Battery Management Systems

battery made simple

www.emusbms.com

EMUS

Remote Monitoring System (RMS)

User Manual 1.0

Contents

RMS Device 4

1 Installation 4

1.1 Wiring 4

1.2 SIM card installation procedure 6

2 Wi-Fi provisioning 9

3 Cellular connection 13

4 OTA Firmware Update 13

5 Factory Reset 13

6 RMS Configuration 14

6.1 Device settings configuration 14

6.2 Parameters configuration 19

7 RMS cyber security 24

7.1 Internet access 24

7.2 Device registration to MQTT server 25

7.3 MQTT data flow 26

7.4 RMS Portal login 26

EMUS RMS Portal guidelines 27

8 Login / Password change 27

9 OTA Firmware Update 28

10 User management 29

10.1 User Groups 29

10.2 Roles 29

10.3 User 30

11 Customers management 31

11.1 Customer groups 31

11.2 Customer 32

12 Devices management 32

12.1 Device groups 32

12.2 Device 33

13 Dashboards management 33

13.1 Dashboard groups 34

13.2 Dashboard 34

14 Entity Management 35
14.1 Entity views groups 35
14.2 Entity view 35
15 Connectivity via TLS 36
15.1 Connection procedure 36

RMS Device

1 Installation

1.1 Wiring

Please proceed to EMUS RMS device installation recommendations which are described in the wiring diagram below. EMUS RMS can be powered using same power-source as an EMUS G1 Control Unit (CU021A).

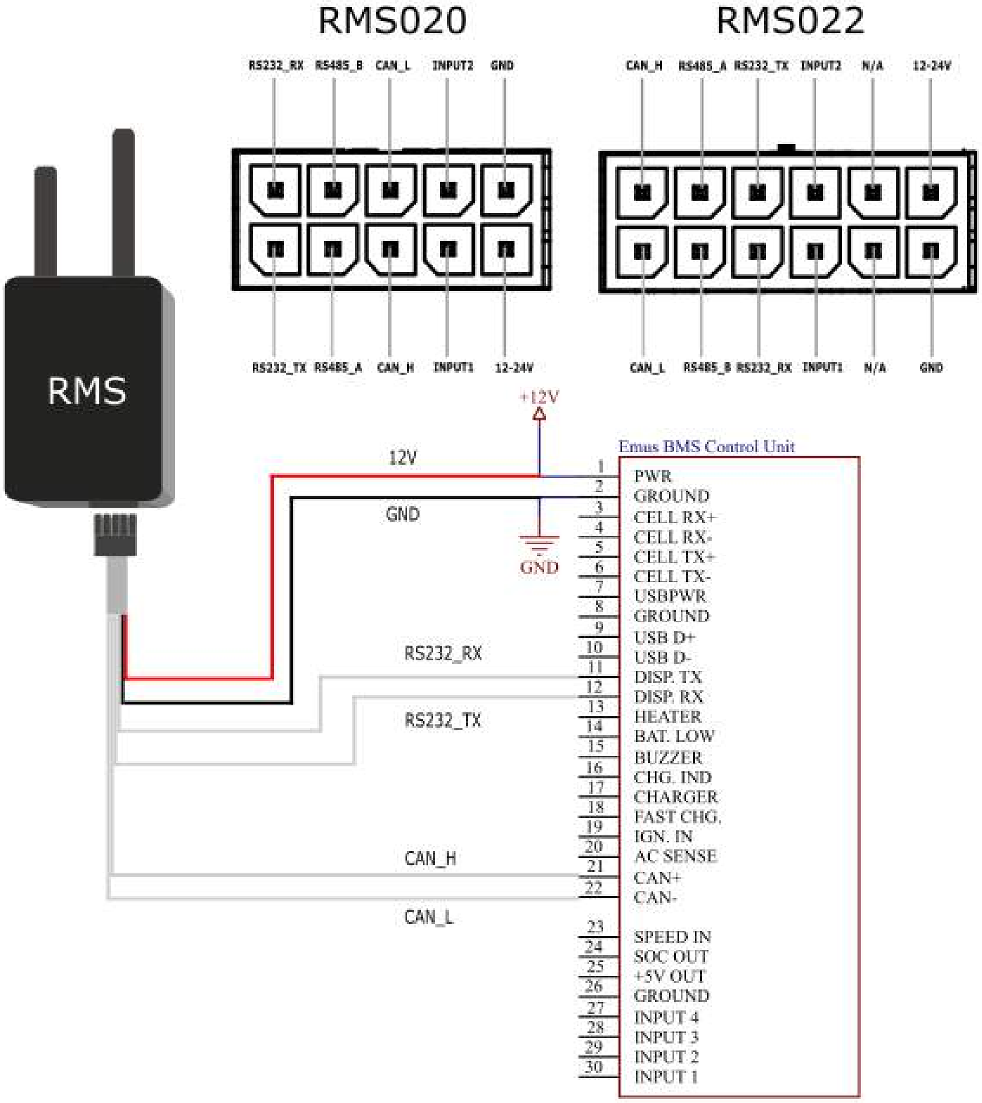


Figure 0-1 RMS020/22 Connection with G1 Control Unit (CU021A)

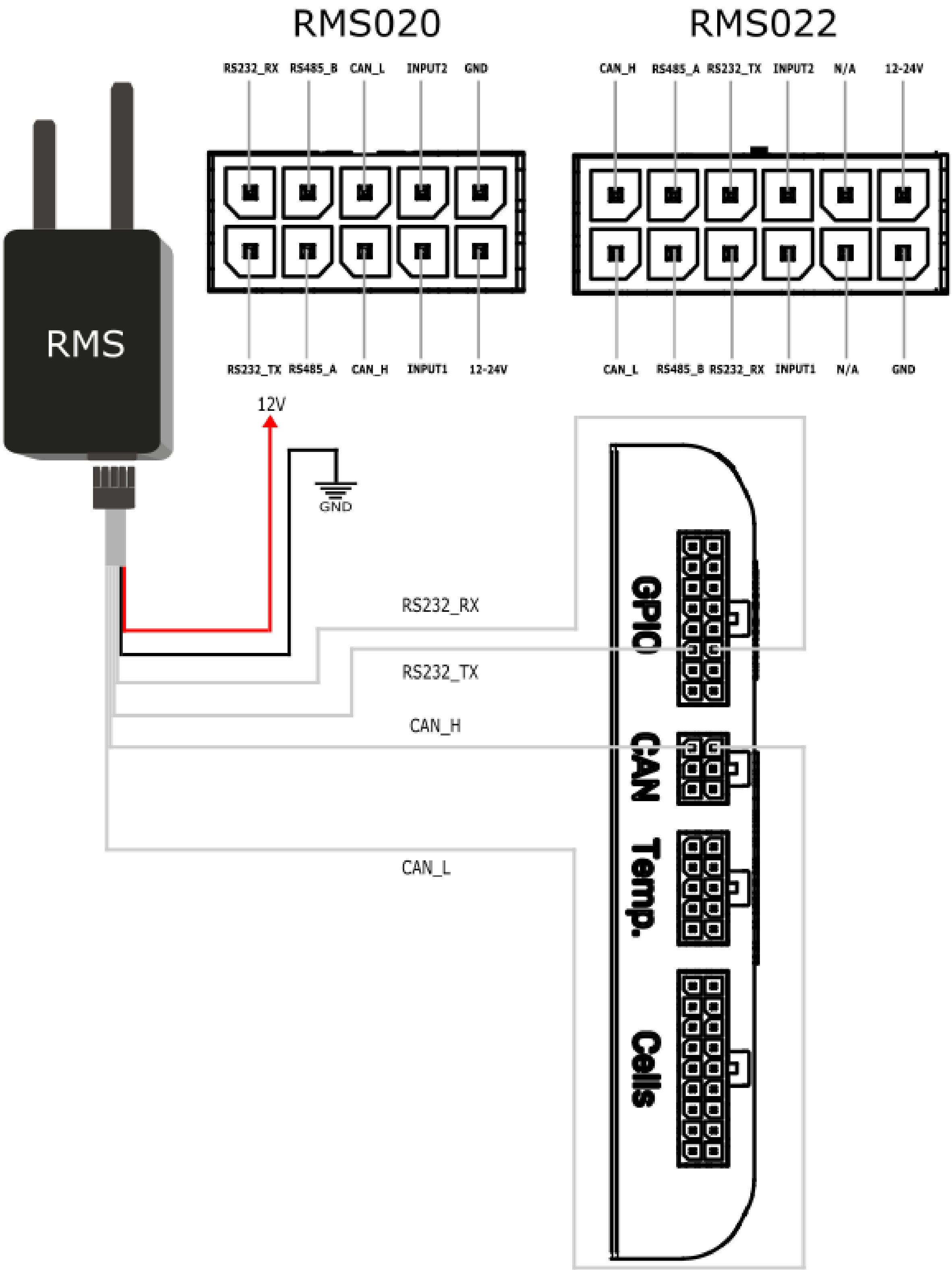
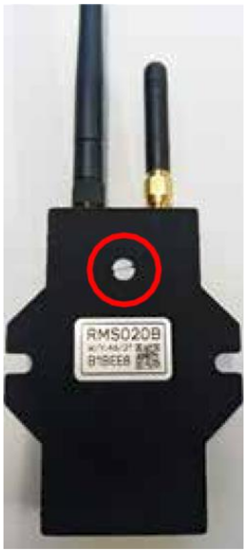


