



**ONMSi**  
**Optical Network Monitoring System**  
User's Guide





# **ONMSi**

## **Optical Network Monitoring System**

### User Manual



Viavi Solutions  
1-844-GO-VIAVI  
[www.viavisolutions.com](http://www.viavisolutions.com)

---

## **Notice**

Every effort was made to ensure that the information in this document was accurate at the time of printing. However, information is subject to change without notice, and Viavi reserves the right to provide an addendum to this document with information not available at the time that this document was created.

## **Copyright**

© Copyright 2009-2016 Viavi, LLC. All rights reserved. Viavi, Enabling Broadband and Optical Innovation, and its logo are trademarks of Viavi, LLC. All other trademarks and registered trademarks are the property of their respective owners. No part of this guide may be reproduced or transmitted electronically or otherwise without written permission of the publisher.

## **Trademarks**

Viavi and ONMSi are trademarks or registered trademarks of Viavi in the United States and/or other countries.

Microsoft, Windows, Windows CE, and Microsoft Internet Explorer are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Oracle and Java are either trademarks or registered trademarks of Oracle Corporation in the United States and/or other countries.

Firefox is a registered trademark of Mozilla Foundation in the United States and/or other countries.

Google Chrome is a registered trademark of Google Incorporation in the United States and/or other countries.

Specifications, terms, and conditions are subject to change without notice. All trademarks and registered trademarks are the property of their respective companies.

## **Ordering information**

This guide is a product of Viavi's Technical Information Development Department.

## **WEEE Directive Compliance**

Viavi has established processes in compliance with the Waste Electrical and Electronic Equipment (WEEE) Directive, 2002/96/EC.

This product should not be disposed of as unsorted municipal waste and should be collected separately and disposed of according to your national regulations. In the European Union, all equipment purchased from Viavi after 2005-08-13 can be returned for disposal at the end of its useful life. Viavi will ensure that all waste equipment returned is reused, recycled, or disposed of in an environmentally friendly manner, and in compliance with all applicable national and international waste legislation.

---

It is the responsibility of the equipment owner to return the equipment to Viavi for appropriate disposal. If the equipment was imported by a reseller whose name or logo is marked on the equipment, then the owner should return the equipment directly to the reseller.

Instructions for returning waste equipment to Viavi can be found in the Environmental section of Viavi's web site at [www.viavisolutions.com](http://www.viavisolutions.com). If you have questions concerning disposal of your equipment, contact Viavi's WEEE Program Management team.





# Table of Contents

<b>About This Guide</b>	<b>xiii</b>
Purpose and scope .....	xiv
Assumptions .....	xiv
Technical assistance .....	xiv
Recycling Information .....	xiv
Conventions .....	xiv
<b>Chapter 1 ONMSi Overview</b>	<b>1</b>
Introduction .....	2
ONMSi Benefits .....	2
ONMSi Features .....	2
ONMSi Architecture .....	3
<b>Chapter 2 ONMSi login and general view</b>	<b>5</b>
Pre-requisite .....	6
Log-in .....	6
Audit logs .....	7
General User Interface .....	7
Text colors .....	8
Shortcuts panel .....	8
Tree view .....	9
Description of the objects in the Tree .....	10
Alarm viewer .....	10
Keyboard shortcuts .....	11
<b>Chapter 3 Setting the Server address</b>	<b>13</b>
Setting up the server address .....	14
<b>Chapter 4 Adding an OTU</b>	<b>15</b>
Adding an OTU .....	16
Testing the connection and refreshing the configuration .....	16
Configuring the OTU .....	18

	Associating OTU address to server .....	18
	Launching an Autotest of the OTU .....	18
	Moving the OTU .....	19
	Replacing an OTU .....	19
<b>Chapter 5</b>	<b>Monitoring a link</b>	<b>21</b>
	Optical Link monitoring principle .....	22
	Provisioning the link .....	22
	Reference trace display .....	24
	Changing the reference trace .....	24
	Landmark setting .....	25
	Checking long term degradation .....	26
<b>Chapter 6</b>	<b>Displaying the alarms</b>	<b>27</b>
	Alarms view .....	28
<b>Chapter 7</b>	<b>Trace Viewer</b>	<b>29</b>
	Opening a trace using the Trace Browser .....	30
	Trace display .....	31
	Zooming on trace .....	31
	Positioning Markers .....	31
	First and Last markers .....	31
	A & B markers .....	32
	Optical events .....	32
	Trace details .....	32
	Displaying the events table .....	33
	Changing the trace color .....	34
	Multi-trace display .....	34
	Adding trace(s) .....	34
	Multi-traces display .....	34
	Changing the active trace and the trace color .....	35
	Trace and events table .....	35
<b>Chapter 8</b>	<b>Managing users</b>	<b>37</b>
	Adding a user .....	38
	Adding a «standard» user .....	38
	Creating a user with LDAP .....	39
	Defining the system and domain roles for the user .....	40
	System and Domain roles principle .....	40
	Creating a System or Domain role .....	41
	Assigning System roles to a user .....	42
	Assigning Domain roles to a user .....	42
	Changing the current user preferences .....	43
	Changing the user password .....	43
	Changing the excel version to be used .....	44
	Modifying the notification address .....	44
	Displaying desktop alert .....	45



	Displaying the connected users.....	46
<b>Chapter 9</b>	<b>Managing domains</b>	<b>47</b>
	Domain principle.....	48
	Creating a domain.....	48
	Adding sub-domains.....	49
	Copying an OTU to another domain.....	50
	Removing an OTU from a domain.....	50
	Deleting an OTU.....	51
	Copying a link to a domain.....	51
<b>Chapter 10</b>	<b>Advanced Monitoring</b>	<b>53</b>
	Advanced Setup.....	54
	Localization distinct from detection.....	54
	Fault distance change notification.....	56
	Downloading budget data.....	57
	Scheduling a test.....	57
	Stopping the test / all tests and forbid any shoot on the link.....	58
	Performing a test on demand.....	59
	Advanced Monitoring.....	59
	Modifying the attenuation thresholds.....	59
	Alarms on test attenuation.....	60
	Fiber length extension.....	60
	New peaks.....	61
	Existing peaks.....	63
	ORL.....	64
	Both end measurement.....	65
	Cable Documentation.....	66
	Activating the Cable documentation function.....	67
	Activating the Association landmarks and optical events.....	67
	Completing the landmark table.....	67
	Creating a landmark table from a trace.....	68
	Create a landmarks table from an Excel file.....	69
	Associating Landmark and Optical Event.....	70
	Splitting section.....	72
	Associating a geographical file to a link.....	73
	Adding an OTU to a schematic.....	75
	Adding an OTU to the schematic.....	75
	Displacing the OTU on schematic.....	76
	Centering the OTU on schematic.....	76
	Displaying the dashboard of an OTU alarm from the schematic.....	76
<b>Chapter 11</b>	<b>Alarms management</b>	<b>77</b>
	Alarms Display.....	78
	Alarms Viewer.....	78
	Alarms details.....	78
	Actions on alarms.....	79
	Changing the alarm severity.....	79

Acknowledging an alarm .....	79
Clearing an alarm .....	80
Downloading a pdf file of the alarm (detail view) .....	80
Alarm History (detail view) .....	81
Injection alarm.....	81
Deleting an alarm (detail view) .....	82
Actions on table display .....	82
Filtering the alarms in the table .....	82
Configuring the alarms table .....	83
Downloading the alarms table.....	84
Other actions on table .....	85
Notification by e-mail of an alarm .....	85
Alarm Desktop alert .....	85
Installing the extension in Google Chrome TM .....	86
Configuring the desktop alerts .....	87
Display of the desktop alerts.....	87
Disabling or removing the Desktop Alert extension .....	88
<b>Chapter 12 Tables and Reports Management</b> .....	<b>91</b>
Downloading data from a table / list.....	92
Configuring the table .....	92
Downloading the data from a table .....	92
Inventory Report.....	93
Generating reports .....	94
Displaying reports templates.....	94
Creating a report .....	94
Launching the report.....	96
<b>Chapter 13 System settings</b> .....	<b>99</b>
Configuring and launching a manual purge.....	100
Configuring an automatic purge .....	100
Configuring server advanced parameters.....	101
Users .....	101
Defining the session duration .....	101
Configuring the LDAP.....	102
Configuring the password policy .....	103
Password quality.....	104
Password history.....	105
Account lockout.....	106
Password expiration.....	106
Advanced configuration .....	106
Point to Point Configuration.....	106
Point to Point General configuration.....	106
Landmarks & optical events configuration .....	107
Monitoring configuration .....	107
Configuring e-mail/sms alert profiles.....	108
Defining Escalation .....	108
Defining filters for the e-mail notifications .....	109

	Configuring the e-mail format .....	110
	Configuring Desktop alert profiles.....	111
	Additional Attributes.....	112
	Configuring an object with additional attributes.....	113
	Displaying and completing the attribute .....	114
	Downloading a schematic.....	114
	Scripts.....	115
<b>Chapter 14</b>	<b>ONMSi System Requirements</b>	<b>117</b>
	ONMSi Server .....	118
	ONMSi Web Client .....	118
	ONMSi Network .....	118
	High availability (option).....	118
	Optical Fiber Mapping (option) .....	119
	Alert notification (option) .....	119
	SNMP Interface (option).....	119
	Web service Interface (option).....	120
	Access from a mobile phone via internet.....	120
	Light Directory Access protocol (LDAP).....	120
<b>Appendix A</b>	<b>Application Programming Interfaces</b>	<b>121</b>
	Content of the Online Help for SNMP API.....	122
	Content of the Online Help for Web Services API .....	124
	SOAP Web Service API .....	124
	Rest Web Service API .....	125
<b>Appendix B</b>	<b>Software License Terms</b>	<b>127</b>
<b>Appendix C</b>	<b>ONMSi Toolkit</b>	<b>133</b>
	Introduction to ONMSi toolkit.....	134
	Configuring the System .....	135
	Dashboard description .....	136
	Backup and Restore the Database .....	137
	Performing a manual Backup.....	137
	Restoring the database .....	137
	Using the OTU Toolkit.....	137
	Testing the remote access to the OTU(s) installed .....	138
	Downloading the logs files for an OTU .....	138
	Updating the OTU .....	139
	Transferring the update files .....	139
	Updating the OTU(s) .....	140
	High Availability Solution .....	141
	Fail over main points and Pre-requisites .....	141
	Main points .....	141
	Pre-requisites .....	141

Activities .....	141
Main service (ONMSi_HAS) activities.....	141
WatchDog service (ONMSi_HAS_WatchDog) activities.....	142
Monitoring principles .....	142
Fail-over conditions in automatic mode.....	142
Failing-over process in automatic mode.....	143
Maintenance issues .....	143
Server's Status.....	144
Activating the passive server.....	144
Alarms.....	144

<b>Index</b>	<b>147</b>
--------------	------------



# About This Guide

Topics discussed in this chapter are as follows:

- [“Purpose and scope” on page xiv](#)
- [“Assumptions” on page xiv](#)
- [“Technical assistance” on page xiv](#)
- [“Recycling Information” on page xiv](#)
- [“Conventions” on page xiv](#)

## Purpose and scope

The purpose of this guide is to help you successfully use the ONMSi features and capabilities. This guide includes task-based instructions that describe how to configure and use the ONMSi. Additionally, this guide provides a complete description of Viavi's terms and conditions of the licensing agreement.

## Assumptions

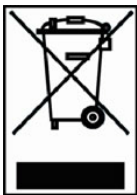
This guide is intended for experienced users and administrators who want to implement ONMSi effectively and efficiently. It is recommended to attend the ONMSi training to learn how to install, configure, use, and troubleshoot the ONMSi.

## Technical assistance

If you require technical assistance, call 1-844-GO-VIAMI. For the latest TAC information, go to <http://www.viavisolutions.com/en/services-and-support/support/technical-assistance>.

## Recycling Information

Viavi recommends that customers dispose of their instruments and peripherals in an environmentally sound manner. Potential methods include reuse of parts or whole products and recycling of products components, and/or materials.



### Waste Electrical and electronic Equipment (WEEE) Directive

In the European Union, this label indicates that this product should not be disposed of with household waste. It should be deposited at an appropriate facility to enable recovery and recycling.

## Conventions

This guide uses naming conventions and symbols, as described in the following tables.

**Table 1** Typographical conventions

Description	Example
User interface actions appear in this typeface.	On the Status bar, click <b>Start</b>

**Table 1** Typographical conventions (Continued)

Description	Example
Buttons or switches that you press on a unit appear in this <b>TYPEFACE</b> .	Press the <b>On</b> switch.
Code and output messages appear in this <b>typeface</b> .	All results okay
Text you must type exactly as shown appears in this <b>typeface</b> .	Type: a : \set.exe in the dialog box.
Variables appear in this <b>typeface</b> .	Type the new <b>hostname</b> .
Book references appear in this <b>typeface</b> .	Refer to <b>Newton's Telecom Dictionary</b>
A vertical bar   means "or": only one option can appear in a single command.	platform [a b e]
Square brackets [ ] indicate an optional argument.	login [platform name]
Slanted brackets < > group required arguments.	<password>

**Table 2** Keyboard and menu conventions

Description	Example
A plus sign + indicates simultaneous key-strokes.	Press <b>Ctrl+s</b>
A comma indicates consecutive key strokes.	Press <b>Alt+f,s</b>
A slanted bracket indicates choosing a sub-menu from menu.	On the menu bar, click <b>Start &gt; Program Files</b> .

**Table 3** Symbol conventions



**NOTE**This symbol represents a general hazard.



**WARNING**

This symbol represents a risk of electrical shock.



**NOTE**

This symbol represents a Note indicating related information or tip.



This symbol, located on the equipment or its packaging, indicates that the equipment must not be disposed of in a land-fill site or as municipal waste, and should be disposed of according to your national regulations.

**Table 4** Safety definitions



**WARNING**

Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.



**CAUTION**

Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.



# ONMSi Overview

This chapter provides a general description of the ONMSi.

Topics discussed in this chapter include the following:

- [“Introduction” on page 2](#)
- [“ONMSi Architecture” on page 3](#)

## Introduction

The explosion of voice, video and data anywhere and anytime means that Network Service Providers need constant availability and performance from their fiber optic network.

The ability to provide quad/triple play and PON (Passive Optical Network) architectures with optical splitters had made fiber monitoring an even bigger challenge.

Viavi ONMSi is an Optical Network Monitoring System that expands network visibility right from the Core across the PON and into the premise improving Operational Support and Quality of Service (QoS) for any type of network.

ONMSi is a remote fiber test system that scans the fiber network 24/7 and automatically detects & locates faults without having to dispatch technicians in the field.

Based on Viavi's leading optical technologies, an Optical Test unit (OTU) integrating an Optical Time Domain Reflectometer (OTDR) and an Optical Switch constantly compares data to a baseline and sends alarms if any fiber degradation occurs.

## ONMSi Benefits

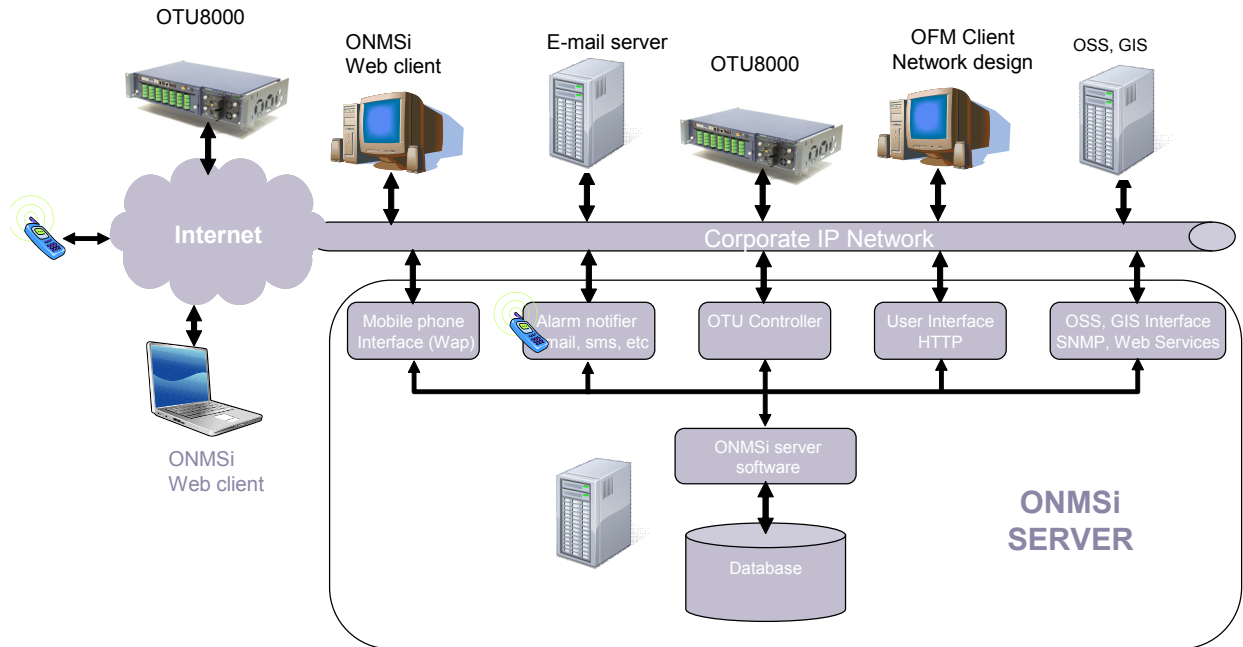
- Reduces Fault location time from 5 hours to 5 minutes (average time)
- Reduces MTTR and network downtime by at least 30%
- Reduces operational costs by providing faster automated dispatch
- Scalable to optimize CAPEX and expand as your network expands
- Flexible to support P2P (Metro/Core/Access) and P2MP (PON) to the ONT
- Enhanced reliability with SLA and asset management
- Anticipates service disruption before service is affected
- Protects network with long term performance monitoring
- Improved troubleshooting and demarcation between networks
- Detects fiber tapping, protecting valuable information from intrusion

## ONMSi Features

- Supports P2P (metro/core/access) and P2MP (PON) to the optical network terminal (ONT)
- Compact and reliable optical test unit (OTU) design
- Domain architecture enables maximum organizational flexibility
- Integrates geographical maps of the fiber network with OTDR trace cursor tracking
- Secures multiuser environments compatible with LDAP
- Supports web services (XML) and SNMP for easy integration with open-source software (OSS) and geographical information systems (GIS)
- High-availability solution with automatic failover between two servers
- Multiple dashboards showing current performance and diagnostics data

# ONMSi Architecture

Figure 1 ONMSi architecture





## ONMSi login and general view

This chapter gives process to open an ONMSi session and describes the man-machine interface.

Topics discussed in this chapter include the following:

- [“Pre-requisite” on page 6](#)
- [“Log-in” on page 6](#)
- [“General User Interface” on page 7](#)

## Pre-requisite

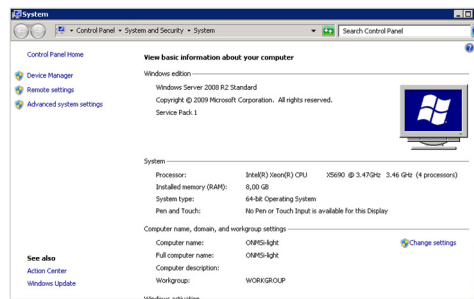
Server is configured with default Windows user (this user cannot be changed, if you need to change password please contact your local technical center).  
ONMSi server communicates with remote test units (OTUs) and client stations via IP.

Server name must be configured (or changed if needed) at first beginning.

To configure the server:

- 1 Open the System dialog box and click on **Change settings**.
- 2 Enter the following parameters:
  - User: rftsmgr
  - Password: System0

Figure 2 Change settings

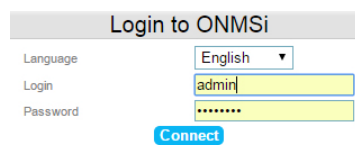


## Log-in

To log-in to ONMSi:

- 1 Open a web Browser: Firefox, Google Chrome or Internet Explorer.  
Google Chrome or Firefox are recommended.  
Internet Explorer from version 9 is also compatible (version 11 or above is recommended).
- 2 In the URL address, type the server name (example: `http://onmsi-light`) or the server IP address (example: `http://10.33.17.xx`).
- 3 In the dialog box Login to ONMSi, select first the language of the application: English / French / Vietnamese / German / Russian.
- 4 Enter your **Login** (default login: admin).
- 5 Enter the **Password** (default password: password).

Figure 3 Login to ONMSi





**CAUTION**

Login and password are case sensitive!

To get more information on user and login parameters (modify ..), see [“Users” on page 101](#).

## Audit logs

To display information concerning the users login and logout (date, user, IP address...):

- 1 From any dashboard, click on **More**
- 2 Click on **Audit logs** button.  
The **Audit logs** window displays.

**Figure 4** Audit logs

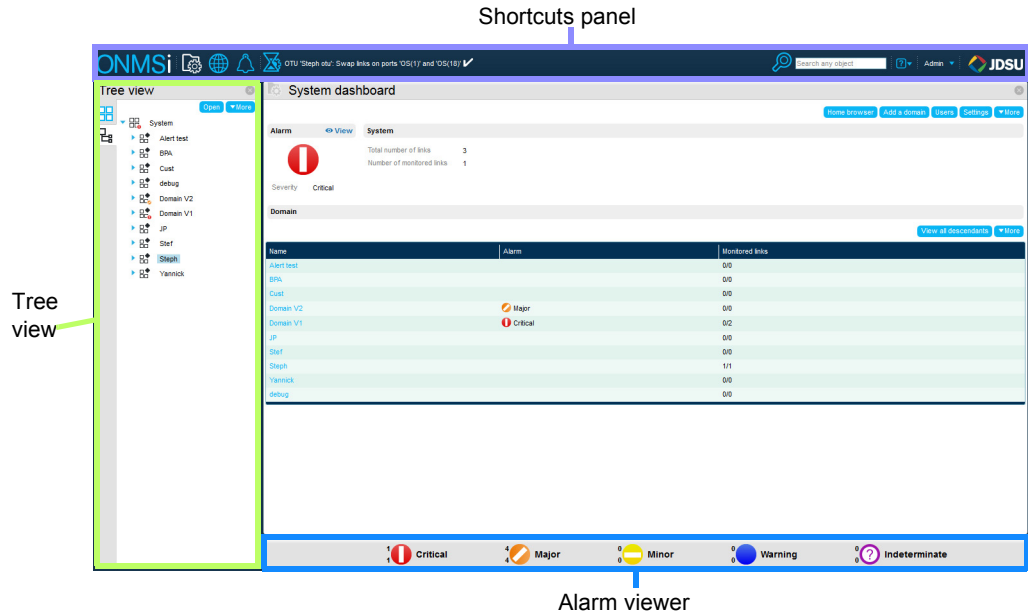
Date	User	IP address	Object type	Object name	Action
2015 Sep 17 10:05:36	admin	10.33.16.85	User	Admin	Login
2015 Sep 17 09:39:06	admin	10.33.17.57	User	Admin	Logout
2015 Sep 17 09:37:34	admin	10.33.16.85	User	Admin	Login
2015 Sep 17 09:32:21	admin	10.33.17.57	User	Admin	Logout
2015 Sep 17 09:27:53	admin	10.33.16.85	User	Admin	Login
2015 Sep 17 09:24:21	brulerd	10.33.17.57	User	Stephanie Brulerd	Logout
2015 Sep 17 09:19:06	admin	10.33.17.57	User	Admin	Logout
2015 Sep 17 08:53:50	brulerd	10.33.16.85	User	Stephanie Brulerd	Login
2015 Sep 17 08:52:34	admin	10.33.20.76	User	Admin	Login
2015 Sep 17 08:52:24	admin	10.33.16.85	User	Admin	Logout
2015 Sep 17 08:51:06	admin	10.33.16.85	User	Admin	Login
2015 Sep 17 08:41:21	admin	10.33.17.57	User	Admin	Logout
2015 Sep 17 08:39:55	admin	10.33.20.76	User	Admin	Login
2015 Sep 16 17:33:21	admin	10.33.17.57	User	Admin	Logout
2015 Sep 16 17:31:25	admin	10.33.16.85	User	Admin	Login
2015 Sep 16 17:16:21	admin	10.33.17.57	User	Admin	Logout
2015 Sep 16 17:14:49	admin	10.33.16.85	User	Admin	Login
2015 Sep 16 17:05:21	admin	10.33.17.57	User	Admin	Logout
2015 Sep 16 17:03:21	admin	10.33.16.85	User	Admin	Logout
2015 Sep 16 17:03:14	admin	10.33.16.85	User	Admin	Login
2015 Sep 16 17:02:06	admin	10.33.17.57	User	Admin	Logout
2015 Sep 16 17:01:51	admin	10.33.17.57	User	Admin	Logout

- Enter the research filters in the window «Search any object» and click on **Filter** to apply the filters.
- Click on **Reset filters** to delete the research filters.
- Click on **More** and download the table in PDF or Excel™ (see [“Downloading data from a table / list” on page 92](#)).

## General User Interface

Once login in, the system dashboard displays.

Figure 5 System dashboard



## Text colors

- If the text is in black, no action is possible.
- All text in blue corresponds to a link: click on blue text to display the corresponding link.
  - Example: in the Figure 4 above, click on one Domain **Name** in the table to display the corresponding domain dashboard.
  - If the text is greyed, the current configuration does not allow any action on the link.
  - Setting the mouse pointer onto the text will indicate the reason why no action is possible.

## Shortcuts panel

On the top of the screen, some buttons are available to reach specific functions of the ONMSi.



Click at any time on this button to get direct access to System Dashboard (domain, users, setting, alert). See [Figure 5 on page 8](#).



Click to hide (icons turns blue) / show (icons turns white) the main window.



Click to hide (icons turns blue) / show (icons turns white) the schematic or map with OFM (option)

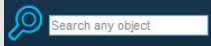




Click to hide (icons turns blue) / show (icons turns white) the alarm viewer.

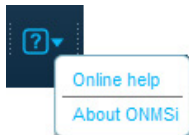


Click to open the action list (running activity):




Click to perform a quick search to access any object (OTU, Domain, Link, PON...)

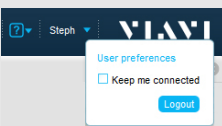
- Starting by: toto
- Finishing by: \*toto
- Containing: \*toto\*



In the **Help** sub-menu, click on:

- **Online help** to get access to training material (pdf).
- **About ONMSi** to get the ONMSi version and revision (debug purpose).

To display a contextual help for the ONMSi use, click on «?» .



In the «**User**» sub-menu, click on:

- **User preferences** to display/modify the user parameters (see [“Changing the current user preferences” on page 43](#))
- **Logout** to logout the current user of ONMSi.
- **Keep me connected** to keep the session active, even if a disconnection after a time of inactivity is configured (in System Settings > Users > Session - see [“Defining the session duration” on page 101](#)). This parameter is displayed exclusively if the parameter «Remain connected» in the System Roles of the User connected is selected: see [“Defining the system and domain roles for the user” on page 40](#).

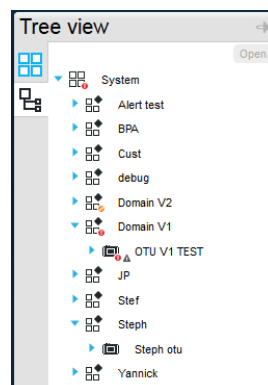
## Tree view

The tree view allows to show the list of domains, OTUs and monitored fibers (link).


The tree icons are displayed on the left of the screen.


- 1 Click on the icon  to open the Tree view.

**Figure 6** Example of Tree view








- 2 Select the object, double click it to open the related dashboard.  
Tree automatically closed.

To keep the tree view displayed on the left of the screen, once it is opened, click on .


Click on the icon  to close the Tree view and return to the system dashboard.

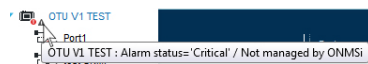
## Description of the objects in the Tree

In the tree view: the different objects are represented by different icons:

-  Domain System (cannot be renamed)
-  Domain or sub-domain
-  OTU
-  Links
-  Section

In case of alarm or default on the object, an icon displays next to the object concerned by the alarm.

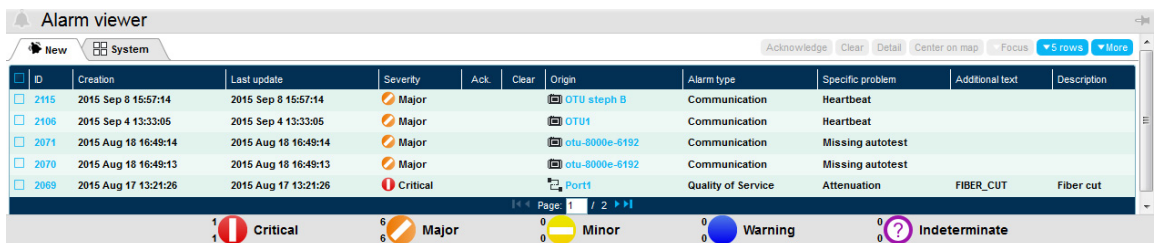
- Example:  indicates an alarm on the OTU and a default for this OTU.
- Drag the mouse onto the icon to display an alarm description



## Alarm viewer

Click on the Alarm banner at the bottom of the page to display the Alarm Viewer.

Figure 7 Alarm viewer



ID	Creation	Last update	Severity	Ack.	Clear	Origin	Alarm type	Specific problem	Additional text	Description
2115	2015 Sep 8 15:57:14	2015 Sep 8 15:57:14	Major			OTU steph B	Communication	Heartbeat		
2106	2015 Sep 4 13:33:05	2015 Sep 4 13:33:05	Major			OTU1	Communication	Heartbeat		
2071	2015 Aug 18 16:48:14	2015 Aug 18 16:48:14	Major			otu-8000e-8192	Communication	Missing autotest		
2070	2015 Aug 18 16:48:13	2015 Aug 18 16:48:13	Major			otu-8000e-8192	Communication	Missing autotest		
2069	2015 Aug 17 13:21:26	2015 Aug 17 13:21:26	Critical			Port1	Quality of Service	Attenuation	FIBER_CUT	Fiber cut

Summary bar: 1 Critical, 6 Major, 0 Minor, 0 Warning, 0 Indeterminate

For details on Alarms, see [Chapter 11 on page 77](#).

## Keyboard shortcuts

Following keyboard shortcuts are available in ONMSi:

Shortcut	Description
CTRL + SHIFT + X	Cycles through the ONMSi areas (main, alarm viewer, ...)
CTRL + SHIFT + F	Runs the "find"
CTRL + SHIFT + Home	Navigates back to the system dashboard
CTRL + SHIFT + F1	Toggles the display of the contextual help
F2 inside a table	Toggles between cell edition and cell navigation with the arrow keys



## Setting the Server address

This chapter provides a description of the configuration of the server address.

Topics discussed in this chapter include the following:

- [“Setting up the server address” on page 14](#)

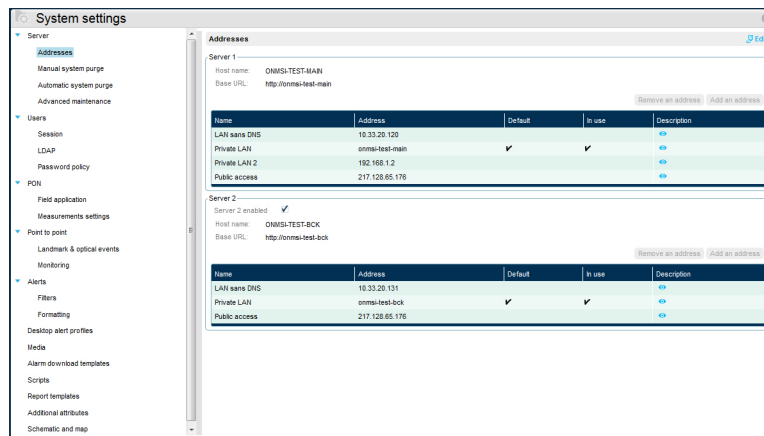
## Setting up the server address

Once logged in to the ONMSi, Server IP details must be configured in ONMSi

This information is used by optical test unit (OTU) to report alarms.

- 1 Click on the logo **ONMSi** to display the system dashboard.
- 2 Press the Settings button **Settings** on the right of the window.
- 3 On the left of the System Settings screen, click on **Server > Addresses**.

Figure 8 Setup Server addresses



- 4 Click on **Edit** and enter the parameters required:
  - **Host name:** server name.
  - **Base URL:** Address used in the URL to access to ONMSi from a web browser.

The addresses entered in this table are used by the OTUs to notify the server when an alarm is detected.

As the OTUs can be placed in different IP networks they may have to use different server IP addresses; for example if they are connected via internet or directly to the LAN. This chapter is for OTU connected to the LAN.

- **Name:** This name will be used within OTU configuration to indicate the server address where the alarms have to be sent to.
  - **Address:** host name of this interface (recommended) or IP address.
- 5 Click on **Save** to save the new server addresses.

### Main and Backup server

In case of problem with the main server, the automatic changing to backup server is possible exclusively if there are 2 networks.

By consequence, both servers must be configured in **Server > Addresses** window.

If the option «**High availability with automatic fail-over**» is not available, the change must be performed manually (if license «**High availability with manual fail-over**» has been purchased). See “[High Availability Solution](#)” on page 141

## Adding an OTU

This chapter provides a description for adding an OTU to an existing domain.

By default, a Domain called **Default** is available at ONMSi opening.

This domain name can be modified and new domains can be added to the existing one: see [Chapter 9 “Managing domains”](#).

Topics discussed in this chapter include the following:

- [“Adding an OTU” on page 16](#)
- [“Testing the connection and refreshing the configuration” on page 16](#)
- [“Configuring the OTU” on page 18](#)

## Adding an OTU

To add an OTU to the domain:




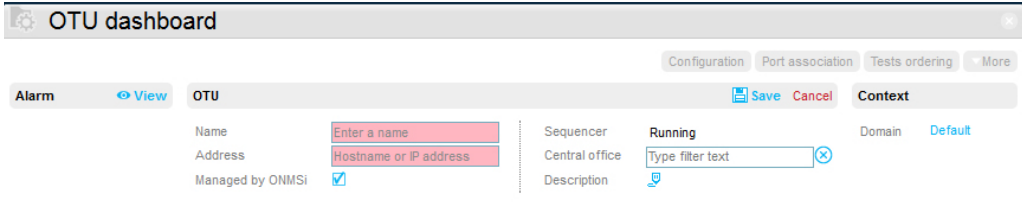
- 1 If necessary, return to the System Dashboard window clicking on the ONMSi logo 
- 2 On the Tree view, right click on the domain name and select **Add an OTU**.  
or  
Click on the **More** button of the Tree view  and click on **Add an OTU**.  


Figure 9 Adding an OTU



The screenshot shows the 'OTU dashboard' window. It has tabs for 'Configuration', 'Port association', 'Tests ordering', and 'More'. The 'OTU' tab is active, showing a form with the following fields: 'Name' (with a placeholder 'Enter a name'), 'Address' (with a placeholder 'Hostname or IP address'), 'Managed by ONMSi' (checked), 'Sequencer' (set to 'Running'), 'Central office' (with a search filter 'Type filter text'), and 'Description'. There are 'Save' and 'Cancel' buttons, and a 'Context' dropdown menu set to 'Default'.

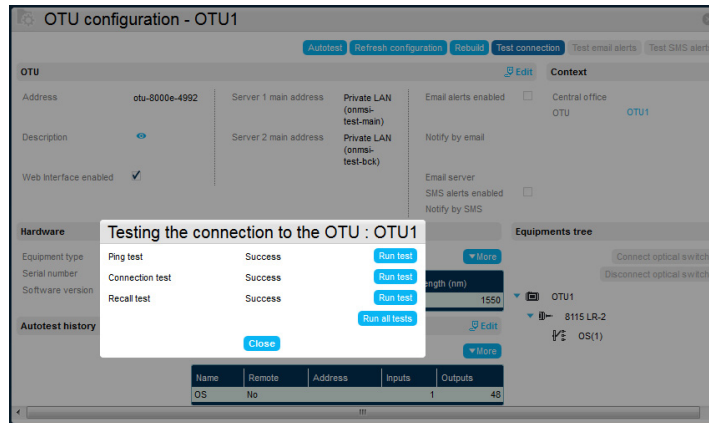
- 3 Enter a **Name** (for example: OTU location) and the IP **Address** of the OTU (Physical IP address or hostname).  
Use the same Address as setup on OTU via OTU web browser.
- 4 Press **Save** to confirm the creation.  
The OTU creation process is completed once the progress bars are no more displayed.

