User Guide

MDM5010 SCPC Satellite Modem

Release 1.1.0

Revision E

January, 2024

ST Engineering iDirect is a global leader in satellite communications (satcom) providing technology and solutions that enable its customers to expand their business, differentiate their services and optimize their satcom networks. Through the merger with Newtec, a recognized industry pioneer, the combined business unites over 35 years of innovation focused on solving satellite's most critical economic and technology challenges, and expands a shared commitment to shaping the future of how the world connects. The product portfolio, branded under the names iDirect and Newtec, represents the highest standards in performance, efficiency and reliability, making it possible for its customers to deliver the best satcom connectivity experience anywhere in the world. ST Engineering iDirect is the world's largest TDMA enterprise VSAT manufacturer and is the leader in key industries including broadcast, mobility and military/government.

Company Website: www.idirect.net | Main Phone EU +32 3 780 65 00 | Main Phone US +1 703 648 8002

Newtec Product Support: Email customersupport@idirect.net | Website www.idirect.net/support-and-training

Revision History

The following table shows all revisions for this document.

Revision	Revision Date	Revision Description
Revision A	March 2022	Initial document creation.
Revision B	August 2022	Updates to *Managing a Remote Device* section of the chapter *Managing the MDM5010 using the GUI*.
Revision C	September 2023	Updated to add info about -48 Vdc power supply option and AUPC feature
Revision D	October 2023	Removed mention of Carrier ID because it is unsupported on the MDM5010 in standalone mode.

Contents

About

Purpose

This document provides information about how to use the MDM5010 SCPC Satellite Modem.

Compliance Statement

The complete ST Engineering iDirect hardware product statements for the MDM5010 satellite modem are available in the following documents:

- Declaration of Conformity
- Compliance and Safety Guide

Safety Regulations

Please read the *Compliance and Safety Guide* carefully before you install and use the equipment. The guide is delivered with the equipment and can be found in the shipping box.

Getting Help

The ST Engineering iDirect Technical Assistance Center (TAC) and the iDirect Government Technical Assistance Center (TAC) are available to provide assistance 24 hours a day, 365 days a year. Software user guides, FAQs, installation procedures, and other documents that support ST Engineering iDirect and iDirect Government products are available on the respective TAC Web site.

ST Engineering iDirect

http://www.idirect.net | +1 703.648.8000 (North America) | +32 3 780 6500 (Europe)

ST Engineering iDirect TAC

https://support.idirect.net | +1 703.648.8151 | tac@idirect.net

Sales and Product Purchasing Information

+1-703.648.8000 | sales@idirect.net

iDirect Government
http://www.idirectgov.com | +1 703.648.8118

iDirect Government TAC
https://partnerportal.idirectgov.com | +1 703.648.8111 | tac@idirectgov.com

Document Conventions

The following conventions are used in this document.

NOTE - A statement or notification that adds to, emphasizes, or clarifies essential information of special importance or interest.

CAUTION: A statement that highlights an essential operating or maintenance procedure, practice, condition, or statement that if not strictly observed, may result in damage to or destruction of equipment, or a condition that adversely affects system operation.

WARNING - *A statement that highlights an essential operating or maintenance procedure, practice, condition or statement that if not strictly observed, may result in injury or death or long term health risks.*

1 Introduction

The *MDM5010 SCPC Satellite Modem User Guide* provides detailed information about operating the MDM5010 Satellite Modem in SCPC standalone mode.

In this chapter:

1.1 The MDM5010 Satellite Modem in Standalone Mode

The MDM5010 is multi-personality, meaning that can be used either as a dedicated SCPC standalone modem, or a flexible Dialog® VSAT modem.

When operating in SCPC standalone mode, the MDM5010 satellite modem is used for point-to-point and high data rate links. The MDM5010 allows service providers to increase the number of services or augment the customer base within the same bandwidth. The MDM5010 can work as a modulator, demodulator, or modem, and integrates seamlessly with terrestrial networks and equipment.The MDM5010 fully complies with the DVB-S2X standard, ensuring optimal efficiency for maximum service availability.

The MDM5010 supports the following features and technologies:

- FlexACM
- Bandwidth cancellation up to 113 Mbaud
- Multi-level quality of service
- OpenAMIP
- DVB-S2X; up to 220 Mbaud and 256APSK, resulting in 1.6 Gbps aggregate throughput
- High packet performance of 500,000 pps
- Multi-personality; the MDM5010 SCPC modem can be switched to a Dialog® VSAT modem.

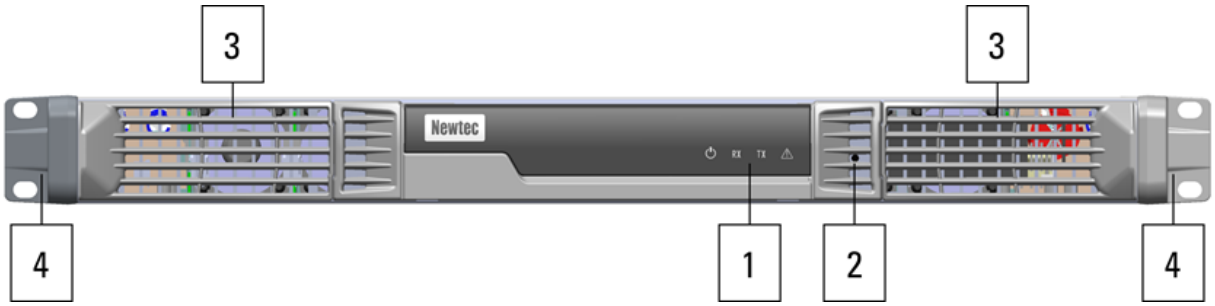
NOTE - The MDM5010 is always shipped as a Dialog® VSAT modem. To use the MDM5010 in SCPC standalone mode, the MDM5010 must switch personalities. This process is described in Switching to Dialog® VSAT Mode

NOTE - For more information about using the MDM5010 satellite modem in Dialog® VSAT mode, refer to the Dialog® documentation.

1.2 MDM5010 Hardware Features

The MDM5010 satellite modem supports the following hardware features.

1.2.1 Front View



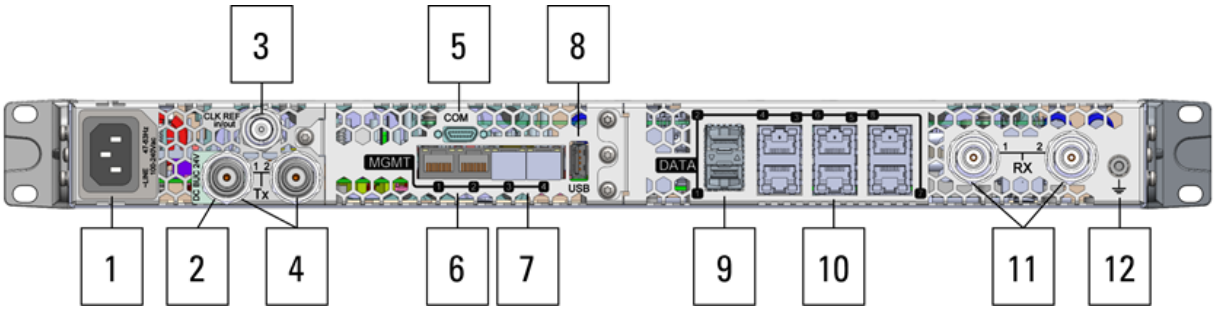
1 Notification LEDs

2 Reset button

3 Air inlets

4 Handles

1.2.2 Rear View



1 110/240 VAC power supply

2 [*Optional*] DC BUC power supply (24 VDC or 48 VDC)

3 Clock reference in- or output

4 Main (TX 1) and for future use (TX 2) female N-type connectors for L-band transmission (50 Ohm)

5 [*For future use*] RS-232 craft interface (COM)

6 Two RJ45 ports for management access (MGMT 1 and MGMT 2)

7 [*Not used*] Two RJ45 ports

8 [*For future use*] Standard USB 3.0 Type A port

9 Two 1G SFP+ ports for data in- and output (DATA 1 and 2)

10 Six RJ45 ports for data in- and output (DATA 3 to 8)

11 Main (RX 1) and for future use (RX 2) female N-type connectors for L-band reception (50 Ohm)

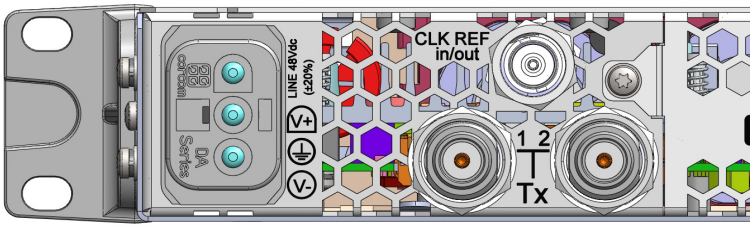
12 Grounding stud

1.2.3 DC Power Supply (Hardware Option)

The MDM5010 can also be equipped with a single DC Power Supply Unit -48 VDC (Range: 38 to 58 Vdc) ; Max power 152 W. Please contact your ST Engineering iDirect account representative for ordering information.

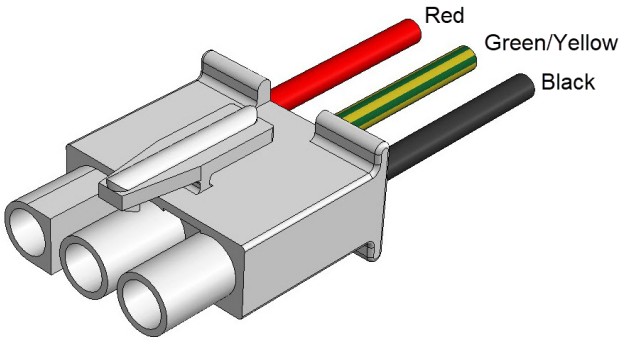
NOTE - The DC Power supply is mutually exclusive with the AC power connector and with the 24 V and 48 V DC BUC options.

When the DC power connector is installed the rear panel looks as follows:



The mating connector is a custom connector assembly with 3, 36" long 18 gauge wires to mate with the DC power connector and is shown below.

Refer to Powering the MDM5010 for connection diagrams.



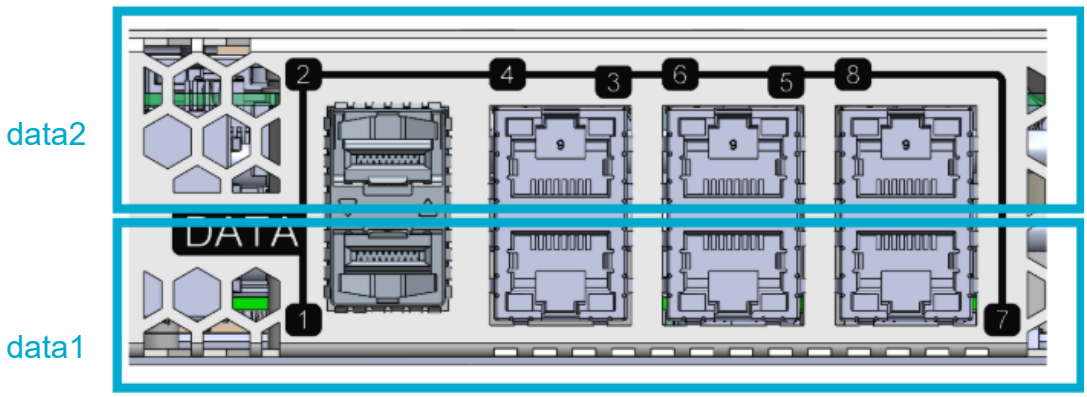
1.3 Data Interfaces

The MDM5010 has two optical and six Ethernet DATA ports. These physical ports are grouped into the following logical data interfaces:

- Logical interface *data1* consists of DATA ports 1, 3, 5, and 7
- Logical interface *data2* consists of DATA ports 2, 4, 6, and 8

Within each logical interface group, the ports behave as a hub.

NOTE - When these ports are connected to a switch, use the Spanning Tree Protocol (STP) to prevent bridge loops. STP ensures that only one port within the hub is actively forwarding data, while all other ports in the hub are disabled to prevent redundancy and network issues.



A logical interface can have one of three link states:

When state is...	Then...
off ( )	the logical port is administratively down. All corresponding physical ports are administratively down as well.
ok ( )	the logical port is administratively up. All corresponding physical ports are administratively up as well, and at least one port is without alarm.
in alarm ( )	all physical ports are in alarm. As soon as one port is OK, the alarm is cleared.

NOTE - Devices connected to the SFP+ ports should support 1G link speeds. If multiple negotiation speeds are supported, make sure that auto-negotiation is disabled, and set the speed to 1G.

1.4 Notification LEDs

The notification LEDs are used to visually indicate the status of the MDM5010.

1.4.1 Front Panel LEDs

The MDM5010 has the following notification LEDs on the front panel:

If LED...	Is *on* then...	Is *off* then...
Power ⏻	the MDM5010 is powered.	the MDM5010 is not powered.
RX	the MDM5010 successfully receives the downlink carrier.	the demodulator has no physical layer (PL) lock or has been disabled.
TX	the MDM5010 is transmitting the uplink carrier.	the MDM5010 is not transmitting. Transmit can be disabled because of an alarm, because the MDM5010 is the standby modem in a redundant setup or can be disabled manually.
Warning ⚠	one or more alarms are active. Use one of the control interfaces to view the active alarms, see Control Interfaces.	there are no alarms on the MDM5010..

1.4.2 Rear Panel LEDs

The MDM5010 has the following notification LEDs on the rear panel:

If...	Is *on* then...	Is *blinking* then...	Is *off* then...
green LED at top of RJ45 port	the link is up.	data is being transmitted.	the link is down.
orange LED at top of RJ45 port	the link operates as a Gigabit connection.	NA	the link does not operate as a Gigabit connection.
LED at SFP+ port	the link is up.	data is being transmitted.	the link is down.

1.5 Control Interfaces

The MDM5010 SCPC Satellite Modem has several control interfaces:

- Graphical User Interface
- REST Application Programming Interface
- Command Line Interface
- SNMP Interface
- SCP Interface

1.5.1 Graphical User Interface

The graphical user interface or GUI provides a visual-based and intuitive interface for controlling the MDM5010.

To access the GUI, browse to the management IP address of the MDM5010 using HTTP. GUI access is enabled by default. To restrict access, see Controlling Access.

There are two user levels:

- The guest user has read-only access; the default login password is *guestguest*.
- The expert user has read-write access; the default login password is *expertexpert*.

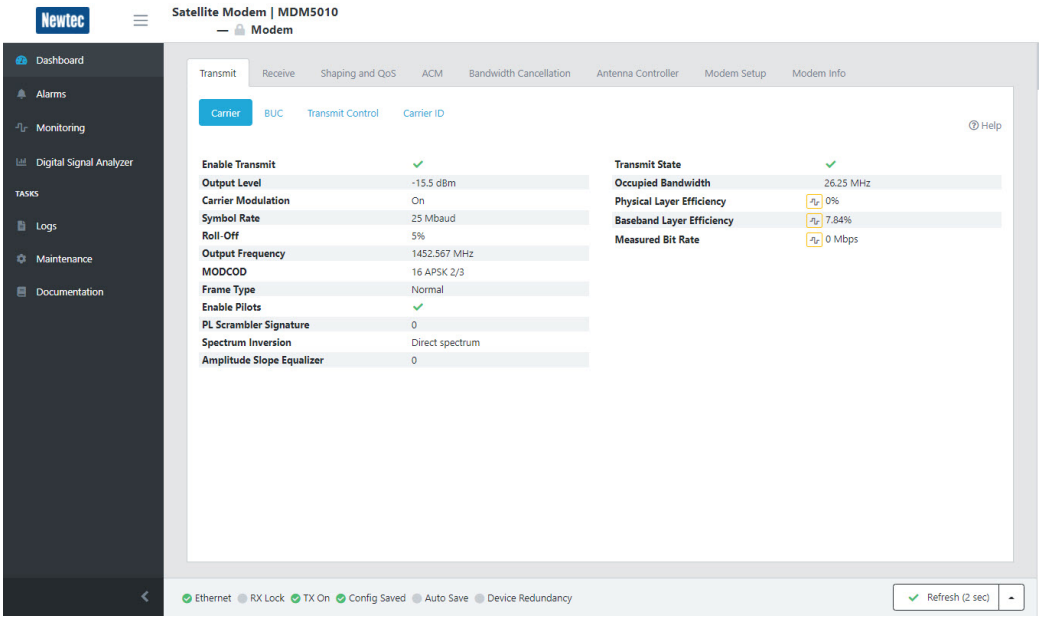
NOTE - Make sure your local computer can reach the management IP address of the MDM5010.

Use one of the following browsers:

Browser	Version
Chrome	latest
Firefox	latest and extended support release (ESR)
Edge	two most recent major versions
Safari	two most recent major versions

CAUTION: When GUI access is enabled, make sure to change the default passwords. For more information, see Changing Login Passwords.

The GUI screen, logged in as guest user and with an example transmit carrier, is shown below:



For more information about accessing the MDM5010, see Accessing the MDM5010.

For more information about using the GUI, see Managing the MDM5010 via the GUI.

1.5.2 REST Application Programming Interface

The REST Application Programming Interface or API enables you to fully control the MDM5010 using REST API calls. The REST API provides a higher level of functionality and granular control compared to the Graphical User Interface. In addition, it can be used for scripting or creating your own control software.

An API is a set of definitions and protocols for building and integrating application software. REST or Representational State Transfer determines how the API looks like. It provides an architectural style using a subset of HTTP.

Use a REST API client application to connect to the management IP address of the MDM5010 (server) and execute the REST queries. The queries must be done as *expert* user. The default password is *expertexpert*.

NOTE - Commonly used REST API client applications are Postman as a standalone app, and cURL as a command line utility (Linux).

NOTE - Make sure your local computer can reach the management IP address of the MDM5010.

NOTE - REST API access is enabled by default. To disable access, see Controlling Access.

CAUTION: When REST API access is enabled, make sure to change the default passwords. For more information, see Changing Login Passwords.

For more information about accessing the MDM5010, see Accessing the MDM5010.

For more information about using the REST API, see Managing the MDM5010 using REST API.

1.5.3 Command Line Interface

The Command Line Interface or CLI enables you to fully control the MDM5010 using the command line shell. The CLI provides a higher level of functionality and granular control compared to the Graphical User Interface. In addition, it can be used for scripting or automating tasks.

The command line shell is accessed using an SSH connection. Log in as *expert* user. The default password is *expertexpert*.

NOTE - PuTTY is a common SSH client for Windows users, see https://www.putty.org/.

NOTE - Make sure your local computer can reach the management IP address of the MDM5010.

NOTE - CLI access is enabled by default. To disable access, see Controlling Access.

CAUTION: When CLI access is enabled, make sure to change the default passwords. For more information, see Changing Login Passwords.

For more information about accessing the MDM5010, see Accessing the MDM5010.

For more information about using command lines, see Managing the MDM5010 using CLI.

1.5.4 SNMP Interface

SNMP or Simple Network Management Protocol is used to manage and monitor the MDM5010 using a Management Information Base or MIB.

Use an SNMP browser, such as HPOpenView or NetworkView, to connect to the management IP address of the MDM5010 (SNMP agent). The SNMP implementation in the MDM5010 has the *AuthNoPriv* security level. This means that SNMP messages are authenticated but not encrypted. Authentication is based on a community string sent with each SNMP message. This string must be known by both the SNMP agent, running on the MDM5010 and SNMP manager, running on your local computer.

NOTE - Make sure your local computer can reach the management IP address of the MDM5010.

NOTE - SNMP access is enabled by default. To disable access, see Controlling Access.

CAUTION: When SNMP access is enabled, make sure to change the community strings. For more information, see Changing SNMP Community Strings.

For more information about accessing the MDM5010, see Accessing the MDM5010.

For more information about using SNMP, see Managing the MDM5010 using SNMP.

NOTE - This user guide does not provide detailed information about managing the MDM5010 using SNMP. It is recommended to manage the MDM5010 using the GUI, REST API, or CLI.

1.5.5 SCP Interface

SCP or Secure Copy Protocol is used to upload files to and download files from the MDM5010, such as uploading configuration files or downloading diagnostic reports.

SCP is based on the SSH protocol. Log in as *expert* user. The default password is *expertexpert*.

NOTE - WinSCP is a common SCP client for Windows users, see https://winscp.net/.

The MDM5010 has a dedicated *upload* and *download* folder. Files available for download are stored in the *download* folder of the MDM5010; files from your local computer should be sent to the *upload* folder of the MDM5010.

NOTE - It is recommended to limit the total size of the upload folder to 128 MB.

The example below shows how to download the diagnostic report from the MDM5010 to your local computer (linux).

```
user@localhost:~$ scp expert@[MGMT_IP]:download/diagnostics.txt .
```

The example below shows how to upload a configuration file from your local computer (linux) to the MDM5010.

```
user@localhost:~$ scp configuration.xml expert@[MGMT_IP]:upload/
```

NOTE - SCP access is disabled by default. To enable access, see Controlling Access.

CAUTION: When SCP access is enabled, make sure to change the default password. For more information, see Changing Login Passwords.

1.6 The MDM5010 Configuration

The MDM5010 has two types of configuration:

Type	Description
System-specific	System-specific configuration includes: • device identification label • autosave setting for application-specific configuration • management interfaces' configuration and link redundancy • device redundancy System-specific configuration is saved automatically and is not part of the configuration file (see application-specific configuration). This avoids the risk of losing connectivity to the MDM5010 when loading a new configuration file, or after a redundancy switch.
Application-specific	This is all configuration, excluding the system-specific configuration. Any change to application-specific configuration is not saved automatically by default. You can enable to automatically save changes to the application-specific configuration. Application-device configuration is stored in a .xml file. This configuration file enables you to: • import a configuration from your local computer • load an existing configuration • export a configuration to your local computer • delete a configuration • make a configuration the boot configuration By default, the initialconfig is the boot configuration. This configuration is loaded onto the MDM5010 in the factory and includes the factory application-specific configuration. It is recommended to save your initial configuration as a different configuration than initialconfig, to make this new configuration the boot configuration, and to delete initialconfig. If MDM5010s have the same license options, configuration files can be shared. The MDM5010 can store up to 48 different configurations. Handling application-specific configuration can be done using the GUI and CLI.

1.7 Licenses

The MDM5010 requires a license to activate the software options. Most options are standard; some options, such as the maximum SCPC TX rate and bandwidth cancellation rate, have to be ordered explicitly. A license is unique per MDM5010 device.

There are two types of license:

Type	Use
permanent	The permanent license includes the software options that have been purchased and is valid until a new permanent license is uploaded.
temporary	The temporary license is valid for a limited amount of time and can be used to test and evaluate new options.

The permanent license is installed on the MDM5010 when purchasing the device. If new or extra software options are needed, the license can be upgraded.

You can use a temporary license to test an option before purchase. The license should be uploaded to the MDM5010 and sits next to the permanent license. If the temporary license is valid, this license will be active.

The temporary license can have one of three validity periods. The license file can be valid:

- Until a fixed end date, for example Dec 31 2023
- For an operational time span, for example 30 days, that counts down when the device is powered on
- For an operational time span, for example 30 days, that counts down when the device is the active one in a redundant setup

When the temporary license expires, the MDM5010 will reset and fall back to the permanent license. The temporary license is deleted.

NOTE - The MDM5010 will trigger an alarms 15 days before the temporary license expires.

A temporary license can be deleted before it expires, see Removing the Temporary License.

If you want to upgrade your permanent license or use a temporary license, contact your ST Engineering iDirect sales representative.

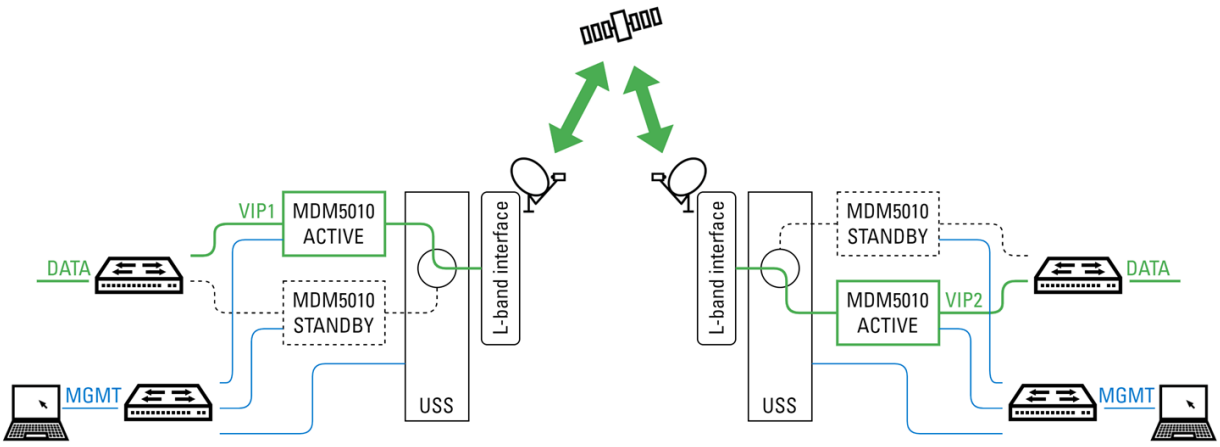
For more information about uploading licenses, see Uploading the License.

To know the active license type and software options, see Checking the Active License Type and Software Options.

1.8 Typical Setup

The MDM5010 SCPC Satellite Modem is used for point-to-point links. It can be set up with another MDM5010 or with an MDM6000, with or without redundancy.

The figure below shows a 1+1 device redundant setup.



When using an MDM6000:

- Make sure that the MDM6000 has *Release MDM6000-P2P-4.0.0* or higher installed; for more information about this release, contact your ST Engineering iDirect sales representative.
- Navigate to the *Label* field of the MDM6000 BBF encapsulator and decapsulator and set at least one channel to **00:00:00:00:00:01**

  Tree View / Encapsulation / BBF Encapsulation / Encapsulation Channels > Label

  Tree View / Decapsulation / BBF Decapsulation / Decapsulation Channels > Label

2 Preparing the Equipment

This chapter describes how to prepare your MDM5010 for use.

In this chapter:

2.1 What's in the Box

NOTE - Inspect the shipping box and contents carefully; if damage or other signs of mishandling are detected, inform the carrier, and either ST Engineering iDirect or the reseller.

The MDM5010 ships in a carton shipping box. To unpack safely, perform the following:

- Open the shipping box where the box indicates OPEN THIS SIDE; take care when using a sharp object
- Remove items from the shipping box.
- Verify that items listed in the order have been received; if not all items are included, contact ST Engineering iDirect or the reseller.
- Carefully remove the MDM5010 chassis from the plastic bag.

CAUTION: Take the necessary ESD precautions when handling the MDM5010.

CAUTION:

NOTE - Do not discard the shipping box and foam after unpacking; you can use it to ship the equipment and accessories to another location, or to return the equipment to ST Engineering iDirect.

The following items can be found in the shipping box:

Item	Included?
MDM5010 chassis	Always
Two N- to F-type 75 Ω adapters	Optional
Power cord	Optional
Rack bolts	Not included when slider kit is ordered
Slider kit	Optional
Quick start guide	Always
Compliance and safety guide	Always
Quality delivery report	Always

2.2 Installing the MDM5010

Please read the *Compliance and Safety Guide* carefully before installing and using the MDM5010.

NOTE - The Compliance and Safety Guide can be found in the shipping box of the MDM5010.

CAUTION: Install and ground the MDM5010 according to national and local area codes and regulations. The MDM5010 must be permanently connected to the protective earth by a skilled person.

CAUTION: When mounting the MDM5010 in a 19" rack, make sure that the MDM5010 is securely sustained by L-profiles or any other type of full support in addition to securing it with the rack bolts. When using the optional slider kit, follow the steps in the *Slider Kit Mounting Instructions*.

CAUTION: The only way to power off the MDM5010 is to unplug the power cord from the power source. Make sure that the power cord and source are accessible and not obstructed when the MDM5010 is powered on.

CAUTION: Make sure that there is enough space along the sides of the MDM5010 to permit proper air circulation. Do not block the air inlets on the front of the MDM5010.

2.3 Powering the MDM5010

The MDM5010 SCPC standalone modem supports the following power options:

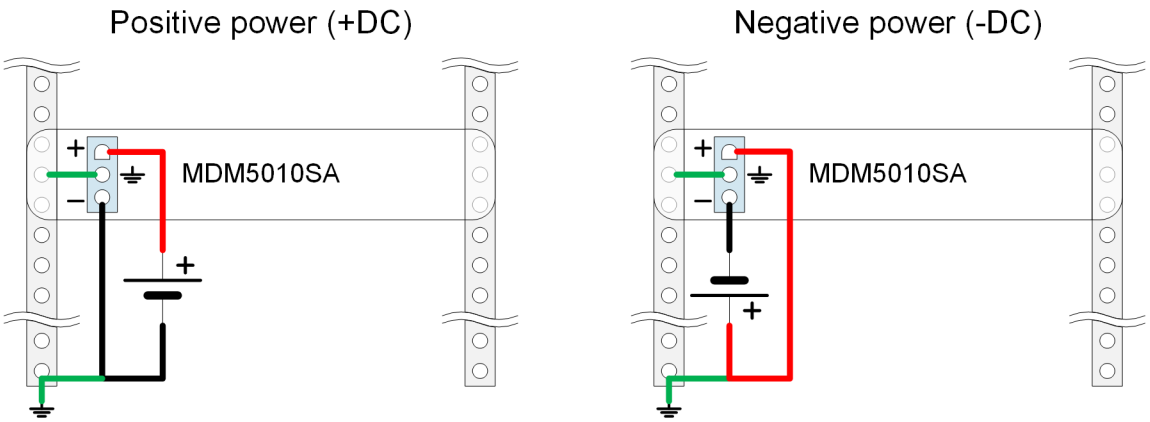
- AC, 50 Hz\220-260 V, 60 Hz\100-130 V
- -38 to -58 Vdc

Refer to MDM5010 Hardware Features for more information about these power options.

To power on the modem, plug the power cord into the MDM5010, and then plug the power cord into the electrical outlet.

To power off the MDM5010, unplug the power cord from the electrical outlet.

Connect DC power to the MDM5010 as shown below.



2.4 Accessing the MDM5010

NOTE - The MDM5010 is always shipped as a Dialog® VSAT modem. To use the MDM5010 in SCPC standalone mode, the MDM5010 must switch personalities. This switch only needs to be performed only once for the modem to run in standalone mode. If required, you can switch back to Dialog® VSAT mode, as described in Switching to Dialog® VSAT Mode.

To switch to SCPC standalone mode:

1 Connect an Ethernet cable to your local computer and one of the DATA interfaces at the rear of the MDM5010, see MDM5010 Hardware Features.

NOTE - The MDM5010 in Dialog® VSAT mode uses the DATA interfaces for management access; the MGMT interfaces are not used.

NOTE - Make sure that DHCP is enabled on your computer.

2 Browse to *http://192.168.1.1/cgi-bin/index?ilogin* and log in as *expert* user. The default login password is *s3p*.

3 Select *Device Info* in the menu at the left of the screen.

4 Select **Standalone SCPC** from the drop-down list in the *Multi-personality* section, and then click **Switch Personalities**. A confirmation window appears. Click **OK** if you want to proceed.

NOTE - You will lose connectivity to the MDM5010.

If the switch is successfully performed, the MDM5010 is now operating as an SCPC standalone modem. You can disconnect the Ethernet cable from the DATA interface at the rear of the MDM5010.

The MDM5010 modem has two physical management ports, as described in MDM5010 Hardware Features. By default, when the the MDM5010 is operating in SCPC standalone mode, MGMT 1 interface is enabled. The default IP address and subnet is 10.0.0.1/24.

To access the MDM5010 in SCPC standalone mode for the first time:

1 Connect an Ethernet cable to your local computer and the MGMT 1 interface at the rear of the MDM5010.

2 Assign an IP address from the default subnet of MGMT 1 to your computer (for example, 10.0.0.5).

3 Access the MDM5010 using the GUI, REST API, CLI, or SNMP. For more information, see Control Interfaces.

You can now configure the MDM5010 in SCPC standalone mode.

It is recommended to start with configuring the management interfaces according to your management network setup. Use the GUI, REST API, or CLI for configuring the management interfaces.

NOTE - When changing the IP address of MGMT 1, you will lose connectivity to the MDM5010. Connect the MDM5010 to your management network to restore access.

2.5 Upgrading the Software

If a software update is available, perform the update before using the MDM5010. A new software version can include new features, enhancements, and bug fixes.

The software can be upgraded using the GUI or CLI.

2.6 Controlling Access

The MDM5010 has several control interfaces. Access to the control interfaces can be limited. Before using the MDM5010 in a network, it is recommended to consider which control interfaces should have limited access.

Control Interface	Access Options	Default Access	To control the access, see...
GUI	• Enabled • Disabled	Enabled	Controlling GUI Access
REST API	• Enabled • Disabled	Disabled	Controlling REST API Access
CLI	• Enabled with inactivity timeout; valid values are from 60 seconds to 5,000,000 seconds, the default value is 600 seconds • Disabled	Disabled	Controlling CLI Access
SCP	• Enabled • Disabled	Disabled	Controlling SCP Access
SNMP	• Enabled • Disabled	Disabled	Controlling SNMP Access

NOTE - The GUI is the only control interface that is enabled by default. Initial access to the REST API, CLI, SCP, and SNMP control interfaces can only be enabled using the GUI, see Controlling Access using the GUI

CAUTION: For security reasons it is highly recommended to change the default passwords for accessing the control interfaces. For more information, see Changing Login Passwords and

CAUTION: Changing SNMP Community Strings.

NOTE - Make sure to save the changes. Saving the configuration can be done using the GUI, see Saving the Active Configuration, or CLI, see Handling Device Configuration.

For more information about the control interfaces, see Control Interfaces.

2.6.1 Controlling GUI Access

GUI access is enabled by default. Access to the GUI can be controlled using REST APIs or the CLI. Authenticate as an Expert user prior to performing these tasks.

2.6.1.1 Controlling GUI Access Using REST APIs

To disable access to the GUI, send the following request:

```
PATCH http://<ip_address>:9000/RestApi/Device/Gui/Enable

"off"
```

To enable access to the GUI, send the following request:

```
PATCH http://<ip_address>:9000/RestApi/Device/Gui/Enable

"on"
```

For more information about using the REST API, see Managing the MDM5010 using REST API.

2.6.1.2 Controlling GUI Access Using the CLI

To disable access to the GUI, go to the *device gui* branch, and then enter the following command:

```
[MDM5010] device gui# set enable=off
```

To enable access to the GUI, go to the *device gui* branch, and then enter the following command:

```
[MDM5010] device gui# set enable=on
```

For more information about using the CLI, see Managing the MDM5010 using CLI.

2.6.2 Controlling REST API Access

REST API access is disabled by default. Access to the REST API can be controlled using the GUI or CLI. Authenticate as an Expert user prior to performing these tasks.

- Controlling REST API Access Using the GUI

- Controlling REST API Access Using the CLI

2.6.2.1 Controlling REST API Access Using the GUI

1. Click the *Dashboard* menu, and then click the *Modem Setup* tab.
2. To disable access to the REST API, click **Access Management**, and then uncheck the *Enable REST API* check box.
3. To enable access, check the *Enable REST API* check box.

For more information about using the GUI, see Managing the MDM5010 via the GUI.

2.6.2.2 Controlling REST API Access Using the CLI

Go to the *device rest* branch, and enter the following command to access to the REST API:

```
[MDM5010] device rest# set enable=off
```

To enable access, enter the following command:

```
[MDM5010] device rest# set enable=on
```

For more information about using the CLI, see Managing the MDM5010 using CLI.

2.6.3 Controlling CLI Access

CLI access is disabled by default. Access to the command line interface can be controlled using the GUI, REST API, or CLI. Authenticate as an Expert user prior to performing these tasks.

- Using GUI
- Controlling CLI Access Using the CLI
- Controlling CLI Access Using REST APIs

2.6.3.1 Controlling CLI Access Using the GUI

1. Click the *Dashboard* menu, and then click the *Modem Setup* tab.
2. To disable SSH access to the CLI, click **Access Management**, and then uncheck the *Enable CLI* check box.
3. To allow SSH access, check the *Enable CLI* check box.

4 To change the time of inactivity after which the user is logged out, edit the *CLI Inactivity Timeout* field.

For more information about using the GUI, see Managing the MDM5010 via the GUI.

2.6.3.2 Controlling CLI Access Using REST APIs

To disable SSH access to the CLI, send the following request:

```
PATCH http://<ip_address>:9000/RestApi/Device/Cli/RemoteEnable

"off"
```

To allow SSH access, send the following request:

```
PATCH http://<ip_address>:9000/RestApi/Device/Cli/RemoteEnable

"on"
```

To change the time of inactivity after which the user is logged out, send the following request:

```
PATCH http://<ip_address>:9000/RestApi/Device/Cli/InactivityTimeout

300
```

For more information about using the REST API, see Managing the MDM5010 using REST API.

2.6.3.3 Controlling CLI Access Using the CLI

Go to the *device cli* branch, and then enter the command to disable SSH access to the CLI:

```
[MDM5010] device cli# set remoteenable=off
```

NOTE - Your SSH session will be closed. Use the other control interfaces to enable SSH access again.

To change the time of inactivity after which the user is logged out, enter the following command:

```
[MDM5010] device cli# set inactivitytimeout=300
```

For more information about using the CLI, see Managing the MDM5010 using CLI.

2.6.4 Controlling SCP Access

SCP access is disabled by default. Access to the SCP interface can be controlled using the GUI, REST API, or CLI. Authenticate as an Expert user prior to performing these tasks.

- Using GUI
- Using REST API
- Using CLI

2.6.4.1 Controlling SCP Access Using the GUI

1. Click the *Dashboard* menu, and then click the *Modem Setup* tab.
2. To disable access to the SCP interface, click **Access Management**, and then uncheck the *Enable SCP* check box.
3. To enable access, check the *Enable SCP* check box.

For more information about using the GUI, see Managing the MDM5010 via the GUI.

2.6.4.2 Controlling SCP Access Using the REST API

To disable access to the SCP interface, send the following request:

```
PATCH http://<ip_address>:9000/RestApi/Device/Scp/Enable

"off"
```

To enable access, send the following request:

```
PATCH http://<ip_address>:9000/RestApi/Device/Scp/Enable

"on"
```

For more information about using the REST API, see Managing the MDM5010 using REST API.

2.6.4.3 Controlling SCP Access Using the CLI

Go to the *device scp* branch, and then enter the command to disable access to the SCP interface:

```
[MDM5010] device scp# set enable=off
```

To enable access, enter the following command:

```
[MDM5010] device scp# set enable=on
```

For more information about using the CLI, see Managing the MDM5010 using CLI.

2.6.5 Controlling SNMP Access

SNMP access is disabled by default. Access to the SNMP interface can be controlled using the GUI, REST API, or CLI. Authenticate as an Expert user prior to performing these tasks.

- Controlling SNMP Access Using the GUI
- Controlling SNMP Access Using REST APIs
- Controlling SNMP Access Using the CLI

2.6.5.1 Controlling SNMP Access Using the GUI

1. Click the *Dashboard* menu, and then click the *Modem Setup* tab.
2. To disable access to the SNMP interface, click **Access Management**, and then uncheck the *Enable SNMP* check box in the *SNMP* section.
3. To enable access, check the *Enable SNMP* check box in the *SNMP* section.

For more information about using the GUI, see Managing the MDM5010 via the GUI.

2.6.5.2 Controlling SNMP Access Using REST APIs

To disable access to the SNMP interface, send the following request:

```
PATCH http://<ip_address>:9000/RestApi/Device/Snmp/Enable

"off"
```

To enable access to the SNMP interface, send the following request:

```
PATCH http://<ip_address>:9000/RestApi/Device/Snmp/Enable

"on"
```

For more information about using the REST API, see Managing the MDM5010 using REST API.

2.6.5.3 Controlling SNMP Access Using the CLI

Go to the *device snmp* branch, and then enter the command to disable access to the SNMP interface:

```
[MDM5010] device snmp# set enable=off
```

To enable access to the SNMP interface, enter the following command:

```
[MDM5010] device snmp# set enable=on
```

For more information about using the CLI, see Managing the MDM5010 using CLI.

2.6.6 Changing Login Passwords

NOTE - Changing the *expert* user password affects the password to log in to the GUI, CLI, REST API, and SCP.

The default password for the guest user is guestguest.

The default password for the expert user is expertexpert.

The login password can be changed using the GUI or CLI.

- Changing Login Passwords
- Changing Login Passwords via the CLI

2.6.6.1 Changing Login Passwords via the GUI

NOTE - Make sure that you log in as the user for who you want to change the password (guest or expert).

1. To change the user password, click expert or guest at the top right of the GUI screen, and then select **Change Password**. A window appears.
2. Enter the current password, and then enter the new password. Confirm the new password.
3. Click **Change Password** to confirm the change.

For more information about using the GUI, see Managing the MDM5010 via the GUI.

2.6.6.2 Changing Login Passwords via the CLI

NOTE - Log in as expert.

Go to the *user password* branch, and then enter the command to change the user login password:

```
[MDM5010] user password# change 'user' 'old_password' 'new_password'
```

- 'user' is 'guest' or 'expert'.
- 'old_password' is the password currently used on the system (for example, 'expertexpert')
- 'new_password' is the new password for the expert user.

For more information about using the CLI, see Managing the MDM5010 using CLI.

2.6.7 Changing SNMP Community Strings

There are three types of community strings:

Type...	Is used to...	Default value
Read-only	get information.	public
Read-write	get and set information.	private
Trap	send notifications.	trapcom

NOTE - The maximum length of a community string is up to 30 characters and can only include alphanumeric characters. It cannot include any spaces.

NOTE - Make sure to update the community strings in the SNMP manager accordingly.

The community strings can be changed using the GUI, REST API, or CLI.

- Changing SNMP Community Strings via the GUI
- Changing SNMP Community Strings via REST APIs
- Changing SNMP Community Strings via the CLI

2.6.7.1 Changing SNMP Community Strings via the GUI

NOTE - Make sure you are logged in as expert.