Figure 0-2 RMS connection with Mini3 (MNC034)

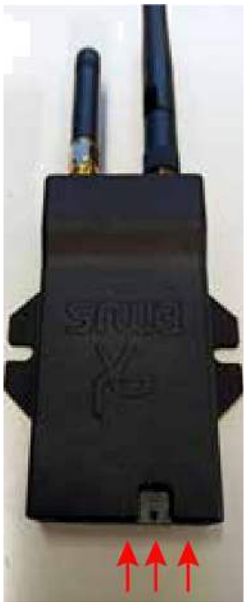
NOTE: The wiring diagrams describes the EMUS RMS connection to the EMUS G1 Control Unit (CM021) and EMUS BMS Mini 3 (MNC034) using RS232 and CAN communication interfaces.

NOTE: One of the RS232, RS485, and Serial interfaces can be used at the same time. In the future EMUS RMS versions, these interfaces will be user-configurable during system operation. Currently, by default, RMS is configured with RS232 interface.

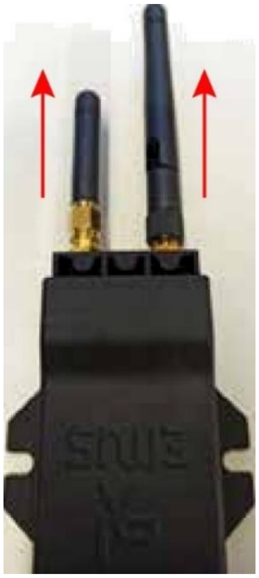
1.2 SIM card installation procedure



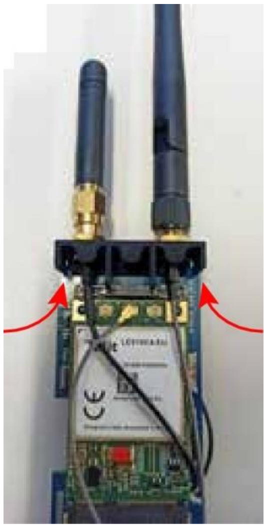
1. Pull out nylon bolt.



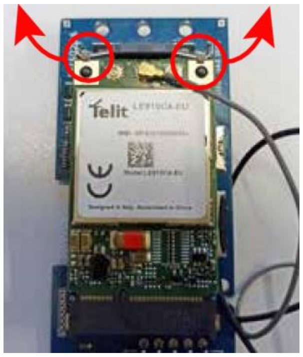
2. Gently, but firmly push connector towards antenna.



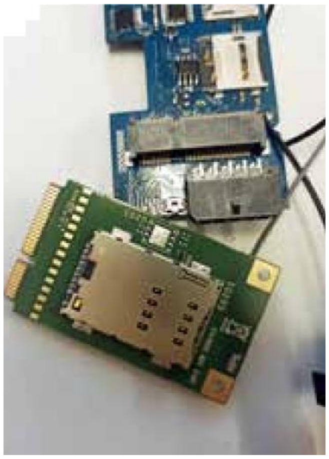
3. When lid opens, pull the lid by the antenna.



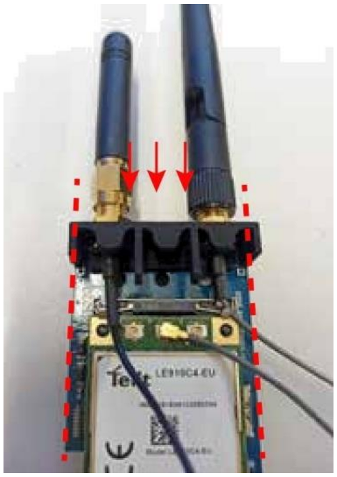
4. Gently, but firmly push the lid away from the PCBa.



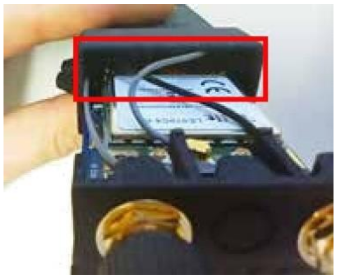
5. Open holding flaps to release GSM board.



6. Flip GSM board, there is a slot for the SIM card. Now insert SIM card and put GSM board back into its slot.



7. Again, gently, but firmly, push the lid back onto the PCBa. Make sure, that PCBa and the lid are aligned.

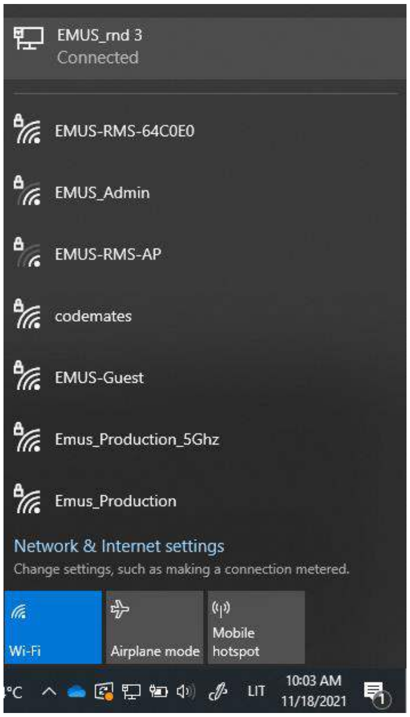


8. Now push PCBa with the lid back into enclosure. Make sure all cables are not stuck on the enclosure. Then firmly tighten the lid into the enclosure and push the nylon bolt back.

2 Wi-Fi provisioning

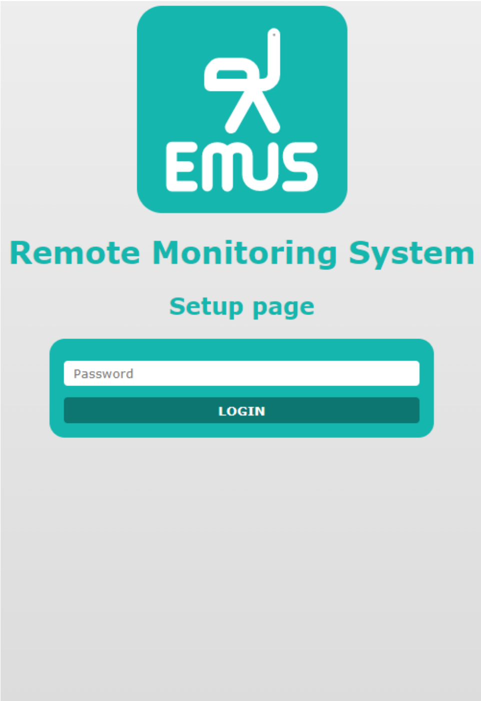
Before device can connect to the internet, it must get access credentials to the users Wi-Fi network. For this, device firstly acts as a router itself together with a http server, so the Wif-Fi credentials can be filled through the web browser. The provisioning procedure is done like this:

- Once device is powered on, access point "EMUS-RMS-xxxxxx" is created. Now the unit is working, but can't connect to the internet, as it doesn't have user Wi-Fi credentials. Mandatory to connect to "EMUS-RMS-xxxxxx" access point with the password **"emusrmswifi"**:



NOTE: “EMUS-RMS-xxxxxx” access point stays active 5 minutes after power-up.

