

VIAVI



ONMSi
Optical Network Monitoring System
User Manual

ONMSi
Optical Network Monitoring System
User Manual



VIAVI Solutions
1-844-GO-VIAVI
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 2009-2025 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.

Ubuntu is a registered trademark of Canonical in the United States and/or other countries.

Red Hat ® Enterprise Linux ® is a registered trademark of Red Hat Inc. in the United States and/or other countries.

Microsoft Internet Explorer and Microsoft Edge are either trademarks or registered trademarks of Microsoft 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.

Java is either trademark or registered trademark of Oracle Corporation 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.

Table of Contents

About This Guide	xv
Purpose and scope	xvi
Assumptions	xvi
Technical assistance	xvi
Conventions	xvi
Chapter 1 ONMSi Overview	1
Introduction	2
ONMSi Benefits.....	2
ONMSi Features	2
ONMSi Architecture	3
Chapter 2 ONMSi login and general view	5
Log-in	6
Accessibility/High contrast.....	6
Audit logs	7
General User Interface	7
Text colors	8
Increasing view.....	8
Shortcuts panel.....	10
Tree view.....	11
Description of the objects in the Tree	12
Alarm viewer	12
Keyboard shortcuts.....	13
Adding a logo to the User Interface	13
Chapter 3 Setting the Server address	15
Setting up the server address	16
Chapter 4 Adding an OTU/FTH	17
Adding an OTU	18
Testing the connection and refreshing the configuration	18
Configuring the OTU	20

Associating OTU address to server	20
Launching an Autotest of the OTU.....	20
Moving the OTU	20
Replacing an OTU.....	21
Chapter 5 Monitoring a link	23
Optical Link monitoring principle	24
Provisioning the link	24
Reference trace display	26
Changing the reference trace.....	27
Landmark setting	28
Checking long term degradation.....	29
Cable Management	29
Defining a Cable Head as Cable Route	30
Cable Route dashboard	31
Alarms on the Cable Route	31
OTU Scans	32
Automatic scan	32
Manual Scan.....	32
Alarm details	33
Ports & Links Field Application.....	33
Opening the Ports & Links field application	34
Details of the link.....	34
Performing a measure on demand of the link	35
Disabling the measurements on link	36
Scheduling a pause period	36
Displaying a trace from the tested link.....	38
Performing a test on demand.....	38
Displaying the alarm details	39
Acknowledging or clearing the alarm.....	39
Adding a comment	40
Displaying the otdr trace of the alarm	40
Displaying the SLM view of the link in alarm	40
Displaying the history of the alarm.....	41
Chapter 6 Displaying the alarms	43
Alarms view.....	44
Chapter 7 Trace Viewer	45
Opening a trace using the Trace Browser.....	46
Trace display	47
Zooming on trace	47
Positioning Markers.....	47
First and Last markers	47
A & B markers	47
Optical events	48
Latency measurement.....	48

Trace details.....	49
Displaying the events table	49
Changing the trace color.....	50
Multi-trace display.....	51
Adding trace(s)	51
Multi-traces display	52
Changing the active trace and the trace color	52
Trace and events table	53
Chapter 8 Managing users	55
Adding a user.....	56
Adding a «standard» user.....	56
Creating a user with LDAP	58
Creating Profiles	59
Defining the system and domain roles for the user.....	60
System and Domain roles principle	60
Creating a System or Domain role	61
Assigning System roles to a Profile	62
Assigning Domain roles to a profile.....	62
Changing the current user preferences.....	63
Changing the user password	63
Changing the excel version to be used	64
Modifying the notification address.....	64
Displaying desktop alert.....	65
Displaying the connected users.....	65
Chapter 9 Managing domains	67
Domain principle.....	68
Creating a domain	68
Adding sub-domains.....	69
Copying an OTU to another domain	70
Removing an OTU from a domain	70
Deleting an OTU.....	71
Copying a link to a domain.....	71
Chapter 10 Advanced Monitoring	73
Advanced Setup	74
Downloading budget data (subject to license)	74
Downloading landmark history	75
Scheduling a test	75
Stopping the test / all tests and forbid any shoot on the link.....	76
Periodical OTDR Trace Storage option	77
Performing a test on demand	78
Advanced Monitoring	78
Modifying the attenuation thresholds.....	78
Alarms on test attenuation.....	79
Fiber length extension.....	80
New peaks	81

Existing peaks	82
High Sensitivity Monitoring	84
Both end measurement	85
Cable Documentation	86
Activating the Cable documentation function	87
Activating the Association landmarks and optical events	87
Completing the landmark table	87
Creating a landmark table from a trace	88
Create a landmarks table from an Excel file	89
Associating Landmark and Optical Event	90
Splitting section	92
Associating a geographical file to a link	93
Chapter 11 Alarms management	97
Alarms Display	98
Alarms Viewer	98
Alarms details	98
Actions on alarms	99
Changing the alarm severity	99
Acknowledging an alarm	99
Clearing an alarm	100
Downloading a pdf file of the alarm (detail view)	100
Alarm History (detail view)	101
Deleting an alarm (detail view)	101
Actions on table display	102
Filtering the alarms in the table	102
Configuring the alarms table	103
Downloading the alarms table	104
Other actions on table	104
Notification by e-mail of an alarm	104
Alarm Desktop alert	105
Installing the extension in Google Chrome TM	105
Configuring the desktop alerts	106
Display of the desktop alerts	107
Disabling or removing the Desktop Alert extension	108
Chapter 12 Tables, Reports and Pinboard Management	111
Downloading data from a table / list	112
Configuring the table	112
Downloading the data from a table	112
Inventory Report	113
Generating reports	114
Creating a report	114
Launching the report	115
Managing Pinboard	116
Configuring the pinboard	116
Saving the Pinboard configuration	118
Other pinboard features	118

Chapter 13	Fiber Sensing	119
	Configuring the OTU with an OTDR Module connected to a DTSS Module	120
	DTSS Configuration Measurement	121
	DTSS Monitoring Test	123
	Reference measurement	124
	Zone Configuration	125
	Zones	126
	Modifying the position of a zone	126
	Adding/Removing a zone	126
	Zone thresholds	127
	Link Dashboard view	128
	Zone Dashboard	128
	Alarms details	130
Chapter 14	ONMSi PON System	133
	Manual PON Creation	134
	Uploading / Downloading Data	134
	Central Office Data	135
	PON Data	135
	Monitored Point Data (called Home in the user interface)	136
	Test Points data	136
	Uploading data	137
	Home Browser page	138
	Adding Filters	139
	Deleting Home or PON Data from the System	139
	Associating Central Office to OTU	139
	PON Calibration	140
	Associate PON to Optical Switch port	140
	Calibration Principle	141
	Calibration process	142
	PON Test	143
	Automated PON creation	145
	PON feeder view	146
	PON feeder card	146
	PON Calibration card	146
	PON distribution/drop card	147
	PON distribution/drop view	147
	ONMSi PON Topology	148
	ONMSi PON Field application	152
	Configuration of the PON field application	153
	Performing an OTDR test	154
	GPS coordinates	155
	Pre-requisites to use GPS coordinates in Field application	156
	GPS information in ONMSi	156
	Modifying the application settings	157
	VIP Permanent Monitoring	158
	Identifying the Home pass	159
	Starting VIP Monitoring	160
	Setting up demarcation	161
	Alarms Viewer	163

Chapter 15	System settings	167
Configuring and launching a manual purge	168	
Configuring an automatic purge	168	
Configuring server advanced parameters	169	
Configuring the unit preferences	169	
Users	170	
Defining the session duration	170	
Configuring the LDAP	170	
Configuring the password policy	172	
Password quality	172	
Password history	174	
Account lockout	174	
Password expiration	174	
Advanced configuration	174	
Single Sign On screen	174	
Links configuration	175	
Link types	175	
OTDR Link type configuration	176	
DTS or DTSS Link type configuration	179	
PON configuration	179	
Point to Point Configuration	180	
Point to Point General configuration	180	
Landmarks & optical events configuration	181	
Monitoring configuration	182	
Cable route Monitoring configuration	182	
Sensing Configuration	183	
Configuring e-mail/sms alert profiles	184	
Defining Escalation	184	
Defining filters for the e-mail notifications	185	
Configuring the e-mail format	186	
Configuring Desktop alert profiles	187	
Configuring the Media servers	188	
Configuring the e-mail server	188	
Configuring the sms server	189	
Plugins	190	
Additional Attributes	191	
Configuring an object with additional attributes	191	
Displaying and completing the attribute	192	
Field application	192	
Chapter 16	Measurements	195
Principle	196	
Display of the measurement page	196	
Domain Management	197	
Adding a Central Office to the domain	197	
Adding an existing OTU/FTH	198	
Adding a Cable Head to the Central Office	199	
Connecting links to the OTU/FTH or to the Cable Head	200	
Applying a label to create links in bulk	201	