1. Click the *Dashboard* menu, and then click the *Modem Setup* tab.
2. To change the community strings, click **Access Management**, and then edit the *Read-Only Community*, *Read-Write Community*, and trap *Community* field.
3. Click  to confirm the change.

For more information about using the GUI, see Managing the MDM5010 via the GUI.

2.6.7.2 Changing SNMP Community Strings via REST APIs

NOTE - Make sure to authenticate as expert user.

To change the read-only and read-write community strings, send the following request:

```
PUT http://<ip_address>:9000/RestApi/Device/Snmp/Authentication

{

"ReadOnlyCommunity": "your_read-only_string",

"ReadWriteCommunity": "your_read-write_string"

}
```

To change the trap community string of destination x, where x = 1, 2, 3, or 4, send the following request:

```
PATCH http://<ip_address>:9000/RestApi/Device/Snmp/Notifications/Destination/x

{

"Community": "your_trap_string"

}
```

For more information about using the REST API, see Managing the MDM5010 using REST API.

2.6.7.3 Changing SNMP Community Strings via the CLI

NOTE - Log in as expert.

Go to the *device snmp* branch.

To change the read-only community string, enter the following command:

```
[MDM5010] device snmp# authentication set readonlycommunity=your_read-only_string
```

To change the read-write community string, enter the following command:

```
[MDM5010] device snmp# authentication set readwritecommunity=your_read-write_string
```

To change the trap community string of destination x, where x = 1, 2, 3, or 4, enter the following command:

```
[MDM5010] device snmp# notifications destination x set community=your_trap_string
```

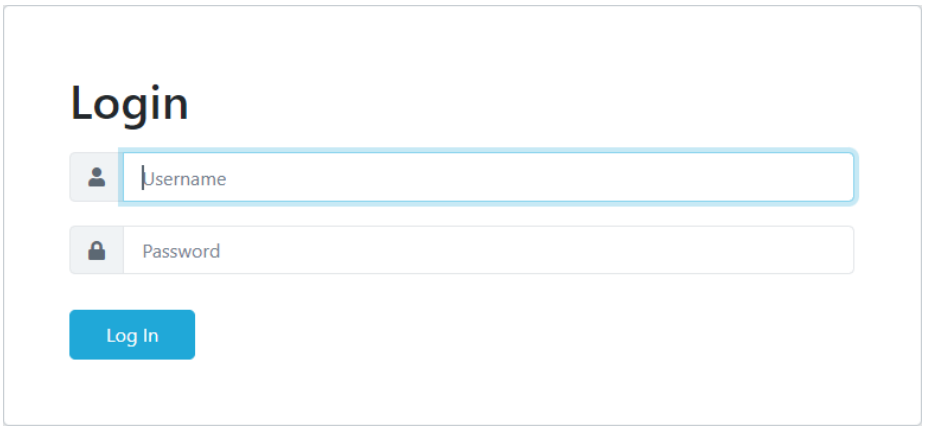
For more information about using the CLI, see Managing the MDM5010 using CLI.

3 Managing the MDM5010 via the GUI

The graphical user interface or GUI provides a visual-based and intuitive interface for controlling the MDM5010.

NOTE - Make sure your local computer can reach the management IP address of the MDM5010.

To access the GUI, browse to the management IP address of the MDM5010 using HTTP. A login window appears.



Log in as *guest* user or *expert* user. The guest user has read-only access, the default login password is *guestguest*. The expert user has read-write access, the default login password is *expertexpert*.

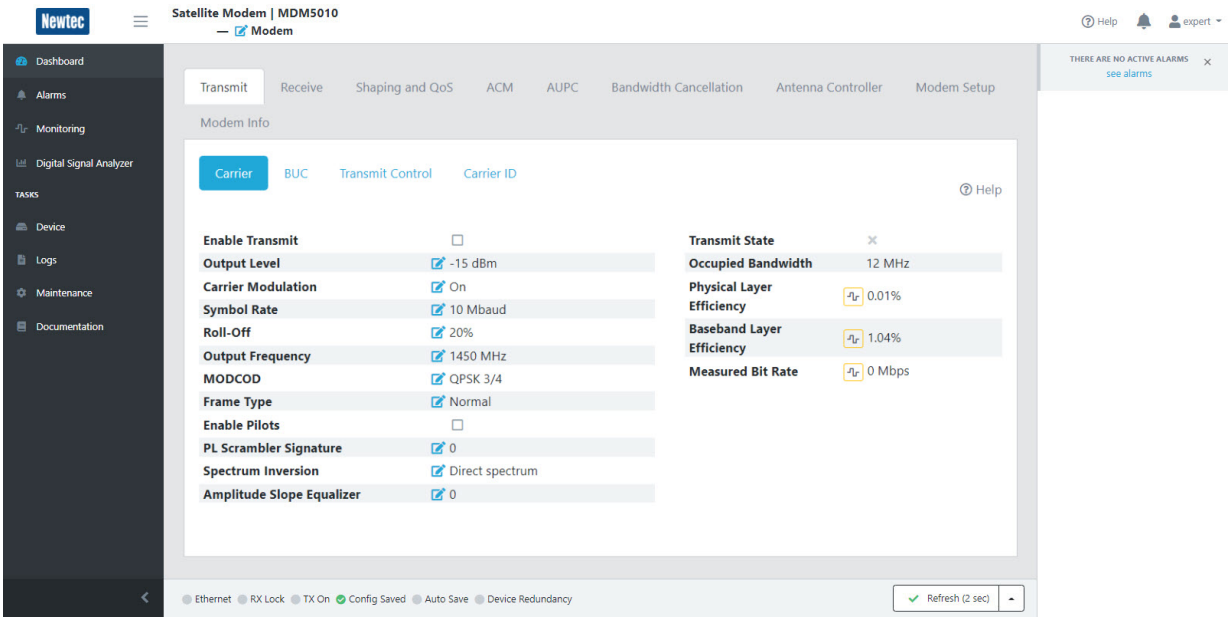
NOTE - GUI access can be disabled. See Controlling Access.

In this chapter:

- Managing AUPC
- Managing Bandwidth Cancellation
- Using an Antenna Controller
- Modem Setup
- Modem Information
- Handling the Configuration
- Viewing the Alarms
- Monitoring Parameter Trends
- Using the Digital Signal Analyzer
- Viewing the Device Log
- Viewing the Diagnostic Report
- Upgrading the Software
- Uploading the License
- Removing the Temporary License
- Resetting the MDM5010
- Downloading SNMP MIB-Modules
- Viewing the Reference Manual
- Switching to Dialog® VSAT Mode

3.1 The GUI Screen

The MDM5010 GUI screen, logged in as expert user, is shown below:



The GUI screen has six sections:

- A banner at the top of the screen
- The menu and tasks overview at the left of the screen, see Menu and Tasks; click at the bottom to minimize the section, click to expand the section
- The body at the center of the screen; the content depends on the selected menu item
- The task button bar at the top of the body; when no task is selected, the bar is not shown
- The list of active alarms at the right of the screen; click × to hide this section; click **see alarms** to call the *Alarms* menu item; for more information about the alarms, see Dealing with Alarms
- The status bar at the bottom of the screen, see Status Bar

There are several buttons in the banner at the top of the screen:

Click...	To...
☰	show or hide the menu and tasks overview.

Click...	To...
	set the name of your MDM5010. The maximum length of the name is up to 50 characters. The name is displayed in the banner at the top of the GUI screen and in the CLI prompt. NOTE: The name can only be edited when logged in as *expert* user.
	view the MDM5010 Help in a new browser tab.
	show or hide the active alarm section. The number of active alarms is indicated in the red circle. The red circle is not shown If there are no active alarm.
	• set the time in local time zone, see Setting the Time in Local Time Zone • switch user, see Switching Users • log out • change the login password, see Changing Login Passwords

3.1.1 Menu and Tasks

There are four menu items:

Click...	To...	For more information, see...
Dashboard	configure and monitor the MDM5010.	MDM5010 GUI Dashboard Overview
Alarms	view the alarms.	Viewing the Alarms
Monitoring	view trend charts of measured parameters and alarms.	Monitoring Parameter Trends
Digital Signal Analyzer	• view the signal constellation diagram • view the signal spectrum	Using the Digital Signal Analyzer

The following conventions are used in this document.

NOTE - The content of a menu item is displayed in the body screen.

There are four tasks:

Click...	To...	For more information, see...
Device	• handle the configuration • perform a reset • switch personalities NOTE: The Device task is only available when logged in as expert user.	• Handling the Configuration • Resetting the MDM5010 • Switching to Dialog® VSAT Mode
Logs	view and download the device log.	Viewing the Device Log
Maintenance	• view and download the diagnostic report • upgrade the software • upload the license NOTE: Upgrading the software and uploading the license is only available when logged in as expert user.	• Viewing the Diagnostic Report • Upgrading the Software • Uploading the License
Documentation	• download the MIB-modules • view the reference manual NOTE: Downloading MIB-modules is only available when logged in as expert user.	• Downloading SNMP MIB-Modules • Viewing the Reference Manual

NOTE - A task displays one or more buttons at the top of the body screen.

3.1.2 Switching Users

To switch users, click expert (can also be guest) at the top right of the screen, and then select **Switch User**. A login window appears.

Enter the *Username* and *Password* and click **Log In**. Click **Cancel** if you do not want to switch users.

Two users exist:

- *guest* with read-only access; the default password is *guestguest*
- *expert* with read-write access; the default password is *expertexpert*

3.1.3 Setting the Time in Local Time Zone

To make sure timestamps are displayed in your local time zone, click expert (can also be guest) at the top right of the screen, and then select the *Times in Local Time Zone* check box. If the check box is not selected, the time zone is UTC.

NOTE - The local time zone corresponds with the time zone set on your local computer.

NOTE - This does not set the time on the MDM5010. To set the time on the MDM5010, see Setting Date and Time.

3.1.4 Status Bar

The status bar at the bottom of the screen shows the status of:

- Ethernet data interfaces
- demodulator
- transmission
- configuration
- device redundancy

Use the table below to understand the different status indicators.

If indicator...	Is ✓ then...	Is ⚠ then...	Is ✗ then...	Is ○ then...
Ethernet	• (no link redundancy) all logical data interfaces that are administratively up are OK • (link redundancy) the active logical data interface is OK For more information about the logical data interfaces, see Data Interfaces.	NA	• (no link redundancy) at least one logical data interface that is administratively up has an alarm • (link redundancy) both logical data interfaces have an alarm	both logical data interfaces are administratively down.
RX Lock	the demodulator is enabled and has physical layer and decoder lock.	the demodulator is enabled and has physical layer lock, but no decoder lock.	the demodulator is enabled but has no physical layer lock.	the demodulator is disabled.
TX On	the MDM5010 is transmitting the uplink carrier.	NA	NA	the MDM5010 is not transmitting. Transmit can be disabled because of an alarm, because the MDM5010 is the standby modem in a redundant setup or can be disabled manually.
Config Saved	the active configuration is saved.	NA	changes to the active configuration have not been saved. To save the configuration manually, see Handling the Configuration.	NA

If indicator...	Is ✓ then...	Is ⚠ then...	Is ✗ then...	Is ○ then...
Auto Save	NA	the MDM5010 saves changes to the application-specific configuration automatically.	NA	the MDM5010 does not save changes to the application-specific configuration automatically.
Device Redundancy	device redundancy is enabled, and the MDM5010 is in active mode.	device redundancy is enabled, and the MDM5010 is in standby mode.	NA	device redundancy is disabled.

Click the drop-down button to change the refresh time of the GUI. Valid values are 2, 5, 10, 30, 60 seconds, or manual. The default value is two seconds.

NOTE - It is recommended to increase the refresh time when accessing the GUI through a high-latency link or when bandwidth is limited.

3.2 MDM5010 GUI Dashboard Overview

Use the *Dashboard* menu item to:

- configure the MDM5010
- view parameters such as performance and link quality measurements, and general device information of the MDM5010.

NOTE - Save the configuration when changes have been applied. For more information, see Saving the Active Configuration.

Editing Fields

Field values can only be edited when you are logged in as *expert*. The field value can be one of the types below:

- A check box; the *guest* user will see ✔ when the check box is selected, and ✖ when the check box is not selected
- A drop-down list with predefined values to select
- A numeric field to enter a number, or use ⇕ to increase or decrease the value with the minimum step size
- A string field
- A date field

Editable fields, except check boxes, are marked with ✎. Click the field to edit the value.

There are several buttons:

Use...	To...
ⓘ	view the valid values that can be entered. This is only available for numeric fields.
✔	confirm the value change.
✖	discard the value change.

3.3 Defining the Modulator

Navigate to **Dashboard > Transmit** to:

- define the uplink carrier to transmit, see Defining the Uplink Carrier
- enable a reference frequency and optionally an output voltage for the BUC, see Managing the BUC
- control the transmission based on alarms, see Controlling the Carrier Transmission

3.3.1 Defining the Uplink Carrier

Navigate to **Dashboard > Transmit > Carrier** to define the carrier that the modem should transmit. Log in as an expert carrier to edit fields.

NOTE - Transmission critical parameters, such as frequency and symbol rate, are by default read-only when the modem is transmitting. It is however possible to allow changing these parameters when the modem is transmitting, see Controlling the Carrier Transmission.

Parameter	Description
Enable Transmit	indicates if the transmission of the carrier is enabled or disabled. When the check box is not selected, the modem does not transmit the carrier. When the MDM5010 does not transmit, the *TX On* indicator in the status bar and the *TX* notification LED on the front panel are off. Disable transmission when using the MDM5010 as a demodulator only or when performing maintenance.
Output Level	Carrier signal level at the TX interface of the MDM5010. Valid values are from -35 dBm to +7 dBm. The default value is -15 dBm.
Carrier Modulation	• **On**: The carrier is modulated with an information-bearing digital signal. • **Continuous wave**: The carrier is a non-modulated pure carrier. A pure carrier can be used to perform a line-up procedure, for cross-pol testing, and so on.
Symbol Rate	Number of transmitted symbols per second. A symbol may consist of two or more bits as determined by the MODCOD. Valid values are from 1 Mbaud to 220 Mbaud.NOTE: Not all MODCODs can operate at the highest symbol rate. To know the limitations, see MODCOD Limitations.

Parameter	Description
Roll-Off	The *Roll-Off* (RO) field is a measure of the excess bandwidth of the filter used for pulse-shaping in digital modulation. Together with the symbol rate it defines the occupied bandwidth (BW) of the modulated carrier: `BW = (1+(RO/100))SR`. Valid values are 2%, 5%, 10%, 15%, 20%, 25%, and 35%. The default value is 20%.
Output Frequency	L-band center frequency of the carrier. Valid values are from 950 MHz to 2450 MHz.
MODCOD	The *MODCOD* field specifies the modulation and coding scheme used to transmit the digital information over the satellite link. The coding scheme (1/4, 8/9, and so on) refers to the FEC (Forward Error Correction) overhead. The modulation order defines how the bits of a FEC frame are mapped into modulation symbols. Valid orders of modulation are QPSK, 8PSK, 16APSK, 32APSK, 64APSK, and 256APSK. The MODCOD to use depends on the link quality. A good link quality enables you to use a higher order modulation and lower FEC overhead, which increases the throughput and performance. When ACM (Adaptive Coding and Modulation) is enabled, the value refers to the MODCOD that will be used for the first frames. Once the ACM controller receives ACM feedback from the remote ACM client, the MODCOD is adjusted according to the actual link conditions. For more information, see Adaptive Coding and Modulation. **NOTE:** The possible MODCODs depend on the Frame Type and the presence of Pilots, see MODCOD Limitations. For more information about MODCODs, frame types, and pilots, see Coding and Modulation.
Frame Type	The *Frame Type* field specifies the size of a single FEC frame. The size can be 64,800 bits (normal) or 16,200 bits (short). Normal frames are more efficient, short frames can reduce end-to-end system latency. Use short frames for low-speed links (< 1 MBaud). For more information about frame types, see Coding and Modulation.
Enable Pilots	Pilots can be used to increase the reliability of the receiver synchronization. Pilots are blocks of 36 un-modulated symbols, which can be received by any receiver. When the *Enable Pilots* check box is selected, the insertion of pilots is enabled. **NOTE:** It is recommended to use pilots, especially when phase noise occurs, data rates are low, or distortion is present. For more information about pilots, see Coding and Modulation.
PL Scrambler Signature	Prior to modulation, each physical layer frame, excluding the header, is randomized for energy dispersal. The *PL Scrambler Signature* specifies the spreading sequence number. Valid values are from 0 to 262141. The default value is 0.

Parameter	Description
Spectrum Inversion	Indicates if the MDM5010 must invert the spectrum or not. A satellite operator always requires a non-inverted spectrum. If the LO (local oscillator) frequency of the BUC is higher than the transmit frequency, the BUC typically inverts the spectrum. The *Spectrum Inversion* value should then be set to **Inverted**. If the BUC does not invert the spectrum, set the value to **Direct**.
Amplitude Slope Equalizer	The *Amplitude Slope Equalizer* can be used to compensate for gain loss at higher frequencies due to RF amplifiers, RF cables, and passive components. The equalizer has a maximum range of ± 8 dB / 500 MHz. Valid values are from -15 to 15. The default value is 0.

At the right of the screen several parameters are shown:

Field...	Shows...
Transmit State	if the modem is transmitting the carrier (✔) or not (✖). There can be several reasons for not transmitting: • The *Enable Transmit* check box is not selected • The MDM5010 is the standby device in a redundant setup • An alarm is active, see Controlling the Carrier Transmission NOTE: When the transmit state is not the expected state, an extra field will display the reason for the current transmit state.
Occupied Bandwidth	the bandwidth of the carrier and is determined by the *Symbol Rate* (SR) and *Roll-Off* (RO) value: `BW = (1+(RO/100))SR`.
Physical Layer Efficiency	how efficiently the physical layer (PL) frames are used. The higher the value, the higher the efficiency. A low value indicates that the filling rate of the PL frames with useful data is low, for instance because the traffic rate is low.
Baseband Layer Efficiency	how efficiently the baseband (BB) frames are used. The higher the value, the higher the efficiency. A low value indicates that the filling rate of the BB frames with useful data is low, for instance because the traffic rate is low and the *Frame Type* field is set to normal.
Measured Bit Rate	the baseband frame bit rate measured at the input of the modulator.

NOTE - Click to trend the measured values over time, see Monitoring Parameter Trends.

3.3.2 Managing the BUC

Navigate to **Dashboard > Transmit > BUC** to send a reference frequency from the MDM5010 to the BUC, and optionally power the BUC.

NOTE - Powering the BUC is only possible if the MDM5010 supports a DC BUC power supply.

A block upconverter (BUC) converts the L-band frequency band to a higher frequency band, such as the Ku-band. Most BUCs use phase-locked loop local oscillators and require an external frequency reference to maintain the correct transmit frequency.

Use the *Clock Reference On TX* field to send a **10 MHz** or **50 MHz** reference frequency on the same feed line as the uplink carrier. Select **Off** if the BUC uses an internal reference.

For more information about the reference clock, see The Reference Clock.

When the MDM5010 has the DC BUC power supply option, the *DC BUC* field is shown. Use the field to provide a **24 VDC** or **48 VDC** signal to the BUC on the same feed line as the uplink carrier. Select **Off** if the BUC uses an external power supply.

NOTE - The output voltage depends on the DC BUC power supply option that has been ordered.

3.3.3 Controlling the Carrier Transmission

Navigate to **Dashboard > Transmit > Transmit Control** to stop the MDM5010 from transmitting when one or more of the following events occur:

- A *General Device Alarm*
- A *General Interface Alarm*
- The *Demod Out of Lock* alarm (corresponds with the *Demodulator No Lock* alarm)

For more information about the alarms, see Dealing with Alarms.

Select **Disable Transmit** if you want to stop transmission when the event occurs, else select **No Impact**.

NOTE - The transmit can also be disabled manually, see Defining the Uplink Carrier.

Select the *Allow Changes While TX On* check box to allow changing transmission critical parameters, such as frequency and symbol rate, without disabling the transmission.

WARNING - *Changes are active immediately. Only enable this in controlled environments.*

3.4 Defining the Demodulator

Navigate to **Dashboard > Receive** to:

- define the carrier to receive, see Defining the Downlink Carrier
- migrate the carrier to receive, see Defining a Downlink Backup Carrier
- view the parameters of received MODCOD(s), see Viewing the MODCOD Statistics
- manage the LNB, see Managing the LNB

3.4.1 Defining the Downlink Carrier

Navigate to **Dashboard > Receive > Carrier** to define the carrier that the MDM5010 should receive.

Parameter	Description
Enable Demodulator	Indicates if the demodulator part of the MDM5010 is activated or not. When the check box is not selected, the demodulator is disabled and the *RX Lock* indicator in the status bar is off.
Symbol Rate	Number of transmitted symbols per second. A symbol may consist of two or more bits as determined by the MODCOD. Valid values are from 1 Mbaud to 220 Mbaud.
Input Frequency	L-band center frequency of the carrier. Valid values are from 950 MHz to 2150 MHz.
Roll-Off	Measure of the excess bandwidth of the filter used for pulse-shaping in digital modulation. Together with the symbol rate it defines the occupied bandwidth (BW) of the modulated carrier: `BW = (1+(RO/100))SR`. Valid values are Auto, 5%, 10%, 15%, 20%, 25%, and 35%. The default value is 20%.
Spectrum Inversion	Specifies if the MDM5010 must invert the incoming spectrum or not. When the LNB inverts the spectrum, the value should be set to **Inverted**. When set to **Automatic**, the demodulator will detect the value automatically. **NOTE:** It is recommended to explicitly set the value when known. This will accelerate locking on to the carrier.
Acquisition Range	Window that the MDM5010 uses to look for the downlink carrier. The *Input Frequency* is the center frequency of this range. Valid values are from 0.05 MHz to 7.5 MHz. The default value is 1 MHz. **NOTE:** It is recommended to set the value to 1.5 x the symbol rate when the symbol rate is lower than 3.33 Mbaud. For higher symbol rates, the acquisition range should be set to 0.3 x symbol rate with a maximum of 7.5 MHz.

Parameter	Description
PL Scrambler Signature	Used by the modulator as a master key to randomize the physical layer frames (excluding the headers) for energy dispersal. The same number must be known by the demodulator so that demodulation is possible. Valid values are from 0 to 262141. The default value is 0.

When the demodulator is enabled, extra information is shown at the right of the screen.

Field...	Shows...
L-band Input Level	the power level of the entire L-band received at the modem.
Carrier Input Level	the power level of the carrier received at the modem.
Carrier Offset	the offset between the configured input frequency and the actual carrier frequency.
Measured Symbol Rate	the actual symbol rate of the carrier measured at the modem.
Es/No Header	the ratio of the energy per symbol (Es) to the noise power spectral density (N0) measured based on the baseband frame headers. It is an indication of the downlink quality.
Frame Counter	the number of baseband frames that the MDM5010 was able to decode.
Dummy PL Frame Counter	the number of dummy physical layer frames in the DVB-S2X stream. Dummy PL frames are transmitted by the modulator when no useful data is ready to be sent.
Errored Frame Counter	the number of baseband frames that the MDM5010 was not able to decode. The counter increases when the link margin is too low, when saturation causes channel distortions, or when non-linear distortions occur.
Cycle Slip Frame Counter	the number of times the symbol phase tracking loop has failed. The counter increases when there is phase noise, or when phase discontinuities due to local oscillator instabilities occur.
Last Non-Dummy MODCOD	the MODCOD of the downlink carrier that the MDM5010 could last demodulate and decode, and that includes useful data.
Phase Noise Indication	the estimated phase noise of the carrier, in degrees. The value is between $-1e^{09}$ and $1e^{09}$. The value depends on the symbol rate.
Offset To Reference Mask	the difference between the estimated phase noise and a reference phase noise. The value is between -100 dB and 50 dB. A positive value indicates that the received phase noise is worse than the reference phase noise mask. The reference phase noise is the critical mask (P1) as defined in the DVB-S2X standard. This value is independent of the symbol rate.

Field...	Shows...
Non Linearity Indication PM	how much the carrier is affected by non-linear phase distortion. The value is between 0% and 100%.
Non Linearity Indication AM	how much the carrier is affected by non-linear amplitude distortion. The value is between 0% and 100%.

NOTE - Click to trend the measured values over time, see Monitoring Parameter Trends.

Five alarms are monitored:

If alarm...	is active ( ) then...	Action
Internal Error	an error occurred which is not one of the next issues.	Contact ST Engineering iDirect customer support.
L-band Input Saturation	the L-band input level at the demodulator is higher than -10 dBm.	• Check for the presence of an interferer • Add an attenuator in front of the L-band input
Physical Layer Lock	the MDM5010 is unable to lock onto the headers of the physical layer (PL) frames. Lock occurs when two consecutive PL headers have been decoded successfully.	• Enable pilots at the transmit side • Make sure that the quality of the incoming signal is OK, for example, check the pointing of the antenna
LNB Power Control Error	there is an error in the LNB power supply, for example, a short circuit on the connector.	Check the hardware connection between the MDM5010 and LNB.
Decoder Overload	the decoder is unable to decode the baseband frames, for example, due to bad signal quality, or the decoder cannot handle the input stream, for example, when the symbol rate is too high for the selected MODCOD.	• Make sure to select the correct MODCOD for the signal quality; lower the MODCOD at the transmit side and increase the ACM margins. • Check if there are no failing hardware components, such as a failing LNB, in the receive link • Make sure that the MODCOD can handle the symbol rate, see MODCOD Limitations

If the alarm persists, contact ST Engineering iDirect customer support.

NOTE - The monitored parameters and alarms are only visible when the demodulator is enabled.

3.4.2 Defining a Downlink Backup Carrier

Navigate to **Dashboard > Receive > Backup Carrier** to define a backup carrier that the MDM5010 should use when it looses lock on the primary carrier (*Demodulator No PL Lock* alarm is active). A backup carrier can be used for migrating carriers, see Migrating a Carrier

NOTE - Disable the backup carrier when the MDM5010 successfully receives and demodulates the backup carrier. This will automatically set the backup carrier as the primary carrier

NOTE - The backup carrier cannot be used when bandwidth cancellation is enabled.

Parameter	Description
Enable Backup Carrier	Indicates if the MDM5010 may switch to a backup carrier or not. When the check box is not selected, the modem should not switch to the backup carrier when it loses lock on the primary carrier.
Input Frequency	L-band center frequency of the carrier. Valid values are from 950 MHz to 2150 MHz.
Symbol Rate	Number of transmitted symbols per second. A symbol may consist of two or more bits as determined by the MODCOD. Valid values are from 1 Mbaud to 220 Mbaud.
Switch Timeout	Time that needs to pass when the primary carrier is lost before switching to the backup carrier. The default value is 60 seconds. Valid values are from 1 second to 1000 seconds.

When the backup carrier is enabled, extra information is shown at the right of the screen.

Field...	Shows...
Active Carrier	which carrier is used: backup or main (primary).
Switch Count	the number of times the MDM5010 has switched between the primary and backup carrier.

NOTE - Click to trend the measured values over time, see Monitoring Parameter Trends.

3.4.3 Viewing the MODCOD Statistics

Navigate to **Dashboard > Receive > MODCOD Statistics** to view the status and quality of the downlink carrier per MODCOD detected in DVB-S2X stream:

Field...	Shows...
MODCOD	the modulation and coding scheme of the DVB-S2X stream.
Frame Type	the size of a single FEC frame: normal or short.
Pilots	if pilots are inserted or not.
Frame Counter	the number of baseband frames that the MDM5010 was able to decode.
Errored Frame Counter	the number of baseband frames that the MDM5010 was not able to decode. The counter increases when the link margin is too low, when saturation causes channel distortions, or when non-linear distortions occur.
Cycle Slip Counter	the number of times the symbol phase tracking loop has failed. The counter increases when there is phase noise, or when phase discontinuities due to local oscillator instabilities occur.
Frame Error Ratio	the ratio of errored FEC frames to the total number of received FEC frames.
Link Margin	how much the noise level can increase, or how much the downlink can fade before the MODCOD Es/No threshold is reached. See Adaptive Coding and Modulation. The value can clip when the link margin is too low (<) or too high (>) to be accurately determined.
C/N	the ratio of the carrier power level (C) to the receiver noise density (N). It is measured at the modem and is an indication of the downlink quality.
C/D	the ratio of the carrier power level (C) to distortion level (D). It is measured at the modem and is an indication of the downlink quality. Distortion can be linear or non-linear. Linear distortion can be caused by, for example, imperfections in the amplitude response of the transponder. Non-linear distortion can be caused by non-linearity in the amplifier of the satellite.
C/ND	the ratio of the carrier power level (C) to receiver noise density (N) + distortion level (D). It is measured at the modem and is an indication of the downlink quality.

NOTE - During the lock acquisition phase the parameters show incorrect data. The metrics are reset automatically after five seconds of stable lock and start showing relevant data.

NOTE - Click to trend the measured values over time, see Monitoring Parameter Trends.

To clear all MODCODs and related parameters, click **Reset MODCOD Statistics**.

NOTE - The reset button is only available when logged in as expert.

3.4.4 Managing the LNB

Navigate to **Dashboard > Receive > LNB** to provide a DC power signal, a frequency band selection signal, and a reference frequency from the MDM5010 to the LNB.

CAUTION: If the LNB power is enabled, make sure to use a DC-block at the input of devices that do not tolerate DC voltages, for example, third-party outdoor units and spectrum analyzers.

For the reception of narrow bandwidth carriers, highly stable and low phase noise LNB local oscillators are required. These use phase-locked loop local oscillators and require an external 10 MHz reference to maintain an accurate frequency.

Parameter	Description
LNB Power Supply A	Provide a DC power signal and frequency band selection signal to the LNB on the same feed line as the downlink carrier. • **None**: no power or frequency band selection signal is provided • **13V/0kHz**: 13 VDC signal is provided • **13V/22kHz**: 13 VDC signal and frequency band selection signal is provided • **18V/0kHz**: 18 VDC signal is provided • **18V/22kHz**: 18 VDC signal and frequency band selection signal is provided
Enable Clock Reference on RX	Select this check box to send a 10 MHz reference frequency on the same feed line as the downlink carrier. Do not select the check box if the LNB uses an internal crystal oscillator or uses a dielectric oscillator. For more information about the reference clock, see The Reference Clock.

3.5 Controlling Traffic

Navigate to **Dashboard > Shaping and QoS** to:

- set the rules to classify and shape IP traffic that enters the MDM5010, see Defining the Classification Rules and Nodes
- control the delay of baseband frames, see Controlling the Delay
- change the VLAN tag of IP traffic that leaves the MDM5010, see Changing the VLAN ID

3.5.1 Defining the Classification Rules and Nodes

Navigate to **Dashboard > Shaping and QoS > Classification Rules** to classify incoming IP traffic in *Nodes* and specify how they are to be shaped.

For more information about classification and shaping, see Quality of Service.

Parameter	Description
GSE Output Interface	Indicates through which data interface traffic is leaving the MDM5010. The default interface is data1, see Data Interfaces.
Forwarding Mode	Indicates if the MDM5010 acts as a layer 2 Ethernet bridge, or as a layer 3 IP router.

Use the following steps to create a node with corresponding classification rule. You can create up to 40 nodes. :

1. Click + Add. A new window appears.
2. Enter the name of the node. The name must be unique and can only include alphanumeric characters, dash (-), underscore (_), and the at symbol (@). It cannot include any spaces. The maximum length of the name is up to 30 characters.
3. Enter the confirmed information rate (CIR). This is the guaranteed or minimum data traffic rate. Valid values are from 0 Mbps to 1000 Mbps. The default value is 0 Mbps.
4. Enter the peak information rate (PIR). This is the maximum data traffic rate. Packets that exceed this rate will be queued, and possibly dropped. Valid values are from 0 Mbps to 1000 Mbps. The default value is 10 Mbps.
5. Enter the priority. The priority specifies if traffic should be treated with higher priority over other traffic. The lower the value, the higher the priority. Valid values are from 0 to 99. The default value is 50.
6. Enter the maximum queue time. The maximum queue time specifies the maximum time a packet can stay in the queue before being dropped. The queue is filled with packets at the data rate of the customer application, but the packets are queued only for the maximum queue time (and up to the

queue size (50 MB)). If traffic is bursty, the timeout should be large enough.
Valid values are from 0 ms to 2000 ms. The default value is 100 ms.

7 Set the expression to match the node, see Classification Expressions. This field is mandatory when the node is enabled.

8 Enter the matching order. This value specifies the order in which the classification rules must be applied to incoming traffic. Valid values are from 1 to 99. The rule with the lowest matching order value is tried first. When there is a match, the classification stops; when there is no match, the rule with the next lowest matching order value is tried, and so on.

NOTE - Give the highest matching order value to a catch-all traffic rule.

9 Click **Create** to add the node or click **Cancel** to discard the node.

To activate or deactivate the node, click the *Enable* check box. When the check box is not selected, the node is not active.

CAUTION: If there are no active nodes, or no nodes have been created, then all traffic is dropped.

CAUTION: Traffic that does not match an active node is dropped.

To edit a node, click a field and change the value.

NOTE - You cannot edit the name.

To delete a node, click in front of the rule, and then click **Confirm**.

The *Monitoring* section shows performance parameters for the overall incoming traffic and for the individual nodes:

Field...	Shows...
Forward Bit Rate	the rate at which the encapsulator (shaper) forwards bits.
Forward Packet Rate	the rate at which the encapsulator (shaper) forwards packets.

Field...	Shows...
Dropped Bytes	the number of dropped bytes due to exceeding the PIR value, or the maximum queue timeout.
Dropped Packets	the number of dropped packets due to exceeding the PIR value, or the maximum queue timeout.
Average Delay	the average time for a packet to enter and leave the queue. This parameter is only available per node.

The *Monitoring* section also shows the traffic rate of the overall outgoing traffic:

Field...	Shows...
Return Bit Rate	the rate at which the decapsulator forwards bits.
Return Packet Rate	the rate at which the decapsulator forwards packets.

NOTE - The rates include overhead. When the forwarding mode is layer 2, the overhead includes layer 2 and 3 overhead. When the forwarding mode is layer 3, the overhead includes layer 3 overhead only.

NOTE - Click to trend the measured values over time, see Monitoring Parameter Trends.

To reset the metrics, click **Reset Counters**. The reset button is only available when logged in as expert.

3.5.2 Controlling the Delay

Navigate to **Dashboard > Shaping and QoS > Delay Control** to control the delay of baseband frames for optimizing the encapsulation stream. For more information about encapsulation, see GSE Encapsulation and Baseband Frames.

NOTE - It is recommended to set the packing time larger than the encapsulation time.

NOTE - If the baseband layer efficiency is too low, you may need to increase the values.

The delay is controlled by two parameters:

Parameter	Description
Packing time	The maximum time to fill a baseband frame with GSE packets. When the packing time is exceeded and the baseband frame is not filled, padding is added to the frame. The baseband frame is then sent to the output of the encapsulator. Baseband frames that are filled before the packing time is exceeded, are immediately forwarded. The *Delay Control Mode* field can be set to: • **Optimized for ACM**: The filling of the baseband frames with GSE packets is optimized. As a result, link efficiency is optimized, but extra jitter can be introduced for low-rate and bursty traffic. The encapsulation interval and packing time are dynamically set. The packing time value is always twice the encapsulation interval value. Use this mode for high-rate continuous (quasi non-bursty) traffic. • **Optimized for low jitter**: The baseband frames are transmitted at a steady pace regardless of their filling rate. As a result, jitter is decreased, but link efficiency can also be reduced. The encapsulation interval is set to 1 ms, the packet time is dynamically set. Use this mode for low-speed links with bursty traffic, and applications that are jitter sensitive. • **Manual**: The manual mode enables you to set the *Encapsulation Interval* field and *Packing Time* field. Valid values are from 1 ms to 1000 ms for the encapsulation interval, and from 0 ms to 1000 ms for the packing time.
Encapsulation interval	Interval at which the baseband frames are forwarded from the encapsulator to the FEC encoder.

3.5.3 Changing the VLAN ID

Navigate to **Dashboard > Shaping and QoS > VLAN Re-Tagging** to change the VLAN ID of traffic that leaves the MDM5010.

CAUTION: Only the 802.1Q VLAN ID field of the Ethernet (layer 2) packet is changed. The VLAN IDs of protocols on top of 802.1Q, such as PVST+, are not changed. This could result in conflicting VLAN information inside an Ethernet packet and in traffic being blocked (VLAN is pruned from the trunk interface of the port connected to the MDM5010). For more information, see Traffic Issue when Changing the VLAN ID.

The following steps describe how to create a VLAN translation rule. You can create up to 40 VLAN translation rules.

1 Click + Add. A new window appears.

2 Enter the name of the rule. The name must be unique and can only include alphanumeric characters, dash (-), underscore (_), and the at symbol (@). It cannot include any spaces. The maximum length of the name is up to 29 characters.

3 Enter the VLAN ID in the *From* field. Any packet with this VLAN ID will be translated to the value in the *To* field at the egress point of the MDM5010 (the point at which traffic leaves the MDM5010). Valid values are from 0 to 4095. The default value is 0.

4 Enter the VLAN ID in the *To* field. Any packet with a VLAN ID equal to the value in the *From* field will be translated to this value at the egress point of the MDM5010. Valid values are from 0 to 4095. The default value is 0.

5 Click **Create** to add the VLAN translation rule or click **Cancel** to discard the rule.

To edit a VLAN translation rule, click a field and change the value.

NOTE - You cannot edit the name.

To delete a VLAN translation rule, click  in front of the rule, and then click **Confirm**.

3.6 Managing ACM

Navigate to **Dashboard > ACM** to control and monitor the adaptive coding and modulation (ACM) behavior. This tab enables you to:

- enable ACM, see Enabling ACM
- define the ACM behavior, see Modeling the ACM Behavior and MODCODs

For more information about ACM, see Adaptive Coding and Modulation.

3.6.1 Enabling ACM

Navigate to **Dashboard > ACM > Setup** to enable ACM.

Parameter	Description
Enable ACM	When this check box is selected, the ACM controller of the MDM5010 is enabled, and the adaptive coding and modulation technique is applied on the transmit carrier of the local modem (this MDM5010).The ACM client of the MDM5010 is always enabled.
ACM Signaling MODCOD	Specifies the MODCOD to use for ACM signaling. Valid values are the DVB-S2 QPSK MODCODs, excluding QPSK 9/10.

The screen always shows the ACM parameters from the ACM client of the local modem. These parameters are based on the downlink carrier received from the remote modem. If ACM is enabled on the remote modem, the ACM client of the local modem sends the ACM feedback to the remote modem, and the remote modem adapts the MODCOD of its uplink carrier accordingly.

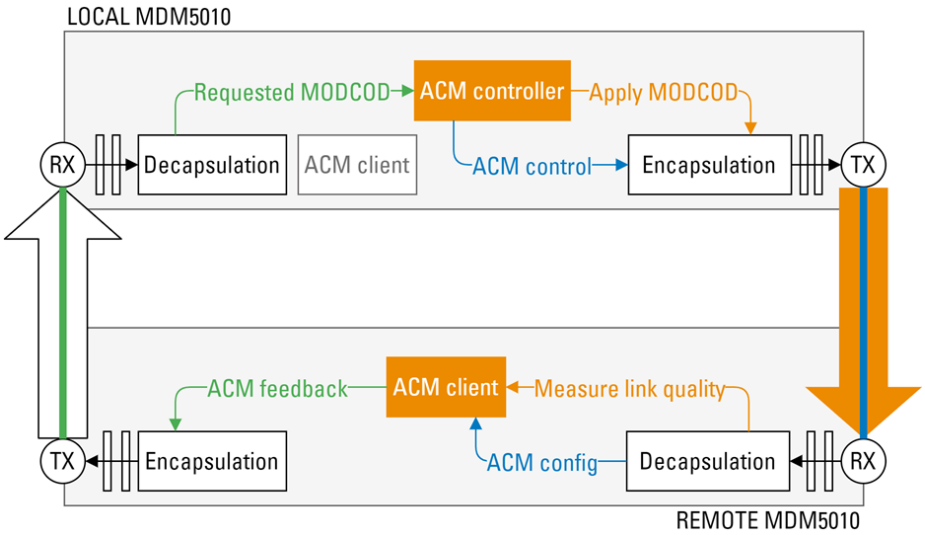
Field...	Shows...
Fading Estimation Margin	the estimated fading margin based on the measured Es/No.
Requested MODCOD	the MODCOD that is requested based on the link quality of the received carrier. The value is **No Request** when ACM is not enabled in the remote modem.
Reference Es/No	the measured Es/No value of the downlink carrier.
Corresponding QEF Es/No	the quasi error-free Es/No value that corresponds with the requested MODCOD. This is a fixed value stored on the MDM5010. A transmission is considered error-free when the packet error rate at reception is less than 10-3.

When ACM is enabled on the local modem, the screen also shows the following parameters:

Field...	Shows...
Transmit MODCOD Used	the MODCOD that the local MDM5010 is currently transmitting. This value should follow the *Requested MODCOD* value shown in the GUI of the remote modem.
Receive Es/No	the header Es/N0 value of the received carrier at the remote modem. This value is measured at the remote modem and sent to the local modem (this MDM5010) in ACM feedback messages.
Receive Link Margin	the link margin of the received carrier at the remote modem. This value is measured at the remote modem and sent to the local modem (this MDM5010) in ACM feedback messages.

NOTE - Click to trend the measured values over time, see Monitoring Parameter Trends.

The figure below shows a simplified diagram where ACM is enabled on the local MDM5010, but not on the remote MDM5010.



The ACM controller and client of the local modem are enabled, but the ACM client is not active. The ACM controller of the remote modem is not enabled, the ACM client is enabled and provides ACM feedback to the local modem.

The MODCOD of the uplink carrier of the local MDM5010 is adapted according to the link quality measured at the remote MDM5010.

For more information about ACM, see Adaptive Coding and Modulation.

3.6.2 Modeling the ACM Behavior

Navigate to **Dashboard > ACM > Tuning** to define the rules for the adaptive coding and modulation behavior. The ACM controller of the local modem (this MDM5010) forwards these settings, except the *Additional ACM Margin*, to the ACM client of the remote modem.

