BRH EMS User Manual

(SL-BRH-2.0.0)

FCC ID: 2AUUC-KAILASH5W00

Revision	Date	Author	Comments
			<previous pre-release data deleted>
1.0	07/18/19	MK	Final Draft to DISH networks
1.1	07/29/2019	AS	(Demo Fdbk) permission to create delete and update alarm for different users.
1.2	09/18/2019	AS	Updated configuration, alarm tables. Added Reboot, Show notifications and Audit logs procedures. Updated Saankhya logo and requirements for ems (Browser versions).
1.3	10/07/2019	AG	Alarms Documentation and other configuration related fixes
1.4	11/04/2019	AG	Document Revamp with latest screenshots
1.5	12/23/2019	AKS	Updated Table 5: Alarms Severity and Colors in User Guid as per RTM EMS-24, Remove Global Configurations
1.6	01/17/2020	AKS	Updated Appendix A : Roles and Actions allowed Updated Hierarchical Diagram for Roles and Users
1.7	02/05/2020	AKS	Replaced the screenshots with latest modification Updated Alarm Severity in Table 1 and Table 4 Removal of severity value column in Table 5 Change the value of MPE PID Removed text like SL-BRH-NNN-BRH-EMS-OAM Architecture
1.8	04/13/2020	AG	Updates based on current screen shots and small text fixes etc.
1.9	05/25/2020	AG	Alarms clear documentation, EMS support contact information and Snapshot documentation.
2.0	10/11/2020	EC	Added description for CW-mode. Added brief description for runtime configurations. Changed revision number on title page to 2.0.0.

Introduction

Kailash EMS is used to manage a network of Broadcast Radio Heads (hereafter referred to as BRH). The management comprises of following:

- Fault Monitoring
- Configuration
- Accounting
- Provisioning
- Security

This confirms with the traditional FCAPS model for management of telecom networks. Details of workflow and how the above model is available to the user is described in the following sections.

For any queries related to this document or operation of EMS, please contact the EMS Support using the Email address provided in the “About” Section of the web page. The EMS Support Contact Email address is support-ems@saankhyalabs.com .

Model Description

The following subsections detail the FCAPS aspect in an order which is relevant from the workflow point of view

Security

EMS Security mainly comprises of two parts -

1. Secure communication between BRH Devices and EMS . This is achieved using TLS based security for communication between a BRH device and EMS and a client authentication using client side certificates.

2. Security of EMS is provided through role based access control and audit logging of user initiated actions. For EMS, role based access control determines which actions can be performed by a user belonging to a given role. An overview of different roles is provided below and Appendix A details the complete capability matrix for individual roles.

   There are three main roles in EMS

   a. Owner - Owner is an owner of all the devices and is like Super Administrator having all the required privileges to perform actions.
   b. Administrator (admin) - This role is a high privilege role in EMS and is capable of performing major provisioning and other actions that require elevated privileges (eg. Uploading a firmware version to be upgraded across devices.)
   c. Operator (operator) - This role is having lowest privilege levels and is mainly concerned with day to day operation of devices. This role is allowed to take only a minimum set of actions against devices in BRH EMS like acknowledging alarm notifications etc.

   The above is better understood from the following hierarchy. Any operation that modifies or tries to view data at level higher in hierarchy is not allowed

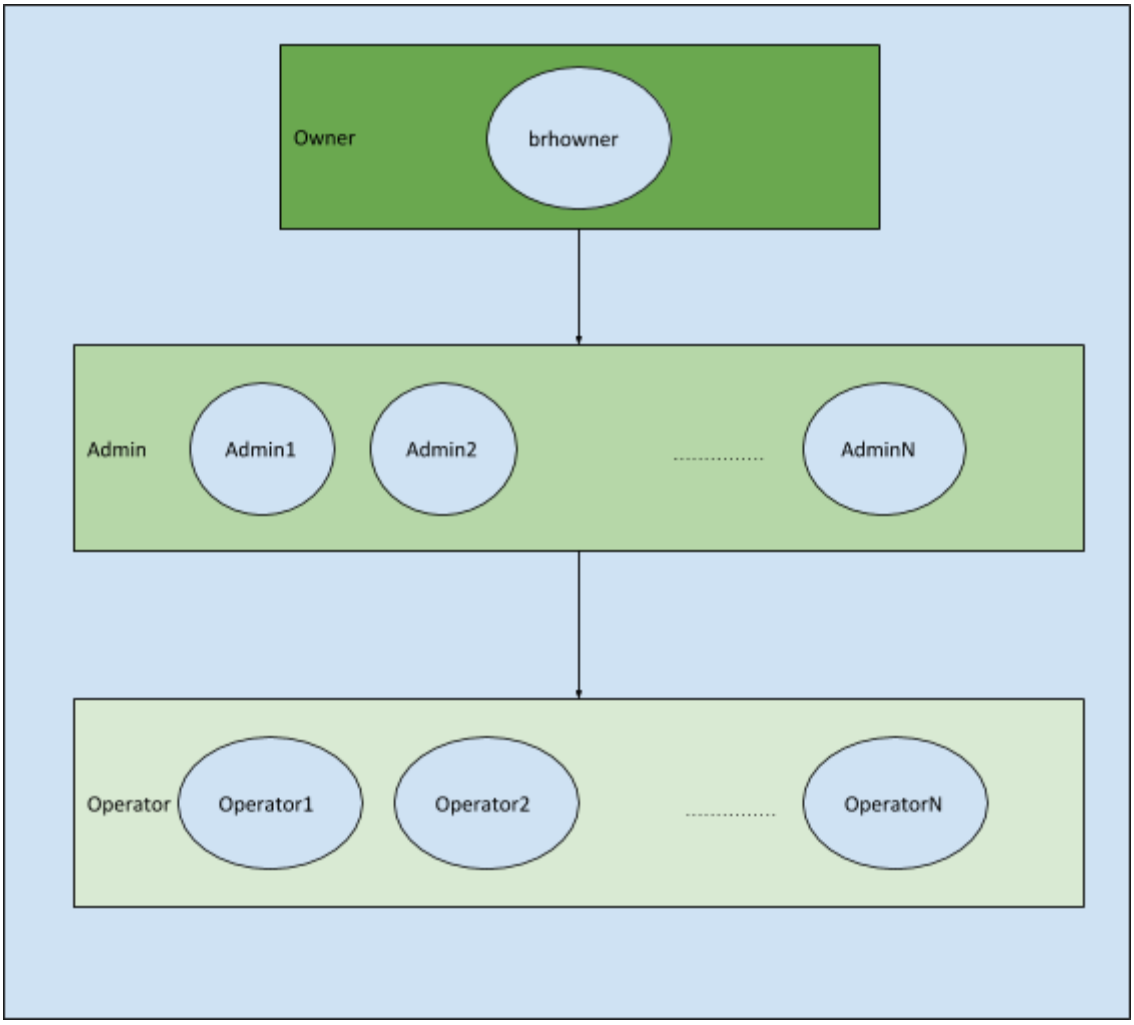


Figure - 1 : EMS Roles and Users

Configuration

Configurations are of 2 types:

1) Device Configuration - This configuration determines both the boot time and run-time behavior of the device. This configuration can be applied per device or for a set of devices. These include parameters for all the different submodules which can be changed etc. (eg. STLIP IP Address/Port, MPE PID etc.)
2) Alarm configurations - These define the alarm ID linked to the alarm with custom settings for severity from one of the INFO, WARNING, MINOR, MAJOR, CRITICAL and allowed actions from ACKNOWLEDGE. Alarms could be set to auto acknowledge by users in which case they do not show up on the dashboard and are directly logged in the audit logs.

Provisioning

Provisioning defines the various user roles and adds device to the list of allowed devices on the network as per the hierarchy shown in Figure 1

Accounting

This being a broadcast solution, there is no per user accounting that is applicable in the case of EMS.

Fault Monitoring

Faults originated at the device are available as Alarm Notifications on EMS. Based on the Alarms Configuration for a given type of Alarm, an alarm can be acknowledged automatically. Details of the alarms supported by the system are mentioned in the table below.

ID	Module	Alarm Type	Default Level	comment
0	EMS	EMS Internal Alarm	Warning	
1	DVBS2	Backhaul Link Status Alarm	Critical	Backhaul BER > 2e-6 for 3mins
2	DVBS2	Backhaul Data Failure Alarm	Warning	MPE Section Errors, RTP Sequence Errors etc.
3	STLTP	STL-TP Link status Alarm	Minor	STL-TP packet error > x for 3 mins
4	GPS	GPS Lock Alarm	Critical	GPS Lock != Lock
5	ATSC3P0	ATSC3.0 Modulation Config Error Alarm	Critical	L1 Signaling != Valid
6	GLOBAL	BRH power status Alarm	Critical	BRH Power Status == OFF
7	GLOBAL	BRH BIST status Alarm	Critical	Built In Self-Test Status == FAIL
8	GLOBAL	BRH Temperature Threshold Alarm	Critical	Temperature > Threshold value
9	GPS	GPS Timing Sync Alarm	Warning	GPS time < EPOCH time
10	GLOBAL	Device Rebooted Alarm	Info	Device Rebooted

Table 1: Alarms Definitions

EMS workflows

EMS Workflows define user interaction with the EMS UI. This workflow typically consists of following three stages

1. Initial Setup - This involves actions required to bootstrap EMS system and setting up initial user for the EMS. This action is not exposed through EMS UI.
2. Provisioning - This includes adding users to system, defining device configurations adding new devices to the system etc.
3. Monitoring - This includes actions like monitoring provisioned devices, exporting statistics, monitoring alarms etc.
4. Management - This includes performing software upgrades, requesting change in device runtime configuration, performing rebooting devices etc.

Initial Setup (Not available Through GUI)

Create Owner User

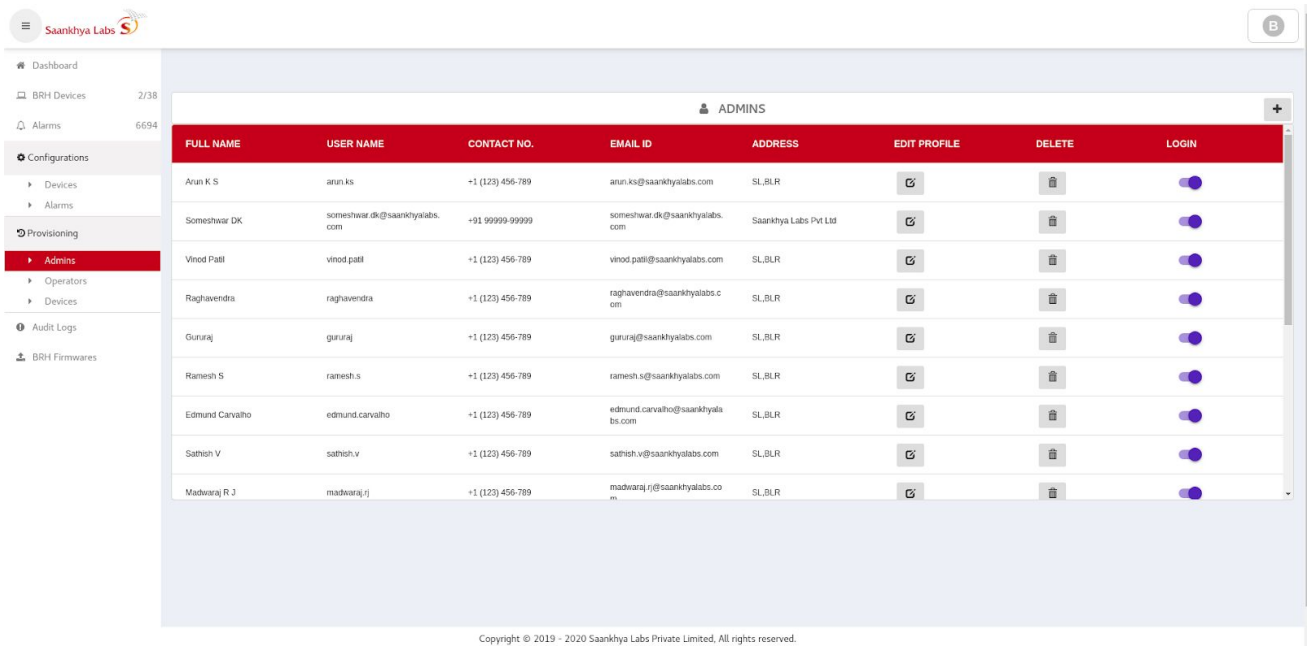
This is one of the prerequisites that needs to be performed before further actions can be performed on the GUI. This involves creating 'owner' user who is responsible for initial few actions. Minimum action required to be performed as 'Owner' Role is creating at-least one user belonging to Administrator role. All the subsequent actions will be performed by the Administrator user created. It is possible to perform actions in this workflow as 'Owner' role, but it is not recommended. For the remainder of the document, it is assumed that a user with login ID 'brhowner' is created.