## Testing the connection and refreshing the configuration

- 1 Press **Configuration** from the OTU dashboard window.
- 2 Press **Test connection** button.
- 3 In the new dialog box, press **Run all tests** to run the three tests available  
or  
Click on each **Run Test** button to preform exclusively the corresponding test.  
All tests must succeed.



Figure 10 OTU Connection tests



- **Ping test** is a simple ping from server to OTU.
- **Connection test** is an SSH connection from server to OTU.
- **Recall test** is an SSH connection from OTU to server.

4 Close the dialog box.

5 Press **Rebuild** button.

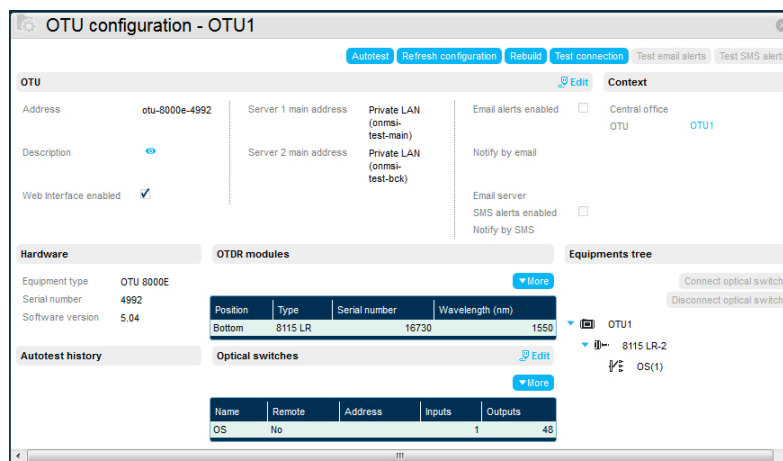
Rebuild is not necessary with brand new OTU.

Rebuild deletes all remaining test on OTU.

Rebuild is recommended in case of any doubt about OTU previous use

6 Press **Refresh configuration** button to complete the OTU configuration.

Figure 11 OTU successfully added to the Domain



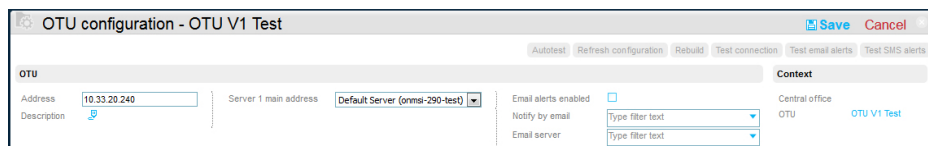
## Configuring the OTU

### Associating OTU address to server

From the OTU Dashboard:

- 1 Click on **Configuration** button.
- 2 Press **Edit** to modify the parameters.
- 3 In the parameter Server 1 main address, select one of the addresses defined in ONMSi > Settings > Addresses (see [Chapter 3 on page 13](#)).

Figure 12 Server / OTU address association

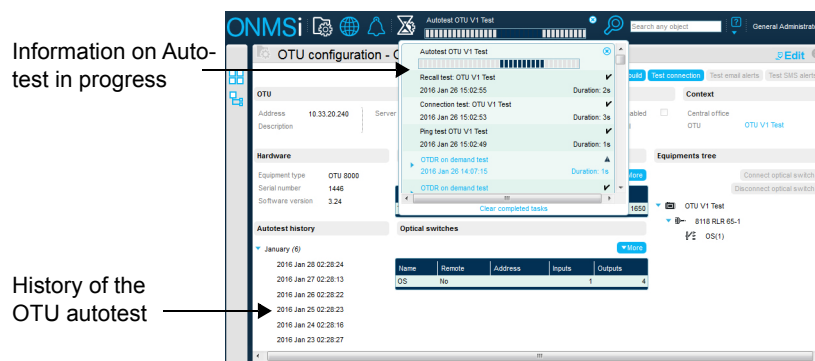


### Launching an Autotest of the OTU

Once is added to a domain, an autotest can be manually launched:

- 1 From the OTU Dashboard, click on **Configuration** button.
- 2 Press **Autotest**.
- 3 The test is launched.
- 4 Click on the notification area to display the autotest in progress

Figure 13 Launching an Autotest of the OTU



Once completed, the autotest history is updated.

## Moving the OTU

To modify the domain into which is installed the OTU:

- 1 On the Tree view, select the OTU (highlighted in grey)
- 2 Right click on the OTU
- 3 Click on **Move the OTU**
- 4 In the new dialog bow, select the new destination (sub-)domain.
- 5 Click on **Ok** to validate.

The OTU is removed form the initial domain and set into the new one.

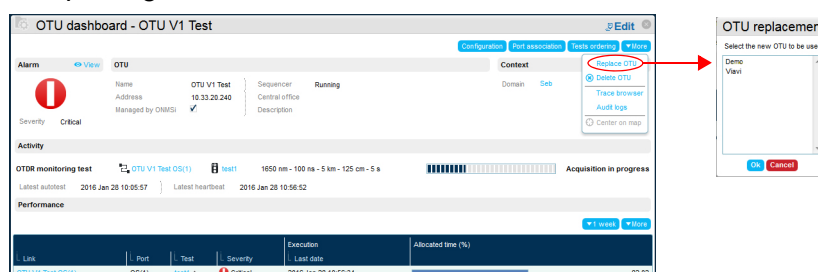
## Replacing an OTU

To replace an OTU by another one in a domain:

- 1 Add the new OTU:
  - with a different name than the one to be replaced.
  - **with a different serial number.**

See “Adding an OTU” on page 16.
- 2 Assign the **same IP** to this new OTU
- 3 Select the OTU to be replaced to open the corresponding Dashboard.
- 4 Click on **More > Replace OTU**.
- 5 Select the OTU replacing the current one and click on **Ok**.  
Auto configuration and rebuild are performed automatically.  
OTDR and switch are replaced clicking on **Refresh configuration**:
  - OTDR replacement module must be same model
  - Replacement switch must be same or higher capacity.
  - Those replacement must be configured in OTU Web Interface.

Figure 14 Replacing an OTU





# Monitoring a link

Once OTU is created on ONMSi, the user can assign a monitored fiber to an optical switch port of the OTU.

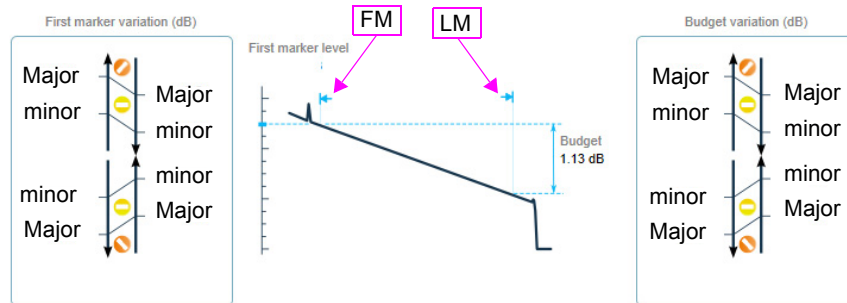
This chapter provides a description on the link monitoring process.

Topics discussed in this chapter include the following:

- [“Optical Link monitoring principle” on page 22](#)
- [“Provisioning the link” on page 22](#)
- [“Landmark setting” on page 25](#)
- [“Checking long term degradation” on page 26](#)

## Optical Link monitoring principle

Figure 15 Optical Link monitoring principle



Minor = +/-1dB and Major = +/-3dB by default

Budget degradation  $\geq 6$  db reported as critical fiber break alarm

LM in the noise floor reported as critical fiber break alarm

FM degradation reported as "injection alarm".

ONMSI monitoring is based on a regular comparison between regular OTDR acquisition and an OTDR reference trace.

A first marker called "FM" is placed at origin and a last marker called "LM" is placed at fiber end.

Difference between first marker and last marker is called **optical budget**.

Any modification along the fiber changing the optical budget generates an optical alarm.

First marker is used to detect and report any degradation or break before the optical ODF.

Such alarm will be reported as "injection alarm".

## Provisioning the link

One single button allows to launch the monitoring of the fiber from the ONMSi application.

From the OTU dashboard window:

- 1 Click on the button **Ports association** to assign fibers.
- 2 From the *Ports association* window; select the **Optical switch port** to be measured.
- 3 Click on the button **Provisioning**.

Figure 16 Port association



The provisioning allows to perform all the process: create the link, test the link, perform the measurement, position the markers...

Once the button is pressed, a dialog box opens and informs you of the process in progress:

4 Configure the OTDR measurement for port provisioning.

5 Press **Start** to launch the process.

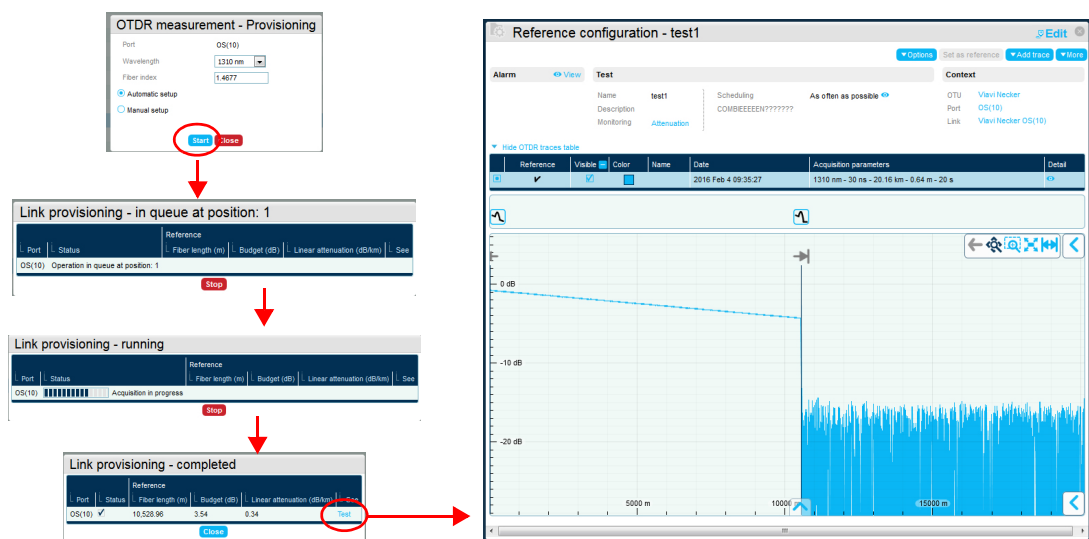
The operation is in queue at a certain position

The acquisition is in progress

Once acquisition is completed, the Link provisioning window displays a summary of the measurement, which will be defined as reference trace.

Click on **Test** to display the trace in a new tab.

Figure 17 Provisioning



1 Click on **Close** to return to Port Association window.

The link is monitored.



**NOTE**

The provisioning of several ports can be performed at the same time:  
In the Port Association, select all the ports to be provisioned and press **Start** in OTDR measurement dialog box.

Link provisioning - running		Reference			
Port	Status	Fiber length (m)	Budget (dB)	Linear attenuation (dB/km)	See
OS/05	Failed: first marker position before minimum (2.04m for selected pulse)	10.37	12.94	1.247.45	Trace
OS/09	✓	10.53	2.79	0.25	Trace
OS/10	✓	10.529.00	3.53	0.34	Trace

## Reference trace display

It is recommended to get the last marker above the “Minimum level of markers” (red line).

The First Marker / Last Marker must be as close as possible to origin / end of fiber and in a linear flat segment.

The position of the first and last markers can be adjusted from the Trace Viewer:

- Zoom around the fiber end and/or fiber start to adjust the last/first marker position if needed (close to fiber end / fiber start):

- On the right of the trace, click on the left arrow to open the menu.



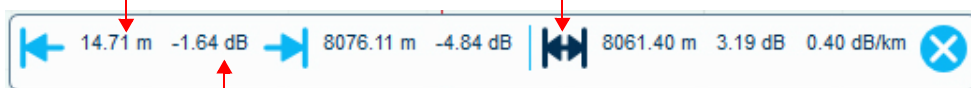
**NOTE**

Check you are on Edition mode to modify the markers position.

- Click on and make a zoom on the end of fiber.

- Click on the button .

Distance, attenuation and slope between first and last markers  
First marker detail with distance from origin and level



Last marker detail with distance from origin and level

- Select the tool / to place first/last marker to a new position then drag and drop it.

- Click on **Save** to apply the new markers position to the OTDR reference trace.

## Changing the reference trace

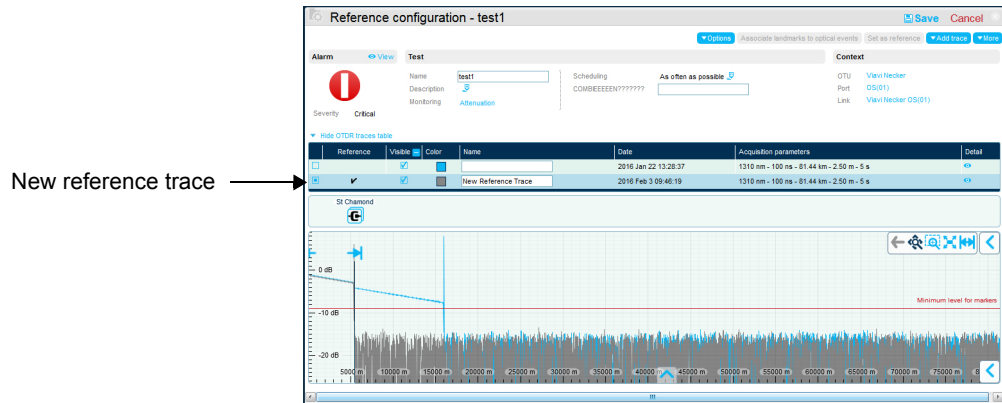
In multi-traces display, the reference trace defined can be modified.

- From the Link Dashboard, click on **Configuration & Reference** button.



- 2 In the OTDR trace table, select the trace to be defined as Reference.
- 3 Click on the **Set as reference** button.  
Landmarks are automatically adjusted according to the new reference trace.

**Figure 18** Changing the Reference trace



- 4 Click on **Save** to save the new reference trace.




## Landmark setting

A landmark can be associated to an optical event on trace.

In the Link Dashboard or Reference configuration window, click on **Edit**.

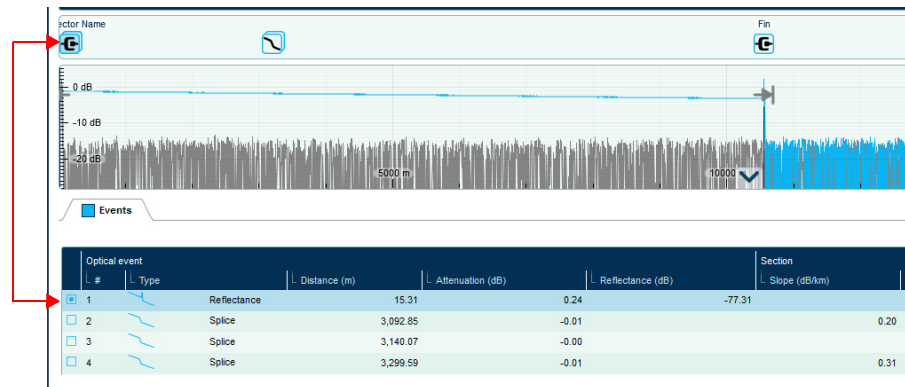
Click on one optical event icon above the trace.

A popup window open, with the event details in the **Event** field, and the **Landmark** field just above.

- 1 Click on **Add landmark** button.
- 2 Select the type of landmark to be associated to the optical event:
  - Connector: 
  - Splice: 
- 3 Enter a **Name** for this Landmark.
- 4 Click on **Save** to validate the new Landmark.  
The Optical event is associated to the Landmark.
- 5 Click on  under the trace to display the results table.
- 6 Click on one optical event in the results table to highlight the landmark associated above the trace.

This function is useful with alarms: when an alarm occurs on a link with landmarks, it is localized in distance, according to those landmarks.

Figure 19 Optical event and associated landmark



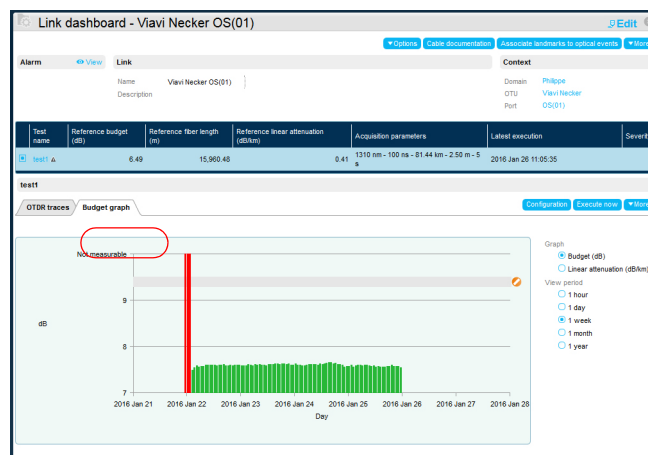
**NOTE**  
This function cannot be used in parallel with the Cable Documentation option; use either this function or the Cable documentation option, not both.

## Checking long term degradation

After a minor alarm, the budget graph allows to check if this alarm is caused by a new event or by a slow degradation.

- 1 Click on the tab **Budget Graph** on the Link Dashboard Window  
The budget graph is updated in real time.
- 2 Modify if necessary the unit for graph display:
  - **Budget (dB)** - selected by default.
  - **Linear Attenuation (dB/km)**: whatever is the fiber length, the linear attenuation keeps proportional.
- 3 Modify if necessary the view period of the budget: from 1 hour up to 1 year.

Figure 20 Budget graph



## Displaying the alarms

This chapter provides a description of the Alarms viewer.

Topics discussed in this chapter include the following:

- [“Alarms view” on page 28](#)

## Alarms view

Once the link is monitored, the alarms displays automatically as soon as a default is detected during measurements.

To display the alarms list:


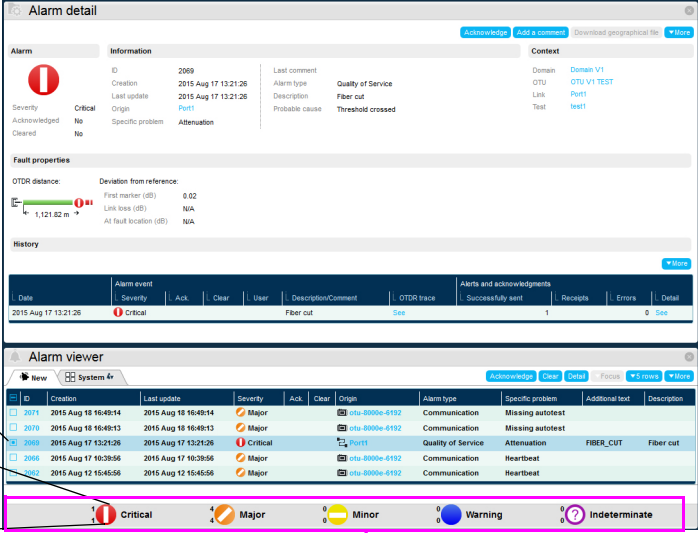
- 1 Click on the alarm banner, at the bottom of the screen
- 2 or
- 3 Click on the Alarm icon , on the shortcut panel.
- 4 Click on **Alarm ID** to get details.

Figure 21 Alarm window



The screenshot shows the 'Alarm detail' window and the 'Alarm viewer' window. The 'Alarm detail' window displays information for a specific alarm (ID: 2069, Severity: Critical, Description: Fiber cut). The 'Alarm viewer' window shows a list of alarms with columns for ID, Creation, Last update, Severity, Ack, Clear, Origin, Alarm type, Specific problem, and Description. The 'Alarm banner' at the bottom of the 'Alarm viewer' window shows the severity levels: Critical, Major, Minor, Warning, and Indeterminate. Annotations include: 'Alarm ID selected' pointing to the ID 2069 in the 'Alarm detail' window; 'Number of not acknowledged alarms' pointing to the number '1' in the 'Alarm detail' window; 'Number of alarms' pointing to the number '1' in the 'Alarm viewer' window; and 'Alarm banner' pointing to the severity level indicators at the bottom of the 'Alarm viewer' window.

# Trace Viewer

This chapter provides a description of the possible actions on traces, whether they are displayed on the Localization/Detection window, or open via the Trace Browser.

Topics discussed in this chapter include the following:

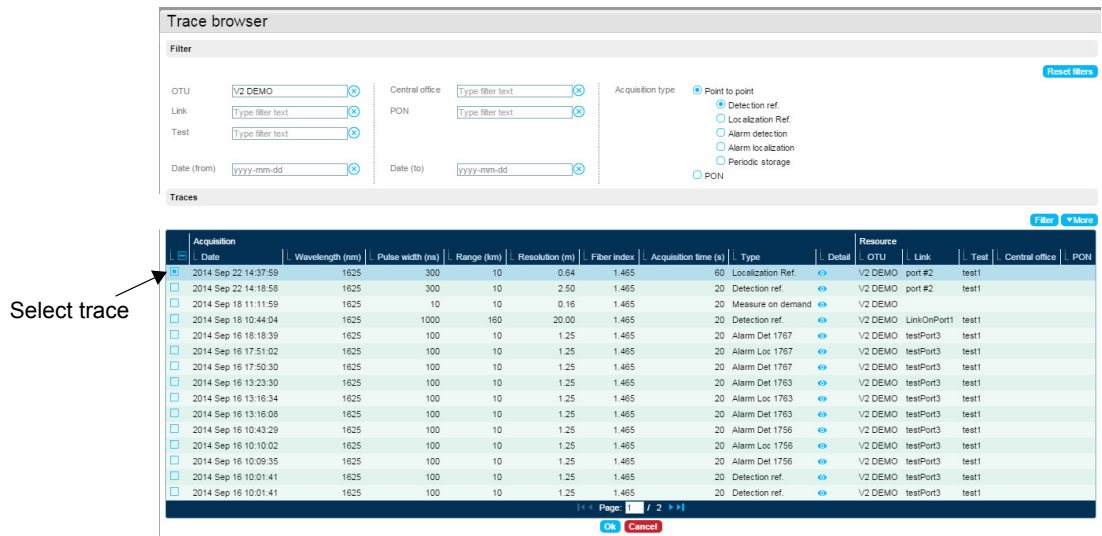
- [“Opening a trace using the Trace Browser” on page 30](#)
- [“Trace display” on page 31](#)
- [“Multi-trace display” on page 34](#)

## Opening a trace using the Trace Browser

From any dashboard except Domain (System dashboard, OTU dashboard, Link dashboard...), a trace saved on the system can be opened using the Trace Browser.

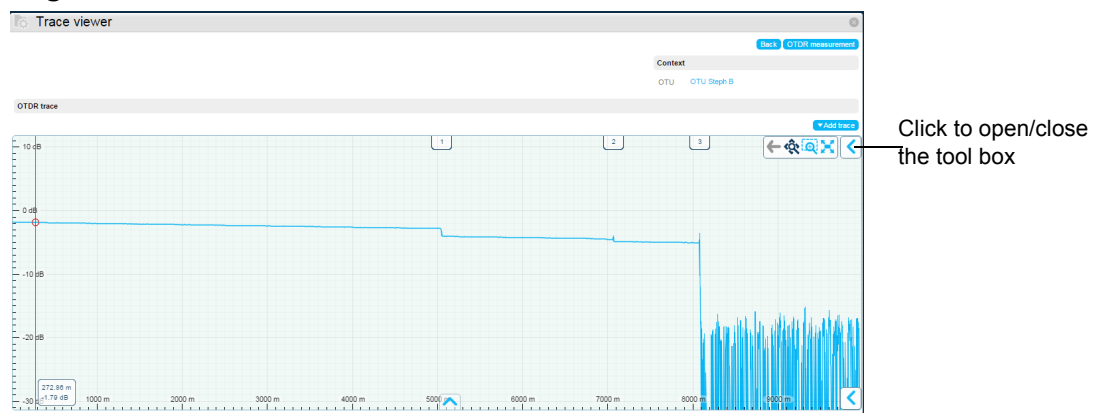
- 1 From the dashboard, click on **More**
- 2 Click on **Trace Browser**.  
A new dialog box displays

Figure 22 Trace Browser



- 3 If needed, define filters to retrieve a trace and press **Filter** button to apply filters.
- 4 Select the trace using the check box.
- 5 Click on **Ok**.  
The trace open on the Trace Viewer window.

Figure 23 Trace viewer



## Trace display





Once a trace is display, either in Detection/Localization window or in the Trace viewer, several actions can be made on trace.

The trace tool box, on the right of the trace display, allows to access different functions: Zoom / Markers / Trace description.

Click on the arrow  to open the Tool box.

## Zooming on trace

Once the Tool box open, different zoom functions are available:

- Click on  and zoom on a selected zone
- Click on  to pan and zoom in/out using the mouse wheel
- Click on  to make a zoom release (adjust zoom to window)
- Click on  to return to previous view

## Positioning Markers

### First and Last markers

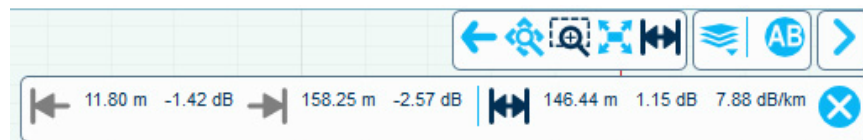


#### NOTE

This function is available exclusively for traces on the Localization or Detection window. Those markers are not available on traces opened via the Trace Browser.

Click on  to open the First and Last markers tool bar:

**Figure 24** First and Last markers tool bar



This tool bar allows to get details on the first and last markers position on trace:

See [“Reference trace display” on page 24](#) to get details on use of the First Marker and Last Marker functions.

## A & B markers

The A & B markers can be set on the trace in order to get distance information on the trace.


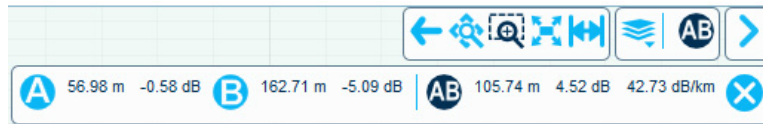
- 1 Click on the  icon to open the A & B markers menu.

Figure 25 A & B tool bar






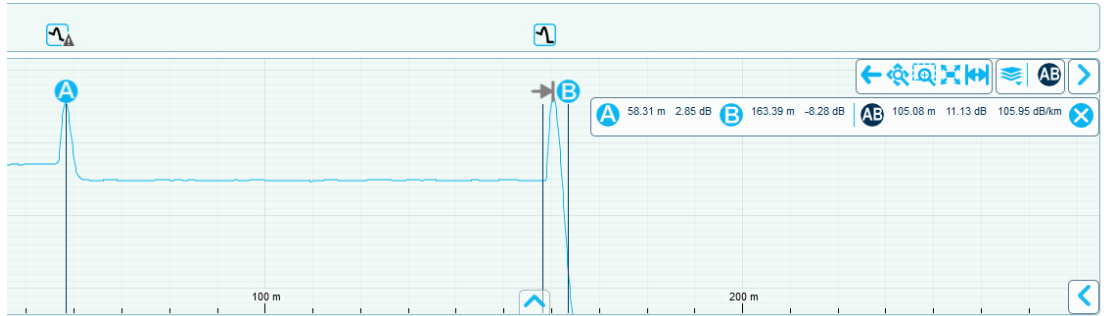

- 2 Before positioning a marker, make a zoom on trace if necessary (see “[Zooming on trace](#)” on page 31)
- 3 Click on the  icon and click on the trace where the marker must be positioned.
- 4 Click on the  icon and click on trace where the marker must be positioned.  
In the tool bar the distance from origin and level information are displayed for each marker.  
Moreover, the distance, attenuation and slope between A and B markers are displayed next to the icon .

Figure 26 Trace with A and B markers



## Optical events


- 1 Click on the icon 
- 2 Select/deselect the parameter **Optical events** to show/hide the optical events position on the trace.

## Trace details

The trace details can be displayed under the trace graphical representation.

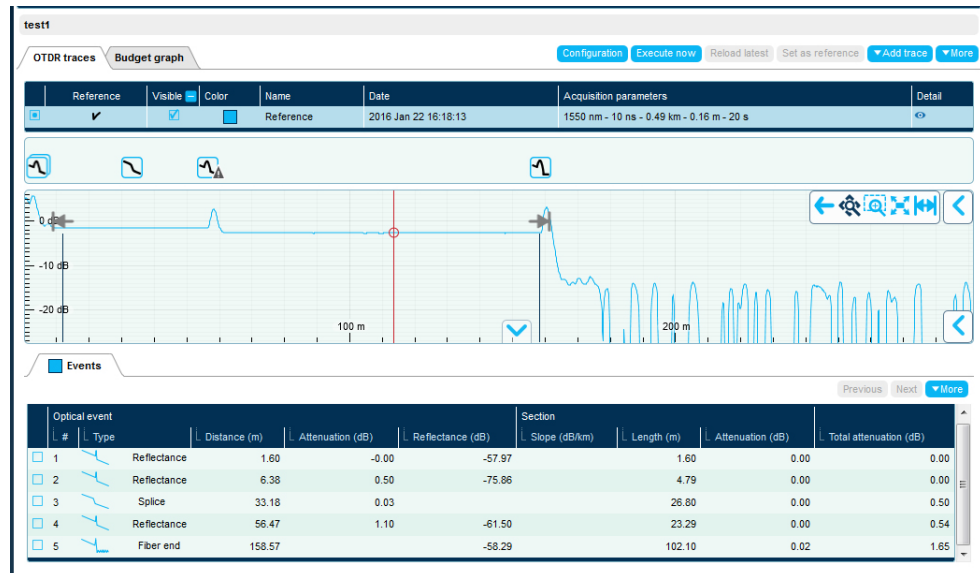


## Displaying the events table

Click on the icon  at the bottom of the trace to display the events table under the results trace.

Click on the icon  to hide the new window.

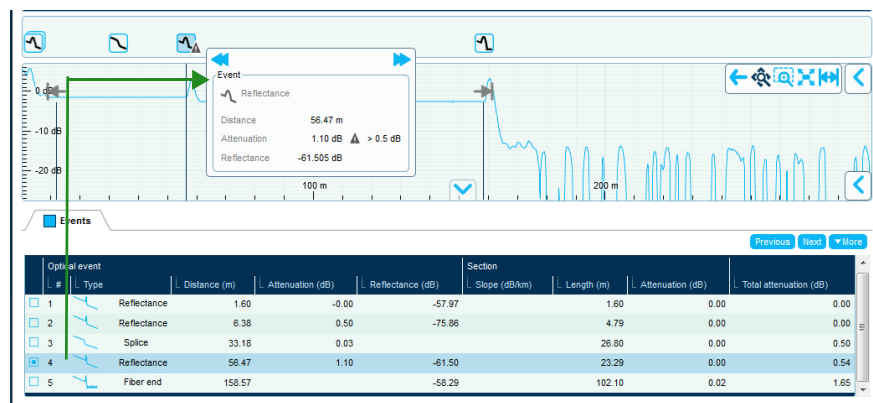
Figure 27 Trace view and Events table




Click on one event into the table to display a cursor line onto the event on trace.

Click on the event icon on the upper part of the trace to display the event details.

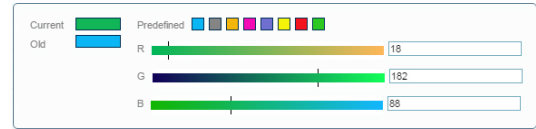
Figure 28 Event details



## Changing the trace color

Click on the icon  in the **Color** column of the traces list to change the trace color using the color palette:

- Click on one predefined color or define your own color.



## Multi-trace display

From the Trace Viewer or from a test result, you can add traces to the existing one, and then get several traces displayed in the same window.

### Adding trace(s)

Once a trace is displayed, in the Localization / Detection window or in the Trace Viewer, click on **Add trace** button

Select the place of the trace to be opened in the sub-menu

Figure 29 Add Traces sub-menu

OTDR measurement - OTUB

OTDR measurement - OTUB

Trace browser

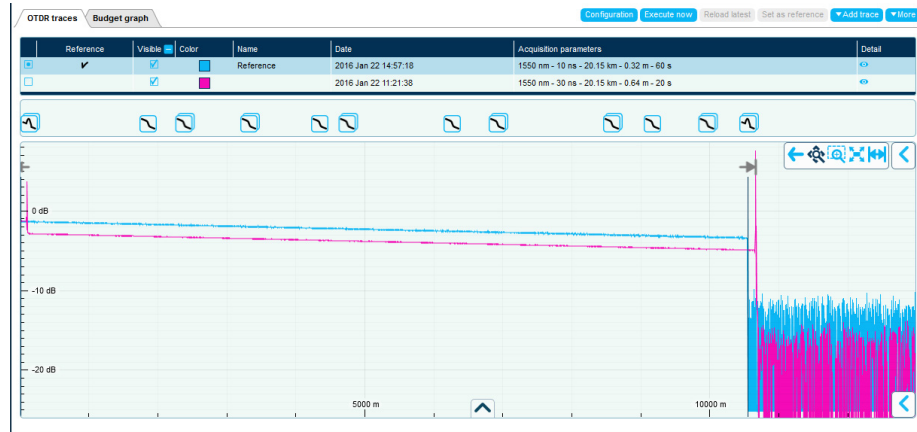
Choose OTDR trace

1: Not available in Trace Viewer window  
2 Exclusively available in Localization view

## Multi-traces display

Once the traces to be added are selected, the Trace Viewer is as follows:

Figure 30 Multi-traces display



## Changing the active trace and the trace color

Once in multi-traces display:




- In the Traces list, select the trace to be active using the radio button on the left.
- Click on the icon  of the **Color** column to change the trace color using the color palette: click on one predefined color or define your own color.

Figure 31 Multi-traces: select one trace and change color



## Trace and events table

The Events table is also accessible clicking on the icon  at the bottom of the trace (click on the icon  to hide the new window).

The events table displays the events detected for the active trace.



# Managing users

This chapter provides a description for the creation and configuration of users of ONMSi application.

Topics discussed in this chapter include the following:

- [“Adding a user” on page 38](#)
- [“Defining the system and domain roles for the user” on page 40](#)
- [“Changing the current user preferences” on page 43](#)
- [“Displaying the connected users” on page 46](#)

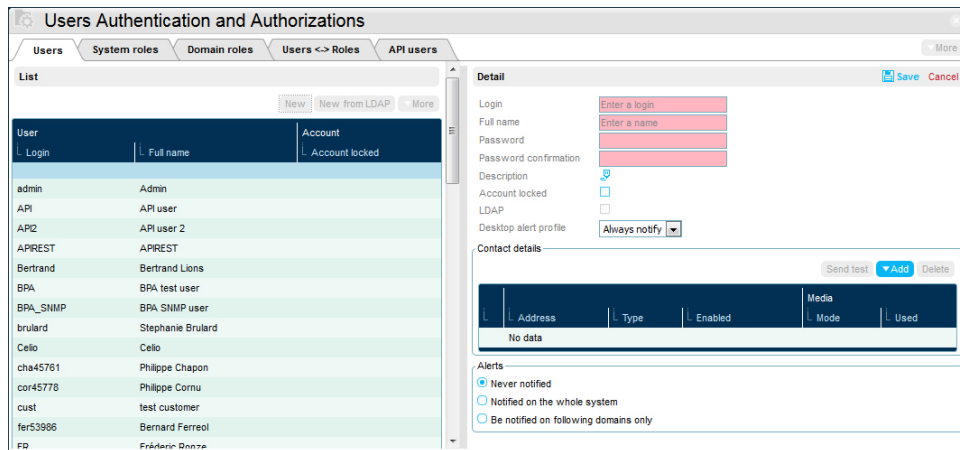
# Adding a user

## Adding a «standard» user


To add a user to the system:

- 1 From the System dashboard page, click on **Users** button, on the right of the screen.  
The page **Users Authentication and Authorizations** displays.
- 2 Check the **Users** tab is selected.
- 3 Press **New** button from the Users tab to create a «standard» user.

