User Guide

ST Engineering

MDM2510 IP Satellite Modem
R4.6.1

Revision 1.1

May 17, 2021

powered by Newtec iDirect

Table of Contents

1 Copyright

2 About this Guide

The *MDM2510 User Guide* provides detailed information necessary to understand and use the MDM2510 Satellite Modem. It describes each of the UI pages associated with installing, configuring and monitoring the modem, as well as basic troubleshooting tips.

The parameter values in the figures are examples. They are randomly chosen and may differ from the predefined settings on your modem.

2.1 Revision History

Version	Date	Reason of new version
1.0	December, 2020	Initial version of this release.
1.1	May, 2021	New features on Expert Mode included. Reviewed Terminal Installation part.

2.2 Important Safety Precautions

Please read the *Compliance and Safety Guide* provided with your modem before installing and using the equipment.

2.3 Cautions and Symbols

The following symbols appear in this guide:

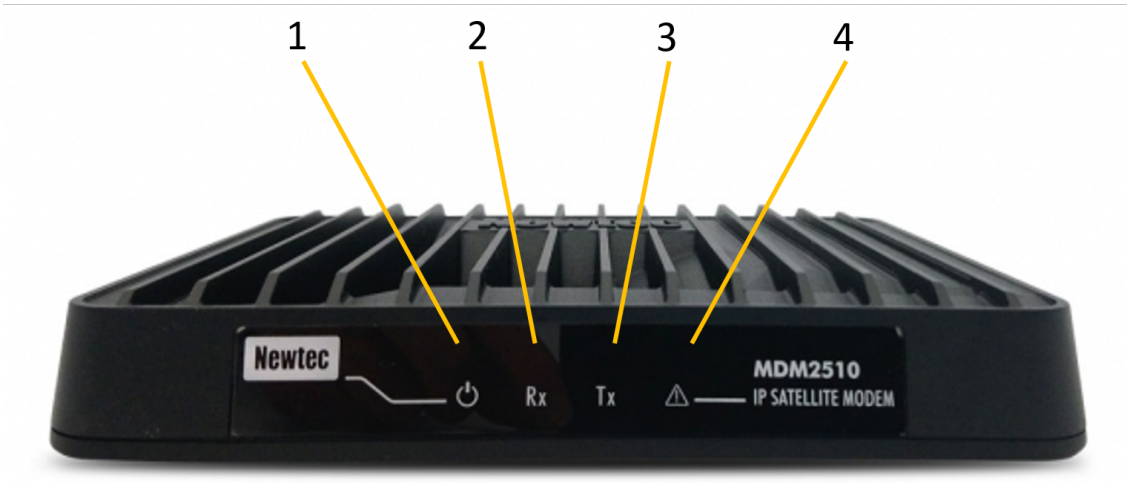
A caution message indicates a hazardous situation that, if not avoided, may result in minor or moderate injury. It may also refer to a procedure or practice that, if not correctly followed, could result in equipment damage or destruction.

A hint message indicates information for the proper operation of your equipment, including helpful hints, shortcuts or important reminders.

A reference message is used to direct to a location in a document with related document or a web-link.

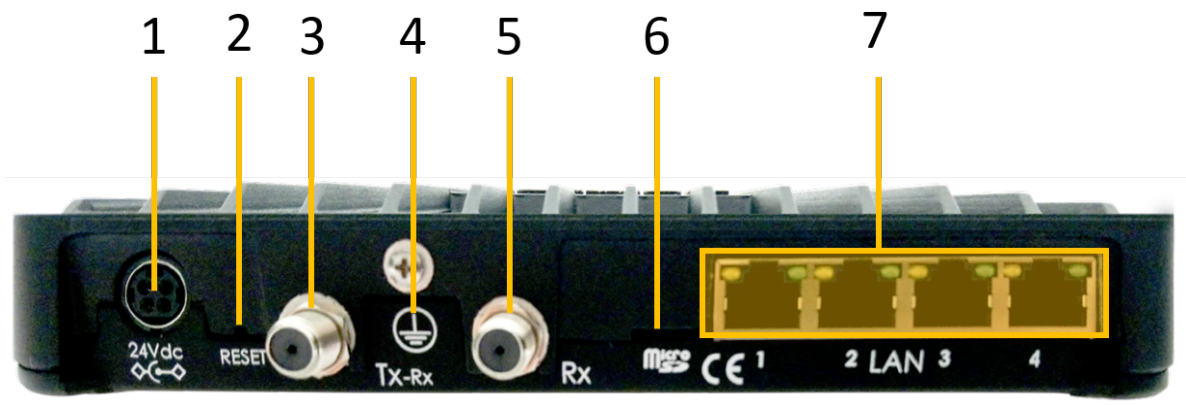
3 Modem Description

3.1 Modem Front Panel



Nr	What	Description
1	Power LED	White continuous - when powered up.
2	Rx LED	White continuous - forward satellite signaling receiving.
3	Tx LED	White blinking / continuous - traffic transmitting via the satellite link.
4	Warning LED	Yellow continuous - when the terminal is not logged on to the satellite network. This LED is also used to indicate the out-of-band configuration status. For more information, refer to Administration on page 90.

3.2 Modem Back Panel



Nr	What	Description
1	Power Connector	24 VDC
2	Reset button	Multi-functional button: • Press briefly (less than 10 seconds) to reboot the modem. • Press and hold for more than 10 seconds to perform a factory reset. This will reboot the modem and change all IP settings back to the default factory settings. ***Warning*** *- Do not use metal or conductive objects to press the reset button. Use a plastic or wooden object, like a toothpick; make sure it is non-conductive.*
3	TX connector	Indoor connection for the transmit coax cable.
4	Ground (⏚)	The earth ground is used when the modem is installed within a rack and ensures that all equipment fixed within that rack are at the same technical earth potential. ***Warning*** *- In accordance to TNV-1 grounding requirements, the grounding thread of the modem must be connected according to the local area codes and regulations.* *The device must be permanently connected to the protective earth by a skilled person.*
5	RX connector	Indoor connection for the receive coax cable.
6	Micro SD slot	The micro SD slot with SD card is used for specific purposes, such as storing GXT files. ***Warning*** *- Do not remove the SD card. If removed, gently re-insert the SD card in the micro SD slot.*

7	Four Gigabit Ethernet cable connectors	Connection for the LAN, type RJ45. Each connector has two LEDs: • The LED at the left of the connector indicates the link layer status (orange continuous). • The LED at the right of the connector indicates that Ethernet frames are received or transmitted (green blinking).

3.3 Power Supply

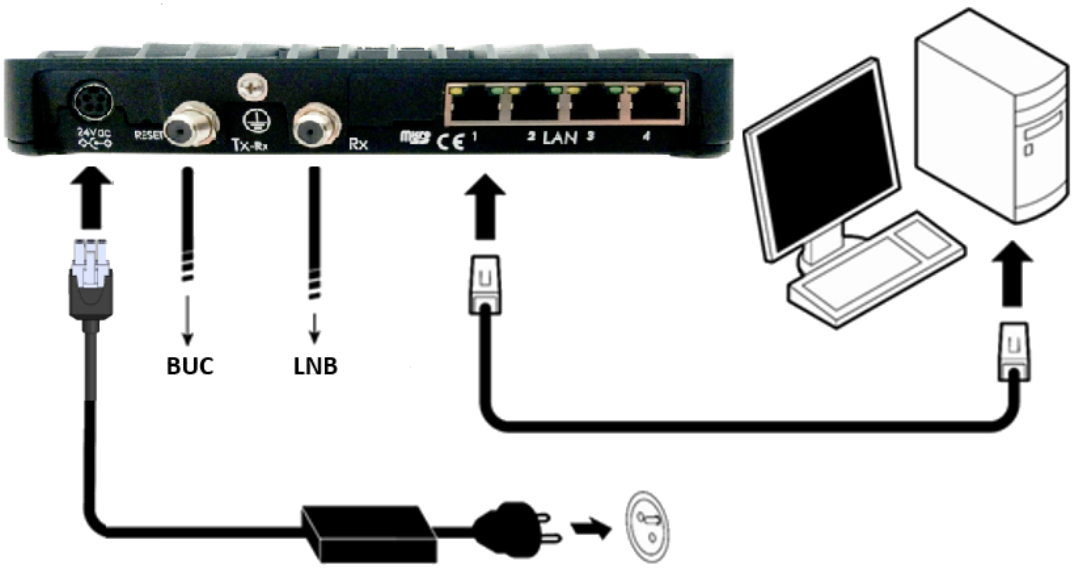
AC/DC Converter

• DC voltage: 24 VDC (external mains adapter) • Mains adaptor input: Mains AC, 50 Hz \ 220-260 V and 60 Hz \ 100-130 V • Power consumption: < 20 W • DIN 4P-din connector power supply locking pin connector	

4 Modem Web Interface

4.1 Connect Computer to Modem

1. Plug the network cable in the modem's and your computer's Ethernet ports.
2. Connect the power adapter provided in the box to the modem and a wall outlet.



3. Make sure your computer is set to DHCP. Your computer will receive an IP address from the modem.

To check and/or change your IP settings, please refer to the help pages of the Operating System on your computer.

4.2 Access Modem Web Interface

In the default operational mode a connected computer should be configured in DHCP mode to automatically receive its IP address and the IP address of a DNS server. The modem will act as the DHCP server for the computer.

Browse to the web interface

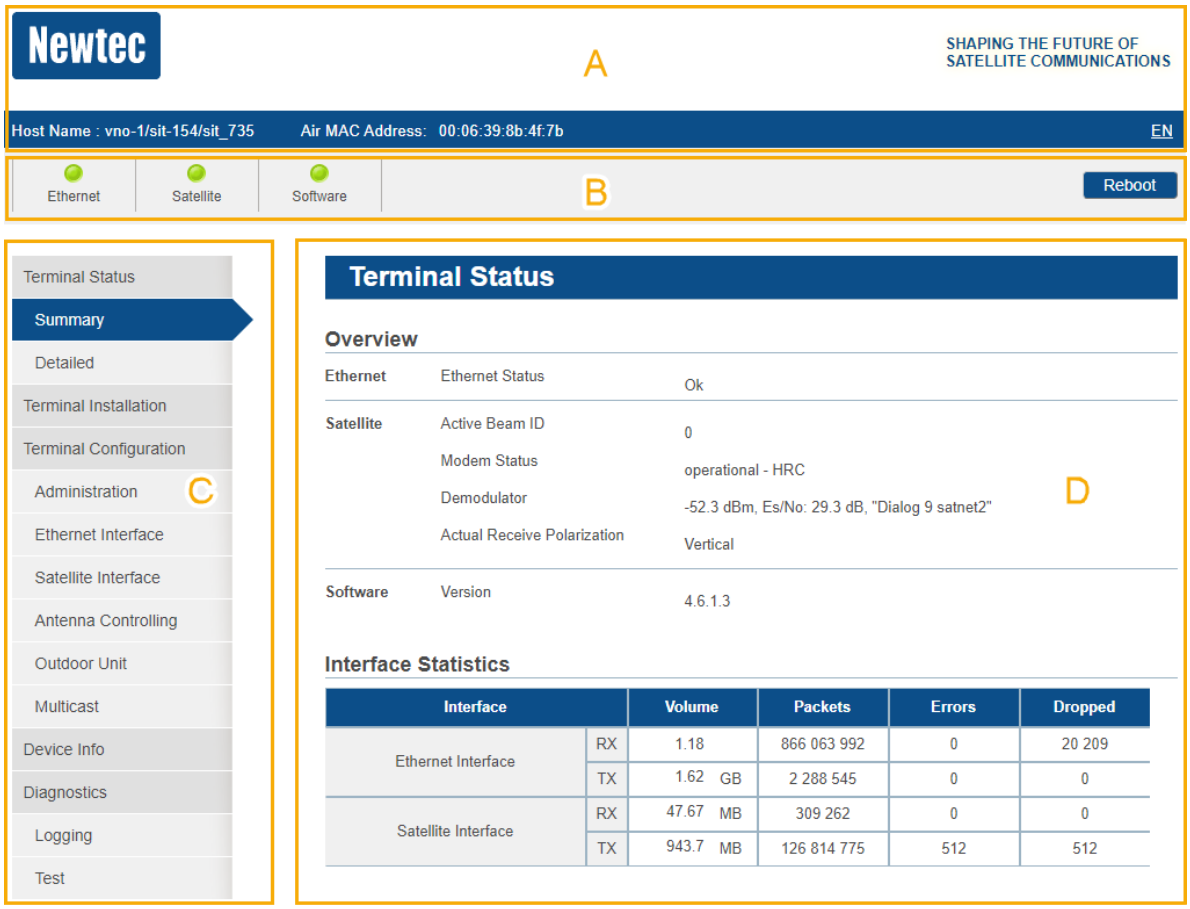
Type the modem's default IP address in the address bar of the browser: 192.168.1.1.

The first time your modem starts up, you are prompted for the Expert password in order to start the installation procedure. If your modem has already been installed before, you are re-directed to the Status page of the terminal.

When the terminal is not linked to the satellite network the computer will automatically receive its IP address from the modem after three minutes, and you will be able to browse the web interface.

If no DHCP address is assigned to your modem, remove the Ethernet cable from your computer. Wait a few seconds and plug the Ethernet cable back into your computer. If the issue persists, you can assign a static IP address to your computer.

4.3 General Layout



Each of the web interface pages contains the same elements.

- **A - Banner** with the terminal's host name as provisioned in the Dialog system, the Air MAC address and the languages in which the GUI can be displayed.
- **B - Status bar** shows the most important status LEDs. The details are specified in the body of the Terminal Status page.
- **C - Menu structure** or site navigation. Click an item to view the corresponding body.
- **D - Body** displays the actual content of the web interface page. It always shows the page title and one or more content blocks or sections.

4.4 Status Bar

4.4.1 Ethernet LED

The **Ethernet** LED indicates the status of the Ethernet connection to the modem.

LED Color Code	Description
Red	Connection is not OK.
Yellow	Connection is OK, but no IP address is handed out. This only appears when DHCP is enabled.
Green	Connection is OK. When DHCP is enabled, an IP address is handed out.

4.4.2 Satellite LED

The **Satellite** LED indicates the status of the satellite connection to the modem.

LED Color Code	Description
Red	No connectivity, no valid signal received.
Yellow	A valid signal was received and the terminal is trying to log on to the satellite network.
Green	The system is operational and the terminal is logged on to the satellite network.

4.4.3 Software LED

The **Software** LED provides information about the installed software or the updates.

LED Color Code	Description
Red	The terminal has a newer software version than the running software version, but the newer software version was not selected because the software upgrade process failed.
Yellow	The terminal is retrieving new software via satellite. This can take up to ten minutes.

Green	The terminal is running with the latest software version known by the terminal.

4.4.4 [optional] VPN LED

The **VPN** LED indicates the status of IPsec.

LED Color Code	Description
Red	No IKE nor IPsec tunnel have been set up.
Yellow	The IKE tunnel is set up, the IPsec tunnel is not set up.
Green	Both IKE and IPSec tunnels are up and running.

The VPN IPsec is an optional feature. When the feature is not supported, the VPN LED is not available.

In case the feature is supported but not enabled, the VPN LED is not available.

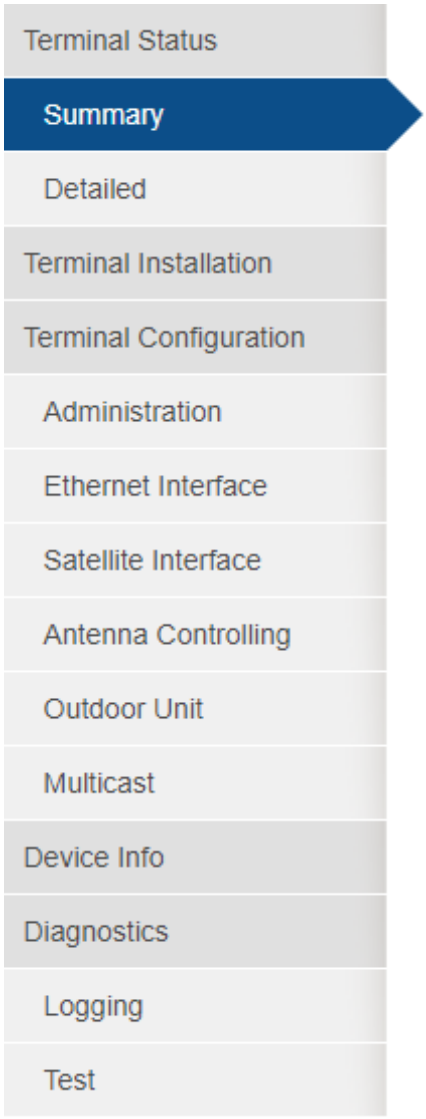
4.4.5 Reboot Modem

Click Reboot in the upper right of the status bar to restart the terminal. The modem will reboot and return to the Status page.

This may take up to one minute, including satellite link initialization.

You can also reboot the terminal using the hardware button. Refer to Modem Back Panel on page 4 for more information.

4.5 Menu Structure



- **Terminal Status**
  - ***Summary*** - Check the device status and interface statistics.
  - ***Detailed*** - Check the modem status details.
- **Terminal Installation** - Run the installation procedure.
- **Terminal Configuration**
  - ***Administration*** - Check information about the modem configuration.
  - ***Ethernet Interface*** - Check and alter the Ethernet interface configuration.
  - ***Satellite Interface*** - Check and alter the Satellite interface configuration.
  - ***Antenna Controlling*** - Enable automatic pointing mode. Check and alter corresponding ACU settings.
  - ***Outdoor Unit*** - Check and alter the Outdoor Unit configuration.
  - ***Multicast*** - Check and alter the multicast configuration.

  - ***[optional] GXT Files*** - Check and edit the GXT files.
  - ***[optional] VPN IPSec Configuration*** - Check and edit the VPN IPsec configuration.
- **Device Info** - Check the hardware version. Check or alter the software version.
- **Diagnostics**
  - ***Logging*** - Generate a diagnostics report.
  - ***Test*** - Run tests on the device.

Your service provider can disable **Terminal Installation**. When terminal installation is disabled, the ***Terminal Installation*** menu item is not available.

The ***GXT Files*** menu item is only available when mobility is enabled. For more information about mobility, refer to Terminal Mobility on page 103.

VPN IPsec is an optional feature. When the feature is not supported, the ***VPN IPSec Configuration*** menu item is not available.

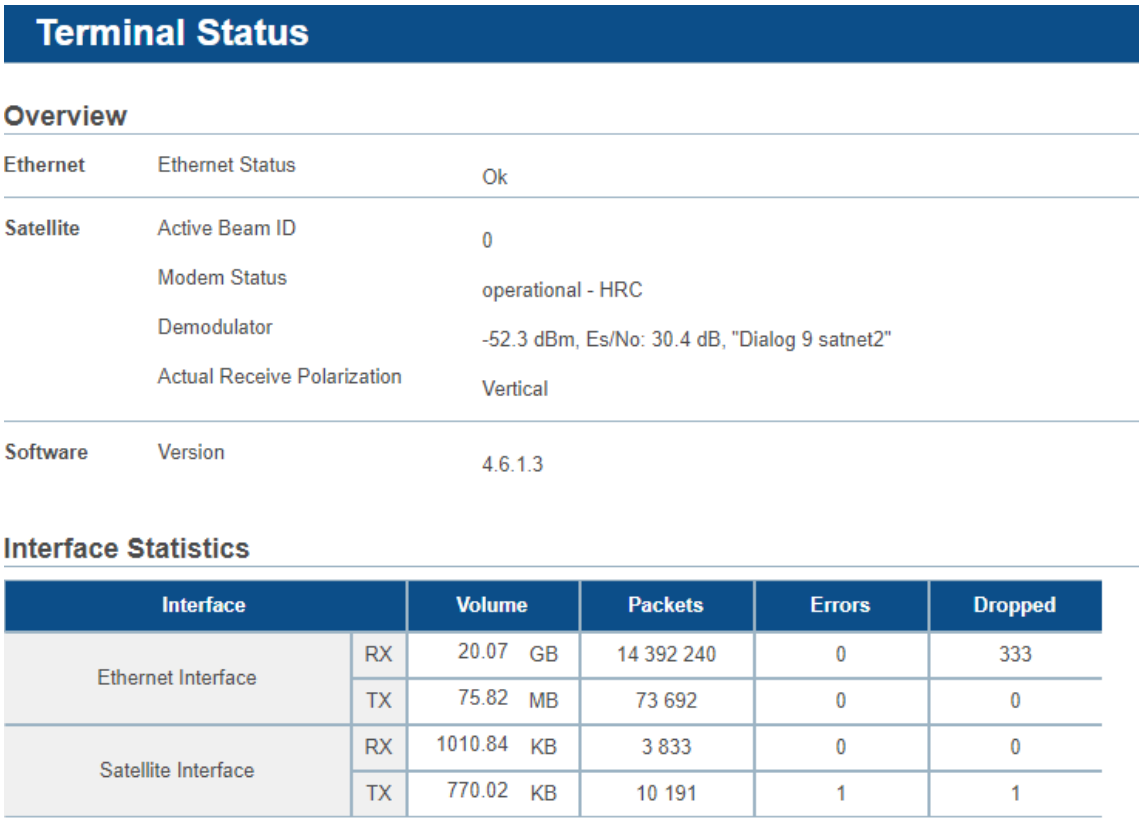
The menu items are explained in the following chapters.

4.6 Terminal Status

4.6.1 Summary

The **Terminal Status Summary** page has two sections:

- **Overview**: This section provides information about the modem and software status.
- **Interface Statistics**: This section provides information about the modem interface statistics.



Terminal Status

Overview

Ethernet	Ethernet Status	Ok
Satellite	Active Beam ID	0
	Modem Status	operational - HRC
	Demodulator	-52.3 dBm, Es/No: 30.4 dB, "Dialog 9 satnet2"
	Actual Receive Polarization	Vertical
Software	Version	4.6.1.3

Interface Statistics

Interface		Volume	Packets	Errors	Dropped
Ethernet Interface	RX	20.07 GB	14 392 240	0	333
	TX	75.82 MB	73 692	0	0
Satellite Interface	RX	1010.84 KB	3 833	0	0
	TX	770.02 KB	10 191	1	1

4.6.1.1 Overview

4.6.1.1.1 Ethernet

The **Ethernet Status** is indicated by a status description. The possible status descriptions are:

Ethernet Status	Description
Ok	Connection is OK. When DHCP is enabled, an IP address is handed out.
Warning	Connection is OK, but no IP address is handed out. This only appears when DHCP is enabled.
Error	Connection is not OK.

4.6.1.1.2 Satellite

The **Active Beam ID** identifies the beam in which the terminal currently operates. When no beam is selected (typically at first startup), the value is set to N/A (Not Applicable).

The **Modem Status** is indicated by a status description. The possible status descriptions are:

Modem state	Description
Idle - Awaiting installer action	Terminal is waiting for an action of the installer.

Idle - Rx disabled	Only for mobile terminals and appears when the terminal is located inside a no-Rx zone. For more information on exclusion zones refer to Terminal Mobility on page 103.
Idle - Automatic Initial Beam Selection ongoing	Only for mobile terminals that are configured to perform Automatic Initial Beam Selection (AIBS) and are currently trying to lock on a beam. This message will normally not be seen in properly configured terminals, because AIBS is very fast. However, if the terminal cannot fetch GPS coordinates from the ACU, or cannot select a beam because it is outside the boundaries of all configured beams, it can stay in this state for a longer time.
Satellite network lookup	Terminal is looking for the satellite network.
Synchronizing	Terminal has found the satellite network and time synchronization.
Synchronized	Terminal is synchronized and can directly log on to the satellite network when IP traffic is received via the Ethernet interface.
Network login	Terminal is trying to log on to the satellite network.
Operational - <return link technology>	Terminal is logged in. The return link technology (MRC, CPM, HRC, MRC or DVB-S2) used by the modem is also displayed

The Modem Status can also display an error message. This error message provides information about the current error status and will be reset when the terminal has entered the satellite network and the terminal is operational.

For more information about possible error messages and possible solutions, refer to Troubleshooting on page 128.

The **Demodulator** status provides the following information: *-95.0 dBM, Es/No: 23.2 dB, "<satellite Network Name>"*

Demodulator Label Value	Description
-xx.x dBm	Indication of the received signal strength, measured in dBm. This indication can change when going from pointing mode to operational mode.
Es/No	Es/No, measured in dB, is an indication of the received signal quality. This indication can change when going from pointing mode to operational mode.
Satellite Network Name	Optional satellite network name as specified by the Network Operator.

The **Actual Receive Polarization** contains the configured RX polarization. This configured value is verified against the detected RX polarization of the LNB. If the values do not match, a warning will be displayed.

4.6.1.1.3 Software

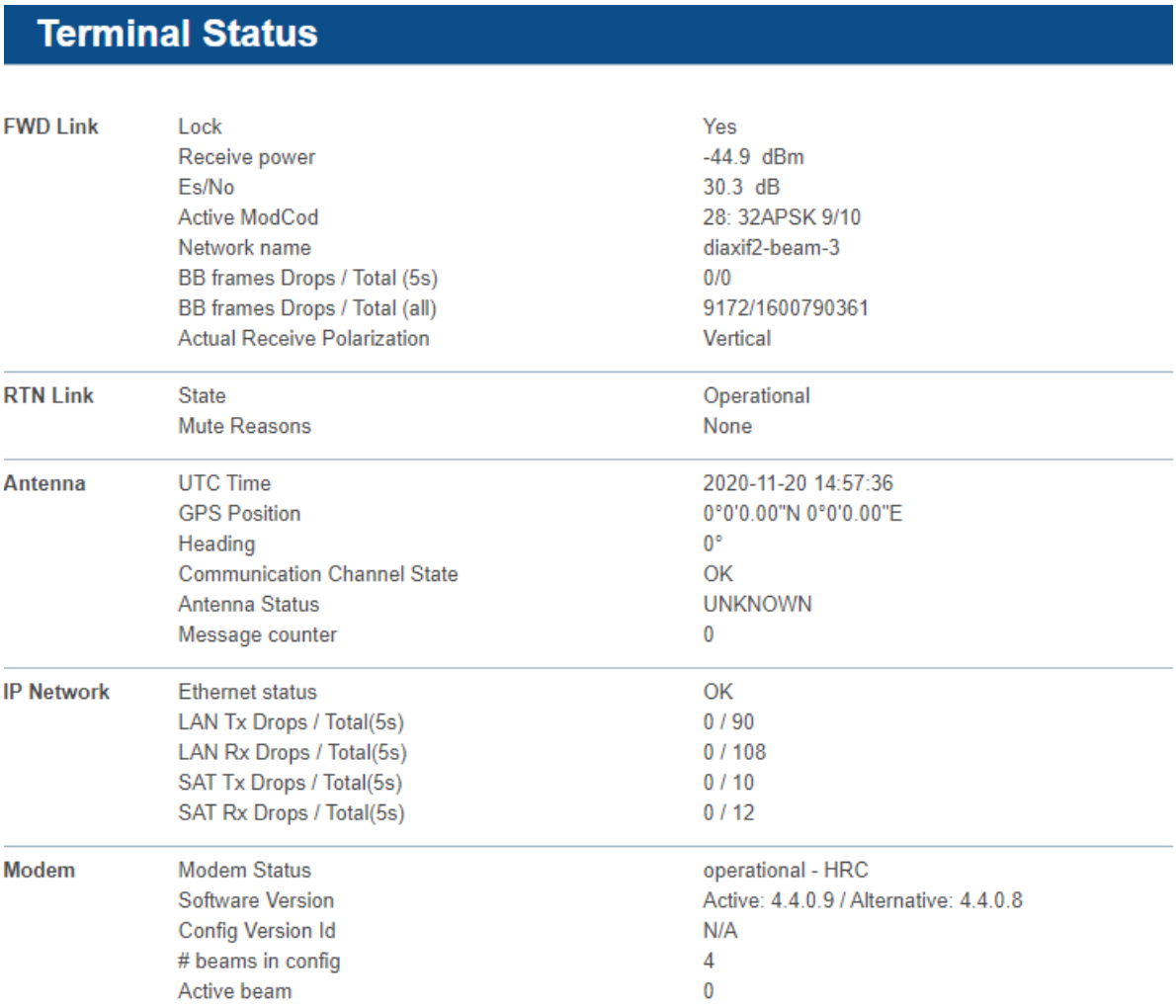
The running software version is indicated by a version number.

4.6.1.2 Interface Statistics

Modem state		Description
Interfaces	Ethernet interface	User side interface (Ethernet frames)
	Satellite interface	Satellite side interface (IP packets)
Directions	RX	Receive IP traffic of the modem, including all multicast and unicast traffic, as well as internal management traffic.
	TX	Transmit IP traffic of the modem, including all transmitted IP packets, unicast traffic, control & management traffic.
Statistics	Volume	Total number of received (or transmitted) bytes.
	Packets	Received (or transmitted) Ethernet frames or IP packets.
	Errors	Number of occurred errors.
	Dropped	Dropped Ethernet frames or IP packets.

4.6.2 Detailed

The **Terminal Status Detailed** page provides a detailed overview of the terminal status. The parameters shown are particularly relevant for mobility troubleshooting.



Terminal Status

FWD Link	Lock	Yes
	Receive power	-44.9 dBm
	Es/No	30.3 dB
	Active ModCod	28: 32APSK 9/10
	Network name	diaxif2-beam-3
	BB frames Drops / Total (5s)	0/0
	BB frames Drops / Total (all)	9172/1600790361
	Actual Receive Polarization	Vertical
RTN Link	State	Operational
	Mute Reasons	None
Antenna	UTC Time	2020-11-20 14:57:36
	GPS Position	0°0'0.00"N 0°0'0.00"E
	Heading	0°
	Communication Channel State	OK
	Antenna Status	UNKNOWN
	Message counter	0
IP Network	Ethernet status	OK
	LAN Tx Drops / Total(5s)	0 / 90
	LAN Rx Drops / Total(5s)	0 / 108
	SAT Tx Drops / Total(5s)	0 / 10
	SAT Rx Drops / Total(5s)	0 / 12
Modem	Modem Status	operational - HRC
	Software Version	Active: 4.4.0.9 / Alternative: 4.4.0.8
	Config Version Id	N/A
	# beams in config	4
	Active beam	0

The parameters are described in the table below.

Parameter	Description
FWD Link	
Lock	Current lock status: Yes/No.
Receive Power	Receive power level, measured in dBm.
Es/No	Energy per symbol (Es) to noise power spectral density (N0) ratio of the forward link, measured in dB.
Active ModCod	MODCOD used for this terminal. Determined by the ACM client.
Network name	Name of the active satellite network.
BB Frames Drops / Total (5s)	Number of dropped baseband frames and number of total received baseband frames during the last five seconds. This number includes all baseband frames from all active MODCODs lower than or equal to the requested MODCOD.
BB Frames Drops / Total (all)	Number of dropped baseband frames and total number of received baseband frames since last reset, for example, in case of a boot or a manual reset.

	Reset can be manually done in the demodulator statistics page.
Actual Receive Polarization	Polarization of the forward carrier in the downlink. The options are the following: • Vertical • Horizontal • Circular left • Circular right
RTN Link	
State	State of the return link. The options are the following: • Idle • Logon • Operational • PureCarrier • ModulatedCarrier • Disabled • Unknown
Mute Reasons	Reasons for Mute in the return link. The options are the following: • ACU • ExclusionZone • HWDiscrete • JsonCommand • LossOfFwLock • PowerMessage • Tim • NoExternalReferencePresent • None
Antenna	
UTC Time	Current time in UTC.
GPS Position	GPS coordinates of the terminal.
Heading	Direction heading of the antenna.
Communication Channel State	Indicates if a session with the antenna is open. The options are the following: • OK • NOK
Antenna Status	As reported by the antenna via the 's' message. The options are the following: • UNKNOWN • OK

	• NOK
Message Counter	Number of messages received by from the antenna since the communication channel was opened.
IP Network	
Ethernet Status	Status of the Ethernet interface of the modem.
LAN Tx Drops / Total (5s)	Number of dropped IP packets and total number of transmitted IP packets measured at the Ethernet interface during the last five seconds.
LAN Rx Drops / Total (5s)	Number of dropped IP packets and total number of received IP packets measured at the Ethernet interface during the last five seconds.
SAT Tx Drops / Total (5s)	Number of dropped IP packets and total number of transmitted IP packets measured at the satellite interface during the last five seconds.
SAT Rx Drops / Total (5s)	Number of dropped IP packets and total number of received IP packets measured at the satellite interface during the last five seconds.
Modem	
Modem Status	The options are the following: • AcquiringForward - The modem is pointed correctly and is trying to acquire lock on the initial carrier, moving to the final carrier or synchronizing on the final carrier signaling; • AcquiringReturn - The modem is correctly synchronized on the forward and trying to log in on the return. The modem will be transmitting in this state; • Aibs - Automatic Initial Beam Selection (AIBS) is enabled, and the modem is searching for an initial beam; • BeamSelection - The modem is in terminal installation state, and waiting for the beam to be manually selected; • Certification - The modem established a bidirectional communication link with the hub and is executing the certification process. The modem will be transmitting in this stat; • Idle - A temporary state that occurs early during the boot progress when the state machine is being initialize; • NetworkConfiguration - The modem established a bidirectional communication link with the hub and is fetching its network configuration data; • OduSelection - The modem is in terminal installation state, and waiting for the ODU to be selected; • Operational - The modem is fully operational; • Pointing - The modem is pointing, either manually or automatically; • PrePointing - When manual pointing is enabled, this state indicates the modem is waiting for pointing carrier selection. If automatic pointing is enabled, this is a very short transitional state that occurs just before the modem goes to pointing state; • RxOnly - The modem is correctly synchronized on the forward, but is for some reason not allowed to transmit; • InstalationCarrier - The modem is transmitting an installation carrier;

	• Debug - An operator brought the modem in a debug state. This is only possible via manual interaction. Typically a reboot, or a manual action is required to bring the modem back in a normal state. The modem might be transmitting in this state; • Error - Most likely indicates a bug, please report; • UnknownState - Most likely indicates a bug, please report.
Software Version	Current software version and alternative software version (if available).
Config Version Id	Configuration version calculated when the terminal is provisioned.
# beams in config	Number of satellite beams currently known in the terminal.
Active beam	Identification of the current active beam.

4.7 Terminal Installation

4.7.1 Introduction

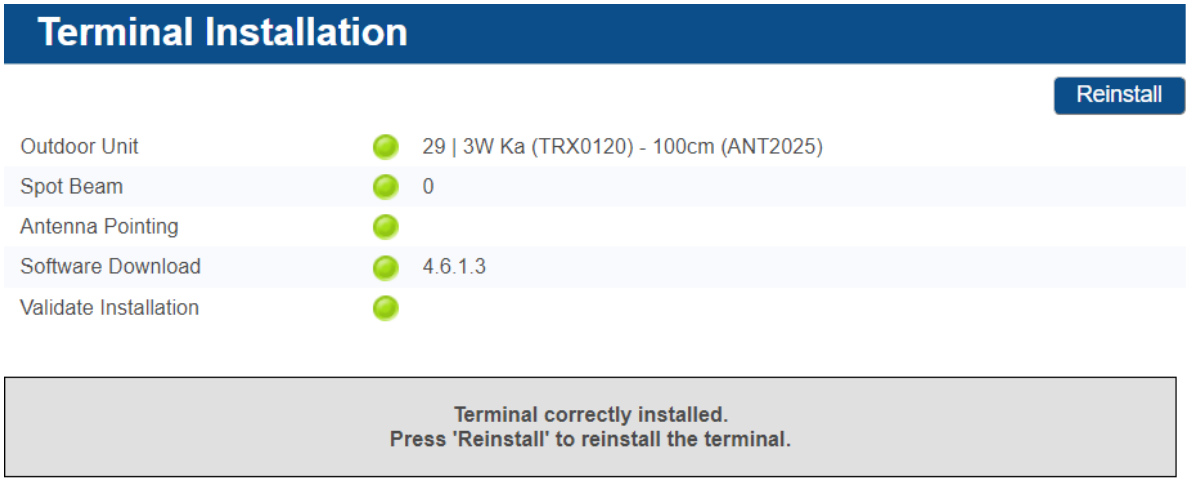
Your service provider can disable terminal installation. When disabled, the **Terminal Installation** menu item is not available and you cannot perform the steps described in this chapter.

The first time the modem starts up, you are redirected to the Terminal Installation page.

During terminal installation, the following steps are executed:

- Define the outdoor unit and spot beam;
- Point the terminal antenna;
- Download the latest software;
- Optionally certify the terminal installation.

When the installation is successfully completed, the following window is shown:



Click Reinstall to restart the complete installation procedure.

To help you with the installation, Dialog provides different installation tools. The tools are listed in the following chapter.

4.7.2 Terminal Installation Tools

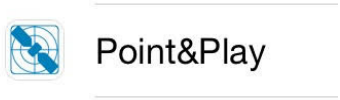
Dialog provides different installation tools which use the patented Point&Play® technology. This technology enables easy manual antenna installation and accurate pointing, and minimizes the adjacent satellite interference.

The tools are:

- Point&Play® Terminal Installation Application (with visual and audio feedback)
- Point&Play® Installation Tool (with audio feedback)
- Point&Play® Integrated Buzzer (with audio feedback, only supported on ILB2220 and ILB2221)

4.7.2.1 Point&Play® Terminal Installation Application

The **Terminal Installation App** is a smartphone application available at the Google Play Store (Android) and Apple App Store (iOS).



When using the Point&Play® Terminal Installation App, terminal installation is triggered from the application itself. No manual modem GUI interaction is required. The application connects to the modem using Wi-Fi.

The application requires a **smartphone** with a **minimum set of specifications**:

- iOS version 9.0 or higher, or Android version 5.0 or higher (app version 3.0)
- GPS sensor;
- Compass;
- Gyroscope;
- Accelerometer;
- Minimum screen size: 4.3”;
- Minimum resolution: 480x800 pixels.

The ST Engineering iDirect terminal can be delivered with a Point&Play® Terminal Installation App kit. The kit includes:

- Two brackets to mount a smartphone on the 2W KU-band ILB2140 or ILB2141;
- Two brackets to mount a smartphone on the 2W Quad Ku-band ILB2145;
- A Wi-Fi access point;
- A 6 m UTP cable;
- A reusable alignment scale band.

To use the application, see Using Point&Play® Terminal Installation App on page 20.

4.7.2.2 Point&Play® Installation Tool

The **Point&Play® Installation Tool** is a piece of hardware used for audio assistance during antenna pointing. It is used in combination with the installation steps in the modem GUI.

The tool is an optional sales item and can be used when your smartphone does not have the required specification for installing the Terminal Installation App, or when you do not have a Wi-Fi access point.

To use the tool, see Using the Point&Play® Installation Tool or Buzzer on page 21.

The tool cannot be used when your outdoor is ILB2220 or ILB2221. In those cases, the iLNB has an integrated Point&Play® buzzer. See Point&Play® Integrated Buzzer on page 20.

4.7.2.3 Point&Play® Integrated Buzzer

The **Point&Play® Integrated Buzzer** is supported on ILB2220 and ILB2221. These iLNBs have integrated audio assistance during antenna pointing. The integrated buzzer can be used in combination with the installation steps in the modem GUI (see Using the Point&Play® Installation Tool or Buzzer on page 21), or with the Terminal Installation App (see Using Point&Play® Terminal Installation App on page 20).

4.7.3 Using Point&Play® Terminal Installation App

When using the Point&Play® Terminal Installation App, terminal installation is triggered from the application itself. No manual modem GUI interaction is required.

The application has a demo mode for tutorial purposes.

To enable the demo mode on **Android**: Open the Point&Play® app and click **Start**. Click the hamburger icon ( ) on the top left, then click the cog icon ( ) on the bottom right. Switch **ON** the **Demo mode**.

To enable the demo mode on **iOS**: Go to the Settings of your mobile device and select the Point&Play® app. Switch **ON** the **Demo Mode**.

Make sure to switch **OFF** the demo mode again **in the field**.

To use the application:

1. Open the Point&Play® Terminal Installation App.
2. Click Start.
3. Enter the satellite orbital position and click Confirm orbital position.
4. Follow the steps in the application. Click Next after each step.
5. For the certification step, you can start or skip certification.
6. After the certification step, you will get a summary. Click Export picture to save the summary in the photo library on your mobile phone.

If certification failed, redo the pointing.

If certification is aborted due to a technical issue, contact your service provider.

7. Click Finish.

Click Start to restart the complete installation procedure. You can do this anytime.

4.7.4 Using the Point&Play® Installation Tool or Buzzer

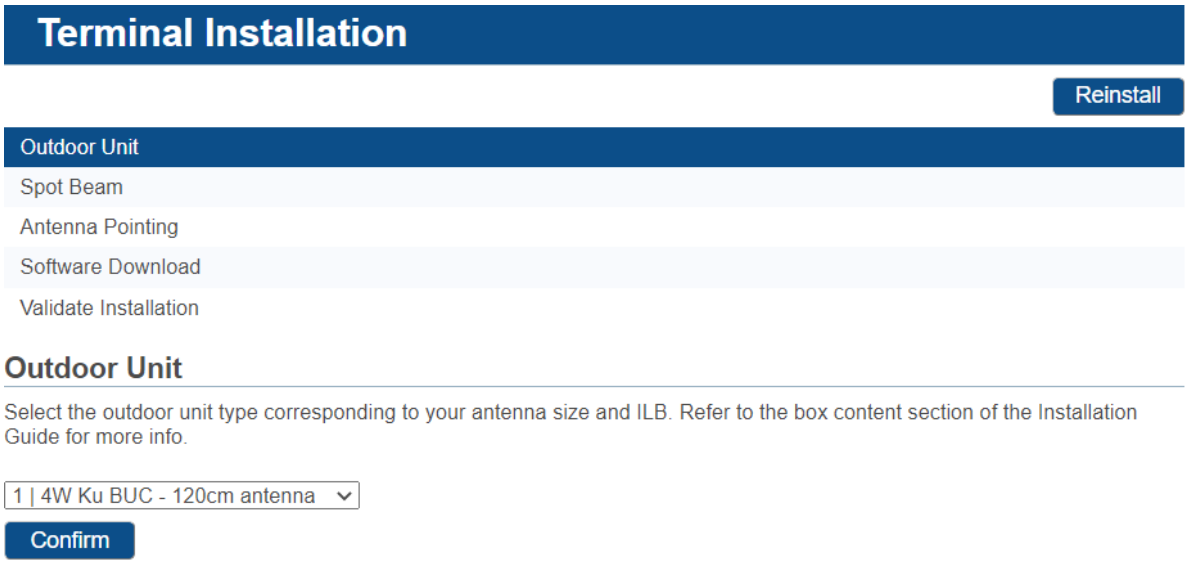
4.7.4.1 Select Outdoor Unit

The supported outdoor unit types are pre-configured in factory.

In the unlikely event that your outdoor unit is not listed, the outdoor unit should be added manually. For more information, refer to Add ODU Configuration on page 60.

Selecting an incorrect outdoor unit type may prevent the modem from logging onto the network.