- After successful connection to “EMUS-RMS-xxxxxx” open your browser and navigate to 192.168.4.1 address. Once admin panel is presented need to login into administrator console. The default password is the same as Wi-Fi password: **“emusrmswifi”**:



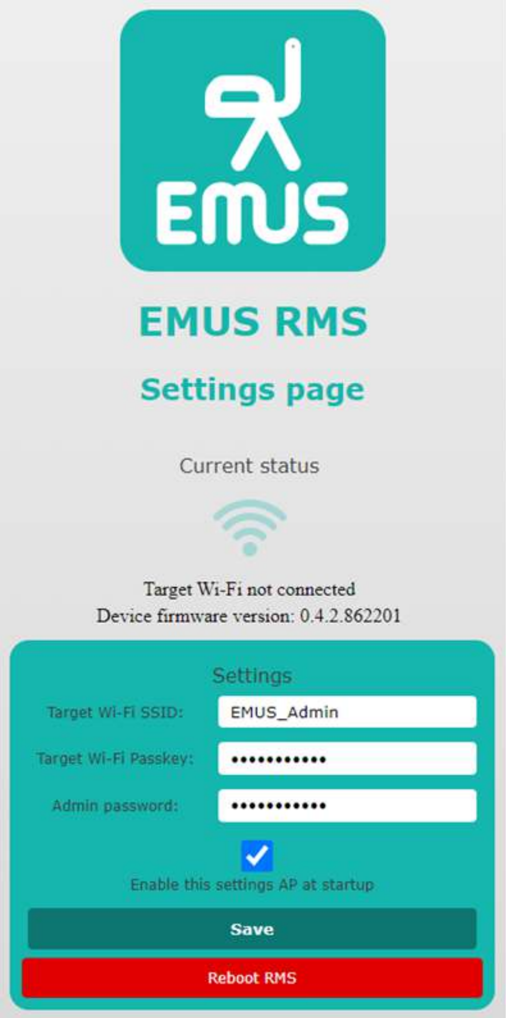
Remote Monitoring System

Setup page

- After login you can monitor current EMUS RMS Wi-Fi connection status. Initially device is not connected to any Wi-Fi spot, to connect it please manually fill your Wi-Fi spot information in the settings page and change your “Admin Password”. For saving new settings, please click button “Save”. After it you should reboot device by clicking “Reboot RMS” button. After these steps, device attempts to connect to the configured Wi-Fi router, and presents status to user.

⚠ NOTE: Changed “Admin password” will be saved in device. This password should be used to future connections to “EMUS-RMS-xxxxxx” spot.

- In case when the password and ssid are correct, you should be seeing “Wi-Fi connected” on the “Current Status” field in the settings page.



EMUS RMS

Settings page

Current status

Target Wi-Fi not connected

Device firmware version: 0.4.2.862201

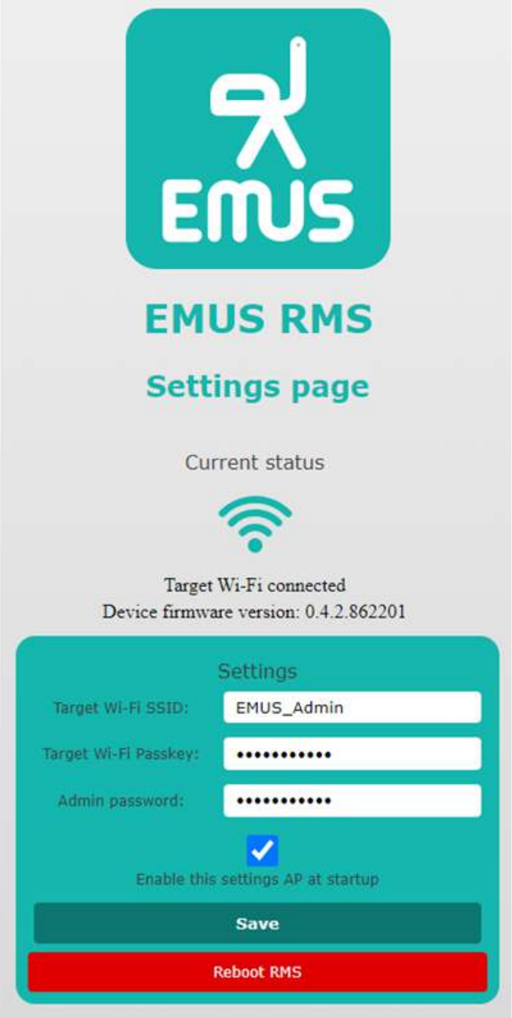
Settings

Target Wi-Fi SSID: EMUS_Admin

Target Wi-Fi Passkey: ••••••••••••

Admin password: ••••••••••••

☑ Enable this settings AP at startup



EMUS RMS

Settings page

Current status

Target Wi-Fi connected

Device firmware version: 0.4.2.862201

Settings

Target Wi-Fi SSID: EMUS_Admin

Target Wi-Fi Passkey: ••••••••••••

Admin password: ••••••••••••

☑ Enable this settings AP at startup

3 Cellular connection

Device also can be connected to the internet using cellular network. For connection to internet need to:

- Have a SIM card with a mobile data plan without any set passwords (e.g., PIN, PUK codes).

NOTE: The SIM card pin code can be cleared using your phone.

4 OTA Firmware Update

The RMS device supports remote over internet firmware updates. The remote firmware update can be performed in cases when RMS Unit is connected to the internet (Cellular or Wi-Fi connection) and using EMUS RMS Portal.

NOTE: More detailed information about the OTA update functionality is described in the EMUS RMS Portal Guidelines chapter.

5 Factory Reset

RMS can be restored to factory defaults by following these steps:

- Turn off the power to the RMS Unit.
- Click and hold “Factory reset” button

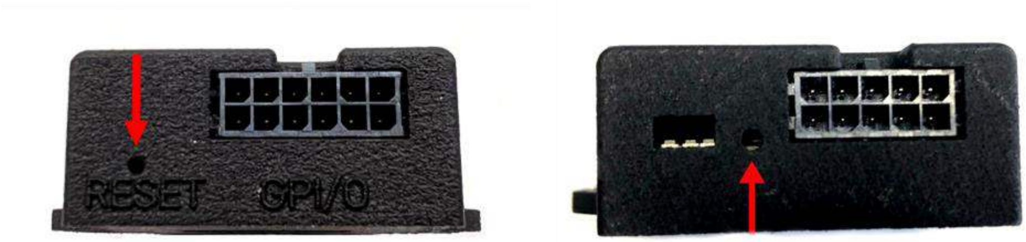


Figure 0-3 "Factory Reset" button

- Turn on power to the RMS Unit
- Release “Factory Reset” button.

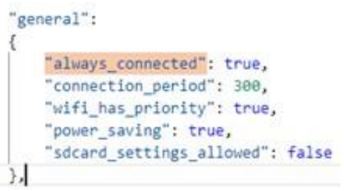
NOTE: After a successful factory reset you will be able to see default RMS configuration parameters. One of the quickest ways to check: is the default Wi-Fi SSID: "EMUS-RMS-AP”.

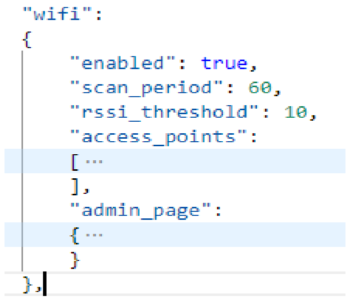
6 RMS Configuration

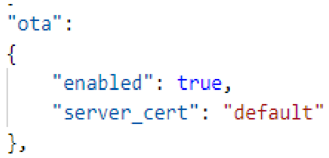
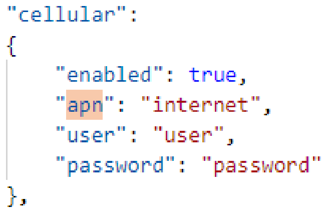
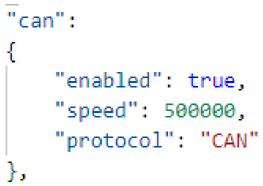
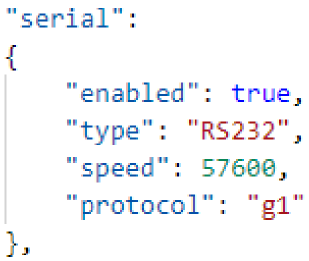
EMUS RMS has configuration files dedicated for your custom needs. They can be found on RMS webpage shared attributes section. These configuration files help to make the system more flexible and firmware independent.

