

Web Management User Manual for MSP3000 and MXP100

MICROSENS

General

The Web Management User Manual describes the Web Management Java applet in regard to the management of the MICROSENS product which is composed of the MXP100 Platform and MSP3000 Platform

Introduction

Product Overview

This Manual is valid for MSP300 modular Platform and the MXP100 which can be used in a transponder or muxponder version. In the muxponder version are 3 different modes available:

- 1: 10GE Version
2. 40G Version
3. Multi-protocol version

All this types are managed in the same way.

Modular Chassis

Two types of 19" modular chassis are available:

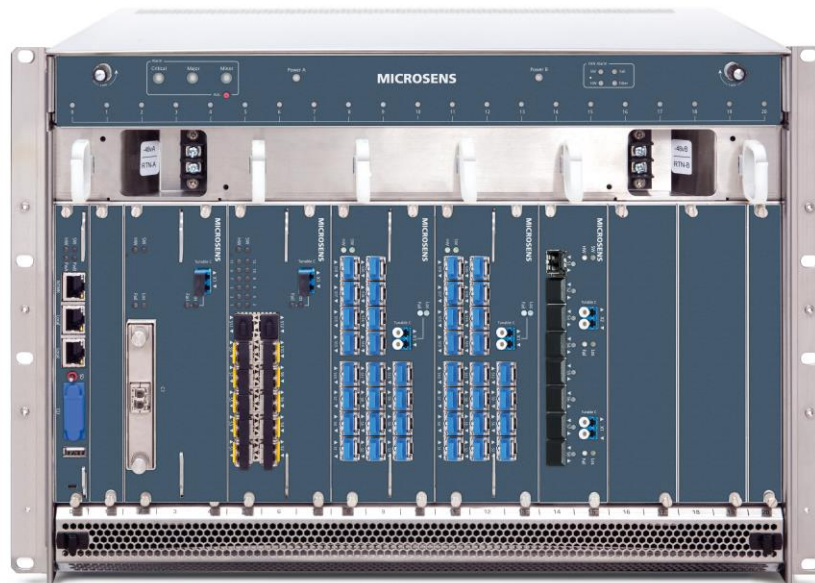
- The MS430504M is a 7 RU chassis, designed for up to 600 Gb/s aggregation and transport.
- The MS430501/3M is a 2 RU chassis, designed for up to 200 Gb/s aggregation and transport.

Their generic slots can receive any service module from MICROSENS MSP3000 Platform. The pluggable module occupies 1, 2 or 3 slots depending on its type. Any combination of service PMs can be used to accommodate channel growth without service interruption.

MS430504M chassis

MS430504M chassis contains:

- One vertical slot (slot 0) dedicated to the management module (called MGNT4).
- One horizontal slot dedicated to the FAN module, composed of six fans. The module is located in slot 23.
- 20 vertical generic slots available for aggregation and transport modules (slot 1 to slot 20).



MS430501/3M chassis

The MS430501/3M chassis contains:

- One management module (called MGNT4).
- One fan module, composed of three fans.
- 6 available generic slots for aggregation and transport modules (slot 1 to slot 6).



MXP100 integrated Chassis

The MXP100 solutions include the MICROSENS MXP100-10GE, MXP100-40GE and MXP100-MP. All share the same design, which consists of a 1 RU rack mountable 19" box containing 100G transponder and muxponder all-in-one. This box can be utilized anywhere 100G is needed, whether for single 100G services or for aggregation of lower rate services onto 100G.

The MXP100 include the following functional modules:

- A management module (called MGNT)
- A fan module (called TR-FAN)
- A transponder/muxponder module (called TRANS)

MXP100



Management Tools

The MSP3000 and MXP100 platform includes an on-board Simple Network Management Protocol (SNMP) agent, which allows local and remote management solutions.

Several tools can be used to manage the MGNT, FAN and Service-cards modules through the SNMP agent:

- The Management Information Base (MIB) is one available method for managing the modules. An SNMP MIB browser enables you to load, browse, and search for managed objects, walk the MIB tree, and perform all other SNMP-related functions.
- The Command-Line Interface (CLI) can be used to manage the modules through the local RS232 port or remotely, through an SSH or Telnet connection.
- The Web-Interface (Craft Terminal) is a Java applet which can be run on a standard Personal Computer (PC) and only needs a Web browser with the correct Java Runtime Environment (JRE) installed. It relies on MIB data and provides a graphical view of the box and of the SNMP managed objects.

The Craft Terminal is an easy-to-use solution for performing common operations. It can be used in combination with the CLI or a MIB browser.

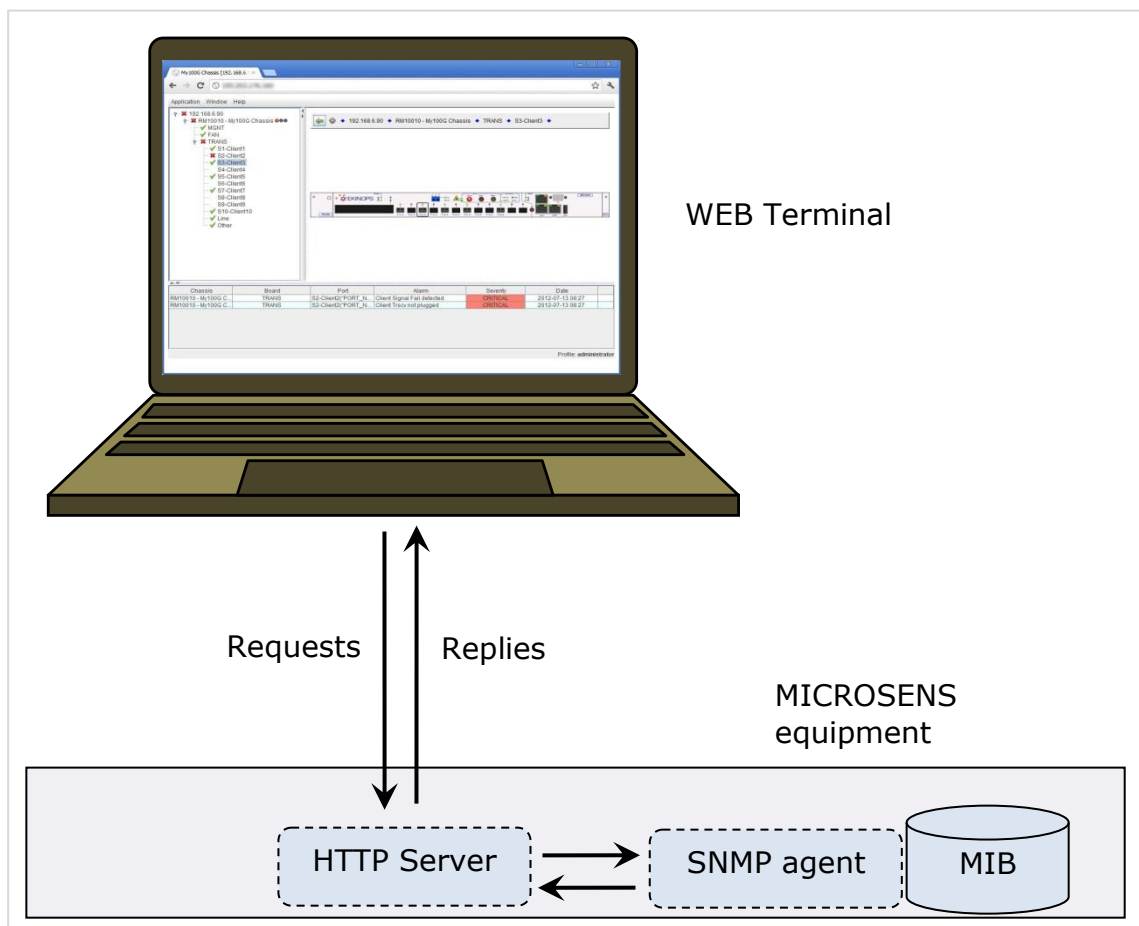
WEB Interface Overview

This chapter is a brief overview of the WEB-Interface. It explains how to open your first session.

Principles

The MICROSENS WEB Interface for the MXP100 is an embedded Java applet which is downloaded from the MICROSENS equipment when the user opens a session using a standard Web browser. It operates by means of standard SNMP requests to the SNMP agent located in the MICROSENS equipment.

The WEB Interface provides a graphical view of the MIB using the information it receives from the SNMP agent.



The Craft Terminal provides a graphical view of the MIB

System Requirements

The WEB Interface does not need any specific software installation. The WEB Interface only requires the following technical specifications.

Hardware

Type	Personal Computer (PC)
Processor	2 GHz minimum (Intel core, AMD Athlon, Intel Pentium...)
Memory	2 GB or more
Screen	Optimized for 1024*768 resolution

Software

Operating system	Windows XP, Vista, 7, 8 or Linux
Java version	j2SE or J2RE v1.6.0 (or above) is recommended. From v1.7, Java security level must be set to Medium.
Windows Web browser	Microsoft Internet Explorer 5.5 (or above), Mozilla 1.2 (or above), Google Chrome 1.0 (or above)
Linux Web browser	Mozilla 1.2 (or above), Google Chrome 5.0 (or above)
TCP port	The WEB Interface advanced administration feature uses TCP port 4010, which must be accessible.

Connection to the equipment

The equipment must be powered-up and ready to operate. .

The equipment default IP settings are:

- Default IP address: **192.168.16.201**.
- Default IP Netmask: **255.255.255.000**.

You can change these settings using a local connection.

Check that the PC IP settings are compatible with the equipment IP settings used.

Procedure below shows how to verify that the PC is able to communicate with the MICROSENS equipment (in this example, the default settings are used).

Procedure

To connect to the MICROSENS equipment for the first time:

1. Using a standard cable, connect the computer to the left Ethernet port.
2. Check the connection:
 - a. Open a DOS command window.
 - b. Perform a **ping** command.

```
ping 192.168.16.201
```

The following kind of message means the MICROSENS equipment is properly connected.

```
Reply from 192.168.16.201: .....
```

- c. Press *Ctrl-C* to stop the **ping** command.
- d. Type *exit* to close the DOS command window.

End

User Accounts

To access the WEB Interface as well as the Command-Line Interface, the user is asked to authenticate via his account name and related password.

1.1.1 User Rights

Each user account includes two profiles that define the user rights in regards of the management tools:

- One profile associated with the CLI (Command Line Interface)
- One profile associated with the WEB Interface (Craft Terminal)

1.1.2 Profile Types

Three profile types are available:

- **administrator** is the super-user profile. An administrator has full rights to administrate and configure the MICROSENS platform.
- **maintenance** is the profile suitable for users who need to control, configure, monitor and upgrade the equipment.
- **readonly** is the profile suitable for users only allowed to display information and monitor the alarms.

Table below summarizes the different user rights associated with the profile types.

Rights / profiles	readonly	maintenance	administrator
User Accounts	No	No	Yes
Change Password	Own account	Own account	Password reset
Community names	No	No	Yes
IP addresses, MICROSENS equipment name	No	No	Yes
Maintenance actions	Read only	Yes	Yes
Module configuration	Read only	Yes	Yes
Module monitoring	Yes	Yes	Yes
Inventory	Yes	Yes	Yes
Alarm information	Yes	Yes	Yes

Local Accounts

Predefined Local Accounts

Three predefined local accounts are provided, that are not modifiable except their passwords. The maintenance and readonly accounts can be deleted by an administrator.