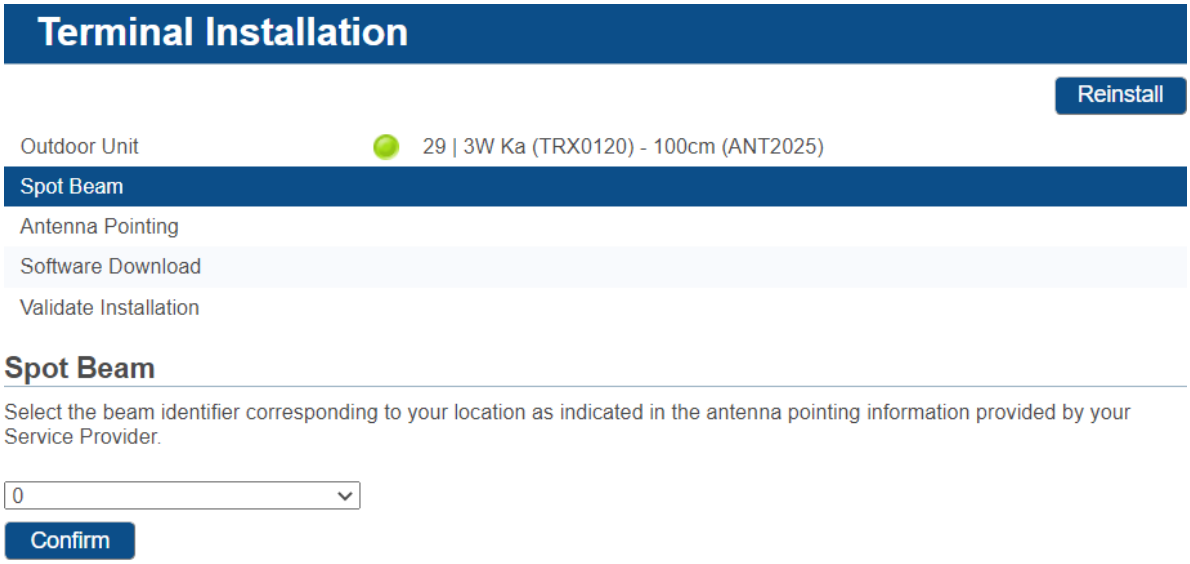
The outdoor unit is defined as the combined set of antenna, LNB and BUC or antenna and iLNB. Select the outdoor unit type from the drop-down list and click Confirm.



4.7.4.2 Select Spot Beam

The spot beams are pre-configured in factory. If, for some reason, a new beam has to be added, refer to Satellite Configuration - Add Beam on page 99.

The spot beam covers the geographical area in which the terminal is serviced. Select the spot beam ID from the drop-down list and click Confirm.



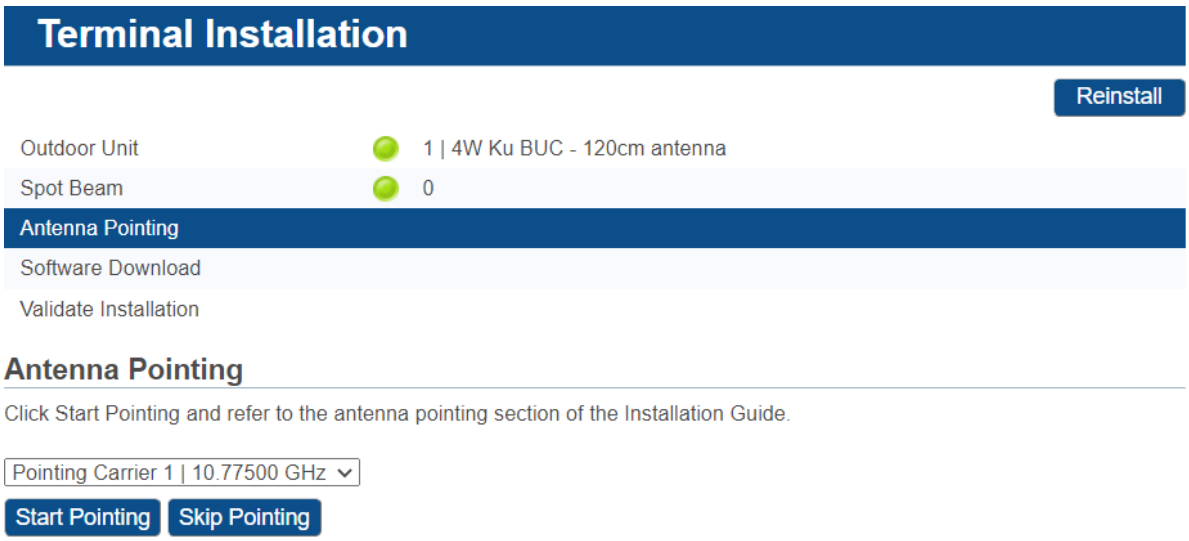
4.7.4.3 Point Antenna

Before proceeding with this step, make sure that:

- Your antenna and LNB/BUC or iLNB are properly installed. For instructions, refer to the manufacturer's installation guide.
- The RX interface of the (I)LNB is connected to the RX interface on the modem.

***Note** - The TX interfaces should not yet be connected, except when working with the ILB2220/ILB2221 outdoor unit. These iLNBs support a single cable connection.*

If two pointing carriers have been pre-configured, keep the pre-selected carrier. If pointing fails during the procedure, repeat this step with the other pointing carrier.



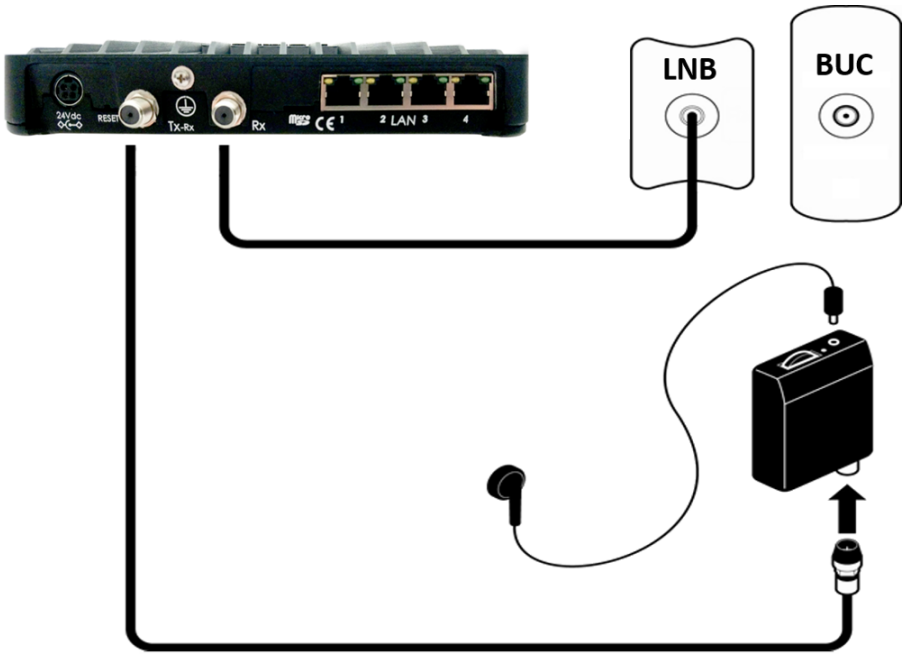
You can skip pointing if the antenna has already correctly been pointed. In that case, you can proceed with the Software Download on page 34.

Click Start Pointing to start the pointing procedure using the tool or buzzer.

The tool cannot be used when your outdoor unit is ILB2220 or ILB2221. In those cases, the iLNB has an integrated Point&Play® buzzer. You can skip step 1 to 3, and step 6 and 7.

Execute the following steps:

1. Connect the TX interface of your modem to the Point&Play® tool.
2. Connect the earphone to the Point&Play® Installation Tool. Make sure the tool is still switched off.
3. Switch on the tool by slowly turning the volume wheel until the green LED illuminates. Put on the earphone and adjust the volume if necessary.

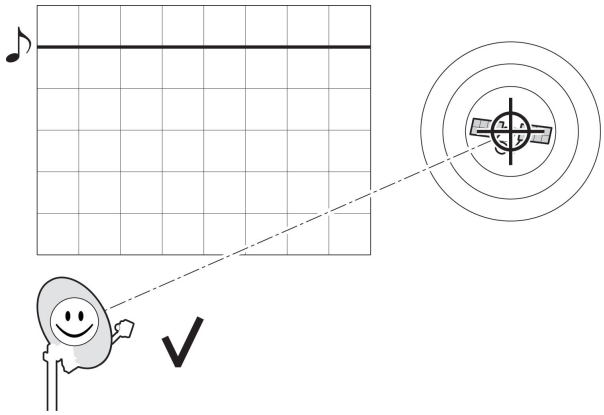


Ensure that the volume of the Point&Play® Installation Tool is not set too loud, otherwise damage to your hearing may occur.

4. Start pointing the antenna. During the pointing procedure, the tool (or buzzer) can produce various sounds, each having a specific meaning.

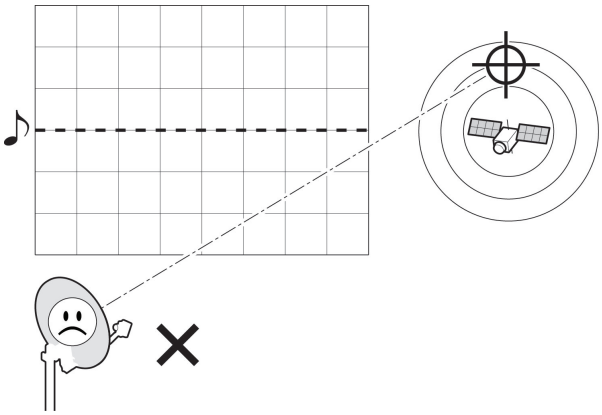
   High uninterrupted tone (correct tone)

   The antenna points to the correct satellite and is receiving the strongest signal. Some fine-pointing might still be required to find the optimal position of the antenna (highest tone within the high uninterrupted tone range).



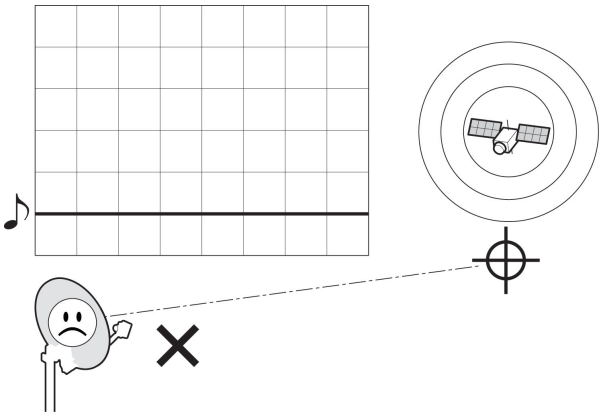
   Medium or high interrupted tone

   The antenna points to the correct satellite but does not receive the strongest signal so far. The pointing procedure must be continued until an uninterrupted high tone is perceived.



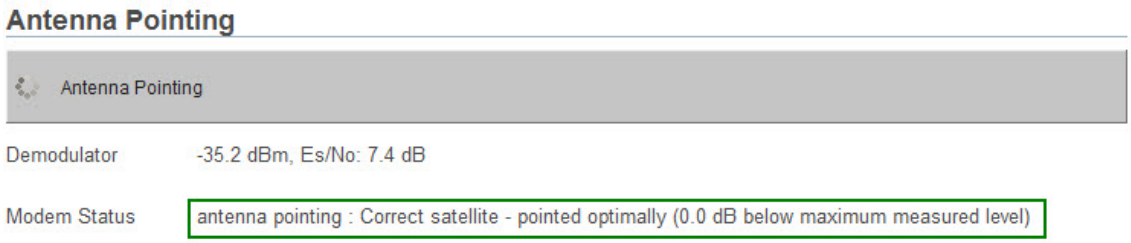
Low uninterrupted tone

The antenna points to a wrong satellite or is not pointing to a satellite.



Your antenna is properly pointed when you hear the highest possible uninterrupted tone.

5. When the antenna is correctly and optimally pointed, the message **Correct satellite - pointed optimally** appears in the modem GUI. You can now proceed to the next step.



If the antenna is not yet optimally pointed, the message **Correct satellite - not pointed optimally** is displayed. Continue the pointing procedure (step 4) until optimal pointing is achieved.

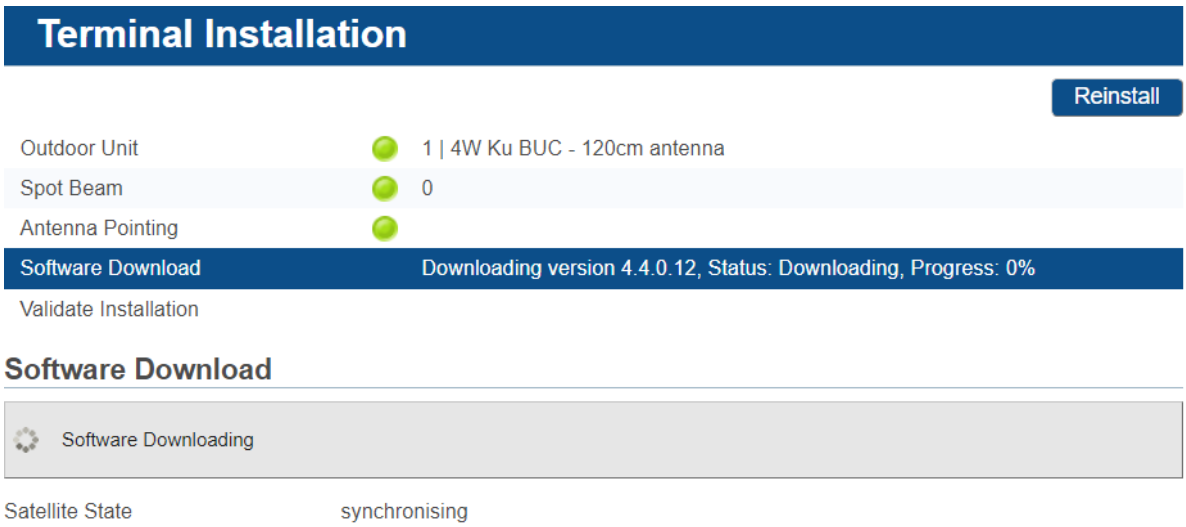
For more information about possible error messages and possible solutions, refer to Troubleshooting on page 128.

6. Switch off the tool.
7. Remove the TX cable from the Point&Play Installation Tool, and connect it to the BUC.
8. Return to the modem GUI and click Finish Pointing.

4.7.4.4 Download Software

The modem continuously checks for software updates. If the software is still up to date, this step is skipped automatically. You can proceed with Validate Installation on page 34.

If a newer software version is available, download will start automatically. The software download can be followed in the modem GUI.



When the download is complete, the new software is written to the flash memory and the modem reboots to activate the new software. After reboot, you can proceed with Validate Installation on page 34.

You may need to refresh the page of your browser manually after the reboot.

4.7.4.5 Validate Installation

Your service provider decides if the terminal installation has to be validated or not.

If validation for your terminal is not required, this step is skipped automatically and the terminals installation is completed. Depending on your service provider, you might need to register first before you can start browsing the web.

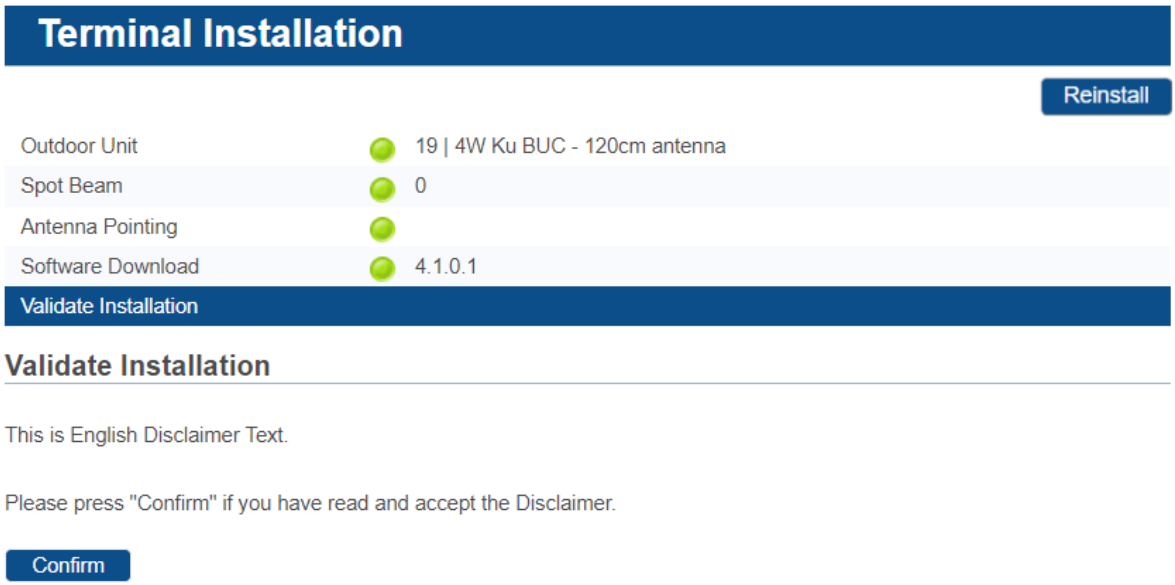
During validation the quality of the installation is verified. The validation procedure exists of the following steps:

- Accept Disclaimer
- Enter your location
- Validation

4.7.4.5.1 Accept Disclaimer

The validation procedure uses sensitive information such as geographical location of the terminal which is subject to legal restrictions. Therefore, a disclaimer is presented.

Read the disclaimer message and click Confirm to accept the disclaimer.



4.7.4.5.2 Enter your Location

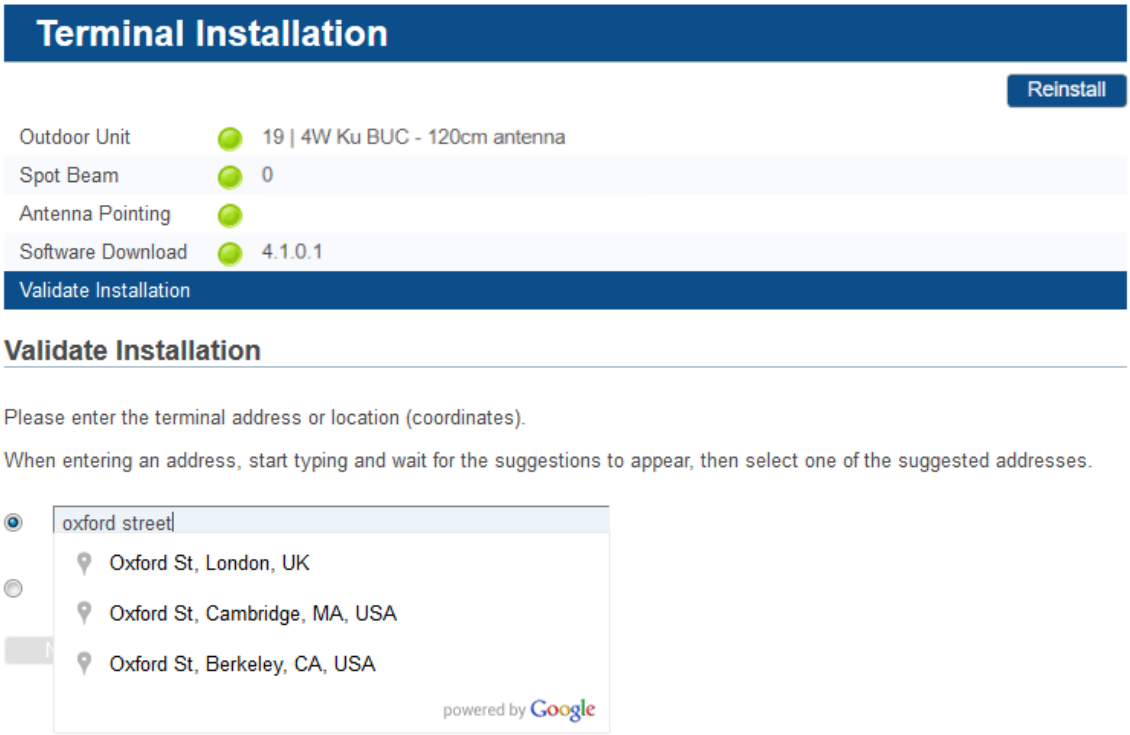
The validation of your installation is based on the geographical location of your terminal.

There are two options to enter this information:

- Option 1: Enter your address.
- Option 2: Enter your location's latitude and longitude.

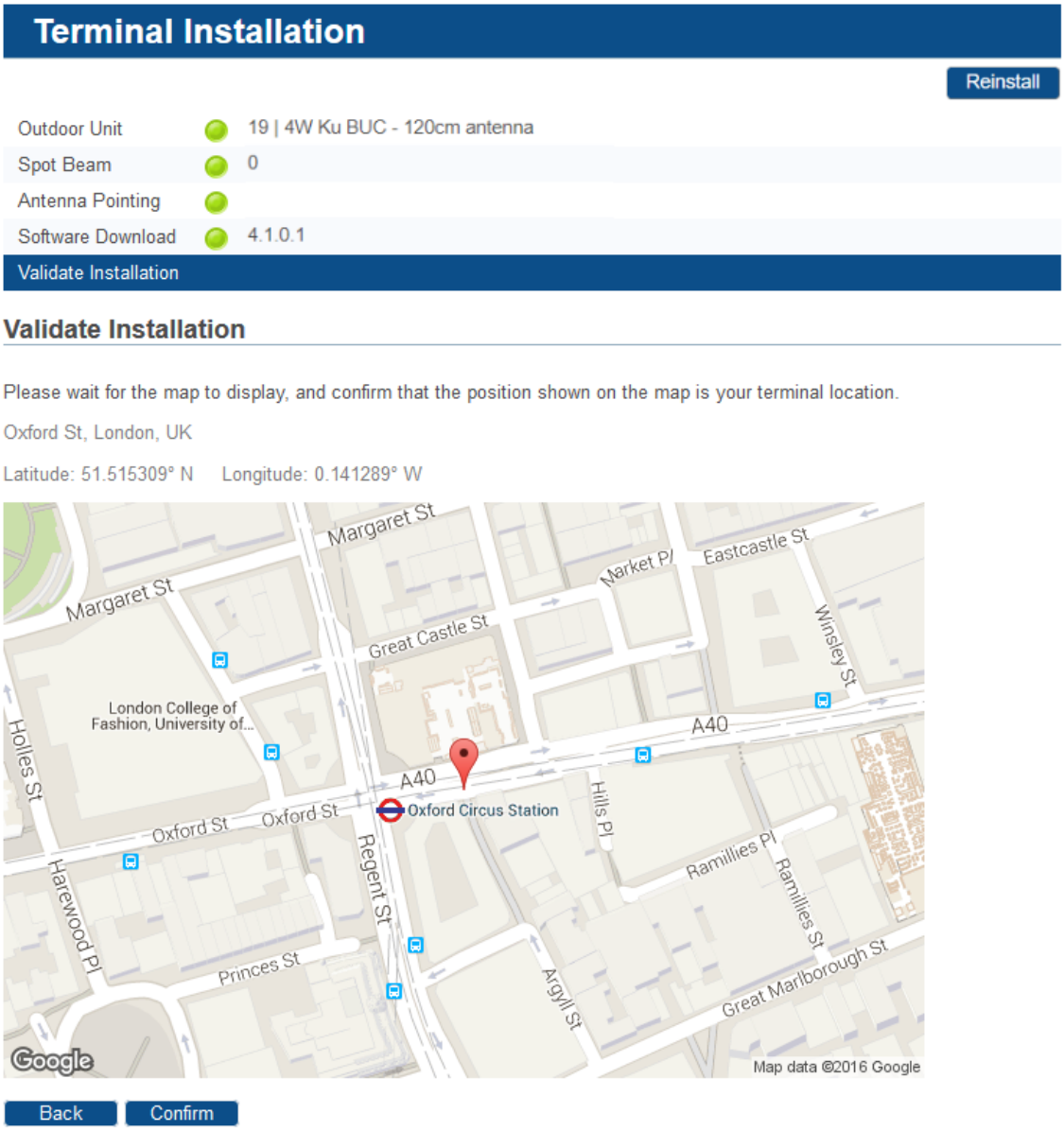
Option 1: Enter your Address

1. Enter the address where the terminal is located. At a minimum, your city and country are required.



A list of one or more matching locations is displayed.

2. Select your address from the list and click Next to view your location on a map.



If your address is not listed or no results are displayed, refer to Troubleshooting on page 128 for a possible reason and solution.

3. Click Confirm to accept and proceed.

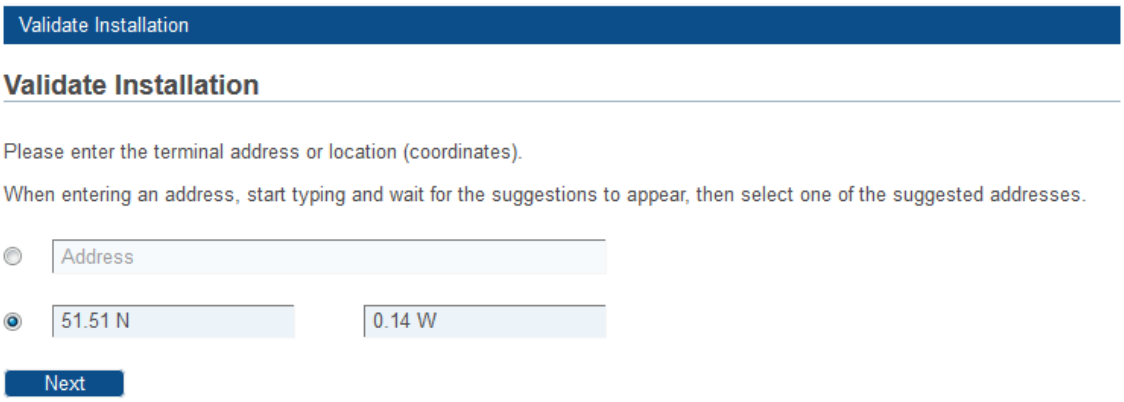
If this is not your location, refer to Troubleshooting on page 128 for a possible reason and solution.

Option 2: Enter your Location

1. Enter your location's latitude and longitude.

The values should be entered in degrees, minutes and seconds notation or in decimal form (using a dot as a separator).

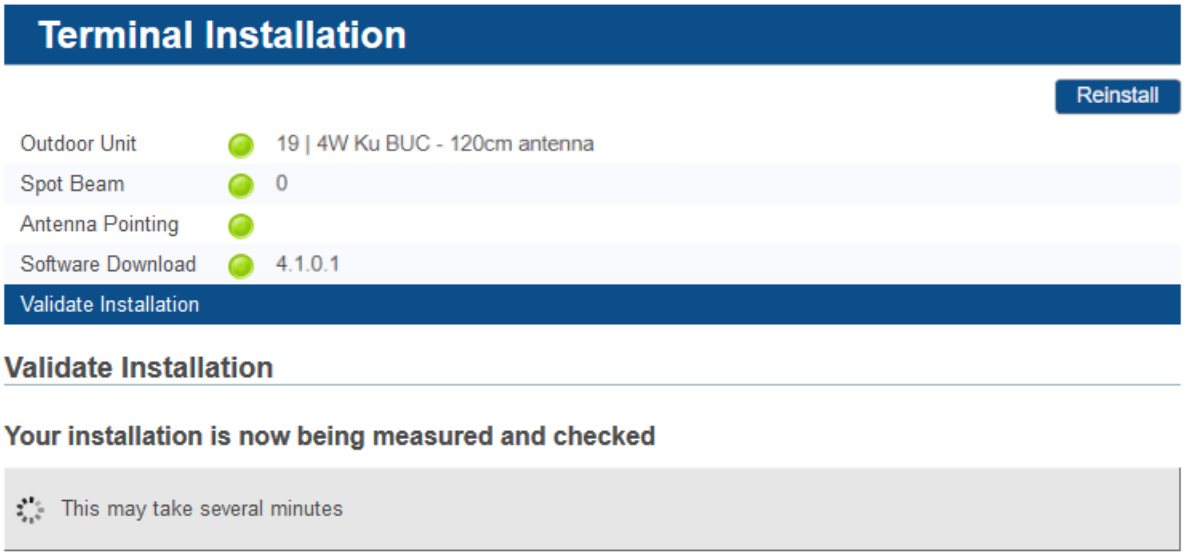
Positive latitude = NORTH, positive longitude = EAST.



2. Click Next to continue.

4.7.4.5.3 Validation

When the location is confirmed, the validation of the installation starts.



When the validation is successful, the following screen is shown:

Click Confirm to finish the terminal installation.

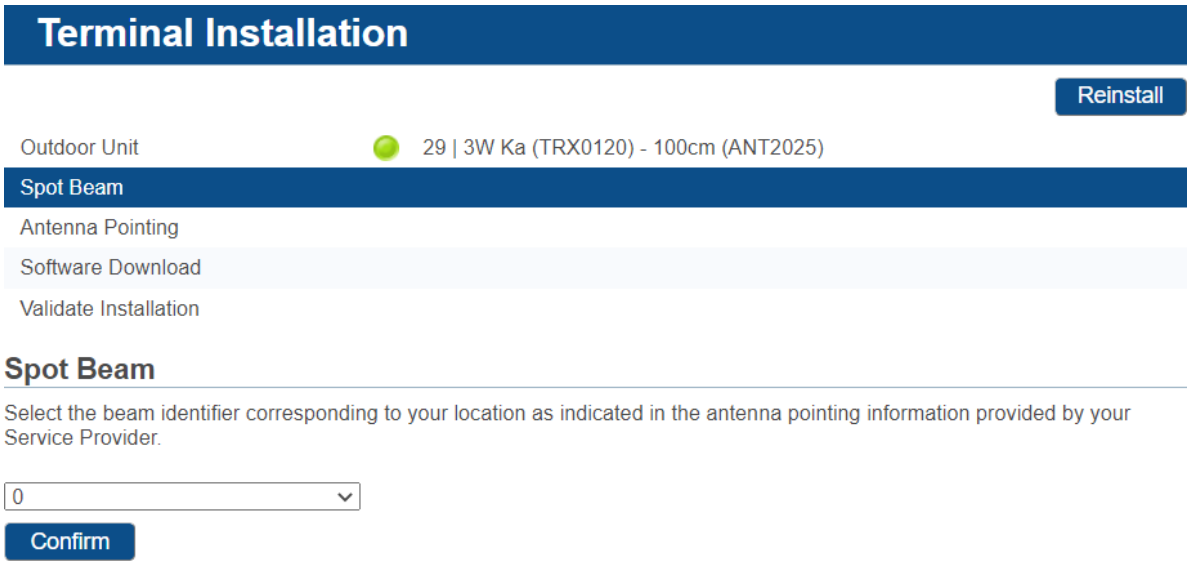
If the validation fails,, refer to Troubleshooting on page 128 for a possible reason and solution.

4.7.5 Using Automatic Pointing

4.7.5.1 Select Spot Beam

The spot beams are pre-configured in factory. If, for some reason, a new beam has to be added, refer to Satellite Configuration - Add Beam on page 99.

The spot beam covers the geographical area in which the terminal is serviced. Select the spot beam ID from the drop-down list and click Confirm.



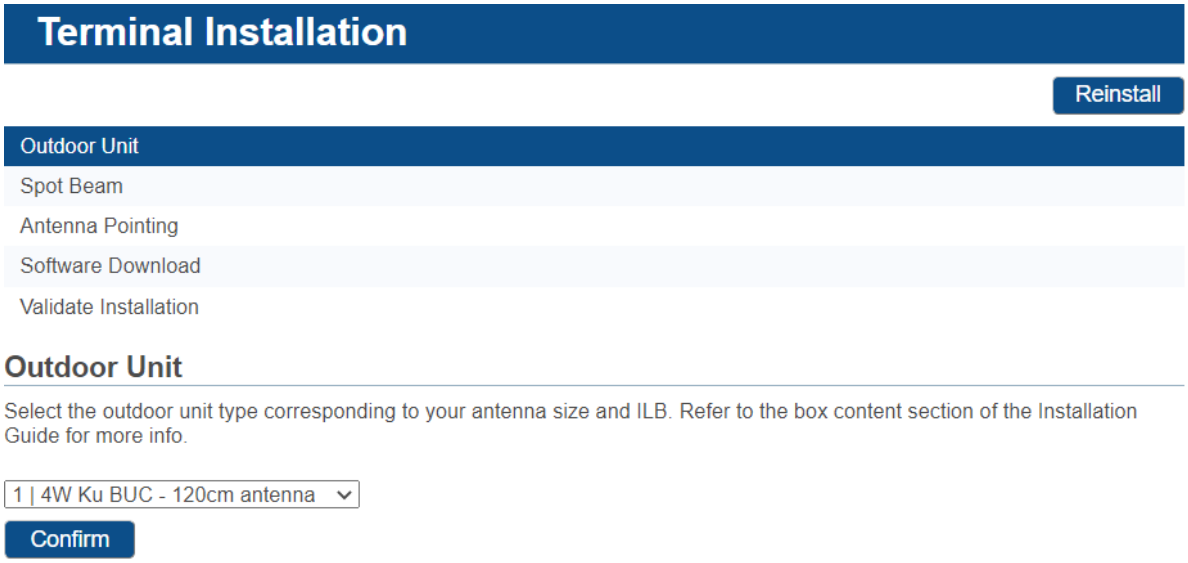
4.7.5.2 Select Outdoor Unit

The supported outdoor unit types are pre-configured in factory.

In the unlikely event that your outdoor unit is not listed, the outdoor unit should be added manually. For more information, refer to Add ODU Configuration on page 60.

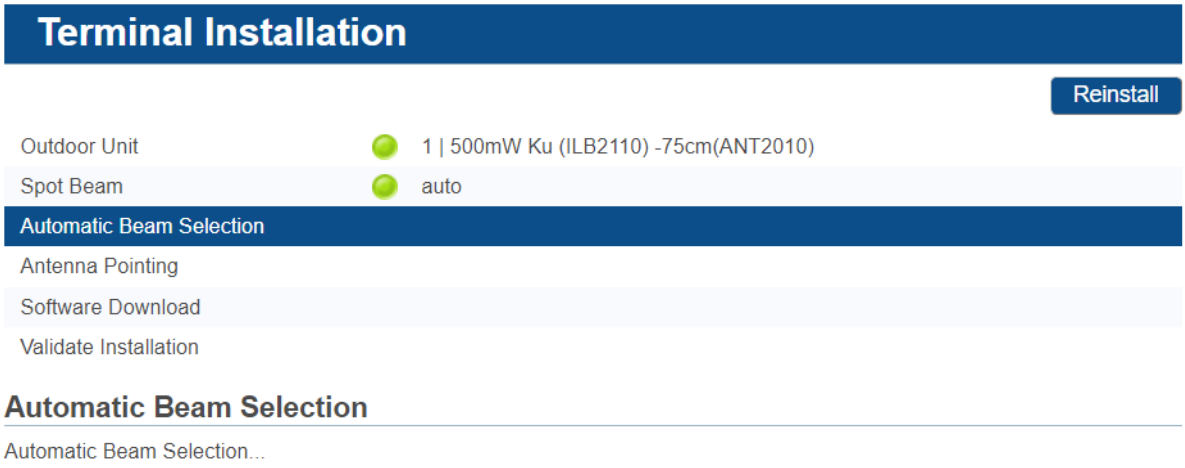
Selecting an incorrect outdoor unit type may prevent the modem from logging onto the network.

The outdoor unit is defined as the combined set of antenna, LNB and BUC or antenna and iLNB. Select the outdoor unit type from the drop-down list and click Confirm.



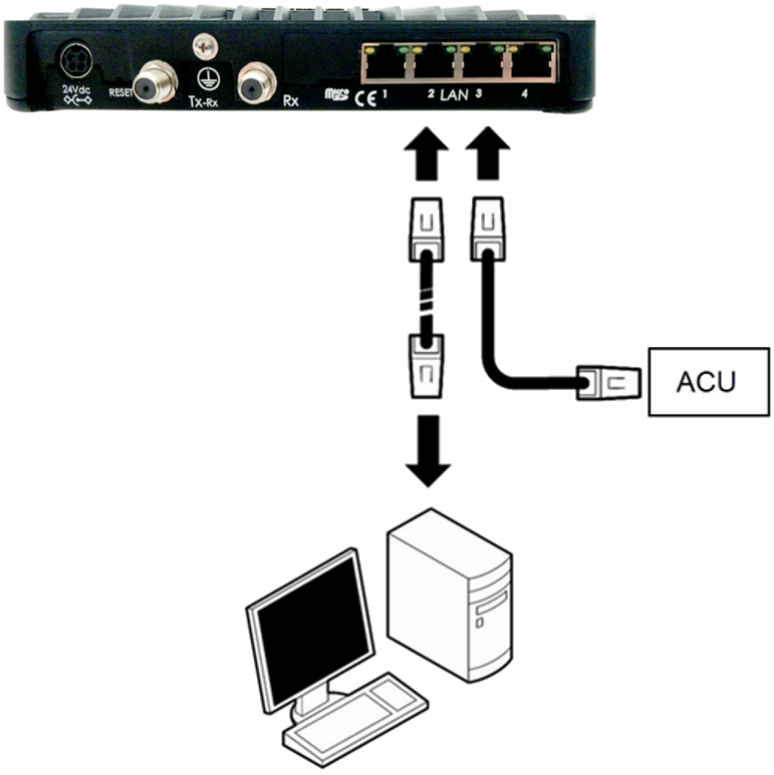
When using **automatic pointing** and **terminal mobility**, you can set the spot beam to **Auto**. This enables Automatic Initial Beam Selection or AIBS. With AIBS the beam is selected based on the GPS coordinates of the terminal and the beam contour information. You will also see the extra installation state **Automatic Beam Selection**.

Refer to Expert Mode on page 88 for more details about enabling terminal mobility.

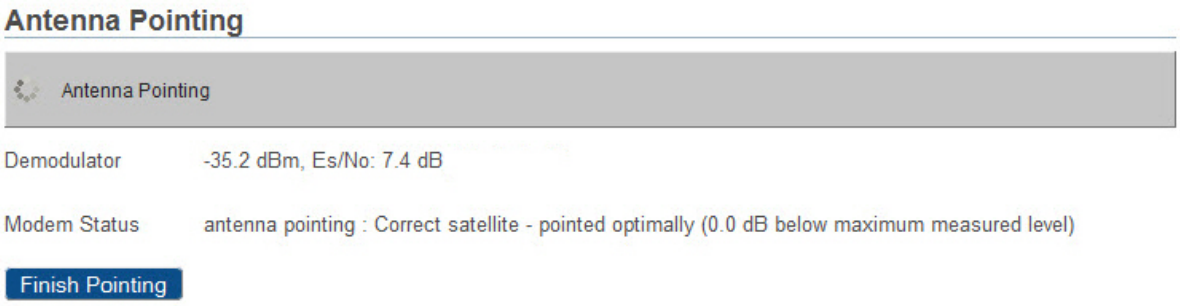


4.7.5.3 Point Antenna

Automatic pointing requires an Antenna Control Unit or ACU. The ACU is connected to the modem via Ethernet.



The modem and ACU communicate using OpenAMIP (Open Antenna to Modem Interface Protocol). The values for the parameters which are used for OpenAMIP communication between the modem and the ACU should be configured in the Antenna Controlling on page 51 menu item. It is advised to click Restart after enabling automatic pointing.
Once automatic pointing is enabled and communication between modem and ACU is established, the modem sends the parameters of the default pointing carrier and the outdoor unit towards the ACU via OpenAMIP messages and the pointing procedure starts.



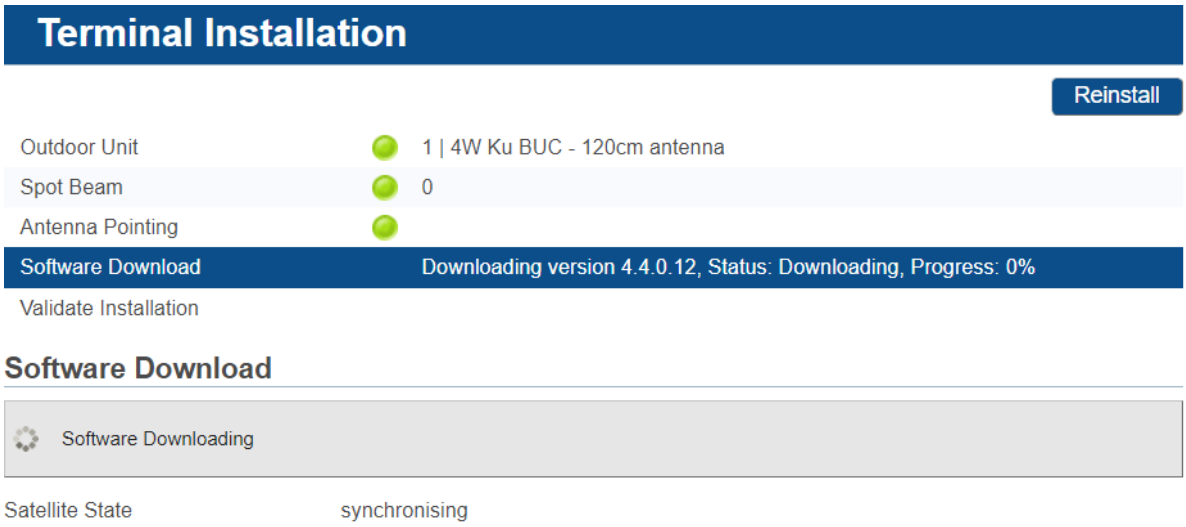
Pointing finishes automatically after the ACU has signaled to the modem that it has found the correct satellite.

Use the Finish Pointing button if the automatic pointing fails and if you want to interrupt the automatic pointing procedure. This allows to verify the automatic pointing settings or to troubleshoot the issue.

4.7.5.4 Download Software

The modem continuously checks for software updates. If the software is still up to date, this step is skipped automatically. You can proceed with Validate Installation on page 34.

If a newer software version is available, download will start automatically. The software download can be followed in the modem GUI.



When the download is complete, the new software is written to the flash memory and the modem reboots to activate the new software. After reboot, you can proceed with Validate Installation on page 34.

You may need to refresh the page of your browser manually after the reboot.

4.7.5.5 Validate Installation

Your service provider decides if the terminal installation has to be validated or not.

If validation for your terminal is not required, this step is skipped automatically and the terminals installation is completed. Depending on your service provider, you might need to register first before you can start browsing the web.

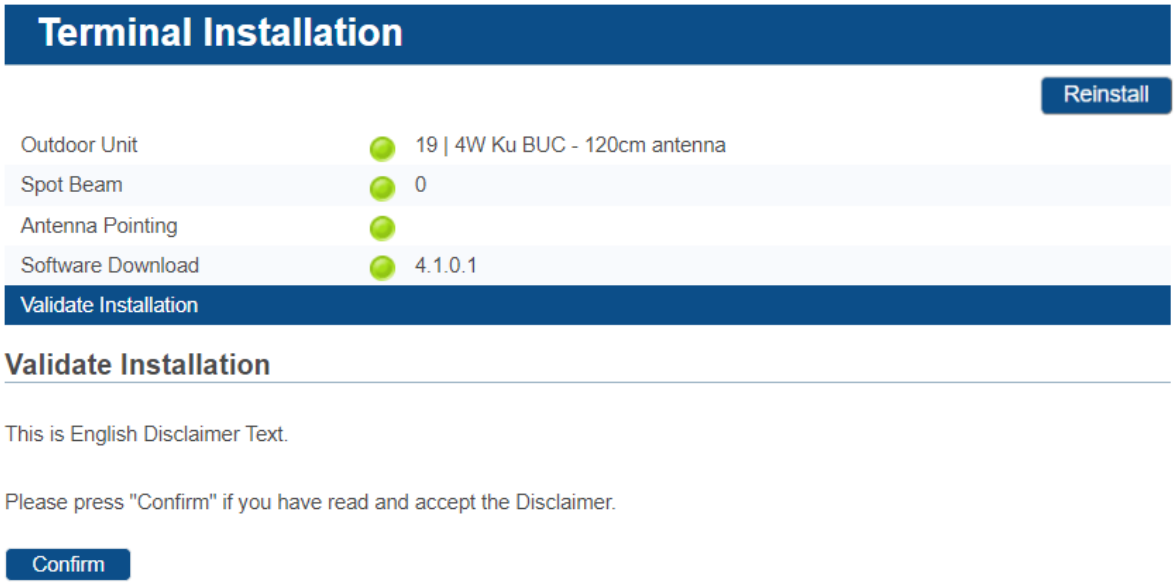
During validation the quality of the installation is verified. The validation procedure exists of the following steps:

- Accept Disclaimer
- Enter your location
- Validation

4.7.5.5.1 Accept Disclaimer

The validation procedure uses sensitive information such as geographical location of the terminal which is subject to legal restrictions. Therefore, a disclaimer is presented.

