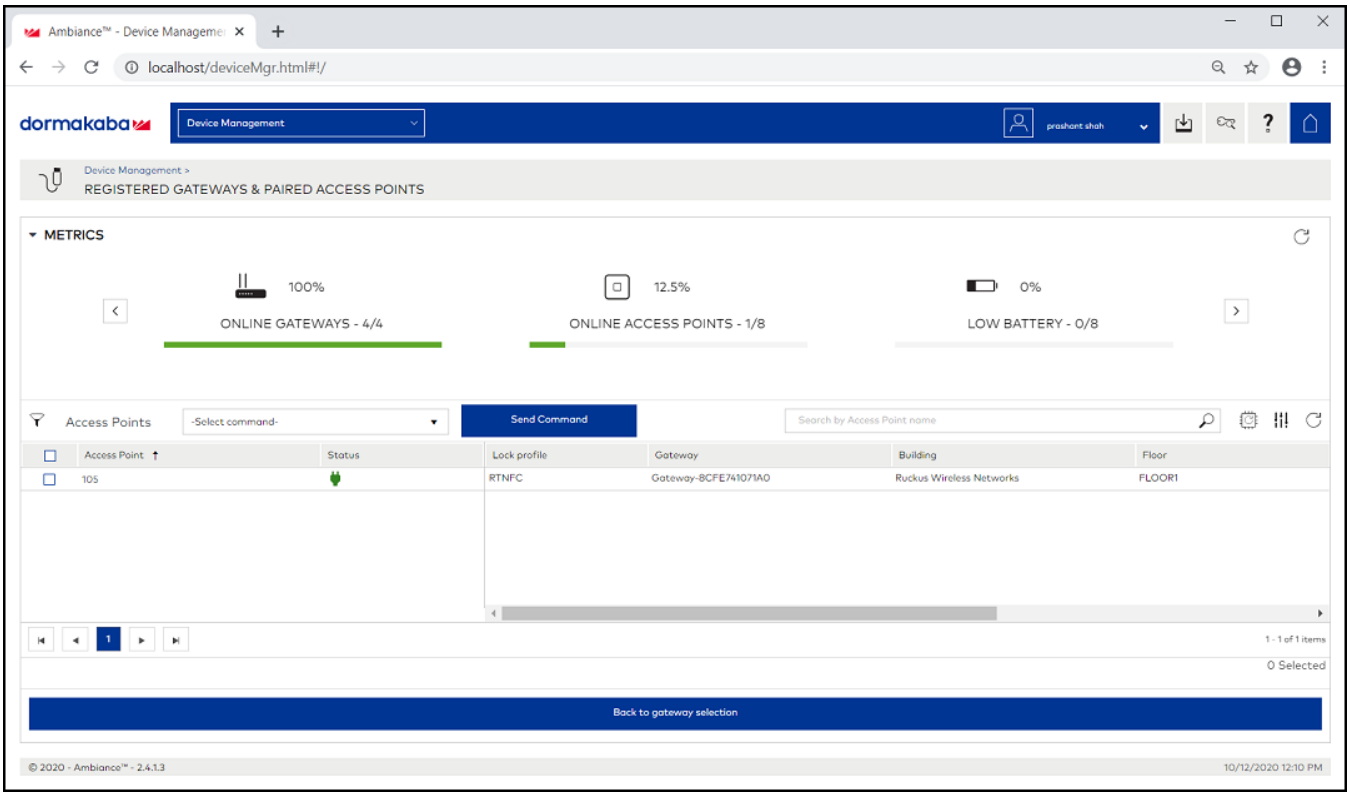


4. From the **Gateways**, select a gateway, and from the pull down select **Pairing ON** and click **Send Command** to start the gateway in scanning mode.
5. Swipe RF Pairing key card.

   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 114 Displaying the Lock



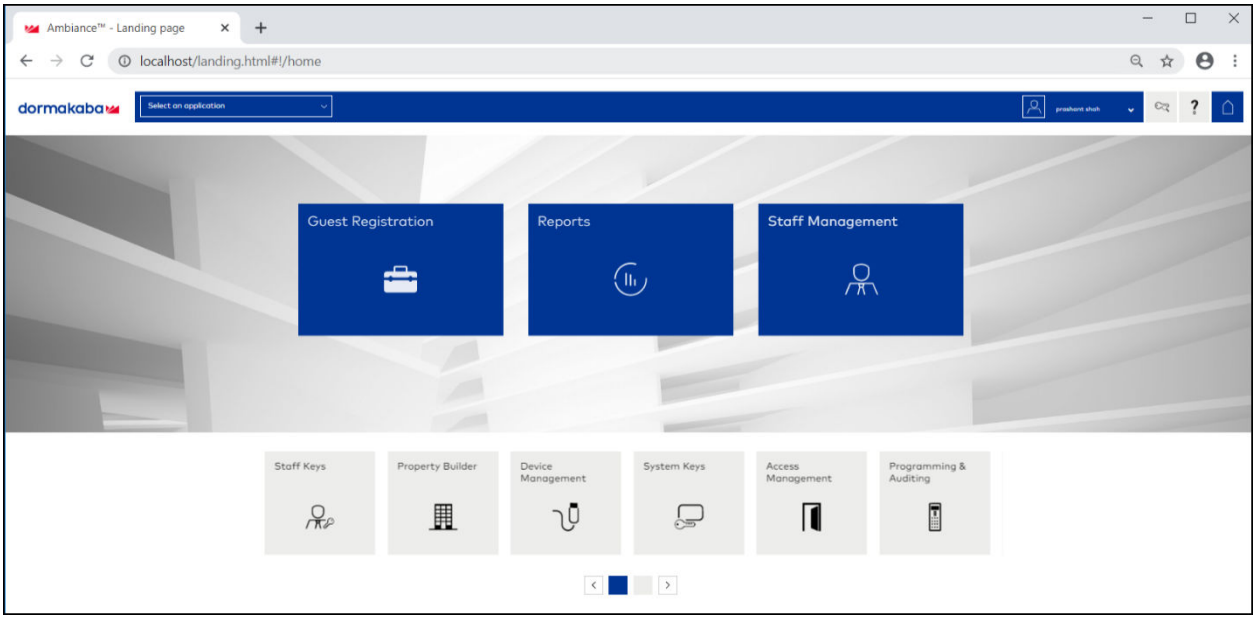
9. To confirm the lock connection, select the sage gateway, and click **Next to Access Point**.