Provisioning

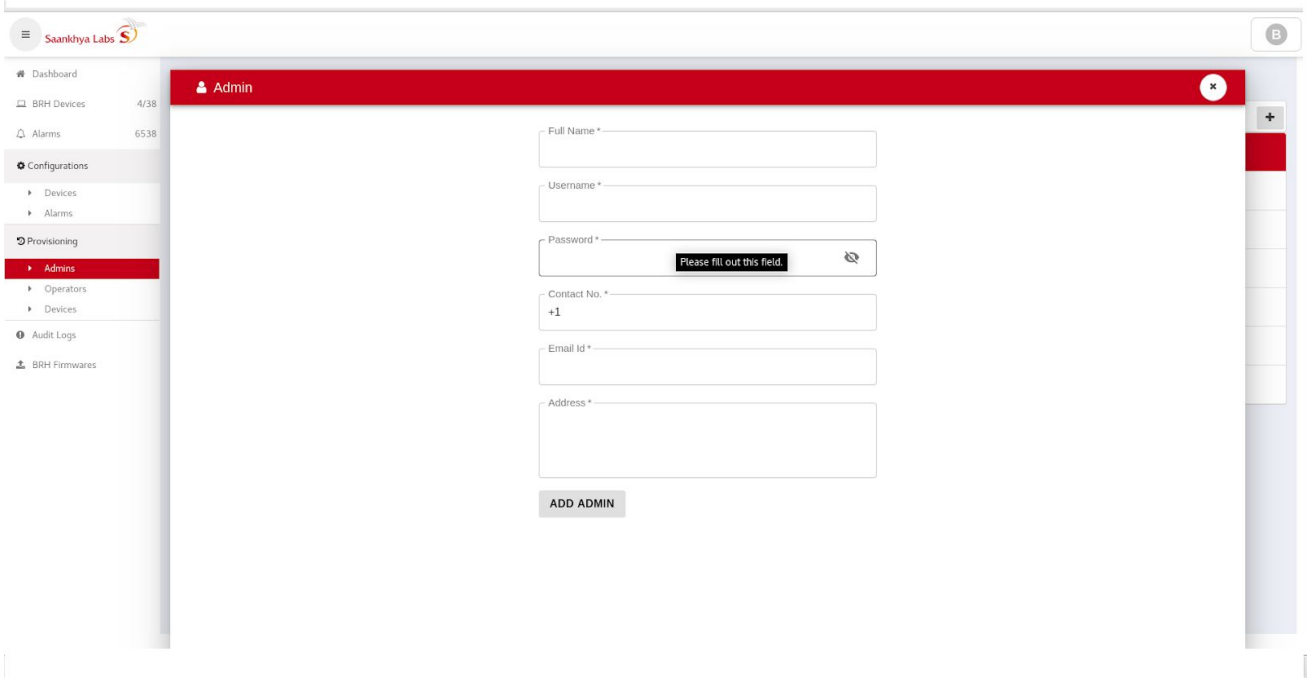
Create User with Administrator Role

1) Login using ‘brhowner’

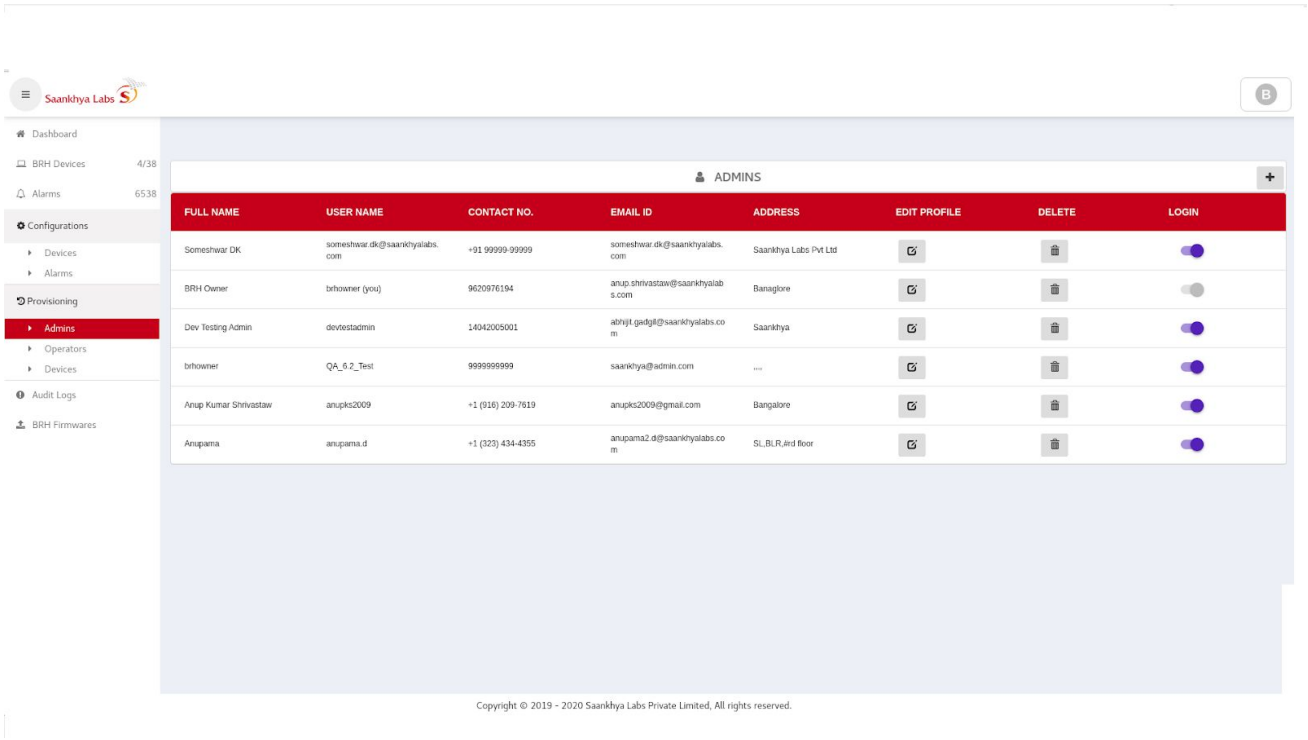
2) Navigate to the Admins submenu provisioning option and click on the Add Admin (+)



3) Fill Required Details (All fields are mandatory)



4) Admin is added to the list

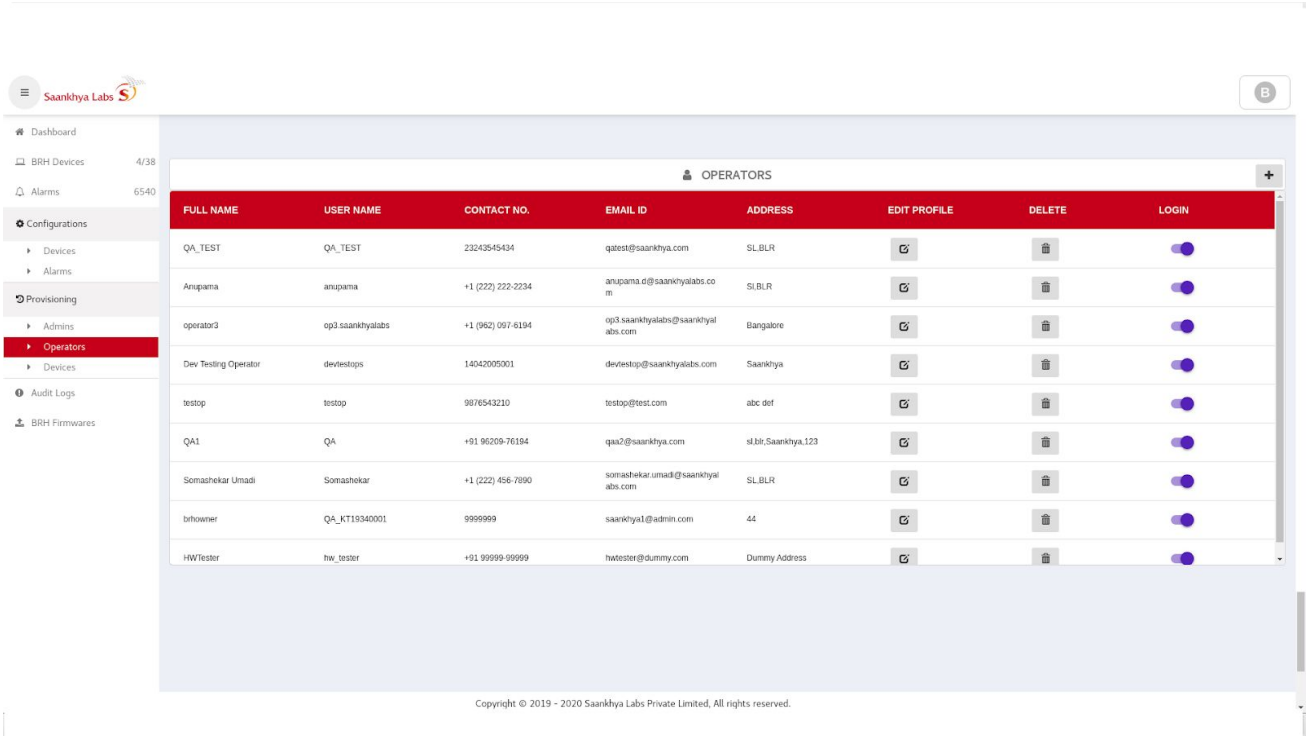


Logout as ‘Owner’ Role and Login as ‘Administrator’ Role (optional)

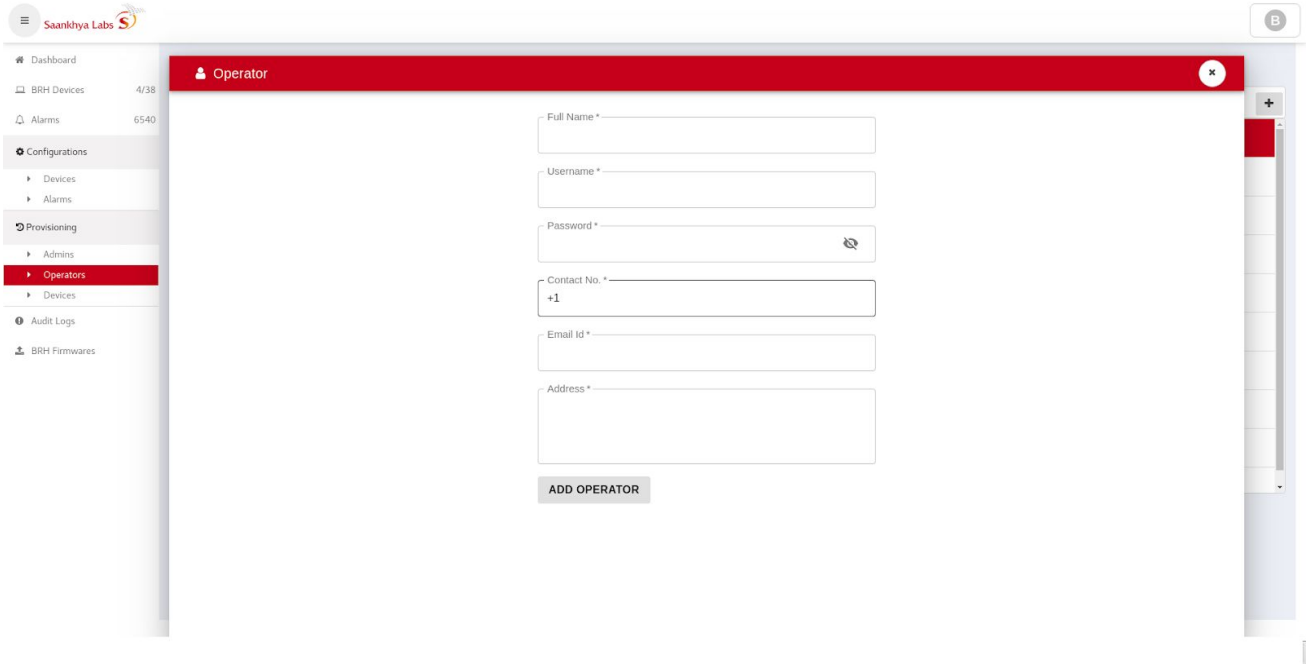
All the subsequent steps are performed with the user logged in at the end of step 3 above. (assumed for discussion below - user with ID 'brhadmin')

Create User with Operator Role

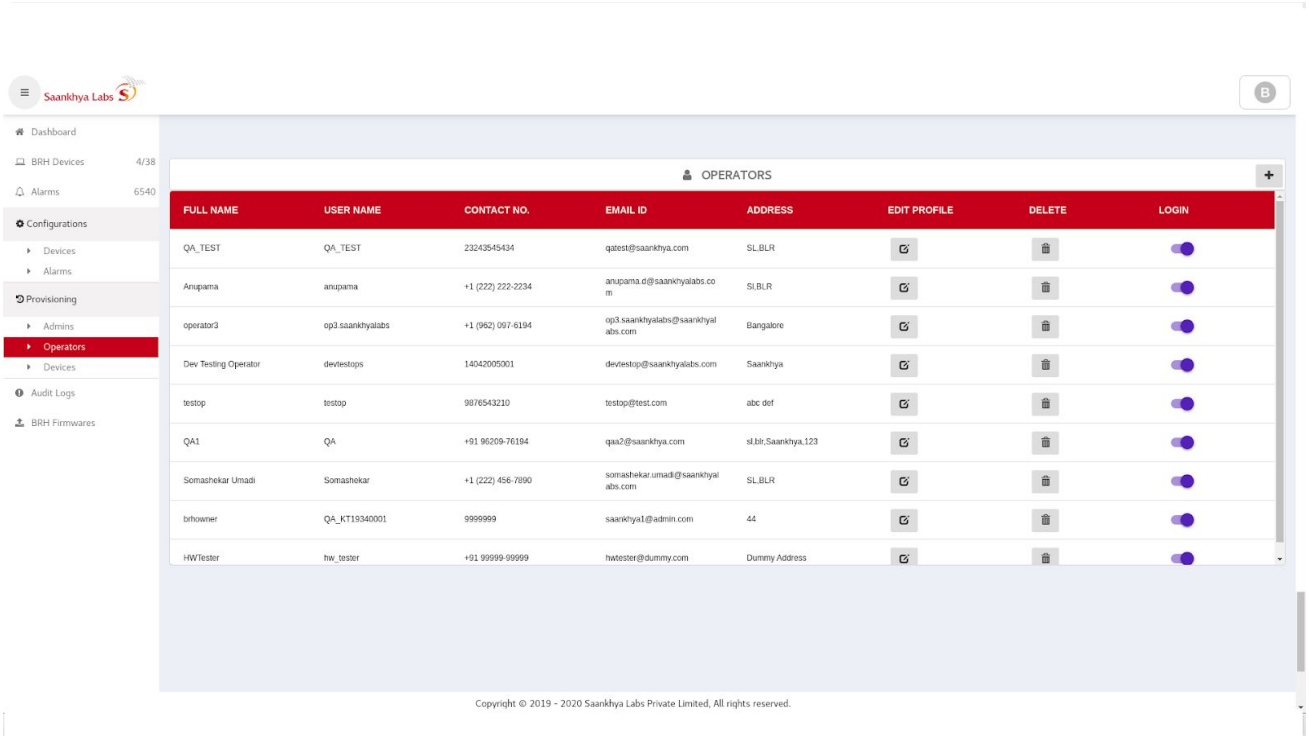
1) Navigate to Operators Menu and Click on Add Operator



2) Fill in the required form (All fields are Required)