Figure 32 Creation of a «standard» user

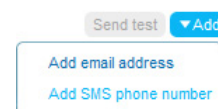


### Details

- 1 Enter the parameters of the new user: **Login / Full name / Password / Password confirmation**
- 2 If wished, click on the **Description** icon  and enter a detailed description of the user in the dialog box.
- 3 Select the level of notification for the desktop alert in the parameter **Desktop alert profile**: Always Notify / Never notify / Time warner or other customized parameter (see “Configuring Desktop alert profiles” on page 111).
- 4 Select if this user has an **Account Locked**: the user still exists but he cannot access anymore to the system

### Contact details

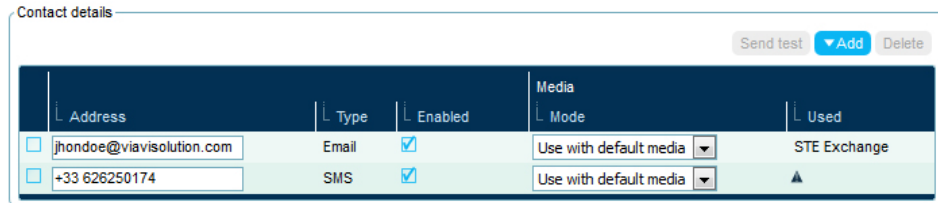
- 1 Click on **Add** button to open the sub menu



- 2 Click on **Add email address** to enter the user email address.

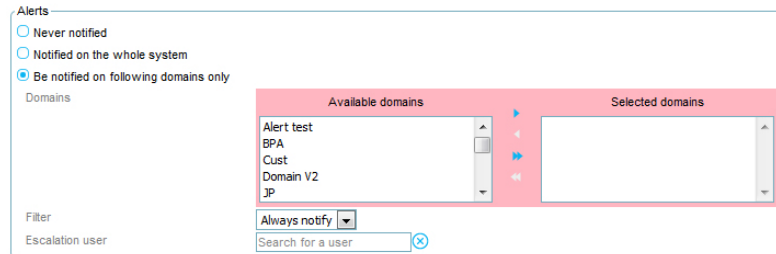
- 3 Click on **Add SMS phone number**, to enter the phone number of the user

**Figure 33** Contact details



## Alerts

**Figure 34** Alerts



- 1 Configure the notifications to be received by the user:
  - **Never notified:** the user is never informed on any domain
  - **Notified on the whole system:** the user is informed of any alarm on the entire system.
  - **Be notified on the following domains only:** select the domain(s) for which the user will be notified in case of alarm.
- 2 Press **Save** to validate the creation of the user.  
The user is displayed and selected on the list, in the Users tab

## Creating a user with LDAP

ONMSi is compatible with protocol LDAP v3 (eg: Active directory, Open LDAP)

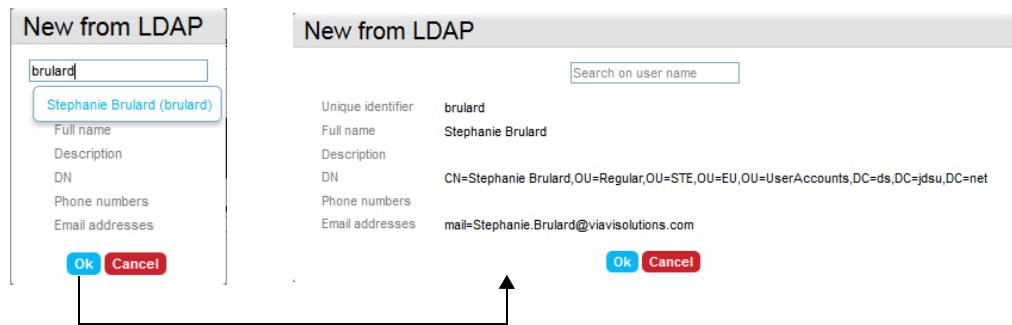
This option allows ONMSi to add users from a company directory. It respects the company password policy, and does not write anything on the directory (Read only)

LDAP configuration details must be given by a person familiar with the directory. To get information on LDAP configuration, see [“Configuring the LDAP” on page 102](#).

- 1 From the System dashboard page, click on **Users** button, on the right of the screen.  
The page **Users Authentication and Authorizations** displays.
- 2 Check the **Users** tab is selected.

- 3 Press **New from LDAP** to add a user from your company using the LDAP directory.  
 The dialog box **New from LDAP** displays
- 4 Enter the first letters of the user name  
 A list of users company displays, updated according to the letters entered.
- 5 Select the user in the list and click **Ok** to confirm.  
 A new dialog box with a full description of the user displays.

**Figure 35** Adding a user from the LDAP



- 6 Click **Ok** to confirm the user to be added to ONMSi
- 7 The Details window is fulfilled with the user parameters used in its company.
- 8 In the Contact Details window, the e-mail and phone number will be automatically proposed if they are defined in the LDAP company directory.
- 9 Follow instructions from [step 1](#) to [step 2](#) on [page 39](#) to complete the addition of a user from LDAP.

## Defining the system and domain roles for the user

Once the user is created, two kind of roles must be defined for him: System roles and Domain roles.

### System and Domain roles principle

System roles are roles applicable to data/functions that do not belong to domains.

Some built-in system and domain roles are available in the ONMSi and cannot be deleted.

System built-in roles	Domain built-in roles
<ul style="list-style-type: none"> <li>• API operator</li> </ul>	<ul style="list-style-type: none"> <li>• Domain administrator</li> </ul>
<ul style="list-style-type: none"> <li>• Data administrator</li> </ul>	<ul style="list-style-type: none"> <li>• Expert</li> </ul>
<ul style="list-style-type: none"> <li>• General administrator</li> </ul>	<ul style="list-style-type: none"> <li>• NOC</li> </ul>



System built-in roles	Domain built-in roles
<ul style="list-style-type: none"> <li>• P2P operator</li> <li>• PON operator</li> </ul>	<ul style="list-style-type: none"> <li>• Observer</li> </ul>
<ul style="list-style-type: none"> <li>• Test supervisor</li> </ul>	

Each user must have at least a system role to access to the system.

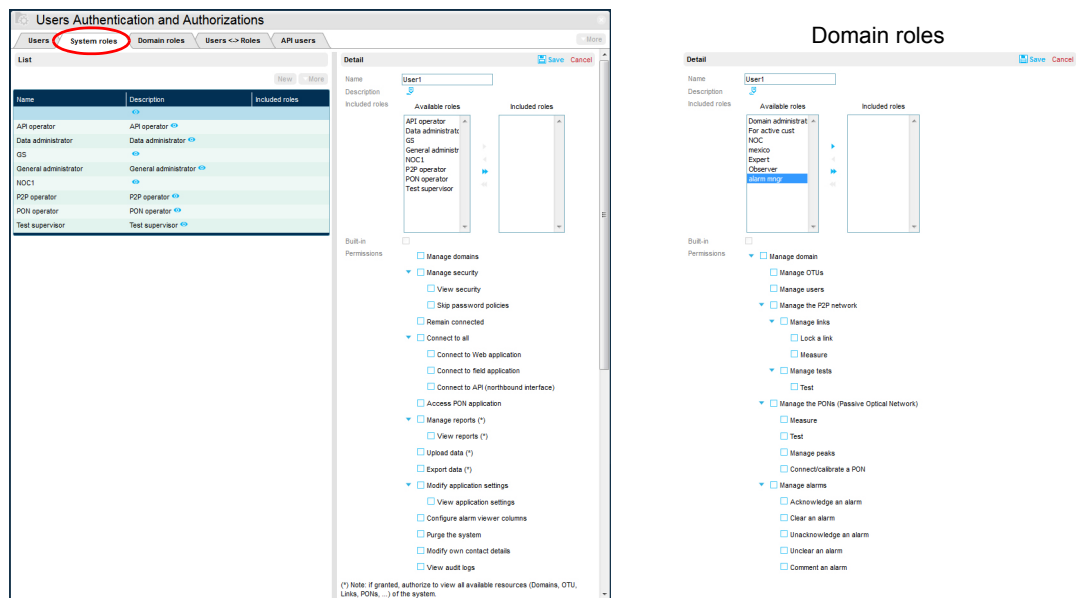
### General Information on System and Domain roles

- Built-in roles cannot be deleted
- Roles cannot be renamed
- Role can be deleted or duplicated from **More** button.

## Creating a System or Domain role

- 1 Select the **System roles** or **Domain roles** tab on the Users Authentication and Authorizations screen.
- 2 On the tab selected, click on **New** button.
- 3 Enter a **Name** for the new System/Domain role
- 4 Select / deselect the parameters to define the authorization for this system/ domain.

Figure 36 Create a System/Domain role



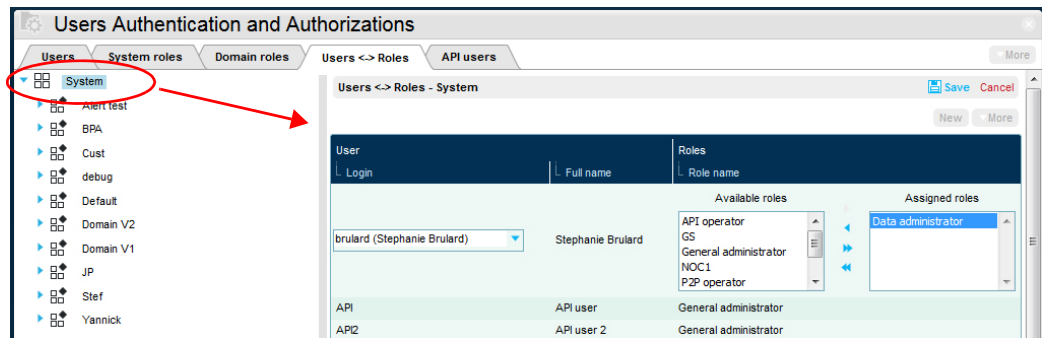
In the System roles, the “Manage domains” gives privileges on ALL domains. If you provide this privilege to a user, you do not need to assign domain roles to this user.

## Assigning System roles to a user

Once the user is created, open the **Users Authentication and Authorization** page and:

- 1 Click on the tab **Users <-> Roles**.
- 2 Select **System** in the left screen
- 3 Click on **New** button

Figure 37 Assign a System role



- 4 Select the user name in the list (you can type the first letters of its name in the field)
- 5 Select the **Role name** to be assigned to the user in the **Available roles** list. Maintain **Ctrl** key pressed to select several roles.
- 6 Click on / to pass the selected role(s) to **Assigned roles** box.
- 7 Press **Save** to save the current assignation.

### Notes on System roles assignation

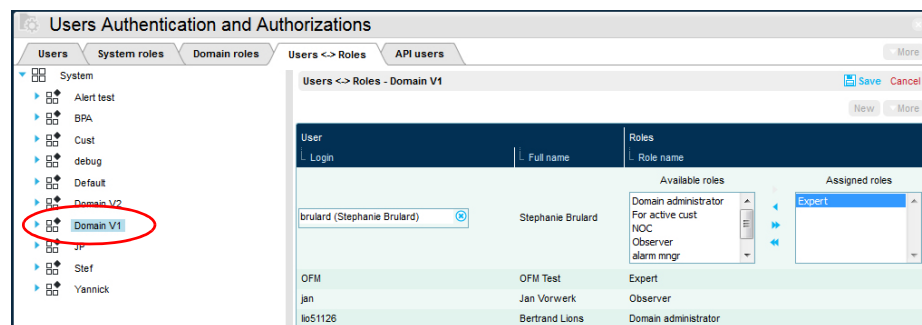
- A same user can have many roles.
- «General administrator» includes all privileges, it does not need other roles.
- You cannot assign new roles on your own. You need role for System be able to log in the application.



## Assigning Domain roles to a user

Once the user is created, open the **Users Authentication and Authorization** page and:

- 1 Click on the tab **Users <-> Roles**.
- 2 Select a **domain** in the left screen.
- 3 Click on **New** button

**Figure 38** Assign a Domain role



- 4 Select the user name in the list (you can type the first letters of its name in the field)
- 5 Select the **Role name** to be assigned to the user in the **Available roles** list. Maintain **Ctrl** key pressed to select several roles.
- 6 Click on  /  to pass the selected role(s) to **Assigned roles** box.
- 7 Press **Save** to save the current assignment.

### Notes on Domain roles assignment

- A same user can have many roles.
- A same user can have different roles on different domains.
- «General administrator» includes all privileges, it does not need other roles.

## Changing the current user preferences

Once logged, a user can modify some user preferences at any time: password, contact details...

### Changing the user password



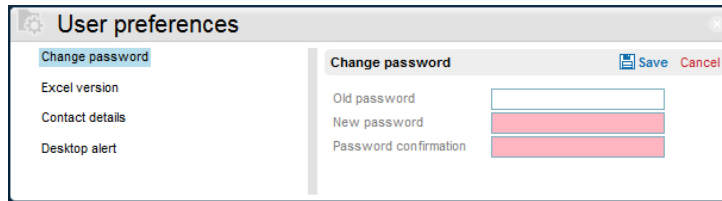
- 1 Click on ONMSi logo to display the System Dashboard.
- 2 Click on the «user» sub menu, on the shortcut panel  and click on **User preferences**. 
- 3 Select **Change password** on the left of the screen
- 4 Press **Edit** to modify the password.

Figure 39 Change user password



- 5 Enter the **Old password** and twice the New one.
- 6 Press **Save** to take into account the modification.  
At the next connection, enter the new password to establish the connection.

## Changing the excel version to be used

The Excel version to be used for downloading of table , results...can be modified from the User preferences screen.



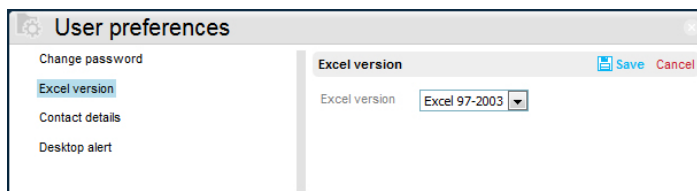
- 1 Click on **ONMSi** logo to display the **System Dashboard**.
- 2 Click on the «user» sub menu, on the shortcut panel  and click on **User preferences**  **and click on User preferences.**
- 3 Select **Excel version** on the left of the screen
- 4 Press **Edit** to modify the version.



Figure 40 Change Excel version

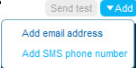


- 5 Select the version to be used in the list.
- 6 Press **Save** to take into account the modification.  
The Excel version selected will be used for downloading of table results... in Excel format.

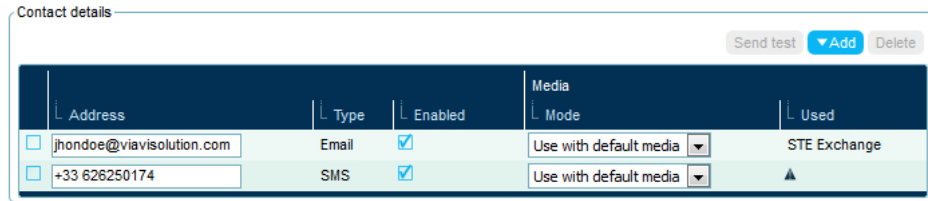
## Modifying the notification address

A notification address (SMS or E-mail) can be added/modified from the User preferences screen.

- 1 Click on **ONMSi** logo to display the **System Dashboard**.
- 2 Click on the «user» sub menu, on the shortcut panel  **and click on User preferences** .

- 3 Select **Contact Details** on the left of the screen
- 4 Press **Edit** to modify/add a notification address
- 5 Click on **Add** button to open the sub menu 
- 6 Click on **Add email address** to enter the user email address.
- 7 Click on **Add SMS phone number**, to enter the phone number of the user

**Figure 41** Contact details



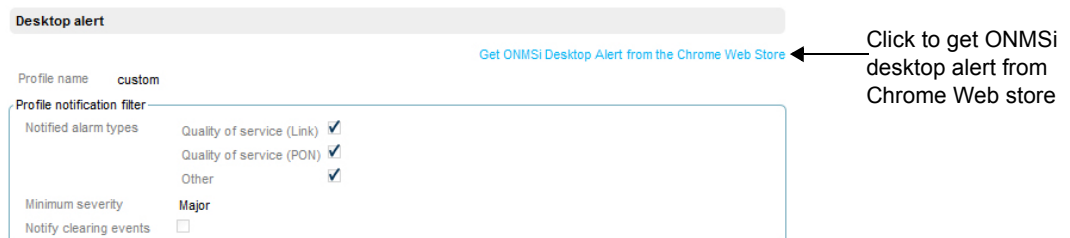
- 8 Select if the email / sms is enabled or not
- 9 In the **Mode** sub-menu, select if the address must be used:
  - with default media. The media is automatically displayed in the **Used** parameter
  - with specific media, in which case, the media will be modified in the **Used** parameter
- 10 Press **Save** to confirm the new notification address.

## Displaying desktop alert

From the User preferences screen, the user can display the notification parameters for desktop alerts.

Click on **Desktop alert** on the left of the screen to display the current desktop alert parameters.

**Figure 42** Desktop alert window



See “[Configuring Desktop alert profiles](#)” on page 111 to modify /add a desktop alert profile.

## Displaying the connected users

At any time, a list of connected users to the ONMSi can be displayed.

From the System dashboard screen:

- 1 Click on **More** button.
- 2 Click on **Connected users**.

**Figure 43** List of connected user



The screenshot shows a window titled 'Connected users' with a close button in the top right. Below the title bar, there is a header 'Connected users' and a sub-header 'Remaining connections: 8'. To the right of the connection count are two buttons: 'Refresh' (in blue) and 'Disconnect' (in grey). Below this is a table with the following columns: 'Login', 'Full name', 'IP address', 'Logged in since', and 'Keep me connected'. The table contains two rows of data.

Login	Full name	IP address	Logged in since	Keep me connected
<input type="checkbox"/> brulard	Stephanie Brulard	10.33.16.101	2015 Sep 4 09:20:54	
<input type="checkbox"/> admin	Admin	10.33.16.101	2015 Sep 4 09:21:20	

Click on **Refresh** to refresh the list.

### **Disconnect a user (general administration privileges)**

A user can be disconnected by another one, who have the general administration privileges):

- 1 Select the user to be disconnected
- 2 Press **Disconnect** button

# Managing domains

This chapter provides a description for the creation and configuration of domains of ONMSi application.

Topics discussed in this chapter include the following:

- [“Domain principle” on page 48](#)
- [“Creating a domain” on page 48](#)

## Domain principle

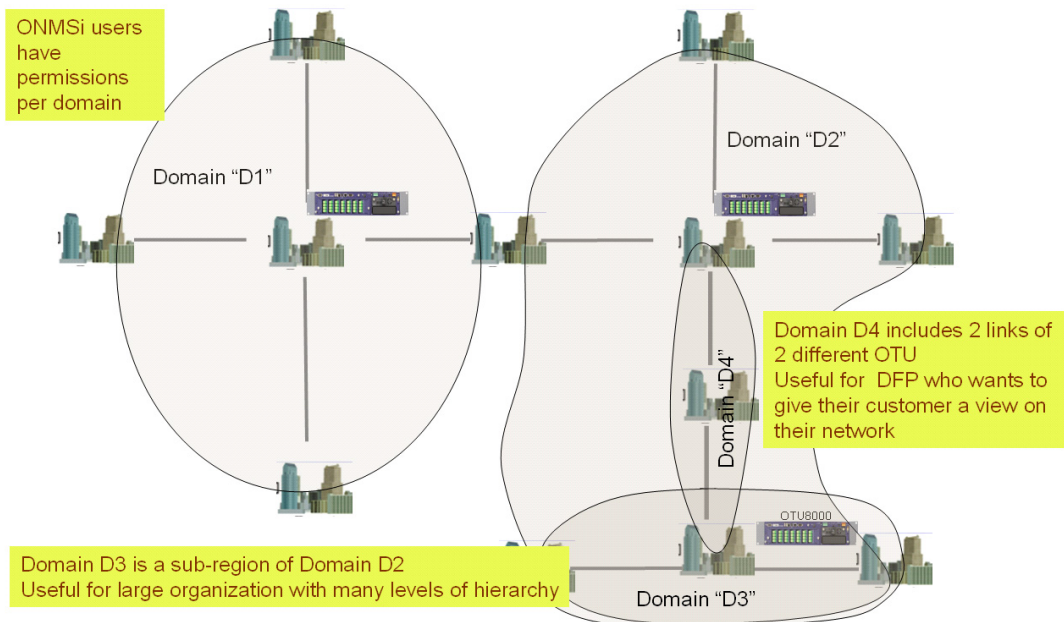
The ONMSi application allows to configure the flexible architecture of the network based on domains.

Domains description

The network can be made of:

- **Domains:** regions where the OTU's network infrastructure is located.
- **Sub-domains:** region into the «main» region (Domain) where the OTU's network infrastructure is located
- **Fictive regions:** regions defined by several links (no OTU) installed in a same or in different (sub-)domain(s).

Figure 44 Domains architecture



## Creating a domain

The user can create a domain if he has the privileges for it.

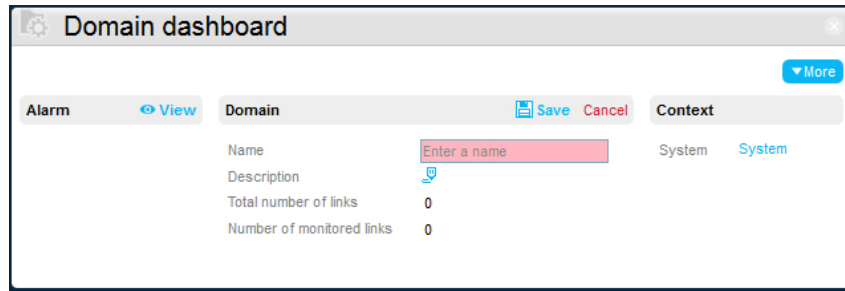
- 1 From the **System dashboard**, click on **Add a domain** button  
or

From the Tree view, select **System**, right click and click on **Add a domain** (or click on **More > Add a domain** buttons)

The domain dashboard displays.



**Figure 45** Adding a domain



- 2 Enter a **Name** for the domain
- 3 If necessary, click on the **Description** icon and enter a detailed description for this domain.
- 4 Click on **Save** to confirm the new domain, or **Cancel** to cancel the domain creation.

Double click on the Domain name in the Tree view to display the corresponding dashboard.

**Figure 46** Domain created

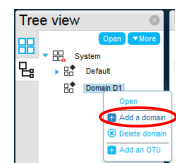


## Adding sub-domains

Once the Domain is created (D1 in the example), the sub-domains can be added to the domain. As many domains as you want can be created.

- 1 From the Domain dashboard (Figure 19), click on Add a domain button  
or

From the Tree view, select the domain just created and right click to select Add a domain (or, once domain is selected, click on More > Add a domain button)



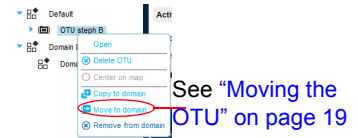
- 2 Follow instructions from [step 2](#) to [step 4](#) on [page 49](#) to validate the sub-domains.

## Copying an OTU to another domain

Some OTUs from other domains can be added to a domain or sub domain.

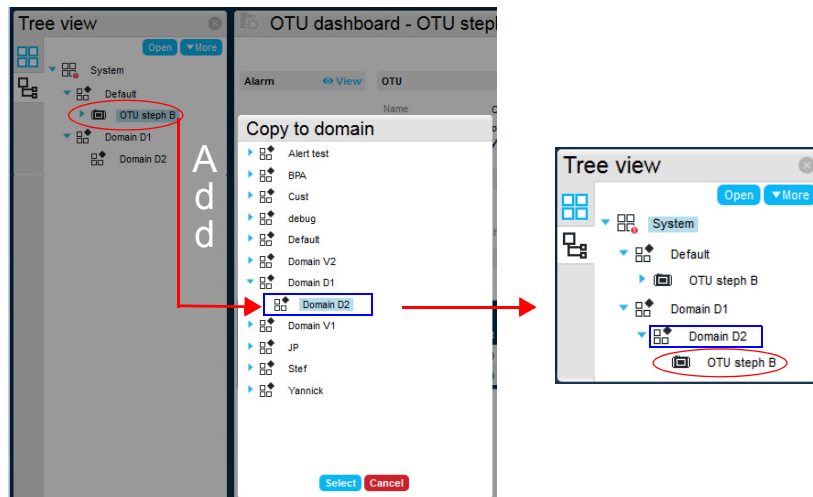
To add an existing OTU to a domain / sub-domain:

- 1 On the Tree view, select the OTU (highlighted in grey)
- 2 Right click on the OTU
- 3 Click on **Copy to domain**.
- 4 In the new dialog bow, select the destination (sub-)domain.
- 5 Click on **Ok** to validate.



The OTU is copied to the (sub-)domain, with the Link(s) and section(s) associated to the OTU, if any.

Figure 47 Copying an OTU to another domain



### CAUTION

If the parameter «Move the OTU» is selected, the OTU will be deleted from the initial (sub-)domain and set into the selected (sub-)domain

## Removing an OTU from a domain

An OTU added to a sub-(domain) can be deleted from this (sub-)domain exclusively, and kept in the initial domain:

- 1 On the Tree view, select the OTU (highlighted in grey)
- 2 Right click on the OTU
- 3 Click on **Remove from domain**.

The OTU is removed from the (sub-)domain, but kept in the other domains it is installed on.

## Deleting an OTU

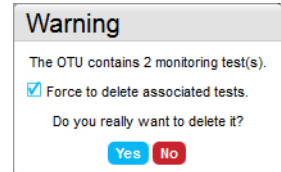
An OTU can be deleted from all the (sub-)domains it has been added:

- 1 On the Tree view, select the OTU (highlighted in grey)
- 2 Right click on the OTU
- 3 Click on **Delete OTU**.

A warning may displays if some monitoring tests are processing, or if an Alarm has been detected on this OTU.

- 4 Click on **Force to delete associated tests/alarms** to confirm the deletion
- 5 Click on **Ok**

The OTU is deleted from the system.



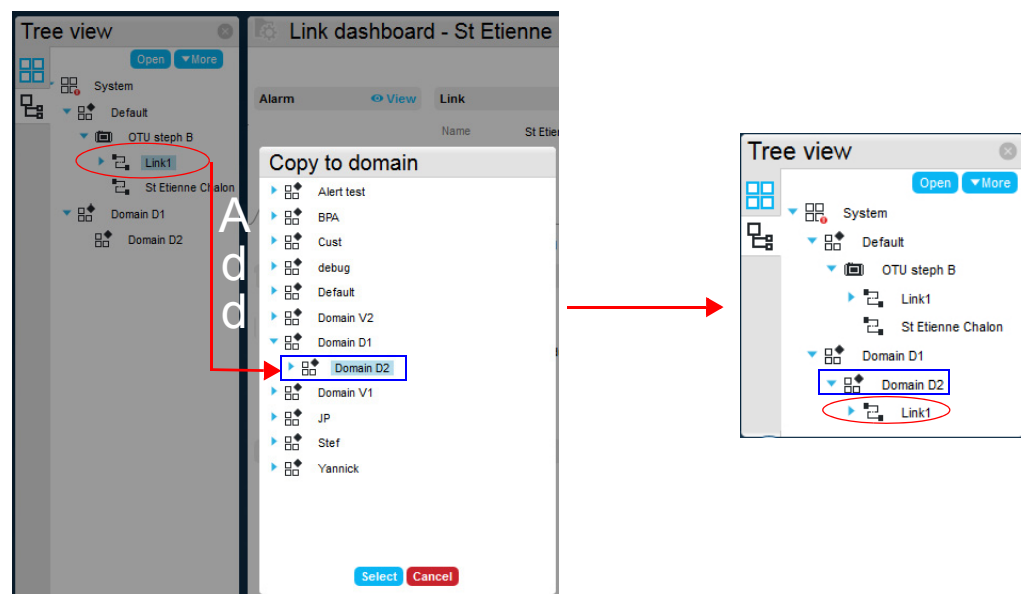
## Copying a link to a domain

Some links from other domains can be added to a (sub-)domain and, if not linked to an OTU, are considered as «fictive regions».

To add an existing link to a domain / sub-domain:

- 1 On the Tree view, select the link (highlighted in grey)
- 2 Right click on the link
- 3 Click on **Copy to domain**.
- 4 In the new dialog bow, select the destination (sub-)domain.
- 5 click on **Ok** to validate.

Figure 48 Copying a link to another domain





# Advanced Monitoring

This chapter provides a description of the possible action on the Link, once reference trace has been defined and link is monitored.

Topics discussed in this chapter include the following:

- [“Advanced Setup” on page 54](#)
- [“Advanced Monitoring” on page 59](#)

# Advanced Setup

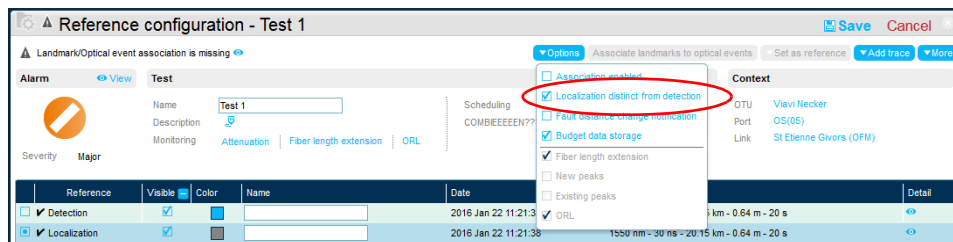
This chapter gives a description of the advanced parameters available for a link.

## Localization distinct from detection

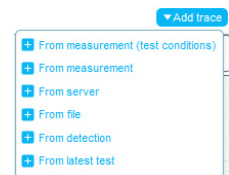
When a fiber fault is detected a 2nd OTDR acquisition is launched to localize the fault. This 2nd acquisition uses the same parameters as the 1st one by default but it is possible to define different parameters by enabling the field **Localization distinct from detection**. It is useful to use this possibility to improve the accuracy by setting a longer acquisition time with a narrower pulse width.

- 1 From the Link dashboard, click on **Configuration & Reference**.
- 2 In the Reference configuration screen, click on **Edit**.
- 3 Click on the **Options** button and select the parameter **Localization distinct from detection**.  
By default, the same trace as the detection trace is added in the traces viewer and list.

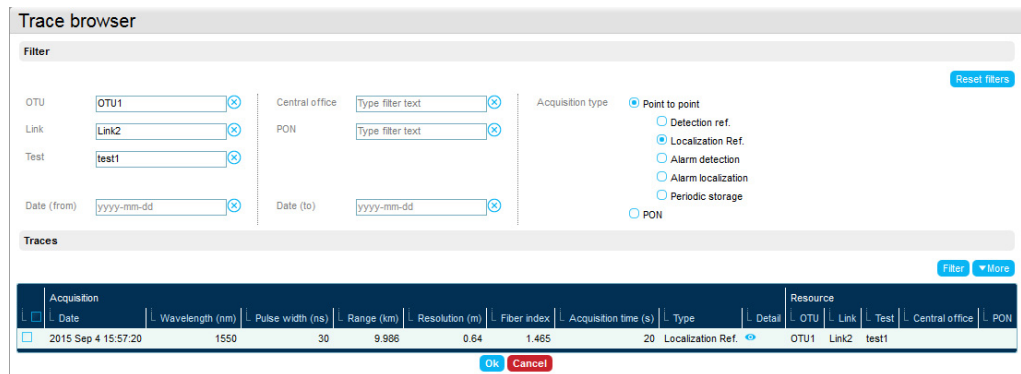
Figure 49 Selection of the parameter



- 4 Click on the **Add trace** button.
- 5 Select the trace localization from the sub-menu.  
**From measurement:** modify the OTDR acquisition parameters (**Manual** mode), then launch the measurement.  
**From measurement (test conditions):** launch an automatic measurement.  
**From Server:** select the trace using the Trace Browser window:



**Figure 50** Trace viewer



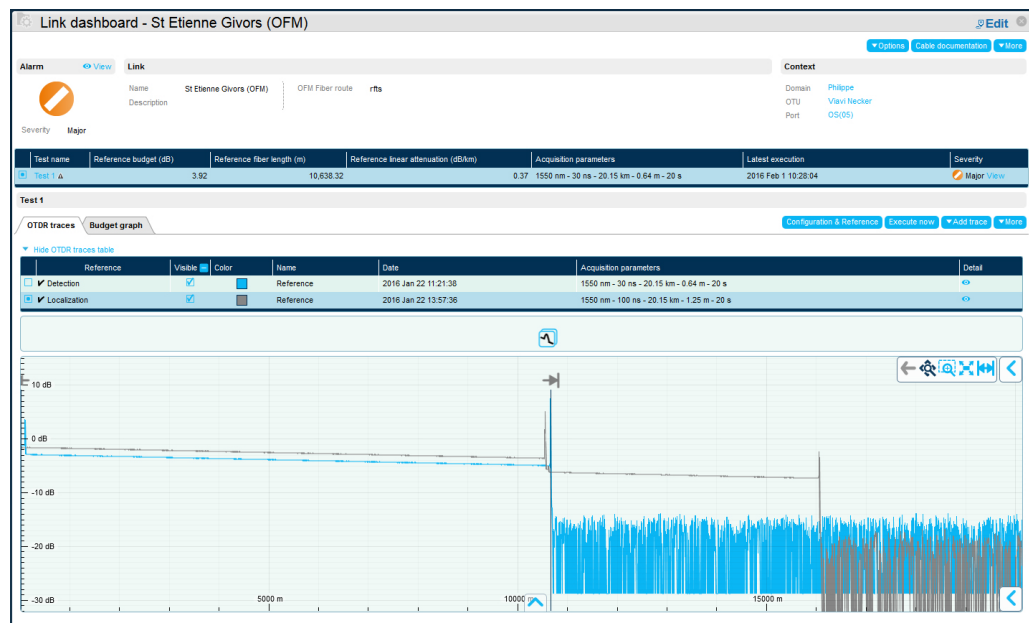
**From File:** click on **Browse** and select the trace from your PC.

**From Detection:** the detection trace become the Localization trace

**From latest test:** the trace acquired from the last test performed is defined as the localization trace.

- 6 Select the trace just added and click on the **Set As Reference** button.
  - 7 Click on the parameter **Set as Localization** to define the selected trace as localization reference trace.
  - 8 Click on **Save** to save the modifications.
  - 9 Click on the **Link** in the Context window to return to Link Dashboard.
- Once localization is distinct from detection trace, the screen is as follow:

**Figure 51** Localization trace



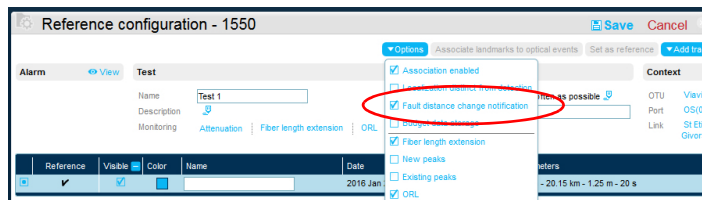
## Fault distance change notification

When a fiber is in alarm, if the fault distance changes, the alarm information is updated accordingly, if it is being processed, if the **Fault distance change notification** field is enabled.

If it is disabled, the alarm is updated only when the severity changes.

- 1 From the **Link dashboard** window, click on **Configuration & Reference** button.
- 2 In the Reference configuration window, click on **Edit**.
- 3 Select the parameter **Fault distance change notification**.
- 4 Press **Save** to confirm the selection.

Figure 52 Selection of the parameter



The alarm is displayed as soon as an event is detected before the first event.

Figure 53 Two alarms of the same severity



### NOTE

This option slows down the scanning in case of alarm.

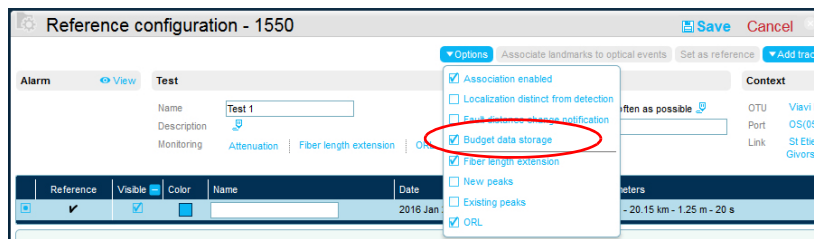


## Downloading budget data

The data of the budget can be download on the PC in an Excel file format.

