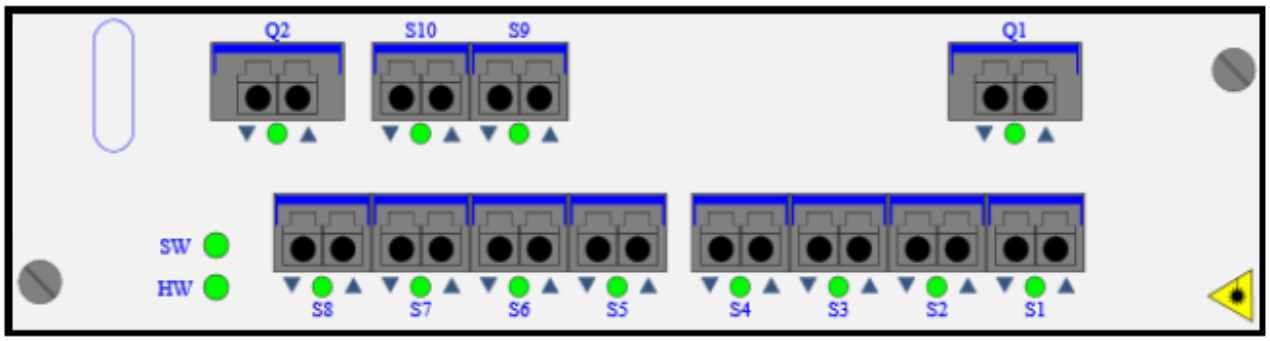
MICROSENS

# Encryption Module (MS430961M) - Quick Start Manual

## Module presentation




MS430961M allows encrypting data transported on a 100G OTU4:

- Line Encryption based on GCM AES-256 algorithm with Diffie Hellman keys exchange
- Ten Multiprotocol client port interfaces
- Standard G709 OTU4 Line interface

QSFP28 module for line port physical interfacing
SFP+ modules for client port physical interfacing.

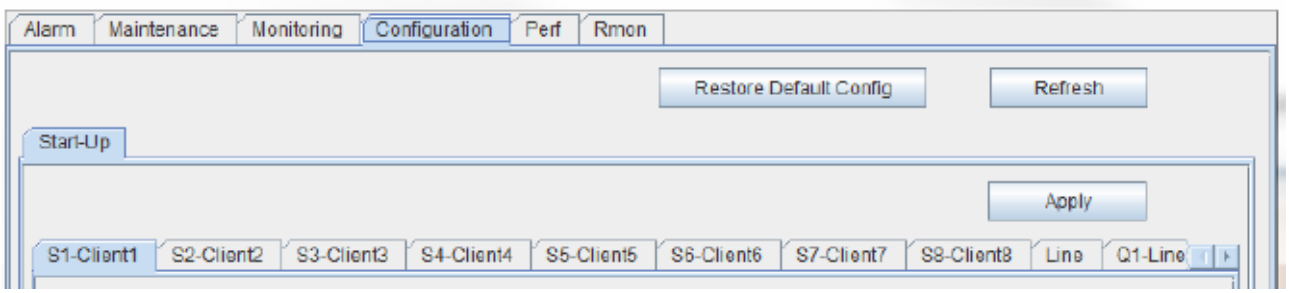
# STEP 1: plugging & configuration of the module

## Insert the PM_CRYPTO module

Wait until HW/SW leds on the module are green and stable. (Around 8 min)

## Configuration of the module :

1/ In case of new installation: "Restore Default Config"
On Web interface -> Select the module -> Right Click -> Configuration/Start-Up