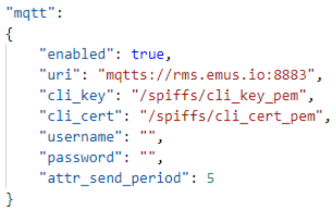
6.1 Device settings configuration

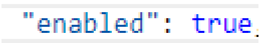
Attribute **settings.json** is used for setting up custom settings for general RMS configuration including general protocol settings, login information, wifi information. These settings can be found on the EMUS RMS portal.

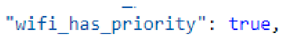
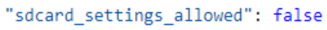
Parameters explanations				
Parameter ID	Description	Type	Default value	Example
Global parameters				
general	General settings being declared here	Container Object	null	 "general": { "always_connected": true, "connection_period": 300, "wifi_has_priority": true, "power_saving": true, "sdcard_settings_allowed": false },

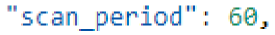
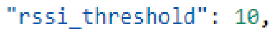
wifi	Wifi settings are being declared here	Container Object	null	
				"wifi":
				{
				"enabled": true,
				"scan_period": 60,
				"rssi_threshold": 10,
				"access_points":
				[…
				],
				"admin_page":
				{…
				}
				},

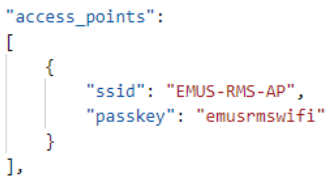
ota	Ota (Over The Air) settings are being declared here	Container Object	null	 "ota": { "enabled": true, "server_cert": "default" },
cellular	Cellular (mobile data) settings are being declared here	Container Object	null	 "cellular": { "enabled": true, "apn": "internet", "user": "user", "password": "password" },
can	CAN protocol settings are being declared here	Container Object	null	 "can": { "enabled": true, "speed": 500000, "protocol": "CAN" },
serial	Serial (G1) protocol settings are being declared here	Container Object	null	 "serial": { "enabled": true, "type": "RS232", "speed": 57600, "protocol": "g1" },

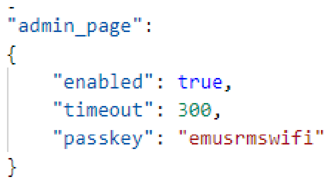
mqtt	MQTT protocol settings are being declared here	Container Object	null	
				"mqtt":
				{
				"enabled": true,
				"uri": "mqtts://rms.emus.io:8883",
				"cli_key": "/spiffs/cli_key_pem",
				"cli_cert": "/spiffs/cli_cert_pem",
				"username": "",
				"password": "",
				"attr_send_period": 5
				}

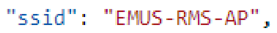
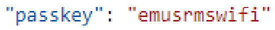
Global meaning settings				
enabled	Option to enable	Boolean	true	 "enabled": true

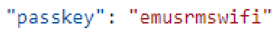
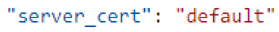
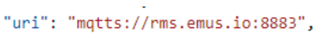
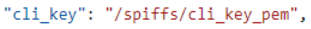
	feature described above			
Protocol related parameters				
speed	Protocol bit speed measured in bps (bits per second)	Integer	250000	"speed": 57600,
protocol	Type of protocol declared here	String	null	"protocol": "CAN"
General settings				
connection_period	Connection period described in milliseconds, which determines the period of time RMS need to wait between switching higher priority connection type over to lower priority	Integer	200	"connection_period": 300,
wifi_has_priority	Option to determine the priority of wifi over cellular, True stands for wifi as a higher priority	Boolean	true	 "wifi_has_priority": true,
power_saving	Option to enable RMS power-saving mode	Boolean	true	"power_saving": true,
sdcard_settings_all	Option to allow	Boolean	true	 "sdcard_settings_allowed": false

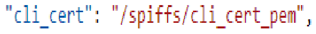
owed	JSON configuration settings from sdcard			
Wifi settings				
scan_period	Wifi scan period of checking its connectivity	Integer	60	 `"scan_period": 60,`
rssi_threshold	Minimum allowed difference between wifi signals strengths before switching to stronger connection wifi	Byte	10	 `"rssi_threshold": 10,`

access_points	A list containing wifi credentials for each wifi being used for having access to described access points	List	null	 `"access_points":`
				`[`
				`{`
				`"ssid": "EMUS-RMS-AP",`
				`"passkey": "emusrmswifi"`
				`}`
				`],`

admin_page	Admin page settings are being declared here	Container Object	null	 `"admin_page":`
				`{`
				`"enabled": true,`
				`"timeout": 300,`
				`"passkey": "emusrmswifi"`
				`}`

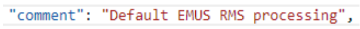
Access point settings				
ssid	Title / Name of the access point	String	""	 `"ssid": "EMUS-RMS-AP",`
passkey	The password of	String	""	 `"passkey": "emusrmswifi"`

	the access point			
Admin page settings				
timeout	-	Integer	300	"timeout": 300,
passkey	Password for logging to admin page	String	""	 "passkey": "emusrmswifi"
Ota settings				
server_cert	Over The Air server certification type.	String	""	 "server_cert": "default"
Cellular settings				
apn	Name of cellular APN	String	"Internet"	"apn": "internet",
user	Username of login to cellular APN	String	"user"	"user": "user",
password	Password of login to cellular APN	String	"pass"	"password": "password"
Serial settings				
type	Serial protocol communication type, usually RS232 is used	String	null	"type": "RS232",
MQTT settings				
uri	Declaration of URI path to RMS server	String	"mqtts://rms.emus.io:8883"	 "uri": "mqtts://rms.emus.io:8883",
cli_key	Path to client key	String	"/spiffs/cli_ke	 "cli_key": "/spiffs/cli_key_pem",

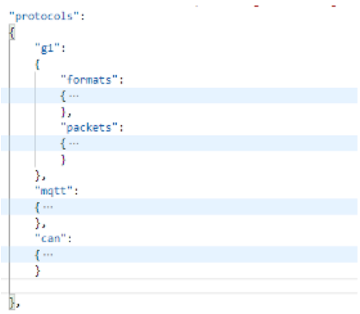
	declared here		y_pem"	
cli_cert	Path to client certificate declared here	String	"/spiffs/cli_cert_pem"	 "cli_cert": "/spiffs/cli_cert_pem",
username	Username of RMS panel login	String	""	"username": "",
password	Password of RMS panel login	String	""	"password": "",
attr_send_period	Period of attributes sending over MQTT described in seconds	Integer	10	"attr_send_period": 5

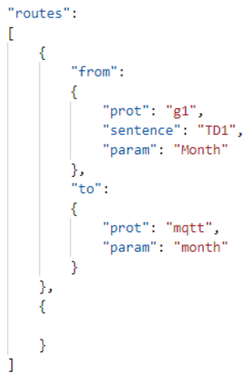
6.2 Parameters configuration

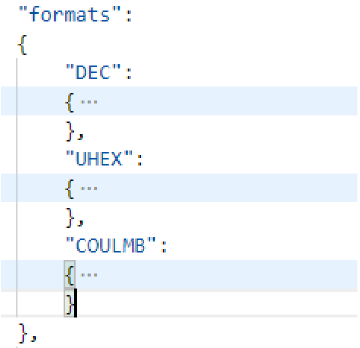
File **params_configx.json** is used for setting up custom settings for incoming and outgoing specific protocol packets. These settings give an opportunity to control packets IDs, types, their formatting, connection with MQTT protocol, etc. These settings can be found on EMUS RMS portal.