Blocking the Key Remotely

Perform the below steps to block the key remotely.

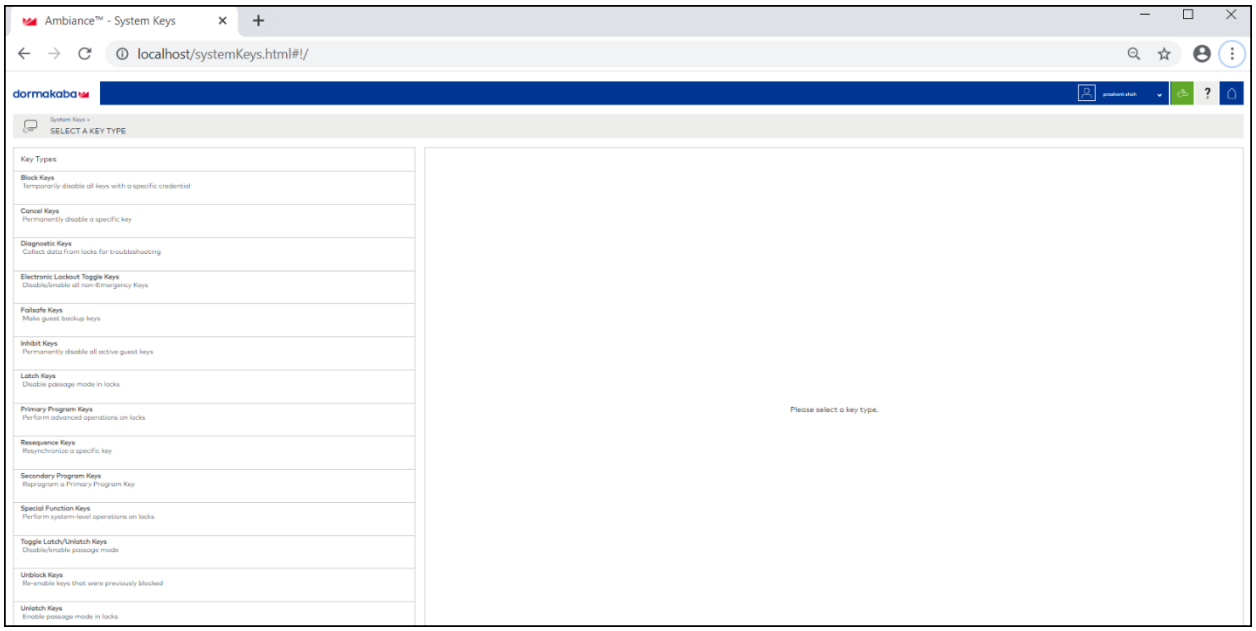
1. Go to Dormakaba Homepage.