Adding manually a link	202
Editing multiple links	202
Disconnecting a link	203
Starting measurements on links	203
Creating and measuring automatically a link.....	204
Canceling a test	205
Results screen from measurement tests.....	206
On-demand bulk measurement window.....	207
Actions on display	207
Overriding the result.....	207
Filtering the display.....	208
Zooming on display	210
Displaying results for measured link(s)	211
Details of the Link	211
Details for several selected Link	212
OTDR results	212
SmartLink view.....	212
Event Table	214
Trace view	215
Sensing results	216
Generating a report for the links	217
Exporting Trace, pdf and / or json data	218
Construction/Analytics Field Application	219
Opening the field application	219
OTU/FTH or Cable Head view	220
Measured link view.....	221
Chapter 17 Cable health monitoring	223
Cable health monitoring principle	224
Starting with the cable health monitoring	225
Defining the Length and Attenuation Tolerance.....	225
Launching the cable health monitoring and analyzing results.....	226
Fibers status	227
Other actions in Configuration screen	228
Cable route dashboard	229
Chapter 18 GeoView	231
Pre-requisites.....	232
Interaction with the map.....	232
Centering the map on the OTU.....	232
Centering the map on the Link	233
Centering the map on the Alarm	233
Trace viewer and map	234
Interaction on map.....	235
Tools and Details panel	236
Setting tools	236
Layers Tools.....	237
Measure Tools.....	238
Object selection	239

Chapter 19 GeoDesign	241
Pre-requisites	242
Adding a domain to the mapping design.....	242
Creating an object.....	243
Before creating an object	243
Creating a path	244
Designing a path without fiber	244
Designing a path with fiber	244
Creating a landmark	246
Connecting a Path to a landmark	247
Adding a fiber to a path.....	247
Adding a landmark.....	248
Adding a landmark on the path with fiber.....	248
Adding a landmark on the path without fiber	249
Adding an OTU	250
Adding an OTU from GeoDesign	250
Adding an OTU from the ONMSi	251
Visualizing a fiber details.....	251
Visualizing a connection details	252
Importing/Exporting KML file	253
Exporting a fiber route.....	253
Importing a KML file	253
Manual import of the KML file.....	254
Automatic import of the KML file	256
Resetting the KML file history	259
Deleting a Fiber Route	260
Path close to an existing one.....	260
Interaction with the map	261
Focus on a fiber route.....	261
Duplicating a fiber route	261
Centering the map on the OTU	261
Centering the map on the Link	262
Centering the map on the Alarm.....	262
Trace viewer and map.....	263
Interaction on map.....	264
Tools and Detail panel.....	265
Legend tool	265
Information tool	266
Layers Tool	266
Measure Tool	268
Object selection and details	268
Chapter 20 Single Sign On (SSO) configuration	271
Purpose.....	272
Prerequisites	272
Connection to Keycloak.....	272
User fields extractors.....	273

Appendix A Software License Terms	275
Appendix B OTU Manager	281
Introduction to OTU Manager	282
Starting OTU Manager	282
Using the OTU Manager.....	283
Manager repository (libraries)	284
Firmware library.....	284
License library	284
SSH Keys library	285
Maintenance operations	286
Firmware upgrade	286
License update	287
SSH key update	288
Support operations	288
Download log files	288
Reboot OTU / FTH	289
Cleanup OTU / FTH	289
Test the remote access to the OTUs / FTHs	289
Appendix C OTU Toolkit	291
Introduction to OTU toolkit	292
Using the OTU Toolkit.....	293
Downloading the logs files for an OTU.....	294
Rebooting OTUs	294
Updating the OTU firmware.....	294
Cleaning OTUs	296
Checking the OTU hard disk	296
Testing the OTU network access.....	296
Uploading a license on the OTU	297
Applying a software patch on the OTU	297
Index	299

Table of Contents



About This Guide

Topics discussed in this chapter are as follows:

- “Purpose and scope” on page xvi
- “Assumptions” on page xvi
- “Technical assistance” on page xvi
- “Conventions” on page xvi

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-VIAVI. For the latest TAC information, go to <http://www.viavisolutions.com/en/services-and-support/support/technical-assistance>.

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 Start
Buttons or switches that you press on a unit appear in this TYPEFACE .	Press the ON switch.
Code and output messages appear in this typeface .	All results okay
Text you must type exactly as shown appears in this typeface .	Type: a:\set.exe in the dialog box.
Variables appear in this typeface .	Type the new hostname .
Book references appear in this typeface .	Refer to Newton's Telecom Dictionary
A vertical bar means “or”: only one option can appear in a single command.	platform [a b e]

Table 1 Typographical conventions (Continued)

Description	Example
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 Ctrl+s
A comma indicates consecutive key strokes.	Press Alt+f,s
A slanted bracket indicates choosing a submenu from menu.	On the menu bar, click Start > Program Files .

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 Benefits](#)” on page 2
- “[ONMSi Features](#)” 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 a 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

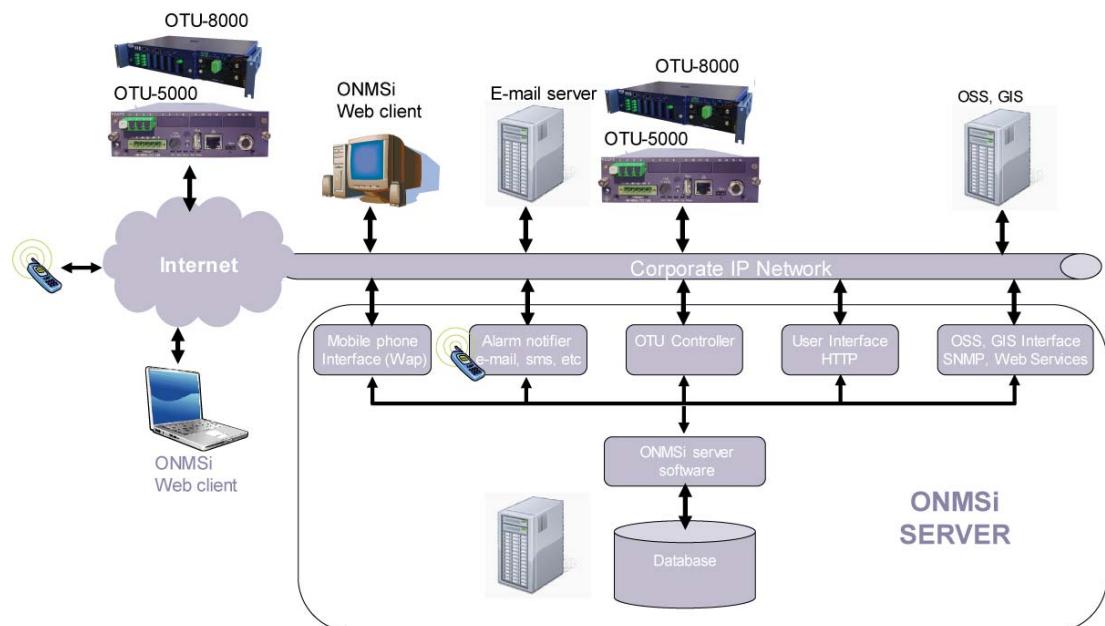
- Reduces Fault location time from 5 hours to 5 minutes (average time)
- Reduces MTTR and network downtime by at least 30%
- Reduces operational costs by providing faster automated dispatch
- Scalable to optimize CAPEX and expand as your network expands
- Flexible to support P2P (Metro/Core/Access) and 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 fail over 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:

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

Log-in

To log-in to ONMSI:

- 1 Open a web Browser:
- 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 2 Login to ONMSI

The screenshot shows a 'Login to ONMSI' dialog box. It has three input fields: 'Language' (set to 'English'), 'Login' (set to 'admin'), and 'Password' (set to 'password'). Below the fields is a blue 'Connect' button.



CAUTION

Login and password are case sensitive!

To get more information on user and login parameters (modify...), see “[Users](#)” on [page 170](#).

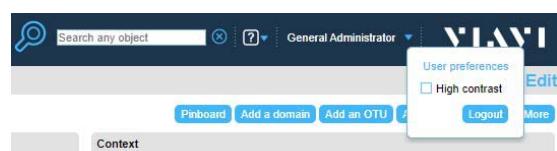
Accessibility/High contrast

High contrast mode is designed for users with weak eyesight to help them read text and navigate more efficiently.