Read the disclaimer message and click Confirm to accept the disclaimer.



4.7.5.5.2 Enter your Location

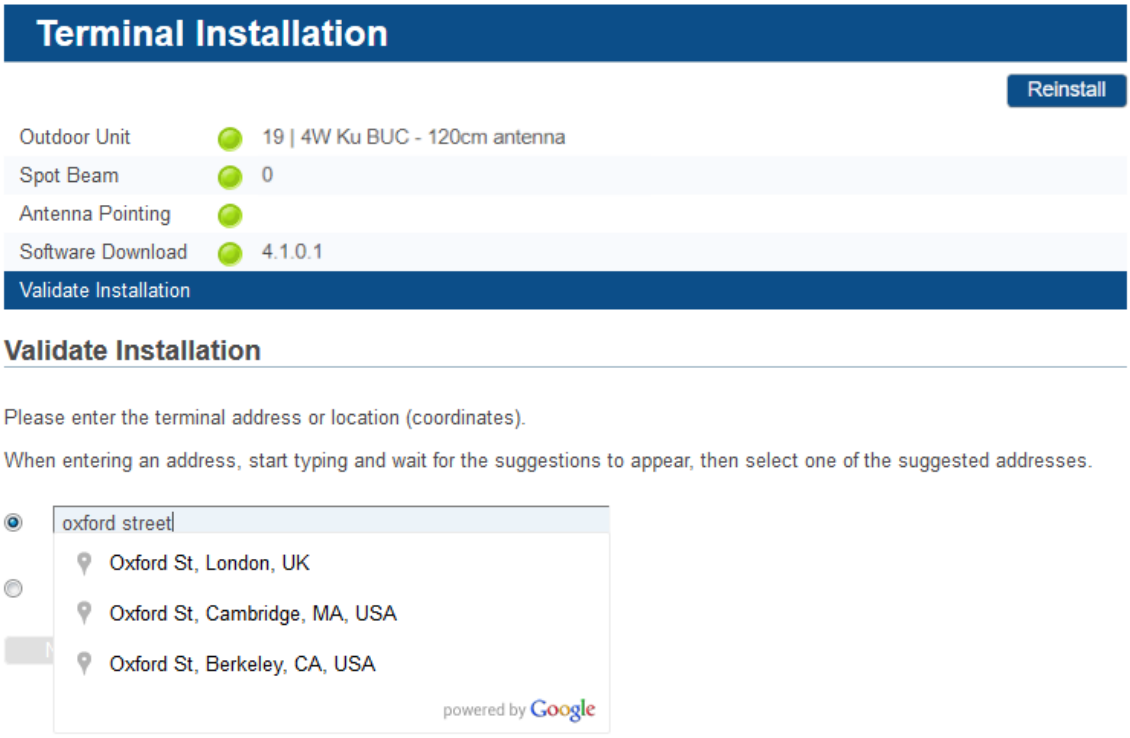
The validation of your installation is based on the geographical location of your terminal.

There are two options to enter this information:

- Option 1: Enter your address.
- Option 2: Enter your location's latitude and longitude.

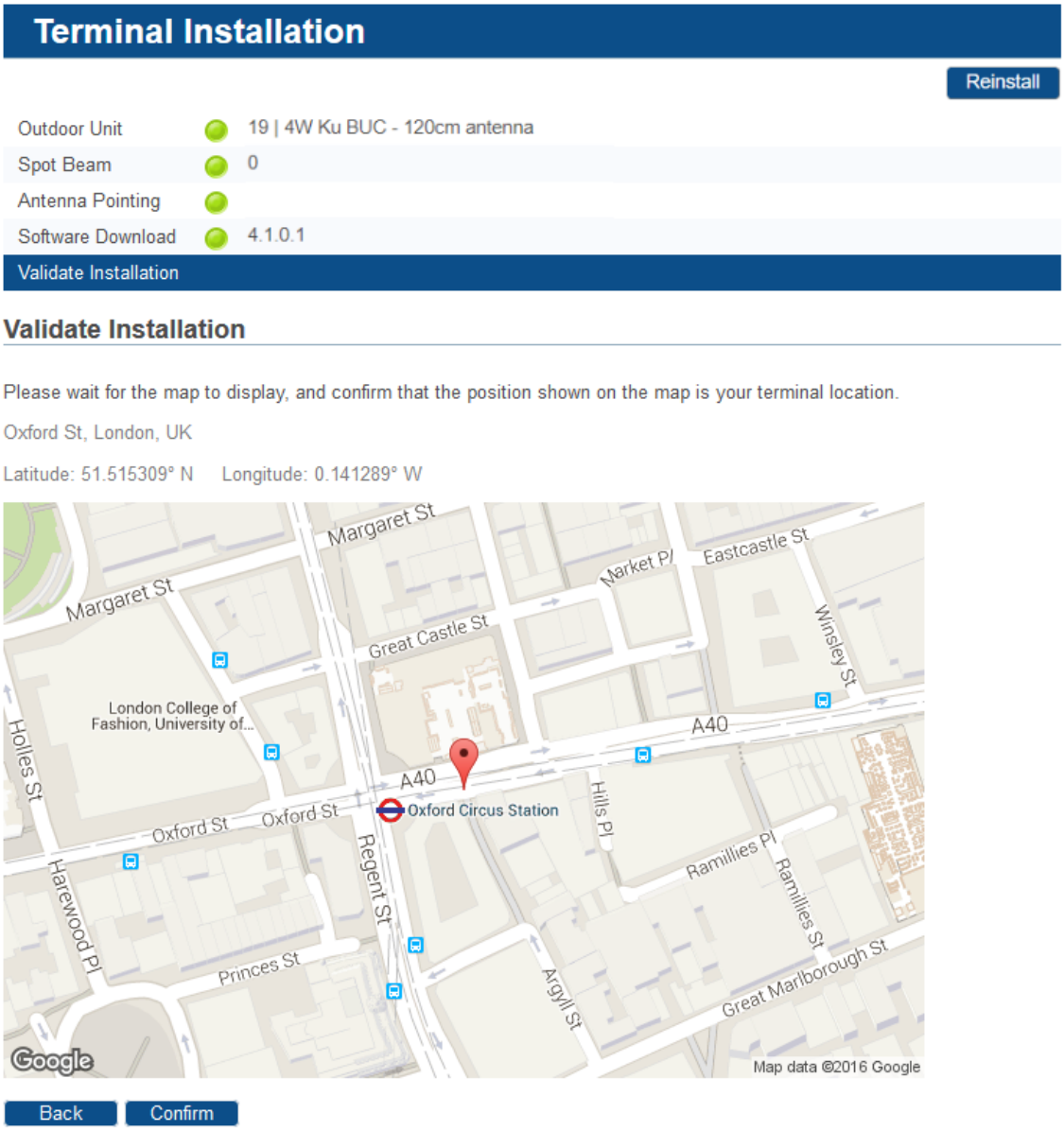
Option 1: Enter your Address

1. Enter the address where the terminal is located. At a minimum, your city and country are required.



A list of one or more matching locations is displayed.

2. Select your address from the list and click Next to view your location on a map.



If your address is not listed or no results are displayed, refer to Troubleshooting on page 128 for a possible reason and solution.

3. Click Confirm to accept and proceed.

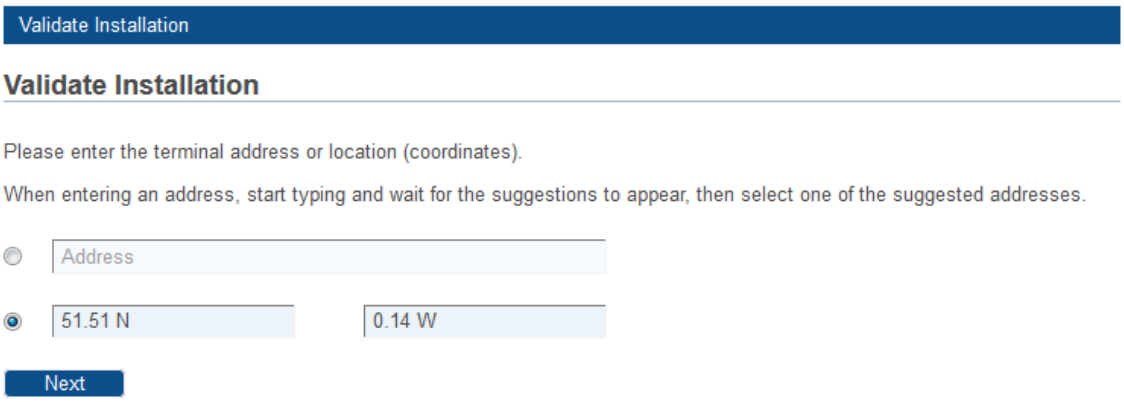
If this is not your location, refer to Troubleshooting on page 128 for a possible reason and solution.

Option 2: Enter your Location

1. Enter your location's latitude and longitude.

The values should be entered in degrees, minutes and seconds notation or in decimal form (using a dot as a separator).

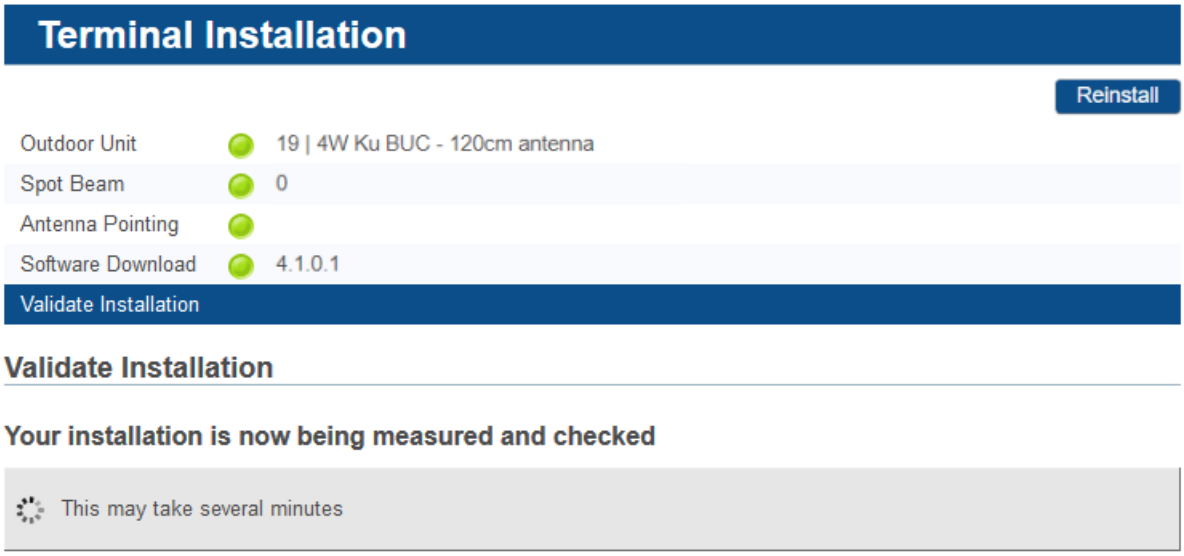
Positive latitude = NORTH, positive longitude = EAST.



2. Click Next to continue.

4.7.5.5.3 Validation

When the location is confirmed, the validation of the installation starts.



When the validation is successful, the following screen is shown:

Click Confirm to finish the terminal installation.

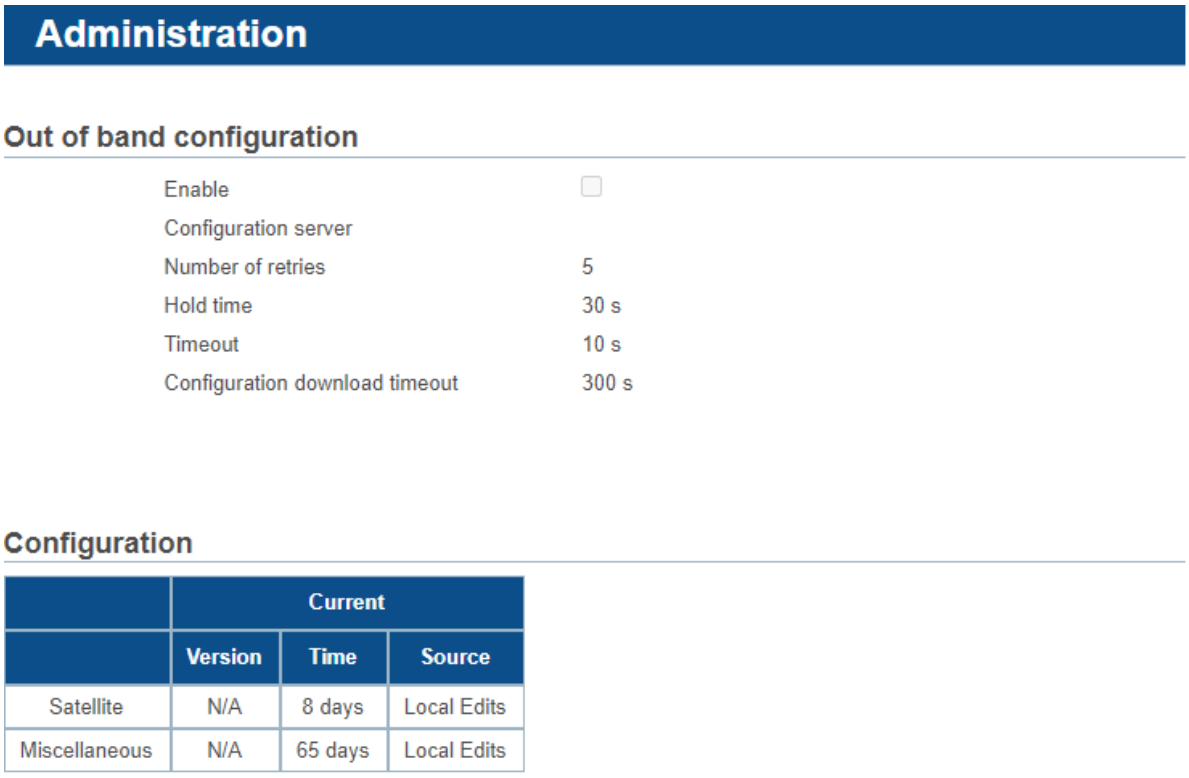
If the validation fails,, refer to Troubleshooting on page 128 for a possible reason and solution.

4.7.6 Line Up

Your network operator may ask to perform a manual line-up procedure. For more information, refer to Installation Carrier on page 125.

4.8 Terminal Configuration

4.8.1 Administration



This page is read-only for the normal user.

When the **Out-of-band Configuration** check box is selected, the terminal is configured through an external **Configuration server**. For more information about out-of-band configuration, refer to Expert: Administration on page 90.

The **Configuration** table shows the version, lifetime and source of the **current** configuration and of a **candidate** configuration if this exists.

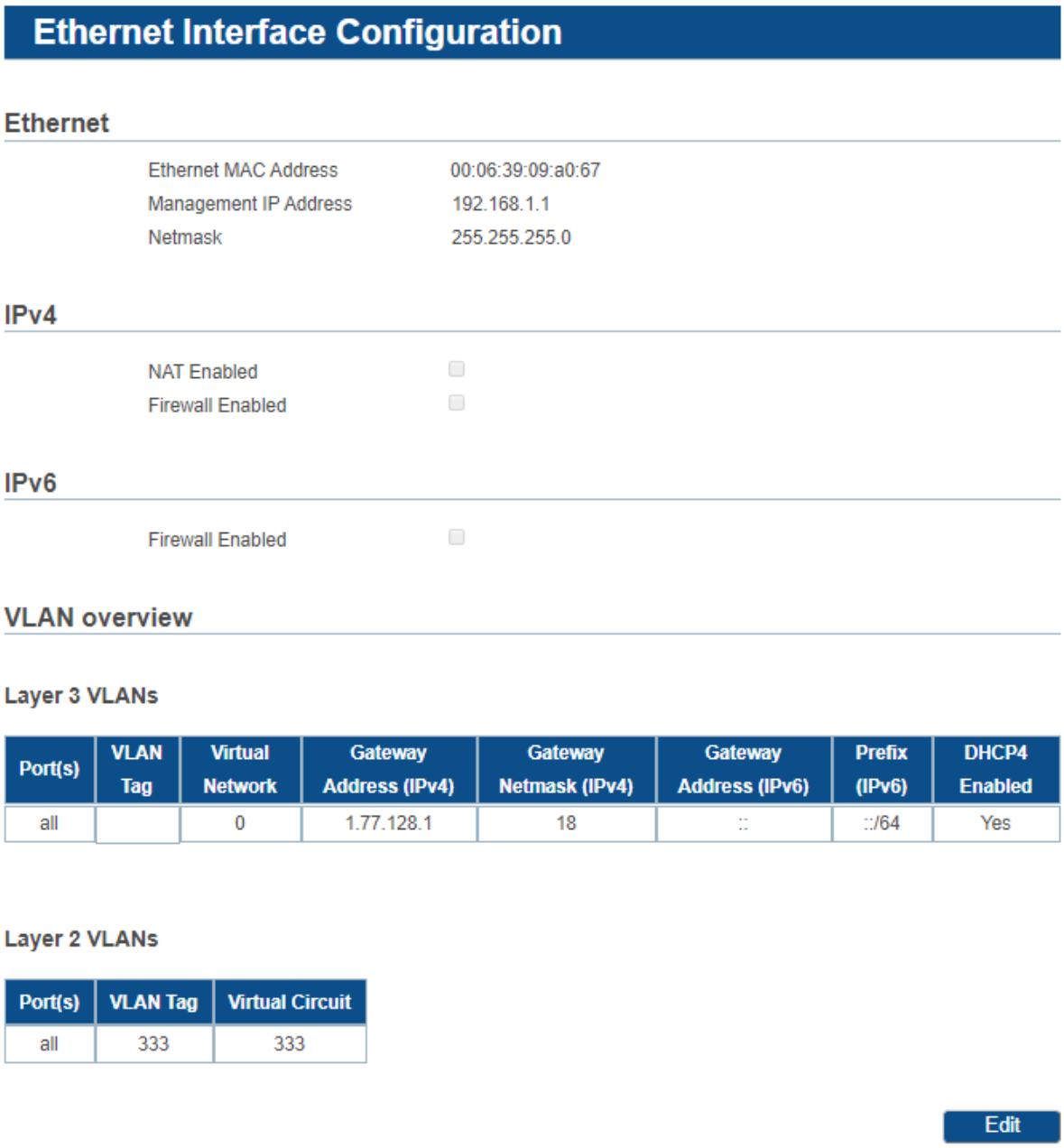
Type	Version	Time	Sources
• **Satellite**: Refers to the satellite configuration. See Satellite Interface	Can be a number or N/A. N/A is used when the configuration is	Lifetime of the configuration. Time is reset upon configuration change.	• **Local Edits**: Indicates that the configuration is edited locally, either via the GUI or JSON

on page 47. • **Miscellaneous**: Refers to the entire modem configuration, excluding the satellite configuration.	locally edited or in case of the candidate configuration, when this configuration has been committed and cleared.		API. • **TCS**: This source is only applicable to the satellite configuration and indicates that the configuration has been downloaded from the hub-side. • **MOOB**: Indicates that the configuration is retrieved via out-of-band. • **Local Upload**: Indicates that the configuration has been loaded using the Load Candidate button.

4.8.2 Ethernet Interface

This page provides detailed information about the interface between the computer and the modem.

4.8.2.1 Ethernet Interface Parameters



The tables below describe the parameters of the Ethernet interface.

Ethernet

Parameter	Description
Ethernet	
Ethernet MAC Address	MAC address of the Ethernet interface.
Management IP Address	Management IP address of the Ethernet interface.
Netmask	Network range for the user's LAN.

Editing the NAT/Firewall Enabled checkbox can be disabled by the service provider. In this case, the parameters are read-only.

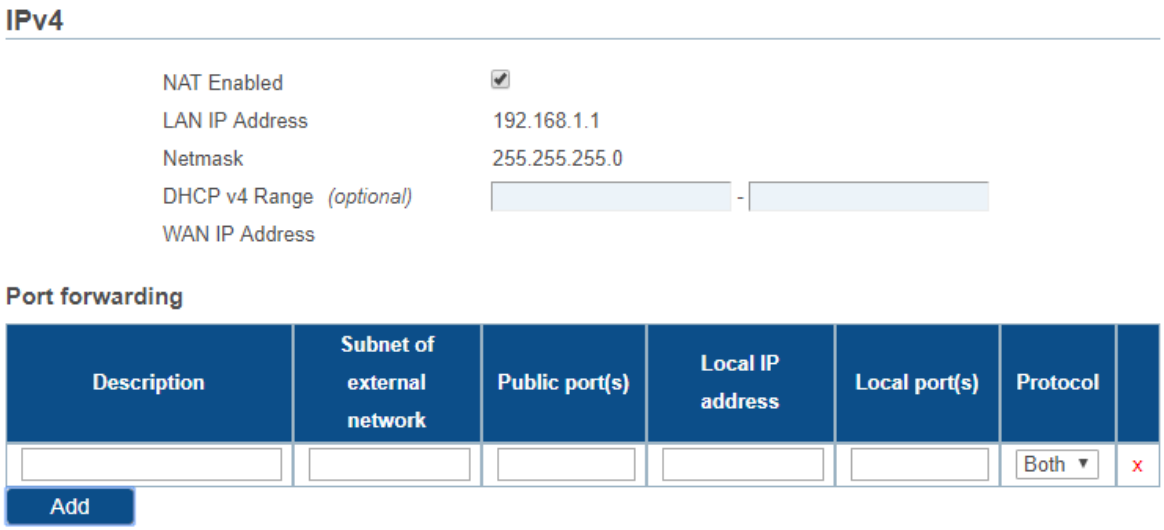
The NAT/Firewall configuration is only applicable to native (untagged) VLAN.

IPv4 NAT/Firewall Enabled checkboxes are mutual exclusive.

IPv4

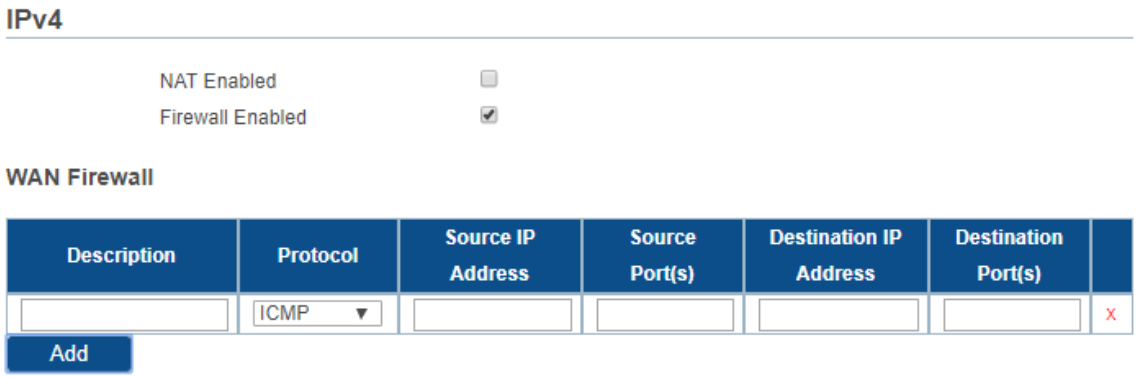
Parameter	Description
IPv4	
NAT Enabled	Enable or disable the Network Address Translation (NAT). Next to translating IP addresses, this function also activates port forwarding. Enabling NAT, means that: • Traffic from the WAN towards the LAN is being blocked. Except for response traffic that was initiated by a device inside the LAN. Add port forwarding rules to directly reach devices inside the LAN. • All outgoing traffic from the LAN towards the WAN is not blocked. If Firewall is enabled, NAT is disabled / not shown.
Firewall Enabled	Enable or disable firewall settings. Enabling Firewall means that: • Traffic from the WAN towards the LAN is being blocked. Add the WAN Firewall rules to create exceptions. • All outgoing traffic from the LAN towards the WAN is not blocked. To provide protection, by default firewall setting is disabled, which means that all incoming traffic is blocked, unless the traffic is requested from the terminal side. If NAT is enabled, firewall setting is disabled / not shown.

If NAT is enabled for IPv4, the following screen is displayed.



Parameter (NAT)		Description
IPv4		
LAN IP Address		This is the LAN IP address.
Netmask		Network range for the user's LAN.
DHCP v4 Range		The DHCP settings are only visible when NAT is enabled. Editable IP range from which the DHCP server can select IP addresses. When no range is specified, the complete range is available to the DHCP server.
WAN IP Address		This is the IP address which is used as source IP address for external traffic.
Port Forwarding	Description	Insert a logical description for the port forwarding. For example the name of the program, service that you want to forward. This feature is only displayed when NAT is enabled.
	Subnet of External Network	Enter the public IP Address from a server in the public domain from which you want to receive data. ***Note** - Entering the public IP address is optional.*
	Public Port(s)	Enter the port number of your modem on which you want to receive the data. This is the port on your modem facing the public network (for example the Internet).
	Local IP Address	Enter the local IP address, indicating to which device on the LAN you want to forward the data. This address must be in the same IP range as the LAN IP address.
	Local Port(s)	Enter the local port number you want to reach on the local device. ***Note** - The local device must be listening on this port to receive the data.*
	Protocol	Select the protocol (TCP or UDP) that is used by the source. Select both if you are not sure which protocol is used by the source.

If IPv4 firewall is enabled, the following screen is displayed.



Parameter (Firewall)	Description
IPv4	
Description	Insert a logical description for the firewall setting.
Protocol	Select any or specific type of protocol from the drop-down list.
Source IP Address	Specific host/subnet source IP address can be set for the selected protocol. The format is dot-decimal notation followed by a slash character (/), and ending with the bit-length of the prefix to specify a subnet. ***Note** - This is an optional parameter. Leave it blank to cover all sources of incoming traffic with the specified protocol*.
Source Port(s)	Specific port number from the selected source address can be set for the chosen protocol. ***Note** - This is an optional parameter. To specify more than one port number, use a dash (-) in between.*
Destination IP Address	Specific destination IP address can be set for the selected protocol. ***Note** - This is an optional parameter. Leave it blank to cover all sources of incoming traffic with the specified protocol.*
Destination Port(s)	Specific port number from the selected destination can be set for the chosen protocol. ***Note** - This is an optional parameter. To specify more than one port number, use a dash (-) in between.*

IPv6

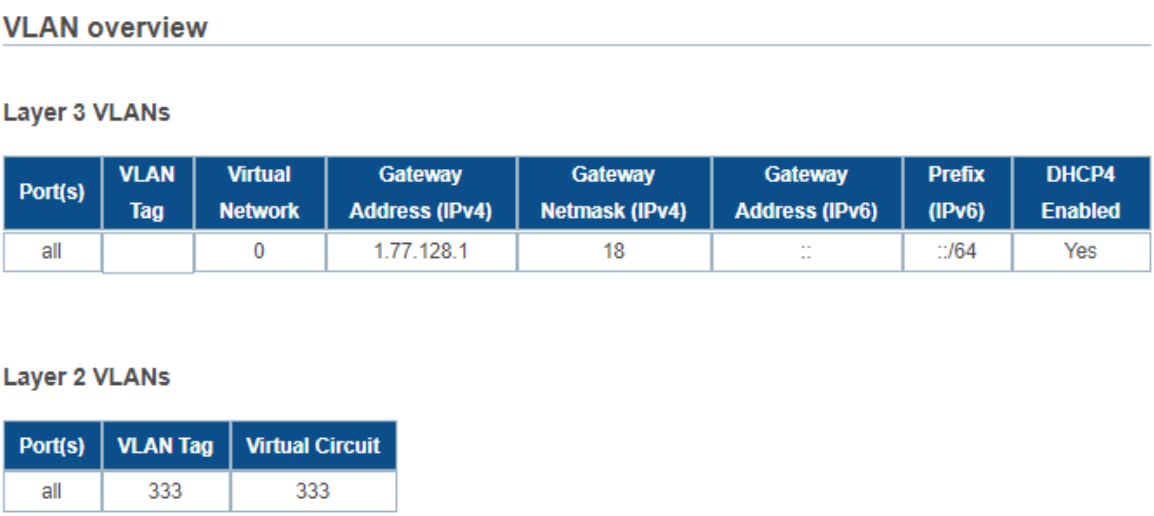
Parameter	Description
IPv6	
Firewall Enabled	Enable or disable firewall settings. ***Note** - Editing firewall enabled can be disabled by service provider.*

If IPv6 firewall is enabled, then the following screen is displayed.

The parameters of the IPv6 firewall setting is similar to those of the IPv4 firewall setting.

VLAN Overview

The VLAN Overview parameters are set by the service provider and cannot be edited by the end user.



VLAN overview

Layer 3 VLANs

Port(s)	VLAN Tag	Virtual Network	Gateway Address (IPv4)	Gateway Netmask (IPv4)	Gateway Address (IPv6)	Prefix (IPv6)	DHCP4 Enabled
all		0	1.77.128.1	18	::	::/64	Yes

Layer 2 VLANs

Port(s)	VLAN Tag	Virtual Circuit
all	333	333

Parameter	Description
Layer 3 VLANs	
Port(s)	Indicates the external Ethernet port.
VLAN Tag	Indicates a separation between different virtual networks.
Virtual Network	Name of the virtual network the modem belongs to.
Gateway Address (IPv4)	IPv4 address used as gateway address for the connected CPEs within that network.
Gateway Netmask (IPv4)	Network range for the user's LAN within that network.
Gateway Address (IPv6)	IPv6 address used as gateway address for the connected CPEs within that network.
Prefix (IPv6)	Network range for the user's LAN within that network.
DHCP4 Enabled	Indicates whether the DHCP server on the terminal is enabled or not.
Layer 2 VLANs	
Port(s)	Indicates the external Ethernet port.
VLAN Tag	Indicates a separation between different virtual networks.
Virtual Circuit	Name of the virtual circuit the modem belongs to.

4.8.2.2 Edit Ethernet Interface Configuration

To edit the parameters of the Ethernet interface, execute the following steps:

1. Click Edit at the bottom right of the page.
2. Change the parameters. Refer to Ethernet Interface Parameters on page 42.
   In case IPv4/v6 Firewall or IPv4 NAT, click Add to create a new firewall or port forwarding rule.

The Layer 2 and 3 VLAN parameters cannot be edited.

3. Click Save to store the new settings or click Cancel to discard the new settings.

4.8.3 Satellite Interface

This page provides detailed information about the interface settings between the terminal and the satellite.

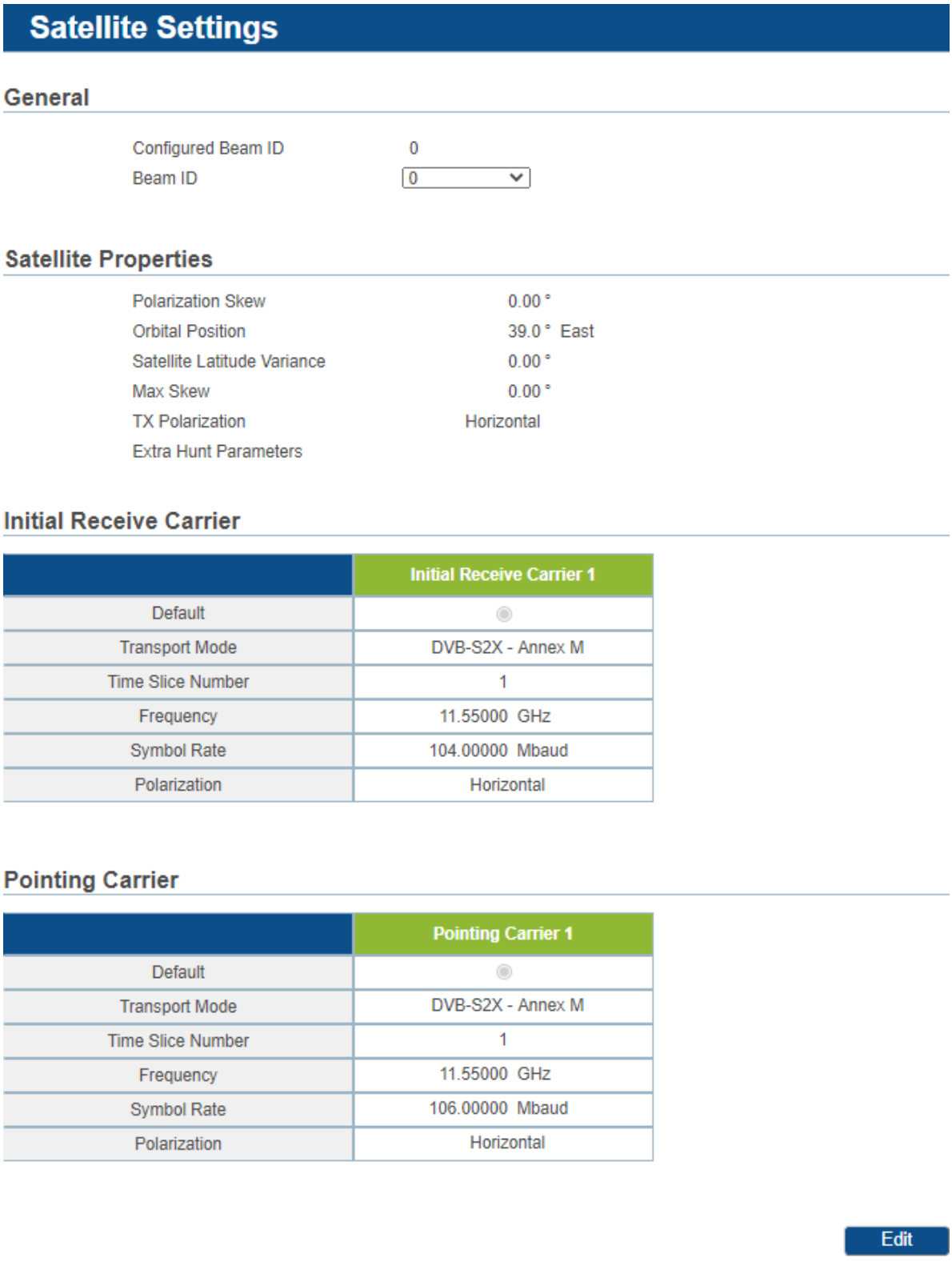
The satellite interface settings are predefined in factory. These settings may only be changed upon advice of your service provider.

A satellite beam covers a limited geographical area in which terminals are serviced by the satellite.

The displayed satellite interface settings depend on the beam that was selected during the terminal installation.

Refer to Terminal Installation on page 18 for more information.

4.8.3.1 View Satellite Settings



If multiple beams are configured, you can select another beam from the drop-down list in the General section to view its satellite settings. Changing the active beam is done via the Terminal Installation menu.

Every satellite interface setting consists of:

- **Initial Receive Carrier**

  This is the initial receive carrier through which the modem will try to gain access to the network.

- **Pointing Carrier**

  This carrier is needed to enable antenna pointing via the Point&Play mechanism or the automatic pointing method. When two different pointing carriers are assigned to the terminal, the installer can perform his pointing on two different pointing carriers. At least one pointing carrier must be enabled.

Maximum two initial receive carrier settings and pointing carrier settings can be assigned and displayed. Only the settings that are enabled are displayed. How to change the satellite interface configuration is described in section Edit Satellite Settings on page 51.

If two initial receive carriers are enabled and displayed, the preferred initial receive carrier is marked green. If two pointing carriers are enabled and displayed, the default pointing carrier is marked green.

The pointing carrier that is used for pointing is selected through the Terminal Installation menu. Refer to Terminal Installation on page 18 for more details.

4.8.3.2 Satellite Interface Parameters

The table below describes the different parameters of the satellite interface.

Parameter	Description
General	
Configured Beam ID	Identifier of the beam that was selected during terminal installation. The terminal operates in this beam. In case automatic beam selection is enabled, this is set to Auto.
Beam ID	Identifier of the beam that has its parameters displayed in the GUI.
Satellite Properties	
Polarization Skew	Skew angle in degrees applied by the satellite operator. Check with your satellite operator to know this value. The value is a positive or negative integer with dotted decimal notation.
Orbital Position	Orbital position of the satellite in degrees and East/West selection.
Satellite Latitude Variance	Only applicable in case of automatic pointing. Typically used for inclined orbit satellites. Check with your satellite operator to know this value.
Max Skew	Polarization adjustment angle.
TX Polarization	Reflects the polarization of the received carrier. The possible values are: • Horizontal • Vertical • Circular Left • Circular Right
Extra Hunt Parameters	This is a free text field in which antenna specific OpenAMIP messages can be entered.
Initial Receive Carrier	

Parameter	Description
Default	Marker for the default Initial Receive Carrier.
Transport Mode	• DVB-S2/DVB-S2X (ACM) • DVB-S2X Annex M
Time Slice Number	This number allows the receivers to pre-select specified streams in the physical layer carrying one or more services. This parameter is only available when Transport Mode is set to DVB-S2X Annex M.
Frequency	Initial receive frequency (GHz).
Symbol Rate	Initial receive symbol rate (Mbaud).
Polarization	Reflects the polarization of the received carrier. The possible values are: • Horizontal • Vertical • Circular Left • Circular Right
Pointing Carrier	
Default	Marker for the default pointing carrier
Transport Mode	• DVB-S2/DVB-S2X (ACM) • DVB-S2X Annex M
Time Slice Number	This number allows the receivers to pre-select specified streams in the physical layer carrying one or more services. This parameter is only available when Transport Mode is set to DVB-S2X Annex M.
Frequency	Initial receive frequency (GHz).
Symbol Rate	Initial receive symbol rate (Mbaud).
Polarization	Reflects the polarization of the received carrier. The possible values are: • Horizontal • Vertical • Circular Left • Circular Right
Automatic Beam Selection (only available when mobility is enabled)	
Beam Name	Name of the beam as mentioned in the corresponding GXT file.
Cost	Value used by the terminal when it can choose to operate in multiple beams. The beam with the lowest cost value is then selected.
Automatic Pointing Timeout Value	Time interval after which a terminal returns to the automatic beam selection procedure if the terminal can not lock on the received forward link.
GXT File Name	Name of the GXT file associated with this beam.
Exclusion Zones	Area in which a terminal is not allowed to operate. This area is determined by the following parameters: • Service Area Number as mentioned in the GXT file. • TX Allowed: Checkbox to indicate of terminal can only transmit in the exclusion zone. • RX Allowed: Checkbox to indicate of terminal can only receive in the exclusion zone.

4.8.3.3 Edit Satellite Settings

Editing the satellite settings can be disabled by the service provider. In that case, the Edit button is not present and the configuration settings are read-only.

To edit the parameters of the satellite interface, execute the following steps:

1. Click Edit at the bottom right of the page.
2. Change the parameters. Refer to Satellite Interface Parameters on page 49.

- At least the preferred initial receive carrier and default pointing carrier must be enabled.
- Automatic Beam Selection parameters are only editable if terminal mobility is enabled.

3. Click Save to save your settings or Cancel to discard your settings.

Refer to Terminal Installation on page 18 for changing the selected beam.

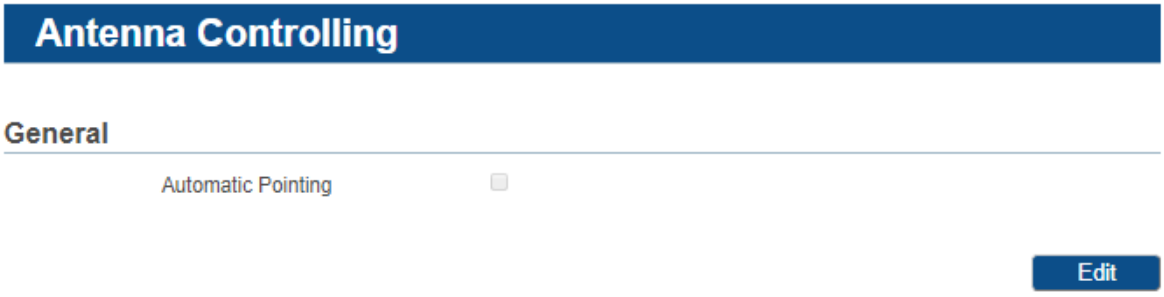
The satellite interface can also be configured remotely from the hub using the **Remote Terminal Satellite Configuration** feature. The remote satellite configuration is created from the data in the central Network Management System or NMS, and is downloaded by the terminal.

4.8.4 Antenna Controlling

The service provider can disable the Antenna Controlling feature. In that case, the Edit button is not present and the Antenna Controlling settings are read-only.

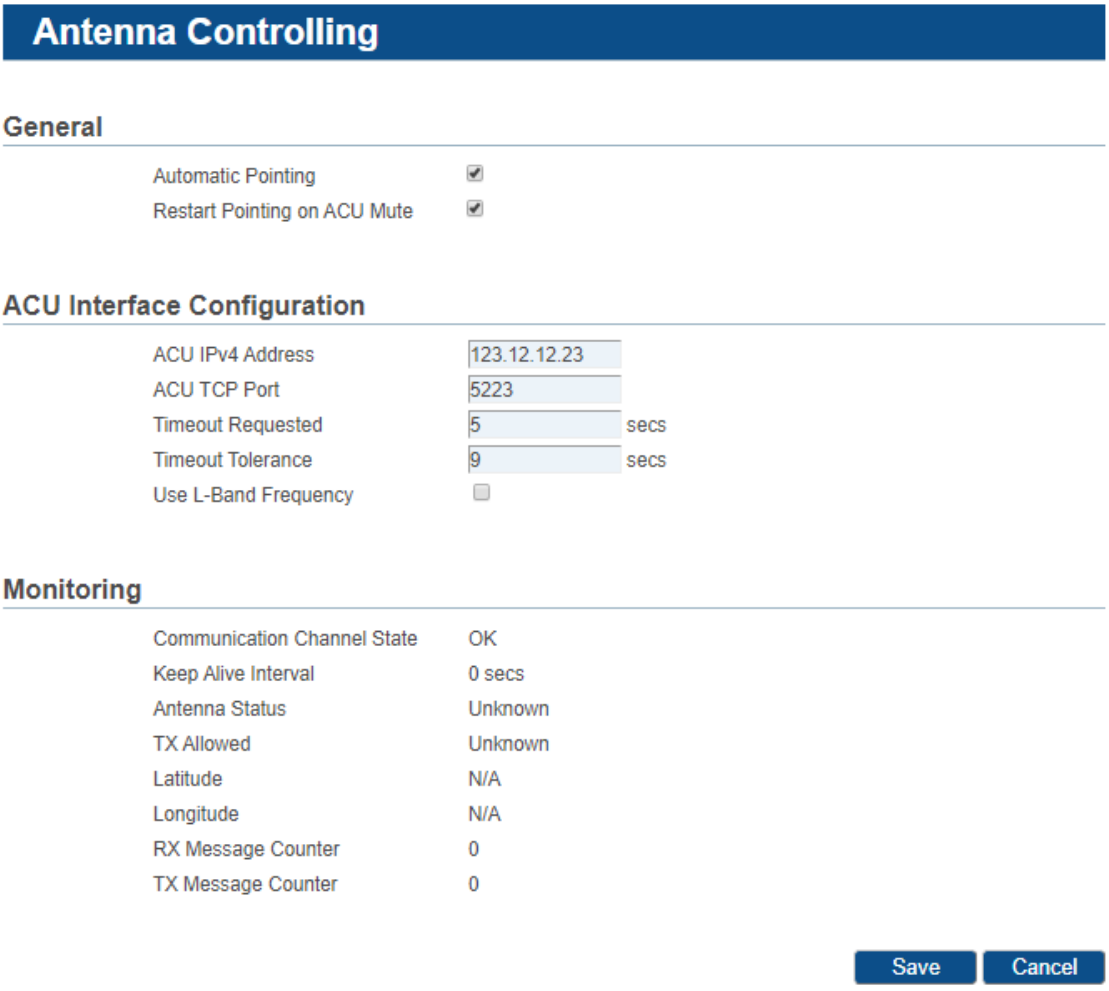
This page is used to enable automatic pointing. Automatic pointing only applies if an Antenna Control Unit or ACU is connected to the modem, as mentioned in Using Automatic Pointing on page 31.