For more information about ACM, see Adaptive Coding and Modulation.

Parameter	Description
MODCOD Selection Algorithm	Specifies the link characteristic that is used for selecting the MODCOD. The value can be set to: • **Header Es/No**: The remote MDM5010 estimates the signal quality by measuring the signal to noise level using the frame headers only. The header Es/No value can be inaccurate for low symbol rates, as the number of headers to use for the measurement is limited. • **Link Margin**: The remote MDM5010 estimates the signal quality by measuring the link margin using the frame data. • **C/ND**: The remote MDM5010 estimates the signal quality by measuring the carrier to noise+distortion level using the frame data.
MODCOD Tuning	This field enables you to manually set the ACM margins per MODCOD, or to use the same ACM margins for all MODCODs. See MODCODs. **CAUTION:** It is recommended to set the value to Automatic and to keep the default values for the margins.
Minimum Margin	Specifies the margin on top of the minimum signal quality required to keep using the MODCOD. This field is not available when *MODCOD Tuning* is set to **Manual**. Valid values are from -10 dB to +30 dB. The default value is 0 dB.
Target Margin	Specifies the margin on top of the minimum signal quality required for using the MODCOD. This field is not available when *MODCOD Tuning* is set to **Manual**. Valid values are from -10 dB to +30 dB. The default value is 0.3 dB.
Minimum MODCOD Maximum MODCOD	These fields specify the range from which a MODCOD can be selected. The range can be narrowed down to optimize the satellite link throughput or availability. By default, the minimum and maximum allowed MODCOD is set to the lowest and highest MODCOD enabled in the **MODCODs** tab, see MODCODs.
Additional ACM Margin	Defines an extra safety margin that is added to the minimum and target margin. Valid values are from -10 dB to +30 dB. The default value is 0 dB.

NOTE - This is a local ACM client setting and affects the margins that the local ACM client receives from the remote ACM controller.

3.6.3 MODCODs

Navigate to **Dashboard > ACM > MODCOCS** to view the MODCODs and corresponding margins that can be used for ACM.

MODCODs can be enabled or disabled. When disabled, the MODCOD cannot be selected for ACM. Limiting the number of MODCODs can increase efficiency. All MODCODs are enabled by default.

NOTE - The table lists all MODCODs. Keep in mind that the available MODCODs for ACM can be limited by the Minimum and Maximum MODCOD field in the Tuning tab.

NOTE - AUPC and ACM use the same MODCOD to communicate. The values of those two MODCODs stay in sync in the GUI: if you change the value in one configuration pane, the other is automatically also changed.

When the *MODCOD Tuning* field in the **Tuning** tab is set to **Automatic**, the *Minimum* and *Target Margin* is the same for all MODCODs and is set in the **Tuning** tab. The *Distortion Margin* is always 0 dB.

When the *MODCOD Tuning* field in the **Tuning** tab is set to **Manual**, the ACM margins can be manually set per MODCOD. Changing the margins can help to achieve higher efficiency (smaller margins) or more robustness (larger margins).

CAUTION: Limiting MODCODs and changing margins manually can reduce efficiency when not done properly. Contact ST Engineering iDirect customer support for assistance.

For more information about ACM, see Adaptive Coding and Modulation.

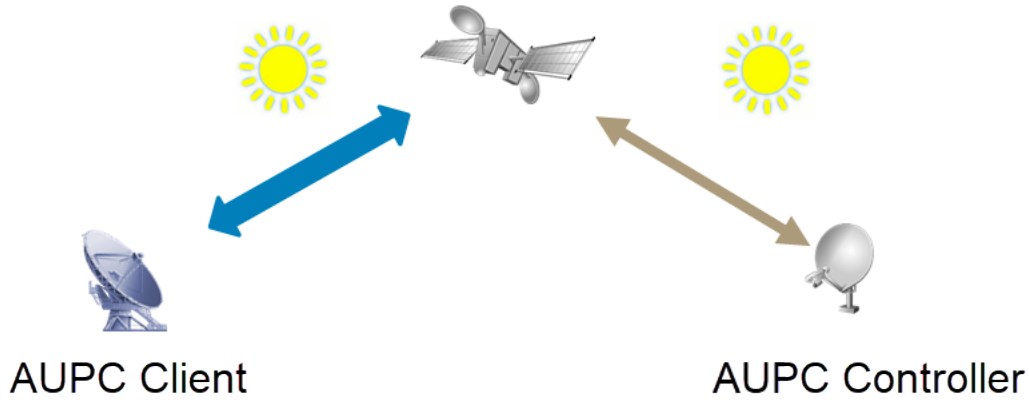
3.7 Managing AUPC

Navigate to **Dashboard > AUPC** to configure the Automatic Uplink Power Control (AUPC) settings and view AUPC client and controller parameters.

3.7.1 AUPC Overview

The AUPC feature on the MDM5010 SCPC Satellite Modem controls the uplink modulator power level in response to uplink fading events. Its goal is to keep a constant power level at the same satellite input.

In an AUPC deployment, one MDM5010 acts as a controller and another as a client. The controller and client are in a point-to-point arrangement, each broadcasting AUPC messages.



When enabled, the AUPC controller adjusts the uplink modulator power level upwards or downwards as required. These adjustments are made in response to data from the AUPC client, which monitors the input level and the Es/No value. If the AUPC controller is disabled, the uplink modulator power specified in the MDM5010 configuration is used.

3.7.2 AUPC Configuration Considerations

- AUPC should be calibrated with the actual terminal and hub equipment in clear sky conditions (without uplink and downlink fades).
- AUPC should only be used for links where the uplink SNR is significantly smaller than the downlink SNR. The antenna of the AUPC controller should be smaller than that of the AUPC client.
- ST Engineering iDirect recommends using AUPC with the Adaptive Coding and Modulation (ACM) feature. The goal of AUPC is to improve the uplink, and that of ACM is to improve the downlink. Refer to Managing ACM for information about how to configure ACM.

3.7.3 AUPC Configuration Overview

1. Prepare both MDM5010 units by configuring them to pass traffic. ST Engineering iDirect recommends that actual traffic be flowing when you enable AUPC.
2. Temporarily disable the AUPC controller.
3. Enable the AUPC client and enter the carrier's expected input level and the expected signal-to-noise ratio (SNR) value in dBm. Alternatively, without enabling the AUPC client, you can use the demodulator's carrier input level and Es/N0 header monitoring values.
4. Configure the maximum output power, maximum step up and maximum step down values on the AUPC Controller.
5. Enable the AUPC Controller.
6. Specify which MODCOD the AUPC controller and client will use for communication over the control plane.

3.7.4 AUPC Client Settings

Navigate to **Dashboard > AUPC > Client** to configure AUPC client settings.

Parameter	Description
AUPC client enable	Turn AUPC client functionality on or off.
Nominal input level	Expected input level of the carrier in dBm.
Nominal Es/N0	Expected signal-to-noise ratio (SNR) value in dBm.

3.7.5 AUPC Controller Settings

Navigate to **Dashboard > AUPC > Controller** to configure the AUPC controller with the desired modulator values.

Parameter	Description
AUPC controller enable	Turn AUPC controller functionality on or off.
Maximum output power	Enter the maximum uplink modulator power level in dBm.

Parameter	Description
Maximum power step up	Define how fast fading will be compensated, or, in other words, configure how much dBm (power) is added per second by the controller during fading. This value is typically set to 0.1 dBm/100 ms, the factory default.
Maximum power step down	Define how fast the power decrease is done, or, in other words, how much dBm is removed per second by the controller. This value should be faster than the power step up value and is typically set to 0.5 dBm/100 ms.

3.7.6 Control Plane Signalling

Navigate to **Dashboard > AUPC > Control Plane Signalling** to select the MODCOD used for control plane signalling.

Parameter	Description
Control Plane Signalling MODCOD	Specify which MODCOD the AUPC controller and AUPC client will use to communicate over the control plane. The default MODCOD is QPSK 3/4. **NOTE -** AUPC and ACM use the same MODCOD to communicate. The values of those two MODCODs stay in sync in the GUI: if you change the value in one configuration pane, the other is automatically also changed.

3.7.7 AUPC Monitoring Information

3.7.7.1 AUPC Client Monitoring Information

At the right of the screen several AUPC client parameters are monitored:

Field	Description
State	This field indicates the current state of the AUPC client: • off = disabled (in fact, in this case the monitoring table will be empty) • no lock = the AUPC client is not receiving a valid Es/No value reading from the demodulator; this corresponds with demodulator out of lock • waiting for controller = the AUPC client has not received a poll message from theAUPC controller in 30 seconds or more (in this state the AUPC client is also not sending feedback) • reporting = AUPC is working as expected: the AUPC client is receiving poll messages and sending feedback messages
Input level	The carrier input level of the demodulator, in dBm.
Es/N0	The Es/N0 header in dB of the demodulator.
Current Power compensation	The last power compensation in dB as read from the previous AUPC controller poll message. If this last poll message is over 30 seconds old, this value is "Unknown".

3.7.7.2 AUPC Controller Monitoring Information

At the right of the screen several AUPC controller parameters are monitored:

Field	Description
Requested output power	The desired final output power. This is the nominal power if the physical layer efficiency is lower than 50%. Otherwise, this value is the nominal output power and the fading estimate. This number is capped so that it does not exceed the maximum output power and minimum output power (minimum is the nominal output power).
Current output power	The current modulator power.

3.8 Managing Bandwidth Cancellation

Navigate to **Dashboard > Bandwidth Cancellation** to enable and manage bandwidth cancellation.

Bandwidth cancellation (BWC) is a technology that enables the transmitted and received carrier at the MDM5010 to use the same satellite frequency band.

Bandwidth cancellation uses the information of the transmitted uplink carrier to extract the echoed uplink carrier from the aggregate carrier, leaving only the carrier from the remote. The echoed uplink carrier is different from the transmitted uplink carrier due to its travel over the satellite. The better the effects of this travel can be estimated, the better the echoed uplink carrier can be cancelled, and the higher the quality of the remaining carrier will be.

For more information, see Bandwidth Cancellation.

NOTE - Bandwidth cancellation cannot be used when the backup carrier is enabled.

NOTE - When using BWC, make sure that the value of the PL Scrambler Signature field of the local modulator and remote demodulator are set to 0, and that the value of the PL Scrambler Signature field of the local demodulator and remote modulator are set to 1. To set the value of the PL Scrambler Signature field, see Defining the Uplink Carrier and Defining the Downlink Carrier.

Parameter	Description
Enable Bandwidth Cancellation	When this check box is selected, bandwidth cancellation is active. The check box is not visible when the backup carrier is enabled.
Expected Round-Trip Delay	Specifies the expected delay that the uplink carrier experiences when traveling from the MDM5010 to the satellite and back. Monitor the delay and change this value accordingly. Valid values are from 0 ms to 500 ms. The default value is 250 ms.
Round-Trip Delay Search Window	Specifies the round-trip delay uncertainty. Start with a large value. Lower the value when bandwidth cancellation is locked to reduce the acquisition time. Make sure to always set a window size to catch delays due to the Doppler effect. Valid values are from 1 ms to 100 ms. The default value is 20 ms.
Local Carrier Receive Frequency Offset	Specifies the offset of the echoed uplink carrier from the received carrier. For symmetrical links this offset can be set close to 0 MHz. For asymmetrical links, this is the difference between the estimated frequency of the echoed uplink carrier and the frequency of the received carrier. Monitor the offset and change this value accordingly. Valid values are from -100 MHz to 100 MHz. The default value is 0 MHz.

Parameter	Description
Local Carrier Receive Search Window	Specifies the echoed uplink carrier frequency uncertainty. Start with a large value. Lower the value when bandwidth cancellation is locked to reduce the acquisition time. Valid values are form 0.05 MHz to 7.5 MHz. The default value is 0.05 MHz.
Local Carrier Spectrum Inversion	Specifies if the BWC must invert the spectrum or not. When the value is set to *Automatic*, BWC continuously toggles between *Inverted* and *Direct* spectrum. Monitor the spectral inversion and change this value accordingly to optimize the cancellation.
Bandwidth Mode	This field can be used to fine-tune the BWC performance. • **Normal**: This is the default mode and provides the best results in most cases. • **Robust**: Use this mode when symbol rates are low, or when phase noise is present. This can increase the acquisition time. • **Fine**: Use this mode when symbol rates are high (> 20 Mbaud), or high local/remote imbalance ratios. This will decrease the acquisition time.
Dummy PL Scrambler Mode	Specifies how dummy PL frames are scrambled. • Set the value to **DVB-S2 Standardized Reset** to reinitialize the randomization sequence at the end of each PL frame header. This is the standard way of PL scrambling in DVB-S2(X). • Set the value to **Continuous** if the randomization sequence should not be reinitialized. As a result, the dummy PL frames will be more random, which makes it easier for the BWC to measure the delay between the transmitted and echoed carrier. **NOTE:** The continuous mode is not DVB compliant.

At the right of several bandwidth cancellation parameters are monitored:

Field...	Shows...
Bandwidth Cancellation State	if bandwidth cancellation is on or off. When BWC is on, the state can be *Searching* or *Locked*. When locked, cancellation is fully operational.
Round-Trip Delay	the round-trip delay measured by BWC. Use this value to update the *Expected Round-trip Delay* field.
Local To Total Carrier Power Ratio	the ratio of the power level of the aggregated carrier and the power level of the echoed uplink carrier measured by BWC. The value should be between -10 dB and 0 dB. If not, adjust the output level of the carriers.
Local To Remote Carrier Power Ratio	the ratio of the power level of the echoed uplink carrier and the power level of the received carrier measured by BWC. The value should be between -10 dB and 10 dB. If not, adjust the output level of the carriers.

Field...	Shows...
Local Carrier Level	the power level of the echoed uplink carrier measured by BWC.
Local Carrier Tracked Symbol Rate	the symbol rate of the echoed uplink carrier measured by BWC.
Local Carrier Frequency Offset	the frequency offset of the echoed uplink carrier measured by BWC. Use this value to update the *Local Carrier Receive Frequency Offset* field.
Local Carrier Spectral Inversion	if spectrum inversion has been applied to the echoed uplink carrier or not. Use this value to update the *Local Carrier Spectral Inversion* field.

NOTE - Click to trend the measured values over time, see Monitoring Parameter Trends.

One alarm is monitored:

If alarm...	Is active ( ) then...	Action
Bandwidth Canceller Not Locked	BWC is enabled but not locked (tracking is not successful).	• Disable BWC and verify the power of each carrier (local and remote) • Verify the delay and offset values • Increase the search windows • Adapt the bandwidth mode

If the alarm persists, contact ST Engineering iDirect customer support.

3.9 Using an Antenna Controller

Navigate to **Dashboard > Antenna Controller** to enable and set up the communication channel between the MDM5010 and the antenna controller.

When using an antenna controller for pointing the antenna to the correct satellite, a TCP connection must be established between the antenna controller (server) and the MDM5010 (client). The connection is used to send antenna control parameters from the MDM5010 to the antenna controller, and to exchange control messages during the satellite acquisition process. The control messages are formatted using the OpenAMIP protocol.

For more information, see Antenna Control.

Parameter	Description
Enable Antenna Controller	This check box idicates if the MDM5010 is using an antenna controller or not. When the check box is selected, the antenna controller is used. The parameters below initialize the connection between the MDM5010 and the antenna controller, and provide information necessary for controlling the antenna.
IP Address	Enter the *IP Address* of the antenna controller. NOTE: Make sure that the IP address of the antenna controller belongs to the same address range as the management IP address of your MDM5010.
Port	TCP *Port* at which the antenna controller is listening for control messages from the MDM5010. Valid values are from 1 to 65535. The default value is 12345.
Connection Timeout Tolerance	Specifies the time between the TCP connection timeout and the trigger of the *Controller Communication Error* alarm. Valid values are from 0 seconds to 120 seconds. The default value is 5 seconds
Satellite Longitude	Specifies the geographical longitude of the satellite in degrees East.
Satellite Latitude Variance	Specifies the maximum drift in degrees North from the latitude of the satellite
Satellite Polarity Skew	Specifies the angle at which the satellite's polarization planes are inclined with respect to the equatorial plane.
RX Polarization	The *RX Polarization* field specifies the polarization that the antenna is receiving, and the *TX Polarization* field specifies the polarization that the antenna is transmitting. The polarization can be horizontal, vertical, left-handed circular, or right-handed circular.
TX Polarization	
RX LO Conversion Frequency	Specifies the local oscillator frequency of the LNB.

Parameter	Description
TX LO Conversion Frequency	Specifies the local oscillator frequency of the BUC.
Short Axis Max Skew	The *Short Axis Max Skew* field is used for antennas with a non-circular radiation pattern and specifies the maximum allowed skew of the beam short axis to the geosynchronous arc. When the maximum skew value is exceeded, the MDM5010 should stop transmitting to avoid that an adjacent satellite enters the antenna beam.

At the right of the screen several antenna control parameters are monitored:

Field...	Shows...
Keep Alive Interval	the frequency at which the antenna controller sends TCP keep-alive packets to the MDM5010. If the antenna controller does not receive a response for three consecutive TCP keep-alive packets, the connection reaches the connection timeout.
Antenna Functional Status	• **OK** if the antenna is working • **Off** if the antenna is not operating • **Unknown** if the status of the antenna is unknown
TX Allowed Status	• **Yes** if the MDM5010 can transmit • **No** if the MDM5010 is not allowed to transmit because the antenna controller has detected a condition such as loss of lock, blockage, cable unwrap, or max skew exceeded • **Unknown** if the status is not known
Antenna Latitude	the geographical latitude of the antenna location in degrees North.
Antenna Longitude	the geographical longitude of the antenna location in degrees East.
Transmitted Message Counter	the number of control messages sent to the antenna controller. This number should increment.
Received Message Counter	the number of control messages received from the antenna controller. This number should increment.

NOTE - Click  to trend the measured values over time, see Monitoring Parameter Trends.

Two alarms are monitored:

If alarm...	Is active ( ) then...	Action
Controller Communication Error	the TCP/IP connection between the MDM5010 and the antenna controller is down, and a configurable timeout has exceeded.	• Make sure that the address in the *IP Address* field is correct, and in the same range as the management IP address of the MDM5010 • Make sure that the TCP port in the *Port* field is correct • Check the hardware connection between the MDM5010 and antenna controller
Antenna Controller Failure	the antenna controller is unavailable due to bad configuration, or equipment failure.	• Make sure that the antenna controller is powered on • Make sure that the configuration of the antenna controller is valid

3.10 Modem Setup

Navigate to **Dashboard > Modem Setup** to:

- configure the interfaces, see Managing the Management Interfaces and Managing the Data Interfaces
- enable device and link redundancy, see Setting Up Redundancy
- manage a remote device, see Managing a Remote Device
- control access, see Controlling Access
- activate the automatic saving of application-specific configuration changes, see General Settings
- manage the reference clock, see General Settings

3.10.1 Managing the Management Interfaces

Navigate to **Dashboard > Modem Setup > Management Interfaces** to define the interfaces through which the MDM5010 can be managed, and view the status, performance parameters, and any alarms.

Carefully design your management network setup. At least one of the management Ethernet interfaces should be connected to your management network. The other interface can be used as a second interface for management access, or the interfaces can operate as a single bond interface if link redundancy is required.

CAUTION: Take care when changing management interface settings. Changes are effective immediately. Wrong settings can block access to the MDM5010.
Only disable an interface when you are sure you can access the MDM5010 using the other management interface.

3.10.1.1 mgmt1 and mgmt2

Parameter	Description
Enable check box	Indicates if the management Ethernet interface is administratively up or down. When the check box is selected, the interface is up. An interface that is not up, cannot be used. By default, *mgmt1* is up. The interfaces are always enabled when link redundancy is enabled, see Setting Up Redundancy.

Parameter	Description
MTU	Specifies the maximum payload that can be encapsulated in an Ethernet frame. For example, the MTU size of a standard Ethernet frame is 1,500 bytes; this is the default value. Valid values are from 68 to 9,582 bytes. Use the REST API or CLI to configure Ethernet interface settings such as auto-negotiation, port speed, and duplex mode.

3.10.1.2 IP Addressing

Parameter	Description
IP Address/Prefix	Specifies the IP address of the interface and the subnet (CIDR notation) to which the IP address belongs.
Virtual IP Address/Prefix	Used for device redundancy. For more information about link redundancy, see Device Redundancy.
State	Iindicates if the interface has a valid IP address (✔) or not (✖). If the status of the Ethernet interface is not OK, this field will also indicate ✖.

3.10.1.3 IP Routes

The default gateway in the data routing table is the access point for the data ports of the device. Other routing table configuration parameters define the exact destination of data. You can define a maximum of 20 routes.

Field	Description
Default Gateway	Access point for the data ports of the device, which is used to reach a subnet. **NOTE**: The default gateway cannot be deleted.
Subnet	Destination subnet to which the forwarding route applies.
Interface	interface to which the forwarding route applies.
Gateway	Enter the IP address for the default IP gateway.
State	Operational state of the route.
Name	Enter the name of the route. The name must be unique, and the maximum length of the name is up to 100 characters.

3.10.1.4 Management Interface Status and Performance

The status and performance parameters of the management interfaces are shown at the right of the screen.

Field...	Shows...
Status	if the Ethernet interface detects a signal (✔) or not (✖). See also *Ethernet Link* alarm.
Link State	the status of the link. The following states exist: • Link Down • 10Bt Half Duplex • 10Bt Full Duplex • 100Bt Half Duplex • 100Bt Full Duplex • 1000Bt Full Duplex
Input Packets	the number of good packets that have been received on the management interface.
Output Packets	the number of packets that have been transmitted by the management interface successfully.
Input Dropped Packets	the number of incoming packets that could not be processed, for example, because of lack of resources or unsupported protocol.
Output Dropped Packets	the number of outgoing packets that have been dropped, for example, because the interface is saturated.

NOTE - Click to trend the measured values over time, see Monitoring Parameter Trends.

3.10.1.5 Management Interface Alarms

Alarms are displayed for enabled interfaces (mgmt1, mgmt2, or mgmt). If an alarm persists, contact ST Engineering iDirect customer support.

If alarm...	Is active (⊗) then...	Action
Ethernet Link	no signal is detected on the physical management interface.	Make sure that the cable is intact and properly connected.

If alarm...	Is active (⊗) then...	Action
Ethernet Half Duplex	the management interface is in half duplex mode as a result of a link negotiation. The alarm does not occur when the interface is configured in half duplex mode.	• Make sure that auto-negotiation is enabled on the managing device • Disable auto-negotiation and manually set the duplex mode
Ethernet Interface	link redundancy is enabled but no signal is detected on either physical management interface.	See *Ethernet Link* alarm.
Ethernet Redundancy Degraded	link redundancy is enabled but only one physical management interface detects a signal.	See *Ethernet Link* alarm.

3.10.2 Managing the Data Interfaces

Navigate to **Dashboard > Modem Setup > Data Interfaces** to define the logical data interfaces and view the status, performance parameters, and any alarms. For more information about the logical data interfaces, see Data Interfaces.

Carefully design your data network setup. The logical data interfaces can be configured as two independent interfaces, or as a single bond interface if link redundancy is required. An interface can also have a virtual IP address for facilitating device redundancy.

CAUTION: Take care when changing data interface settings. Wrong settings can impact traffic. Disabling a data interface can impact traffic.

3.10.2.1 data1 and data2

Parameter	Description
Enable check box	If the logical data interface is administratively up or down. When the check box is selected, the interface is up. An interface that is not up, cannot be used. The interfaces are always enabled when link redundancy is enabled, see Setting Up Redundancy.
MTU	Specifies the maximum payload that can be encapsulated in an Ethernet frame. For example, the MTU size of a standard Ethernet frame is 1,500 bytes; this is the default value. Valid values are from 68 to 9,582 bytes. Use the REST API or CLI to configure Ethernet interface settings such as auto-negotiation, port speed, and duplex mode.

3.10.2.2 IGMP Version

Parameter	Description
IGMP Version	Specifies the version of the IGMP protocol. IGMP allows the MDM5010 to join the multicast group specified in the *IP Multicast* table.

3.10.2.3 IP Addressing

Parameter	Description
IP Address/Prefix	Specifies the IP address of the interface and the subnet (CIDR notation) to which the IP address belongs.
Virtual IP Address/Prefix	Used for device redundancy. For more information about link redundancy, see Device Redundancy.
State	Indicates if the interface is up and detects a signal (✔) or not (✖). **NOTE -** When link redundancy is enabled, only the bond interface (data) is displayed. For more information about link redundancy, see Link Redundancy.

3.10.2.4 IP Multicast

Click + Add to specify the IP multicast streams that the MDM5010 should receive. You can create up to 20 IP multicast streams.

CAUTION: Make sure that there is node that matches the multicast stream, see Defining the Classification Rules and Nodes.

- Click **Create** to add the multicast stream or click **Cancel** to discard the multicast stream.
- To edit a multicast stream, click a field and change the value.
- To delete a multicast stream, click  in front of the rule, and then click **Confirm**.

Parameter	Description
Name	Name of the multicast stream. The name must be unique, and the maximum length of the name is up to 100 characters.

Parameter	Description
Interface	Interface that receives the multicast stream. This field is optional..
Multicast Address	IP multicast address. Valid IP multicast addresses are in the range 224.0.0.0 through 239.255.255.255.
Source address A Source address B	When the *IGMP Version* is set to **v3**, *Source Address A* and *B* of the multicast stream can be set.

3.10.2.5 IP Routes

The default gateway in the data routing table is the access point for the data ports of the device. Other routing table configuration parameters define the exact destination of data. You can define a maximum of 20 routes.

Field	Description
Default Gateway	Access point for the data ports of the device, which is used to reach a subnet. **NOTE**: The default gateway cannot be deleted.
Subnet	Enter the destination subnet to which the forwarding route applies.
Interface	Select the data interface.
Gateway	Enter the IP address for the default IP gateway.
State	Operational state of the route.
Name	Enter the name of the route. The name must be unique, and the maximum length of the name is up to 100 characters.

3.10.2.6 Data Interface Status and Performance

The status and performance parameters of the data interfaces are shown at the right of the screen.

Field	Description
Link State	the status of the link. The following states exist: • Link Down • 10bt Half Duplex • 10bt Full Duplex • 100bt Half Duplex • 100bt Full Duplex • 1000bt Full Duplex
Input Bytes	the number of good bytes that have been received on the data interface. This includes Ethernet overhead.
Input Packets	the number of good packets that have been received by the data interface.
Input Dropped	the number of incoming packets that could not be processed, for example, because of lack of resources or unsupported protocol.
Input Errors	the number of bad packets that have been received on the data interface. A bad packet is, for example, a packet with a CRC error or invalid packet length.
Output Bytes	the number of bytes that have been transmitted by the data interface successfully. This includes Ethernet overhead.
Output Packets	the number of packets that have been transmitted by the data interface successfully.
Output Dropped	the number of outgoing packets that have been dropped, for example, because the interface is saturated.
Output Errors	the number of transmit errors, for example, because of late collisions.

NOTE - Click to trend the measured values over time, see Monitoring Parameter Trends.

To reset the metrics, click **Reset Counters**.

NOTE - The reset button is only available when logged in as expert user.

3.10.2.7 Data Interface Alarms

Alarms are displayed for enabled interfaces (data1, data2, data). If an alarm persists, contact ST Engineering iDirect customer support.

If alarm...	Is active (⊗) then...	Action
Ethernet Link	no signal is detected on any of the physical data ports that are part of the logical data interface. See Data Interfaces.	Make sure that the cable is intact and properly connected.
Ethernet Half Duplex	all physical data ports that are part of the logical data interface are in half duplex mode as a result of a link negotiation.	• Make sure that auto-negotiation is enabled on the connected device • Disable auto-negotiation and manually set the duplex mode
Ethernet Interface	link redundancy is enabled but no signal is detected on either logical data interface.	See *Ethernet Link* alarm.
Ethernet Redundancy Degraded	link redundancy is enabled but only one logical data interface detects a signal.	See *Ethernet Link* alarm.

3.10.3 Setting Up Redundancy

Navigate to **Dashboard > Modem Setup > Redundancy** to configure device redundancy and link redundancy.

Device redundancy is achieved using a Universal Switching System (USS). The supported redundancy scheme is N+1, where there are N (can be 1) active MDM5010s and one standby MDM5010. For more information, see Device Redundancy.

NOTE - When redundancy is set up, the Spanning Tree Protocol (STP) should be used to prevent bridge loops.

3.10.3.1 Device Redundancy

Parameter	Description
Enable check box	When the check box is selected, the MDM5010 is considered as part of a redundant setup.

Parameter	Description
Initial State	Specifies the redundancy role in which the MDM5010 is set when redundancy is enabled, or after a reset. If the redundant setup is not up and running, the MDM5010 will be in the initial state. When the state is standby, the MDM5010 will not transmit or receive data. When the redundant setup is up and running, the USS will ensure that all but one MDM5010 is active.
Operational State	the redundancy role of the MDM5010. The following states exist: • Active; the MDM5010 is the active device • Standby; the MDM5010 is the standby device • N/A; device redundancy is disabled

3.10.3.2 Management Link Redundancy

Link-level redundancy protects against loss of link connectivity; if one link fails, the other can take over and restore traffic forwarding that had been previously sent over the failed link. The redundant interfaces act as one bond interface. The MDM5010 supports link redundancy for both the management and logical data interfaces. For more information, see Link Redundancy.

Parameter	Description
Enable check box	Indicates if the link redundancy is enabled or disabled. When the check box is selected, link redundancy is enabled, and the physical interfaces are joined into one bond interface (*mgmt* / *data*). NOTE - Enabling link redundancy automatically enables the physical interfaces, see Managing the Management Interfaces and Managing the Data Interfaces.
MTU	Specifies the maximum payload that can be encapsulated in an Ethernet frame. For example, the MTU size of a standard Ethernet frame is 1,500 bytes; this is the default value. Valid values are from 68 to 9,582 bytes.
Protection Mode	If set to **Revertive**, link redundancy will always switch back to the *Preferred Interface* when this one is available.
Interface A Interface B	These fields are linked to the management or data interfaces that are part of the redundant setup.

Parameter	Description
Preferred Interface	Specifies the initial interface to use when redundancy is activated. If this interface becomes unavailable, the other interface will be used. If the *Protection Mode* is set to **Revertive**, the interface will switch back to the preferred interface as soon as this one is available again. If the *Protection Mode* is set to **Non-revertive**, the interface will not switch to the preferred interface even when it is available again.
Operational State	the state of the link redundancy. The following states exist: • OK; both redundant interfaces are up and detect a signal • Degraded; only one of the redundant interfaces is up and detects a signal • Link Down; none of the redundant interfaces detect a signal
Active interface	the interface that is currently used.
Switch Count	the number of times the active interface has switched.

3.10.4 Managing a Remote Device

Navigate to **Dashboard > Modem Setup > Redundancy** to access a remote device over the satellite link through the management interface of this MDM5010. The remote device can be the remote MDM5010 itself or a device behind that modem.

On the local MDM5010:

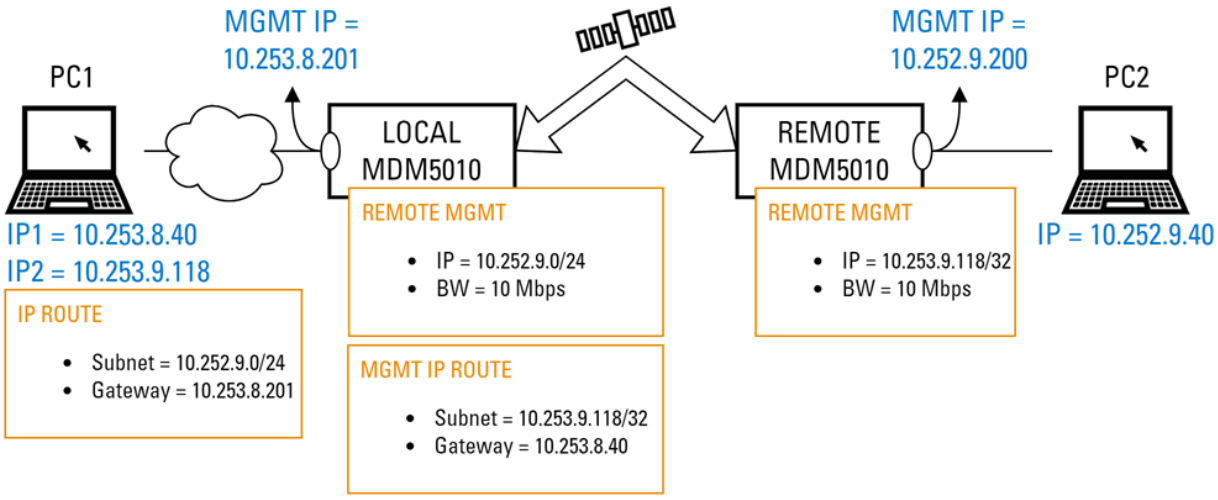
Parameter	Description
Enable check box	To enable or disable management access to a remote device, click the *Enable* check box. When the check box is selected, access is enabled.
IP Address/Prefix	Specifies the management IP address of the remote device. This can also be a range of IP addresses allowing the control of multiple remote devices.  ***CAUTION:*** If layer 2 mode is enabled (see Defining the Classification Rules and Nodes), make sure that the remote management IP addresses and the IP addresses of the management interfaces do not overlap. To avoid overlap, it is recommended to use a single host address (/32 prefix) for remote management.
Bandwidth	Specifies the maximum rate of the management traffic. When there is no remote management traffic, this bandwidth is available for user traffic. The field can be temporarily set to a higher value when, for example, upgrading the software of a remote MDM5010.

To make sure that the remote device can return management traffic, enable remote management on the remote MDM5010 and:

- Set the *IP Address/Prefix* field to the IP address of the managing device (PC1 in the example below).
- Set the *Bandwidth* field to the maximum rate allowed for the management traffic.

NOTE - Make sure that the necessary IP routes have been configured, both on the MDM5010s and your management network.

The figure below shows an example configuration.



From PC1, you can now:

- Browse to 10.252.9.200 to access the GUI of the remote MDM5010
- Send a ping to PC2

When the remote device is an MDM6000, see Typical Setup:

- Set the *IP Address/Prefix* field to the IP address of the management interface of the MDM6000
- Set the *Label* field of the MDM6000 BBF encapsulator and decapsulator for at least one channel to **00:00:00:00:00:02**

```
Tree View / Encapsulation / BBF Encapsulation / Encapsulation Channels > Label

Tree View / Decapsulation / BBF Decapsulation / Decapsulation Channels > Label
```

3.10.5 Controlling Access

Navigate to **Dashboard > Modem Setup > Access Management** to control access to the MDM5010 and configure SNMP trap messages.

The MDM5010 has several control interfaces. Access to the control interfaces can be limited. Before using the MDM5010 in a network, it is recommended to consider which control interfaces should have limited access.

The GUI enables you to control REST API, CLI, SNMP, and SCP access.

Control Interface	Default Access	To enable access, ...
CLI	Disabled	check the *Enable CLI* check box. The *CLI Inactivity Timeout* field specifies the time of inactivity after which the user is logged out. Valid values are from 60 seconds to 5,000,000 seconds. The default value is 600 seconds.
REST API	Disabled	check the *Enable REST API* check box.
SCP	Disabled	check the *Enable SCP* check box
SNMP	Disabled	check the *Enable SNMP* check box in the SNMP section.

When access to a control interface is available, it is recommended to change the default password. For more information, see Changing Login Passwords.

When access to the SNMP interface is enabled, it is recommended to change the read-only and read-write community strings. For more information, see Changing SNMP Community Strings.

To receive SNMP trap messages from the MDM5010, the trap destination, type, and community string must be configured. For more information, see SNMP Traps.

NOTE - Make sure to update the read-only, read-write, and trap community string in the SNMP manager accordingly.

3.10.6 General Settings

Navigate to **Dashboard > Modem Setup > General** to automatically save application-specific and manage the reference clock of the MDM5010.

Parameter	Description
Enable check box	When the check box is selected, any change to the application-specific configuration is saved immediately without manual interaction. The *Auto Save* inidcator in the status bar shows ⚠, and the *Config Saved* indicator always shows ✔.
Active Configuration State	Indicates if the active configuration is saved or not. When the *Enable Auto Save* check box is selected, it is always set to **Saved**. When the check box is not selected, and the active configuration has changed but has not been saved, it is set to **Updated, but not saved**. See Saving the Active Configuration for saving the configuration manually. System-specific configuration is always saved automatically. For more information about application- and system-specific configuration, see The MDM5010 Configuration
Reference Clock Mode	Specifies if the clock reference interface at the rear of MDM5010 is used as an input or output interface. For more information about the reference clock, see The Reference Clock.
Active Clock Reference	When the clock reference interface at the rear of MDM5010 is used as an input, this field indicates if the MDM5010 is using its internal reference frequency, or if it is slaved to an external reference clock which is connected to the clock reference interface. When used as an output, any device connected to the clock reference interface is slaved to the internal reference clock.

3.11 Modem Information

Navigate to **Dashboard > Modem Info**to:

- identify the MDM5010, see Identifying the MDM5010
- set the correct date and time, see Setting Date and Time
- monitor the MDM5010 resources, see Monitoring Resources
- manage the log file, see Managing the Device Log

3.11.1 Identifying the MDM5010

Navigate to **Dashboard > Modem Info > Identification** to view the product information, such as serial number, software version, and license type. If you have a temporary license, the remaining validity period is also indicated. For more information about licenses, see Licenses.

The *Sales Code* field shows which software options have been activated on your MDM5010. For more information about the sales codes, contact your ST Engineering iDirect sales representative.

Edit the *Label* field to set a user-friendly name for your MDM5010. The maximum length of the name is up to 50 characters. The name is displayed in the banner at the top of the GUI screen and in the CLI prompt.

3.11.2 Setting Date and Time

Navigate to **Dashboard > Modem Info > Data and Time** to view and set the date and time on the MDM5010. This setting is used for time stamping the activation and clearance of alarms, and entries in the log file.

Parameter	Description
Date and Time	Indicates the date and time set on the MDM5010.The time zone can be UTC or your local time zone, see Setting the Time in Local Time Zone. • To change the value, click the value field. A window appears. • Enter the date (dd/mm/yyyy or using the calendar button) and time. Click **Set** to confirm. • Click **Sync with this computer** to synchronize the date and time of the MDM5010 with the date and time of your computer.
Enable NTP	Indicates if the MDM5010 uses NTP (Network Time Protocol) to synchronize its clock with other devices in the network (NTP peers). When the check box is selected, NTP is enabled, and the MDM5010 will periodically (every 5 to 10 seconds) query the NTP peers for a time update.
NTP Peers	Add more than one NTP peer to increase the reliability of clock synchronization. You can add up to four NTP peers. The *Peer* is identified by its *IP Address*.

3.11.3 Monitoring Resources

Navigate to **Dashboard > Modem Info > Monitor** to view device resources, such as temperature and CPU usage.

This screen also shows the reason of an internal error. If the internal error is persistent, contact ST Engineering iDirect customer support.

NOTE - Click to trend the measured values over time, see Monitoring Parameter Trends.

3.11.4 Managing the Device Log

The device log contains information about activities within the MDM5010, and can be used to observe, troubleshoot, or debug the MDM5010.

Navigate to **Dashboard > Modem Info >Log** to change the log level of a facility, and to enable or disable logging.

The facility specifies the type of activity that occurred, for example, an alarm, a configuration change, and so on. The level or log severity is a piece of information telling how important a given log message is. For more information, see The Device Log.

Local device logging is enabled by default. Select *Logs* in the *Tasks* list at the left to view, download, or clear the log file. See Viewing the Device Log.

Remote logging can be enabled. The log messages are then sent to a remote syslog server using UDP:

1. Enter the IP address of the syslog server in the *IP Address* field. Make sure that the syslog server is located in your management network and can be reached by the MDM5010.
2. Enter the UDP port at which the syslog server is listening in the *Syslog UDP Port* field.

3.12 Handling the Configuration

The configuration handled in this chapter refers to the application-specific configuration. For more information about the device configuration, see The MDM5010 Configuration.

Select *Device* in the *Tasks* list. Two buttons appear at the top.

Use button...	To...
Configurations	• save the active configuration, see Saving the Active Configuration • import a configuration from your local computer, see Importing a Configuration • load an existing configuration, see Loading a Configuration • export a configuration to your local computer, see Exporting a Configuration • delete a configuration, see Deleting a Configuration • make a configuration the boot configuration, see Changing the Boot Configuration NOTE: The MDM5010 can store up to 48 different configurations.
Reset	delete all saved and unsaved configurations. The MDM5010 is reset to the factory default configuration, see Resetting the Configuration.

3.12.1 Saving the Active Configuration

When the *Config Saved* indicator in the status bar marks , the configuration of the MDM5010 has been changed but has not been saved. Save the configuration to not lose the configuration after a reset, or to easily load the configuration onto the MDM5010 when needed.

NOTE - By default, the MDM5010 has the initialconfig configuration including the factory default settings. It is recommended to save your MDM5010 configuration as a different configuration than initialconfig, to make this new configuration the boot configuration, and to delete initialconfig

To save the active configuration:

1. Select *Device* in the *Tasks* list. The Configurations button appears at the top.
2. Click **Configurations**. The *Configs* window appears.
3. Click **Save...**. The *Save Config* window appears.
4. Enter the configuration name or select an existing configuration from the drop-down list, and then click **Save Config**.

NOTE - When selecting an existing configuration, the configuration will be overwritten with the active configuration.

Another way to overwrite an existing configuration is to click next to the configuration name, and then click **Overwrite**.

After saving the active configuration, the *Config Saved* indicator in the status bar marks .

NOTE - Changes to the application-specific configuration can also be saved automatically, see General Settings.

3.12.2 Importing a Configuration

NOTE - Make sure that the content of the configuration file is correct, and settings comply with the options in your license.

NOTE - Importing a configuration does not load the configuration onto the MDM5010. To load the configuration, see Loading a Configuration.

1. Select *Device* in the *Tasks* list. The Configurations button appears at the top.
2. Click **Configurations**. The *Configs* window appears.
3. Click **Import...**.
4. Navigate to the location of the configuration file (*.xml), select it, and then click **Open**.
5. Read the message and click **Import** if you are sure you want to import the configuration now.