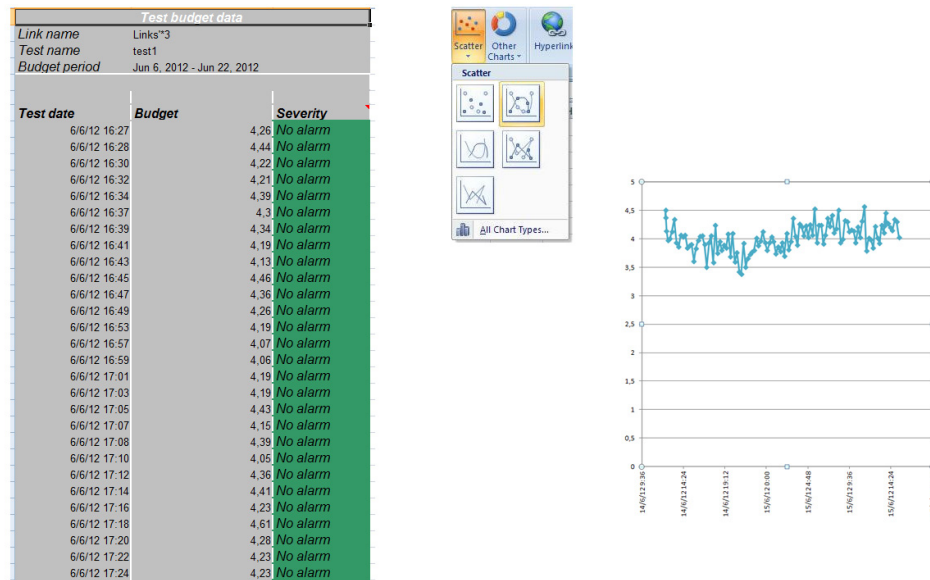
- 1 From the **Link dashboard** window, click on **Configuration & Reference** button.
- 2 In the Reference configuration window, click on **Edit**.
- 3 Select the parameter **Budget data storage**.
- 4 Press **Save** to confirm the selection.

**Figure 54** Budget data storage selection



- 5 Click on the **Link** in the Context window to return to Link Dashboard.
- 6 Click on **More** button and select **Download budget data as Excel**.
- 7 Click on **Save file** to store the Excel file, or click on **Open with** to directly open the file.

**Figure 55** Budget data in Excel format




## Scheduling a test

The **Scheduling** parameter allows to schedule the:

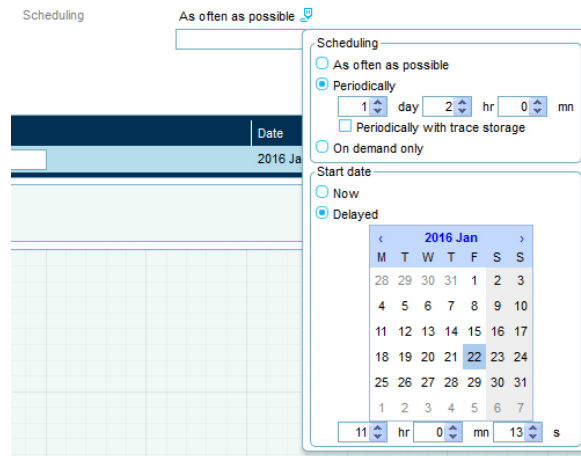
- the monitoring period of the test/link

- starting date of the monitoring.

This allows to assign higher or lower different priority to a particular test or link.

- 1 From the Link dashboard, click on **Configuration & Reference**.
- 2 In the Reference configuration screen, click on **Edit**
- 3 In the **Scheduling** parameter, click on the icon  to modify the monitoring scheduling parameters.


**Figure 56** Scheduling window



- 4 In the **Scheduling** window, select:
  - **As often as possible**: the fiber is tested as soon as the OTDR is available.
  - **Periodically**: for a test at regular time interval
    - Minimum period 1 minute
    - Maximum period 999 days
  - **On demand only**: to launch a test exclusively on demand.
- 5 In the **Start day** window, select:
  - **Now**: to start immediately the monitoring.
  - **Delayed**: to start the monitoring later. Select a start date in the calendar.
- 6 Click on **Save** to save the scheduling of the test.

## Stopping the test / all tests and forbid any shoot on the link

- 1 In the Port association screen, select in the list, the port(s) for which measurements must be forbidden.
- 2 Click on **More**
- 3 Click on **Disable Measurement**.
- 4 **Save** the modification.

The symbol  displays next to the port for which measurements are forbidden



## Performing a test on demand

At any time during the monitoring, a test of the link can be performed from the Link dashboard:

- 1 Select the link to be tested.
- 2 Click on **Execute now**.

The test starts using the references parameters and an alarm is generated in case of fiber cut (severity: critical).

## Advanced Monitoring

This chapter describes the process to add monitoring tests such as fiber length, ORL...




### NOTE

All those measurements can generate alarms expect in case of critical alarms (fiber cut) or attenuation alarms.

## Modifying the attenuation thresholds

To modify the thresholds of attenuation for a monitored link:

- 1 From the **Link dashboard**; click on **Configuration & Reference** to open the Reference configuration window.
- 2 Click on the arrow  at the bottom of the trace.
- 3 Click on the tab **Attenuation**.

Under the trace, the **Attenuation** thresholds are displayed.

Figure 57 Attenuation thresholds



- 4 Click on **Edit** to modify the attenuation parameters

- 5 Configure the threshold for the attenuation:
  - Define the maximum threshold for the **First marker variation**, in dB
  - Define the maximum threshold for **Budget variation**, in dB.
- 6 Click on **Threshold** button and select the following parameter(s):
  - **Minor threshold enabled**: to display and modify of necessary the minor thresholds for First marker variation and budget variation.
  - **Advanced configuration**: to manually define the hysteresis; if not selected the hysteresis is calculated automatically (0.2 dB).
- 7 Press **Save** to save the thresholds.

### Alarms on test attenuation

First Marker (FM) level	Last Marker (LM) level	Budget variation	Severity	Additional text
Above FM minor	Above the noise floor	< Minor	No alarm	
	Above the noise floor	Between minor & major	Minor	Attenuation
	Above the noise floor	> Major	Major	Attenuation
	Above the noise floor	> 6 dB	Critical	Fiber cut
Between FM minor & FM major	Below the noise floor	Not measured	Critical	Fiber cut
	Above the noise floor	< Minor	Minor	Injection
	Above the noise floor	Between minor & major	Minor	Injection
	Above the noise floor	> Major	Major	Attenuation
	Above the noise floor	> 6 dB	Critical	Fiber cut
For FM Major <sup>a</sup>	Below the noise floor	Not measured	Critical	Fiber cut
	Any	Any	Major	Injection

a. For OTU8000 V2 Version ≥ 6.00 and OTU8000 V1 Version ≥ 3.30

### Fiber length extension

The fiber length extension consists in triggering an alarm if the fiber length is shifted and exceeds the threshold.

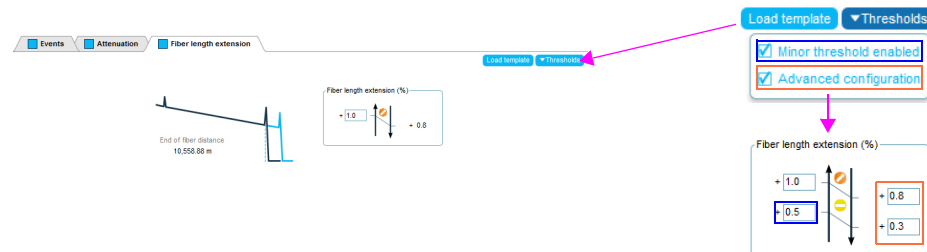
- 1 From the **Link dashboard**; click on **Configuration & Reference** to open the Reference configuration window.
- 2 Click on **Edit**.
- 3 Click on **Options** button and select **Fiber Length extension**.  
Under the trace, the new tab **Fiber length extension** is displayed.



**CAUTION**

This option is not available if the parameter Localization distinct from Detection is selected.

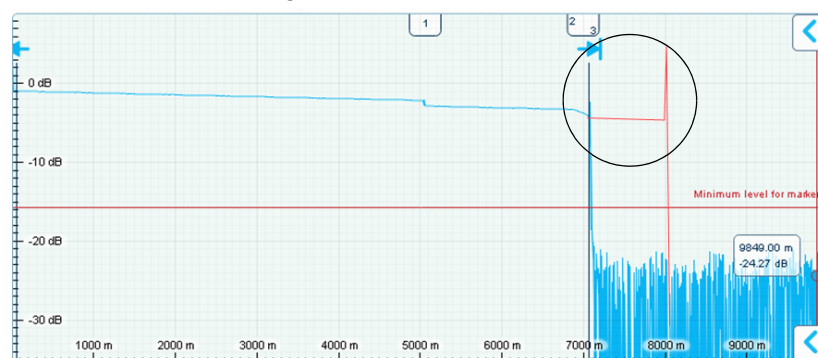
**Figure 58** Fiber length extension



- 4 Configure the threshold for the fiber length, in %.  
Default values: 0.8% for minor
- 5 Click on **Threshold** button and select the following parameter(s):
  - **Minor threshold enabled**: to display and modify of necessary the minor thresholds for fiber length.
  - **Advanced configuration**: to manually define the hysteresis; if not selected the hysteresis is calculated automatically (0.1%).
- 6 Press **Save** to save the thresholds.

Once a measurement with fiber length extension is performed, a trace as the following one displays:

**Figure 59** Trace with Fiber length extension

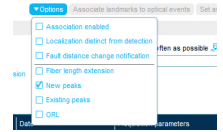


## New peaks

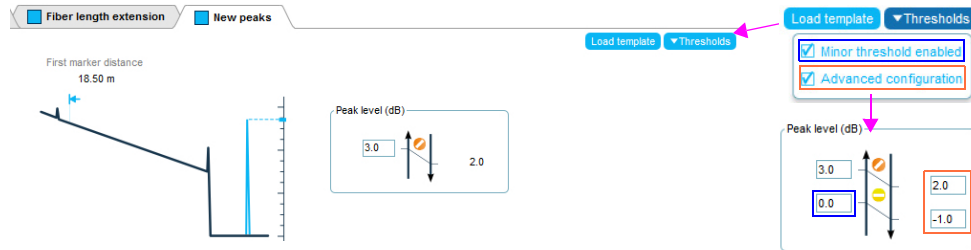
The new peaks parameter consists in triggering an alarm when any new peak appears after fiber end.

The aim of this function is to detect a fiber break after the end of measured fiber.

- 1 From the **Link dashboard**; click on **Configuration & Reference** to open the Reference configuration window.
- 2 Click on **Edit**.
- 3 Click on **Options** and select **New peaks**.  
Under the trace, the new tab **New peaks** is displayed.



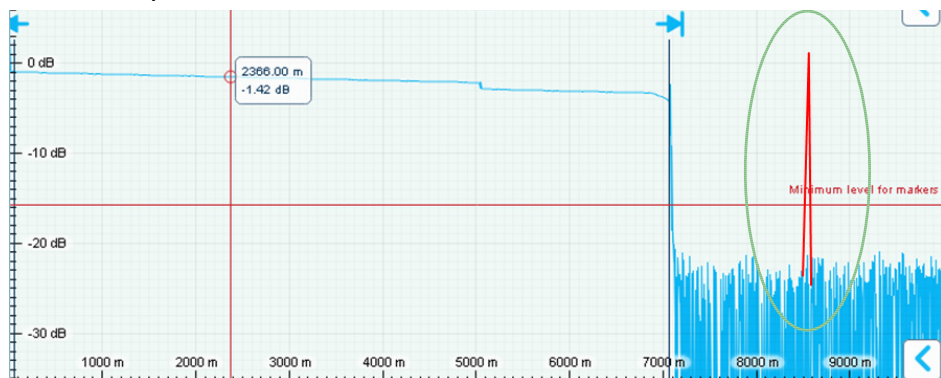
**Figure 60** Thresholds for New Peaks



- 4 Configure the threshold for the peak detection, in dB.  
Default values: 0 dB for minor
- 5 Click on **Threshold** button and select the following parameter(s):
  - **Minor threshold enabled**: to display and modify of necessary the minor thresholds for peak detection.
  - **Advanced configuration**: to manually define the hysteresis; if not selected the hysteresis is calculated automatically (0.5 dB).
- 6 Press **Save** to save the thresholds.

Once a measurement with a new peak after fiber end is performed, a trace as the following one displays:

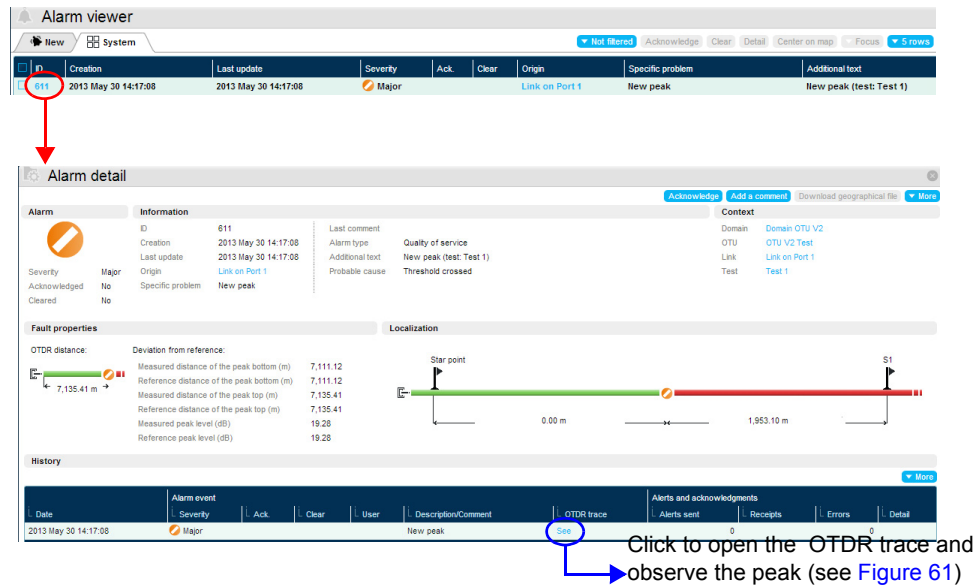
**Figure 61** New peak after fiber end



### Alarm details for new peaks detected

In the **Alarm Viewer**, click on the **Alarm Id** of the New peak to open the details for the alarm.

Figure 62 Alarm details for a new peak



## Existing peaks

With the **Existing peaks** parameter, if a peak changes (distance or level), an alarm is triggered.

- 1 From the **Link dashboard**; click on **Configuration & Reference** to open the Reference configuration window.
- 2 Click on **Edit**.
- 3 Click on **Options** and select **Existing peaks**.  
Under the trace, the new tab **Existing peaks** is displayed.

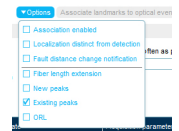
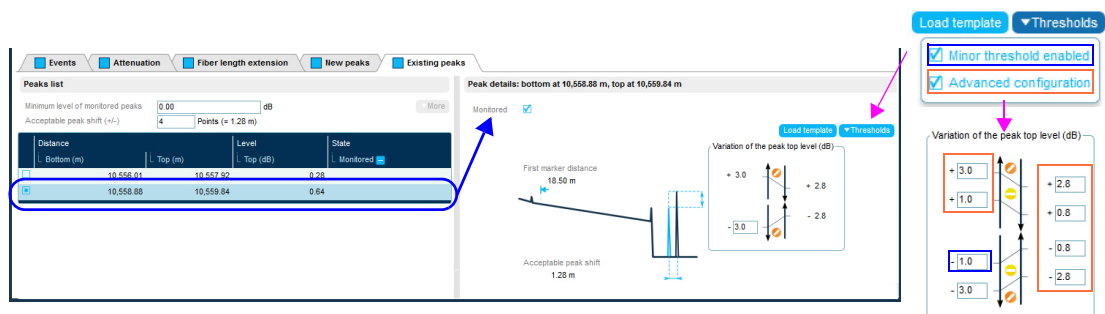


Figure 63 Thresholds for Existing Peaks



The peak list contains the peaks with a level greater than **Minimum level of monitored peaks**.

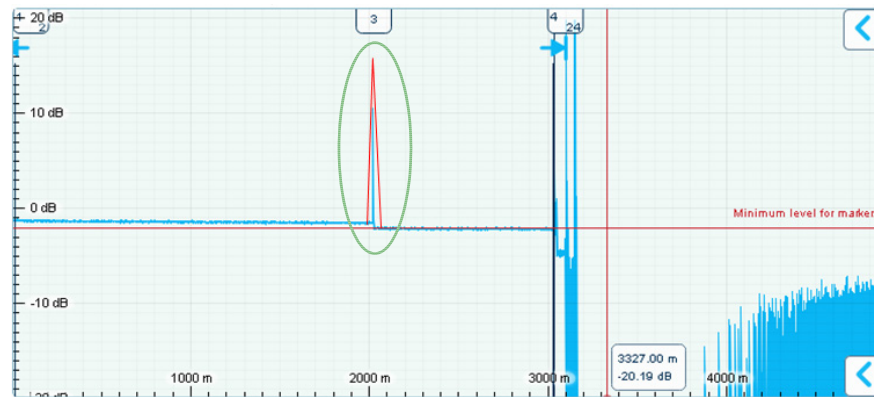
If necessary, modify this parameter in order to reduce/raise the list of peaks.

- 4 Select one peak on the table to define a threshold for this peak and select the **Monitored** parameter.

- 5 Configure the threshold for the existing, in dB.  
Default values: 1 dB for minor / 3 dB for major
- 6 Click on **Threshold** button and select the following parameter(s):
  - **Minor threshold enabled**: to display and modify of necessary the minor thresholds for First marker variation and budget variation.
  - **Advanced configuration**: to manually define the hysteresis; if not selected the hysteresis is calculated automatically (0.1 dB).
- 7 Press **Save** to save the thresholds.

Once a measurement with an existing peak which have changed is performed, a trace as the following one displays:

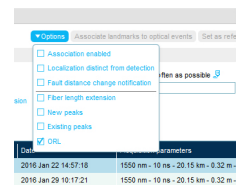
**Figure 64** Existing peak



## ORL

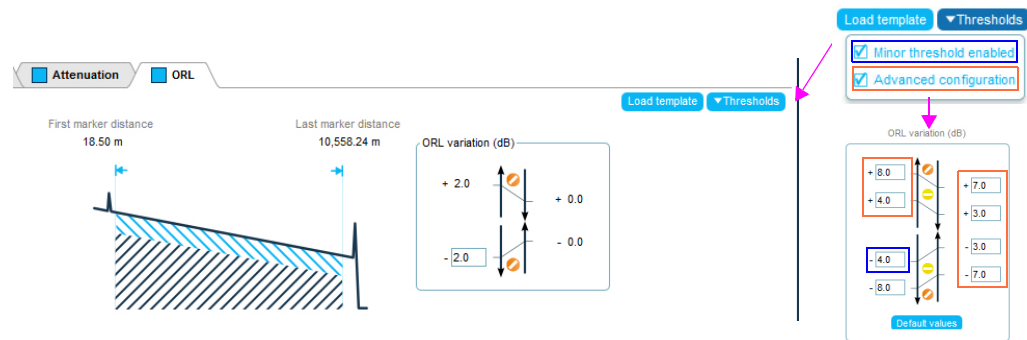
The ORL function allows to triggers an alarm if the ORL between the first and the last marker exceeds the thresholds defined.

- 1 From the **Link dashboard**; click on **Configuration & Reference** to open the Reference configuration window.
- 2 Click on **Edit**.
- 3 Click on **Options** and select **ORL**.  
Under the trace, the new tab **ORL** is displayed.





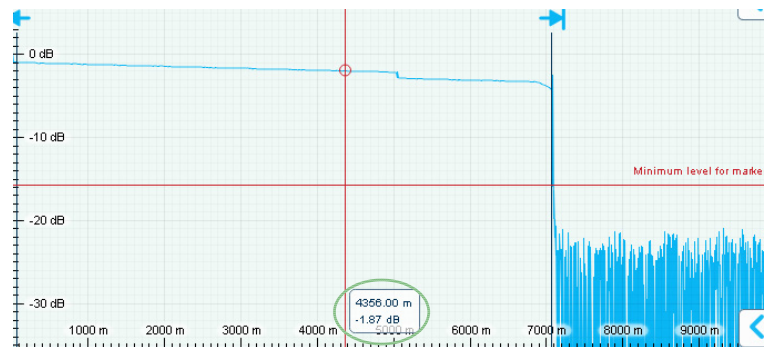
**Figure 65** Thresholds for ORL



- 4 Configure the threshold for the ORL, in dB.  
Default values: 4 dB for minor / 8 dB for major
- 5 Click on **Threshold** button and select the following parameter(s):
  - **Minor threshold enabled**: to display and modify of necessary the minor thresholds for First marker variation and budget variation.
  - **Advanced configuration**: to manually define the hysteresis; if not selected the hysteresis is calculated automatically (1 dB).
- 6 Press **Save** to save the thresholds.

Once a measurement with an ORL is performed, a trace as the following one displays:

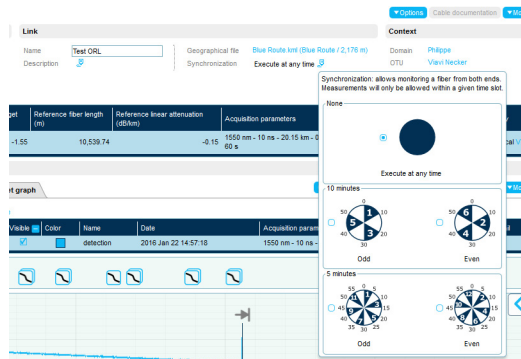
**Figure 66** ORL result




## Both end measurement

In the case the link between two central offices is too long to be monitored from one end, an OTU-8000 is connected at each link end and a both end measurement can be performed.

**Figure 67** Both end measurement configuration



Once in the Link dashboard:

- 1 Click on **Edit**.
- 2 Click on Options button to select **Synchronization**  
The synchronization parameters display in the Link window.
- 3 Click on the icon  .
- 4 Select the **Timeslot**
- 5 Click on **Save**
- 6 Check if the synchronization is configured properly.



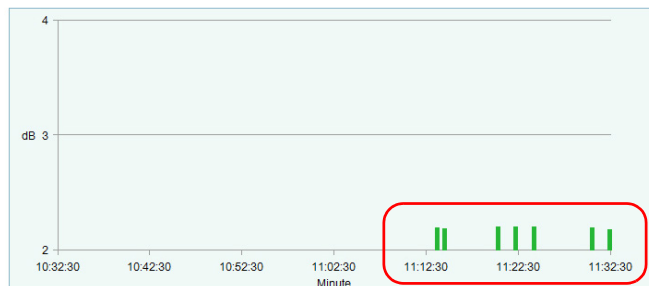
**CAUTION**

Do not forget to set up the opposite time slot on the other test.

**Budget with a time slot**

The budget graphic is impacted by the timeslot, and the display is as following:

**Figure 68** Budget with a time slot



**Cable Documentation**

The Cable document option uses landmarks to serve as reference points for localizing faults.

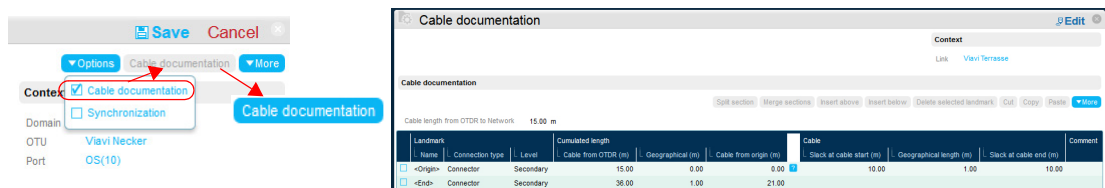
## Activating the Cable documentation function

From the Link dashboard:

- 1 Click on the **Edit** button
- 2 Click on the **Options** button and select **Cable documentation** parameter.
- 3 Click on **Save** to validate.

The button **Cable documentation** displays on the right of the Link window.

**Figure 69** Cable documentation: selection and display



## Activating the Association landmarks and optical events

The Cable documentation is very useful when used in combination with the option **Association enabled**.

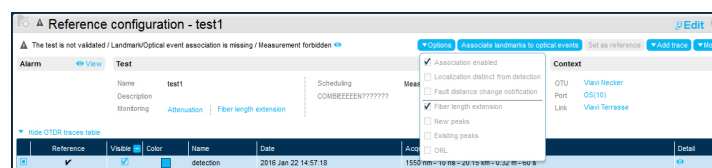
To validate the Association enabled parameter:

- 1 From the Link Dashboard, click on **Configuration & Reference** button.
- 2 In the Reference configuration window, press **Edit**.
- 3 Click on the **Options** button and select the parameter **Association enabled**.

Once selected, the error message **Landmark/Optical event association is missing** is displayed.

The button **Associate landmarks to optical events** turns active.

**Figure 70** Option «Association enabled» selected



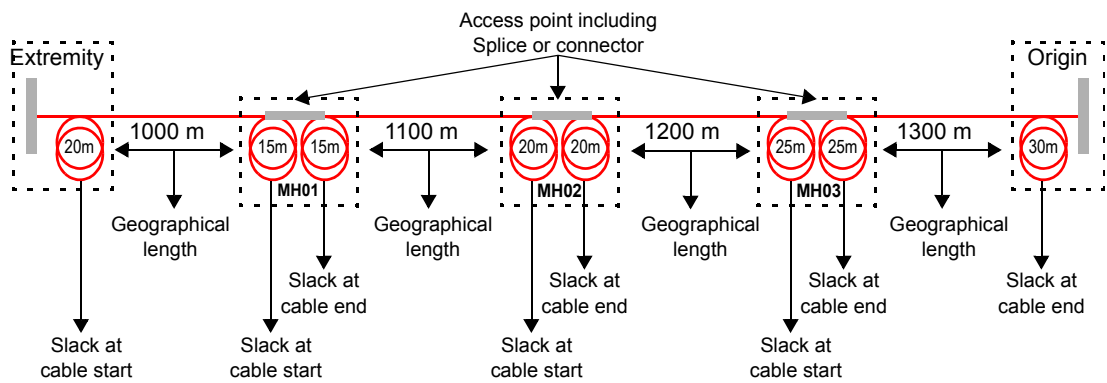
- 4 Click on the button to display the window «Associate landmarks to optical events» for the link selected.

## Completing the landmark table

- 1 Click on **Cable documentation** button.  
The **Origin** and **Extremity** landmarks are defined by default.
- 2 Click on **Edit** to complete the table with the necessary components of the fiber to be tested.

- 3 Configure the **Origin** and **Extremity** parameters
- 4 Add and configure as many landmarks as wished:
  - a Select one parameter and click on the **Insert above** or **Insert below** button to add a new line on the table.
  - b Enter a **Name** for the new connection
  - c Select the **Connection type** in the list: **Connector** / **Splice** / **No connection**.
  - d Select if this must be a **Primary** element, used in alarm fault distances.  
The **Primary** function allows to get the distance of the fault according to the previous primary element and according to the next primary element.
  - e Enter the size of the **Slack at cable start**, in meter.
  - f Enter the **Geographical length**, in meter, of the element from the start of the fiber.
  - g Enter the size of the **Slack at cable end**, in meter.

**Figure 71** Completing the landmark table according to the optical events



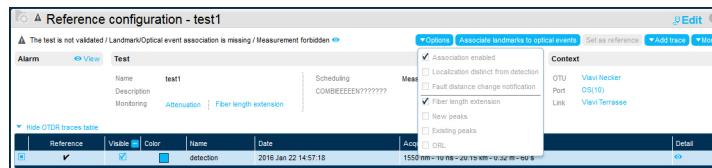
Description	Cable			Cable			
	Name	Connection type	Primary	Total Geographical length (m)	Total cable length (m)	Slack at cable start (m)	Geographical length (m)
Origin	Connector	<input checked="" type="checkbox"/>	0.00	0.00	20	1000	15
MH01	Splice	<input type="checkbox"/>	1,000.00	1,035.00	15	1100	20
MH02	Splice	<input type="checkbox"/>	2,100.00	2,170.00	20	1200	25
MH03	Splice	<input checked="" type="checkbox"/>	3,300.00	3,415.00	25	1300	30.00
Extremity	Connector	<input checked="" type="checkbox"/>	4,600.00	4,770.00			

- 5 Click on **Save** to save the modifications.

### Creating a landmark table from a trace

A landmarks table can be created directly from an acquisition trace, such as from the reference trace.

Figure 72 Option «Association enabled» selected



- 1 In the Reference configuration screen, click on the button **Associate landmarks to optical events** to display the window «Associate landmarks to optical events» for the link selected.
- 2 Click on **Edit**.
- 3 Click on **Landmarks** and select **Events to landmarks**.
- 4 In the **Information** dialog box, modify the Scale factor and size of cable slack if needed.
- 5 Click on **Ok** to start the landmarks table creation.  
The landmarks are automatically created according to the optical events on trace.

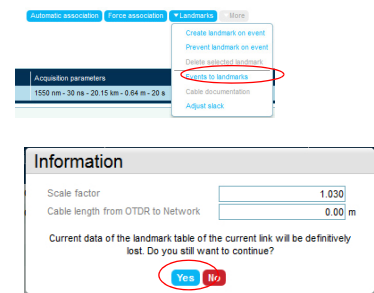
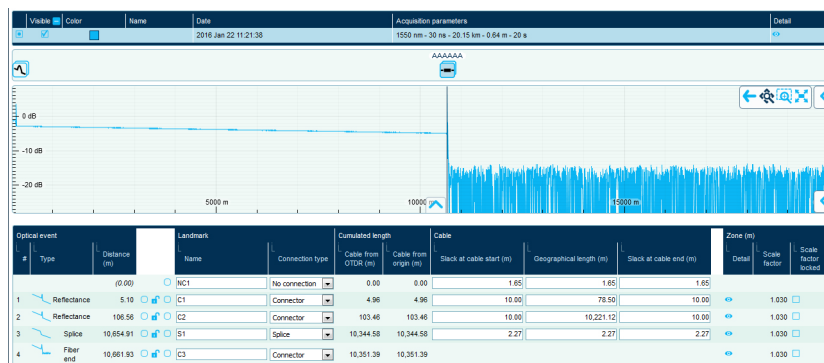


Figure 73 Landmark table and trace



- 6 Click on **Edit** and modify some parameters if necessary.
- 7 Click on **Save** to validate the modifications.

### Create a landmarks table from an Excel file

- 1 Create the landmark table in an Excel™ file.  
We advise you to download a landmark table from ONMSi toward your PC and to modify and save the file in Excel.

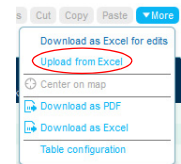
**Figure 74** Example of Excel file for landmark table

Bold columns are mandatory

1	A	B	C	D	E	F	G	H
2	Landmark Table							
3	Link Name	Port1			Cable			Comment
4	Landmark							
5	<b>Landmark Name</b>	<b>Landmark ID Ext</b>	<b>Connection type</b>	<b>Level</b>	<b>Slack at cable start (m)</b>	<b>Geographical length (m)</b>	<b>Slack at cable end (m)</b>	<b>Comment</b>
6	ODF		Connector	Primary	10	5000		10 OTU
7	Shelter		Connector	Primary	25	1800		25 SC/APC
8	SP1		Splice	Secondary	20	100		20 Fusion
9	SP2		Splice	Secondary	10	1000		10 Mechanical
10	Fiber End		Connector	Primary	0	0		0 SC/APC
11								

2 Upload the file from the Landmark table screen:

- From the Link dashboard, click on Cable Documentation
- In the Table window, click on **More > Upload from Excel**.
- In the new dialog box select the excel file and click Ok to confirm.  
The Upload results dialog box displays.
- Click on **Close** to return to landmark table.



Upload result	
Added	4
Updated	0
Failed	0
Warnings	0
<a href="#">Close</a>	

## Associating Landmark and Optical Event

Once landmark table has been configured,

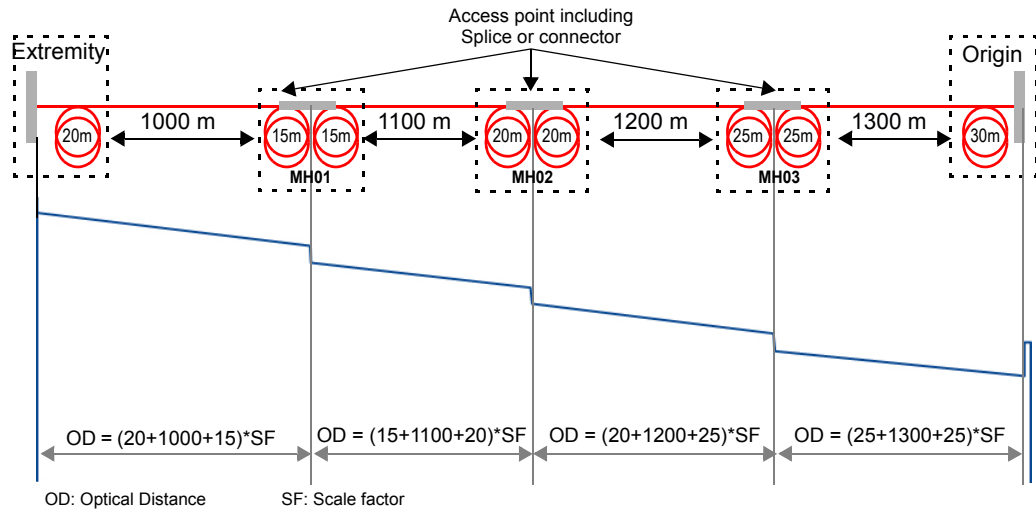
- Return to Reference configuration window (for Link Dashboard, click on **Configuration & Reference** button).
- Click on **Associate landmarks to optical events** button
- Press **Edit** button

**Figure 75** Table and trace before association



- Press **Automatic association** to automatically associate the events of the test to the events entered in the landmark table

**Figure 76** Associations Landmarks optical events



### Force association

If an association has not been performed as it should be in automatic mode:

- 1 Select the landmark and the event to be associated using the radio button on the right of the event and on the left of the landmark
- 2 Click on **Force association** button.
- 3 Check the association.

**Figure 77** Force association

Associate landmarks to optical events

Adjust slack Automatic association **Force association** Force dissociation Create landmark Delete selected landmarks Landmark table More

Cable length from OTDR to Network: 10.00

Optical event #	Type	Distance (m)	Landmark Name	Connection type	Cumulated length Cable from OTDR (m)	Cable from origin (m)	Slack at cable start (m)	Geographical length (m)	Slack at cable end (m)	Zone (m) Detail	Scale factor	Scale factor locked
			Origin	Connector	10.00	0.00	10.00	1.00	10.00			
			Extremity	Connector	31.00	21.00						
1	Splice	5,046.85										
2	Splice	7,011.36										
3	Reflectance	7,065.07										
4	Fiber end	8,078.03										

#### Forced Association

Optical event #	Type	Distance (m)	Landmark Name	Connection type	Cumulated length Cable from OTDR (m)	Cable from origin (m)	Slack at cable start (m)	Geographical length (m)	Slack at cable end (m)	Zone (m) Detail	Scale factor	Scale factor locked
1	Splice	5,046.85	Origin	Connector	10.00	0.00	10.00	1.00	10.00		504.685	

Deselect to unlock the event

### Remarks on association

- If all landmarks are still not matching properly, lock the correct associations and try a new automatic association or force a new association (see “Force association” on page 71).

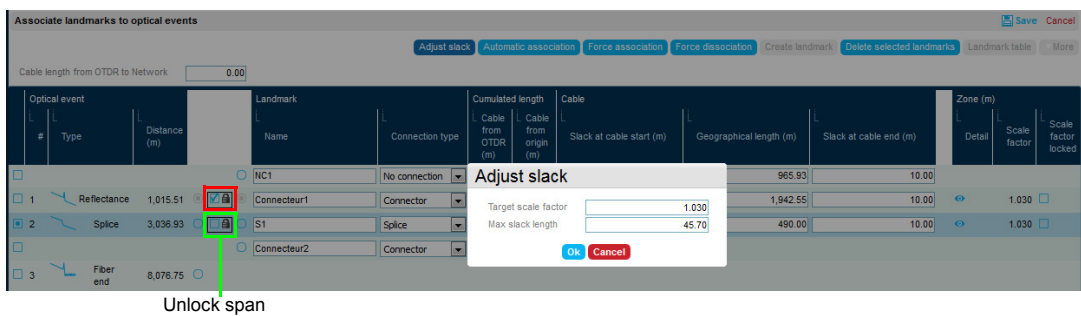
- If a landmark is still not matching properly, you can dissociate it:
  - a Select both radio buttons
  - b Click on **Force dissociation** to unlock the association

### Adjusting scale factor and slacks

You can correct the scale factor, either changing the geographical length or adjusting the slacks.