User name	CLI profile	WEB profile
administrator	administrator	administrator
maintenance	maintenance	maintenance
readonly	readonly	readonly

Since R6.3.501, there is only one predefined local account : administrator account

Other Local Accounts

An administrator can add other local accounts that can be modified or deleted as needed.

Password Management

Each user is responsible for the management of his account password.

By default, the account password is identical to the account name. All users are strongly recommended to change their password at first session.

An administrator can reset any non-administrator account password to its default value, which is the account name.

Radius Server

In addition to local accounts, a Radius server can be used to authenticate users.

Like a local account, a Radius account must be associated with a CLI profile and an WEB profile.

User Account Management

To manage user accounts refer to section 0 of the *Administration* chapter.

Administration operations are reserved to administrators except password management which is accessible to all users.

Administrator can lock or unlock all users. A user account can be locked due to failed password entry, only user with administrator profile can lock and unlock user account

Community Names

An SNMP community name is a text string used to authenticate messages that are sent between the WEB Interface, or any other management tool, and the SNMP agent which is located in the MICROSENS equipment.

Three community names are used:

- The Get community name allows the user to obtain information on managed objects,
- The Set community name allows the user to modify configuration and settings,
- The Trap community name allows the user to receive trap notifications.

Community names used by the WEB Interface

When opening a WEB Interface session, the user is asked to type the community names that will be used in the WEB Interface requests to the SNMP agent. There is generally no need to modify the community names provided by default in the edit fields.

These values must be modified only if the community names of the SNMP agent have changed since the last WEB session. Once the community names used by the WEB Interface have been modified, the new values are stored and become the default values for the next sessions.

Community names of the SNMP agent

The WEB Interface can be used to change the community names of the SNMP agent (administrator profile only).

Opening the First Session

If the terminal meets the system requirements and is properly connected to the MXP100, a WEB session can be opened.

Procedure

To open a WEB Interface session:

1. Launch the Web browser.
2. In the location bar (also called address bar or URL bar), type the MICROSENS device IP address. For example, if the default IP address is still in use, type **"192.168.16.201"**.

A login dialog box is displayed.

3. Choose a user account.
4. Type the associated password. For a first connection, the default passwords are as follows:

Account name	Default password
administrator	administrator
maintenance	maintenance
readonly	readonly

Table 1: Default passwords of the predefined user accounts

5. Click the *Login* button

A dialog box asking for community names is then displayed.

A screenshot of a web-based dialog box titled "SNMP community names". It contains three text input fields. The first field is labeled "GET community name :" and contains the text "public". The second field is labeled "SET community name :" and contains the text "private". The third field is labeled "TRAPs community name :" and contains the text "public". Below these fields is a blue button labeled "Apply".

SNMP community names	
GET community name :	<input type="text" value="public"/>
SET community name :	<input type="text" value="private"/>
TRAPs community name :	<input type="text" value="public"/>
<input type="button" value="Apply"/>	

"Name of communities" dialog box

6. Type your community names. The default values of the community names of the SNMP agent are as follows:

Community	Default name
GET community	public
SET community	private
TRAP community	public

Table 2: Default community names

7. Click *Apply*

An Alert box informs you on equipment-information upload progress.

The WEB Interface (Craft Terminal) home page is then displayed. Visual indications on alarm status update after a few seconds.

The session is now open. It will end when the Web browser is closed or using the *Application/Logout* menu.

End

General Management

This chapter describes the WEB interface and general management tasks accessible through the menu.

Interface Description

The WEB Interface allows you to monitor and manage the equipment through a menu and a graphical interface.

The graphical interface is divided into three views:

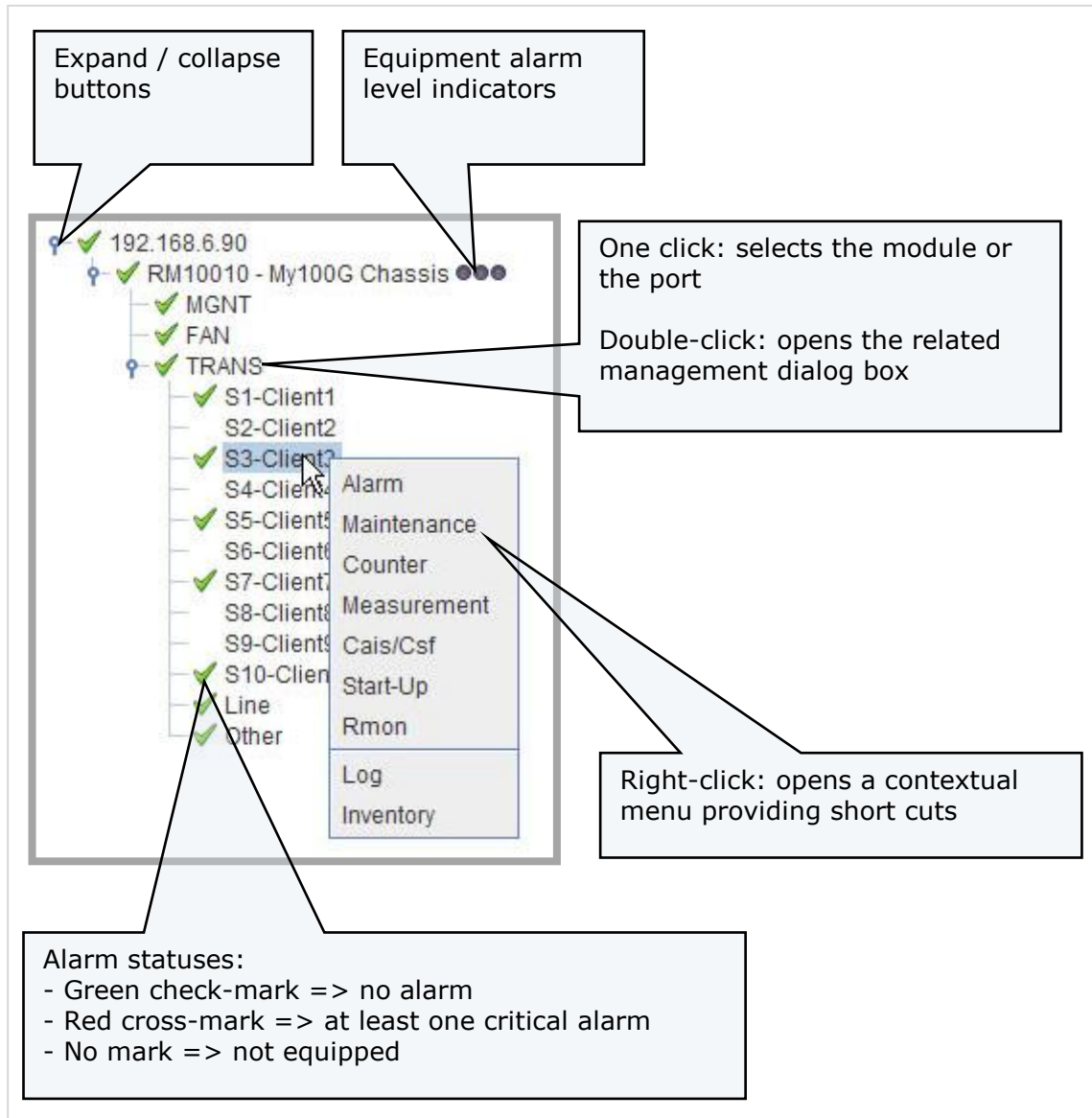
- The equipment tree is a hierarchical view of the equipment components.
- The equipment snapshot is a graphic representation of the equipment front panel.
- The alarm listing displays all ongoing minor, major and critical alarms.

Each of these three views can be resized, hidden or detached in a separate window.

Equipment Tree

The equipment tree is a hierarchical view of the equipment modules and components. It provides a quick view on alarm statuses and short cuts to management.

You can detach the equipment tree view from the main window (see 0).

**Equipment Tree (MXP100)**

Equipment Snapshot

The equipment snapshot is a graphic representation of the front panel very similar to the real one. It updates automatically when any event occurs (after some delay), providing a quick view on the operational statuses of all equipment components.

In particular:

- The graphic representations of lines and ports indicate their service status (graphic representation is empty if the line or port is out of service). Note that these graphic representations are also clickable hotspots providing useful short cuts to port and line management.
- Graphic LEDs behave in the same manner as the real ones.

You can detach the equipment snapshot view from the main window.

Hotspots

The Equipment snapshot provides you with several hotspots that you can use to select the different components:

- For the MXP100, you can select (one click) or manage (second click) the client and line ports that are in use.

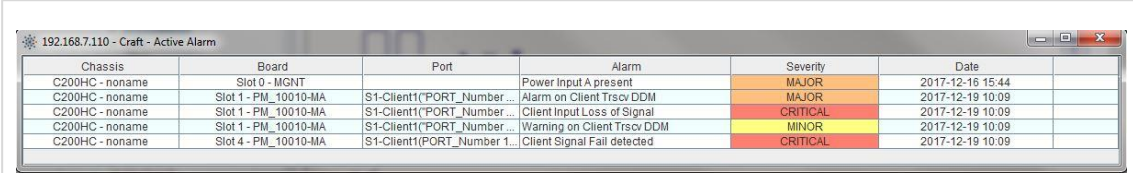
Equipment Snapshot and Equipment Tree Synchronization

You can use either the Equipment Snapshot hotspots or the Equipment Tree items to select a component and display the related management windows. Both views work in full synchronization.

Alarm Listing

The alarm listing is a display-only view that lists all active alarms.

You can detach the alarm listing view from the main window (see 0).



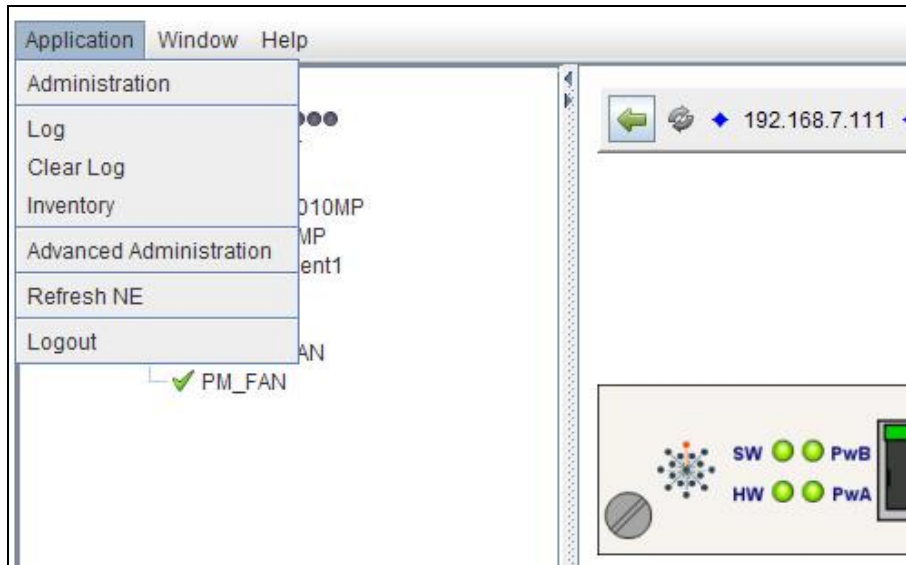
Chassis	Board	Port	Alarm	Severity	Date
C200HC - noname	Slot 0 - MGNT		Power Input A present	MAJOR	2017-12-16 15:44
C200HC - noname	Slot 1 - PM_10010-MA	S1-Client1(PORT_Number ...	Alarm on Client Trscv DDM	MAJOR	2017-12-19 10:09
C200HC - noname	Slot 1 - PM_10010-MA	S1-Client1(PORT_Number ...	Client Input Loss of Signal	CRITICAL	2017-12-19 10:09
C200HC - noname	Slot 1 - PM_10010-MA	S1-Client1(PORT_Number ...	Warning on Client Trscv DDM	MINOR	2017-12-19 10:09
C200HC - noname	Slot 4 - PM_10010-MA	S1-Client1(PORT_Number 1...	Client Signal Fail detected	CRITICAL	2017-12-19 10:09

Menu: Application

The *Application* menu gives access to general management tasks detailed in this section.