3.12.3 Loading a Configuration

NOTE - The loaded (or active) configuration is marked in bold.

1. Select *Device* in the *Tasks* list. The Configurations button appears at the top.
2. Click **Configurations**. The *Configs* window appears.
3. To load a saved configuration onto the MDM5010, click next to the name of the configuration. The loaded configuration is now the active one.

3.12.4 Exporting a Configuration

An exported configuration file can be used:

- for backup purposes
- for configuring another MDM5010, see Importing a Configuration
- for offline editing
- as input to ST Engineering iDirect customer support in case of technical issues

To export a configuration:

1. Select *Device* in the *Tasks* list. The Configurations button appears at the top.
2. Click **Configurations**. The *Configs* window appears.
3. To export a saved configuration to your local computer, click  next to the name of the configuration. The exported configuration is saved as an .xml file in the *Downloads* folder.

3.12.5 Deleting a Configuration

NOTE - When the active configuration (in bold) is deleted, the *Config Saved* indicator in the status bar marks  , and the configuration must be saved again.

CAUTION: Deleting the boot configuration will reset the boot configuration to the initialconfig file with the factory default configuration.

1. Select *Device* in the *Tasks* list. The Configurations button appears at the top.
2. Click **Configurations**. The *Configs* window appears.
3. To delete a saved configuration, click  next to the name of the configuration.
4. Read the message and click **Delete** if you are sure you want to delete the configuration now.

3.12.6 Changing the Boot Configuration

The boot configuration is the configuration that is loaded onto the MDM5010 at boot-time.

NOTE - By default, the boot configuration is initialconfig. It is recommended to save your MDM5010 configuration in a different configuration than initialconfig, to make it the boot configuration, and to delete initialconfig.

To change the boot configuration:

1. Select *Device* in the *Tasks* list. The Configurations button appears at the top.
2. Click **Configurations**. The *Configs* window appears. The current boot configuration is marked with BOOT.
3. Click Make Boot next to the name of the configuration that you want use as the boot configuration. This configuration now has the BOOT label.

3.12.7 Resetting the Configuration

Resetting the configuration deletes all saved and unsaved configuration. The MDM5010 is reset to the *initialconfig* configuration including the factory default settings.

NOTE - The system-specific configuration is excluded from this reset to avoid losing connectivity with the MDM5010.

CAUTION: This reset includes a software reset, and traffic will be impacted.

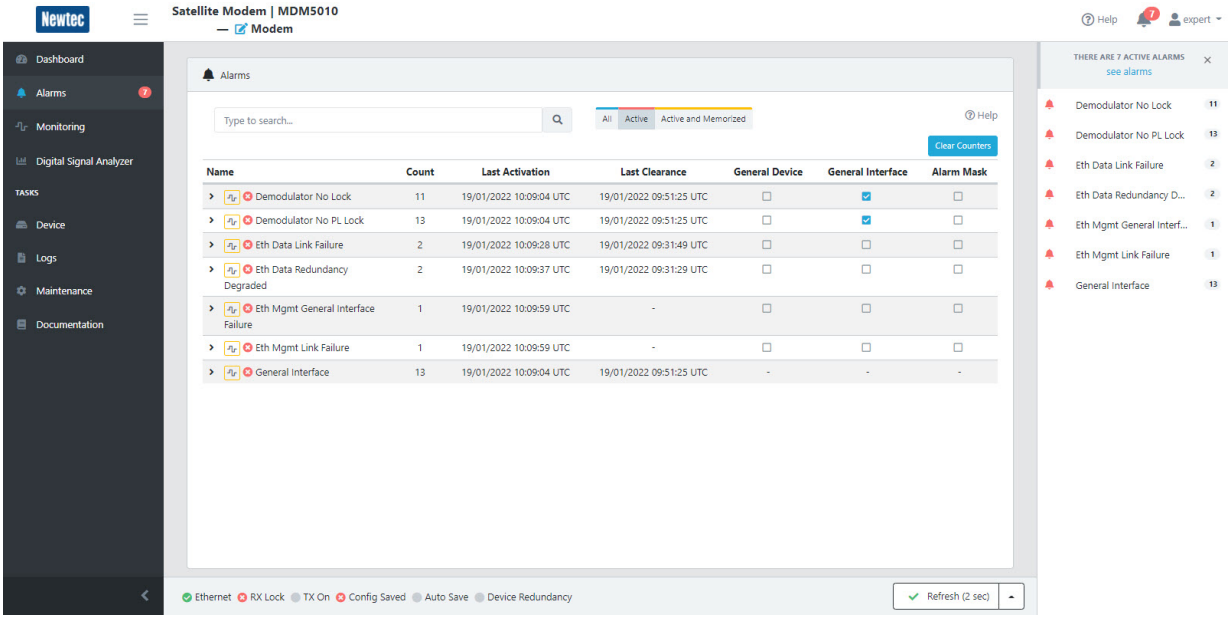
For more information about the configuration, see The MDM5010 Configuration.

1. Select *Device* in the *Tasks* list. The Reset button appears at the top.
2. Click **Reset**, and then click **Configs**. A confirmation window appears.
3. Read the message and click **Reset** if you are sure you want to proceed. The reset can take up to one minute.
4. When finished, click **OK** to reload the GUI and log in again.

3.13 Viewing the Alarms

In the menu at the left, make sure *Alarms* is selected. The red label (4) indicates the number of alarms that are currently active.

The *Alarms* screen with seven active alarms is shown below:



There are three states of alarm:

State	Means that...
Not active	there is no issue on the MDM5010 that raises the alarm.
Active	the MDM5010 has an issue that raises the alarm. An active alarm is marked with and the time of activation. An active alarm is marked with the time of activation.
Memorized	an issue that raises the alarm occurred on the MDM5010, but the issue has been resolved. A memorized alarm is marked with the time of activation and clearance.

Use the quick filters at the top to view all alarms, only the active alarms, or the active and memorized alarms.

Use the search bar at the top to look for specific alarms. The search only applies to the name of the alarm.

The *Count* field in the alarms table indicates how many times the alarm has occurred. Click **Clear Counters** to reset the counters to 0. The counters are also cleared after a hardware or software reset. The clear button is only available when logged in as expert user.

Click › in front of the alarm to get a brief description of the alarm. For more information about alarms, see Dealing with Alarms.

Click to trend the alarm over time, see Monitoring Parameter Trends.

An alarm has three parameters that enable you to manage the impact of the alarm:

Select...	If you want to...
General Device generaldevice GeneralDevice	mark the alarm as a general device alarm. When an issue occurs that raises this alarm, the *General Device* alarm*GeneralDeviceAlarm* is also activated. By default, general device alarms are monitored by the USS and trigger a redundancy switch. NOTE: For more information about device redundancy, see Device Redundancy.
General Interface generalinterface GeneralInterface	mark the alarm as a general interface alarm. When an issue occurs that raises this alarm, the *General Interface* alarm*GeneralInterfaceAlarm* is also activated. The USS can be configured to monitor general interface alarms and trigger a redundancy switch when the alarm occurs. NOTE: For more information about device redundancy, see Device Redundancy.
Alarm MaskmaskMask	ignore the alarm. When an issue occurs that would raise the alarm, the alarm is not activated. NOTE: Masked alarms are not considered for device redundancy swaps.

3.14 Monitoring Parameter Trends

The measurements shown in the *Dashboard* screen, and the alarms shown in the *Alarms* screen can be added to trend charts.

Trend charts are used to show trends in data over time. Displaying data over time increases understanding of the real performance of the MDM5010, particularly with regard to an established target or goal.

To create a trend chart for a parameter:

1 Click in front of the parameter, and then click **Add To Monitoring**.

2 Select **New Chart** to create a new trend chart for the parameter, or select the chart name to add the parameter to an existing trend chart.

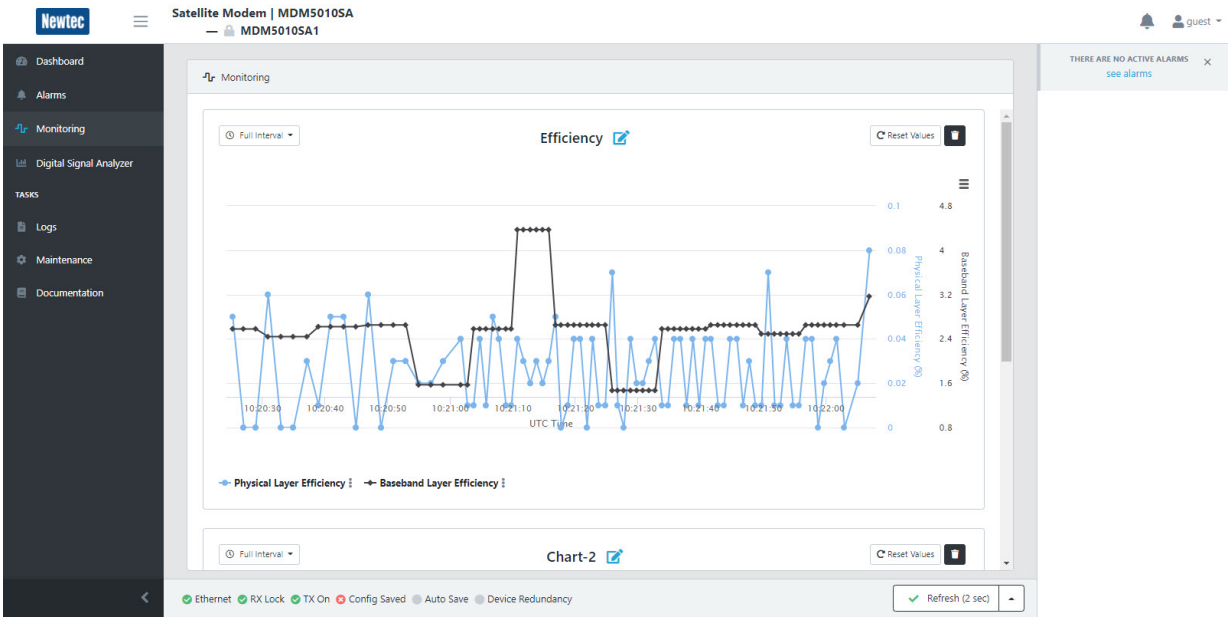
NOTE - You can add the parameter to multiple trend charts.

When the parameter is monitored, the icon in front of it changes to .

3 To remove the parameter from a trend chart, click , and then click **Remove from Monitoring**. Select the chart name of the trend chart from which the parameter should be removed. When the parameter is added to multiple charts, select **Remove From All** to stop monitoring the parameter.

To view the trend chart, select *Monitoring* in the menu at the left.

The *Monitoring* screen is shown below:



The monitored parameters are listed at the bottom left of the chart. Click the icon in front of the parameter name to show or hide the trend line. Click ⋮ at the right of the parameter name, and then click:

- to jump to the parameter in the *Dashboard* or *Alarms* screen
- to remove the parameter from the trend chart

Hover over the chart to see the individual measurements.

There are several buttons on a trend chart:

Click...	To...
Full Interval	change the trend time interval. The selected interval is displayed on the button.
	change the name of the trend chart. Click to confirm the change or click to discard the change.
Reset Values	clear the chart and restart monitoring. A confirmation window appears.
	to delete the trend chart. A confirmation window appears.
	• view the trend chart in full screen; click ESC to exit full screen • print the trend chart • download the trend chart in different formats

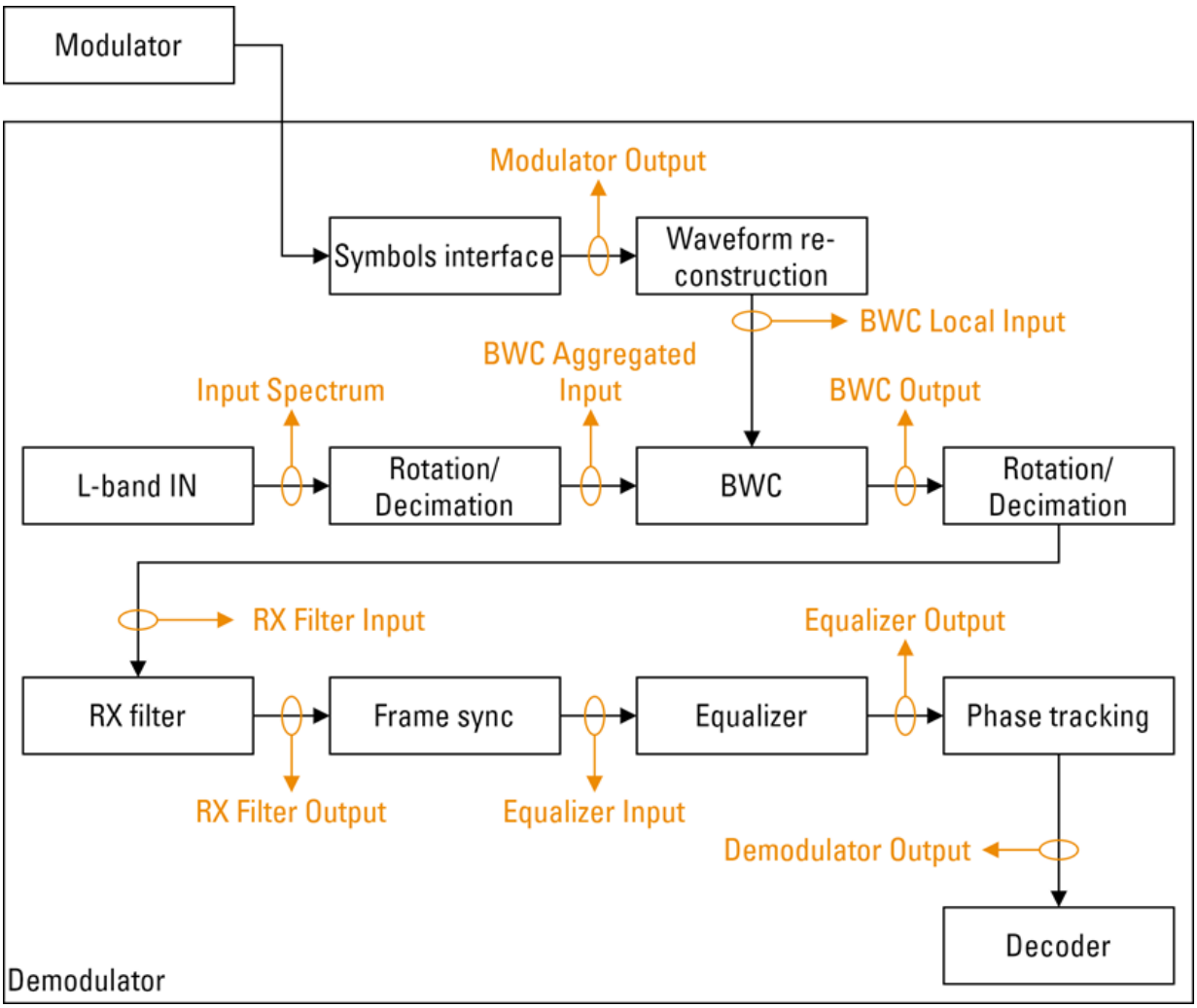
3.15 Using the Digital Signal Analyzer

The digital signal analyzer enables you to perform basic signal analysis using the constellation diagram and the frequency spectrum.

The constellation diagram can be used to assess the signal's integrity. When there is excess noise, distortion, spurious signals, or other problematic contributions degrading a signal's integrity, amplitude and phase errors occur, causing the symbols mapped in the diagram to deviate from the ideal signal locations.

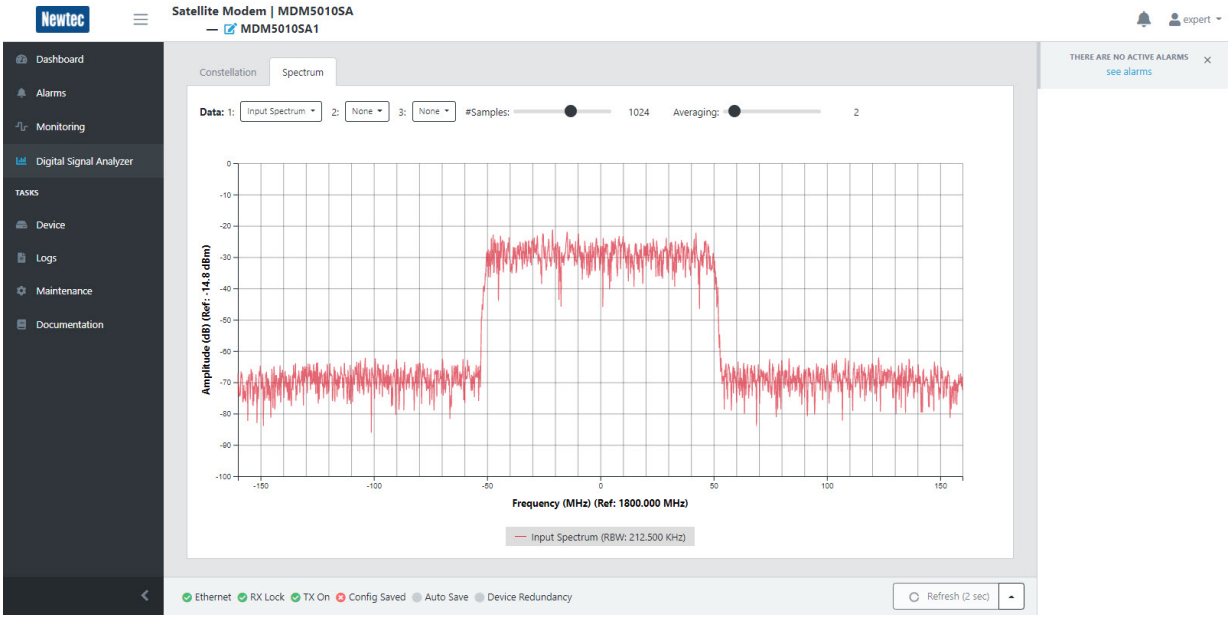
The frequency spectrum of the signal can be used to expose signal distortion, interference, spurious signals, and so on.

The digital signal analyzer can display the constellation diagram and spectrum of data sampled at different points in the demodulator:



To view the digital signal analyzer, select *Digital Signal Analyzer* in the menu at the left.

The *Digital Signal Analyzer* screen is shown below:



The screen has two tabs: *Constellation* and *Spectrum*.

3.15.1 Constellation

Select the sample point of the data in the drop-down list of the *Data* fields at the top of the *Constellation* screen. The data of the selected sample point is shown in the constellation display. When selecting **None**, no data is displayed. You can add up to two sample points (Data 1 and Data 2).

NOTE - When logged in as guest, only Modulator Output and Demodulator Output are available.

Use the *#Samples* slider to specify the number of I/Q samples to represent the constellation diagram. Valid values are from 100 to 4000. The default value is 1000 samples. A small number of samples can lead to alternating patterns, or even an empty display when the symbol rate is low and the number of dummy frames is high. Many samples provides a more stable constellation diagram but requires more memory resources. Many samples can also display pilots more easily. Pilots are displayed as four dots.

At the bottom of the constellation screen, the selected sample point and corresponding display color is shown. Click the sample point to hide or show the constellation diagram.

3.15.2 Spectrum

Select the sample point of the data in the drop-down list of the *Data* fields at the top of the *Spectrum* screen. The data of the selected sample point is shown in the spectrum display. When selecting **None**, no data is displayed. You can add up to three sample points (Data 1, Data 2, and Data 3).

NOTE - When logged in as guest, only Input Spectrum is available.

Use the *#Samples* slider to specify the number of samples to represent the frequency spectrum. Valid values are 128, 256, 512, 1024, 2048, and 4096. The default value is 1024 samples. The higher the number of samples, the better the spectrum and carrier are displayed.

Use the *Averaging* slider to control the signal vibrations. Valid values are from 1 to 16. The default value is 2. The number specifies the number of sweeps that are averaged.

NOTE - When the number of samples is set to 4096, the maximum value of averaging is 8. When the averaging is set to 16, the maximum number of samples is 2048.

The values on the *Frequency* axis are normalized to the input frequency of the downlink carrier. The carrier input frequency maps to 0 MHz.

The values of the *Amplitude* axis are normalized to the input level of the downlink carrier. The carrier input level maps to 0 dB.

At the bottom of the constellation screen, the selected sample point with corresponding display color and resolution bandwidth is shown. Click the sample point to hide or show the frequency spectrum.

3.16 Viewing the Device Log

The device log contains information about activities within the MDM5010, and can be used to observe, troubleshoot, or debug the MDM5010.

Select *Logs* in the *Tasks* list. Two buttons appear at the top.

Use...	To...
Device Log	• view the log file; the log file is opened in a new browser tab • download the log file to your local computer; the log file is saved as a .txt file in the *Downloads* folder
Clear Device Log	remove all existing log messages and start a new log file. **NOTE -** This button is only shown when you are logged in as expert.

For more information about the device log, see The Device Log.

3.17 Viewing the Diagnostic Report

The diagnostic report includes the complete device configuration, software and hardware information, monitoring and alarms information, the device log, and any other technical information that can be useful for troubleshooting or debugging the MDM5010.

Select *Maintenance* in the *Tasks* list. The **Diagnostic Report** drop-down button appears at the top.

Use drop-down item...	To...
View	view the diagnostic report. The report is opened in a new browser tab.
Download	download the diagnostic report to your local computer. The report is saved as a .txt file in the *Downloads* folder.
Download (Debug)	download the extended and encrypted diagnostic report to your local computer. The report is saved as a .enc file in the *Downloads* folder. **NOTE -** This file can only be viewed by ST Engineering iDirect customer support.

For more information about the report, see The Diagnostic Report.

3.18 Upgrading the Software

The procedure describes how to upgrade the software of the MDM5010 SCPC Satellite Modem.

Make sure you have the new software image file (*.bin) on your local computer.

CAUTION: The MDM5010 will reset during the procedure, and traffic will be impacted.

NOTE - Save your configuration before upgrading the software, see Saving the Active Configuration.

To upgrade the software:

1. Select *Maintenance* in the *Tasks* list. The Software Upgrade button appears at the top.
2. Click **Software Upgrade**. Navigate to the location of the new software image file, select it, and then click **Open**. A confirmation window appears.
3. Read the message and click **Upgrade** if you are sure you want to update your device now. The upgrade can take up to five to ten minutes, depending on your network connection for uploading the image, and the size of the image.
4. When finished, click **OK** to reload the GUI and log in again.

NOTE - You may need to clear the browser cache to reflect the changes.

Navigate to **Dashboard > Modem Info > Identification** to view the software version.

3.19 Uploading the License

The procedure describes how to upload a license to the MDM5010. For more information about licenses, see Licenses.

Make sure you have the new license file (*.ini) on your local computer.

CAUTION: The MDM5010 will reset during the procedure, and traffic will be impacted.

NOTE - Save your configuration before uploading the license, see Saving the Active Configuration.

To upload the license:

1. Select *Maintenance* in the *Tasks* list. The License Upgrade button appears at the top.
2. Click **License Upgrade**. Navigate to the location of the new license file, select it, and then click **Open**. A confirmation window appears.
3. Read the message and click **Upgrade** if you are sure you want to upload your license now. The upgrade can take up to five minutes.
4. When finished, click **OK** to reload the GUI and log in again.

NOTE - You may need to clear the browser cache to reflect the changes.

Navigate to **Dashboard > Modem Info > Identification** to view the software version.

3.20 Removing the Temporary License

The procedure describes how to remove the temporary license from the MDM5010 SCPC Satellite Modem before it has expired. When removed, the permanent license becomes active again. For more information about temporary licenses, see Licenses.

CAUTION: The MDM5010 will reset during the procedure, and traffic will be impacted.

NOTE - Save your configuration before removing the temporary license, see Saving the Active Configuration.

To remove the temporary license:

1. Select *Maintenance* in the *Tasks* list. The Remove Temporary License button appears at the top.
2. Click **Remove Temporary License**. A confirmation window appears.
3. Read the message and click **Remove Temporary License** if you are sure you want to remove the license now. The procedure can take up to five minutes. When finished, the login window appears.

NOTE - The MDM5010 may raise the Boot Configuration Failure alarm because certain configuration might no longer be available. Load or import a valid configuration to clear the alarm, see Handling the Configuration.

NOTE - Uploading a new permanent license will also remove the temporary license from the MDM5010. For more information about uploading licenses, see Uploading the License.

3.21 Resetting the MDM5010

CAUTION: Traffic will be impacted.

NOTE - Save the configuration before a hardware or software reset, see Saving the Active Configuration.

Select *Device* in the *Tasks* list. The **Reset** drop-down button appears at the top.

Use drop-down item...	To...
Hardware	power cycle the MDM5010. A confirmation window appears; read the message and click **Reset** if you are sure you want to continue. The reset can take up to five minutes. When finished, click **OK** to reload the GUI and log in again. Any unsaved configuration is lost, the device log is reset, and the boot configuration is loaded.
Software	reboot the operating system. A confirmation window appears; read the message and click **Reset** if you are sure you want to continue. The reset can take up to one minute. When finished, click **OK** to reload the GUI and log in again. Any unsaved configuration is lost, and the boot configuration is loaded.
Configs	delete all saved and unsaved application-specific configuration. The MDM5010 is reset to the *initialconfig* configuration including the factory default settings. The reset can take up to one minute. For more information, see Resetting the Configuration.

3.22 Downloading SNMP MIB-Modules

1. Select *Documentation* in the *Tasks* list. The SNMP MIBs button appears at the top.
2. Click **SNMP MIBs** to download the MIB-modules onto your local computer. The *mibs.zip* file is saved in the *Downloads* folder.

For more information about SNMP, see Managing the MDM5010 using SNMP.

3.23 Viewing the Reference Manual

The reference manual provides detailed information of all parameters used to manage the MDM5010, such as factory defaults, valid values, and access permissions.

1. Select *Documentation* in the *Tasks* list. The Reference Manual button appears at the top.
2. Click **Reference Manual** to view the reference manual. The reference manual is opened in a new tab.

3.24 Switching to Dialog® VSAT Mode

The MDM5010 is s a multi-personality modem. With a simple switch of the software, the MDM5010 SCPC standalone modem can be converted into a flexible Dialog® VSAT modem. When operating as a VSAT modem, you can easily switch back to the SCPC standalone personality and resume operation where you have left it.

CAUTION: Save your configuration before switching. When switching from VSAT back to SCPC standalone mode, the boot configuration will be loaded.

To switch to Dialog® VSAT mode:

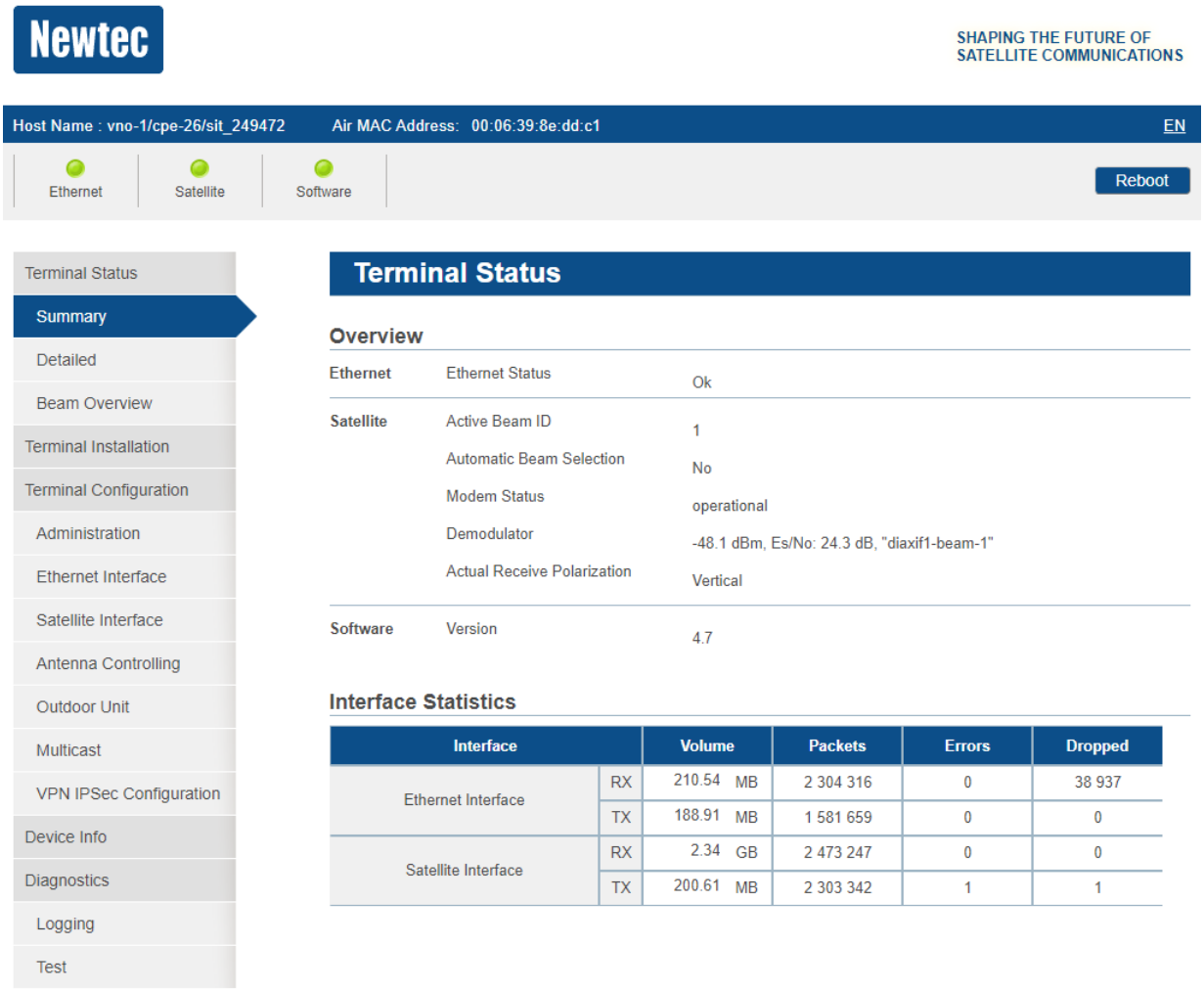
1. Select *Device* in the *Tasks* list. The Switch to Dialog VSAT Mode button appears at the top.
2. Click **Switch to Dialog VSAT Mode**. A window appears.
3. Select the *Reboot* check box to trigger a hardware reset at the end of the switch procedure. If the check box is not selected, the MDM5010 will not reset during the switch procedure and will continue operating in SCPC standalone mode. The VSAT mode will then only be activated at the next hardware reset.
4. Click **Switch** if you are sure that you want to proceed.

If the *Reboot* check box was not selected, the VSAT mode is scheduled and will be executed at the next hardware reset. If the MDM5010 did not reset, it will continue operating in SCPC standalone mode.

To abort the scheduled switch:

1. Select *Device* in the *Tasks* list. The Switch to Dialog VSAT Mode button appears at the top.
2. Click **Switch to Dialog VSAT Mode**. A window appears.
3. Click **Abort Switch to Dialog VSAT Mode** if you are sure you want to proceed. The MDM5010 will no longer switch to VSAT mode after a reset.

If the *Reboot* check box was selected, or you have manually performed a hardware reset to activate the scheduled switch, the MDM5010 is now a VSAT modem, which can be used in a Dialog® VSAT network. The configuration of your last session in VSAT mode is loaded. To access the GUI, browse to the management IP address of the MDM5010 using HTTP. The default management IP address of the MDM5010 in VSAT mode is 192.168.1.1. The window below appears:



To switch from Dialog® VSAT mode to SCPC standalone mode, refer to the *MDM5010 Dialog User Guide* for Dialog® R4.6.5 or up.

4 Managing the MDM5010 using REST API

The REST Application Programming Interface or API enables you to fully control the MDM5010 using REST API calls. The REST API provides a higher level of functionality and granular control compared to the Graphical User Interface. In addition, it can be used for scripting or creating your own control software.

An API is a set of definitions and protocols for building and integrating application software. REST or Representational State Transfer determines how the API looks like. It provides an architectural style using a subset of HTTP.

Use a REST API client application to connect to the management IP address of the MDM5010 (server) and execute the REST queries. The queries must be done as *expert* user. The default password is *expertexpert*.

Commonly used REST API client applications are Postman as a standalone app, and cURL as a command line utility (Linux).

NOTE - It is recommended to change the default password. For more information about changing the password, see Changing Login Passwords.

REST API access is disabled by default. To enable access, see Controlling Access.

REST API uses HTTP requests to access and use resources.

In this chapter:

4.1 HTTP Request Syntax and Semantics

A request is made up of four things:

- The endpoint
- The method
- The headers
- The body

The *endpoint* is the URL you request for. It follows this structure: `http://<IP_address>:9000/RestApi/path/query_parameters`. *IP_address* is the management IP address of the MDM5010. *path* determines the resource (also called URI). *query_parameters* are optional and used to control what data is returned in the response. A query parameter is a key-value pair (key=value). The list of query parameters always starts with a question mark (?). Each parameter pair is then separated with an ampersand (&). The supported query parameters are:

Key	Value	Use...
filter	alarms	if you only want to display alarm resources.
filter	monitoring	if you only want to display read-only resources, excluding the alarms resources.

NOTE - REST API endpoint syntax is case-sensitive.

The *method* is the type of request. The MDM5010 supports four types:

Use...	To...
GET	get a resource. As a result, the MDM5010 returns the requested data in a response body. The data can be a single variable or a group of variables, depending on the requested resource.
PUT	update a resource, create a new instance (row) in a table, reset an instance to the default settings, or delete all instances in a table. NOTE: When a recursive resource is not included, the value is reset to the factory default.
PATCH	update a resource or create a new instance (row) in a table. The difference with the PUT method is that a PATCH request only needs to contain the changes to the resource and not all recursive resources.
DELETE	delete an instance in a table.

Headers are used to provide information to both the client and server. It can be used for many purposes such as authentication and providing information about the body content.

The *body* (also called data or message) contains the information to send to the MDM5010. The data should be delivered in JSON (JavaScript Object Notation). Despite its name, JSON is completely language-agnostic, so it can be used with any programming language, not just JavaScript. A body is only used with PUT, PATCH, and DELETE requests.

4.2 Status and Error Codes

REST API always returns an HTTP response including a status code, headers, and optionally a body (in JSON). The status code informs the client whether the HTTP request has been successfully completed or not. HTTP defines standard status codes that can be used to convey the result of a client's request.

The supported REST API status codes are:

Status code	Is returned when...
200 (OK)	A 200 response includes a response body. The information returned with the response depends on the method used in the request, for example: • GET: an entity corresponding to the requested resource is sent in the response • POST: an entity describing or containing the result of the action
201 (Created)	a new resource is created. The newly created resource can be referenced by the URI(s) returned in the entity of the response, with the most specific URI for the resource given by a Location header field.
400 (Bad request)	no other 4xx error code is appropriate. 400 is the generic client-side error status. Errors can be like malformed request syntax, invalid request message parameters, or deceptive request routing.
401 (Unauthorized)	the client tried to operate on a protected resource without providing the proper authentication. It may have provided the wrong credentials or no credentials. The response must include a WWW-Authenticate header field containing a challenge applicable to the requested resource.
404 (Not found)	the REST API endpoint cannot map the client’s URI to a resource.

4.3 Resources

Resources are uniquely identified by the path in the endpoint, also called the URI (Uniform Resource Identifier). A resource can be a singleton or a collection. A resource may contain sub-collection resources also.

To understand what resources (or paths) are available in the MDM5010, use the following HTTP request:

```
GET http://<IP_address>:9000/RestApi
```

The HTTP response body returns the entire data model.

There are 16 top-level resources.

Use resource...	To...
/Device	• view modem information such as serial number, software version, and license type • set date and time • control access, see Controlling Access • handle the device log, see Managing the Device Log • monitor sensors • enable or disable automatic saving of the configuration changes • view alarms
/Ethernet	configure and monitor the Ethernet interfaces, see Managing the Management Interfaces.
/Ip	• configure the interface IP addresses and routes, see Managing the Management Interfaces • configure multicast streams • view alarms
/DeviceRedundancy	• enable device redundancy, see Device Redundancy • view alarms
/ReferenceClock	specify if the clock reference interface at the rear of the MDM5010 is used as an input or output interface. For more information, see The Reference Clock.

Use resource...	To...
/Modulators	• define the uplink carrier • control carrier transmission • manage the BUC (reference clock and power signal) • monitor the carrier status • view alarms NOTE: Only mod1 is used.
/Demodulators	• define the downlink carrier • define the backup carrier, see Migrating a Carrier • manage the LNB (clock reference and power signal) • monitor the carrier status • view alarms NOTE: Only demod1 is used.
/BandwidthCancellation	configure and monitor bandwidth cancellation. For more information, see Bandwidth Cancellation.
/AntennaController	configure and monitor antenna control. For more information, see Antenna Control.
/GseEncapsulation	• set the forwarding mode (linked to corresponding GseDecapsulation setting) • define the classification rules and shaping nodes • control the delay • monitor the nodes For more information, see Quality of Service and GSE Encapsulation and Baseband Frames.
/GseDecapsulation	• set the forwarding mode (linked to corresponding GseEncapsulation setting) • select the data interface for outgoing traffic • change the VLAN ID of outgoing traffic
/RemoteManagement	enable managing a remote device over the satellite link.

Use resource...	To...
/AcmControllers	• enable the ACM controller • configure the ACM behavior and MODCODs • monitor ACM For more information about ACM, see Adaptive Coding and Modulation.
/AcmClients	• configure an additional ACM margin • monitor ACM NOTE: The ACM client is always enabled. For more information, see Adaptive Coding and Modulation.
/DemodOutOfLockMutesMod	specify if the MDM5010 should stop transmitting when the demodulator is out of lock.
/FanController	view the fan failure alarm.
/Alarms	configure the impact of alarms, see Viewing the Alarms.

For more information about configuring the resources, see Configuration Quick Reference.

4.4 Working with Tables

The REST API data model in the MDM5010 includes several tables (arrays). Tables can be read-only, for example, *GseEncapsulation/Monitoring/MonitoringTable*, or can be read-write, for example, *Ip/Configuration/Management/IpItfTable*. Tables can be static and have a fixed number of instances (rows), for example, *Ethernet/Configuration/Management/PhysicalLinkTable*, or can be dynamic and have changing numbers of instnaces. Some dynamic tables allow you to create and delete instances, for example, in *GseEncapsulation/Configuration/NodesTable*.

4.4.1 Getting All Instances from a Table

Method	URI	Response body
GET	.../<Table>	An array of all table instances.

The example below shows the REST API request to get the information of the physical data interfaces.

HTTP request:

```
GET http://<ip_address>:9000/RestApi/Ethernet/Configuration/Data/PhysicalLinkTable
```

Response body:

```
[
	{
		"Interface": "data1",
		"MacAddress": "ac:1f:6b:46:d2:35",
		"ForcedSpeed": "100BTFullDuplex",
		"InterfaceState": "1000BTFullDuplex"
	},
	{
		"Interface": "data2",
		"MacAddress": "ac:1f:6b:46:d2:37",
		"ForcedSpeed": "100BTFullDuplex",
		"InterfaceState": "linkDown"
	}
]
```


4.4.2 Getting One Instance from a Table

Method	URL	Response body
GET	.../<Table>/<InstanceId>	The instance with all parameters.

The example below shows the REST API request to get the configuration of the first NTP peer.

HTTP request:

```
GET http://<ip_address>:9000/RestApi/Device/DateTime/Ntp/Peer/1
```

Response body:


```
{
	"Peer": 1,
	"IpAddress": "0.0.0.0"
}
```

4.4.3 Getting a Parameter From an Instance

Method	URL	Response body
GET	.../<Table>/<InstanceId>/<Parameter>	The parameter value.

The example below shows the REST API request to get the output level of the uplink carrier.

HTTP request:

```
GET http://<ip_
address>:9000/RestApi/Modulators/Configuration/ConfigurationTable/mod1/OutputLevel
```

Response body:

```
-10.000000000000000
```

4.4.4 Updating a Parameter in an Instance

Method	URL	Request body
PATCH or PUT	.../<Table>/<InstanceId>/<Parameter>	The parameter value. NOTE: When using the PUT method, an empty request body will reset the parameter to the default value.
PATCH or PUT	.../<Table>/<InstanceId>	The parameter:value pair. NOTE: When using the PUT method, any parameter:value pair not included in the request body will reset the parameter to the default value. An empty request body will reset all parameters of the instance to their default value.

The examples below show REST API requests to change the output level of the uplink carrier.

HTTP request 1:

```
PATCH http://<ip_
address>:9000/RestApi/Modulators/Configuration/ConfigurationTable/mod1/OutputLevel

-12.000000000000000
```

HTTP request 2:

```
PATCH http://<ip_address>:9000/RestApi/Modulators/Configuration/ConfigurationTable/mod1

{

        -12.000000000000000

}
```

CAUTION: Using the PUT method in the examples will reset all other uplink carrier related parameters, such as OutputFrequency and SymbolRate.

4.4.5 Creating a New Instance

Method	URL	Request body
PATCH or PUT	.../<Table>/<NewInstanceId>	<empty> or a list of parameter:value pairs. NOTE: When a parameter:value pair is not included in the request body, the value of the parameter is set to the default value.
PATCH or PUT	.../<Table>	Array of new <InstanceId>. NOTE: When a parameter:value pair is not included in the request body, the value of the parameter is set to the default value. NOTE: When using the PUT method, any existing instance not included in the array will be removed from the table.

The examples below show REST API requests to create a classification and shaping node.

HTTP request 1:

```
PATCH http://<ip_address>:9000/RestApi/GseEncapsulation/Configuration/NodesTable/Node-1
```

HTTP request 2:

```
PATCH http://<ip_address>:9000/RestApi/GseEncapsulation/Configuration/NodesTable

[

      {

              "Name": "Node-1"

      }

]
```

NOTE - Using the PUT method in the second example will delete any existing instance in the table. Only the new instance remains.

4.4.6 Deleting an Instance

Method	URL	Request body
DELETE	.../<Table>/<InstanceId>	<empty>

The example below shows the REST API request to delete a classification and shaping node.