- 1 Lock the spans with correct scale factor
- 2 Click on **Landmarks** button and select **Adjust slack**.

Figure 78 Adjust slack

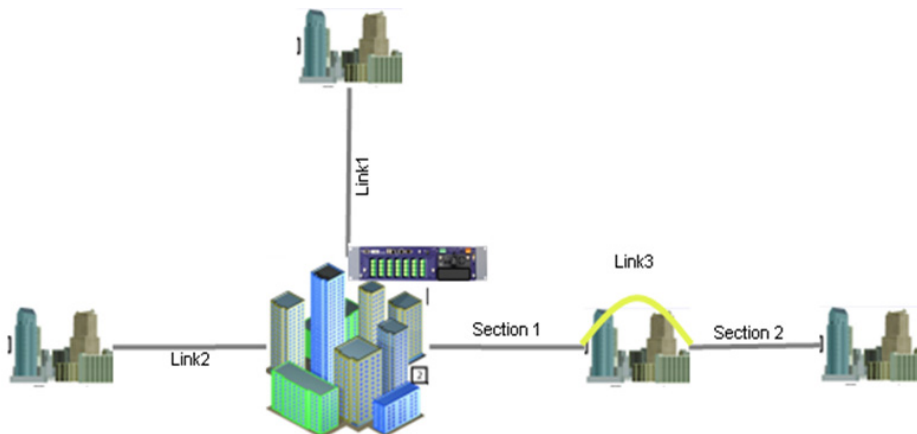


- 3 Adjust scale factor and max length if needed.
- 4 Click on **Ok** to validate.

### Splitting section

ONMSi offers the possibility to split a monitored fiber in different sections. In the case where section 1 and 2 correspond to leased fiber of different customer, this feature allow to clearly separate all the events that can affect one or the other section.

Figure 79 Section on monitored fiber

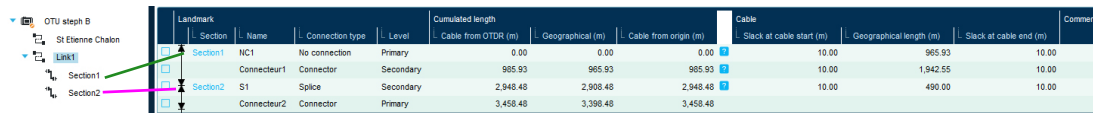


- 1 From the Link dashboard, click on **Cable documentation**.



- 2 Click on **Edit**.
- 3 Select the intersection landmark.
- 4 Click on **Split section**.
- 5 Modify the **Name** of each section if wished.
- 6 Click on **Save** to validate the section.

**Figure 80** Sections representation



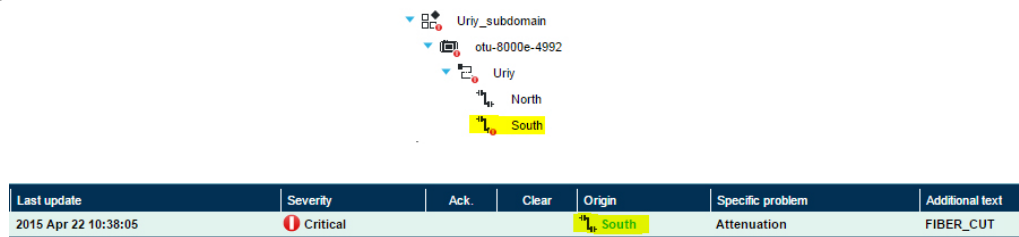
Landmark	Section	Name	Connection type	Level	Cumulated length			Cable		
					Cable from OTDR (m)	Geographical (m)	Cable from origin (m)	Slack at cable start (m)	Geographical length (m)	Slack at cable end (m)
	Section1	NC1	No connection	Primary	0.00	0.00	0.00	10.00	965.93	10.00
		Connecteur1	Connector	Secondary	965.93	965.93	965.93	10.00	1,942.55	10.00
	Section2	S1	Splice	Secondary	2,948.48	2,908.48	2,948.48	10.00	490.00	10.00
		Connecteur2	Connector	Primary	3,458.48	3,398.48	3,458.48			

### Alarms on section

The section with alarm is displayed as faulty.

In the alarm viewer, the **Origin** displays the section name.

**Figure 81** Alarm on section



Last update	Severity	Ack.	Clear	Origin	Specific problem	Additional text
2015 Apr 22 10:38:05	Critical			South	Attenuation	FIBER_CUT

## Associating a geographical file to a link

You can associate a geographical file, to a link in ONMSi.

This allows to create a path of the link on a map and to geographically locate the alarms on this map.

This feature can be used with all the mapping software supporting KML. KLM format (**Keyhole Markup Language**) is an XML notation for expressing geographic annotation and visualization within Internet-based, two-dimensional maps and three-dimensional Earth browsers. It is an international standard of the Open Geospatial Consortium.

The process below is given for Google Earth™.

- 1 Draw a path on Google Earth™ using the path tool.



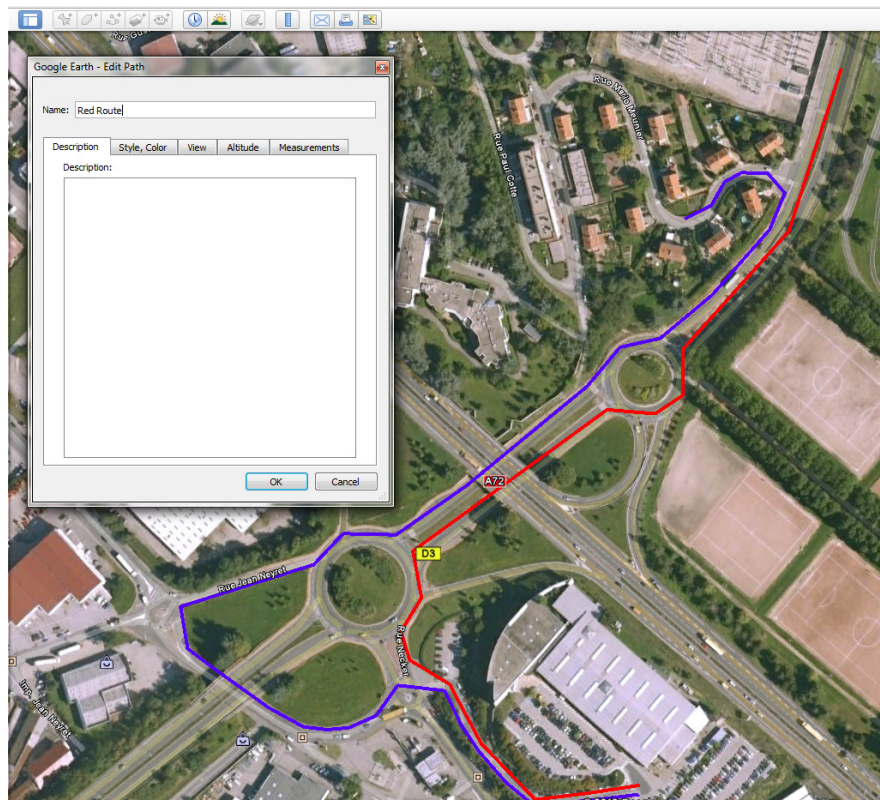
#### NOTE

The path must start at the OTDR location.

- 2 Enter a name for the path and click OK.

- 3 Make sure the Path is saved in the folder **My Places**; if it is saved in the folder **Temporary places**, save it in the folder My places (from the File menu, select Save > Save to my places).
- 4 Once in the places folder, click on **File > Save Place as...** and enter a name for the path.  
You can save the path as kml or kmz file.  
All the folder My Places can be saved in one single kml or kmz file (click on File > Save My places...).

Figure 82 Path drawn in Google Earth™



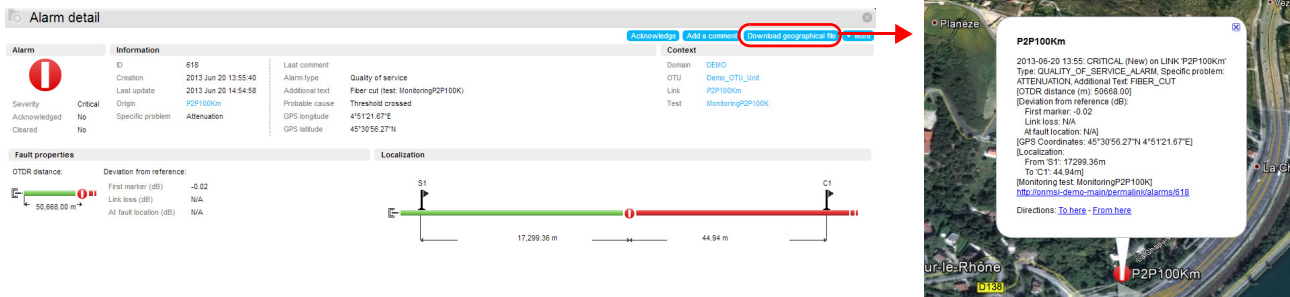
### In the Link dashboard

From the link dashboard of the ONMSi, the link can be associated to the kml or kmz file just created:

- 1 Open the Link dashboard of the link, to associate a geographical file to it.
- 2 Click on **More > Associate geographical file**.
- 3 In the Geographical file association, click on **Browser**
- 4 Select the kml or kmz file just saved.  
If several paths had been saved in the kml or kmz file, select the proper route.
- 5 Click on **Ok**.  
Once an alarm is detected on the link, the detailed view of the alarm is modified:
  - The GPS coordinates are displayed.

- Click on the **Download geographical file** to generate the kmz file for the alarm.
- Click on the alarm on the map to display the details on this alarm.

Figure 83 Alarm details on map



## Adding an OTU to a schematic

A picture can be downloaded from PC and used as schematic to graphically represent the network and visualize the OTUs, and the alarm related to those OTUs.

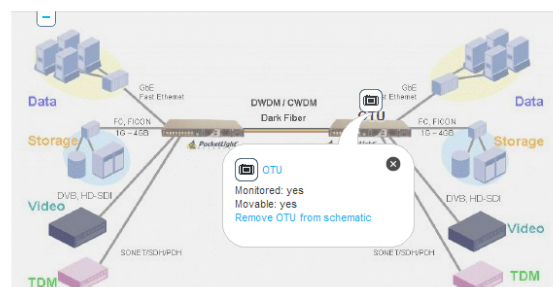
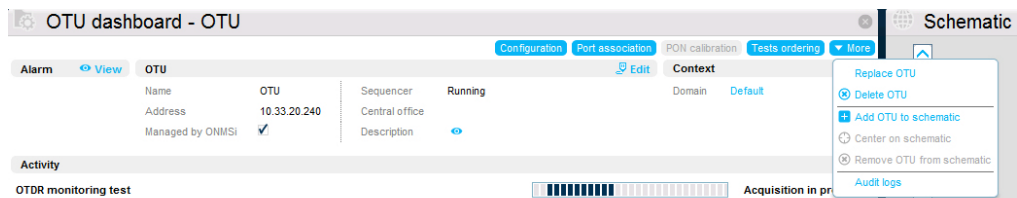
To download a schematic, refer to “[Downloading a schematic](#)” on page 114.

## Adding an OTU to the schematic

Once the schematic is downloaded:



- 1 Open the dashboard of the OTU to be added in the schematic.
- 2 Click on **More**.
- 3 Click on **Add OTU to schematic**.
- 4 Click **Ok** to confirm.
- 5 The OTU is displayed on the schematic

Figure 84 OTU on schematic




## Displacing the OTU on schematic

The position of the OTU on the schematic can be modified from this schematic:

- 1 In the schematic view, click on the icon  .
- 2 Place the mouse onto the OTU and drag and drop it at the correct place.  
The OTU icon  is displaced.

## Centering the OTU on schematic

The position of the OTU can be centered on the schematic:

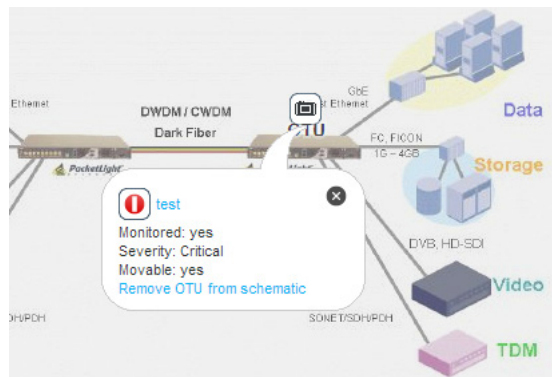
- 1 In the OTU dashboard, click on More.
- 2 Click on Center on schematic.  
The OTU icon  is centered onto the schematic.

## Displaying the dashboard of an OTU alarm from the schematic

If an alarm on the OTU set onto the schematic appears, the alarm icon and related information are displayed on the schematic.

Click on the link of the alarm (blue text) to display the dashboard for this alarm:

**Figure 85** Schematic with an alarm on OTU



Click on the name of the OTU to display the OTU dashboard and visualize the details of the alarm.

# Alarms management

This chapter provides a description of the Alarms management.

Topics discussed in this chapter include the following:

- [“Alarms Display” on page 78](#)
- [“Actions on alarms” on page 79](#)
- [“Actions on table display” on page 82](#)
- [“Notification by e-mail of an alarm” on page 85](#)
- [“Alarm Desktop alert” on page 85](#)

# Alarms Display

## Alarms Viewer

In the Alarm viewer, two tabs are available:

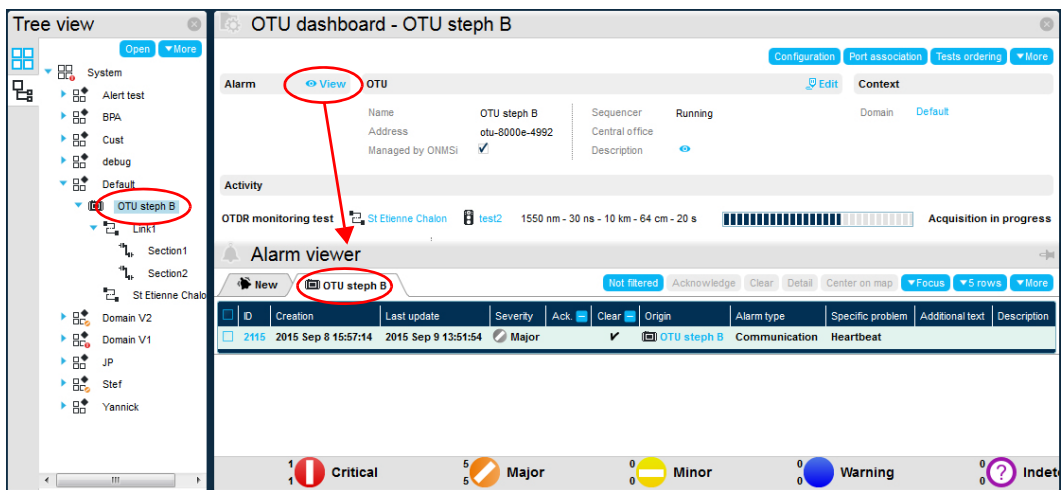
- The tab **New**, which shows the list of Non-acknowledged alarms.  
From this tab, the alarms can be cleared and/or acknowledged (bulk)
- The tab «**Contextual**»: which content depends on the dashboard selected (system, domain, otu, port..).

To display the list of alarms for a specific object:

- a Double click on the object on the tree (for example: an OTU)
- b In the corresponding dashboard, click on the **View** button of the Alarm window

The list of alarms on the selected object displays at the bottom of the screen:

**Figure 86** List of alarms for a specific object



## Alarms details

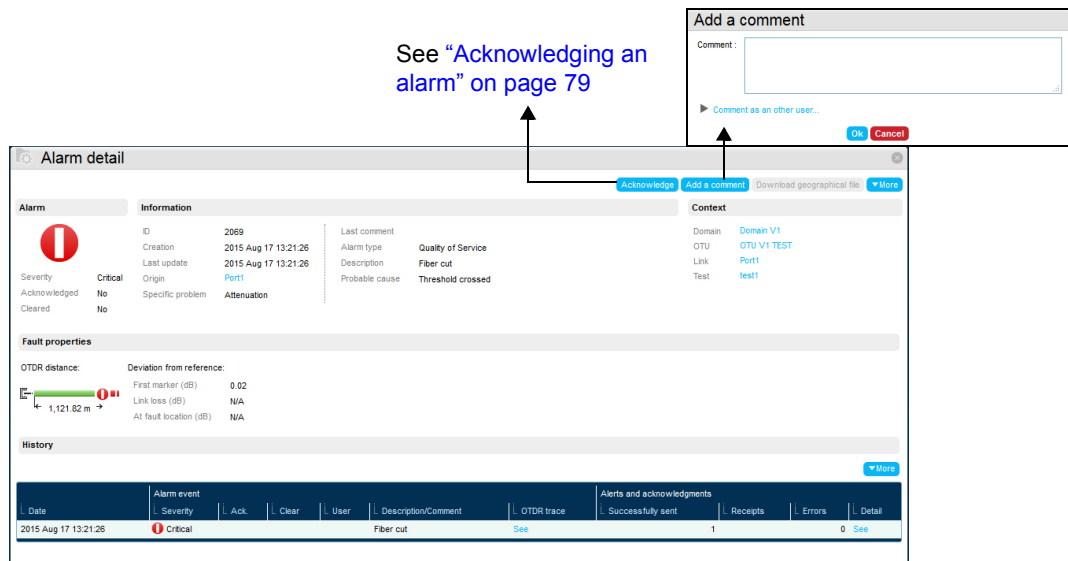
You can access to detail for any alarm (active or cleared).

From the alarm viewer:

- 1 Click on an Alarm **ID** to display the details for.
- 2 Click on **Detail** buttons above the alarms table.

The details of the selected alarm display above the Alarm Viewer.

Figure 87 Alarms details



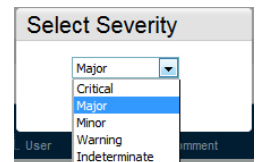
## Actions on alarms

### Changing the alarm severity

From the detailed view of an alarm, the severity level can be modified.

In the detailed view, click on the **More** button

- 1 Click on **Change severity**.
- 2 In the dialog box, select the severity to be applied to the current alarm.
- 3 Press **Ok** to validate



The alarm icon is modified according to the severity selected.

### Acknowledging an alarm

An alarm can be acknowledged, either from the Alarm Detail window or from the Alarm viewer.

- 1 From the Alarm viewer, select first the **Alarm ID**.
- 2 Click on **Acknowledge** button
- 3 Confirm the acknowledgement clicking on **Ok**.
- 4 Click on **Refresh** button to refresh the display.

The alarm is greyed in the list and the **Acknowledged** parameter is selected.

## Unacknowledging the alarm

At any time, the acknowledgement of an alarm can be cancelled.

- 1 In the Alarm viewer, select the **ID** of the acknowledged alarm.
- 2 Click on **More** button
- 3 Click on **Unacknowledge**.

## Clearing an alarm

An alarm can be cleared from the Alarm viewer.

- 1 From the Alarm viewer, select first the **Alarm ID**.
- 2 Click on **Clear** button
- 3 Click on Ok to confirm the clearing.
- 4 Click on **Refresh** button to refresh the display.  
The alarm is greyed in the list and the **Clear** parameter is selected.

## Cancelling the clearing of the alarm

At any time, the clearing of an alarm can be cancelled.

- 1 In the Alarm viewer, select the **ID** of the acknowledged alarm.
- 2 Click on **More** button
- 3 Click on **Unclear**.

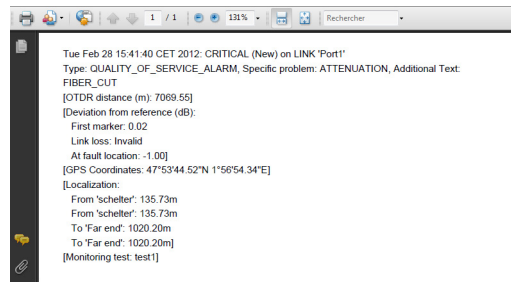
## Downloading a pdf file of the alarm (detail view)

From the alarm detail view:

- 1 Click on **More**.
- 2 Click on **Download as PDF**.
- 3 Click on **Save file** to store the PDF / Excel file, or click on **Open with** to directly open the file.
- 4 Click on **Ok** to validate.



Figure 88 Alarms Table in PDF

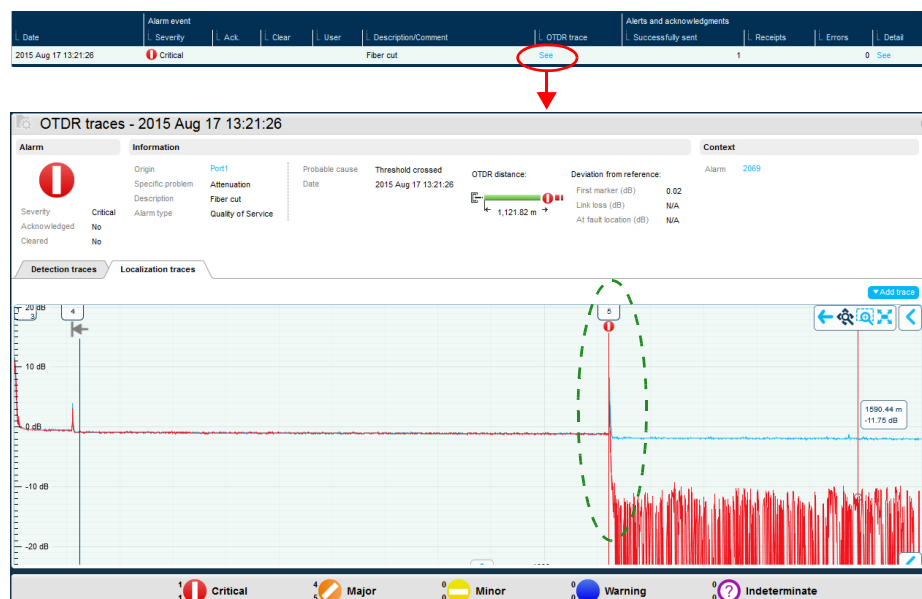


## Alarm History (detail view)

Once in the Detailed view of an alarm, the History window is updated as soon as an event occurs on the alarm (example: a comment is added, severity is changed...)...

In the history, if the alarm concerns a problem on the monitored fiber (fiber cut, attenuation...), the link **See** allows to display the corresponding OTDR trace, with the alarm marked on trace.

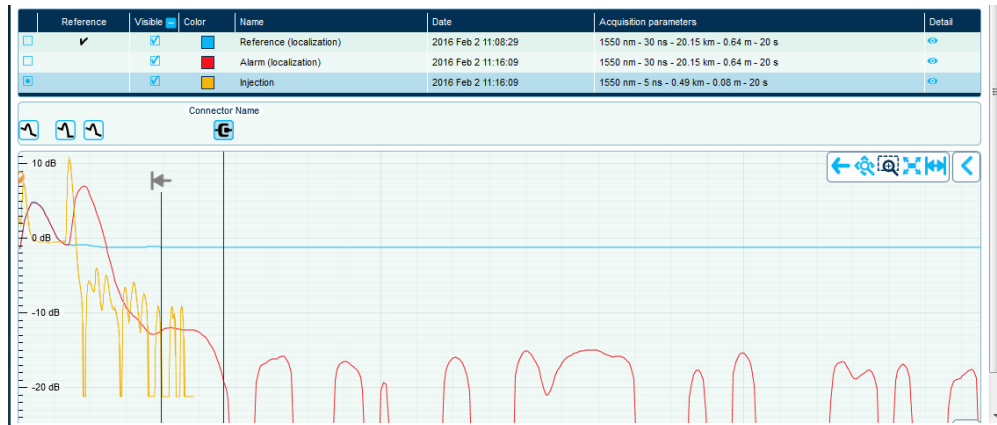
Figure 89 Alarm details and trace



## Injection alarm

If an alarm of injection triggers, an additional trace, with the shortest pulse width, is automatically added to the OTDR trace in alarm in order to localize precisely the injection default,

Figure 90 Injection Alarm: Trace with shortest pulse width



## Deleting an alarm (detail view)

The cleared alarms can be deleted from the application.



- The privilege «Purge the System» is required.
- Only the alarms that are cleared can be deleted.
- This action cannot be undo.

- 1 Select a cleared alarm in the alarms table
- 2 Click on **Detail** to display the alarm details (not mandatory)
- 3 Click on **More > Delete** buttons.
- 4 Confirm the alarm deletion from the application clicking on **Ok** in the new dialog box.

## Actions on table display

### Filtering the alarms in the table

From the Alarm viewer, you can define filters for the alarm table

- 1 Click on **Not Filtered** button above the table
- 2 Select/deselect alarms parameters
  - In the **Alarm type** window, select/deselect the alarms to be displayed or hided.
  - In the **Clear status** window, select/deselect the alarm status to be displayed/ hided.
  - In the **Acknowledgement** window, select/deselect the alarm which have been acknowledged or not.

- 3 In the **Severity** window, select the alarms severity to be displayed,  
or  
Select the severity and check the parameter **and above** to display the alarms from this severity and above.
- 4 In the **By date** parameter, define the starting and end dates of the alarms to be displayed.
- 5 Click on **Ok** to apply the Filters (or on **Cancel** to not apply filters).

**Figure 91** Alarms filters

Click to show all alarms

## Configuring the alarms table

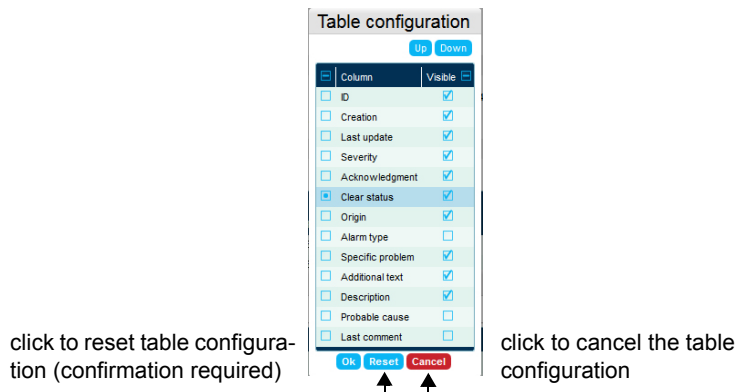
In the alarm viewer, configure the table:

- display/hide some columns
- change the columns position.

From the Alarm viewer:

- 1 Click on **More** button
- 2 Select **Table configuration**.  
In the dialog box:
  - 3 Select a column using the left check box
  - 4 Click on Up/Down button to move the column upward/downward
  - 5 Deselect the check box on the right to delete the column from the table.

**Figure 92** Alarms table configuration



- 6 Click on **Ok** to validate the table configuration.  
Click on **Reset** to return to table configuration by default;  
Click on **Cancel** to not apply the modification.

## Downloading the alarms table

The alarm table displayed in the Alarm Viewer can be downloaded to a PDF or Excel file onto the PC:

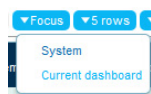
From the Alarm viewer:

- 1 Click on **More** button
- 2 Select **Download as PDF** or **Download as Excel**
- 3 Click on **Save file** to store the PDF / Excel file, or click on **Open with** to directly open the file.

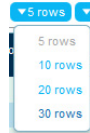
**Figure 93** Alarms Table in PDF

ID	Creation	Last update	Severity	Ack.	Clear	Origin	Specific problem	Addition al text	Descripti on
2117	Sep 9, 2015 3:00:14 PM	Sep 9, 2015 3:00:14 PM	Major			OTU1	Heartbeat		
2071	Aug 18, 2015 4:49:14 PM	Aug 18, 2015 4:49:14 PM	Major			otu-8000e-6192	Missing autotest		
2070	Aug 18, 2015 4:49:13 PM	Aug 18, 2015 4:49:13 PM	Major			otu-8000e-6192	Missing autotest		
2069	Aug 17, 2015 1:21:26 PM	Aug 17, 2015 1:21:26 PM	Critical			Port1	Attenuation	FIBER CUT	Fiber cut
2062	Aug 12, 2015 3:45:56 PM	Aug 12, 2015 3:45:56 PM	Major			otu-8000e-6192	Heartbeat		

## Other actions on table



**Focus:** allows to configure the display of the second tab: either the alarms of the **Current dashboard** or the **System** alarms.

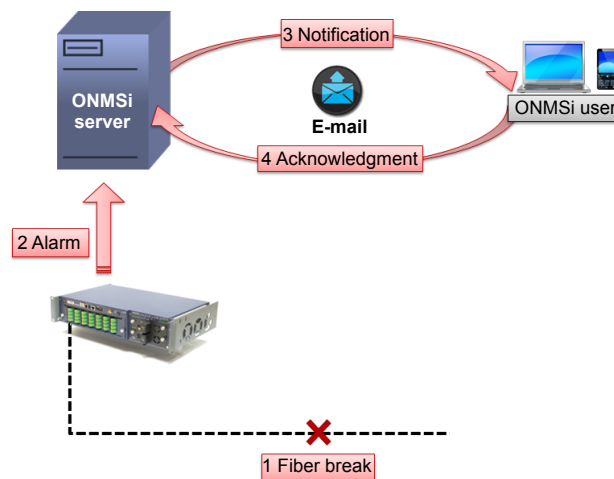


**Rows:** allows to configure the number of lines for the alarms table: from 5 to 30 rows.

## Notification by e-mail of an alarm

If a fault occurs on fiber, an alarm is automatically sent to the ONMSi server, which will notify the user via the ONMSi application.

**Figure 94** Alert process



To define the e-mail and alarm parameters, go to the **System settings** page.

See [“Configuring e-mail/sms alert profiles” on page 108](#)

## Alarm Desktop alert

Desktop Alert is a Google Chrome™ browser extension. As such, it needs Chrome to be installed on the client desktop. Then, the extension program must be installed.

ONMSi Desktop Alert is a program running in the background on the user's desktop computer or laptop. It receives ONMSi alarms and shows alerts accordingly. Those alerts are balloons that pop up on the desktop while optionally playing a sound.

Installing both Google Chrome™ and Desktop Alert extension is preferably done directly from the Internet.

If however, you do not have Internet access, Chrome and the Desktop Alert extension must be downloaded from the ONMSi server (see Online Help for more details).

## Installing the extension in Google Chrome™



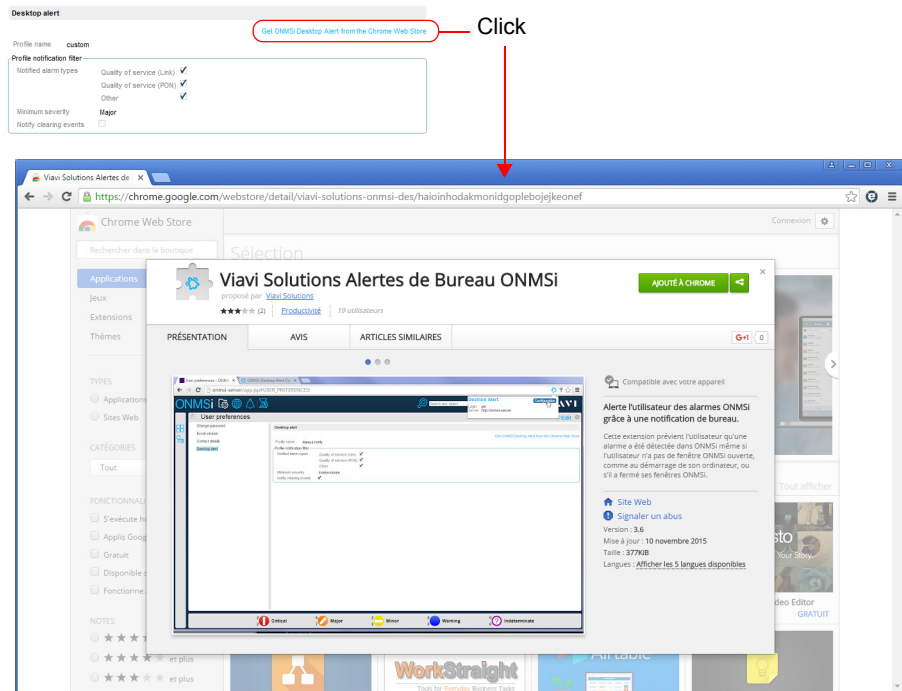
### CAUTION

Install Google Chrome and **open the ONMSi application from Google Chrome.**

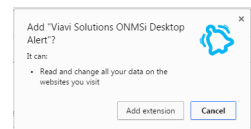
- 1 On the ONMSi, click on **User preferences** in the «User» sub-menu
- 2 In the **User preferences** screen, double click on **Desktop Alert** and click on the link **Get ONMSi Desktop Alert from the Chrome Web Store.**


The Google Chrome page opens and propose to install the Desktop alert extension.

Figure 95 Desktop alert

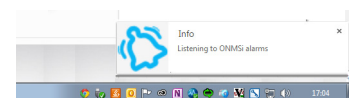


- 3 Click on **Add to Chrome** button  
A new message displays at the top of the window, asking for a confirmation of the extension installation




- 4 Click on **Add the extension** to validate the installation.  
Once installation is completed, the icon  displays on the right of the address bar, with a message informing the user that the extension has been added in Google Chrome™.

In the taskbar, a popup message informs the PC is «Listening to the ONMSi alarms».

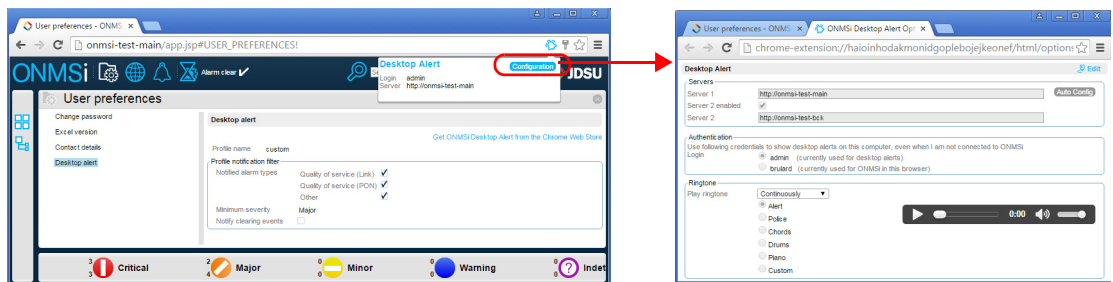


## Configuring the desktop alerts

Once the extension is installed in Google Chrome™, the alerts notification on PC can be modified.

- 1 Return to the ONMSi application (and login if necessary)
- 2 In the Google Chrome address bar, click on the icon .
- 3 Click on **Configuration** button in the popup message.

**Figure 96** Desktop alerts configuration



- 4 Press **Auto Configuration** to apply automatic configuration for desktop alerts or

Click on **Edit** to modify the current parameters:

- Modify if necessary the addresses for server 1 and/or server 2 (if enabled).
- Because not all ONMSi users see the same set of alarms (due to domains visibility or to different notification filtering profiles), you should use the appropriate user in the desktop alert configuration. Only a user who is currently authenticated in ONMSi can be chosen.
- In the Ringtone window, select the ringtone to be played when an alert is raised onto the PC. Listen the ringtone selected using the player bar.

- 5 Press **Save** to save the modifications.

## Display of the desktop alerts



### NOTE

Desktop alert works even if the web browser is closed and no ONMSi session is open.

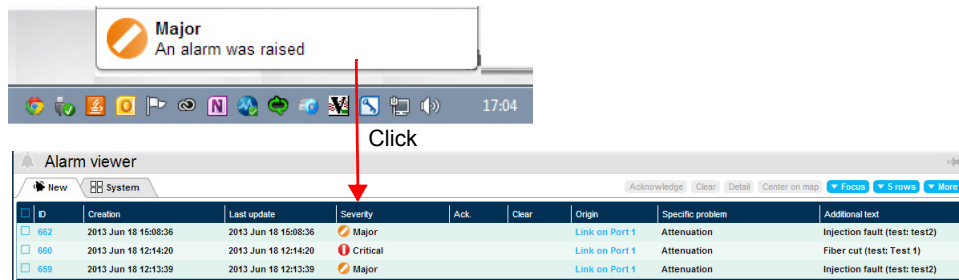
Once the ONMSi Desktop Alert is installed on the client station, any alarm from the ONMSi application is received on the PC.

The desktop alert allows to open a pop-up window and sound (if configured) when an alarm occurs.