They can see the buttons and text with more pronounced borders with the background, making them more visible.

The **High Contrast** mode is a built-in accessibility feature could be enabled from the user preference menu:

Figure 3 High Contrast mode



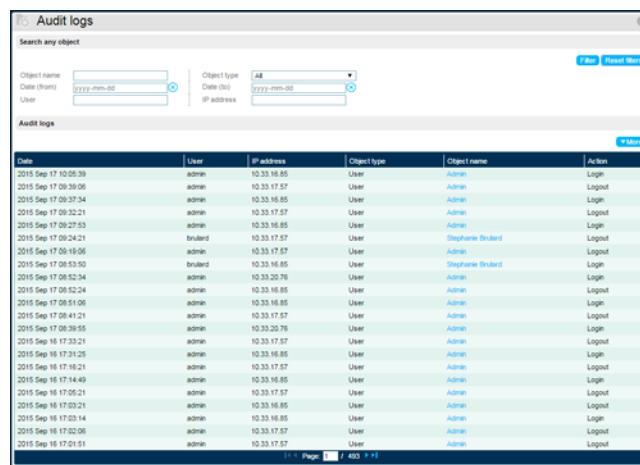
Once this option is enabled, it is kept after a logout/login on the same web browser.

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



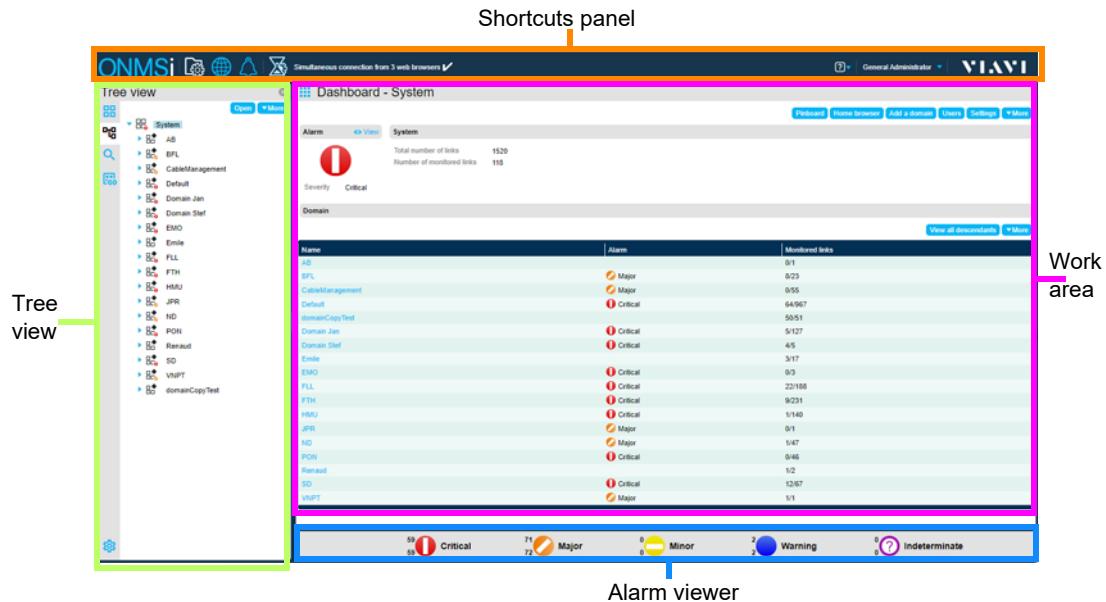
The screenshot shows a table titled "Audit logs" with columns: Date, User, IP address, Object type, Object name, and Action. The table lists numerous log entries from September 17, 2015, to September 18, 2015, detailing user logins and logouts from various IP addresses. At the top of the window, there are search filters for "Object name", "Date (from)", "Object type", "Date (to)", and "IP address". Buttons for "Filter" and "Reset filters" are also present.

- 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 112).

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.

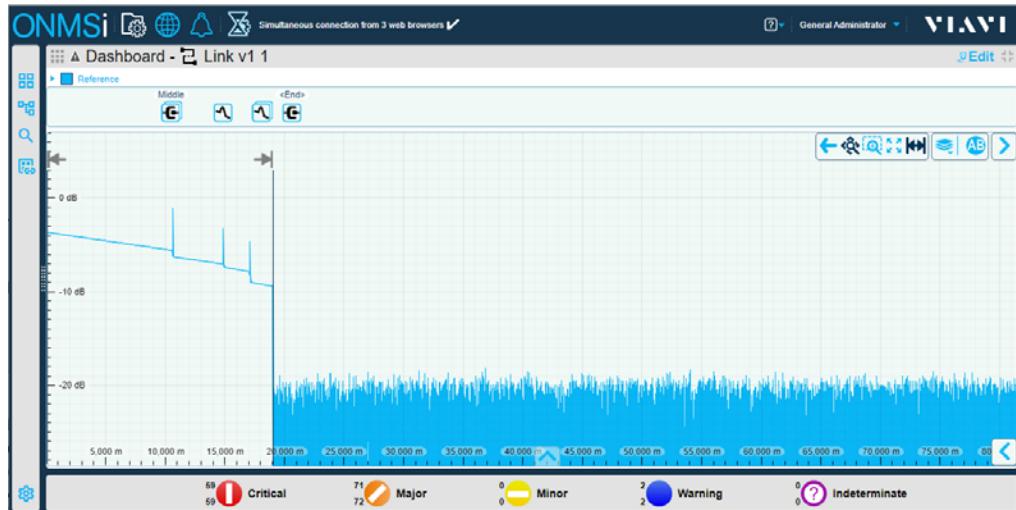
Increasing view

The icon available in different views of the application, allows to enlarge the main view in the work area.

Once the view wished is displayed (trace, table, budget graph, alarm event view...):

- 1 Click on the right of the view on the icon .

Figure 6 Example of Trace view increased



Click on the icon  to return to initial view.



CAUTION

Pressing the **Edit**, **Save** or **Cancel** key cancels the full screen view, the screen returns to initial view.

Example of Full screen view for Trace with association

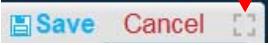


NOTE

It is recommended to validate the edition mode first, and then to pass to full screen mode before performing the association markers/optical events.

If the Edition is validate after the full screen, this last one is canceled, the user returns to initial view.

In case of a trace opened in association view:

- 1 Click on **Edit**.
- 2 Click on the icon 

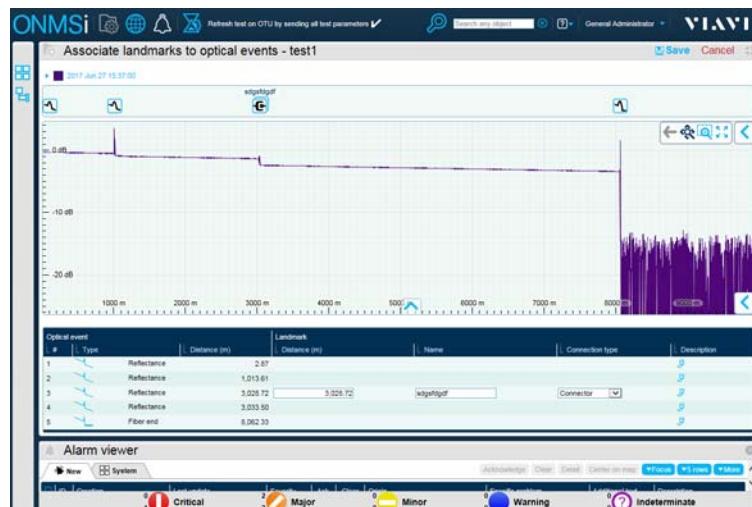
- 3 Select the view to be increased:

- Table
- Trace & Table
- Trace



The display is modified according to the view selected.

Figure 7 Example of Trace & Table view in full screen, in «Association» mode



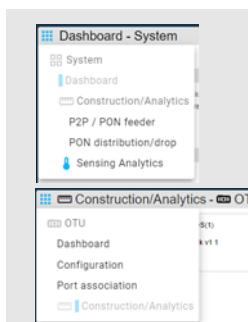
Click on the icon to return to initial view.

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 on the icon of the page open (ex. System dashboard, OTU, Central Office overview...) to open the menu for shortcuts: according to the page open, the sub-menu is different and refers to all the elements linked to the page.



