Xcor Admin User Guide

Xcor-ADUG-v.1.0.5

8/15/2010

This document details the functions and operation of the Xcor Admin program. The Xcor Admin program is used to control administrative tasks as well as to configure system settings and parameters that cannot be set using the Xcor Client program.

Table of Contents

Overview

The Xcor Admin program is companion software to the Xcor Client program. The Xcor Client is designed for use post-setup; to access the Hunter System, and its data and statistics related to occurrences of CPD, Ingress, and impairments within the network. Functionality related to system setup, administration, database auditing, and changes to system parameters such as threshold levels and FSK carrier frequency does not exist within the Xcor Client as these are not “user” tasks.

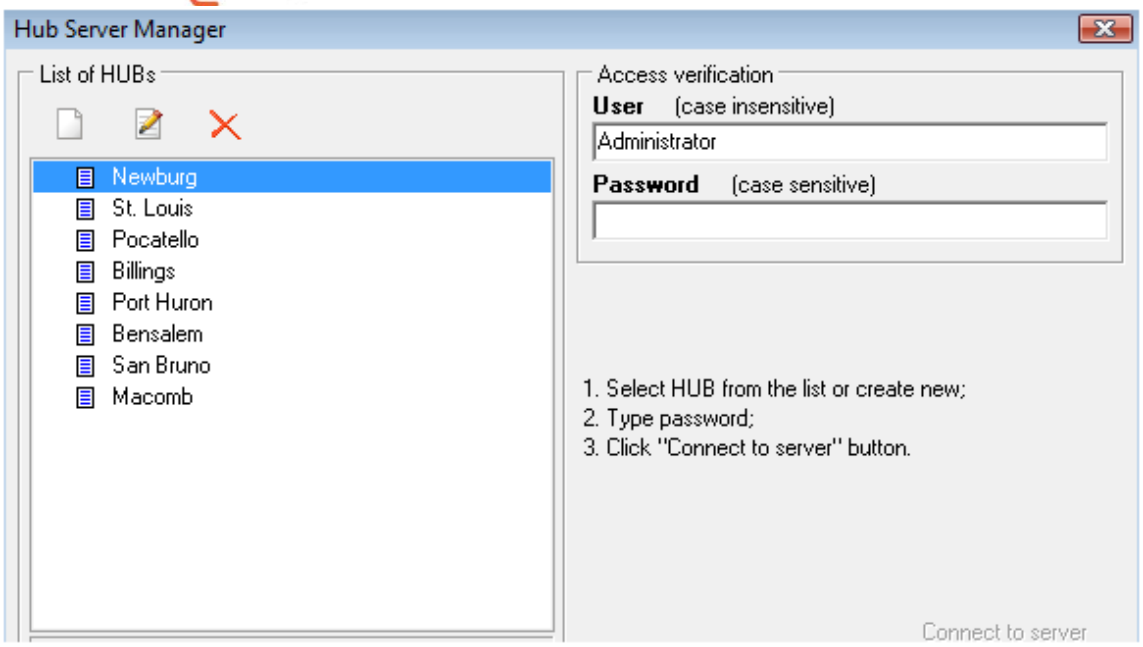
Access to these types of features is available only through the Xcor Admin program. The purpose of the program separation is to ensure that changes to important parameters are only made by administrators that have been provided access to the software.

Startup

The program can be started by clicking on Xcor Admin icon on your desktop. The following screen will appear. For information on how to load the Xcor Administrator program please contact your Arcom Digital representative.

Select Hub / Create new Hub

The next step is to select an established hub or create a new hub by entering its name and appropriate IP address. Click the **Connect to server** icon to connect to the hub server, the following screen will appear.

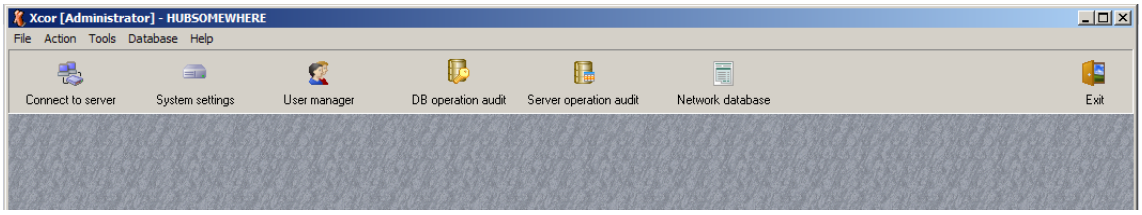


To enter a new hub, click the new hub icon. 

To edit an existing hub click on hub and then select the edit icon. 

After selecting the hub name enter the user name and password then click OK.

The following Xcor Admin main screen will appear.

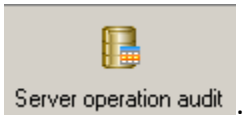


Basic functions

The basic functions of the Administrator are to connect to the Hunter Server program and to set initial or important parameters of the hardware and the software of the system. The program allows the administrator to create user accounts that will let them

connect to the system database using the Xcor Client program. The Hunter users who are allowed to access the Xcor Admin must have accounts created with user name: Administrator.

The system additionally has tools that prevent losing important i-scout probe location data, scan intervals and calibration data. Data can be saved in backup files which can be sent to MHV server for backup. Always create the backup data as i-scout probe locations, fiber node calibrations and adjusting scan intervals are time and labor consuming tasks.

All server actions are monitored and information about its action is available via 

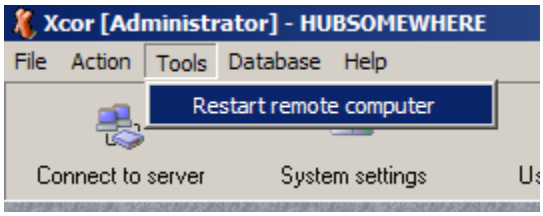
.

The user actions are also monitored. Details related to connecting with the Client or Admin is registered together with information about changes in system parameters. That data can be viewed here: 

.

Remote PC restart

In case there is a problem with the spectrum analyzer or the radar device, or any other situation where the remote server should be restarted, use the following option accessible via Tools menu:



How does it work

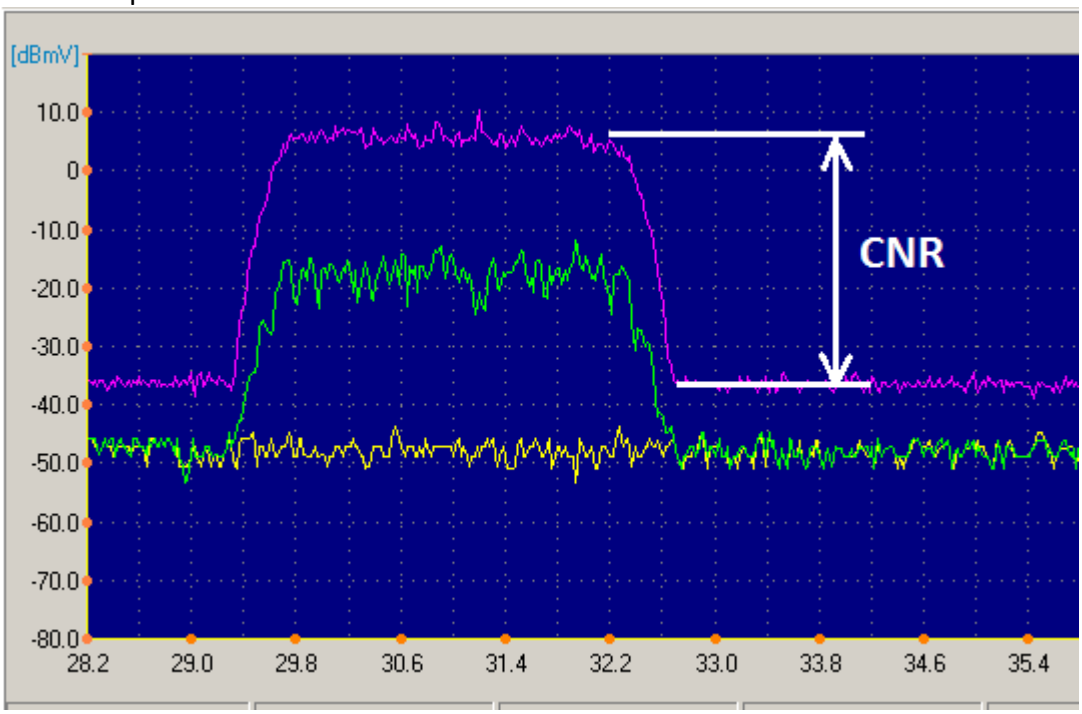
Below you will find brief information on how the CNR is measured, and how Impulse noise and laser clipping are detected.

CNR/CNIR measurement

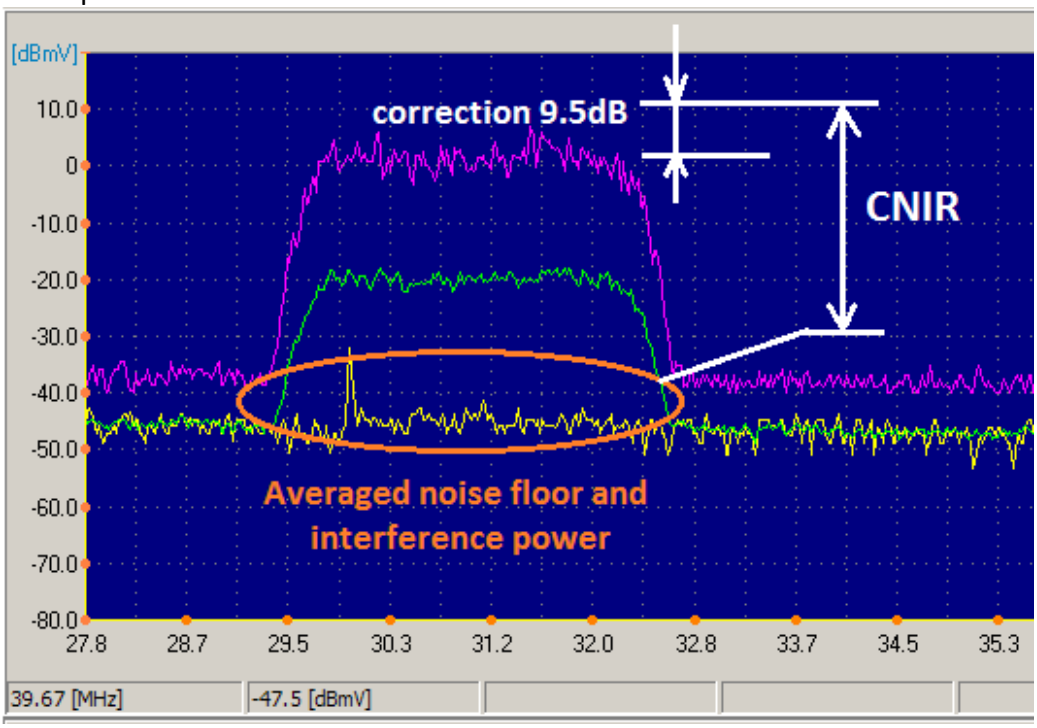
The spectrum analyzer used in the Hunter system can operate to 70MHz or to 120MHz depending on hardware version. Both units are built into the single 1 RU chassis together with the radar. This real time FFT spectrum analyzer with 2048 resolution points provides excellent signal analysis detail.

The firmware of the spectrum analyzer is capable of reading the CNR parameter of the return path data carriers. When the noise floor under the QAM carrier is free of peak type interferences, the displayed CNR is accurately termed and described as CNR.

CNR example for RBW 30kHz:



CNIR example for RBW 30kHz:



If a peak-like interference is present under the QAM data carrier, the displayed CNR is more accurately described as CNIR (Carrier to Noise + Interference Ratio). Note: power of the QAM carrier and the power of the noise floor + interference power under the QAM channels are used in calculations.

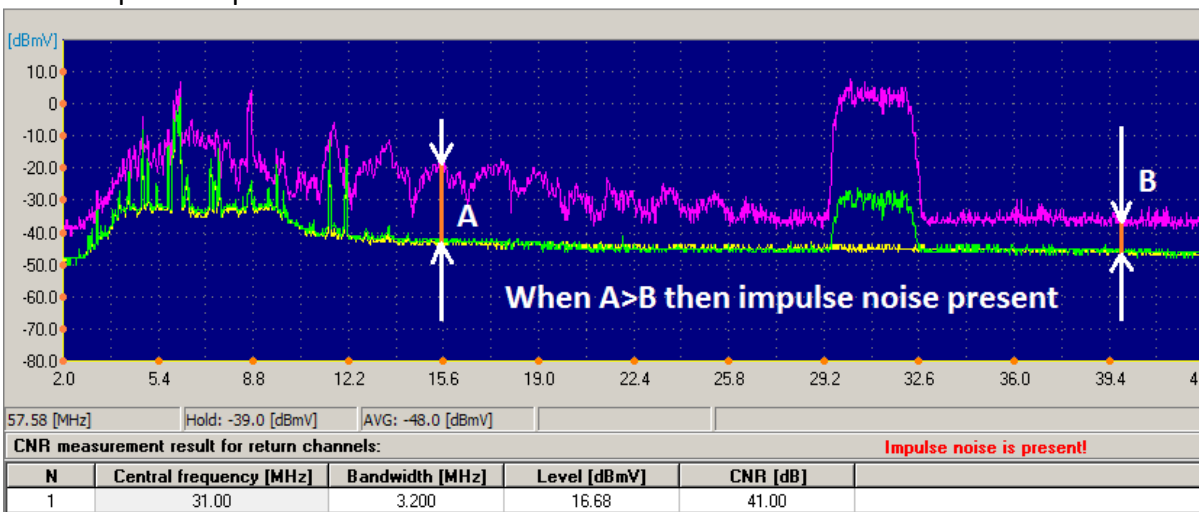
CNR calculations are made using the average QAM signal signatures of the most recent 20 modem signals records for each central frequency. Then required RBW is used for calculating actual CNR.

Impulse noise detection

The impulse noise can be easily recognized by the Hunter spectrum analyzer. By simultaneous measurement of signal level at 400 points with 256 scans per second, the variations of the signal max hold and average traces can be detected.

The Impulse noise condition is alarmed once the difference between noise max hold and average levels reach 20dB in different parts of the spectrum between 5 MHz and the lowest frequency QAM.

Graphical explanation:

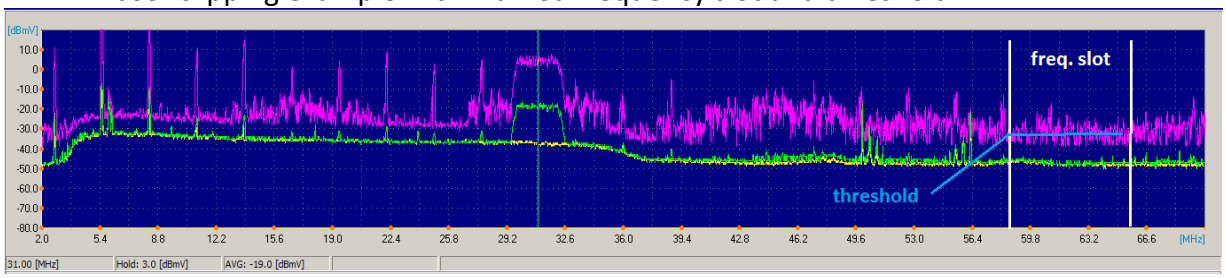


N	Central frequency [MHz]	Bandwidth [MHz]	Level [dBmV]	CNR [dB]
1	31.00	3.200	16.68	41.00

Laser clipping detection

Laser clipping is detected by checking a selected frequency band for signals reaching certain threshold levels. Once the threshold is reached, the laser clipping alarm condition is indicated. The alarming frequency band must be selected above the regular return path band.

A laser clipping example with marked frequency slot and threshold:

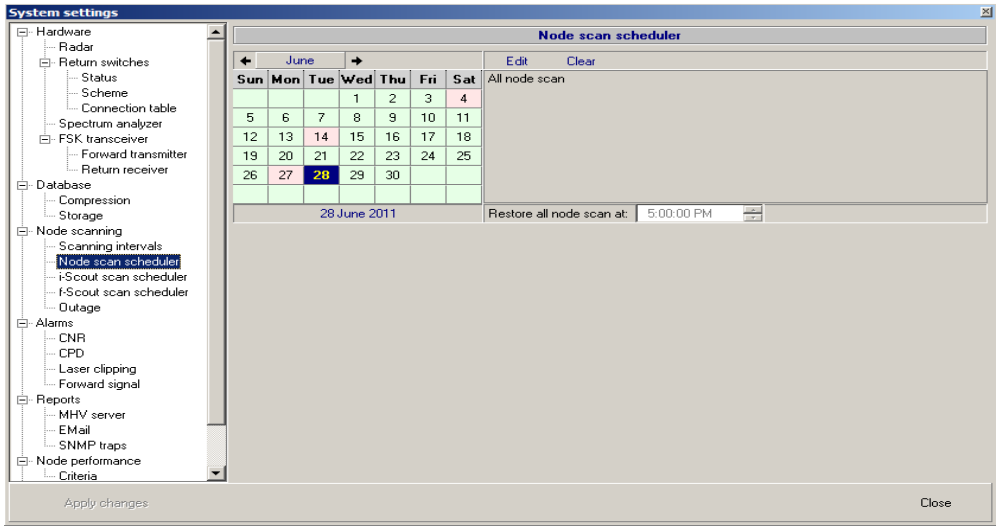


System settings

The system settings window can be open by clicking on the toolbar **System settings** icon. The screen with system setting tabs for various hardware and software adjustments will open at the Node Scan Scheduler tab.

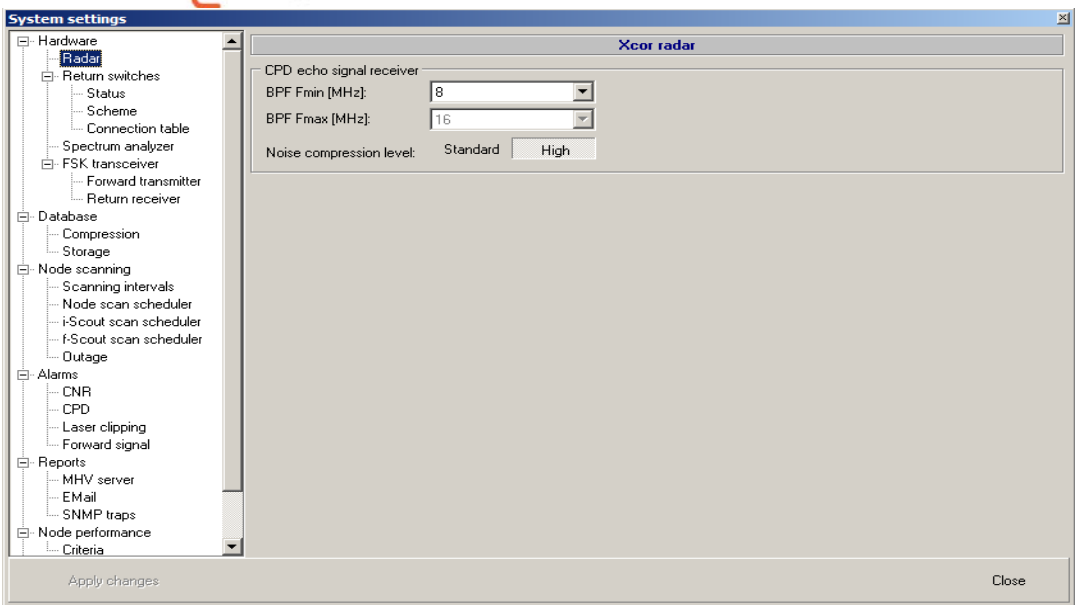
Hardware and software

Various settings items are listed in a form of a directory on the left hand side of the screen. Access to each item is achieved by left mouse click on the name of the item.



Xcor Radar

This tab provides access to important hardware settings. These parameters should be changed only by an administrator and double checked before any changes are saved.