When automatic pointing is enabled, the modem sends the parameters of the default pointing carrier and the outdoor unit towards the ACU via OpenAMIP messages. Pointing carrier parameters are set as described in Satellite Interface on page 47. The ACU uses this data to track the correct satellite.



To enable automat automatic pointing, execute the following steps:

1. Click Edit and select the Automatic Pointing check box. The following window appears:



2. Enter the parameter values:
   - **Restart Pointing on ACU Mute**: Select the check box to restart pointing in case the ACU signals the modem that the antenna is not pointed and that the modem should not transmit. If not selected, the modem will disable its transmit but remain operational. The check box is by default selected.
   - **ACU Interface Configuration**: These are the parameters that define the OpenAMIP communication channel between the modem and the ACU.

Parameter	Description
ACU IPv4 Address	IPv4 address of the ACU. The modem uses the entered IP address to reach the ACU. Make sure the management IP address of the modem and the ACU are in the same IP subnet.
ACU TCP Port	TCP port of the ACU. The modem uses the entered TCP port to reach the ACU.
Timeout Requested	Keep alive time in which the modem asks the ACU to send its GPS coordinates and the antenna status.
Timeout Tolerance	If the modem does not receive the status within this time interval, the modem switches back to pointing mode.

Use L-Band Frequency	Checkbox to indicate if modem sends L-band frequency or RF frequency to the ACU.

3. Click Save to save your settings or Cancel to discard your settings.

Check the monitoring parameters to verify the OpenAMIP communication between modem and ACU.

Parameter	Description
Communication Channel State	Indicates if the TCP communication between modem and ACU is OK or not.
Keep Alive Interval	Time interval in which the ACU expects feedback from the modem.
Antenna Status	Message from the ACU informing the modem about antenna pointing status. Possible values are: OK Not OK Unknown
TX Allowed	Message from the ACU informing the modem that it can transmit a signal. Transmission is typically allowed after pointing is successfully completed.
Latitude	Latitude provided by the GPS of the ACU.
Longitude	Longitude provided by the GPS of the ACU.
RX Message Counter	Number of OpenAMIP messages sent by the ACU and received by the modem.
TX Message Counter	Number of OpenAMIP messages sent by the modem towards the ACU.

4.8.5 Outdoor Unit

An Outdoor Unit (ODU) is defined as the combined set of antenna, LNB and BUC.

The modem hardware and software support several ODU types but in order to verify the quality of a terminal installation, the system should know which ODU is actually used. An ODU type is known to the terminal in one of the following ways:

- One or more ODU types are **pre-configured** in factory. If only one ODU type is configured, this ODU will be selected automatically during the installation procedure. If multiple types are predefined, the user can select the ODU he is actually using via a drop-down list during the installation procedure. For more information about terminal installation, refer to Terminal Installation on page 18.
- If no ODU types have been pre-configured in factory, the user should add the ODU types before starting the installation procedure. For more information, refer to Add ODU Configuration on page 60.

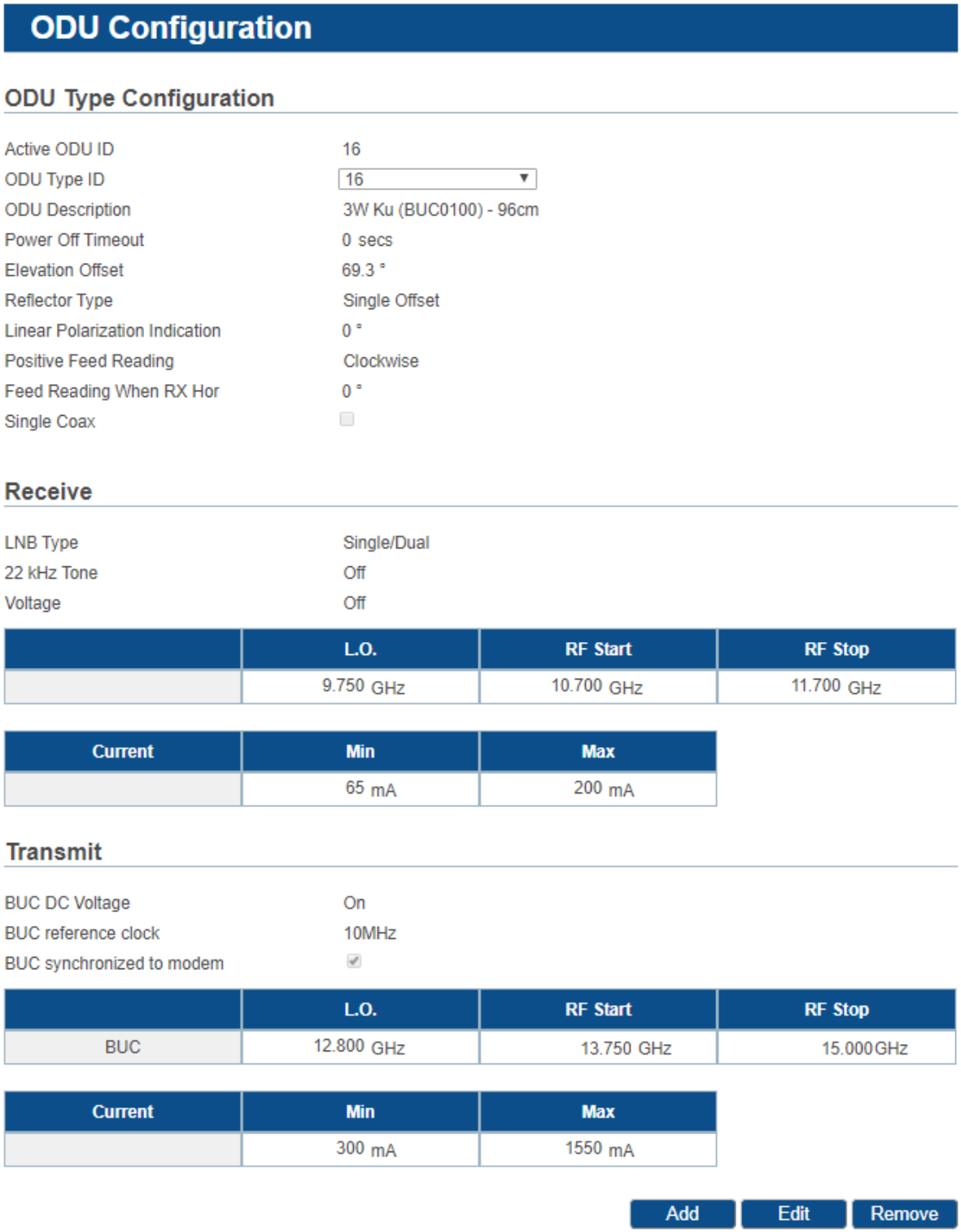
Be careful when changing or adding ODU types. If you use the Terminal Installation Certification System (TICS), the ODU parameters in the modem GUI must match with the ones defined in TICS.

The ODU types are not affected by a factory reset of the modem.

4.8.5.1 View ODU Configuration

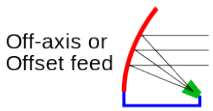
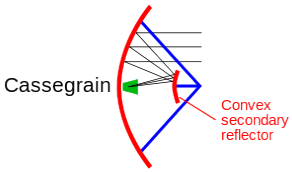
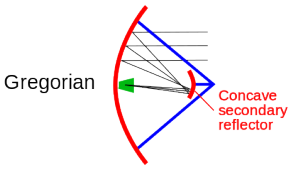
When selecting the Outdoor Unit menu item, the parameters of the ODU which was selected during installation are displayed by default. If multiple outdoor unit types are defined, use the drop-down box to select the ODU for which you want to display the parameters.

Editing/adding/removing an ODU configuration can be disabled by the service provider. In this case, the Edit/Add/Remove buttons are not present and the ODU configuration settings are read-only.



4.8.5.2 ODU Parameters

The table below describes the different parameters of the satellite interface.

Parameter	Description
ODU Type Configuration	
Active ODU ID	Indicates which outdoor unit is active at the moment. This is the ODU that has been selected during terminal installation.
ODU Type ID	This is the ID of the ODU for which the parameters are displayed. This is the active ODU by default. When adding a new ODU, the following convention should be used: • The ID is a positive integer. • Range 1-32 is reserved for ST Engineering iDirect ODU types. • Range 33-64 is for user definable ODU types.
ODU Description	This is a string describing the ODU.
Power Off Timeout	Not yet supported.
Elevation Offset	This parameter is used as input to the Point&Play app. It is the delta between the antenna real elevation and the elevation of the reference plane to which the smartphone will be placed for the elevation measurement. This offset is different for different antenna types. For ANT2010 75cm, the elevation offset is 72.97°. For ANT2025 1m, the elevation offset is 71.50°. For ANT2035 1.2m, the elevation offset is 68.40°. For a 3rd party antenna, contact your manufacturer for this value.
Reflector Type	This parameter is used as input to the Point&Play app. The following antenna types are supported: • Single-offset antennas  • Cassegrain antenna with a convex subreflector  • Gregorian antenna with a concave subreflector  All ST Engineering iDirect antennas are single-offset antennas.

Parameter	Description
Linear Polarization Indication	This parameter is used as input to the Point&Play app. It indicates the midrange value of the feed reading. For example, if the reading is from 0° to 180° the value is 90°.
Positive Feed Reading	This parameter is used as input to the Point&Play app. This indicates if the feed reading is clockwise or counterclockwise: • Clockwise means that the reading from the lowest degrees to the highest degrees is done clockwise. • Counterclockwise means that the reading from the lowest degrees to the highest degrees is done counterclockwise. For example, if the reading from 0° to 180° is done clockwise the value is 'clockwise'. If the reading from -45° to +45° is done counterclockwise, the value is 'counterclockwise'.
Feed Reading When RX Hor	This parameter is used as input to the Point&Play app. It indicates the feed reading when the antenna and (i)LNB are aligned with a linear polarized horizontal signal from the satellite. For example, for the combination ANT2010 (75cm) and ILB2120(Ku) this is +90°.
Single Coax	Indicates if the Tx and Rx of the iLNB are combined into a single coax. This is the case for ILNB2220 and ILNB2221.
Receive	
LNB Type	• Single/Dual indicates that the LNB contains one or two local oscillators. • Multiband indicates that the LNB contains more than two local oscillators. All ST Engineering iDirect iLNBs have two local oscillators, except ILB2210, which has one local oscillator. This is usually indicated on the LNB itself or can be found in the data sheet.
22 kHz Tone	Used to inform the LNB about the frequency band it needs to use. Refer to the LNB data sheet to know the value. Possible values are: • Off • On • Band selection
Voltage	Used to inform the LNB about which polarization it needs to use. Refer to the LNB data sheet to know which value to set. Possible values are: • Off • Fixed 13 V • Fixed 18 V

Parameter	Description
	• Band selection (if not set via 22 kHz tone) • Polarization selection
Low Band L.O.	Local oscillator frequency (in GHz) used when the LNB is operating in low band. Only applicable if 'Band selection' is used in 22 kHz or Voltage settings. If 'Band selection' is not used, then only set one local oscillator frequency (as there is no distinction between high and low band). The value can be found on the LNB or in the LNB data sheet.
Low Band RF Start	Minimum frequency used by the LNB when operating in low band. Only applicable if 'Band selection' is used in 22 kHz or Voltage settings. If 'Band selection' is not used, then only set one RF Start frequency (as there is no distinction between high and low band). The value can be found on the LNB or in the LNB data sheet.
Low Band RF Stop	Maximum frequency used by the LNB when operating in low band. Only applicable if 'Band selection' is used in 22 kHz or Voltage settings. If 'Band selection' is not used, then only set one RF Stop frequency (as there is no distinction between high and low band). The value can be found on the LNB or in the LNB data sheet.
High Band L.O.	Local oscillator frequency (in GHz) used when the LNB is operating in high band. Only applicable if 'Band selection' is used in 22 kHz or Voltage settings. If 'Band selection' is not used, then only set one local oscillator frequency (as there is no distinction between high and low band). The value can be found on the LNB or in the LNB data sheet.
High Band RF Start	Minimum frequency used by the LNB when operating in high band. Only applicable if 'Band selection' is used in 22 kHz or Voltage settings. If 'Band selection' is not used, then only set one RF Start frequency (as there is no distinction between high and low band). The value can be found on the LNB or in the LNB data sheet.
High Band RF Stop	Maximum frequency used by the LNB when operating in high band. Only applicable if 'Band selection' is used in 22 kHz or Voltage settings. If 'Band selection' is not used, then only set one RF Stop frequency (as there is no distinction between high and low band). The value can be found on the LNB or in the LNB data sheet.
Current Min / Max	Minimum/maximum allowed current on the RX interface. This input is required for correct functioning of the current measurement test (see section Hardware Test on page 83).
Transmit	
Transmitter Type	Select the type of transmitter: • BUC • MUC

Parameter	Description
BUC DC Voltage	You can put a DC voltage on the TX connector. Possible values are: • Off • On The DC voltage (24V) is typically used to power a BUC. ***Warning*** *- Make sure to disable the DC output voltage when using a BUC that is externally powered. Or use a DC blocker to avoid damaging the externally powered BUC.*
BUC reference clock	You can put a reference frequency on the TX connector. Possible values are: • Off • 10MHz • 50MHz Select **Off** if the BUC uses an internal reference or is slaved to a reference source other than the modem.
BUC synchronized to modem	This parameter is by default enabled. In this case, the variations between the clock used by the modem and the BUC are reduced to a minimum. The advantage is that the terminal logon times are kept as low as possible. In this way the Maximum Frequency Uncertainty range is limited to a minimum. When disables, the Maximum Frequency Uncertainty must be increased resulting in a higher terminal logon times. It is recommended to enable the BUC reference clock in combination with this synchronization parameter. Typically **BUC Synchronized to Modem** is enabled when a **BUC reference clock** is selected. Only in special uses cases the configuration can differ from one another. For example when one BUC is used by multiple modems. In this case: • Select a BUC reference clock on only one modem. This frequency is used as the reference signal for the BUC. • Enable BUC Synchronized to Modem on all modems to keep the devices in sync.
BUC L.O.	Local oscillator frequency (in GHz) used by the BUC, which can typically be found in the BUC data sheet.
BUC RF Start	Minimum RF frequency the BUC can transmit.
BUC RF Stop	Maximum RF frequency the BUC can transmit.
MUC Multiplicator	Multiplication factor used by the MUC to convert from IF to RF-band (as n*transmitted IF freq = transmitted RF freq, where n = multiplication factor). Only visible if ILB2220 is used as outdoor unit type. As the ILB2220 operates in Ka-band, the multiplication factor = 10.
MUC RF Start	Minimum RF frequency the MUC can transmit.

Parameter	Description
MUC RF Stop	Maximum RF frequency the MUC can transmit.
Current Min / Max	Minimum/maximum allowed current on the TX interface. This input is required for correct functioning of the current measurement test (see section Hardware Test on page 83).

4.8.5.3 Edit ODU Configuration

The service provider can disable editing an ODU configuration. In that case, the Edit button is not present and the ODU configuration settings are read-only.

To edit the parameters of the ODU, execute the following steps:

1. If there are multiple ODU types defined, select the **ODU Type ID** of the ODU you want to change.
2. Click Edit.
3. Change the parameters. Refer to ODU Parameters on page 55.

The Active ODU ID, the ODU Type ID and the ODU Description parameters cannot be edited.

Entering incorrect settings can prevent your modem from logging onto the network! Only change outdoor unit settings when requested by your Service Provider or Network Operator.

4. Click Save to save your settings or Cancel to discard your settings.

4.8.5.4 Add ODU Configuration

The service provider can disable adding an ODU Configuration. In that case, the Add button is not present and the ODU configuration settings are read-only.

Take care when adding ODU types. If you use the Terminal Installation Certification System (TICS), the ODU parameters in the modem GUI must match with the ones defined in TICS.

Contact your service provider or network operator in case of doubt.

To create a new ODU type, execute the following steps:

1. Click Add.
2. Enter the values for the parameters of the new ODU type. Refer to ODU Parameters on page 55.

Incorrect settings can prevent your modem from logging onto the network! Contact your service provider or network operator in case of doubt.

3. Click Save to create the new ODU type or Cancel to discard your settings.

4.8.5.5 Remove ODU Configuration

The service provider can disable removing an ODU Configuration. In that case, the Remove button is not present and the ODU configuration settings are read-only.

To remove a configured outdoor unit configuration, execute the following steps:

1. Select the **ODU Type ID** of the ODU you want to remove and click Remove. A confirmation message pops up.
2. Click OK to remove the ODU parameter set or click Cancel to keep the ODU parameter set.

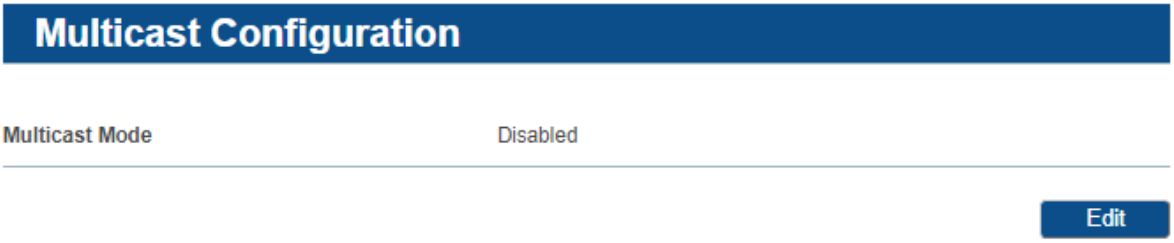
4.8.6 Multicast

The modem can receive one or more multicast streams over satellite. The maximum number of multicast streams is ten.

The configuration to receive a multicast stream can be based on a static IP address or the IGMP protocol.

- **Static IP addresses**: In this case, you statically set the multicast IP addresses of the multicast stream.
- **IGMP**: In this case, the modem uses the IGMP protocol to request membership to a multicast stream.

4.8.6.1 Multicast Parameters



Parameter	Description
Multicast Mode	• Disabled: Multicast mode is disabled. • Static: The active Multicast Configuration is based on entered Static Multicast IP Addresses. • IGMP Dynamic: Dynamic IGMP multicast mode.
Static Multicast IP Addresses (max. 10)	Only appears when the Multicast Mode is Static. Maximum 10 multicast IP Addresses can be assigned.

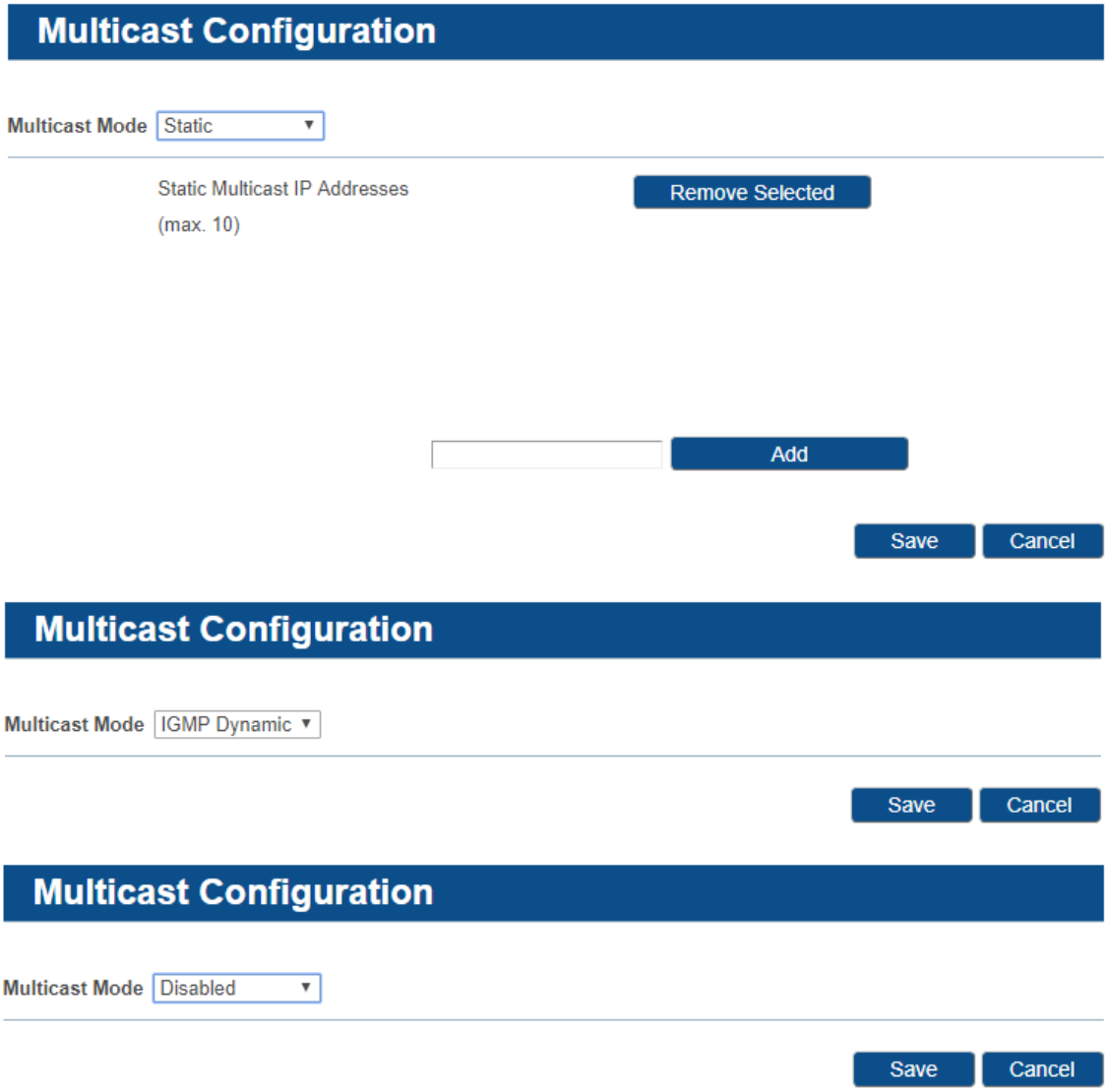
4.8.6.2 Edit Multicast Configuration

The service provider can disable editing a multicast. In this case, the Edit button is not present and the Multicast Configuration settings are read-only.

To edit the parameters, execute the following steps:

1. Click Edit.
2. Select the Multicast Mode.

   If you select Static, the parameter Static Multicast IP Addresses is added. Click Add to define a static IP address. Click Remove Selected to delete a static IP address. You cannot edit an address; you will need to delete the old address and then add the new address.



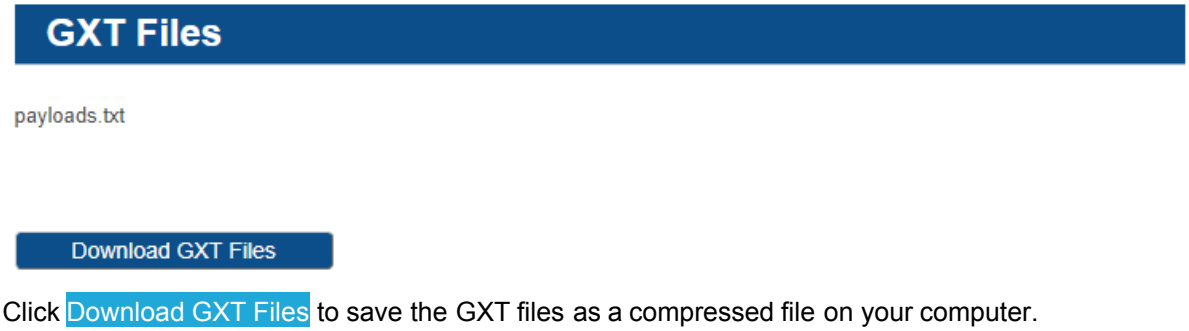
3. Click Save to save your settings or Cancel to discard your settings.

In case an invalid multicast IP address is replacing a valid multicast IP address, the last valid multicast IP address will still be in use.

4.8.7 [optional] GXT Files

The **GXT Files** menu item is only available if terminal mobility is enabled.

Here you can find all GXT files that are known in the modem.



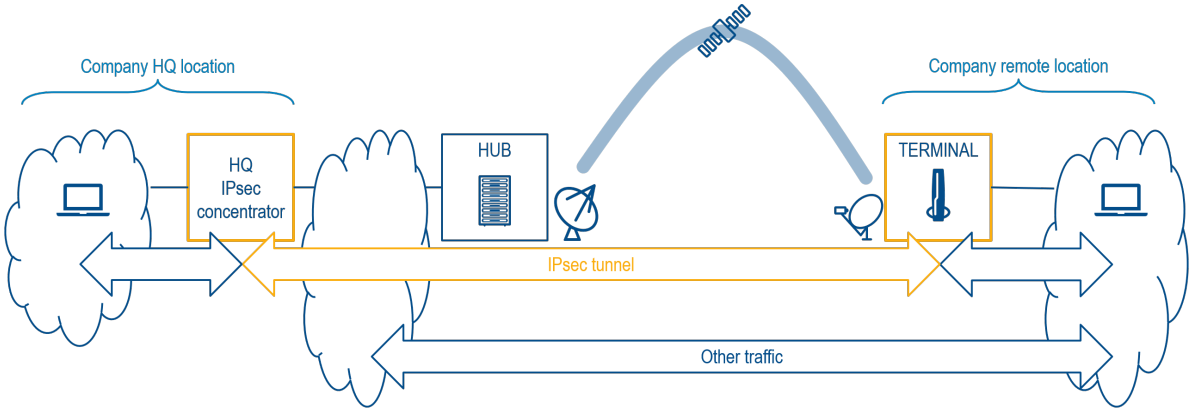
Click Download GXT Files to save the GXT files as a compressed file on your computer.

More functionality is available when logged in as Expert. Refer to Terminal Mobility on page 103 for more information.

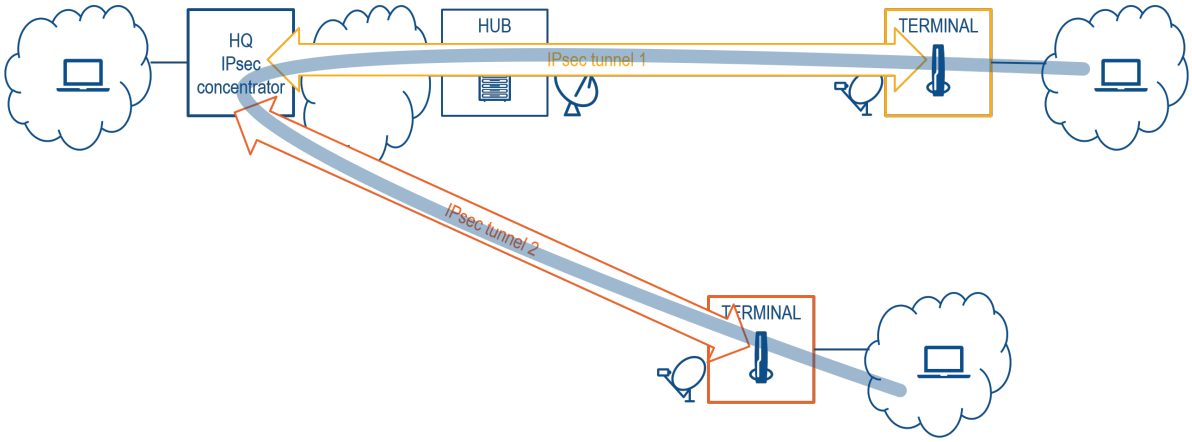
4.8.8 [optional] VPN IPSec Configuration

IPsec or Internet Protocol Security is a suite of protocols that provides security to Internet communications at the IP layer. IPsec also provides methods for the manual and automatic negotiation of security associations (SAs) and key distribution. IPsec is commonly used in Virtual Private Networks or VPNs. IPsec can protect data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host).

Dialog supports IPsec between a pair of hosts. The figure shows an end-to-end IPsec tunnel between a Dialog modem and a company headquarters (HQ). Traffic between the modem and headquarters goes trough the IPsec tunnel. Other traffic bypasses the IPsec tunnel.



In case of multiple remote locations, a dedicated IPsec tunnel exists for each remote location. Communication between the remote sites always pass the headquarters.



VPN IPsec is only supported on modems that belong to a shared subnet.

A security association (SA) is a unidirectional agreement between the VPN participants regarding the methods and parameters to use in securing a communication channel. Full bidirectional communication requires at least two SAs, one for each direction. Through the SA, an IPsec tunnel can provide the following security functions:

- Privacy (through encryption)
- Content integrity (through data authentication)
- Sender authentication and - if using certificates - nonrepudiation (through data origin authentication)

The distribution and management of keys are critical to using VPNs successfully. IPsec supports the automated generation and negotiation of keys and security associations using the Internet Key Exchange (IKE) protocol. IKE uses pre-shared keys or X.509 certificates for authentication and a Diffie–Hellman key exchange to set up a shared session secret from which cryptographic keys are derived.

- IKE with pre-shared keys - Using IKE with pre-shared keys to authenticate the hosts in an IKE session, each host must configure the pre-shared key in advance. In this regard, the issue of secure key exchange is the same as that with manual keys. However, once exchanged, the pre-shared key, unlike a manual key, can automatically change at predetermined intervals using the IKE protocol. Frequently changing keys greatly improves security, however, changing keys increases traffic overhead; therefore, changing keys too often can reduce data transmission efficiency.
- IKE with certificates - When using certificates to authenticate the hosts during an IKE negotiation, each host generates a public-private key pair and acquires a certificate. As long as the issuing certificate authority (CA) is trusted by both sides, the hosts can retrieve the peer's public key and verify the peer's signature. There is no need to keep track of the keys and SAs; IKE does it automatically.
- A Diffie-Hellman (DH) key exchange allows hosts to produce a shared secret value. The strength of the technique is that it allows hosts to create the secret value over an unsecured medium without passing the secret value through the wire.

To establish an IKE IPsec tunnel, two phases of negotiation are required:

- In Phase 1, the hosts establish a secure authenticated communication channel by using the Diffie–Hellman key exchange algorithm to generate a shared secret key to encrypt further IKE communications.
- In Phase 2, the IKE hosts use the secure channel established in Phase 1 to negotiate the IPsec SAs for encrypting and authenticating the ensuing exchanges of user data.

Two versions of IKE exist: v1 and v2. V2 has some improvements over v1 as shown in the table.

		IKEv1	**IKEv2**
Simplicity	**Phase 1**	6 messages (main mode), 3 messages (aggressive mode)	4 messages
	Phase 2	3 messages	2 messages
Security	**Identity hiding**	Optional, only in main mode	Always
Reliability	**Message ACK**	None	All messages are acknowledged and sequenced
Flexibility	**Backward compatibility**	No	Yes
	Authentication	None	Extensible Authentication Protocol
	Rekeying	Requires re-authentication	No re-authentication required

IPsec uses two protocols to secure communications at the IP layer:

- Authentication Header (AH) - A security protocol for authenticating the source of an IP packet and verifying the integrity of its content.
- Encapsulating Security Payload (ESP) - A security protocol for encrypting the entire IP packet and authenticating its content.

4.8.8.1 View VPN IPSec Configuration

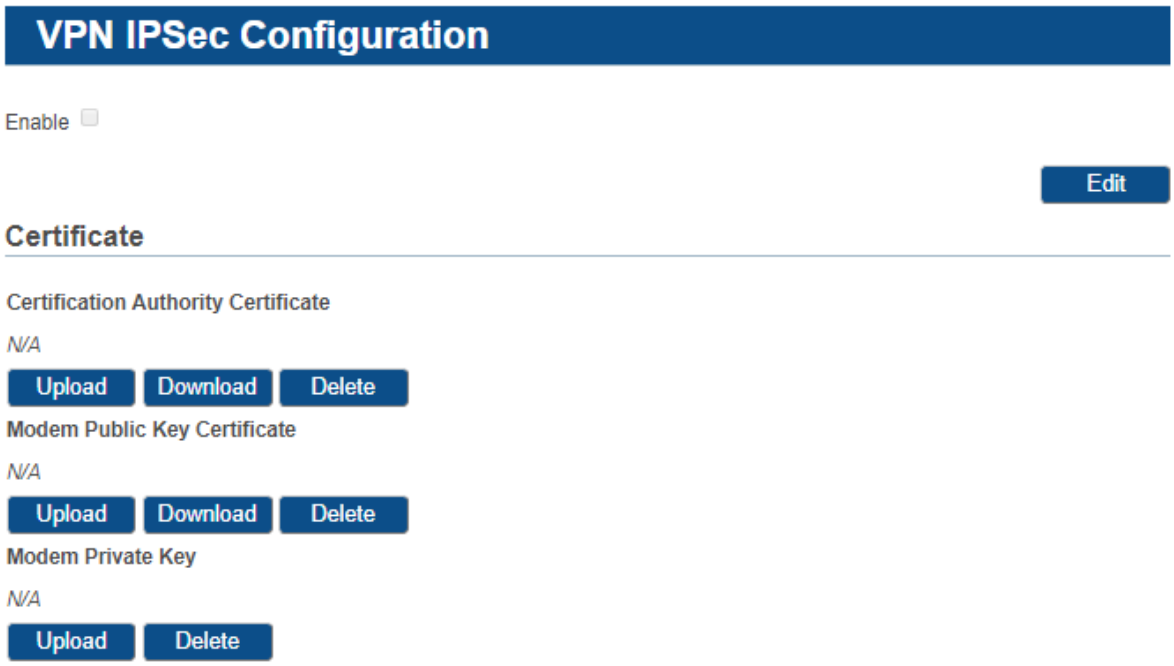
VPN IPSec is an optional feature on your modem. If your modem does not support the feature, the **VPN IPSec Configuration** menu item is not visible.

When IPsec is enabled, we recommend to set the MTU size to 1600 bytes. The MTU size at the modem Ethernet interface is 1600 bytes - IPsec overhead, which is 1500 bytes. An MTU size of 1500 bytes is a common value for IP data.

The MTU size is set when configuring the hub termination point for your layer 3 network. For more information, refer to *How to Create Layer 3 Network Resources* in the *Newtec Dialog Configuration User Guide*.

IPSec is by default disabled.

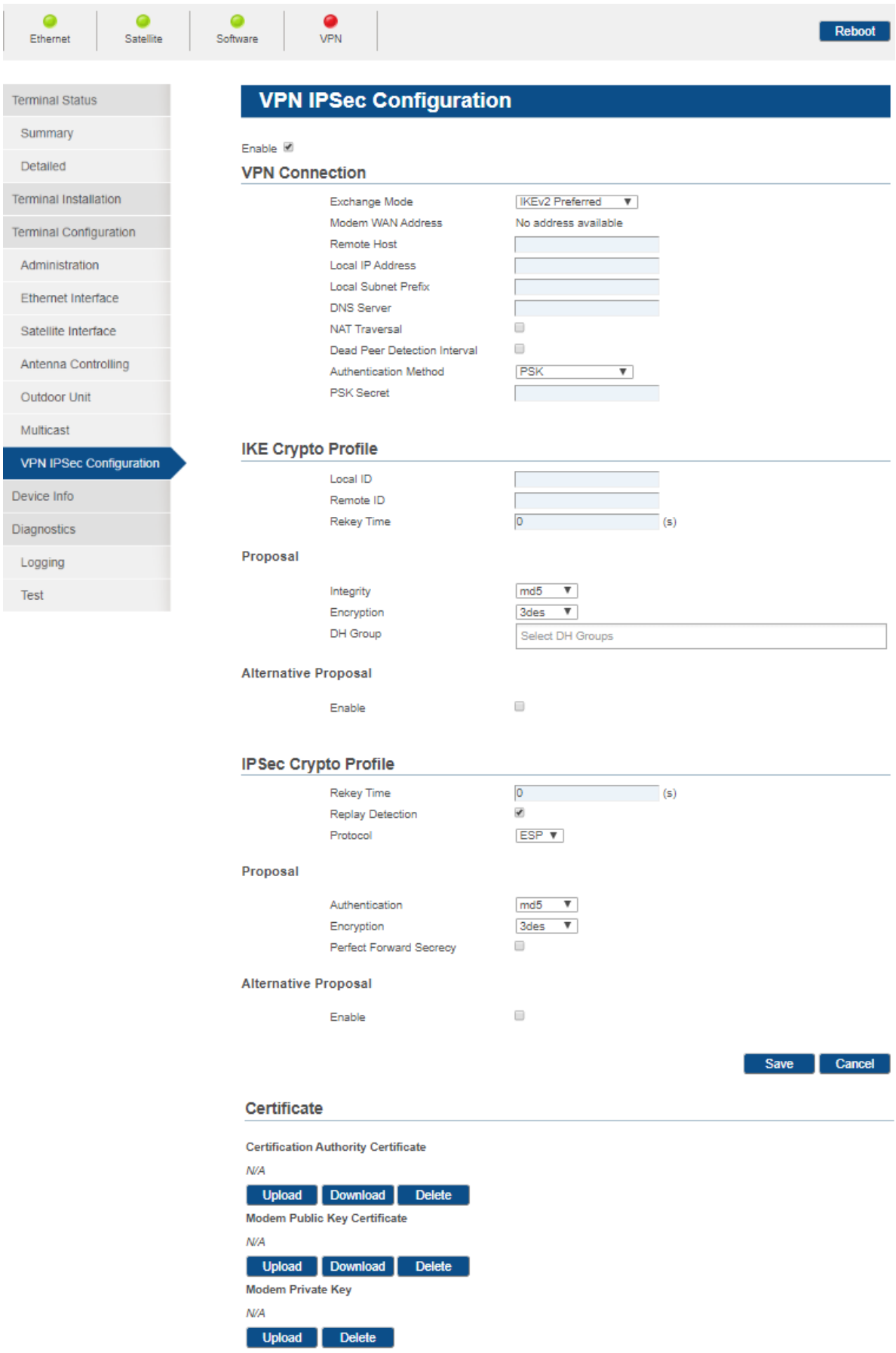
- The check box **Enable** is not selected.
- There is no **VPN** LED in the status bar.



To enable VPN IPsec, click the Edit button and select the check box **Enable**. The VPN IPSec configuration settings and the VPN LED in the status bar appear.

The VPN LED indicates the status of IPSec:

- If the LED is red, no IKE and no IPSec is up.
- If the LED is orange, the IKE is up but IPSec is not up.
- If the LED is green, both IKE and IPSec are up.


Ethernet
Satellite
Software
VPN
Reboot
Terminal Status
Summary
Detailed
Terminal Installation
Terminal Configuration
Administration
Ethernet Interface
Satellite Interface
Antenna Controlling
Outdoor Unit
Multicast
VPN IPSec Configuration
Device Info
Diagnostics
Logging
Test
VPN IPSec Configuration
Enable
VPN Connection
Exchange Mode
IKEv2 Preferred
Modem WAN Address
No address available
Remote Host
Local IP Address
Local Subnet Prefix
DNS Server
NAT Traversal
Dead Peer Detection Interval
Authentication Method
PSK
PSK Secret
IKE Crypto Profile
Local ID
Remote ID
Rekey Time
0
(s)
Proposal
Integrity
md5
Encryption
3des
DH Group
Select DH Groups
Alternative Proposal
Enable
IPSec Crypto Profile
Rekey Time
0
(s)
Replay Detection
Protocol
ESP
Proposal
Authentication
md5
Encryption
3des
Perfect Forward Secrecy
Alternative Proposal
Enable
Save
Cancel
Certificate
Certification Authority Certificate
N/A
Upload
Download
Delete
Modem Public Key Certificate
N/A
Upload
Download
Delete
Modem Private Key
N/A
Upload
Delete

4.8.8.2 VPN IPSec Parameters

Dialog supports IPsec between a pair of hosts and using IKE.

The VPN IPsec configuration is divided in the following sections:

- **VPN Connection**

  In this section you define the hosts between which the IPsec connection should be established. You also define the IKE mode to set up the security association or SA and the mode for authenticating the hosts.

- **IKE Crypto Profile**

  In this section you define how to establish the secure authenticated communication channel by using the Diffie–Hellman key exchange algorithm to generate a shared secret key to encrypt further IKE communications. This defines phase 1 of IKE.

- **IPsec Crypto Profile**

  In this section you define how to negotiate the security associations on behalf of IPsec. This defines phase 2 of IKE.

- **Certificate**

  This section allows you to manage the certificates in case certificates are used for authentication.

Following tables describe the parameters in detail.

Parameter	Description
Enable	By default, the check box is not selected. When activated, the settings can be edited.
VPN Connection	
Exchange Mode	This defines the IKE version to set up a security association (SA) in the IPsec. In case IKEv1 is used, you can choose the mode for phase 1 (main or aggressive). There are four possible values: • IKEv2 Preferred. This is the default value. The system always first tries to assign IKEv2 and then IKEv1. • IKEv1 - Aggressive: In aggressive mode, the identity of the hosts and the hash of the shared key are not protected in phase 1. • IKEv1 - Main: In main mode, the identity of the hosts and the hash of the shared key are protected using encryption in phase 1. • IKEv2
Modem WAN Address	This is the public IP address that has been assigned to the network interface of the modem. This field is read-only and cannot be updated.
Remote Host	This is the IPv4 address of the host with which you want to set up the IPsec communication.
Local IP Address	This is the IPv4 network address of the local network behind the modem. The same network should be configured at the peer side for correct routing.

Parameter	Description
Local Subnet Prefix	This is the size of the local network. The number is the count of leading 1 bits in the subnet mask (CIDR notation).
DNS Server	You can configure the remote DNS sever of the HeadQuarter. The IP address of the DNS server will be given via DHCP toward the local network. A DNS server, which is present at the terminal side will not be used. DNS requests will always go through the IPSec tunnel.
NAT Traversal	When NAT Traversal or NAT-T is enabled, IKE and ESP data is encapsulated in UDP port 4500 allowing these protocols to pass through a device or firewall performing NAT. By default, the check box is not selected.
Dead Peer Detection Interval	When two peers communicate using IKE and IPsec, it is possible that the connectivity between the two peers drops unexpectedly. But the SAs can still remain until their lifetimes expire, resulting in the packets getting tunneled into a "black hole". Dead Peer Detection or DPD is an integral part of IKEv2, which refers to this feature as a "liveness check" or "liveness test". By default, the check box is not selected.
Dead Peer Detection Interval (s)	Number of seconds for dead peer detection interval. Only available if the check box Dead Peer Detection Interval is activated.
Authentication Method	There are two possible values: • PSK or Pre-shard Key. This key should be identical for the two host to be able to negotiate. No certificates are used. • Certificate (X.509). Use the buttons Upload, Download and Delete to manage these certificates.
PSK Secret	This is the pre-shared key and is only available in case of PSK is used as Authentication Method.

