commsignia

User Guide for Commsignia ITS-RS4-M Roadside Units

Document ID: USR-005
Document Version: 20.55
Software version: y20.55
Publication date August 29, 2024

This document may be revised without prior notice. For most recent releases, please visit our website.

It is the sole responsibility of the user to ensure that the device and its application complies with all necessary local, regional, national, and international radio frequency laws and regulations at the installation location, prior to its commissioning, unless expressly set forth otherwise regarding compliance with specific laws, regulations and standards in the relevant quotation of Commsignia issued to the user or in a written agreement between Commsignia. Commsignia is not liable for any costs or damages or other consequences resulting from the non-compliance of the aforementioned radio frequency laws and regulations.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

—Reorient or relocate the receiving antenna.
—Increase the separation between the equipment and receiver.
—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
—Consult the dealer or an experienced radio/TV technician for help.

Any changes or modifications made to this device that are not expressly approved by Commsignia, Inc. may void the user's authority to operate the equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This transmitter must be at least 20 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.

Revisions with respect to version 20.48:

Type of change	Added/revised section
New section	• **Section 2.2** **"Connecting to the RSU over LTE connection" [3]**
Major revision	• **Section 5.2** **"Converting data formats" [23]** New switches have been added to the description of the `asn1x` tool. Examples have been revised.
Minor revision	–

Table of Contents

1. Before connecting to the device ... 1
2. Connecting to the device ... 2
    2.1. Connecting to the RSU over wireless or wired connection ... 2
    2.2. Connecting to the RSU over LTE connection ... 3
        2.2.1. Inserting the SIM card ... 3
        2.2.2. Configuring the LTE modem interface ... 4
        2.2.3. Connecting to the device ... 7
3. Validating V2X communication ... 8
    3.1. Using the GUI to check the status of the stack ... 8
    3.2. Using the CLI to generate a status report ... 8
    3.3. Creating Packet Capture files on the RSU ... 9
        3.3.1. Configuring the C2P module ... 9
        3.3.2. Writing data stream into PCAP files ... 10
4. Basic settings of the RSU ... 11
    4.1. Changing the passwords ... 11
        4.1.1. Changing the WiFi password ... 11
        4.1.2. Changing the login password ... 12
    4.2. Restoring the default configuration ... 13
    4.3. Configuring navigation settings ... 13
    4.4. Configuring station parameters ... 15
    4.5. Configuring radio settings ... 15
        4.5.1. Configuring the radio interface ... 15
        4.5.2. Configuring Dual Active mode ... 19
5. Message handling on RSUs ... 23
    5.1. Converting data formats ... 23
    5.2. Store-and-Repeat messages (SRMs) ... 23
        5.2.1. Configuring SRM settings ... 23
        5.2.2. Formatting SRMs ... 24
    5.3. Immediate forwarding ... 25
        5.3.1. Configuring IFM settings ... 25
        5.3.2. Formatting IFMs ... 26
    5.4. Deploying and transmitting SRMs/IFMs ... 27
    5.5. Transmitting Signal Phase and Timing (SPaT) messages on RSUs ... 28
6. Additional features ... 30
    6.1. Datalogger tool ... 30
        6.1.1. Description of the Datalogger tool ... 30
        6.1.2. Configuring the Datalogger ... 32
    6.2. Integrating object detections from smart sensors into the Cooperative Filtering and Fusion framework ... 35
        6.2.1. Overview ... 35
        6.2.2. Interfacing with the CFF UDP adapter ... 35
        6.2.3. Data requirements ... 36
        6.2.4. Message composition using Python language ... 36
        6.2.5. Message composition using C++ language ... 38
        6.2.6. Configuring the UDP adapter and message generation on the RSU ... 39
        6.2.7. Quick guide for configuration ... 43
        6.2.8. Restrictions ... 43
7. Advanced configuration of the software stack ... 45
    7.1. Factory reset ... 45
        7.1.1. Performing factory reset on the GUI ... 45
        7.1.2. Performing factory reset on the CLI ... 46
    7.2. Upgrading the firmware ... 47
        7.2.1. Prerequisites ... 47

7.2.2. Upgrade process 48
7.3. Enabling security for V2X messages using the GUI 49
7.4. Relicensing the device 51
7.4.1. Prerequisites 51
7.4.2. Relicensing process 52
7.5. Enabling IPv6 tunneling on RSUs 54
8. Troubleshooting V2X communication 59
8.1. General validation steps 59
8.2. V2X messages are not secured or not transmitted 59
8.3. The HMI is not displaying SPaT on the map 59
8.4. The HMI displays a SPaT that is different from the actual traffic signal 59
8.5. The HMI is not displaying the local vehicle 59
A. Glossary of terms 60

List of Figures

1. Login screen of the GUI 2
2. Interfaces page on the GUI 3
3. Location of the SIM socket at the bottom of the unit 4
4. Inserting the SIM card into the SIM socket 4
5. Creating a new interface for WWAN connection 5
6. Configuration page of the WWAN connection 5
7. Firewall settings for the WWAN interface 6
8. IP address assigned by the LTE provider 7
9. V2X stack status page 8
10. Commsignia Capture Protocol (C2P) settings for localhost 9
11. Wireless Overview group 11
12. Interface configuration group 12
13. Creating new login password 13
14. V2X profile preset 13
15. Navigation configuration 14
16. Manual navigation settings 14
17. GPSD navigation settings 14
18. Station information settings 15
19. Qualcomm radio interface settings 15
20. Autotalks CUT2 radio interface settings 16
21. Autotalks CUT3 radio interface settings 17
22. WSMP configuration 17
23. BSM module 18
24. GeoNetworking configuration 18
25. CAM transmission configuration 19
26. Enabling Dual Active mode 19
27. SRM/IFM tool configuration settings for Dual Active mode 20
28. TLC settings for Dual Active mode 21
29. Transmitted and received packet statistics for DSRC and V2X radios 22
30. Changing the location of the SRM directory 24
31. SRM/IFM configuration menu 25
32. TLC configuration page 28
33. TrafficWare protocol settings 28
34. Battelle protocol settings 29
35. Schematic of the Datalogger operation 30
36. Schematics of smart sensor integration into the CFF 35
37. Factory reset page 45
38. Rebooting screen 46
39. Security configuration 50
40. Facility receive module configuration 50

41. Statistics for secured messages 51
42. Licensing page on the GUI 52
43. License Activation page 53
44. Generation of a new license key 53
45. IPv6 tunneling setup 54
46. IPv6 module configuration 54
47. WSA configuration 55
48. Setting the static IPv6 address for the device 56
49. Firewall settings 57
50. Enabling IPv6 forwarding in the Firewall settings. 58

List of Tables

1. Filtering options for the Datalogger tool 30
2. Options for different output types 31
3. PSIDs and message IDs of various messages (US) 34
4. ITS-AID and message IDs of various messages (EU) 34
5. Firmware variants 48

1. Before connecting to the device

Roadside units (RSUs) are responsible for the infrastructure aspect of V2X communications. They are typically installed in a fixed location (such as an intersection or alongside a stretch of highway) and relay information between each V2X-equipped participant of the ongoing traffic as well as the traffic management system they are connected to.

Traffic lights in intersections can be connected to RSUs to offer information about intersection topology and lanes, light signal statuses, and to provide reconfigurability for real-time traffic management and road usage statistics as well. The Commsignia V2X software stack is compatible with most Traffic Light Controller (TLC) solutions owing to its compliace with various different standards.

Before connecting to the RSU, please ensure the following:

1. The RSU is fully assembled according to the provided Quick Start Guide.
2. The RSU is powered on through the Power over Ethernet (PoE) connector.
3. Your computer is connected to same network as the RSU, using Ethernet of wireless (Wi-Fi) connection.
4. For the Graphical User Interface (GUI) an internet browser is available on your computer.
5. For the Command Line Interface (CLI) a Secure Shell Protocol (SSH) client is available on your computer.

Commsignia devices are delivered ready-to-use with a basic configuration. In order to configure the features of the Commsignia V2X software stack, a connection needs to be established to at least one V2X device running the stack.

2. Connecting to the device

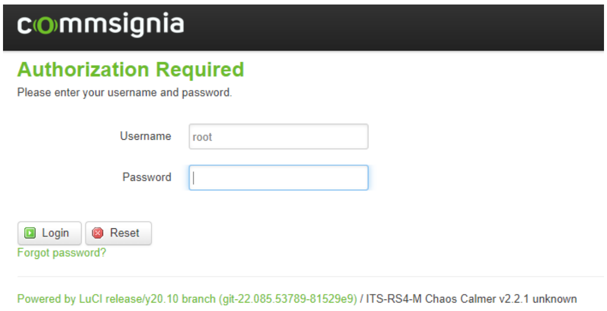
2.1. Connecting to the RSU over wireless or wired connection

Commsignia devices are delivered ready-to-use with a basic configuration. In order to configure the features of the Commsignia V2X software stack, a connection needs to be established to at least one V2X device running the stack. The device can be accessed via wireless or wired connection using a GUI or a CLI.

> Please note that the device has two separate IP addresses for wireless and wired connections. Please ensure that your computer is connected to the same wireless or wired network as the RSU. All passwords are case-sensitive.

1. Connecting to the device over wireless (Wi-Fi) network:
   The SSID of the RSU is **ITS-RS4-XXXXXXX**, where XXXXXXX is the last seven digits of the serial number of the RSU, which can be found on the product label. The default Wi-Fi password is **Commsignia**.

   a. In a web browser enter the IP address of the device, which is **172.29.148.54** by default, or use the domain name **my.cms.device/**. Use the username **root** and enter the default password, **UK5BJLFZVBPZLIM55Y**, to log in, as shown in Figure 1.



Authorization Required

Please enter your username and password.

Username: root

Password:

Powered by LuCI release/y20.10 branch (git-22.085.53789-81529e9) / ITS-RS4-M Chaos Calmer v2.2.1 unknown

Figure 1. Login screen of the GUI

   b. Alternatively, an SSH connection can be established from the CLI as

```
ssh root@192.168.1.54
```

   and entering the same root password, **UK5BJLFZVBPZLIM55Y**, when prompted.

2. Connecting to the device over wired (Ethernet) connection:

   a. Please ensure that your computer is connected to the same wired network as the RSU. Your computer needs to use the same subnet as the Commsignia default of the RSU.

   b. In a web browser enter the IP address of the device, which is **192.168.0.54** by default. Use the user name **root** and enter the default password, **UK5BJLFZVBPZLIM55Y**, to log in, as shown in Figure 1.

   c. Alternatively, an SSH connection can be established from the CLI as

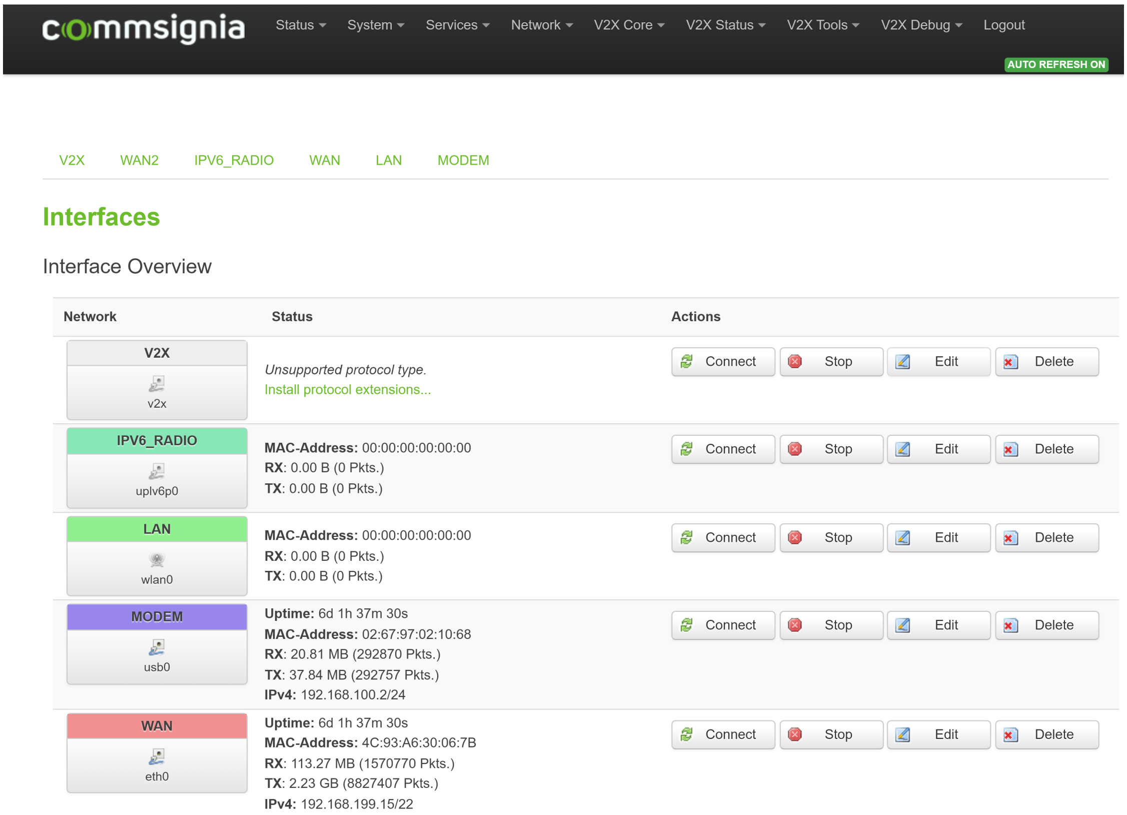
```
ssh root@192.168.0.54
```

and entering the same root password, **UK5BJLFZVBPZLIM55Y**, when prompted.