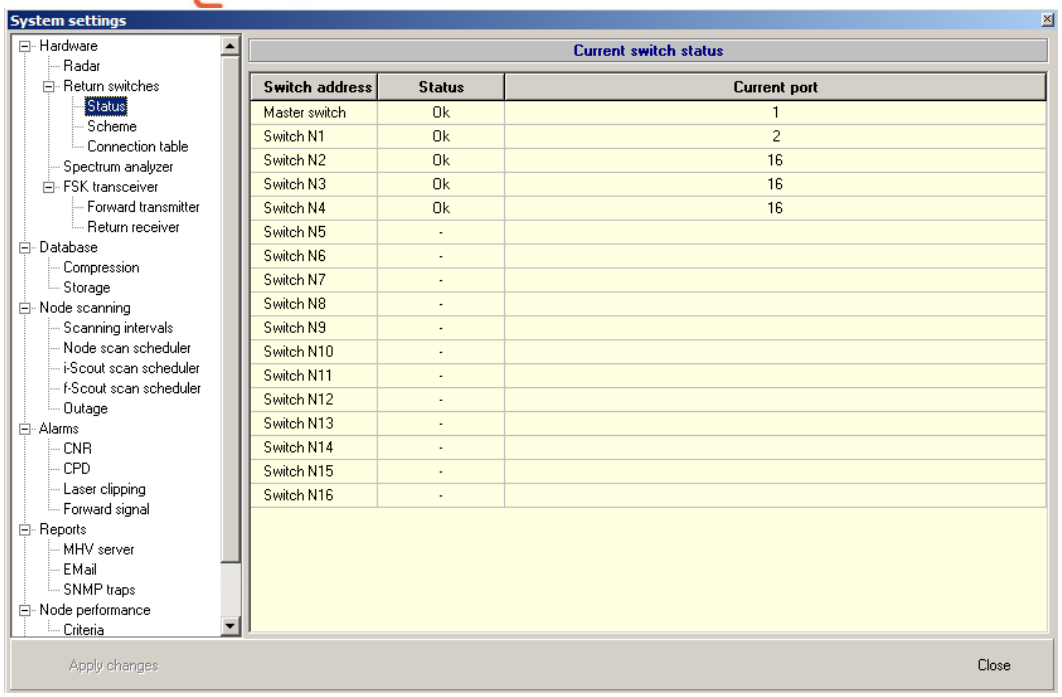
The CPD radar is equipped with a variable bandpass filter. The user can utilize this bandpass filter to select a frequency band which is not affected by strong CW-like carriers that disturb correlation processing of the signals. The lower frequency of the filter band can be switched between 8,9,10.5 and 12MHz .

The Noise compression level setting selects integration time for the CPD signal samples in the correlator. In situations when the return path in the 6-18MHz region is clear of numerous CW-like jamming carriers the *Standard* setting can be used. With this setting the system scans node more quickly than with the *High* setting.

Return Path Switches

Click the required sub item in the **Return path switches** to access information related to switch connections and configuration.

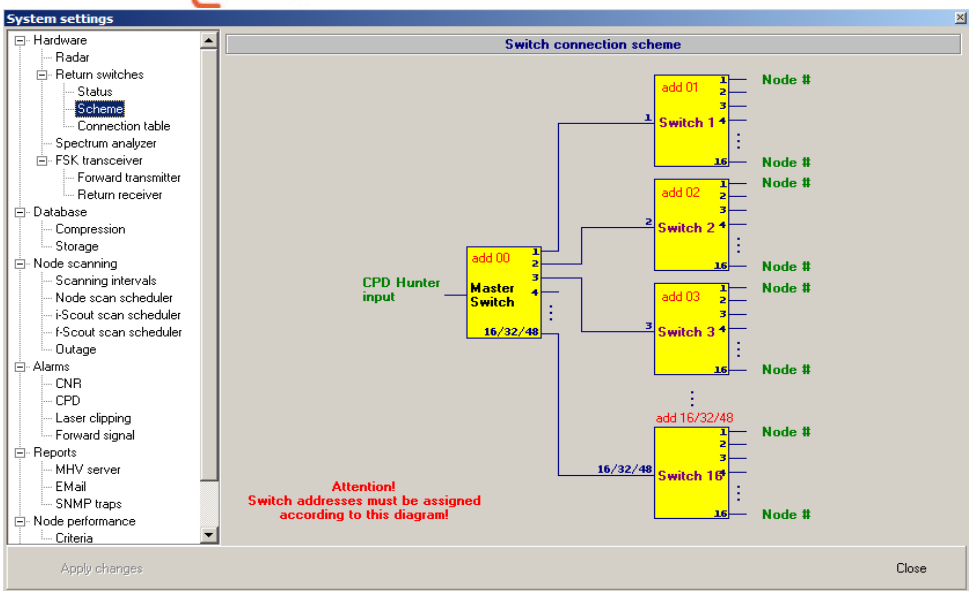
Switch status tab displays information about current switch status. Details on indications are described in Help text available by pressing the F1 key while window is open.



The following markers are used for indicating status of the switches and current active port number of each switch:

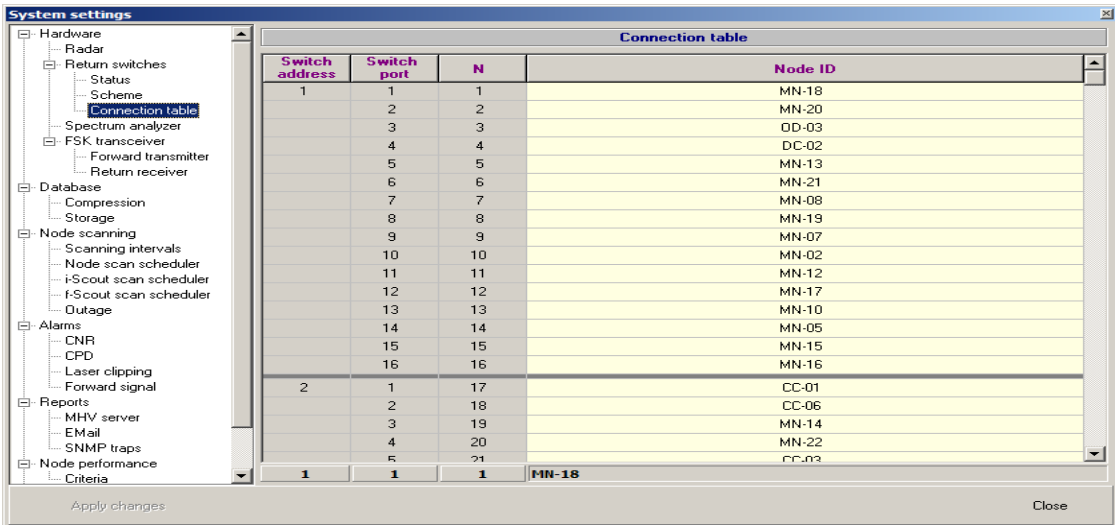
OK - switch works correct;
Error - switch does not respond to commands;
- - switch is not connected.

The **Switch scheme** provides general information about switching configuration.



The node/switch connection list can be viewed by clicking on the **Connection table** item. It provides information about which switch port is connected to which node receiver, and which node ID corresponds to which node number used when working with the Quiver in the field.

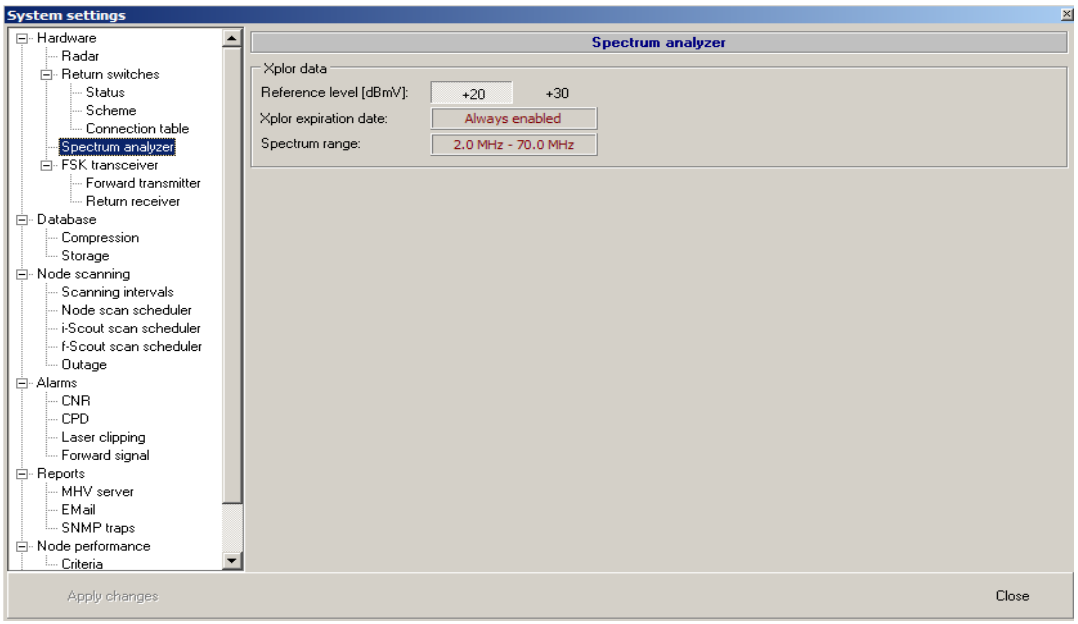
Data contained in this table is generated when the database is built by Arcom Digital, it cannot be changed by either a user or an administrator.



Print table – Prints a list of connected nodes, it provides an option to print either partial or a full listing of nodes.

Spectrum analyzer

This tab is active in system with an activated Xplor module.



Reference level

These settings allow for matching the dynamic range of the input with actual signal levels. Two settings are available: +20 and +30dBmV defining max allowed input signal level.

Xplor expiration date

Provides information about when the Xplor module will stop working if that option was not purchased.

Spectrum range

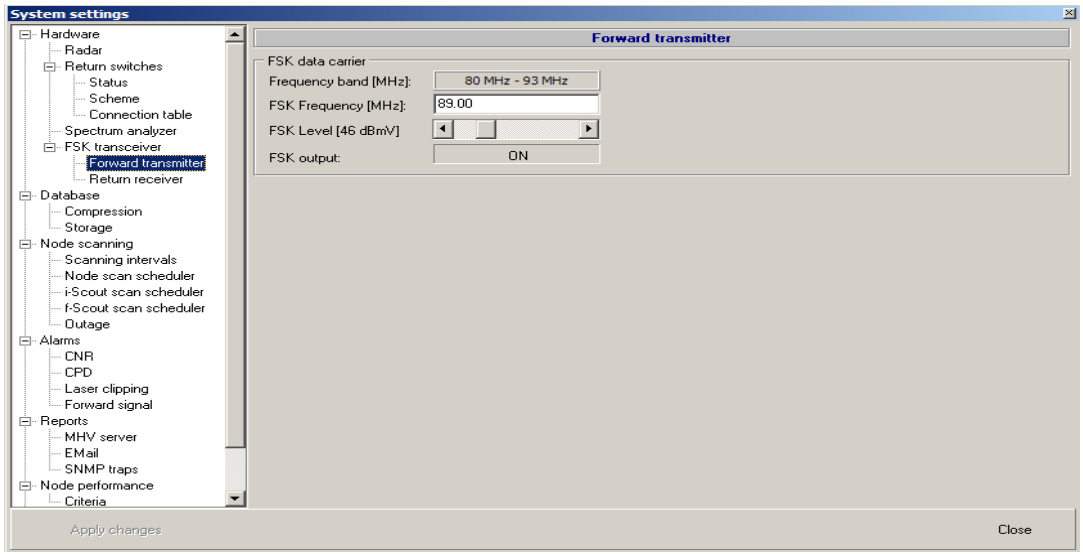
Provides information about the installed spectrum analyzer frequency range.

FSK transceiver

These parameters should be changed by an administrator only and double checked before any changes are saved. If the user does not know exactly what they are doing, it is recommend to first consult with an Arcom Digital Field Engineer. In this screen vital information on FSK carrier frequency in the forward and in the return can be changed. If the frequency is switched to a frequency occupied by a video channel **an outage will result**!

Forward transmitter

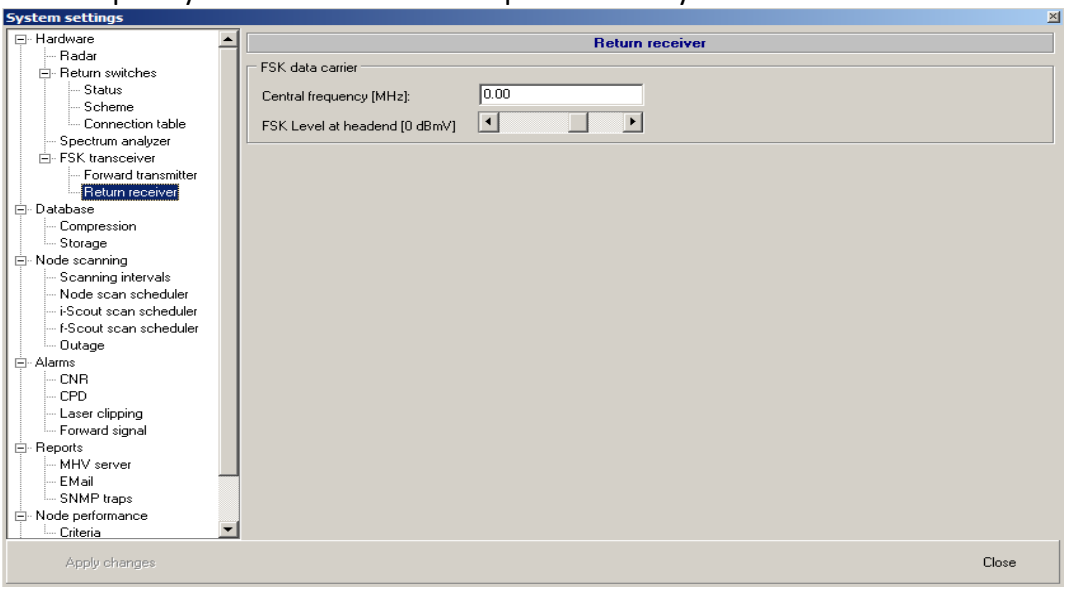
Sets the frequency for the telemetry data carrier transmitting information from the headend Xcor hardware to the Quivers in the field. The data is transmitted over an FSK carrier. It is used for communicating which node is currently scanned, what is the CPD status in a currently scanned node (Headend view mode) and sending confirmation on positively recorded calibration signal.



The FSK signal frequency can be chosen within hardwired factory selected basic FSK transmitter bandwidths. The FSK carrier level can be adjusted and turned ON or OFF. It should be turned OFF and output level set to min. during initial install as long as the proper frequency was not set. After selecting proper operating parameters the signal can be turned ON. The FSK output should be connected to a system combiner via a dedicated filter delivered with the hardware.

Return receiver

Sets the frequency of the f-Scout remote spectrum analyzer data receiver.

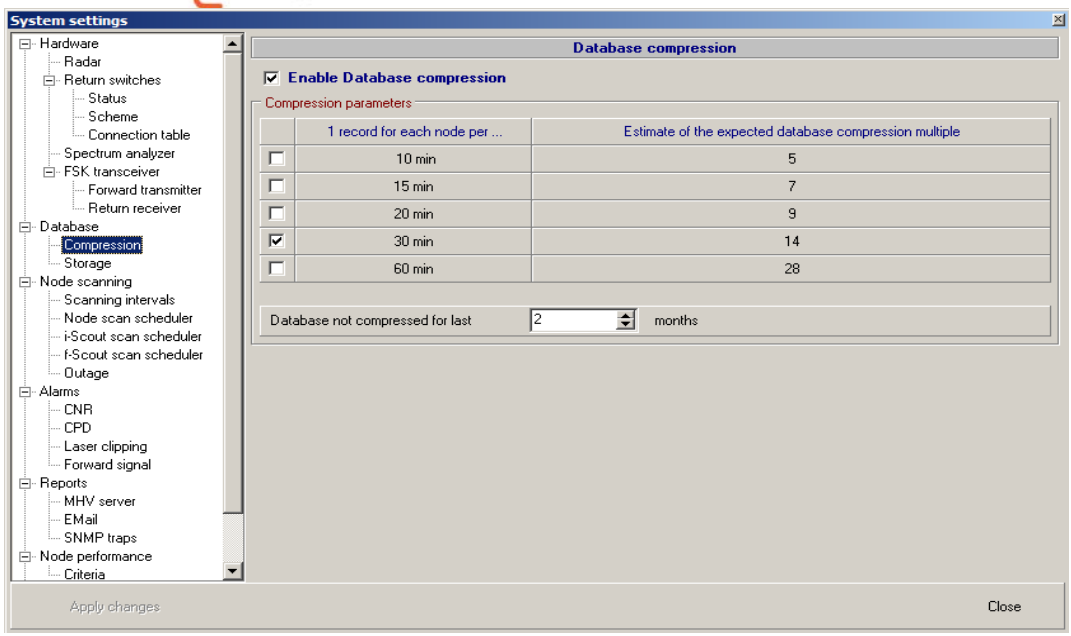


Database maintenance

The database files can grow very large. To avoid overloading disk space certain settings can be made to save only the important information and reduce amount of space occupied by obsolete or not important data.

Database compression

The amount of stored data can be reduced, by applying compression setting from the following screen:



Large numbers of spectrum screenshot records taken in a large system may result in the system quickly running out of hard disk space. The database compression allows for database size reduction by selecting only the worst case records for selected time periods. The system will then delete unnecessary records, saving only the vital information. The records remain in full for the prior two months as a selectable minimum.

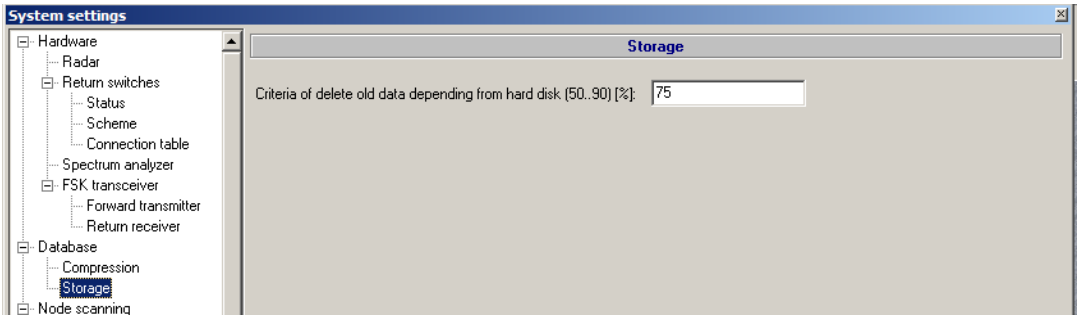
The number of months when complete records would remain preserved can be selected here:

Older records will be audited and compressed automatically according to the choice made in Compression parameters column where the user can select which records need to be saved. For example if "1 record per each node every… 10 min." was chosen the system will then keep for each node only the worse impairment records made each 10 minutes and delete all other.

Database compression feature can be turned on or off by selecting this switch:

Storage room control

Storage sub item of **Database** allows for setting the percentage of the hard drive space that will trigger automated old spectrum and CPD data deletion once the parameter is reached.



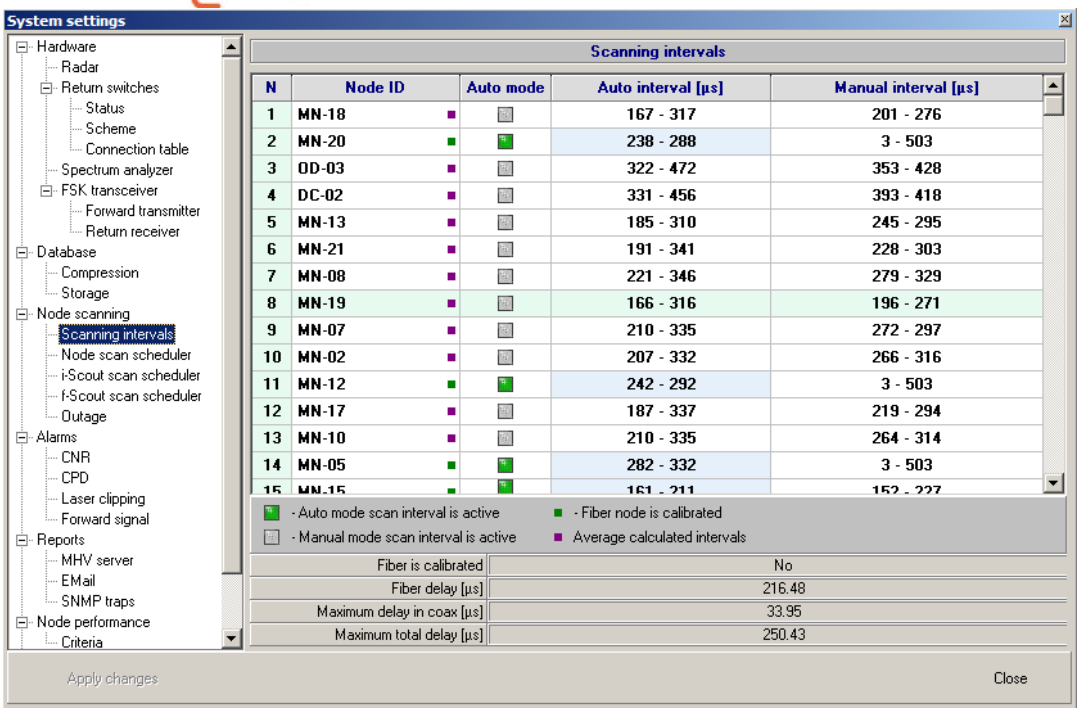
This feature prevents overloading the hard drive and reduces users maintenance efforts.