HTTP request:

```
DELETE http://<ip_address>:9000/RestApi/GseEncapsulation/Configuration/NodesTable/Node-1
```

4.4.7 Deleting all Instances

Method	URL	Request body
DELETE	.../<Table>	<empty>
PUT	.../<Table>	<empty>

The example below shows the REST API call to delete all existing classification and shaping nodes.

HTTP request:

```
DELETE http://<ip_address>:9000/RestApi/GseEncapsulation/Configuration/NodesTable
```

Using the PUT method in the example returns the same result.

4.5 Managing the Management Interfaces

The MDM5010 in SCPC standalone mode has two physical management ports, see MDM5010 Hardware Features. By default, the MGMT 1 interface (mgmt1) is enabled. The default IP address and subnet is 10.0.0.1/24.

Carefully design your management network setup. At least one of the management Ethernet interfaces should be connected to your management network. The other interface can be used as a second interface for management access, or the interfaces can operate as a single bond interface if link redundancy is required.

CAUTION: Take care when changing management interface settings. Changes are effective immediately. Wrong settings can block access to the MDM5010.

4.5.1 Configure the Ethernet Links

The REST API enables you to configure the Ethernet interface settings such as auto-negotiation, port speed, and duplex mode.

The example below shows the REST API request to get the link status and MTU size of the mgmt1 interface.

HTTP request:

```
GET http://<ip_address>:9000/RestApi/Ethernet/Configuration/Management/LinkTable/mgmt1
```

Response body:

```
{

      "Interface": "mgmt1",

      "Enable": "on",

      "Mtu": 1500

}
```

Use the *PATCH* or *PUT* method to change the settings.

This can be set for the physical mgmt1 and mgmt2 interface, and the mgmt bond interface. Enabling the bond interface automatically enables the mgmt1 and mgmt2 Ethernet interfaces.

CAUTION: Only disable an interface when you are sure you can access the MDM5010 using the other management interface.

The example below shows the REST API request to get the information of the physical mgmt1 interface, such as port speed and duplex mode.

HTTP request:

```
GET http://<ip_
address>:9000/RestApi/Ethernet/Configuration/Management/PhysicalLinkTable/mgmt1
```

Response body:

```
{

      "Interface": "mgmt1",

      "MacAddress": "00:06:39:09:8c:58",

      "AutoNegotiation": "on",

      "AdvertizedSpeeds": "all",

      "ForcedSpeed": "100BTFullDuplex",

      "InterfaceState": "100BTFullDuplex"

}
```

Use the *PATCH* or *PUT* method to change the settings.

4.5.2 Configure Link Redundancy

The example below shows the REST API request to get the link redundancy settings.

HTTP request:

```
GET http://<ip_
address>:9000/RestApi/Ethernet/Configuration/Management/LinkRedundancyTable/mgmt
```

Response body:

```
{

       "Interface": "mgmt",

       "ProtectionMode": "revertive",

       "InterfaceA": "mgmt1",

       "InterfaceB": "mgmt2",

       "PreferredInterface": "ifa",

       "OperationalState": "down",

       "ActiveInterface": "None",

       "SwitchCount": 0

}
```


Use the *PATCH* or *PUT* method to change the settings.

See Configure the Ethernet Links for enabling link redundancy (bond interface).

For more information about link redundancy, see Link Redundancy.

4.5.3 IP Addressing

Assign an IP address to at least one enabled management interface. The other interface can be used as a second interface for management access, or the interfaces can operate as a single bond interface if link redundancy is required. An interface can also have a virtual IP address for facilitating device redundancy. For more information about device redundancy, see Device Redundancy.

The example below shows the REST API request to get the IP address information of the mgmt1 interface.

HTTP request:

```
GET http://<ip_address>:9000/RestApi/Ip/Configuration/Management/IpItfTable/mgmt1
```

Response body:

```
{
	"Interface": "mgmt1",
	"IpAddress": "10.254.2.80/24",
	"VirtualIpAddress": "0.0.0.0/24",
	"State": "on"
}
```


Use the *PATCH* or *PUT* method to change the settings.

The *State* parameter indicates if the interface has a valid IP address (**on**) or not (**off**). The state will also be **off** when the Ethernet interface is not OK.

NOTE - This can be set for the physical mgmt1 and mgmt2 interface, and the mgmt bond interface.

4.5.4 IP Routing

Configure the next-hop address.

The example below shows the REST API request to get the IP route information.

HTTP request:

```
GET http://<ip_address>:9000/RestApi/Ip/Configuration/Management/IpRouteTable
```

Response body:


```
[
	{
		"Name": "Default Gateway",
		"DestSubnet": "0.0.0.0/0",
		"Interface": "mgmt1",
		"GateWay": "10.254.2.254",
		"State": "on"
	}
]
```

Use the *PATCH* or *PUT* method to change the settings.

NOTE - The Default Gateway row is always there. Create new rows to add more routes if needed.

4.5.5 Monitoring

The example below shows the REST API request to view the performance parameters of the mgmt1 interface.

HTTP request:

```
GET http://<ip_address>:9000/RestApi/Ethernet/Monitoring/Management/MonitoringTable/mgmt1
```

Response body:

```
{

	"Interface": "mgmt1",

	"InputBytes": 778199411,

	"InputPackets": 9991811,

	"InputDropped": 0,

	"InputErrors": 0,

	"OutputBytes": 1097808793,

	"OutputPackets": 1081187,

	"OutputDropped": 0,

	"OutputErrors": 0

}
```

NOTE - If link redundancy is enabled, you can also select the mgmt interface.

4.5.6 Alarms

The example below shows the REST API request to view the alarms of the mgmt1 interface.

HTTP request:

```
GET http://<ip_
address>:9000/RestApi/Ethernet/Alarms/Management/PhysicalAlarmStatusTable/mgmt1
```

Response body:

```
{

      "Interface": "mgmt1",

      "EthLinkFailure": "statusOK",

      "EthHalfDuplex": "statusOK"

}
```

The example below shows the REST API request to view the alarms of the bond interface.

The mgmt row in the table is only available if link redundancy is enabled.

HTTP request:

```
GET http://<ip_
address>:9000/RestApi/Ethernet/Alarms/Management/LinkRedundancyAlarmStatusTable/mgmt
```

Response body:

```
{

      "Interface": "mgmt",

      "EthRedundancyFailure": "statusOK",

      "EthRedundancyDegraded": "alarm"

}
```

For more information about the alarms, see Dealing with Alarms.

4.6 Viewing the Alarms

To view the alarms, send the following request:

```
GET http://<ip_address>:9000/RestApi/?filter=alarms
```

Each alarm has the following information:

Parameter...	Indicates...
StatusState	if the alarm is active (*ONalarm*) or not (*OFFstatusOK*). An alarm is activated when the MDM5010 has an issue that raises the alarm.
Counter StatusCnt	how many times the alarm has occurred.
Time OnOnTime	when the alarm was triggered. If the alarm is not active but memorized, it indicates the last time the alarm was active.
Time OffOffTime	when the alarm was cleared.

For more information about the alarms, see Dealing with Alarms.

An alarm has three parameters that enable you to manage the impact of the alarm:

Select...	If you want to...
General Device generaldevice GeneralDevice	mark the alarm as a general device alarm. When an issue occurs that raises this alarm, the *General Device* alarm*GeneralDeviceAlarm* is also activated. By default, general device alarms are monitored by the USS and trigger a redundancy switch. NOTE: For more information about device redundancy, see Device Redundancy.
General Interface generalinterface GeneralInterface	mark the alarm as a general interface alarm. When an issue occurs that raises this alarm, the *General Interface* alarm*GeneralInterfaceAlarm* is also activated. The USS can be configured to monitor general interface alarms and trigger a redundancy switch when the alarm occurs. NOTE: For more information about device redundancy, see Device Redundancy.
Alarm MaskmaskMask	ignore the alarm. When an issue occurs that would raise the alarm, the alarm is not activated. NOTE: Masked alarms are not considered for device redundancy swaps.

To view the configuration of the parameters for the alarms, send the following request:

```
GET http://<ip_address>:9000/RestApi/Alarms/Configuration
```

Use the *PATCH* method to change a parameter. The example below masks the hardware failure alarm.

```
PATCH http://<mgmt_ip_address>:9000/RestApi/Alarms/Configuration/hardwareFailure/Mask

"on"
```

4.7 Managing the Device Log

The device log contains information about activities within the MDM5010, and can be used to observe, troubleshoot, or debug the MDM5010.

Local device logging is enabled by default. To disable local logging, send the following request:

```
PUT http://<ip_address>:9000/RestApi/Device/Log/Local

{

"Enable": "off"

}
```

Remote logging can be enabled. The log messages are then sent to a remote syslog server using UDP. The example below enables remote logging to a server with IP address 10.10.10.10 and using UDP port 514 (default port).

```
PATCH http://<ip_address>:9000/RestApi/Device/Log/Remote

{

"Enable": "on",

"IpAddress": "10.10.10.10"

}
```

Use the *filter* resource to manage the log level per facility.

```
GET http://<ip_address>:9000/RestApi/Device/Log/Filter

[

{

"Facility": "alarms",

"Level": "info"

},

{

"Facility": "configuration",

"Level": "info"

},

{

"Facility": "system",

"Level": "info"

},

{

"Facility": "internalerror",

"Level": "info"

},

{

"Facility": "authentication",

"Level": "info"

},

{

"Facility": "networking",

"Level": "info"

}

]
```

For more information about facilities and log levels, see The Device Log.

NOTE - The device log can be viewed and downloaded using the GUI or CLI.

5 Managing the MDM5010 using CLI

The Command Line Interface or CLI enables you to fully control the MDM5010 using the command line shell. The CLI provides a higher level of functionality and granular control compared to the Graphical User Interface. In addition, it can be used for scripting or automating tasks.

The command line shell is accessed using an SSH connection. Log in as *expert* user. The default password is *expertexpert*.

PuTTY is a common SSH client for Windows users, see https://www.putty.org/.

When logged in, the command line shell displays a welcome text and the command prompt.

```
** Welcome to the CLI interface on 'Satellite Modem[MDM5010]' **

[MDM5010] #
```

The name between brackets is configurable, see device/identification/ branch.

In this chapter:

- Switching to Dialog® VSAT Mode
- Exporting SNMP MIB-modules

CLI access is disabled by default. To enable access, see Controlling Access.

5.1 CLI Syntax and Semantics

The general pattern of a command line is: *prompt command param1 param2 .. paramN*

- The prompt consists of the device name and the current working branch. It ends with the #-sign.
- The command is the action that the CLI should execute.
- param1 …paramN are optional parameters. The format and meaning of the parameters depend upon the command issued.

NOTE - Use the tab button to auto-complete commands and parameters.

There are several generic commands:

Use...	To...
quit	exit the command line interface.
source	execute a script. A script is a text file with a sequence of CLI commands.
transaction	to schedule multiple CLI commands that set parameters without executing them yet. To execute the commands, enter the *commit* command. To clear the scheduled commands, enter the *cancel* command.
exit	move one level up in the data structure. This command is not available at root level.
exitall	return to the root of the data structure (main branch). This command is not available at root level.
show	view the underlying data structure (branches), branch-specific commands, and parameters names and values.
help	view the underlying data structure (branches), branch-specific commands, and parameters names and values.

A branch name always ends with a slash (/). A command always ends with an asterisk (*).

The example below displays the result of the *show* command at root level. The result returns the available root branches. There are no root-specific commands or parameters.

```
[MDM5010] # show
device/
debug/
mgmtinterface/
datainterface/
deviceredundancy/
refclock/
modulators/
demodulators/
demodoutoflockmutesmod/
bandwidthcancellation/
antennacontroller/
gseencapsulation/
gsedecapsulation/
remotemanagement/
acmcontrollers/
acmclients/
alarms/
alarmmanager/
bbfoveripout/
deviceinformation/
user/
```

To move to an underlying branch, enter the name of the branch. The example below shows how to enter the *alarms* branch.

```
[MDM5010] # alarms
[MDM5010] alarms#
```

The example below displays the result of the *help* command at the *alarms* branch. The result returns the underlying branch *configuration/* and the alarms-specific commands.

```
[MDM5010] alarms# help

configuration/

all*

active*

memorized*

resetcounters*
```

help can also be used as a parameter.

Use...	To...
<command> help	get the command description and syntax.

The example below displays the result of the *help* parameter used for the *cli set* command.

```
[MDM5010] device cli# set help

set Cli

Optional parameters:

* RemoteEnable {enum}: Enable or disable the remote CLI (Command Line Interface) interface.
(default value = on) (options: off on)

* InactivityTimeout {unsigned int}: This parameter specifies the time a CLI session is open
without interaction. (default value = 600 s) ([0 , 0] [60 , 5000000] (s))
```

There are several branch-specific commands, such as *get* and *set*. Use the *help* parameter to view the command description and syntax.

The example below gets the device's date and time.

```
[MDM5010] device datetime# get

Date : 15/03/2021

Time : 12:54:18
```

The example below masks the *unit redundancy* alarm.

```
[MDM5010] device datetime# /alarms configuration unitredundancy set mask=on

OK
```

The example below shows the active alarms.

```
[MDM5010] # alarms active

+------------------------+-------+---------+--------------------------+----------+

| Alarm | State | Counter | Time On | Time Off |

+------------------------+-------+---------+--------------------------+----------+

| General Interface | ON | 1 | Tue Apr 13 16:57:34 2021 | never |

| Demodulator No PL Lock | ON | 1 | Tue Apr 13 16:57:34 2021 | never |

| Demodulator No Lock | ON | 1 | Tue Apr 13 16:57:34 2021 | never |

+------------------------+-------+---------+--------------------------+----------+
```

The example below exports the SNMP MIB.

```
[MDM5010] device mibs# export

NOTE - Use SCP to retrieve the mibs.zip file from the download folder on the MDM5010.
```

NOTE - The examples show different ways to execute commands. Commands can be executed starting from any branch, if you specify the data structure correctly.

The CLI supports special keys and key combinations:

Use...	To...
? or double-tab	view the underlying data structure (branches), branch-specific and generic commands, and branch-specific parameters names.
<command> ?	view the command description and syntax.
<command> double-tab	view the command parameters.
<char(s)>? or double-tab	view the available branches, commands, and parameter names that start with <char(s)>.
tab	auto-complete a command or parameter name.
/	return to the root of the data structure (main branch). This is the same as using the *exitall* command or the *CTRL+z* key combination.

Use...	To...
Arrow up/down	scroll through previously used command lines.
Arrow left/right	move the cursor to the left or to the right in a command line.
CTRL + a	move the cursor to the beginning of the command line.
CTRL + b	move the cursor to the left. This is the same as using the left-arrow key.
CTRL + c	clear the command line.
CTRL + d	exit the command line interface.
CTRL + e	move the cursor to the end of the command line.
CTRL + f	move the cursor to the right. This is the same as using the right-arrow key.
CTRL + h	delete characters to the left. This is the same as using the backspace key.
CTRL + k	delete the characters from the cursor position to the end of the command line.
CTRL + p	recall the previously used command line. This is the same as using the up-arrow key.
CTRL + n	go to the next used command line. This is the same as using the down-arrow key.
CTRL + u	delete the characters from the beginning of the command line to the cursor position.
CTRL + s	suspend asynchronous tracing and pause the information stream.
CTRL + q	resume asynchronous tracing and resume the information stream.
CTRL + z	return to the root of the data structure (main branch). This is the same as using the *exitall* command or the / key.

5.2 Root Branches

Use the *show* command at root level to list the root branches. There are 22 root branches.

Use...	To...
device	• view modem information such as serial number, software version, and license type • set date and time • control access, see Controlling Access • handle the device log, see Managing the Device Log • view and download the diagnostic report, see Viewing the Diagnostic Report • monitor sensors from main board (MB), demod board (ntc7304, and router board (x86_pkg_temp) • handle device configuration, see Handling Device Configuration • view alarms • upgrade software, see Upgrading the Software • handle licenses, see Uploading the License • reset the device, see Resetting the MDM5010 • export MIB-modules, see Exporting SNMP MIB-modules
mgmtinterface	configure and monitor the management interfaces, see Managing the Management Interfaces.
datainterface	configure and monitor the data interfaces.
deviceredundancy	• enable device redundancy, see Device Redundancy • view alarms
refclock	specify if the clock reference interface at the rear of the MDM5010 is used as an input or output interface. For more information, see The Reference Clock.

Use...	To...
modulators	• define the uplink carrier • control carrier transmission • manage the BUC (reference clock and power signal) • monitor the carrier status • view alarms NOTE: Only mod1 is used.
demodulators	• define the downlink carrier • define the backup carrier, see Migrating a Carrier • manage the LNB (clock reference and power signal) • monitor the carrier status • view alarms NOTE: Only demod1 is used.
demodoutoflockmutesmod	specify if the MDM5010 should stop transmitting when the demodulator is out of lock.
bandwidthcancellation	configure and monitor bandwidth cancellation. For more information, see Bandwidth Cancellation.
antennacontroller	configure and monitor antenna control. For more information, see Antenna Control.
gseencapsulation	• set the forwarding mode (linked to corresponding gsedecapsulation setting) • define the classification rules and shaping nodes • control the delay • monitor the nodes For more information, see Quality of Service and GSE Encapsulation and Baseband Frames.
gsedecapsulation	• set the forwarding mode (linked to corresponding gseencapsulation setting) • select the data interface for outgoing traffic • change the VLAN ID of outgoing traffic
remotemanagement	manage a remote device over the satellite link.

Use...	To...
acmcontrollers	• enable the ACM controller • configure the ACM behavior and MODCODs • monitor ACM For more information about ACM, see Adaptive Coding and Modulation.
acmclients	• configure an additional ACM margin • monitor ACM NOTE: The ACM client is always enabled. For more information, see Adaptive Coding and Modulation.
alarms	configure the impact of alarms, see Viewing the Alarms.
alarmmanager	view the active, memorized, and non-active alarms.
deviceinformation	import or export device information in .xml format.
multipersonality	switch modem personality, see Switching to Dialog® VSAT Mode.
user	change the user login password, see Changing Login Passwords.

For more information about configuring the branches, see Configuration Quick Reference.

5.3 Working with Tables

The CLI data model in the MDM5010 includes several tables. Tables can be read-only, for example *gseencapsulation/monitoring/monitoringtable*, or can be read-write, for example *mgmtinterface ip ipitftable*. Tables can be static and have a fixed number of rows, for example *mgmtinterface/ethernet/configuration/physicallink*, or can be dynamic and have changing numbers of rows. In some dynamic tables you can add or delete rows, for example in *gseencapsulation/configuration/nodestable*.

In this topic:

5.3.1 Show a table

Use the *showtable* command to display the table rows including the header row.

The example below shows the CLI command to get the information of the physical data interfaces table.

```
[MDM5010] datainterface ethernet configuration physicallink# showtable

+-------------+----------+--------+--------------------+---------------+------------------+

| Interface | Enable | Mtu | MacAddress | ForcedSpeed | InterfaceState |

+-------------+----------+--------+--------------------+---------------+------------------+

| data1 | off | 1500 | ac:1f:6b:46:d2:35 | N/A | 1000BTFullDuplex |

| data2 | off | 1500 | ac:1f:6b:46:d2:37 | N/A | linkDown |

+-------------+----------+--------+--------------------+---------------+------------------+
```

5.3.2 Update a parameter in a row

To update a parameter in a row, type the row key, and then *set* the parameter to the desired value.

The example below shows the command line to change the output level of the uplink carrier.

```
[MDM5010] modulators configuration configurationtable# mod1 set OutputLevel=-12
```

5.3.3 Create a new row

Use the *new* command to create a new row.

The example below shows the command line to create a classification and shaping node.

```
[MDM5010] gseencapsulation configuration nodestable# new Node-1
```

NOTE - The parameter values are set to the default values.

5.3.4 Delete a row

Use the *delete* command to delete a row.

The example below shows the command line to delete a classification and shaping node.

```
[MDM5010] gseencapsulation configuration nodestable# delete Node-1
```

5.4 Managing the Management Interfaces

The MDM5010 in SCPC standalone mode has two physical management ports, see MDM5010 Hardware Features. By default, the MGMT 1 interface (mgmt1) is enabled. The default IP address and subnet is 10.0.0.1/24.

Carefully design your management network setup. At least one of the management Ethernet interfaces should be connected to your management network. The other interface can be used as a second interface for management access, or the interfaces can operate as a single bond interface if link redundancy is required.

CAUTION: Take care when changing management interface settings. Changes are effective immediately. Wrong settings can block access to the MDM5010.

In this section:

- Configure the Ethernet Links
- Enable Link Redundancy
- IP Addressing
- IP Routing
- Monitoring
- Alarms

5.4.1 Configure the Ethernet Links

The CLI enables you to configure Ethernet interface settings, such as auto-negotiation, port speed, and duplex mode.

Go to the branch *mgmtinterface ethernet configuration physicallink mgmtx*, where x is 1 or 2, and then enter the *show* command to view the available parameters.

The example below shows the CLI command to get the settings of the physical mgmt1 interface.

```
[MDM5010] mgmtinterface ethernet configuration physicallink mgmt1# show

interface : mgmt1

enable : on

mtu : 1500

macaddress : 00:06:39:09:8d:dd

autonegotiation : on

advertizedspeeds : all

interfacestate : 100BTFullDuplex
```

CAUTION: Only disable an interface when you are sure you can access the MDM5010 using the other management interface.

5.4.2 Enable Link Redundancy

Go to the branch *mgmtinterface ethernet configuration linkredundancy mgmt*, and then enter the *show* command to view the available parameters.

```
[MDM5010] mgmtinterface ethernet configuration linkredundancy mgmt# show

interface : mgmt

enable : off

mtu : 1500

protectionmode : revertive

interfacea : mgmt1

interfaceb : mgmt2

preferredinterface : ifa

operationalstate : down

activeinterface : None

switchcount : 0
```

NOTE - Enabling link redundancy automatically enables the mgmt1 and mgmt2 Ethernet interfaces.

For more information about link redundancy, see Link Redundancy.

5.4.3 IP Addressing

Assign an IP address to at least one enabled management interface. The other interface can be used as a second interface for management access, or the interfaces can operate as a single bond interface if link redundancy is required. An interface can also have a virtual IP address for facilitating device redundancy. For more information about device redundancy, see Device Redundancy.

Go to the branch *mgmtinterface ip ipitftable mgmtx*, where x is 1 or 2, and then enter the *show* command to view the available parameters.

The example below shows the CLI command to get the IP settings of the mgmt1 interface.

```
[MDM5010] mgmtinterface ip ipitftable mgmt1# show

interface : mgmt1

ipaddress : 10.254.2.81/24

virtualipaddress : 0.0.0.0/24

state : on
```

The *state* parameter indicates if the interface has a valid IP address (**on**) or not (**off**). The state will also be **off** when the Ethernet interface is not OK.

NOTE - If link redundancy is enabled, only the mgmt interface is available.

5.4.4 IP Routing

Configure the next-hop address.

Go to the branch *mgmtinterface ip iproutetable*, and then enter the *showtable* command to view the available routes.

```
[MDM5010] mgmtinterface ip iproutetable# showtable

+------------------+-------------+-------------+----------------+-------+

| Name | DestSubnet | Interface | GateWay | State |

+------------------+-------------+-------------+----------------+-------+

| Default Gateway | N/A | | 10.254.2.254 | on |

+------------------+-------------+-------------+----------------+-------+
```

NOTE - The Default Gateway row is always there. Create new rows to add more routes if needed.

5.4.5 Monitoring

Go to the branch *mgmtinterface ethernet monitoring monitoringtable mgmtx*, where x is 1 or 2, and then enter the *show* command to view the available performance parameters.

The example below shows the CLI command to get the performance parameters of the mgmt1 interface.

```
[MDM5010] mgmtinterface ethernet monitoring monitoringtable mgmt1# show

interface : mgmt1

inputbytes : 132630873 bytes

inputpackets : 1096453 packets

inputdropped : 0 packets

inputerrors : 0 packets

outputbytes : 942595269 bytes

outputpackets : 827668 packets

outputdropped : 0 packets

outputerrors : 0 packets
```

NOTE - If link redundancy is enabled, you can also select the mgmt interface.

5.4.6 Alarms

Go to the branch *mgmtinterface ethernet alarms physicallinkalarmstatustable mgmtx*, where x is 1 or 2, and then enter the *show* command to view the alarms of the physical links.

The example below shows the CLI command to view the alarms of the mgmt1 interface.

```
[MDM5010] mgmtinterface ethernet alarms physicallinkalarmstatustable mgmt1# show

interface : mgmt1

ethlinkfailure : statusOK

ethhalfduplex : statusOK
```

Go to the branch *mgmtinterface ethernet alarms redundancylinkalarmstatustable mgmt*, and then enter the *show* command to view the alarms of the bond interface.

NOTE - The mgmt row in the table is only available if link redundancy is enabled.

```
[MDM5010] mgmtinterface ethernet alarms redundancylinkalarmstatustable mgmt# show

interface : mgmt

ethredundancyfailure : statusOK

ethredundancydegraded : alarm
```

For more information about the alarms, see Dealing with Alarms.

5.5 Handling Device Configuration

The configuration handled in this chapter refers to the application-specific configuration. For more information about the device configuration, see The MDM5010 Configuration.

Go to the branch *device configuration*, and then enter the *show* command to view the available configuration-specific commands.

```
[MDM5010] device configuration# show

activeconfigname*

activeconfigurationstate*

bootconfig*

bootconfigname*

current*

currentsystem*

delete*

deleteall*

export*

import*

list*

load*

loadunforced*

print*

save*

activeconfigstate : saved

autosave : off
```

Use command...	To...
activeconfigstate	know if the active configuration has been saved or not: • saved • updatedNotSaved; changes to the configuration have not yet been saved

Use command...	To...
autosave	• enable or disable saving the application-specific settings automatically • know if automatic saving is enabled or not
activeconfigname	get the name of the configuration file that is currently deployed onto the MDM5010.
activeconfigurationstate	know if the active configuration has been saved or not: • Saved • NotSaved; changes to the configuration have not yet been saved
bootconfig	make a configuration the boot configuration.
bootconfigname	get the name of the current boot configuration file.
current	view the active configuration (application- and system-specific), including any changes that have not been saved yet.
currentsystem	view the system-specific configuration.
delete	delete a configuration file.
deleteall	delete all configuration files, except the *initialconfig* file. The *initialconfig* file is reset to the factory default configuration and is the boot configuration.
export	export a configuration. The configuration is saved as an .xml file in the *Download* folder of the MDM5010. Retrieve the configuration file using SCP, see SCP Interface.
import	import a configuration from your local computer. Upload the .xml configuration file to the *upload* folder on the MDM5010 using SCP, see SCP Interface. NOTE: Importing a configuration does not load the configuration onto the MDM5010.
list	list the existing configuration files.
load	load an existing configuration and apply all parameters, even when they are not different from the current configuration. Parameters that are not specified in the configuration file will be reset to the factory default values.
loadunforced	load an existing configuration and only apply the parameters that are different from the current configuration.
print	view the content of an existing configuration.
save	save the active configuration. NOTE: Set autosave to on to allow that the application-specific configuration is saved automatically.

5.6 Viewing the Alarms

Use the *show* command at the *alarms* branch to view the available branches and branch-specific commands.

```
[MDM5010] alarms# show

configuration/

all*

active*

memorized*

resetcounters*
```

There are three states of alarm:

State	Means that...
Not active	there is no issue on the MDM5010 that raises the alarm.
Active	the MDM5010 has an issue that raises the alarm. An active alarm is marked with and the time of activation. An active alarm is marked with the time of activation.
Memorized	an issue that raises the alarm occurred on the MDM5010, but the issue has been resolved. A memorized alarm is marked with the time of activation and clearance.

Use the alarms-specific commands to view all alarms, only the active alarms, or only the memorized alarms. The example below shows the active alarms.

```
[MDM5010] alarms# active

+------------------------+-------+---------+--------------------------+----------+

| Alarm | State | Counter | Time On | Time Off |

+------------------------+-------+---------+--------------------------+----------+

| General Interface | ON | 1 | Tue Apr 13 16:57:34 2021 | never |

| Demodulator No PL Lock | ON | 1 | Tue Apr 13 16:57:34 2021 | never |

| Demodulator No Lock | ON | 1 | Tue Apr 13 16:57:34 2021 | never |

+------------------------+-------+---------+--------------------------+----------+
```

Each alarm has the following information:

Parameter...	Indicates...
StatusState	if the alarm is active (*ONalarm*) or not (*OFFstatusOK*). An alarm is activated when the MDM5010 has an issue that raises the alarm.
Counter StatusCnt	how many times the alarm has occurred.
Time OnOnTime	when the alarm was triggered. If the alarm is not active but memorized, it indicates the last time the alarm was active.
Time OffOffTime	when the alarm was cleared.

To reset the alarms counter, use the *resetcounter* command.

You can also view alarms per root branch. The example below shows the demodulator alarms.

```
[MDM5010] # demodulators alarms alarmstatustable showtable

+----------+---------------------------+-----------------+------------+----------+---------
----------+-------------------+

| Name | DemodulatorInternalError | InputSaturated | NoPlLock | NoLock | LnbPowerControl |
DecoderOverloaded |

+----------+---------------------------+-----------------+------------+----------+---------
----------+-------------------+

| demod1 | statusOK | statusOK | alarm | alarm | statusOK | statusOK |

+----------+---------------------------+-----------------+------------+----------+---------
----------+-------------------+
```

For more information about the alarms, see Dealing with Alarms.

An alarm has three parameters that enable you to manage the impact of the alarm:

Select...	If you want to...
General Device generaldevice GeneralDevice	mark the alarm as a general device alarm. When an issue occurs that raises this alarm, the *General Device* alarm*GeneralDeviceAlarm* is also activated. By default, general device alarms are monitored by the USS and trigger a redundancy switch. NOTE: For more information about device redundancy, see Device Redundancy.

Select...	If you want to...
General Interface generalinterface GeneralInterface	mark the alarm as a general interface alarm. When an issue occurs that raises this alarm, the *General Interface* alarm*GeneralInterfaceAlarm* is also activated. The USS can be configured to monitor general interface alarms and trigger a redundancy switch when the alarm occurs. NOTE: For more information about device redundancy, see Device Redundancy.
Alarm MaskmaskMask	ignore the alarm. When an issue occurs that would raise the alarm, the alarm is not activated. NOTE: Masked alarms are not considered for device redundancy swaps.

To configure an alarm, go to the *configuration* branch, and then set the parameter. The example below masks the hardware failure alarm.

```
[MDM5010] alarms# configuration hardwarefailure set mask=on

OK
```

5.7 Managing the Device Log

The device log contains information about activities within the MDM5010, and can be used to observe, troubleshoot, or debug the MDM5010.

Go to the branch *device log*, and then enter the *show* command to view the available branches and branch-specific commands.

```
[MDM5010] device log# show

replay*

local/

remote/

filter/

clear*

export*
```

Use command...	To...
replay	view the device log. Use the parameter *maxlines* to specify the maximum number of log entries to display. Valid values are from 0 to 100000. The default value is 0 which means no limit.
clear	remove all existing log messages and start a new log file.
export	export the device log. The log file is saved as a .txt file in the *Download* folder of the MDM5010. Retrieve the log file using SCP, see SCP Interface.

Local device logging is enabled by default. To disable local logging, go to the *local* branch, and then set the *enable* parameter to **off**.

```
[MDM5010] device log local# set enable=off

OK
```

The *replay* command will now show:

```
[MDM5010] device log# replay

Log empty: Local syslog disabled
```

Remote logging can be enabled. The log messages are then sent to a remote syslog server using UDP.

To enable remote logging, go to the *remote* branch, and then set the parameters. The example below enables remote logging to a server with IP address 10.10.10.10 and using UDP port 514 (default port).

```
[MDM5010] device log remote# set enable=on ipaddress=10.10.10.10

OK
```

Use the *filter* branch to manage the log level per facility.

```
[MDM5010] device log filter# show

alarms/

configuration/

system/

internalerror/

authentication/

networking

[MDM5010] device log filter# alarms show

facility : alarms

level : info
```

For more information about facilities and log levels, see The Device Log.

5.8 Viewing the Diagnostic Report

The diagnostic report includes the complete device configuration, software and hardware information, monitoring and alarms information, the device log, and any other technical information that can be useful for troubleshooting or debugging the MDM5010.

Go to the branch *device diagnotics*, and then enter the *show* command to view the available branch-specific commands.

```
[MDM5010] device diagnostics# show

view*

export*
```

Use command...	To...
view	view the diagnostic report.
export	export the diagnostic report. Use the *type=user* parameter to export the standard report (default). The report is saved as a .txt file in the *Download* folder of the MDM5010. Use the *type=debug* parameter to export the extended and encrypted report. the report is saved as a .zip.enc file in the *Download* folder of the MDM5010. Retrieve the diagnostic report from the MDM5010 using SCP, see SCP Interface.

For more information about the report, see The Diagnostic Report.

5.9 Upgrading the Software

The procedure describes how to upgrade the software of the MDM5010 SCPC Satellite Modem.

Make sure you have the new software image file (*.bin) on your local computer.

CAUTION: The MDM5010 will reset during the procedure, and traffic will be impacted.

CAUTION: Save your configuration before upgrading the software, see Handling Device Configuration.

To upgrade the software:

1. Upload the *installer.bin* file to the *upload* folder on the MDM5010 using SCP, see SCP Interface.
2. Access the command line shell. Log in as *expert*.
3. Go to the *device* branch, and then enter the command to update the software:

```
[MDM5010] device# softwareupgrade filename=installer.bin
```

NOTE - Use parameter 'reboot=no' if you want to upgrade the software but not yet activate it. The software will be activated at the next hardware reset.

NOTE - Make sure to use the correct file name. The file name in the procedure is just an example.

The upgrade can take up to five to ten minutes, depending on your network connection for uploading the image, and the size of the image. Log in to the CLI again when finished.

Go to the *device identification* branch, and then enter the *show* command to view the software version.

5.10 Uploading the License

The procedure describes how to upload a license to the MDM5010. For more information about licenses, see Licenses.

Make sure you have the new license file (*.ini) on your local computer. By default, the MDM5010 has a permanent license including the software options ordered when the MDM5010 was purchased.

CAUTION: The MDM5010 will reset during the procedure, and traffic will be impacted.

CAUTION: Save your configuration before upgrading the software, see Handling Device Configuration.

To upload the license:

1. Upload the new license file to the *upload* folder on the MDM5010 using SCP, see SCP Interface.
2. Access the command line shell. Log in as *expert*.
3. Go to the branch *device license*, and then enter the command to upload the license file:

```
[MDM5010] device license# import filename=license.ini
```

NOTE - Use parameter 'reboot=no' if you want to upload the license but not yet activate it. The license will be activated at the next hardware reset.

NOTE - Make sure to use the correct file name. The file name in the command is just an example.

The upgrade can take up to five minutes.

5.11 Removing the Temporary License

The procedure describes how to remove the temporary license from the MDM5010 SCPC Satellite Modem before it has expired. When removed, the permanent license becomes active again. For more information about temporary licenses, see Licenses.

CAUTION: The MDM5010 will reset during the procedure, and traffic will be impacted.

CAUTION: Save your configuration before upgrading the software, see Handling Device Configuration.

To remove the temporary license, go to the branch *device license*, and then enter the command:

```
[MDM5010] device license# remove temporary
```

NOTE - After reset the MDM5010 may raise the Boot Configuration Failure alarm because certain configuration might no longer be available. Load or import a valid configuration to clear the alarm.

NOTE - Uploading a new permanent license will also remove the temporary license from the MDM5010. For more information about uploading licenses, see Uploading the License.

5.12 Resetting the MDM5010

CAUTION: Traffic will be impacted.

CAUTION: Save the configuration before a hardware or software reset, see Handling Device Configuration.

Go to the branch *device* and use the *reset* command.

```
[MDM5010] device# reset help

reset the device

Mandatory parameters:

* Reset {enum}: Reset (default value = Software) (options: Hardware Software Factory Configs)
```

Use one of the following parameters:

Use...	To...
Hardware	power cycle the MDM5010. The reset can take up to five minutes. When finished, log in to the CLI again. Any unsaved configuration is lost, the device log is reset, and the boot configuration is loaded.
Software	reboot the operating system. The reset can take up to one minute. When finished, log in to the CLI again. Any unsaved configuration is lost, and the boot configuration is loaded.
Configs	delete all saved and unsaved application-specific configuration. The MDM5010 is reset to the *initialconfig* configuration including the factory default settings. The reset includes a software reset and can take up to one minute. When finished, log in to the CLI again. NOTE: The system-specific configuration is excluded from the reset to avoid losing connectivity with the MDM5010.
Factory	reset the MDM5010 to the factory default settings, including the system-specific configuration, password settings, time zone setting, and so on. The reset includes a hardware reset and can take up to five minutes. NOTE: You might lose connectivity to the MDM5010.

For more information about the configuration, see The MDM5010 Configuration.

5.13 Switching to Dialog® VSAT Mode

The MDM5010 is a multi-personality modem. With a simple switch of the software, the MDM5010 modem in SCPC standalone mode can be converted into a flexible Dialog® VSAT modem. When operating as a VSAT modem, you can easily switch back to the SCPC standalone personality and resume operation where you have left it.

CAUTION: Save your boot configuration before switching. When switching from VSAT back to SCPC standalone mode, the boot configuration will be loaded.

To switch to Dialog® VSAT mode, go to the branch *multipersonality*, and then enter the command:

```
[MDM5010] multipersonality# switch reboot=yes
```

This command includes a hardware reset. After the reset, the MDM5010 will run in VSAT mode and can be used in a Dialog® VSAT network.

NOTE - To switch from Dialog® VSAT mode to SCPC standalone mode, see the *MDM5010 User Guide* for Dialog® R4.6.5 or up.

To schedule the switch but not yet execute it, enter the command:

```
[MDM5010] multipersonality# switch reboot=no

OR

[MDM5010] multipersonality# switch
```

The MDM5010 will not reset and will continue operating in SCPC standalone mode. The VSAT mode will then only be activated at the next hardware reset.

To check if a switch is scheduled, enter the command:

```
[MDM5010] multipersonality# switch scheduled
```

If the command returns **yes**, a switch is scheduled and will be executed at the next hardware reset.

If the command returns **no**, no switch is scheduled.

To abort a scheduled switch, enter the following command:

```
[MDM5010] multipersonality# manager abort
```

5.14 Exporting SNMP MIB-modules

1 Enter the branch name *device*, and then enter the command to export the MIB-modules:

```
[MDM5010] device# mibs export
```

The *mibs.zip* file is added to the *download* folder of the MDM5010.

2 Retrieve the *mibs.zip* file using SCP, see SCP Interface.

For more information about SNMP, see Managing the MDM5010 using SNMP.

6 Managing the MDM5010 using SNMP

NOTE - This user guide does not provide detailed information about managing the MDM5010 using SNMP. It is recommended to manage the MDM5010 using the GUI, REST API, or CLI

SNMP or Simple Network Management Protocol is used to manage and monitor the MDM5010 using a Management Information Base or MIB.

Use an SNMP browser, such as HPOpenView or NetworkView, to connect to the management IP address of the MDM5010 (SNMP agent). The SNMP implementation in the MDM5010 has the *AuthNoPriv* security level. This means that SNMP messages are authenticated but not encrypted. Authentication is based on a community string sent with each SNMP message. This string must be known by both the SNMP agent, running on the MDM5010 and SNMP manager, running on your local computer.

SNMP access is disabled by default. To enable access, see Controlling Access.

NOTE - It is recommended to change the default community string. For more information, see Changing SNMP Community Strings.

In this chapter:

NOTE - Make sure your local computer can reach the management IP address of the MDM5010.

6.1 Management Information Base

A management information base (MIB) defines the data that can be managed through SNMP. The MIB is a hierarchical database (tree-structured) and each entry is addressed through an object identifier (OID). For the SNMP agent and manager to communicate successfully, both need to know which OIDs are available. The agent (MDM5010) collects the data locally and stores it, as defined in the MIB. The manager uses the database to request the agent for specific information, or to modify or assign the value of the managed data. The MDM5010 supports several MIB-modules, each representing a subset of the management information. They are defined according to the ASN.1 or Abstract Syntax Notation One.

The MIB-modules can be downloaded from the MDM5010 using GUI or CLI:

- Download the MIB-modules using the GUI
- Download the MIB-modules using the CLI

6.2 SNMP Traps

Next to the SNMP messages initiated by the SNMP manager, such as *Get* and *Set*, the MDM5010 also supports SNMP trap messages. A trap is sent by the MDM5010 (SNMP agent) without having been requested by the SNMP manager. Traps are sent upon determined conditions, such as in the event of an error, or upon a crossing of a threshold. Incoming traps are used to inform an SNMP manager when an important event happens at the MDM5010. A benefit of using traps for monitoring and managing alarms is that they trigger instantaneously, rather than waiting for a status request from the manager.

The MDM5010 supports three trap types:

Type	Description
TrapV1	This is an SNMP v1 trap. Use this type when the supported SNMP version of your manager is v1.
TrapV2	This is an SNMP v2 trap. Use this type when the supported SNMP version of your manager is v2.
Inform	An SNMP Inform message is confirmed by the SNMP manager. Inform messages are not supported in SNMP v1.

To receive trap messages from the MDM5010, the IP address of the destination, the trap type, and trap community string must be configured. For more information about the trap community string, see Community Strings.

You can add up to four trap destinations.

NOTE - Make sure that the MDM5010 can reach the trap destination IP address.

The SNMP trap configuration can be done using the GUI, REST API, CLI, or SNMP.

- SNMP Trap Configuration Via the GUI
- SNMP Trap Configuration Using REST APIs
- SNMP Trap Configuration Via the CLI
- Using SNMP

6.2.1 SNMP Trap Configuration Via the GUI

1. Log in as an expert user.
2. Select *Dashboard* in the menu at the left, and then select the *Modem Setup* tab.
3. Click **Access Management** and edit the *Trap Configuration* table.

- Enter the IPv4 address of the SNMP manager in the *IP Address* field
- Select the type of trap message from the *Type* drop-down list
- Change the trap community string in the *Community* field

4 Click to confirm each setting.

For more information about using the GUI, see Managing the MDM5010 via the GUI.