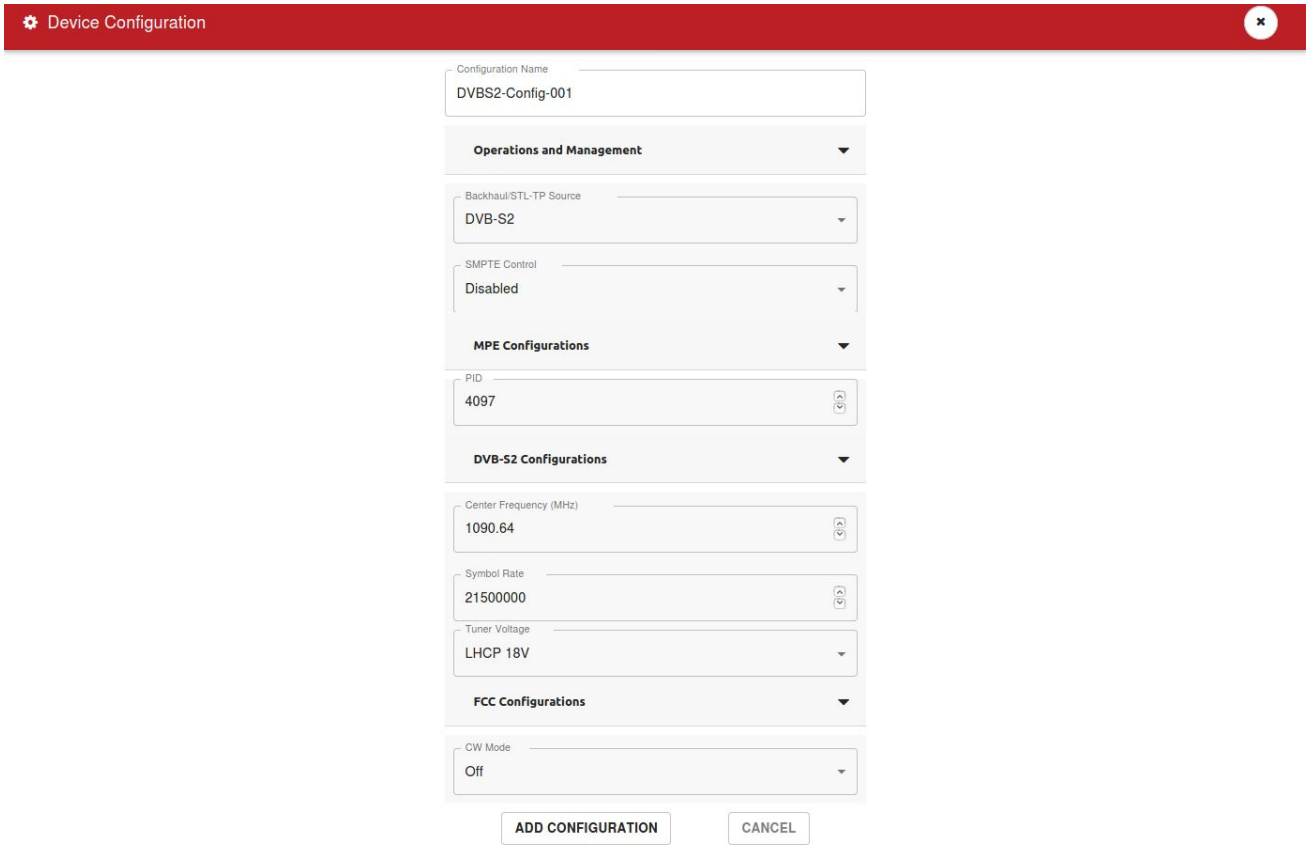


3) Operator if Added is shown successfully.



Create Configuration for the Device

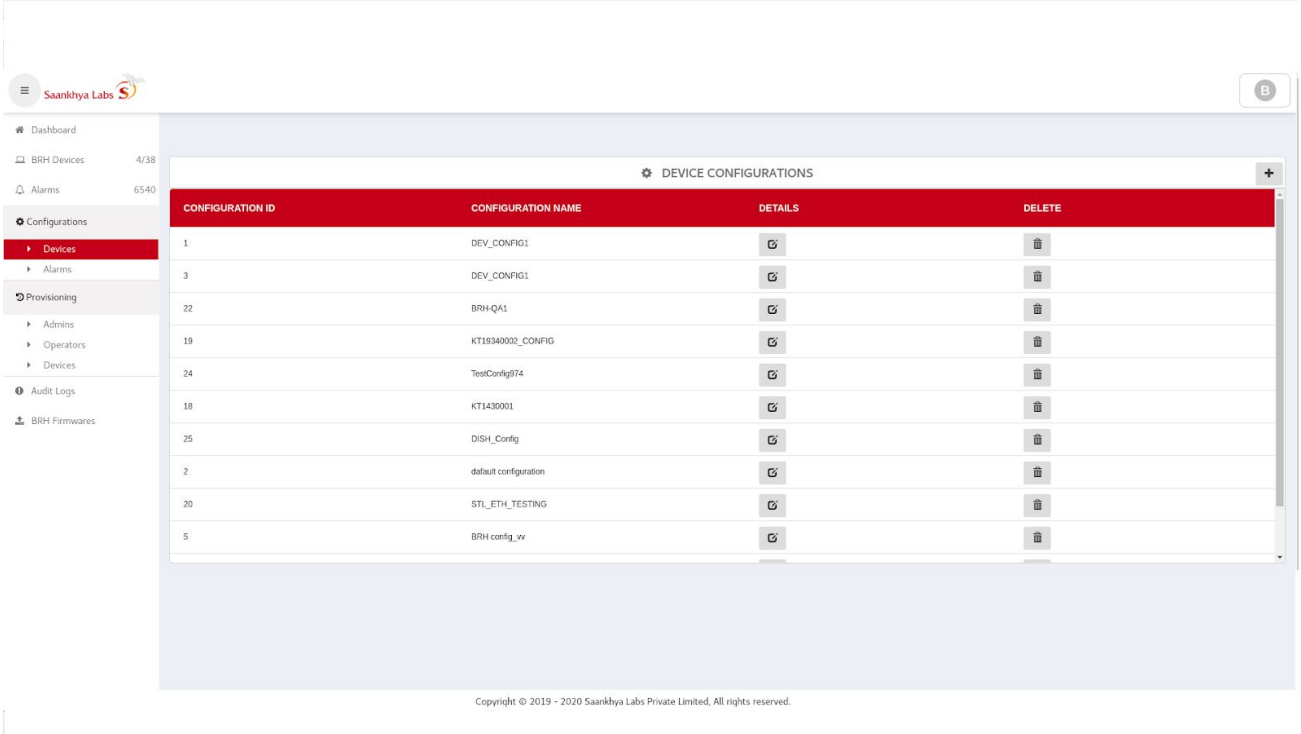
1) Navigate to the Configurations -> Devices sub-menu and click on + sign to create a new configuration



Note: FCC Configuration is available only in devices with latest firmware and for the user with Owner privilege.

⚠ Warning : CW mode is strictly to be used in a controlled environment, And is intended to be used for FCC testing purposes only.

Device Configuration, if added, is shown successfully.



2) Fill in the appropriate values of the configuration as indicated in the table below

Supported Values are as below

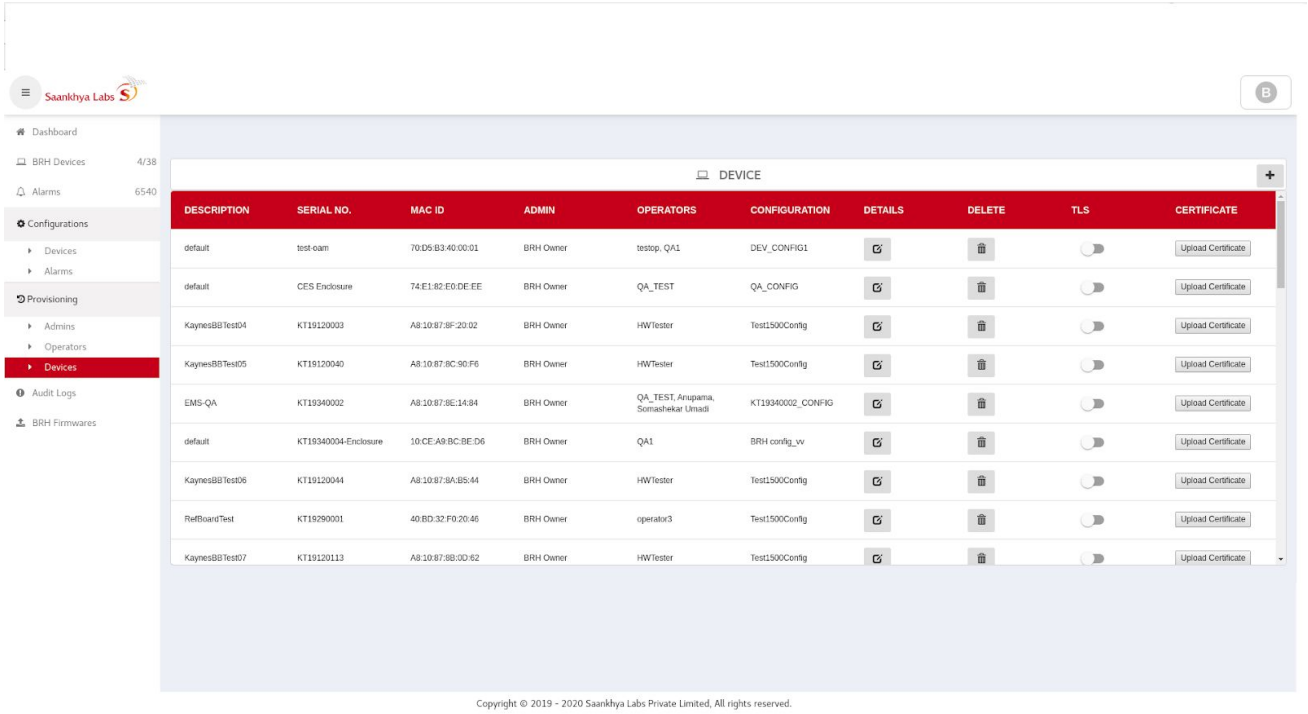
Component	Parameter	Value type	Value range	Comments
DVBS2	Center Frequency (MHz)	Float	950-2150Mhz	In 100 KHz step
	Symbol rate (MSPS)	uint32	1000000-40000000 Samples/sec	
MPE	PID	uint16	0 - 8191	
Operations & Management STL-TP				
Source - Ethernet	Multicast IP	uint32		239.127.1.0
	Multicast port	uint16		4000
Source - DVBS2 (ARM)	Turner Voltage	unit32_t	“RHCP_13V” “LHCP_18V” “RHCP_13V_22kHZ” “LHCP_18V_22kHZ”	None

FCC Configuration	CW mode		"off" "on"	When CW mode is "off" the BRH unit will transmit an ATSC3.0 signal. When CW mode is "on" the BRH unit will transmit a continuous waveform signal with center frequency 725Mhz; With transmission power fixed at 37dbm/5Watt.

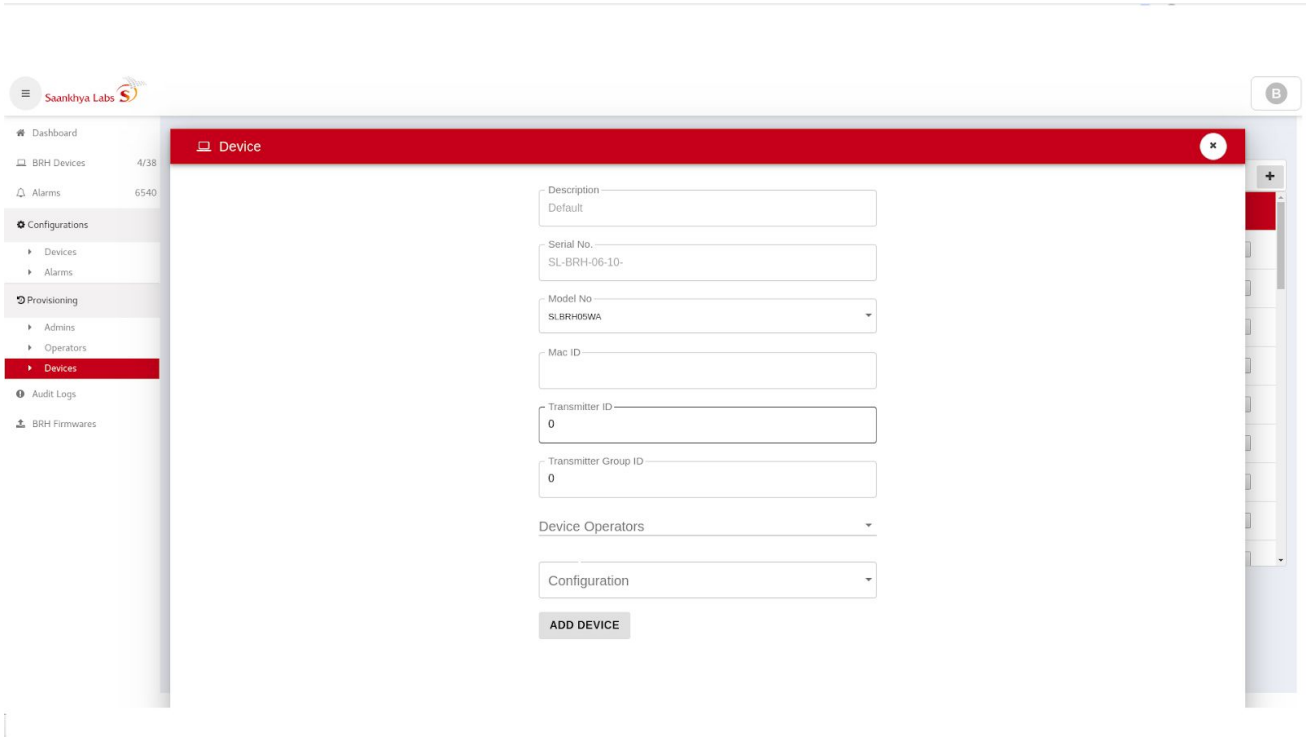
Table 2: Boot Time Configuration Options

Provision a Device

1) Navigate to Provisioning -> Devices submenu and click on the + icon as shown below