Note

The *Administration* and *Advanced Administration* entries are described in chapter 0 dedicated to administration.



Log

In the *Application* menu, select *Log* to display traps or logs.

A dropdown list allows you to choose between:

- Traps
- The MGNT module log
- One of the PMs log (modular chassis) or the TRANS module log (all-integrated chassis)
- The FAN module log

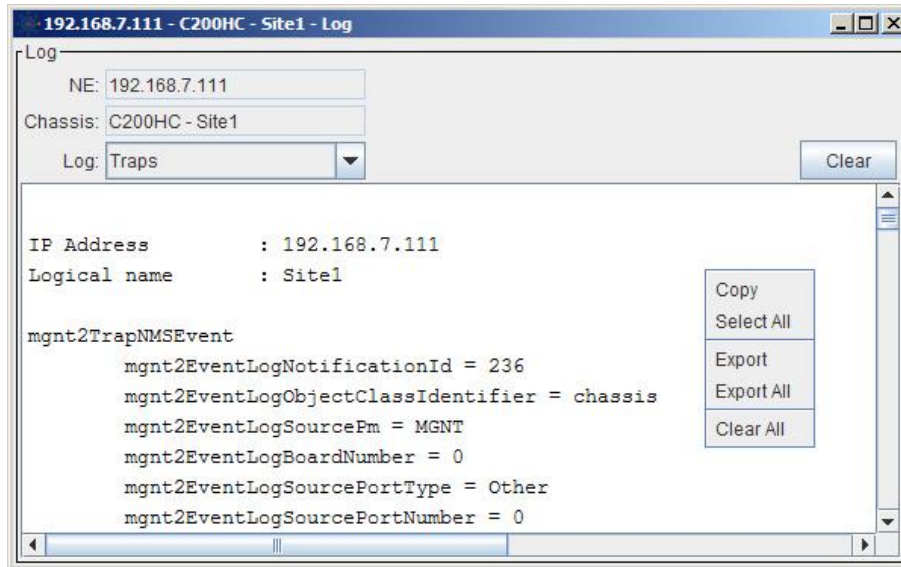
Available Actions

Clicking the *Clear* button clears the current log file.

Right-clicking in the display zone opens a contextual menu:

- Select a part of the log with the mouse or the whole log with *Select all* and then click *Copy* to copy it into memory.

- Click *Export* to export the current log to a text file or *Export All* to export all logs.
- Click *Clear All* to clear all logs.



Log and relating contextual menu

Clear log

In the *Application* menu, select *Clear Log* to clear all log files straight from the menu.

Inventory

In the *Application* menu, select *Inventory* to obtain information on system hardware and software. A dropdown list allows you to specify whether the inventory applies to all modules or to one module: MGNT, FAN, Servicecards.

Available Actions

Right-clicking in the display zone opens a contextual menu:

- Select a part of the inventory with the mouse or the whole inventory with *Select all* and then click *Copy* to copy it into memory.
- Click *Export* to export the inventory to a text file.
- Click *Refresh All* to refresh all available inventories.
- Click *Styled* to change the display style. Revert to the default by clicking *Styled* a second time.

Refresh NE

In the *Application* menu, select *Refresh NE* to synchronize the displayed information with the reality. Use it for example after you have modified some settings via the Command Line Interface.

Use also the *Refresh NE* option if you notice that several colored indicators that should be colored green or red are colored grey.

Logout

In the *Application* menu, select *Logout* to close your session.

Menu: Window

New Window

In the *Window* menu, select *New Window* to open a new independent WEB Interface window. This new window has the same functionalities and behavior as the initial window.

Detach View

In the *Window* menu, select *Detach View* to detach one of the three main views in an independent window.

You can detach:

- the equipment tree,
- the equipment snapshot,

- the alarm listing.

To come back to the initial three-view window, you can:

- close the detached view,
- or use *Detach View* to uncheck the option.

Image Preferences

In the *Window* menu, select *Image Preferences* to tune the display according to your computer, graphic card and screen performances.

Menu: Help

In the *Help* menu, select *Dynamic Help* to open a context-sensitive help pop-up window.

Dynamic Help

When a management dialog box is open, move the mouse pointer over the alarm and parameter labels to display additional information.

Administration

In the *Application* menu, click *Administration*.

From the *Administration* window:

- *administrator* users can change several settings such as IP addresses, SNMP settings or equipment name, as well as manage user accounts and configuration files.
- *maintenance* and *readonly* users have a limited access to some information.

The screenshot shows a web-based administration interface for a device. The title bar indicates the IP address 192.168.7.112 and the device model C200. The main window has five tabs: IP Properties (selected), SNMP Settings, Miscellaneous, User Accounts, and Files Management. The IP Properties tab is active, displaying two columns of settings: 'Current Properties' and 'Start-up Properties'. Each column contains four rows of fields: 'Chassis IP Address', 'IP Netmask', 'Gateway 1 IP Address', and 'Gateway 2 IP Address'. Each IP field is accompanied by a 'Rank' field. The 'Apply' button is located at the bottom right of the form area.

Current Properties		Start-up Properties	
Chassis IP Address :	192.168.007.112		192.168.007.112
IP Netmask :	255.255.255.000		255.255.255.000
Gateway 1 IP Address:	192.168.016.254	Rank :	1 000
Gateway 2 IP Address:	192.168.007.003	Rank :	1

Apply

The Administration Window

IP Properties

Use the IP Properties panel to display network management information.

Information displayed is divided into two sections:

- The Current Properties section displays the values that are currently used. They are not modifiable.
- The Start-up Properties section displays the values that will take effect on next MGNT module reset.

Current Properties		Start-up Properties	
Chassis IP Address :	192.168.007.112	192.168.007.112	
IP Netmask :	255.255.255.000	255.255.255.000	
Gateway 1 IP Address:	192.168.016.254 Rank: 1 000	192.168.016.254 Rank: 1 000	
Gateway 2 IP Address:	192.168.007.003 Rank: 1	192.168.007.003 Rank: 1	

Apply

IP Properties Panel

You can change the following IP properties:

- The equipment IP address is set by default to **192.168.016.201**. You can change it to another value (format: xxx.xxx.xxx.xxx).
Note that, after the change has been applied, the Web browser connection to the MICROSENS equipment is no longer valid. You will then need to close the session, reconnect the Web browser to the MICROSENS equipment using the new IP address, and open a new session.
- The Netmask IP address specifies the sub-network mask. It is set by default to **255.255.255.000**.
- Gateway IP addresses can be used to access outside networks.

Procedure

To modify IP Properties:

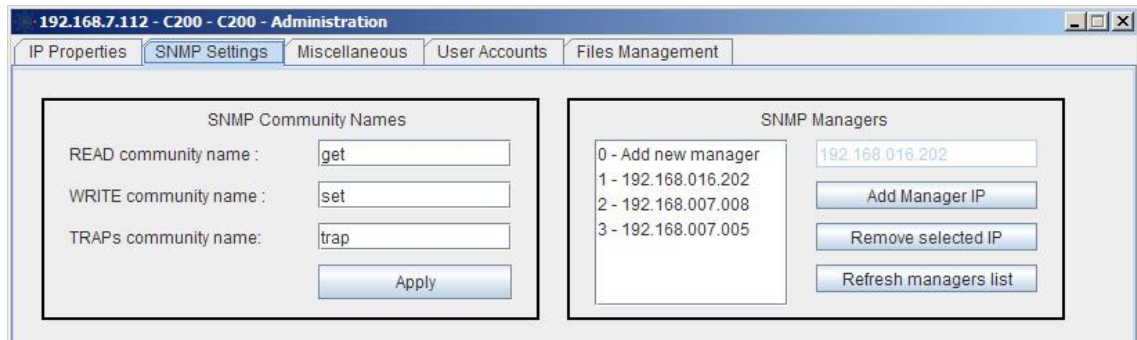
1. Modify the Start-up properties.
2. Click *Apply*.

A message warns you that the changes will take effect on next MGNT module reset.

End

SNMP Settings

Use the SNMP Settings panel to modify SNMP community names or SNMP manager addresses.



SNMP Settings Panel

Changing the SNMP Community Names

Procedure

To modify the community names:

1. Modify one or several community names. Note: the last string character cannot be a digit or a '\$'.
2. Click *Apply*.

A message warns you that the changes will take effect on next MGNT module reset and offers you to perform a warm reset immediately.

3. Click *Yes* to reset immediately, click *No* otherwise.

Note

After the reset completed, the community names that are used by the WEB Interface to interact with the SNMP agent are no longer valid. You must close the WEB session and reopen a new session, typing in the new values in the "Name of communities" dialog box.

End

Changing the SNMP Manager Addresses***Procedure***

To add a new address, enter an IP address and click *Add Manager IP*.

To remove an address, select an IP address and click *Remove Selected IP*.

End

Miscellaneous Settings

The *Miscellaneous* panel gathers several settings distributed into three groups.

The screenshot shows the 'Miscellaneous' tab in the 'Administration' section of the web management interface. The interface is divided into three main sections:

- Top Left Section:** Contains fields for 'Chassis name' (C200), 'System uptime' (0 days 3 h 04'), 'Time (hh:mm)' (15 : 6), 'Date (yyyy - mm - dd)' (2 014 - 11 - 24), and 'Inactivity Timeout' (-1). There are 'Refresh' and 'Apply' buttons at the bottom.
- Top Right Section:** Contains fields for 'NTP server IP address' (192.168.007.008) and 'NTP Timezone' (+1). There is an 'Apply' button at the bottom.
- Bottom Section:** Contains a 'Syslog server IP Address' field (192.168.007.013) and four checkboxes: 'Log Alarm updates', 'Log Control updates', 'Log Config updates', and 'Log other events'. There is an 'Apply' button at the bottom.

Syslog Server Settings

Use the Syslog server settings to send log information (alarms, control modifications, configuration modifications, or events) to a syslog server.

Procedure

To modify the Syslog server settings:

1. Enter the Syslog server IP address.
2. Use the available checkboxes to select log information.
3. Click *Apply*.

A message warns you that the changes will become effective from next MGNT module reset, and offers you to perform a warm reset immediately.

4. Click *Yes* to reset immediately, click *No* otherwise.

End

Name, Time, Date, Inactivity

In the top-right group of settings:

- "Chassis name" identifies the equipment. You are recommended to give a customized name to facilitate the differentiation of each equipment in the network.
- "System uptime" displays how long the MGNT board is running since last reset.
- "Time" and "Date" can be used to change the chassis current time and date.
- "Inactivity Timeout" specifies the maximum number of minutes a user session remains open if no user activity is detected. This value applies to CLI sessions as well as to WEB sessions. Value "-1", which is the default, disables the feature.