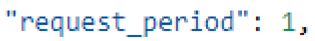
Parameters explanations					
Parameter ID	Description	Type	Protocol support	Default value	Examples
Global parameters					
comment	Comment for declaring this json configuration	String	-	" "	 "comment": "Default EMUS RMS processing",

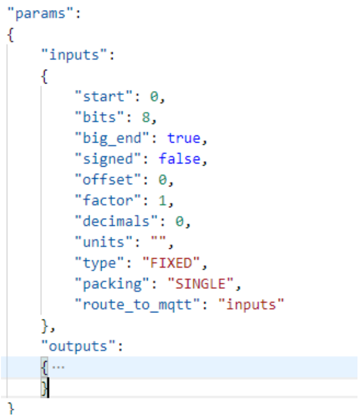
	purpose				

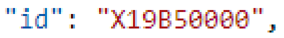
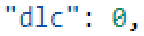
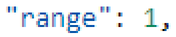
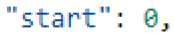
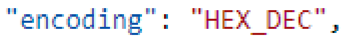
protocols	This parameter abstracts various protocols supported by RMS	Container Object	G1, CAN	{}	 "protocols":
					{
					"g1":
					{
					"formats":
					{…
					},
					"packets":
					{…
					}
					},
					"mqtt":
					{…
					},
					"can":
					{…
					}
					},

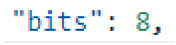
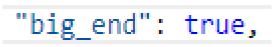
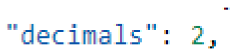
routes	Configurable routes between different protocols	Container Object	G1, CAN	null	 "routes":
					[
					{
					"from":
					{
					"prot": "g1",
					"sentence": "TD1",
					"param": "Month"
					},
					"to":
					{
					"prot": "mqtt",
					"param": "month"
					}
					},
					{
					
					}
					]

formats	This parameter abstracts protocol formats, which can be used to declare specific types of formatting.	Container Object	G1	{}	 "formats":
					{
					"DEC":
					{…
					},
					"UHEX":
					{…
					},
					"COULMB":
					{…
					}
					},

Protocol parameters					
request_period	Period time (described in seconds) between requests for data receiving	double	G1, CAN	0.5	 "request_period": 1,

params	This section is for describing protocol packets / sentences params formatting	Container Object	G1, CAN	{}	
					`"params":`
					`{`
					`    "inputs":`
					`    {`
					`        "start": 0,`
					`        "bits": 8,`
					`        "big_end": true,`
					`        "signed": false,`
					`        "offset": 0,`
					`        "factor": 1,`
					`        "decimals": 0,`
					`        "units": "",`
					`        "type": "FIXED",`
					`        "packing": "SINGLE",`
					`        "route_to_mqtt": "inputs"`
					`    },`
					`    "outputs":`
					`    {…`
					`    }`
					`}`

id	Protocol packet id 'X' stands for extended 'S' stands for standard	String	G1, CAN	null	 `"id": "X19B50000",`
dlc	Packet for receiving length described in bytes	Byte	CAN	-1	 `"dlc": 0,`
range	Checking a range of the packet ID, with range > 1 sends to specified id with looping over a range	Integer	CAN	1	 `"range": 1,`
Parameters settings					
start	Start position described in bits from where parameter will be read	Byte	CAN	0	 `"start": 0,`
encoding	Encoding type for format	String	G1	null	 `"encoding": "HEX_DEC",`

bits	Length of parameter described in bits	Byte	CAN	8	 "bits": 8,
big_end	Byte ordering type. True stands for Big-Endian	Boolean	G1, CAN	true	 "big_end": true,
signed	True - negative / positive values allowed False - only positive values allowed	Boolean	G1, CAN	false	"signed": false,
offset	Value from which will start increasing.	Float	G1, CAN	0.0	"offset": 200,
factor	Stepping value by which result value getting increased in steps	Float	G1, CAN	1.0	"factor": 0.01,
decimals	Decimal places after the dot.	Byte	G1, CAN	-1	 "decimals": 2,
units	Type units describing value. Example: "V", "%", "A", "°C"	String	G1, CAN	null	"units": "V",
type	Precision type for negating data loss over decimals.	String	G1, CAN	null	"type": "FIXED",
route_to_mqtt	Name / ID of	String	G1, CAN	null	"route_to_mqtt": "minVolt"

	parameter sent over MQTT (you will see it on the RMS website)				
packing	Type of packing in packet	String	CAN	"SINGLE"	`"packing": "SINGLE",`
pack_length	Attribute for list packing types, which includes more than 1 parameter in packing, determines how many elements will be in a packet	Byte	CAN	1	`"pack_length": 4,`
send_invalid	Option for enabling or disabling out of bounds values sent to the website	Boolean	CAN	false	`"send_invalid": true,`
valid_top	Maximum valid value	Double	CAN	0	`"valid_bot": 2,`
valid_bot	Minimum valid value	Double	CAN	0	`"valid_top": 4,`
format	Custom declared formatting abstraction which can be applied for each packing	Container Object	G1	null	`"format": "STR",`
field	Field position from where	Byte	G1	1	`"field": 2,`

	sentence bytes will be read, currently used for G				
bit	Describing bit position for reading in a field	Byte	G1	0	"bit": 1,

7 RMS cyber security

Emus Remote Monitoring System has various up-to-date algorithms to keep our clients safe from random attackers, who may affect the stability of the system or cause any danger in getting data stolen. We use these technologies for safety:

- TLS 1.2
- WPA / WPA2 (AP dependent)

7.1 Internet access

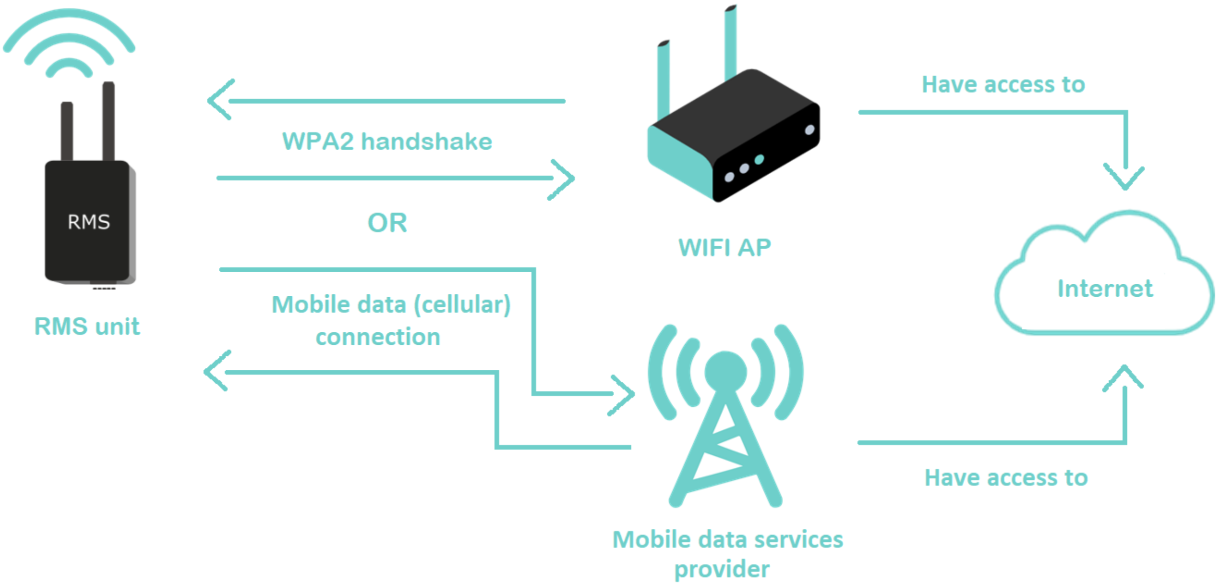
EMUS RMS can access Internet using two ways: via Wi-Fi Access Point or Mobile Cellular Data connectivity.