3. Connecting to multiple devices by connecting them to the same switch on your network after configuring a unique fixed IP address for the devices:

   a. Connect to a device using one of the methods described in this chapter.

   b. Set the IP address and gateway of the device under the **Network** → **Interfaces** menu by editing the **eth0** interface, as shown in Figure 2.



Interfaces

Interface Overview

Network	Status	Actions
V2X v2x	*Unsupported protocol type.* Install protocol extensions...	Connect Stop Edit Delete
IPV6_RADIO uplv6p0	**MAC-Address:** 00:00:00:00:00:00 **RX**: 0.00 B (0 Pkts.) **TX**: 0.00 B (0 Pkts.)	Connect Stop Edit Delete
LAN wlan0	**MAC-Address:** 00:00:00:00:00:00 **RX**: 0.00 B (0 Pkts.) **TX**: 0.00 B (0 Pkts.)	Connect Stop Edit Delete
MODEM usb0	**Uptime:** 6d 1h 37m 30s **MAC-Address:** 02:67:97:02:10:68 **RX**: 20.81 MB (292870 Pkts.) **TX**: 37.84 MB (292757 Pkts.) **IPv4:** 192.168.100.2/24	Connect Stop Edit Delete
WAN eth0	**Uptime:** 6d 1h 37m 30s **MAC-Address:** 4C:93:A6:30:06:7B **RX**: 113.27 MB (1570770 Pkts.) **TX**: 2.23 GB (8827407 Pkts.) **IPv4:** 192.168.199.15/22	Connect Stop Edit Delete

Figure 2. Interfaces page on the GUI

   c. Click on the Save & Apply button for the changes to take effect on the device.

   d. Repeat the steps above for all devices.

2.2. Connecting to the RSU over LTE connection

2.2.1. Inserting the SIM card

The device can accommodate a mini-SIM (2FF) card. To insert the SIM card proceed as follows:

1. Unscrew the transparent plastic cap shown in Figure 3 at the bottom of the unit using a 25 mm hexagonal 6-point socket.

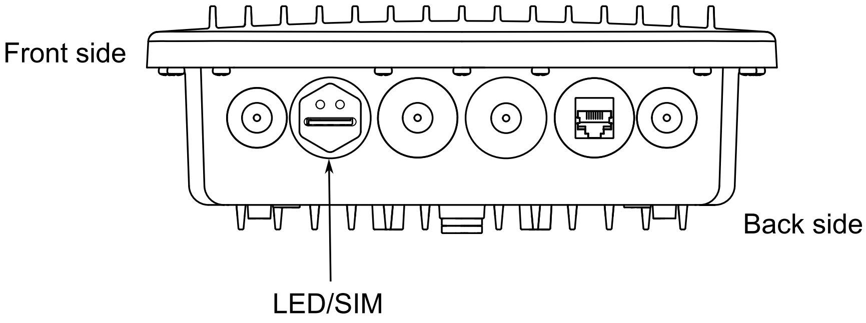


Figure 3. Location of the SIM socket at the bottom of the unit

2. Insert the SIM card into the SIM socket as shown in Figure 4.

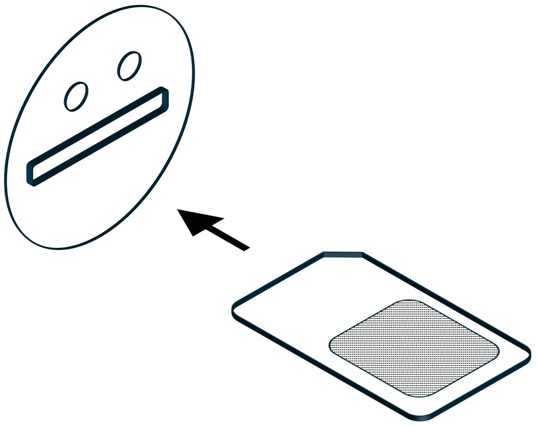


Figure 4. Inserting the SIM card into the SIM socket

3. Screw back and tighten the transparent plastic cap.

> Do not use the socket wrench when tightening the plastic cap! Use the socket and hand force only, as the plastic cover might break or the rubber gasket might be damaged!

2.2.2. Configuring the LTE modem interface

The RSU have a built-in LTE modem for mobile network connections. If the LTE modem interface has not been installed in the unit, then modems with a Qualcomm MSM Interface (QMI) can be used. The units have been tested to work with the following modems:

- Quectel EG25-G (USB 2c7c:0125)
- Sierra Wireless AirPrime MC7455 (USB 1199:9071)

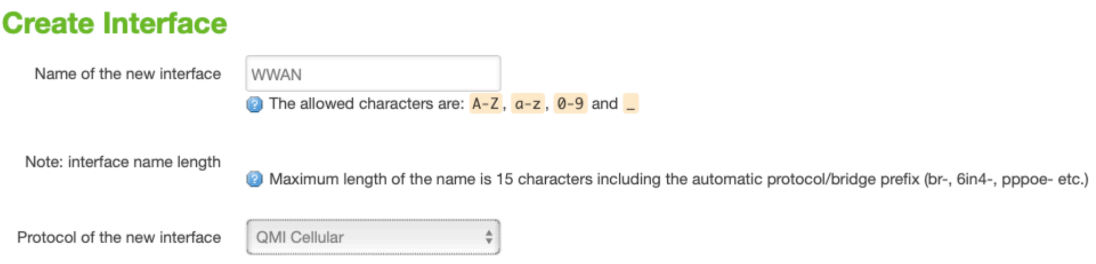
To set up a new Wireless wide area network (WWAN) interface for LTE connection, proceed as follows:

1. Connect to the device either over wireless or wired connection, as described in section "Connecting to the RSU over wireless or wired connection" [2].

2. Log into the GUI. For more information, refer to section “Connecting to the RSU over wireless or wired connection” [2].

3. Open the **Network** → **Interfaces** menu item, and click on the Add new interface... button below the list of interfaces.

4. Specify the name of the interface (for example WWAN) in the field "Name of the new interface," as shown in Figure 5.



Create Interface

Name of the new interface: WWAN

The allowed characters are: `A-Z`, `a-z`, `0-9` and `_`

Note: interface name length: Maximum length of the name is 15 characters including the automatic protocol/bridge prefix (br-, 6in4-, pppoe- etc.)

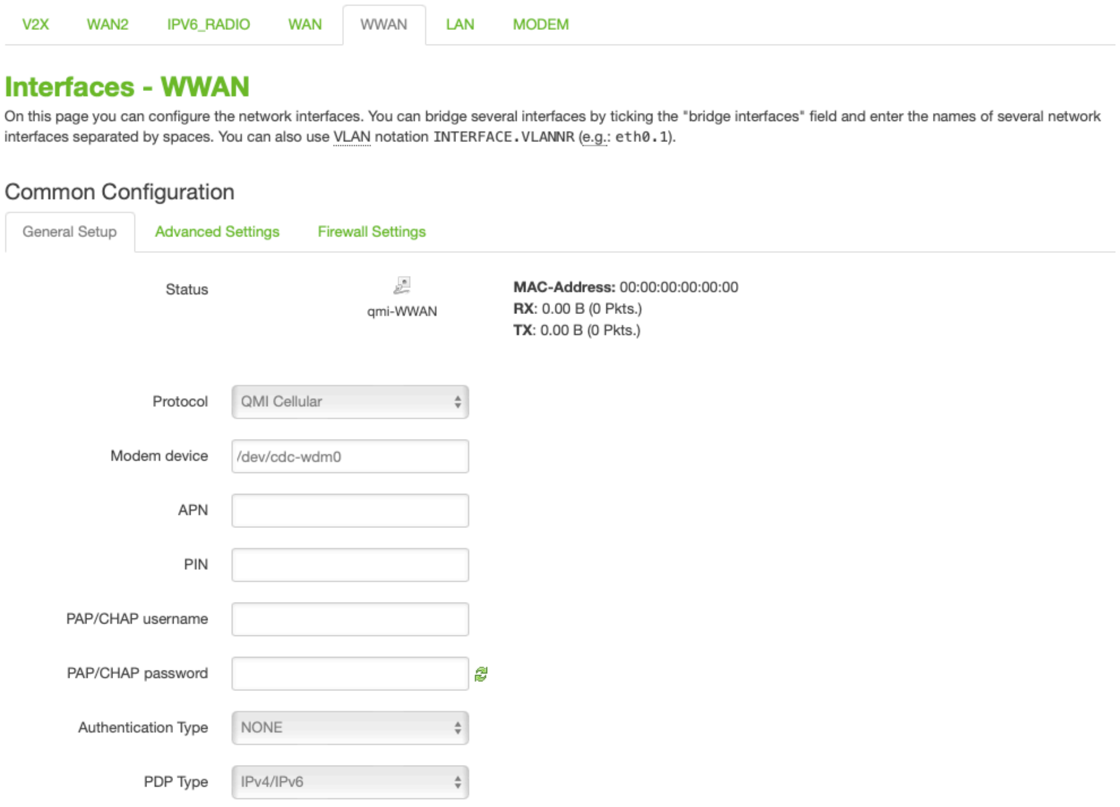
Protocol of the new interface: QMI Cellular

Figure 5. Creating a new interface for WWAN connection

5. In the "Protocol of the new interface" drop-down menu, select QMI Cellular, as shown in Figure 5.

6. To proceed to the configuration page of the interface, click on Submit button to proceed, or the Back to Overview to revert to the previous page.

7. On the configuration page, shown in Figure 6 set the following items:



Interfaces - WWAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

Status: qmi-WWAN

MAC-Address: 00:00:00:00:00:00
RX: 0.00 B (0 Pkts.)
TX: 0.00 B (0 Pkts.)

Protocol: QMI Cellular

Modem device: /dev/cdc-wdm0

APN:

PIN:

PAP/CHAP username:

PAP/CHAP password:

Authentication Type: NONE

PDP Type: IPv4/IPv6

Figure 6. Configuration page of the WWAN connection

a. Set the access point name (APN) in the field "APN" as provided by the mobile connection provider.

b. If the SIM card is PIN protected, set its PIN in the field "PIN."

> Disabling PIN checking is strongly recommended.

c. Select "NONE" in the "Authentication type" drop-down menu.

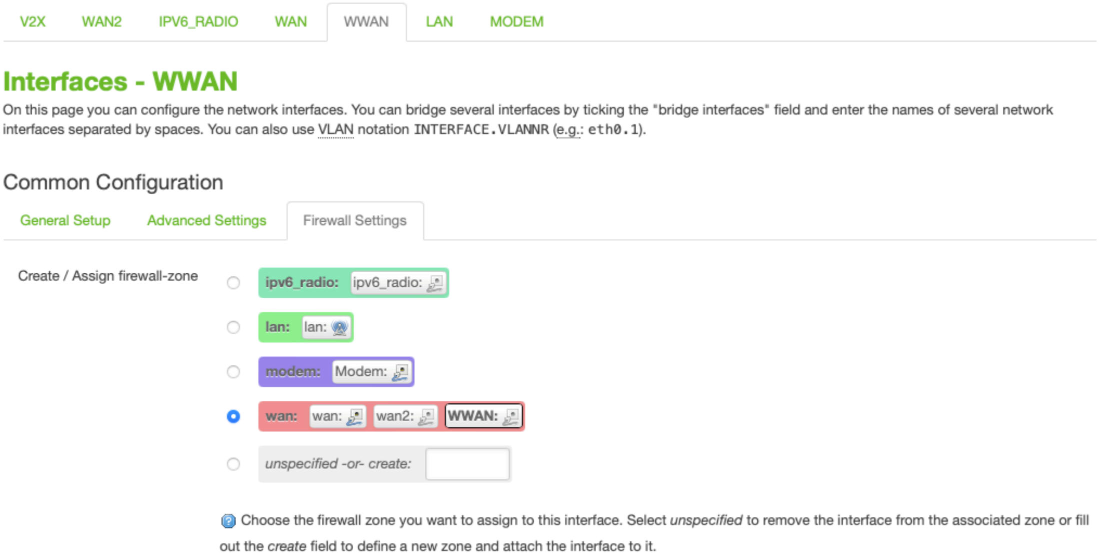
d. To save the configuration, click on Save & Apply button to proceed, or the Back to Overview to revert to the previous page.