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



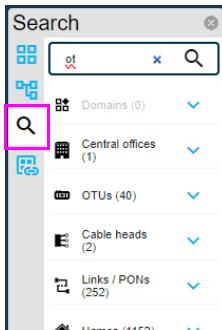
Click to hide (icons turns blue) / show (icons turns white) the map with **FNM** (option)



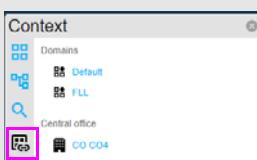
Click to hide (icons turns blue) / show (icons turns white) the alarm viewer.



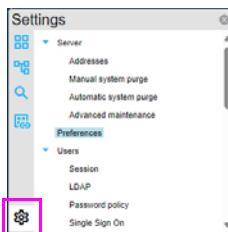
Click to open the action list (running activity).



Enter the first letter(s) of the searched element. The Search tool will display all the elements in order to search according to the type of element.



Click on the icon Context to display the context of the open page, the objects linked to the one displayed on the main screen.



Click to open the **System Settings** menu (see [Chapter 15](#)).



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 63](#))
- **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 170](#)). 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 60](#).

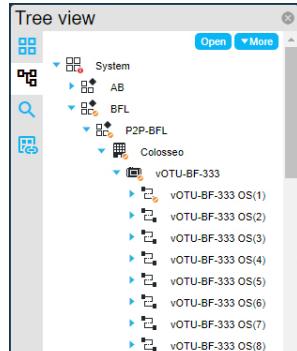
Tree view

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 8 Example of Tree view



2 Select the object, double click it to open the related dashboard.

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

Click on the icon to return to the system dashboard.

Click on the cross to close the Tree view.

On the lower left side of the screen, in the Tree view, click on the icon to directly display the **Settings** screen.

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
- Central Office
- OTU
- Cable Head
- Links
- PON
- 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 9 Alarm viewer



For details on Alarms, see [Chapter 11 on page 97](#).

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
← ↑ → ↓ with focus on trace viewer	Pan the trace
+/- with focus on trace viewer	Zoom or Unzoom the trace

Adding a logo to the User Interface

A specific logo can be added to the VIAVI logo on the upper right side of the Interface. This logo will be still visible after a disconnection and re connection.

To add your own logo to the ONMSi interface

- 1 Name your file `customerlogo.png`
- 2 Paste it in the directory: `/opt/rfts_apps/conf/topaz/topaz-conf/images`

NOTE

The customer logo will be displayed in the xls or pdf reports generated: see [“Launching the report” on page 115](#).

Figure 10 Customer logo on the user interface



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 16

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 11 Setup Server addresses

Addresses				
Server 1				
Host name:	ONMSI-TEST-MAIN			
Base URL:	http://onmsi-test-main			
				Edit
				Remove an address Add an address
Name	Address	Default	In use	Description
LAN sans DNS	10.33.20.120			Edit
Private LAN	onmsi-test-main	✓	✓	Edit
Private LAN 2	192.168.1.2			Edit
Public access	217.128.65.176			Edit
Server 2				
Server 2 enabled:	✓			
Host name:	ONMSI-TEST-BCK			
Base URL:	http://onmsi-test-bck			
				Edit
				Remove an address Add an address
Name	Address	Default	In use	Description
LAN sans DNS	10.33.20.131			Edit
Private LAN	onmsi-test-bck	✓	✓	Edit
Public access	217.128.65.176			Edit

- 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 OTU/FTHs 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).

Adding an OTU/FTH

This chapter provides a description for adding an OTU/FTH 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 18](#)
- [“Testing the connection and refreshing the configuration” on page 18](#)
- [“Configuring the OTU” on page 20](#)

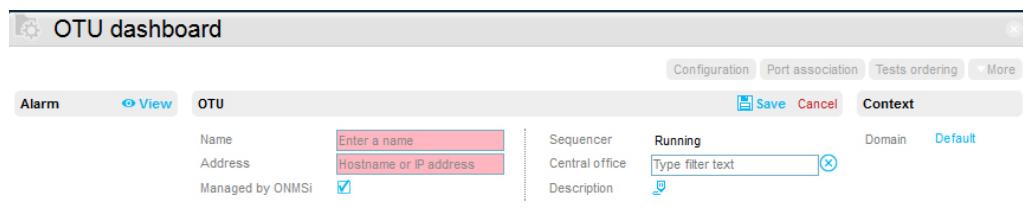
Adding an OTU

To add an OTU to the domain:

- 1 If necessary, return to the System Dashboard window clicking on the ONMSI logo **ONMSI**.
- 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 12 Adding an OTU

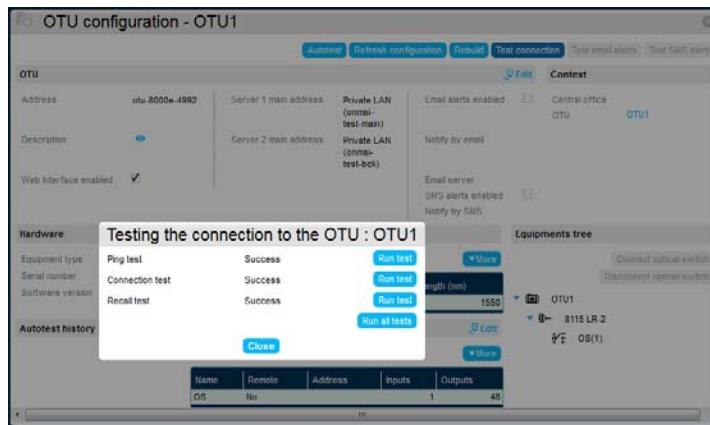


- 3 Enter a **Name** (for example: OTU/FTH location) and the IP **Address** of the equipment (Physical IP address or hostname).
Use the same Address as setup on OTU via OTU web browser.
- 4 Press **Save** to confirm the creation.
The OTU creation process is completed once the progress bars are no more 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 perform exclusively the corresponding test.
All tests must succeed.

Figure 13 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.

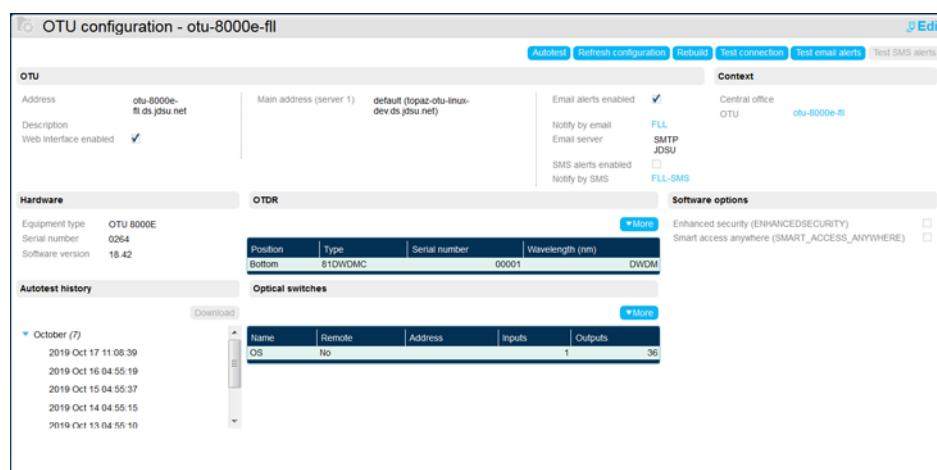
Rebuild is not necessary with brand new OTU.

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 14 OTU successfully added to the Domain



The OTDR and DWDM module installed are displayed.

To recognize the type of module, the parameter **Wavelength** displays **DWDM** instead of the wavelength if a DWDM Module is installed.

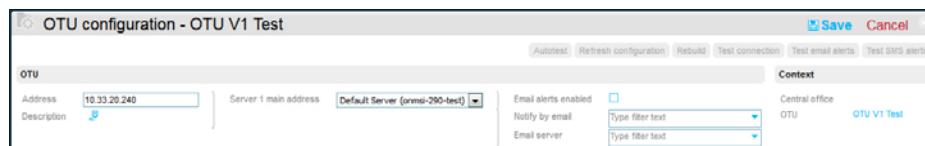
Configuring the OTU

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 15](#)).