The user is also alerted when the server is not reachable.

Once alarm is raised an alert is displayed:

Figure 97 Alert on PC




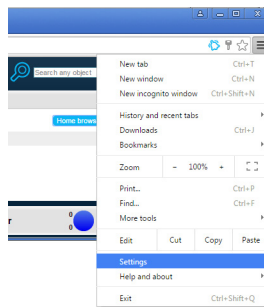
Click on the alert to open the ONMSi alarm viewer

Once alarm is cleared an alert is also displayed  .

## Disabling or removing the Desktop Alert extension

From the ONMSi page open in Google Chrome:

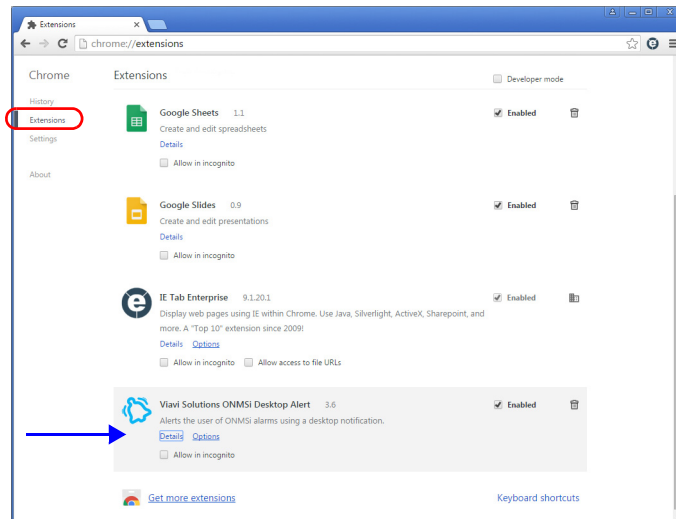
- 1 Click on the «Customize and control Google Chrome» button  in the browser address bar and click on **Settings**.




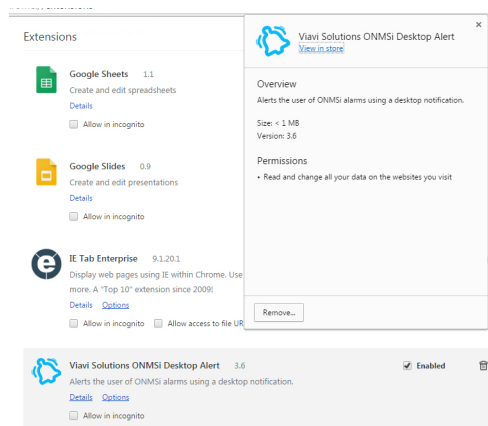
- 2 In the **Settings** page, click on **Extensions** on the left of the screen.  
The ONMSi Desktop Alert extension is available among all the extensions enable.



Figure 98 List of extensions available in Google Chrome™



- Deselect **Enabled** parameter to stop receiving alerts on PC, but keep the extension available
- Click on the icon  to delete the extension from Google Chrome™.
- Click on [Options](#) to display the configuration page in a new tab (see “[Configuring the desktop alerts](#)” on page 87).
- Click on [Details](#) to display information on the extension





# Tables and Reports Management

This chapter provides a description of the reporting process and the configuration to perform automatic reports.

Topics discussed in this chapter include the following:

- [“Downloading data from a table / list” on page 92](#)
- [“Inventory Report” on page 93](#)
- [“Generating reports” on page 94](#)

## Downloading data from a table / list

The contents of most of ONMSi tables can be downloaded to post processing with Excel, or to a PDF file.

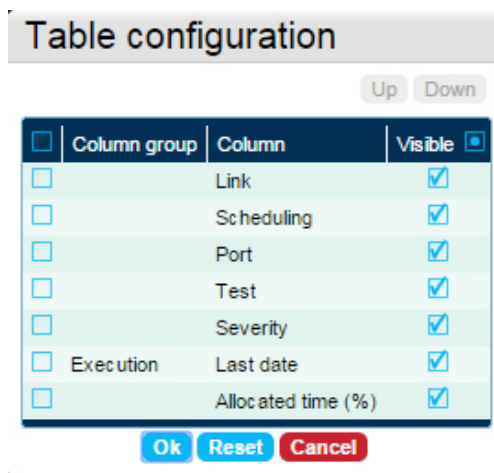
### Configuring the table

Some tables on the ONMSi can be configured: some columns can be added/removed to display more or less details.

This configuration is kept in memory for downloading of tables in Excel or PDF.

- 1 Once a table is open, click on More button
- 2 Select Table configuration.  
A list of available columns displays in a new dialog box (different according to the table configured).

**Figure 99** Table configuration (example with the alarms table)



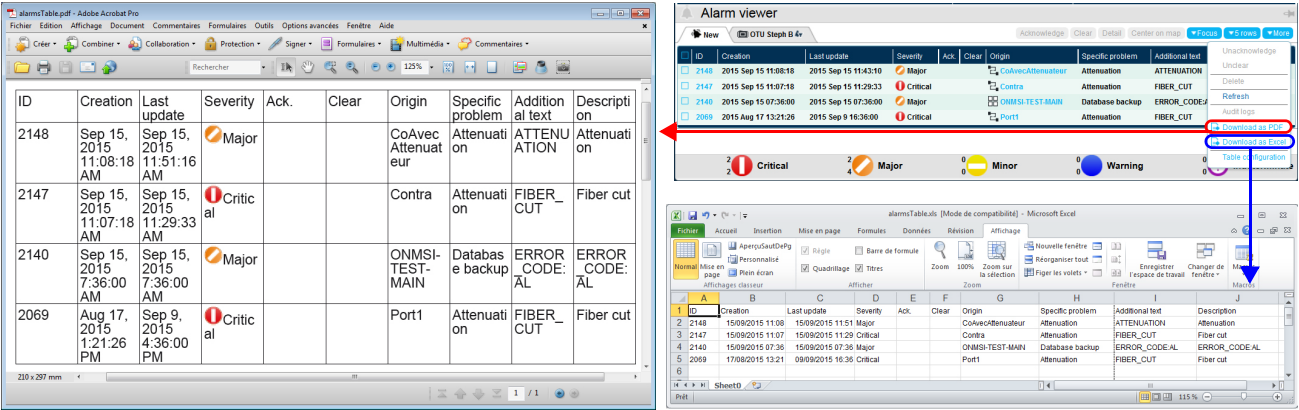
- 3 Select a column using the left check box
- 4 Click on **Up/Down** button to move the column upward/downward
- 5 Deselect the check box on the right to delete the column from the table.
- 6 Click on **Ok** to validate the table configuration.  
Click on **Reset** to return to table configuration by default;  
Click on **Cancel** to not apply the modification.

### Downloading the data from a table

- 1 Open the table which must be downloaded on the PC (for example, alarms table).
- 2 Click on **More** button.
- 3 Select **Download as Excel** or **Download as PDF**.

- 4 Select if the file must be opened or saved onto the PC.
- 5 Click **Ok**
- 6 Open the file on the PC.

Figure 100 Table from ONMSi in Excel and in PDF

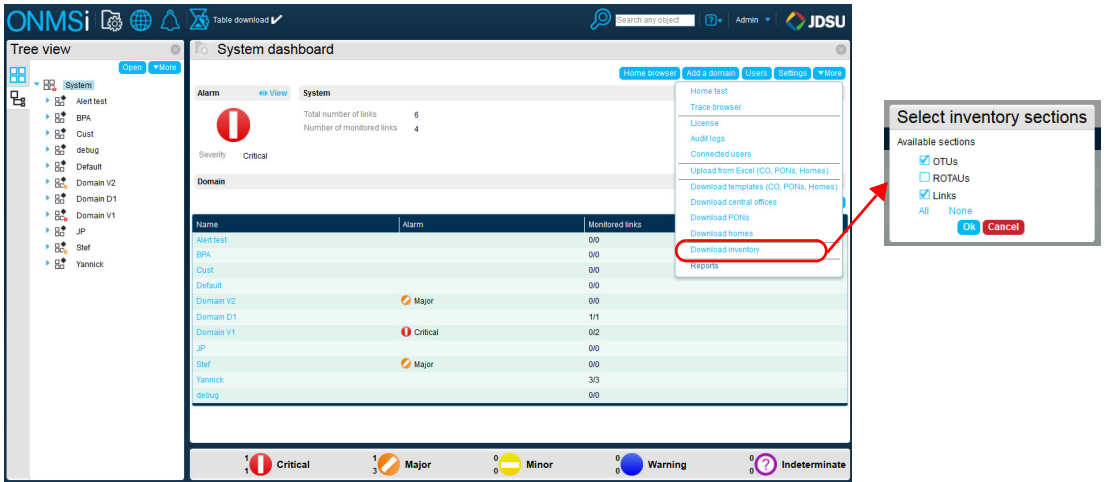


## Inventory Report

An inventory report of the OTU's) and monitored link(s) of the System can be downloaded from the System dashboard.

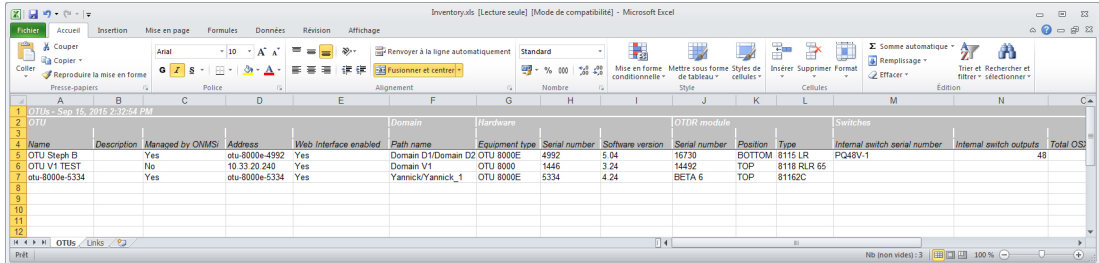
- 1 Open the System dashboard (double-click on **System** in the Tree View).
- 2 Click on **More** button.
- 3 Select **Download inventory**.
- 4 in the new dialog box, select the sections to be included into the inventory. Click on **All** to select all sections.
- 5 Click **Ok**

Figure 101 Download inventory



- 6 Select if the file must be opened or saved onto the PC.
- 7 Click **Ok**
- 8 Open the file on the PC.

Figure 102 Inventory in Excel



## Generating reports

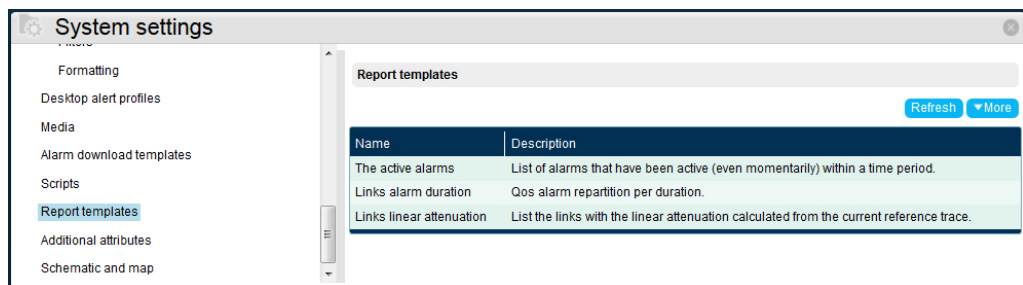
### Displaying reports templates

Three templates for reports generation can be used from the ONMSi:

- Reports on active alarms
- Reports on alarm duration
- Reports on Linear attenuation

To display the list of report templates, from the System dashboard, click on **Settings** and select **Report templates** in System Settings screen.

Figure 103 Report templates



### Creating a report

To create a report (or modify an existing one):

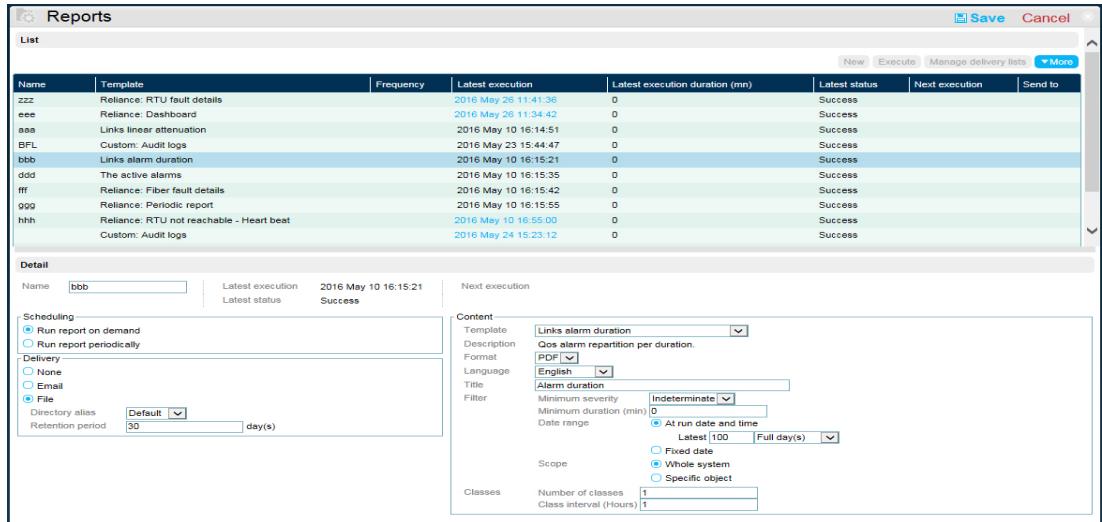
- 1 From the System dashboard, click on **More > Reports**.

2 Click on **New** in the Reports window.

or

Select one existing report which must be modified using the appropriate check box and click on **Edit**.

Figure 104 Reports configuration



3 Configure the report:

- **Name:** enter/modify the report name
- In **Scheduling** window, define a schedule for the report:
  - **Run report on demand**
  - **Run report periodically:** definer the **Frequency** (Daily / Weekly / Monthly) and define the **Run date and time** accordingly.
- Select the **Delivery** mode of the report:
  - **None:** the report is available in the list exclusively (see [Figure 105 on page 97](#))
  - **Email:** select the user to which the report will be **Send to**, by e-mail, and enter the **Subject** of the mail. The report is available in the list, and is sent to the recipient selected.
  - **File:** the report is saved in a directory.

a Select the available directory **Default**, which allows to save the report in C:\rfts\_apps\topaz-report.

or

Create a new alias of directory:

- i Go to: C:\rfts\_apps\jboss\standalone\topaz\_conf
- ii Open topaz.properties using a text editor.
- iii Enter a name for the directory as shown below:

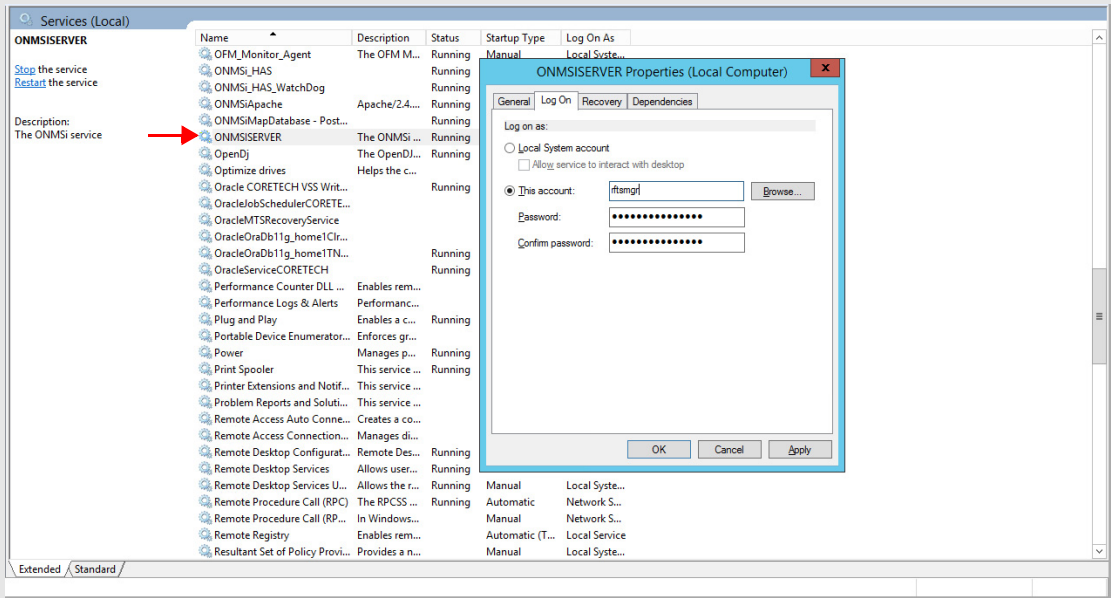
```
[ReportFileDeliveryDirectoryAliases]
Local=c:\temp\Reports - - - - - → the directory alias is Local; report(s) will be saved in C: ...
Network=\\servappl\TmpEchan\Reports - - - - - → the directory alias is Network; report(s) will be saved in servappl...
```



### CAUTION

ONMSi Server being executed as a Windows service (Log on as Local system Account) it can't access network shares.

To access to network share, change the account used for the ONMSi Server service: use `rftsmngr` account.



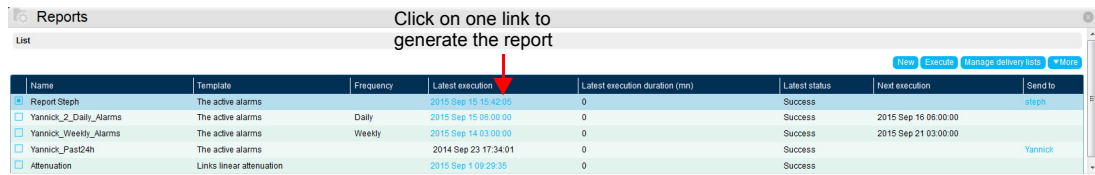
- iv Refresh the display of the ONMSi application to display the list of aliases available in the **File** parameter and select one.
  - b In the **Retention Period** parameter, define the number of days after which the report(s) generated are automatically deleted from the directory.
    - In Content window, define report contents.
      - Select the **Template**
      - Select the **Format** of the report file: XLS / XLSX / PDF / CSV...
      - Configure the other parameters to be included in the report, different according to the templates selected (**Language / Title / Filter / CSV Delimiter...**)
- 4 Click on **Save** to save the new report in the list.

## Launching the report

- 1 From the System dashboard, click on **More > Reports**.
- 2 Select the report which must be generated.
- 3 Click on **Execute** to launch the report
- 4 Once completed, click on the link of the Latest execution date column to open the corresponding report.

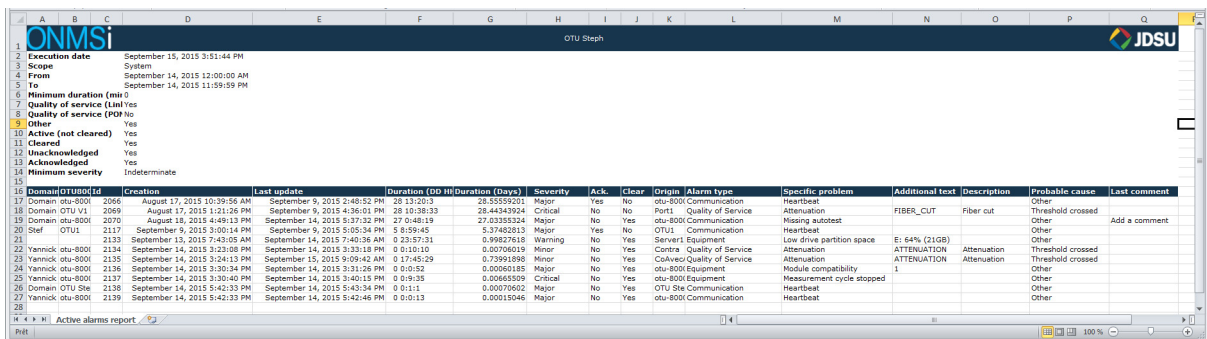


Figure 105 Reports available



- 5 Select if the file must be opened or saved onto the PC.
- 6 Click on **Ok**
- 7 Open the file on the PC.

Figure 106 Example of report open in Excel™





# System settings

This chapter provides a description of all possible actions to manage your ONMSi system.

Topics discussed in this chapter include the following:

- [“Configuring and launching a manual purge” on page 100](#)
- [“Configuring an automatic purge” on page 100](#)
- [“Users” on page 101](#)
- [“Configuring e-mail/sms alert profiles” on page 108](#)
- [“Configuring Desktop alert profiles” on page 111](#)
- [“Additional Attributes” on page 112](#)
- [“Downloading a schematic” on page 114](#)
- [“Scripts” on page 115](#)

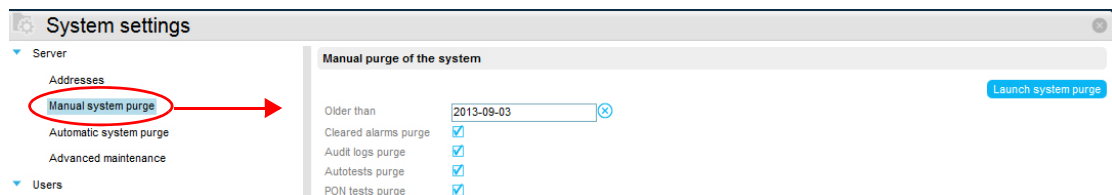
## Configuring and launching a manual purge

It is strongly recommended to launch a purge of the system, when the user is notified of a critical alarm «Database size has exceeded max threshold».

Once System Settings page is opened:

- 1 Click on **Server > Manual system purge**
- 2 If necessary, modify the starting date of the purge or click on the blue cross to deleted the date currently displayed.
- 3 Select or deselect the elements of the system to be purged:  
Alarms / Audit logs / Autotests / PON.
- 4 Click on **Launch system purge** to start the process.

Figure 107 Manual system purge



You will be asked to log in: enter login and password in the dialog box.



### CAUTION

The user must have the system purge permission to launch the process.

## Configuring an automatic purge

Once **System settings** page is opened:

- 1 Click on **Server > Automatic system purge**
- 2 Click on **Edit** to modify the purge date for:  
Alarms / Audit logs / Autotests / PON / Budgets.
- 3 Click on **Save** to define the date of the automatic purge for each element.

Figure 108 Automatic system purge





**NOTE**

The automatic purge is done at midnight.

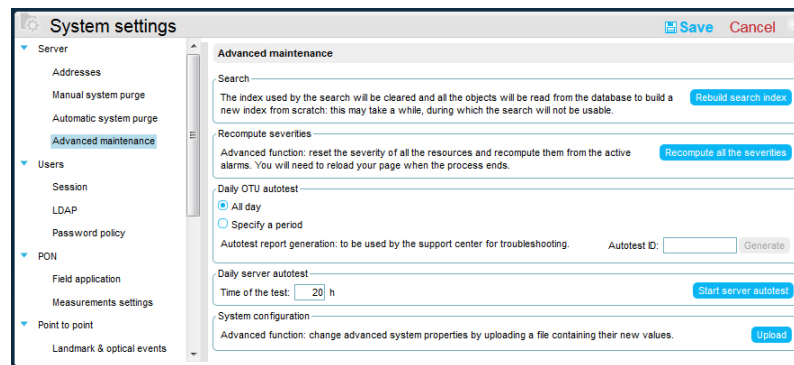
## Configuring server advanced parameters

From the System Settings screen, the parameters for advanced maintenance processes for servers can be configured.

Once **System settings** page is opened:

- 1 Click on **Server > Advanced maintenance**.

**Figure 109** Advanced maintenance parameters for the Server



- 2 Click on **Edit** and configure the parameters / click on the buttons wished to perform the maintenance operation required.
- 3 Once configured completed, press **Save** to keep the modified configuration.

## Users

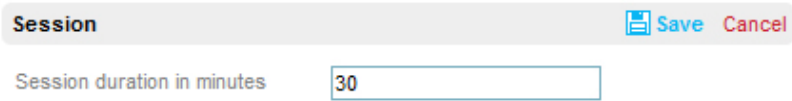
The **Users** page allows to define parameters for Session, LDAP and password policy.

### Defining the session duration

Once **System settings** page is opened:

- 1 Click on **Users > Session**
- 2 Click on **Edit** to modify the time.
- 3 Click on **Save** to save the time of inactivity, in minutes, after which the user is disconnected.

Figure 110 Session duration



## Configuring the LDAP



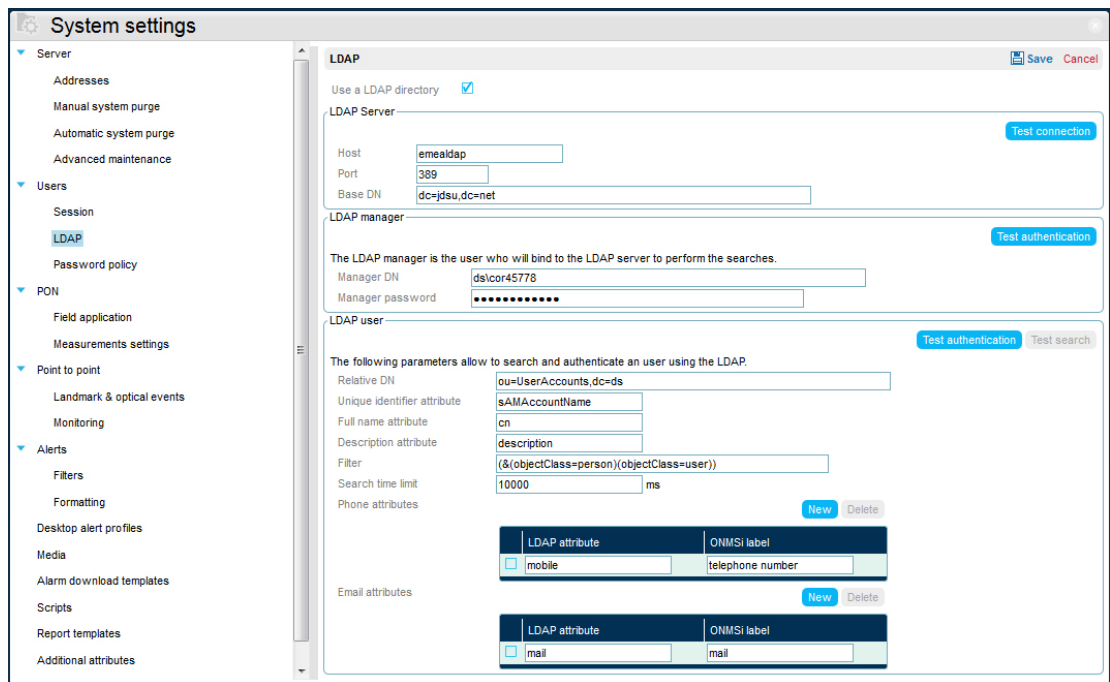
### CAUTION

LDAP configuration details must be given by a person familiar with the directory

Once **System settings** page is opened:

- 1 Click on **Users > LDAP**.
- 2 Click on **Edit** to modify the LDAP parameters.

Figure 111 LDAP parameters



- Select the parameter **Use a LDAP directory** to use LDAP to add users (the LDAP option is not activated by default).

### LDAP Server configuration

- 1 Enter/modify the parameter of the server used for LDAP:
  - Host: Server address (IP address or host name)
  - Port: Port Number of the LDAP server connection
  - Base DN: Base of the domain name
- 2 Press **Test connection** to confirm the connection of ONMSi with LDAP server has succeeded.

### LDAP Manager configuration

- LDAP Manager is an account able to read the directory.
- 1 Enter/modify the parameter of the LDAP manager:
    - Manager DN: Manager domain name
    - Manager password: Password to access to the domain
  - 2 Press **Test Authentication** before going to LDAP User

### LDAP User configuration

Contact your IT to complete the LDAP user fields.

## Configuring the password policy

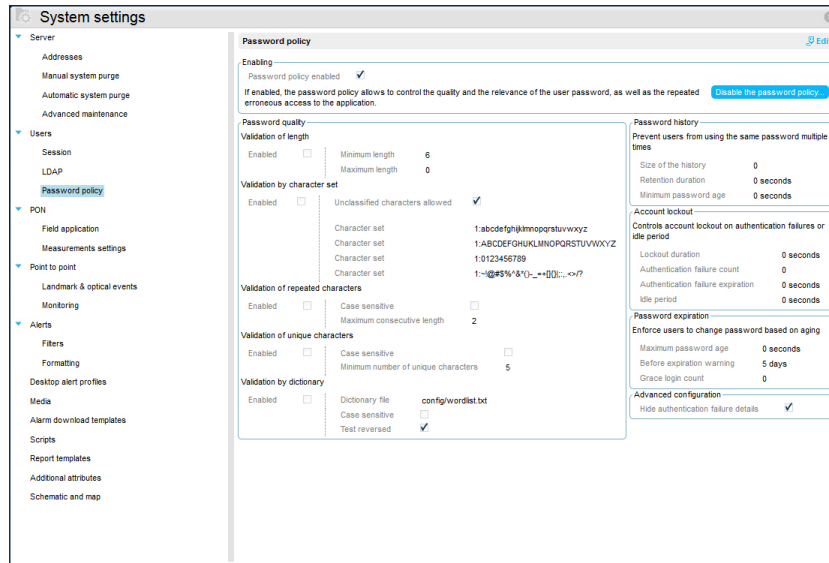
The password policy available in ONMSi allows to add restrictions and control the quality and relevance of user passwords for the System, as well as the repeated erroneous access to the application.

- Users having the «Manage Security» privileges are not concerned by the Password Policy.
- API users should have the privilege of his policy in order to avoid problems when the password expires.

Once **System settings** page is opened:

- 1 Click on **Users > password Policy**.
- 2 The password policy is not enabled by default.
- 3 Click on **Enable the password policy** to active it.

Figure 112 Password Policy



4 Click on **Edit** to modify the defined parameters.

### Remarks on durations syntax on the right of the screen:

In the configuration of the right panel, some durations have to be specified

- Syntax is: positive integer + unit
- Units are: w (weeks), d (days), h (hours), m (minutes), s (seconds), m (milliseconds)
- Example: one week, one day and twelve hours is: 1w1d12h

### Password quality

This window allows to configure the validations. Each type of validation can be enabled and is independent from the others.

#### Validation of length

- Choose the minimum and the maximum length of the passwords.
- If value is 0 there is no limitation.

#### Validation by character set

- A character set indicates a list of characters and the minimum required characters from this set to be in a password
- If the number is 0, the character set is optional
- A character can not be in more than one character set



- **Unclassified characters allowed:** to allow or not password to contain characters which are not in the defined sets.(if not enable, password with characters outside of the sets will be rejected).
  - Example: “Pass1@” → ok  
“pass1@” → Nok

### Validation of repeated characters

- To allow or not repeated characters in a password (defined number of consecutive characters)
- Value of 0 means no limitation
- **Case sensitive:** if enable, only the same capitalization is checked
  - Example: “pass” → ok  
“passS” → Nok

### Validation of unique characters

- To define how many unique characters should be in the password
- Value of 0 means no limitation
- **Case sensitive:** if enable, only the same capitalization is checked
  - Example: “pasSword” → ok  
“pasS” → Nok

### Validation by dictionary

- The dictionary file contains a list of words forbidden to be used as passwords
- You can put a complete path: C:/workshop/policy/wordlist.txt  
or the default embedded LDAP path: (/rfts\_apps/opensj/)config/wordlist.txt
- The text file can be with one word per line
- **Case sensitive:** if enable, password is rejected if it is in the same capitalization than in the text file
- **Text reversed:** it checks the password in the both ways. If “System0” is entered, “0metsyS” will be tested

## Password history

This window allows to prevent users from using the same password multiple times.

- **Size of the history:** maximum number of passwords save in the history. When a password is changing, it is compared to the current password and to the history. If value is zero, there is no password history
- **Retention duration:** maximum time for a password to be saved in the history. If value is zero, there is no time limitation
- **Minimum password age:** minimum time for changing a password again.

## Account lockout

This window allows to controls account lockout on authentication failures or idle period.

- **Lockout duration:** an account is locked for this duration after too many authentication failure.If value is zero, the account stay locked until an administrator resets the password
- **Authentication failure count:** number of authentication failure allowed, after that the account is locked
- **Authentication failure expiration:** after this duration, the failure count is restarted to 0
- **Idle period:** after this duration, an account without any activity is locked

## Password expiration

This window allows to enforce users to change password, based on aging.

- **Maximum password age:** maximum duration a password wan be used before it has to be changed.If value is zero, it never expires
- **Before expiration warning:** server notifies a user to change the password during this time (before the password expires). If value is zero, there is no notification
- **Grace login count:** number of grace login allowed for a user to change his password (after password expiration). If value is zero, no grace login is allowed. Password has to be changed by an administrator.

## Advanced configuration

This window allows to define if the authentication failures must be hidden or reported to users.

For a higher level of security, it's recommended to hide these details (check box selected).

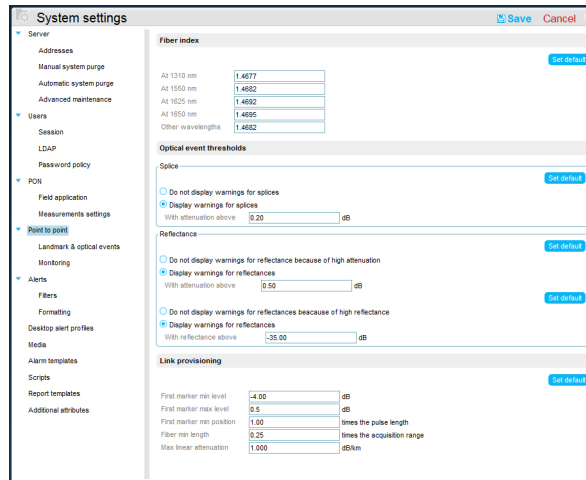
# Point to Point Configuration

The Point to Point menu allows to modify the parameters for monitoring and results.

## Point to Point General configuration

- 1 Click on **Point to Point** in the System settings window
- 2 The current configuration for Fiber Index, Optical event Thresholds and Link provisioning is displayed.
- 3 Click on **Edit** and modify the wished parameters.
- 4 Click on **Save** to save the new configuration.

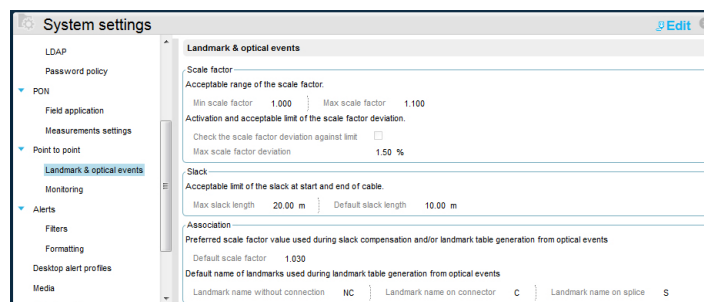
Figure 113 Point to Point: general configuration



## Landmarks & optical events configuration

- 1 Click on **Point to Point** in the System settings window
- 2 Click on **Landmarks & optical events**.  
The current configuration for Scale Factor, Slack and Association parameters is displayed.
- 3 Click on **Edit** and modify the wished parameters.
- 4 Click on **Save** to save the new configuration.

Figure 114 Configuration for Landmarks and optical events

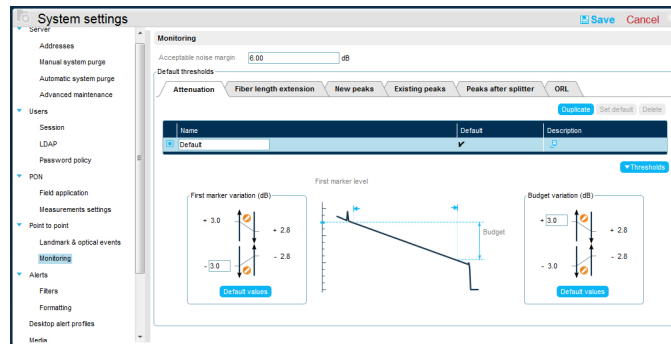


## Monitoring configuration

- 1 Click on **Point to Point** in the System settings window
- 2 Click on **Monitoring**.  
The current configuration for noise margin and Default thresholds is displayed.
- 3 Click on **Edit** and modify the wished thresholds: Attenuation / Fiber length extension / New peaks / Existing peaks / Peaks after splitter / ORL.

- 4 Click on **Save** to save the new configuration.