   FIGURE 115 Dormakaba Homepage



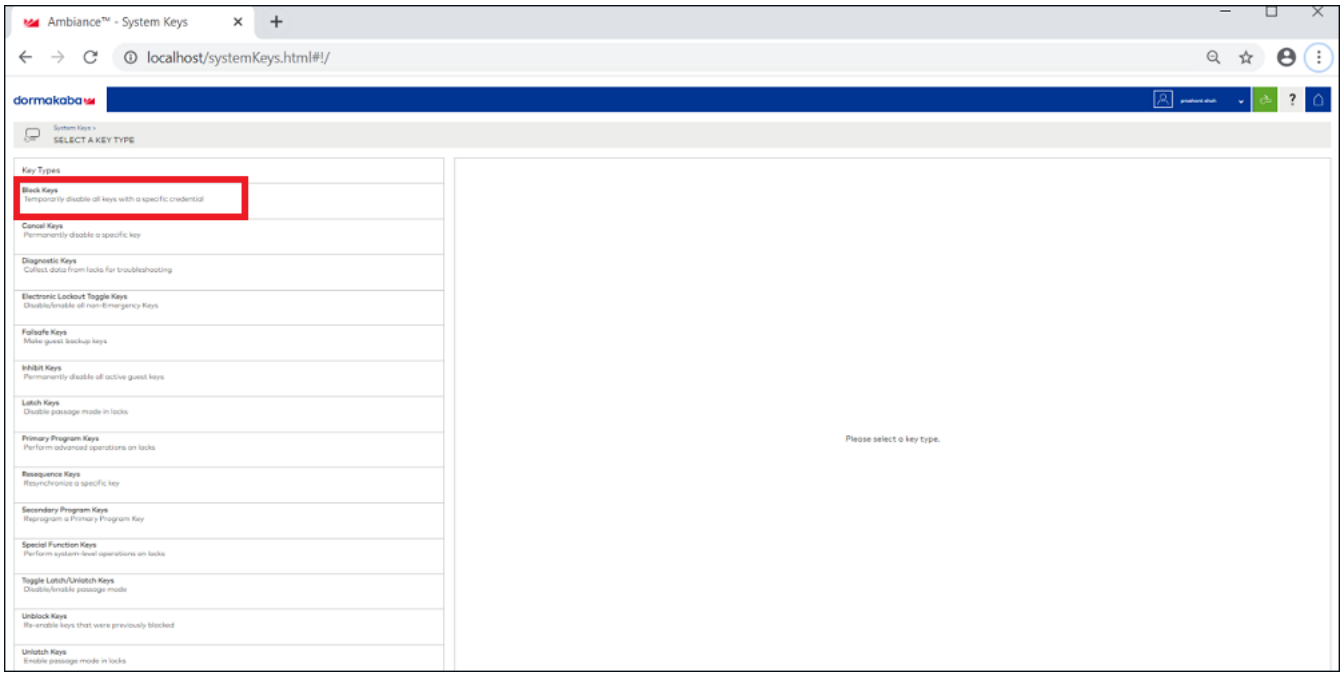
2. Click **System Keys**.

   FIGURE 116 Selecting the System Keys



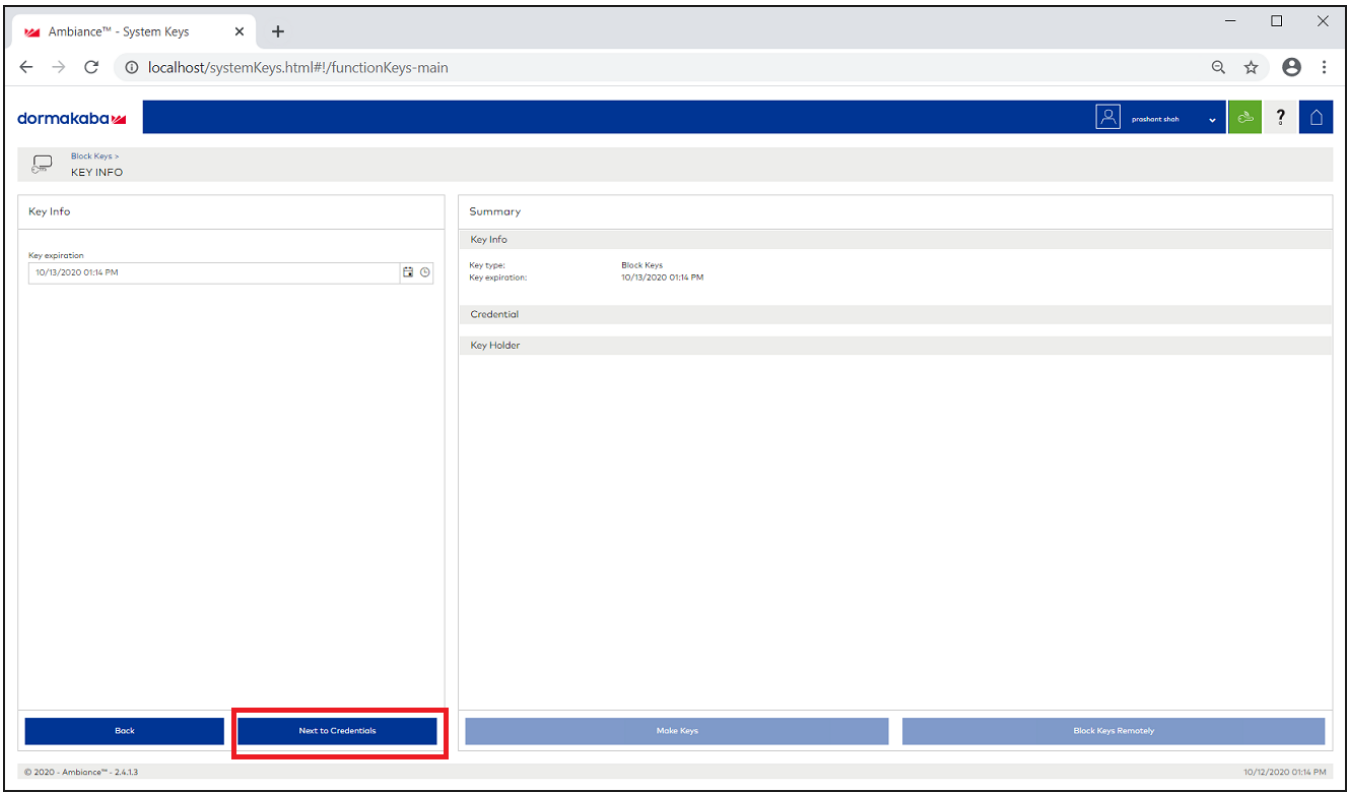
3. Click **Block Keys**.