6.2.2 SNMP Trap Configuration Using REST APIs

NOTE - Make sure to authenticate as expert user.

To configure SNMP traps for destination x, where x = 1, 2, 3, or 4, send the following request:

```
PATCH http://<ip_address>:9000/RestApi/Device/Snmp/Notifications/Destination/x

{

"Destination": x,

"IpAddress": "10.10.10.10",

"Type": "Inform",

"Community": "your_trap_string"
}
```

NOTE - The IP address, type and community string are just examples.

For more information about using the REST API, see Managing the MDM5010 using REST API.

6.2.3 SNMP Trap Configuration Via the CLI

Log in as an expert user.

Enter the branch name *device snmp notification destination*, and the command to configure SNMP traps for destination x, where x = 1, 2, 3, or 4:

```
[MDM5010] device snmp notifications destination# x set ipaddress=10.10.10.10 type=inform
community=your_trap_string
```

NOTE - The IP address, type and community string are just examples.

For more information about using the CLI, see Managing the MDM5010 using CLI.

6.2.4 Using SNMP

Make sure to use the correct read-write community string.

To configure the IP address of destination x, where x = 1, 2, 3, or 4, send the following request:

```
SET

.iso.org.dod.internet.private.enterprises.ntcMIB.ntcPublic.ntcFunction.ntcDevice.ntcDevObject
s.ntcDevSnmp.ntcDevSnmpNotification.ntcDevSnmpNotifDestTable.ntcDevSnmpNotifDestEntry.ntcDevS
nmpNotifDestIpAddress.x

10.10.10.10
```

To configure the trap type of destination x, where x = 1, 2, 3, or 4, send the following request:

```
SET

.iso.org.dod.internet.private.enterprises.ntcMIB.ntcPublic.ntcFunction.ntcDevice.ntcDevObject
s.ntcDevSnmp.ntcDevSnmpNotification.ntcDevSnmpNotifDestTable.ntcDevSnmpNotifDestEntry.ntcDevS
nmpNotifDestType.x

inform
```

To configure the trap community string of destination x, where x = 1, 2, 3, or 4, send the following request:

```
SET

.iso.org.dod.internet.private.enterprises.ntcMIB.ntcPublic.ntcFunction.ntcDevice.ntcDevObject
s.ntcDevSnmp.ntcDevSnmpNotification.ntcDevSnmpNotifDestTable.ntcDevSnmpNotifDestEntry.ntcDevS
nmpNotifDestCommunity.x

your_trap_string
```

NOTE - The IP address, type and community string are just examples.

6.3 Community Strings

The SNMP implementation in the MDM5010 has the *AuthNoPriv* security level. This means that SNMP messages are authenticated but not encrypted. Authentication is based on a community string sent with each SNMP message. This string must be known by both the SNMP agent, running on the MDM5010 and SNMP manager, running on your managing device. If the community string is incorrect, the agent will disregard the request from the manager, or the manager will disregard the notification from the agent.

There are three types of community strings:

Type...	Is used to...	Default value
Read-only	get information.	public
Read-write	get and set information.	private
Trap	send notifications.	trapcom

NOTE - The maximum length of a community string is up to 30 characters and can only include alphanumeric characters. It cannot include any spaces.

It is recommended to change the default community string. For more information, see Changing SNMP Community Strings.

A Maintenance Procedures

In this chapter:

A.1 Upgrading the Software

The procedure describes how to upgrade the software of the MDM5010.

Make sure you have the new software image file (*.bin) on your local computer.

The software can be upgraded using the GUI or CLI:

- Upgrading the software using the GUI
- Upgrading the software using the CLI

CAUTION: The MDM5010 will reset during the procedure, and traffic will be impacted..

NOTE - Save your configuration before upgrading the software.

A.2 Uploading the License

The procedure describes how to upload a license to the MDM5010. For more information about licenses, see Licenses.

Make sure you have the new license file (*.ini) on your local computer.

The license can be uploaded using the GUI or CLI.

- Uploading the license using the GUI
- Uploading the license using the CLI
- Upgrading the software using the CLI

CAUTION: The MDM5010 will reset during the procedure, and traffic will be impacted..

NOTE - Save your configuration before uploading a license.

NOTE - If the license is not valid, or wrongly authenticated, the upload procedure will fail, and the current license will remain active.

A.3 Removing the Temporary License

The procedure describes how to remove the temporary license from the MDM5010 before it has expired. When removed, the permanent license becomes active again. For more information about temporary licenses, see Licenses.

The license can be removed using the GUI or CLI:

- Removing the temporary license using the GUI
- Removing the temporary license using the CLI

CAUTION: The MDM5010 will reset during the procedure, and traffic will be impacted.

NOTE - Save your configuration before removing the temporary license.

A.4 Resetting the MDM5010

CAUTION: Traffic will be impacted during a hardware or software reset.

NOTE - Save your configuration before a hardware or software reset.

There are four types of reset:

Use...	To...
Hardware reset	power cycle the MDM5010. Any unsaved configuration will be lost, the device log is reset, and the boot configuration is loaded. The reset can take up to five minutes.
Software reset	reboot the operating system. Any unsaved configuration will be lost, and the boot configuration is loaded. The reset can take up to one minute.
Configuration reset	delete all saved and unsaved application-specific configuration. The MDM5010 is reset to the *initialconfig* configuration including the factory default settings. The reset can take up to one minute. **NOTE -** The system-specific configuration is excluded from the reset to avoid losing connectivity with the MDM5010.
Factory reset	reset the MDM5010 to the factory default settings, including the system-specific configuration, password settings, time zone setting, and so on. The reset includes a hardware reset and can take up to five minutes. **Caution:** You might lose connectivity to the MDM5010.

There are three ways to perform a *hardware* reset:

Unplug the power cord of the MDM5010 from the electrical outlet, not from the back of the MDM5010 (when possible); wait a few seconds, and then plug the power cord back into the outlet

- Use the GUI
- Use the CLI

NOTE - The hardware reset performed through the GUI or CLI only power cycles the router board. Unplugging the power cable power cycles all internal components.

A *software* or *configuration* reset can be performed using the GUI or CLI.

There are two ways to perform a *factory* reset:

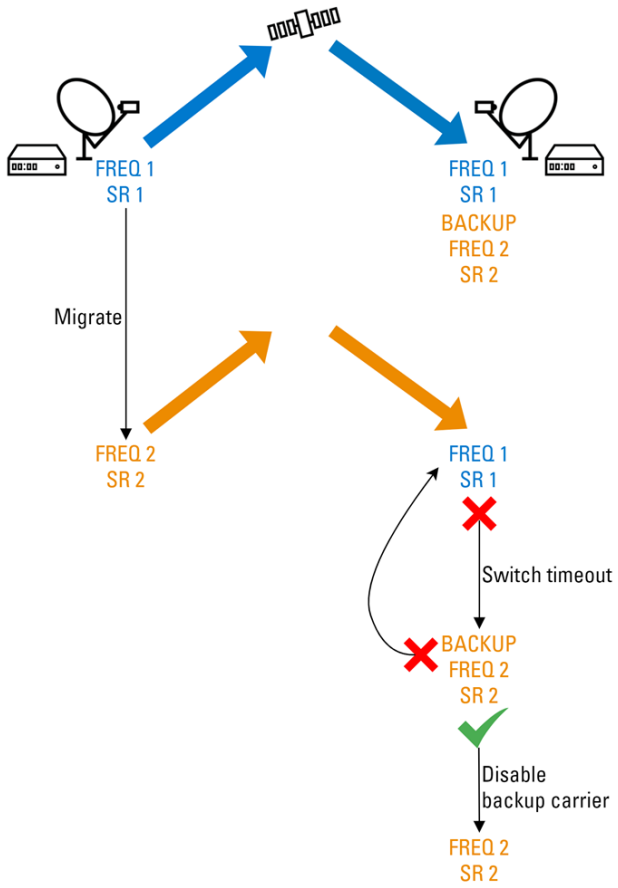
- Press the reset button on the front of the MDM5010, see MDM5010 Hardware Features

CAUTION: Do not use metal or conductive objects to press the reset button. Use a plastic or wooden object, like a toothpick.

- Use the CLI

A.5 Migrating a Carrier

The process flow to migrate a carrier using a backup carrier is shown below:



Set the backup downlink carrier in the receiving MDM5010 to the carrier to which you want to migrate (freq 2 and SR 2 in the example above).

When the transmit carrier is migrated, the receiving MDM5010 will no longer be able to lock on the primary downlink carrier (freq 1 and SR 1 in the example above). After a switch timeout, the MDM5010 will try the backup carrier.

When the MDM5010 successfully receives and demodulates the backup carrier, you can disable the backup carrier. This will automatically set the backup carrier as the primary carrier.

NOTE - If the MDM5010 does not lock on the backup carrier within the switch timeout, it will try the primary carrier again.

The backup carrier can be configured using the GUI, REST API, or CLI, see Configuration Quick Reference.

A.6 Switching to Dialog® VSAT Mode

The MDM5010 is a multi-personality modem, meaning that it can operate either as a SCPC standalone modem or a Dialog VSAT modem. When operating as a VSAT modem, you can easily switch back to the SCPC standalone personality and resume operation where you have left it.

CAUTION: Save your configuration before switching. When switching from VSAT back to SCPC standalone mode, the boot configuration will be loaded.

The personality switch can be done using the GUI or CLI:

- Switch personalities using the GUI
- Switch personalities using the CLI

NOTE - The switch is effective after a hardware reset and takes about five minutes

B Troubleshooting

In this chapter:

B.1 Dealing with Alarms

The table below describes the alarms that may appear on the MDM5010, and the appropriate action to take. If the problem persists, contact ST Engineering iDirect customer support.

Alarm...	Occurs when...	Action
Antenna Controller Communication	the TCP/IP connection between the MDM5010 and the antenna controller is down, and a configurable timeout has exceeded.	• Make sure that the configured IP address and TCP port are correct • Check the hardware connection between the MDM5010 and antenna controller
Antenna Controller Failure	the antenna controller is unavailable due to bad configuration, or ACU equipment failure.	• Make sure that the antenna controller is powered on • Make sure that the configuration of the antenna controller is valid
Bandwidth Cancellation No Lock	bandwidth cancellation is enabled but not locked (tracking is not successful).	• Disable BWC and verify the power of each carrier (local and remote) • Verify the delay and offset values • Increase the search windows • Adapt the bandwidth mode
Boot Configuration Failure	the boot configuration fails to load. This can happen, for example, when a temporary license includes software options which are no longer supported when the temporary license is removed or expired. The MDM5010 will reset to the *initialconfig* configuration including the factory default application-specific settings.	Make sure that the content of the configuration file is correct.
Demodulator Buffer Overflow	the internal buffer is overflown.	Contact ST Engineering iDirect customer support.

Alarm...	Occurs when...	Action
Demodulator Decoder Overloaded	the decoder is unable to decode the baseband frames, for example, due to bad signal quality, or the decoder cannot handle the input stream, for example, when the symbol rate is too high for the selected MODCOD.	• Make sure to select the correct MODCOD for the channel quality; lower the MODCOD at the transmit side and increase the ACM margins • Check if there are no failing hardware components, such as the LNB, in the receive link • Make sure that the MODCOD can handle the symbol rate, see MODCOD Limitations
Demodulator Input Saturated	the L-band input level at the demodulator is higher than -10 dBm.	• Check for the presence of an interferer • Add an attenuator in front of the L-band input
Demodulator Internal Error	the demodulator has an internal failure.	Contact ST Engineering iDirect customer support.
Demodulator LNB Power Control Error	there is an error in the LNB power supply, for example, a short circuit on the connector.	Check the hardware connection between the MDM5010 and LNB.
Demodulator No Lock	the demodulator cannot lock on the received carrier.	• Make sure that the frequency and symbol rate of the downlink carrier are correct • Check the RX hardware connection • Make sure that traffic is not too low, see Demodulator Lock Issue • Make sure transmit at the remote MDM5010 is not disabled
Demodulator No PL Lock	the demodulator cannot lock onto the headers of the physical layer (PL) frames. Lock occurs when two consecutive PL headers have been decoded successfully.	• Enable pilots at the transmit side • Make sure that the quality of the incoming signal is OK, for example, check the pointing of the antenna
Eth Data General Interface Failure	(no link redundancy) no signal is detected on at least one of the logical data interfaces. (link redundancy) no signal is detected on either logical data interface.	Make sure that the cables are intact and properly connected.

Alarm...	Occurs when...	Action
Eth Data Half Duplex	at least one logical data interface is in half duplex mode as a result of a link negotiation. The alarm does not occur when the interface is configured in half duplex mode.	• Make sure that auto-negotiation is enabled on the connected device • Disable auto-negotiation and manually set the duplex mode
Eth Data Link Failure	no signal is detected on at least one of the enabled logical data interfaces.	Make sure that the cables are intact and properly connected.
Eth Data Redundancy Degraded	link redundancy is enabled but only one logical data interface detects a signal.	Make sure that the cables are intact and properly connected.
Eth Data Redundancy Failure	link redundancy is enabled but no signal is detected on either logical data interface.	Make sure that the cables are intact and properly connected.
Eth Mgmt General Interface Failure	(no link redundancy) no signal is detected on at least one of the enabled management interfaces. (link redundancy) no signal is detected on either management interface.	Make sure that the cables are intact and properly connected.
Eth Mgmt Half Duplex	at least one management interface is in half duplex mode as a result of a link negotiation. The alarm does not occur when the interface is configured in half duplex mode.	• Make sure that auto-negotiation is enabled on the connected device • Disable auto-negotiation and manually set the duplex mode
Eth Mgmt Link Failure	no signal is detected on at least one of the enabled management interfaces.	Make sure that the cables are intact and properly connected.
Eth Mgmt Redundancy Degraded	link redundancy is enabled but only one physical management interface detects a signal.	Make sure that the cables are intact and properly connected.
Eth Mgmt Redundancy Failure	link redundancy is enabled but no signal is detected on either physical management interface.	Make sure that the cables are intact and properly connected.
Fan Failure	the fan has poor performance or stopped working.	Contact ST Engineering iDirect customer support.
General Device	an active alarm is marked as a *General Device* alarm. General Device alarms trigger by default device redundancy swaps.	The action depends on the underlying active alarm.

Alarm...	Occurs when...	Action
General Interface	an active alarm is marked as a *General Interface* alarm. General Interface alarms can trigger device redundancy swaps.	The action depends on the underlying active alarm.
Hardware Inventory	the hardware does not correspond with what has been set in the software.	Contact ST Engineering iDirect customer support.
Internal Error	the MDM5010 has an internal error, such as DAC failure.	Contact ST Engineering iDirect customer support.
Invalid License	the license file is not available or is not correctly authenticated.	Contact ST Engineering iDirect customer support.
IP Data Gateway Unreachable	the gateway IP address for the data interfaces cannot be reached, or no MAC address can be obtained using ARP.	• Make sure that the gateway IP address is correct • Check your data network
IP Mgmt Gateway Unreachable	the gateway IP address for the management interfaces cannot be reached, or no MAC address can be obtained using ARP.	• Make sure that the gateway IP address is correct • Check your management network
License About To Expire	the temporary license file's expiry time is less than 15 days.	• Order and upload a new temporary license to extend the validity period • Remove the temporary license before expiry; the MDM5010 will fall back to the permanent license When the temporary license file expires, the MDM5010 will reboot and fall back to the permanent license.
License Upgrade Failure	the license file you want to upload is corrupted, invalid, or wrongly authenticated.	Contact ST Engineering iDirect customer support.
Modulator Buffer Overflow	the input buffer is full.	Contact ST Engineering iDirect customer support.
Modulator Buffer Underflow	the input buffer is empty.	Contact ST Engineering iDirect customer support.
Modulator Calibration Data	no calibration data is available for the modulator.	Contact ST Engineering iDirect customer support.
Modulator Input Frame Sync	the modulator cannot synchronize with the incoming baseband frames.	Contact ST Engineering iDirect customer support.

Alarm...	Occurs when...	Action
Modulator Input Signal	no signal is detected at the input of the modulator.	Contact ST Engineering iDirect customer support.
Modulator Internal Failure	the modulator has an internal failure, such as a DAC failure.	Contact ST Engineering iDirect customer support.
NTP No Peer Failure	NTP is enabled but none of the configured NTP peers can be reached.	Make sure that the MDM5010 can reach at least one NTP peer.
Temperature	the temperature of the MDM5010 is higher than 85 °C.	• Make sure that the fans of the MDM5010 work as expected • Make sure that there is enough space around the MDM5010 • Verify the air cooling in the room where the MDM5010 is located
Unit Redundancy	device redundancy is enabled but there is no redundant setup.	Make sure that the redundant MDM5010(s) is(are) available and working.

B.2 The Device Log

The device log contains information about activities within the MDM5010, and can be used to observe, troubleshoot, or debug the MDM5010.

A log message is a single entry in the log file and has the following format: `[Facility - Log level] [Time stamp] Description`

- The *facility* specifies the type of activity that occurred, for example, an alarm, a configuration change, and so on
- The *log level* or log severity is a piece of information telling how important a given log message is
- The *time stamp* indicates the time that the activity occurred (according to the date and time set on the MDM5010)
- The *description* provides information about the logged activity

The MDM5010 has six facilities:

Facility...	Is used when logging...
alarms	alarm triggers and clearances.
configuration	configuration changes.
system	system changes.
internal error	internal errors.
authentication	control interfaces access.
networking	activities impacting the network interfaces.

Per facility a log level can be set. There are nine log levels, including log level OFF which disables the logging of the facility. The log level is set to INFO for all facilities by default.

Use log level...	To...
OFF	turn off logging.
TRACE	log all actions and details you possibly can. This is the most verbose log level and will enable all subsequent log levels.

Use log level...	To...
DEBUG	log diagnostic information that is most useful for troubleshooting.
INFO	log informational messages that highlight the normal progress.
NOTICE	log conditions that are normal, but that may require special handling.
WARN	log potentially harmful situations that may require intervention when the issue persists or recurs.
ERROR	log serious situations that require intervention either immediately, or in the near future.
ALERT	log critical situations that need immediate action.
EMERG	log catastrophic situations where the system is about to abort to prevent corruption or serious problem, if possible. This is the most restrictive log level. When this log level is enabled, all events under other levels are not logged.

NOTE - When choosing log levels, keep in mind that logging has a performance penalty when your system is doing time critical operations.

Local device logging is enabled by default. The local device log can be viewed, downloaded, and cleared using the GUI or CLI.

Remote logging can be enabled. The log messages are then sent to a remote syslog server using UDP.

Use the GUI, REST API, or CLI control interface to change the log level of a facility, and to enable or disable logging.

B.3 The Diagnostic Report

When the MDM5010 has one or more issues, the diagnostic report can be used for debugging. There are two types of diagnostic report:

- The standard diagnostic report that you can view
- The extended diagnostic report that is encrypted and that can only be viewed by ST Engineering iDirect customer support

NOTE - When contacting ST Engineering iDirect customer support for help, it is good practice to provide the encrypted diagnostic report by default.

The standard diagnostic report includes:

- FPGA information
- NIOS information
- Hardware capabilities
- General device and main board information
- Boot configuration file name
- Stored configuration files
- Current system configuration
- Current volatile configuration
- Uptime
- Process monitoring state
- Linux file system
- Persistent storage usage
- Memory usage
- Log file, see The Device Log
- Overview file descriptors
- Ethernet interfaces
- Ethernet links
- Multicast addresses
- System routing tables
- Build information
- Datamodel view

The diagnostic report can be viewed and downloaded using the GUI, or CLI.

B.4 Checking the Active License Type and Software Options

The procedure describes how to check the active license type and software options. For more information about licenses, see Licenses.

The license type can be checked using the GUI, REST API, or CLI.

- Using GUI
- Using REST API
- Using CLI

B.4.1 Using GUI

1. Click the *Dashboard* menu, and then click the *Modem Info* tab.
2. To view the license type and software options, click **Identification**.

B.4.2 Using REST API

Authenticate as expert user.

To view the license type, send the following request:

```
GET http://<ip_address>:9000/RestApi/Device/Identification/LicenseType

"permanent"
```

To view the software options, send the following request:

```
GET http://<ip_address>:9000/RestApi/Device/Identification/DeviceOptions

{

"SalesCode": "OX-17",

"Description": "300 Mbps max Tx rate"

}
```

B.4.3 Using the CLI

Log in as expert.

Go to the *device identification* branch, and then enter the *show* command to view the license type:

```
[MDM5010] device identification# show
```

To view the software options, enter the following command:

```
[MDM5010] device identification# deviceoptions show
```

B.5 Demodulator Lock Issue

When return traffic is low (few bytes per second), the demodulator may experience issues with locking. These issues could, for example, affect the performance of bandwidth cancellation.

To make sure that the demodulator always remains locked:

1. Generate and send a continuous data stream to the demodulator. For example, send traffic from a laptop in the local data network to a laptop in the remote data network, and vice versa if bi-directional traffic is needed. The dummy traffic should not interfere with the regular data traffic and the rate should be at least 1 Mbps.

2. Create a classification node that matches and forwards the dummy data stream. Set the *Matching Order* value to 99, making sure that the regular traffic gets priority. For more information about creating a classification node, see Defining the Classification Rules and Nodes.

B.6 Traffic Issue when Changing the VLAN ID

Traffic can be blocked if the following scenario occurs:

- The *Forwarding Mode* is set to **Layer 2**, see Defining the Classification Rules and Nodes
- Both the local and remote MDM5010 are connected to a switch that runs the PVST+ protocol.

  Note that it can happen with other protocols. The spanning tree protocol, such as PVST+, is explicitly mentioned here as this protocol should be used to support redundancy.
- The local and remote side use different VLAN IDs and each MDM5010 has a corresponding VLAN ID translation rule.

When a PVST+ packet is sent from the local network, the local switch sets the local VLAN ID (for example, 20) in the *802.1Q VLAN ID* field of the layer 2 (Ethernet) header, and in the *Originating VLAN* field of the PVST+ header. At the remote MDM5010 the *802.1Q VLAN ID* (20) is translated according to the rule (for example, to 30), the *Originating VLAN* value (20) of the PVST+ header is not changed. When the remote switch receives the layer 2 packet, it will identify two different VLAN IDs (30 and 20) and will assume there is a loop between both VLANs. As a result, the remote switch will prune the remote VLAN (30) from the trunk line and traffic from the remote switch to the remote MDM5010 is blocked. The same applies to PVST+ packets sent from the remote network to the local network. The local switch will prune the local VLAN (20) from the trunk line.

To solve this issue:

- Disable the spanning tree protocol; only do this when you are not using redundancy, or there is no risk of bridge loops
- Avoid sending PVST+ packets by filtering out PVST+ packets using a classification rule, see Defining the Classification Rules and Nodes

  For example, using the expression that matches all packets except the ones with destination MAC address 01:00:0C:CC:CC:CD (which is the Cisco shared spanning tree protocol address):

```
all and not dst ether 01:00:0C:CC:CC:CD
```

- Only have one switch, either behind the local or remote MDM5010.
- Use IEEE STP/RSTP/MSTP as spanning tree protocol; these protocols do not have an *Originating VLAN* field

C Technical Descriptions

In this chapter:

C.1 Quality of Service

Quality of Service (QoS) is the ability to differentiate diverse classes of traffic based on predefined criteria, and assign priorities based on traffic variables that affect the treatment of traffic in the network.

The first step in the deployment of QoS is to identify the various traffic classes that need to be supported. Traffic can be classified based on any field of the packet, such as VLAN tag, IP addresses, ToS byte. After traffic has been classified into different classes, the next step is to identify what shaping will be performed on each of these classes.

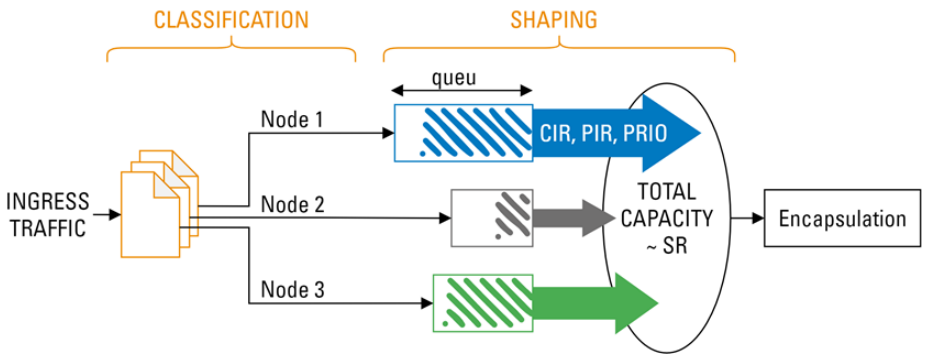
Three broad types of traffic are typically distinguished: sensitive, best-effort, and undesired.

Sensitive traffic is traffic that has an expectation to deliver on time, such as VoIP, and video conferencing. The quality of service of sensitive traffic is typically guaranteed, or at least prioritized over other classes of traffic.

Best-effort traffic is all other kinds of non-detrimental traffic. This is traffic that is not sensitive to QoS metrics, such as jitter, packet loss, latency. A typical example would be email applications. Best-effort traffic generally gets what is left after sensitive traffic.

Undesired traffic is generally limited to the delivery of spam and traffic created by worms, botnets, and other malicious attacks. In these cases, traffic is either blocked entirely, or severely hampered.

In the MDM5010, classification and shaping are combined in the concept of a node. The node includes a classification expression and defines how traffic that matches the expression is to be shaped.



At the ingress point (the point at which traffic enters the MDM5010) the traffic is matched against the classification expression in the nodes. The nodes have a matching order defining the sequence in which the nodes are checked. The expression of the node with the lowest matching order value is tried first. When there is a match, the classification stops; when there is no match, the expression of the node with the next lowest matching order value is tried, and so on.

NOTE - The more specific the expression is, the lower the matching order should be. Give the highest matching order value to a catch-all traffic rule.

Traffic that does not match an active node is dropped.

For more information about the syntax of an expression, see Classification Expressions.

After matching an expression, the traffic is shaped based on the following characteristics:

Characteristic	Description
Confirmed information rate (CIR)	This is the guaranteed or minimum data traffic rate.
Peak information rate (PIR)	This is the maximum data traffic rate. Packets that exceed this rate will be queued, and possibly dropped.
Priority	The priority specifies if traffic should be treated with higher priority over other traffic. The lower the value, the higher the priority.
Maximum queue time	The maximum queue time specifies the maximum time a packet can stay in the queue before being dropped. The queue is filled with packets at the data rate of the customer application, but the packets are queued only for the maximum queue time (and up to the queue size (50 MB)). NOTE: If traffic is bursty, the timeout should be large enough.

The rates include overhead. When the forwarding mode is layer 2, the overhead includes layer 2 and 3 overhead. When the forwarding mode is layer 3, the overhead includes layer 3 overhead only.

The shaping mechanism first assigns the CIR to the available nodes, starting with the highest priority nodes. When the required traffic rate is lower than the CIR value, only the required traffic rate is assigned. When congestion occurs (nodes with equal priority are competing for capacity), the PIR value will decide how much rate each node will get.

For example, two nodes (node 1 and 2) each have a CIR of 1 MB. The total capacity to distribute is 1 MB. Node 1 has a PIR of 1 MB, node 2 has a PIR of 0.5 MB. Both nodes have the same priority. When both nodes are asking for 1 MB throughput, node 1 will get twice the throughput of node 2 according to this formula: $CIR_{assigned\_node\ x} = (CIR_{node\ x} * PIR_{node\ x}) / sum_{nodes}(PIR)$

- For node 1: (1 * 1)/(1 + 0.5) = 0.66 MB
- For node 2: (1 * 0.5)/(1 + 0.5) = 0.33 MB

When the sum of CIR values of the configured nodes exceeds the total capacity, CIR cannot be guaranteed.

When, after assigning the CIR, capacity is still left ($total\ capacity - sum_{nodes}(CIR_{assigned\_node}) > 0$), PIR is assigned, again starting with the highest priority nodes.

The total rate per node is $CIR_{assigned\_node} + PIR_{assigned\_node}$.

After classification and shaping, traffic is encapsulated in GSE packets which are added to baseband frames. See GSE Encapsulation and Baseband Frames.

C.2 GSE Encapsulation and Baseband Frames

After classification and shaping (see Quality of Service), the traffic is encapsulated in GSE packets and added to baseband frames.

The MDM5010 uses GSE (generic stream encapsulation) encapsulation, a standard DVB protocol, to carry network-layer packets (also called Protocol Data Units or PDUs) on top of the uni-directional physical layer DVB-S2X.

The PDUs are encapsulated in one or more GSE packets. The encapsulation process adds control information, such as the network protocol type and address label, and provides an overall integrity check when needed.

GSE packets are sent in DVB-S2X baseband frames. The flexible PDU fragmentation allows adapting of the size of each GSE packet to the length of the baseband frame, or to the remaining space. This typically permits a reduction of padding in baseband frames and to optimize capacity gain.

The filling of a baseband frame with GSE packets is controlled by the encapsulation interval and the packet time.

Parameter...	Defines...
Packing time	the maximum time to fill a baseband frame with GSE packets. When the packing time is exceeded and the baseband frame is not filled, padding is added to the frame. The baseband frame is then sent to the output of the encapsulator. Baseband frames that are filled before the packing time is exceeded, are immediately forwarded.
Encapsulation interval	the interval at which the baseband frames are forwarded from the encapsulator to the FEC encoder.

The packing time should be larger than the encapsulation interval.

The MDM5010 can automatically set the parameters to increase the link efficiency (optimized for ACM), or to decrease the jitter (optimized for jitter).

After encapsulation, the baseband frames are coded and modulated. See Coding and Modulation.

C.3 Coding and Modulation

The MODCOD specifies the coding and modulation scheme used to transmit the digital information (baseband frames) over the satellite link. The coding scheme (1/4, 8/9, and so on) refers to the FEC (Forward Error Correction) overhead. These are redundant bits added to the user's data to ensure that traffic is reliably transported from one point to another, by detecting and often correcting errors in the transmission. A coding scheme of 1/4 indicates that on a total number of four bits, there are three redundant FEC bits and one bit of user date. The size of a coded baseband frame (FECFRAME) is fixed. The size (frame type) can be 64,800 bits (normal) or 16,200 bits (short). Normal frames are more efficient than short frames; short frames can reduce end-to-end system latency.

NOTE - Use short frames for low-speed links (< 1 MBaud).

The bits of each FECFRAME are then mapped into modulation symbols depending on the modulation order. Valid orders of modulation are QPSK, 8PSK, 16APSK, 32APSK, 64APSK, and 256APSK. The result is a compleX FEC frame (XFECFRAME). An XFECFRAME is translated into a PL (Physical Layer) frame (PLFRAME) with a PL header and optionally pilot blocks. *Pilots* can be used to increase the reliability of the receiver synchronization. The XFECFRAME is sliced into slots of 90 symbols and a pilot is inserted after every 16 slots. Pilots are blocks of 36 unmodulated symbols which can be received by any receiver. Dummy PLFRAMEs are added when no XFECFRAME is ready to be processed and transmitted.

Prior to modulation, each PLFRAME, excluding the PLHEADER, is randomized for energy dispersal. The PL scrambler signature specifies the spreading sequence number. This number is used by the modulator as a master key to scramble the PLFRAMEs. The same number must be known by the demodulator so that demodulation is possible.

The MODCOD to use depends on the link quality. A good link quality enables you to use a higher order modulation and lower FEC overhead, which increases your throughput and performance. When ACM (Adaptive Coding and Modulation) is enabled, the MODCOD is adjusted according to the actual link conditions. For more information, see Adaptive Coding and Modulation.

Finally, the modulation turns the PL frames into an analog signal that can be transmitted over the satellite link.

The analog signal is specified by the following parameters:

- Power level, at TX interface of the MDM5010
- L-band center frequency
- Symbol rate (SR) and roll-off, resulting in the carrier bandwidth = (1+α)SR; when roll-off = 5%, then α = 0.05
- Spectrum inversion

(*source: DVB-S2(X) standard ETSI EN 302 307*)

C.4 Adaptive Coding and Modulation

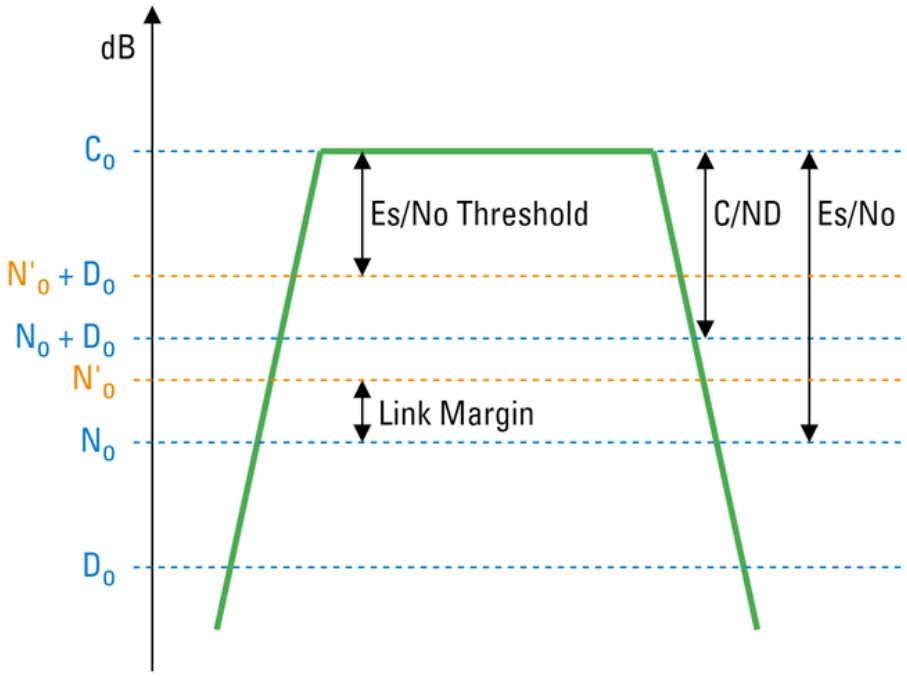
The Adaptive Coding and Modulation (ACM) technique enables real-time modification of the FEC overhead and modulation of baseband frames, based on link quality feedback from the receiver side.

A MODCOD has a minimum Es/No (threshold) required at the receiver side. This Es/No value guarantees that the receiver can demodulate the symbols. The value depends on the quality of the demodulator. This threshold, together with the link budget specify which MODCODs can be used at the transmitter side. The link budget depends on the ground equipment, satellite, power, atmospheric conditions, but also possible interference, rain fading, and so on.

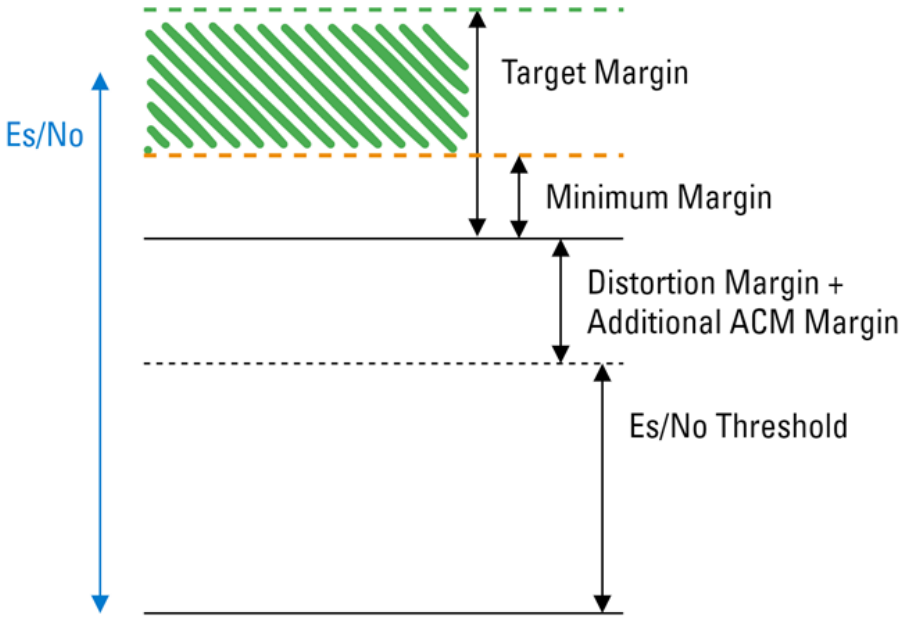
In Constant Coding and Modulation (CCM) mode, the choice of the MODCOD is a trade-off between efficiency and availability. High-order MODCODs provide high throughput but require good link quality. Low-order MODCODs can operate in less good link conditions but provide less throughput.

With ACM, the MODCOD is automatically adapted according to the link quality measured at the receiver side. When the link quality deteriorates, for instance due to rain fading, the ACM mechanism switches to a lower-order and more robust MODCOD, making sure that the receiver can still demodulate the signal. When the link quality is optimal, the highest-order MODCOD can be used, providing the highest efficiency.

In the MDM5010 the link quality, expressed as Es/No, is measured form the header Es/No, the link margin, or the C/ND.



The decision for using a MODCOD is based on the measured Es/No, the Es/No threshold value of the MODCOD, and several ACM margins.

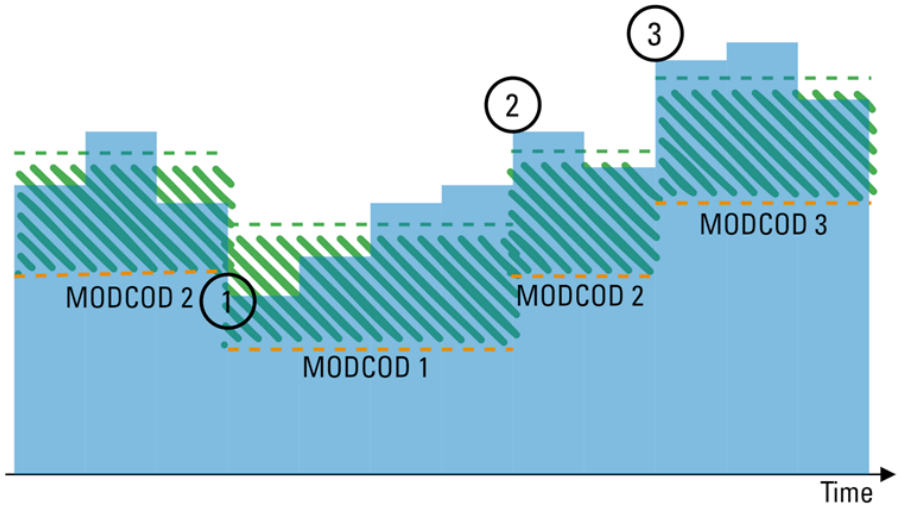


The *Target*, *Minimum*, and *Distortion Margin* can be set per MODCOD. The *Distortion Margin* should be used when there is non-linear degradation.

The *Additional ACM Margin* is an extra safety margin that can be added to the *Minimum* and *Target Margin*. It applies to all MODCODs.

At the receiver side, the measured Es/No is checked against two reference values. The ACM client at the receiver side will request a higher-order MODCOD if the link quality is better than the upper limit of the green zone in the figure above for that MODCOD. The ACM client will request a more robust MODCOD if the link quality is worse than the lower limit of the green zone for the current MODCOD.

The figure below shows an example of how ACM works. The blue bars represent the link quality.



1 At point 1, the link quality drops below the lower threshold of the currently used MODCOD2. The MODCOD changes from MODCOD2 to the more robust MODCOD1.

2 At point 2, the link quality exceeds the higher threshold of MODCOD2. The MODCOD changes from MODCOD1 to the more efficient MODCOD2.

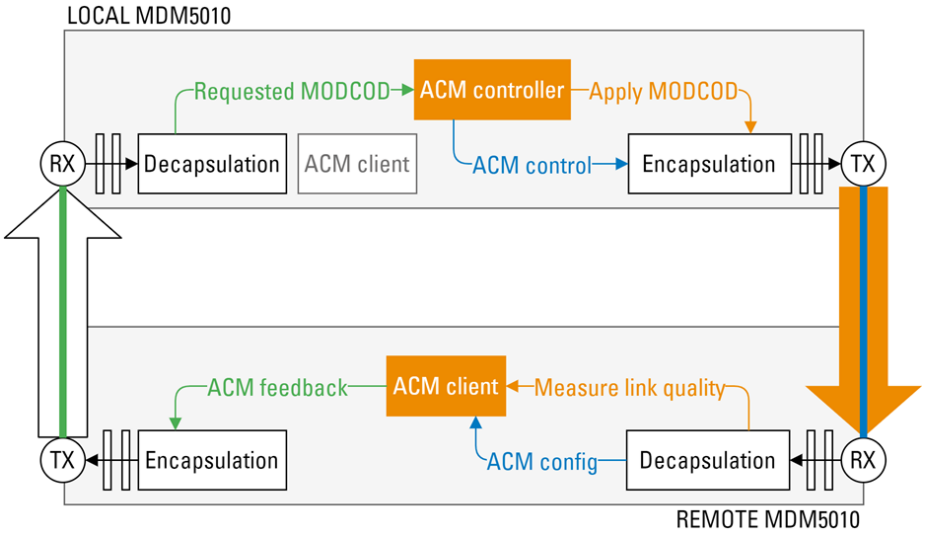
3 At point 3, the link quality exceeds the higher threshold of MODCOD3. The MODCOD changes from MODCOD2 to the more efficient MODCOD3.

ACM is handled by the ACM controller of the transmitting MDM5010 and the ACM client of the receiving MDM5010. The ACM parameters and MODCODs are configured on the ACM controller. ACM margins can be set for each MODCOD separately (manual tuning) or can be the same for all MODCODs (automatic tuning). The selectable MODCODs are limited by a minimum and maximum MODCOD, and MODCODs can be excluded from the list.

CAUTION: Limiting MODCODs or changing margins manually can reduce efficiency when not done properly. Contact ST Engineering iDirect customer support for assistance.

The ACM controller sends the MODCOD list and related margins to the ACM client. The ACM client uses this information to select the best MODCOD for the measured link quality, and returns it to the ACM controller. The ACM client can also add a margin for extra safety. The ACM controller makes sure that the MODCOD is applied. ACM signaling is exchanged in-band.