Parameter	Description
IKE Crypto Profile	
Local ID	Specify the local IKE identity to send in the exchange with the destination host to establish communication. If you do not configure a local-identity, the device uses the IPv4 address corresponding to the local endpoint by default. This parameter is optional, except when using NAT-T.
Remote ID	Specify the remote IKE identity to exchange with the destination host to establish communication. If you do not configure a remote-identity, the device uses the IPv4 address corresponding to the remote endpoint by default. This parameter is optional, except when using NAT-T.
Rekey Time	The keys negotiated during IKE phase 1 should only be used for a limited amount of time and to protect a limited amount of data. This means that each SA should expire after a specific lifetime. To avoid interruptions a replacement SA may be negotiated before that happens, which is called "rekeying". The Rekey Time is the number of seconds before rekeying.
Proposal An IKE proposal is a component of an IKE peer, and it defines IKE negotiation parameters, including the encryption algorithm, authentication method, authentication algorithm, Diffie-Hellman (DH) group, and security association (SA) lifetime. The two hosts must have at least one matching IKE proposal for IKE negotiation. Two matching IKE proposals define the same encryption algorithm, authentication mode, authentication algorithm, and DH group. If the IKE SA lifetimes of two hosts are different, the two hosts use the smaller IKE SA lifetime for IKE negotiation.	
Integrity	Integrity guarantees that the packets are original. You can authenticate the packet by the checksum calculated through a Hash Message Authentication Code (HMAC) using a secret key and either MD5 or SHA hash functions. • Message Digest 5 (MD5) is an algorithm that produces a 128-bit hash from a message of arbitrary length and a 16-byte key. The resulting hash is used, like a fingerprint of the input, to verify content and source authenticity and integrity. • Secure Hash Algorithm (SHA) is an algorithm that produces a 160-bit hash from a message of arbitrary length and a 20-byte key. It is generally regarded as more secure than MD5 because of the larger hashes it produces. Because the computational processing is done in the ASIC, the performance cost is negligible. The following hash functions are supported: • md5 • sha1 • sha256 • sha512
Encryption	For encryption, you can choose one of the following encryption algorithms: • Triple DES (3DES) is a more powerful version of DES in which the original DES algorithm is applied in three rounds, using a 168-bit key. DES provides significant performance savings but is considered unacceptable for many classified or sensitive material transfers.

Parameter	Description
	• Advanced Encryption Standard (AES) is an encryption standard which offers greater interoperability with other devices. The following encryption techniques are supported: • 3des • aes128 • aes192 • aes256
DH Group	IKE negotiations include a Diffie-Hellman exchange, which establishes a shared secret to which both parties contributed. This value is used to generate keying material to protect both the IKE SA and the IPsec SA. The following DH groups are supported: • modp768 (DH-1) • modp1024 (DH-2) • modp1536 (DH-5) • modp2048 (DH-14) • modp3072 (DH-15) • modp4096 (DH-16) • modp6144 (DH-17) • modp8192 (DH-18) • ecp256 (DH-19) • ecp384 (DH-20) • ecp521 (DH-21) • modp2048s256 (DH-24)

Parameter	Description
IKE Crypto Profile	
Alternative Proposal Beside the default proposal, you can create an alternative one. During IKE phase 1, the initiator sends its own IKE proposal to the peer end for matching. The responder starts with the highest-priority IKE proposal and matches the peer in the order of priority until it finds a matching IKE proposal to use. The matching IKE proposal will be used to establish an IKE tunnel.	
Enable	Select the check box to configure the alternative proposal.
Integrity	For more information, refer to the Proposal section.
Encryption	For more information, refer to the Proposal section.
DH Group	For more information, refer to the Proposal section.

Parameter	Description
IPSec Crypto Profile	
Rekey Time	The keys negotiated during IKE phase 2 should only be used for a limited amount of time and to protect a limited amount of data. This means that each SA should expire after a specific lifetime. To avoid interruptions a replacement SA may be negotiated before that happens, which is called "rekeying". The Rekey Time is the number of seconds before rekeying.
Replay Detection	Replay detection is a feature of the IPSec protocol for the detection of replay attacks. In a replay attack, an unauthorized host logs data and sends this, either repeatedly or with a delay, to a remote host to simulate a different identity.
Protocol	IPsec uses two protocols to secure communications at the IP layer: • Authentication Header (AH) - A security protocol for authenticating the source of an IP packet and verifying the integrity of its content. • Encapsulating Security Payload (ESP) - A security protocol for encrypting the entire IP packet and authenticating its content. ESP is the default value.
Proposal An IPSec proposal, as part of an IPsec profile, defines security parameters for IPsec SA negotiation, including the security protocol, encryption and authentication algorithms, and encapsulation mode. Both ends of an IPsec tunnel must be configured with the same parameters.	
Integrity	The AH and ESP protocol provide a means to verify the authenticity and integrity of the content and origin of a packet. You can authenticate the packet by the checksum calculated through a Hash Message Authentication Code (HMAC) using a secret key and either MD5 or SHA hash functions. • Message Digest 5 (MD5) is an algorithm that produces a 128-bit hash from a message of arbitrary length and a 16-byte key. The resulting hash is used, like a fingerprint of the input, to verify content and source authenticity and integrity. • Secure Hash Algorithm (SHA) is an algorithm that produces a 160-bit hash from a message of arbitrary length and a 20-byte key. It is generally regarded as more secure than MD5 because of the larger hashes it produces. Because the computational processing is done in the ASIC, the performance cost is negligible. The has functions are supported: • md5 • sha1 • sha256 • sha512
Encryption	The Encapsulating Security Payload (ESP) protocol provides a means to ensure privacy (encryption). For encryption, you can choose one of the following encryption algorithms: • Triple DES (3DES) is a more powerful version of DES in which the original DES algorithm is applied in three rounds, using a 168-bit key. DES provides significant performance savings but is considered unacceptable for many classified or sensitive material transfers.

Parameter	Description
	• Advanced Encryption Standard (AES) is an encryption standard which offers greater interoperability with other devices. The following encryption techniques are supported: • 3des • aes128 • aes192 • aes256
Perfect Forward Secrecy	If the check box is enabled, then the DH Groups are shown. Perfect forward secrecy or PFS is a feature of specific key agreement protocols that gives assurances that session keys will not be compromised even if the private key of the server is compromised.
Alternative Proposal Beside the default proposal, you can create an alternative one. During IKE pahse 2, the initiator sends its own IPsec proposal to the peer end for matching. The responder starts with the highest-priority IPsec proposal and matches the peer in the order of priority until it finds a matching IPsec proposal to use. The matching IPsec proposal will be used to establish an IKE tunnel.	
Enable	Select the check box to configure the alternative proposal.
Integrity	For more information, refer to the Proposal section.
Encryption	For more information, refer to the Proposal section.
Perfect Forward Secrecy	For more information, refer to the Proposal section.

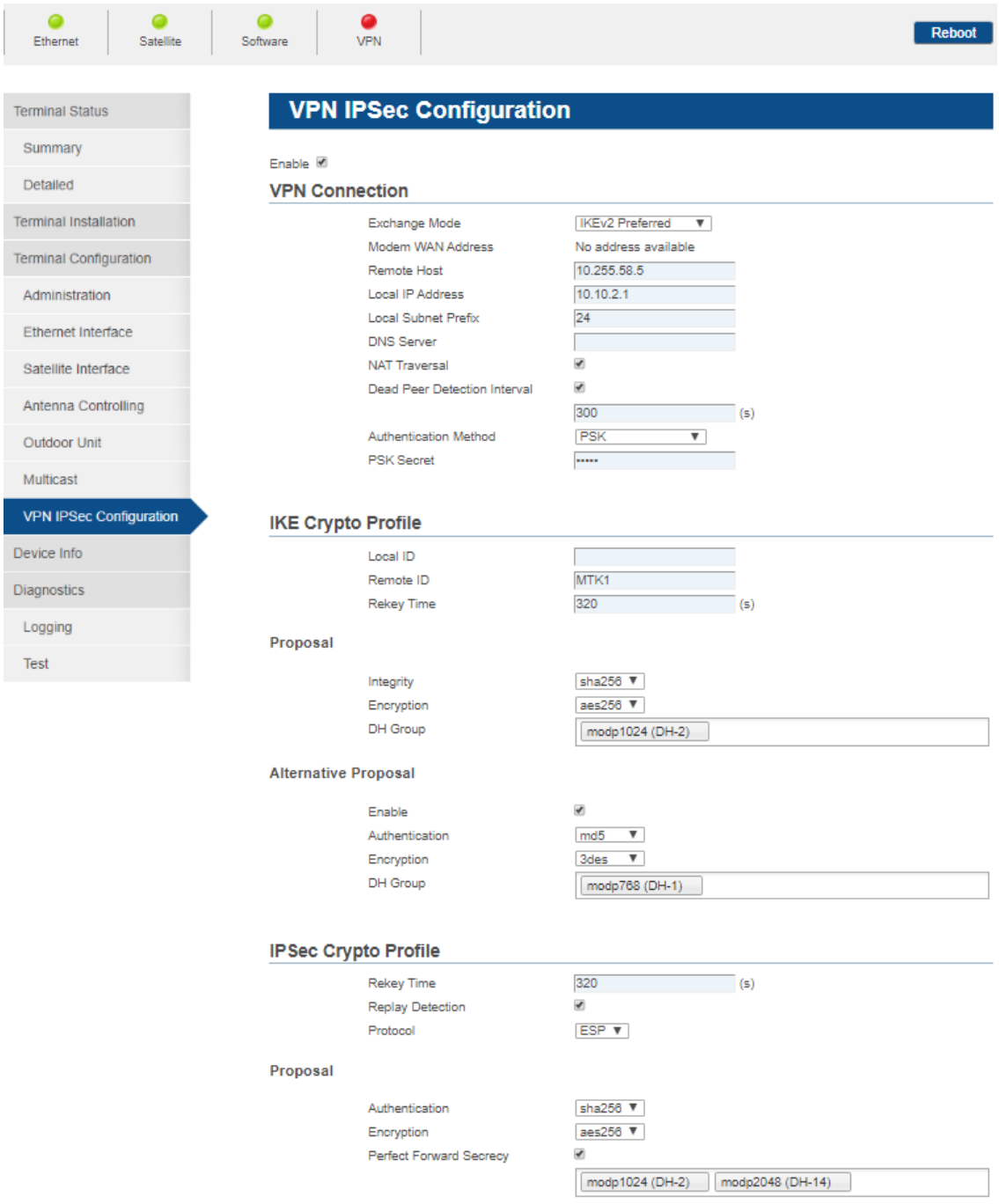
Parameter	Description
Certificate All files should be in PEM or DER format.	
Certification Authority Certificate	The Certification Authority or CA certificate is used to authenticate the CA signature on the host certificate.
Modem Public Key Certificate	A public key certificate is used to prove the ownership of a public key. The certificate includes information about the key, information about the identity of its owner (called the subject), and the digital signature of the CA (called the issuer). If the signature is valid, and the software examining the certificate trusts the issuer, then it can use that key to communicate securely with the certificate's subject.
Modem Private Key	The public key always comes with a private key. Data encrypted with the public key can only be decrypted with the private key. The private key remains locked and secure in the host, while the public key is pinned to the certificate. During secure communication, a host sends its certificate which contains the public key. The receiving host can then use this public key (after validation) to encrypt data and send it to first host, which is now the only one able to decrypt such data thanks to its private key.

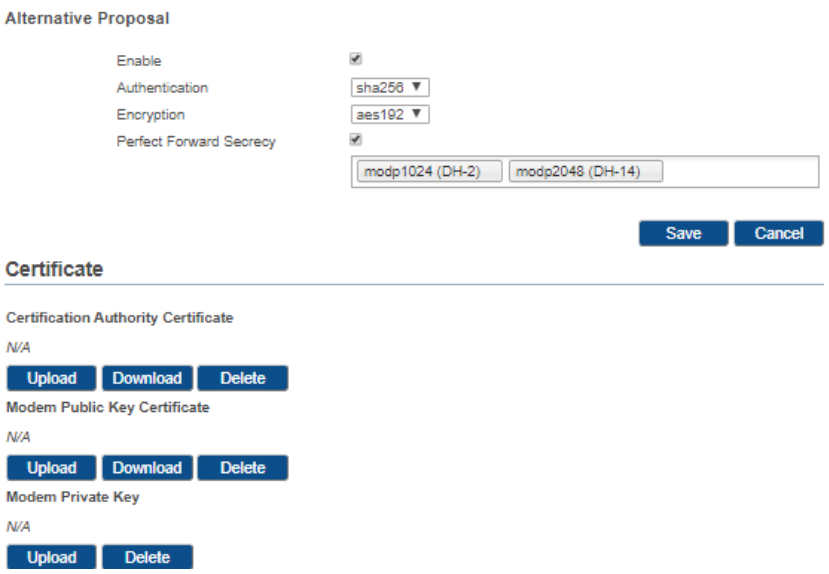
4.8.8.3 Edit VPN IPSec Configuration

VPN IPSec is an optional feature on your modem. If your modem does not support the feature, the **VPN IPSec Configuration** menu item is not visible.

To edit the parameters of VPN IPsec, execute the following steps:

1. Click Edit. If VPN IPsec is not yet enabled, select the check box **Enable**.





2. Edit the parameters. Refer to VPN IPSec Parameters on page 68.
3. Click Save to save your settings or Cancel to discard your settings.

To manage the different certificates:

1. Click Upload to upload a file.
2. Click Download to download a file. It is not possible to download a private key certificate.
3. Click Delete to delete a file.
4. Click the Save button to store the new settings.

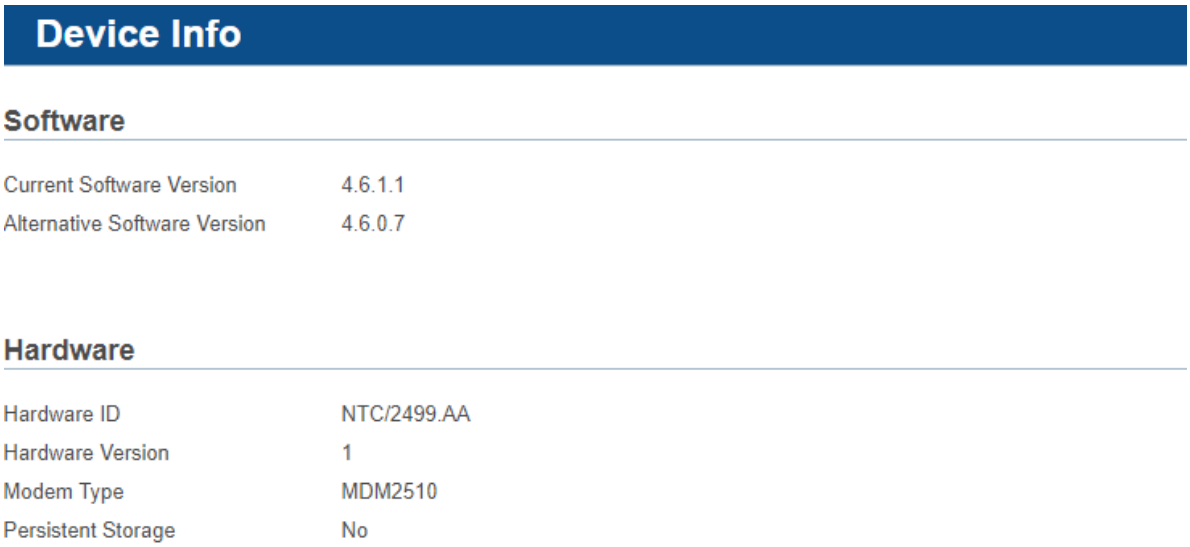
   The color of the status VPN LED changes into green.

   OR

   Click Cancel to discard the settings.

4.9 Device Info

This page provides information about the modem software and hardware.



4.9.1 Software

The modem software is automatically upgraded over the satellite without any user interaction. In general, the only requirement for a successful upgrade is for the modem to have satellite connectivity during the time of upgrade.

When the software upgrade fails but the software has been downloaded, it is saved as the alternative software version. This situation can for example occur when your modem looses power during the upgrade process. In that case, the passive memory bank contains a newer software version that did not yet pass the complete upgrade process and the Try Alternative Version button is available. Use this button to manually trigger the modem to upgrade to the new software version

When a newer version is present and the upgrade failed, the software LED is red.

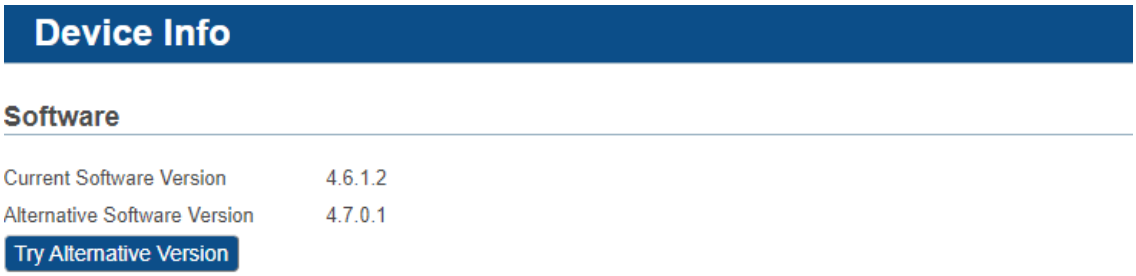
Refer to section Software LED on page 8 for more information on the meaning of the software status LEDs.

The parameters in the Software section are:

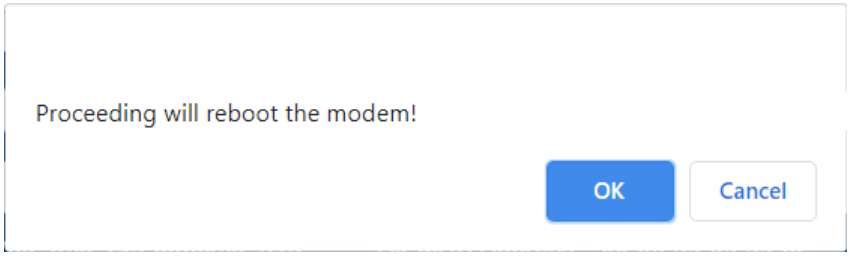
Parameter	Description
Software	
Current Software Version	The currently installed software version is displayed.
Alternative Software Version	Only displayed when an alternative software version is present.

To upgrade the software manually, execute the following steps:

1. Click Try Alternative Version to activate the new version of the software.



A confirmation window appears:



2. Click OK to continue or Cancel to abort.

A total upgrade, including satellite link initialization might take up to ten minutes.

If the web interface does not refresh automatically, navigate back to the Status page.

The **Try Alternative Version** button is only available when the alternative version is higher than the current version. This means that you can only manually upgrade the software. Only the expert user on page 88 can downgrade the software.

4.9.2 Hardware

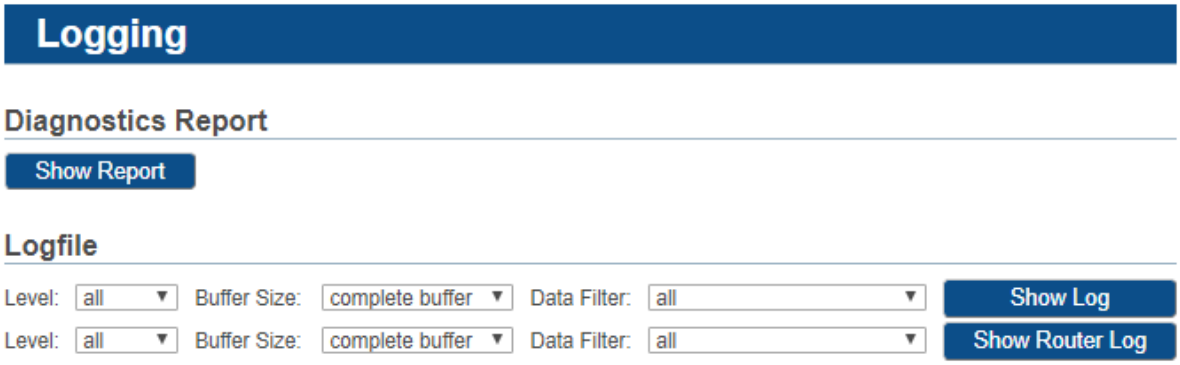
The parameters in the Hardware section are read-only.

Parameter	Description
Hardware	
Hardware ID	Hardware identifier of the modem
Hardware Version	Hardware version number of the modem
Modem Type	The modem hardware type of your modem: MDM2510
Persistent Storage	Indicates if the modem has persistent storage available or not.

4.10 Diagnostics

4.10.1 Logging

4.10.1.1 Diagnostics Report



Click Show Report to generate a diagnostic report. The report and the log files are downloaded in a zip file.

Log files contain a detailed list of configuration and events associated with your Dialog terminal, and can be used to keep track and debug possible errors. They are presented in the .log extension. As they are recorded in plain text, you can use any text editor to open and read them.

The diagnostic report is contained in the device_info.log file. The following list describes extensively its content.

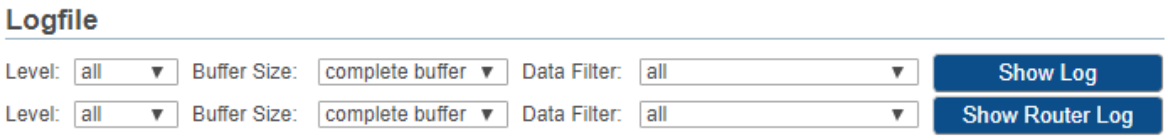
The diagnostic report has two major sections:

- The **Short Introduction Diagnostic Report**, which includes
  - **Terminal Identification**, which contains basic information about the modem, for example, the MAC address, the serial number and the uptime.
  - **Terminal Status**, which briefs the status of the interfaces of the modem (Ethernet, WI-Fi and Satellite interfaces), and the software.
  - **Terminal Configuration**, which includes
    1. Ethernet configuration parameters (MAC and IP addresses).
    2. Satellite interface properties (polarization skew, orbital position and satellite latitude variance).
    3. Initial Receive Transponders information, such as the mode, frequency, polarization, and symbol rate.
    4. Mobility data. Including GXT files data, beam name, cost and exclusion zones.
    5. Multicast mode (enable/disabled).
    6. ODU Information.
    7. General Configuration Information.
  - **Terminal Capabilities**, which includes polarization and power configuration.
- The **Extended Terminal Diagnostic Report**, which contains more detailed information about the modem, and point towards the log files that keep track of the events that occurred on the terminal.

1. **Terminal Firmware + FPGA version** which contains information about the terminal running firmware and FPGA.
2. **Terminal general status report**.
   - Modem State. Contains the modem general status. For example, return and forward state, error state, BER, C/N or signal strength,
   - Physical Layer Forward State. Contains information about the forward link, for example, ID of the demodulator used EsNo, used forward technology, frequency, power level or symbol rate.
   - Physical Layer Return State. Contains information about the return link, for example, absolute power, frequency, MODCODs, power spectral density, used return technology, roll-off factor, spreading factor or symbol rate.
   - MC State. Contains information about the Modem Controller.
   - CP State. Contains information about the Control Plane.
3. **Internal modem driver states**. Includes the modem running state and internal settings.
4. **Demod statistics**. Contains the demodulator historical information. It is possible to see here the accumulated number of dropped BBF for each MODCOD in the return link of the modem.
5. **ACM Statistics**. Contains the current ACM settings for each MODCOD and its statistics.
6. **Layer 2 counters of modem driver**. Includes statistics on the received and transmitted IP packets and L2 frames, tellishape, tellinet or netring bridge.
7. **Terminal initial configuration**. Includes several modem initial configuration parameters.
8. **Terminal operational configuration.** Includes several general Tellishape and network configuration parameters.
9. **Running processes**. Lists the processes that are currently running in the modem with their memory and CPU usage.
10. **Ethernet link status**. Settings for the Ethernet interfaces.
11. **Memory usage info**. Current memory status.
12. **Network configuration**, which includes:
    - IP interface Address list
    - Multicast Address list
    - Ethernet ARP Cache list
    - Policy-based Routing rules
    - Link interfaces configuration
    - IP routing configuration
    - IP-v4 routing tables
    - IP-v6 routing tables
    - ARP tables
13. **DHCP leases**, which includes the IP assigned by the DHCP server.
14. **HW Info**., which includes temperature information.
15. **Demod monitoring log files**. To look at the demod monitoring log files, open demodmonitor.log and demodmonitor.log.xx in archive. The most important demodulator state changes, occurred errors and events are recorded into these log files.

16. **Internal Error Log File**. To look at the demod monitoring log files, open InternalError.log in archive. The most important internal state changes, occurred errors and events are recorded into these log files.
17. **Terminal Log File** To look at the modem board log files, open main_board.log and main_board.log.xxx in archive. The most important modem state changes, occurred errors and events are recorded into these log files.
    To look at the router board log files, open modem_board.log and router_board.log.xxx archive. These log files provide information about BGP routing protocol, firewall and NAT. These logs can also be seen in the Logging interface. For more information, refer to Log Files on page 81.
18. **Segment4 Report Log File.** Includes the Segment 4 configuration.
    Segment 4 realizes the network edge processing and controls the endpoints of the satellite channels.
19. **Tellitec-client configuration**, which includes:
    - Tellinet client configuration
    - Tellishape client configuration
20. **Monitoring**. Addresses of local files within the terminal with application checks.

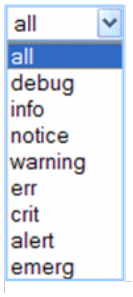
4.10.1.2 Log Files



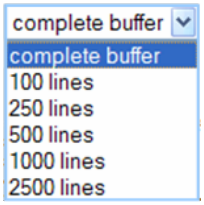
- Click Show Log to view the terminal log file. The most important modem state changes, occurred errors, events, etc. are logged in this log file.
- Click Show Router Log to view the segment 4 report log file. This log file provides information about BGP routing protocol, firewall and NAT.

The user has the possibility to filter in terms of severity level, buffer size and data type.

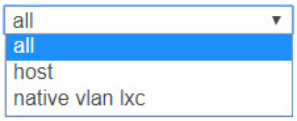
- Severity levels



- Buffer size



- Data types



Every five minutes specific performance counters will be added to the logfile.The logged values correspond with the values displayed on the status page - interface statistics part of the screen.

```
Jan  1 00:05:01 (none) user.info perf: eth0: 21516 185 0 0 44428 117 0 0 21516 185 0 0 44428 117 0 0
Jan  1 00:05:01 (none) user.info perf: modem: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Jan  1 00:10:01 (none) user.info perf: eth0: 35756 332 0 0 63006 185 0 0 14240 147 0 0 18578 68 0 0
Jan  1 00:10:01 (none) user.info perf: modem: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Jan  1 00:15:01 (none) user.info perf: eth0: 46253 435 0 0 78032 240 0 0 10497 103 0 0 15026 55 0 0
Jan  1 00:15:01 (none) user.info perf: modem: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Jan  1 00:20:01 (none) user.info perf: eth0: 63598 666 0 0 391703 500 0 0 17345 231 0 0 313671 260 0 0
Jan  1 00:20:01 (none) user.info perf: modem: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Jan  1 00:25:01 (none) user.info perf: eth0: 77945 842 0 0 563701 674 0 0 14347 176 0 0 171998 174 0 0
Jan  1 00:25:02 (none) user.info perf: modem: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
```

The meaning of the respective counter is described in the table below:

Counter Number	Counter Description
Counter 1	Total - RX bytes
Counter 2	Total - Rx packets
Counter 3	Total - RX errors
Counter 4	Total - RX packets dropped
Counter 5	Total - TX bytes
Counter 6	Total - TX packets
Counter 7	Total - TX errors
Counter 8	total - TX packets dropped
Counter 9	Last 5 minutes - RX bytes
Counter 10	Last 5 minutes - RX packets
Counter 11	Last 5 minutes - RX errors
Counter 12	Last 5 minutes - RX packets dropped
Counter 13	Last 5 minutes - TX bytes
Counter 14	Last 5 minutes - TX packets
Counter 15	Last 5 minutes - TX errors
Counter 16	Last 5 minutes - TX packets dropped

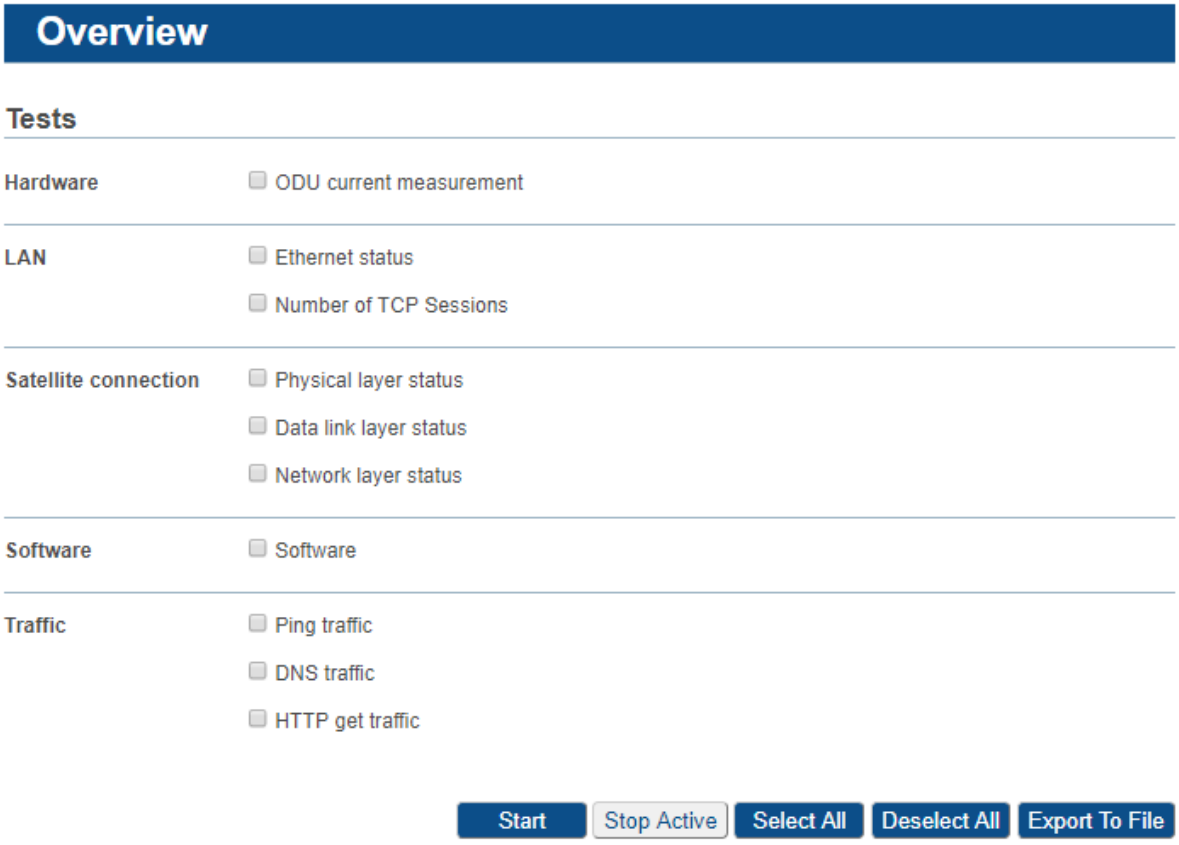
If the modem has persistent storage available, the log files are compressed and rotated on the persistent storage. If the modem does not have persistent storage, the log files are compressed and rotated on an in-memory file system.

The availability of persistent storage is automatically detected.

Log files will contain at least 48 hours of data.

4.10.2 Test

To view the functioning status of the satellite terminal, or to identify problems that may occur, several tests can be run on the terminal:



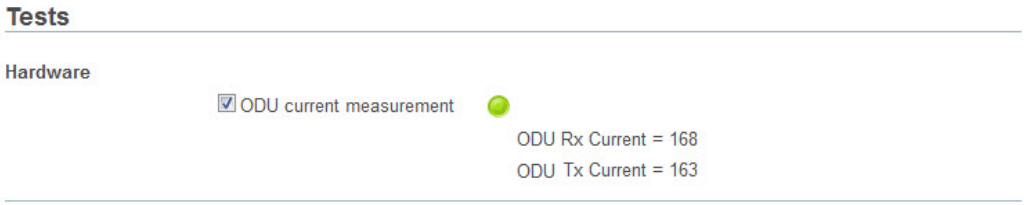
4.10.2.1 Test Descriptions

4.10.2.1.1 Hardware Test

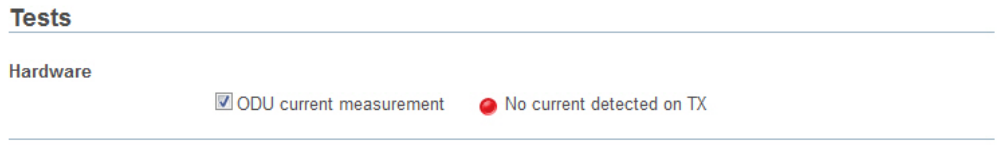
The Hardware test measures the current in the receive and transmit path between modem and ODU.

Possible test results:

- A successful hardware test means that TX and RX current is within the expected range. The figure below shows an example of a successful hardware test.

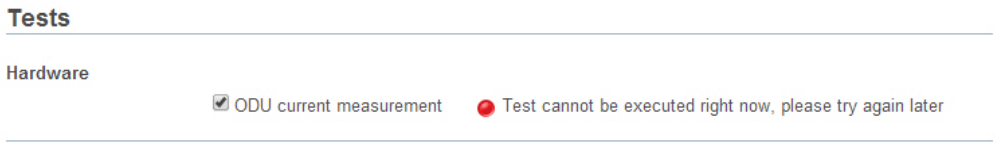


- A failed hardware test means that at least one of the measured currents falls outside the expected range. This indicates a problem in the receive and/or transmit path.



If the hardware test has failed, please always verify the installation of the coaxial cable. A defect cable, swapped TX and RX cables, or loose contacts at one or more connectors can cause the hardware test to fail even if the BUC and LNB are working correctly.
If the problem persists, please contact your Service Provider.

- In some cases, the hardware test cannot be executed because of the actual modem state e.g. during pointing. In this case, one is requested to try again later.



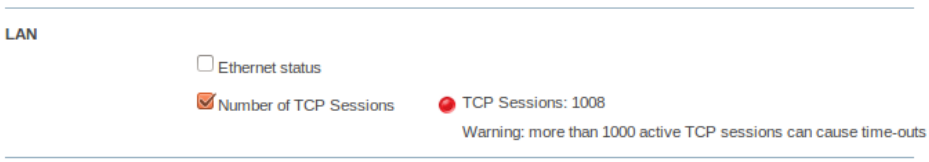
4.10.2.1.2 LAN Test

The LAN test has two tests.

1. The "Ethernet status", which performs the following:
   - Checking the Ethernet physical layer.
   - Obtaining the IP address off the computer connected to the modem.
   - Checking the IP address of the computer, provided via DHCP by the modem.
2. The "Number of TCP sessions", which shows how many TCP sessions are currently active.

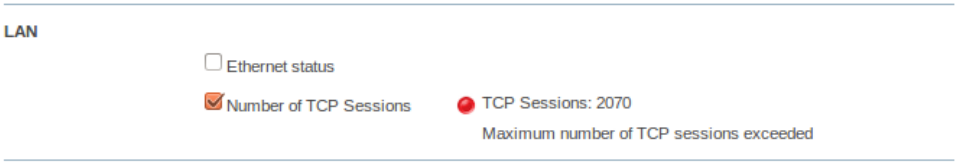
The maximum number of TCP sessions is set by the Network Operator.

If more than half the maximum allowed number of TCP sessions is active, a warning message is displayed. In the example shown below, the maximum number was set to 2000.



If the number of active TCP sessions exceeds the maximum number set by the Network Operator, an error message is displayed, TCP sessions will be delayed until the number drops

again below the maximum. In the example shown below, the maximum number was set to 2000.



4.10.2.1.3 Satellite Connection Test

The Satellite connection test is composed of three tests:

- The Physical layer test, checks if the physical layer of the modem - satellite connection is able to receive data.
- The Data link layer test, checks if the system is able to send data to the satellite.
- The Network layer test, checks the IP connection.

4.10.2.1.4 Software Test

The Software test verifies the validity of the software.

4.10.2.1.5 Traffic Test

The Traffic test is composed of three tests:

- A ping traffic test, tests if ping packets can be transported over the network from the modem, over the satellite to the hub site.
- The DNS traffic test resolves a URL via a name server at the hub site.
- The HTTP GET traffic test verifies the TCP acceleration and pre-fetching.

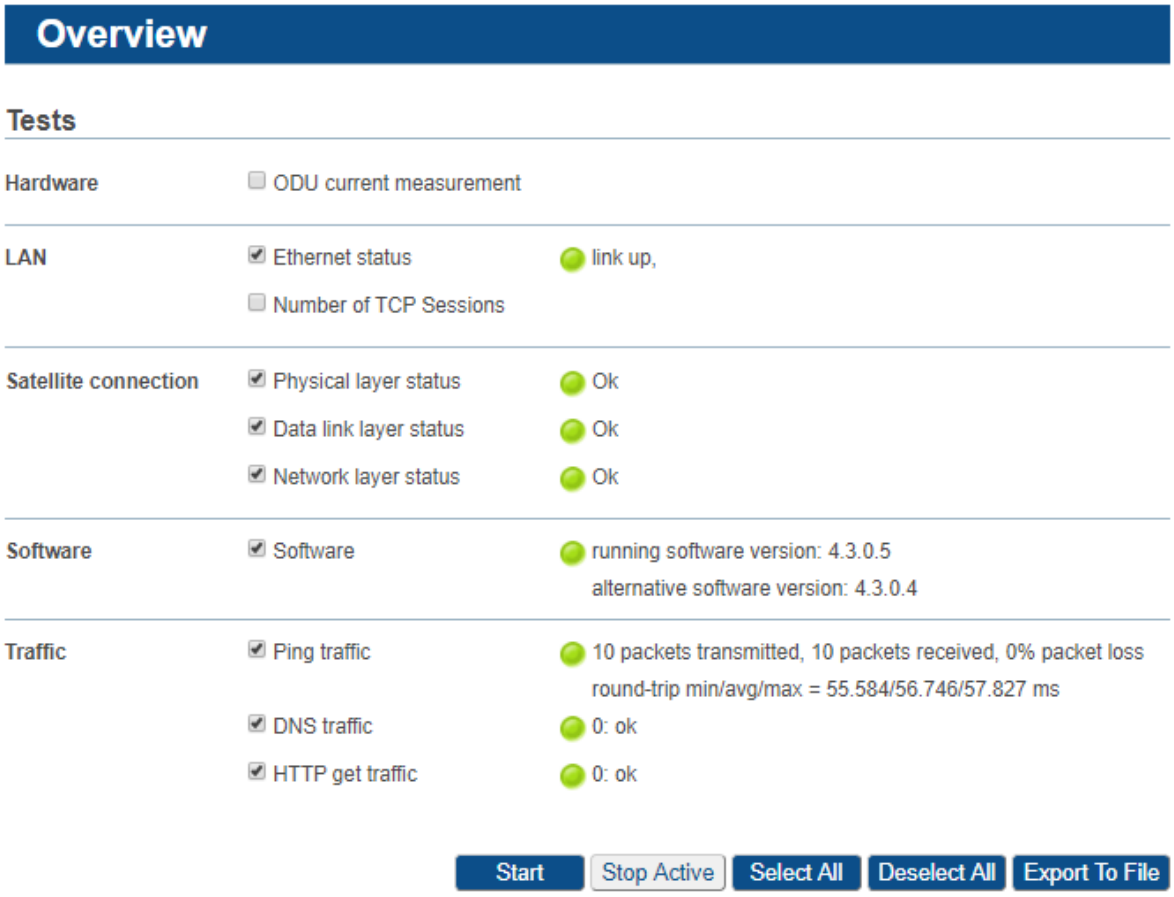
The HTTP GET traffic test uses a TCP connection and can hence not be executed when the maximum number of TCP sessions is exceeded. In this case the HTTP GET traffic test will time out or should be stopped manually.

4.10.2.2 On-Screen Test Results

Mark (☑) the tests that you want to run and click Start to start the execution of the tests.

During and after test execution, the state of the tests is shown on screen until finally are results are available.

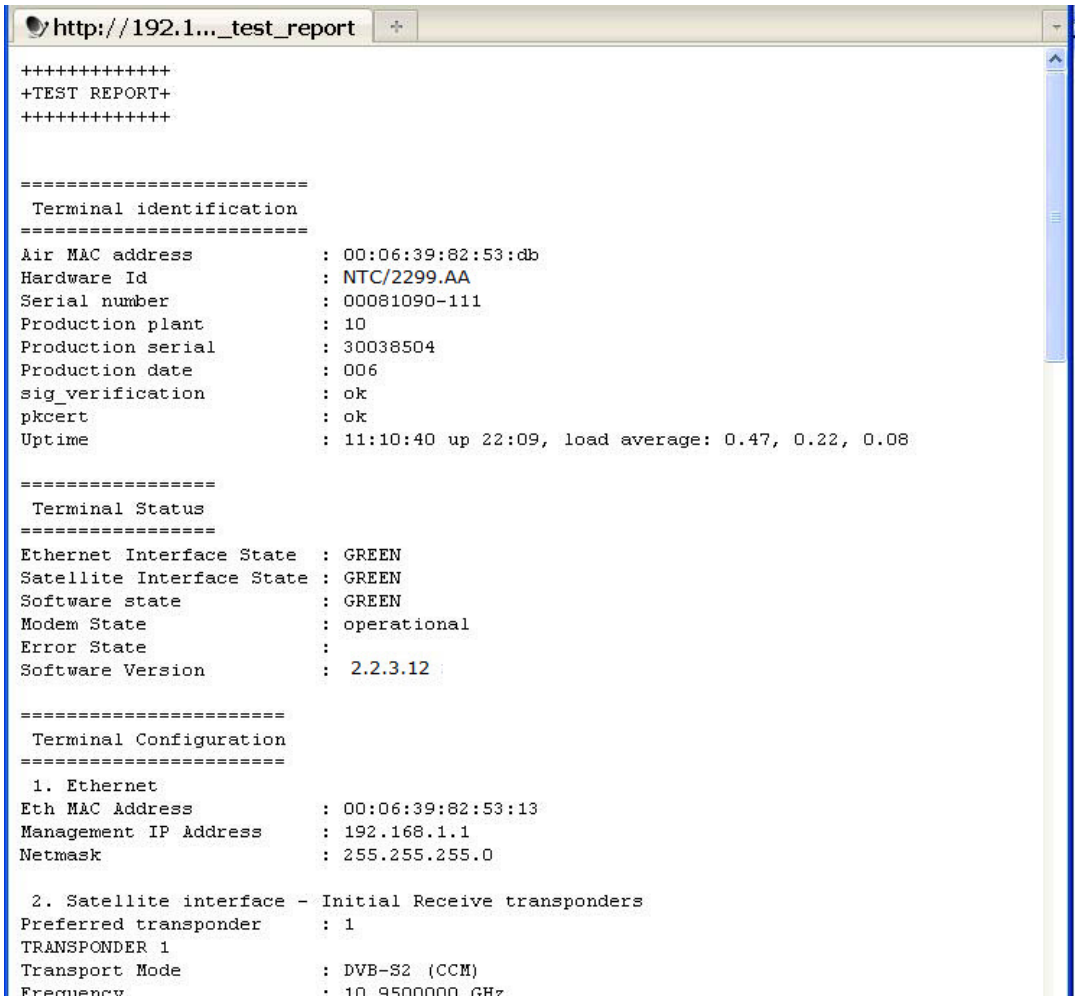
Test waiting for execution	
Test is being executed	
Test is finished and successful (passed)	
Test is finished and unsuccessful (failed)	



4.10.2.3 Export Test Results

Click Export To File to export the on-screen test results. A web page with the test results in text format will be provided.