Figure 115 Configuration for Monitoring



## Configuring e-mail/sms alert profiles

Different profile can be created to receive alarms by e-mail and/or sms.

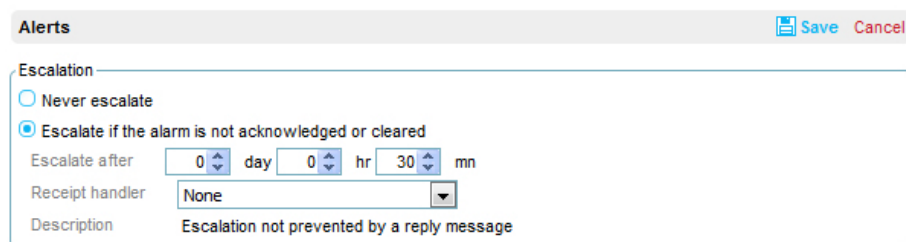
### Defining Escalation

Escalation

Once **System settings** page is opened:

- 1 Click on **Alerts**
- 2 Click on **Edit** to define the Escalation parameters.

Figure 116 Escalation parameters



The escalation can be activated and configured for each user.

- 3 Define the escalation parameter:  
**Never escalate:** whatever is the alarm status  
or

**Escalate if the alarm is not acknowledged or cleared.**

In this case, the escalation users (defined for each user) will be alerted if all of the following conditions are true:

- The specified delay (after the initial alert) has elapsed

- The alarm is not cleared
- The alarm is not acknowledged
- The alert is not already escalated
- None of the alerted contacts have replied to the received e-mail or SMS (requires incoming media defined) with the proper emission code

Note: Comments are never escalated.

- 4 Click on **Save** to save the escalation configuration.

## Defining filters for the e-mail notifications

From the **System settings** screen > **Alerts** sub-menu, some filters can be applied on e-mail alerts.

Once **System settings** page is opened:

- 1 Double-click on **Alerts > Filters**
- 2 Click on **New** to create a new filter for the alert  
or  
Select one existing filter and click on **Edit** to modify the current filter parameters.

Figure 117 Alerts > Filters

The screenshot shows the 'Filters' configuration page. At the top, there are 'New' and 'More' buttons. Below is a table with two filters: 'Always notify' and 'Stress alert filter'. Below the table is a 'Save' and 'Cancel' button. The main form is titled 'Filter for email notifications' and has three radio buttons: 'Never notify', 'Always notify', and 'Advanced filter'. The 'Advanced filter' option is selected. Under 'Advanced filter', there are several settings: 'Filter' (Advanced alarm filter), 'Description' (Accepts an alarm event, depending on the alarm and alarm event), 'Notify acknowledging events' (checkbox), 'Notify comment events' (checkbox), 'Notify injection QOS alarms' (checkbox), 'Minimum Severity' (Indeterminate), and 'Notified Alarm Types' (Quality of Service (PON), Quality of Service (Link), and Other, all checked). There is also a 'Filter for SMS notifications' section with three radio buttons: 'Never notify', 'Always notify', and 'Advanced filter'.

- 3 Select if the user must be  
  - **Never notify**: in case of alarm, no e-mail will be sent
  - **Always notify**: in case of alarm, whatever is the kind of alarm and whatever is the severity, an e-mail is sent.

- **Advanced filter:** allows to configure the conditions for sending a notification by e-mail:
    - **Filter:** select if the filter is an **Advanced alarm filter** or a **Wavelength alarm filter**
    - If **Wavelength alarm filter is selected**, select first the wavelength of the test for which notifications will be sent.
    - Select or not the notification parameter: Notify acknowledged events / Notify comment events / Notify injection QOS alarms
    - Select the **Severity** from which a notification will be sent
    - Select or not the **Notified Alarm Type:** Quality of Service (PON) / Quality of Service (Link) / Other.
- 4 Click on **Save** to save the new profile / the modifications of the existing profile.

## Configuring the e-mail format

From the System Settings page ,you can define the e-mail format (template to be used, language, information included in the e-mail...).

Once **System settings** page is opened:

- 1 Double-click on **Alerts > Formatting**.
- 2 Click on **Edit** to modify the current format parameters.

Figure 118 Alerts > e-mail Formatting

The screenshot shows the 'Formatting' dialog box for email alerts. The 'Email' section contains the following fields and options:

- Template:** Default Alert Template (dropdown)
- Description:** Attempts to show what is the most sensible data in the alarm event or the alarm
- Date Format:** 1970-12-31 23:59 (dropdown)
- Language:** English (dropdown)
- Subject:** Prefix: ONMSi Alarm (text input)
- Content:**
  - GPS coordinates
  - Localization
  - Monitoring test
  - Include additional attributes
  - Hyperlink
  - Emission code
  - Event date
- Attachments:**
  - Geographical file
  - PDF file
  - Trace files

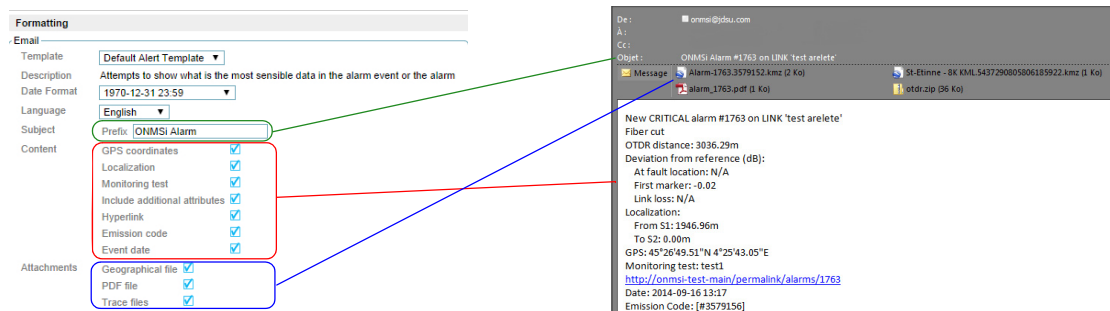
- 3 Select the **Template** to be used:
  - **Run Alert Template;** Shows the raw content of the alarm event without much interpretation
  - **Default Alert Template:** Attempts to show what is the most sensible data in the alarm event or the alarm

- 4 Select the **Date Format**
  - 

- 5 Select the **Language** of the e-mail: English / French / German / Vietnamese.
- 6 Enter the **Subject** of the e-mail.
- 7 In the **Content** parameter, select the information to be contained in the e-mail.
- 8 In the **Attachments** parameter, select the type of file(s) to be attached to the e-mail: Geographical file / PDF file / Trace files.
- 9 Click on **Save** to save the e-mail format.

### Example of e-mail: formatting parameters and e-mail view

Figure 119 Example of e-mail according to formatting configured



## Configuring Desktop alert profiles

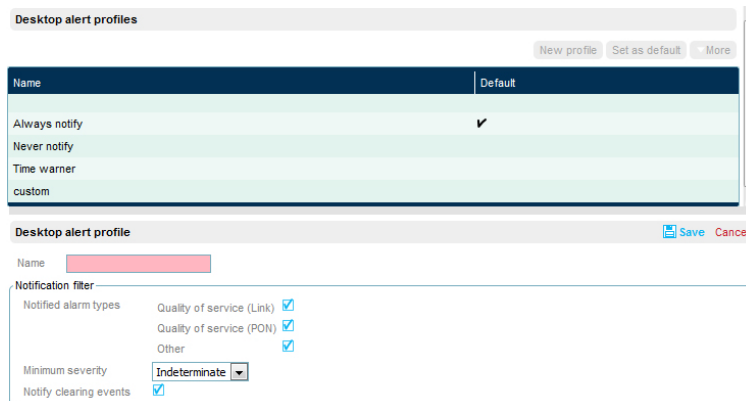
Different profile can be created to receive only specific alarm on PC.

See “Alarm Desktop alert” on page 85 to get information on desktop alerts.

Once **System settings** page is opened:

- 1 Click on **Desktop alert profiles**
- 2 Click on **New profile** to create a new profile for the desktop aler notifications.  
The dialog box to create a new profile displays.

Figure 120 Create a new profile



- 3 Enter a **Name** for the profile
- 4 Select the alarm types for which a notification will be received: **Quality of service (Link)** / **Quality of service (PON)** / **Other**
- 5 Select the **Minimum severity** from which an alert will be received.
- 6 In the parameter **Notify clearing events**, select if an alert must be received when events are cleared.
- 7 Click on **Save** to save the current profile.

### Modify an existing profile

- 1 Select the profile to be modified in the first window.
- 2 In the second window; click on **Edit** to modify some parameters.
- 3 Follow instructions from [step 4](#) to [step 7 on page 112](#) to apply new parameters to profile.

### Profile by default

The profile defined by default can be modified pressing the **Set as default** button, as soon as you are not in edition mode.

This profile is then automatically applied to any new user created.

## Additional Attributes

For the main objects of the application, one (or more) extra user-defined column can be added.  
This allows the user to add his own customized information concerning an object of the System.





**NOTE**

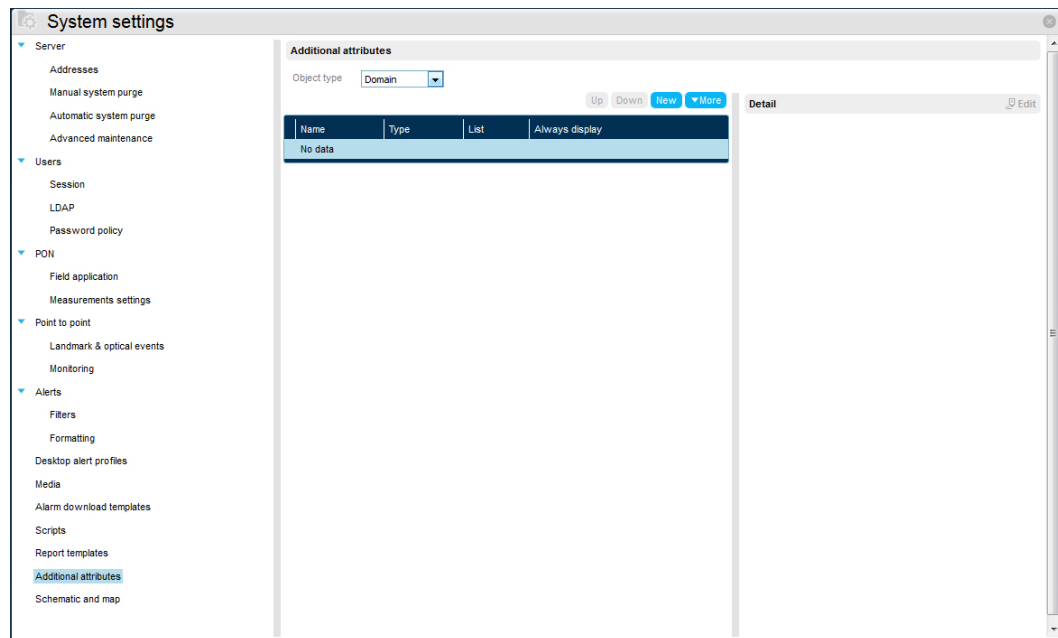
For PON and Central Office, there is one Attribute pre-created called **External Key** used during Data Import.

## Configuring an object with additional attributes

Once **System settings** page is opened:

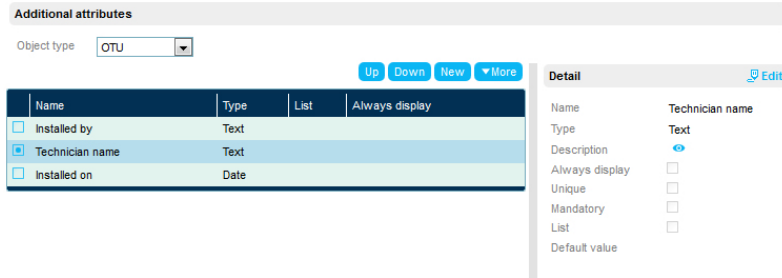
- 1 Click on **Additional Attributes**.  
The following screen displays.

**Figure 121** Additional Attributes configuration screen



- 2 Select the **Object type** for which an attribute must be added in the scrolling list.
- 3 Click on **New**
- 4 In the **Detail** window on the right of the screen, define the different characteristics of the attribute (Name, Type, Mandatory or not...)
- 5 Once correctly configured, click on **Save** button.
- 6 Create as many attributes as required
- 7 In the **Additional Attributes** window, click on Up/Down buttons to move the attributes upwards/downwards, in the order to be displayed on the dashboard.

Figure 122 Additional Attributes created (for OTU)

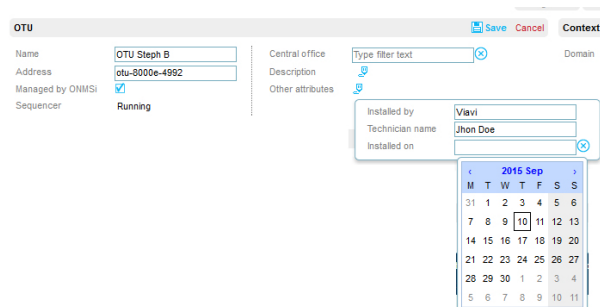


## Displaying and completing the attribute

To check the attributes have been correctly added to the selected object:

- 1 Open the dashboard of the object concerned by the attribute.
- 2 In the upper part, check the attribute has been added
- 3 Click on **Edit** to complete the field of the attribute.

Figure 123 Additional Attribute in the Object dashboard (for OTU)



## Downloading a schematic

In the ONMSi, the picture to be defined as schematic, in order to visualize the network and localize the OTUs in alarm, can be downloaded from the System Settings page.

Once **System settings** page is opened:


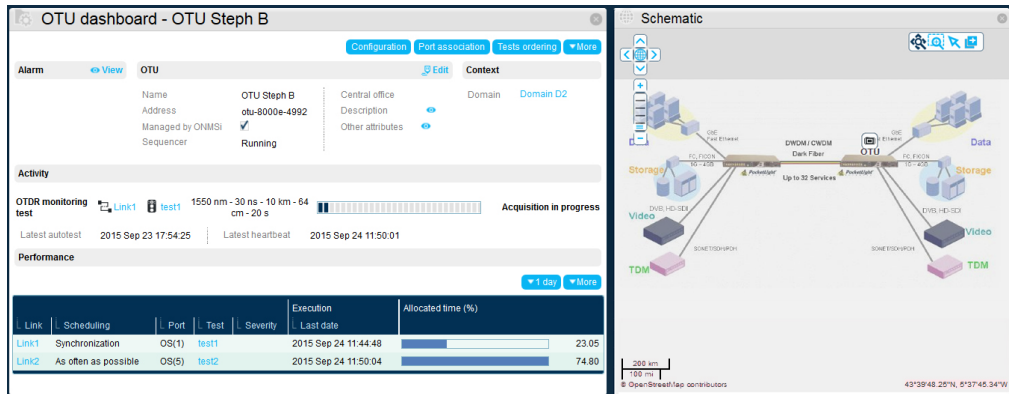
- 1 Click on **Schematic and Map**.
- 2 In the new right window, click on Browse and select on the PC the picture to be used as schematic.
- 3 Click **Ok** to confirm the selection
- 4 Click on the icon  to display the schematic on the right of the screen.

Figure 124 Schematic added



Refer to “Adding an OTU to a schematic” on page 75 to get information on the use of schematic with OTU.

## Scripts

From the System settings window, a table of scripts can be displayed and downloaded into Excel or PDF.

Once **System settings** page is opened:

- 1 Click on **Scripts**.  
The Scripts table displays.

Figure 125 Scripts

The image shows a screenshot of the 'System settings' window. On the left sidebar, the 'Scripts' menu item is circled in red. The main content area displays a table of scripts with columns for Type, Name, Description, Class name, and Module.

Type	Name	Description	Class name	Module
Alarm download template	Default Formatter	Formats an alarm with default content	DefaultAlarmExportTemplate	alarm_export_templates.py
Alert notification filter	Advanced alarm filter	Accepts an alarm event, depending on the alarm and alarm event	DefaultAlarmFilter	notification_rules.py
Alert notification filter	Wavelength alarm filter	Accepts an alarm event, depending on the alarm, the alarm event, and the wavelength of the test	WavelengthAlarmFilter	notification_rules.py
Alert receipt handler	Default handling of alert receipts	Finds a string like [#123456] in the subject then in the body and extracts 123456 as the receipt ID	DefaultReceiptHandler	alert_receipt_handlers.py
Alert template	Raw Alert Template	Shows the raw content of the alarm event without much interpretation	RawAlertTemplate	alert_templates.py
Alert template	Default Alert Template	Attempts to show what is the most sensible data in the alarm event or the alarm	FineAlertTemplate	alert_templates.py
Dynamic Application	Standard PON Field Application	Allows binding a measured peak to a home, possibly by running two measurements	FieldApp	field_app.py

- 2 Click on **Refresh** to refresh the scripts; this can take few minutes.
- 3 Click on **More** and download the scripts on the PC (see “Downloading data from a table / list” on page 92)



# ONMSi System Requirements

This chapter provides a general description of the ONMSi requirements for installation of the equipment.

Topics discussed in this chapter include the following:

- “ONMSi Server ” on page 118
- “ONMSi Web Client” on page 118
- “ONMSi Network ” on page 118
- “High availability (option)” on page 118
- “Optical Fiber Mapping (option)” on page 119
- “Alert notification (option)” on page 119
- “SNMP Interface (option)” on page 119
- “Web service Interface (option)” on page 120
- “Access from a mobile phone via internet” on page 120
- “Light Directory Access protocol (LDAP)” on page 120

## ONMSi Server

- OS: 64-bits Windows Server 2012 R2 or Windows Server 2008 R2 SP1 Standard or Enterprise (US or French version)

	<b>Very Large system PON or more than 50 test units</b>	<b>Medium System Up to 50 test units</b>	<b>Small System Less than 50 monitored fibers</b>
<b>CPU</b>	2.4GHz, 8 Cores	2.4GHz, 6 Cores	2.4GHz, 4 Cores
<b>RAM (GB)</b>	16	16	8
<b>Hard Disk (OS, Application and Database)</b>	Raid 1 2x400GB <b>RAID1</b> (Write intensive SAS SSD)	Raid 1 2 x 300GB <b>RAID1</b> (SAS: 15KRPM)	1 x 300GB (SATA: <b>7K2RPM</b> )
<b>Hard Disk for Backup</b>	1x 1000 GB (SAS <b>7K2RPM</b> )	1x 1000 GB (SAS <b>7K2RPM</b> )	1x 1000 GB (SATA: <b>7k2RPM</b> )

- Backup: Viavi does not support data recovery if the backup hard disk is not used
- The server must be dedicated to ONMSi software
- Virtual machine can be used. Consult us for compatibility and configuration
- IP Ports: 80/HTTP (in/out) or 443 (HTTPS if required), 22/SSH (in/out).

## ONMSi Web Client

- Internet Explorer 9 Minimum, 11 or above Recommended
- Firefox 10 or above
- Google Chrome 16 or above
- JavaScript and cookies enabled
- Memory: At least 1 GB RAM (at least 2 GB RAM for Vista or Win 7)
- IP Port: 80/HTTP (out)), (or 443 (HTTPS if required)),
- Recommended display resolution 1680 x 1050

## ONMSi Network

- OTU network bandwidth: Min: 1Mb/s, Recommended: 2Mb/s

## High availability (option)

- Primary network:
  - Bandwidth: Min: 10Mb/s, Recommended: 100Mb/s

- Backup network for automatic failover:
  - Bandwidth: Min: 2Mb/s, Recommended: 20Mb/s
- IP Ports: 1521 (in/out); 873 (in/out); 624 (in/out) in case IPMI is used
- ICMP (Ping) must be enabled.

## Optical Fiber Mapping (option)

- Client station:
  - OS: Windows XP, 7
  - Memory: 2 GB RAM for XP (4 GB RAM for Win 7)
  - IP Ports: 1521(out), 4446(out), 5000(in/out), 5001(in/out), 1098(out), 1099(out), 80/HTTP
- Maps formats: shape files; open street maps. (Consult Viavi for other formats).

## Alert notification (option)

SMS Alert:

- Modem
  - USB port available on the server
  - GSM Modem (Tested with GenPro 30e)
  - Other wireless protocol need to be qualified.
  - SIM card with a valid subscription

Other wireless protocol need to be qualified

- SMPP 3.3 and 3.4 supported if SMS server is available
- Consult Viavi for SMS by Web services
- E-mail:
  - Alert Notification: SMTP Server (Microsoft Exchange is not supported if it is configured with “Integrated Windows Authentication” or NTLM)
  - Alert acknowledgement (not mandatory): POP Server
  - TCP Ports out: configurable (typically 25 for SMTP and 110 for POP, or 465 for SMTP over SSL and 995 for POP over SSL)

## SNMP Interface (option)

- SNMP V2C or SNMP V3
- Documentation available at: <http://<myserver>/docs>
- IP Ports: 161 (in/out), 162 (in/out)

## Web service Interface (option)

- Webservice SOAP/REST
- Documentation available at: <http://<myserver>/docs>

## Access from a mobile phone via internet

- The server must be accessible from an internet public address.

## Light Directory Access protocol (LDAP)

- LDAP V3
- Port: 389
- Tested with Active Directory and Open LDAP
- SSL Encryption on demand





# Application Programming Interfaces

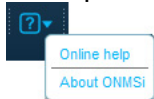
This chapter described the content you will find in the Online Help of the ONMSi concerning the API (Application Programming Interfaces).

Topics discussed in this chapter are as follows:

- [“Content of the Online Help for SNMP API” on page 122](#)
- [“Content of the Online Help for Web Services API” on page 124](#)

# Content of the Online Help for SNMP API

To access the Online Help for SNMP API:

- 1 Click on «?» in the shortcut panel
- 2 Click on **Online Help** . The icon is a blue square with a white question mark. The menu shows 'Online help' and 'About ONMSi'.
- 3 In the **Home** page of the Online Help, in Table of Contents, click on the link [10 Application Programming Interfaces \(APIs\)](#).

The content of the chapter 10 displays

- 4 Click on the link [SNMP API](#).

The SNMP API provides the following chapters:

---

## 1 General SNMP principles

- 1.1 Overview
- 1.2 SNMP network
- 1.3 Management Information Base (MIB)

---

## 2 ONMSi SNMP setup

- 2.1 SNMP user setup
  - 2.1.1 Create an ONMSi user
  - 2.1.2 Setup the SNMP user privileges
  - 2.1.3 Register the user to be API notified
- 2.2 Update SNMP configuration files
  - 2.2.1 jdmk.acl (V2 and V3)
    - 2.2.1.1 acl (V2)
    - 2.2.1.2 trap (V2 and V3)
  - 2.2.2 jdmk.uacl (V3)
  - 2.2.3 jdmk.security (V3)
  - 2.2.4 snmp.properties (V2 and V3)
    - 2.2.4.1 snmpEnabled (mandatory for V2 and V3)
    - 2.2.4.2 password
  - 2.2.5 Multiple manager support
- 2.3 Open SNMP ports in the firewall

---

## 3 ONMSi MIB

- 3.1 Files
- 3.2 Main nodes
- 3.3 The service concept

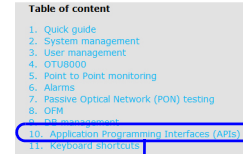


Table of content

1. Quick guide
2. System management
3. User management
4. OTU8000
5. Point to Point monitoring
6. Alarms
7. Passive Optical Network (PON) testing
8. OFM
9. Web management
10. Application Programming Interfaces (APIs)
11. Keyboard shortcuts

## 10. Application Programming Interfaces (APIs)

Following APIs are available to programmatically control ONMSi:

- [SNMP API](#)
- [Web Services API](#)

3.3.1 Data

3.3.2 Functions

**3.4** *I'm alive* trap

**3.5** Alarm event synchronization

3.5.1 Alarm event sequence number

3.5.2 Alarm event trap loss detection

3.5.3 Re-sending lost alarm event traps

3.5.4 Full alarm event re-synchronization

---

**4** **Cook book**

**4.1** Running a PON test

4.1.1 Finding a PON

4.1.2 Starting a PON test

4.1.3 Receiving the PON test result

**4.2** Running a test on demand on a link

4.2.1 Finding a link

4.2.2 Finding a monitoring test on the link

4.2.3 Starting a monitoring test

**4.3** Alarm event synchronization

4.3.1 Synchronization problem detection

4.3.2 Synchronization fix

---

**5** **SNMP testing**

**5.1** Testing tool setup

5.1.1 SNMP v2

5.1.2 SNMP v3

**5.2** Working with the MIB

5.2.1 Get operation

5.2.2 Set operation

**5.3** Receiving Traps

5.3.1 SNMP v2

5.3.1.1 Trap viewer setup

5.3.1.2 Trap reception

5.3.2 SNMP v3


5.3.2.1 Trap viewer setup

5.3.2.2 Trap reception

5.3.3 Tips

## Content of the Online Help for Web Services API

To access the Online Help for Web Services API:

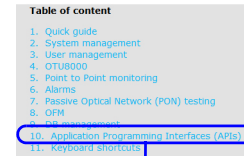
- 1 Click on «?» in the shortcut panel
- 2 Click on **Online Help** 
- 3 In the **Home** page of the Online Help, in Table of Contents, click on the link **10 Application Programming Interfaces (APIs)**.

The content of the chapter 10 displays

- 4 Click on the link **Web Services API**.

The Web Services API provides the following chapters:

- 1 **API Principles**
- 2 **Terms & Definitions**
- 3 **Web Service API**
- 4 **Web Service Data**
- 5 **Network considerations: Proxy, HTTPS and SSH tunneling**
- 6 **Server to client notification**
- 7 **Web Service API version history**
- 8 **Web Service Tester (WSTester)**



1. Quick guide
2. System management
3. User management
4. OTU8000
5. Point to Point monitoring
6. Alarms
7. Passive Optical Network (PON) testing
8. OFM
9. Web management
10. Application Programming Interfaces (APIs)
11. Keyboard shortcuts

### 10. Application Programming Interfaces (APIs)

Following APIs are available to programmatically control ONMSI:

- **SNMP API**
- **Web Services API**

## SOAP Web Service API

The button SOAP  allows to display the following content for SOAP API:

- 1 **SOAP Web Services**
  - 1.1 Data and Services
  - 1.2 Generating Java classes from WSDL
  - 1.3 Authentication
  - 1.4 Getting hold of a service
  - 1.5 Event types, API users and alarm event filtering
    - 1.5.1 Operation events
    - 1.5.2 Sequential alarm events

1.5.3 Getting again lost alarm events

- 1.6 Finding objects
- 1.7 Additional Attributes

---

**2 Running repetitive tasks without pain**

- 2.1 Getting hold of a service - revised
- 2.2 Waiting for a specific event

---

**3 PON cook book**

- 3.1 Running a PON test
- 3.2 Running a Home test
- 3.3 Getting the history of the tests on a PON
- 3.4 Changing the termination type for a home
- 3.5 Assigning a reference peak to a home
- 3.6 Changing the state of a peak
- 3.7 Changing the reference of a peak
- 3.8 Creation of PON and Home elements into ONMSi

---

**4 Point to point cook book**

- 4.1 Enable/disable link monitoring
- 4.2 Start a test on demand on a link
- 4.3 Changing alarm states

## Rest Web Service API

The button REST  allows to display the following content for SOAP API:

---

**1 REST Web Services**

- 1.1 Authentication
- 1.2 Main resources
- 1.3 Simple API call
- 1.4 Event types, API users and alarm event filtering
  - 1.4.1 Operation events
  - 1.4.2 Sequential alarm events
  - 1.4.3 Getting again lost alarm events
- 1.5 Finding objects
- 1.6 Additional Attributes

---

## **2 Running repetitive tasks without pain**

- 2.1 Simple API call - revised
- 2.2 XML management
- 2.3 Waiting for a specific event

---

## **3 Reference guide**

- 3.1 OTUs
- 3.2 Links
- 3.3 Monitoring Tests
- 3.4 Central Offices
- 3.5 PONs
- 3.6 Homes
- 3.7 Alarms
- 3.8 Events

---

## **4 PON cook book**

- 4.1 Running a PON test
- 4.2 Running a Home test
- 4.3 Getting the history of the tests on a PON
- 4.4 Changing the termination type for a home
- 4.5 Assigning a reference peak to a home
- 4.6 Changing the state of a peak
- 4.7 Changing the reference of a peak
- 4.8 Creation of PON and Home elements into ONMSi

---

## **5 Point to point cook book**

- 5.1 Enable/disable link monitoring
- 5.2 Start a test on demand on a link
- 5.3 Changing alarm states
- 5.4 Alarm event synchronization

# Software License Terms

These Software License Terms apply to any quote, order, order acknowledgment, and invoice, and any license or delivery of Software by Viavi Solutions Inc. or any of its subsidiaries or affiliates ("Viavi"), in addition to Viavi's General Terms, which are incorporated by reference herein and are either attached hereto, or available at [www.viavisolutions.com/terms](http://www.viavisolutions.com/terms) or on request.

**1. SCOPE AND DEFINITIONS.** The definitions in Viavi's General Terms shall apply in addition to the following definition:

"Authorized Users" means officers, employees and independent contractors of Customer, who are bound by enforceable written obligations to (i) treat the Software and Documentation of Viavi as Confidential Information (as set forth in Viavi's General Terms); and (ii) use such Software, Documentation and Confidential Information only on behalf of Customer and only in accordance with these Software License Terms. These Software License Terms do not apply to Firmware as defined in the General Terms.

"Arieso Software" means any Arieso software product, module or modules identified in a relevant order form, and (where applicable) all future corrections, modifications, updates and new versions provided under this Agreement from time to time for use in conjunction with such software. Except where expressly stated otherwise, Arieso Software forms part of the Software under these Software License Terms.

"End User" means a customer of Customer to whom Customer is permitted to distribute a copy of the Software.

"EULA" means the "Viavi Software and Data End User License Agreement" that is presented to End Users as part of the local installation of the Software or as part of the web-based/remote access to the Software

**2. NO SALE.** Software and Documentation (and any copies thereof), are licensed only, not sold. Viavi reserves all rights, except as expressly granted in these Software License Terms

## **3. LICENSE.**

**3.1 License Grant.** Subject to the terms and conditions of this Agreement, Viavi grants Customer a non-sublicensable, non-exclusive, non-transferable, limited license to permit Authorized Users and End Users to use copies of the Software in accordance with the applicable Documentation, within the scope of the applicable License Model(s) ("License Models") described in Section 3.2 (License Models) and solely for Customer's internal business purposes. Viavi's license grant is conditioned upon Customer's continuous compliance with these Software License Terms and, if Customer violates any of these limitations or restrictions or any other terms of this Agreement, the license grant will automatically and immediately expire without notice from Viavi. Customer acknowledges that the license descriptions in this Section 3.1 and in Section 3.2 (License Models) define the scope of rights that Viavi grants to Customer and that any usage of the Software outside the scope of that license grant and the scope of any statutory rights constitutes an infringement of Viavi's and/or its licensors' Intellectual Property and/or Proprietary Rights as well as a material breach of these Software License Terms.

**3.2 License Models.** Any license grant under these Software License Terms is subject to the limitations defined in this Section 3.2 as applicable to Customer's License Model(s). Unless Viavi expressly specifies or

agrees otherwise in a duly signed writing, all Software shall be governed by a Standard License (see Section 3.2.1 (Standard License)).

**3.2.1. Standard License.** Unless Viavi expressly specifies in writing that one or more additional or different License Models apply per Subsections 3.2.2 (Licensed Hardware) through 3.2.4 (Time Limit) below, Customer may install the Software on computers solely in accordance with one of the following options:

(i) **Single User License.** Unless Viavi specifically describes in writing a license for the Software as a “multi-user license”, Customer may install and permit Authorized Users and/or End Users to install and use one (1) copy of the Software on either (i) one (1) stand-alone computer or (ii) one (1) Product, neither of which may be connected to a network in a manner that allows more than one (1) Authorized User to access, manipulate or otherwise create or use a copy of the Software. Customer may not use the Software other than on one (1) computer or Product.

(ii) **Multi-User License.** If Viavi identifies a license for the Software in a duly signed writing as a “multi-user license”, then Customer may install and permit Authorized Users and/or End Users to install and use copies of the Software on stand-alone computers or Products, provided that the Software is installed for no more than the maximum number of Authorized Users and/or End Users specified by Viavi. Each Authorized User or End User may not use the Software other than on one (1) computer or Product. The maximum number of Authorized Users and End Users for the “multi-user” license shall be two (2), unless Viavi specifies another number in writing.

**3.2.2 Licensed Hardware.** Except in respect of Arieso Software, if Viavi in writing identifies a certain computer or Product (“Licensed Hardware”) on which the Software may be used, then Customer may install and permit Authorized Users and/or End Users to use the applicable Software only on such Licensed Hardware. Customer may migrate the Software to a different computer or Product only if (i) Customer gives thirty (30) days’ prior written notice to Viavi; (ii) Customer does not upload or use the Software on the Licensed Hardware after installing it on the destination computer or Product; and (iii) Customer removes all copies from the Licensed Hardware within two (2) weeks after installing it on the destination computer or Product, which will thereafter become the Licensed Hardware for purposes of these Software License Terms. Installation of the Software on such different

destination computer or Product terminates Customer’s license to use the previous installations of the Software.

**3.2.3 Server-Client Architecture.** If Viavi identifies Software in a duly signed writing as a “server software product” (“Server Software”) then Customer may install and host one (1) copy of the server portion of such Software on a single server. Customer may install and permit Authorized Users and/or End Users to install and use copies of the client portion of such Software on computers in accordance with one of the following options:

(i) **Floating Licenses.** If Viavi specifically describes a license for Server Software in writing as a “floating license,” Customer may install and permit Authorized Users to install and use the client portion of such Software on a reasonable number of computers solely in connection with the use of the Server Software and on the condition that no more than the maximum number of concurrent Authorized Users and End Users specified by Viavi may use the client or have access to the server portion of the Software at any one time. If Viavi does not specify in writing a different maximum number of concurrent Authorized Users for a floating license, the maximum number of concurrent Authorized Users shall be one (1).

(ii) **Node-Locked Licenses.** Unless Viavi specifically describes in writing a license for Server Software as a “floating license,” Customer may install and permit Authorized Users and/or End Users to install and use the client portion of such Software solely in connection with the use of the Server Software and only on one (1) computer for each authorized node (“Authorized Customer Computer”). All activities related to the operation of the client portion of the Software must be performed on the same Authorized Customer Computer. The maximum number of Authorized Customer and End User Computers shall be one (1), unless Viavi specifies another number in writing.

(iii) **Arieso Licenses.** If Viavi specifically describes in writing a license for Server Software as an Arieso Software license, Customer may use the Server Software on the condition that: (1) no more than the total number of Authorized Users and/or End Users specified by Viavi may access the Server Software, and (2) no more than the maximum number of concurrent Authorized Users and/or End Users specified by Viavi may access to the Server Software at any one time. If Viavi does not specify in writing different numbers of maximum total and concurrent Authorized Users and End Users for this license, the maximum total and concurrent numbers of Authorized Users and End Users shall be one (1). If expressly specified in writing



by Viavi, the license for such Server Software may also be limited to one Customer cellular/wireless network having the specified number of nodes and/or wireless technology.

**3.2.4 Time Limit.** Subject to Customer's ongoing compliance with the terms and conditions of this Agreement, including, without limitation, the payment of all fees or charges related to this Agreement, the term of the license(s) contained herein shall either a) continue for the Viavi-specified period for any limited duration license, at which point such license shall automatically expire at the end of such period, or b) if no period is specified by Viavi, continue until terminated in accordance with Section 6.1 below. Notwithstanding the foregoing, Viavi has the right to revoke Customer's license(s) at any time due to Customer's non-payment.

**3.3 Copies.** Except as expressly specified herein or agreed otherwise in writing, Customer may duplicate each item of Software that Viavi delivers only by (i) permanently installing one (1) copy on a computer (provided that Customer keeps the original copy that Viavi delivered only as a back-up copy, separately from any actively used Software; keeps records of such original copies indicating the location of its storage; and provides such records to Viavi upon request), and (ii) temporarily uploading such copy of the Software into the working memory of the computer on which it has been installed to the extent necessary for using the Software in accordance with the applicable Documentation and License Models. Customer may not create any other copies of the Software, unless Viavi expressly permits additional copies in writing.