Procedure

To refresh the values such as the system uptime, click *Refresh*.

To modify the chassis name, time, date, or inactivity timeout:

1. Change one or several values.
2. Click *Apply*.

End**NTP Time Server Settings**

Use the NTP time server settings to synchronize the chassis date and time with a universal time.

Procedure

To modify the NTP time server settings:

1. Enter the NTP time-server IP-address. Value "0.0.0.0", which is the default, disables the feature.
2. Enter the NTP time zone value, which specifies, in hours, the local time difference from the universal time.
3. Click *Apply*.

A message warns you that the changes will become effective from next MGNT module reset, and offers you to perform a warm reset immediately.

4. Click *Yes* to reset immediately, click *No* otherwise.

End

User Account Management

The *User Account* panel allows an administrator to manage local accounts and configure the use of a Radius server.

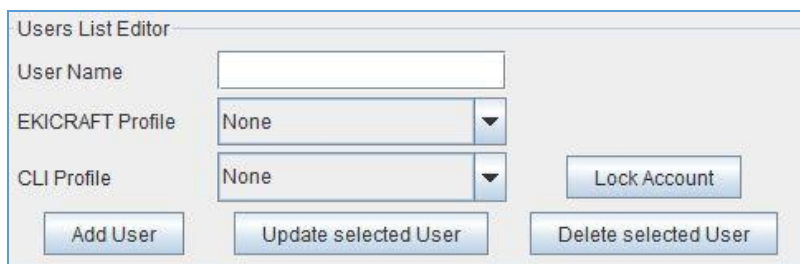
Other users can also access this panel to change their password.

Read section 0 to get general information on user accounts, profiles and associated rights.

User Accounts Panel

The panel is divided in four zones with, on top, the list of local accounts.

Local account management

The screenshot shows a web interface titled "Users List Editor". It contains three input fields: "User Name" (a text box), "EKICRAFT Profile" (a dropdown menu with "None" selected), and "CLI Profile" (a dropdown menu with "None" selected). Below these fields are three buttons: "Add User", "Update selected User", and "Delete selected User". To the right of the "CLI Profile" dropdown is a button labeled "Lock Account".

Use the *User List Editor* to add, modify or delete a local account. This Editor works together with the list of local accounts located on top of the panel

Procedures

To add a local account

1. Enter a user name.
2. Select a CLI profile.
3. Select an WEB profile.
4. Click *Add User*. The account list automatically updates.

To modify a local account

1. Select an account in the local account list. The account settings are displayed in the User List editor.
2. Modify these settings.

3. Click *Update selected User*. The account list automatically updates.

To delete a local account

1. Select an account in the local account list
 2. Click *Delete selected User*.
 3. Confirm. The account list automatically updates.
 - 4.
5. To Lock/Unlock a local account
 6. 1. Select an account in the local account list
 7. 2. Click *Lock(or Unlock)Account*.
 8. 3. Confirm. The account is automatically lock or unlock

End

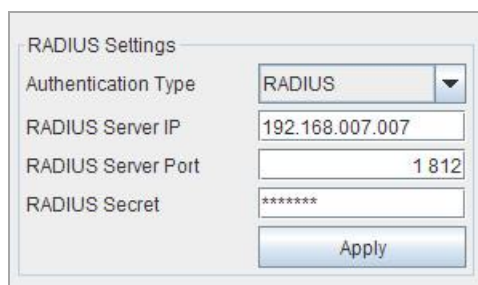
Radius Server Authentication

In addition to local accounts, a Radius server can be used to authenticate users.

When a Radius server is used, the authentication requests are processed in the following order:

1. By the Radius authentication service
2. If unsuccessful, by the local authentication service

Radius Service Configuration



The screenshot shows a 'RADIUS Settings' dialog box. It contains four labeled input fields: 'Authentication Type' with a dropdown menu showing 'RADIUS', 'RADIUS Server IP' with the text '192.168.007.007', 'RADIUS Server Port' with the text '1 812', and 'RADIUS Secret' with a masked password '*****'. Below these fields is an 'Apply' button.

Procedure

To configure a Radius service

1. Select the authentication type: *RADIUS*
2. Enter the Radius server IP address.
3. Enter the Radius server port.

4. Enter the Radius secret string.
5. Click *Apply*.

A message warns you that the modifications will take effect at the next management module reset (refer to section 0).

In addition you must specify the MICROSENS vendor specific attributes as described in the section following.

End

Vendor Specific Attributes (VSAs)

Authenticating through a Radius server requires that MICROSENS vendor specific attributes are associated with the Radius user accounts concerned.

MICROSENS specify the CLI and WEB profiles in accordance with the format below.

Number	Radius VSA	type	Description
1	CLI-Profile	Integer	Cli profile value: 1 Administrator 2 Maintenance 3 Readonly 4 None
2	WEB-Profile	Integer	WEB profile value: 1 Administrator 2 Maintenance 3 Readonly 4 None

For an example of Radius server configuration, see Appendix **Błąd! Nie można odnaleźć źródła odwołania..**

Password Management



The screenshot shows a web form titled "Password Management". It contains three input fields on the left: "Username:" with a dropdown menu showing "administrator", "New password:" with a masked password field (two dots), and "Confirm password:" with an empty text field. To the right of these fields are two buttons: "Reset password for the selected user" and "Apply".

Password management is accessible to all users.

By default (e.g. at account creation) the account password is identical to the account name. All users are strongly recommended to change their password at their first Command Line Interface or WEB session.

An administrator can reset any non-administrator account password to its defaults value, which is the account name.

Procedures

To modify your own password (accessible to all users):

1. In the list box, select your account.
2. Type the new password. Passwords are case sensitive.
3. Confirm the new password in the confirmation field.
4. Click *Apply*.

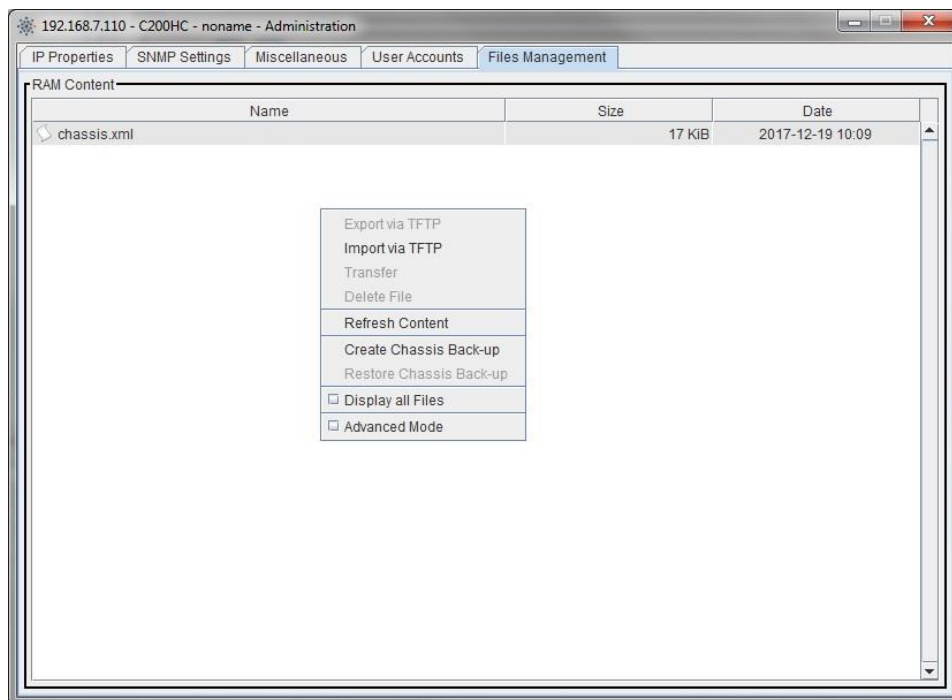
To reset a password to the default (administrator only):

1. In the list box, select one account.
2. Click *Reset*
3. Confirm the password reset.

End

File Management

The *File Management* panel provides several file and configuration management facilities through shortcut menus that pop up on a right mouse click (figure below).



The shortcut menus include the *Display All Files* and *Advanced Mode* options that the following paragraphs first introduce.

Default Display

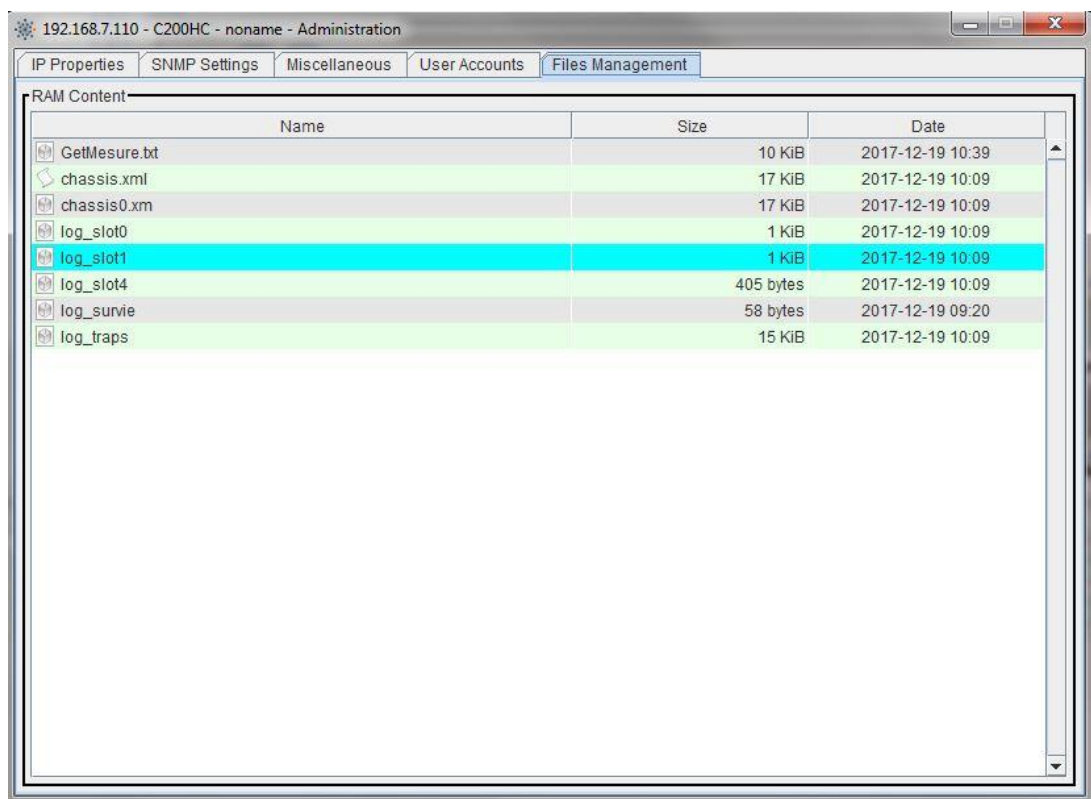
By default, only the configuration files located in RAM are displayed.

Display All Files

Use *Display All Files* to display all the files located in RAM.

Note: if the *Advanced Mode* is active, *Display All Files* also apply to the *Other Locations* panel (refer to next sub-section).

Figure below shows the *File Management* panel while only the *Display All Files* mode is active.