8. Configure the firewall settings as follows:

a. On the Interfaces page click on the WWAN tab, or select the WWAN interface from the network list.

b. On the configuration page, shown in Figure 6 click on the "Firewall settings" tab.

c. Select "wan" in the "Create / Assign firewall-zone" section as shown in Figure 7.



Interfaces - WWAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

Create / Assign firewall-zone

○ ipv6_radio: ipv6_radio:

○ lan: lan:

○ modem: Modem:

● wan: wan: wan2: WWAN:

○ *unspecified -or- create:*

Choose the firewall zone you want to assign to this interface. Select *unspecified* to remove the interface from the associated zone or fill out the *create* field to define a new zone and attach the interface to it.

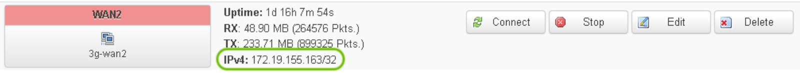
Figure 7. Firewall settings for the WWAN interface

d. To save the configuration, click on Save & Apply button to proceed, or the Back to Overview to revert to the previous page.

The network connection starts up in a few seconds. If the connection is not working, then check the status of the SIM card or that of the radio network.

9. Log back into the device still connecting over wireless or wired connection and open the **Network** → **Interfaces** menu item.

10. Seletc the LTE connection and check the IP address assigned by the LTE service provider as shown in Figure 8.



Uptime: 1d 16h 7m 54s
RX: 48.90 MB (264576 Pkts.)
TX: 233.71 MB (899325 Pkts.)
IPv4: 172.19.155.163/32

Figure 8. IP address assigned by the LTE provider

2.2.3. Connecting to the device

To connect to the device over LTE connection only, proceed as follows:

1. In a web browser, enter the IP address of the device assigned by the LTE provider. Use the username **root** and enter the default password, **UK5BJLFZVBPZLIM55Y**, to log in, as shown in Figure 1.

2. Or, alternatively, use SSH connection by opening a terminal on Linux/MacOS/OS X computers as

```
ssh root@<IP address assigned by the LTE provider>
```

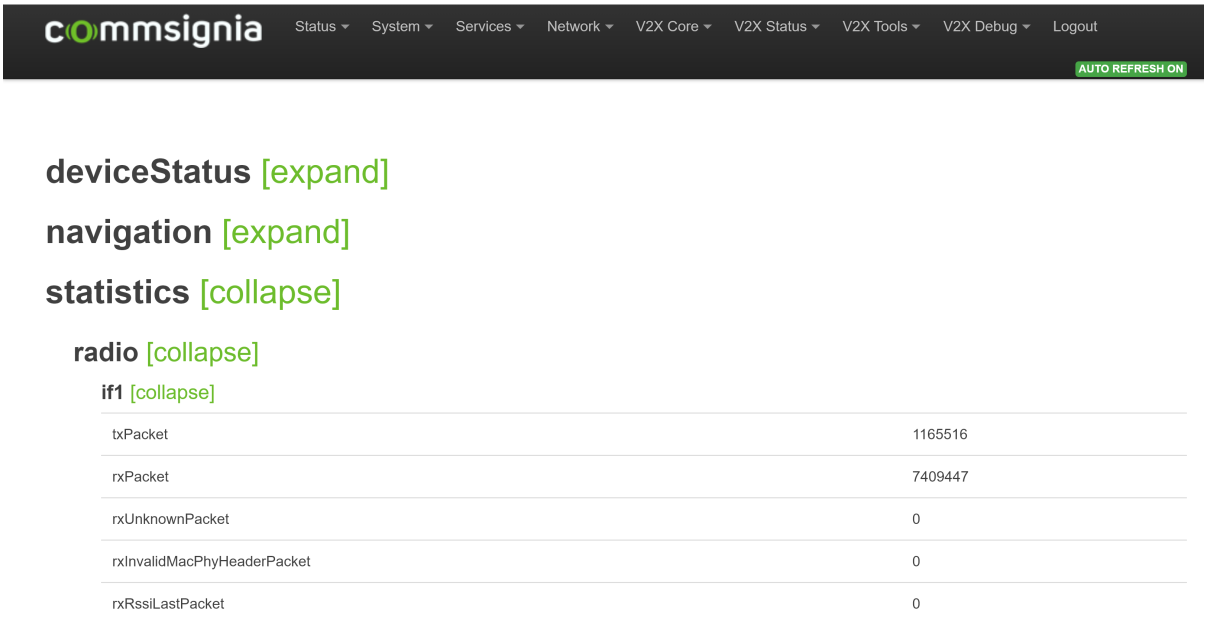
   or using an SSH client (such as PuTTY) on Windows computers, with the IP address assigned by the LTE provider and the username *root*.
   The default SSH password is **UK5BJLFZVBPZLIM55Y** as well.

3. Validating V2X communication

3.1. Using the GUI to check the status of the stack

The recommended method for the validation of the transmission and reception of V2X messages is using the GUI of the software stack. Log into the GUI as described in section “Connecting to the RSU over wireless or wired connection” [2].

The status of the V2X software stack can be monitored under the **V2X Status** → **Status** menu. Scroll down to the **statistics** module, expand it, then expand the appropriate radio and interface modules, as shown in Figure 9.



deviceStatus [expand]

navigation [expand]

statistics [collapse]

radio [collapse]

if1 [collapse]

txPacket	1165516
rxPacket	7409447
rxUnknownPacket	0
rxInvalidMacPhyHeaderPacket	0
rxRssiLastPacket	0

Figure 9. V2X stack status page

The transmission and reception of the packets can be verified by the increase of the values of the transmitted (txPacket) or received (rxPacket) packets. If the counters do not change, refer to the section “Troubleshooting V2X communication” [59].

3.2. Using the CLI to generate a status report

A status report of the running software stack can be generated using the CLI. Log into the device using SSH as described in section “Connecting to the RSU over wireless or wired connection” [2].

Use the following command to generate a status report:

```
v2x-status-json-gen
```

The `j` utility can be used to filter the required values, for example the command `v2x-status-json-gen| jq '.statistics.radio.if1'` list the counter values related to radio interface 1 only:

```
{
  "txPacket": 1151711,
  "rxPacket": 7196345,
  "rxUnknownPacket": 0,
  "rxInvalidMacPhyHeaderPacket": 0,
  "rxRssiLastPacket": 0
}
```

If the values of the transmitted (txPacket) or received (rxPacket) are not increasing, please refer to the section "Troubleshooting V2X communication" [59].

3.3. Creating Packet Capture files on the RSU

For a comprehensive analysis, Packet Capture (PCAP) files can be saved on the RSU using the optional Commsignia Capture Protocol (C2P) module, which generates a User Datagram Protocol (UDP) data stream from the sent and received V2X packets, This data stream can be locally saved on the device into a PCAP file, that can then be copied to a computer using SSH, and the packets can be parsed using the optional packet analyzer *Capture Application* by Commsignia.

The C2P module can be enabled and configured on the RSU RSU using the GUI or the `muci` tool.

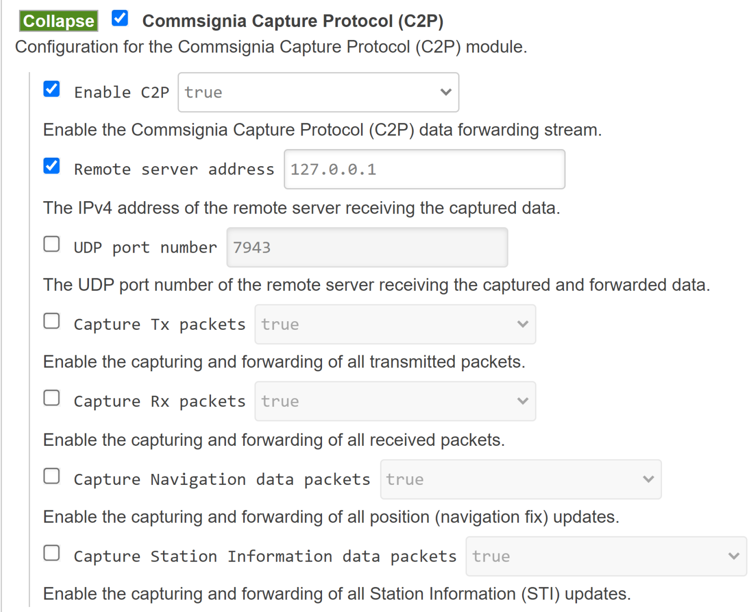
3.3.1. Configuring the C2P module

3.3.1.1. Using the GUI for configuring the C2P module

To use the GUI for configuring the C2P module, proceed as follows:

1. Log into the GUI. For more information, refer to section "Connecting to the RSU over wireless or wired connection" [2].

2. Open the V2X Core → Core stack menu item, check the box near the option **Commsignia Capture Protocol (C2P)**, and expand it, as shown in Figure 10.



Collapse ☑ **Commsignia Capture Protocol (C2P)**

Configuration for the Commsignia Capture Protocol (C2P) module.

☑ `Enable C2P` true

Enable the Commsignia Capture Protocol (C2P) data forwarding stream.

☑ `Remote server address` 127.0.0.1

The IPv4 address of the remote server receiving the captured data.

☐ `UDP port number` 7943

The UDP port number of the remote server receiving the captured and forwarded data.

☐ `Capture Tx packets` true

Enable the capturing and forwarding of all transmitted packets.

☐ `Capture Rx packets` true

Enable the capturing and forwarding of all received packets.

☐ `Capture Navigation data packets` true

Enable the capturing and forwarding of all position (navigation fix) updates.

☐ `Capture Station Information data packets` true

Enable the capturing and forwarding of all Station Information (STI) updates.

Figure 10. Commsignia Capture Protocol (C2P) settings for localhost

3. To enable the C2P data stream, check the box next to `Enable C2P` and set its value to `true`.

4. Check the box next to `Remote server address` and specify the IP address of the localhost, 127.0.0.1.

5. Click on the Save & Apply button for the changes to take effect on the device.

3.3.1.2. Using the muci tool for configuring the C2P module

If the `muci` tool is available on the device (only ion OB4/RS4 devices) it can be used for configuring the C2P module as follows:

1. Log into the device using SSH. For more information, refer to section "Connecting to the RSU over wireless or wired connection" [2].

2. Use the following command to enable the C2P data stream:

```
muci its set capture.enable true
```

3. Specify the IP address of the localhost, 127.0.0.1 as follows:

```
muci its set capture.address 127.0.0.1
```

4. Restart the stack using the command

```
unplugged-rt-restart.sh
```

3.3.2. Writing data stream into PCAP files

To write the data stream into a PCAP file the `tcpdump` command line program can be used. To save a PCAP file and copy to the computer running the Capture Application, proceed as follows:

1. Log into the device using SSH. For more information, refer to section "Connecting to the RSU over wireless or wired connection" [2].

2. Use the following command to start writing the data stream into a PCAP file in the `/tmp` directory:

   ```
   tcpdump -v -pi lo -w /tmp/c2p-$HOSTNAME-$(date +%Y%m%d%H%M%S).pcap port 7943
   ```

   The `tcpdump` program starts writing the data into a PCAP file with a filename containing the hostname and the date and time of the capture.

   Please note that the `/tmp` directory is erased after rebooting the V2X device.

3. After the necessary number of packet were captured, terminate the `tcpdump` program by pressing *Ctrl + C*.

4. On the computer running the Capture Application, enter the directory where the PCAP file needs to be downloaded from the V2X device and use the following SCP command in a terminal window:

   ```
   scp root@<IP address of the V2X device>:/tmp/c2p-HOSTNAME-
   DATE.pcap <name>.pcap
   ```

   Alternatively, on a Windows computer an SCP client, such as Win SCP can be used.

   If the `scp` command returns with the error message `ash: /usr/libexec/sftp-server: not found` and fails, the -O switch needs to be used after the command.

5. Open the copied PCAP file using a packet analyzer, such as the optional *Capture Application* by Commsignia.

4. Basic settings of the RSU

Roadside units are typically deployed in a fixed location and they broadcast standard V2X messages automatically upon startup based on a default configuration preset. However, several configuration options are available to customize the behavior of RSUs.

4.1. Changing the passwords

To ensure the secure operation of the device, it is strongly recommended to change both its WiFi and login passwords after the first login. The passwords can be changed by using either the GUI or the CLI of the deice.