Figure 15 Server / OTU address association

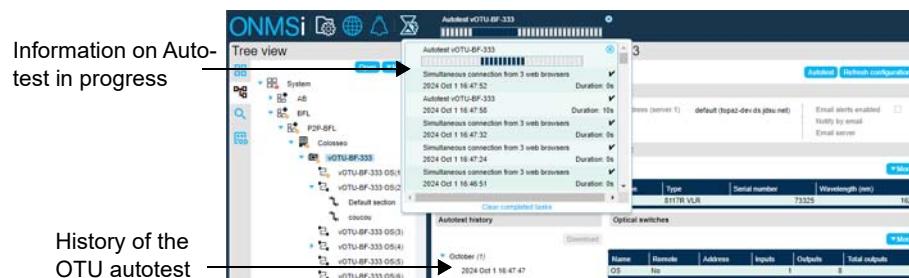


Launching an Autotest of the OTU

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 16 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.

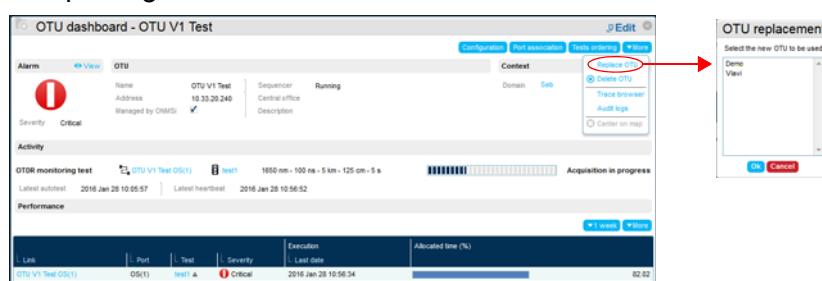
The OTU is removed form the initial domain and set into the new one.

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 18.
- 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 17 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.

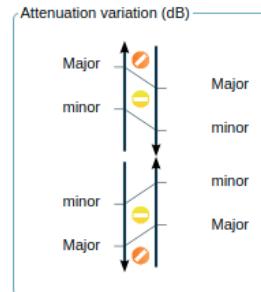
This chapter provides a description on the link monitoring process.

Topics discussed in this chapter include the following:

- “Optical Link monitoring principle” on page 24
- “Provisioning the link” on page 24
- “Landmark setting” on page 28
- “Checking long term degradation” on page 29
- “Cable Management” on page 29
- “Ports & Links Field Application” on page 33

Optical Link monitoring principle

Figure 18 Optical Link monitoring principle



The monitoring is based on comparison between a reference acquisition and the current acquisition.

The reference trace is composed of two acquisitions (these dual acquisitions is called SmartAcq):

- An acquisition using a short pulse to minimize the front end dead zone
- An acquisition using an appropriate setting to cover the whole fiber or user's acquisition parameters

A first marker is placed after the front end dead zone and a last marker is placed at the end of the trace.

If a fault occurs before the first marker, it is classified "injection fault".

The deviations between the reference and the actual trace are compared against threshold.

If a threshold is crossed, an alarm is generated with a severity according to the type of level (minor, major, critical) which is crossed.

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 **Link provisioning**.

Figure 19 Port association

Port association - OTU-5000-00101							Context			
Port association							Central office CO 101			
Total number of ports	40	Number of unused ports	31	OTU						
Port	Link Name	Type	PON Name	PON calibration	Zone (m)	Level (dB)	Deviation (dB)			
OS(01)	etu-5000-00101 OS(01)	Default OTDR								
OS(02)	MyLinkWithEverything	Build_Auto_Splitter1x4								
OS(03)	etu-5000-00101 OS(03)	Build_Auto_Launch15m								
OS(04)	etu-5000-00101 OS(04)	0 pon PON 1x8-1x8 1625	etu-5000-00101 OS(04)	Calibrated	7.97 - 11.00	-2.43				
OS(05)	etu-5000-00101 OS(05)	0 pon PON 1x8-1x8 1625	etu-5000-00101 OS(05)		11.63 - 14.66	-13.85				
OS(06)	385 prep. 6	0 pon_link_type_PTP								
OS(07)	etu-5000-00101 OS(07)	Build_Auto_Splitter1x4_2GSON	etu-5000-00101 OS(07)							
OS(08)	etu-5000-00101 OS(08)	0 pon_link_type_PTP								
OS(09)										
OS(10)										

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 20 Provisioning



6 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.

Port	Status	Reference			
		Fiber length (m)	Budget (dB)	Linear attenuation (dB/km)	Test
OS(08)	Failed: first marker position before minimum (2.04m for selected pulse)	10.37	12.84	1.247.45	Trace
OS(09) ✓		10.53	2.79	0.25	Test
OS(10) ✓		10.529.60	3.53	0.34	Test

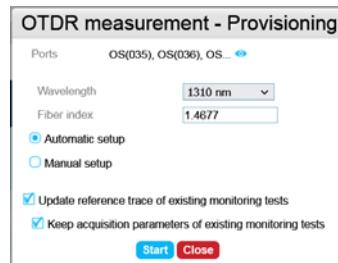
Changing the reference for existing tested links

To update the reference trace for existing tests:

- 1 Select the links in the **Port association** window.
- 2 Click on **Provisioning**.

The OTDR measurement window opens

Figure 21 Provisioning with update of reference



- 3 Select parameter **Update reference trace of existing monitoring test** in order to modify the reference for links already tested.
- 4 Deselect the parameter **Keep acquisition parameters of existing monitoring tests** (selected by default) to use the acquisition parameters configured on this box for the new reference.
- 5 Press **Start** to launch the process.

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:

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

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

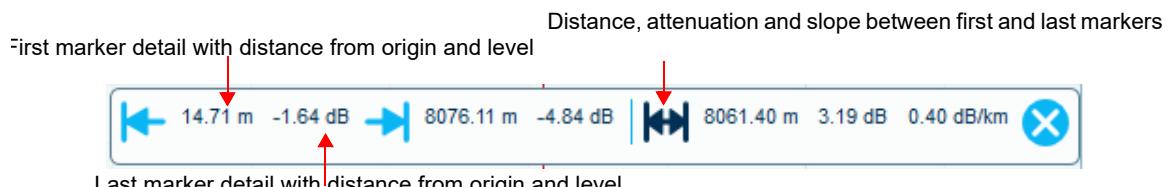


NOTE

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

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

- c Click on the button .



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

- 2 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.

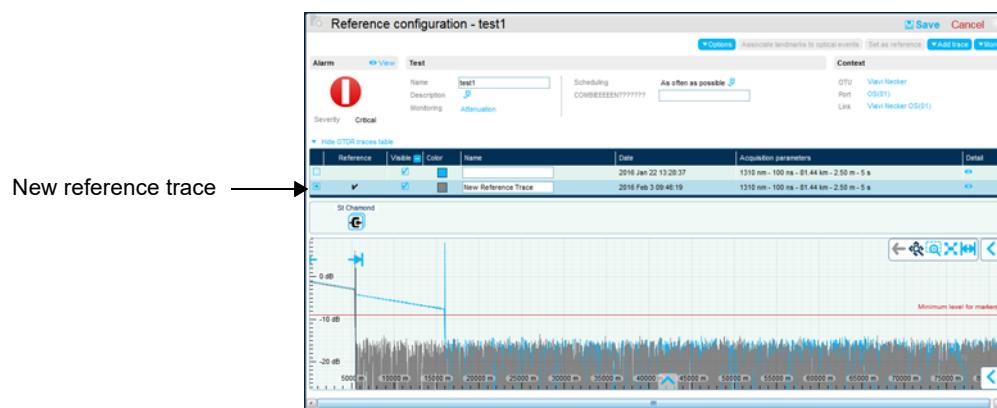
- 1 From the Link Dashboard, click on **Configuration & Reference** button.

- 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 the new reference trace.

Figure 22 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 23 Optical event and associated landmark



NOTE

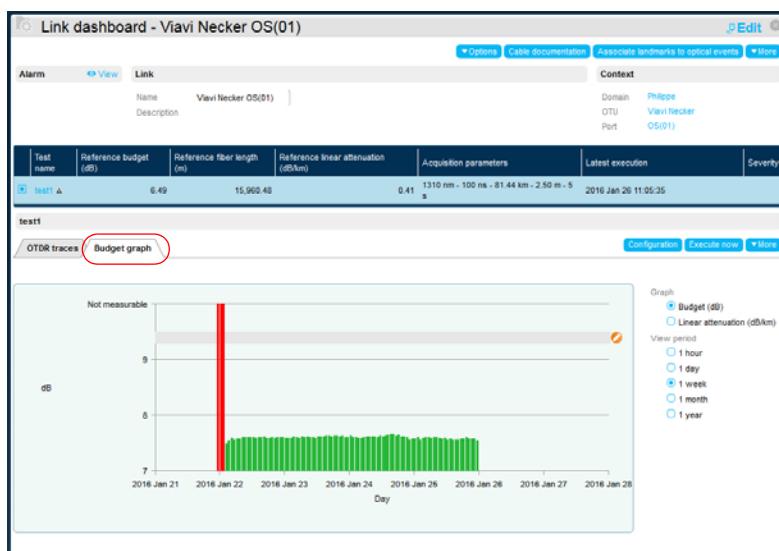
This function cannot be used in parallel with the Cable Documentation option; use either this function or the Cable documentation option, not both.