2) Add the relevant device information as shown below

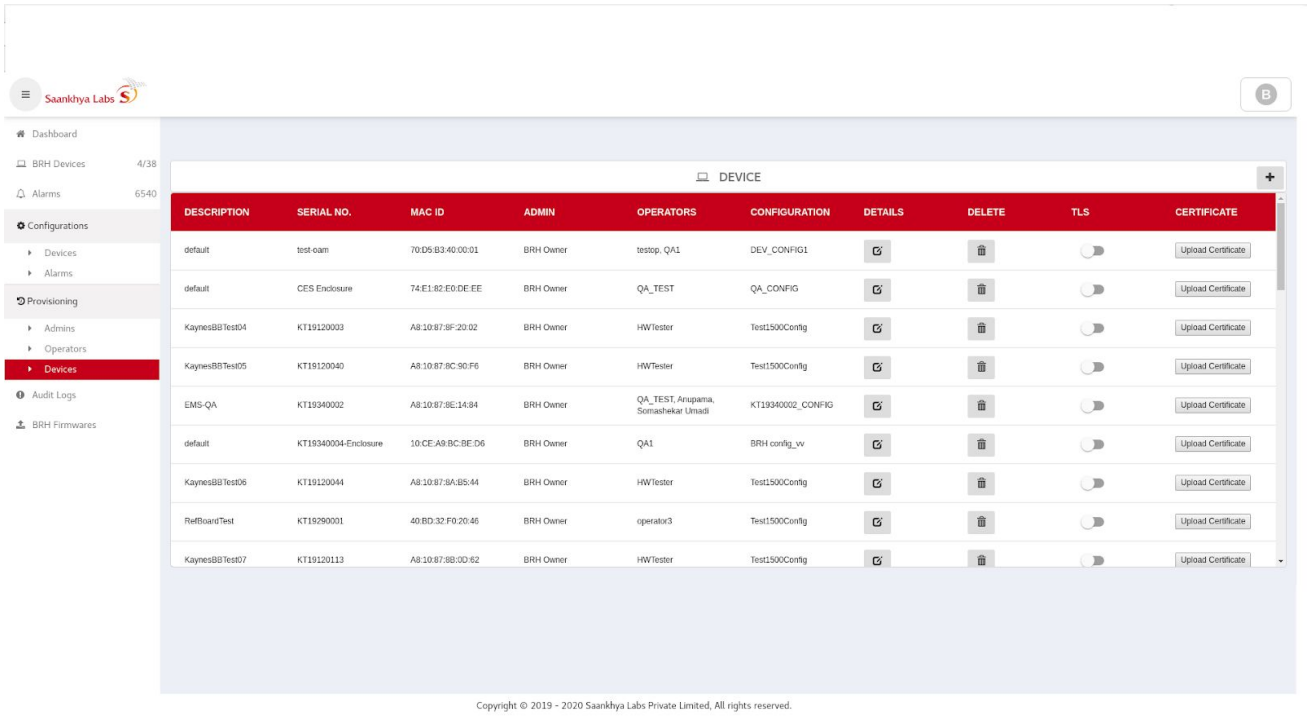


The parameters are as discussed below

Parameter	Type	Valid range	Comment
Serial Number	ASCII string		SLBRH05W-TX725-11-A-XXXXX
Model No	Drop down	SLBRH05WA	
MAC ID	ASCII String		MAC ID in AA:BB:CC:DD:EE:FF format
Operator	Drop down list of Operators.	Operators configured for this owner	
Configuration	Drop Down list of Config Names	Configurations created for the devices.	
Transmitter group id	uint16	0-127	
Transmitter id	uint32	0-8191	

Table 3: Device Provisioning Options

3) On successful addition, the device should be listed in the devices page

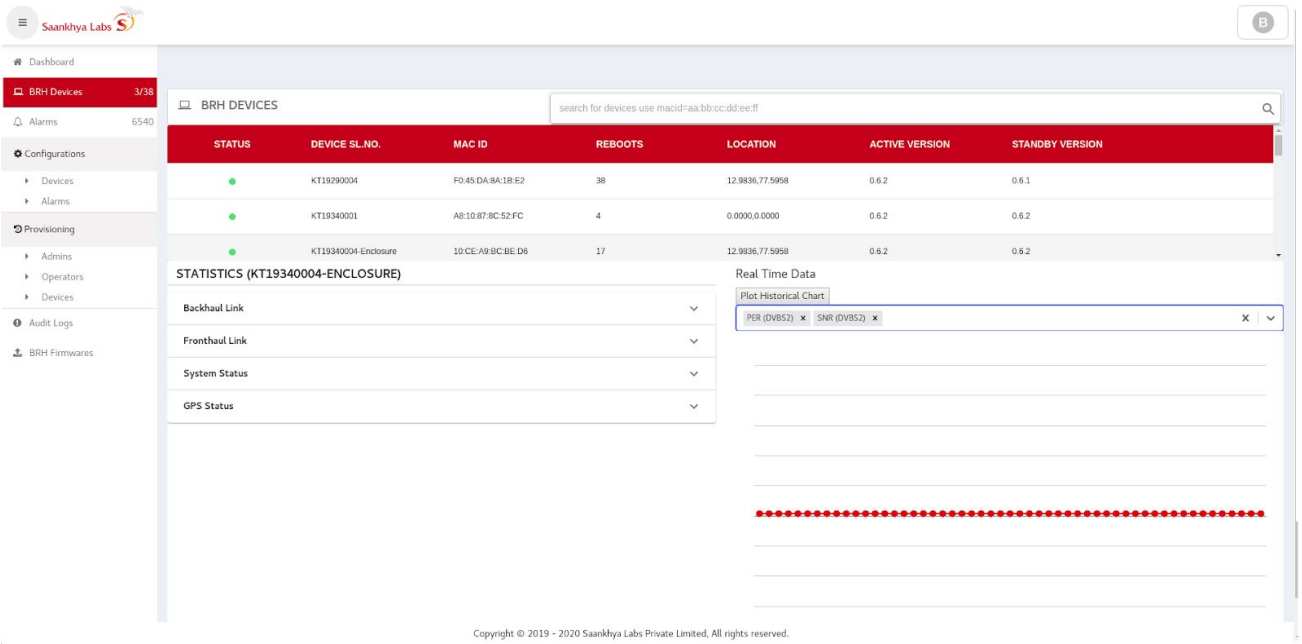


Boot-up the Device

Once the device is provisioned, it is ready to be connected to the network. Power on the device and ensure that the device has network connectivity. The device should initiate contact with the EMS server. The change in the states of the device is observed on the status icon as shown in Figure above.

Wait for the icon to turn green indicating device is now functional

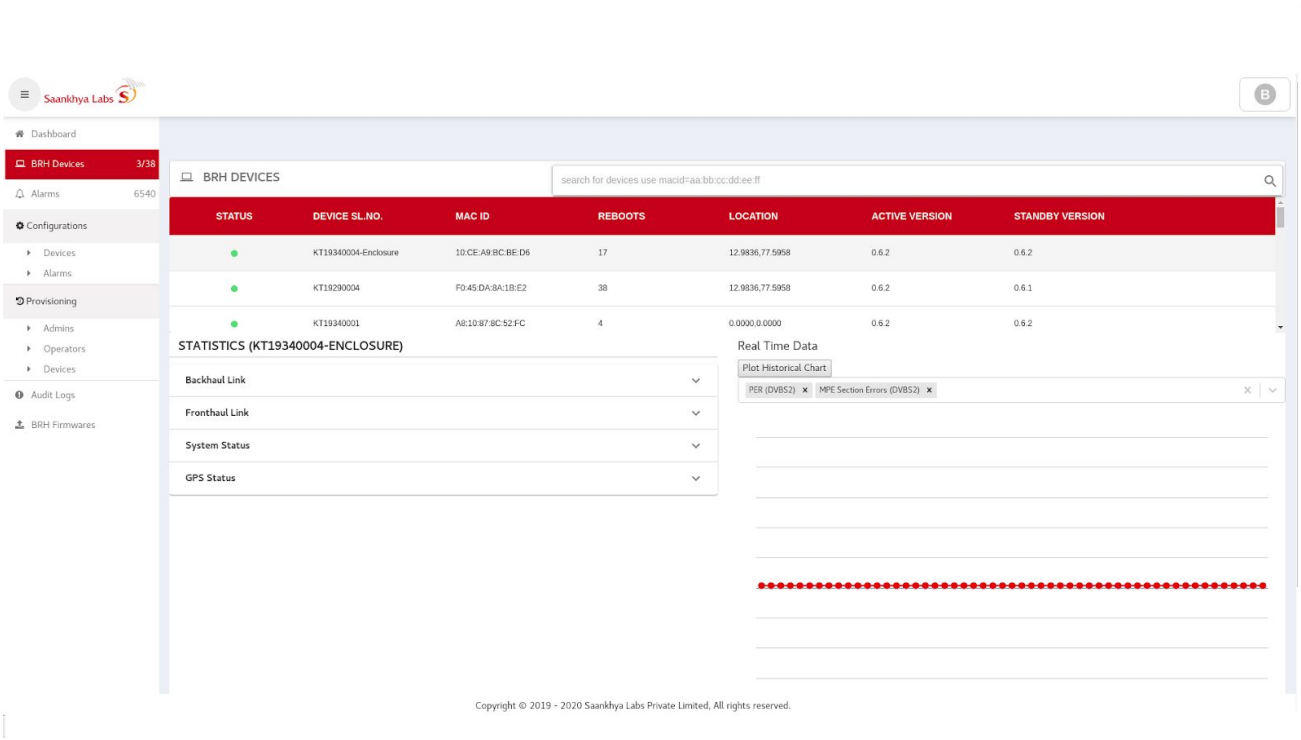
When the device is operational, Device Status, Serial No., MAC ID, Reboot Counts, Location and Active/Standby software versions of the device are shown on EMS as below -



Monitoring Device Statistics

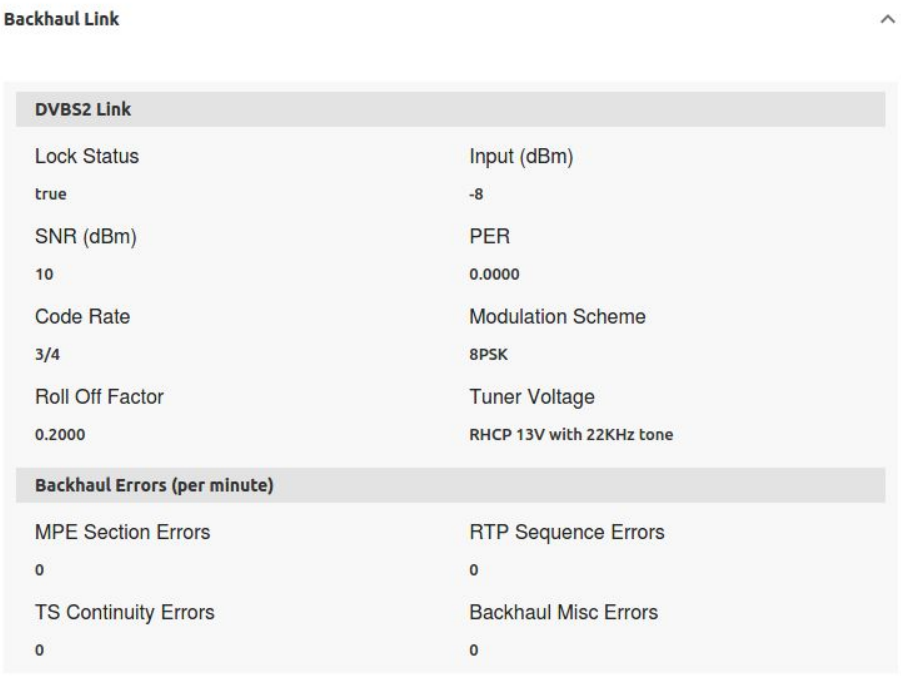
Once the device is operational, device statistics can be monitored from the EMS UI.

1) Navigate to BRH Devices and click on the device to be monitored



2) Details of each of the statistics that are supported are captured below

a Backhaul Statistics

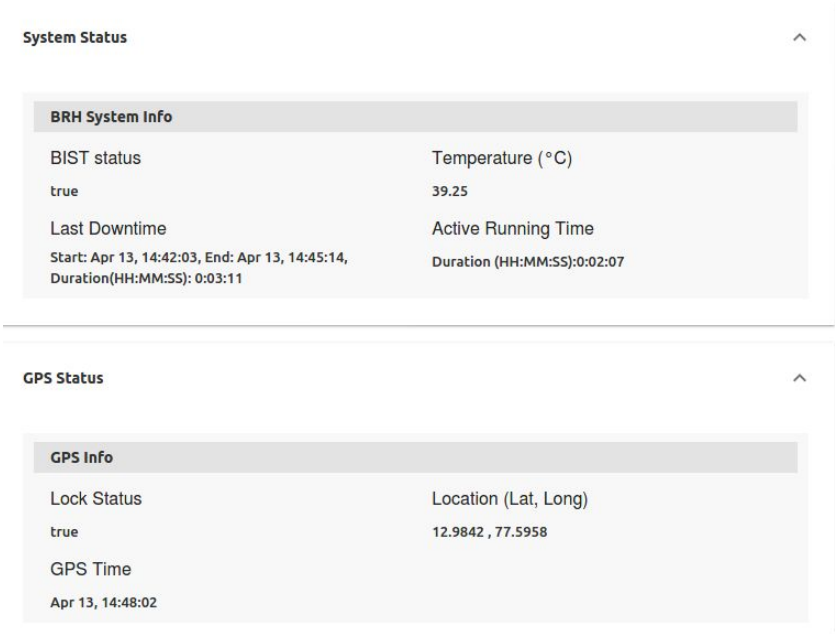


b Fronthaul Link Statistics

Fronthaul Link

Pipeline Scheduler	
Current Sampling Rate (Msps)	**6912**
Last Pkt Proc Latency (µSec)	**129.0000**
STL-Out Rate (Frames/Sec)	**277**
Emission Rate (Frames/Sec)	**281**
Buffered Jitter Frame Count	**590**
Transmitter Status	
Transmission Power	**37dBm/5W**
Transmission Frequency (MHz)	**725.0**
BB Board TX Gain (dB)	**-6.50**
RF Transmission	**On**
Subframe 0 Parameters	
FFT Size	**8K**
Guard Interval	**GI5_1024**
Pilot Config	**SP3_4**
Subframe0: PLP 0	
Code Rate	**11/15**
Modulation Scheme	**16QAM-NUC**
Outer Parity Type	**BCH**
LDPC Length	**64800**
LDPC Type	**Type-B**

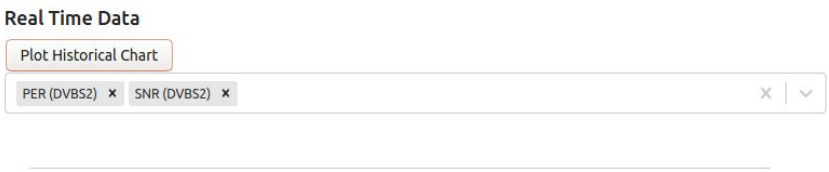
c System and GPS Statistics



3) It is possible to monitor real time values for different statistics graphically. Please select the value(s) to be plotted and then the values appear along with their plot in the area for the plot.