4.1.1. Changing the WiFi password

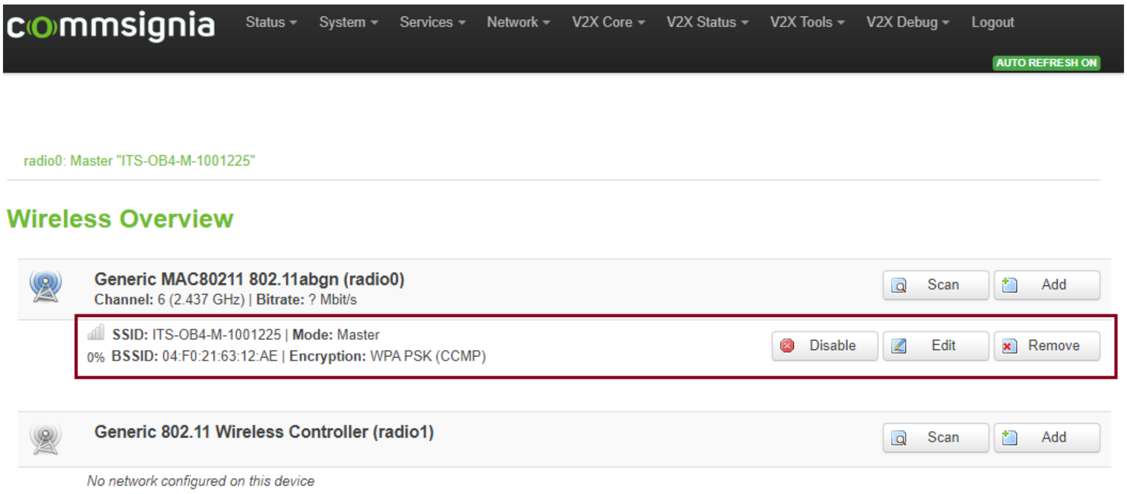
Please note that the WiFi password must be at least 8 characters long.

4.1.1.1. Changing the WiFi password using the GUI

To change the WiFi password of the device using the GUI, proceed as follows:

1. Log into the GUI. For more information, refer to section "Connecting to the RSU over wireless or wired connection" [2].

2. Open the **Network** → **Wifi** menu and select the SSID of the device on the **Wireless Overview** group, as shown in Figure 11.



radio0: Master "ITS-OB4-M-1001225"

Wireless Overview

Generic MAC80211 802.11abgn (radio0)
Channel: 6 (2.437 GHz) | Bitrate: ? Mbit/s

SSID: ITS-OB4-M-1001225 | Mode: Master
0% BSSID: 04:F0:21:63:12:AE | Encryption: WPA PSK (CCMP)

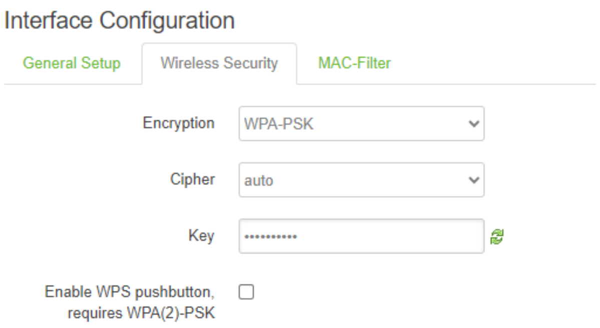
Generic 802.11 Wireless Controller (radio1)

No network configured on this device

Figure 11. Wireless Overview group

Click on the Edit button.

3. In the Interface Configuration group, click on the Wireless Security tab as shown in Figure 12.



Interface Configuration

Encryption: WPA-PSK

Cipher: auto

Key: ••••••••••

Enable WPS pushbutton, requires WPA(2)-PSK ☐

Figure 12. Interface configuration group

4. Specify the applicable encryption method and add a new password in the Key field.

5. Click on the Save & Apply button for the changes to take effect on the device.

4.1.1.2. Changing the WiFi password using the CLI

To change the WiFi password of the device using the CLI, proceed as follows:

1. Log into the device using SSH. For more information, refer to section "Connecting to the RSU over wireless or wired connection" [2].

2. Use the following commands to set a new password:

```
uci set wireless.@wifi-iface[0].key='<Enter password here>'
```

3. Apply the changes as:

```
uci commit wireless
```

4. Reload the LuCI interface as:

```
reload_config
```

If an error message `uci: Entry not found` appears, please ignore it.

4.1.2. Changing the login password

Please note that the login password must contain at least 8 characters, including a capital letter, a special character, and at least 2 numbers.

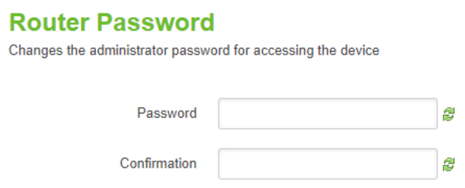
4.1.2.1. Changing the login password using the GUI

To change the login password of the device using the GUI, proceed as follows:

1. Log into the GUI. For more information, refer to section "Connecting to the RSU over wireless or wired connection" [2].

2. Open the **System** → **Administration** menu.

3. Under **Router Password** enter new password and confirm it as shown in Figure 13.



Router Password

Changes the administrator password for accessing the device

Password	
Confirmation	

Figure 13. Creating new login password

4. Click on the Save & Apply button for the changes to take effect on the device.

4.1.2.2. Changing the login password using the CLI

To change the login password of the device using the CLI, proceed as follows:

1. Log into the device using SSH. For more information, refer to section “Connecting to the RSU over wireless or wired connection” [2].

2. Use the following command to change the password:

```
passwd
```

3. Add your current password and press Enter.

4. Add your new password and press Enter.

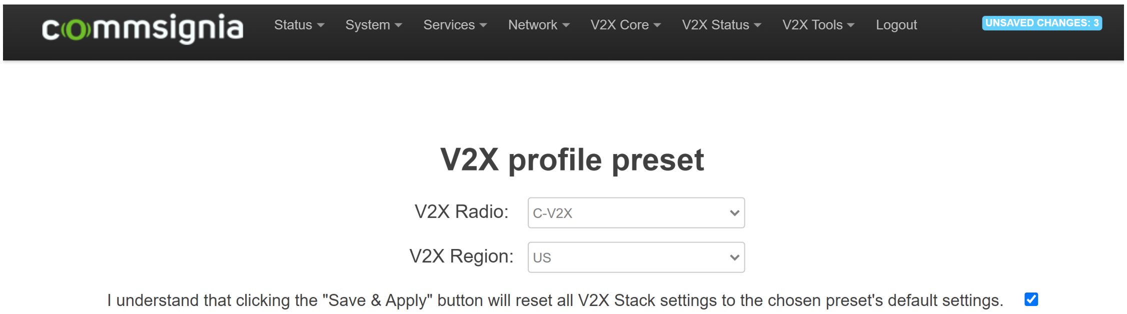
5. Confirm your new password and press Enter.

4.2. Restoring the default configuration

If, for any reason, the default configuration of the device needs to be restored, proceed as follows:

1. Log into the device using SSH. For more information, refer to section “Connecting to the RSU over wireless or wired connection” [2].

2. Open the **V2X Core** → **V2X profile preset** item, as shown in Figure 14.



V2X profile preset

V2X Radio: C-V2X

V2X Region: US

I understand that clicking the "Save & Apply" button will reset all V2X Stack settings to the chosen preset's default settings. ☑

Figure 14. V2X profile preset

3. Set the appropriate V2X Radio and V2X Region, then check the box on the right of the disclaimer.

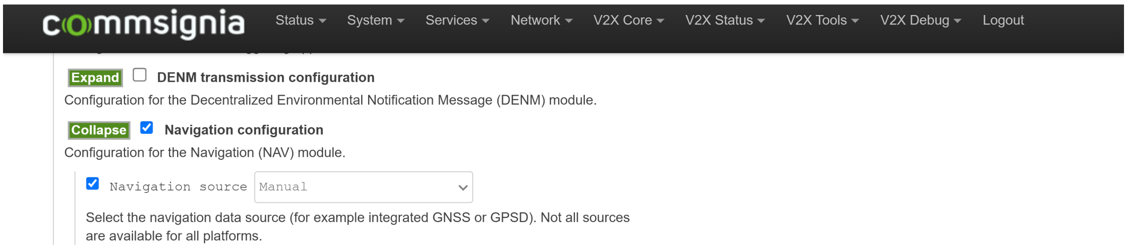
4. Click on the Save & Apply button for the changes to take effect on the device.

4.3. Configuring navigation settings

Three navigation modes are available for the device: "Real," "Gpsd," and "Manual." Te default setting is "Real;" however, if you require gpsd-based or manual navigation fix, it can be set using the GUI as follows:

1. Log into the device using SSH. For more information, refer to section “Connecting to the RSU over wireless or wired connection” [2].

2. Open the **V2X Core** → **Core stack** menu item and expand the option **Navigation configuration**, as shown in Figure 15.



Expand ☐ DENM transmission configuration

Configuration for the Decentralized Environmental Notification Message (DENM) module.

Collapse ☑ Navigation configuration

Configuration for the Navigation (NAV) module.

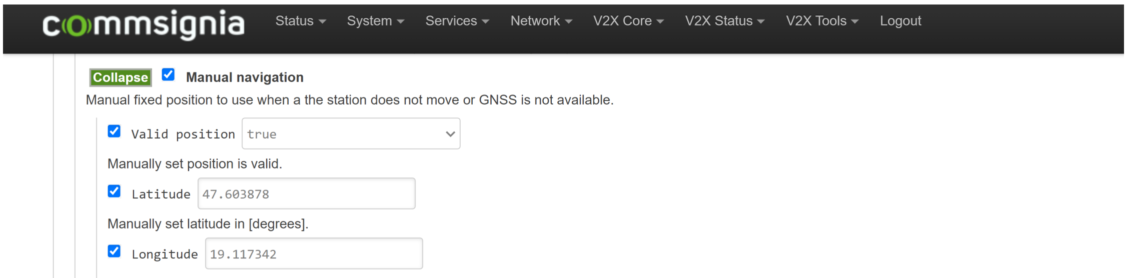
☑ `Navigation source` Manual

Select the navigation data source (for example integrated GNSS or GPSD). Not all sources are available for all platforms.

Figure 15. Navigation configuration

3. For the manual navigation source, set the `Navigation source` to `Manual`.

   a. To configure the manual navigation source, expand the **Manual navigation** option on the same page, as shown in Figure 16.



Collapse ☑ Manual navigation

Manual fixed position to use when a the station does not move or GNSS is not available.

☑ `Valid position` true

Manually set position is valid.

☑ `Latitude` 47.603878

Manually set latitude in [degrees].

☑ `Longitude` 19.117342

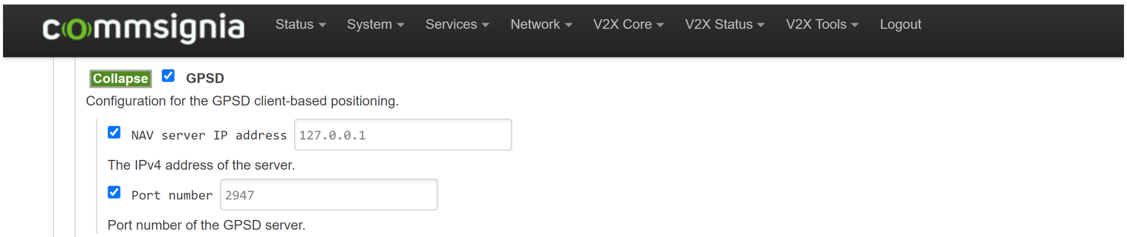
Figure 16. Manual navigation settings

   b. Expand and select the checkbox next to **Manual navigation** , check the box next to `Valid position` and set it to `true` , then enter the `Latitude` and `Longitude` information, as shown in Figure 16, and, if applicable, other values as well.

   c. Click on the Save & Apply button for the changes to take effect.

4. For the gpsd navigation source, set the`Navigation source` to `Gpsd`.

   a. To configure the gpsd navigation source, expand the **GPSD** option on the same page, as shown in Figure 16.



Collapse ☑ GPSD

Configuration for the GPSD client-based positioning.

☑ `NAV server IP address` 127.0.0.1

The IPv4 address of the server.

☑ `Port number` 2947

Port number of the GPSD server.

Figure 17. GPSD navigation settings

   b. Select the checkbox new **GPSD** and enter the gpsd server and port information, as shown in Figure 17.