7.1.1 Wi-Fi access point

When RMS gets access internet over the WIFI AP, it has supported standard WIFI authentication algorithms WEP, WPA, WPA2, but since WEP and WPA have security weaknesses, it has by default enabled only WPA2 algorithm, anyways it can be customized later depending on client router authentication support. Wi-Fi AP SSID and passkey are configurable on RMS device to allow it access customer's Wi-Fi AP.

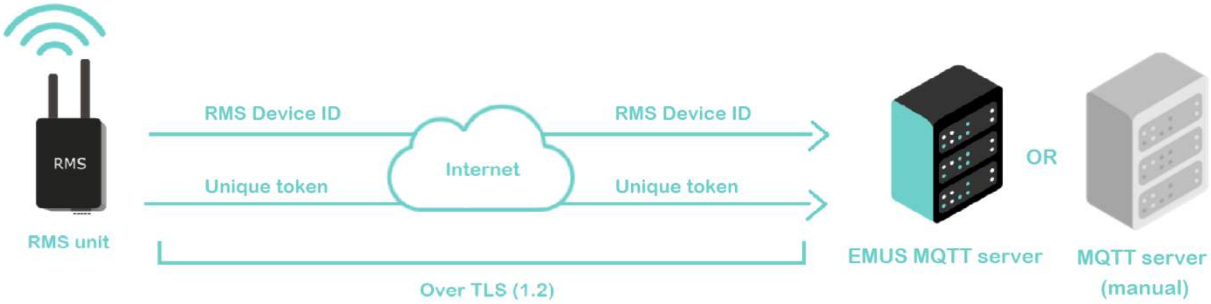
7.1.2 Mobile data

RMS can connect the internet over mobile data virtual access points as well. For this access point, credentials (APN, username, and password) can be configurable in RMS device. In most cases, it is not needed, as mobile network operator automatically provides default credentials for Internet access.



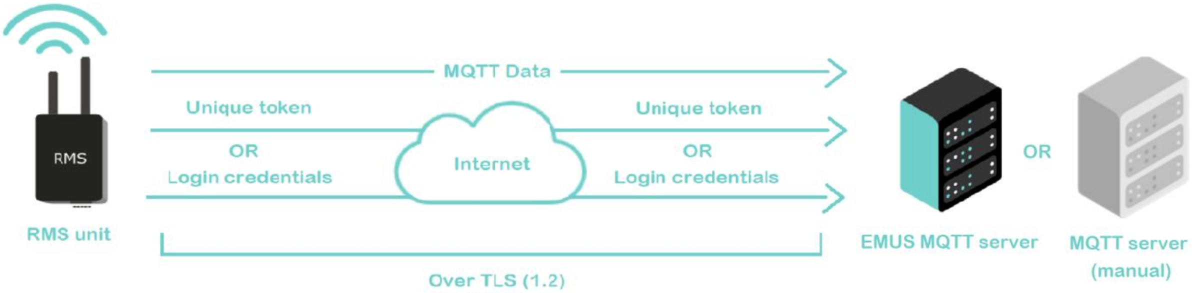
7.2 Device registration to MQTT server

After being connected to the internet each RMS device on the first launch (happening in the production phase at EMUS factory) gets registered to the MQTT server by its unique device ID. Device ID provisioning provides RMS an authentication token, which will be used on later authentications. In the settings file you can set up manually login credentials also, that is another method for logging continuous sessions. Our security system disables the opportunity to register the device to a panel more than once using the same Device ID, so attackers do not have the opportunity to receive tokens by just knowing Device ID itself. If needed can connect to other MQTT servers like Amazon.



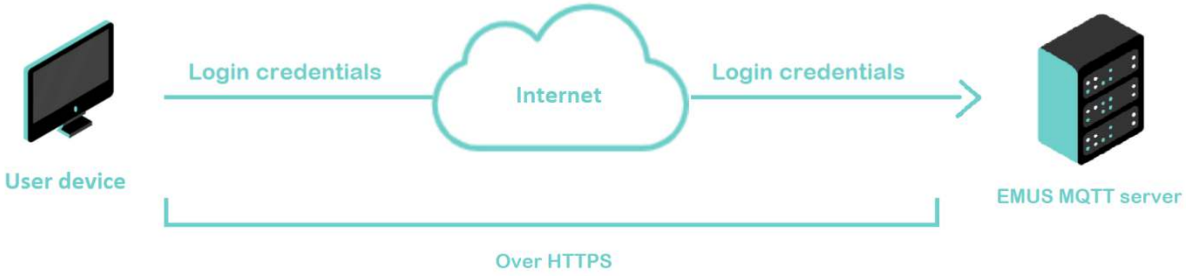
7.3 MQTT data flow

We assume that connections over the internet are not safe, since that is fully controllable by the client itself, so we cannot control it. For such situations, EMUS Remote Monitoring System has supported TLS 1.2 security protocol, which will prevent client data from being abused by attackers or any other unwanted third parties while doing continuous data flow over MQTT. Our current TLS is based on *ECDHE-RSA-AES256-SHA, HIGH* ciphers.



7.4 RMS Portal login

Remote monitoring system portal uses HTTPS connection via TLS 1.2 for communication with client browser, HTTP connection attempts are automatically redirected by RMS portal to secure HTTPS port, helping to avoid sniffing attacks. Currently requires user login credentials for logging in site, which can be provided only by EMUS company for each client manually, which leads to extra security level.



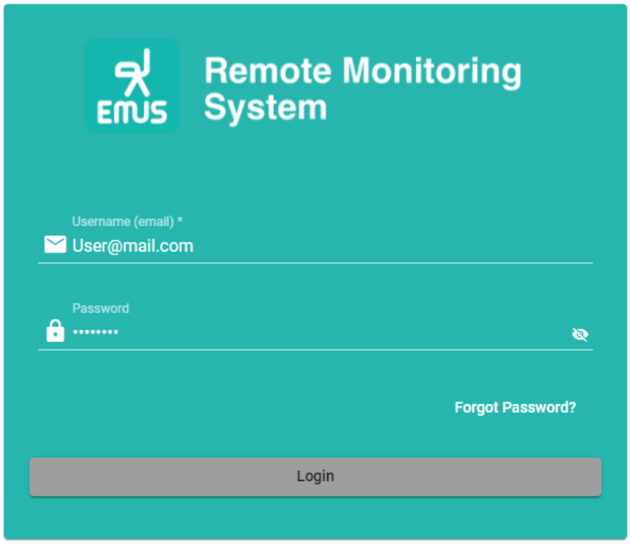
EMUS RMS Portal guidelines

EMUS RMS Portal is an open-source IoT platform that enables rapid development, management, and scaling of IoT projects. Features of this platform enable the user: provisioning of the devices, assets, customers, and creation of the relations between them. It is also a very powerful tool to collect and visualize data from devices and assets. The next paragraph briefly describes the main features, which allow management and monitor the EMUS BMS performance.

NOTE: For EMUS RMS Portal usage you need to have EMUS provided access to the web portal, which allows management and monitoring of the EMUS BMS performance.

8 Login / Password change

Firstly, all users must have their EMUS RMS Portal accounts. All EMUS RMS Portal user credentials is provided by EMUS. Once you have your credentials please navigate with your browser to: "rms.emus.io". After it you are navigated to login page, please fill your email, password and click Login button.



Username (email) *
User@mail.com

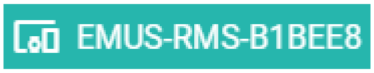
Password
••••••••

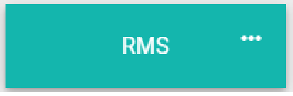
When you logged in recommended to change your account password by making these steps:

- Click “more three points vertical button” ⋮
- Select profile button 👤 .
- After these steps you can see your account general information and have ability to change your password.

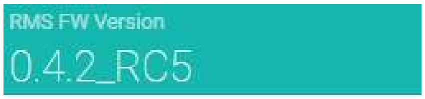
9 OTA Firmware Update

RMS OTA Update Procedure:

- Go to the “Dashboard groups” page.
- Open “EMUS Dashboards (“Customer Name”).
- Open “BMS Panel” dashboard.
- Select your RMS unit on top of the dashboard panel. 

  EMUS-RMS-B1BEE8
- Go to the “RMS” tab. 