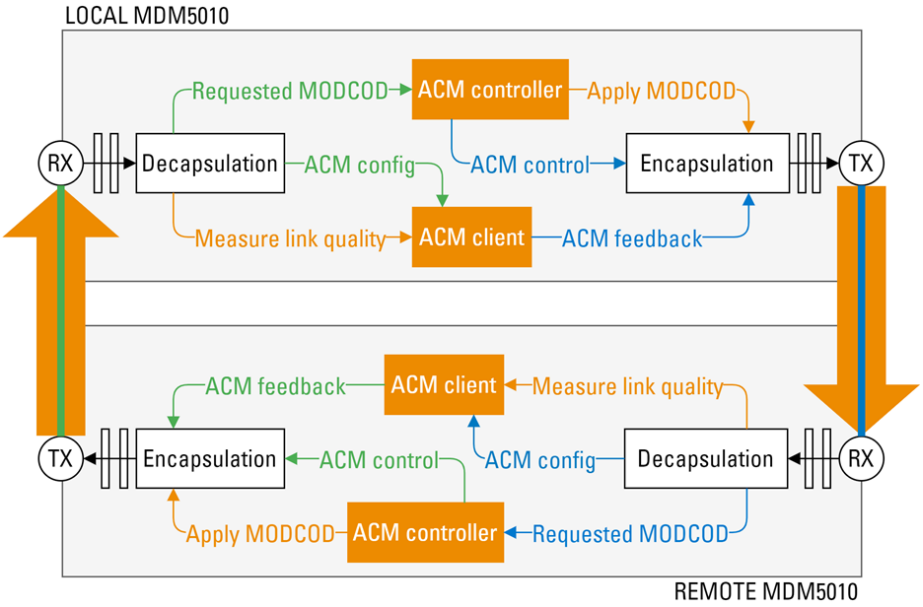
The figure below shows a simplified diagram where ACM is enabled on the local MDM5010, but not on the remote MDM5010.



The ACM controller and client of the local modem are enabled, but the ACM client is not active. The ACM controller of the remote modem is not enabled, the ACM client is enabled and provides ACM feedback to the local modem.

The MODCOD of the uplink carrier of the local MDM5010 is adapted according to the link quality measured at the remote MDM5010.

When ACM is also enabled on the remote MDM5010, ACM is applied on the uplink carrier of both the local and remote MDM5010:



C.5 The Reference Clock

The MDM5010 can internally generate a reference frequency or can be slaved to an external reference clock which is connected to the clock reference interface at the rear of the MDM5010. The reference interface is then used as an input interface. When the MDM5010 detects an external reference clock, it will automatically use this clock. Valid external reference frequency values are from 10 MHz to 100 MHz, in multiples of 10 MHz.

The internal reference clock can be used as a reference clock for any device connected to the clock reference interface at the rear of the MDM5010. The reference interface is then used as an output interface. The outgoing reference frequency is 10 MHz.

The specifications of the internal reference clock are:

Feature	Specification
Stability	~2000 ppb over 0°C to 70°C
Aging	~1000 ppb/year

The MDM5010 also enables you to slave the BUC and LNB to the reference clock of the MDM5010.

Most BUCs use phase-locked loop (PLL) local oscillators and require an external frequency reference to maintain the correct transmit frequency. The BUC can be slaved to the reference clock of the MDM5010 by multiplexing a 10 MHz or 50 MHz reference frequency on the L-band TX interface.

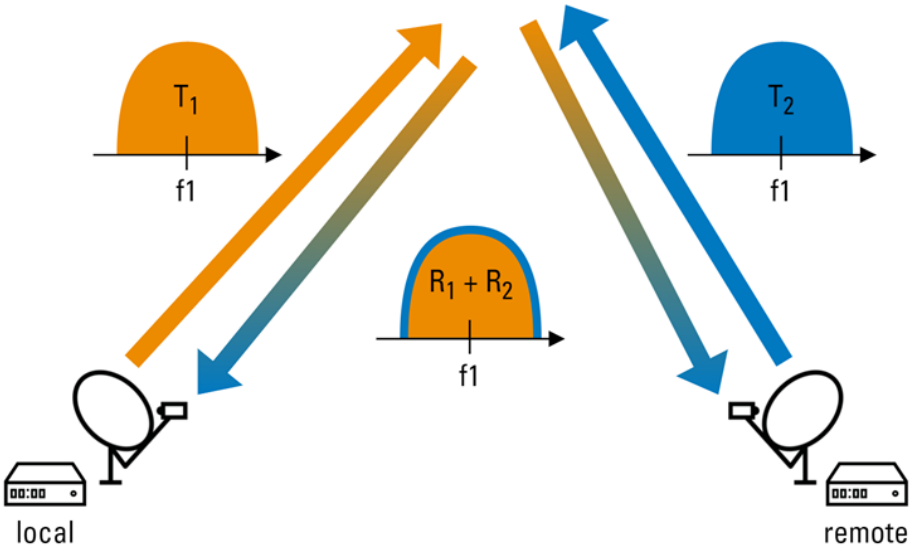
For the reception of narrow bandwidth carriers, highly stable and low phase noise LNB local oscillators are required. These use phase-locked loop local oscillators and require an external 10 MHz reference to maintain an accurate frequency. The LNB can be slaved to the reference clock of the MDM5010 by multiplexing a 10 MHz reference frequency on the L-band RX interface.

The multiplexed reference frequency can be internal or external; the MDM5010 automatically switches to the external reference clock when it detects a signal on the clock reference interface at the rear of the MDM5010.

NOTE - To have the highest stability, it is recommended to use an external reference clock.

C.6 Bandwidth Cancellation

Bandwidth cancellation (BWC) is a technology that enables the transmitted and received carrier at the MDM5010 to use the same satellite frequency band.



The MDM5010 transmits the uplink carrier (T1) and receives an aggregate carrier (R1 + R2), which is the combination of the carrier from the remote MDM5010 (T2) and the echoed uplink carrier.

NOTE - Bandwidth cancellation can only be used when both modems are in the same satellite footprint.

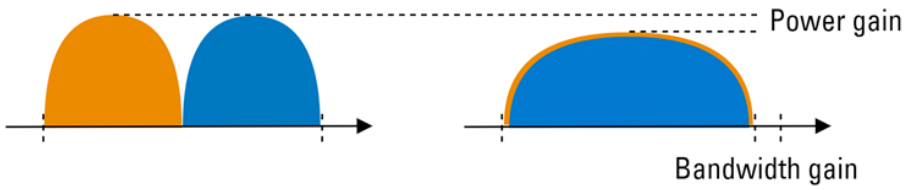
Bandwidth cancellation uses the information of the transmitted uplink carrier to extract the echoed uplink carrier from the aggregate carrier, leaving only the carrier from the remote. The echoed uplink carrier is different from the transmitted uplink carrier due to its travel over the satellite. The better the effects of this travel can be estimated, the better the echoed uplink carrier can be cancelled, and the higher the quality of the remaining carrier will be.

The first step of the BWC is to estimate the amplitude variation, frequency offset, and time delay of the echoed uplink carrier with respect to the transmitted one. It will use a configured delay and offset (with a search window), and the symbols coming from the modulator. When the BWC has an estimate, it can re-construct the echoed uplink carrier and verify if the echoed uplink carrier in the aggregate carrier can be tracked and extracted. If tracking fails, the BWC will search for new delay and offset estimates. If tracking succeeds, the BWC is locked, and cancellation is started.

The BWC functionality can be tested without a carrier from the remote. The aggregate carrier will then only contain the echoed uplink carrier.

The performance of the BWC has an influence on the link budget. An echoed uplink carrier that is poorly cancelled occurs as wideband noise for the received carrier from the remote.

When comparing a dual carrier scenario with a bandwidth cancellation scenario, the gain in bandwidth efficiency (same throughput, less bandwidth) or throughput (same bandwidth, more throughput) when using BWC can be around 30% for symmetrical carriers, or even higher when using linearized transponders.



Bandwidth cancellation provides less gain in asymmetric scenarios.

C.7 Antenna Control

The MDM5010 can be used with an antenna controller (also called antenna control unit or ACU) to point the antenna to the correct satellite. The antenna controller is connected to the MDM5010 using one of the DATA ports at the rear of the MDM5010, see MDM5010 Hardware Features

The MDM5010 communicates with the antenna controller using a TCP connection. The TCP connection is used to send antenna control parameters from the MDM5010 to the antenna controller, and to exchange control messages during the satellite acquisition process. The control messages are formatted using the OpenAMIP protocol.

OpenAMIP is an ASCII message-based protocol to exchange information between an ACU and a modem. As well as antenna control, OpenAMIP provides several status messages which allow the modem to determine the state of the antenna and the antenna to notify the modem of specific events.

The MDM5010 supports OpenAMIP v1.17.

Before any control messages can be sent, the MDM5010 (client) must establish the TCP connection using the IP address of the antenna controller (server) and the TCP port at which the antenna controller is listening.

NOTE - Make sure that the IP address of the antenna controller belongs to the same address range as the management IP address of your MDM5010.

When the TCP connection is established, the MDM5010 sends a set of OpenAMIP messages to control the antenna, such as:

Message...	Includes...
S	the satellite longitude, latitude variance, and polarity skew.
P	the polarization that the antenna should be receiving (RX) and the polarization that the antenna should be transmitting (TX).
B	the local oscillator frequency of the LNB (RX) and BUC (TX).
F	a trigger to start locating the satellite, using the information from commands S, P, and B. The ACU should reply with an "s" message including the antenna functional status and if the modem may transmit or not.

Message...	Includes...
A	the frequency at which the ACU should send the antenna status ("s" message). This value is fixed to 10 seconds. If the MDM5010 does not receive a response for three consecutive intervals, the connection reaches the connection timeout. NOTE: An additional connection timeout tolerance can be set on the MDM5010. Only when this value is exceeded after the connection timeout, the TCP connection is killed, and communication between the MDM5010 and antenna controller is broken.
W	the frequency at which the ACU should send the GPS coordinates of the antenna location ("w" message).
L	the lock status of the modem. The modem should send this message immediately when the status changes. The modem should send this message periodically at intervals specified by the ACU in the "a" message.

The antenna controller sends OpenAMIP messages, such as:

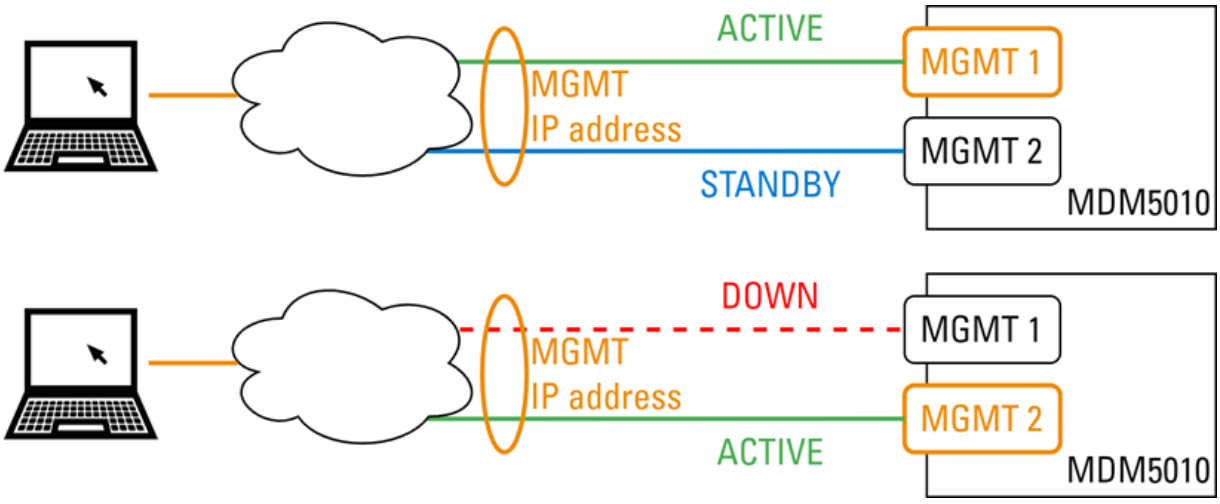
Message...	Includes...
a	the frequency at which the antenna controller expects "L" messages from the MDM5010. If the antenna controller does not receive a response for three consecutive intervals, the connection reaches the connection timeout.
s	the antenna functional status and the modem transmit mode.
w	the antenna location (longitude and latitude).

C.8 Link Redundancy

Link-level redundancy protects against loss of link connectivity; if one link fails, the other can take over and restore traffic forwarding that had been previously sent over the failed link. The redundant interfaces act as one bond interface.

The MDM5010 supports link redundancy for both the management and logical data interfaces.

The figure below shows the example of management link redundancy. If one of the management interfaces (MGMT 1 or MGMT 2) is up, accessing the MDM5010 using the IP address of the bond interface (MGMT) always works. The physical interfaces included in the bond are called slaves and do not have IP addresses.



Link redundancy is characterized by a *preferred interface* and a *protection mode*. The preferred interface is the initial interface that will be used when redundancy is activated. If this interface becomes unavailable, the other interface will be used. If the protection mode is set to revertive, the interface will switch back to the preferred interface as soon as this one is available again. If the protection mode is set to non-revertive, the interface will not switch to the preferred interface even when it is available again.

For more information about the physical interfaces, see MDM5010 Hardware Features and Data Interfaces.

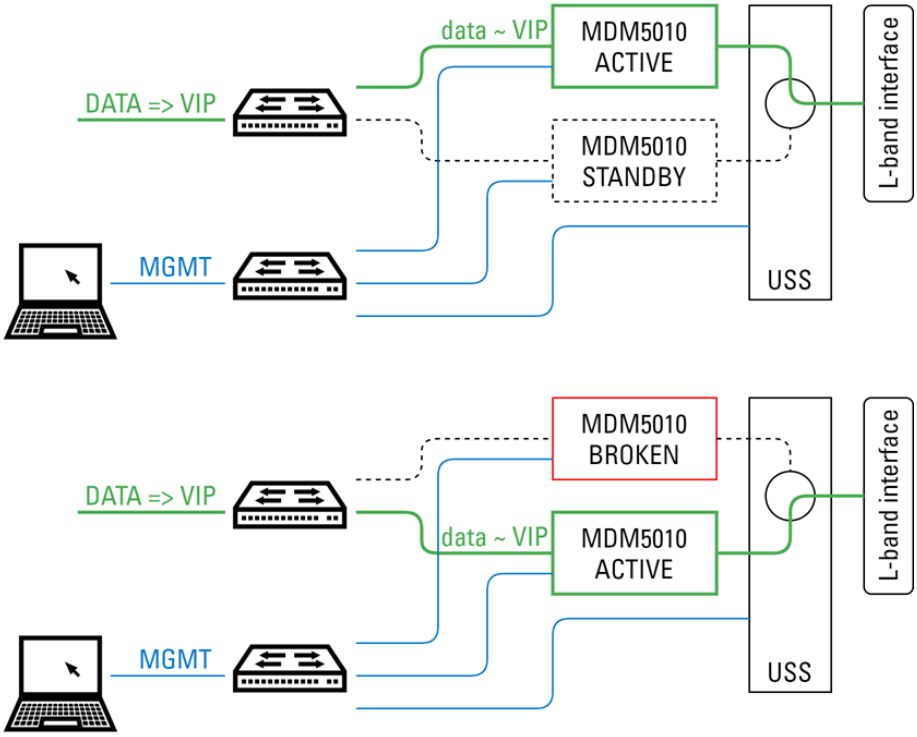
C.9 Device Redundancy

Device-level redundancy protects your setup against a failing MDM5010. Redundancy adds a backup MDM5010 and ensures that the backup device can take over the operations from a failed MDM5010.

The redundancy setup is achieved using a Universal Switching System (USS). The supported redundancy scheme is N+1, where there are N (can be 1) active MDM5010s and one standby MDM5010.

Device redundancy can use a virtual IP address for the data and management interfaces. The virtual IP address is assigned to the activated MDM5010 during the redundancy swap.

A 1+1 device redundancy with data link redundancy and the use of a virtual IP address is shown below:



The MDM5010 that is part of the redundancy setup should have an *initial state*. This is the state in which the MDM5010 is set when redundancy is enabled, or after a reset. If the redundant setup is not up and running, the MDM5010 will be in the initial state.

NOTE - When the redundant setup is up and running, the USS will make sure that all but one MDM5010 is active. Refer to the *USS User Guide* for more information about setting up device redundancy using a USS.

D MODCOD Limitations

The table below shows the limitations of the MODCODs.

MODCOD	Symbol Rate (Mbaud)			
	Frame Type: NORMAL Pilots: OFF	Frame Type: NORMAL Pilots: ON	Frame Type: SHORT Pilots: OFF	Frame Type: SHORT Pilots: ON
QPSK 1/4	220	220	220	220
QPSK 1/3	220	220	220	220
QPSK 2/5	220	220	220	220
QPSK 1/2	220	220	220	220
QPSK 3/5	220	220	220	220
QPSK 2/3	220	220	220	220
QPSK 3/4	220	220	220	220
QPSK 4/5	220	220	220	220
QPSK 5/6	220	220	220	220
QPSK 8/9	220	220	220	220
QPSK 9/10	220	220	-	-
8PSK 3/5	220	220	220	220
8PSK 2/3	220	220	220	220
8PSK 3/4	220	220	220	220
8PSK 5/6	220	220	220	220
8PSK 8/9	220	220	220	220
8PSK 9/10	220	220	-	-

MODCOD	Symbol Rate (Mbaud)			
	Frame Type: NORMAL Pilots: OFF	Frame Type: NORMAL Pilots: ON	Frame Type: SHORT Pilots: OFF	Frame Type: SHORT Pilots: ON
16APSK 2/3	220	220	220	220
16APSK 3/4	220	220	220	220
16APSK 4/5	220	220	220	220
16APSK 5/6	220	220	220	220
16APSK 8/9	220	220	220	220
16APSK 9/10	220	220	-	-
32APSK 3/4	211.67	220	209.21	213.82
32APSK 4/5	198.14	202.6	198.97	203.36
32APSK 5/6	189.91	194.19	189.68	193.86
32APSK 8/9	177.65	181.66	177.22	181.14
32APSK 9/10	175.41	179.37	-	-
QPSK 13/45	220	220	-	-
QPSK 9/20	220	220	-	-
QPSK 11/20	220	220	-	-
8APSK 5/9-L	220	220	-	-
8APSK 26/45-L	220	220	-	-
8PSK 23/36	220	220	-	-
8PSK 25/36	220	220	-	-
8PSK 13/18	220	220	-	-
16APSK 1/2-L	220	220	-	-
16APSK 8/15-L	220	220	-	-

MODCOD	Symbol Rate (Mbaud)			
	Frame Type: NORMAL Pilots: OFF	Frame Type: NORMAL Pilots: ON	Frame Type: SHORT Pilots: OFF	Frame Type: SHORT Pilots: ON
16APSK 5/9-L	220	220	-	-
16APSK 26/45	220	220	220	220
16APSK 3/5	220	220	220	220
16APSK 3/5-L	220	220	-	-
16APSK 28/45	220	220	-	-
16APSK 23/36	220	220	-	-
16APSK 2/3-L	220	220	-	-
16APSK 25/36	220	220	-	-
16APSK 13/18	220	220	-	-
16APSK 7/9	220	220	-	-
16APSK 77/90	220	220	-	-
32APSK 2/3-L	220	220	-	-
32APSK 32/45	220	220	214.72	220
32APSK 11/15	220	220	-	-
32APSK 7/9	203.93	208.52	-	-
64APSK 32/45-L	185.85	190.25	-	-
64APSK 11/15	180.08	184.34	-	-
64APSK 7/9	169.52	173.53	-	-
64APSK 4/5	164.68	168.58	-	-
64APSK 5/6	157.81	161.56	-	-
128APSK 3/4	150.69	154.25	-	-

MODCOD	Symbol Rate (Mbaud)			
	Frame Type: NORMAL Pilots: OFF	Frame Type: NORMAL Pilots: ON	Frame Type: SHORT Pilots: OFF	Frame Type: SHORT Pilots: ON
128APSK 7/9	145.14	148.58	-	-
256APSK 29/45-L	153.62	157.09	-	-
256APSK 2/3-L	148.34	151.69	-	-
256APSK 31/45-L	143.41	146.65	-	-
256APSK 32/45	138.78	141.92	-	-
256APSK 11/15-L	134.44	137.48	-	-
256APSK 3/4	131.35	134.32	-	-
QPSK 11/45	-	-	220	220
QPSK 4/15	-	-	220	220
QPSK 14/45	-	-	220	220
QPSK 7/15	-	-	220	220
QPSK 8/15	-	-	220	220
QPSK 32/45	-	-	220	220
8PSK 7/15	-	-	220	220
8PSK 8/15	-	-	220	220
8PSK 26/45	-	-	220	220
8PSK 32/45	-	-	220	220
16APSK 7/15	-	-	220	220
16APSK 8/15	-	-	220	220
16APSK 32/45	-	-	220	220
32APSK 2/3	-	-	220	220

E Classification Expressions

This chapter describes the syntax of the expressions used to classify the ingress traffic into shaping nodes. Traffic can be classified based on any field of the packet, such as VLAN tag, IP addresses, protocols, and so on.

Two or more expressions can be combined using logical operators: && (AND), || (OR), ! (NOT). Use brackets to group expressions. For stacking of identical protocol layers, a "containing" clause can be used.

- expression = expression AND expression
- expression = expression && expression
- expression = expression OR expression
- expression = expression || expression
- expression = NOT expression
- expression = !expression
- expression = (expression)
- expression = protocol containing expression
- expression = protocol
- expression = field value
- expression = protocol field value
- expression = always
- expression = never

Protocol Fields	
capture • type <capturetype> • interface <interface>	ethernet • dst ether <mac> • src ether <mac> • unicast • unicast-this-host • unicast-other-host • multicast • broadcast • this-host • protocol <ethertype> • nr-vlans <count> • vlan/vlan2/vlan3 <tag> • vlan-priority/vlan-priority2/vlan-priority3 <prio> • vlan-type/vlan-type2/vlan-type3 <ethertype> • nr-mpls <count> • mpls/mpls2/mpls3 <label> • mpls-priority/mpls-priority2/mpls-priority3 <prio> • mpls-type <ethertype>

Protocol Fields	
arp	ip4
• operation <operation> • src ether <mac> • dst ether <mac> • src host <ip4address> • src net <ip4address>-<ip4address> • src net <ip4address> mask <ip4netmask> • src net <ip4address>/<ip4bits> • dst host <ip4address> • dst net <ip4address>-<ip4address> • dst net <ip4address> mask <ip4netmask> • dst net <ip4address>/<ip4bits>	• tos <tos> • dscp <dscp> • protocol <protocol> • src host <ip4address> • src net <ip4address>-<ip4address> • src net <ip4address> mask <ip4netmask> • src net <ip4address>/<ip4bits> • dst host <ip4address> • dst net <ip4address>-<ip4address> • dst net <ip4address> mask <ip4netmask> • dst net <ip4address>/<ip4bits> • unicast • multicast • broadcast • ah • esp

Protocol Fields	
ip6 • class <tos> • dscp <dscp> • label <flowlabel> • protocol <protocol> • src host <ip6address> • src net <ip6address>-<ip6address> • src net <ip6address>/<ip6bits> • dst host <ip6address> • dst net <ip6address>-<ip6address> • dst net <ip6address>/<ip6bits> • src scope <ip6scope> • src scope <ip6scope>-<ip6scope> • dst scope <ip6scope> • dst scope <ip6scope>-<ip6scope> • unicast • multicast • ah • esp	igmp • type <igmptype> • host <ip4address> • net <ip4address>-<ip4address> • net <ip4address> mask <ip4netmask> • net <ip4address>/<ip4bits>
udp • src port <port> • src port <port>-<port> • dst port <port> • dst port <port>-<port> • rtp-detection <rtpdetect> • rtcp-detection <rtcpdetect>	udplite • src port <port> • src port <port>-<port> • dst port <port> • dst port <port>-<port> • rtp-detection <rtpdetect> • rtcp-detection <rtpdetect>

Protocol Fields	
tcp • src port <port> • src port <port>-<port> • dst port <port> • dst port <port>-<port>	dccp • src port <port> • src port <port>-<port> • dst port <port> • dst port <port>-<port>
sctp • src port <port> • src port <port>-<port> • dst port <port> • dst port <port>-<port>	icmp4 • type <icmp4type> • code <icmp4code>
icmp6 • type <icmp6type> • code <icmp6code> icmp6-neighbor-solicitation target <ip6address> icmp6-neighbor-advertisement target <ip6address>	gre • protocol <ethertype> • nr-vlans <count> • vlan/vlan2/vlan3 <tag> • vlan-priority/vlan-priority2/vlan-priority3 <prio> • vlan-type/vlan-type2/vlan-type3 <ethertype> • nr-mpls <count> • mpls/mpls2/mpls3 <label> • mpls-priority/mpls-priority2/mpls-priority3 <prio> • mpls-type <ethertype>

Input Parameter	Description
<capturetype>	Captured protocol (ethernet, ip4, ip6)
<interface>	Configured interface name
<mac>	Ethernet MAC address (XX:XX:XX:XX:XX:XX)
<ethertype>	Ethertype (arp, ip4, ip6, 0-65535, 0x0-0xFFFF)
<count>	VLAN or MPLS count (0-3)
<tag>	VLAN tag (0-4095)

Input Parameter	Description
<prio>	Priority code point (0-7)
<label>	MPLS label (0-1048575)
<operation>	ARP operation (request, reply, rrequest, rreply, 0-65535)
<ip4address>	IPv4 address (XXX.XXX.XXX.XXX)
<ip4netmask>	IPv4 netmask (XXX.XXX.XXX.XXX)
<ip4bits>	IPv4 netmask length (0-32)
<ip6address>	IPv6 address (XXXX:XXXX:...:XXXX)
<ip6bits>	IPv6 netmask length (0-128)
<ip6scope>	IPv6 address scope (0-15)
<flowlabel>	IPv6 flow label (0-1048575)
<tos>	IPv4 TOS/IPv6 traffic class byte (0-255)
<dscp>	IP differentiated services code point (0-63)
<protocol>	IP protocol (icmp, icmp4, icmp6, igmp, tcp, udp, udplite, dccp, gre, sctp, 0-255)
<icmp4type>	ICMPv4 type (echo-request, destination-unreachable, ..., 0-255)
<icmp4code>	ICMPv4 code (network-unreachable, host-unreachable, ..., 0-255)
<igmptype>	IGMP type (query, report-v1, report-v2, leave-group, report-v3, 0-255)
<icmp6type>	ICMPv6 type (echo-request, destination-unreachable, ..., 0-255)
<icmp6code>	ICMPv6 code (no-route, prohibited, ..., 0-255)
<port>	Port number (0-65535)
<rtpdetect>	Result of the heuristic RTP/RTCP detection (rejected/unknown/matched)

E.1 Classification Expression Examples

Expression that matches all incoming packets:

```
all
```

Expression that matches IPv4 packets with ToS value 17 and destination address 10.1.2.3 or 10.10.10.10:

```
tos 17 and (dst host 10.1.2.3 or dst host 10.10.10.10)
```

Expression that matches all traffic with VLAN ID set to to 620:

```
vlan 620
```

Expression that matches all packets in VLAN 620 and with a destination IPv4 address in network 192.168.5.0/24:

```
vlan 610 and ip4 dst net 192.168.5.0/24
```

Expression that matches all packets in VLAN 610 but not the ARP protocol:

```
vlan 610 and not (ethernet protocol arp)
```

Expression that matches all IPv4 packets:

```
ip4 dst net 0.0.0.0/0
```

Expression that matches a subnet:

```
ip4 dst net 10.4.1.0/24
```

F Acronyms & Abbreviations

8PSK	Eight Phase-Shift Keying - A modulation technique that transmits symbols by modulating the phase of a carrier wave. One symbol contains three bits.
16APSK	Sixteen Amplitude- and Phase-Shift Keying - A modulation technique that transmits symbols by modulating both the amplitude and phase of a carrier wave. One symbol contains four bits.
32APSK	Thirty-two Amplitude- and Phase-Shift Keying - A modulation technique that transmits symbols by modulating both the amplitude and phase of a carrier wave. One symbol contains five bits.
64APSK	Sixty-four Amplitude- and Phase-Shift Keying - A modulation technique that transmits symbols by modulating both the amplitude and phase of a carrier wave. One symbol contains six bits.
256APSK	Two hundred and fifty-six Amplitude- and Phase-Shift Keying - A modulation technique that transmits symbols by modulating both the amplitude and phase of a carrier wave. One symbol contains eight bits.
AC	Alternating Current - An electric current which periodically reverses direction and changes its magnitude continuously with time
ACM	Adaptive Coding and Modulation - A method of applying coding to a data stream in DVB-S2(X) networks in which every baseband frame can be transmitted on a different MODCOD.
ACU	Antenna Control Unit - A device to control and monitor the antenna system.
AM	Amplitude Modulation - A technique where the carrier wave is transmitted by modulating the amplitude of the carrier.
API	Application Programming Interface - A set of definitions and protocols for building and integrating application software.
APSK	Amplitude and Phase-Shift Keying - A digital modulation scheme that conveys data by modulating both the amplitude and the phase of a carrier wave.
ARP	Address Resolution Protocol - A communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address.
ASCII	American Standard Code for Information Interchange - A character encoding standard for electronic communication.

ASN.1	Abstract Syntax Notation One - A standard that defines a formalism for the specification of abstract data types.
B	Byte - Unit of digital information consisting of eight bits.
BB	Baseband - The original frequency range of a transmission signal before it is modulated.
BBF	Baseband Frame - The signal format of an input signal after mode and stream adaptation (DVB definition).
BUC	Block Up Converter - A BUC converts a band of lower frequencies to a band of higher frequencies.
BW	Bandwidth - The difference in the upper and lower frequency components present in a signal.
BWC	Bandwidth Cancellation - A technology which allows transmission of two carriers into the same leased satellite bandwidth.
CCM	Constant Coding and Modulation - A method of applying coding to a data stream in DVB-S2(X) networks in which every baseband frame is transmitted on the same MODCOD.
CID	Carrier ID - A signal embedded into a video or data transmission path to correctly identify a carrier when it is causing interference in the satellite network.
CIDR	Classless Inter-Domain Routing - A set of Internet Protocol (IP) standards that is used to create unique identifiers for networks and individual devices.
CIR	Committed Information Rate - The guaranteed or minimum data traffic rate.
CLI	Command Line Interface - A command line program that accepts text input to execute operating system functions.
COM	Communication (as in COM port).
CPU	Central Processing Unit - The core component of a computing device responsible for processing and executing instructions.
CRC	Cyclic Redundancy Check - An error-detecting code used to determine if a block of data has been corrupted.
cURL	Client URL - A command-line tool for getting or sending data including files using URL syntax.
DAC	Digital-to-Anaolg Converter - A system that converts a digital signal into an analog signal.

dB	Decibel - Unit for expressing the ratio between two physical quantities, usually amounts of acoustic or electric power, or for measuring the relative loudness of sounds.
DC	Direct Current - An electric current that is uni-directional.
DHCP	Dynamic Host Configuration Protocol - A network management protocol used on Internet Protocol networks for automatically assigning IP addresses and other communication parameters to devices connected to the network using a client–server architecture.
DVB	Digital Video Broadcasting - A set of international open standards covering all aspects of digital television from transmission through interfacing, conditional access and interactivity for digital video, audio and data.
DVB-S2X	Digital Video Broadcasting Second Generation Satellite Extensions - See https://dvb.org/.
ESD	Electrostatic Discharge - A sudden and momentary flow of electric current between two electrically charged objects caused by contact, an electrical short, or dielectric breakdown.
ETSI	European Telecommunications Standards Institute - An independent, non-profit, standardization organization in the field of information and communications.
EU	Europe.
EUI-64	64-bit Extended Unique Identifier - Extended identifier based on the organizational identifiers assigned by the IEEE Registration Authority.
FEC	Forward Error Correction - An error correction technique to detect and correct a limited number of errors in transmitted data without the need for retransmission.
FlexACM	ST Engineering iDirect's unique end-to-end solution combining a range of technologies to optimize satellite links in the most efficient way.
FPGA	Field-Programmable Gate Array - An integrated circuit designed to be configured by a customer or a designer after manufacturing
freq	Frequency.
G	Gigabit - Unit of information equal to one billion bits.
GPS	Global Positioning System - A satellite-based radionavigation system.
GSE	Generic Stream Encapsulation - Data link layer protocol defined by DVB.
GUI	Graphical User Interface - A type of user interface through which users interact with electronic devices via visual indicator representations.

HTTP	Hypertext Transfer Protocol - An application-layer protocol for transmitting hypermedia documents, such as HTML.
ID	Identifier - A name that identifies either a unique object or a unique class of objects, where the "object" or class may be an idea, physical countable object, or physical noncountable substance. The abbreviation ID often refers to identity, identification, or an identifier.
IEEE	Institute of Electrical and Electronics Engineers - Technical professional organization dedicated to advancing technology for the benefit of humanity.
IGMP	Internet Group Management Protocol - A protocol used between hosts and multicast routers on a single physical network to establish hosts' membership in particular multicast groups.
IP	Internet Protocol - The network layer communications protocol in the Internet protocol suite for relaying datagrams across network boundaries.
JSON	Javascript Object Notation - An open standard file format and data interchange format that uses human-readable text to store and transmit data objects consisting of attribute–value pairs and arrays.
LED	Light-Emitting Diode - A semiconductor light source that emits light when current flows through it.
LNB	Low-Noise Block Downconverter - A device that is used to receive a signal from a satellite, down convert the frequency and amplify the signal for further processing.
LO	Local Oscillator (as in LO frequency) - A local oscillator is an electronic oscillator used with a mixer to change the frequency of a signal.
MAC	Media Access Control (as in MAC address).
MB	Megabyte - Unit of information equal to one million bytes.
Mbaud	Megabaud - Unit of rate equal to one million baud or symbols per second.
Mbps	Megabits per second - Unit of rate equal to one million bits per second.
MGMT	Management.
MHz	Megahertz - Unit of frequency equal to one million hertz.
MIB	Management Information Base - A formatted text file that resides within the SNMP manager designed to collect information and organize it into a hierarchical format.
MODCOD	Modulation and Coding.

ms	Milliseconds - Unit of time equal to a thousandth of a second.
MTU	Maximum Transmission Unit - The size of the largest protocol data unit that can be communicated in a single network layer transaction.
NA	Not Applicable.
NIOS	Network Identity Operating System.
NTP	Network Time Protocol - A protocol designed to synchronize the clocks of computers over a network.
OpenAMIP	Open Antenna to Modem Interface Protocol - IP-based protocol that facilitates the exchange of information between an antenna controller unit and a satellite.
PDU	Protocol Data Unit - A specific block of information transferred among peer entities of a network.
PIR	Peak Information Rate - The maximum data traffic rate without any guarantees.
PL	Physical Layer - The physical layer defines the means of transmitting a stream of raw bits over a physical data link connecting network nodes. The bitstream may be grouped into code words or symbols and converted to a physical signal that is transmitted over a transmission medium.
PLL	Phase-Locked Loop - A control system that generates an output signal whose phase is related to the phase of an input signal.
PM	Phase Modulation (as in Non Linearity Indication PM) - A technique where the carrier wave is transmitted by modulating the phase of the carrier.
ppb	Parts Per Billion (related to a clock) - Unit of clock accuracy.
pps	Packets Per Second - Unit of packet rate.
QEF	Quasi-Error Free (ACM related) - A transmission is considered error-free when the packet error rate at reception is less than 10-3.
QPSK	Quadrature Phase-Shift Keying - A modulation technique that transmits symbols by modulating the phase of a carrier wave. One symbol contains two bits.
QoS	Quality of Service - The ability to differentiate diverse classes of traffic based on predefined criteria, and assign priorities based on traffic variables that affect the treatment of traffic in the network.
REST	Representational state transfer - a software architectural style that defines a set of constraints for how the architecture of an Internet-scale distributed hypermedia system, such as the Web, should behave.

RF	Radio Frequency - The oscillation rate of an alternating electric current or voltage or of a magnetic, electric or electromagnetic field or mechanical system in the frequency[1] range from around 3 kHz to around 300 GHz.
RO	Roll-off - A measure of the excess bandwidth of the filter used for pulse-shaping in digital modulation. Together with the symbol rate it defines the occupied bandwidth (BW) of the modulated carrier.
RS	Recommended Standard (as in RS-232) - A standard for serial communication transmission of data.
RX	Receive.
satcom	Satellite Communication.
SCP	Secure Copy Protocol - A means of securely transferring computer files between a local host and a remote host or between two remote hosts.
SCPC	Single Carrier Per Channel - SCPC refers to using a single signal at a given frequency and bandwidth.
SFP	Small Form-factor Pluggable (as in SFP port) - A compact, hot-pluggable network interface module used for both telecommunication and data communications applications.
SNMP	Simple Network Management Protocol - An Internet Standard protocol for collecting, controlling and exchanging management information between network devices.
SR	Symbol Rate - The number of transmitted symbols per second. A symbol may consist of one or more bits as determined by the MODCOD.
SSH	Secure Shell - A method for secure remote login from one computer to another.
STP	Spanning Tree Protocol - A network protocol that builds a loop-free logical topology for Ethernet networks.
TCP	Transmission Control Protocol - A connection-oriented transport protocol that is used on top of IP to ensure reliable transmission of packets.
TDMA	Time Division Multiple Access - An access method for shared-medium networks.
ToS	Type of Service (as in TOS field) - A field in the IPv4 header used to classify IP packets for QoS purposes.
TX	Transmit.

UDP	User Datagram Protocol - A connectionless transport protocol that is used on top of IP to transmit datagrams over a network.
URI	Uniform Resource Identifier - A unique sequence of characters that identifies a logical or physical resource used by web technologies. A URL is a sort of URI.
URL	Uniform Resource Locator - A unique identifier used to locate a resource on the Internet. It is also referred to as a web address.
US	United States.
USB	Universal Serial Bus (as in USB port) - A plug and play interface that allows a computer to communicate with peripheral and other devices.
USS	Universal Switching System - ST Engineering iDirect product designed to provide a cost effective and scalable 1+1 and N+1 protection scheme for a wide variety of equipment such as modulators, demodulators, modems and converters.
UTC	Universal Time Coordinated - The primary time standard by which the world regulates clocks and time.
VAC	Volts of Alternating Current.
VDC	Volts of Direct Current.
VIP	Virtual IP Address - An IP address that can be assigned to multiple instances at once or become a second address to the network interface.
VLAN	Virtual Local Area Network - A logical subnetwork that groups a collection of devices from different physical LANs.
VSAT	Very Small Aperture Terminal - A small-sized earth station used in the transmit/receive of data, voice and video signals over a satellite communication network, excluding broadcast television.

G Configuration Quick Reference

This chapter provides a quick reference to the resources and parameters that can be configured on the MDM5010.

NOTE - The valid values refer to the values that can be set using the REST API, or CLI. The default value, if available, is marked with *.

G.1 General Settings

Parameter	Description	GUI	REST API	CLI
Label	Unique user-friendly name for the MDM5010. Up to 50 characters.	Modem Info > Identification	Device/Identification	device identification
Auto save	Enable or disable that the application-specific configuration is saved automatically. See The MDM5010 Configuration. Valid values are: • on • off*	Modem Setup > General	Device/Configuration	device configuration
Forwarding mode	Specifies if the MDM5010 acts as a layer 2 bridge, or a layer 3 router when forwarding IP packets over satellite. Valid values are: • l2 • l3*	Shaping and QoS > Classification Rules	GseEncapsulation/Configuration OR GseDecapsulation/Configuration (both settings are linked)	gseencapsulation configuration OR gsedecapsulation configuration (both settings are linked)

Parameter	Description	GUI	REST API	CLI
Enable GSE encapsulation	Enable or disable GSE encapsulation. Valid values are: • on* • off	NA	GseEncapsulation/Configuration/ConfigurationTable/encap1	gseencapsulation configuration configurationtable encap1
Enable GSE decapsulation	Enable or disable GSE decapsulation. Valid values are: • on* • off	NA	GseDecapsulation/Configuration/ConfigurationTable/decap1	gsedecapsulation configuration configurationtable decap1
GSE output interface	Specifies through which data interface IP packets are leaving the MDM5010. Valid values are: • data1* • data2 • data bond	Shaping and QoS > Classification Rules	GseDecapsulation/Configuration/ConfigurationTable/decap1	gsedecapsulation configuration configurationtable decap1

G.2 Date and Time

Set the date and time on the MDM5010. This setting is used for time stamping the activation and clearance of alarms, and entries in the log file.

Parameter	Description	GUI	REST API	CLI
Date	dd/mm/yyyy	Modem Info > Date and Time	Device/DateTime	device datetime
Time	hh:mm:ss	Modem Info > Date and Time	Device/DateTime	device datetime
NTP	Use NTP (Network Time Protocol) to synchronize the clock with other devices in the network (NTP peers).	Modem Info > Date and Time	Device/DateTime/Ntp	device datetime ntp

G.3 Log Settings

See The Device Log.