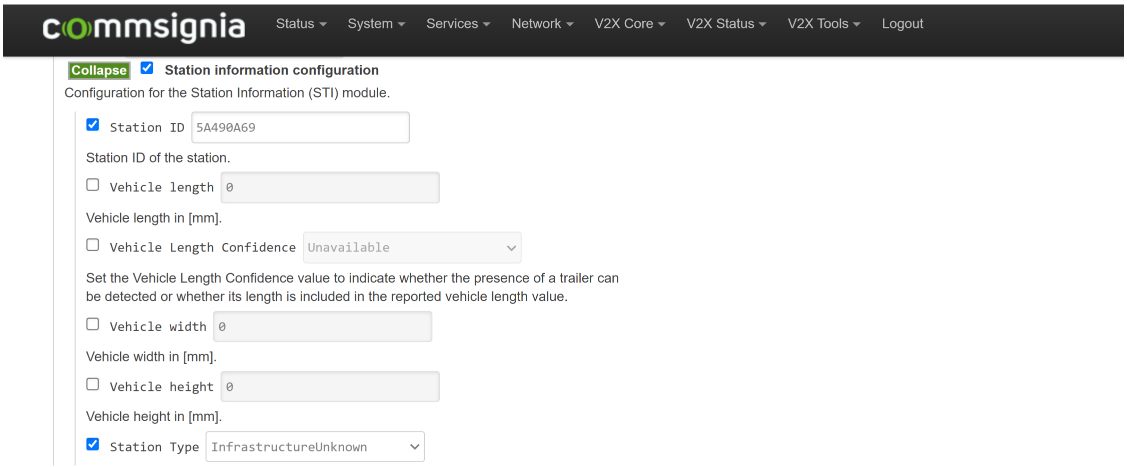
c. Click on the Save & Apply button for the changes to take effect.

4.4. Configuring station parameters

Station parameters can be optionally set for the RSUas follows.

1. Log into the device using SSH. For more information, refer to section “Connecting to the RSU over wireless or wired connection” [2].

2. Open the V2X Core → Core stack menu item and expand the option **Station information configuration**, as shown in Figure 18.



☑ Station information configuration

Configuration for the Station Information (STI) module.

☑ Station ID 5A490A69

Station ID of the station.

□ Vehicle length 0

Vehicle length in [mm].

□ Vehicle Length Confidence Unavailable

Set the Vehicle Length Confidence value to indicate whether the presence of a trailer can be detected or whether its length is included in the reported vehicle length value.

□ Vehicle width 0

Vehicle width in [mm].

□ Vehicle height 0

Vehicle height in [mm].

☑ Station Type InfrastructureUnknown

Figure 18. Station information settings

3. Select the checkbox next to **Station information configuration** and enter the required information. For example, for RSUs the `Station type` is `InfrastructureUnknown`.

4. Click on the Save & Apply button for the changes to take effect.

4.5. Configuring radio settings

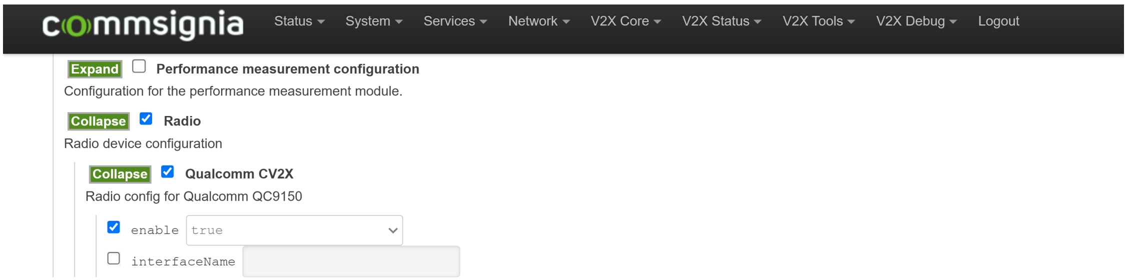
4.5.1. Configuring the radio interface

Radio interfaces can be set to be compliant with US or EU standards.

1. Log into the device using SSH. For more information, refer to section “Connecting to the RSU over wireless or wired connection” [2].

2. To enable the V2X communication, open the V2X Core → Core stack menu item, expand the option **Radio**. According to the radio hardware the following settings are available:

   a. For devices with Qualcomm radio (mainly US, C-V2X) the follow settings can be configured: Select the checkbox near **Qualcomm CV2X** as shown in Figure 19.



□ Performance measurement configuration

Configuration for the performance measurement module.

☑ Radio

Radio device configuration

☑ Qualcomm CV2X

Radio config for Qualcomm QC9150

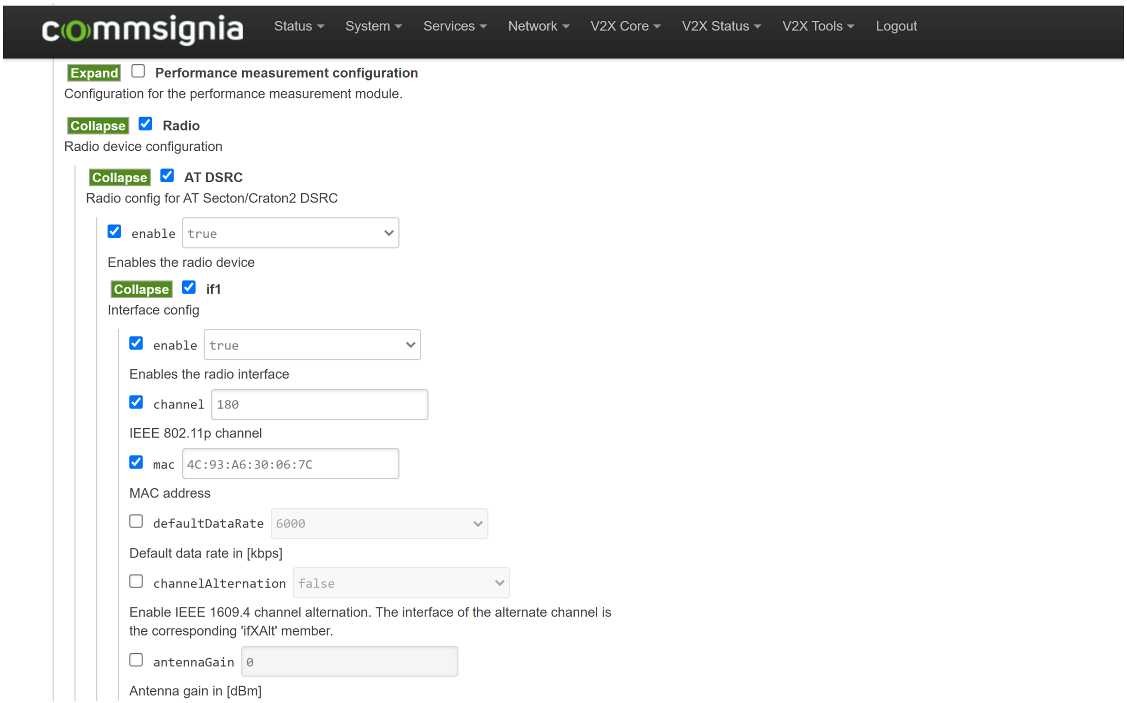
☑ enable true

□ interfaceName

Figure 19. Qualcomm radio interface settings

As Qualcomm configures all parameters automatically upon startup based on GPS information, according to the region; this option cannot be configured further.

b. For devices with Autotalks CUT2 radios (mainly EU, DSRC) the follow settings can be configured:
Select the checkbox near **AT DSRC** as shown in Figure 20.



Expand □ Performance measurement configuration
Configuration for the performance measurement module.

Collapse ☑ Radio
Radio device configuration

Collapse ☑ AT DSRC
Radio config for AT Secton/Craton2 DSRC

☑ enable true
Enables the radio device

Collapse ☑ if1
Interface config

☑ enable true
Enables the radio interface

☑ channel 180
IEEE 802.11p channel

☑ mac 4C:93:A6:30:06:7C
MAC address

□ defaultDataRate 6000
Default data rate in [kbps]

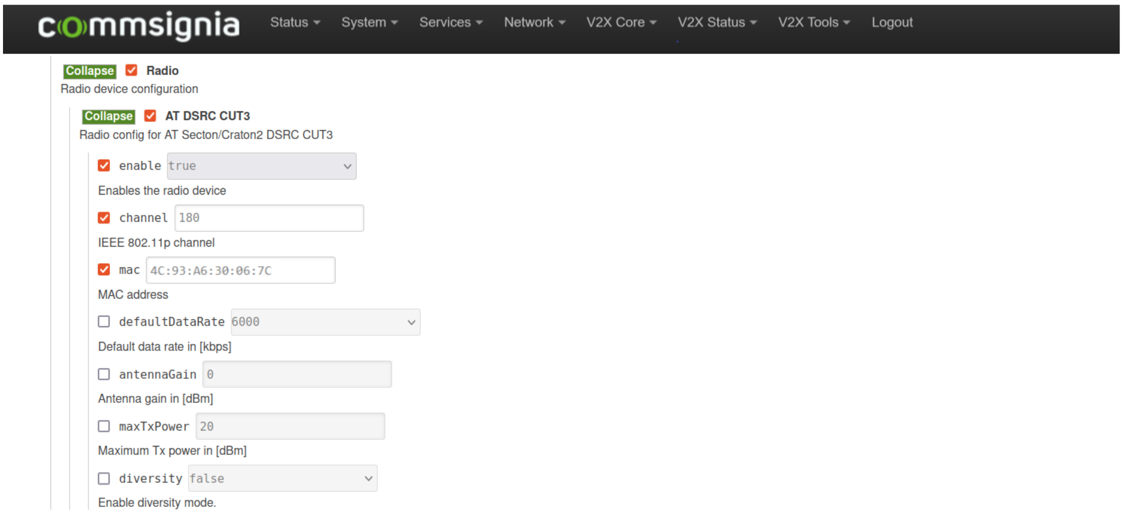
□ channelAlternation false
Enable IEEE 1609.4 channel alternation. The interface of the alternate channel is the corresponding 'ifXAlt' member.

□ antennaGain 0
Antenna gain in [dBm]

Figure 20. Autotalks CUT2 radio interface settings

For CUT2 radios the settings for the two interfaces can be configured separately. By default only the **if1** interface is enabled and all messages are transmitted and received through this interface. To enable the if2 interface expand the **if2** option and select the checkbox next to it and set the `enable` field to `true`. Channel, MAC address, data rate, antenna gain, and maximum transmission power can be set for both interfaces separately. Setting the `diversity` option to `true` set both interfaces to use the same, if1 channel to combine their signal for an improved signal reception.

c. For devices with Autotalks CUT3 radios (mainly EU, DSRC) the follow settings can be configured:
Select the checkbox near **AT DSRC CUT3** as shown in Figure 21.



☑ Radio
Radio device configuration

☑ AT DSRC CUT3
Radio config for AT Secton/Craton2 DSRC CUT3

☑ `enable` true
Enables the radio device

☑ `channel` 180
IEEE 802.11p channel

☑ `mac` 4C:93:A6:30:06:7C
MAC address

□ `defaultDataRate` 6000
Default data rate in [kbps]

□ `antennaGain` 0
Antenna gain in [dBm]

□ `maxTxPower` 20
Maximum Tx power in [dBm]

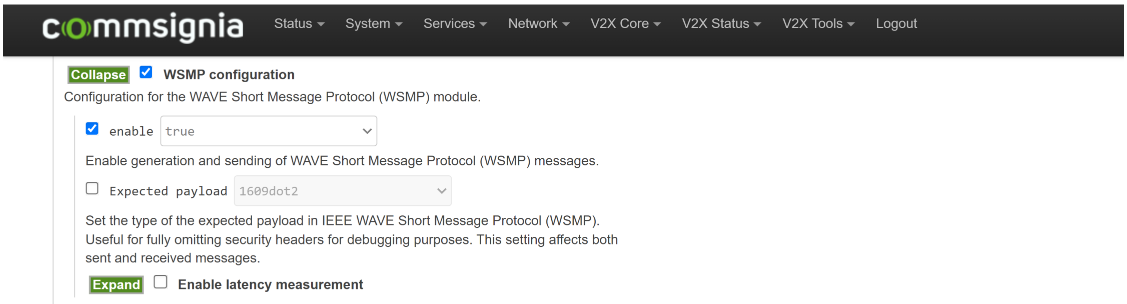
□ `diversity` false
Enable diversity mode.

Figure 21. Autotalks CUT3 radio interface settings

Channel, MAC address, data rate, antenna gain and maximum transmission power can be set for only interface if1. Setting the `diversity` option to `true` enables the second interface to use the if1 channel to combine the signal of both interfaces for an improved signal reception. Channel alternation is not available for CUT3 radios.

3. Further configurations for US settings

   a. Turn on the WAVE Short Message Protocol (WSMP) module for US regional standard compliance, by expanding the option **WSMP** and selecting the checkbox next to **WSMP configuration**, as shown in Figure 22.



☑ WSMP configuration
Configuration for the WAVE Short Message Protocol (WSMP) module.

☑ `enable` true
Enable generation and sending of WAVE Short Message Protocol (WSMP) messages.