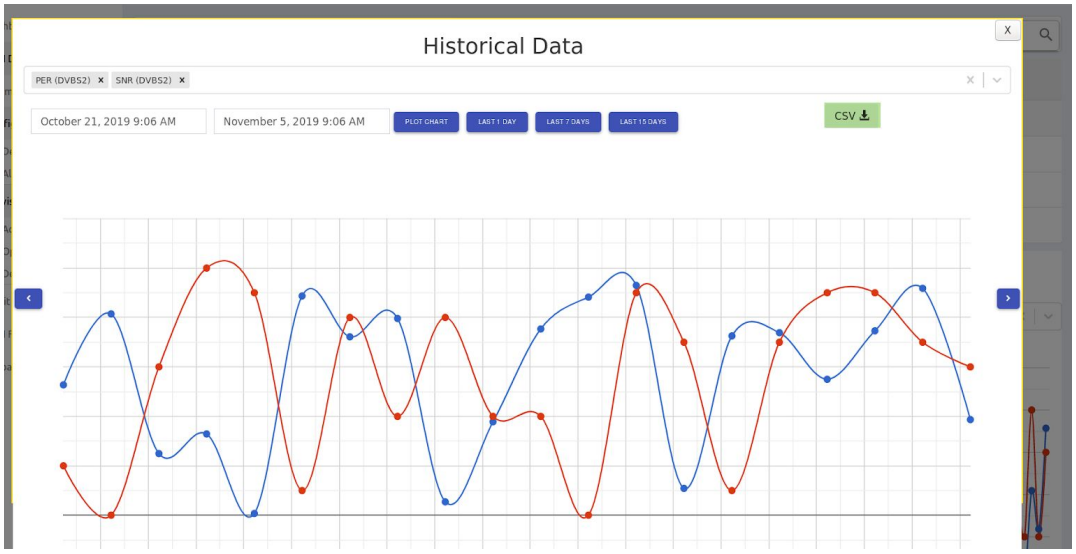
4) It is possible to plot historical data by clicking “Plot Historical Chart” button. A historical chart window pops up. It is possible to plot using user selected time intervals. Also, pre-configured buttons for 1day, 7day and 15day historical data is available. The historical statistics data can be downloaded as a CSV file.

a Click “Plot Historical Chart”



b Historical Char Dialog as below pops up

c It is possible to download historical data as a CSV.



Configuration of Device Alarms (Notifications)

Notifications are triggered from the BRH Device under deviation from expected behaviors. These notifications are displayed in the EMS as Alarms. Alarms provide a window into the health of a given BRH Device as well as across several BRH devices across the network.

Alarms that will be generated are system defined and are captured in the table below. Actions that can be taken as well as severity level of a given alarm are user configurable. This allows EMS Owner to customize actions that can be performed as per the requirements of a particular installation. The configuration is system wide and applies to ALL devices. In the current version of the EMS, creation of User Defined Alarm Configurations (for the alarm sources that are not yet supported by the system) is not supported. Instead, a flexible mechanism that allows configuring Severity/Automatic acknowledgement of alarms etc. is provided. This section provides an overview of this configuration. Discussed below are the default severity levels for the alarms. Actual values may be changed by the Owner and what is reflected in the page is current settings of the alarm severities.`

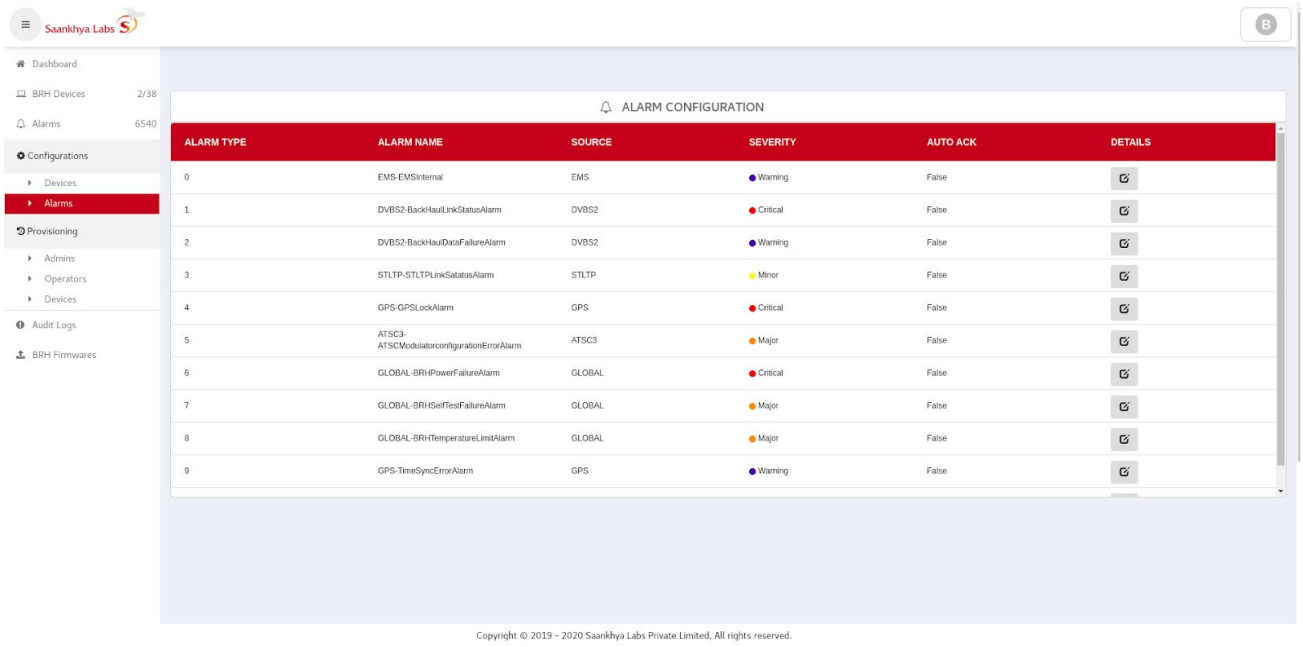
EMS Supported Alarms

Type	Name String	Source	Severity	Auto ack
0	EMSInternal	EMS	Warning	False
1	BackHaulLinkStatusAlarm	DVBS2	Critical	False
2	BackHaulDataFailureAlarm	DVBS2	Warning	False
3	STLTPLinkStatusAlarm	STLTP	Minor	False
4	GPSLockAlarm	GPS	Critical	False
5	ATSCModulatorconfigurationErrorAlarm	ATSC3P0	Critical	False
6	BRHPowerFailureAlarm	GLOBAL	Critical	False
7	BRHSelfTestFailureAlarm	GLOBAL	Critical	False
8	BRHTemperatureLimitAlarm	GLOBAL	Critical	False
9	TimeSyncErrorAlarm	GPS	Warning	False
10	Reboot	GLOBAL	Info	False

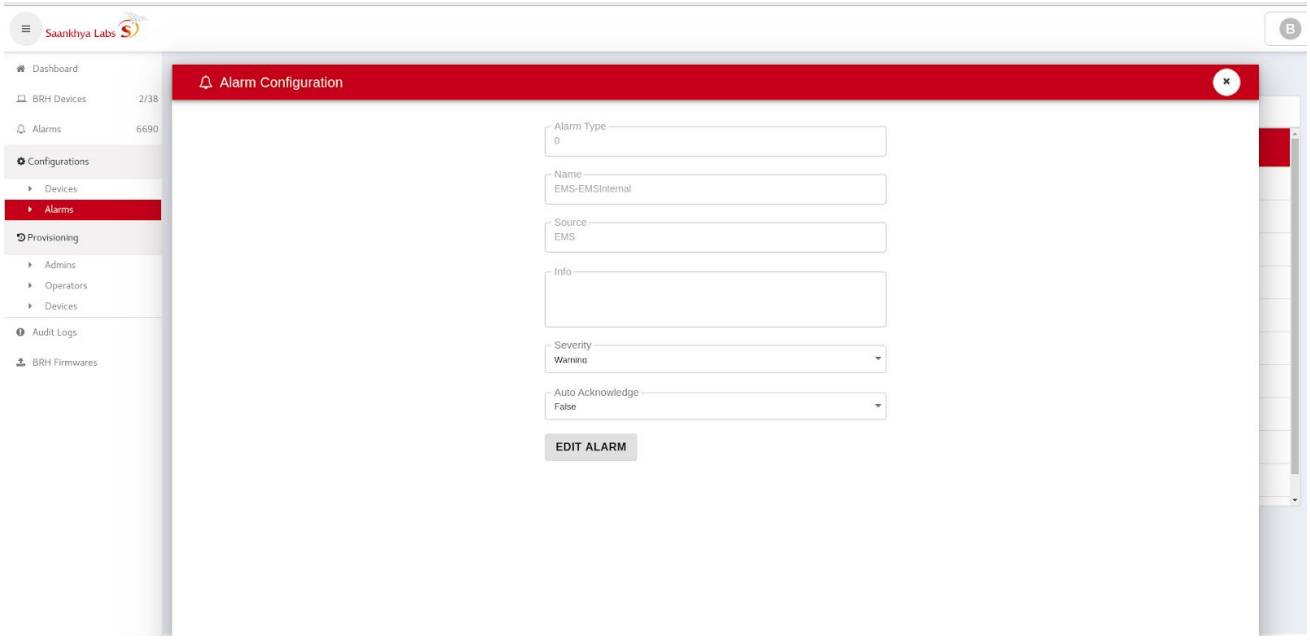
Table 4: Alarms Configuration Definitions

“Owner” role privilege is required to be able to configure changes in Alarms (Notifications) severity as well as changing ‘Auto-Acknowledge’ behavior of a given alarm.

1) Navigate to Configurations and then click Alarms sub-menu. This should display a list of system supported Alarms and their current configuration. Clicking on “Details” button Opens a dialog to view details of an individual alarm.



2) Details of a given System Supported alarm are as shown below. Once changes are performed to Configuration, the changes can be saved by clicking the “Edit Alarm” button.

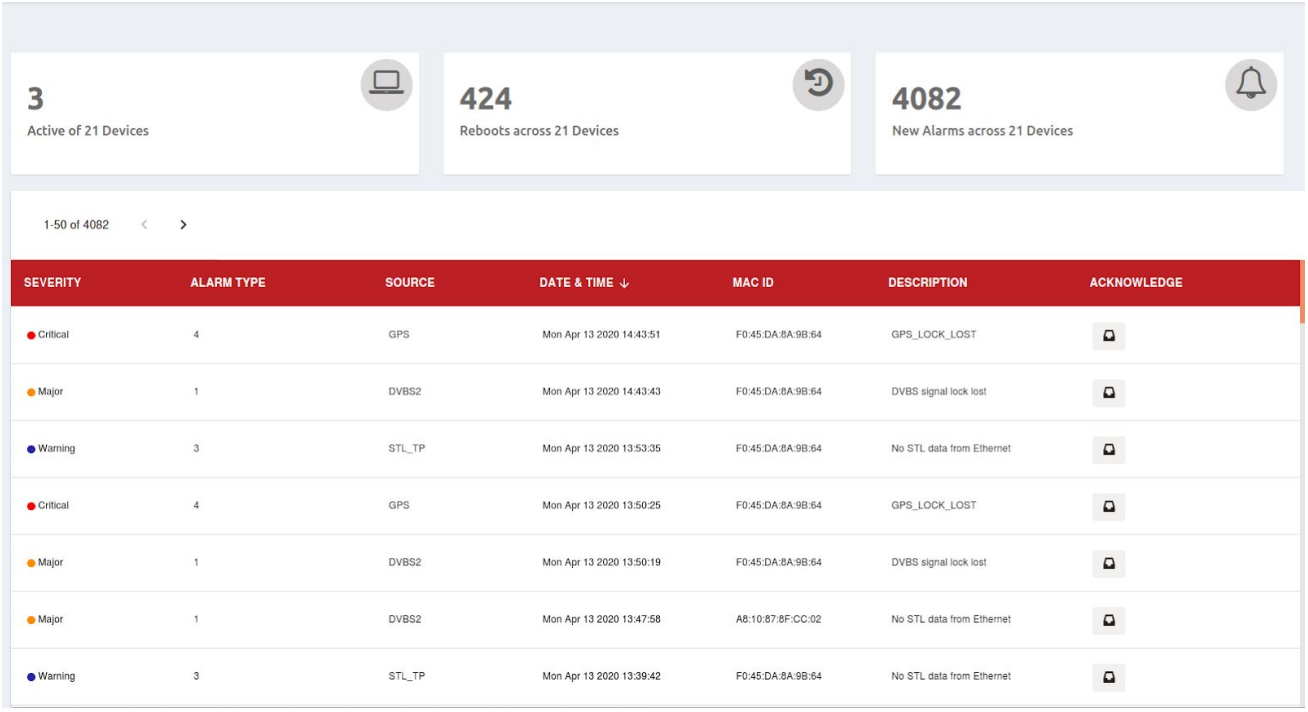


Alarms - Monitoring and Acknowledging

Generated Alarms that are not automatically acknowledged are visible on Both Dashboard and Top Level Alarms page. Dashboard being the landing page of the application, user actionable things are available on the dashboard.

Also an alarm "clear" functionality is implemented in the EMS. When a device reports that a given alarm condition no longer exists, the previously generated alarm is moved to a new state called "Cleared" and is not required to be explicitly required to be "Acknowledged". Alarms that are automatically "cleared" are no longer visible on the Dashboard or Alarms Submenu.