FIGURE 117 Selecting the Block Keys



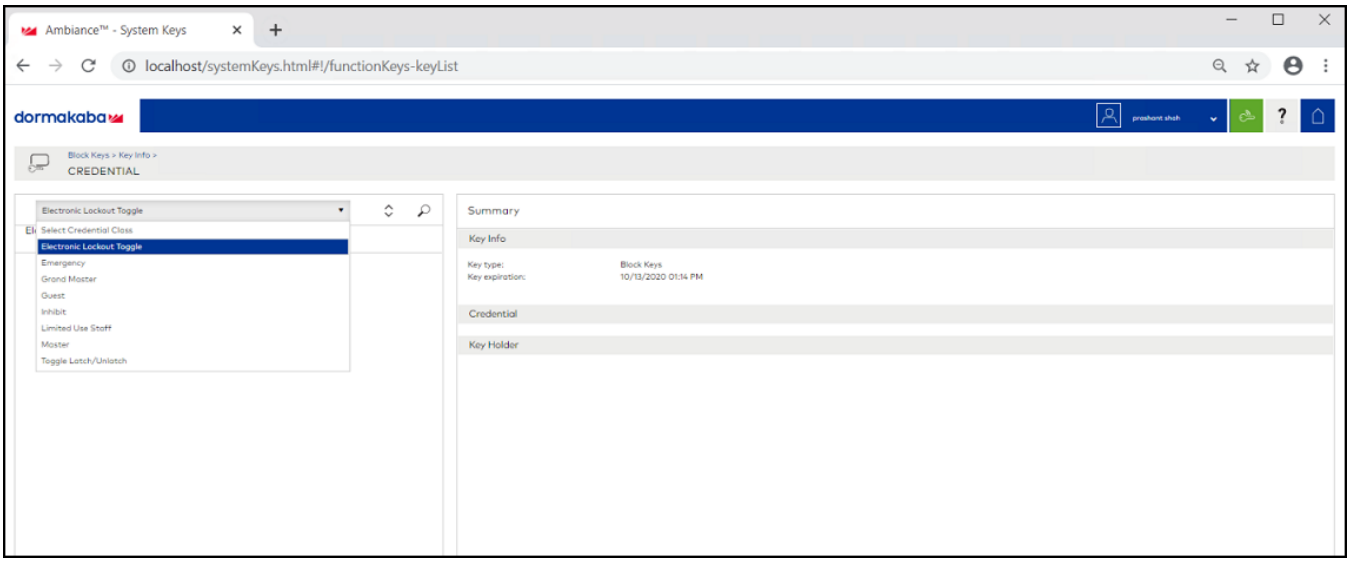
4. Click **Next to credential**.

FIGURE 118 Clicking the option Next to credential



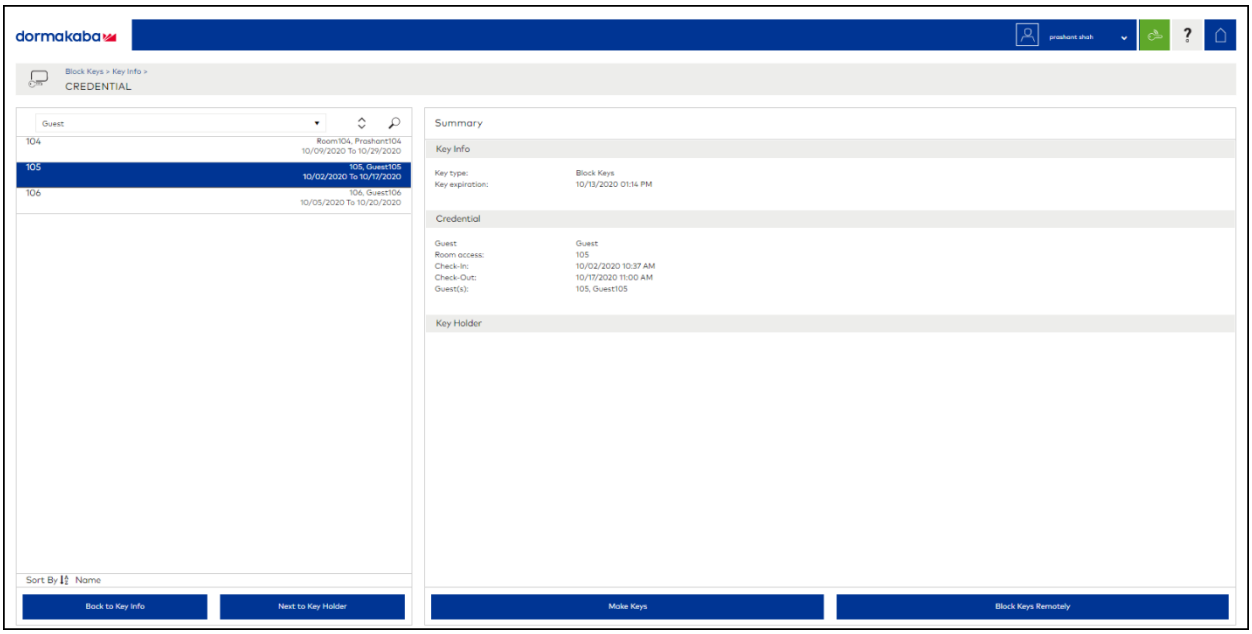
5. From the list, select **Guest** to block a **Guest room**.