Node scanning

In node scanning the user can set Scanning intervals, Node scan scheduler, i-Scout scan scheduler, f-Scout scan scheduler and outage monitoring parameters.

Scanning Intervals

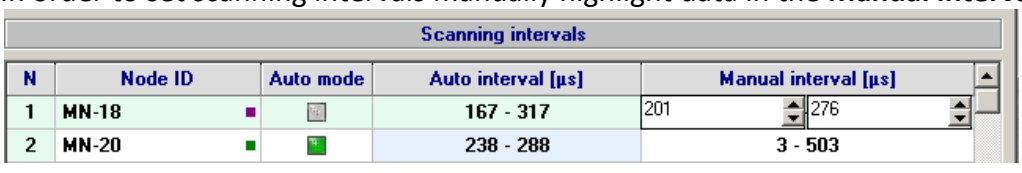
The radar does not need to scan through the entire length of the fiber as the CPD signals do not occur in the fiber. The system scans through the expected coax part of the system with a buffer at the beginning and the end of the coax cable. The system is delivered with the scanning intervals set to values corresponding to the data provided by the electronic system maps. This data doesn't need to be very accurate and the actual distance could be different. In order to prevent scan interval errors and speed up scanning, the fiber node locations can be calibrated using the calibration procedures described in the Quiver manual. The scanning intervals can be set to Auto or Manual. It is possible to set scanning intervals using CPD detection data accumulated in Day Average.



If the scanning intervals are set to **Auto mode** the indicator in the corresponding column shows green color. In a situation when the system is using the data calculated from the maps, the system will scan a wider range than the expected coax time delay. If the node was calibrated, then scanning will begin 10 microseconds before the expected coax and will be continued up to 10 microseconds after the coax range. This will prevent situations of not seeing a part of the network which may not be indicated on the maps.

Manual interval setting is dedicated for working in a situation that the fiber length is unknown or very much different than shown on the available maps. In such a situation the calibration signals (and CPD) may not be seen by the system. It will therefore be necessary to set the scanning intervals manually to a wider range in order to make the system see the calibrator signal. After calibrating, the system can be turned to auto mode which uses measured time delay distances. Widening the scanning intervals can cause very long scanning on a selected node. **Do not use this feature for anything other than calibrating nodes with unknown fiber length.**

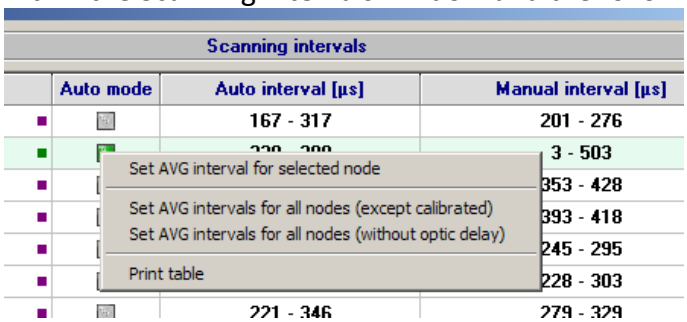
In order to set scanning intervals manually highlight data in the **Manual interval** column:



That will activate the adjustment tool in the highlighted cell. Set required values and click on any other cell – this action will cause saving manual interval setting data. The system will be now scanning within the selected time delay window.

The window with scanning interval settings shows information on whether the node was calibrated or not, time delay in fiber, max time delay in coaxial cable, and max total time delay.

Average calculated intervals can be used for automated system pre-calibration. This is possible when all the nodes display CPD traces that are recorded in the wide scan intervals during initial system work. To use this feature, right mouse click anywhere within the Scanning intervals window and the following menu will open:



The average data can be used for calibrating a single previously highlighted node, for all nodes except of those that were calibrated already or for all nodes that have no information about the fiber length. This operation can reduce scanning time of each node.
Note: once Average scan intervals are used the information transmitted to the Quiver in Headend view mode does not reflect the real time delay of visible CPD signals from the fiber node.

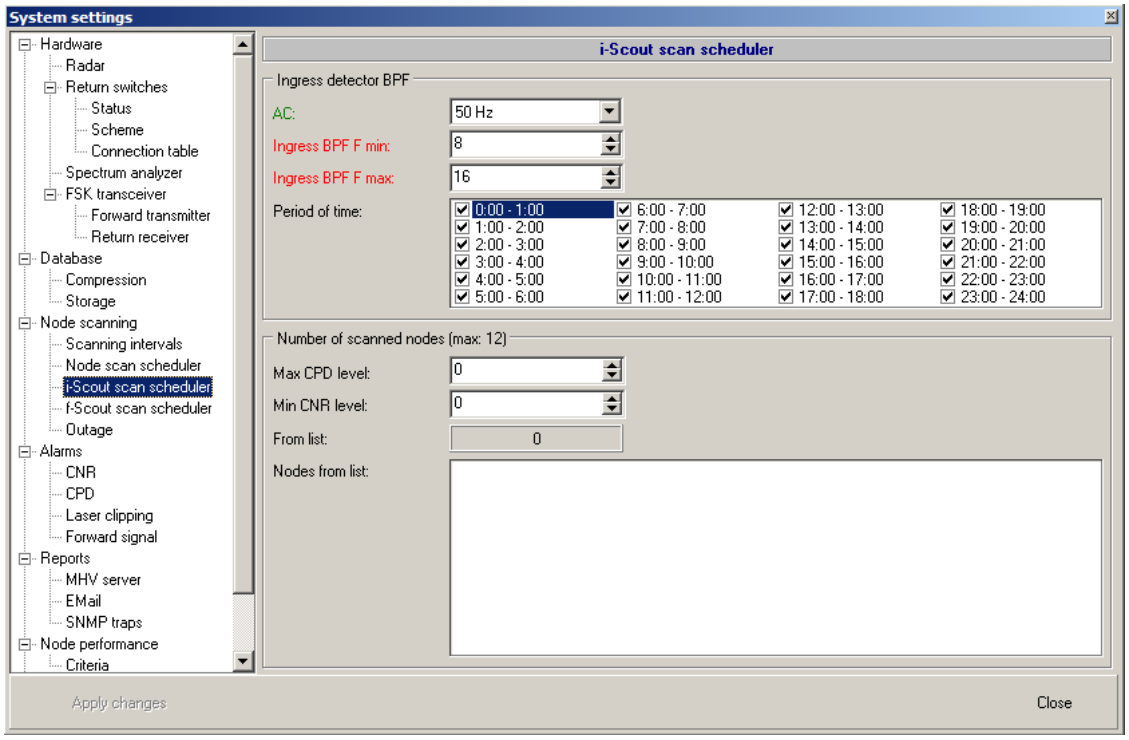
Detailed description about how to operate this window is available in Help text accessible by pressing F1 key.

Node scan scheduler

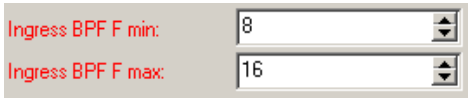
This sub item is dedicated for daily use by technicians and described in the Xcor Client user guide. Functions related to scan scheduling are not normally used by Administrators.

i-Scout scan scheduler

The i-Scout scanning task schedule feature can be set in the following System settings tab:

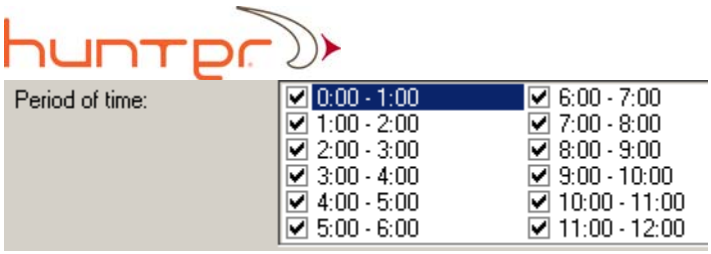


Ingress detector BPF



For automatic ingress detection in i-Scout mode the ingress monitoring window has to be set. This frequency window is set by adjusting the bandwidth of the Ingress detector BPF. The start and stop frequency for the filter can be set separately. The min. bandwidth is 1MHz. The frequencies can be selected between 8 and 16MHz.

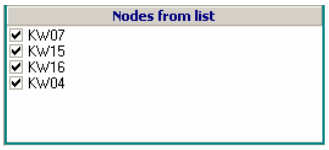
Period of time scheduler



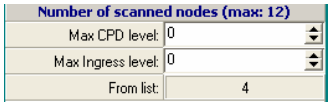
i-Scout demodulation for all the probes in one node takes approximately 150 seconds. Since the automated scanning can disrupt field work, in order to provide flawless operation during daily technician use (since regular CPD scanning is suspended during the scan interval), it is recommended that i-Scout scanning only be performed during periods that technicians are not in the field. The time slots desired for automated scanning can be selected in this window. Automatic i-Scout scanning will then only be performed in the time frames selected by the user. In the moments when the scanning is active the database signals can be viewed, but access to Signal Analyzer in manual mode will be blocked.

i-Scout node scanning patterns

The system will scan for i-Scout modulation in up to 12 nodes per sequence. It will scan the nodes selected in the Nodes from list window. The number was selected because 12 nodes will take a little less than half an hour, this was deemed to be a reasonable maximum time limit in which to suspend regular CPD scanning.

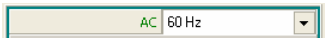


And in the nodes selected by the following rules:



The system will not allow the total number of nodes included in scanning to go beyond 12.

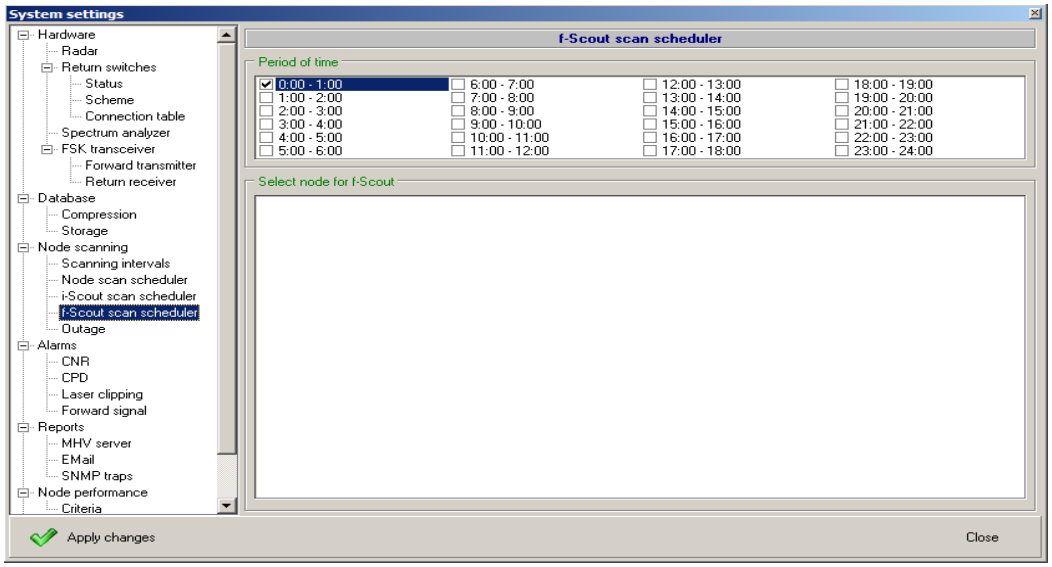
AC power frequency setting



The frequency of the power supply AC is VERY important for i-Scout demodulation and must be set accordingly to local situation. Two settings are possible: 50 and 60Hz.

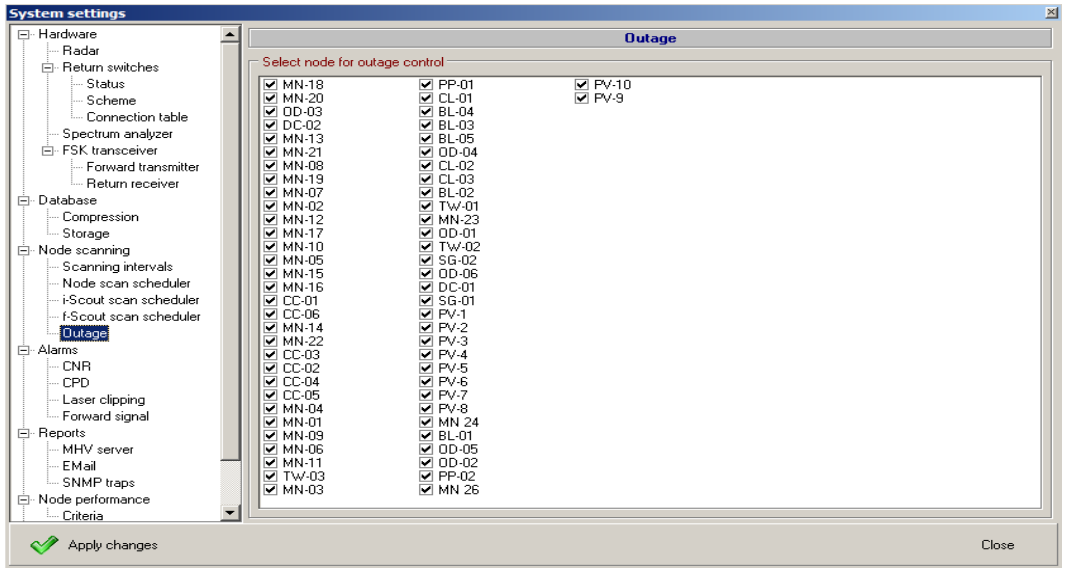
f-Scout scan scheduler

This subitem allows the user to select when the data from the f-Scout remote spectrum analyzers will be retrieved. Check the box next to each hour slots when the reading should be conducted:



Outage control settings

The nodes that should be included in the list of nodes monitored for outage occurrence can be added and removed by marking the checkboxes in the following System settings window tab:



Remark: the nodes with device count less than 100 may create unwanted Outage alarms due to clarity of the return path spectrum and lack of data signal activity. Should such a node create repeatable unwanted outage alarm, the operator can exclude it by unchecking the required node in the above list.

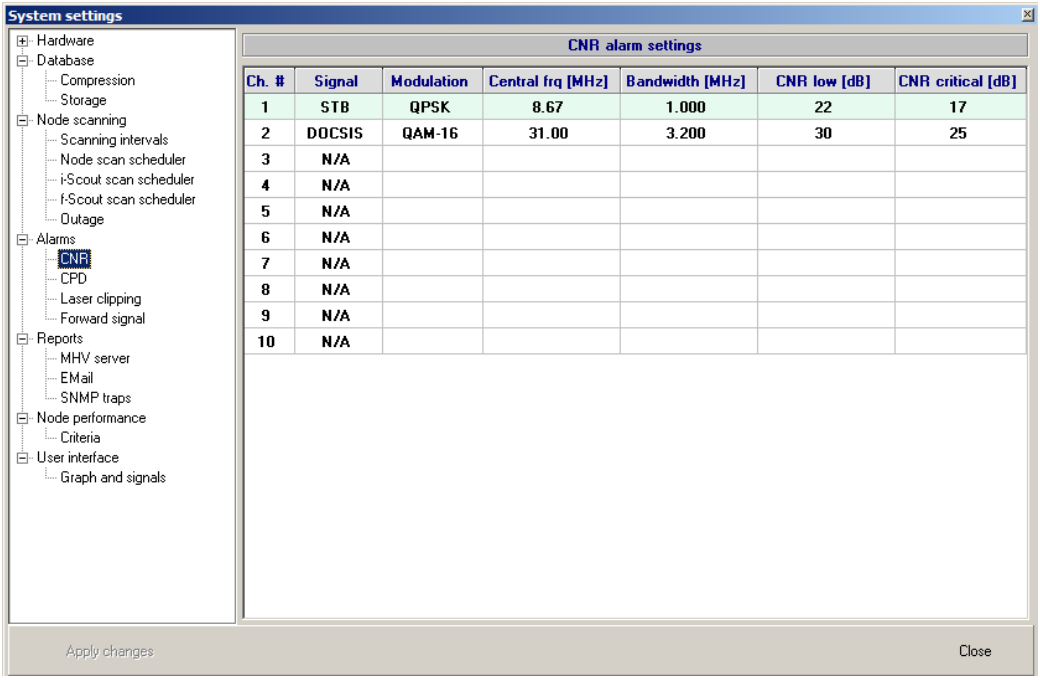
Alarms

In this item users can set thresholds and other parameters for monitoring CNR, CPD, Laser clipping and forward signal by the f-Scout probes

CNR

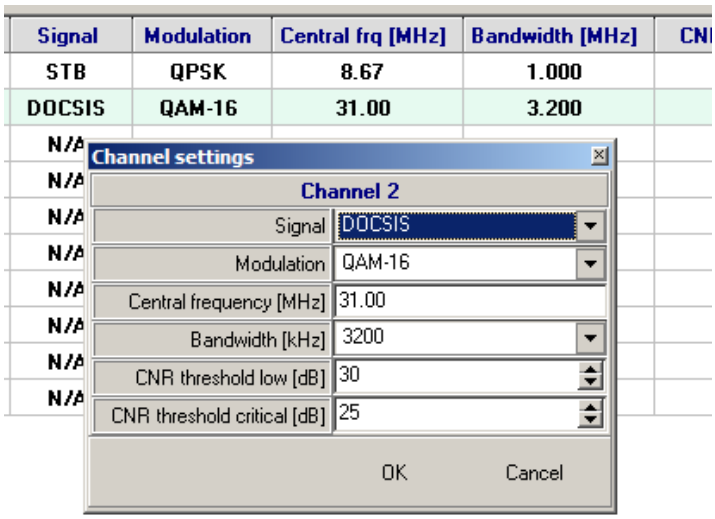
Here the user must set parameters of each active useful return path signal which CNR will be monitored.

For the CNR alarm feature to operate properly, information is required about the data carriers central frequency, their bandwidth, modulation type and the threshold levels for triggering alarm condition. Access to these settings is organized via the CNR subitem in the Alarms branch:

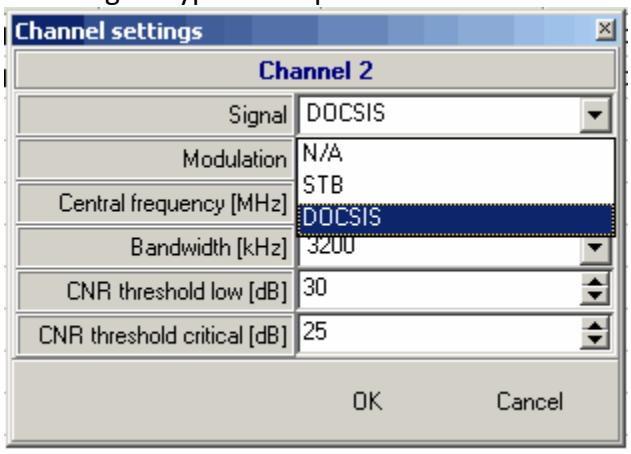


Ch. #	Signal	Modulation	Central frq [MHz]	Bandwidth [MHz]	CNR low [dB]	CNR critical [dB]
1	STB	QPSK	8.67	1.000	22	17
2	DOCSIS	QAM-16	31.00	3.200	30	25
3	N/A					
4	N/A					
5	N/A					
6	N/A					
7	N/A					
8	N/A					
9	N/A					
10	N/A					

Monitored return path channel settings
Double click on the Ch.# row to open settings for selected data carrier. The following screen comes up:

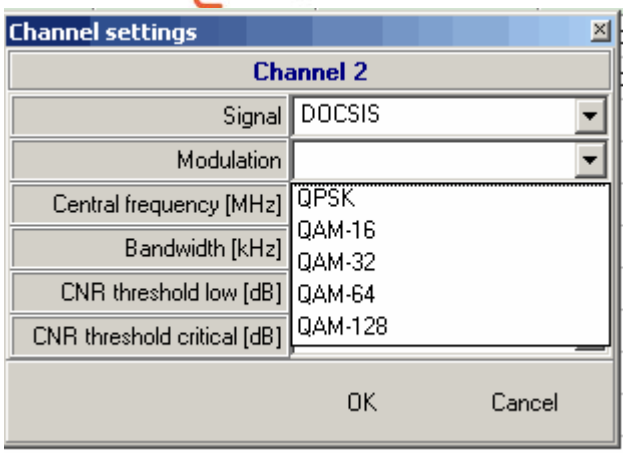


Entering signal transmission parameters
Select signal type in the pull down menu:

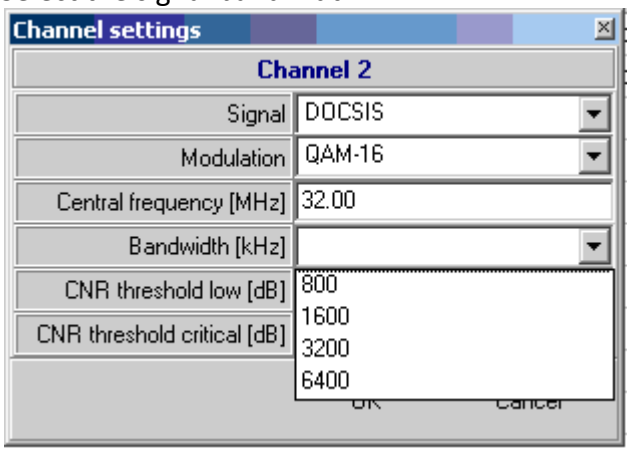


N/A should be selected if that is not present in the channel allocation.