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 24 Budget graph

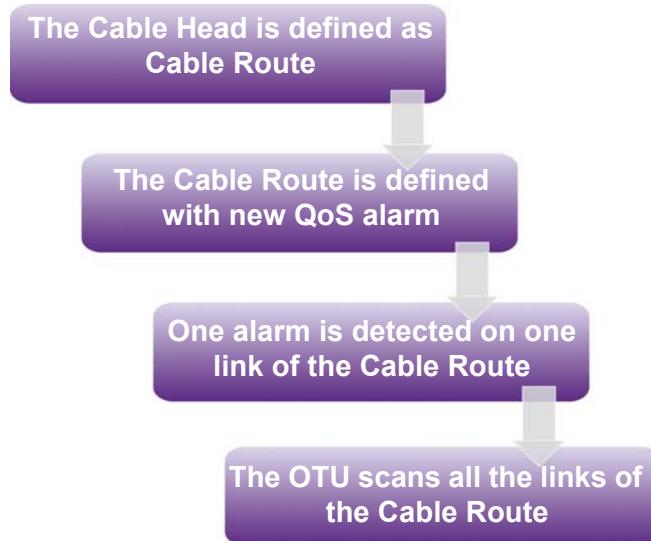


Cable Management

In ONMSi, you can now define a Cable Head as a Cable Route and then group the alarms per cable in order to receive less notifications.

This new alarm is generated to summarize a set of alarms on links.

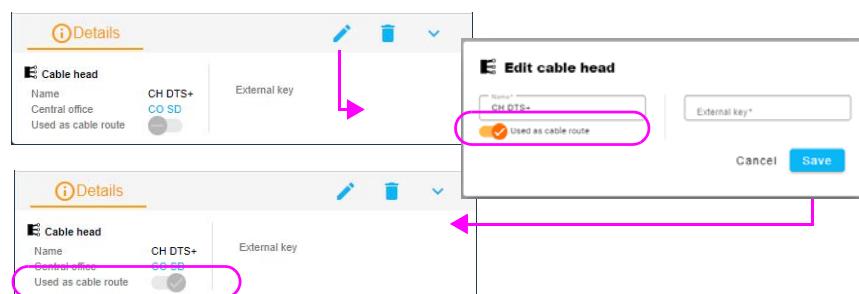
Figure 25 Cable Management



Defining a Cable Head as Cable Route

- 1 In the Tree view, double click on the **Cable Head** () to be defined as Cable Route.
- 2 In the **Construction/Analytics** view, in the Details window of this Cable Head, click on to Edit the Cable Head information.
- 3 Select **Use as Cable Route** parameter.
- 4 Click on **Save** to validate.

Figure 26 Cable Route settings



See chapter “[Measurements](#)”: “[Applying a label to create links in bulk](#)” and “[Adding manually a link](#)” to add links to the Cable Route.

Once the Cable Route is defined, a QoS alarm is managed, as the QoS alarm for PON, Link...



CAUTION

The links declared in the Cable Route must follow the same route.

Cable Route dashboard

Once the Cable Route is defined, a dedicated dashboard is available in ONMSI.

- 1 From **System** page, right click on the Cable Route in the Tree View.

- 2 Click on **Open Cable Route**.

The Cable route dashboard is displayed.

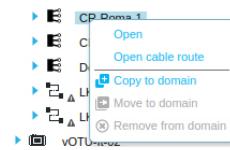


Figure 27 Cable Route dashboard

Main Information on the Cable Route

3 links composing the Cable Route

Cable Route architecture

The screenshot shows the "Cable route dashboard - CR-Roma-1" interface. It includes sections for "Information" (Cable route: CR-Roma-1, Total number of links: 3, Number of links in alarm: 0), "Links and active alarms" (listing three links: 100, 101, 102, all labeled "OK"), and an "Alarm viewer" (showing one critical alarm for link 102 with ID 37, created at 2023 Jan 27 14:27:13, last updated at 2023 Jan 27 14:31:05, severity: Major, origin: LK-R-102-CH-1, specific problem: Attenuation, additional test: ATTENUATION, description: Attenuation (test: test1) - 1,000.00 m). A context menu is open on the right side of the dashboard.

Alarms on the Cable Route

Once the OTU performs measurements on fibers, if one alarm occurs on one link of the Cable Route, it is displayed in the Alarm viewer.

Figure 28 Cable route with alarms

Links, of the Cable Route, in alarm

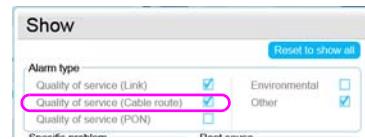
Cable Route in alarm

The screenshot shows the "Cable route dashboard - CR-Roma-1" interface. It includes sections for "Information" (Cable route: CR-Roma-1, Total number of links: 3, Number of links in alarm: 1), "Links and active alarms" (listing three links: 100, 101, 102, where link 102 is highlighted in red), and an "Alarm viewer" (showing three alarms for link 102 with IDs 37, 38, and 39, all critical, created at 2023 Jan 27 14:27:13, last updated at 2023 Jan 27 14:32:51, severity: Critical, origin: LK-R-102-CH-1, specific problem: Attenuation, additional test: ATTENUATION, description: Attenuation (test: test1) - 1,000.00 m, Attenuation (test: test2) - 1,007.00 m, and Cable degradation, status: SCAN_COMPLETED). A context menu is open on the right side of the dashboard.

NOTE

An alarm notification is sent by e-mail if the parameter **Notify Alarm Type: Quality of Service (Cable Route)** is selected in the **System Settings** screen. See “[Defining filters for the e-mail notifications](#)” on page 185.

In Alarm viewer, click on **Filter** to filter the display of the table and add the Cable route alarms if not already selected.



The Cable route is displayed in alarm:

- the icon  identifies the Cable Route
- the Cable Route alarm type is «Cable Degradation».

The links in alarm are displayed above the Cable route

- the icon  identifies the links
- the specified problem is described for each alarm (example: Attenuation)

OTU Scans

Automatic scan

If an alarm exceeds the severity threshold **Major**, the OTU starts automatically a scan of all the fibers of the Cable Route.

Figure 29 Scan in progress



If one new defect is detected on fiber, a new alarm is raised and appears in the Alarm table.

Manual Scan

A manual scan on the OTU can be performed by the user at any time:

- 1 From the Cable Route dashboard, click on Scan Now button  .
A confirmation is required.

Click on the icon  to display the scan detailed information:



The scans starts, and if a defect is detected on one fiber, an alarm is raised and displayed in the **Alarm** table (see [Figure 28 on page 31](#)).

Alarm details

Once a link is in alarm in the Cable Route:

- Click on this Cable route to display the alarm details screen for this cable route.

Figure 30 Alarm details of a Cable route

- Click on one link to display the alarm details for the link.

Figure 31 Alarm details of a link

Ports & Links Field Application

The Ports & Links Field application is dedicated for monitoring and testing for technicians on the field.

Use the field application to:

- Launch test of a link
- View results of the test
- Display the status of the links

The Field application does not allow to create, edit or remove new items.

Opening the Ports & Links field application

The field application is available from the URL: `https://<server address>/m/`.

The user must have the appropriate permissions for using the field application.

- 1 In the **Home** page, press **Ports & Links**.

The list of ports and links displays:



port with link



port without link

- 2 Click on and apply filters to the list.

- 3 Click on to return to links display, with filter(s) applied.

Figure 32 Ports & Links application

The screenshot shows the 'Ports & Links' application interface. On the left is a 'Filter configuration' sidebar with fields for Alarm ID, Domain SD, OTU, Cable head, Link, Severity (Warning selected), and a checkbox for 'and above'. In the center is a main list titled 'Ports & links' showing links: FO STE-LYS 09, FO STE-LYS 10, FO STE-LYS 11, FO STE-LYS 12, otu-8000e-10548 / OS(015), and otu-8000e-10548 / OS(016). On the right is an 'Actions' sidebar with options: Refresh, Sort by OTU/port (selected), Sort by name, Sort by severity, and Sort by duration.