- Ensure that “RMS Uptime” continuously increasing, and “Active” parameter is true.
- Press the “Update firmware” button. ☁
- Select “RMS020_FW (x.x.x)” firmware version and press “Update” button. (Do not select “DO_NOT_FLASH” versions. Some versions are in development phase).
- Monitor downloading new firmware process on the graph on “RMS” tab.
- After successful firmware download and update “RMS FW Version” parameter must be updated to the new one.



RMS FW Version

0.4.2_RC5

⚠ **NOTE**: To ensure the success of the firmware download process the signal of the selected Internet connection must be stable.

10 User management

User is an entity that can log in to the EMUS RMS Portal web interface, execute REST API calls, access devices, assets, and other entities if they have permissions to do so. Users are grouped into user groups.

10.1 User Groups

A User group is group of users of the same level with the same permissions. One user can simultaneously belong to several user groups. By default, two different user roles are created in the EMUS RMS Portal: “Customer Users” and “Customer Administrators”.

- Customer Administrators: Having all permissions to manage EMUS RMS Portal system.
- Customer Users: Having read-only permissions in EMUS RMS Portal system.

User with sufficient permissions can add new user group by making these steps:

- Navigate to “Device groups” page.
- Press “Add entity group” + button.
- Fill entity group name, description.

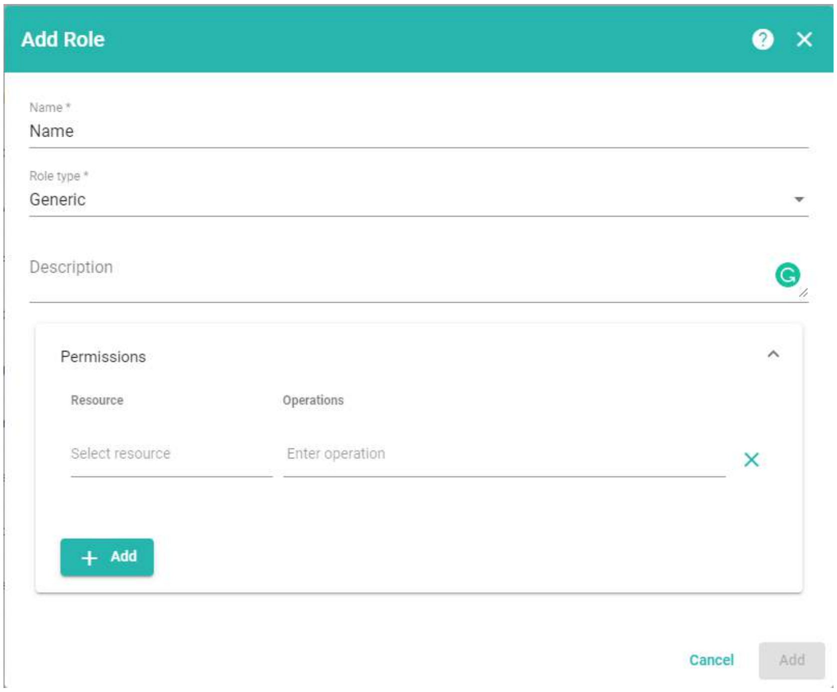
10.2 Roles

Using “Roles” possible to quickly create specific access to the EMUS RMS Portal elements permission levels. EMUS RMS Portal provides two different role types:

- **Generic**: Each Role is related to one or more User Group. Each User Group has only one Owner. With the Generic Role, you grant User Group with the same permissions over all entities that belong to the same Owner and all its’ sub-customers recursively. We use a special “connection” object called Group Permission Entity to make a connection between User Group and Generic Role.
- **Group**: Group Role allows you to map a set of Permissions for a specific User Group to a particular Entity Group. We use special “connection” object called Group Permission Entity to make a connection between User Group, Entity Group and Group Role.

To create new role, need to:

- Navigate to “Roles” page.
- Press “Add entity group” + button.
- Fill role name, select role type,
- Select permission levels.



Add Role

Name *
Name

Role type *
Generic

Description

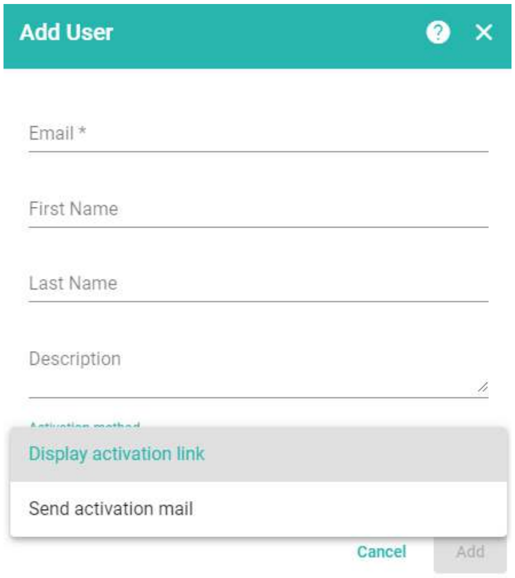
Permissions

Resource	Operations
Select resource	Enter operation

10.3 User

To add new user for specific user group, need to make these steps:

- Open user group where you can add new user.
- Press ⊕ button.
- Write new user information and select activation method. User can be activated by displaying activation link on the screen or sending activation link by previously written email.



Add User

Email *

First Name

Last Name

Description

Activation method

Display activation link

Send activation mail

Cancel

Add

11 Customers management

EMUS RMS Portal allows users with sufficient permissions to manage their customer’s information. Like users’ management, customers also can be divided into groups. Users with “Customer Administrators” permission role can add and manage all customers information.

11.1 Customer groups

By default, EMUS RMS Portal do not include created customer groups.

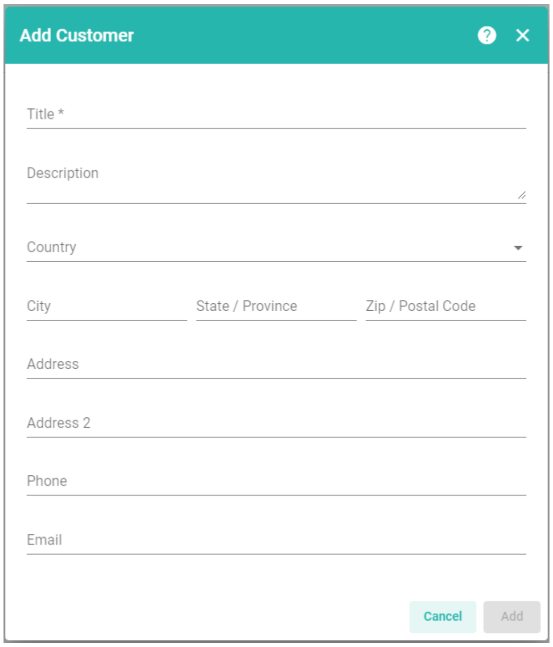
User with sufficient permissions can add new customer group by making these steps:

- Navigate to “Customer groups” page.
- Press “Add entity group” + button.
- Fill entity group name, description.
- By clicking “next” possible to share this entity group with different permission levels to the specific customers and their users.

11.2 Customer

To add new customer for specific customers group, need to make these steps:

- Open customer group where you can add new user.
- Press ⊕ button.
- Write new user information and select activation method.



12 Devices management

EMUS RMS Portal allows users to manage their, and customer’s devices. Like users’ or customers management, devices also can be divided by groups. By default settings of the EMUS RMS Portal, users who have “Customer Administrators” permission roles can add and manage all devices information.

12.1 Device groups

By default, EMUS RMS Portal do not include created device groups.

User with sufficient permissions can add new device group by making these steps:

- Navigate to “Device groups” page.
- Press “Add entity group” + button.

- Fill entity group name, description.
- By clicking “next” possible to share this entity group with different permission levels to the specific customers and their users.

12.2 Device

To add new device for specific customer, need to make these steps:

- Open device group where your device is located. You can find it by selecting “All” in device group page.
- Select your specific device by checking checkbox.
- Press above located button and select new target owner.

12.2.1 Device attributes management

To configure device “**settings.json”, “params_configx.json”** or other attributes need to make these steps:

- Open device group where your device is located. You can find it by selecting “All” in device group page.
- Select your specific device by clicking on device row.
- Press “Attributes” button.
- Select from drop-down menu “Shared attributes”.
- Modify devices attributes.