FIGURE 119 Selecting Guest from the drop-down list



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

FIGURE 120 Selecting the Guest Room Number



7. Click **Block Key Remotely**.

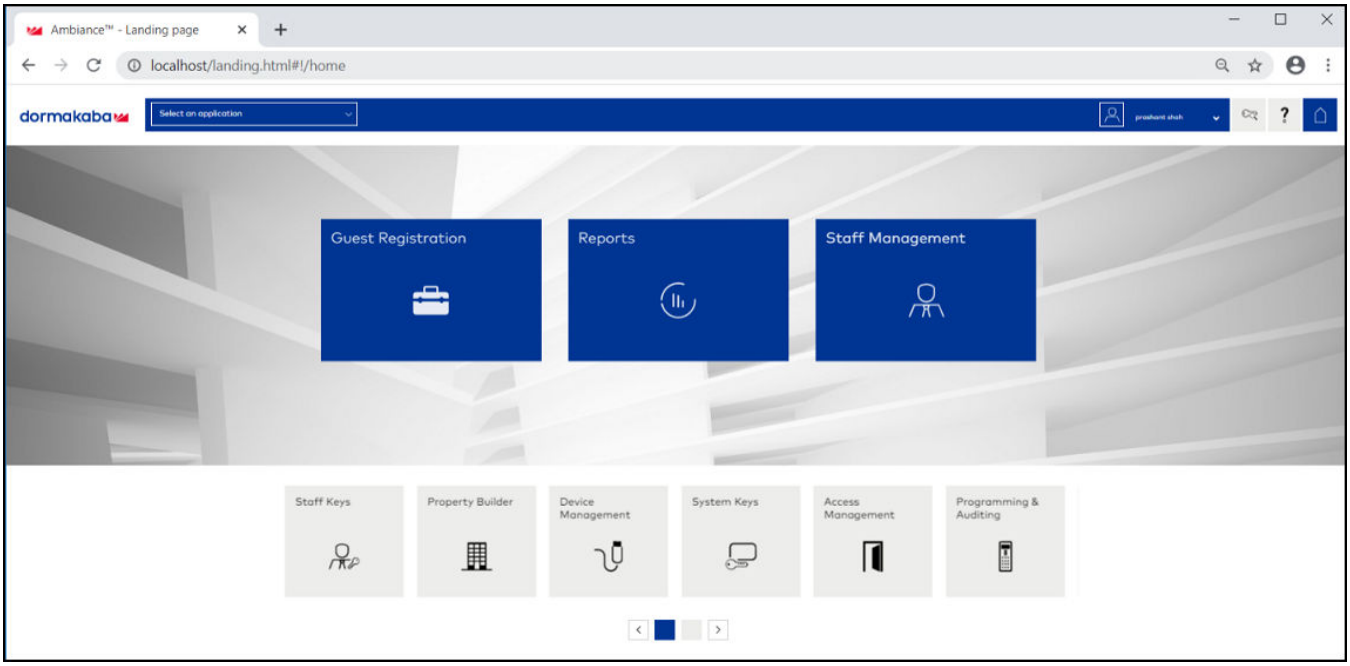
After you click **Block Key Remotely**, the LEDs will glow in the following pattern - one solid red LED, six green, and yellow LED together.

Unblocking the Key Remotely

Perform the below steps to unblock the keys remotely.

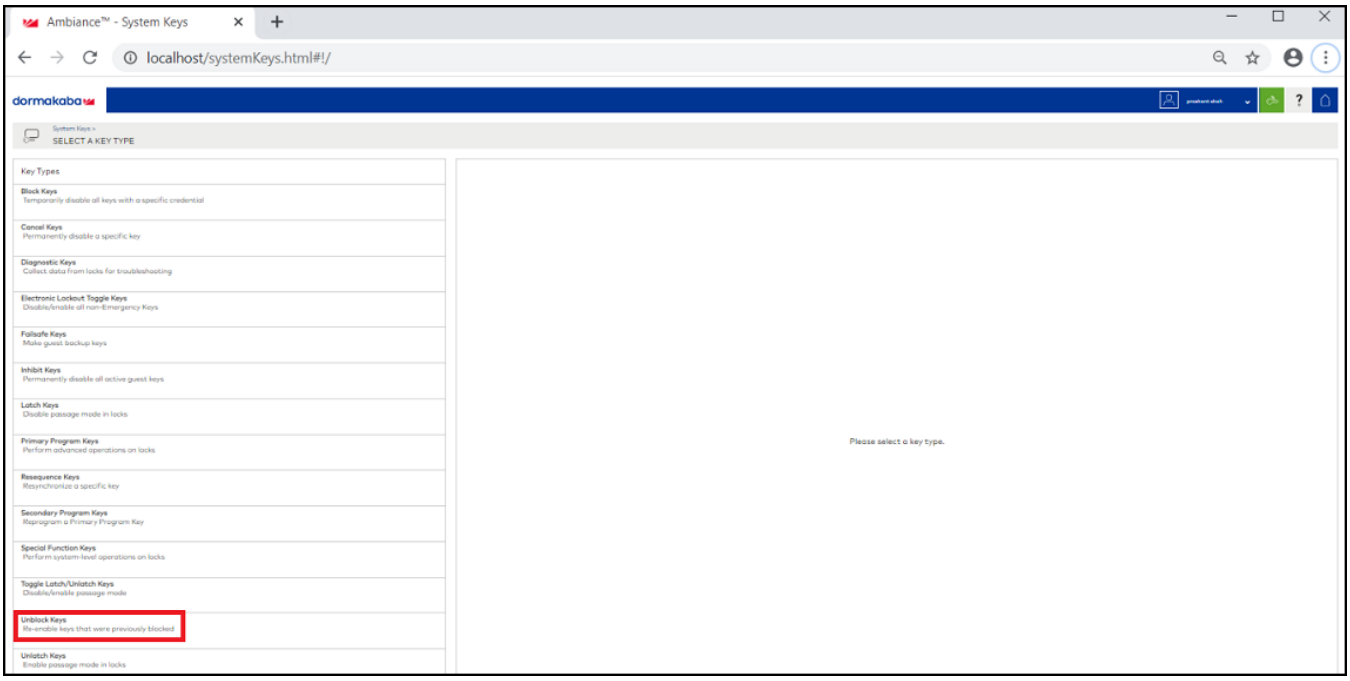
1. Go to the Dormakaba Homepage.