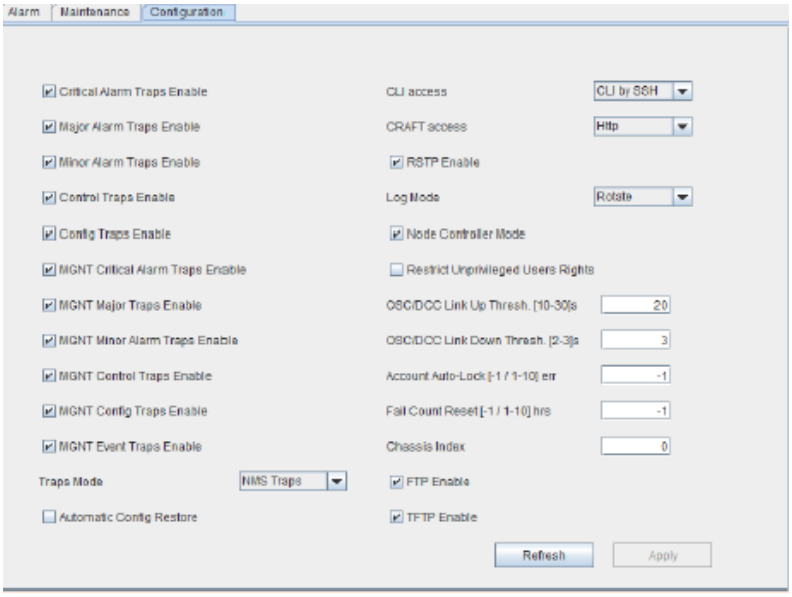



On CLI -> configure_pm -c 'slot_number'

```
administra@noname(20000)> configure_pm -c 6
This will erase the current configuration and reset the board.
Continue ? (y/N)
```

*SAFETY WARNING:* By default, the line Tx and all the client ports are "In Service". It means that all Tx are power on.

2/ In case of PM replacement :
On Web interface -> Tic the parameter "Automatic Config Restore" on MGNT/Configuration menu. Wait for the Cold restart and plug the new Encryption module (MS430961M).



On CLI -> set_mgnt_config

```
20) Traffic Modules conf auto restore (Enable/Disable, current is Enable):
```

Wait for the Cold restart and plug the new Encryption module (MS430961M).

## STEP 2: Module setup

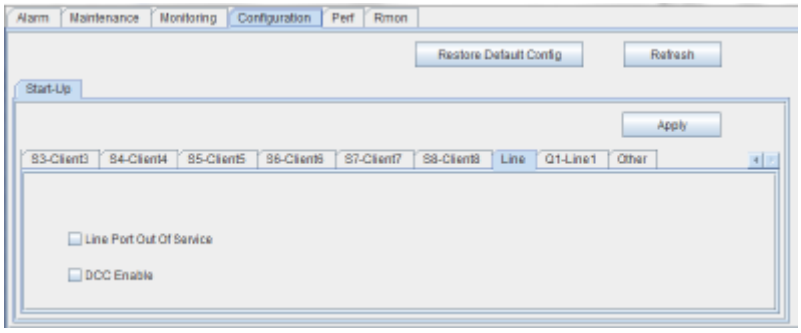
### Optical connection

Connect the module on line and client side with optical patchcords.
-> Line side to a client port of Flex rate cards (ex. MS430943M)
-> Client side to the respective equipment

*WARNING:* Line_Tx is emitting by default, so optical power will be received from the far end module.
In order to prevent Rx damage, use LC/PC attenuator to adjust the input power, and be as close as possible of the typical value.

### DCC channel configuration (if necessary)

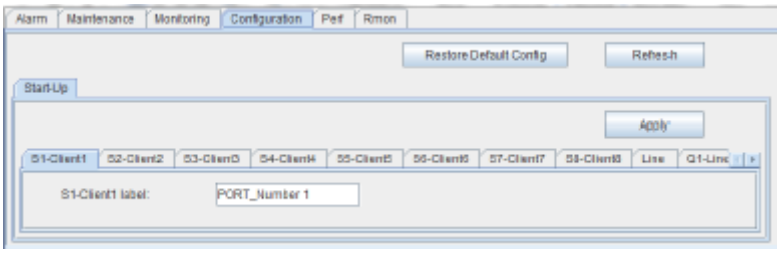
On Web interface -> Select the module -> Right Click -> /Configuration/Start-Up/Line




On CLI -> set_config 'slot_number' other

```
administra@IP181(24072)> set_config 3 other
1) DCC Enable ; possible values : (Disable,Enable), current is Disable :
```

**Label the Client and the Line ports** to make easier their identification
On Web interface -> Select the module -> Right Click -> /Configuration/Start-up/Si-Client#i (and Configuration/Q1-Line1)