This page can be saved as a text file.


http://192.1..._test_report
++++++++++++
+TEST REPORT+
++++++++++++
========================
Terminal identification
========================
Air MAC address : 00:06:39:82:53:db
Hardware Id : NTC/2299.AA
Serial number : 00081090-111
Production plant : 10
Production serial : 30038504
Production date : 006
sig_verification : ok
pkcert : ok
Uptime : 11:10:40 up 22:09, load average: 0.47, 0.22, 0.08
================
Terminal Status
================
Ethernet Interface State : GREEN
Satellite Interface State : GREEN
Software state : GREEN
Modem State : operational
Error State :
Software Version : 2.2.3.12
======================
Terminal Configuration
======================
1. Ethernet
Eth MAC Address : 00:06:39:82:53:13
Management IP Address : 192.168.1.1
Netmask : 255.255.255.0
2. Satellite interface - Initial Receive transponders
Preferred transponder : 1
TRANSPONDER 1
Transport Mode : DVB-S2 (CCM)

5 Expert Mode

The expert mode offers extra functionality to the modem graphical user interface.

5.1 Login as Expert

1. Connect your PC to the modem as described in section Connect Computer to Modem on page 6.
2. Type *?ilogin* behind the *http://192.168.1.1/cgi-bin/index* URL.

   The following login screen appears:

3. Enter the password in the text field.

   The Expert password can be obtained from your modem supplier.

4. Click Login. You are now logged in as the expert user.

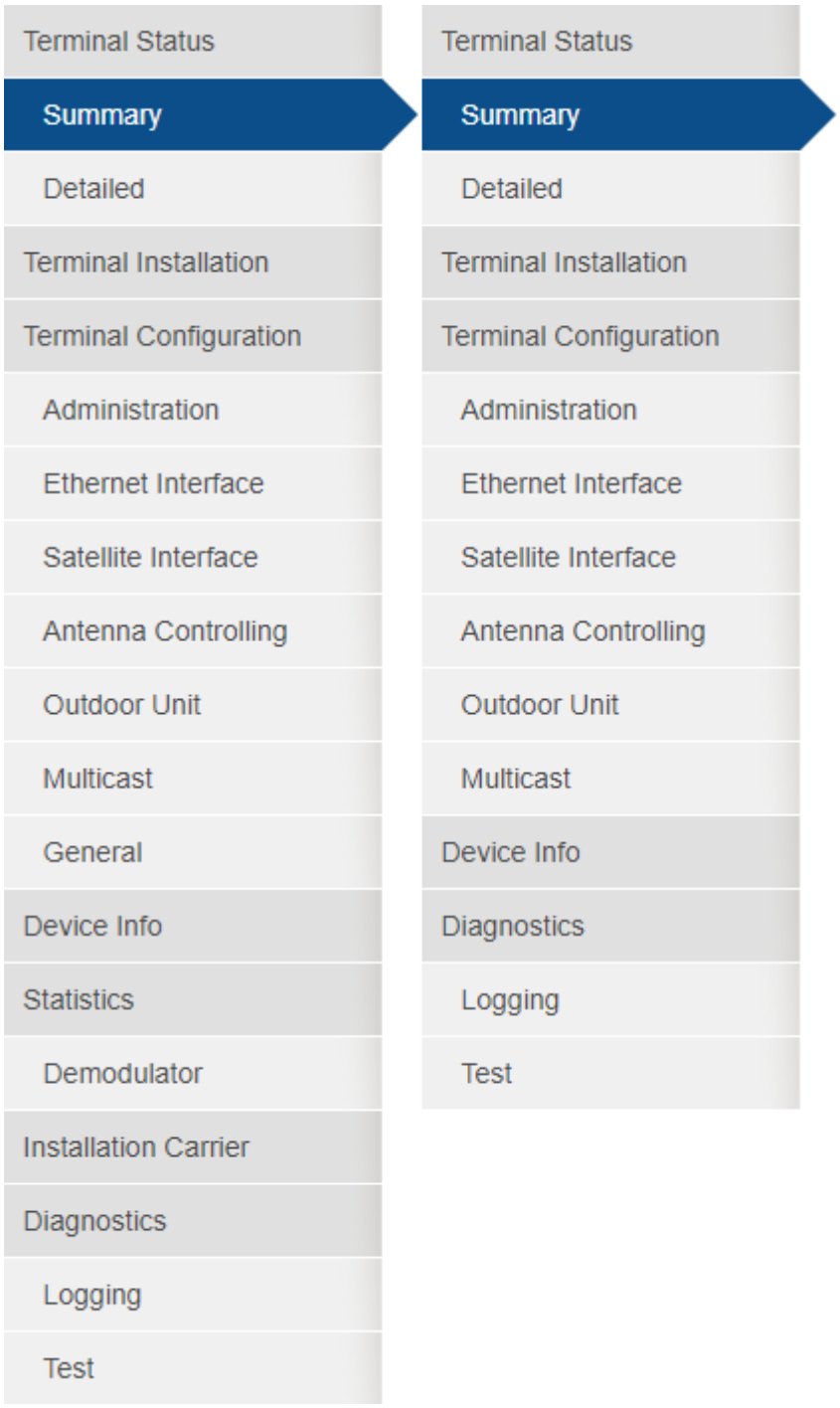
   

5. Click Logout to return to the normal user mode.

5.2 Additional Functionality in Expert Mode

The expert mode adds extra menu items to the menu structure:

- General
- Statistics/Demodulator
- Installation Carrier



The expert mode adds extra functionality to **Administration**, **Ethernet Interface** and **Device Info**, and can add extra functionality to the **Satellite Interface** and **Outdoor Unit** configuration as some of the features in these two menus can be disabled by the Network Operator in normal mode.

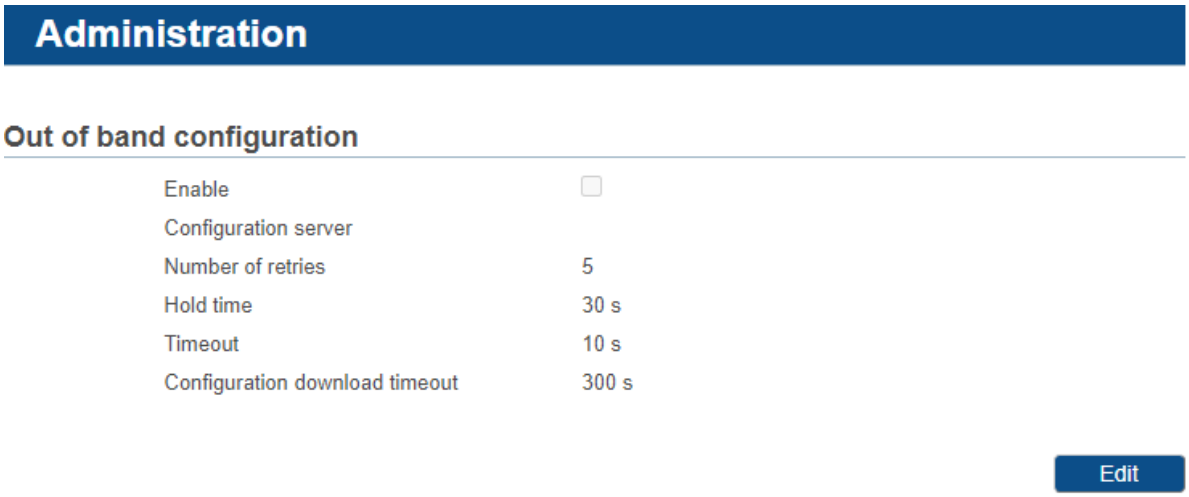
Enabling terminal mobility via the **General** menu item adds extra functionality to the **Satellite Interface** and **Terminal Installation** and displays the **GXT Files** menu item.

The VPN IPsec is an optional feature. When the feature is not supported, the ***VPN IPSec Configuration*** menu item is not available.

5.2.1 Administration

Only enable the modem out-of-band configuration if you have the external infrastructure with the configuration server installed.

A factory reset disables the out-of-band configuration feature and returns to the normal operation mode.



The out-of-band configuration feature allows you to configure the modem from an external server located outside the Dialog platform. Select the **Enable** check box to enable the feature and set the address of the external **Configuration server**. The address can be a hostname or an IP address. Additionally, you can change the default settings of the timers used in the out-of-band configuration process flow.

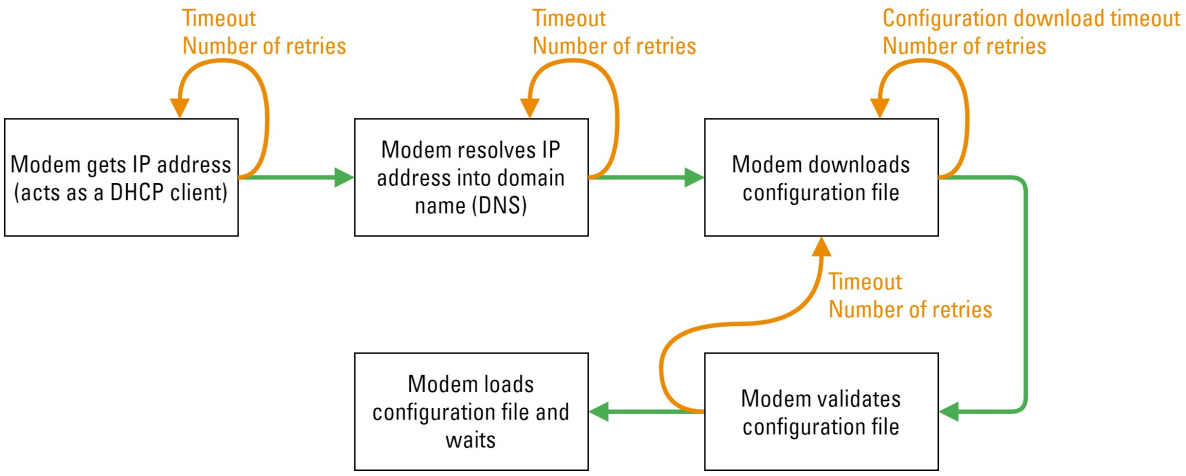
Alternatively, use the JSON API SetOutOfBandConfig command. For more information about the JSON API, refer to JSON API Description on page 122.

As soon as the feature is enabled, the modem will act as a DHCP client.

The modem out-of-band, also referred to as MOOB, configuration process flow can be split in two phases. In the first phase, the modem contacts the server and requests an out-of-band configuration. If a configuration is available, the modem downloads and verifies the configuration. If the configuration is valid, it stores the out-of-band configuration as a candidate configuration.

Make sure that the LAN interface of the modem is connected to the network where your configuration server resides.

The exact steps of the first phase are shown in the figure below.



1. The modem acquires an IP address from the DHCP server in the LAN network.
2. The modem resolves the hostname of the configuration server to an IP address (DNS resolve).
3. The modem downloads the configuration file using an HTTP request.
4. The modem validates the configuration file. The validation includes a validity check of the config.json file and of the parameter values in that file. For example, are frequencies within expected range.
   - If the validation fails, the modem returns to the previous step (3).
   - If the validation succeeds, the modem stores the out-of-band configuration as a candidate configuration and waits until it is rebooted.

In case of any error during the first phase of the MOOB configuration flow:

- And the modem has never successfully performed the out-of-band configuration process flow, the modem continuously retries the steps until it succeeds or until it is rebooted.
- And the modem has already performed a successful out-of-band configuration process flow in the past, the modem retries the steps until it succeeds or until the number of retries expires. The default number of retries is 5. When the retries have expired, the modem considers the out-of-band configuration retrieval as failed and continues with the normal boot sequence using the existing configuration. The modem will wait for the *Hold time* before starting the normal boot sequence in order for the modem operator to see the warning LED error pattern.

  There is one special case: when the modem successfully acquires the IP address but all other steps fail, the modem will remain in the error state until it is rebooted. This is to avoid any IP conflicts with the internal management IP address of the modem.

After each retry the modem waits for the *Timeout* time.

In case the first phase completes successfully, the **Configuration** table on the UI page will display the version, lifetime, source and options of the candidate configuration. The options column indicates if the confirmation cycle in the second phase is enabled or not. If enabled, it also displays the confirmation timeout value. See configuration table on page 94 for more information.

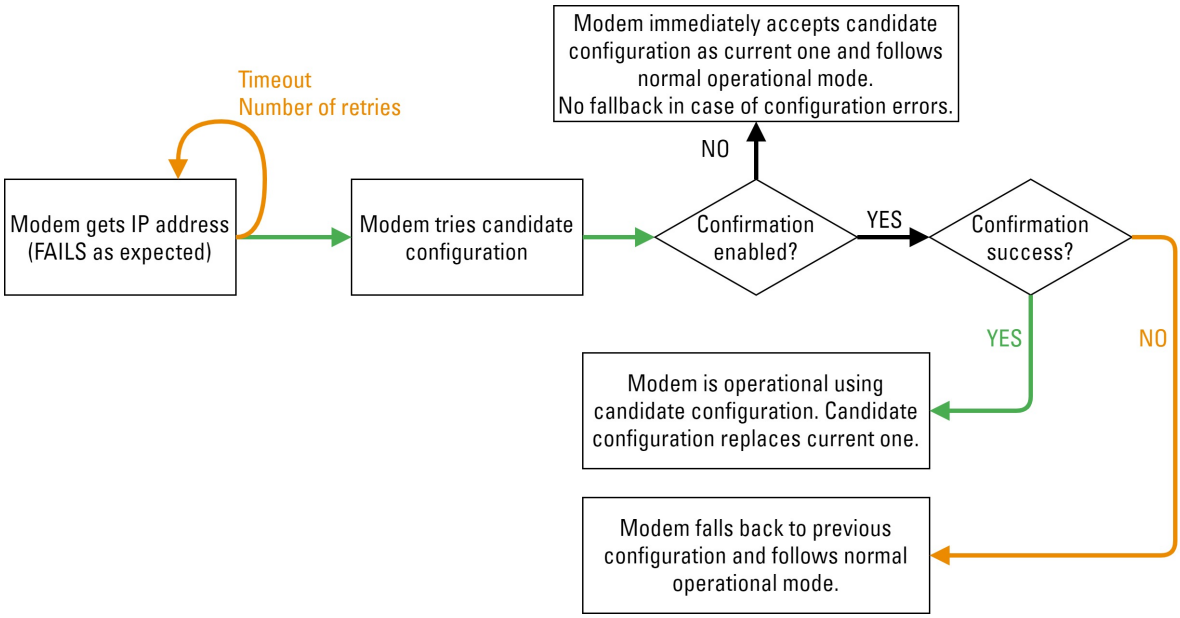
To initiate the second phase, manually execute the following steps:

1. Disconnect the modem from the external network where the configuration server resides.
2. Connect the RF cables from the outdoor unit.

3. Reboot the modem.

In the second phase, the modem tries or immediately applies the candidate configuration and continues with the normal operational flow.

The exact steps of the second phase are shown in the figure below.



1. The modem tries to acquire an IP address from the DHCP server in the external network. As expected, this step will fail after timeout and a number of retries.
2. The modem tries the candidate configuration.
   - By default, the candidate has to go through a confirmation cycle before being accepted. This confirmation cycle is considered successful when the modem has become operational using the candidate configuration settings. The candidate configuration becomes the current one and is deleted as a candidate.

     If the modem cannot become operational within a certain timeout time, it falls back to its current configuration and follows the normal operational flow. The candidate configuration is not deleted.
   - If the confirmation cycle is disabled, the candidate configuration is immediately accepted and the modem follows the normal operational flow. If your candidate configuration has incorrect settings, the modem will not become operational and will not fall back to the previous configuration.

   You can enable or disable the confirmation cycle and set the confirmation timeout value in the configuration file. See out-of-band configuration file on page 93 for more information.

The MOOB configuration flow can work together with the Remote Terminal Satellite Configuration feature. If this feature is enabled and there is a more recent version of the satellite configuration on the TCS at the hub-side, the modem will request the satellite configuration from the TCS and will consider this as the candidate satellite configuration.

The **warning LED** on the modem indicates the modem status during the MOOB configuration flow.

Event	Pattern Warning LED

MOOB in progress and going well	2 seconds ON - 2 seconds OFF
Error in acquiring IP	0.5 seconds ON - 5 seconds OFF
Error in resolving hostname	0.5 seconds ON - 0.5 seconds OFF - 0.5 seconds ON - 5 seconds OFF
Error in fetching MOOB configuration file	2x (0.5 seconds ON - 0.5 seconds OFF) - 0.5 seconds ON - 5 seconds OFF
Error in validating MOOB configuration file	3x (0.5 seconds ON - 0.5 seconds OFF) - 0.5 seconds ON - 5 seconds OFF
Error in processing candidate configuration	4x (0.5 seconds ON - 0.5 seconds OFF) - 0.5 seconds ON - 5 seconds OFF
MOOB success	0.5 seconds ON - 0.5 seconds OFF
Normal mode - operational	OFF
Normal mode - not operational	ON

The MOOB configuration flow can be followed in the diagnostic report.

The modem out-of-band configuration is a zip file containing:

- The modem configuration in JSON format (config.json);
- An optional directory that contains GXT files (gxt);
- GXT file(s) referenced by the config.json.

The name of the zip file is the air MAC address of the modem.

The config.json file contains the modem configuration in JSON format as described below:

```
{
      "FileFormatVersion": Number,
            //Optional. Used to prevalidate the configuration file.
      "SatelliteConfiguration": SatelliteConfiguration,
            //Optional. Description of spot beams from which the modem can
            acquire the network and to which they can switch while moving.
      "Miscellaneous": Miscellaneous,
            //Optional. Contains modem configurations that are not remotely
            manageable.
      "CandidateConfirmationTimeout": Number,
```

```
        //Optional. Represents the number of seconds that shall be
        waited for the candidate configuration before it rolls back to
        the previous configuration. If missing the default(2h) will be
        used to wait.

    "CandidateConfirmationTimeoutEnabled": Boolean,

        //Optional. Used to disable the candidate confirmation timeout.

    "CandidateConfirmationEnabled": Boolean,

        //Optional. Used to enable/disable the candidate try/rollback
        mechanism . If disabled the candidate will be accepted
        immediately after the pre-validation is passed. If missing the
        try/rollback mechanism is enabled by default.

}
```

Refer to Appendix C - Modem Configuration File on page 136 for the complete content of the modem configuration file.

It is also possible to manually load a configuration. Click the Load Candidate button and select a configuration zip file. The configuration is stored as a candidate.

If the confirmation cycle is enabled for this configuration, the Try Candidate, Force Candidate and Discard Candidate buttons are available. If the confirmation cycle is not enabled for this configuration, the Apply Candidate and Discard Candidate buttons are available.

- To validate the candidate configuration and start the confirmation cycle, click Try Candidate. During this process, the GUI is read-only mode. If the configuration file does not pass the validity check or the modem does not become operational within a certain timeout value, the modem falls back to its current configuration. The default timeout value is two hours but can be edited in the configuration file.
- To replace the current configuration with the candidate configuration without the confirmation cycle, click Force Candidate or Apply Candidate. If your candidate configuration has incorrect settings, the modem will not become operational and will not fall back to the previous configuration.
- To discard the candidate configuration, click Discard Candidate.

To download the current (active) modem configuration, click Download Current.

The **Configuration** table in the GUI shows the version, lifetime, source of the **current** configuration and of a **candidate** configuration if this exists. For the candidate configuration it also displays an extra Options column.

Type	Version	Time	Sources	Options (only for candidate)
• **Satellite**: Refers to the satellite configuration. See Satellite Interface on page 47.	**Satellite** Can be a number or N/A. N/A is used when the configuration is locally edited or in case of the	Lifetime of the configuration. Time is reset upon configuration change.	• **Local Edits**: Indicates that the current configuration is edited locally, either via the GUI or JSON API.	• **Acceptance**: Indicates if the candidate is accepted immediately (Immediate) or only

• **Miscellaneous**: Refers to the entire modem configuration, excluding the satellite configuration.	candidate configuration, when this configuration has been committed and cleared.		• **TCS**: This source is only applicable to the satellite configuration and indicates that the configuration has been downloaded from the hub-side. • **MOOB**: Indicates that the configuration is retrieved via out-of-band. • **Local Upload**: Indicates that the configuration has been loaded using the Load Candidate button.	after the confirmation cycle (If operational). • **Confirmation Timeout**: Indicates the timeout value for the confirmation cycle to be considered as failed. Only displays when the confirmation cycle is enabled. Mind that the timeout period can be disabled in the configuration file, in which case the candidate configuration is tried forever.

5.2.2 Ethernet Interface

In the Ethernet section of the Ethernet Interface Configuration page, the expert user can configure to forward the local logs to an external syslog server.

The TFTP server and TFTP file parameters are obsolete.

By default the logs are written to an in-memory buffer of 256 kB.

1. Click Edit to change the **Logging Mode** to **Remote - Static**.
2. Enter the **Syslog UDP Port** and the **Syslog IP Address** of the external server.
3. Click Save to save your settings or Cancel to discard your settings.

In the VLAN overview section, it is possible to set the IPv4 DHCP lease time for all provisioned VLANs (VRFs):

1. Click Edit to check the DHCPv4 Lease Time Enabled.
2. Enter the desired value in DHCPv4 Lease Time Seconds. Values must be between 120 and 86400 seconds. For indefinite lease time, enter 0.

In case DHCPv4 Lease Time is not configured, the default value is 120 seconds.

3. Click Save to save your settings or Cancel to discard your settings.

5.2.3 Satellite Interface

5.2.3.1 Edit Satellite Interface Configuration

In normal user mode, editing the satellite interface configuration can be disabled by your network operator. In expert user mode, editing is always possible.

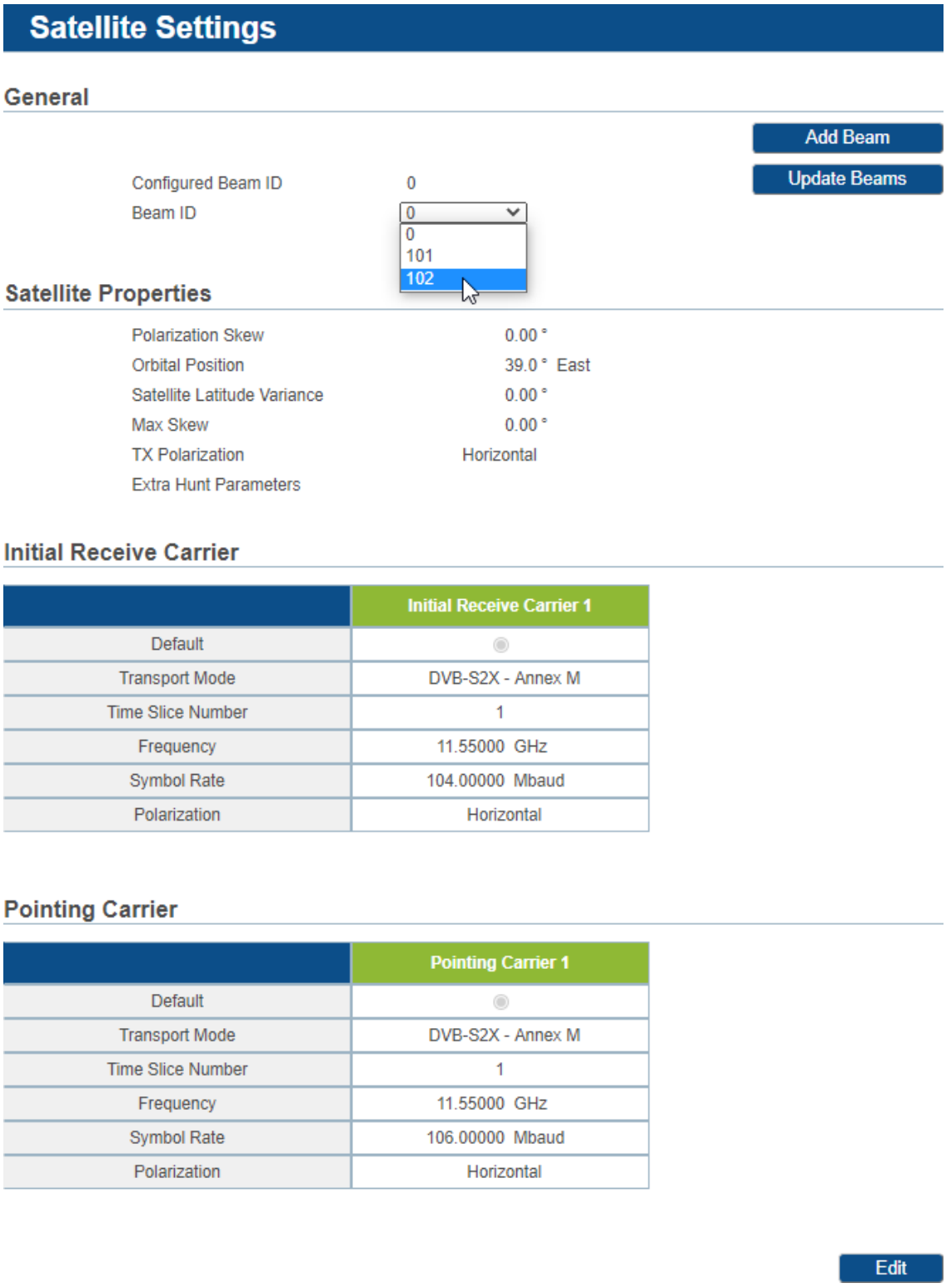
For more information about how to edit the satellite settings, refer to section Edit Satellite Settings on page 51.

5.2.3.2 Satellite Configuration - Select Beam

If multiple beam identifiers are pre-configured or signaled to the terminal, you can use this feature to check or edit another beam identifier than the one currently used.

The currently selected beam identifier, or the active beam, is indicated in the Terminal Status Summary page.

1. Select a beam identifier from the drop-down list. The settings of the selected beam are displayed. The active beam (Configured Beam ID) is not impacted.



2. To edit the settings of the selected beam, click Edit.
3. To delete the selected beam, click Remove.

You cannot delete the active beam from this menu. To know how to delete the active beam, refer to Satellite Configuration - Update Beams on page 99.

5.2.3.3 Satellite Configuration - Add Beam

The expert user can define other beam settings than the one signaled from the hub.

Typical use case for this feature is when for some reason the pre-configured beam settings are no longer valid, preventing the modem from gaining access to the network. This feature allows an installer to add another beam with the correct settings.

1. Click Add Beam.
2. Enter the settings as described in section Satellite Interface Parameters on page 49.
3. Click Save to save your settings or Cancel to discard your settings.

5.2.3.4 Satellite Configuration - Update Beams

The expert user can update all beams simultaneously.

1. Click Update Beams. A new window appears where you can upload a configuration file.

   If the new beam configuration file contains:

   – New beam identifiers, then these are **added** in the modem

   – Existing beam identifiers, then these are **updated** in the modem

   – Omitted beam identifiers, then these are **deleted** from the modem

   If the active beam is not in the new list of beams (meaning, it is deleted) or if the active beam is updated, then the modem moves back to the ODU selection installation state.

   If Automatic Initial Beam Selection (AIBS) is activated, deleting or updating the active beam results in the modem going back to the AIBS state where it will select a new initial beam. This is required because the modem at all times has to be able to check the Tx exclusion zones which are coupled to the active beam.

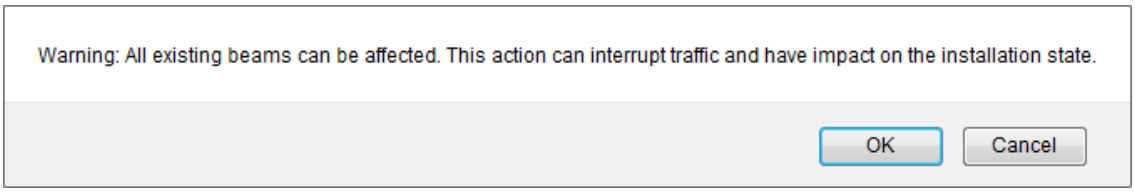
   The configuration file should contain a valid JSON object which is defined as described next.

```
{
      "Beams": Array[Object[EditableBeamData]]
}

OBJ EditableBeamData
{
    "BeamId": Number,
    "InitialCarrier1": Object[CarrierData],
    "InitialCarrier2": Object[CarrierData],
    "DefaultInitialCarrier": Number,                // 1 or 2
    "PointingCarrier1": Object[PointingCarrier],
    "PointingCarrier1": Object[PointingCarrier],
    "DefaultPointingCarrier": Number,               // 1 or 2
    "OrbitalDegrees": Number,                       // float, expressed in degrees
    "Hemisphere": String,                           // east or west
    "PolarizationSkew": Number,                     // float, expressed in degrees
    "SatLatitudeVariance": Number,                  // float, expressed in degrees
    "TxPolarization": Number,                       // 0 horizontal, 1 vertical, 2 circular left, 3 circular right
    "BeamName": String,                             // 4 (or 8, depending on GXT version) char beam id from GXT file
    "Cost": Number,
    "AutomaticPointingTimeout": Number,
    "GxtFileName": String,                          // Name of the GXT file containing the beam's contours
    "ExclusionZones": Array[Object[ExclusionZone]],
    "AcuXString": String,                           // Freeform string containing the extra hunt parameters (X) when using the OpenAMIP protocol
    "MaxSkew": Number,                               // float, expressed in degrees. Maximum skew angel to be sent to antenna (K)
    "TxFrequency": Number,                          // Hz, unsigned 64 bit integer. Will overrule the Tx Frequency sent to the ACU (only if > 0 and TxBandwidth also > 0). RF frequency, converted to LBand if needed
    "TxBandwidth": Number                           // Baud, unsigned 64 bit integer. Will overrule the Tx Bandwidth sent to the ACU (only if > 0 and TxFrequency also > 0)
}

OBJ ExclusionZone
{
    "ServiceArea": Number,        //The service area number in the GXT file corresponding to the exclusion zone
    "RxAllowed": Boolean,
    "TxAllowed": Boolean,
    "EIRPOmax": Number,
    "MinAlt": Number,
    "MaxAlt": Number
}

OBJ CarrierData
{
    "Enabled": Boolean,
    "TSMode": String,           // dvbs, dvbs2_ccm, dvbs2_acm, dvbs2x or dvbs2x_timesliced
    "TimeSliceNumber": Number,  // The primary TSN for the virtual carrier, from 1->62, only parsed in case TSMode == dvbs2x_timesliced
    "Freq": Number,             // Expressed in Hz, internally stored with a granularity of 10 kHz, unsigned 64 bit integer
    "SymbolRate": Number,       // Expressed Baud, unsigned 64 bit integer
    "Polarization": Number      // 0 horizontal, 1 vertical, 2 circular left, 3 circular right
}
OBJ PointingCarrier
{
    "Carrier": Object[CarrierData]
}
```

- The '//' is used to comment fields in the JSON description These are not part of the actual format and cannot be used in a real file as it is not valid JSON

- The JSON key-value pair show the name of the field followed by the JSON value type
- When the value of a key-value pair contains another JSON object, we use the syntax 'Object[ObjectName]'. In the real file, this object should be replaced by an object document further with the syntax 'OBJ ObjectName'
- When the value of a key-value pair is an array, this is described as Array[type], where type can be either a JSON type, or an object as described above

After selecting a new configuration file, a warning message is displayed:



2. Click Save to continue or Cancel to abort.

Beams can also be added, updated or deleted remotely from the hub using the **Remote Terminal Satellite Configuration** feature. The remote satellite configuration is created from the data in the central Network Management System or NMS, and is downloaded by the terminal.

5.2.4 Outdoor Unit

In normal user mode editing, adding or removing an ODU configuration can be disabled by your network operator. In expert user mode, editing, adding or removing an ODU is always possible.

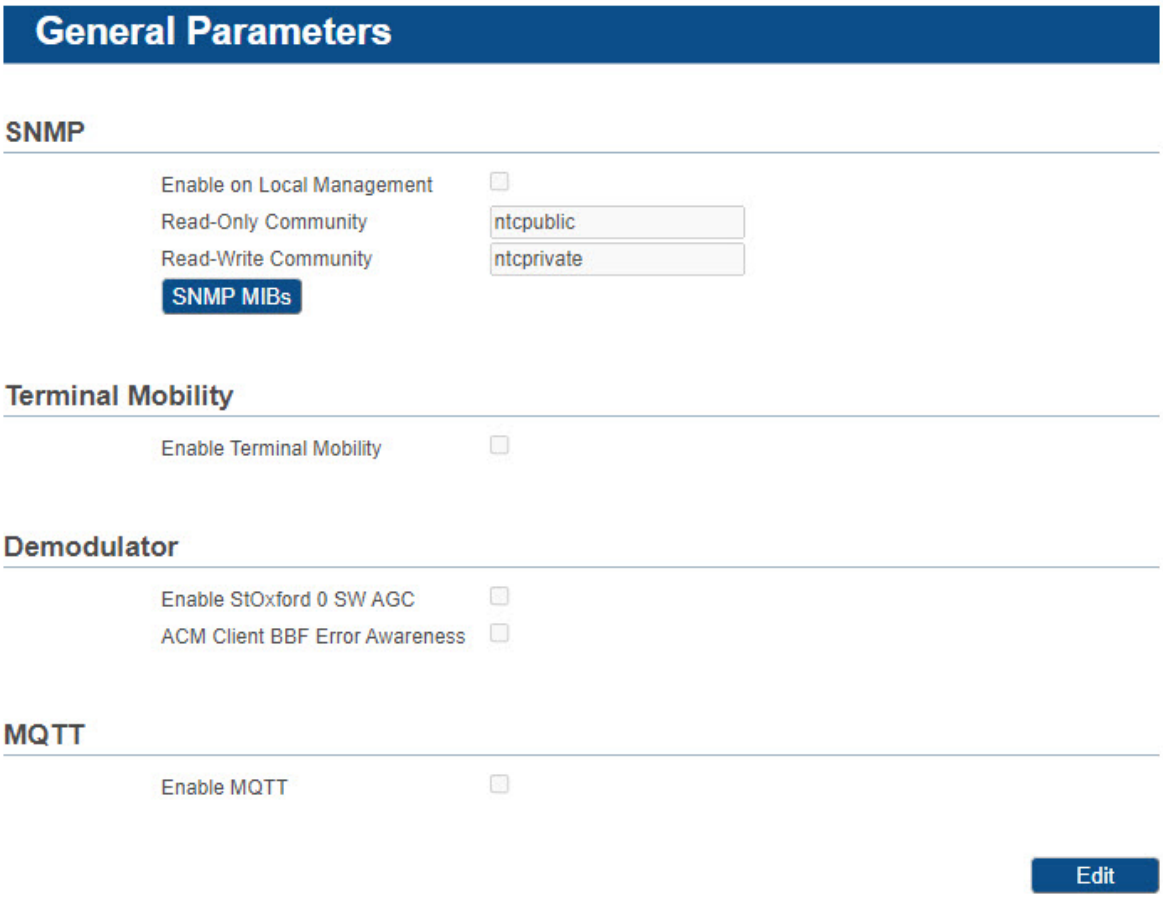
For more information, refer to section Outdoor Unit on page 53.

5.2.5 General

5.2.5.1 View General Parameters

In the **General** page you can:

- View and edit SNMP settings
- Enable terminal mobility and edit the settings
- Enable software controlled AGC or Automatic Gain Control
- Enable BBF Error-Aware ACM
- Enable MQTT



5.2.5.2 SNMP

Simple Network Management Protocol or SNMP is a standard protocol that is widely used for managing devices on IP networks. It is used by network administrators to monitor, configure and solve problems from a central point.

SNMP is an application-layer protocol. It runs over UDP at the transport level. The protocol is based on a manager / agent model.

The modems are SNMP manageable. This means that they have an SNMP agent that can be polled for information from a Network Management Station or NMS. The following figure presents the setup between the Dialog hub and a modem.

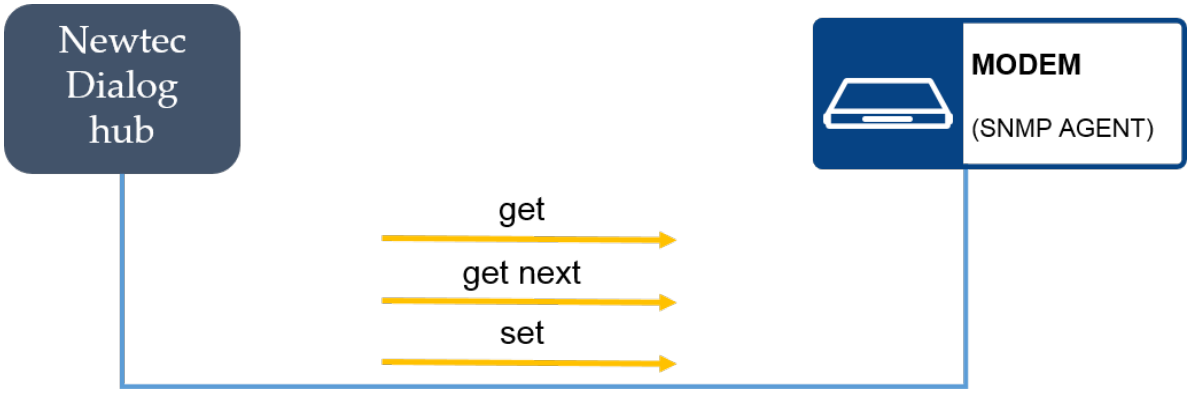
The SNMP agent used is MIB-II compliant.

The Management Information Base or MIB provides a standard representation of the SNMP Agent's available information and where it is stored. The MIB is defined according to the ASN.1 (Abstract Syntax Notation One).

The following SNMP operations are available:

Operation	Description	Action by the
get	Readout the current value of specific objects in the MIB.	NMS
get next	Readout the current value of the next object in the MIB.	NMS
set	Change a value of a specific object in the MIB.	NMS

The different operations are displayed in the following figure:



Specific SNMP ports are used to allow SNMP information to be sent to the correct application.

Currently only port number 161 is used. The port is used by an external SNMP manager to communicate with the SNMP agent.

5.2.5.2.1 Used MIBs

The Management Information Base or MIBis a database that describes the structure of the management data that can be used within a device.

The MIB uses hierarchical names containing Object Identifiers or OIDs to describe the management data of the device in a structured way. Every OID describes a variable that can be read and/or set using SNMP.

The MIB provides a standard representation of the SNMP Agent's available information and where it is stored.

The MIB is defined according to the ASN.1 (Abstract Syntax Notation One).

The MIB is derived from the device definition database and allows full monitor and control over the complete device using any SNMP browser (HPOpenView, NetworkView).

We support a limited subset of OIDs.

The customer must compile the obtained .mib files from within his Network Management Software. The following MIB files exist:

- NEWTEC-MAIN-MIB.mib:
- NEWTEC-DIALOG-TERMINAL-MIB.mib: This is the MIB Module for the management of the modem.

- SNMPv2-CONF.mib
- SNMPv2-SMI.mib
- SNMPv2-TC.mib

Click SNMP MIBs to download the SNMP MIB files. A mib.zip file is downloaded into your default download folder.

5.2.5.2.2 Edit SNMP

By default SNMP messages are exchanged between the modem and the Dialog hub. Next to this it is also configurable via the hub. It is possible to enable/disable SNMP on IPv4 and on IPv6 separately for each VLAN and this independently from ICMP.

If you want to use SNMP between the modem and a management PC. You have to enable the parameter "Enable on Local Management".

The following SNMP parameters can be edited:

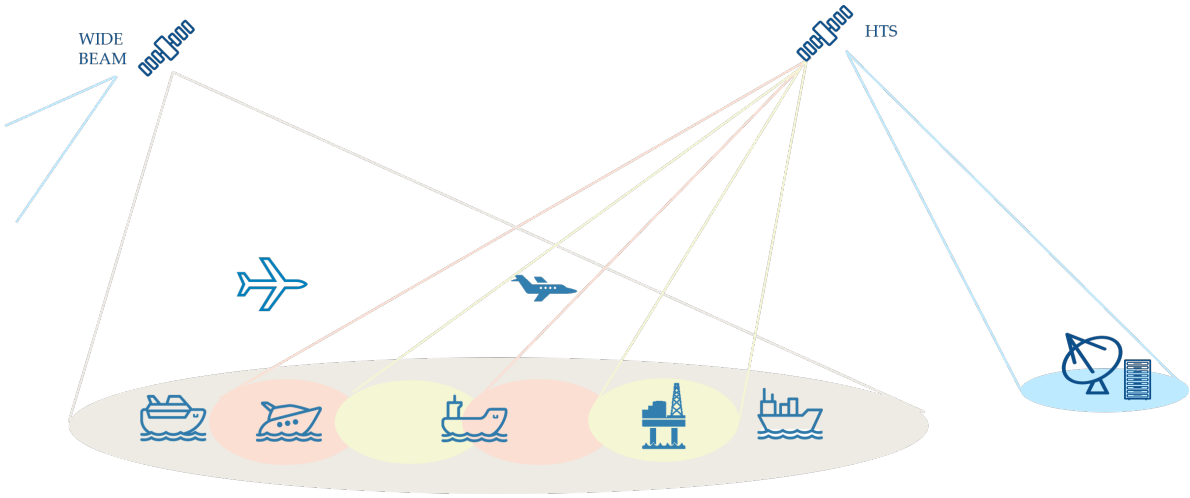
Parameter	Description
Enable on Local Management	Enable this parameter to make SNMP communication possible between the modem and a local management PC. ***Note** - SNMP communication is by default possible between the modem and the Dialog hub.*
Read-Only Community	The SNMP Read-Only Community String is like a password. It is sent along with each SNMP Get-Request and allows (or denies) access to device. The default public community string is set to ntcpublic. ***Note** - We recommend changing the community string. Do not to use "public" for the Read-Only Community string.*
Read-Write Community	The read-write community string protects the device against unauthorized changes. The default RW community is ntcprivate. ***Note** - We recommend changing the community string. Do not to use "private" for the Read-Write Community string.*

To edit the SNMP parameters, execute the following steps:

1. Click Edit at the bottom of the page.
2. Change the parameters.
3. Click Save to save your settings or Cancel to discard your settings.

5.2.5.3 Terminal Mobility

Mobile terminals are terminals that move during operation. They have a certain speed and optionally an acceleration and they can pass multiple satellite beam areas during their journey.



COTM terminals that can operate in multiple beams should have **Terminal Mobility**, **Automatic Initial Beam Selection (AIBS)** and **Automatic Pointing** enabled in the GUI.

At the hub-side, the terminals should be provisioned in all beams that they can encounter during their operation. The provisioning is done using **Attachment Profiles**, which consists of multiple home network attachments. Each attachment corresponds with a beam, a satellite network and the corresponding forward and return resources. The terminal should also have **COTM** and **Beam Roaming** enabled.

The COTM terminal operating in multiple beams can come online in any beam it supports. As it is not possible to predict in which beam the mobile terminal will become operational, **AIBS** and **Automatic Pointing** is used. AIBS controls the initial network acquisition process for the terminal and selects a beam using the geographical position of the terminal. Automatic pointing will make sure that the terminal antenna is optimally pointed towards the beam. AIBS and automatic pointing are entirely terminal-side driven. For more information about the initial beam selection, refer to Extra Terminal Mobility Functionality in GUI on page 106.

COTM terminals use the OpenAMIP protocol to instruct the antenna controller to target a particular satellite. The exchanged information includes, but is not limited to, satellite longitudinal position, tracking frequencies, LNB band selection, polarity (horizontal/vertical), cross pol / co-pol selections.