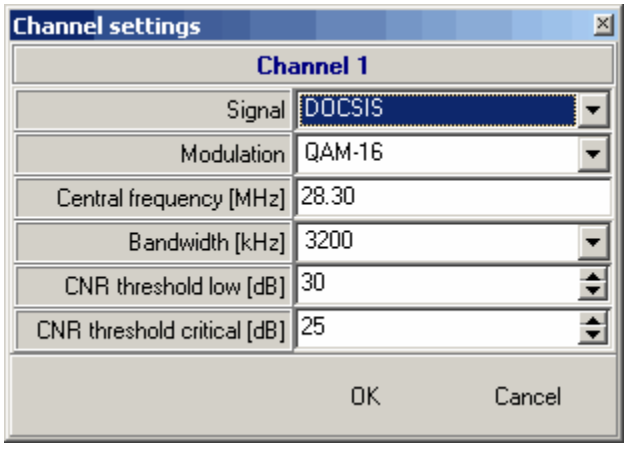
Select modulation format of the monitored signal:



Select the signal bandwidth:



Select CNR alarm threshold levels for selected channel:



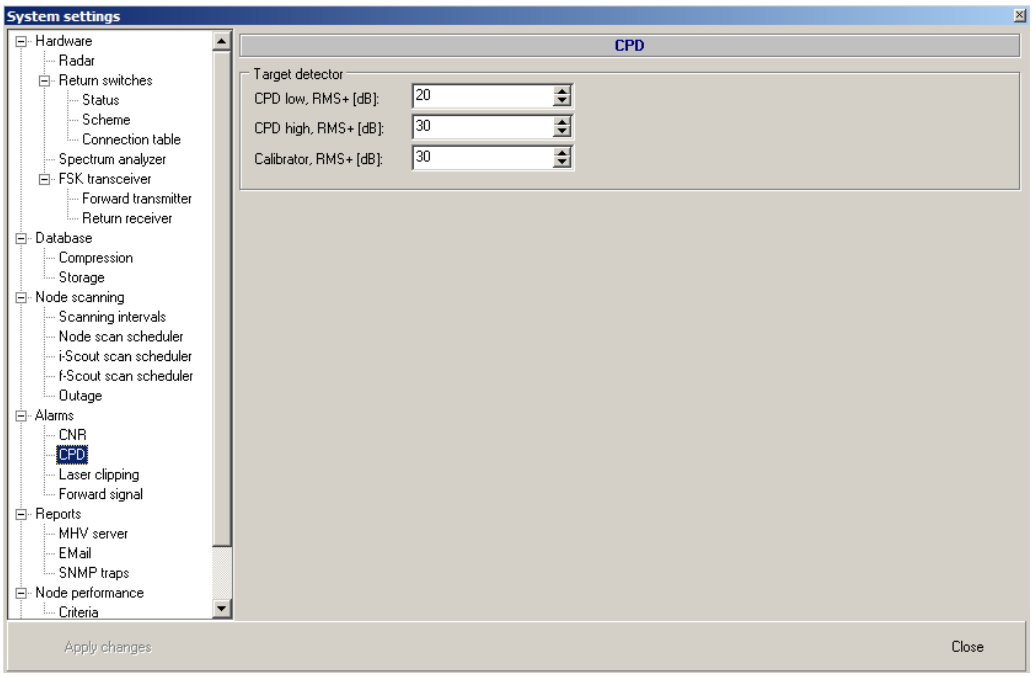
The CNR threshold low and high parameters are adjustable separately.

After selecting all parameters, left click OK to save the data and proceed with setting next channel parameters.

Please, note that the CNR Alarm monitoring parameters can be copied to other hubs, which are working with same settings. That operation can be done with the MHV server program with Administrator privileges.

CPD

This sub item adjusts the CPD signal detection thresholds.



The target detector is responsible for making decisions on when to save particular signal records into the database and what indictor should be assigned to it.

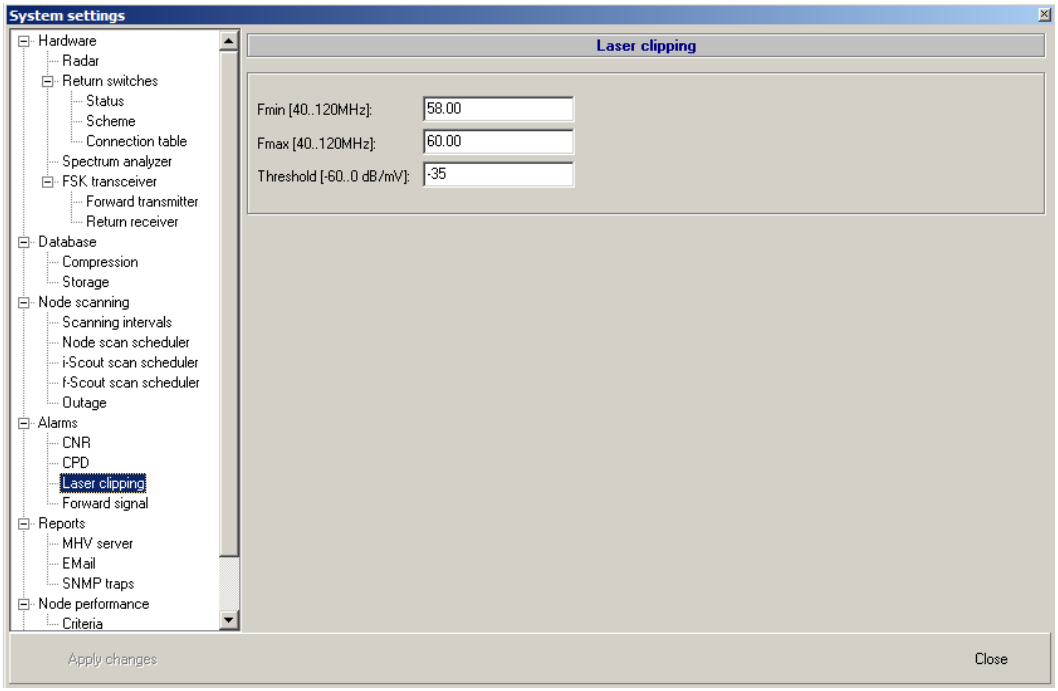
The CPD signal is recognized as a peak over the average level of the noise floor represented by the correlation function. The peak above the noise floor is accepted by the system as a CPD signal low if it is visible over the noise RMS with level higher than the level set by CPD low. Value for the CPD low should not be set lower than 20dB as random peaks in the noise could be mistaken for CPD signals, creating multiple CPD signal records without repeatable time delay positions in consecutive scans. The CPD high signal threshold establishes the level above the RMS noise floor necessary for a

CPD high alarm to be recorded in the database. Parameters set here do not describe the absolute level values of the detected CPD signals.

Calibrator threshold sets detection level for the Calibrator signals. It is recommended to use 30dB value.

Laser clipping

Laser clipping sub item sets the parameters of the laser clipping detector. The alarm condition is set once the selected noise floor level within an adjusted frequency range exceeds a certain value. **Note that setting too low value might cause unwanted alarms in the Hub impairments Statistics.**



When setting parameters, remember to select a frequency band that is free of ingress and useful return signals that could trigger false alarms. The frequency window should be selected above the return path. Also be aware that poor diplex filters that allow forward signals into the return path could be interpreted as laser clipping.

Forward signal

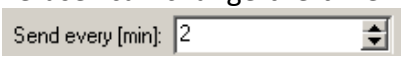
This item is dedicated to the systems equipped with f-Scout probes - remote forward spectrum analyzers.

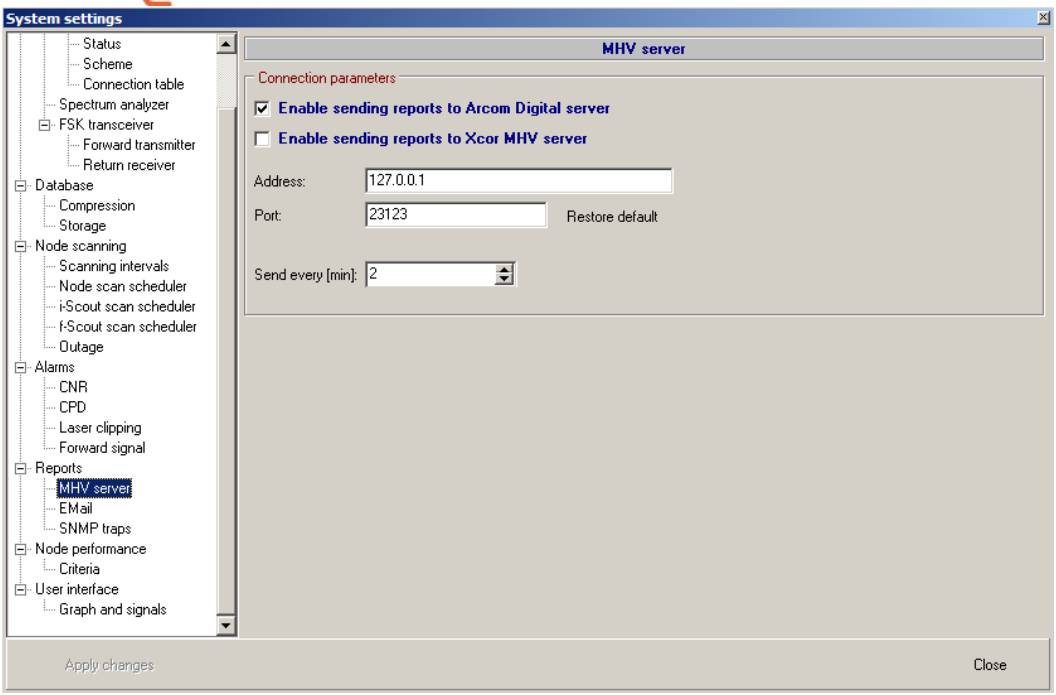
The next manual revision will describe this feature in detail.

Reports

This submenu groups access to settings of various reports that can be sent by the Hunter server.

MHV server

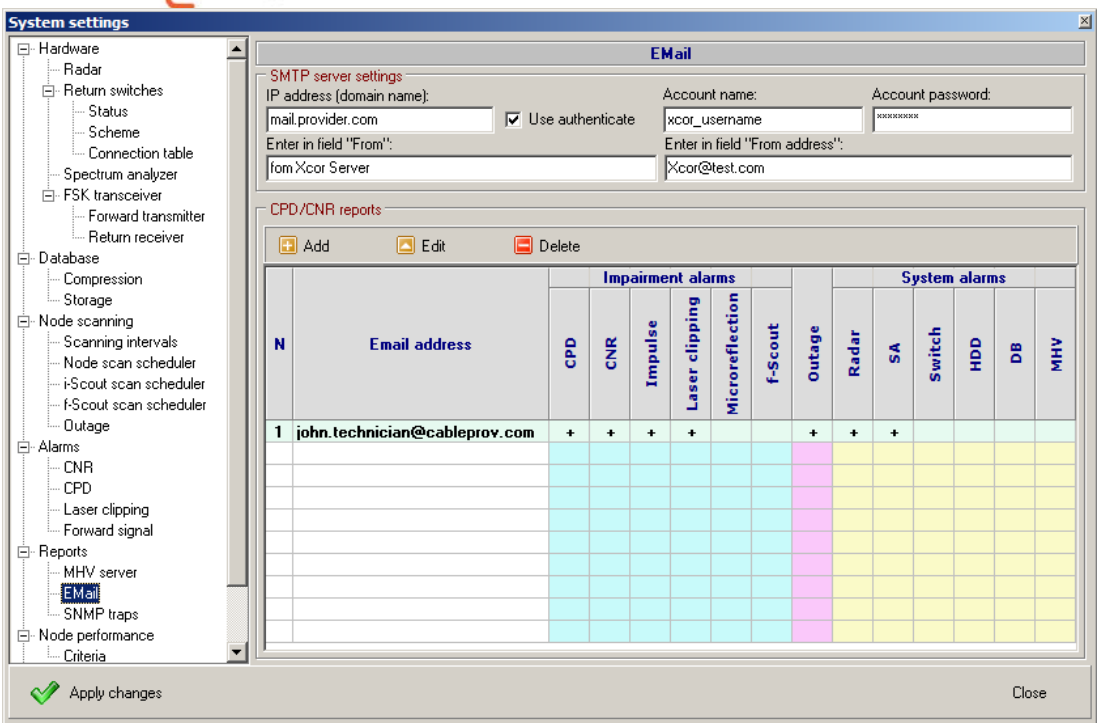
This sub item sets parameters for connecting with customers' MHV server. Xcor servers installed at various hubs can be monitored simultaneously by a separate system responsible for collecting information about the hub statuses. This information is then available at a single place where it can be sorted and analyzed for use by management, the NOC, and for workforce planning. To configure the hub to send information to the MHV server, the connection parameters must be entered. The IP address of the computer hosting MHV server software must be entered and the checkbox marked to activate reporting on current software, hardware and impairment status to the MHV server. The port must be set to 23123 (default). The user can change the time interval for sending data to the MHV server in this section: 



Arcom Digital maintains its' own MHV server for monitoring systems under warranty and the demo kits. This option is activated by marking the following check box: 

E-mail

The system can send email messages with information about CPD/Ingress alarms and status of the server. In order to make it possible an SMTP server must be used and the following data must be entered into the following fields:



SMTP server settings
IP address (domain name);
Enter here the IP address or the domain name of the SMTP server.

Use authenticate
Should be marked when the SMTP server requires authentication.

User name
Enter here the name of the user, registered on the SMTP server.

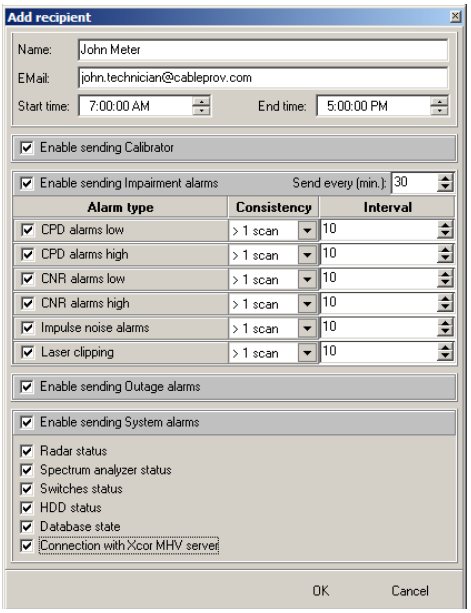
User password
Enter here the password of the user, registered on the SMTP server.

Enter in field “From”
Enter here the text which will be put in the e-mail “From” field.

Enter in field “From address”
The text which will be put in this field will be used as “From address” when email received.

Adding e-mail recipients

Click add button  to open menu for adding recipient and selecting report types to send. The Add recipient window will open:

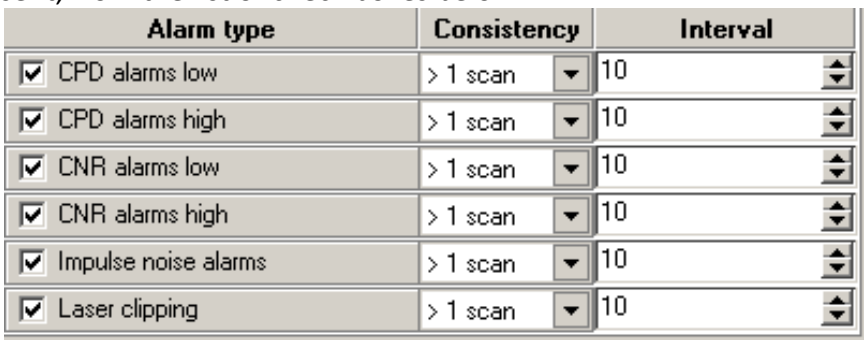


For each e-mail recipient the alarms can be freely assigned. Populate name and e-mail address fields and select time window when the e-mails will be sent.

Explanations to the checkbox fields

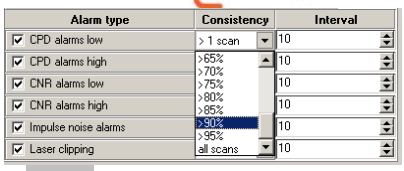
 - mark for receiving a message about node calibration

 - mark for activating and select time interval between each data refresh, then select which impairment type alarms will be sent, from the list of check boxes below:



Selecting alarm consistency

This criterion decides when alarm condition is generated. From the pull down menu select required number:



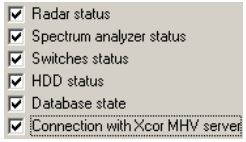
If >1scan selected, all occurrences of impairment will be alarmed. If all scans selected, then alarm condition occurs when each node scan reports impairment presence.

Interval

Sets the number of consecutive scans within which the impairment consistency is calculated.

- when checked, information about detected outages will be send to the e-mail recipient

- when checked, information about detected selected hardware and software irregularity will be send to the e-mail recipient



- check required hardware and software to monitor

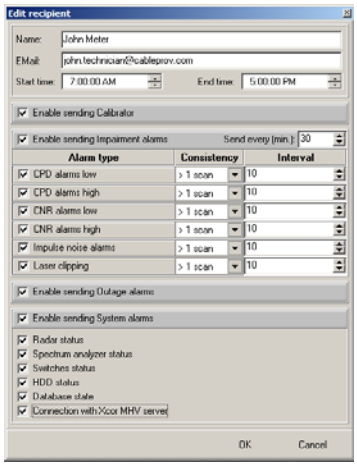
The new data is accepted and saved by clicking 

button.

Editing email recipient settings

Click 

button to open Edit recipient screen:



The new data is accepted and saved by clicking 

button.

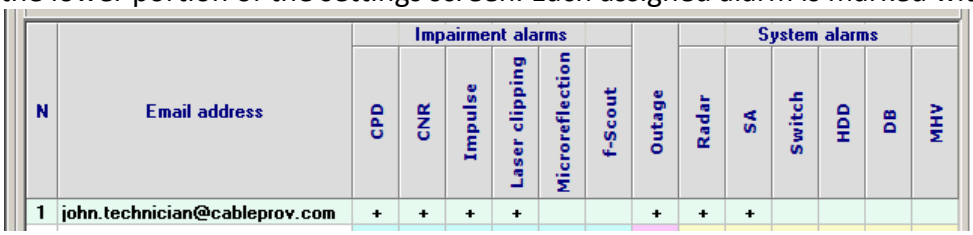
Deleting e-mail recipient

Highlight the e-mail recipient in the list first, then click Delete button to delete recipient. In the confirmation screen select yes to complete operation.

The new data is accepted and saved by clicking Apply changes button.

E-mail recipient status

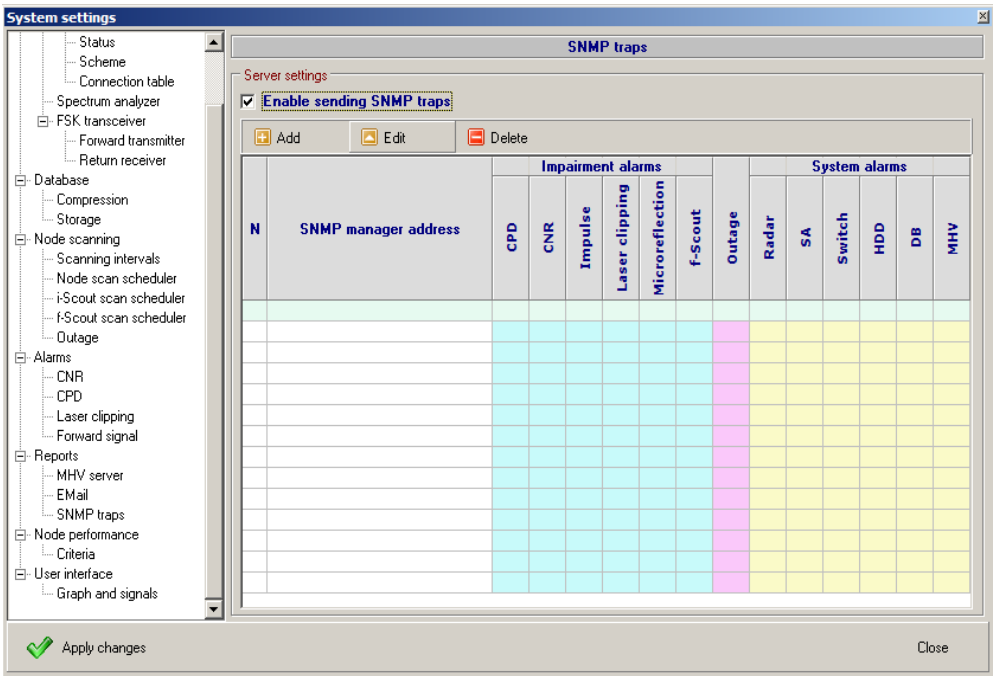
Current status of assigned alarm reports that will be sent to the recipient is presented in the lower portion of the settings screen. Each assigned alarm is marked with + mark:



N	Email address	Impairment alarms							System alarms					
		CPD	CNR	Impulse	Laser clipping	Microreflection	f-Scout	Outage	Radar	SA	Switch	HDD	DB	MHV
1	john.technician@cableprov.com	+	+	+	+			+	+	+				

SNMP traps

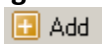
The system can send Impairment and System alarms in a form of SNMP traps. The MIB for decoding the traps on the reception side is available on Arcom Digital FTP server for downloading.