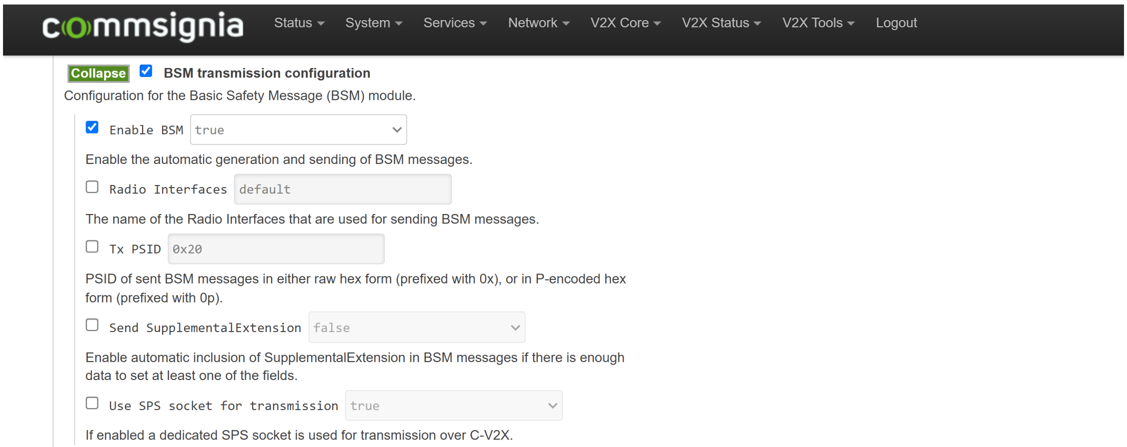
□ `Expected payload` 1609dot2
Set the type of the expected payload in IEEE WAVE Short Message Protocol (WSMP). Useful for fully omitting security headers for debugging purposes. This setting affects both sent and received messages.

□ Enable latency measurement

Figure 22. WSMP configuration

Select the checkbox next to `enable` and set it to `true`.

   b. Turn on the Basic Safety Message (BSM) module for US regional compliant basic V2X messages by expanding the option **BSM** and selecting the checkbox next to **BSM Transmission configuration**, as shown in Figure 23.



☑ BSM transmission configuration

Configuration for the Basic Safety Message (BSM) module.

☑ `Enable BSM` true

Enable the automatic generation and sending of BSM messages.

☐ `Radio Interfaces` default

The name of the Radio Interfaces that are used for sending BSM messages.

☐ `Tx PSID` 0x20

PSID of sent BSM messages in either raw hex form (prefixed with 0x), or in P-encoded hex form (prefixed with 0p).

☐ `Send SupplementalExtension` false

Enable automatic inclusion of SupplementalExtension in BSM messages if there is enough data to set at least one of the fields.

☐ `Use SPS socket for transmission` true

If enabled a dedicated SPS socket is used for transmission over C-V2X.

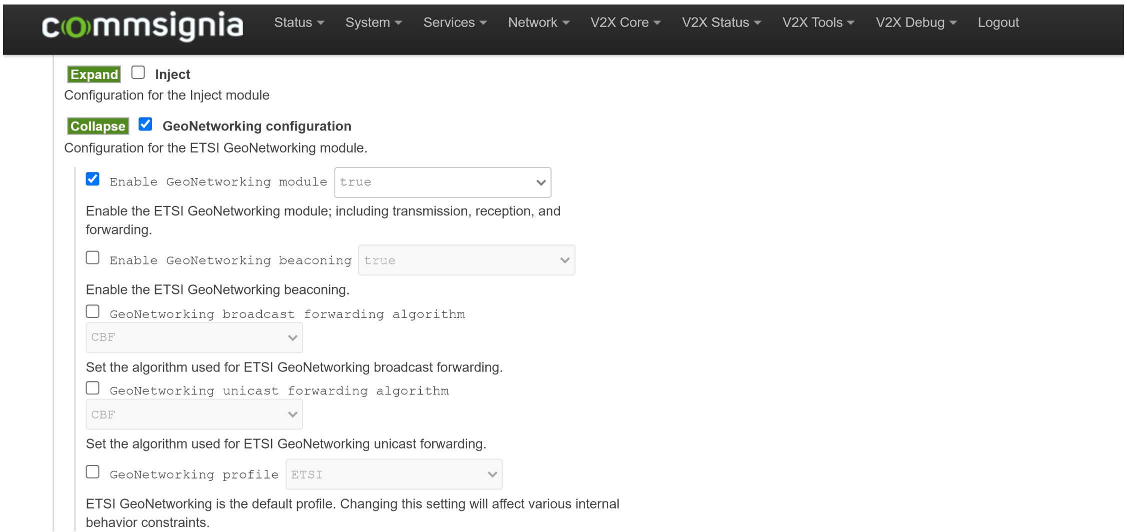
Figure 23. BSM module

Select the checkbox next to `Enable BSM` and set it to `true`.

> Please note that for US regional standards Dedicated Short-Range Communication (DSRC) radio is not available.

4. Further configurations for EU settings

   a. Turn on the GeoNetworking module for EU regional standard compliance, by expanding and selecting the checkbox next to the option **GeoNetworking configuration**, as shown in Figure 24.



☐ Inject

Configuration for the Inject module

☑ GeoNetworking configuration

Configuration for the ETSI GeoNetworking module.

☑ `Enable GeoNetworking module` true

Enable the ETSI GeoNetworking module; including transmission, reception, and forwarding.

☐ `Enable GeoNetworking beaconing` true

Enable the ETSI GeoNetworking beaconing.

☐ `GeoNetworking broadcast forwarding algorithm` CBF

Set the algorithm used for ETSI GeoNetworking broadcast forwarding.

☐ `GeoNetworking unicast forwarding algorithm` CBF

Set the algorithm used for ETSI GeoNetworking unicast forwarding.

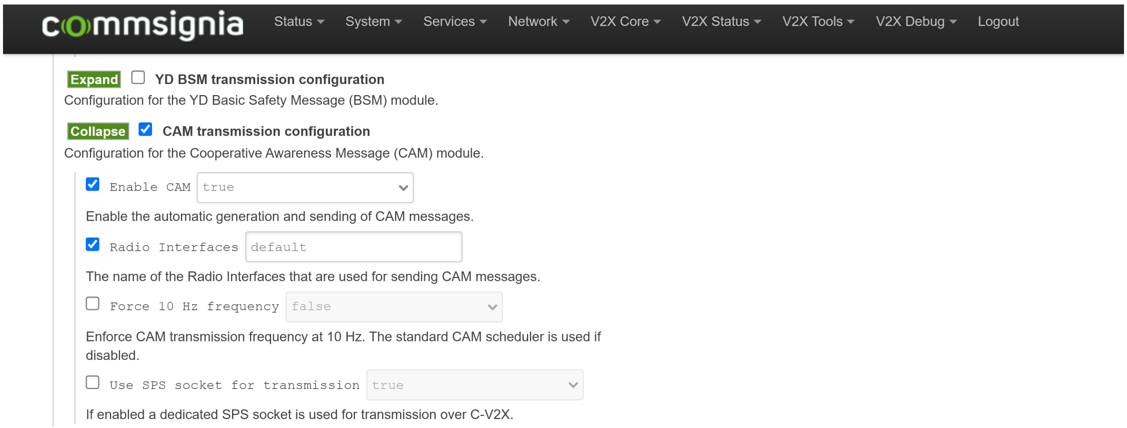
☐ `GeoNetworking profile` ETSI

ETSI GeoNetworking is the default profile. Changing this setting will affect various internal behavior constraints.

Figure 24. GeoNetworking configuration

Select the checkbox next to `Enable GeoNetworking module` and set it to `true`.

   b. Turn on the Cooperative Awareness Message (CAM) module for EU regional compliant basic V2X messages by by expanding and selecting the checkbox next to the option **CAM transmission configuration**, as shown in Figure 25.



Expand □ YD BSM transmission configuration

Configuration for the YD Basic Safety Message (BSM) module.

Collapse ☑ CAM transmission configuration

Configuration for the Cooperative Awareness Message (CAM) module.

☑ `Enable CAM` true

Enable the automatic generation and sending of CAM messages.

☑ `Radio Interfaces` default

The name of the Radio Interfaces that are used for sending CAM messages.

□ `Force 10 Hz frequency` false

Enforce CAM transmission frequency at 10 Hz. The standard CAM scheduler is used if disabled.

□ `Use SPS socket for transmission` true

If enabled a dedicated SPS socket is used for transmission over C-V2X.

Figure 25. CAM transmission configuration

Select the checkbox next to `Enable CAM` and set it to `true`.

5. Click on the Save & Apply button for the changes to take effect.

4.5.2. Configuring Dual Active mode

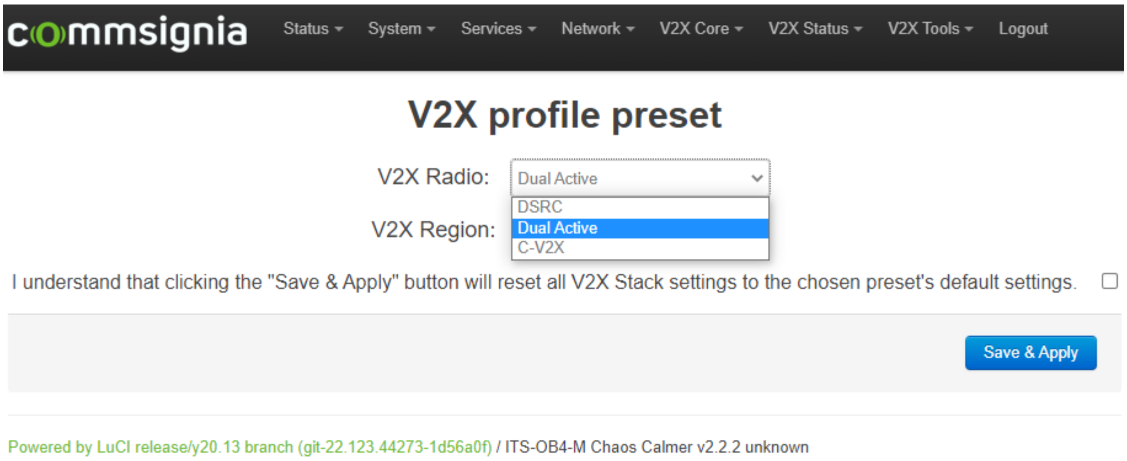
In Dual Active mode, both the DSRC and V2X antennas can be used simultaneously for broadcast and receiving.

4.5.2.1. Prerequisites

To enable Dual Active mode, a firmware version **y20.13.x** or later is required. To verify the firmware version, please select the **Status** → **Overview** menu item, and check the **System** section. In addition, the firmware version needs to support both radio standards, this is indicated by the naming convention of the firmware. For example "ob4-cut2-qc9150cv2x-sectondsrc-qcgnss" indicates a C-V2X radio manufactured by Qualcomm Technologies, Inc (qc9150cv2x) and a SECTON DSRC radio by Autotalks, Ltd. (sectondsrc). Devices supplied as "Dual Ready" are Dual Active compatible as well.

4.5.2.2. Enabling Dual Active mode

To enable Dual Active mode, please open the **V2X Core** → **V2X profile preset** menu item. Set the V2X Radio to "Dual Active," as shown in Figure 26 and select the appropriate region in V2X Region. To save the changes, check the box on the right of the statement and click on the Save & Apply button.



V2X profile preset

V2X Radio: Dual Active

V2X Region:

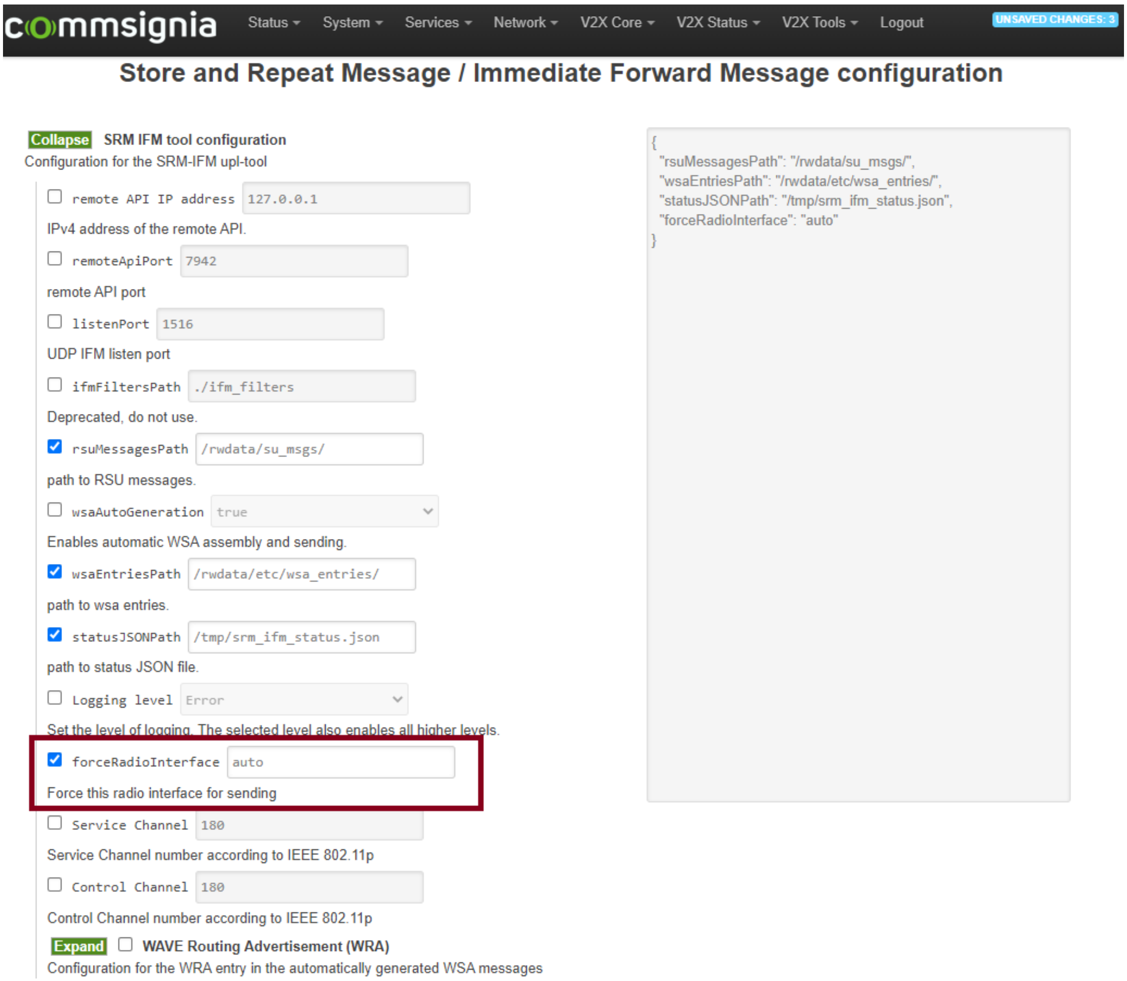
I understand that clicking the "Save & Apply" button will reset all V2X Stack settings to the chosen preset's default settings. □