3) Navigate to Dashboard

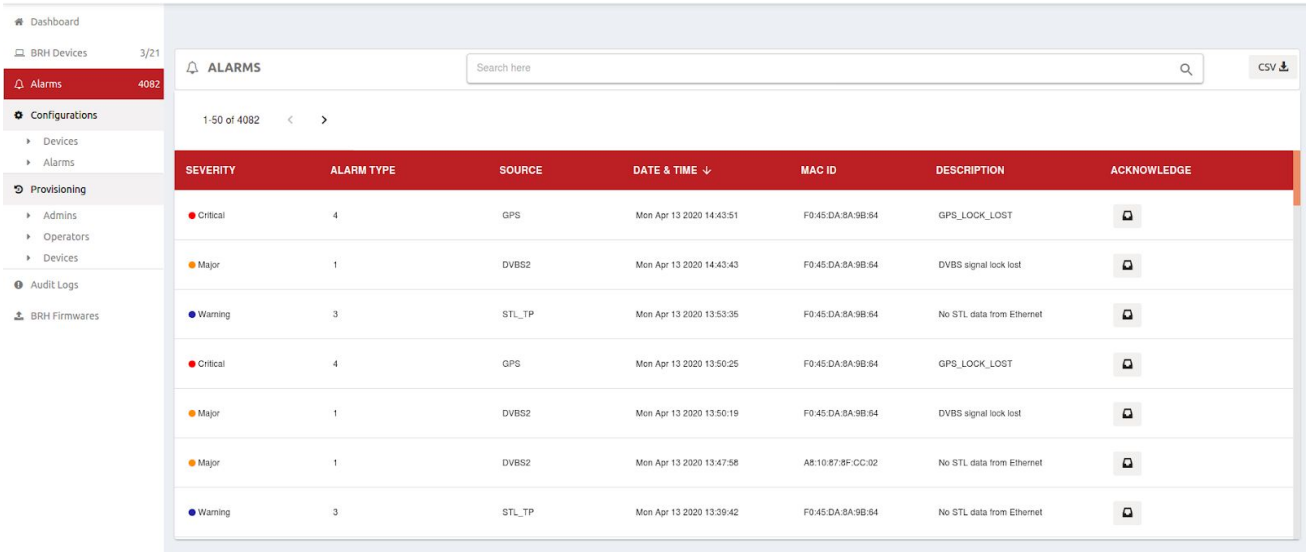


4) Based on the severity the color of icon changes as indicated in the table below

Alarm Severity	Icon Color
Critical	Red
Major	Orange
Minor	Yellow
Warning	Blue
Info	Green

Table 5: Alarms Severity and Colors

5) Navigate to "Alarms" sub-menu. It is possible to Acknowledge alarms that are unacknowledged or are not cleared yet by clicking on the "Acknowledge" button.



6) Alarms can be filtered using different filtering criteria -

- Alarm source
- MAC ID of the device
- Severity (See values in the Table 5 above.)
- Time based filtering (last n days/ n hours)

Alarms - Downloading Historical Data

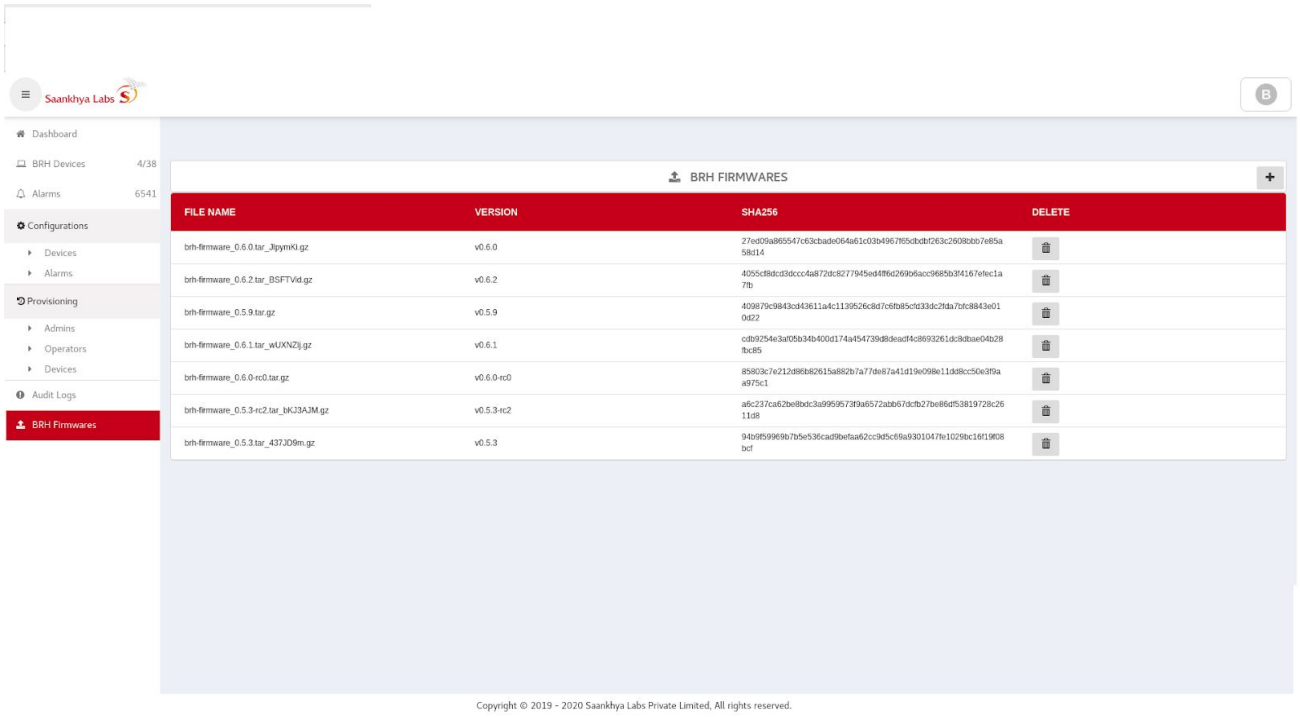
It is possible to download historical data for the alarms up to 30 days prior at-least. Note: in some cases additional data may also be available. This data can be downloaded by clicking on the “CSV” button on the alarms page. This data contains all the alarms that are generated, including alarms that are automatically cleared and alarms that are explicitly acknowledged by the user as above.

Device Actions

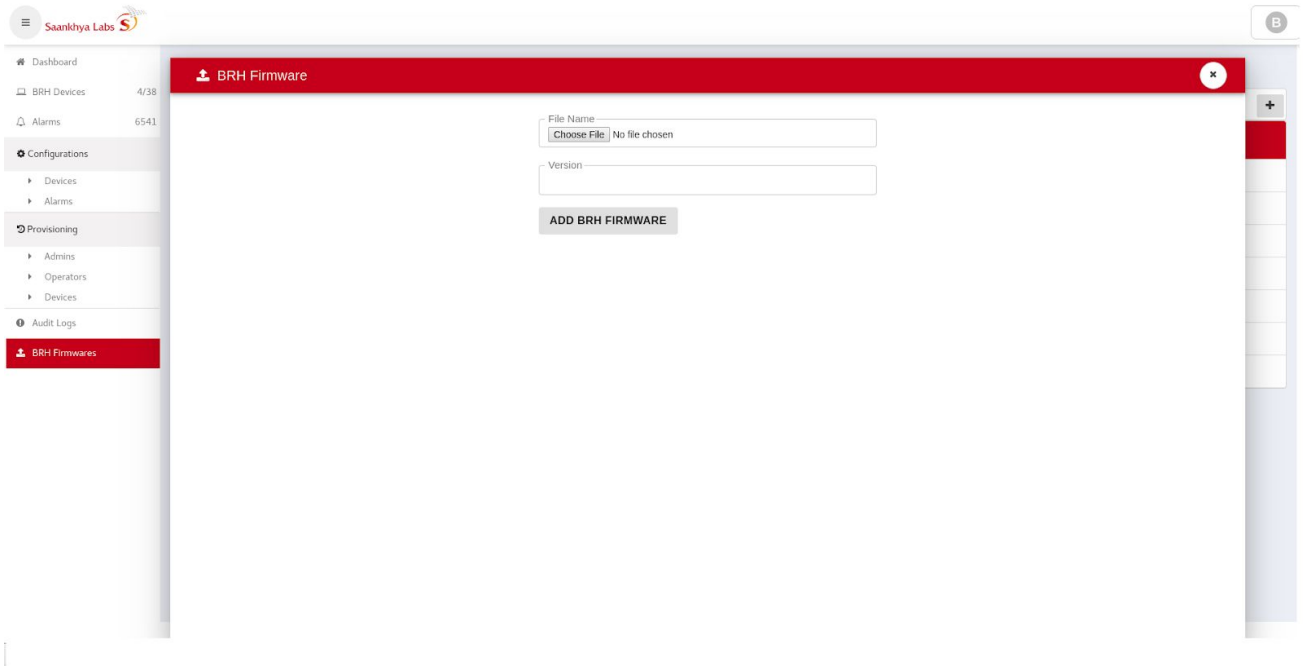
Upgrading BRH Software

EMS Supports remote Upgrade of BRH Device Software. Upgrading the software is a two step process. First the new firmware needs to be uploaded to EMS. Once the new firmware is uploaded, A user can go to a device and then upgrade an individual device with a given firmware.

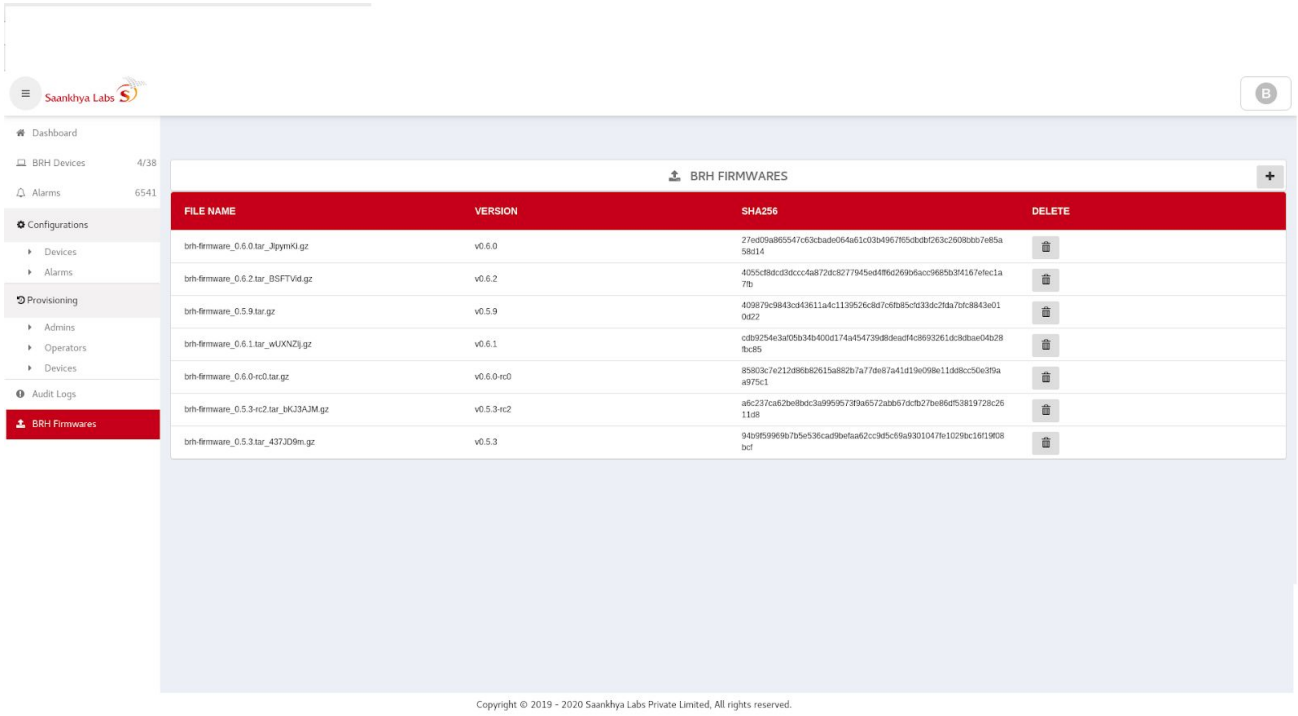
1) Navigate to BRH Firmwares and Click “+” to add a new Firmware. This will open a dialog to upload firmware to EMS.



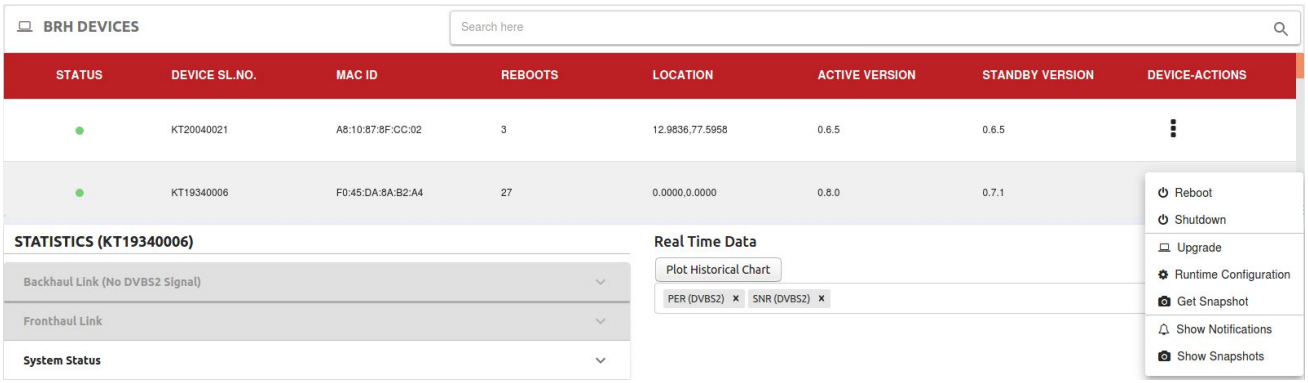
2) Click on choose file to select firmware, and add version.



3) On successful addition, the firmware should be visible in the list of BRH Firmwares.