FIGURE 121 Dormakaba Homepage



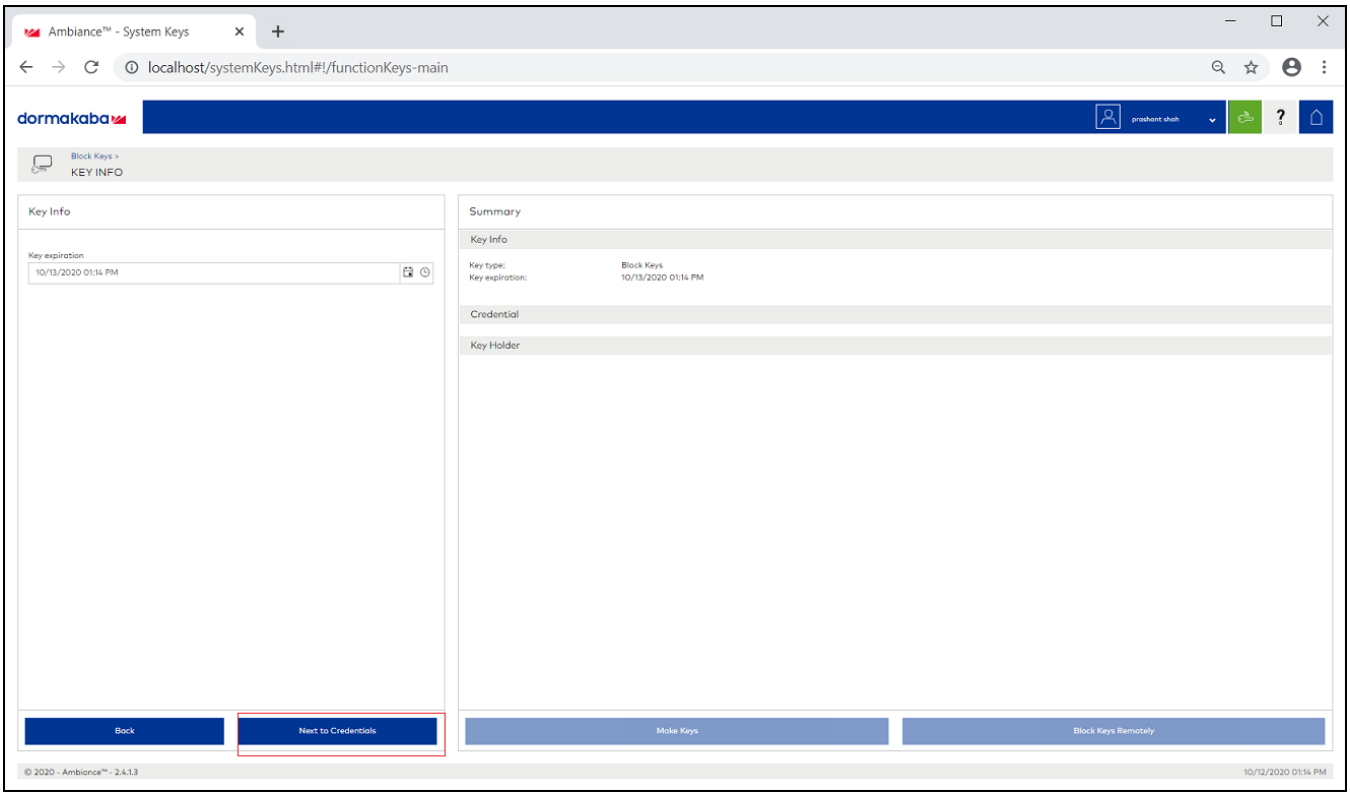
2. Click **System Keys**.