Powered by LuCI release/y20.13 branch (git-22.123.44273-1d56a0f) / ITS-OB4-M Chaos Calmer v2.2.2 unknown

Figure 26. Enabling Dual Active mode

In addition to enabling the Dual Active mode, two configuration changes need to be performed for radio interfaces in the Store and Repeat Message/Immediate Forward message (SRM IFM) and Traffic Light Controller (TLC) configuration pages.

Please open the **V2X tools** → **SRM/IFM** menu item and expand "SRM IFM tool configuration." Set the **forceRadioInterface** to "auto," as shown in Figure 27.



Store and Repeat Message / Immediate Forward Message configuration

SRM IFM tool configuration
Configuration for the SRM-IFM upl-tool

☐ remote API IP address: 127.0.0.1
IPv4 address of the remote API.

☐ remoteApiPort: 7942
remote API port

☐ listenPort: 1516
UDP IFM listen port

☐ ifmFiltersPath: ./ifm_filters
Deprecated, do not use.

☑ rsuMessagesPath: /rwdata/su_msgs/
path to RSU messages.

☐ wsaAutoGeneration: true
Enables automatic WSA assembly and sending.

☑ wsaEntriesPath: /rwdata/etc/wsa_entries/
path to wsa entries.

☑ statusJSONPath: /tmp/srm_ifm_status.json
path to status JSON file.

☐ Logging level: Error
Set the level of logging. The selected level also enables all higher levels.

☑ forceRadioInterface: auto
Force this radio interface for sending

☐ Service Channel: 180
Service Channel number according to IEEE 802.11p

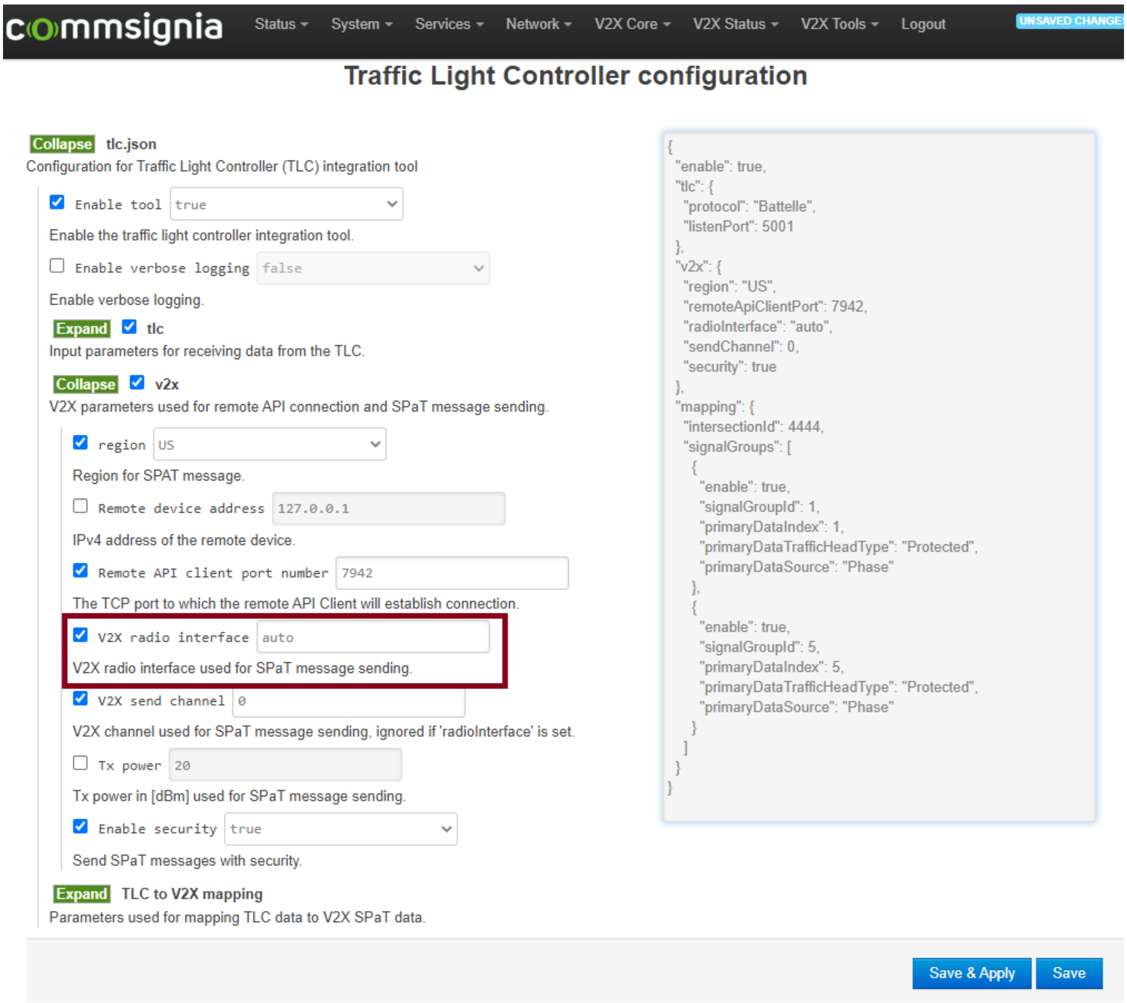
☐ Control Channel: 180
Control Channel number according to IEEE 802.11p

☐ WAVE Routing Advertisement (WRA)
Configuration for the WRA entry in the automatically generated WSA messages

```
{
 "rsuMessagesPath": "/rwdata/su_msgs/",
 "wsaEntriesPath": "/rwdata/etc/wsa_entries/",
 "statusJSONPath": "/tmp/srm_ifm_status.json",
 "forceRadioInterface": "auto"
}
```

Figure 27. SRM/IFM tool configuration settings for Dual Active mode

Finally, please open the **V2X tools** → **TLC** menu item and expand the **tlc.json** tree, then expand the **v2x** branch. Set the **V2X radio interface** to "auto," as shown in Figure 28.



Traffic Light Controller configuration

Collapse tlc.json
Configuration for Traffic Light Controller (TLC) integration tool

☑ Enable tool true
Enable the traffic light controller integration tool.

☐ Enable verbose logging false
Enable verbose logging.

Expand ☑ tlc
Input parameters for receiving data from the TLC.

Collapse ☑ v2x
V2X parameters used for remote API connection and SPaT message sending.

☑ region US
Region for SPAT message.

☐ Remote device address 127.0.0.1
IPv4 address of the remote device.

☑ Remote API client port number 7942
The TCP port to which the remote API Client will establish connection.

☑ V2X radio interface auto
V2X radio interface used for SPaT message sending.

☑ V2X send channel 0
V2X channel used for SPaT message sending, ignored if 'radioInterface' is set.

☐ Tx power 20
Tx power in [dBm] used for SPaT message sending.

☑ Enable security true
Send SPaT messages with security.

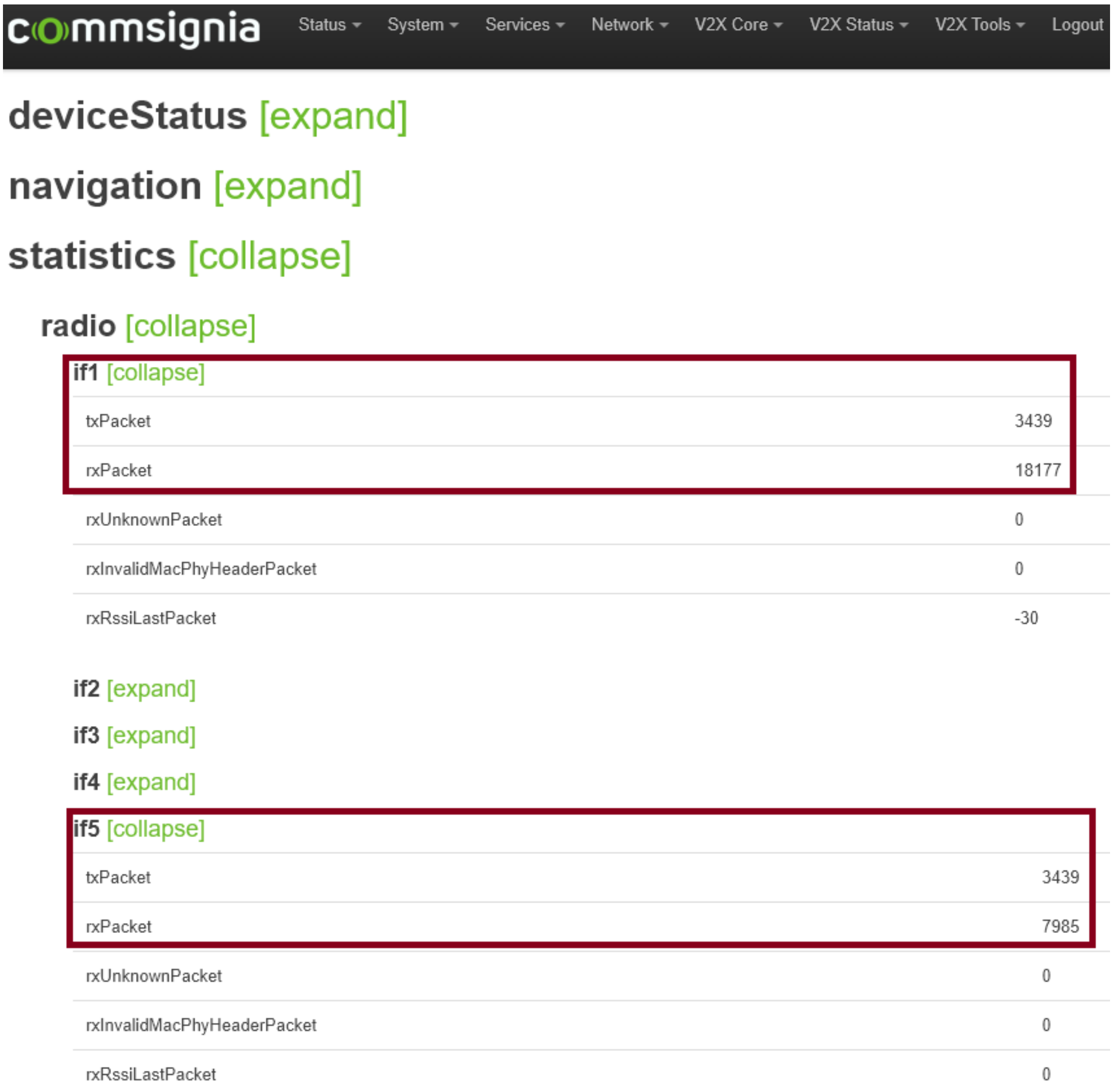
Expand TLC to V2X mapping
Parameters used for mapping TLC data to V2X SPaT data.

```
{
 "enable": true,
 "tlc": {
  "protocol": "Battelle",
  "listenPort": 5001
 },
 "v2x": {
  "region": "US",
  "remoteApiClientPort": 7942,
  "radioInterface": "auto",
  "sendChannel": 0,
  "security": true
 },
 "mapping": {
  "intersectionId": 4444,
  "signalGroups": [
   {
    "enable": true,
    "signalGroupId": 1,
    "primaryDataIndex": 1,
    "primaryDataTrafficHeadType": "Protected",
    "primaryDataSource": "Phase"
   },
   {
    "enable": true,
    "signalGroupId": 5,
    "primaryDataIndex": 5,
    "primaryDataTrafficHeadType": "Protected",
    "primaryDataSource": "Phase"
   }
  ]
 }
}
```

Figure 28. TLC settings for Dual Active mode

4.5.2.3. Verification of Dual Active mode

To verify that both the DSRC and V2X radios are transmitting and receiving packets, please open the V2X status → Status menu item and expand **statistics**, then expand **radio**. As shown in Figure 29, there are five interfaces labelled **if1–if5**. Expand **if1** and **if5**, which are the interfaces for the DSRC and C-V2X radios, respectively. If the values of the transmitted (txPackets) and received (rxPackets) packets are increasing, than both radios are broadcasting and receiving; thus, the Dual Active mode is operational.



deviceStatus [expand]

navigation [expand]

statistics [collapse]

radio [collapse]

if1 [collapse]

txPacket	3439
rxPacket	18177
rxUnknownPacket	0
rxInvalidMacPhyHeaderPacket	0
rxRssiLastPacket	-30

if2 [expand]

if3 [expand]

if4 [expand]

if5 [collapse]

txPacket	3439
rxPacket	7985
rxUnknownPacket	0
rxInvalidMacPhyHeaderPacket	0
rxRssiLastPacket	0

Figure 29. Transmitted and received packet statistics for DSRC and V2X radios

5. Message handling on RSUs

Roadside units broadcast standard V2X messages to other devices in their vicinity. Commsignia RSUs can handle several different types of custom messages. In addition, tools are also provided on the devices to convert different message formats.