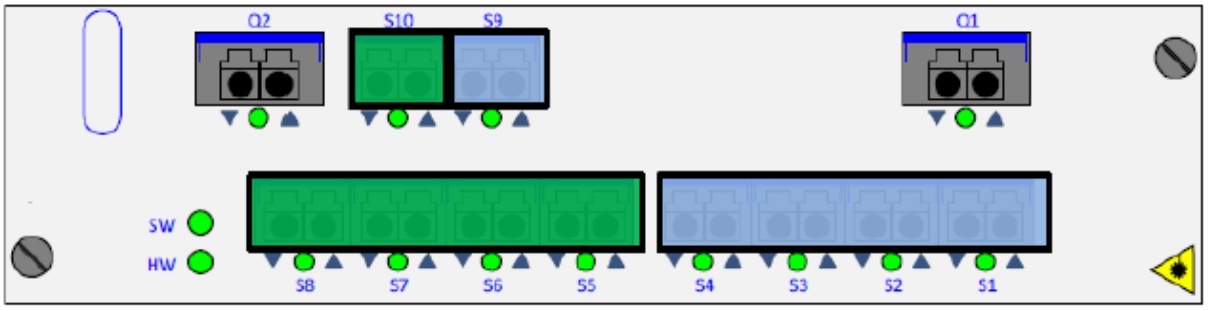
On CLI -> set_config 'slot_number' S1-Client1 (for client1) / set_config 'slot_number' Q1-Line1

```
administra@IP181(24072)> set_config 12
Q1-Line1      S2-Client2    S4-Client4    S6-Client6    S8-Client8
S1-Client1    S3-Client3    S5-Client5    S7-Client7    other
```

For unused client, it is recommended to set the client port(s) "Out Of Service" to not interfere with the management of the port(s) in service.

## Traffic type

The MS430961M client part is made of 2 groups of 5 SFPs. Each group of 5 ports can be configured in the following protocol mode: 5 x MP, 4 x EMP, 2 x MP + 2 x 16GFC, 3 x 16GFC




Group 1 (Client 1, 2, 3, 4 and 9)

Group 2 (Client 5, 6, 7, 8 and 10)

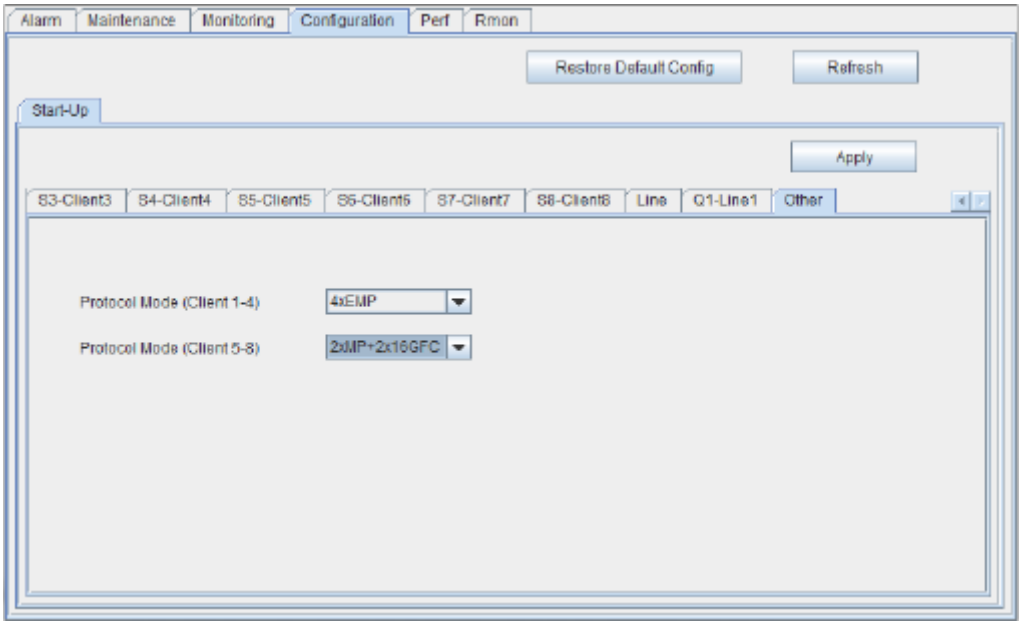
The following table provides the port used upon the select mode:

| | Client port 1<br>Client port 5 | Client port 2<br>Client port 6 | Client port 3<br>Client port 7 | Client port 4<br>Client port 8 | Client port 9<br>Client port 10 |
|---|---|---|---|---|---|
| 5 x MP | MP | MP | MP | MP | MP |
| 4 x EMP | EMP | EMP | EMP | EMP | OOS (1) |
| 2 x MP + 2 x 16GFC | 16GFC | 16GFC | MP | MP | OOS (1) |
| 3 x 16GFC | 16GFC | 16GFC | 16GFC | OOS (1) | OOS (1) |
| (1) OOS: Out Of Service (the port is not used). | | | | | |