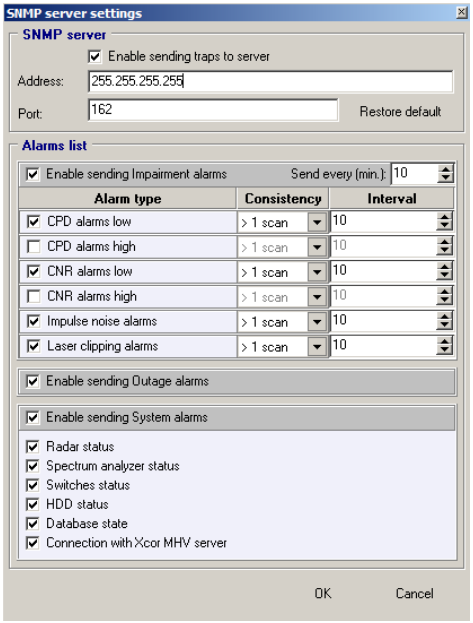


To activate SNMP traps mark  box.

The traps can be sent to multiple SNMP manager addresses.
Each SNMP manager can control individually assigned list of alarms.

Adding SNMP manager address

Click  button to open the SNMP server settings screen:

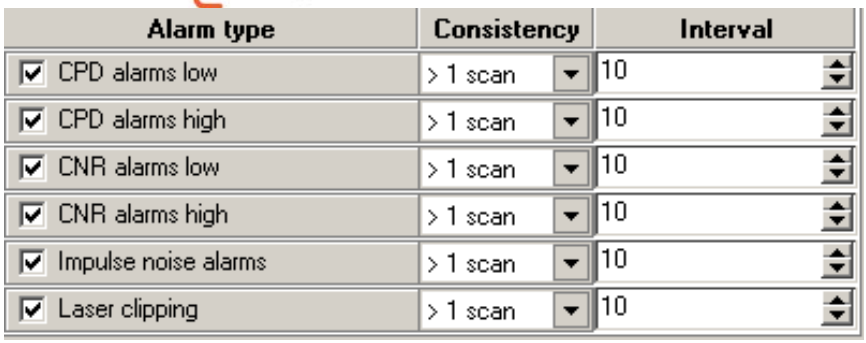


In the appearing window set the IP address of the target server. Leave the Port 162 setting as default.

Explanations to the checkbox fields:

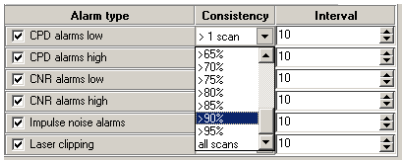
 - mark it for receiving a trap message about fiber node calibration

 - mark for activating, then select time interval between each data refresh, and select which impairment type alarm trap will be sent from the list of check boxes below:



Selecting alarm consistency

This criterion decides when an alarm condition is generated. From the pull down menu select required number:



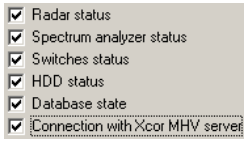
If >1scan selected, all occurrences of impairment will be alarmed. If all scans selected, then alarm condition occurs when each node scan reports the impairment presence.

Interval

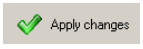
Sets the number of consecutive scans within which the impairment consistency is calculated.

- when checked, a trap with information about detected outages will be sent.

- when checked, a trap with information about detected selected hardware and software irregularity will be sent



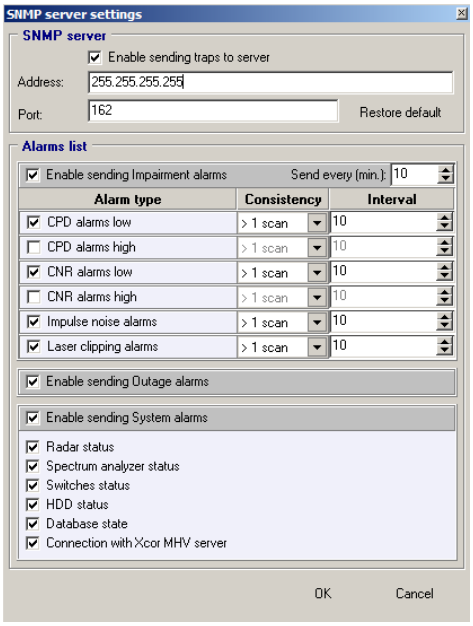
- check required hardware and software to monitor

The new data is accepted and saved by clicking 

button.

Editing SNMP manager settings

Click Edit button to open Edit recipient screen:



The new data is accepted and saved by clicking Apply changes button.

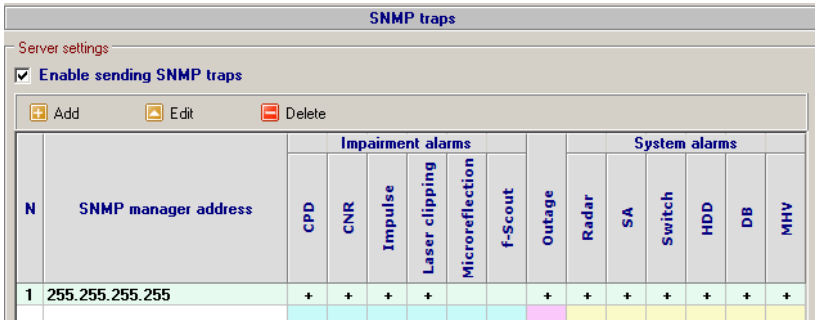
Deleting SNMP server address

Highlight the SNMP server in the list first, then click Delete button to delete recipient. In the confirmation screen select yes to complete operation.

The new data is accepted and saved by clicking Apply changes button.

SNMP settings status

Current status of assigned SNMP server where the traps will be sent to is presented in the lower portion of the settings screen. Each assigned alarm is marked with a + mark:

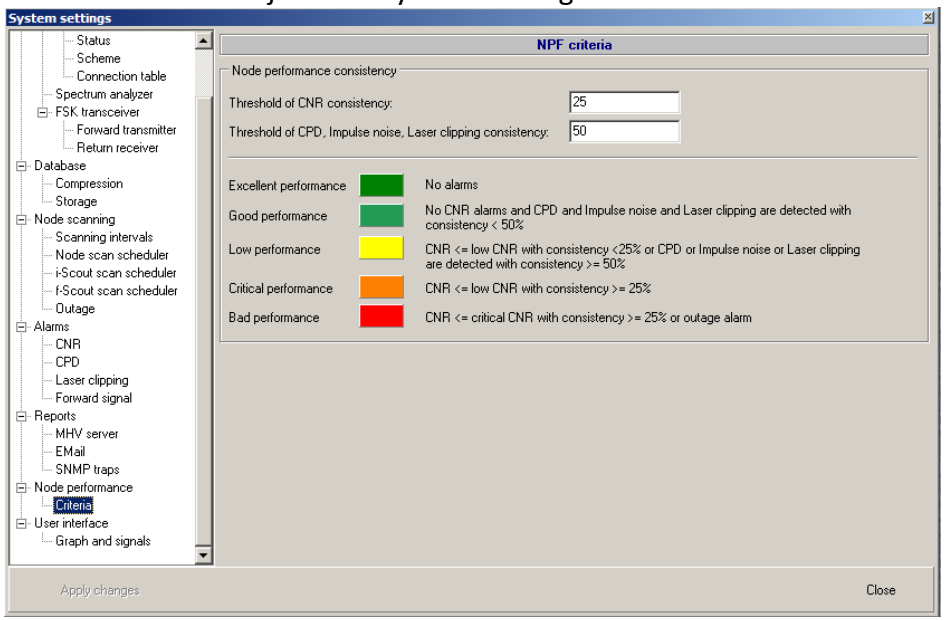


Node performance

Node performance provides overall rating information about the condition of each node throughout the day. Status is indicated by different colors marking each hourly cell in the Impairment statistics window accessible with Xcor Client program. Information presented with different colors makes it very easy to see how the node behaves without spending time on detailed analysis.

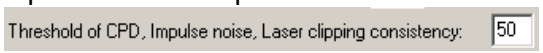
Criteria

Various impairments and their consistency of detections are used for calculating current rating. The thresholds are adjustable by the user together with associated colors:



Threshold settings

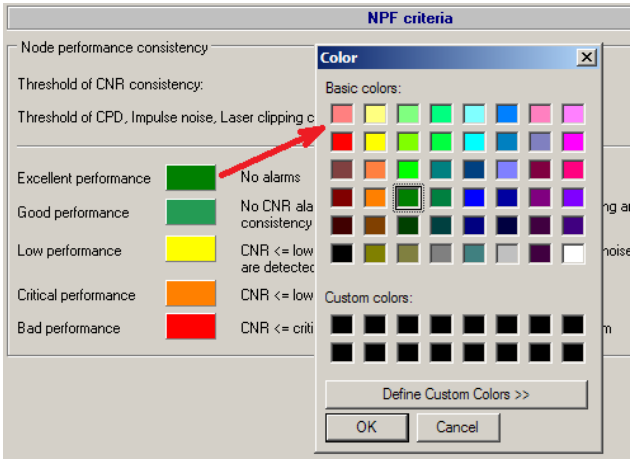
- the number here represents the percentage of scans that report CNR alarm presence



- the number in this field sets the percentage of scans that report CPD or Impulse noise or Laser clipping alarm presence

Performance indicators

The performance indicators have different colors associated with different node condition, depending on the impairment type and its consistency. If a user wants to change the default settings, the colors can be assigned for each condition by clicking the color field and selecting the new one from the color palette:



The performance rating definition for each color is explained directly on the settings screen after the thresholds are set:

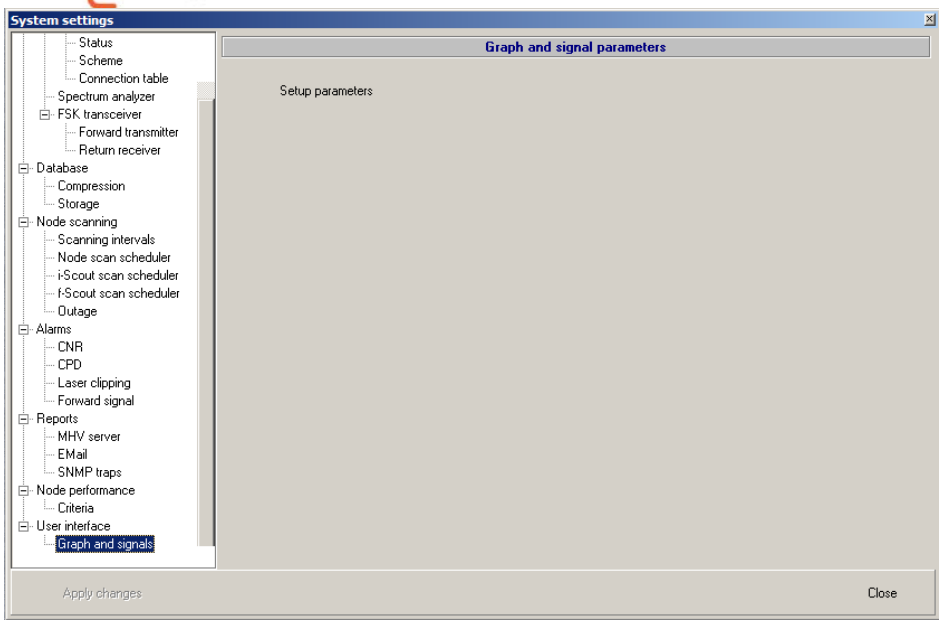
Excellent performance		No any alarms
Good performance		No CNR alarms and CPD and Impulse noise and Laser clipping are detected with consistency < 50%
Low performance		CNR <= low CNR with consistency <25% or CPD or Impulse noise or Laser clipping are detected with consistency >= 50%
Critical performance		CNR <= low CNR with consistency >= 25%
Bad performance		CNR <= critical CNR with consistency >= 25% or outage alarm

User interface

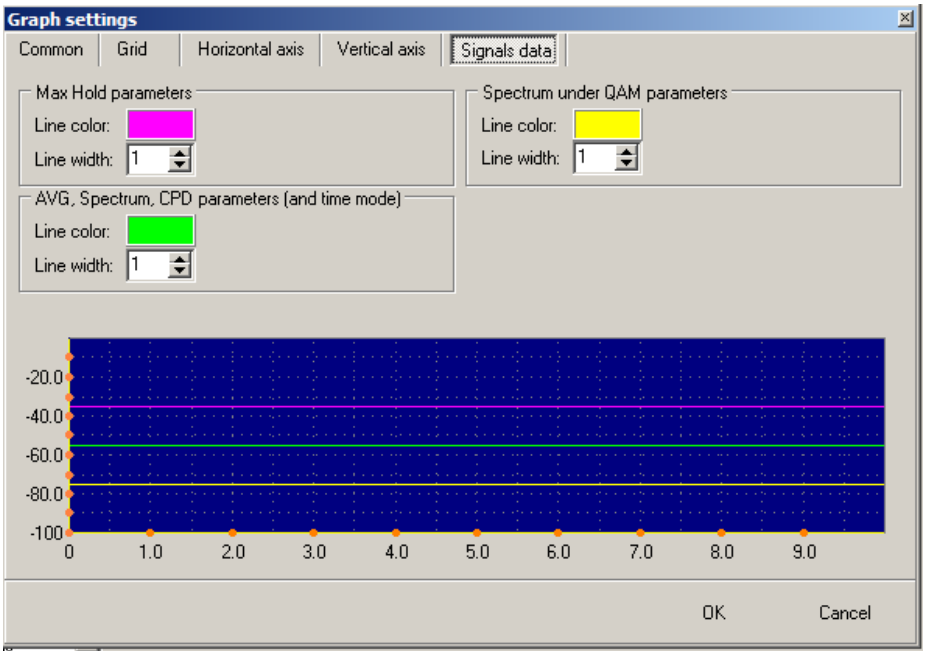
The user can change the default colors that are used for drawing graphs.

Graph and signals

Click on this sub item to open the Graph and signal parameters screen.



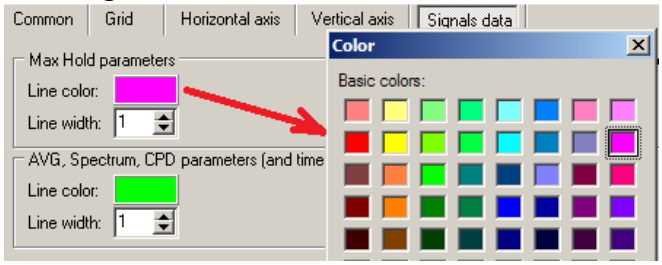
Then click Setup parameters button to open the next screen:



Signals data line colors

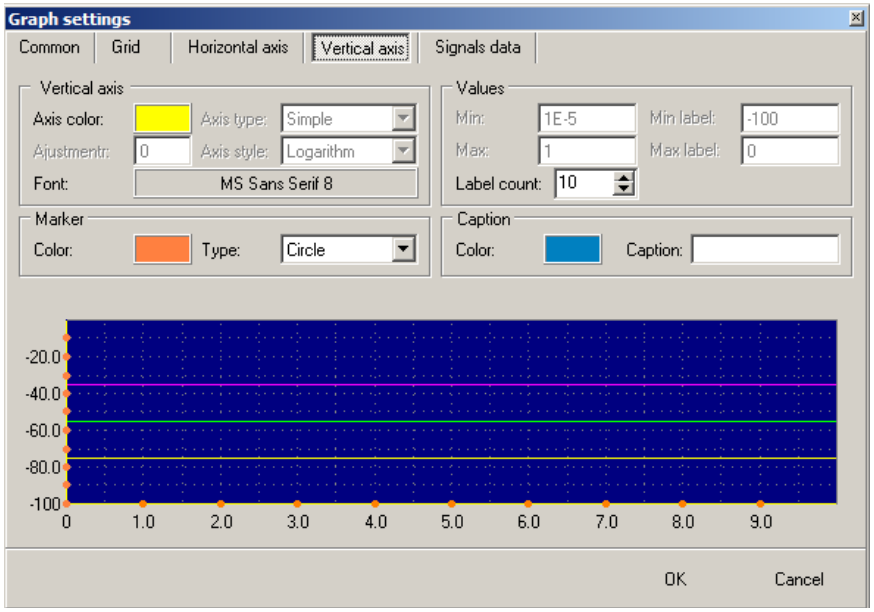
The Signals data tab defines which colors are used for creating lines that plot the spectrum and CPD signal shapes. The line widths can be changed as well.

To change the line color click the line color field and the color palette screen will open:



Vertical axis line

The Vertical axis tab defines colors used for drawing graphs' vertical axis.



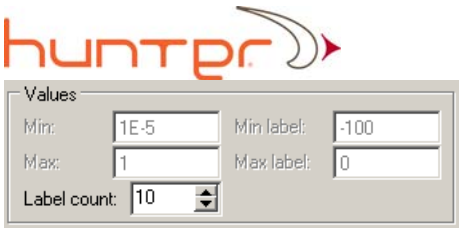
The color of the vertical line drawing the Y axis can be selected by clicking the color rectangle here: 

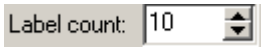
. That operation will open the color palette. Select desired color and click OK.

To select the font type that will be used for describing the values on the Y axis, click the font name here: 

. Select desired font from the appearing menu and confirm by clicking OK.

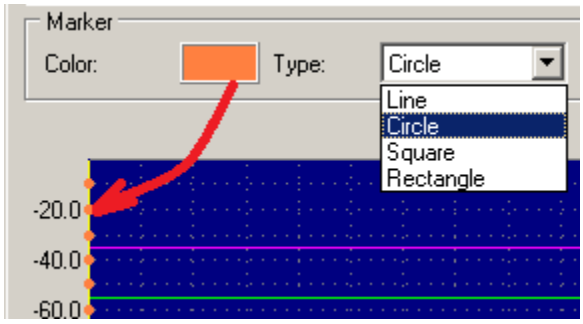
The following setting decides how the values are marked on the vertical axis:



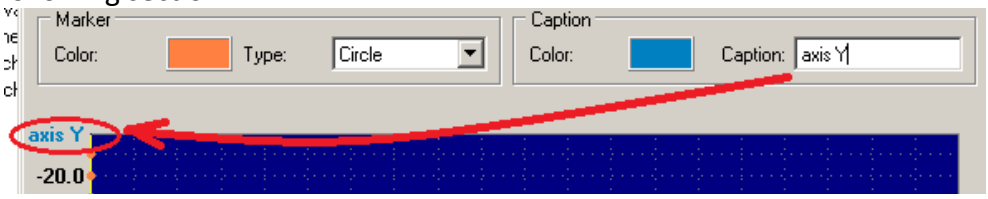
The 

sets the number of labels that will be put on the Y axis. Other fields are not active in this software version.