5.1. Converting data formats

Commsignia provides a tool on the device to convert XML data format to standardized Abstract Syntax Notation One (ASN.1) interface description language format used by certain V2X messages. The asn1x tool can be used to convert data between ASN.1 Unaligned Packed Encoding Rules (UPER), Extensible Markup Language (XML), JSON, JSON Encoding Rules (JER), Octet Encoding Rules (OER), and XE formats.

- After connecting to the device over SSH with root access (see section “Connecting to the RSU over wireless or wired connection” [2]), the conversion tool can be started using the following syntax:

  ```
  asn1x -i <input format> -o <output format> -T <string specifying the type>
  ```

  The following values are available for the the -i and -o switches to denote the format: jer, json, oer, uper, xer, and xml.
  The -T switch, followed by a string, specifies the type of the message; the possible message type strings are as follows: CN_MSG_FRAME, CN_BSM CN_MAP, CN_RSI CN_RSM, CN_SPAT, EU_CAM, EU_CoopAwareness, EU_CPM, EU_CollectivePerceptionMessage, EU_DENM, EU_DecentralizedEnvironmentalNotificationMessage, EU_IVI, EU_IviStructure, EU_MAP EU_SPAT, US_MSG_FRAME, US_BSM, US_RTCMcorrections, US_SPAT, US_TravelerDataFrame, US_WSA, and Cv2xPreconfig.

- For example, to convert UPER to XML data format the echo command can be used, as follows:

  ```
  echo \
  "001f2a001000609e2f1f0c73698d320000a92c400f28 \
  0002001020a95c59290623c73bc647af58418000000810" \
  | asn1x -i uper -o xml -T US_MSG_FRAME > TIM.xml
  ```

- To convert XML to JSON format, for example, the TIM.xml file above, the cat command can be used, as shown in the following example:

  ```
  cat TIM.xml | asn1x -i xml -o json -T US_MSG_FRAME > TIM.json
  ```

5.2. Store-and-Repeat messages (SRMs)

Store-and-Repeat messages, such as MAP or Traveler Information Messages (TIMs), can be conveniently created in the Commsignia Central Device and Data Management Platform or using Commsignia V2X Studio. In addition to the creation of these messages both Commsignia products are capable of deploying messages to the appropriate RSU and starting their transmission automatically.

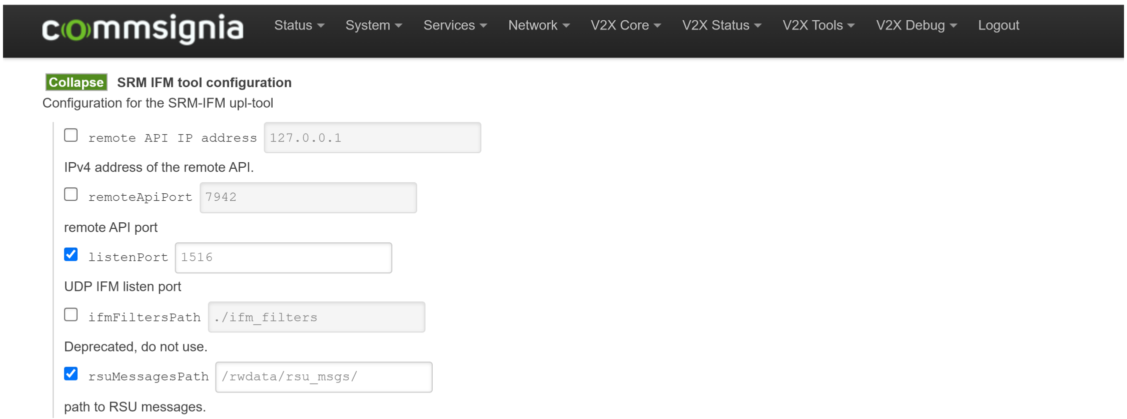
However, any custom message in RSU 4.1 format can be deployed to RSUs manually, and further configuration options are available for the handling and transmission of these messages.

5.2.1. Configuring SRM settings

To change the default directory of the messages on the device using the GUI, proceed as follows:

1. Log into the device using SSH. For more information, refer to section “Connecting to the RSU over wireless or wired connection” [2].

2. The location of the directory can be changed on the GUI under the **V2X Tools** → **SRM/IFM** menu item, as shown in Figure 30.



SRM IFM tool configuration

Configuration for the SRM-IFM upl-tool

□ remote API IP address 127.0.0.1

IPv4 address of the remote API.

□ remoteApiPort 7942

remote API port

☑ listenPort 1516

UDP IFM listen port

□ ifmFiltersPath ./ifm_filters

Deprecated, do not use.

☑ rsuMessagesPath /rwdata/rsu_msgs/

path to RSU messages.

Figure 30. Changing the location of the SRM directory

3. Select the box next to `rsuMessagesPath` and enter the path of the new directory.

4. Click on the Save & Apply button for the changes to take effect on the device.

Alternatively, the `muci` tool can be used as follows:

1. Log into the device using SSH. For more information, refer to section "Connecting to the RSU over wireless or wired connection" [2].

2. Use the following command to set a new directory for the SRMs:

```
muci set ifm.rsuMessagesPath </new directory>
```

3. Restart the V2X stack using the command

```
unplugged-rt-restart.sh
```

5.2.2. Formatting SRMs

Please note that all SRMs need to be in RSU 4.1 format. The message format needs to match the regional standard.

The following example shows a MAP message:

```
Version=0.7
Type=MAP
PSID=E0000017
Priority=0
TxMode=CONT
TxChannel=SCH
TxInterval=1
DeliveryStart=08/18/1990, 15:55
DeliveryStop=08/18/2039, 15:59
Signature=False
Encryption=False
Payload=0012...
```

As can be seen in the example, the transmission interval (`TxInterval`) needs to be set to 1, which means that the messages are transmitted with a frequency of 1 Hz. The start and expiration time of the message can be set in the `DeliveryStart` and `DeliveryStop` fields, respectively.

Please ensure that the signing of the messages are compatible with the security settings of the device:

- If the system is enrolled and the security is turned on, use `Signature=True` to transfer signed SRMs. Setting the signature to `False` is typically not recommended on an enrolled device.
- If the system is not enrolled or security is turned off, use `Signature=False` to trasmit unsigned SRMs. **Do not** set the signature to `True` on such devices, as the messages cannot be signed, and fail to be transmitted.

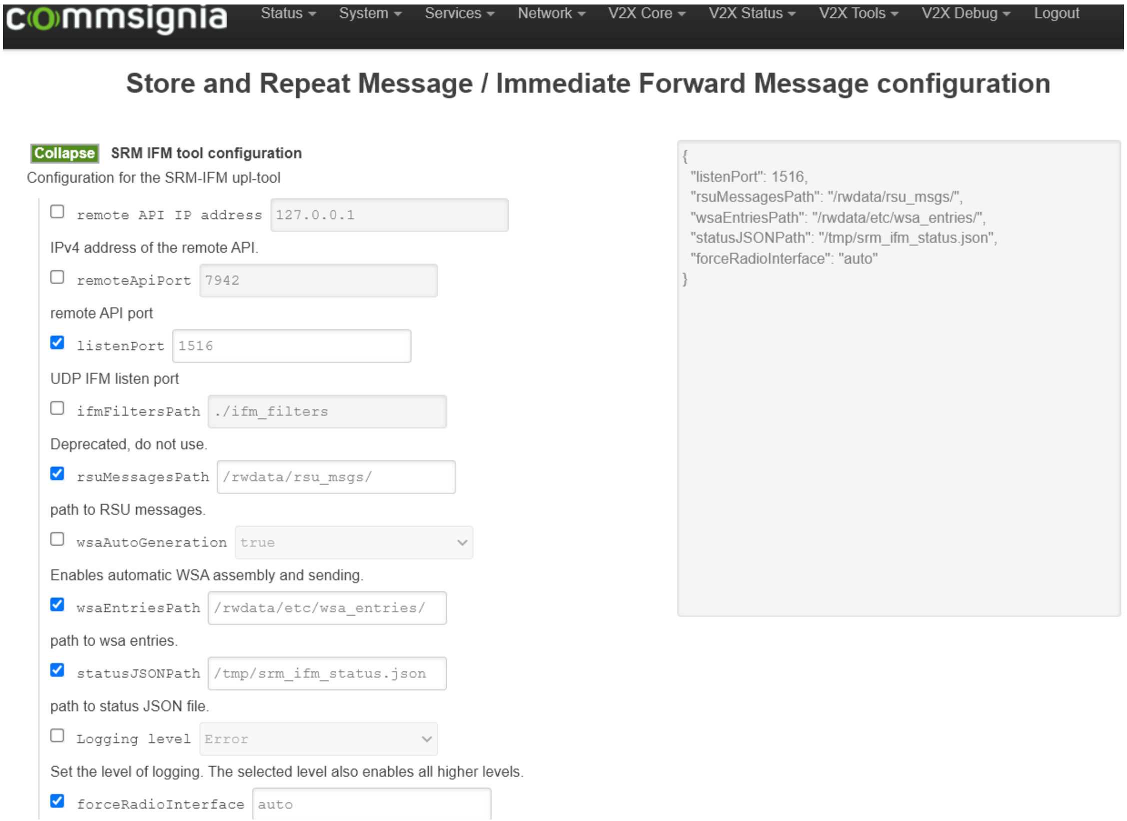
5.3. Immediate forwarding

The RSU is capable of relaying appropriately formatted messages fed through the User Datagram Protocol (UDP) port of the device. These Immediate Forward Messages (IFMs) are directly forwarded to the radio and only signed if it requested.

5.3.1. Configuring IFM settings

To change the UDP listening port or message directory on the device, proceed as follows:

1. Log into the GUI. For more information, refer to section “Connecting to the RSU over wireless or wired connection” [2].
2. Open the **V2X Tools** → **SRM/IFM** menu item as shown in Figure 31.



Store and Repeat Message / Immediate Forward Message configuration

SRM IFM tool configuration

Configuration for the SRM-IFM upl-tool

☐ remote API IP address 127.0.0.1

IPv4 address of the remote API.

☐ remoteApiPort 7942

remote API port

☑ listenPort 1516

UDP IFM listen port

☐ ifmFiltersPath ./ifm_filters

Deprecated, do not use.

☑ rsuMessagesPath /rwdata/rsu_msgs/

path to RSU messages.

☐ wsaAutoGeneration true

Enables automatic WSA assembly and sending.

☑ wsaEntriesPath /rwdata/etc/wsa_entries/

path to wsa entries.

☑ statusJSONPath /tmp/srm_ifm_status.json

path to status JSON file.

☐ Logging level Error

Set the level of logging. The selected level also enables all higher levels.

☑ forceRadioInterface auto

```
{
 "listenPort": 1516,
 "rsuMessagesPath": "/rwdata/rsu_msgs/",
 "wsaEntriesPath": "/rwdata/etc/wsa_entries/",
 "statusJSONPath": "/tmp/srm_ifm_status.json",
 "forceRadioInterface": "auto"
}
```

Figure 31. SRM/IFM configuration menu

3. To change the default UDP listening port, select the checkbox next to `listenPort` and enter a new value.