Additionally, if the Group 1 and Group 2 are both configured in 3 x 16GFC mode, an extra 16GFC client port is enabled on Client port 4 of the Group 1.
The module can then transport 7 x 16GFC protocols. In that case, the client ports of the Group 1 and Group 2 will be configured as following:

| Group | Group 1 | | | | | Group 2 | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Client Port | 1 | 2 | 3 | 4 | 9 | 5 | 6 | 7 | 8 | 10 |
| Protocol | 16GFC | 16GFC | 16GFC | 16GFC | OOS | 16GFC | 16GFC | 16GFC | OOS | OOS |

On Web interface -> Select the module -> Right Click -> Configuration/Start-Up/Other




On CLI -> set_config 'slot_number' other

```
**********************
*   Slot 12          *
*   CRYPTO           *
*   other Config     *
**********************

1) DCC Enable ; possible values : (Disable,Enable), current is Disable :
2) Protocol Mode (Client 1-4) ; possible values : (5xMP,4xEMP,2xMP+2x16GFC,3x16GFC), current is 4xEMP :
3) Protocol Mode (Client 5-8) ; possible values : (5xMP,4xEMP,2xMP+2x16GFC,3x16GFC), current is 2xMP+2x16GFC
4) Perf Enable ; possible values : (Disable,Enable), current is Enable :
Do you want to apply this new configuration now (this won't affect traffic).
Continue ? (y/N)
```

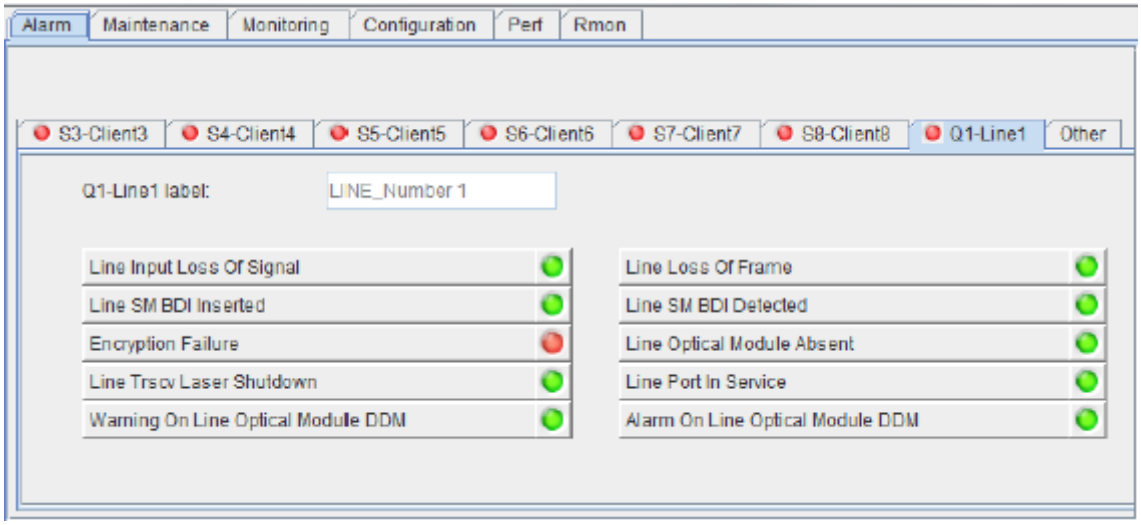
## STEP 3: Specific encryption feature configuration

*WARNING:* Encryption configuration panel is available only through CLI commands.

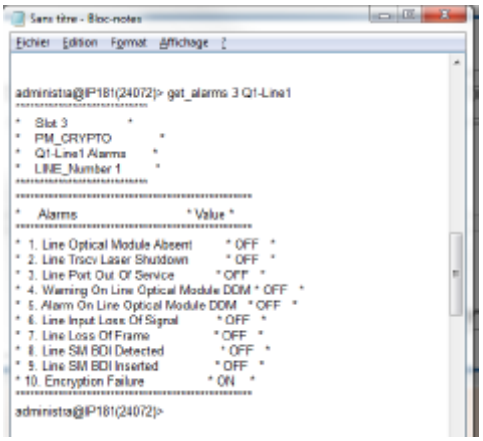
*WARNING:* Encryption feature is based on a key exchange between two modules so this feature is available only if two encryption modules are correctly running and facing each other.