Name	Size	Date
GetMeasure.txt	10 KiB	2017-12-19 10:39
chassis.xml	17 KiB	2017-12-19 10:09
chassis0.xml	17 KiB	2017-12-19 10:09
log_slot0	1 KiB	2017-12-19 10:09
log_slot1	1 KiB	2017-12-19 10:09
log_slot4	405 bytes	2017-12-19 10:09
log_survie	58 bytes	2017-12-19 09:20
log_traps	15 KiB	2017-12-19 10:09

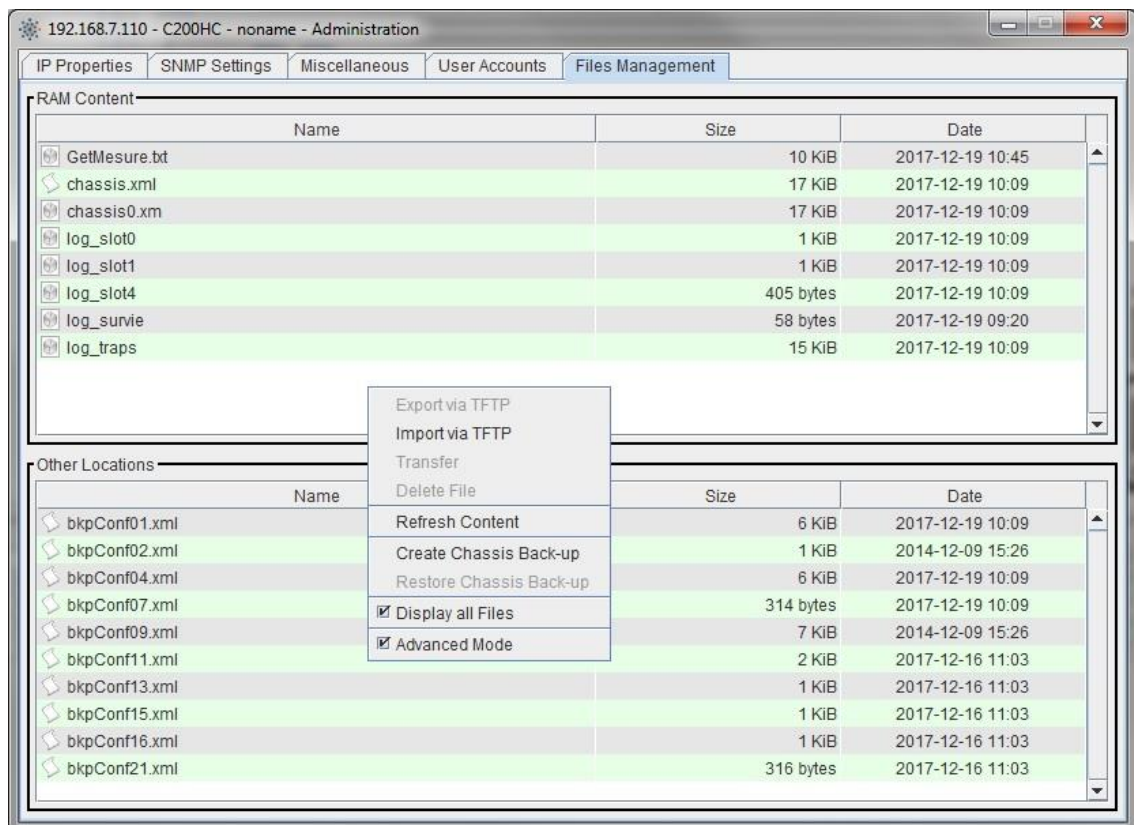
Advanced Mode

Use *Advanced Mode* to display a second panel that relates to other locations, which can be:

- CONF partition (default)
- or SCRIPT partition

A right mouse click within the *Other Location* panel allows you to access a dedicated shortcut menu. In this menu, use the *Location* option to select the partition that you want to display the content.

Figure below shows the *Other Locations* panel and the dedicated shortcut menu.



Note: the *Display All Files* mode must be active to display the script files.

Managing Files in the "RAM Content" Panel

From the *RAM Content* panel, you can:

- Export a file you have selected to a PC using *Export via TFTP*
- Import a file from a PC using *Import via TFTP*
- Transfer a configuration file from RAM to CONF partition using *Transfer* (the Extended Mode must be active and the CONF location must be selected)
- Transfer a script file from RAM to SCRIPT partition using *Transfer* (the Extended Mode must be active and the SCRIPT location must be selected)
- Delete the selected file using *Delete File*

Managing Files in the "Other Locations" Panel

From the *Other Locations* panel, you can:

- Transfer a file to RAM using *Transfer*
- Delete the selected file using *Delete File*

Create Chassis Backup

The *Create Chassis Backup* option provides the operator with a convenient way to gather all module configurations in a single configuration file named "chassis.xml".

Procedure

To backup the full-chassis configuration:

1. From the *RAM Content* panel, open the shortcut menu by a right mouse click.
2. Select *Create Chassis Backup*.
3. Answer the questions related to port configurations that pop up on the screen

Note: *Always/Never* are equivalent to *Yes/No*.

Three cases may occur:

- The port configuration already exists. Confirm if you want to update the configuration file.
 - There is no configuration file. Confirm if you want to create the configuration file.
 - The configuration file does not correspond to the module type. Confirm if you want to create a new configuration file.
4. Wait for the end of the chassis backup.

When the backup is complete, the chassis configuration file appears in the file list.

End

Restore Chassis Backup

The *Restore Chassis Backup* option requires that a "chassis.xml" already exists in the file list of the RAM Content panel.

Procedure

To restore a full-chassis configuration:

1. From the *RAM Content* panel, open the shortcut menu by a right mouse click.
2. Select *Restore Chassis Backup* (requires that a chassis configuration file exists).
3. Answer the questions that pop up on the screen.

Note: *Always/Never* are equivalent to *Yes/No*.

The following cases may occur:

- The module configuration already exists. Confirm if you want to overwrite the configuration file.
 - There is no configuration file. Confirm if you want to create the configuration file.
 - The configuration is not compatible with the equipment type. This message is for information only.
4. Answer the question related to the TRANS module reset (example below).



5. Answer the question related to the MGNT module reset (figure below).



The full-chassis configuration restore is complete.

End

Get PM Configuration

The *Get PM Configuration* option allows the user to save the current configuration:

- of a PM in a modular chassis
- of the TRANS module in an all-integrated chassis

Procedure

To save the current configuration:

1. From the *Other Locations* panel displaying the CONF partition content, open the shortcut menu by a right mouse click.
2. Select *Get PM Configuration*.
3. In the selection box that pops up on the screen (example below, in a modular chassis), select the slot and click *OK*.

End

Advanced Administration

The Rapid Spanning Tree Protocol (RSTP) can be used to prevent Ethernet data loops from forming by ensuring that only one path exists between the end nodes in a network.

If RSTP is enabled, use the *Advanced Administration* menu option to display the different Ethernet ports and their RSTP statuses (example below).

Note: The *Advanced Administration* feature uses TCP port 4010, which must be open.

If RSTP is disabled, the *Advanced Administration* window is empty.

Refer to section 0 relating to MGNT configuration to enable/disable RSTP.

Alarm Management

This chapter describes colored indicators and alarm management. Colored indicators provide the user with a quick view on possible alarms and their level of severity. The content of this chapter applies to all modules.

Alarm Level Indicators

Three alarm level indicators, visible in the equipment tree as well as in the equipment snapshot, offer a quick view on alarms. They signal if any critical, major or minor alarm is currently active in any part of the equipment, including MGNT, TRANS, and FAN modules.

The three alarm level indicators summarize the equipment operational status:

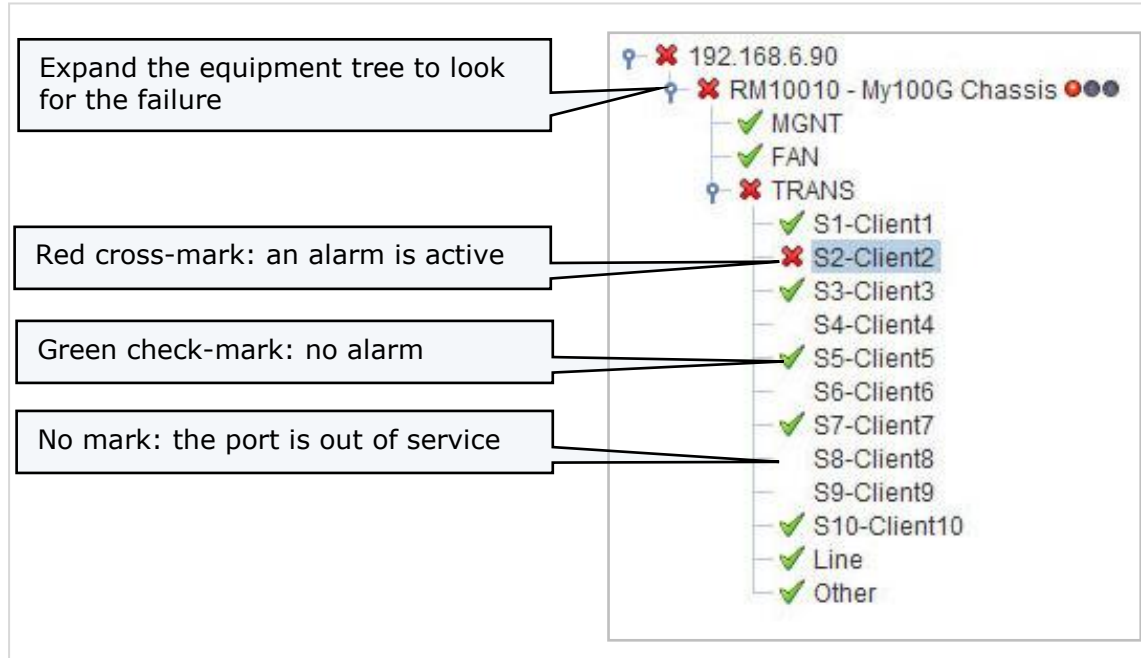
- All of them are off: no alarm detected.
- The yellow indicator is on: at least one minor alarm is active.
- The orange indicator is on: at least one major alarm is active.
- The red indicator is on: at least one critical alarm is active.



Alarm level Indicators: detail of the snapshot view

Alarm Marks in the Equipment Tree

When an alarm occurs, expand the equipment tree items to look for the red cross-marks that signal failures.



Alarm Marks in the Equipment Tree

Alarm Panel

After you have located a faulty element, open the relating alarm panel by double clicking on this element (or use the *Alarm* shortcut via a right click).

Alarm Color Meanings

Alarm panels display several types of statuses:

- Alarm statuses are the most important. The traffic might be affected.
- Other statuses inform you of problems that do not affect traffic (warnings).