G.3.1 Local Log Settings

Parameter	Description	GUI	REST API	CLI
Enable	Enable or disable local logging. Valid values are: • on* • off	Modem Info > Logs	Device/Log/Local	device log local

G.3.2 Remote Log Settings

Parameter	Description	GUI	REST API	CLI
Enable	Enable or disable remote logging to a syslog server. Valid values are: • on • off*	Modem Info > Logs	Device/Log/Remote	device log remote
IP address	IP address of the remote syslog server.	Modem Info > Logs	Device/Log/Remote	device log remote
UDP port	UDP port at which the syslog server is listening.	Modem Info > Logs	Device/Log/Remote	device log remote

G.3.3 Log level

Parameter	Description	GUI	REST API	CLI
Level	Define log level per facility. Valid values are: • off • trace • debug • info* • notice • warn • error • alert • emerg	Modem Info > Logs	Device/Log/Filter/[Facility]	device log filter [facility]

G.4 Management Interfaces

G.4.1 mgmt1 and mgmt2 link

Parameter	Description	GUI	REST API	CLI
Enable	Enable or disable the management interface (admin up/down). Valid values are: • on* • off	Modem Setup > Management Interfaces	Ethernet/Configuration/Management/PhysicalLinkTable/mgmt[1|2]	mgmtinterface ethernet configuration physicallink mgmt[1|2]
Auto-negotiation	Enable or disable auto-negotiation. Valid values are: • on* • off	NA	Ethernet/Configuration/Management/PhysicalLinkTable/mgmt[1|2]	mgmtinterface ethernet configuration physicallink mgmt[1|2]

Parameter	Description	GUI	REST API	CLI
Advertised speed	Advertised speed and duplex mode for auto-negotiation. Valid values are: • all* • 10BTHalfDuplex • 10BTFullDuplex • 100BTHalfDuplex • 100BTFullDuplex • 1000BTFullDuplex	NA	Ethernet/Configuration/Management/PhysicalLinkTable/mgmt[1|2]	mgmtinterface ethernet configuration physicallink mgmt[1|2]
Forced speed	Forced speed and duplex mode when auto-negotiation is off. Valid values are: • 10BTHalfDuplex • 10BTFullDuplex • 100BTHalfDuplex • 100BTFullDuplex*	NA	Ethernet/Configuration/Management/PhysicalLinkTable/mgmt[1|2]	mgmtinterface ethernet configuration physicallink mgmt[1|2]

Parameter	Description	GUI	REST API	CLI
MTU	Ethernet MTU packet size. Default is 1500 B.	Modem Setup > Management Interfaces	Ethernet/Configuration/Management/LinkTable/mgmt[1|2]	mgmtinterface ethernet configuration physicallink mgmt[1|2]

G.4.2 mgmt link

See Link Redundancy.

Parameter	Description	GUI	REST API	CLI
Enable	Enable or disable link redundancy. Valid values are: • on • off*	Modem Setup > Redundancy	Ethernet/Configuration/Management/LinkTable/mgmt	mgmtinterface ethernet configuration linkredundancy mgmt
Protection mode	Enable or disable to always use the preferred interface when available. Valid values are: • revertive • nonrevertive	Modem Setup > Redundancy	Ethernet/Configuration/Management/LinkRedundancyTable/mgmt	mgmtinterface ethernet configuration linkredundancy mgmt

Parameter	Description	GUI	REST API	CLI
Interface A	Bond interface A. Valid values are: • mgmt1 • mgmt2	Modem Setup > Redundancy	Ethernet/Configuration/Management/LinkRedundancyTable/mgmt	mgmtinterface ethernet configuration linkredundancy mgmt
Interface B	Bond interface B. Valid values are: • mgmt1 • mgmt2	Modem Setup > Redundancy	Ethernet/Configuration/Management/LinkRedundancyTable/mgmt	mgmtinterface ethernet configuration linkredundancy mgmt
Preferred interface	Preferred bond slave interface. Valid values are: • ifa • ifb	Modem Setup > Redundancy	Ethernet/Configuration/Management/LinkRedundancyTable/mgmt	mgmtinterface ethernet configuration linkredundancy mgmt
MTU	Ethernet MTU packet size. Default is 1500 B.	Modem Setup > Redundancy	Ethernet/Configuration/Management/LinkTable/mgmt	mgmtinterface ethernet configuration linkredundancy mgmt

G.4.3 IP addressing for mgmt1, mgmt2, and mgmt

Parameter	Description	GUI	REST API	CLI
IP address/prefix	IPv4 address and network prefix (CIDR notation) to access the MDM5010.	Modem Setup > Management Interfaces	Ip/Configuration/Management/IpItfTable/mgmt[|1|2]	mgmtinterface ip ipitftable mgmt[|1|2]
Virtual IP address/prefix	IPv4 address and network prefix (CIDR notation) to facilitate device redundancy, see Device Redundancy.	Modem Setup > Management Interfaces	Ip/Configuration/Management/IpItfTable/mgmt[|1|2]	mgmtinterface ip ipitftable mgmt[|1|2]

G.4.4 Management IP Routes

This is a dynamic table. Create IP forwarding routes using the parameters below. The table always includes the *Default Gateway* row. You can have up to 20 forwarding routes.

Parameter	Description	GUI	REST API	CLI
Name	Unique name, the maximum length of the name is up to 100 characters.	Modem Setup > Management Interfaces	Ip/Configuration/Management/IpRouteTable	mgmtinterface ip iproutetable

Parameter	Description	GUI	REST API	CLI
Interface	Interface to which the forwarding route applies. Valid values are: • mgmt1 • mgmt2 • mgmt • *empty**	Modem Setup > Management Interfaces	Ip/Configuration/Management/IpRouteTable	mgmtinterface ip iproutetable
Destination subnet	Destination subnet to which the forwarding route applies. The default value is 0.0.0.0/0. This field is not used for the default gateway.	Modem Setup > Management Interfaces	Ip/Configuration/Management/IpRouteTable	mgmtinterface ip iproutetable
Gateway address	Next-hop IP address. The default value is 0.0.0.0.	Modem Setup > Management Interfaces	Ip/Configuration/Management/IpRouteTable	mgmtinterface ip iproutetable

G.5 Data Interfaces

G.5.1 data1 and data2 link

NOTE - Auto-negotiation is always on.

Parameter	Description	GUI	REST API	CLI
Enable	Enable or disable the data interface. Valid values are: • on* • off	Modem Setup > Data Interfaces	Ethernet/Configuration/Data/LinkTable/data[1|2]	datainterface ethernet configuration physicallink data[1|2]
Forced speed	Forced speed and duplex mode when auto-negotiation is off.	NA	[*Not used*] Ethernet/Configuration/Data/PhysicalLinkTable/data [1|2]	NA
MTU	Ethernet MTU packet size. Default is 1500 B.	Modem Setup > Data Interfaces	Ethernet/Configuration/Data/LinkTable/data[1|2]	datainterface ethernet configuration physicallink data[1|2]

G.5.2 Data Link

See Link Redundancy.

Parameter	Description	GUI	REST API	CLI
Enable	Enable or disable link redundancy. Valid values are: • on • off*	Modem Setup > Redundancy	Ethernet/Configuration/Data/LinkTable/data	datainterface ethernet configuration linkredundancy data
Protection mode	Enable or disable to always use the preferred interface when available. Valid values are: • revertive • nonrevertive	Modem Setup > Redundancy	Ethernet/Configuration/Data/LinkRedundancyTable/data	datainterface ethernet configuration linkredundancy data
Interface A	Bond interface A. Valid values are: • data1 • data2	Modem Setup > Redundancy	Ethernet/Configuration/Data/LinkRedundancyTable/data	datainterface ethernet configuration linkredundancy data

Parameter	Description	GUI	REST API	CLI
Interface B	Bond interface B. Valid values are: • data1 • data2	Modem Setup > Redundancy	Ethernet/Configuration/Data/LinkRedundancyTable/data	datainterface ethernet configuration linkredundancy data
Preferred interface	Preferred bond slave interface. Valid values are: • ifa • ifb	Modem Setup > Redundancy	Ethernet/Configuration/Data/LinkRedundancyTable/data	datainterface ethernet configuration linkredundancy data
MTU	Ethernet MTU packet size. Default is 1500 B.	Modem Setup > Redundancy	Ethernet/Configuration/Data/LinkTable/data	datainterface ethernet configuration linkredundancy data

G.5.3 IP Addressing for data1, data2, and data

Parameter	Description	GUI	REST API	CLI
IP address/prefix	IPv4 address and network prefix (CIDR notation) to access the MDM5010.	Modem Setup > Data Interfaces	Ip/Configuration/Data/IpItfTable/data [1|2]	datainterface ip ipitftable data[1|2]
Virtual IP address/prefix	IPv4 address and network prefix (CIDR notation) to facilitate device redundancy, see Device Redundancy.	Modem Setup > Data Interfaces	Ip/Configuration/Data/IpItfTable/data [1|2]	datainterface ip ipitftable data[1|2]

G.5.4 Data IP Routes

This is a dynamic table. Create IP forwarding routes using the parameters below. The table always includes the *Default Gateway* row. You can have up to 20 forwarding routes.

Parameter	Description	GUI	REST API	CLI
Name	Unique name, the maximum length of the name is up to 100 characters.	Modem Setup > Data Interfaces	Ip/Configuration/Data/IpRouteTable	datainterface ip iproutetable
Interface	Interface to which the forwarding route applies. Valid values are: • data1 • data2 • data • *empty**	Modem Setup > Data Interfaces	Ip/Configuration/Data/IpRouteTable	datainterface ip iproutetable
Destination subnet	Destination subnet to which the forwarding route applies. The default value is 0.0.0.0/0. This field is not used for the default gateway.	Modem Setup > Data Interfaces	Ip/Configuration/Data/IpRouteTable	datainterface ip iproutetable
Gateway address	Next-hop IP address. The default value is 0.0.0.0.	Modem Setup > Data Interfaces	Ip/Configuration/Data/IpRouteTable	datainterface ip iproutetable

G.5.5 IGMP

Parameter	Description	GUI	REST API	CLI
IGMP version	Specifies the version of the IGMP protocol. Valid values are: • v2* • v3	Modem Setup > Data Interfaces	Ip/Configuration/Data/Igmp	datainterface ip igmp

G.5.6 Multicast

This is a dynamic table. Create the IP multicast streams that should be received by the MDM5010. You can create up to 20 IP multicast streams.

Parameter	Description	GUI	REST API	CLI
Name	Unique name, the maximum length of the name is up to 100 characters.	Modem Setup > Data Interfaces	Ip/Configuration/Data/MulticastItfTable	datainterface ip multicastitftable

Parameter	Description	GUI	REST API	CLI
Interface	Interface that receives the multicast stream. Valid values are: • data1 • data2 • *empty**	Modem Setup > Data Interfaces	Ip/Configuration/Data/MulticastItfTable	datainterface ip multicastitftable
IP multicast address	Valid IP multicast addresses are in the range 224.0.0.0 through 239.255.255.255. The default value is 224.1.0.1.	Modem Setup > Data Interfaces	Ip/Configuration/Data/MulticastItfTable	datainterface ip multicastitftable
Source A IP address	Source IP address of the multicast stream. This field is only available when the IGMP version is set to v3. The default value is 0.0.0.0.	Modem Setup > Data Interfaces	Ip/Configuration/Data/MulticastItfTable	datainterface ip multicastitftable
Source B IP address	Second source IP address of the multicast stream. This field is only available when the IGMP version is set to v3. The default value is 0.0.0.0.	Modem Setup > Data Interfaces	Ip/Configuration/Data/MulticastItfTable	datainterface ip multicastitftable

G.6 Device Redundancy

See Device Redundancy.

Parameter	Description	GUI	REST API	CLI
Enable	Specifies if the MDM5010 is part of a redundant setup or not. Valid values are: • on • off*	Modem Setup > Redundancy	DeviceRedundancy	deviceredundancy
Initial state	State in which the MDM5010 is set when redundancy is enabled. If the redundant setup is not up and running, the MDM5010 will be in the initial state. When the initial state is standby, the MDM5010 will not transmit or receive data. Valid values are: • active • standby* When the redundant setup is up and running, the USS will make sure that all but one MDM5010 is active.	Modem Setup > Redundancy	DeviceRedundancy	deviceredundancy

G.7 Reference Clock

See The Reference Clock.

Parameter	Description	GUI	REST API	CLI
Mode	Specifies if the clock reference interface at the rear of MDM5010 is used as an input or output interface. Valid values are: • input* • output	Modem Setup > General	ReferenceClock	refclock configuration

G.8 Transmit Control

Control the transmission of the uplink carrier.

Parameter	Description	GUI	REST API	CLI
General device alarm	Enable or disable transmitting the uplink carrier when a general device alarm occurs. Valid values are: • disabletransmit* • noimpact	Transmit > Transmit Control	Modulators/Configuration/TransmitCtrl	modulators configuration transmitctrl
General interface alarm	Enable or disable transmitting the uplink carrier when a general interface alarm occurs. Valid values are: • disabletransmit • noimpact*	Transmit > Transmit Control	Modulators/Configuration/TransmitCtrl	modulators configuration transmitctrl

Parameter	Description	GUI	REST API	CLI
Demod out of lock	Enable or disable transmitting the uplink carrier when the demodulator is out of lock. Valid values are: • disabletransmit • noimpact*	Transmit > Transmit Control	DemodOutOfLockMutesMod/Configuration/ConfigurationTable/1	demodoutoflockmutesmod configuration configurationtable 1
Allow changes when TX is on	Enable or disable changing the uplink carrier setting when transmitting. Valid values are: • on • off*	Transmit > Transmit Control	Modulators/Configuration/TransmitCtrl	modulators configuration transmitctrl

G.9 Transmit Carrier

See Coding and Modulation.

Parameter	Description	GUI	REST API	CLI
Transmit	Enable or disable transmitting the uplink carrier. Valid values are: • on • off*	Transmit > Carrier	Modulators/Configuration/ConfigurationTable/mod1	modulators configuration configurationtable mod1
Output level	Carrier signal level at TX interface. Valid values are from -25 to +7 (dBm). The default value is -15 dBm.	Transmit > Carrier	Modulators/Configuration/ConfigurationTable/mod1	modulators configuration configurationtable mod1
Carrier modulation	Specifies if the carrier is modulated or not. Valid values are: • on* (modulated carrier) • purecarrier (non-modulated continuous wave)	Transmit > Carrier	Modulators/Configuration/ConfigurationTable/mod1	modulators configuration configurationtable mod1

Parameter	Description	GUI	REST API	CLI
Symbol rate	Number of transmitted symbols per second. Valid values are from 1 Mbaud to 220 Mbaud. The default value is 10 Mbaud. NOTE: Not all MODCODs can operate at the highest symbol rate. To know the limitations, see MODCOD Limitations.	Transmit > Carrier	Modulators/Configuration/ConfigurationTable/mod1 Unit: baud	modulators configuration configurationtable mod1 Unit: Mbaud
Roll-off	Indication of the roll-off factor (α). Together with the symbol rate it defines the occupied bandwidth (BW) of the modulated carrier: `BW = (1+α)SR`; when roll-off = 5%, then α = 0.05. Valid values are: • rolloff2 • rolloff5 • rolloff10 • rolloff15 • rolloff20* • rolloff25 • rolloff35	Transmit > Carrier	Modulators/Configuration/ConfigurationTable/mod1	modulators configuration configurationtable mod1

Parameter	Description	GUI	REST API	CLI
Output frequency	L-band center frequency. Valid values are from 950 MHz to 2450 MHz. The default value is 1450 MHz.	Transmit > Carrier	Modulators/Configuration/ConfigurationTable/mod1 Unit: Hz	modulators configuration configurationtable mod1 Unit: MHz

Parameter	Description	GUI	REST API	CLI
MODCOD	Modulation and coding scheme used to transmit the digital information over the satellite link. The default value is QPSK 3/4 (qpsk34). Valid values are: qpsk14 qpsk13 qpsk25 qpsk12 qpsk35 qpsk23 qpsk34 qpsk45 qpsk56 qpsk89 qpsk910 8psk35 8psk23 8psk34 8psk56 8psk89 8psk910 16apsk23 16apsk34 16apsk45 16apsk56 16apsk89 16apsk910 32apsk34 32apsk45 32apsk56 32apsk89 32apsk910 qpsk1345 qpsk920 qpsk1120 8apsk59l 8apsk2645l 16apsk12l 16apsk815l 16apsk59l 16apsk2645 16apsk35l 16apsk2845 16apsk2336 16apsk23l 16apsk2536 16apsk1318 16apsk79 32apsk23l 32apsk3245 32apsk1115 32apsk79 64apsk3245l 64apsk1115 64apsk79 64apsk45 64apsk56 256apsk2945l 256apsk23l 256apsk3145l 256apsk3245 256apsk1115l 256apsk34 NOTE: The possible MODCODs depend on the Frame Type and the presence of Pilots, see MODCOD Limitations.	Transmit > Carrier	Modulators/Configuration/Dvbs2ConfigurationTable/mod1	modulators configuration dvbs2configurationtable mod1

Parameter	Description	GUI	REST API	CLI
Frame type	Size of a single FEC frame. Valid values are: • normal* • short	Transmit > Carrier	Modulators/Configuration/Dvbs2ConfigurationTable/mod1	modulators configuration dvbs2configurationtable mod1
Pilots	Use pilots to increase the reliability of the receiver synchronization. Valid values are: • on • off*	Transmit > Carrier	Modulators/Configuration/Dvbs2ConfigurationTable/mod1	modulators configuration dvbs2configurationtable mod1
PL scrambler signature	Used by the modulator to randomize the PLFRAMEs (excluding PLHEADER) for energy dispersal. Valid values are from 0 to 262141. The default value is 0.	Transmit > Carrier	Modulators/Configuration/Dvbs2ConfigurationTable/mod1	modulators configuration dvbs2configurationtable mod1

Parameter	Description	GUI	REST API	CLI
Spectrum inversion or polarity	Specifies if the MDM5010 should invert the spectrum or not. Valid values are: • directspectrum* • invertedspectrum	Transmit > Carrier	Modulators/Configuration/ConfigurationTable/mod1	modulators configuration configurationtable mod1
Amplitude slope equalizer	Used to compensate for gain loss at higher frequencies due to RF amplifiers, RF cables, and passive components. The equalizer has a maximum range of ± 8 dB / 500 MHz. Valid values are from -15 to 15. The default value is 0.	Transmit > Carrier	Modulators/Configuration/ConnectorsConfigurationTable/con1	modulators configuration connectorsconfigurationtable con1

G.10 BUC

Parameter	Description	GUI	REST API	CLI
BUC clock reference	Specifies if a reference frequency should be sent on the same feed line as the uplink carrier. Valid values are: • off* • 10MHz • 50MHz For more information, see The Reference Clock.	Transmit > BUC	Modulators/Configuration/ConnectorsConfigurationTable/con1	modulators configuration connectorsconfigurationtable con1
[*optional*] BUC power signal	Specifies if a power signal should be sent to the BUC on the same feed line as the uplink carrier. Valid voltage values are: • 24V • 48V The output voltage depends on the DC BUC power supply option that has been ordered.	Transmit > BUC	Modulators/Configuration/DcBucConfigurationTable/con1	modulators configuration dcbucconfigurationtable con1

G.11 Receive Carrier

Parameter	Description	GUI	REST API	CLI
Enable	Enable or disable the demodulator function.	Receive > Carrier	Demodulators/Configuration/ConfigurationTable/demod1	demodulators configuration configurationtable demod1
Symbol rate	Number of transmitted symbols per second. Valid values are from 1 Mbaud to 220 Mbaud. The default value is 10 Mbaud.	Receive > Carrier	Demodulators/Configuration/ConfigurationTable/demod1 Unit: baud	demodulators configuration configurationtable demod1 Unit: Mbaud
Input frequency	L-band center frequency. Valid values are from 950 MHz to 2150 MHz. The default value is 2000 MHz.	Receive > Carrier	Demodulators/Configuration/ConfigurationTable/demod1 Unit: Hz	demodulators configuration configurationtable demod1 Unit: MHz

Parameter	Description	GUI	REST API	CLI
Roll-off	Indication of the roll-off factor (α). Together with the symbol rate it defines the occupied bandwidth (BW) of the modulated carrier: `BW = (1+α)SR`; when roll-off = 5%, then α = 0.05 Valid values are: • rolloff2 • rolloff5 • rolloff10 • rolloff15 • rolloff20* • rolloff25 • rolloff35	Receive > Carrier	Demodulators/Configuration/ConfigurationTable/demod1	demodulators configuration configurationtable demod1
Spectrum inversion or polarity	Specifies if the MDM5010 should invert the spectrum or not. Valid values are: • direct • inverted • automatic*	Receive > Carrier	Demodulators/Configuration/ConfigurationTable/demod1	demodulators configuration configurationtable demod1

Parameter	Description	GUI	REST API	CLI
Acquisition range	Window that the MDM5010 uses to look for the downlink carrier. The input frequency is the center frequency of this range. Valid values are from 0.05 MHz to 7.5 MHz. The default value is 1 MHz. It is recommended to set the value to 1.5 x the symbol rate when the symbol rate is lower than 3.33 Mbaud. For higher symbol rates, the acquisition range should be set to 0.3 x symbol rate with a maximum of 7.5 MHz.	Receive > Carrier	Demodulators/Configuration/ConfigurationTable/demod1 Unit: Hz	demodulators configuration configurationtable demod1 Unit: MHz
PL scrambler signature	Used by the modulator to randomize the PLFRAMEs (excluding PLHEADER) for energy dispersal. The same number must be known by the receiver so that demodulation is possible. Valid values are from 0 to 262141. The default value is 0.	Receive > Carrier	Demodulators/Configuration/Dvbs2ConfigurationTable/demod1	demodulators configuration dvbs2configurationtable demod1

G.12 Backup Carrier

See Migrating a Carrier.

NOTE - The backup carrier cannot be used when bandwidth cancellation is enabled.

Parameter	Description	GUI	REST API	CLI
Enable	Enable or disable the backup carrier. Valid values are: • on • off*	Receive > Backup Carrier	Demodulators/Configuration/BackupCarrierConfigTable/demod1	demodulators configuration backupcarrierconfigtable demod1
Input frequency	L-band center frequency. Valid values are from 950 MHz to 2150 MHz. The default value is 2000 MHz.	Receive > Backup Carrier	Demodulators/Configuration/BackupCarrierConfigTable/demod1 Unit: Hz	demodulators configuration backupcarrierconfigtable demod1 Unit: MHz

Parameter	Description	GUI	REST API	CLI
Symbol rate	Number of transmitted symbols per second. Valid values are from 1 Mbaud to 220 Mbaud. The default value is 10 Mbaud.	Receive > Backup Carrier	Demodulators/Configuration/BackupCarrierConfigTable/demod1 Unit: baud	demodulators configuration backupcarrierconfigtable demod1 Unit: Mbaud
Switch timeout	Time that needs to pass when the primary carrier is lost before switching to the backup carrier. Valid values are from 1 second to 1000 Seconds. The default value is 60 seconds.	Receive > Backup Carrier	Demodulators/Configuration/BackupCarrierConfigTable/demod1	demodulators configuration backupcarrierconfigtable demod1

G.13 LNB

Parameter	Description	GUI	REST API	CLI
LNB power supply	Specifies if a power signal should be sent on the same feed line as the downlink carrier. Valid values are: • none* • 13V/0kHz • 13V/22kHz • 18V/0kHz • 18V/22kHz	Receive > LNB	Demodulators/Configuration/ConnectorGroupsConfigurationTable/connectorgroup1	demodulators configuration connectorgroupsconfigurationtable connectorgroup1

Parameter	Description	GUI	REST API	CLI
10 MHz LNB reference	Specifies if a reference frequency should be sent on the same feed line as the downlink carrier. Valid values are: • off* • on For more information, see The Reference Clock.	Receive > LNB	Demodulators/Configuration/ConnectorGroupsReferenceConfigurationTable/connectorgroup1	demodulators configuration connectorgroupsreferenceconfigurationtable connectorgroup1

G.14 Bandwidth Cancellation

See Bandwidth Cancellation.

NOTE - Bandwidth cancellation cannot be used when the backup carrier is enabled.

Parameter	Description	GUI	REST API	CLI
Enable	Enable or disable bandwidth cancellation. Valid values are: • on • off*	Bandwidth Cancellation	BandwidthCancellation/Configuration/ConfigurationTable/BWC-1	bandwidthcancellation configuration configurationtable bwc-1
Expected round-trip delay	Expected delay that the uplink carrier will experience when traveling from the MDM5010 to the satellite and back. Valid values are from 0 ms to 500 ms. The default value is 250 ms.	Bandwidth Cancellation	BandwidthCancellation/Configuration/ConfigurationTable/BWC-1 Unit: ms	bandwidthcancellation configuration configurationtable bwc-1 Unit: ms

Parameter	Description	GUI	REST API	CLI
Round-trip delay search window	Echoed uplink carrier round-trip delay uncertainty. Valid values are from 1 ms to 100 ms. The default value is 20 ms.	Bandwidth Cancellation	BandwidthCancellation/Configuration/ConfigurationTable/BWC-1 Unit: ms	bandwidthcancellation configuration configurationtable bwc-1 Unit: ms
Local carrier receive frequency offset	Offset of the echoed uplink carrier from the received carrier. Valid values are from -100 MHz to 100 MHz. The default value is 0 MHz.	Bandwidth Cancellation	BandwidthCancellation/Configuration/ConfigurationTable/BWC-1 Unit: Hz	bandwidthcancellation configuration configurationtable bwc-1 Unit: MHz
Local carrier receive frequency search window	Echoed uplink carrier frequency uncertainty. Valid values are form 0.05 MHz to 7.5 MHz. The default value is 0.05 MHz.	Bandwidth Cancellation	BandwidthCancellation/Configuration/ConfigurationTable/BWC-1 Unit: Hz	bandwidthcancellation configuration configurationtable bwc-1 Unit: MHz
Local carrier spectrum inversion	Specifies if the BWC needs to invert the spectrum or not. Valid values are: • direct • inverted • automatic*	Bandwidth Cancellation	BandwidthCancellation/Configuration/ConfigurationTable/BWC-1	bandwidthcancellation configuration configurationtable bwc-1

Parameter	Description	GUI	REST API	CLI
Bandwidth mode	Fine-tune BWC performance. Valid values are: • normal* (in most cases) • robust (low symbol rates, or a lot of phase noise) • fine (high symbol rates, or local/remote imbalance ratio)	Bandwidth Cancellation	BandwidthCancellation/Configuration/ConfigurationTable/BWC-1	bandwidthcancellation configuration configurationtable bwc-1
Dummy PL scrambler mode	Specifies how dummy PL frames should be scrambled. Valid values are: • dvbs2standard* (reinitialize the randomization sequence at the end of each PL frame header) • continuous (do not reinitialize the randomization sequence; dummy PL frames will be more random making it easier for the BWC to measure the delay between the transmitted and echoed carrier)	Bandwidth Cancellation	Modulators/Configuration/Dvbs2ConfigurationTable/mod1	modulators configuration dvbs2configurationtable mod1

G.15 Antenna Control

See Antenna Control.

Parameter	Description	GUI	REST API	CLI
Enable	Enable or disable antenna control. Valid values are: • on • off*	Antenna Controller	AntennaController/Configuration/ConfigurationTable/control_1	antennacontroller configuration configurationtable control_1
IP address	IP address of the antenna controller.	Antenna Controller	AntennaController/Configuration/ConfigurationTable/control_1	antennacontroller configuration configurationtable control_1
Port	TCP port at which the antenna controller is listening for control messages. Valid values are from 1 to 65535. The default value is 12345.	Antenna Controller	AntennaController/Configuration/ConfigurationTable/control_1	antennacontroller configuration configurationtable control_1

Parameter	Description	GUI	REST API	CLI
Connection timeout tolerance	Specifies how long the connection between the MDM5010 and antenna controller should remain active when the TCP connection has reached the connection timeout. Valid values are from 0 seconds to 120 seconds. The default value is 5 seconds.	Antenna Controller	NA	antennacontroller configuration configurationtable control_1 Unit: seconds
Satellite longitude	Longitude of the satellite. Valid values are from -180 to +180 (degrees East). The default value is 0 degrees.	Antenna Controller	AntennaController/Configuration/ConfigurationTable/control_1	antennacontroller configuration configurationtable control_1
Satellite latitude variance	Maximum drift from the latitude of the satellite. Valid values are from -90 to +90 (degrees North). The default value is 1 degree.	Antenna Controller	AntennaController/Configuration/ConfigurationTable/control_1	antennacontroller configuration configurationtable control_1
Satellite polarity skew	Angle at which the satellite's polarization planes are inclined with respect to the equatorial plane. Valid values are from -10 to +10 degrees. The default value is 0 degrees.	Antenna Controller	AntennaController/Configuration/ConfigurationTable/control_1	antennacontroller configuration configurationtable control_1

Parameter	Description	GUI	REST API	CLI
RX polarization	Polarization that the antenna is receiving. Valid values are: • lefthanded* • righthanded • horizontal • vertical	Antenna Controller	AntennaController/Configuration/ConfigurationTable/control_1	antennacontroller configuration configurationtable control_1
TX polarization	Polarization that the antenna is transmitting. Valid values are: • lefthanded* • righthanded • horizontal • vertical	Antenna Controller	AntennaController/Configuration/ConfigurationTable/control_1	antennacontroller configuration configurationtable control_1
RX LO conversion frequency	Local oscillator frequency of the LNB. Valid values are from 0 GHz to 42 GHz. The default value is 0 GHz.	Antenna Controller	AntennaController/Configuration/ConfigurationTable/control_1	antennacontroller configuration configurationtable control_1

Parameter	Description	GUI	REST API	CLI
TX LO conversion frequency	Local oscillator frequency of the BUC. Valid values are from 0 GHz to 42 GHz. The default value is 0 GHz.	Antenna Controller	AntennaController/Configuration/ConfigurationTable/control_1 Unit: kHz	antennacontroller configuration configurationtable control_1 Unit: kHz
Short axis maximum skew	Specifies the maximum allowed skew of the beam short axis to the geosynchronous arc; used for antennas with a non-circular radiation pattern. Valid values are from 0 to 90 degrees. The default value is 90 degrees.	Antenna Controller	AntennaController/Configuration/ConfigurationTable/control_1	antennacontroller configuration configurationtable control_1

G.16 Classification Rules and Nodes

See Quality of Service.

This is a dynamic table. Create nodes using the parameters below. You can create up to 40 nodes.

Parameter	Description	GUI	REST API	CLI
Enable	Enable or disable the node. Valid values are: • on • off*	Shaping and QoS > Classification Rules	GseEncapsulation/Configuration/NodesTable	gseencapsulation configuration nodestable
Name	Name of the node; must be unique and only include alphanumeric characters, dash (-), underscore (_), and the at symbol (@); it must not include any spaces. Up to 30 characters.	Shaping and QoS > Classification Rules	GseEncapsulation/Configuration/NodesTable	gseencapsulation configuration nodestable
CIR	Guaranteed or minimum data traffic rate. Valid values are from 0 Mbps to 1000 Mbps. The default value is 0 Mbps.	Shaping and QoS > Classification Rules	GseEncapsulation/Configuration/NodesTable Unit: bps	gseencapsulation configuration nodestable Unit: Mbps

Parameter	Description	GUI	REST API	CLI
PIR	Maximum data traffic rate. Packets that exceed this rate will be queued, and possibly dropped. Valid values are from 0 Mbps to 1000 Mbps. The default value is 10 Mbps.	Shaping and QoS > Classification Rules	GseEncapsulation/Configuration/NodesTable Unit: bps	gseencapsulation configuration nodestable Unit: Mbps
Priority	Specifies if traffic should be treated with higher priority over other traffic. The lower the value, the higher the priority. Valid values are from 0 to 99. The default value is 50.	Shaping and QoS > Classification Rules	GseEncapsulation/Configuration/NodesTable	gseencapsulation configuration nodestable
Maximum queue timeout	Specifies the maximum time a packet can stay in the queue before being dropped. Valid values are from 0 to 2000 ms. The default value is 100 ms.	Shaping and QoS > Classification Rules	GseEncapsulation/Configuration/NodesTable Unit: ms	gseencapsulation configuration nodestable Unit: ms
Classification expression	Expression to match the node, see Classification Expressions.	Shaping and QoS > Classification Rules	GseEncapsulation/Configuration/NodesTable	gseencapsulation configuration nodestable
Matching order	Specifies the order in which the classification rules must be applied to incoming traffic. The rule with the lowest matching order value is tried first. Valid values are from 1 to 99. The default value is 50.	Shaping and QoS > Classification Rules	GseEncapsulation/Configuration/NodesTable	gseencapsulation configuration nodestable

G.17 Encapsulation Delay Control

See GSE Encapsulation and Baseband Frames.

Parameter	Description	GUI	REST API	CLI
Delay control mode	Use pre-defined modes, or manual mode. Valid values are: • optimizedacm* (filling of the baseband frames with GSE packets is optimized) • optimizedjitter (baseband frames are transmitted at a steady pace regardless of their filling rate) • manual (set encapsulation interval and packet time manually)	Shaping and QoS > Delay Control	GseEncapsulation/Configuration/DelayControlTable/encap1	gseencapsulation configuration delaycontroltable encap1
Encapsulation interval	Interval at which the baseband frames are forwarded from the encapsulator to the FEC encoder. This field is only available when delay control mode is set to manual. Valid values are from 1 ms to 1000 ms.	Shaping and QoS > Delay Control	GseEncapsulation/Configuration/DelayControlTable/encap1 Unit: ms	gseencapsulation configuration delaycontroltable encap1 Unit: ms
Packing time	Maximum time to fill a baseband frame with GSE packets. This field is only available when delay control mode is set to manual. Valid values are from 1 ms to 1000 ms.	Shaping and QoS > Delay Control	GseEncapsulation/Configuration/DelayControlTable/encap1 Unit: ms	gseencapsulation configuration delaycontroltable encap1 Unit: ms

G.18 VLAN Re-tagging

Change the VLAN tag of traffic that leaves the MDM5010.

CAUTION: Only the 802.1Q VLAN ID field of the Ethernet (layer 2) packet is changed. The VLAN IDs of protocols on top of 802.1Q, such as PVST+, are not changed. This could result in conflicting VLAN information inside an Ethernet packet and in traffic being blocked (VLAN is pruned from the trunk interface of the port connected to the MDM5010. For more information, see Traffic Issue when Changing the VLAN ID.

This is a dynamic table. Create VLAN translation rules using the parameters below. You can create up to 40 translation rules.

Parameter	Description	GUI	REST API	CLI
Name	Name of the rule; must be unique and only include alphanumeric characters, dash (-), underscore (_), and the at symbol (@); it must not include any spaces. Up to 29 characters.	Shaping and QoS > VLAN Re-Tagging	GseDecapsulation/Configuration/VlanRetaggingTable	gsedecapsulation configuration vlanretaggingtable
From	Packets with this VLAN tag will be translated to the value in the To field at the egress point of the MDM5010. Valid values are from 0 to 4095. The default value is 0.	Shaping and QoS > VLAN Re-Tagging	GseDecapsulation/Configuration/VlanRetaggingTable	gsedecapsulation configuration vlanretaggingtable

Parameter	Description	GUI	REST API	CLI
To	Packets with a VLAN tag equal to the value in the From field will be translated to this value at the egress point of the MDM5010. Valid values are from 0 to 4095. The default value is 0.	Shaping and QoS > VLAN Re-Tagging	GseDecapsulation/Configuration/VlanRetaggingTable	gsedecapsulation configuration vlanretaggingtable

G.19 Remote Management

Access remote MDM5010 over satellite.

Parameter	Description	GUI	REST API	CLI
Enable	Enable or disable remote management. Valid values are: • on • off*	Modem Setup > Remote Management	RemoteManagement/Configuration/ConfigurationTable/remote1	remotemanagement configuration configurationtable remote1
IP address/prefix	Remote network or host address to manage. If layer 2 mode is enabled (see Defining the Classification Rules and Nodes), make sure that the remote management IP addresses and the IP addresses of the management interfaces do not overlap. To avoid overlap, it is recommended to use a single host address (/32 prefix) for remote management.	Modem Setup > Remote Management	RemoteManagement/Configuration/ConfigurationTable/remote1	remotemanagement configuration configurationtable remote1

Parameter	Description	GUI	REST API	CLI
Bandwidth	Maximum rate allowed for remote management traffic. The remote management traffic capacity is taken from the user traffic capacity. When there is no remote management traffic, all capacity is available for the user traffic.	Modem Setup > Remote Management	RemoteManagement/Configuration/ConfigurationTable/remote1	remotemanagement configuration configurationtable remote1

G.20 ACM

See Adaptive Coding and Modulation.

Parameter	Description	GUI	REST API	CLI
Enable	Enable or disable the ACM controller. Valid values are: • on • off*	ACM > Setup	AcmControllers/Configuration/ConfigurationTable/controller1	acmcontrollers configuration configurationtable controller1

Parameter	Description	GUI	REST API	CLI
ACM signaling MODCOD	Specifies the MODCOD to use for ACM signaling. The default value is QPSK 3/4 (qpsk34). Valid values are: unspecified qpsk14 qpsk13 qpsk25 qpsk12 qpsk35 qpsk23 qpsk34 qpsk45 qpsk56 qpsk89 qpsk910 8psk35 8psk23 8psk34 8psk56 8psk89 8psk910 16apsk23 16apsk34 16apsk45 16apsk56 16apsk89 16apsk910 32apsk34 32apsk45 32apsk56 32apsk89 32apsk910 qpsk1345 qpsk920 qpsk1120 8apsk59l 8apsk2645l 16apsk12l 16apsk815l 16apsk59l 16apsk2645 16apsk35 16apsk35l 16apsk2845 16apsk2336 16apsk23l 16apsk2536 16apsk1318 16apsk79 32apsk23l 32apsk3245 32apsk1115	ACM > Setup	AcmControllers/Configuration/SignallingConfigurationTable/controller1	acmcontrollers configuration signallingconfigurationtable controller1

Parameter	Description	GUI	REST API	CLI
	32apsk79 64apsk3245l 64apsk1115 64apsk79 64apsk45 64apsk56 256apsk2945l 256apsk23l 256apsk3145l 256apsk3245 256apsk1115l 256apsk34 qpsk1145 qpsk415 qpsk1445 qpsk715 qpsk815 qpsk3245 8psk715 8psk815 8psk2645 8psk3245 16apsk715 16apsk815 16apsk3245 32apsk23 qpsk29 bpsk15 bpsk1145 bpsk13 bpsks15 bpsks1145 bpsk415			
MODCOD selection algorithm	Link characteristic used for selecting the MODCOD. Valid values are: • headeresno • linkmargin • cond*	ACM > Tuning	AcmControllers/Configuration/ConfigurationTable/controller1	acmcontrollers configuration configurationtable controller1

Parameter	Description	GUI	REST API	CLI
MODCOD tuning	Set the ACM margins per MODCOD manually or use the same ACM margins for all MODCODs. Valid values are: • auto* • manual	ACM > Tuning	AcmControllers/Configuration/ConfigurationTable/controller1	acmcontrollers configuration configurationtable controller1
Minimum margin	Margin on top of the minimum signal quality required to keep using the MODCOD. Used when MODCOD tuning is set to auto. Valid values are from -10 dB to +30 dB. The default value is 0 dB.	ACM > Tuning	AcmControllers/Configuration/ConfigurationTable/controller1	acmcontrollers configuration configurationtable controller1

Parameter	Description	GUI	REST API	CLI
Target margin	Margin on top of the minimum signal quality required for using the MODCOD. Used when MODCOD tuning is set to auto. Valid values are from -10 dB to +30 dB. The default value is 0.3 dB.	ACM > Tuning	AcmControllers/Configuration/ConfigurationTable/controller1	acmcontrollers configuration configurationtable controller1
Additional ACM margin	Extra safety margin that is added to the minimum and target margin . Valid values are from -10 dB to +30 dB. The default value is 0 dB. **NOTE -** This is a local ACM client setting and affects the margins that the local ACM client receives from the remote ACM controller.	ACM > Tuning	AcmClients/Configuration/ConfigurationTable/client1	acmclients configuration configurationtable client1

Parameter	Description	GUI	REST API	CLI
Minimum/maximum MODCOD	Range from which a MODCOD can be selected. Valid values are: unused qpsk14 qpsk13 qpsk25 qpsk12 qpsk35 qpsk23 qpsk34 qpsk45 qpsk56 qpsk89 qpsk910 8psk35 8psk23 8psk34 8psk56 8psk89 8psk910 16apsk23 16apsk34 16apsk45 16apsk56 16apsk89 16apsk910 32apsk34 32apsk45 32apsk56 32apsk89 32apsk910 qpsk1345 qpsk920 qpsk1120 8apsk59l 8apsk2645l 16apsk12l 16apsk815l 16apsk59l 16apsk2645 16apsk35 16apsk35l 16apsk2845 16apsk2336 16apsk23l 16apsk2536 16apsk1318 16apsk79 32apsk23l 32apsk3245 32apsk1115 32apsk79 64apsk3245l 64apsk1115 64apsk79	ACM > Tuning	AcmControllers/Configuration/ConfigurationTable/controller1	acmcontrollers configuration configurationtable controller1

Parameter	Description	GUI	REST API	CLI
	64apsk45 64apsk56 256apsk2945l 256apsk23l 256apsk3145l 256apsk3245 256apsk1115l 256apsk34 qpsk1145 qpsk415 qpsk1445 qpsk715 qpsk815 qpsk3245 8psk715 8psk815 8psk2645 8psk3245 16apsk715 16apsk815 16apsk3245 32apsk23 The default value is "unused" and corresponds with lowest/highest MODCOD enabled, see next table.			

Per MODCOD

Parameter	Description	GUI	REST API	CLI
Enable	Enable or disable the MODCOD. Valid values are: • on • off*	ACM > MODCODs	AcmControllers/Configuration/Modcods/[Index]	acmcontrollers configuration modcods [Index]

Parameter	Description	GUI	REST API	CLI
Minimum margin	Margin on top of the minimum signal quality required to keep using the MODCOD. Only editable when MODCOD tuning is set to manual. Valid values are from -10 dB to +30 dB. The default value is 0 dB.	ACM > MODCODs	AcmControllers/Configuration/Modcods/[Index]	acmcontrollers configuration modcods [Index]
Target margin	Margin on top of the minimum signal quality required for using the MODCOD. Only editable when MODCOD tuning is set to manual. Valid values are from -10 dB to +30 dB. The default value is 0.3 dB.	ACM > MODCODs	AcmControllers/Configuration/Modcods/[Index]	acmcontrollers configuration modcods [Index]
Distortion margin	Extra margin when non-linear degradation occurs. Only editable when MODCOD tuning is set to manual. When MODCOD tuning is set to auto, the distortion margin is 0 dB. Valid values are from 0 dB to 30 dB. The default value is 0 dB.	ACM > MODCODs	AcmControllers/Configuration/Modcods/[Index]	acmcontrollers configuration modcods [Index]

ST Engineering iDirect (Europe) CY NV

Laarstraat 5

9100 Sint-Niklaas Belgium

+32 3 780 6500

www.idirect.net