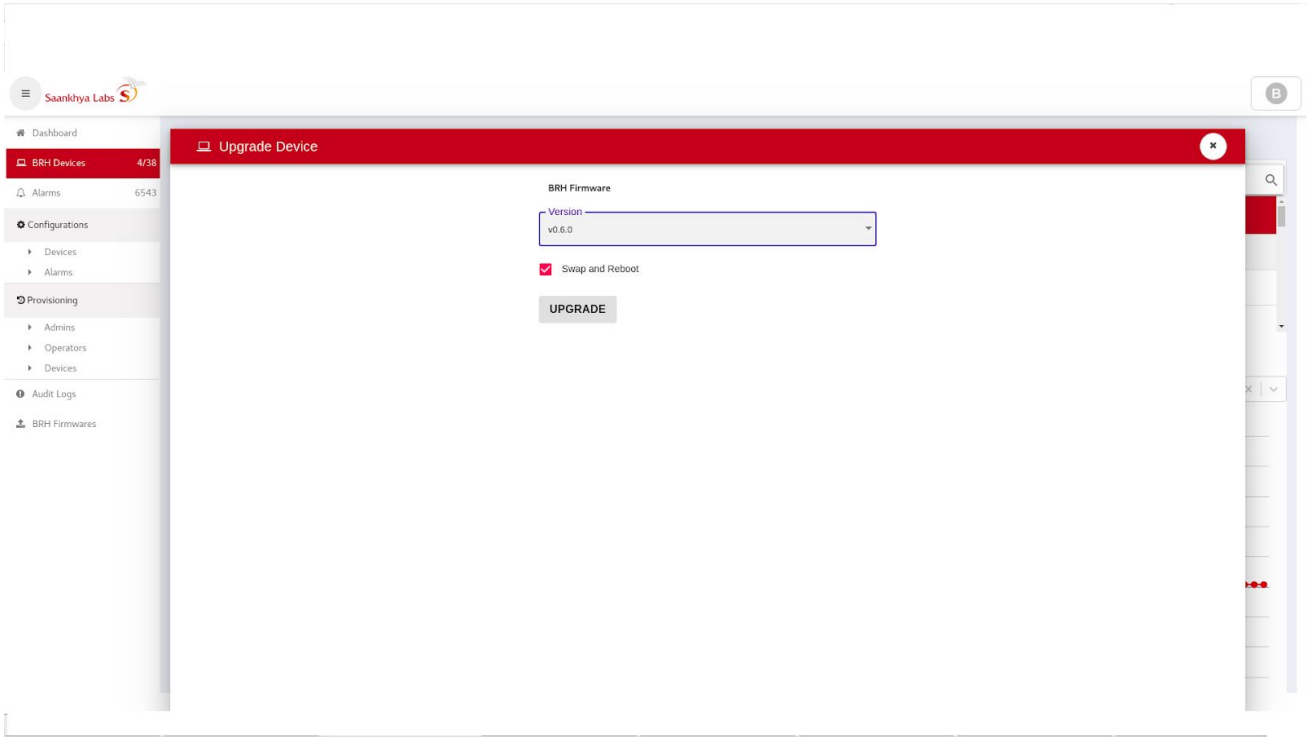
4) Navigate to BRH Device and click on more, and select software upgrade from the drop down menu.



Note: Some Options may be available only on devices with latest firmware and they are also available only to a user belonging to a certain role. (eg. Snapshot Related options are available only on device with latest firmware only for the users belonging to Owner Class.)

5) In the dialog that is shown, Choose the firmware that is to be uploaded. In the current version of EMS, once “Upgrade” is requested, device automatically swaps the active partition and reboots in a new firmware.

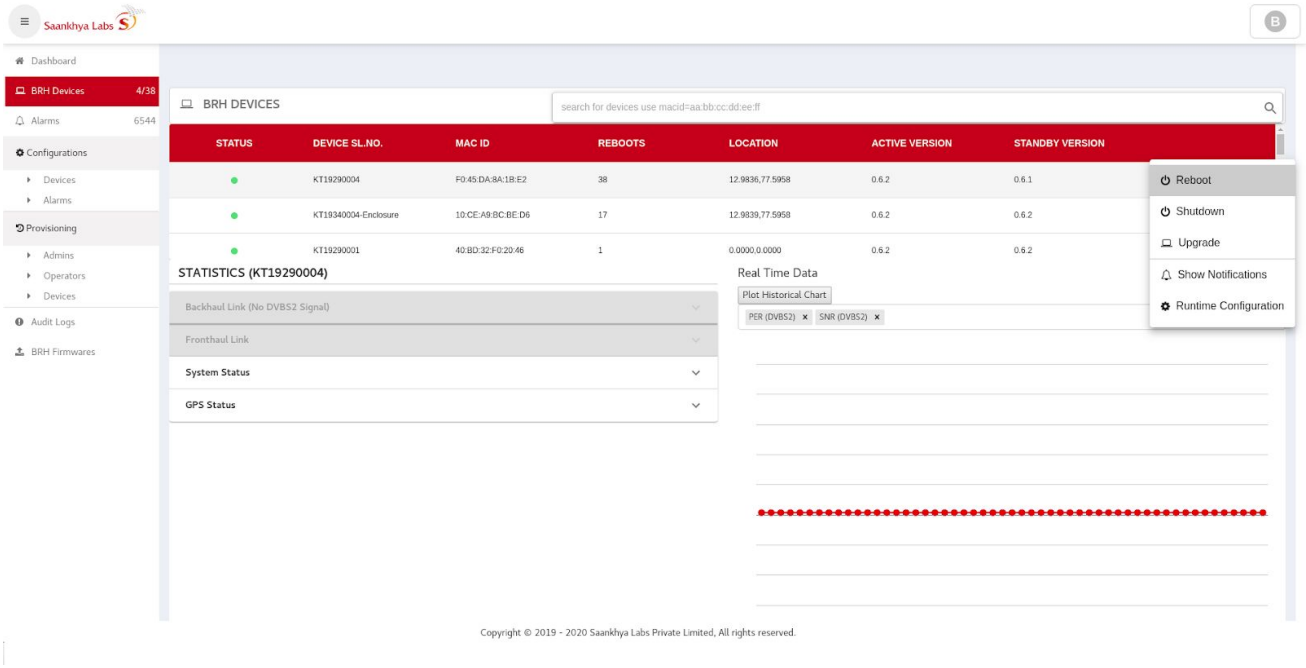
6)



Once Firmware upgrade is triggered, User will be notified of success or failure of the triggered action. The result of triggered action is also captured in the Audit Logs. Upon successful Upgrade the “active” and “standby” version of the device software are updated.

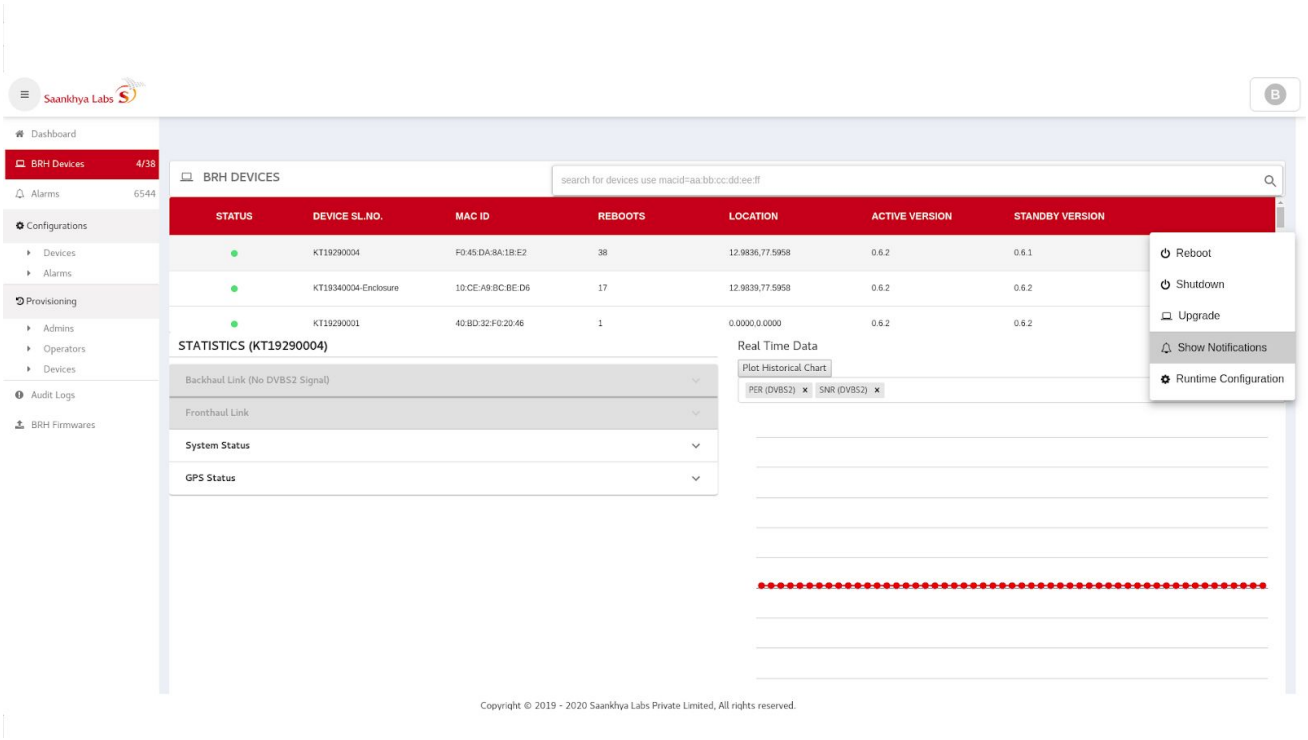
Rebooting Device

1) Navigate to BRH Device and click on more, and select Reboot from the drop down menu and Confirm.

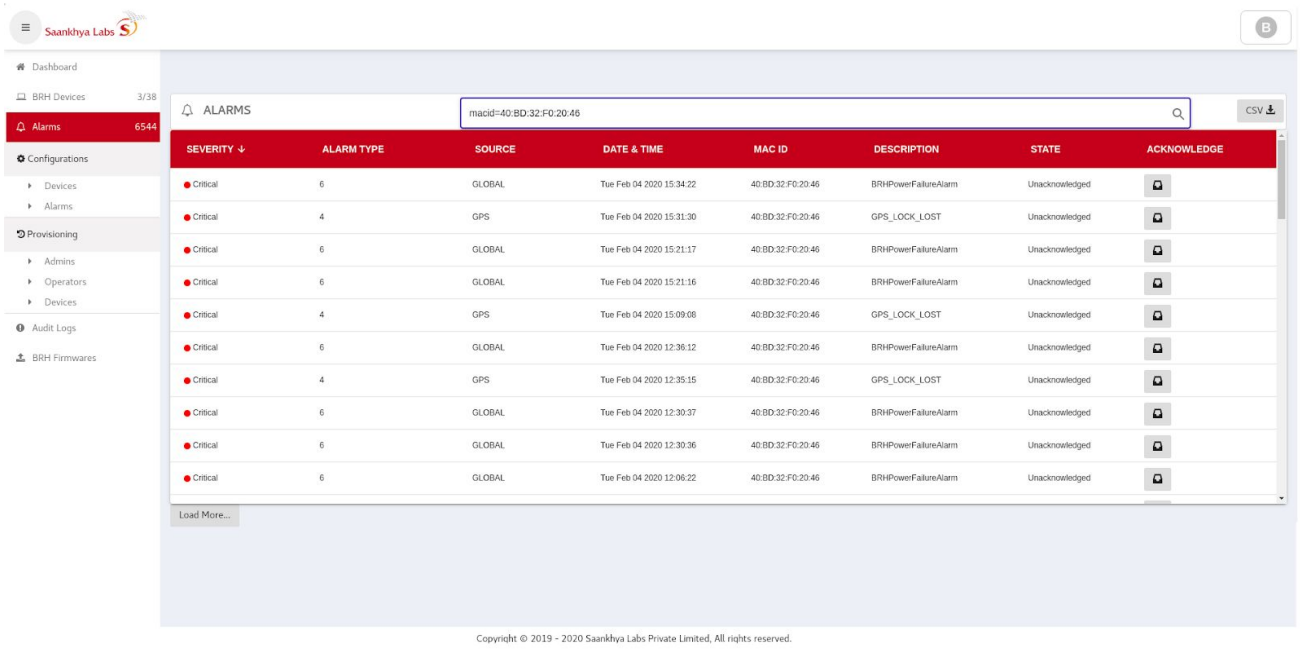


Viewing Device Notifications (Alarms)

1) Navigate to BRH Device and click on more, and select Show Notifications from the drop down menu.



2) Alarms TAB is shown with filter set to Device MAC Address



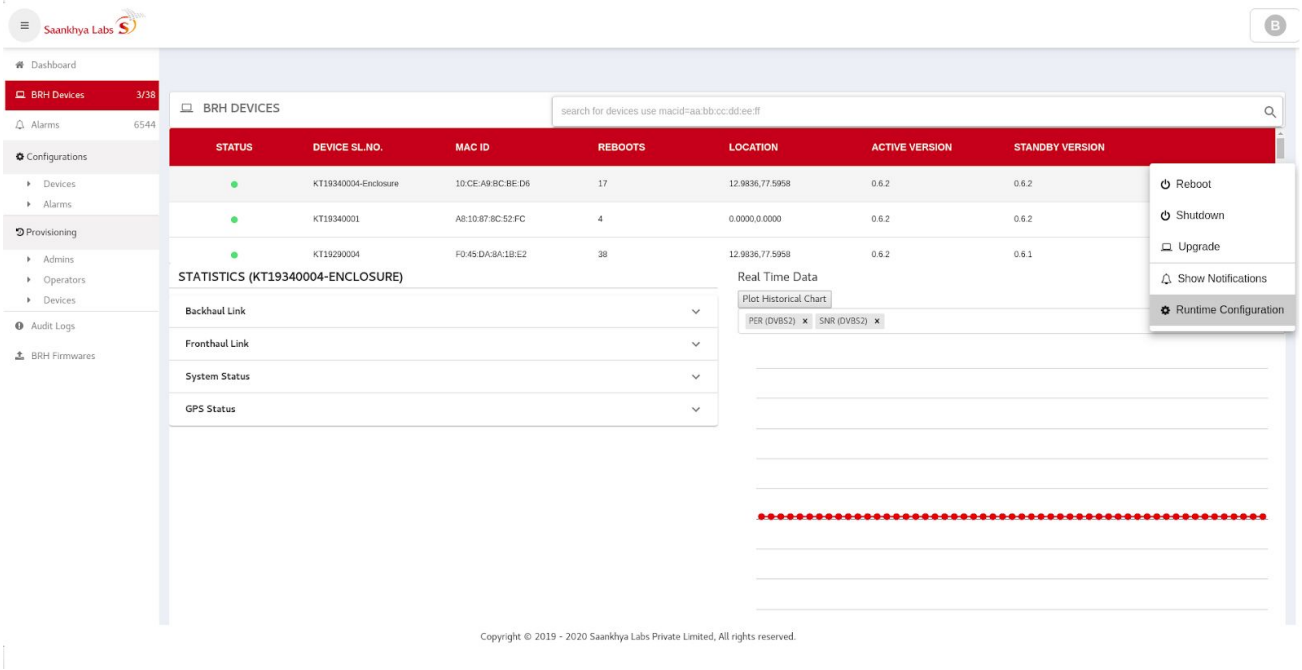
Updating Runtime Configs

Runtime configuration of a BRH device can be upgraded through an action provided on “BRH Devices” Page.