FIGURE 122 Selecting the Unblock Keys



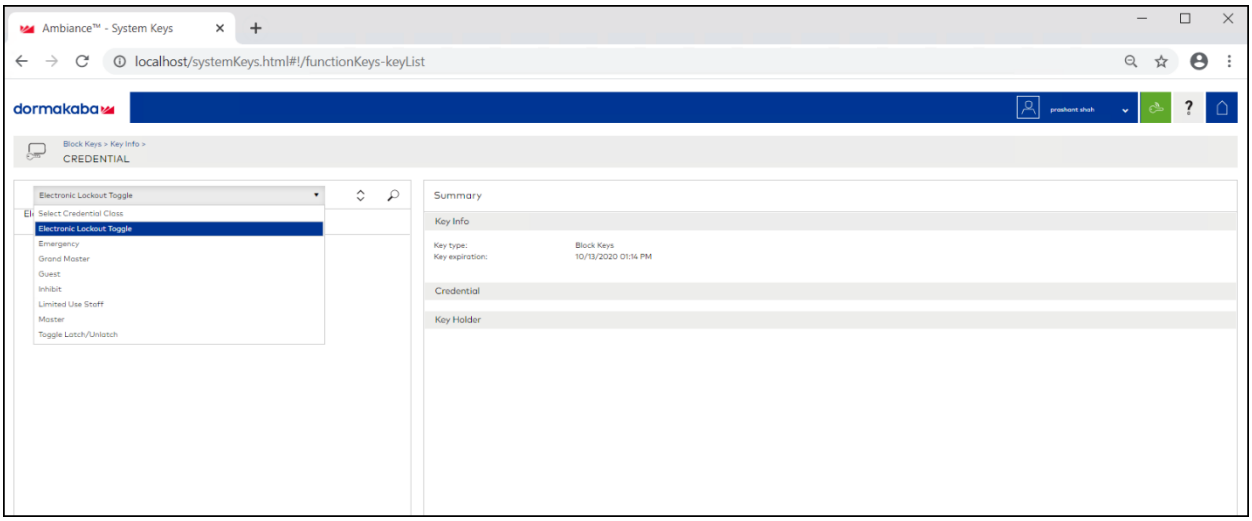
3. Click **Next to Credntial**.

FIGURE 123 Clicking the option Next to Credential



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

FIGURE 124 Selecting Guest from the drop-down list



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.

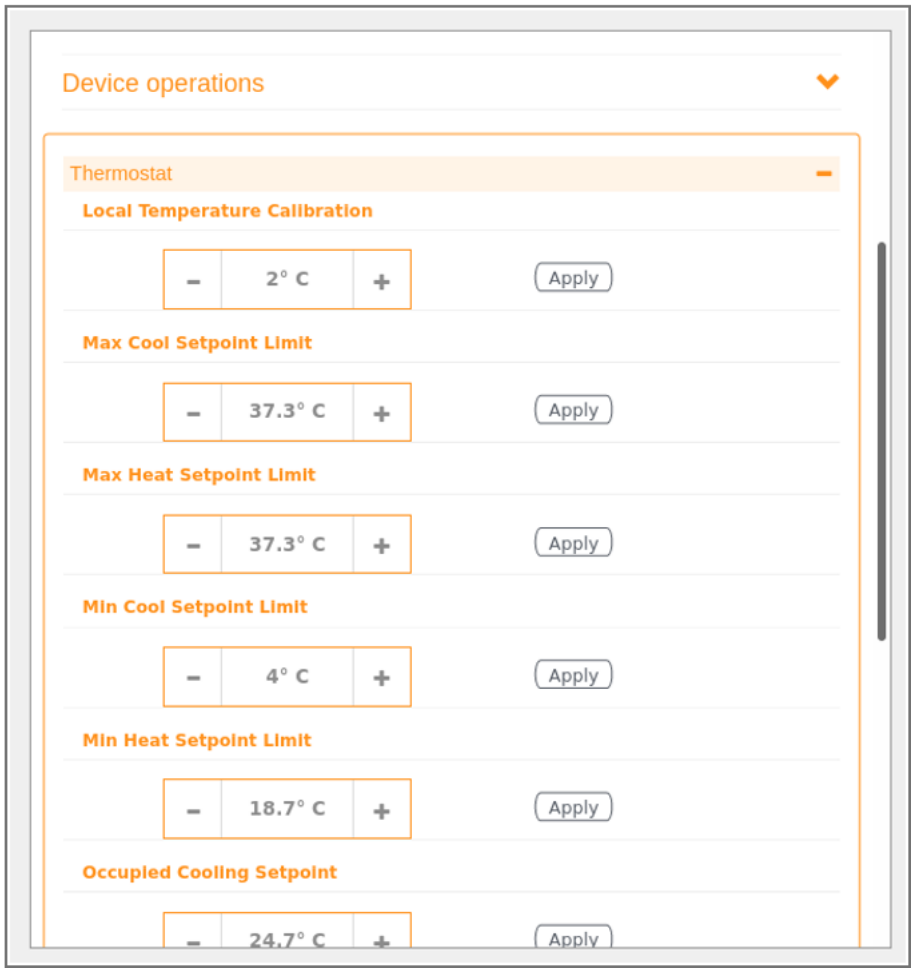
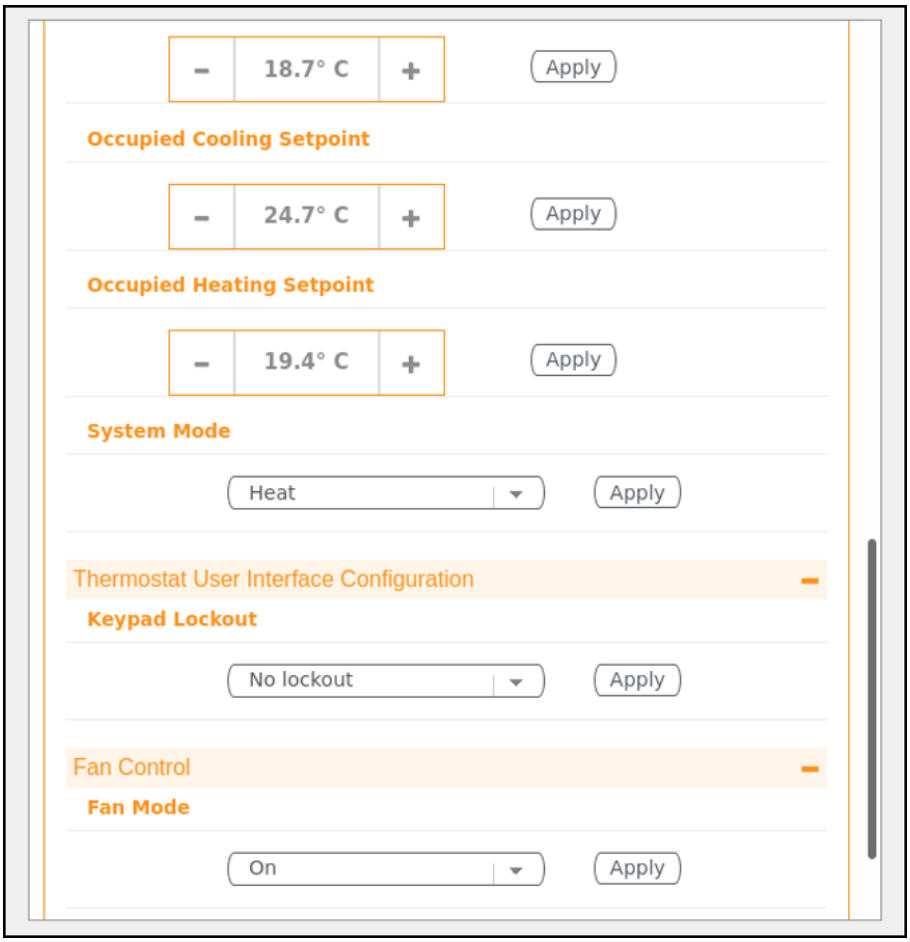