### 1/ First Status Checking:

Confirm the link is up and running between the two encryption modules.
On Web interface -> Select the module -> Right Click -> Alarm (for Line)




On CLI -> get_alarm 'slot_number' Line




On both modules, the only alarm ON have to be: 'Encryption failure'.
If another alarm is ON please go back to step 1.

## 2/ Crypto Officer accounts creation:

Considering the two crypto cards are located on separate sites, the creation of a new "crypto officer" role account is needed on both NEs:
On CLI -> manage_user_account –a

```
administra@IP181(24072)> manage_user_account -a
Enter the user account name : admin_crypto
Enter the 'admin_crypto' CLI Profile ; possible values : (administrator, maintenance, readonly, none)
[Defaults to 'readonly' if left blank] : administrator
Enter the 'admin_crypto' CRAFT Profile ; possible values : (administrator, maintenance, readonly, none)
[Defaults to 'administrator' if left blank] : administrator
Enter the 'admin_crypto' Crypto Role ; possible values : (crypto user, crypto officer, none)
[Defaults to 'none' if left blank] : crypto officer
```

NOTE: The CRAFT profile can be either administrator, maintenance, readonly or none. The CLI profile has to be at least readonly profile in order for the crypto officer to be able to connect through CLI.
NOTE: when you first create a user, the password is similar to the account name.

Confirm the crypto officer account is created on both NEs:

On CLI -> manage_user_account –l

```
administra@IP181(24072)> manage_user_account -l
*****************************************************************************************
*    User name     * CLI profile   * CRAFT profile * Crypto Role    * Status            *
*****************************************************************************************
*  1. administrator * administrator * administrator * none          * Logged In CLI+CRAFT *
*  2. admin_crypto  * administrator * administrator * crypto officer * Logged In CLI      *
*****************************************************************************************
```

## 3/ Authentication Key setting:

Connect to both NEs via CLI and under your new "crypto officer" accounts previously created. Set up the authentication key on both crypto card. The keys have to be similar on both encryption cards.

On CLI -> manage_crypto 'slot_number' –authentication_key='mynewkey'

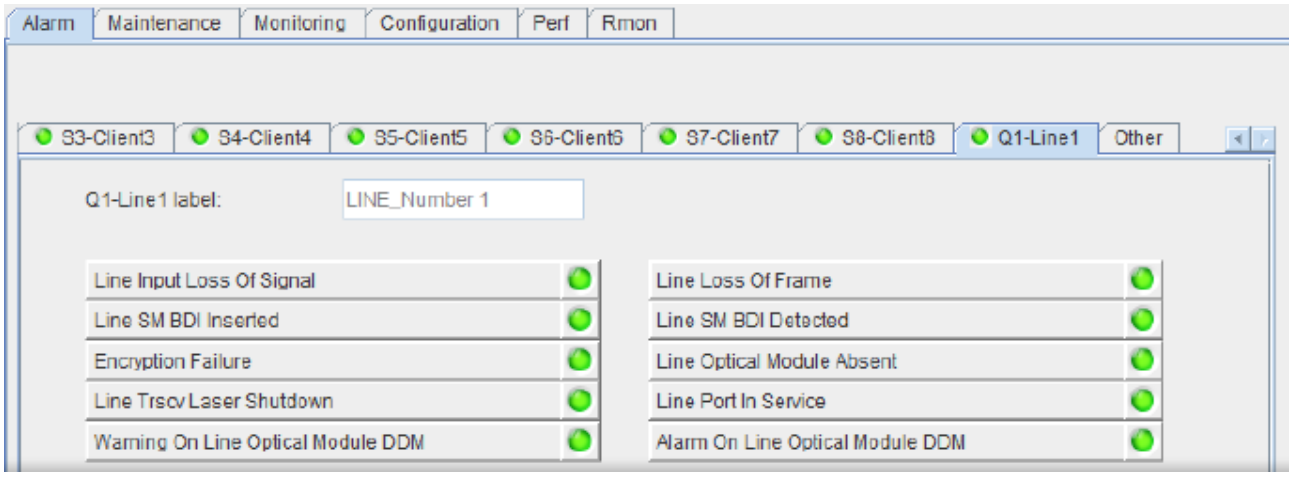
```
admin_cryp@IP181(17751)> manage_crypto 3 -authentication_key='mynewkey'
```

WARNING: The key is not stored anywhere into the module or management board memory. If in any case the module restarts (or has to be cold reset) the authentication key needs to be reloaded.