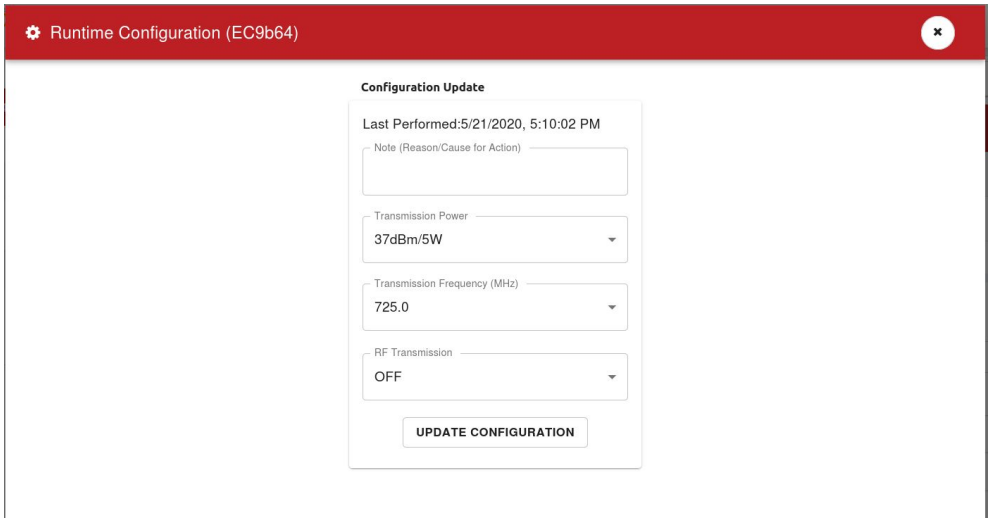
The following RF Transmission parameters can be updated during runtime once the device has connected to EMS:

- Transmission Power can be configured between 37dbm/5Watt and 30dbm/1Watt.
- Transmission Frequency(Mhz) can be configured to 725.0 Mhz.
- RF Transmission can be configured to "on" to enable RF transmissions or "off" to mute RF transmissions.

1) Go to “BRH Devices” Page and Open device specific Context Menu and click “Runtime Configuration”, a Dialog will appear.



2) Click on “Update Configuration” after selecting the right frequency and Power Level.



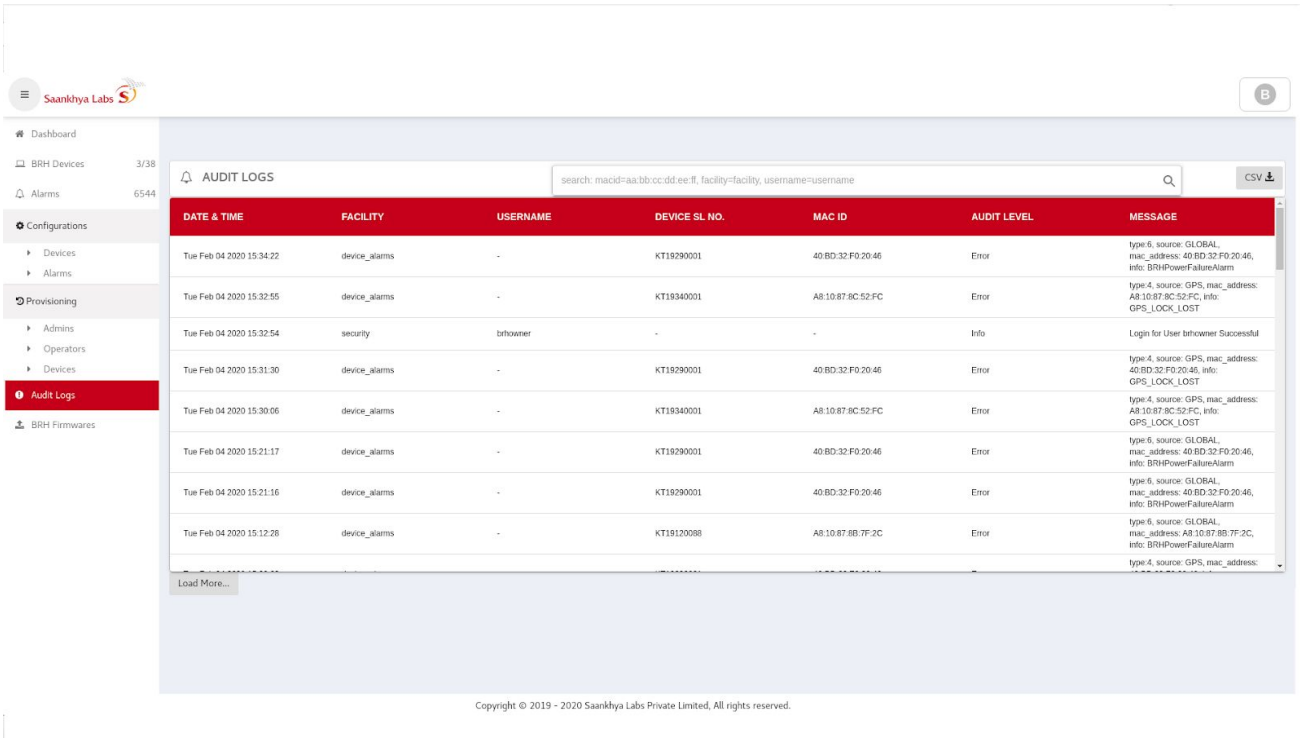
Note: Ability to control RF Transmission will be available for only devices with latest firmware versions. For devices with older firmware versions, the default choice is On.

3) The updated configuration will be applied to the device and a result of success or failure will be logged in the audit logs.

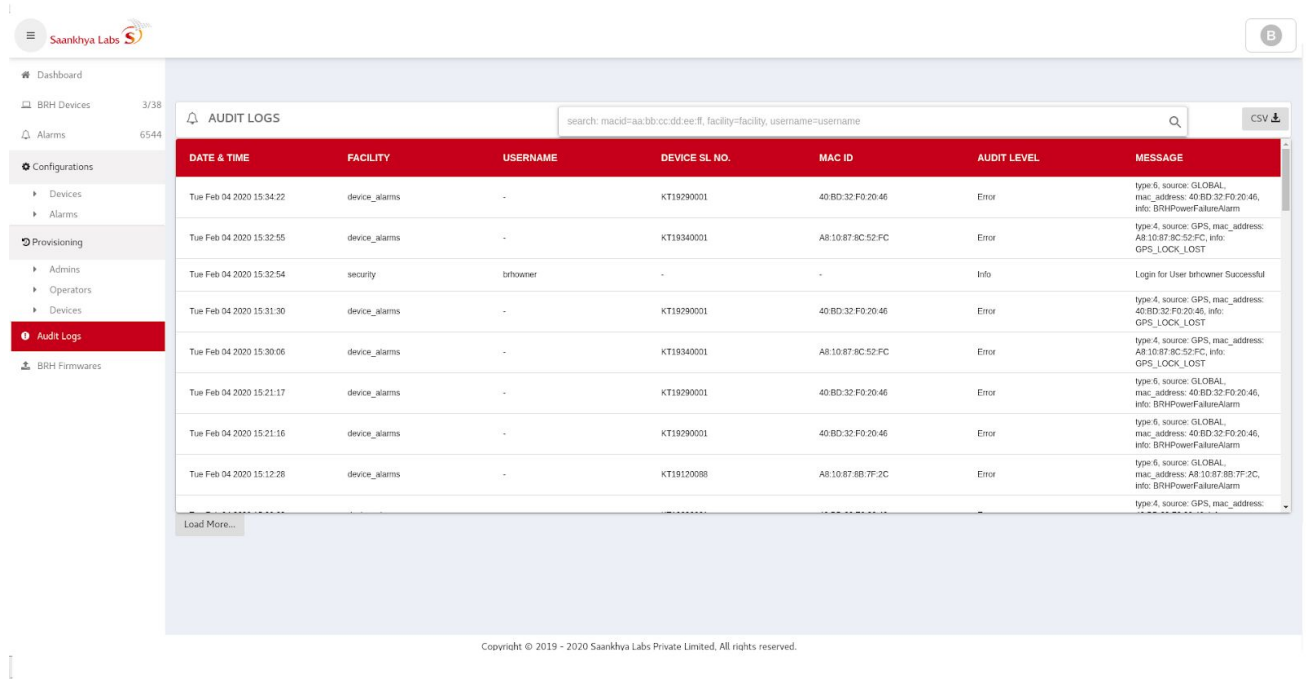
Monitoring Audit logs

Audit logs provide a window into actions performed by Users as well as Alarms/Events generated at the device and thus it is a single pane where all the activities / events can be observed. User with “Owner” and “Admin” roles are able to view audit logs.

1) Navigate to Audit Logs for monitoring device logs.

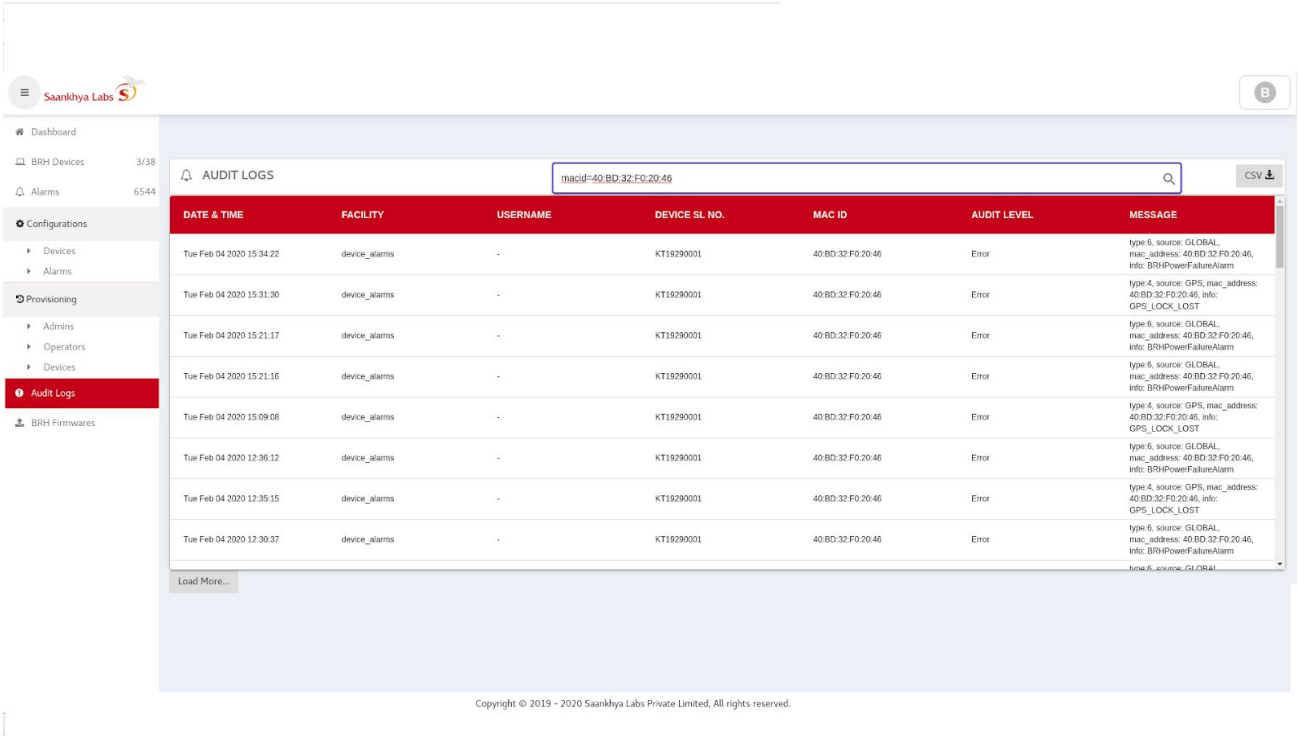


2) Audit logs can be viewed in pages. All the historical audit logs generated can be downloaded as a CSV File by the user by clicking the “CSV” button.



3) It is possible to filter audit logs using following filtering criteria -

a username (User that triggered the option)
b deviceid (Devices for which action was triggered)
c facility (Security - login etc. or device_tasks - Reboot/Upgrade etc.)



Device Snapshots

This feature is available for users with “owner” privileges. Using this feature it is possible to collect logs at a device from the EMS. Note: This feature consumes a lot of upstream bandwidth at the device end and should only be used sparingly only for debugging purposes. In the normal flow of operations, it is recommended to not use this feature. Please contact EMS Support if you are required to use this feature and EMS support should guide you about using this feature.

Appendix A – Roles and Actions Allowed

Operation	Owner	Admin	Operator
Create Admin	Yes	Yes	No
Edit Admin	Yes	No*	No
Disable Login for Admin	Yes	No	No
Delete Admin	Yes	No	No
View Admin Details	Yes	Yes	No
Create Operator	Yes	Yes	No
Update Operator	Yes	No	No*
Delete Operator	Yes	Yes	No
Disable Login for Operator	Yes	No	No
View Operators	Yes	Yes	No*
Create Device Configuration	Yes	Yes	No
Update Device Configuration	Yes	Yes	No
View Device Configurations	Yes	Yes	Yes
Delete Device Configurations	Yes	Yes	No
Create Alarm Configuration	No	No	No
View Alarm Configuration	Yes	Yes	Yes
Update Alarm Configuration	Yes	No	No
Delete Alarm Configuration	No	No	No
Create (Provision) Device	Yes	Yes	No
Update Device (Config, Admin and Operators)	Yes	Yes	No
Delete Device	Yes	Yes	No
Acknowledge Device Alarms	Yes	Yes	Yes

Operation	Owner	Admin	Operator
View Device Statistics	Yes	Yes	Yes
View Running Devices List	Yes	Yes	Yes
View Audit Logs	Yes	No	No
Add New Firmware	Yes	Yes	No
View List of Firmwares	Yes	Yes	Yes
Delete Firmware	Yes	Yes	No
Upgrade device with new Firmware (already added)	Yes	Yes	Yes
Reboot Device	Yes	Yes	Yes
Update Runtime Configuration	Yes	Yes	Yes

Table 6: Role Actions

Note :- “*” means A user can view / update his/her own data.

Browser Requirements

Browser versions which support EMS -

Google Chrome Version 75.0.3770.142(Official Build) (64 bit) or above.

Firefox Quantum Version 60.8.0esr(64bit) or above.