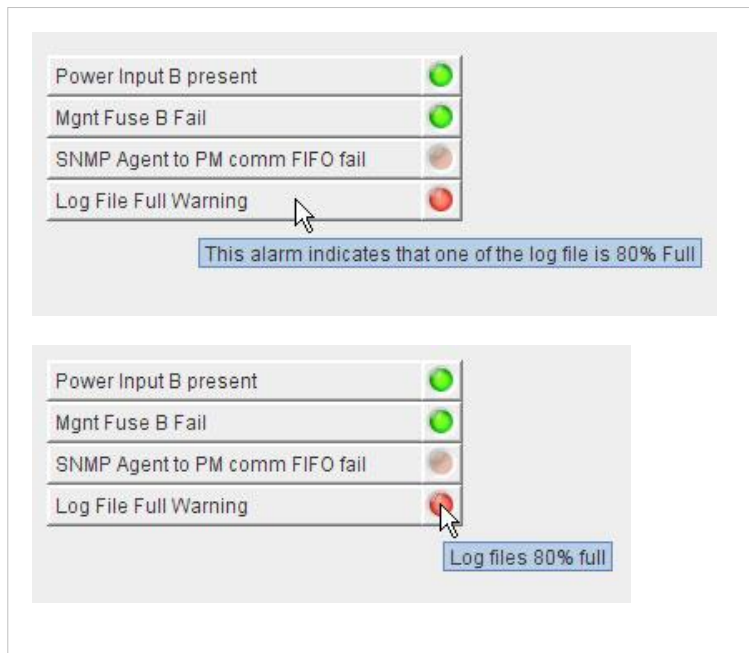
Table below list the different color meanings.

Alarm status	No alarm	Bright green
	Alarm detected	Bright red
Presence status	Absent	Bright red
	Present	Soft red
Activity status	Active	Bright green
	Not active	Soft green

More Information with Tooltips

You can obtain more information by positioning the mouse pointer as shown in figure below:

- Place the mouse pointer over the alarm label to display the detailed label (after a short delay).
- Place the mouse pointer over the colored indicator to display the current status (after a short delay).



How to display alarm tooltips

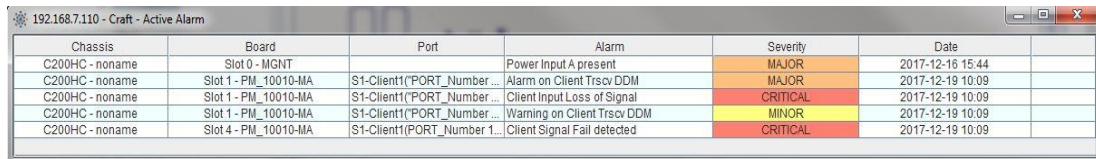
Note

As an alternative, you can obtain additional information on alarm labels and statuses by using the context-sensitive help. Refer to section 0 relating to the Dynamic Help feature.

Alarm Listing

The Alarm Listing, located at the bottom of the main window, shows a comprehensive view of active alarms on all equipment components, which helps alarm correlation.

You can detach the Alarm listing in an independent window to keep it all the time visible (refer to the *Detach View* option, section 0).



Chassis	Board	Port	Alarm	Severity	Date
C200HC - noname	Slot 0 - MGNT		Power Input A present	MAJOR	2017-12-16 15:44
C200HC - noname	Slot 1 - PM_10010-MA	S1-Client1(PORT_Number...	Alarm on Client Trscv DDM	MAJOR	2017-12-19 10:09
C200HC - noname	Slot 1 - PM_10010-MA	S1-Client1(PORT_Number...	Client Input Loss of Signal	CRITICAL	2017-12-19 10:09
C200HC - noname	Slot 1 - PM_10010-MA	S1-Client1(PORT_Number...	Warning on Client Trscv DDM	MINOR	2017-12-19 10:09
C200HC - noname	Slot 4 - PM_10010-MA	S1-Client1(PORT_Number 1...	Client Signal Fail detected	CRITICAL	2017-12-19 10:09

Alarm Listing in a Detached Window

Correlation of alarms

When an alarm occurs, check whether other alarms are also active. This may help you to identify the real cause of alarms.

For example, if a "Fuse B fail" alarm occurs on a service PM (modular chassis) or on the TRANS module (all-integrated chassis) check first the alarms of the MGNT module. If the "Power input B" alarm is active, the problem is probably there. If this is the case, the "Fuse B fail" alarm is only a result of the "Power input B" failure.

MGNT Module Management

This chapter describes the management tasks that are specific to the MGNT module.

MGNT Module and Chassis Types

The MGNT module is:

- case of a modular chassis: a pluggable unit inserted in a slot (MGNT4)
- case of an all-integrated chassis: a functional unit

In both cases, you manage the MGNT module exactly in the same way.

MGNT Management Window

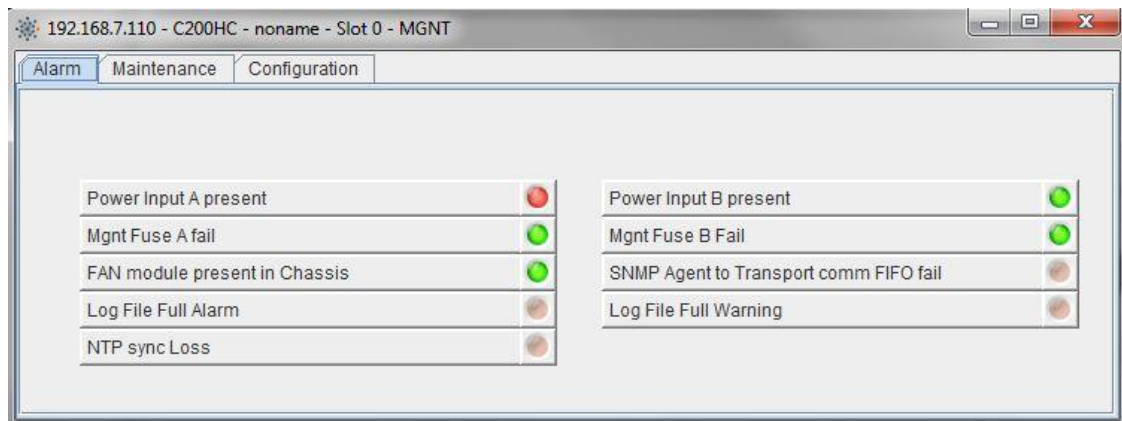
To open the MGNT management window, navigate through the *Equipment Tree* and double-click the MGNT item. You can also right-click the MGNT item to open the shortcut menu which provides you with direct access to the management panels.

The MGNT management window consists of three tab panels:

- An alarm panel
- A maintenance panel
- A configuration panel

MGNT Alarm Panel

The alarm panel lists potential alarms related to the MGNT module. Colored indicators show the alarm statuses.

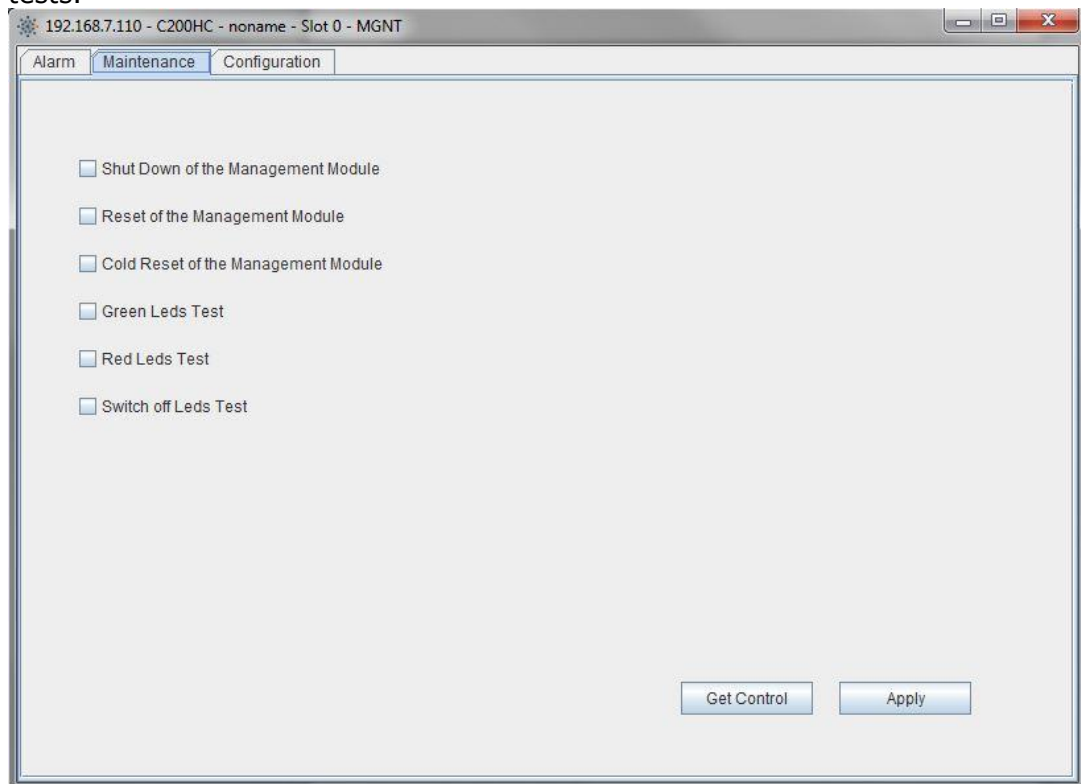


View of the MGNT Module Alarms

Refer to the current equipment *Documentation* for details on MGNT alarms.

MGNT Maintenance Panel

The Maintenance panel gives access to maintenance actions only, such as MGNT module reset and led tests.



Maintenance Panel of an MGNT Module

The maintenance panel contains several checkboxes.

Procedure

To perform an action:

1. First click *Get control* to update the checkboxes with the current settings.
2. Modify the settings.
3. Click *Apply*.

You can check that the modifications have been taken into account by clicking *Get control* a second time.

End

Available Actions

The following actions are available:

- **Shutdown of the Management Module.** Use the shutdown checkbox to shut the chassis down properly, for example before turning off the power for transport.
A 5-minute timer is launched as the MGNT module enters the shutdown mode. The chassis should be powered down during this period of time. If not, the MGNT module restarts automatically at timer expiration. Refer to the current equipment *Documentation* for details.
- **Reset of the Management Module.** This performs a warm reset of the MGNT module. It does not affect the traffic and needs from 35 seconds to several minutes to complete. Refer to the current equipment *Documentation* for details.
- **Cold reset of the Management Module.** A cold reset reloads the management module software and configuration, and clears all logs and alarms. It does not affect the traffic and needs from 35 seconds to several minutes to complete. Refer to the current equipment *Documentation* for details.
- **Green LED test.** This test allows you to check that the SW controllable LEDs of all boards turn green for 10 seconds.
- **Red LED test.** This test allows you to check that the SW controllable LEDs of all boards turn red for 10 seconds.
- **Switch-off LED test.** This test allows you to check that the SW controllable LEDs of all boards switch off for 10 seconds.

MGNT Configuration Panel

The configuration panel allows the user to manage several parameters and the traps. You can display traps by using the Command Line interface or a traps manager.

Configuration options are stored in non-volatile memory. They remain valid after a reset.

Configuration Panel of an MGNT Module

The configuration panel contains several options.

Procedure

To perform an action:

1. First click *Get Config* to update the checkboxes with the current settings.
2. Modify the settings.
3. Click *Apply*. This saves the configuration.

A message offers you an immediate reset with the new settings. Click *Yes* for an automatic reset. Click *No* if you prefer to reset the MGNT module manually later. MGNT reset does not affect traffic.

End

Available Options

The following options are available:

- **XXXXXX Traps Enable.** Check these options to filter the traps that are stored in the log_traps file (detailed mode only).
- **MGNT XXXXX Traps Enable.** Check these options to filter the traps that are stored in the log_traps file (detailed mode only).
- **Traps Mode.** Traps are stored in the log_traps file according to one of the following modes:
 - The synthetic mode, which only gives Port Up or Port Down status.
 - The detailed mode, which provides detailed and explicit labels.
 - The NMS mode which is to be used together with the MICROSENS NMS called MPSN (Multi Protocol and Service Network) manager.