Once operational, the terminal can move from one beam to another. The terminal should be able to switch between different satellite beam areas without losing the satellite connection. This can be done using a **Mobility Manager**. The mobility manager decides to switch beams based on the position of the terminal and some specific beam information, such as contours, cost, and load.

Dialog provides two types of mobility manager:

- The **Central Mobility Manager** located at the hub side. In this case the modem sends its GPS coordinates over the satellite link to the mobility orchestrator. The central mobility manager gets the GPS coordinates of the terminal from the Mobility Orchestrator and applies the configured beam switching logic and business rules to make a beam switching decision if needed.
- The **Remote Mobility Manager** located at the terminal side. In this case, the modem does not send its GPS coordinates over the satellite link, since they could be considered as sensitive information. The remote mobility manager, which is integrated In the modem, periodically monitors the position of the terminal and applies the locally configured beam switching logic to make a beam switching decision if needed.

When the mobility manager takes the beam switching decision, it sends the target beam to the **Mobility Orchestrator** and the mobility orchestrator organizes the actual beam handover. The mobility orchestrator is an application running on the hub.

The central mobility manager can be an in-house add-on to the Dialog platform or it can be a third party application running on an external server. Make sure to enable the **Send status updates to DMM** parameter in the local modem GUI in order for the terminal to send its GPS coordinates to the mobility orchestrator. The mobility orchestrator will send these coordinates to the central mobility manager.

Remote mobility management is disabled by default. To enable it, make sure to:

- Select **Remote Mobility Management** check box in the Mobility tab of the Terminal Provisioning interface.
- Disable the **Send status updates to DMM** parameter in the local modem GUI. This will make sure that the terminal does not send GPS coordinates to the mobility orchestrator.

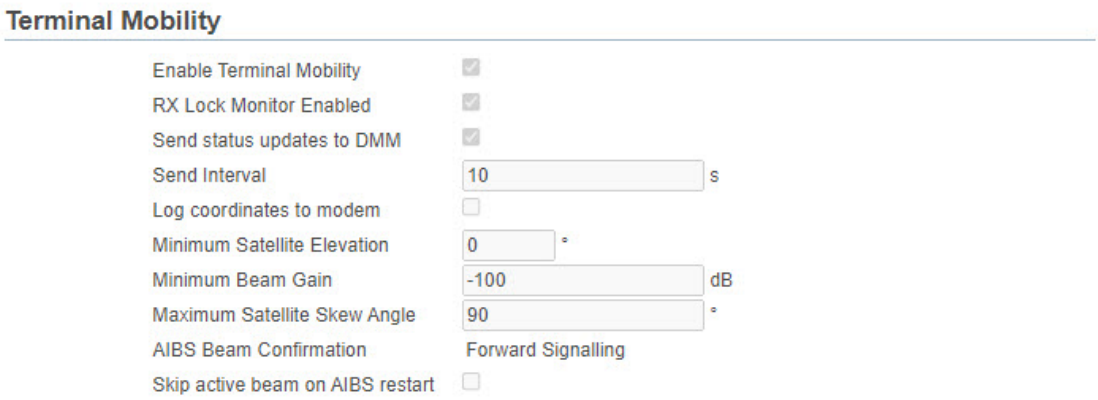
Both types of mobility manager can coexist on the Dialog platform. The Forward Table Broadcaster (FTB) includes a POP-ID that indicates whether or not remote mobility management is enabled.

For more information about the configuration, refer to the *Newtec Dialog Configuration User Guide*.

5.2.5.3.1 Enable Terminal Mobility

To enable terminal mobility, execute the following steps:

1. Click Edit at the bottom right of the page and select the **Enable Terminal Mobility** check box.



2. Edit the parameters.

Parameter	Description
RX Lock Monitor Enabled	When this check box is selected, the terminal's TX is disabled as soon as it detects a loss of forward lock.
Send status updates to DMM	When this check box is selected, the terminal is allowed to send information, such as GPS coordinates, to the mobility orchestrator. Select it when using a central mobility manager. Do not select it when using a remote mobility manager and GPS coordinates cannot be sent over the air.
Log coordinates to modem	Select the check box if you want to log the GPS coordinates of the modem.

Minimum Satellite Elevation	This is the minimum satellite elevation value at the terminal's location for a beam to be eligible during automatic beam selection and during target beam selection by the remote mobility manager.
Minimum Beam Gain	This is the minimum gain value at the terminal's location for a beam to be eligible during automatic beam selection and during target beam selection by the remote mobility manager.
Maximum Satellite Skew Angle	This is the maximum satellite skew angle value at the terminal's location for a beam to be eligible during automatic beam selection and during target beam selection by the remote mobility manager.
AIBS Beam Confirmation	This setting defines when the AIBS beam selection is considered successful. • Select **Forward Signalling** if the beam selection is considered successful when the terminal has a lock on the forward and can receive a NIT. • Select **Operational** if the beam selection is considered successful when the terminal is fully operational.
Skip Active Beam on AIBS restart	When this feature is enabled, if a terminal locks on a beam and AIBS timeout exceeds, then this beam will be skipped in next AIBS calculation.

3. Click Save to save your settings or Cancel to discard your settings.

5.2.5.3.2 Extra Terminal Mobility Functionality in GUI

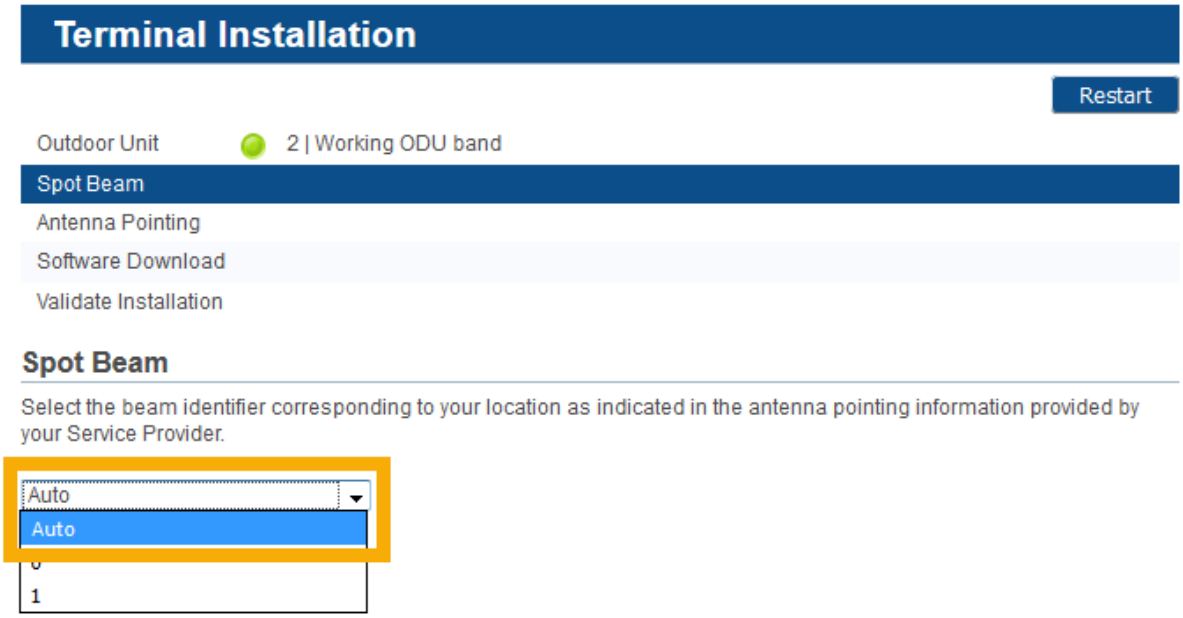
Enabling terminal mobility introduces extra functionality in the following menus:

Terminal Installation

An important mobility aspect is the ability for the satellite modem to autonomously acquire the network. As it is not possible to predict in which beam a multi-beam terminal will log on, Dialog implements the Automatic Initial Beam Selection or AIBS. AIBS is used to control the initial network acquisition process.

AIBS allows the modem to automatically select the best satellite beam from the list of configured beams at startup of the modem.

To enable AIBS, select **Auto** as **Spot Beam** value in the GUI during the installation of the terminal.



To select a beam, the terminal has to know its location on earth. Therefore, the **Antenna Control Unit** or **ACU** sends the GPS coordinates at regular intervals to the terminal using the OpenAMIP protocol.

For more information about the ACU, refer to Using Automatic Pointing on page 31.

When the modem knows it location, it parses all the configured beams to find out which beams are eligible. The modem uses **GXT files**, which contain beam contour data, to verify if it is located inside the contours of a beam.

When multiple beams are eligible the following policies are used in the specified order to select the initial beam.

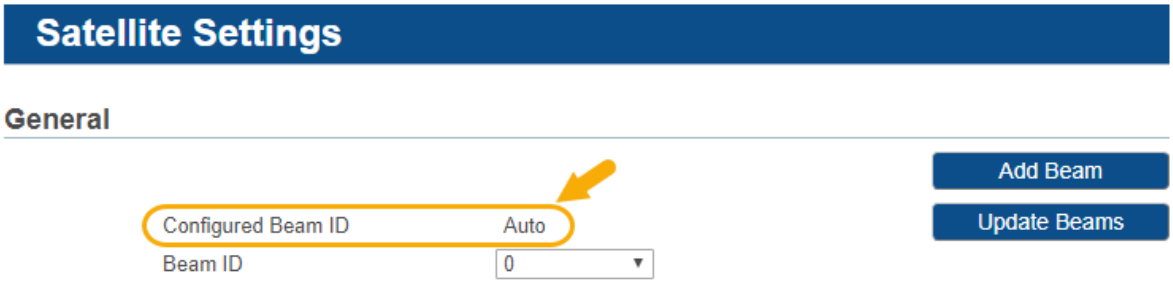
- The terminal is allowed to transmit in the beam (no exclusion zone).
- The cost of the beam; the lower the cost, the more eligible the beam is.
- The beam gain at the terminal position; the higher the gain, the more eligible the beam is.
- The beam elevation angle at the terminal position; the higher the elevation angle, the more eligible the beam is. The elevation angle determines which beam is closest to the modem. A higher elevation means a closer distance in longitude. A higher elevation has better link quality than a lower elevation.

When the modem has found the preferred beam, it sends the corresponding antenna pointing data to the ACU. If the parsing of the beams did not result in an eligible beam, no beam is selected!

Satellite Interface

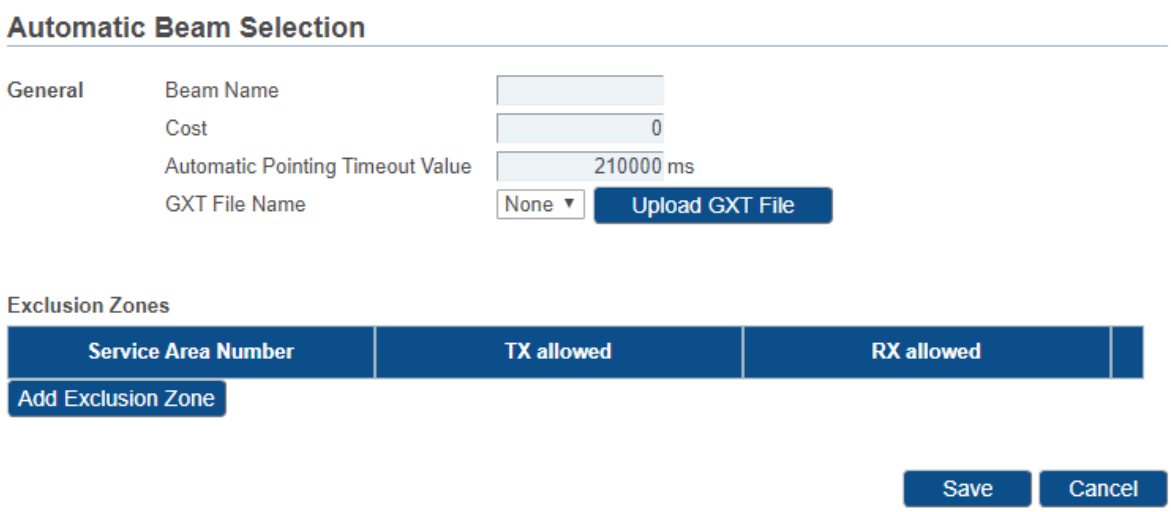
A **Configured Beam ID** text box is displayed in the **General** section. This corresponds with the identifier of the beam that was selected during terminal installation. Possible values are "Auto" (if AIBS is enabled) or any other numeric beam identifier.

The configured beam identifier can be different from the Active Beam identifier, for example if the terminal has moved to and operates in another beam than the one set during terminal installation.



The **Automatic Beam Selection** section is displayed.

Click Edit to change the Automatic Beam Selection parameters.



Automatic Beam Selection (only visible when terminal mobility is enabled)	
Beam Name	Name of the beam as mentioned in the corresponding GXT file
Cost	Value used by the terminal when it can choose to operate in multiple beams. The beam with the lowest cost value is then selected.
Automatic Pointing Timeout Value	Time interval after which a terminal returns to the automatic beam selection procedure (if the terminal can not lock on the received forward link).
GXT File Name	Select a GXT file from the drop-down list or click Upload GXT File to upload a file from your local computer. The uploaded files will also appear under the GXT Files menu, see below. The modem parses the uploaded file to make sure it has the correct format and content before writing it to memory. A warning message is displayed if the file is incorrect. GXT files are typically provided by the satellite operator.
Exclusion Zones	Click Add Exclusion Zone to add an area in which a terminal is not allowed to operate. This area is determined by the following parameters: • Service Area Number: as mentioned in the GXT file • Tx Allowed: checkbox to indicate of terminal can only transmit in the exclusion zone. For future use. • Rx Allowed: checkbox to indicate of terminal can only receive in the exclusion zone. For future use.

GXT Files

When terminal mobility is enabled, the GXT Files menu item appears. Here you can find all GXT files that are known to the modem.

A GXT file contains information of one or more beams that are available on the same satellite. Every beam has its specific beam identifier within that file. There is at least one GXT file per satellite. GXT files are typically provided by the satellite operators.

GXT is a standardized file format from the International Telecommunication Union (ITU).

The standard GXT format has the intention to provide a topographic description of the beam coverage. This means that the diagrams in the GXT file provide a description of the beam coverage in function of equal gain contours and bores (peaks) similar to a topographic map (relief map). This type of data is used to perform gain interpolation at a specific point of interest (for example, the terminal position).

AIBS and the remote mobility manager do not perform gain interpolation but rely on a simpler algorithm which determines if a point is within a specific contour associated to a specific gain value. The contours therefore have a different meaning than the contours in the original GXT format. Whereas the contour in the original GXT format is a contour containing points having the same gain value, the contour used by the modem must enclose an area within which the gain is greater or equal than a specific value.

Although in most cases both definitions result in the same contour, there are several corner cases where this is not the case. Therefore the standard GXT files and those used by the modem differ in a number of aspects (the ones used by the modem contain less information). Additionally, the modem uses only one GXT files for both the uplink and downlink coverage of the beam. This GXT files represents the worst case coverage, which is usually the uplink coverage.

As an Expert user, you can:

- **Delete GXT files**: Select one or more GXT files using the check boxes and click Delete Selected Files. If the selected GXT file is still used in a beam, it will not be deleted. Only unused GXT files can be deleted.
- **Download GXT files**: Click Download GXT Files to save the GXT files as a compressed file on your computer.
- **Upload GXT files**: If you want to upload one or more GXT files, click Upload GXT Files. Select on or more GXT files from your PC.

The modem parses the uploaded file to make sure it has the correct format and content before writing it to memory. A warning message is displayed if the file is incorrect.

GXT files are typically provided by the satellite operator.

5.2.5.4 Demodulator

5.2.5.4.1 Automatic Gain Control

AGC or **Automatic Gain Control** is a closed-loop control system used to ensure that the received signal is consistently amplified to a level that allows for efficient processing by the demodulator. AGC uses the signal power of the entire L-band to control the gain of the received signal.

SW AGC has a positive impact on fast pulsing interference (pulse length in the range of 10 ms or smaller) and has been optimized for interference with a C/I value down to -10 dB. This means that the interferer has the 10-fold power of the useful carrier. Pulsing interference can be caused for example by a radar signal.

Without software controlled AGC, the AGC loop reacts fast to power changes in the L-band. Fast pulsing interference in the L-band (not in-band) can therefore lead to sudden and significant Es/N0 variations. These variations can cause packet loss and can even unlock the demodulator.

With software controlled AGC or SW AGC, the gain is determined such that the received L-band power achieves a minimum required power. SW AGC will not change the gain as long as the received power is within acceptable boundaries. The lower boundary is such that there is no quantization noise floor at the lowest input level (-50 dBm), the higher boundary is such that there is no clipping in the presence of a signal without adjacents. If the received power exceeds these boundaries, SW AGC will only slowly adjust the gain. The power is monitored every 250 ms; if the power exceeds the higher boundary, the gain is decreased; if the power exceeds the lower boundary, the gain is increased. In case of fast pulsing interference the Es/N0 variations will therefore be limited and can be handled by the ACM algorithm.

5.2.5.4.2 BBF Error-Aware ACM

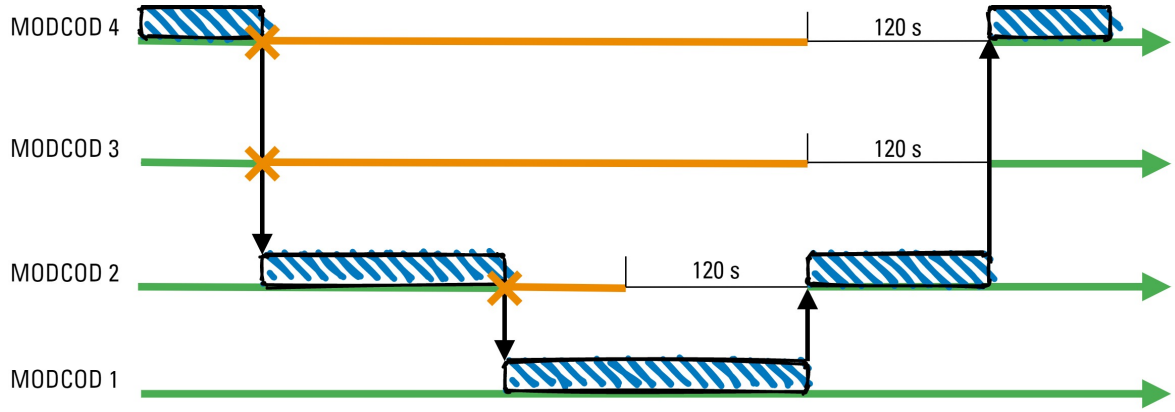
Adaptive Coding and Modulation or **ACM** allows modification of the modulation parameters of a satellite signal on the fly, without interrupting the transmission and without losing data. When combined with a measurement of the instantaneous link conditions every few seconds and a system that automatically adjusts the modulation parameters when needed, ACM allows using the highest possible modulation scheme and the lowest possible level of error correction at all times.

ACM allows to take into consideration if there are any frame errors on a specific MODCOD and not to use it again for a specific time.

For each available MODCOD the terminal monitors the errored baseband frames. Errored baseband frames are dropped at the modem's decoder. A MODCOD becomes 'unavailable' from the moment that errored frames occur and will remain 'unavailable' 120 seconds after the last errored frame occurred.

When the modem notices a baseband frame drop for the MODCOD it has selected according to the ACM algorithm described above, it will select a lower and error-free MODCOD. An error-free MODCOD is a MODCOD where there has not been an errored baseband frame in the last 120 seconds.

The mechanism is explained in the example below.



In the example we assume that, according to the ACM algorithm, the modem is able to use MODCOD 4. We also assume that at some point in time a local source of distortion appears, which degrades the forward link quality for the modem.

Due to this link degradation, MODCOD 4 starts showing errored baseband frames. This triggers the modem to select a lower error-free MODCOD. As MODCOD 3 also has errored baseband frames, the modem selects MODCOD 2. The modem keeps on using this MODCOD as long as there are no errored frames and the higher MODCODs are not error-free. In this example the link degradation gets worse and starts affecting MODCOD 2 as well. MODCOD 2 shows errored frames and the modem selects a lower error-free MODCOD, which is MODCOD 1. The modem keeps on using this MODCOD as long as there are no errored frames and the higher MODCODs are not error-free. After some time the link degradation is less severe and MODCOD 2 is considered error-free, meaning that the last errored frame occurred 120 seconds ago. The modem moves up from MODCOD 1 to MODCOD 2 and uses that MODCOD as long as there are no errored frames and the higher MODCODs are not error-free. When the source of distortion disappears, MODCOD 3 and 4 are considered error-free after 120 seconds the last errored frame occurred. When that happens the modem moves from MODCOD 2 to the highest error-free MODCOD, which is in this case MODCOD 4 and thus skips MODCOD 3.

5.2.5.5 MQTT

MQTT or Message Queue Telemetry Transport is a client/server publisher/subscriber messaging transport protocol. It is a light-weight, open standard designed to be easy to use and implement.

MQTT is originally designed for connections with remote locations where a "small code footprint" is required or the network bandwidth is limited. The goal is to provide a protocol, which is bandwidth-efficient and uses little battery power. It is mainly applicable in the IoT or Internet of Things use cases.

Documentation concerning MQTT is widely available.

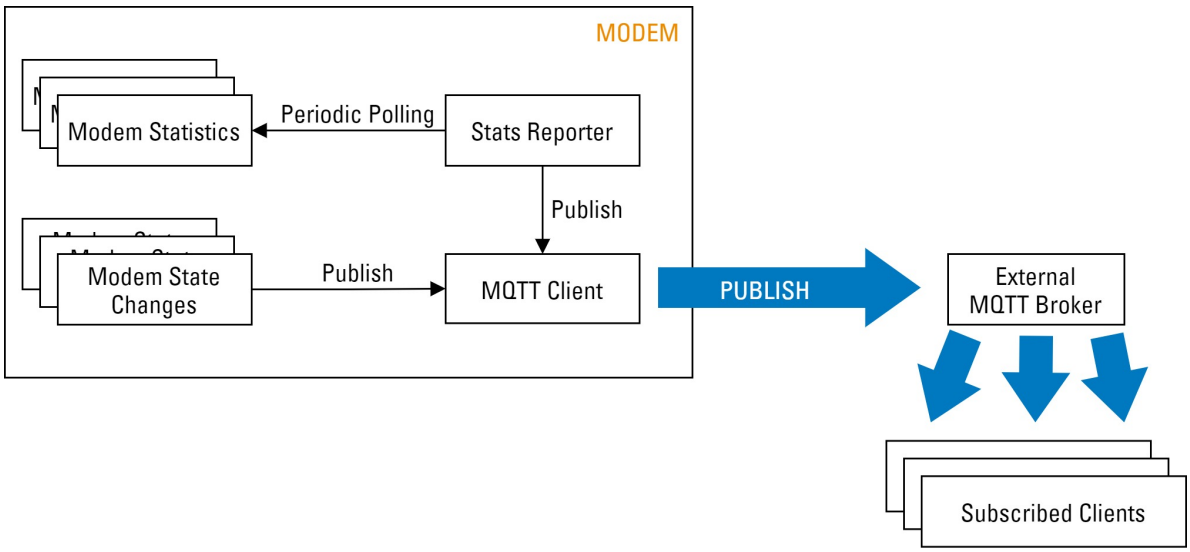
The protocol uses a publish/subscribe architecture. Publish/Subscribe is event-driven and enables messages to be pushed to clients. The central communication point is the MQTT broker, in charge of dispatching all messages between the senders and the rightful receivers. Key elements of the communication are:

- Each client that publishes a message to the broker, includes a topic into the message.
- The topic is the routing information for the broker.
- Each client that wants to receive messages subscribes to a certain topic and the broker delivers all messages with the matching topic to the client.

MQTT on the modem is used for monitoring the modem state changes and statistics. The modem is an MQTT client that publishes messages to an external broker at the LAN side.

Whenever a state change occurs in a component of the modem, the event is immediately sent to the modem MQTT client and published to the broker.

Statistics are collected and sent every 20 seconds to the modem MQTT client which then publishes the message.



The following modem state change events generate an MQTT message:

- Active beam change
- Beam switch
- Terminal operational state change
- Terminal TX mute state change
- Demodulator lock state change

The following modem statistics are polled and generate an MQTT message every 20 seconds:

- System
- Demodulator
- Events
- Traffic
- TCP
- Terminal Position data

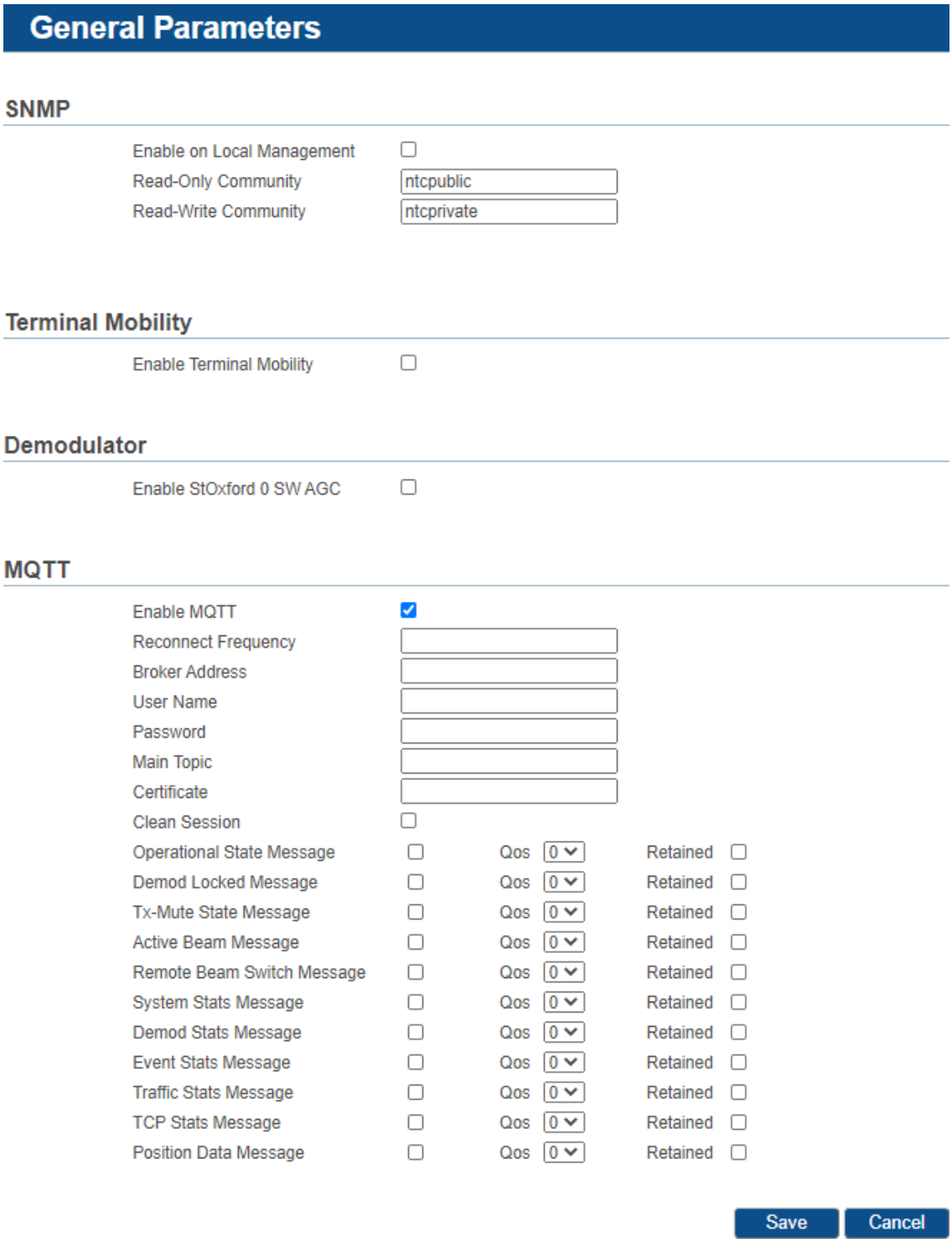
The payload of the MQTT messages are formatted in Message Pack.

For more information about the messages, refer to Modem State Change Event Messages on page 115 and Modem Statistics Messages on page 117.

5.2.5.5.1 Enable MQTT

To enable MQTT, execute the following steps:

1. Click Edit at the bottom right of the page and select the **Enable Terminal Mobility** check box.



2. Edit the parameters.

Parameter	Description
Reconnect Frequency	This is the time in seconds that the MQTT client tries to reconnect to the MQTT broker in case it disconnected. The default value is 2 seconds. Valid values are from 2 to 30 seconds.

Broker Address	This is the IP address of the broker.
User Name	This is the user name of the MQTT client and is used to authenticate the client towards the broker. The broker should know this user name as well.
Password	This is the password of the MQTT client and is used to authenticate the client towards the broker. The broker should know this password as well.
Main Topic	This string is pre-pended to the message topics.
Certificate	This is a X.509 certificate to establish a secure MQTT connection. If a valid certificate is set, the client will connect to the broker with TLS encryption. ***Important** - The modem must have a valid time set; secure connection attempts without a valid time will be refused by the broker.*
Clean Session	When the client connects to the broker it uses the clean session flag to indicate whether or not a persistent connection is required. With a non-persistent connection the broker does not store any subscription information or undelivered messages for the client. This mode is ideal when the client only publishes messages. It can also connect as a durable client using a persistent connection. In this mode the broker will store subscription information, and undelivered messages for the client. ***Note** - Not all messages will be stored for delivery, as the quality of service of the subscriber and publisher has an effect.*
Per MQTT Message	• Each MQTT message can be **enabled** or **disabled** individually. When disabled, the message is not sent to the broker. • **Qos**: – **0** (at most once): QoS 0 is the lowest QoS level that only guarantees best effort delivery. The client simply publishes the message to the broker. The broker will not send an acknowledgement. This QoS offers no real guarantee that the message will arrive. – **1** (at least once delivery to the broker): The client publishes a message to the broker and stores it until it receives a PUBACK packet from the broker. If the client does not receive the PUBACK packet, it resends the publish message and sets the duplicate flag to '1' indicating that the message was already sent in the past. The client repeats this until he receives a PUBACK packet. – **2** (exactly once delivery): This QoS class guarantees that the message is received once and only once. The client publishes a message to the broker. The broker sends a PUBREC packet to indicate that the message was received. If the client does not receive the PUBREC packet, it assumes that the broker did not receive the publish message and the client resends it with the duplicate flag set to '1'. The client repeats this until it receives

	the PUBREC packet from the broker. Upon receipt of the PUBREC packet, the client sends a PUBREL packet. This message informs the broker that it can release the message to the subscribers. If the broker succeeds in sending the message to the subscribers, it sends a PUBCOMP packet to the publishing client informing it that the publishing is completed. If the client does not receive the PUBCOMP packet, the client resends the PUBREL packet. The client repeats this until it receives the PUBCOMP packet from the broker. • **Retained**: If this flag is set, the last message published on this topic will be saved on the broker. When a new client subscribes to the topic it will receive the last message published in the past on the topic. If the flag is not set, the messages are not saved on the broker. When a new client subscribes to the topic it will only get a message as soon as a new message is published on the topic.

5.2.5.5.2 Modem State Change Event Messages

The following state change event messages exist:

- Active beam change on page 115
- Beam switch on page 115
- Terminal operational state change on page 116
- Terminal TX mute state change on page 116
- Demodulator lock state change on page 116

The timestamp value in the message payload will be "null" as long as the modem did not receive the NTP multicast from the hub.

Active Beam Change

MQTT Topic	*maintopic*/terminal/airmac/mobility/activeBeam

MQTT Payload	{
	"airMac": (fixstr) //MAC address of the terminal,
	"timestamp": (timestamp 64) //Seconds and nanoseconds since epoch,
	"beamCfgId": (nil) or (uint 64) //Identical to the beam ID signaled in the beam switch TIM
	}

Beam Switch

MQTT Topic	*maintopic*/terminal/airmac/mobility/remoteBeamSwitch

MQTT Payload	{
	"airMac": (fixstr) //MAC address of the terminal,
	"timestamp":(timestamp 64) //Seconds and nanoseconds since epoch ,

	"beamCfgId": (nil) or (uint 64) //ID of the target beam as signaled in the beam switch TIM,
	"acuxString": (fixstr) //As signaled in the beam switch TIM,
	"custData": (fixstr) //Customer defined data as signaled in the beam switch TIM
	}

Terminal Operational State Change

MQTT Topic	*maintopic*/terminal/airmac/mobility/operationalState

MQTT Payload	{
	"airMac": (fixstr) //MAC address of the terminal,
	"timestamp": (timestamp 64) //Seconds and nanoseconds since epoch,
	"opState": (fixstr) //Possible values are: "Idle", "Antenna Pointing", "Satellite Network Lookup", "Synchronizing", "Synchronized", "Network Layer Initialization", "Operational"
	}

Terminal TX Mute State Change

MQTT Topic	*maintopic*/terminal/airmac/mobility/operationalState

MQTT Payload	{
	"airMac": (fixstr) //MAC address of the terminal,
	"timestamp": (timestamp 64) //Seconds and nanoseconds since epoch,
	"state": (bool) //True = mute, False = unmuted,
	"longitude": (float32) //Longitude,
	"latitude": (float32) //Latitude
	If 'state'==True:
	,
	"reason": (fixstr) //Indicates the reason for switching off TX. Possible values are "exclusionZone", "api_disable", "Tim_disable", "hw_discrete_disable", "no_fwd_lock", "no_power_message", "no_reference_clock"
	}

Demodulator Lock State Change

MQTT Topic	*maintopic*/terminal/airmac/mobility/operationalState

MQTT Payload	{
	"airMac": (fixstr) //MAC address of the terminal,
	"timestamp": (timestamp 64) //Seconds and nanoseconds since epoch,
	"demodId": (fixstr) //ID of the demodulator,
	"lockStatus": (bool) //True if demodulator was continuously locked during the last second, False if demodulator goes/is out of lock
	}

5.2.5.5.3 Modem Statistics Messages

The following statistics messages exist:

- System statistics on page 117
- Demodulator statistics on page 117
- Event statistics on page 119
- Traffic statistics on page 119
- TCP statistics on page 121
- Terminal Position data on page 121

The timestamp value in the message payload will be "null" as long as the modem did not receive the NTP multicast from the hub.

System Statistics

MQTT Topic	*maintopic*/terminal/airmac/systemStats

MQTT Payload	{
	"airMac": (fixstr) //MAC address of the terminal,
	"timestamp": (timestamp 64) //Seconds and nanoseconds since epoch,
	"uptime": (unit 64) //Modem uptime in 0.01 seconds,
	"temp": (float32) //CPU temperature in degree Celsius,
	"tempState": (fixstr) //Temperature state of the CPU. Possible values are: "Normal", "Below Operational", "Above Operational",
	"cpuUsage": (array) //One array per physical CPU core, expressed in total CPU usage % per core
	}

Demodulator Statistics

MQTT Topic	*maintopic*/terminal/airmac/demodStats

MQTT Payload

```
{
   "airMac": (fixstr) //MAC address of the terminal,
   "timestamp": (timestamp 64) //Seconds and nanoseconds
   since epoch,
   "stats": (array) //Array of demodstats maps
      (demodstats map) {
         "demodId": (uint8) //ID of the demodulator,
         "lockStatus": (bool) //Lock status,
         "locks": (uint16) //Counter which is incremented
         every time a new terminal acquires terminal
         lock.Only available for the first demod,
         "rxCarPwr": (float32) //Received Carrier power
         measured in dBm,
         "rxComPwr": (float32) //Received composite
         L-band power measured in dBm,
         "esNo": (float32) //Es/No in dB,
         "rxFreq": (uint64) //Downlink RF Receive
         Frequency in Hz,
         "rxSymRate": (uint32) //Symbol rate in Baud,
         "phyFrms": (uint64) //Total number of received
         physical layer frames,
         "dmmyFrms": (uint64) //Total number of received
         dummy frames,
         "bbdFrms": (uint64) //Total number of received
         baseband frames of selected MODCOD or lower,
         "bbdDrpFrms": (uint64) //Total number of dropped
         baseband frames of selected MODCOD or lower,
         "modCod": (uint8) //Active MODCOD, determined by
         the ACM client; only available for first demod,
         If 'demodtype'==fpga:
         "pn": (float 32) //Phase noise value in dB,
         "lm": (float 32) //Link margin in dB,
         "modCods":(array) //Array of modcodstats maps
            (modcodstats map){
               "id": (uint8) //ID of the MODCOD,
               "bbdFrms": (uint32) //Total number of
               received baseband frames for the given
               MODCOD,
               "bbdDrpFrms": (uint32) //Total number of
               received baseband frames for a given MODCOD
               which could not be decoded
               If 'demodtype'==fpga:
               ,
               "cond": (float 32) //C/(N+D) value in dB,
               "cod": (float 32) //C/D value in dB
            },
```

	}, }

Event Statistics

MQTT Topic	*maintopic*/terminal/airmac/eventStats

MQTT Payload	{
	"airMac": (fixstr) //MAC address of the terminal,
	"timestamp": (timestamp 64) //Seconds and nanoseconds since epoch,
	"l3CfgFails": (uint32) //Number of times the network layer initialization failed, for example when TCS could not be reached,
	"fwErrs": (uint32) //Number of errors reported on the forward signaling,
	"rtErrs": (uint32) //Number of errors reported on the return signaling,
	"fullReinits": (uint32) //Number of times a full terminal initialization was triggered,
	"fastSyncs": (uint32) //Number of times a fast terminal synchronization was triggered,
	"opers": (uint32) //Number of times a terminal became fully operational,
	"syncs": (uint32) //Number of times a terminal reached the synchronized state,
	"ncrLates": (uint32) //Number of times the NCR signaling was too late,
	"ncrWrongs": (uint32) //Number of times a wrong NCR value was received,
	"ncrNotRecvds": (uint32) //Number of times an error event occurred for NCR signaling
	}

Traffic Statistics

MQTT Topic	*maintopic*/terminal/airmac/trafficStats

MQTT Payload	{
	"airMac": (fixstr) //MAC address of the terminal,
	"timestamp": (timestamp 64) //Seconds and nanoseconds since epoch,
	"stats": (array) //Array of trafficstats maps
	(trafficstats map){
	"name": (fixstr) //Identification of the QoS traffic class,
	"trfType": (fixstr) //Type of traffic; possible values are: "Layer 2", "Layer 3 unicast", "Layer 3 multicast", "Unknown",
	"RtRxPkts": (uint32) //Number (incremental) of received packets for the return link,
	"rtRxBytes": (uint32) //Number (incremental) of received bytes on the return link; for layer 3 this is only counting the payload bytes; for layer 2 this includes the complete layer 2 packet,
	"rtRxBitRate": (uint32) //Bit rate in kbps of the received data for the return link, this is the value averaged over the second before the request,
	"rtRxPkts": (uint32) //Number (incremental) of transmitted packets for the return link; the transmitted byte count can be different from the received byte count because packets can be transformed (encryption, compression, aggregation and tunneling), or packets can be dropped,
	"rtTxBytes": (uint32) //This parameter will count the transformed packet count,
	"rtTxBitRate": (uint32) //Bit rate in kbps of the transmitted data for the return link; this is the value averaged over the second before the request,
	"rtDropPkts": (uint32) //Total number of dropped packets of the return link (transformation before the dropping happens),
	"rtDropBytes": (uint32) //Total number of dropped bytes of the return link,
	"rtDropBitRate": (uint32) //Total drop rate in kbps of the return link; this is the value averaged over the second before the request,
	"rtQueueTime ": (uint32) //Average time in msec a packet for this return link is queued; this is the weighted average over the last five seconds
	}
	}

TCP Statistics

MQTT Topic	*maintopic*/terminal/airmac/tcpStats

MQTT Payload	{
	"airMac": (fixstr) //MAC address of the terminal,
	"timestamp": (timestamp 64) //Seconds and nanoseconds since epoch,
	"stats": (array) //Array of tcpstats maps
	(tcpstats map){
	"name": (fixstr) //Identification of the QoS traffic class,
	"tcpSess": (uint32) //Number of pending TCP sessions,
	"tcpSessLan": (uint32) //Number of incoming TCP sessions triggered from the modem LAN side; for every new TCP session this value will be incremented,
	"tcpSessHub": (uint32) //Number of incoming TCP sessions triggered from the hub module side; for every new TCP session this value will be incremented,
	"tcpSessDest": (uint32) //Number of TCP sessions which are destroyed and no longer supported by Tellinet; a TCP session is typically destroyed when there is no traffic for several minutes
	},
	}

Terminal Position Data

MQTT Topic	*maintopic*/terminal/airmac/positionData

MQTT Payload	{
	"airMac": (fixstr) //MAC address of the terminal,
	"timestamp": (timestamp 64) //Seconds and nanoseconds since epoch,
	"longitude": (float 32) //Longitude,
	"latitude": (float 32) //Latitude,
	"altitude": (nil) or (float 32) //Altitude,
	"skewAngle": (nil) or (float 32) //Skew angle,
	"heading": (nil) or (float 32) //Heading,
	"speed": (nil) or (float 32) //Speed,
	"yaw": (nil) or (float 32) //Yaw,
	"pitch": (nil) or (float 32) //Pitch,
	"roll": (nil) or (float 32) //Roll
	}

5.2.6 Device Info

5.2.6.1 Load Alternative Software

The modem software is automatically upgraded over the satellite without any user interaction. In general, the only requirement for an upgrade to be successful is for the modem to have satellite connectivity during the time of upgrade.

In case the modem is not able to establish a lock on the forward link, an upgrade over the satellite link cannot be done. The expert user can manually trigger the modem to upgrade.

1. Click the Load Alternative Software button to put a modem firmware file on the passive memory bank via the GUI. This can also be an older firmware version, in which case you can downgrade the modem.
2. Select a modem firmware file from your PC.

The modem parses the uploaded file to make sure it has the correct format and content before writing it to memory. A warning message is displayed if the file is incorrect.

Modem firmware files are typically provided by the service provider or manufacturer.

3. Click the Try Alternative Software button to activate the newly installed modem firmware.

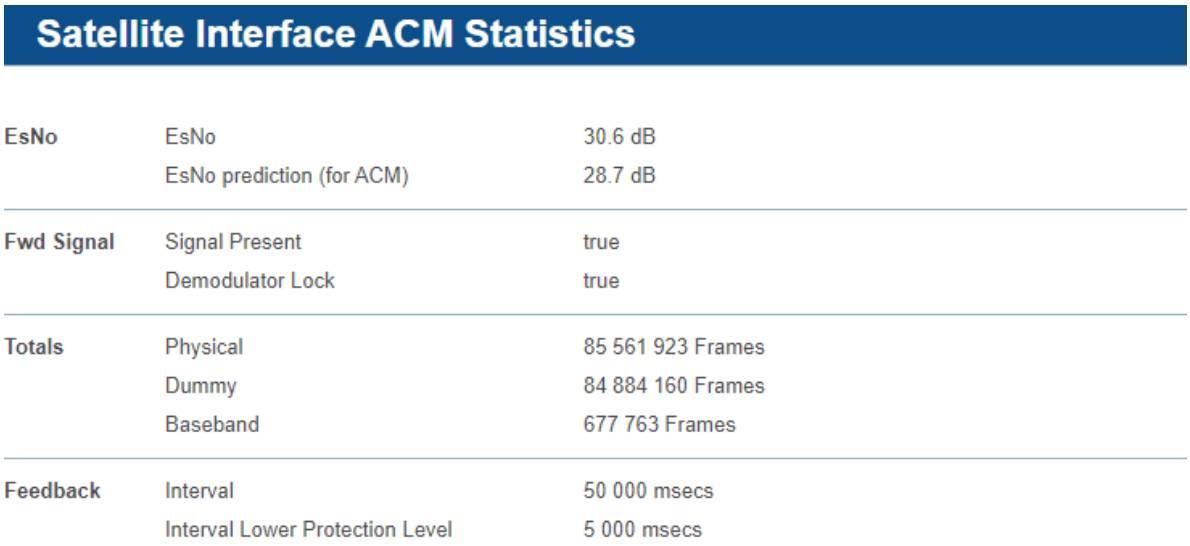
5.2.6.2 JSON API Description

Click the link Public API (opens in new tab) to get the JSON API description. The JSON API can be used by 3rd party applications to interact with or query the modem.