**3.4 License Key Management.** Viavi may, at its sole discretion, use or combine license management programs with any Software, which automatically monitor and enforce license restrictions and limitations, provided that such precautions shall not relieve Customer of its primary responsibility to ensure compliance with these Software License Terms. Customer expressly agrees to be fully responsible for compliance by all Authorized Users with these Software License Terms and all End Users with the EULA, to take all actions reasonably requested by Viavi to protect the rights of Viavi in the Software and Documentation, and to indemnify and hold Viavi harmless against any loss resulting from any breach of these Software License Terms by any Authorized User and from any breach of the EULA by an End User or any other individual or entity that Customer caused, enabled or allowed to use the Software in any manner not authorized under these Software License Terms

**3.5 License Restrictions.** To the extent permitted by applicable law, Customer agrees not to (i) translate or create any derivative works based on the Software or Documentation or modify or alter the Software or Documentation in any manner whatsoever; (ii) sell, sublicense, lease, rent, loan, assign, convey, distribute, or otherwise transfer the Software or Documentation to any third parties; (iii) copy or use the Software or Documentation for any purpose or in any manner not expressly permitted in these Software License Terms; (iv) use the Software outside the permitted scope of the applicable License Model(s); (v) use the Software or Documentation, in any format, for or in the interest of any third party other than by Authorized Users; (vi) disclose the results of any benchmark test of the Software to any third party, without Viavi's prior written approval; or (vii) permit or encourage any third party to do any of the foregoing. Customer acknowledges that the structure, organization and source code of the Software remain confidential trade secrets of Viavi and its licensors. Customer shall cooperate with Viavi, and shall render all reasonable assistance requested by Viavi, to assist Viavi in preventing and identifying any use of, or access to, the Software and Documentation, by Authorized Users, End Users or otherwise, in violation of these Software License Terms. Any computer(s) and/or server(s) contemplated herein shall only contain one (1) single core, single central processing unit (CPU) per such computer or server. Additional fees may be applicable for multi-core/multi-CPU computers and servers. For greater clarity, no source code shall be licensed under these Software License Terms (except as set forth under the terms of any applicable Specific License(s) (defined below))

**3.6 Specific Licenses.** To the extent that Customer acquires from Viavi any Software that is accompanied by or made available subject to end user license terms (other than the EULA) and/or other terms (in shrink-wrap, click-through or other format), either from Viavi or originating from third party licensors ("Specific Licenses") (i) Customer shall agree to such Specific Licenses vis-à-vis the licensor specified in such Specific Licenses; (ii) to the extent such Specific Licenses conflict with Section 3.1 (License Grant) through 3.5 (License Restrictions), the Specific Licenses shall take precedence with respect to the software (or portion thereof) subject to such Specific Licenses; and (iii) Customer's right to use the software (or portion thereof) subject to such Specific Licenses will be defined and restricted as set forth in such Specific Licenses. Original software developed by Viavi is not subject to Specific Licenses, including open source software licenses. Terms of these Software License Terms that are different from applicable Specific Licenses are offered by Viavi alone.

**4. AUDIT.** Upon reasonable notice, Viavi or its agent(s) may inspect Customer's facilities (including computers) and records to verify Customer's compliance with these Software License terms and payment for all Software licensed (including applicable support fees) to Customer. Customer will keep records regarding its use in sufficient detail to permit this verification. Customer shall fully cooperate with such audit, and grant all required assistance and dial-in and/or on-site access to all networks, records, materials and equipment. If, after an audit, it is determined that Customer has underpaid any amounts due, Viavi will invoice Customer for and Customer will pay the amount of the underpayment plus interest from the date payment was due. If the underpayment is more than five (5%) percent of the amount properly due, Customer will also pay Viavi inspection expenses. Viavi's rights and remedies under this Section 4 shall be in addition to and not in lieu of any other rights or remedies that are available to Viavi at law or in equity

## 5. LIMITED WARRANTY AND DISCLAIMERS.

**5.1 Limited Warranty.** Viavi warrants that on the Delivery Date, the Software will substantially conform to Viavi's specifications in the applicable Documentation, subject to the limitations and exclusions in Section 5.1.1 (Excluded Causes) through Section 5.1.3 (No Warranties for Updates).

**5.1.1 Excluded Causes.** Customer has no warranty rights with respect to defects or non-conformities caused by or related to (i) use of the Software with hardware or software that was not expressly specified in writing by Viavi as suited for use with the Software; (ii) Customer's failure to follow Viavi's operating instructions; (iii) failure to implement all updates, upgrades, and other new releases of Software made available to Customer (provided, for the avoidance of doubt, that Viavi is not obligated to make available any such new releases outside the scope of a separate maintenance agreement); (iv) changes to the Customer environment, in which Software was provided; or (v) acts or omissions of persons other than Viavi or its authorized representatives.

**5.1.2 Modifications.** Customer has no warranty rights with regard to any Software (i) that has been modified by someone other than Viavi, unless such modifications were directed or approved by Viavi in writing and made in conformance with all specifications and instructions provided by Viavi in such writing; (ii) that Viavi modified in accordance with Customer's request, specifications, or instructions, unless Viavi agreed in a duly signed writing that the modified Software would be covered by the limited warranty specified in Section 5.1 (Limited Warranty); or (iii) third party products

**5.1.3 No Warranties for Updates.** Viavi does not extend any warranties under these Software License Terms for any updates that Viavi may make available under Viavi's Software Maintenance Terms. Any warranties for any updates are exclusively and finally provided for under Viavi's Software Maintenance Services Terms, if applicable.

**5.2 Exclusive Remedies.** If the Software materially fails to conform to the limited warranty set forth in Section 5.1 (Limited Warranty), Viavi shall, at its sole discretion (i) repair or replace the non-conforming Software to remedy the non-conformity identified by Customer in accordance with Section 5.3 (Warranty Period); or (ii) issue a credit to Customer equal to the amounts paid for the Software in exchange for return of the non-conforming Software, in which case all licenses granted to Customer under these Software License Terms for such Software shall automatically terminate. This Software warranty does not obligate Viavi to provide any on-site repair or on-site replacement of Software. At Viavi's discretion, repair of the Software may be made in later releases of Software and may require the purchase of additional software or hardware at Customer's expense. THE REMEDIES EXPRESSLY PROVIDED IN THIS SECTION 5.2 (EXCLUSIVE REMEDIES) WILL BE CUSTOMER'S SOLE AND EXCLUSIVE REMEDIES AND SHALL BE IN LIEU OF ANY OTHER RIGHTS OR REMEDIES CUSTOMER MAY HAVE AGAINST VIAVI WITH RESPECT TO ANY NONCONFORMANCE OF SOFTWARE.

**5.3 Warranty Period.** Unless Viavi expressly specifies or agrees on a different warranty period in a duly signed writing, the Limited Warranty period set forth in Section 5.1 shall be ninety (90) days and begin on the Delivery Date. Customer shall have no warranty claims under Section 5.1 (Limited Warranty), unless Viavi receives from Customer, during the warranty period and within thirty (30) days of the date on which Customer noticed or should have known about the warranty breach, (i) a written notice describing the warranty breach in reasonable detail ("Warranty Claim"); (ii) remote and physical access to the affected Software as well as information in sufficient detail to enable Viavi to reproduce and analyze the failure.

**5.4 Disclaimer.** EXCEPT AS SPECIFIED IN SECTION 5.1 (LIMITED WARRANTY), VIAVI MAKES NO EXPRESS REPRESENTATIONS OR WARRANTIES WITH REGARD TO ANY SOFTWARE. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, VIAVI DISCLAIMS ALL IMPLIED WARRANTIES, CONDITIONS, AND REPRESENTATIONS, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OR CONDITIONS OF MERCHANTABILITY,

SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT, REGARDLESS OF THE LEGAL THEORY ON WHICH SUCH IMPLIED WARRANTY, CONDITION OR REPRESENTATION MAY BE BASED, INCLUDING, WITHOUT LIMITATION, CONTRACT, COURSE OF DEALING, USAGE, OR TRADE PRACTICE AND, WITHOUT LIMITING THE FOREGOING, MAKES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE, THAT ITS PERFORMANCE OR OPERATION WILL BE UNINTERRUPTED, OR THAT THE SOFTWARE WILL PERFORM ON ANY HARDWARE OR WITH ANY SOFTWARE, EXCEPT AS EXPRESSLY CERTIFIED AS INTEROPERABLE BY VIAVI IN THE APPLICABLE DOCUMENTATION. THE SOFTWARE IS NOT FAULT-TOLERANT AND IS NOT DESIGNED, MANUFACTURED, OR INTENDED FOR USE OR RESALE AS SOFTWARE FOR USE IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL-SAFE PERFORMANCE IN WHICH THE FAILURE OF THE SOFTWARE COULD LEAD DIRECTLY TO DEATH, PERSONAL INJURY, OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE.

**5.5 U.S. Government End Users.** The Software is made available to non-Department of Defense (DOD) agencies of the United States Government with RESTRICTED RIGHTS and its supporting documentation is provided with LIMITED RIGHTS. Use, duplication, or disclosure by the United States Government is subject to the restrictions as set forth in subparagraph "C" of the Commercial Computer Software - Restricted Rights clause at FAR 52.227-19 or any successor clause. In the event the sale is to a DOD agency, the Government's rights in software, supporting documentation, and technical data are governed by the restrictions in the Technical Data Commercial Items clause at DFARS 252.227-7015 and DFARS 227.7202 or any successor clauses. The Software is a trade secret of Viavi for all purposes of the Freedom of Information Act or its successor legislation or any other disclosure statute, regulation or provision and in all respects is and shall remain proprietary to Viavi or its licensors. The U.S. Government must refrain from changing or removing any insignia or lettering from the Software or from producing copies of the Software and manuals (except one copy of the Software for backup purposes). Use of the Software shall be limited to the facility for which it is acquired. All other U.S. Government personnel using the Software are hereby on notice that use of the Software is subject to restrictions that are the same as, or similar to, those specified above

## 6. TERMINATION.

**6.1 Termination for Cause.** Without limiting Section 3.1 (License Grant) with respect to the automatic termination of license rights for specific Software, Viavi may terminate - at Viavi's sole discretion either all or specific - licenses to Software granted hereunder, by giving written notice, effective immediately, if within ten (10) days of Viavi's delivery of a reasonably detailed written request to cure, Customer has not cured all breaches of payment obligations, license limitations and restrictions, including, but not limited to, the License Models, or any other substantial obligations under these Software License Terms or the Agreement. Upon such termination, Customer shall immediately pay all outstanding fees, cease use of all Software and related Documentation, return or delete, at Viavi's request and sole discretion, all copies of the Software and Documentation in Customer's possession, and certify compliance with all foregoing obligations to Viavi in writing. These termination rights are in addition to any other rights and remedies that Viavi may have at law or inequity

**6.2 Survival.** Viavi's General Terms and these Software License Terms, except Sections 3.1 (License Grant), 3.2 (License Models), 3.3 (Copies) and 5.1 (Limited Warranty) shall survive termination of any or all licenses granted hereunder.



# ONMSi Toolkit

This chapter provides a description of the ONMSi toolkit

Topics discussed in this chapter are as follows:

- [“Introduction to ONMSi toolkit” on page 134](#)
- [“Configuring the System” on page 135](#)
- [“Dashboard description” on page 136](#)
- [“Backup and Restore the Database” on page 137](#)
- [“Using the OTU Toolkit” on page 137](#)
- [“High Availability Solution” on page 141](#)

## Introduction to ONMSi toolkit

The ONMSi toolkit is installed on the ONMSi server, after the ONMSi application.

This toolkit allows to:

- Start and Stop ONMSi services.
- Backup/Restore Database.
- Display the Dashboard, to check if everything is working correctly.
- Performs OTUs operations.
- Send Trap notifications or e-mails if it has been configured.

The ONMSi Toolkit can send alarms directly to ONMSi for following issues:

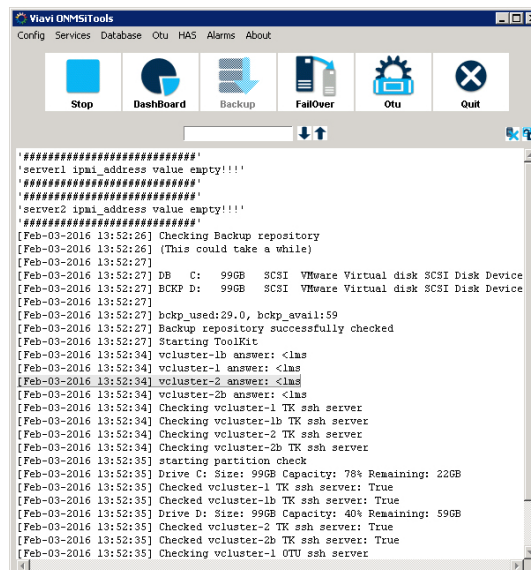
- Backup problem
- Synchronization problem
- Partition size problem

Other issues are sent by email and/or snmp traps.

- 1 To launch the ONMSi toolkit, double-click on the Viavi ONMSi Tool icon



Figure 126 ONMSiTools



- All the functions are accessible via the Menu bar.
  - The main actions are available using buttons under the menu bar.
  - The unauthorized operations are greyed, and depend of the server role.
- 2 To start or stop the ONMSi services, use the **Start/Stop** button.

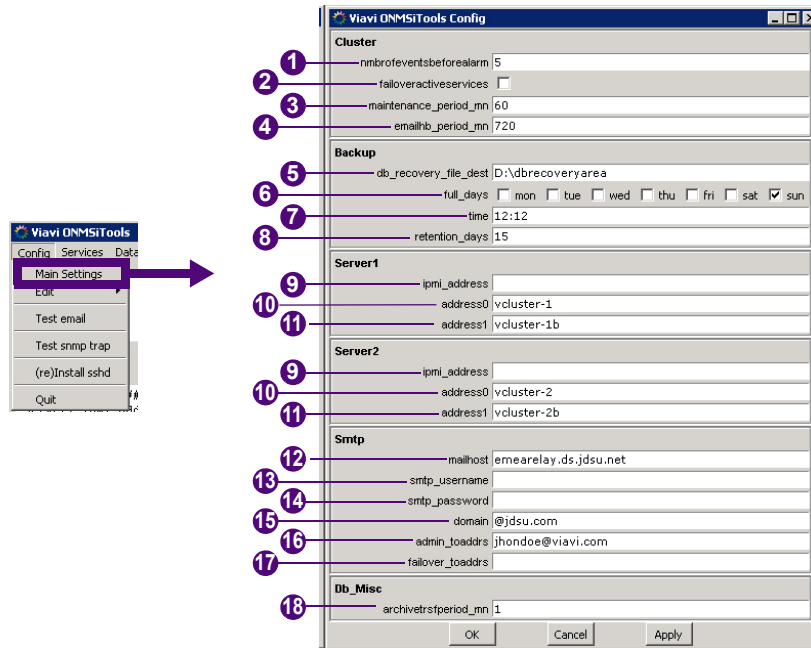
## Configuring the System

At first use, configure the system from the ONMSi toolkit:

- 1 Click on **Config**.
- 2 Select **Main Settings**.

The following screen displays:

Figure 127 Main Settings



- 3 Enter the wished parameters for Cluster / Backup / Server / SmtP.

1	Number of events before sending an alarm (minimum 5)	10	Primary and Standby servers hostname or IP address
2	Select to perform a failover if remote active service is not launched	11	Primary and Standby servers second hostname or IP address, mandatory if autofailover option
3	Period for maintenanceneeded reminders (in mn)	12	Enter SMTP server address
4	Period for ONMSi Toolkit «I'm Alive» notifications (in mn)	13	Server username, if authentication is required
5	Database and customized files backup repository, on another disk than Database	14	Server password, if authentication is required
6	Days for which a full backup is performed (at least one)	15	Domain to append to the sender: machine@domain.com
7	Daily backup time (format 24h)	16	Email address of the administrator(s). Separate the addresses with comma. Test the address using the menu <b>Config</b> . > <b>Test email</b> .
8	Number of days to keep the database backups (min 15)	17	Email address of the system user(s) in case of failover. Separate the addresses with comma.
9	Primary and Secondary server ipmi address in case of autofailover	18	Standby database synchronization period (min 5 mn.)






## Backup and Restore the Database

### Performing a manual Backup

At any time, a manual backup of the database can be performed via the ONMSi Tool:

- 1 Click on **Backup** button  .  
The Backup process starts.  
Once completed, a dialog box informs you the backup has succeeded.
- 2 In the dialog box, click on **Yes** to confirm the start of the backup.  
The Backup process starts.  
Once completed, a dialog box informs you the backup has succeeded.
- 3 Click **Ok** to close the dialog box.  
The database backup and ONMSi configuration files are stored in the directory `dbrecoveryarea/corectech` in the destination defined in the **Main settings** screen, in the parameter `db_recovery_file_dest` (see [Figure 127 on page 135](#)).

### Restoring the database

- 1 In the ONMSi Toolkit, click on **Database**
- 2 Click on **Restore** to restore as much as possible:  
Click on **Restore selected** to select a defined restoration: select the restore from the list opened and click on OK.
- 3 In the dialog box open, click on **Yes** to confirm the restoration of database and customized files.
- 4 Click **Ok** to close the dialog box.

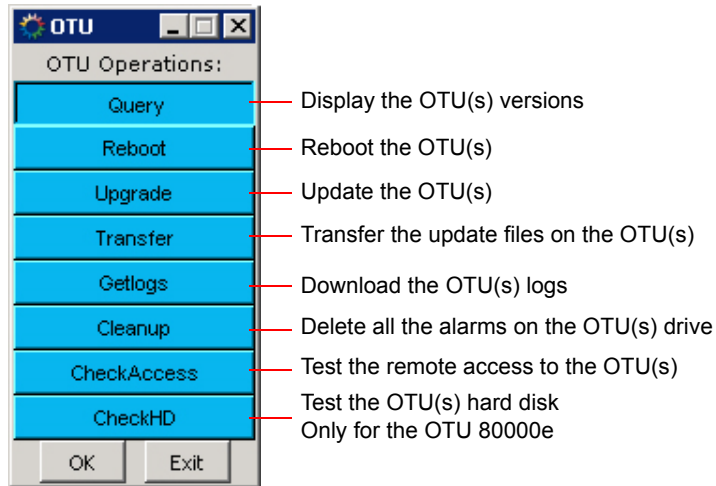
### Using the OTU Toolkit

From the ONMSi toolkit, you can manage the OTU(s) declared in ONMSi.

Click on the **Otu** button  to open a list of OTU operations:

Otu

Figure 130 OTU operations



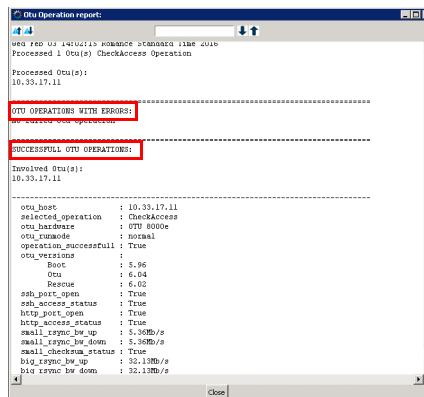
## Testing the remote access to the OTU(s) installed

From the OTU operations window:

- 1 Click on **CheckAccess** > Ok.
- 2 Select the OTU to be tested
- 3 Click on **OK**.

The OTU Operation Report displays. Faulty and successful operations are listed.

Figure 131 Remote OTU tested



## Downloading the logs files for an OTU

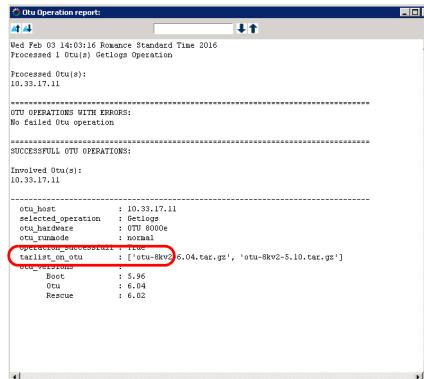
From the OTU operations window:

- 1 Click on **Getlogs**.

- 2 Select the OTU for which logs must be downloaded.
- 3 Click on **OK**.

The OTU Report displays. A file containing the OTUs logs file is generated in: \RFTS\\_SCRIPTS\cluster\log\otu\snapshots\[OTU name or IP]\get-snapshot.SN.YYYYMMDDHHMM.tar.gz.

**Figure 132** Getlogs



## Updating the OTU

### Transferring the update files

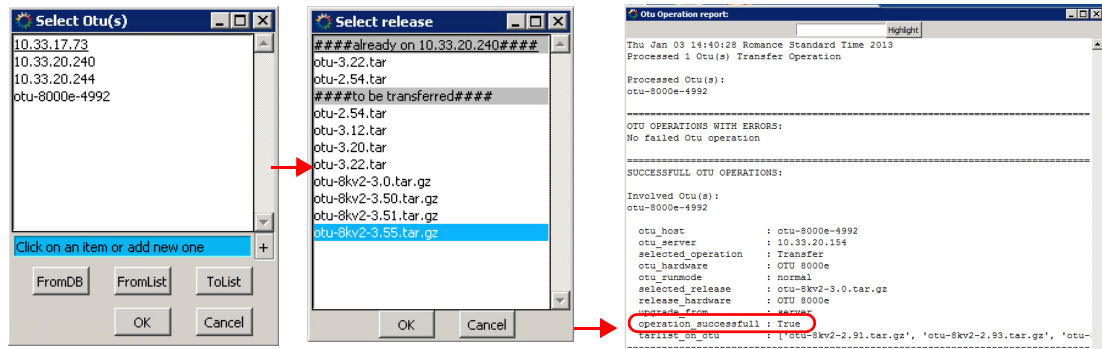
Transfer the update files in prevision of a future update of the OTU(s):

- 1 In the OTU operations, click on **Transfer** button.
- 2 Select the OTU(s) for which the update files must be transferred.
- 3 Click on **OK**.
- 4 In the new dialog box, select the Release to be transferred for the selected OTU(s).

The .tar file must be in \RFTS\\_SCRIPTS\Release\_OTU.

- 5 Click on **OK**.
- 6 Check in the report if the transfer is valid.

Figure 133 Transfer update file



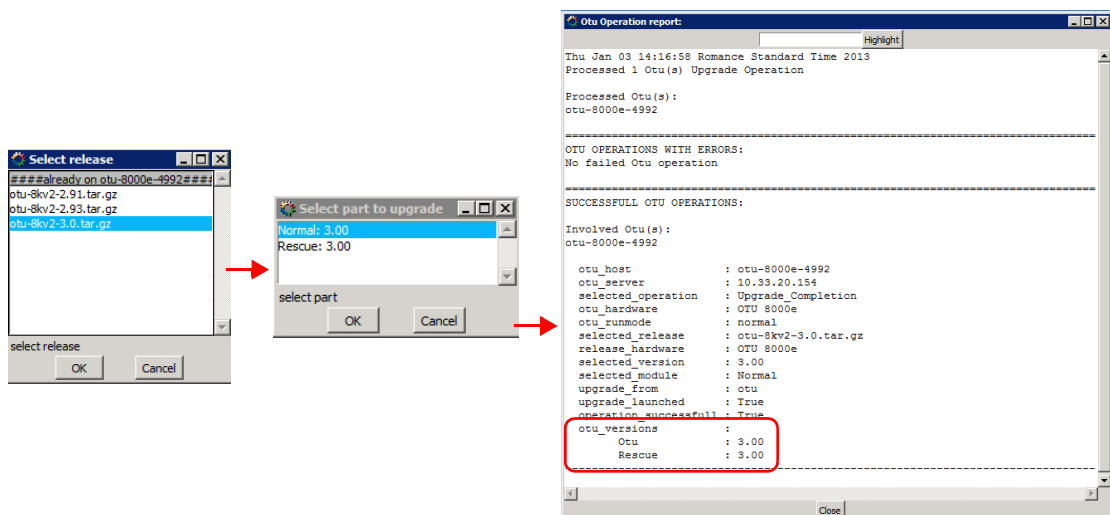
## Updating the OTU(s)

The OTU(s) can be updated via the ONMSi Toolkit

The update file will be transferred if it is not present on the OTU.

- 1 In the OTU operations, click on **Upgrade** button.
- 2 Select the version to be installed on the OTU(s).
- 3 Click on **OK**.
- 4 In the new dialog box, select the part to be updated.
- 5 Click on **OK**.
- 6 Check in the report if the update is valid. There is no report when updating more than one OTU.

Figure 134 Updating the OTU(s)



## High Availability Solution

The High Availability Service menu on ONMSi Toolkit allows to manage the server(s) and the failover for ONMSi backup server:

- Display the server status
- Activate the standby server
- For the Failover, switch to On demand mode or to Automatic mode (license required)
- Upgrade the standby server to the same ONMSi version as the main server
- Rebuild standby database if unable to synchronize automatically.



### NOTE

Do not forget to configure HAS information on ONMSi, when installing the standby server: see [“Main and Backup server” on page 14](#).

## Fail over main points and Pre-requisites

### Main points

- 2 independent physical networks between servers (**mandatory in automatic mode**)
- Automatic or manual failover (license required)
- Uses OTUs visibility to failover, (**only in automatic mode**)
- Automatic database synchronization
- Automatic standby reconstruction
- One single server active at same time
- Notification by email or snmp trap

### Pre-requisites

- 2 identical servers

For more information on pre-requisites and configuration of servers, refer to [Chapter 14 “ONMSi System Requirements”](#).

## Activities

### Main service (ONMSi\_HAS) activities

- Database status (every 1 min)
- ONMSi Server heart beat (every 1 min)
- OTUs reachability for automatic mode (every 30 / 4 min)

- Database synchronization (as defined in main Settings screen - see [Figure 127 on page 135](#))
- Networks status
- In automatic mode, checking failover conditions
- Sending notification through email or snmp traps
- Database backup

### **WatchDog service (ONMSi\_HAS\_WatchDog) activities**

- Checking if main service is running
- (Re)launching main service if needed.
- (Re)booting server if needed
- Sending email or snmp trap notifications

## **Monitoring principles**

- Running a periodic Heart Beat batch on both servers:
  - Every minute
  - Local and remote net (ping)
  - Local and remote ssh status
  - Remote IPMI status - only if used (for Automatic mode only)
  - Main application (ONMSi) heartbeat
  - ONMSi Active services
  - Local and remote Database status
  - Remote main service alive status
- 30 minutes cycling, faster on issues (configurable)
  - OTUs health (OTU alive status) evaluation (every 4 minutes after failure)
  - Both server's common OTUs evaluation

## **Fail-over conditions in automatic mode**

Failover conditions are regularly checked on standby server (every 1 minute)

Without network and no common OTU:

- Fail over if passive server sees more than 60% of OTUs
- ONMSi server stopped on current active server

With network and local OTU visibility fail over when:

- Main application no more answering on active server
- OTU SSH status False on active server

Failover is triggered after a configurable number of successive failures (>10 by default)

Failover is triggered only if current active server is or can be deactivated (no dual activated servers).

## Failing-over process in automatic mode

- Try to softly deactivate faulty server (stopping active services)
- In case of failure try a soft shutdown (ssh shutdown)
- In automatic mode, in case of failure try it the hard way (IPMI power-off) – Only if IPMI is used
  
- If deactivation succeeded try to activate machine:
  - Activate and update database and launch active services
  - Launch a full backup
  
- If activation failed, go into «maintenance\_needed» mode
- If deactivation succeeded previous active server automatically configured as standby server
- Email or snmp trap notifications for main steps

## Maintenance issues

Sometimes a server issue can't be solved, in that case the server goes into a 'maintenanceneeded' state with periodic (configurable) reminder email notifications.

The main 'maintenanceneeded' issues are:

- Cannot open active database (leads to a failover)
- Local db incarnation younger than remote one, but remote server seems to be active
- Giving up rebuilding stby database, too much failures: 5
- Activation aborted due to other server's visibility and deactivation failure
- Local backup server activation failure
- An active service already started or unknown state on another server

In that state applications are not launched

Restarting the 'ONMSi\_HAS' service can help solve the problem.



### NOTE

Do not hesitate to contact Viavi in case of problem or doubt.


## Server's Status

Different server status are available:

<b>localdbcheck</b>	server checks his db (at startup or temporary not reachable)
<b>remotedbcheck</b>	server checks remote db (at startup or temporary not reachable)
<b>noremotenet_</b>	cannot ping other server on either network links (deactivates himself and waitsfor net coming back)
<b>normal</b>	passive server: syncs regularly with main server's db, ready to failover active server:runs ONMS applications
<b>degraded</b>	passive server: would not failover due to ssh or less than 60% OTUs visible active server: stops active services for same reasons
<b>failingover</b>	standby server becomes active
<b>rebuildingstby</b>	standby server makes a full db sync
<b>maintenance_needed</b>	cannot solve 'maintenancereason' pb alone (service restart can help)

## Activating the passive server

In case of problem on main server, the manual activation of the passive server may be required.

- 1 In the ONMSi toolkit, click on **FailOver** button 
- 2 In the dialog box, click on **Yes** to confirm you want to failover to passive server.
- 3 Follow the steps described in the Dashboard.

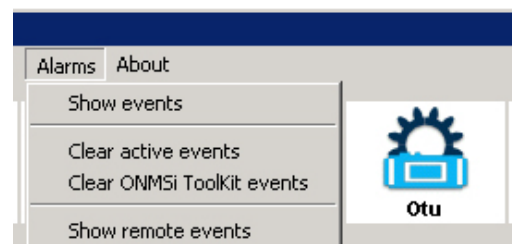
## Alarms

The Alarms menu allows to consult the local or remote issues detected by the ONMSi toolkit.

Click on **Alarms > Show events** to display all the events active on local server.

Click on **Alarm > Remote events** to display all the events active on remote server.

Click on **Alarms > Clear active events** to delete all the alarms on the local server.





Click on **Alarms > Clear ONMSi Toolkit events** to delete all the alarms sent to the ONMSi.

**Test email:** allows to test the e-mail configured in the Main Settings screen (see [“Main Settings” on page 135](#)).

**Test snmp trap:** allows to test the snmp trap, configured in the Main Settings screen (see [“Main Settings” on page 135](#)).



# Index

## A

About ONMSi [9](#)  
Account lockout [106](#)  
Action list [9](#)  
Add Trace [34](#)  
Additional attributes [112](#)  
Alarm [109](#)  
    acknowledge [79](#), [82](#)  
    attenuation [60](#)  
    clean [80](#)  
    clear [82](#)  
    delete [82](#)  
    details [78](#), [79](#)  
    download pdf [80](#)  
    history [81](#)  
    ID [28](#), [80](#)  
    list [78](#)  
    OTU on schematic [76](#)  
    pdf [80](#)  
    peak [63](#)  
    purge [100](#)  
    section [73](#)  
    severity [79](#)  
    table [82](#), [83](#)  
    viewer [10](#), [78](#)  
Attenuation [24](#), [32](#), [59](#), [60](#), [94](#)  
Audit log [100](#)  
Authentication [38](#), [39](#), [42](#), [103](#), [106](#)  
Automatic fail-over [14](#)

## B

Backup [118](#)  
Backup server [14](#)  
Bandwidth [118](#), [119](#)  
Both end measurement [65](#)  
Budget [22](#)  
    data download [57](#)  
    graph [26](#)  
    time slot [66](#)  
    variation [60](#)

## C

Connection test [17](#)  
Contact details [45](#)  
Contextual help [9](#), [11](#)  
CPU [118](#)

## D

Dashboard [30](#)  
    system [8](#)  
Desktop Alert  
    disable [88](#)  
Desktop alert [45](#), [85](#)  
    configure [87](#)  
    display [87](#)  
    installation [86](#)  
    profile [111](#)  
    remove [88](#)  
Detection [54](#), [55](#)  
Domain  
    add [48](#)  
    copy a link [51](#)  
    delete otu [51](#)  
    remove otu [50](#)  
Domain role [40](#), [41](#)  
Download [92](#)  
    alarm [80](#)  
    alarm table [84](#)

## E

E-mail [38](#), [44](#), [85](#), [108](#), [109](#), [110](#)  
    formatting [110](#)  
Escalation [108](#)  
Events table [33](#)  
Excel [7](#), [44](#), [57](#), [84](#), [92](#), [94](#), [97](#), [115](#)  
    landmarks table [69](#)

## F

Fail-over [14](#)  
Fiber Length extension [60](#)

Filters [30](#), [34](#), [82](#), [83](#), [110](#)

audit log [7](#)  
e-mail [109](#)

First Marker (FM) [22](#), [24](#), [31](#)

Formatting [110](#)

## G

Geographical file [73](#)

## H

History [81](#)

## I

Inventory report [93](#)

IP Address  
OTU [16](#)

IP address [7](#), [14](#), [103](#)  
server [6](#)

IP Port [118](#), [119](#)

## K

KLM [73](#)

## L

LAN [14](#)

Landmarks [66–72](#)  
association [71](#)  
force association [71](#)  
table [??–70](#)

Last Marker (LM) [22](#), [24](#), [31](#)

LDAP [39–40](#), [102–103](#)  
Manager [103](#)

Localization [54](#), [55](#)

## M

Main server [14](#)

Manual fail-over [14](#)

Marker A & B [32](#)

Modem [119](#)

## N

Notification [38](#), [44](#), [56](#), [85](#), [87](#), [106](#), [110](#)

Notifications [39](#)

## O

Online help [9](#)

Optical events [32](#)  
landmarks [70](#)

ORL [64](#), [65](#)

OTDR [2](#), [22](#), [54](#), [58](#), [63](#), [73](#), [81](#)  
reference trace [24](#)

OTU [50](#)

add [16–17](#)  
add to schematic [75](#)  
connection test [17](#)  
delete from domain [51](#)  
ping test [17](#)  
recall test [17](#)  
remove from domain [50](#)  
run test [16](#)  
test connection [16](#)

## P

Password [6](#)

expiration [106](#)  
history [105](#)  
policy [103](#), [104](#)  
quality [104](#)  
system [6](#)  
user [38](#), [43](#)

PDF [7](#), [80](#), [84](#), [92](#), [111](#), [115](#)

Peak [61–63](#)

Ping test [17](#)

Ports association [22](#), [23](#)

Purge [100](#)

## Q

Quick search [9](#)

## R

RAM [118](#)

Rebuild (OTU) [17](#)

Recall test [17](#)

Refresh

config. (OTU) [17](#)

Report

create [94](#)  
excel [97](#)  
execute [96](#)  
templates [94](#)

Ringtone [87](#)

## S

Scale factor (Landmarks) [72](#)

Schematic [114](#)  
OTU [75](#)

Section [10](#)

Server

address [13–14](#), [87](#)  
backup & main [14](#)  
IP address [6](#)  
LDAP [103](#)  
name [6](#)  
system [6](#)

Severity [79](#)

Slacks (Landmarks) [72](#)

SMPP [119](#)

---

Splitting section (Landmarks) [72](#)  
Sub-domains [49](#)  
Synchronization [66–??](#)  
System dashboard [48](#)  
System role [40–41](#)

## T

Table  
  configuration [92](#)  
  download [92](#)  
  events [33](#)  
  landmarks [67–70](#)  
TCP Ports [119](#)  
Test  
  connection [16](#)  
  on demand [59](#)  
  purge [100](#)  
  schedule [57](#)  
  stop [58](#)  
Time slot [66](#)  
Trace  
  add [34](#)  
  color [34](#)  
  multi- [34](#)  
Trace Browser [30](#)  
Trace viewer [30](#)

## U

User  
  add [38](#)  
  alerts [39](#)  
  API [103](#)  
  connected [46](#)  
  contact details [38](#)  
  details [38](#)  
  disconnect a [46](#)  
  domain [40](#)  
  domain role [42](#)  
  LDAP [39–40](#), [102–103](#)  
  password [6](#), [43](#)  
  preferences [9](#)  
  session duration [101](#)  
  system [40](#)  
  system role [42](#)

## Z

Zoom [24](#), [31](#)







70ONMSI0302  
Rev. 003, November 2016  
English



**Viavi Solutions**

<b>North America:</b>	<b>1.844.GO VIAVI / 1.844.468.4284</b>
<b>Latin America</b>	<b>+52 55 5543 6644</b>
<b>EMEA</b>	<b>+49 7121 862273</b>
<b>APAC</b>	<b>+1 512 201 6534</b>
<b>All Other Regions:</b>	<b><a href="http://viavisolutions.com/contacts">viavisolutions.com/contacts</a></b>
<b>email</b>	<b><a href="mailto:TAC@viavisolutions.com">TAC@viavisolutions.com</a></b>