For successful device “**settings.json”, “params_configx.json”** attributes update need to reset your device using one of the RMS portal dashboards or just by disconnecting your device from the power supply.

13 Dashboards management

EMUS RMS Portal allows users to manage their, and customer’s dashboards. By using your own or EMUS created dashboards monitoring of the battery management systems activity becomes more flexible and comfortable. Like other EMUS RMS Portal elements, dashboards also can be divided by groups. By default settings of the EMUS RMS Portal, users who have “Customer Administrators” permission roles can add and manage all dashboards information.

13.1 Dashboard groups

By default, EMUS RMS Portal includes by EMUS created standard dashboard groups.

User with sufficient permissions can add new dashboard group by making these steps:

- Navigate to “Dashboard groups” page.
- Press “Add entity group” + button.
- Fill entity group name, description.
- By clicking “next” possible to share this entity group with different permission levels to the specific customers and their users.

If you want to make your dashboard group public and share a link to it, you should:

- Go to the Dashboard groups.
- Click the ⋖ icon next to the dashboard group that you want to make public.
- In the confirmation dialog box, click “Yes”.
- Open the dashboard group and click the link icon 🔗 opposite the needed dashboard.
- In the “Public dashboard link” dialog, click a copy button next to the link.

Now you can share a dashboard with this link. Note that you shouldn’t forget to make related devices, assets, and entity views public to access their data.

13.2 Dashboard

Each dashboard can contain plenty of widgets. Dashboards display data from many entities: devices, assets, etc. Dashboards can be assigned to customers.

To add a new dashboard, you should:

- Go to Dashboard groups through the main menu on the left of the screen.
- Open dashboard group where you want to add new one.

- Click the + sign in the upper right corner of the screen.
- In the opened dialog, necessary to enter a dashboard title, description is optional. Click “Add”.

14 Entity Management

14.1 Entity views groups

By default, EMUS RMS Portal do not include created entity groups.

User with sufficient permissions can add new device group by making these steps:

- Navigate to “Entity view groups” page.
- Press “Add entity group” + button.
- Fill entity group name, description.
- By clicking “next” possible to share this entity group with different permission levels to the specific customers and their users.

14.2 Entity view

Like SQL database views, which limits the degree of exposure of the underlying tables to the outer world, EMUS RMS Portal Entity Views limit the degree of exposure of the Device or Asset telemetry and attributes to the Customers. As a Tenant Administrator, you can create multiple Entity Views per Device or Asset and assign them to different Customers.

Supported use cases:

- Share specific device or asset data with multiple Customers simultaneously. Prior Entity views feature was not possible due to restrictions of the EMUS RMS Portal security model.
- Allow particular Customer users to see collected data (e.g., sensor readings), but hide debug info like battery level, system errors, etc.
- Device-as-a-Service (DaaS) model where data collected by the device at different periods of time belongs to different Customers.

15 Connectivity via TLS

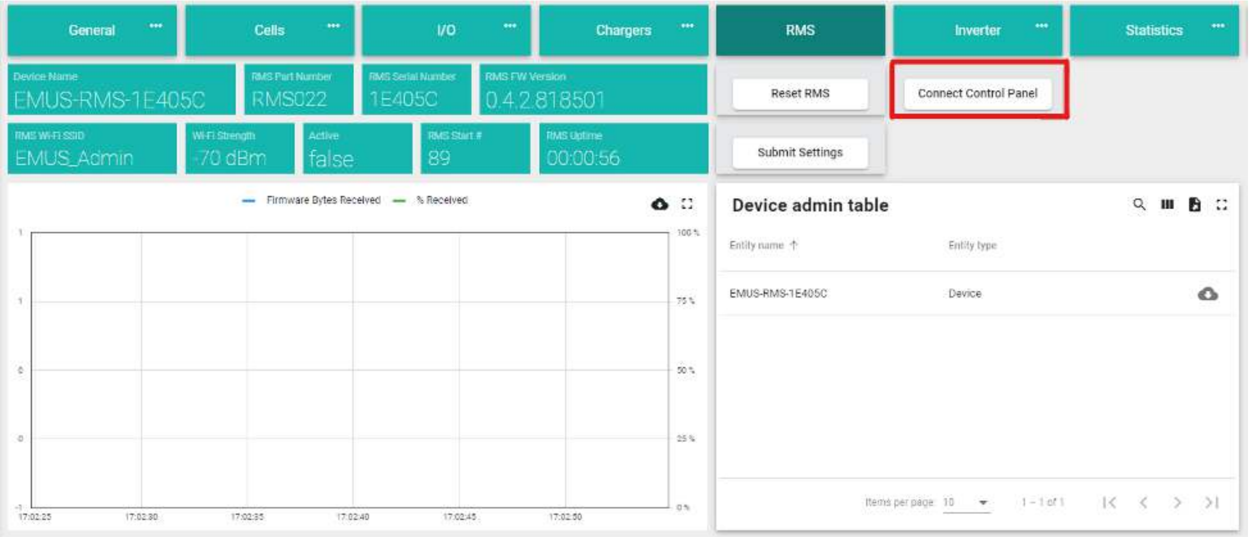
EMUS RMS allows users the possibility to connect EMUS Control Panel application remotely, it provides ability to manage and configure the EMUS BMS devices without being in any physical connection with them. EMUS RMS initializes a remote secured tunnel, which is responsible for encrypting all data flow between the EMUS devices and EMUS Control Panel application.

⚠ NOTE: Before the TLS connection procedure please make sure you have a compatible EMUS Control Panel Application version. After downloading the EMUS Control Panel application for the first time, launch it before attempting to connect using a TLS connection.

⚠ NOTE: Please download EMUS Control Panel Application from the official EMUS web page. For more information, please contact the EMUS support team.

15.1 Connection procedure

- To start off user needs to navigate and login to the EMUS RMS Portal.
- Open “EMUS Public Dashboard” and navigate to the “RMS” page.
- Click on the “Connect Control Panel” button.



Device Name: EMUS-RMS-1E405C

RMS Part Number: RMS022

RMS Serial Number: 1E405C

RMS FW Version: 0.4.2.818501

RMS Wi-Fi SSID: EMUS_Admin

Wi-Fi Strength: -70 dBm

Active: false

RMS Start #: 89

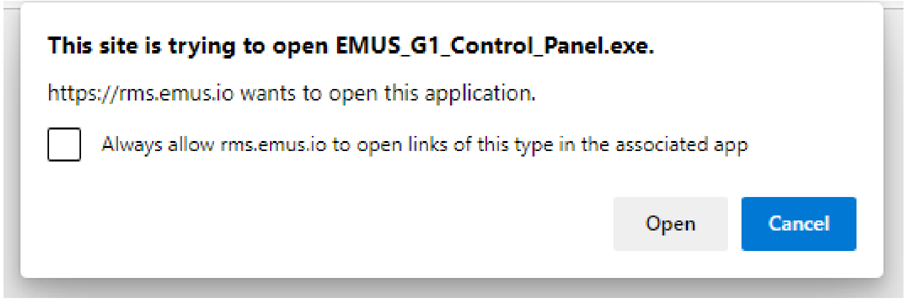
RMS Uptime: 00:00:56

Device admin table

Entity name ↑	Entity type
EMUS-RMS-1E405C	Device

Items per page: 10 1 – 1 of 1

- Popup box in the upper part the of page will appear.



This site is trying to open EMUS_G1_Control_Panel.exe.

https://rms.emus.io wants to open this application.

□ Always allow rms.emus.io to open links of this type in the associated app

- To open the EMUS Control Panel application, click on the “Open” button. After these steps, all EMUS Control Panel Application functionality stays the same as it is used with a USB.

NOTE: If the popup box did not appear, make sure you have a compatible version of the EMUS Control Panel Application.

NOTE: The EMUS Control Panel Application using TLS may run slower in case of poor internet connection.

Support

Please contact EMUS for BMS installation or support questions to:

support@emusbms.com

Thank you for choosing EMUS BMS products!

Battery Management Systems

battery made simple

www.emusbms.com

EMUS