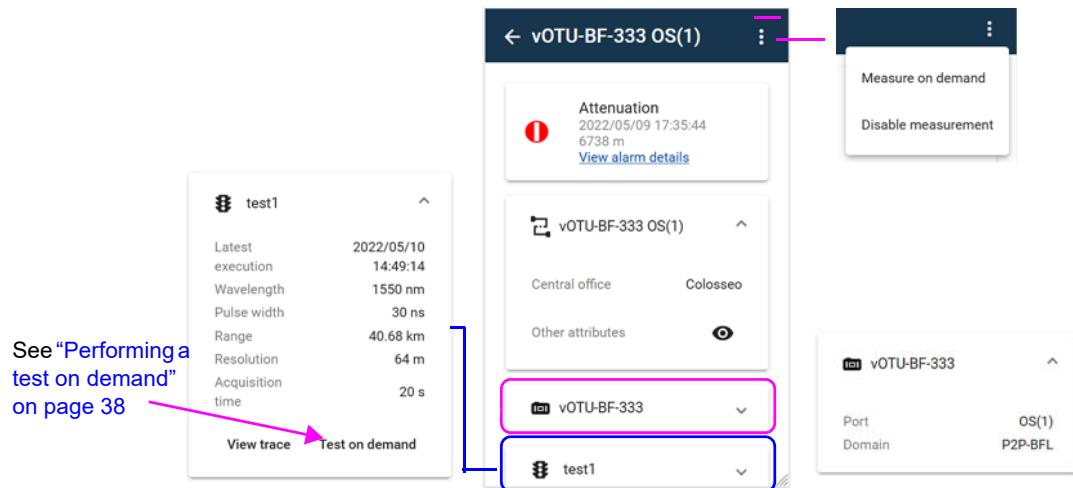
Click on to open the menu and refresh the display or to sort the list according to specific features (OTU/port, severity...).

Click on one link to display details for this link, perform test and measurements, see results trace...

Details of the link

Click on one link to display the details relating to this link:

Figure 33 Link details



If an alarm is detected on the link, it is displayed on the upper part of the screen.

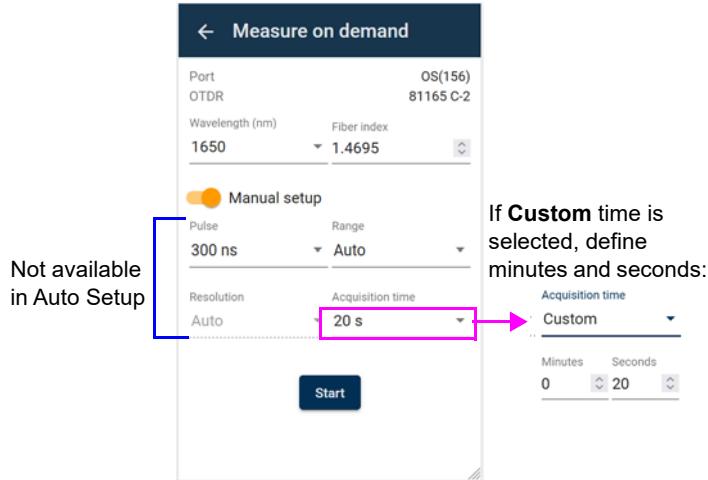
Click on the alarm date to replace it with the number of days since the alarm occurred (and vice versa): 2022/05/09 17:35:44 <-- click--> > 9 days 16 hours .

Performing a measure on demand of the link

- 1 In the Link details view, click on > Measure on demand.
or
From the trace view menu, click on **Measure on demand** (see [Figure 39 on page 38](#)).
- 2 In the new window, modify the measurement parameters if necessary:
- 3 Click on **Manual Setup** to manually configure the measurement and have access to other parameters
- 4 Press **Start** to launch the measure.

The measurement is launched, using the parameters defined in the setup window and an alarm is generated in case of fiber cut (severity: critical).

Figure 34 Measure on demand



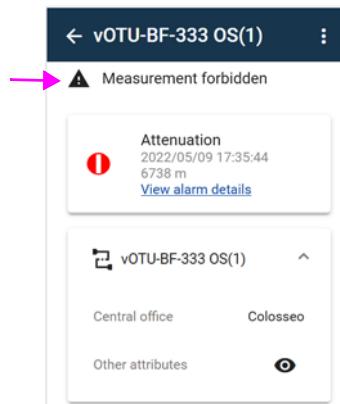
Disabling the measurements on link

Once the link details are displayed, the measurement on this link can be forbidden:

Open the Link menu and click on **Disable measurement** (see [Figure 33 on page 35](#)).

A message displays on the upper part of the link view:

Figure 35 Measurement disabled on the link



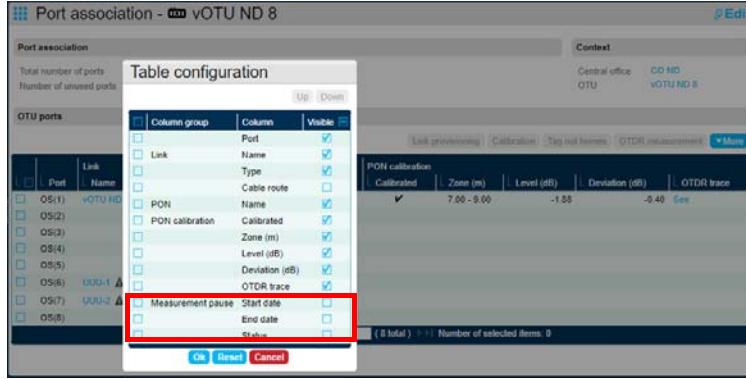
Return to Link menu and select **Enable measure** to re authorized the measurement on the link.

Scheduling a pause period

The user can define a period when monitoring/measurement will not be executed on a specific port (for ex, when a maintenance is scheduled on a fiber).

- On the **Port Association** window, the required fields must first be displayed from the **Table Configuration** window: select the required fields from **Measurement pause** section.

Figure 36 Table configuration



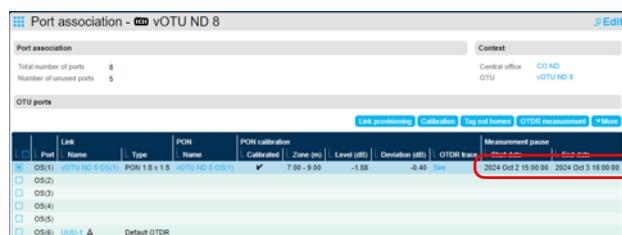
- Add a pause period: right click on the port and click on **Add Measurement pause**.
- In the new dialog box, define the **Start date** and/or the **End date** (according to fields previously defined in the Table configuration).

Figure 37 Defining pause period



- Click on **Save** to validate.

Figure 38 Pause period defined on measurement

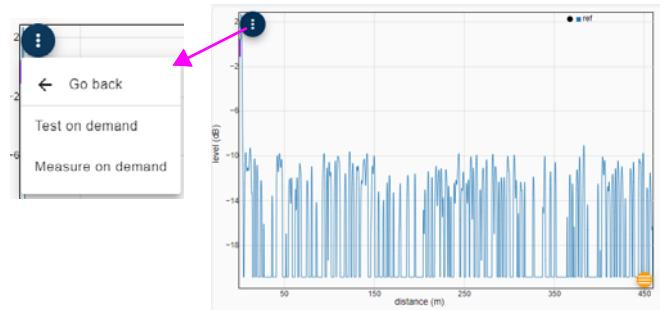


- During a Pause period, the port will be on "measurement Forbidden" status
- Once the pause period is over, it disappears from the screen and the monitoring resumes.
- Only one measurement period per port at a time can be defined.

Displaying a trace from the tested link

Once the link details are display, click on the **View trace** button in the test window to display the results trace of the link.

Figure 39 Trace view



Click on the button to open the sub-menu and access to the different actions available.

- Click on **Go Back** to return to Link details screen.
- Click on **Fit to content** to adjust the trace to the screen size.

Click on the icon to open the Zoom sub-menu and modify the view using the zoom features available.

NOTE

For a better visibility of the trace, set your device to landscape mode.



Performing a test on demand

- 1 From the trace menu, click on **Test on demand**.
or

From the Link details window, open the test menu and click on **Test on demand** button (see [Figure 33 on page 35](#)).

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

During the test, a Loading bar displays:



Displaying the alarm details

If an alarm has been detected on the link, click on **View alarm details** in the link details screen, to display the alarm information.