5.2.7 Demodulator Statistics

This page provides information about the terminal demodulator statistics. The statistics are displayed in two sections.

Satellite Interface ACM Statistics



Satellite Interface ACM Statistics Parameters		Description
EsNo	EsNo	Internal Es/N0 value used by the ACM client on the terminal to determine what modulation and coding scheme will be used.
	EsNo prediction (for ACM)	Actual Es/N0 value used by the ACM client on the terminal to determine what modulation and coding scheme will be used. Corrections are based upon this value.
Fwd Signal	Signal Present	Is the signal present (true/false)?
	Demodulator Lock	Is the demodulator locked (tue/false)?
Totals	Physical	Total number of physical frames
	Dummy	Total number of dummy frames
	Baseband	Total number of baseband frames
Feedback	Interval	This is the time interval (in milliseconds) the ACM parameters are updated in the Terminal.
	Interval Lower Protection Level	This is the duration (in milliseconds) that the signal level has to exceed the minimum threshold of a higher MODCOD before requesting the hub to switch to the higher MODCOD.

Demodulator MODCODs

ID	Name	Threshold (dB)	EsNo.In (dB)	EsNo.Down (dB)	BB Frames	Dropped BB Frames
1	QPSK 1/4	-1.0	-1.0	-1.0	0.0	0.0
2	QPSK 1/3	-0.5	-0.5	-0.5	0.0	0.0
3	QPSK 2/5	0.5	0.5	0.5	0.0	0.0
4	QPSK 1/2	1.6	2.3	1.8	659895.0	0.0
5	QPSK 3/5	2.9	3.6	3.1	7.0	0.0
6	QPSK 2/3	3.8	4.5	4.0	7.0	0.0
7	QPSK 3/4	4.7	5.4	4.9	9.0	0.0
8	QPSK 4/5	5.5	6.2	5.7	9.0	0.0
9	QPSK 5/6	6.0	6.7	6.2	8.0	0.0
10	QPSK 8/9	7.0	7.7	7.2	6.0	0.0
11	QPSK 9/10	7.1	7.1	7.1	0.0	0.0
12	8PSK 3/5	6.3	6.3	6.3	0.0	0.0
13	8PSK 2/3	7.1	7.8	7.3	7.0	0.0
14	8PSK 3/4	8.5	9.2	8.7	8.0	0.0
15	8PSK 5/6	10.0	10.0	10.0	0.0	0.0
16	8PSK 8/9	11.4	11.4	11.4	0.0	0.0
17	8PSK 9/10	11.5	11.5	11.5	0.0	0.0
18	16APSK 2/3	9.7	10.4	9.9	6.0	0.0
19	16APSK 3/4	10.9	11.6	11.1	7.0	0.0
20	16APSK 4/5	11.7	12.4	11.9	7.0	0.0
21	16APSK 5/6	12.2	12.9	12.4	8.0	0.0
22	16APSK 8/9	13.5	14.2	13.7	10.0	0.0
23	16APSK 9/10	13.7	13.7	13.7	0.0	0.0
24	32APSK 3/4	13.9	13.9	13.9	0.0	0.0
25	32APSK 4/5	14.9	15.6	15.1	8.0	0.0
26	32APSK 5/6	15.6	16.3	15.8	23051.0	0.0
27	32APSK 8/9	17.1	17.1	17.1	0.0	0.0
28	32APSK 9/10	17.4	17.4	17.4	0.0	0.0
32	QPSK 11/45	-100.0	-100.0	-100.0	0.0	0.0
33	QPSK 4/15	-100.0	-100.0	-100.0	0.0	0.0
34	QPSK 13/45	-1.0	-1.0	-1.0	0.0	0.0

Demodulator MODCOD Parameter	Description
ID	Identification assigned to the specific MODCOD.
Name	Name of the Modulation and Coding Scheme.
Threshold (dB)	Minimum hard-coded threshold value for each MODCOD.

Es/No.In (dB)	This is Threshold (dB) + (DM + ML) (dB) + ACM.in (dB). These reference value is used to decide when to move up to a next higher MODCOD, when its measured Es/No > Es/No_IN.
Es/No.Down (dB)	This is Threshold (dB) + (DM + ML) (dB) + ACM.Down (dB). A lower MODCOD is requested when the measured Forward Es/No < Es/No_DOWN.
BB Frames	Number of received baseband Frames.
Dropped BB Frames	Number of dropped baseband Frames.

The rows in the table can have different colors:

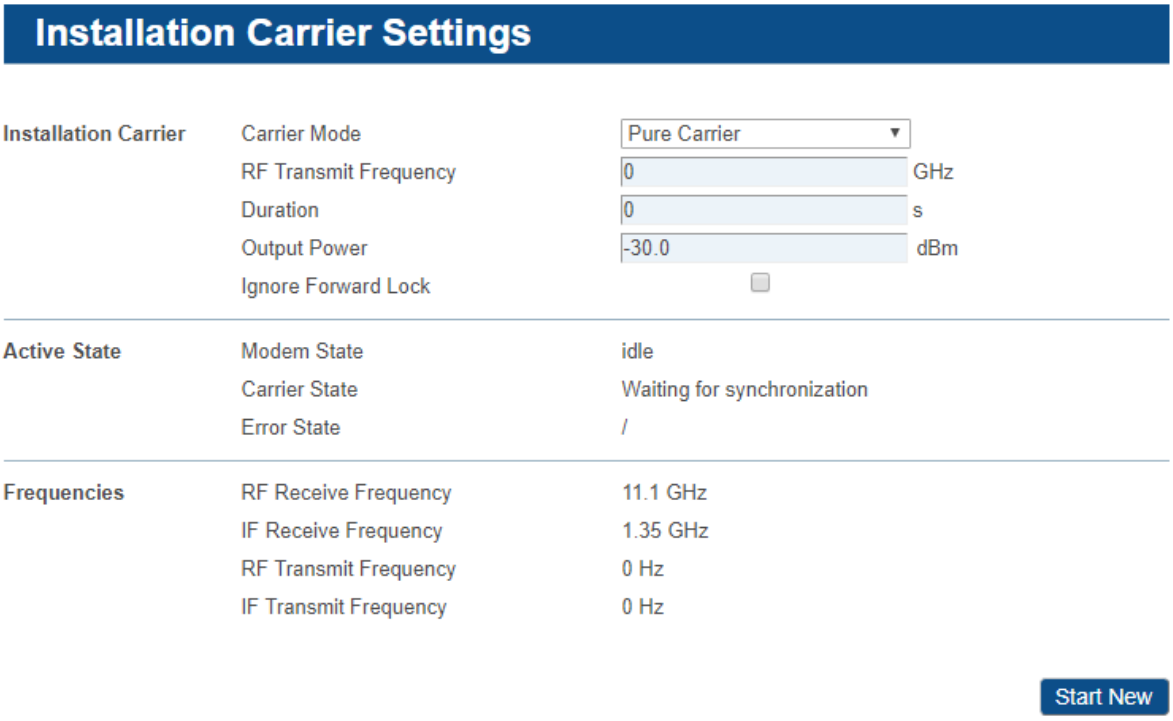
- Green: MODCOD that the terminal is using.
- Black: MODCOD that the terminal can receive.
- Grey: MODCOD that is not configured on the terminal.

Click Reset to set the counters to zero.

5.2.8 Installation Carrier

The expert user has the possibility to activate a dedicated installation carrier test mode to verify the correct terminal installation and pointing of the antenna, or to perform a manual line-up procedure to set the correct modem TX output level. When doing so, the terminal transmits a modulated signal or pure carrier. This signal can only be picked up and measured at the network hub site when the terminal is correctly installed and the antenna properly pointed.

5.2.8.1 Installation Carrier Parameters



Installation Carrier	Description
Carrier Mode	Select which type of carrier the modem needs to send out: • Pure carrier • CPM Carrier • HRC Carrier • MRC Carrier • ULOGON carrier
RF Transmit Frequency	Set the frequency of the outgoing transmitted carrier in GHz. This is a value between 3 and 31 GHz.
Duration	Specify how long the modem needs to transmit the carrier. This is a value between 10 and 1800 seconds.
Output Power	Set the output power level of the installation carrier. This is a value between -50 and +5 dBm. Typically this value depends on the used outdoor unit, RF cable length and satellite.
Ignore Forward Lock	Use this check box to transmit the installation carrier even if there is no forward link synchronization.
Active State	**Description**
Modem State	The test is only possible in case the modem state is: • Synchronized • Network Login • Operational
Carrier State	This indicates the status of the test: • Transmitting. • Transmit Possible, Not Active. • Transmit Not Possible, Not In Correct State; this means the Modem State does not allow to start the test.
Error State	• If the test is not possible due to an incorrect modem state, the corresponding modem error state will be displayed. • If the test is started while transmit is not possible, or the test fails for another reason, the message “Error 999 - Installation carrier setup failed” will be displayed.
Frequencies	**Description**
RF Receive Frequency	Displayed during installation carrier on which carrier the terminal is receiving and on which RF frequency. ***Note** - This information is also displayed in other sections of the user interface of the terminal, but to facilitate installation, this information is also displayed on this location.*
IF Receive Frequency	Displayed during installation carrier on which carrier the terminal is receiving and on which IF-Band. ***Note** - This information is also displayed in other sections of the user interface of the terminal, but to facilitate installation, this information is also displayed on this location.*
RF Transmit Frequency	Displayed during installation carrier on which carrier the terminal is transmitting and on which RF frequency.

	***Note** - This information is also displayed in other sections of the user interface of the terminal, but to facilitate installation, this information is also displayed on this location.*
IF Transmit Frequency	Displayed during installation carrier on which carrier the terminal is transmitting and on which IF-band. ***Note** - This information is also displayed in other sections of the user interface of the terminal, but to facilitate installation, this information is also displayed on this location.*

5.2.8.2 Start Carrier Test

This test mode can only be activated when the terminal has found the satellite network and is able to synchronize with the satellite network clock (NCR signal). However this can be bypassed using the **Ignore Forward Lock** check box. The test mode will interrupt the normal terminal operation. After a (configurable) timeout or a manual stop, the test mode is ended and the normal operational mode restored.

To start transmitting the carrier:

1. Enter the correct values for the Installation Carrier.
2. Click Start New to validate the entered values and start the test. If another test is still ongoing, it will be interrupted.
3. Optionally, you can click Stop Active to manually stop the test. If you do not click this button, the test will automatically stop when the test duration has expired.

6 Troubleshooting

This chapter describes some possible error scenarios that users can encounter during the installation or operation of the ST Engineering iDirect terminal, as well as the possible solutions for these error conditions. If a problem persists, please contact your service provider for assistance.

6.1 Possible Issues during Installation

Error Message	Issue	Possible Solutions
On Terminal Installation interface: ODU and Beam ID combination invalid. Please select another Beam ID	The frequency of the initial receive carrier and/or pointing carrier of the selected beam are outside the frequency range defined for the selected outdoor unit. For example, a Ku-band outdoor unit is selected in combination with a Ka-band spot beam.	• Select the correct spot beam or restart the installation to select the correct outdoor unit. • Make sure the frequency of the initial receive carrier and/or pointing carrier of the selected beam is within the frequency range defined for the selected outdoor unit.
On Terminal Installation interface, Antenna Pointing: Modem Status: No lock on Satellite You keep hearing a low pitch tone through the Point&Play tool.	There may not be a clear line of sight between the antenna and the satellite. The pointing carrier may not be correct or the beam was not correctly selected.	• Check if there is a clear line of sight and no building, tree or other obstruction is blocking the path between the antenna and the satellite. Select a place with clear line of sight to set up the antenna. • Check is your compass is functioning correctly • Try the other pointing carrier if two pointing carriers are available • Check with your Service Provider if the pointing carrier setting are still correct. • If the problem persists, you might have selected an incorrect beam.
On Terminal Installation interface, Antenna Pointing: Modem Status: Wrong Satellite You keep hearing a low pitch tone through the Point&Play tool.	The antenna may not be correctly pointed.	• Point the antenna correctly.
On Terminal Installation interface, Validate Installation: Terminal location not listed	The location of your terminal is not displayed during the first step of the validation procedure.	• Check there is no typing mistake in the entered address. • Check that enough address details are given.
On Terminal Installation interface, Validate Installation: Express the latitude/longitude in one of the following ways. As a range from 0 to 90 indicating N and S (for example 41.24N) or in a range between -90 and 90 (for example 41.24)	An incorrect notation is used.	• Check that the following notation rules are applied: – A dot must be used as separator, not a comma – The hemisphere needs to be specified: • Positive longitude value = EAST • Negative longitude value = WEST • Positive latitude value = NORTH • Negative latitude value = SOUTH
On Terminal Installation interface, Validate Installation: Location is invalid for the beam.	Incorrect address or wrong beam has been selected	• Check the address selected is correct. • Check the beam selected is correct.

On Terminal Installation interface, Validate Installation: Certification Result Status: Aborted (Unknown ODU type)	The outdoor unit which was selected on the modem has an ID which is unknown by the hub.	• Check if the selected ID is correct • Contact your Service Provider if this error persists.
Installation Failed. Error Message Code 010 No demodulator lock. Modem LED is red LED error indication: The RX indicator LED is off.	Error in handling of the Rx signal. The Rx demodulator cannot lock. The modem is not receiving any input signal.	• Verify the pointing of the antenna. • Verify the connectivity between the modem and the antenna. • Verify the configuration of the satellite interface parameters: frequency, polarization, symbol rate. • Check with satellite operator that the forward carrier is in the air.
Installation Failed. Error Message Code 020 Terminal specific forward carrier lookup is ongoing. LED error indication: Warning LED is on, RX LED is on	The modem is determining on which traffic carrier it is provisioned.	• If the message does not disappear within 10 minutes, take a copy of Diagnostic Report and reset the modem. For more information, refer to Diagnostics Report on page 79. • Contact your Service Provider, if the problem still persists, to check if your modem is provisioned in the network.
Installation Failed. Error Message Code 030 Network lookup failed. LED error indication: Warning LED is on, RX LED is on.	The outdoor unit which was selected on the modem has an ID which is unknown by the hub.	• Check if antenna is pointed to a correct satellite. • Verify the configuration of the satellite interface: if the pointing data is correct. • Take copy of Diagnostic report and Reset the modem. For more information, refer to Diagnostics Report on page 79. • Contact the Service Provider if this error is persistent for more than four hours.
Installation Failed. Error Message Code 040 LED error indication: Warning LED is on, RX LED is on	The time synchronization process failed. The modem can physically lock in the forward carrier but it does not complete the synchronization. The error can be an indication of a general network problem.	• Take a copy of Diagnostic Report and reset the modem. For more information, refer to Diagnostics Report on page 79. • Contact your Service Provider if this error is persistent for more than four hours.
Installation Failed. Error Message Code 045 Synchronization lost. LED error indication: Warning LED is on, RX LED is on.	The time synchronization is lost.	• Take a copy of Diagnostic Report and reset the modem. For more information, refer to Diagnostics Report on page 79. • Contact your Service Provider if this error is persistent for more than four hours.
Installation Failed. Error Message Code 050 Error information on the modem. LED error indication: Warning LED is on, RX LED is on.	The modem could not login to the satellite.	• Verify if the TX cable is correctly connected. • If the error is still occurring after a number of hours, contact your Service Provider to report the problem and to check if your modem is provisioned in the network.
Installation Failed. Error Message Code 055 Network Layer configuration failed.	This error means that an error occurred during the configuration of the network layers after a valid satellite network login.	• Take a copy of Diagnostic Report and reset the modem. For more information, refer to Diagnostics Report on page 79.

LED error indication: Warning LED is on, RX LED is on.		• Contact your Service Provider if this error persists, and provide them with any additional error information displayed.
Installation Failed. Error Message Code 060 TCP acceleration service failed. LED error indication: Warning LED is on, RX LED is on.	This error means that an error occurred during the configuration of the network layers after a valid satellite network login.	• Take a copy of Diagnostic Report and reset the modem. For more information, refer to Diagnostics Report on page 79. • Contact your Service Provider if this error is persistent for more than four hours.
Installation Failed. Error Message Code 070 Network connectivity lost. LED error indication: Warning LED is on, RX LED is on.	The connectivity with the satellite network is lost.	• Take a copy of Diagnostic Report and reset the modem. For more information, refer to Diagnostics Report on page 79. • Contact your Service Provider if this error is persistent for more than four hours.
Installation Failed. Error Message Code 999 Installation carrier setup failed. LED error indication: Warning LED is on, RX LED is on.	The activation of the installation carrier test mode failed because the modem was not in the correct state.	• Run again the installation
Installation Failed. Error Message Code 999 ODU configuration is not correct. LED error indication: Warning LED is on, RX LED is on.	The modem does not accept the ODU configured: ODU and Beam selected result into a non valid frequency band. Reception or Transmission frequency resulting of the current forward carrier and ODU selected result into a carrier out of range in Rx S-band or L-band) or Tx (L-band).	• Review the ODU configuration.

6.2 Possible Issues during Operation

Issue	Checklist
Cannot browse in Internet.	• Try rebooting the modem. • Is the modem reachable? Ping the modem. • Is the modem directly connected to the PC, or is it there a switch or router in between? Try to connect your modem directly to your PC. • Is the terminal properly installed? Verify the receive EsN0 level. • Is DHCP enabled on the PC behind? If not, enable it. • Ping the modem IP, edge router and DNS (for example, 8.8.8.8). If the DNS is reachable but you cannot browse, there could be a DNS issue. • If the issue persists, contact your service provider. The service provider will find it useful that you provide them with the following information: • The diagnostic report, which you can download from the Terminal GUI. For more information, refer to Diagnostics Report on page 79. • The LED status of the modem. In a functioning terminal the Tx, Rx and Network LEDs should be green. • The context of the issue. When did the problem appear?
Unsatisfying browsing experience.	• Try rebooting the modem. • Is the modem directly connected to the PC, or is it there a switch or router in between? Try to connect your modem directly to your PC. • Is terminal GUI Ethernet LED green? If not, there can be an Ethernet connection issue. • Try surfing in another web. If that one works, it could be a website issue. If the issue persists, contact your service provider. The service provider will find it useful that you provide them with the following information: • The diagnostic report, which you can download from the Terminal GUI. For more information, refer to Diagnostics Report on page 79. • The LED status of the modem. In a functioning terminal the Tx, Rx and Network LEDs should be green. • The context of the issue. When did the problem appear?
VoIP calls do not work	• Try rebooting the modem. If the issue persists, contact your service provider. The service provider will find it useful that you provide them with the following information: • The diagnostic report, which you can download from the Terminal GUI. For more information, refer to Diagnostics Report on page 79. • The context of the issue. When did the problem appear?
Multicast connections do not work.	• Try rebooting the modem. • Is the modem directly connected to the PC, or is it there a switch or router in between? Try to connect your modem directly to your PC. If the issue persists, contact your service provider. The service provider will find it useful that you provide them with the following information: • The diagnostic report, which you can download from the Terminal GUI. For more information, refer to Diagnostics Report on page 79. • The LED status of the modem. In a functioning terminal the Tx, Rx and Network LEDs should be green • The context of the issue. When did the problem appear?

7 Appendix A - Acronyms

Acronym	Definition
AC	Alternating Current
ACM	Adaptive Coding Modulation
ACU	Antenna Control Unit
AIBS	Automated Initial Beam Selection
APSK	Amplitude Phase Shift Keying
ASN	Abstract Syntax Notation
BUC	Block Up Converter
CCM	Constant Coding Modulation
CE	Conformité Européenne
CNI	Carrier to Noise Interference
CPE	Customer Premises Equipment
CPM	Continuous Phase Modulation
DC	Direct Current
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DVB-S	Open standard for Digital Video Broadcasting over Satellite
DVB-S2	Improved version of DVB-S standard
FPGA	Field-Programmable Gate Array
GHz	GigaHertz
GUI	Graphical/Graphics User Interface
GXT	File format used for satellite beam contour data (according ITU standard)
HTTP	Hyper Text Transfer Protocol
ID	Identifier
IF	Intermediate Frequency
IGMP	Internet Group Management Protocol
IP	Internet Protocol (IETF)
LAN	Local Area Network
LED	Light Emitting Diode
LNB	Low Noise Blocker
LO	Local Oscillator

Acronym	Definition
MAC	Media Access Control (IEEE 802)
MHz	MegaHertz
MIB	Management Information Base
MODCOD	Modulation and Coding scheme
MODEM	Modulator/Demodulator
NCR	Network Clock Reference
NMS	Network Management System
ODU	Outdoor Unit
OID	Object Identifier
PC	Personal Computer
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying (DQDB)
RF	Radio Frequency
RX	Receive
SNMP	Simple Network Management Protocol
TCP	Transport Control Protocol
TFTP	Trivial File Transfer Protocol
TX	Transmit
UDP	User Datagram Protocol (IETF)
URL	Universal Resource Locator (WWW)
USB	Universal Serial Bus

8 Appendix B - Licenses

GNU software is used in this product:

You can download GNU Wget from the following location:
http://www.gnu.org/software/wget/

9 Appendix C - Modem Configuration File

The out-of-band configuration feature allows you to configure the modem from an external server located outside the Dialog platform. This appendix describes the modem configuration file format.

The modem will ignore any configuration that is not supported.

General

The modem remote configuration is a zip file with the following content:

Type	Location	Name	Description
file	\	config.json	The modem configuration in JSON format.
directory	\	gxt	Optional directory that conatins GXT files.
file	\gxt	<filename>.gxt	GXT files referenced by config.json file.

Configuration File Format

The config.json file contains the modem configuration in JSON format as described below:

```
{
      "FileFormatVersion": 2,
            //Optional. Used to prevalidate the configuration file.
      "SatelliteConfiguration": SatelliteConfiguration,
            //Optional. Description of spot beams from which the modem can
            acquire the network and to which they can switch while moving.
      "Miscellaneous": Miscellaneous
            //Optional. Contains modem configurations that are not remotely
            manageable.
      "CandidateConfirmationTimeout": Number
            //Optional. Represents the number of seconds that shall be
            waited for the candidate configuration before it rolls back to
            the previous configuration. If missing the default(2h) will be
            used to wait.
      "CandidateConfirmationTimeoutEnabled": Boolean
            //Optional. Used to disable the candidate confirmation timeout.
      "CandidateConfirmationEnabled": Boolean
            //Optional. Used to enable/disable the candidate try/rollback
            mechanism . If disabled the candidate will be accepted
            immediately after the pre-validation is passed. If missing the
            try/rollback mechanism is enabled by default.
}
```

OBJ SatelliteConfiguration

```
{
      "SatelliteConfigurationVersion": Number,
            // Unique identifier of the configuration. Changing the
            configuration settings without generating a new version might
            cause the terminal to ignore the update. A good idea is to
            generate the version based on a hashing alghorithm applied on
            the values.
      "Beams": Array[Object[Beam]]
            // List of described spot beams.
}
```

OBJ Beam

```
{
      "BeamId": Number,
            // Unique beam identifier within the list of beams. It is the
            key to reference the beam from other configurations (e.g.
            installation) but not GXT files, which usese the BeamName
            field.
      "InitialCarrier1": Object[Carrier],
            // Initial receive carrier through which the modem will try to
            gain access to the network. After failing during a preset time,
            the alternate InitialCarrier2 data will be used, if enabled.
      "InitialCarrier2": Object[Carrier],
            // Alternate initial forward carrier data. Used for cases like
            redundancy and forward carrier migration. It can be disabled by
            settung the 'Enabled' inner field to false.
      "DefaultInitialCarrier": Number,
            // Optional index for specifying the default initial carrier (1
            or 2). If missing, InitialCarrier1 is default.
      "PointingCarrier1": Object[PointingCarrier],
            // Pointing carrier used for initial antenna (manual or
            automatic) pointing. It can be the same as the initial carrier.
      "PointingCarrier2": Object[PointingCarrier],
            // Alternative carrier used for antenna pointing. It can be
            disabled by settung the 'Enabled' inner field to false.
      "DefaultPointingCarrier": Number,
            // Optional index for specifying the default pointing carrier
            (1 or 2). If missing, PointingCarrier1 is default.
      "OrbitalDegrees": Number,
            // Orbital position of the satellite in degrees(float). Valid
            values 0-360°.
      "Hemisphere": String,
            // "east" or "west" Satellite position.
      "PolarizationSkew": Number,
```

```
        // Skew angle in degrees applied by the satellite operator
        (signed, float). Valid values 0-360°.

    "SatLatitudeVariance": Number,

        // Value in degrees which is typically used for inclined orbit
        satellites. Only applicable in case of automatic pointing.
        Valid values 0-360°.

    "TxPolarization": Number,

        // Polarization of the return carrier: 0 horizontal, 1
        vertical, 2 circular left, 3 circular right.

    "BeamName": String,

        // Name of the beam as referenced from the associated GXT file.
        It is a 4 (or 8, depending on GXT version) char array.

    "Cost": Number,

        // Value used by the terminal when it can choose to operate in
        multiple beams. The beam with the lowest cost value is then
        selected.

    "AutomaticPointingTimeout": Number,

        // Time interval after which a terminal returns to the
        automatic beam selection procedure (if the terminal can not
        lock on the received forward link).

    "GxtFileName": String,

        // Name of the GXT file containing the beam's contours.

    "ExclusionZones": Array[Object[ExclusionZone]],

        // Area in which a terminal is not allowed to operate.

    "AcuXString": String,

        // Freeform string containing the extra hunt parameters (X)
        when using the OpenAMIP protocol.

    "MaxSkew": Number,

        // Maximum skew angle to be sent to antenna (K) in degrees,
        float. Valid values 0-360°.

    "TxFrequency": Number,

        // Hz, unsigned 64 bit integer. Will overrule the Tx Frequency
        sent to the ACU (only if > 0 and TxBandwidth also > 0). RF
        frequency, converted to LBand if needed

    "TxBandwidth": Number

        // Baud, unsigned 64 bit integer. Will overrule the Tx
        Bandwidth sent to the ACU (only if > 0 and TxFrequency also >
        0)

}
```

OBJ PointingCarrier

```
{

    "Carrier": Object[Carrier]

}
```

OBJ Carrier

```
{
      "Enabled": Boolean,
            // Flag to specify if carrier data is valid and can be used
            (true) or invalid and to be ignored (false).
      "TSMode": String,
            // One of: dvbs, dvbs2_ccm, dvbs2_acm, dvbs2x or
            dvbs2x_timesliced
      "TimeSliceNumber": Number,
            // The primary TSN for the virtual carrier, from 1->62, only
            parsed in case TSMode == dvbs2x_timesliced
      "Freq": Number,
            // Expressed in Hz, internally stored with a granularity of 100
            Hz, unsigned 64 bit integer. Valid values 0-100 GHz
      "SymbolRate": Number,
            // Expressed Baud, unsigned 64 bit integer. Valid values 0.1
            Mbaud - 133 Mbaud.
      "Polarization": Number
            // Carrier polarization: 0 horizontal, 1 vertical, 2 circular
            left, 3 circular right
}
```

OBJ ExclusionZone

```
{
      "ServiceArea": Number,
            //The service area number in the GXT file corresponding to the
            exclusion zone.
      "RxAllowed": Boolean,
            //Flag to specify if the terminal is allowed to receive in the
            given exclusion zone.
      "TxAllowed": Boolean,
            //Flag to specify if the terminal is allowed to transmit in the
            given exclusion zone.
      "EIRP0max": Number,
            //See GXT file. Optional, default 0.0, for future use.
      "MinAlt": Number,
            //Lower limit of the altitude of the exclusion zone. Optional,
            default 0, for future use.
      "MaxAlt": Number
            //Upper limit of the altitude of the exclusion zone. Optional,
            default 0, for future use.
}
```

OBJ Miscellaneous

```
{
      Id: Number,
            // Unique identifier of the configuration. Changing the
            configuration settings without generating a new version might
            cause the terminal to ignore the update. A good idea is to
            generate the version based on a hashing alghorithm applied on
            the values.
      InstallationConfiguration: Object[InstallationConfiguration],
            // Settings for the installation state.
      OduConfiguration: Object[OduConfiguration],
            // Settings for the outdoor unit equipment.
      PointingConfiguration: Object[PointingConfiguration],
            // Settings for the antenna pointing strategy.
      MulticastConfiguration: Object[MulticastConfiguration],
            // Multicast settings.
      GeneralConfiguration: Object[GeneralConfiguration]
            // General settings.
      NetworkConfiguration: Object[NetworkConfiguration]
            // Network settings.
      CustomizationConfiguration: Object[CustomizationConfiguration]
            // Customization settings.
}
```

OBJ InstallationConfiguration

```
{
      "AIBSEnabled": Boolean,
            //Flag whether AIBS should be used, both during installation
            and (non)operational mode.
      "ActiveBeam": Number,
            //Optional if AIBS is enabled. Otherwise, active beam must be
            one of the defined beam ids in SatelliteConfiguration.
      "SelectedOduConfiguration": Number,
            //Selected ODU configuration must be one of the defined ODU
            configurations.
      "ForceAcuConfigurationEnabled": Boolean,
            //If enabled, the next installation will force sending the
            configuration parameters to the ACU, even if none have changed.
      "PointingStatus": Boolean
            //Optional. If automatic pointing is disabled, setting the
            pointing status to false will force going back to the unpointed
            state.
```

```
}
OBJ OduConfiguration
{
      "OduConfigurationDataStore": Array[Object[OduType, OduData]],
            //List of Odu configuration descriptions.
}
OBJ OduType
{
      "Id": Number,
            //Unique identifier of the configuration. (1-64)
      "Description": String
            //Short description of the configuration, to be displayed in
            modem GUI.
}
OBJ OduData
{
      "ToneSelection": String,
            //Used to inform the LNB about band selection through a 22KHz
            tone. Check LNB datashet if supported. Possible values: "off",
            "on" and "band"
      "VoltageSelection": String,
            //Used to inform the LNB about band/polarization selection
            through voltage value. Band selection can be either tone based
            or voltage based, not both at the same time. Check LNB
            datasheet if supported. Possible values: "off", "13v", "18v",
            "band" or "polarization"
      "PolarizationStackingOffset": Number,
            //Optional offset between the LBand frequencies of data
            received by a stacking antenna on different polarization at the
            same time. VoltageSelection must not be set to "polarization"
            for it to work.
      "LowBand": Object[BandData],
            //Description of the: Band in single band mode / Lowband in
            dual band mode / first Band in multi band mode.
      "HighBand": Object[BandData],
            //Description of the HighBand in case of dual band
            (tone/voltage based band selection)
      "ExtraLNBBands": Array[Object[BandData]],
            //Optional description of extra bands in case of multi-band.
            HighBand is not taken into consideration in this case.
      "TransmitterType": String,
            //Selects the UpConverter type: "buc" (block) or "muc" (multi)
```

```
"BUCData": Object[BandData],

     //Description of BlockUpConverter (optional, but one of BUCData
     or MUCData must be described).

"MUCData": Object[MucData],

     //Description of MultiUpConverter (optional, but one of BUCData
     or MUCData must be described).

"LnbTXMin": Number,

     //Minimum allowed current on the Transmit interface. Used for
     passing the current measurement test. Valid values 0-50000 mA.

"LnbTXMax": Number,

     //Maximum allowed current on the Transmit interface. Used for
     passing the current measurement test. Valid values 0-50000 mA.

"LnbRXMin": Number,

     //Minimum allowed current on the Receive interface. Used for
     passing the current measurement test. Valid values 0-50000 mA.

"LnbRXMax": Number,

     //Maximum allowed current on the Receive interface. Used for
     passing the current measurement test. Valid values 0-50000 mA.

"PoweroffTimeout": Number,

     //Timeout in seconds.

"TxDcOutput": String,

     //When enabled, the modem will provide power to the BUC. Make
     sure to disable the DC output voltage when using a BUC that is
     externally powered! Possible values: "off", "on", "24v" or
     "48v".

"ElevationOffset": Double,

     //The delta in degrees between the antenna real elevation and
     the elevation of the reference plane to which the smartphone
     will be placed for the elevation measurement. This offset is
     different for different antenna types.

"ReflectorType": String,

     //Reflector type: single-offset, cassegrain-offset,
     gregorian-offset, single-prime-focus, cassegrain-prime-focus or
     gregorian-prime-focus.

"LinearPolarizationIndication": Double,

     //This indicates the mid-range value of the feed reading range
     (e.g. 0 degrees for -45->45).

"PositiveFeedReading": String,

     //"clockwise" or "counterclockwise".

"FeedReadingWhenRxHor": Double,

     //For future use.

"BucReferenceClock": String,
```

```
            //Enable reference synchronization signal to be sent to Buc.
            Possible values: "off", "10MHz" or "50MHz".

      "LnbReferenceClock": String,

            //Enable reference synchronization signal to be sent to Lnb.
            Possible values: "off" or "10MHz".

      "BucModemSynced": Boolean,

            //Enable Buc synchronization with modem.

      "SingleCoax": Boolean

            //Single coaxial cable option for the iLNB connection.

}
```

OBJ BandData

```
{
      "L0": Number,

            //The Local Oscillator frequency in Hz. Valid values 3 - 30
            GHz.

      "RFStart": Number,

            //Begin frequency of the supported transmit range in Hz. Valid
            values 3 - 30 GHz.

      "RFStop": Number

            //End frequency of the supported transmit range in Hz. Valid
            values 3 - 30 GHz.

}
```

OBJ MucData

```
{
      "Multiplicator": Number,

            //The multiplication factor the MUC is using. Valid values
            1-1.000.000

      "RFStart": Number,

            //Begin frequency of the supported transmit range in Hz. Valid
            values 3 - 30 GHz.

      "RFStop": Number

            //End frequency of the supported transmit range in Hz. Valid
            values 3 - 30 GHz.

}
```

OBJ PointingConfiguration

```
{
      "Jitter": Number,

            // Max drop in SNR before generating pulsed tone, expressed in
            0.1 dB.

      "AutomaticPointingEnabled": Boolean,

      "AutomaticPointing": Object[AutomaticPointing]
```

```
            // Mostly contains parameters for the OpenAMIP protocol.
}
OBJ AutomaticPointing
{
      "ACUAddress": String
            // The ip address of the ACU. It should be in the same subnet
            as the local management address of the modem.
      "ACUPort": Number
            // The tcp port of the ACU.
      "TimeoutRequested": Number
            // The timeout in seconds that will be sent to the ACU. Valid
            values 5 sec - 15 sec.
      "TimeoutTolerance": Number
            // Timeout tolerance in seconds. If the modem does not receive
            the GPS coordinates within this time interval, the modem
            switches back to pointing mode. Valid values 1 sec - 120 sec.
      "UseLBand": Boolean
           // Indicates if the frequencies sent to the ACU should be
           converted to L-band.
}
OBJ MulticastConfiguration
{
      "Mode": String, // "disabled", "static", or "igmp_dynamic"
            // Disabled: Multicast mode is disabled.
            // Static: The active Multicast Configuration is based on
            entered Static Multicast IP Addresses.
            // IGMP Dynamic: Dynamic IGMP multicast mode.
      "StaticAddresses": Array[String] // A naximum of 10 multicast IP
      Addresses can be assigned and active in case of Static Multicast
      Mode.
}
OBJ GeneralConfiguration
{
      "Mobility": Object[Mobility],
            //Optional. Mobility feature is disabled if missing.
      "SNMPAgent": Object[SNMPAgent],
            //SNMP related parameters.
      "ReferenceClockConnectorMode": Number,
            //Usage mode for ReferenceClock connector. Can be "off",
            "input" (salve) or "output" (act as 10MHz master clock)
      "NCRTimeout": Number,
```

```
            //Timeout (in ms) for NCR reception, after which the terminal
            will re-synchronize.

      "NITTimeout": Number

            //Timeout (in ms) for NIT reception (when NIT is expected).

}
```

OBJ Mobility

```
{
      "RxLockMonitorEnabled": Boolean,

            //If enabled, mobile terminals will disable Tx when they detect
            a loss of forward lock.

      "SendCoordinatesToDMMEnabled": Boolean,

            //If enabled, mobile terminal will periodically send the
            coordinates to DMM.

      "SendCoordinatesToDMMInterval": Number,

            //The interval, in seconds, with which to send the terminal's
            position to the DMM.

      "LogCoordinatesEnabled": Boolean,

            //If enabled, will also log the coordinates in the log.

      "LogCoordinatesInterval": Number,

            //The interval, in seconds, with which to log the coordinates.

      "Eligibility": Object[MobilityEligibility]

            //Parameters that describe limits that make beam eligible for
            automatic beam selection or remote mobility management.

}
```

OBJ MobilityEligibility

```
{
      "MinimumSatelliteElevation": Number,

            //Minimum satellite elevation at the terminal's location,in
            degrees as float. Valid values 0°-90° .

      "MinimumBeamGain": Number,

            //Minimum beam gain at the terminal's current location,in dB as
            float.

      "MaximumSatelliteSkew": Number

            //Maximum satellite skew angle,in degrees as float. Valid
            values 0°-90°.

}
```

OBJ SNMPAgent

```
{
      "LocalManagementEnabled": Boolean,
```

```
            //Enable local SNMP management. If set to false, only
            over-the-air management is possible (requires operational
            modem)
      "ReadOnlyCommunityString": String,
            //Cummunity name for read only properties.
      "ReadWriteCommunityString": String,
            //Cummunity name for writable properties.
      "SysContact": String
            //Contact information regarding the managed node, e.g. e-mail
            address
      "SysName": String,
            //Adminsitrative information regarding the managed node, e.g.
            terminal name
      "SysAddress: String
            //Location information of the managed node, e.g. street address
}
OBJ CustomizationConfiguration
{
      "BrandingImageData": String,
            //Base64 ASCII string that represents the binary data of the
            image.
      "GUILanguages": Array[String],
            //List of languages that can be selected in the GUI, in IETF
            format.
      "GUIEditPermissions": Object[GUIEditPermissions],
            //Edit permissions per GUI page. Can be set to "normal" or
            "expert". Values get applied only after reboot.
      "AESEncryptionKeyLength": Number,
            //The AES key length used for encryption. Default value "56".
            Values get applied only after reboot.
      "DiffieHellmanKeyLength": Number
            //Timeout (in ms) for NIT reception (when NIT is expected).
            Values get applied only after reboot.
}
OBJ GUIEditPermissions
{
      "Satellite": String,
            //Applies to "Satellite Interface" page.
      "ODU": String,
            //Applies to "Outdoor Unit" page.
      "AutomaticPointing": String,
```

```
            //Applies to "Automatic Pointing" checkbox and related
            settings.
      "Multicast": String,
            //Applies to "Multicast" page.
      "Installation": String
            //Applies to "Installation" page.
}
OBJ NetworkConfiguration
{
      "WifiRemotelyManaged": Boolean,
      "Wifi": Object[Wifi]
      "IPSecRemotelyManaged": Boolean,
      "IPSec": Object[IPSec],
      "NATRemotelyManaged": Boolean,
      "NAT": Object[NAT],
      "IPv4FirewallRemotelyManaged": Boolean,
      "IPv4Firewall": Object[IPFirewall],
      "IPv6FirewallRemotelyManaged": Boolean,
      "IPv6Firewall": Object[IPFirewall]
}
OBJ Wifi
{
      "CountryCode": String,
      "2.4GHz": Object[WifiBand]
}
OBJ WifiBand
{
      "Enabled": Boolean,
      "Channel": Number,
      "TxPower": Number,
      "AccessPoints": Array[Object[AccessPoint]]
}
OBJ AccessPoint
{
      "SSID": String,
      "EncryptionKey": String,
      "Encryption": String,
```

```
            //one of "none", "wep-64", "wep-128", "wpa", "wpa-mixed" or
            "wpa2"
      "WPACypher": String,
            //one of "none", "tkip", "ccmp" or "tkip+ccmp"
      "WPS": Boolean
}
OBJ IPSec
{
      "Enabled": Boolean,
      "IkeSAs": Array[Object[IkeSA]]
}
OBJ IkeSA
{
      "Id": String,
      "Description": String,
      "IkeVersion": Number,
      "Aggressive": Boolean,
      "RemoteHost": String,
      "LocalSubnetPrefix": String,
      "DNS": String,
      "NatTraversal": Boolean,
      "DpdInterval": Number,
      "AuthMethod": String,
            //"psk" or "pubkey"
      "PskSecret": String,
      "LocalId": String,
      "RemoteId": String,
      "RekeyTime": Number,
      "Proposals": String,
      "IpsecSAs": Array[Object[IpsecSA]]
}
OBJ IpsecSA
{
      "Id": String,
      "RekeyTime": Number,
      "ReplayWindow": Number,
      "AhProposals": String,
      "EspProposals": String
```

```
}
OBJ NAT
{
      "Enabled": Boolean,
      "DHCPv4Range": Object[DHCPv4Range],
      "IPv4PortForwardings": Array[Object[IPv4PortForwarding]]
}
OBJ DHCPv4Range
{
      "Enabled": Boolean,
      "Start": String,
            //Start IP
      "Stop": String
            //Stop IP
}
OBJ IPv4PortForwarding
{
      "Description": String,
            //max 40 characters, optional
      "LocalIpAddress": String,
      "LocalPorts": String,
            //single port or range e.g. "5000" or "5000-5010"
      "PublicIpAddress": String,
      "PublicPorts": String,
            //single port or range e.g. "5000" or "5000-5010". Range size
            of source and destination ports must match.
      "Protocol": String
            //one of "tcp", "udp", "tcpudp"
}
OBJ IPFirewall
{
      "Enabled": Boolean,
            //IP v4 port forwarding and IP v4 firewall can be enabled
            exclusively only.
      "FirewallRules": Array[Object[FirewallRule]]
}
OBJ FirewallRule
{
```

```
      "Description": String,
      "SourceIpAddress": String,
      "SourcePorts": String,
      "DestinationIpAddress": String,
      "DestinationPorts": String,
      "Protocol": Number
}
OBJ ManagementConfiguration
{
      "EthernetInterfaceData": Object[EthernetInterfaceData],
            //Section that describes the interface between the modem and
            the local network.
      "LoggingData": Object[LoggingData]
            //Section that describes logging mode. Values get applied only
            after reboot.
}
OBJ EthernetInterfaceData
{
      "MgmtAddr": Object[IPv4Address],
            //IP address for modem management interface, including mask
            size. If not set, default value is 192.168.1.1/24.
      "DHCPEnabled": Boolean
            //Flag that enables or disables the DHCP server functionality
            of the native vlan. By default it is enabled, if not already
            remotely configured by TCS.
}
OBJ IPv4Address
{
      "Address": String,
            //IP address (e.g. 192.168.1.1)
      "Prefix": Number
            //Length of netmask (e.g. 24 for 255.255.255.0)
}
OBJ LoggingData
{
      "LoggingMode": String,
            //"local" for terminal only logging. "remote" for both local
            and remote logging, using the configured IP address + UDP port
      "LocalLogBufferSize": Number,
            //Number of KBytes used for the local log.
```

```
    "SyslogAddress": String,
        //IPv4 address used in remote log configuration.
    "SyslogPort": Number
        //UDP port used in remote log configuration.
}
```

ST Engineering iDirect (Europe)
Laarstraat 5
9100 Sint-Niklaas Belgium
+32 3 780 6500
wwww.idirect.net