Use the selection list to select the desired trap mode.

- **CLI Access.** Use the selection list to specify the way the Command Line Interface (CLI) can be accessed remotely.
- **RSTP Enable.** The Rapid Spanning Tree Protocol (RSTP) can be used to prevent data loops from forming by ensuring that only one path exists between the Ethernet ports. Check this option to enable RSTP.
- **Log Mode.** In Linear mode, the logs are not stored anymore once the log file is full (LIFO mode). In Rotate mode, once the log file is full, a new log replaces the oldest log entry (FIFO mode).
- **Node Controller Mode.** Enable the node controller feature. This feature enables automatically RSTP and LLDP feature.
- **Restrict Unprivileged Users Rights.** Prevent the users which are not administrator to change their own password.
- **OSC/DCC Link Up Threshold.** Define the time a OSC/DCC link must be bidirectional before being declared up (linked to RSTP feature).
- **OSC/DCC Link Down Threshold.** Define the time an OSC/DCC link can be unidirectional before being declared down (linked to RSTP feature).
- **Account Auto-Lock.** Define the number of error password to lock an account. This counter is reset on successful login or after administrator defines period(see fail counter reset) Set to -1 to disable function.
- **Fail Count Reset** Define the minimum in hours to reset failed login counter. This counter is also reset on successful login. Set to -1 to disable function.

PM Module/TRANS Management

This chapter introduces you with the management principles of the service modules which can be, depending on the chassis type, a set of PMs or a TRANS module.

PM/TRANS Management Window

To open a PM/TRANS management window:

- From the *Equipment Tree*, double-click the desired item. You can also right-click the item to open the shortcut menu which provides you with direct access to the management panels.
- From the *Equipment Snapshot*, you can access directly some management panels such as port management by double-clicking the available hotspots.

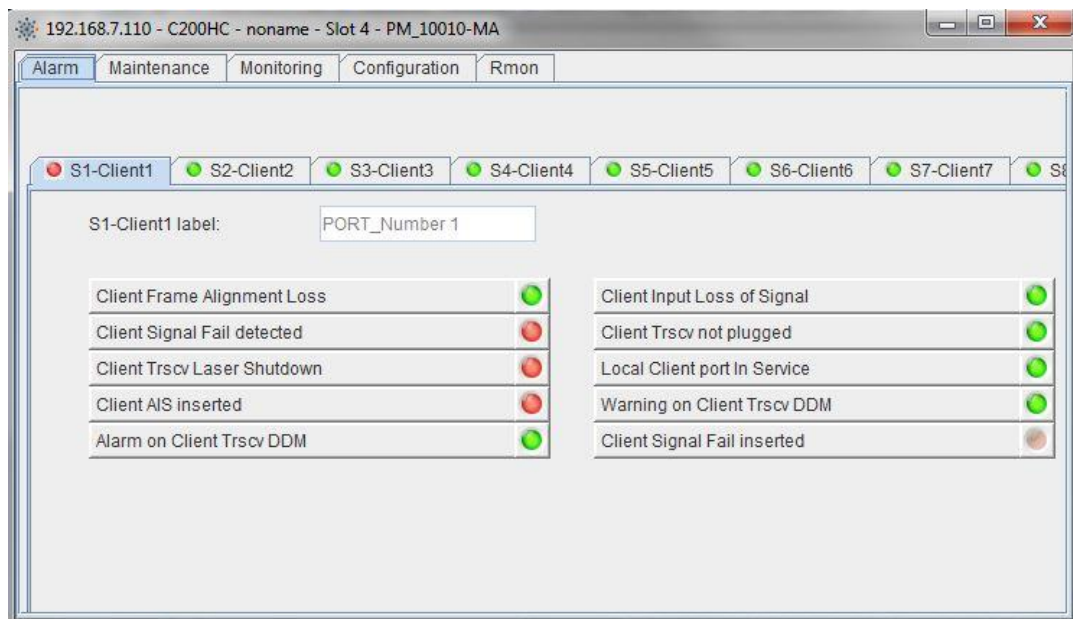
The PM/TRANS management window consists of several tab panels, some of them being specific to certain services.

The available tabs are:

- The Alarm panel
- The Maintenance panel
- The Monitoring panel
- The Configuration panel
- The Perf panel
- The Rmon panel

PM/TRANS Alarm Panel

The alarm panel lists potential alarms related to the current TRANS, including line and ports.

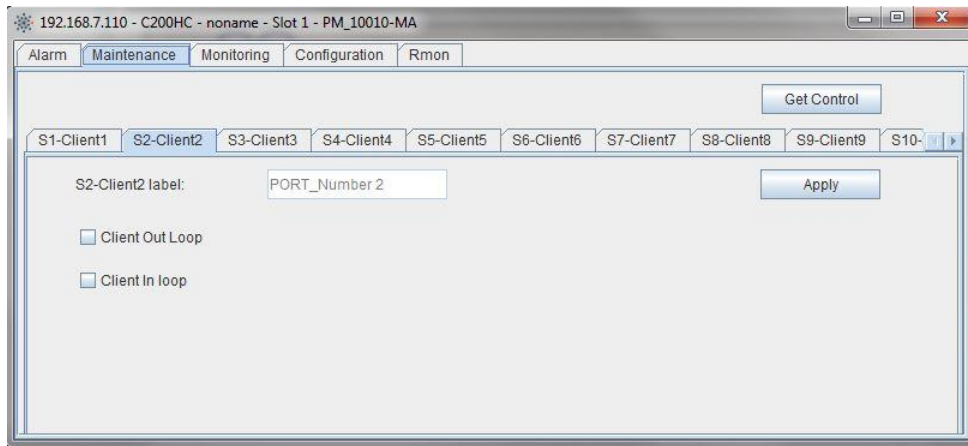


Alarm Panel

To obtain more information on an alarm, refer to the related PM *Documentation* or to the related MXP100 chassis *Documentation*, that describe alarms, probable causes and corrective actions.

PM/TRANS Maintenance Panel

The Maintenance panel gives access to maintenance actions including client port loops, line port loops and module reset.



Maintenance panel

How to reset a PM/TRANS module

Two types of reset are available:

- **Warm reset.** A warm reset reloads software into operational memory. A warm reset does not affect traffic.
- **Cold reset.** A cold reset reloads software and gateway, and restarts the configuration. A cold reset causes a service interruption lasting several minutes.

Procedure

To reset a PM/TRANS module:

1. Select the *Maintenance* tab.
2. Select the *Other* tab.
3. According to the reset you want to perform, Click *Warm Reset* or *Cold Reset*.

The equipment tree view and the equipment snapshot view automatically update to show that the module reset is in progress.

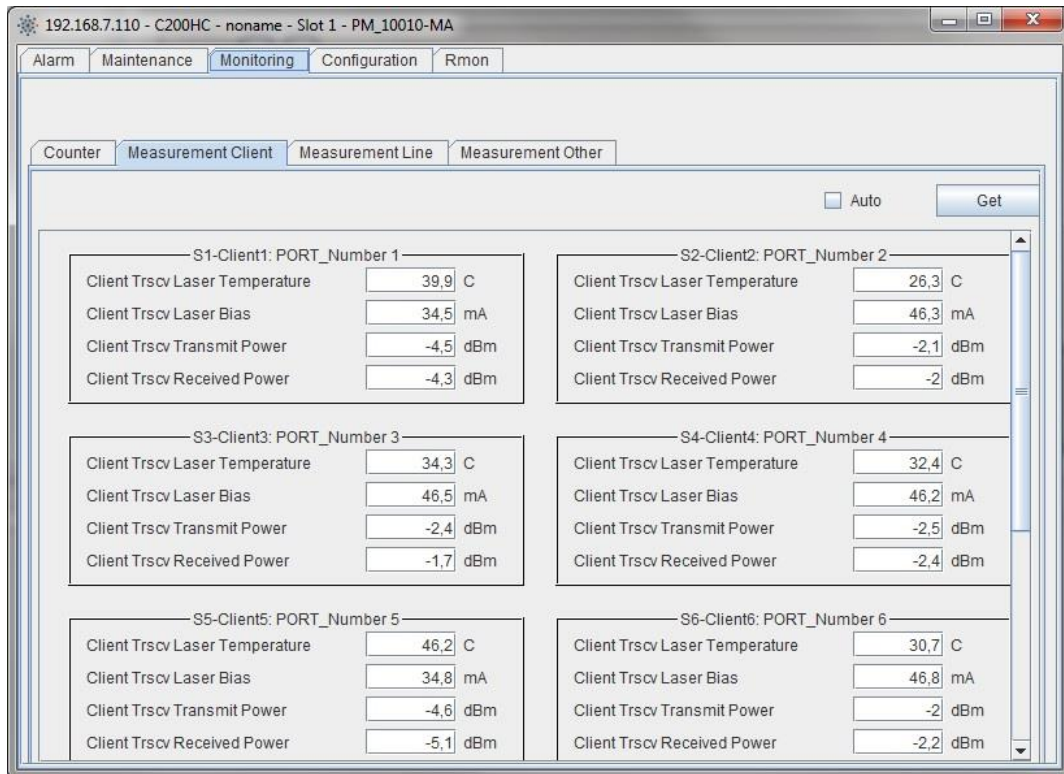


4. When the reset is complete, the module is normally displayed in the equipment tree and equipment snapshot views.

End

PM/TRANS Monitoring Panel

The monitoring panel consists of several sub-panels.



Monitoring panel

Counter sub-panel

In the *Counter* sub-panel:

- Click *Get* to display the current counter values.
- Check the *Auto* option and click *Get* to observe the evolution of the counters on a period of time.
- Click the *Reset* command button to clear the counters.
- Check/uncheck *Rate* to switch between rate and counting display.

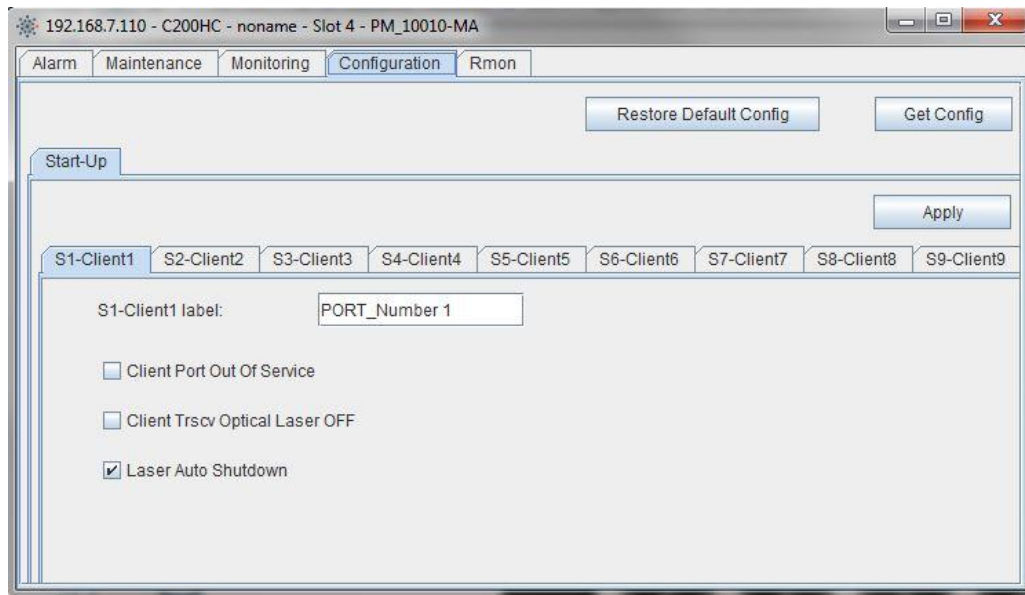
Measurement sub-panel (client, line or other)

In a *Measurement* sub-panel:

- Click *Get* to display the measurements.
- Check the *Auto* option and click *Get* to observe the evolution of the measurements on a period of time.