FIGURE 125 Thermostat User Interface Configuration and Fan Control Cluster operations


18.7° C
Apply
Occupied Cooling Setpoint
24.7° C
Apply
Occupied Heating Setpoint
19.4° C
Apply
System Mode
Heat
Apply
Thermostat User Interface Configuration
Keypad Lockout
No lockout
Apply
Fan Control
Fan Mode
On
Apply

Events

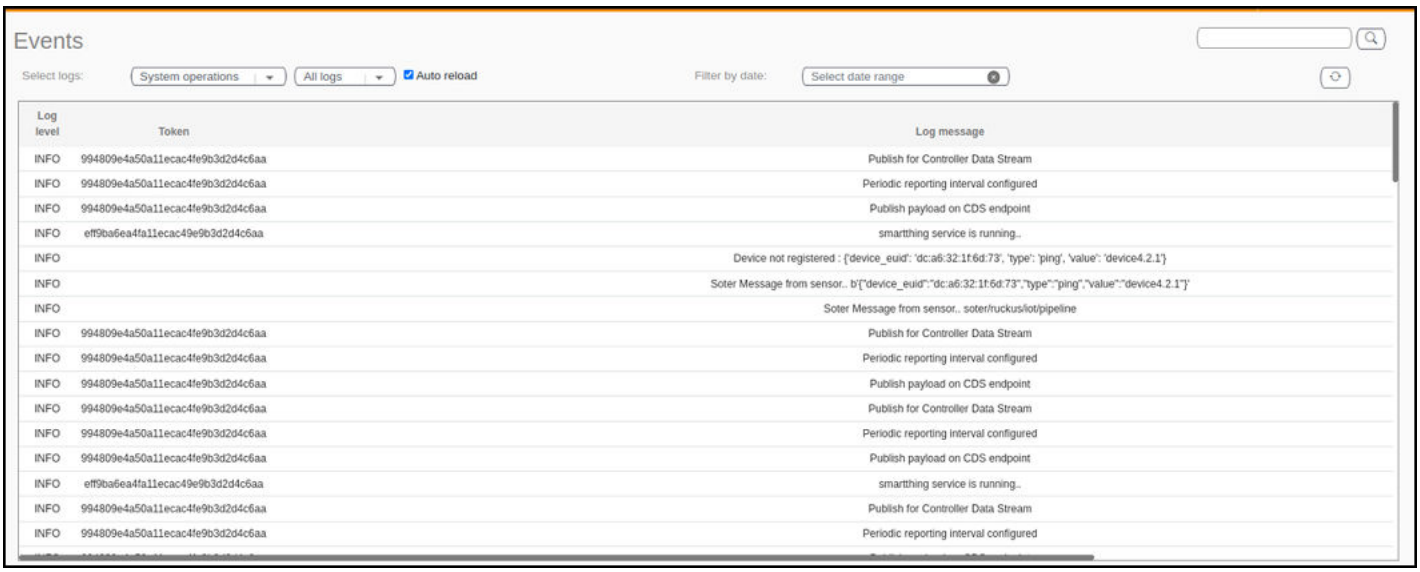
- Viewing Events..... 133

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 126 Events Page



© 2024 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com