The scale on the Y axis can be marked with different marks selectable from the pull down menu. The color of the mark can be selected from the color palette accessible by clicking on the color field:



The color of the caption and text used for describing the vertical axis can be set in the following section:

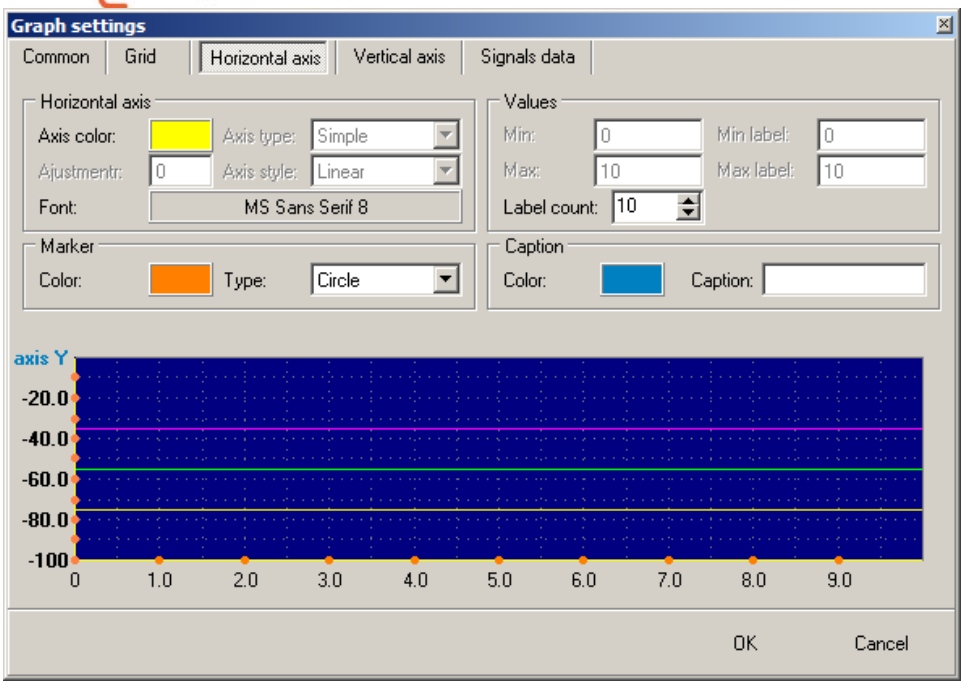


To set the color click the color field and select required color from the palette.

Horizontal axis line and mark colors

The 

tab defines colors used for drawing graphs' horizontal axis.



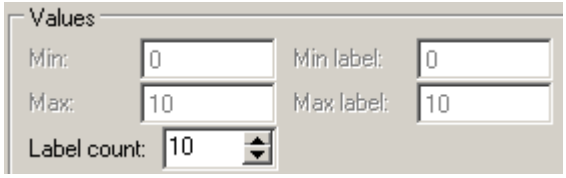
The color of the horizontal line drawing the X axis can be selected by clicking the color rectangle here: 

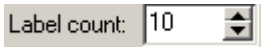
This operation will open the color palette. Select desired color and click OK.

To select the font type that will be used for describing the values on the X axis, click the font name here: 

. Select desired font from the appearing menu and confirm by clicking OK.

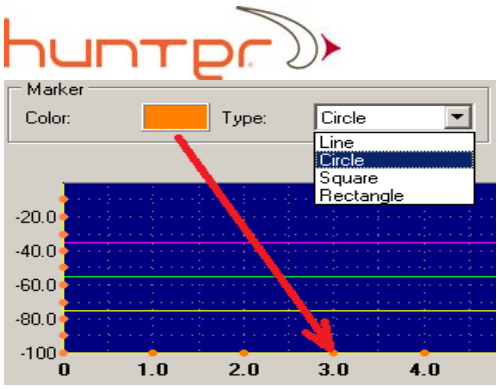
The following setting decides how the values are marked on the horizontal axis:



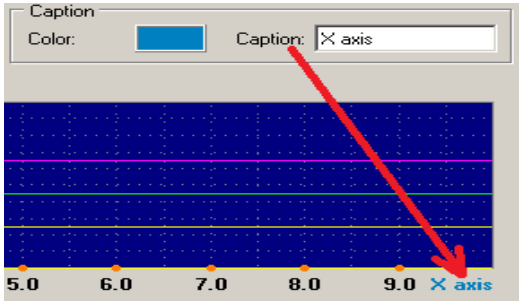
The 

sets the number of labels that will be put on the X axis. Other fields are not active in this software version.

The scale on the X axis can be marked with different marks selectable from the pull down menu. The color of the mark can be selected from the color palette accessible by clicking on the color field:

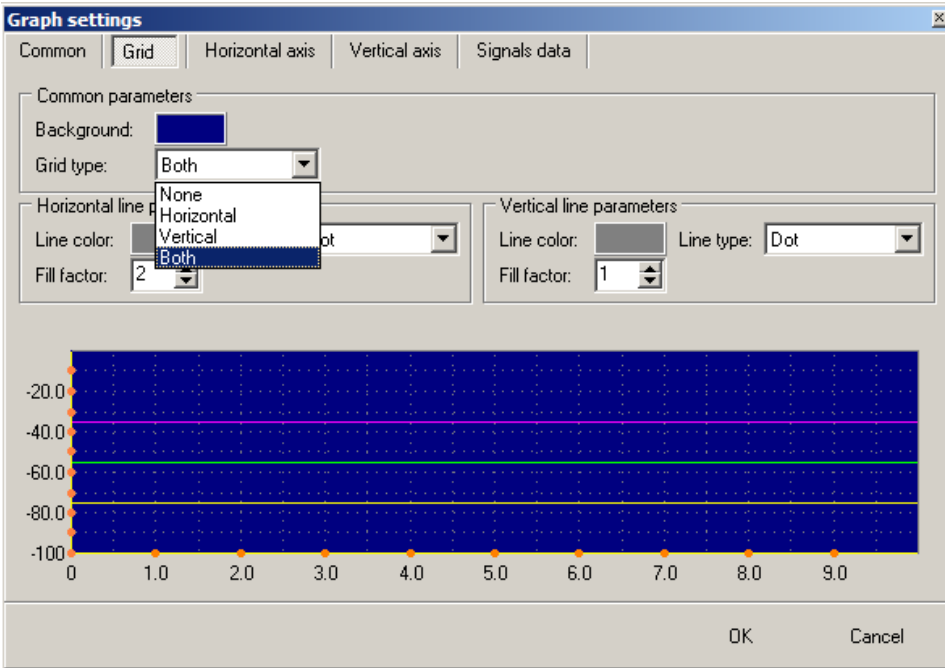


The color of the caption and text used for describing the horizontal axis can be set in the following section:

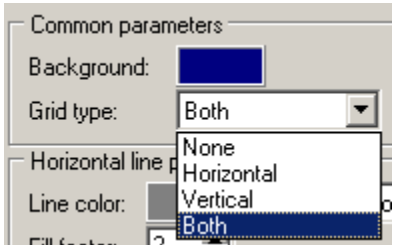


To set the color click the color field and select required color from the palette.

Grid tab  allows administrator to change the shape and appearance of the scale grid.

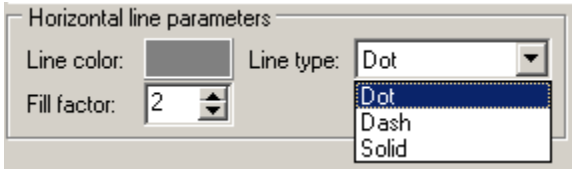


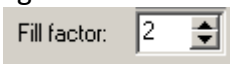
Common parameters like Background and Grid type can selected using the following fields:



The Background is set by clicking on the color field and selecting desired background color from the palette.
The Grid type can be selected as only vertical, only horizontal, both present or none present.

Horizontal grid line parameters can be selected in the following section:



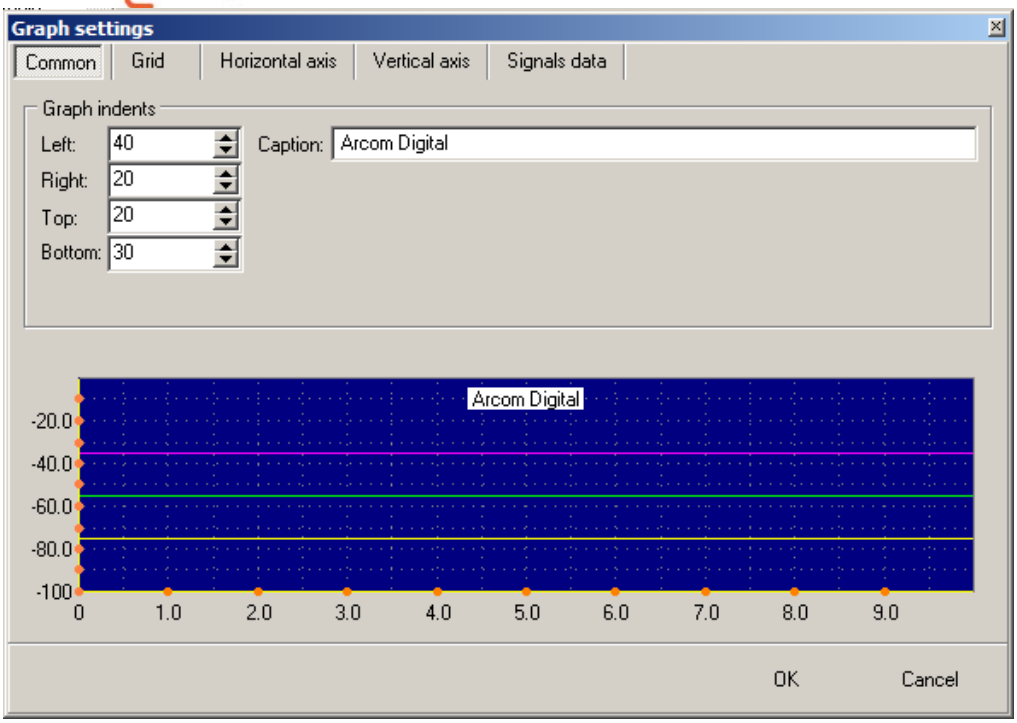
The line color can be changed by clicking the color field and selecting another from the color palette.
The line can be drawn as dotted, dashed or solid, select required type from pull down menu.
The filling factor for the dashed and dotted line type can be selected in the fill factor setting: 

.

Vertical grid line parameters are set using exactly same adjustments like for the horizontal line.

Common setting tab offers access to adjust the caption that will be imposed on each of the signal scan records and the graph indents.

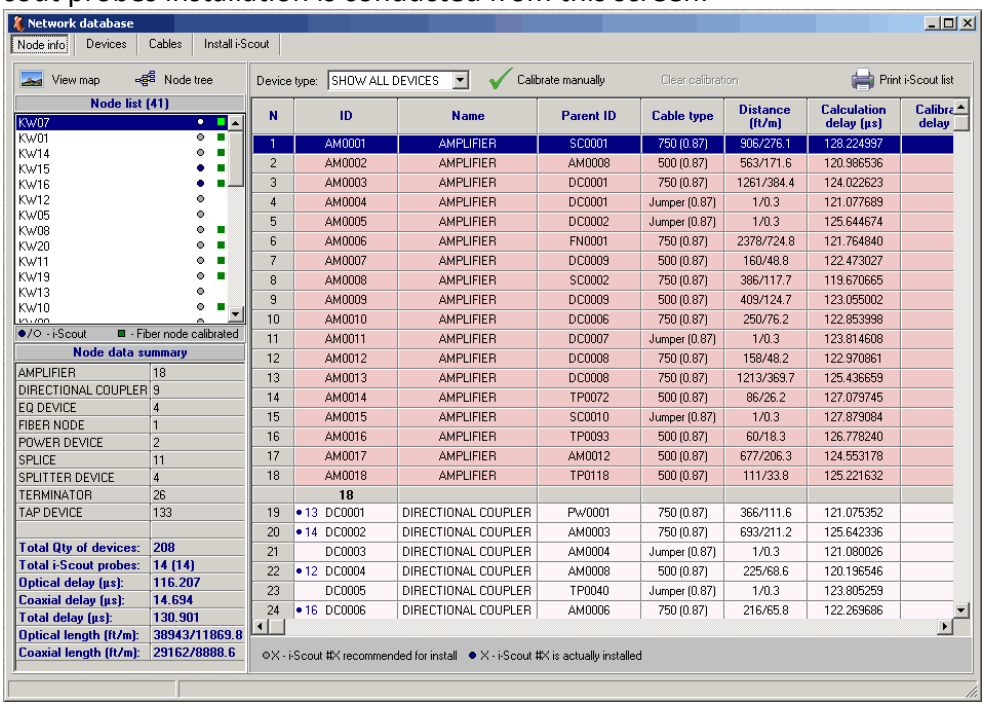
The screen below shows where these settings can be changed:



To save adjusted values click OK button the lower right hand corner of the window.

Network Database and i-Scout installation process

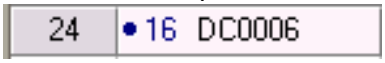
The i-Scout probes installation is conducted from this screen:



The following information regarding i-Scout is displayed on the network database screen:

- the number of the i-Scout probes planned and installed in a particular node:

- i-Scout probes actually installed are marked with a blue dot and the probe ID number next to the device ID of actual installation of the probe:



- information about probes recommended for installation, in this case instead of a blue dot a grey ring is used

- **Print i-Scout** list icon 

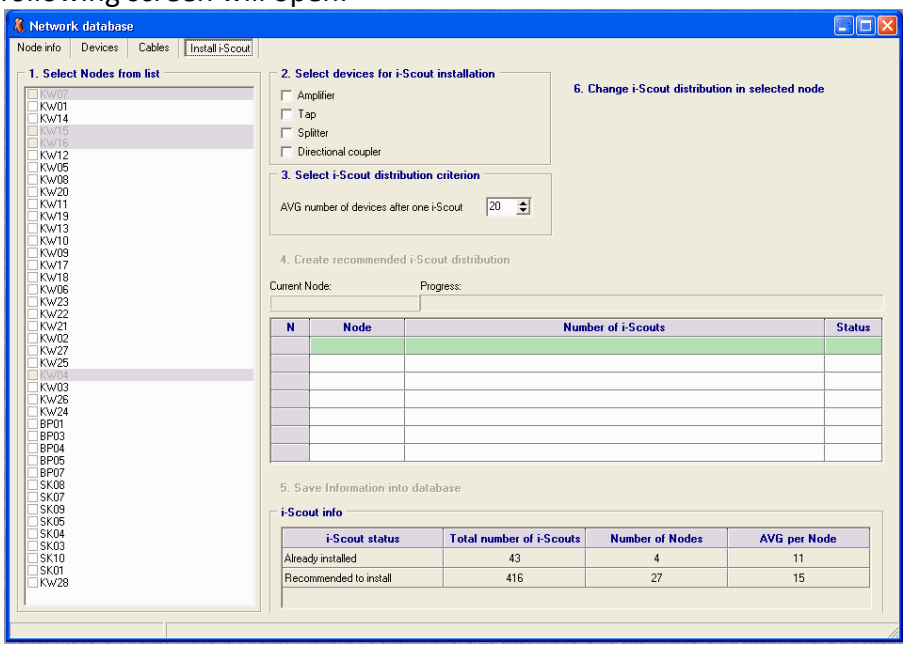
allows for generating a list of locations where the i-Scout probes are installed. THAT LIST MUST BE PRINTED FOR TECHNICIANS WHO WILL GO INTO THE FIELD TO PROGRAM AND INSTALL THE PROBES.

- **Node tree** icon 

will display a simplified schematic of the node with indicated i-Scout positions highlighted.

Install i-Scout tab

Before the i-Scout probes can be installed in the field, a list of their placements must be created. Locations for the probes will be analyzed and assigned by a special program feature available from the Install i-Scout tab. After clicking on Install i-Scout tab the following screen will open:



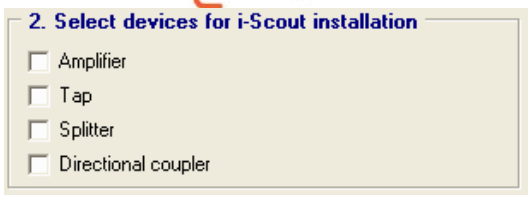
Preparing to create a distribution list for probe installation

In order to create a distribution list for a selected node, the node must be selected from the list on the left hand side of the screen first. It is possible to select node by node by checking the box on the left side of the node IDs, or all at once in the submenu which will open after pointing the mouse cursor on the list and clicking the right mouse button: 

.

Selecting devices for i-Scout installations

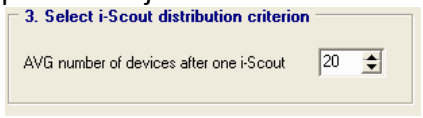
After selecting nodes, the next step is to select where the program can recommend to install the probes. Remember that at some amplifiers there is no possibility for installing the probe due to lack of the seizure screw access. The program will distribute the probes only on the device types marked on this screen part:



Typical choice will be that the *Tap*, *Splitter* and *Directional coupler* boxes are checked.

Selecting distribution criterion

The user then selects the number of devices which are located after the i-Scout probe site. This provides a method to limit the number of probes used as well as control the size of location zone after each probe. The number of the devices which are after the probe is adjustable in this screen:

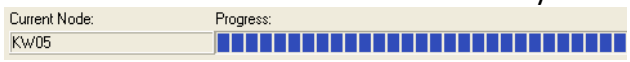


The lower the number, the smaller the zones created, therefore making problem location easier especially for ingress. The smaller the zone (the number of devices after each i-Scout), the greater the quantity of required probes.

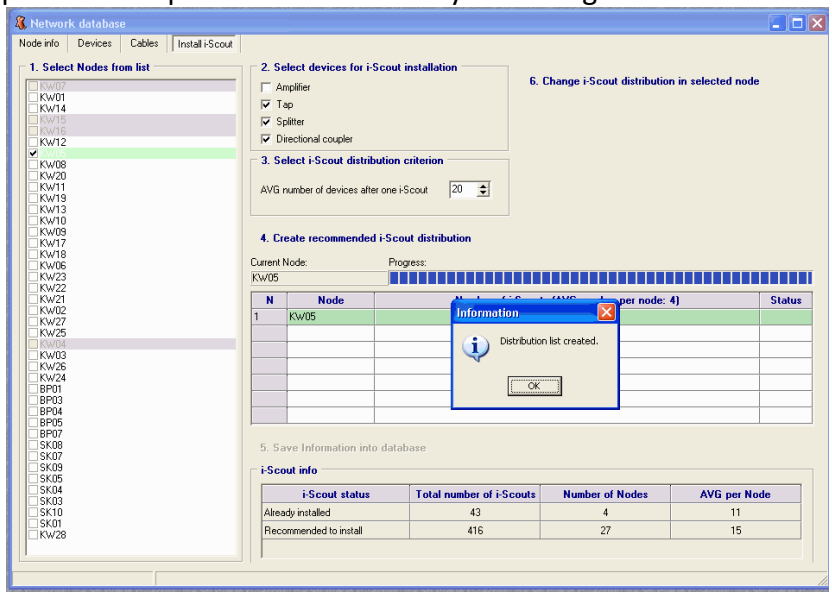
Creating distribution list for probes installation

After completing the above actions the

button will be highlighted. The list creation process starts after this button is clicked. Progress of calculations is shown by a blue expanding bar:



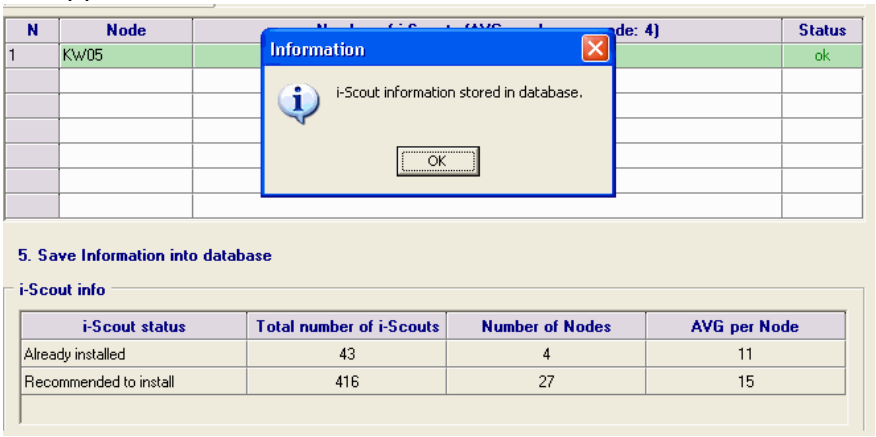
Successful process completion is indicated by a message “Distribution list created” on the screen:



In the information window the number of probes required for the selected node will be displayed.

Saving created list into the database

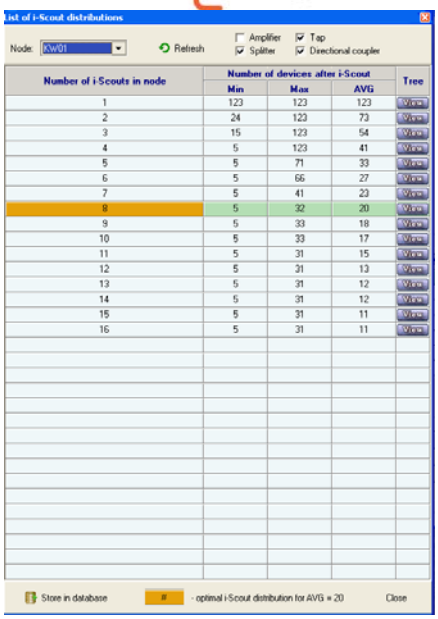
The next step is to save information into the database. Click on the OK button in the process end information window. Then a 5. Save Information into database button will become highlighted. Click on that button to save the list. Information about a successful process will appear.