PM/TRANS Configuration Panel

The configuration panel allows you to configure the client and line port settings. Configuration settings are stored in non-volatile memory. They remain valid after a reset.



Configuration panel

Generic buttons

The *Get Config* button displays the current configuration.

The *Restore Default Config* button reinitializes the configuration with the default settings. This requires a PM/TRANS cold reset.

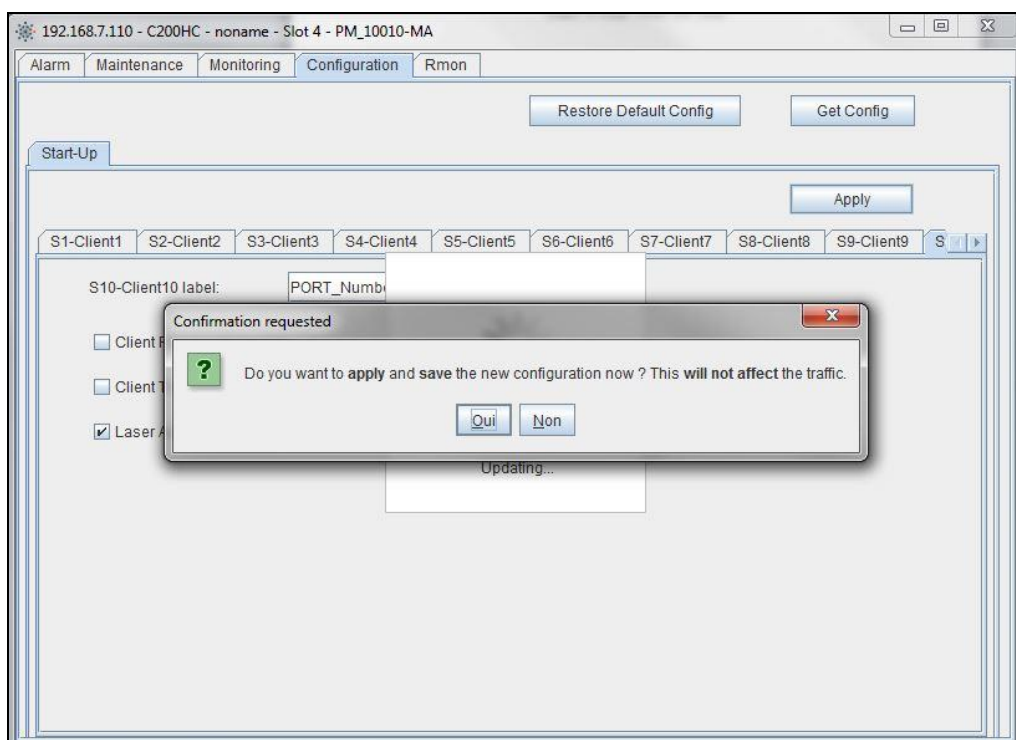
Configuration modification

Procedure

To modify the start-up settings:

1. In the *Configuration* panel, select the *Start-Up* tab.
2. Select the desired ports and modify their settings.
3. To save and apply all port settings, click *Apply*.

A pop-up message dialog box requests for a confirmation. This message specifies whether applying the configuration affects the traffic or not.



4. Press Yes to save and apply the new configuration.

Note: pressing *No* leaves the configuration unchanged.

End

Performance Panel

Depending on their types, some PMs provide performance statistics, which can be Telecom statistics (TDM interfaces) or Datacom statistics (packet based interfaces). In this context, a *Perf* tab allows the user to display the performance counters.

S3-Client1 S4-Client2 S2-Client3 S6-Line2					
Get Reset		15-min Elapsed Time (s) 230		24-hours Elapsed Time (s) 54229	
Period	Input Bytes	Input CRC	Input Broadcast	Input Multicast	Input Unicast
Current 24-hours	2410629924000	0	3214173232	0	0
24-hours History 1	0	0	0	0	0
24-hours History 2	0	0	0	0	0
Current 15-minutes	27881428500	0	37175238	0	0
15-minutes History 1	109578996750	0	146105329	0	0
15-minutes History 2	109701035250	0	146268047	0	0
15-minutes History 3	109456853250	0	145942471	0	0
15-minutes History 4	109576642500	0	146102190	0	0
15-minutes History 5	109581346500	0	146108462	0	0
15-minutes History 6	109578975750	0	146105301	0	0
15-minutes History 7	109578975000	0	146105300	0	0
15-minutes History 8	109575486000	0	146100648	0	0
15-minutes History 9	109582461750	0	146109949	0	0
15-minutes History 10	109578936000	0	146105248	0	0
15-minutes History 11	109579018500	0	146105358	0	0
15-minutes History 12	109574879250	0	146099839	0	0
15-minutes History 13	109583037750	0	146110717	0	0
15-minutes History 14	109579016250	0	146105355	0	0
15-minutes History 15	109578978750	0	146105305	0	0
15-minutes History 16	109578978750	0	146105305	0	0
15-minutes History 17	109578937500	0	146105250	0	0
15-minutes History 18	109579009500	0	146105346	0	0
15-minutes History 19	109457635750	0	145942381	0	0

Perf Panel

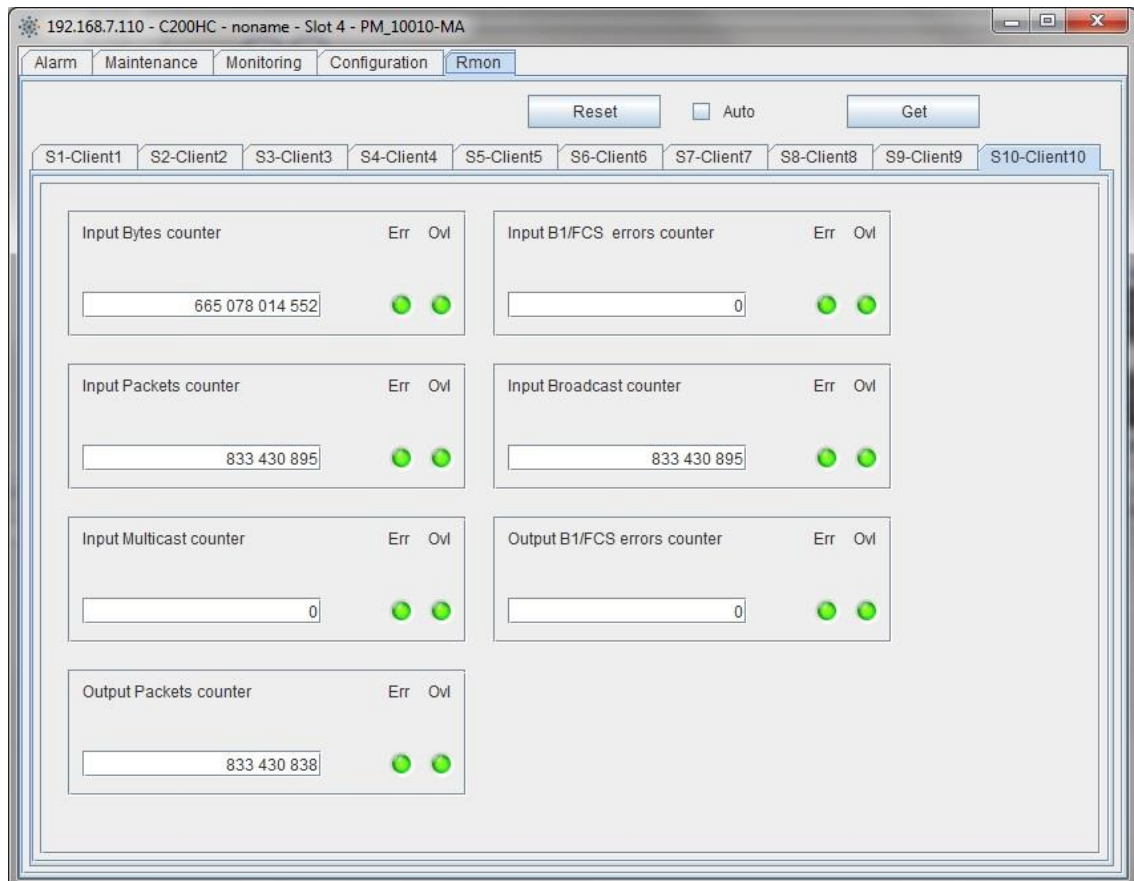
Actions Available

Click *Get* to refresh the displayed counters.

Click *Reset* to reset the counters.

Rmon Panel

Use the *Rmon* panel to display Remote Network Monitoring counters.



Rmon panel

Actions Available

Click *Reset* to reset the counters.

Click *Get* to refresh the counter values manually.

Check *Auto* and click *Get* to enable automatic polling.

FAN Module Management

This chapter briefly describes the FAN module management principles.

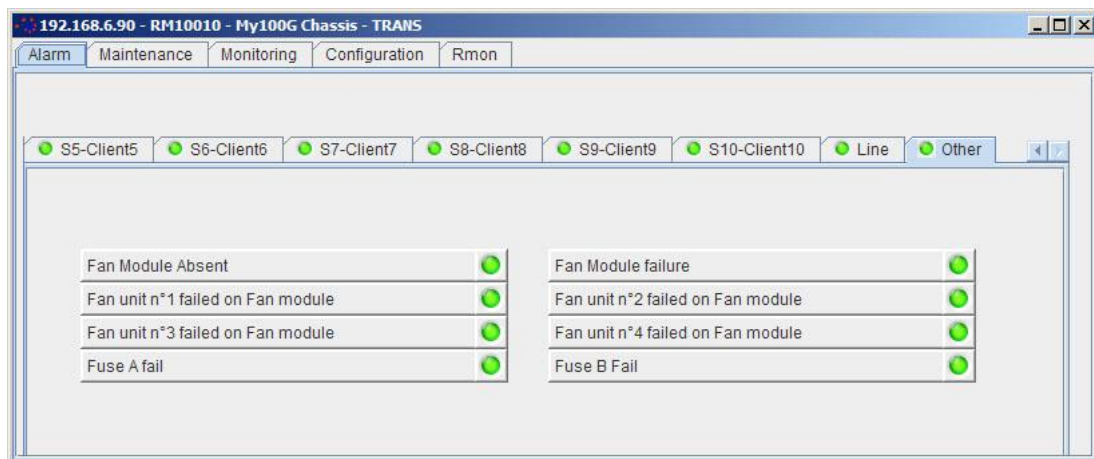
FAN module and Chassis Types

Depending on the chassis type, the FAN module is:

- case of a HC modular chassis: a standard pluggable module (PM)
- case of a non HC modular chassis: a pluggable unit
- case of an all-integrated chassis: a pluggable unit

FAN Management Window

To open the FAN management window, double-click the FAN item in the *Equipment Tree*.



FAN alarm panel (MXP100)