## 4/ End of crypto feature configuration:

Confirm the 'Encryption Failure' alarm is now cleared:

On Web interface -> Select the module -> Right Click -> Alarm (for Line)



On CLI -> get_alarm 'slot_number' Line

```
administra@IP181(24072)> get_alarms 3 Q1-Line1
**************************
*   Slot 3              *
*   PM_CRYPTO           *
*   Q1-Line1 Alarms     *
*   LINE_Number 1       *
**************************
*****************************************************
*   Alarms                          * Value *
*****************************************************
*  1. Line Optical Module Absent      * OFF   *
*  2. Line Trscv Laser Shutdown       * OFF   *
*  3. Line Port Out Of Service        * OFF   *
*  4. Warning On Line Optical Module DDM * OFF   *
*  5. Alarm On Line Optical Module DDM   * OFF   *
*  6. Line Input Loss Of Signal       * OFF   *
*  7. Line Loss Of Frame              * OFF   *
*  8. Line SM IBDI Detected           * OFF   *
*  9. Line SM IBDI Inserted           * OFF   *
* 10. Encryption Failure              * OFF   *
*****************************************************
administra@IP181(24072)>
```

Check the crypto counter and reset it on both modules:

On CLI -> manage_crypto 'slot_number' -reset_monitoring
On CLI -> manage_crypto 'slot_number' –monitoring

```
admin_cryp@IP181(17751)> manage_crypto 3 -reset_monitoring
admin_cryp@IP181(17751)> manage_crypto 3 -monitoring
Counter failed key exchange   = 0
Encryption off time remaining = 0 seconds
Session key time remaining    = 10 seconds
admin_cryp@IP181(17751)>
```

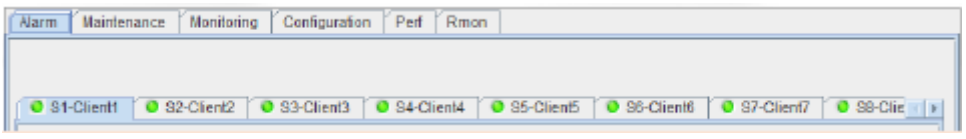
Counter failed key exchange has to stay to 0.

## STEP 4: End of installation

**Leds status**
Verify that all the led are green or unlighted (in case of port Out Of service).

**Alarms status**
Check that no alarm is present on line side and on each client In Service.

On Web interface -> Select the module -> Right Click -> Alarm (for Si-Client#i and Line)



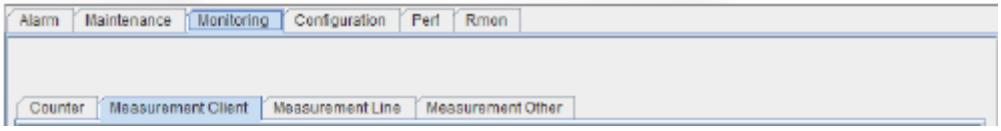

On CLI -> get_alarm 'slot_number' S1-Client1 (for client1 and Line)

```
administra@IP181(24072)> get_alarms 3 S1-Client1
```

## Power Monitoring

Check that input/output power on line side and on each client In Service and verify it is in the correct range according to the QSFP28 and SFP+ module specifications.
Adjust the input power if necessary with LC/LC attenuator, in order to be as close as possible of the typical value.

On Web interface -> Select the module -> Right Click -> Monitoring/ Measurement (for Si-Client#i and Line)



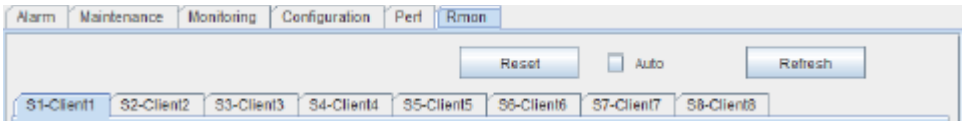

On CLI -> get_measurement 'slot_number' Line (for Line)

```
administra@IP181(24072)> get_measurements 3 Q1-Line1
```

## Remote Network Monitoring (Rmon) on client

Open the Monitoring window to display the counters of traffic on each port In Service. Check no error is present.

On Web interface -> Select the module -> Right Click -> Rmon (for Si-Client#i)




On CLI -> get_counters 'slot_number' S1-Client1 (for client1)

```
administra@IP181(24072)> get_counters 3 S1-Client1
```

*MICROSENS reserves the right to make any changes without further notice to any product to improve reliability, function or design. MICROSENS does not assume any liability arising out of the application or use of any product. pp/0719*