In the i-Scout info screen portion, statistics for already distributed probe locations and for those recommended to install will be displayed.

Changing probes distribution in selected nodes

The way the probes are distributed can be easily changed. To change distribution click on the following button: 6. Change i-Scout distribution in selected node and the following screen will open:



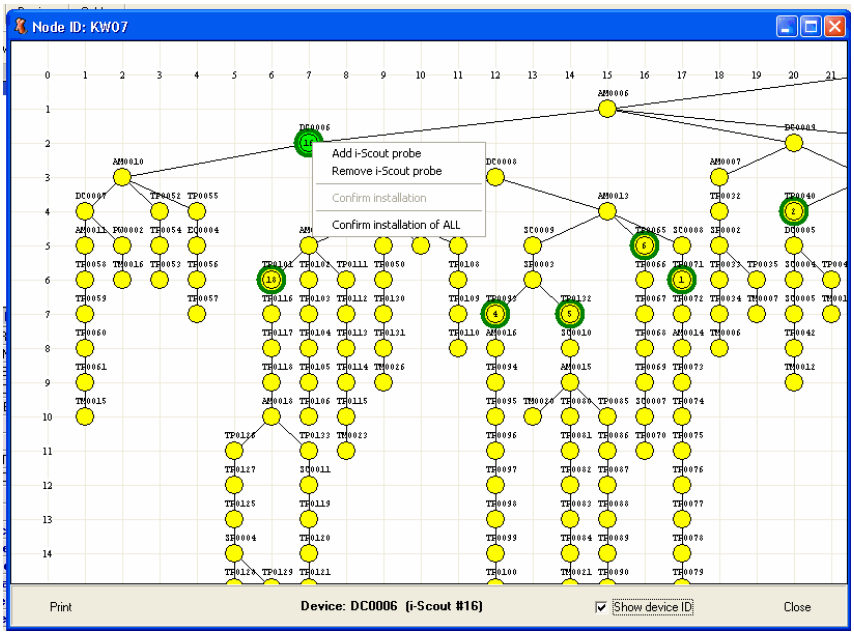
The node where changes need to be made can be selected here: 

After selecting the node click on the Refresh button: 

. The screen will open with optimal selection marked with orange color. The green color bar marking the row can be moved up and down thus selecting other zone configurations in a selected node. By clicking the 

button, the user gains access to the node tree view, which displays the node with the selected distribution criterion. The selected distribution scheme must be saved into the database by clicking the Store in database button. If you decide to move probes around, that can easily be done from the node tree screen that is accessible from the Network Database screen. Remember to use probe IDs selected by the software feature described here.

Node tree view screen



The i-Scout probe locations are marked with a green ring around the device where the particular probes were physically installed  and confirmed in the database. Probe sites selected for install but not confirmed in the database will be displayed with a grey ring.

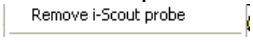
On the node tree screen an Administrator can perform the following actions:

Adding i-Scout probes from the node tree

To add an i-Scout probe at a device location, point to the device using the mouse cursor. The device will then turn green  and by clicking on the right mouse button the probe management menu will appear: 

In this menu the required action can be performed at the selected device location.

Removing i-Scout probes from the node tree

- i-Scout probes can be removed from a location in the system by selecting 

and confirming the selected action. The system will then not take in consideration that probe location.

Confirm i-Scout probe installation

The probe MUST BE PHYSICALLY INSTALLED IN THE FIELD at a desired location and ONLY THEN the administrator, after receiving confirmation from technicians that the installation was performed exactly at that location, can confirm installation of the probe in the system. This is conducted by accessing this screen, and at the required device select the Confirm installation button for a single probe or Confirm installation of ALL for all the probes in this node. It is advised that probes are confirmed one by one. Using the confirm all button may lead to mistakes and activating non-existing probes in the software.

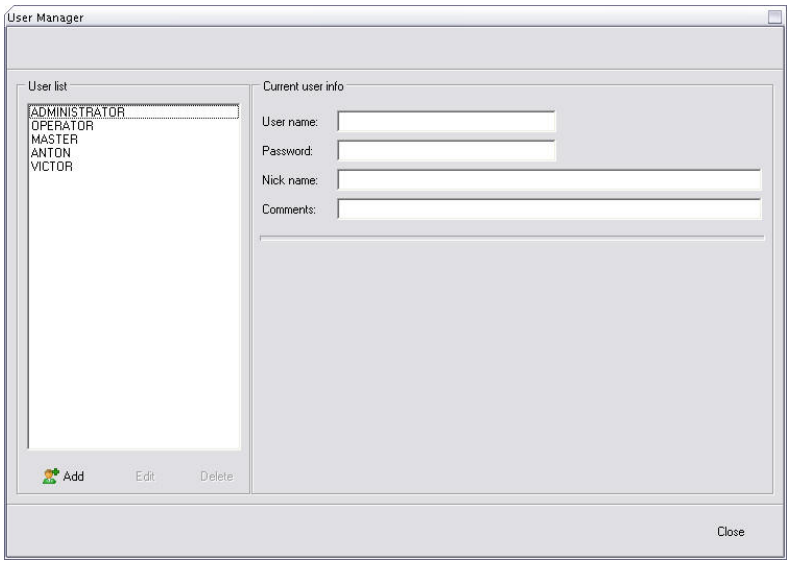
The above actions can be performed also in the main Network Database screen in the Xcor Admin.

Printing a node tree

The node tree can be printed by pressing Print in the left lower corner of the window.

User manager

In the user manager window, administrator can create new users, set passwords for them and delete user accounts.



Adding a new user

To add a new user in the system press the 

button.

In window:

Fill in all user name and password. In the Confirm cell repeat new user password, fill in other fields if necessary and press OK.
Remember that the "User name", "Password" and "Confirm" fields must be populated. The "Nick name" field can stay empty without compromising system audit and information exchange capabilities.

Changing user info settings

To change the user info setting, select the required user from the list in the “User list” window and press 

button.

In the **User info** window user parameters can be changed (change of password, the Nick name or Comments) after entering a valid user password in the field “Old password". If a valid user password is entered correctly, then field becomes white, in other case it will stay pink:

Remember that the **user name can not be changed.** In order to change the user name you have to delete the required user first, and then set up a new account with a new name.

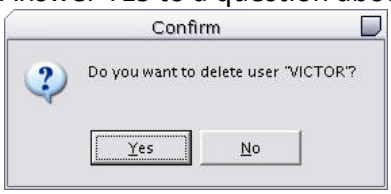
Attention! Do not leave the password field empty because the password is rerecorded with each editing. In order to make the user keep a valid password, it is necessary enter it again into the fields “Password” and “Confirm".
After the finishing editing press OK button.

User removal

In order to delete a user select required user from the list in the “User list“ window and press 

button.

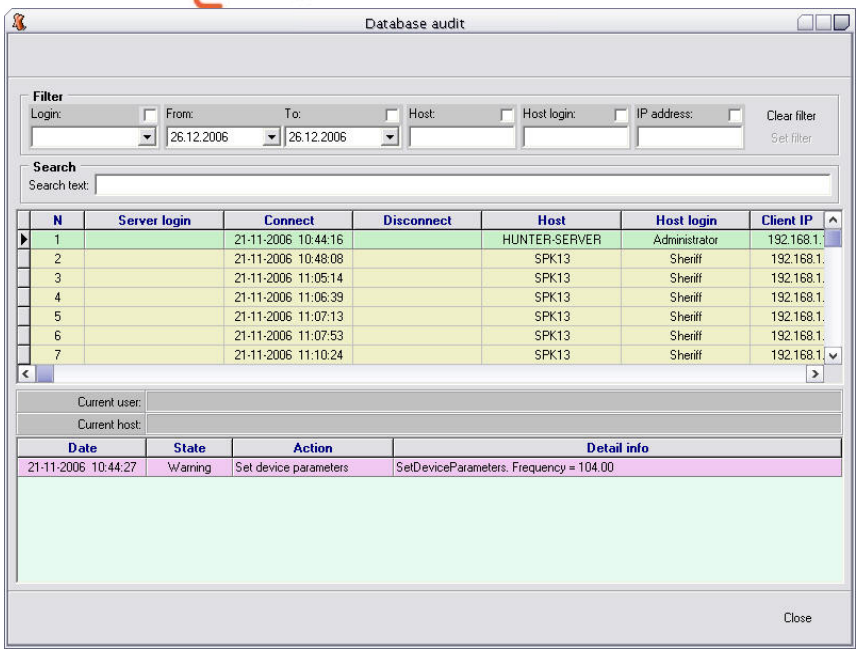
Answer YES to a question about confirmation of removal.



All user registration information will be removed. However, in the Audit connections and the actions of users, information about a deleted user will remain.

DB operation audit

The **DB operation audit** window contains general information on connections and actions of all users that have connected to the system. It is designed to track any changes that have been made.

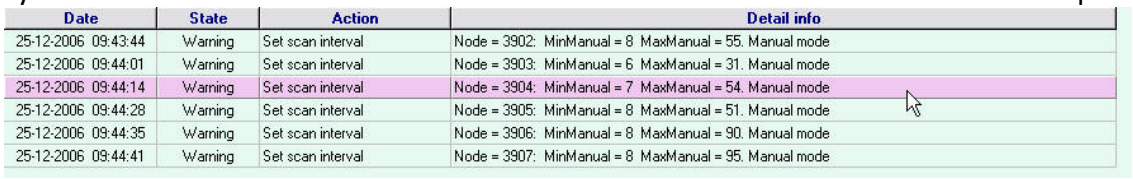


The Upper table contains the list of the users connections (and disconnections), sorted out by the time of connection.

Frame:

Contains brief information about the selected user and his IP address.

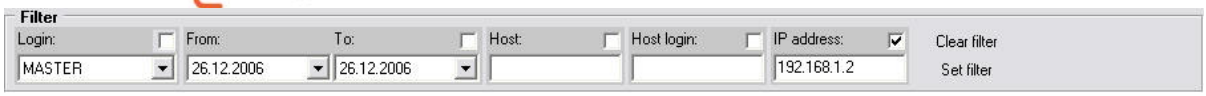
The lower table contains the user actions list for the entire connection session, sorted by the time the action was complete.



Date	State	Action	Detail info
25-12-2006 09:43:44	Warning	Set scan interval	Node = 3902: MinManual = 8 MaxManual = 55. Manual mode
25-12-2006 09:44:01	Warning	Set scan interval	Node = 3903: MinManual = 6 MaxManual = 31. Manual mode
25-12-2006 09:44:14	Warning	Set scan interval	Node = 3904: MinManual = 7 MaxManual = 54. Manual mode
25-12-2006 09:44:28	Warning	Set scan interval	Node = 3905: MinManual = 8 MaxManual = 51. Manual mode
25-12-2006 09:44:35	Warning	Set scan interval	Node = 3906: MinManual = 8 MaxManual = 90. Manual mode
25-12-2006 09:44:41	Warning	Set scan interval	Node = 3907: MinManual = 8 MaxManual = 95. Manual mode

Filtering

For filtering the list by required criterion, in the “Filter“portion of the window indicate the necessary filter parameters and press the Set filter button.



Login - filter by user login (logins are selected from the list of those permitted);

From - To - filter by the time of connection

Host - filter by the computer name from which the user was accessing the server;

Host login - filtering by user login on the computer from the connection was made;

IP address - filtering by IP address of the user computer.

For clearing the filter press 

button.

Searching for records in the list

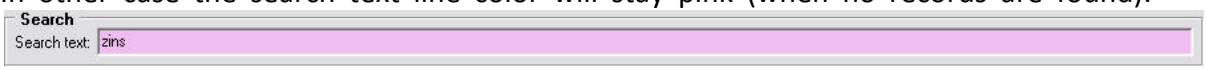
Record searching is possible only in the user connections (disconnection) list. Information search criterion is set by the text entered in the search line.

Search is register-independent.

If a line which satisfies the search condition is found, then it will become activated and highlighted in the table.

N	Server login	Connect	Disconnect	Host	Host login	Client IP	External IP
204	MASTER	30-11-2006 15:52:49		SPK13	Sheriff	192.168.1.14	192.168.1.14
205	MASTER	01-12-2006 07:46:40		SPK13	Sheriff	192.168.1.14	192.168.1.14
206	MASTER	01-12-2006 09:36:23		SPK13	Sheriff	192.168.1.14	192.168.1.14
207	ADMINISTRATOR	01-12-2006 10:07:19		ZINEVICH	User	192.168.1.2	192.168.1.2
208	ADMINISTRATOR	01-12-2006 10:24:23		ZINEVICH	User	192.168.1.2	192.168.1.2
209	MASTER	01-12-2006 10:37:44		SPK13	Sheriff	192.168.1.14	192.168.1.14
210	MASTER	01-12-2006 10:38:12		SPK13	Sheriff	192.168.1.14	192.168.1.14
211	MASTER	01-12-2006 10:39:40		SPK13	Sheriff	192.168.1.14	192.168.1.14

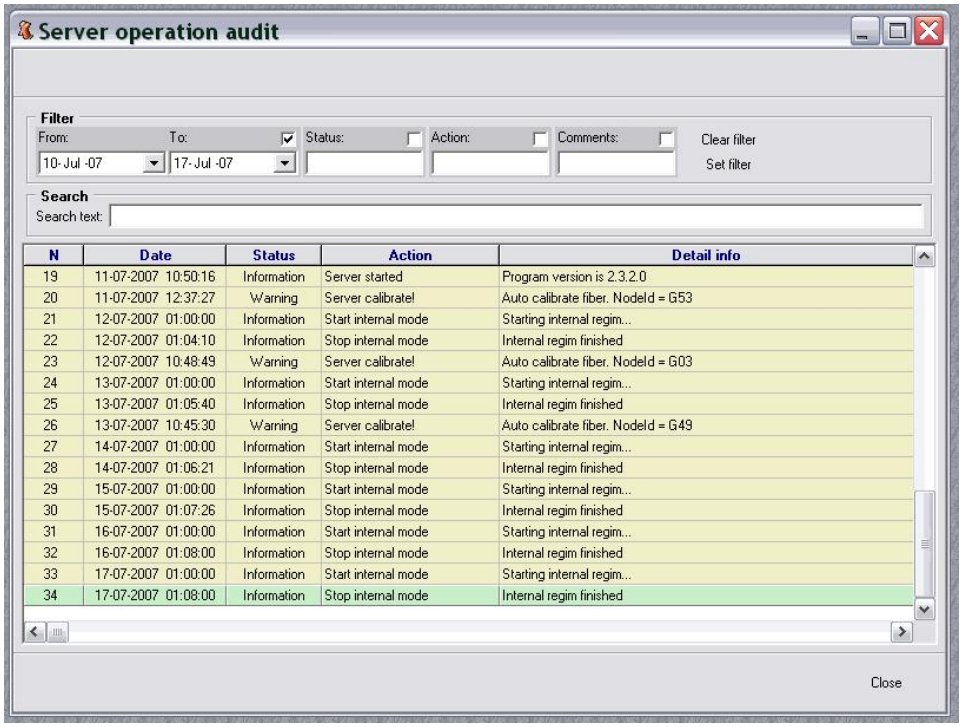
In other case the search text line color will stay pink (when no records are found):



One should remember that the search is conducted only along the fields "Client IP", "Server login", "Host" and "Host login" in the indicated order.

Server Operation Audit

The **Server operation audit** window contains general information about the conditions of the server, automatic Fiber node calibrations, and starting and the stopping of the server.



List filtering

For filtering the list by the given parameters, in the "Filter" area check the desired item and press the *Set filter* button.

Filter settings:
From - *To* - filter by the time of connection;
Status - filter by the status type of the message;
Action - filtering by the action type of the message;
Comments - filtering by comments.
For clearing the filter press *Clearfilter* button.

Searching through the records list

Record searching is possible only in the user connections (disconnection) list. Information search criterion is set by the text entered in the *Search text* line.

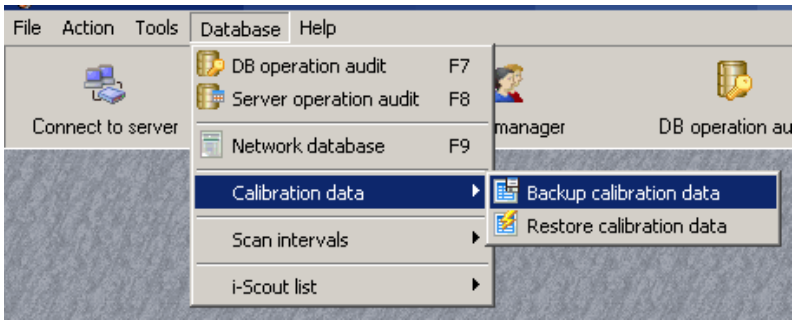
Search is register-independent.

If a line which satisfies the search condition is found, then it will become activated and highlighted in the table with green color. In other case the *Search text* line color will stay pink (when no records are found).

Calibration data management

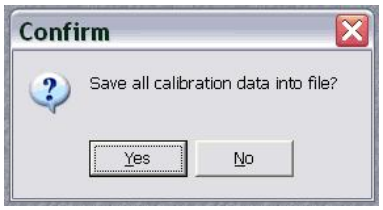
Calibration data contains very important information about measured time delays associated with reference sites in the cable plant. This information can be very expensive if lost because it would be necessary to again visit calibration points and measure time delays to necessary components. This is recommended to save calibration data and preserve it in a safe place to be available should any calibration data become corrupt.

Access to backup features is available from the following main screen:

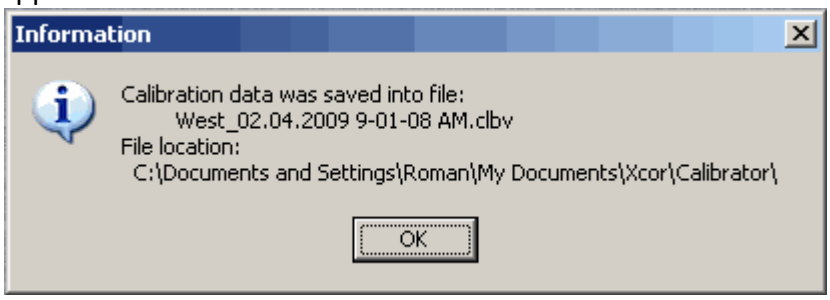


Backup calibration data

For saving the calibration data of all nodes of system into a file, select the menu item "Database" -> “Calibration data” -> "Backup calibration data".



In confirmation window click Yes button.
After saving the calibration data, the screen message with information of saved file will appear.

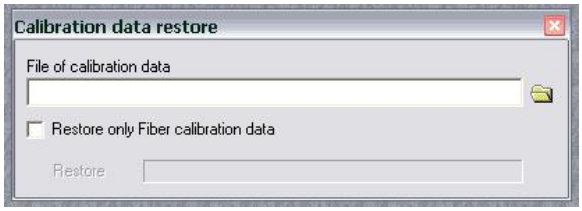


The calibration data files will be saved into folder "Documents and Settings\User\My Documents\Xcor\Calibrator\" with format of <Hub Name>_ <date> <time>.clbv
For example: TOWN SQUARE_07.11.2008 7-35-44 PM.clbv

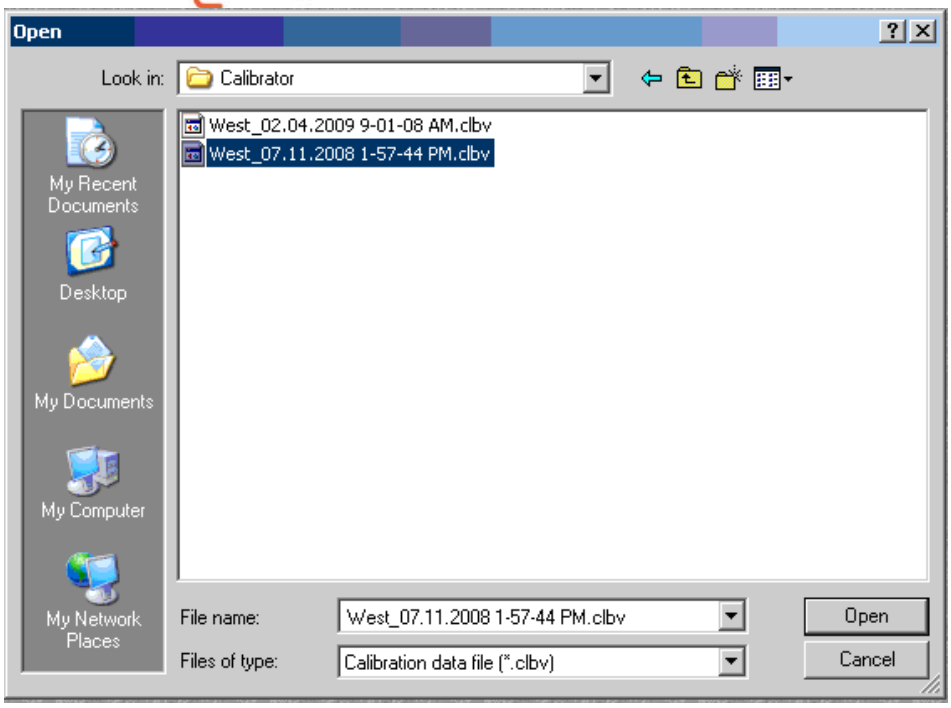
Restoring Calibration Data

For restoring from file the calibration data of all nodes, select the menu item "Database" -> “Calibration data”->"Restore calibration data".

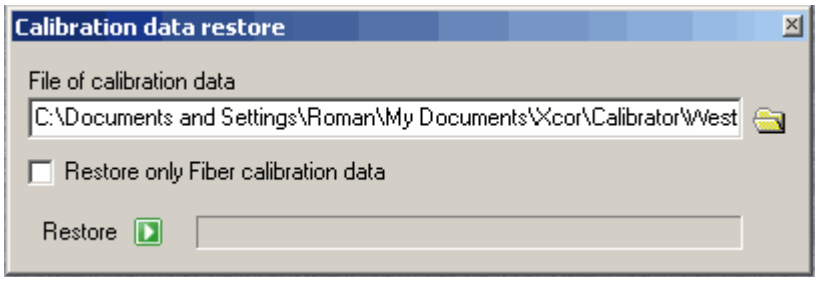
In confirmation window click the Yes button.
The following screen will appear:

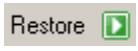


Left click on the folder icon then select the file in \Xcor\Calibrator folder:



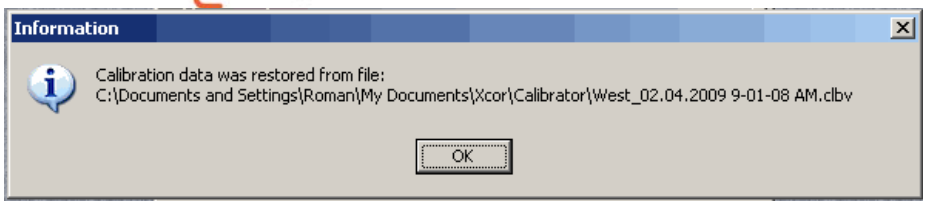
Open the file with required calibration data. Confirm that the required file will be used in the process.



Select (if necessary) the check box "Restore only Fiber calibration data" . Then left click  button to start the process.

Remark: Restoring the fiber only data is very useful when recovering the data base from wrong calibration made on devices other than fiber nodes.

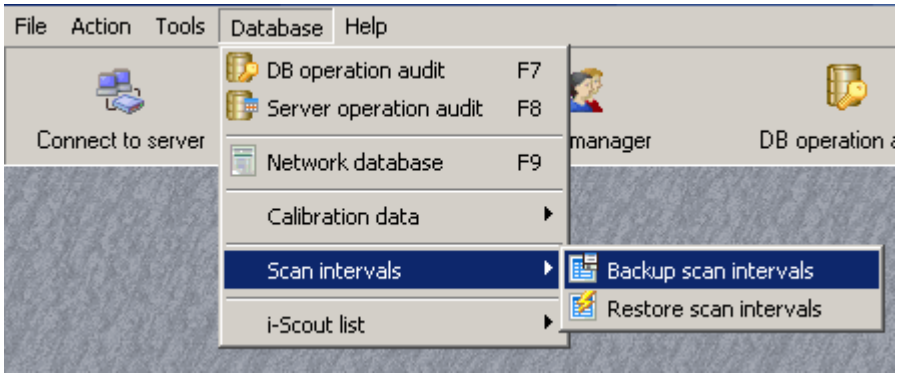
After the restoring operation, the screen message with information of status will appear.



Scan intervals data management

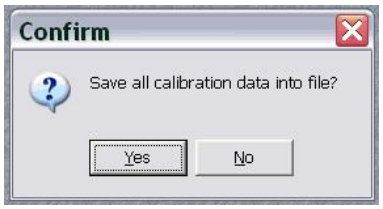
Scan intervals data is related to calibrations and contains very important information about the time delay ranges associated with coax length of the nodes. This information can be very expensive if lost because it would be necessary to again visit calibration points and measure time delays and adjust scanning ranges for all necessary nodes. It is recommended to save scan intervals data and preserve it in a safe place to be available should any calibration data become corrupt.

Access to backup features is available from the following main screen:

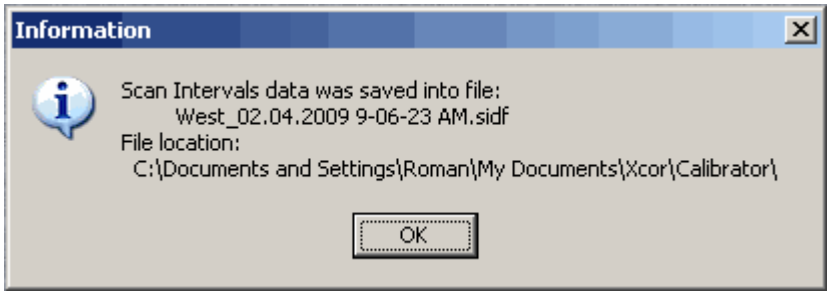


Backup scan intervals

For saving the calibration data of all nodes of system into a file, select the menu item "Database" -> “Scan intervals” -> "Backup scan intervals".



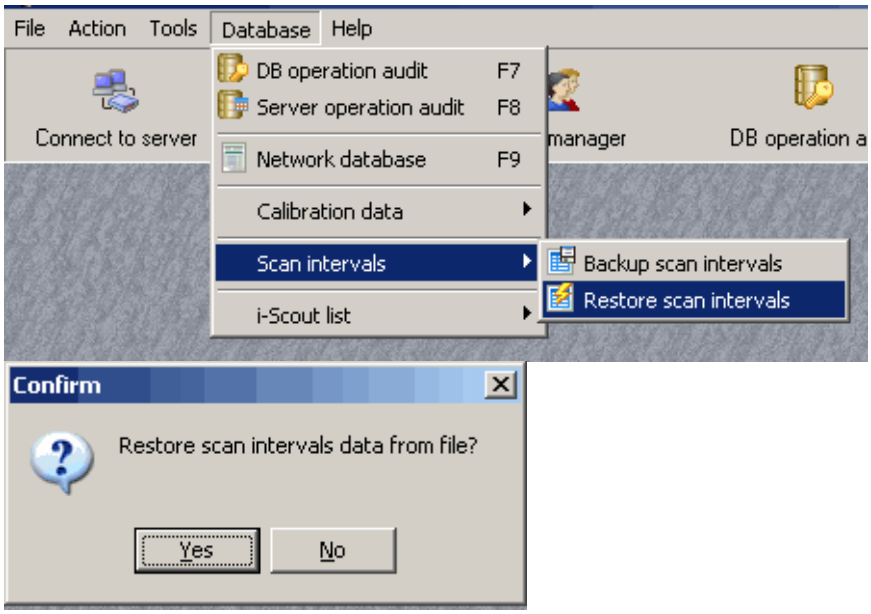
In confirmation window click Yes button.
After saving the calibration data, the screen message with information of saved file will appear.



The Scan Intervals data files will be saved into folder "Documents and Settings\User\My Documents\Xcor\ScanIntervals\" with format of <Hub Name>_ <date> <time>.sidf For example: TOWN SQUARE_07.11.2008 1-57-12 PM.sidf

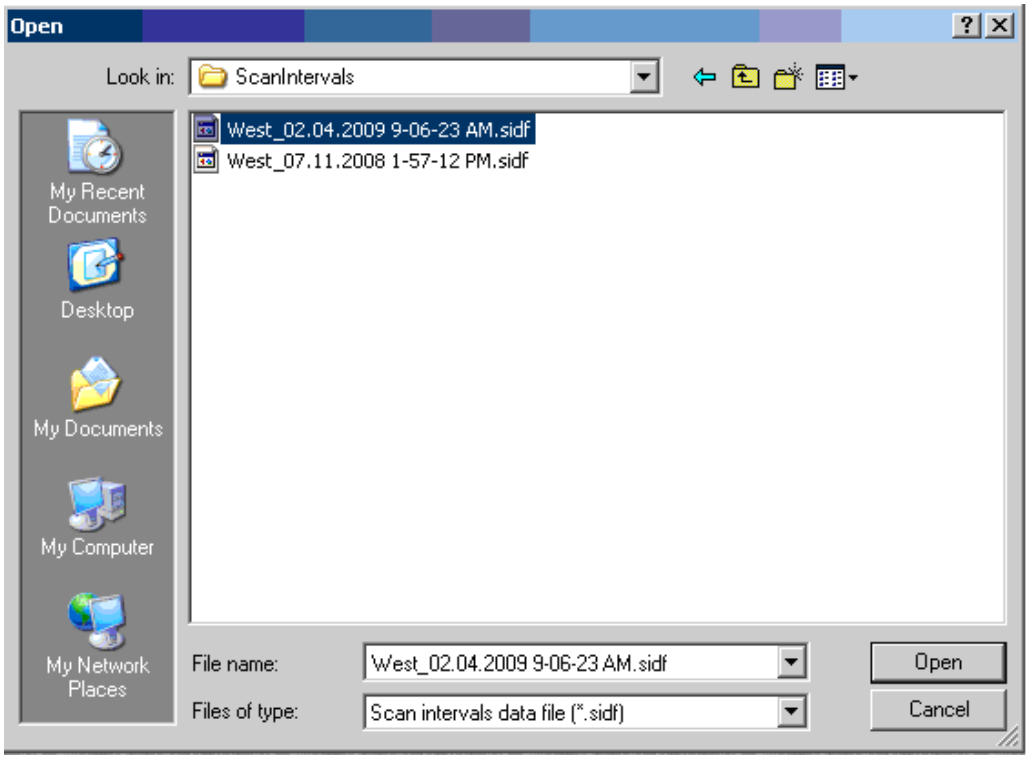
Restoring scan intervals data

For restoring from file the calibration data of all nodes, select the menu item "Database" -> “Scan intervals”->"Restore scan intervals".

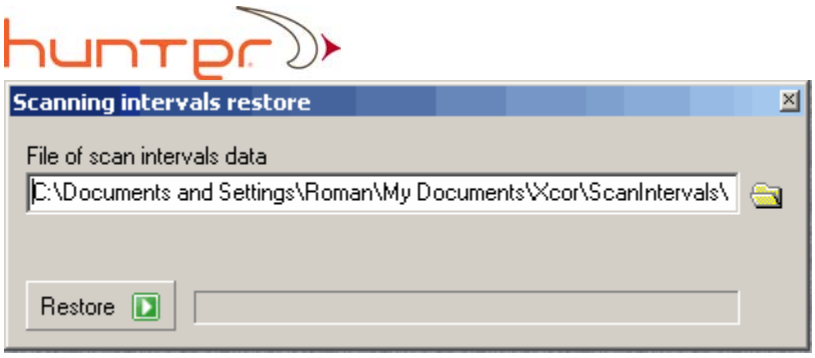


In confirmation window click the Yes button.
The following screen will appear:

Left click on the folder icon then select the file in \Xcor\ScanIntervals folder:

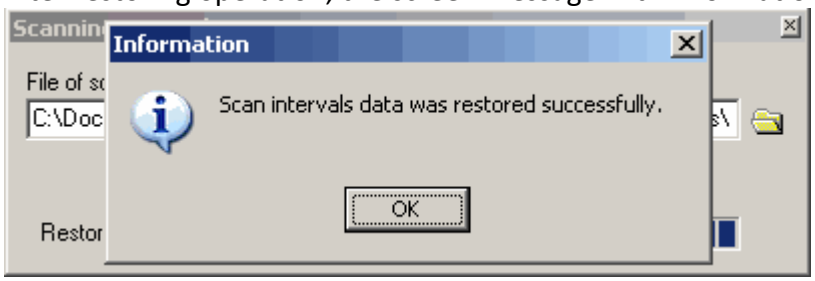


Open the file with required Scan intervals data. Confirm that the required file will be used in the process.



Left click Restore button to start the process.

After restoring operation, the screen message with information of status will appear.

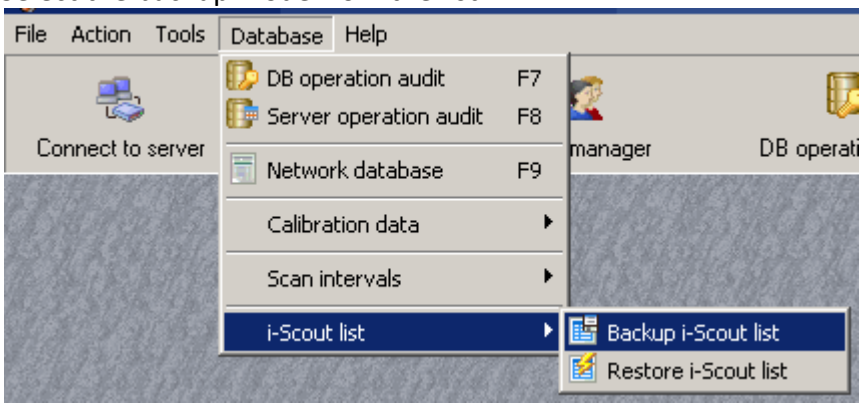


i-Scout install data management

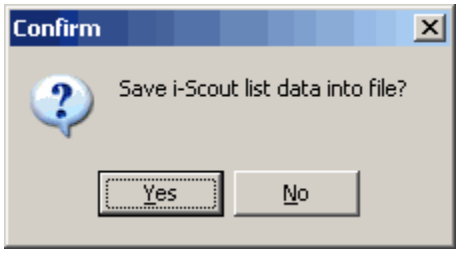
Information about the sites where i-Scout probes are installed and about their IDs is extremely important. Losing information about the probe locations would render them useless and would necessitate the time and expense of an audit to recreate. To avoid this, the i-Scout list containing probe ID and location in the network should be saved into a backup file and stored on a safe device should damage to the server occur.

Saving i-Scout list into a backup file

Select the backup mode from the list:

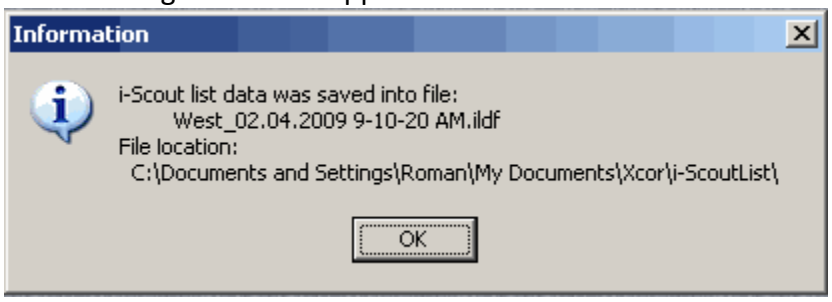


In confirmation window:



click the Yes button.

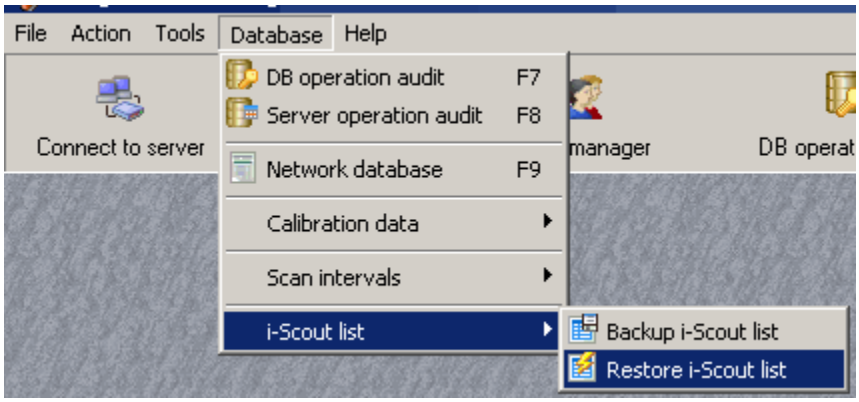
The following screen will appear:

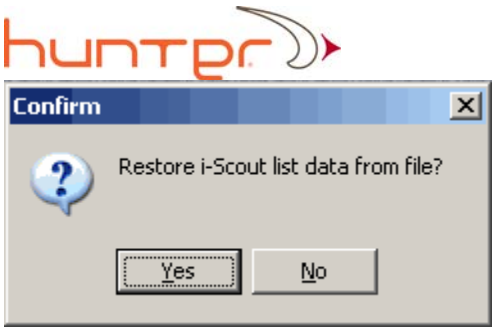


The i-Scout List data files will be saved into folder "Documents and Settings\User\My Documents\Xcor\i-ScoutList\" with format of <Hub Name>_ <date> <time>.ildf For example: TOWN SQUARE_07.11.2008 7-35-44 PM.ildf

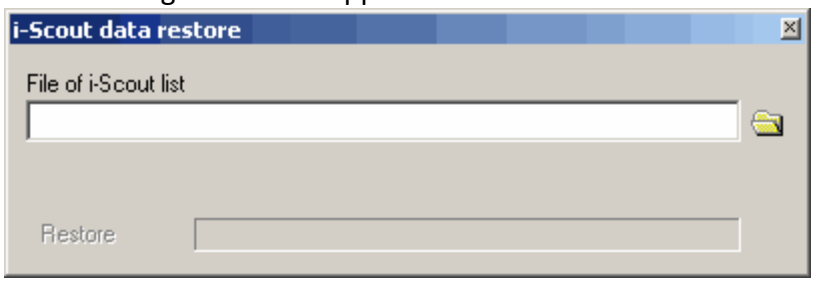
Restoring i-Scout List from a backup file

For restoring from file the calibration data of all nodes, select the menu item "Database" -> “i-Scout list”->"Restore i-Scout list".

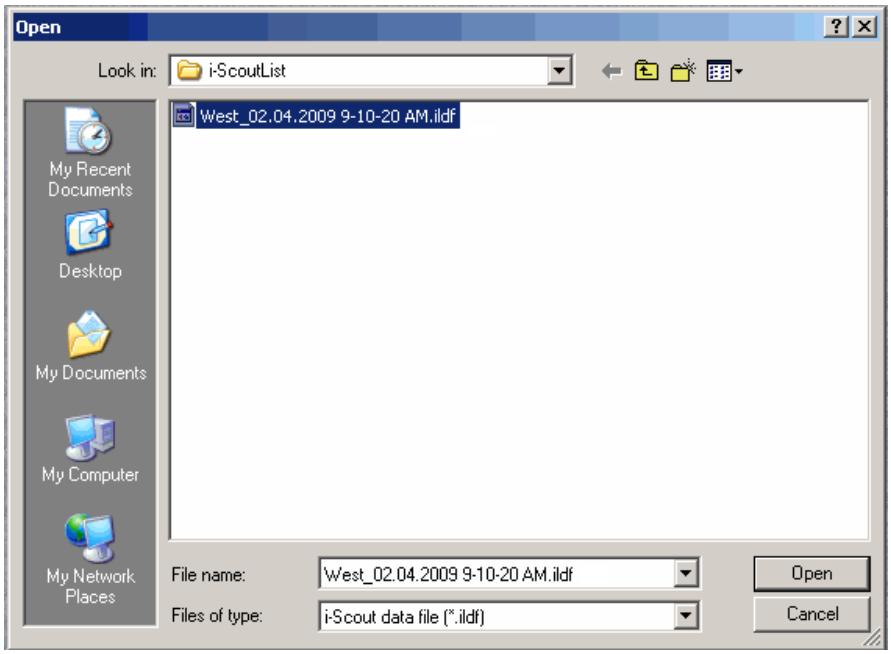




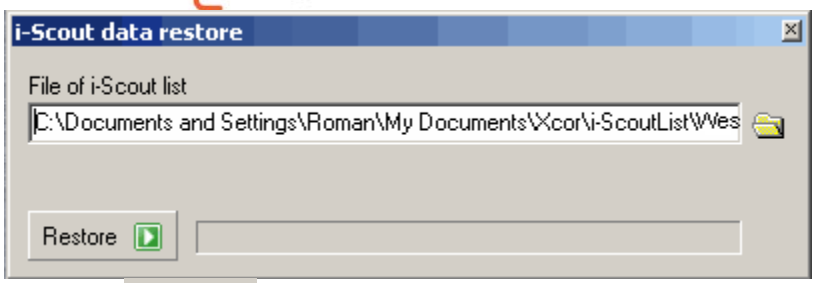
In confirmation window click the Yes button.
The following screen will appear:

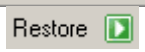


Left click on the folder icon then select the file in \Xcor\i-ScoutList folder:



Open the file with required i-ScoutList data. Confirm that the required file will be used in the process.



Left click  button to start the process.

After restoring operation, the screen message with information of status will appear.