Figure 40 Alarm details

Attenuation	
Threshold crossed	
Cleared	No
Acknowledged	No
Link	vOTU-BF-333 OS(1)
GPS	41° 55' 0.44" N 12° 27' 17.82" E
OTDR Distance	6738 m
From	Piazzale Clodio: 37 m
To	Parco Tor di Quinto: 3860 m
Creation	2022/05/09 17:35:44
Update	2022/05/18 14:54:56
Deviation from reference	
First marker	0.12 dB
Link loss	3.40 dB
At fault location	-15.00 dB
Information	
Alarm ID	45
Alarm type	see "Adding a comment" on page 40
Description	
Last comment	
Quality of service	Fiber cut
	OK

If the alarm is localized on a map, click on the GPS coordinates displayed to visualize it on the map configured (Google Earth, Google Map...).

Acknowledging or clearing the alarm

To acknowledge/clear the displayed alarm, open the alarm menu and click on **Acknowledge / Clear**.

- If the alarm is acknowledged, the alarm icon is displayed with a tick
- If the alarm is cleared, the alarm icon is grayed out

In both cases, the status is modified to **Yes**:

Cleared

Acknowledged

Yes

Yes

Open again the Alarm menu and select **Unacknowledge / Clear** to reset the alarm.

Adding a comment

To add a comment to the alarm, click on **Add comment** in the Alarm menu.

Modify/enter a comment and press **Ok**.

The comment is visible in the Information view of the alarm (see [Figure 40 on page 39](#)).



Displaying the otdr trace of the alarm

To display the otdr results trace from the link with alarm, click on **View OTDR trace** in the alarm menu.

The trace is open, with the alarm icon displayed on trace.

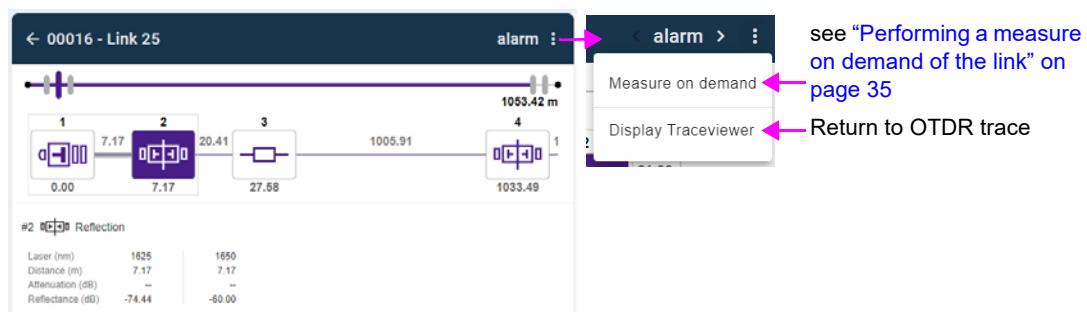
Figure 41 OTDTR trace



Displaying the SLM view of the link in alarm

To display the SLM view from the link with alarm, from the OTDR trace view, click on **Display SLM view**.

Figure 42 SLM view



If there are several SLM traces, switch from one to another clicking on the buttons around the trace name, in the header bar.

Displaying the history of the alarm

To display the history of the alarm, from the day when the alarm occurred until now,:

Open the alarm menu (from Alarm details view, see [Figure 40 on page 39](#)) clicking on  and click on **History**.

Figure 43 Alarm History

← History		
 Cleared : No Acknowledged : No	2023/05/02 11:25:13	admin
 Cleared : No Acknowledged : Yes	2023/05/02 11:24:33	admin
 Cleared : No Acknowledged : No	2023/07/08 16:32:00	admin
 Cleared : No Acknowledged : No	2023/06/15 14:07:30	admin
 Cleared : No Acknowledged : No	2023/05/09 10:44:13	Fiber cut
 Cleared : No Acknowledged : No	2023/06/09 10:41:11	
 Cleared : No Acknowledged : No	2023/06/09 10:41:03	

Displaying the alarms

This chapter provides a description of the Alarms viewer.

Topics discussed in this chapter include the following:

- [“Alarms view” on page 44](#)

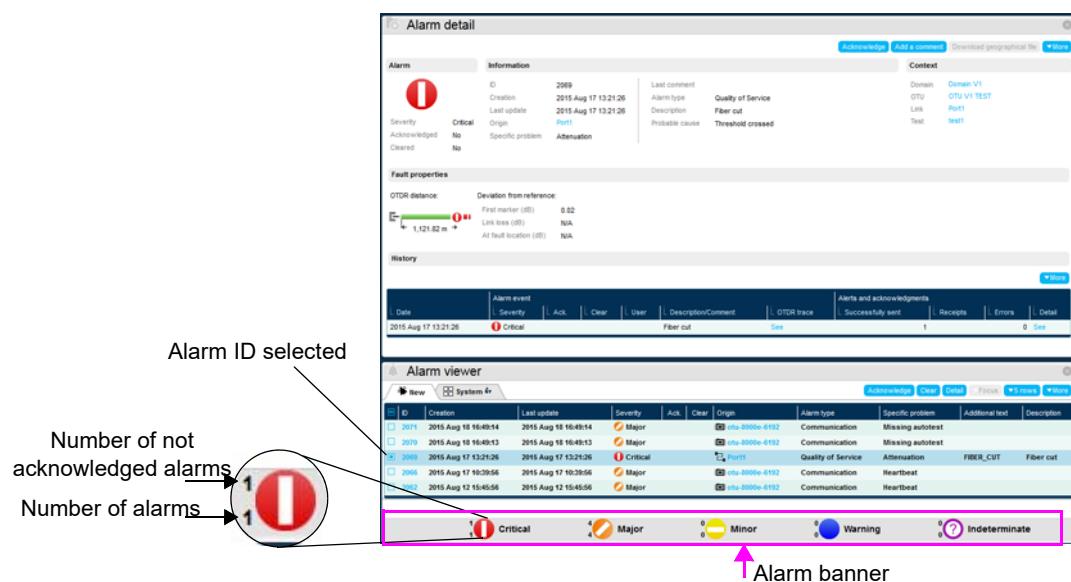
Alarms view

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 44 Alarm window



Trace Viewer

This chapter provides a description of the possible actions on traces, whether they are open via the Trace Browser.

Topics discussed in this chapter include the following:

- “Opening a trace using the Trace Browser” on page 46
- “Trace display” on page 47
- “Multi-trace display” on page 51

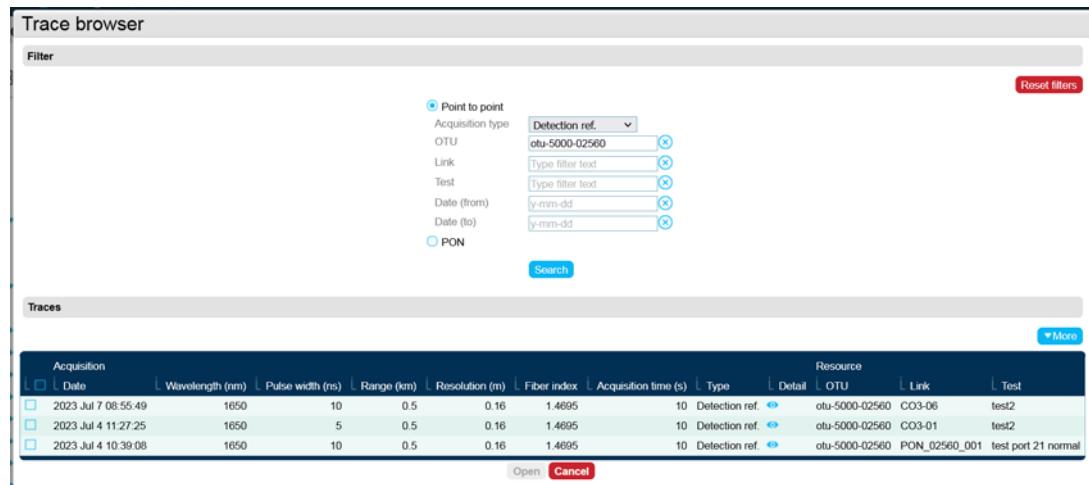
Opening a trace using the Trace Browser

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 45 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 46 Trace viewer



Trace display

Once a trace is displayed, 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

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

Figure 47 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 26 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 48 A & B tool bar



- 2 Before positioning a marker, make a zoom on trace if necessary (see “[Zooming on trace](#)” on page 47)
- 3 Click on the **A** icon and click on the trace where the marker must be positioned.
- 4 Click on the **B** 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 **AB**.

Figure 49 Trace with A and B markers



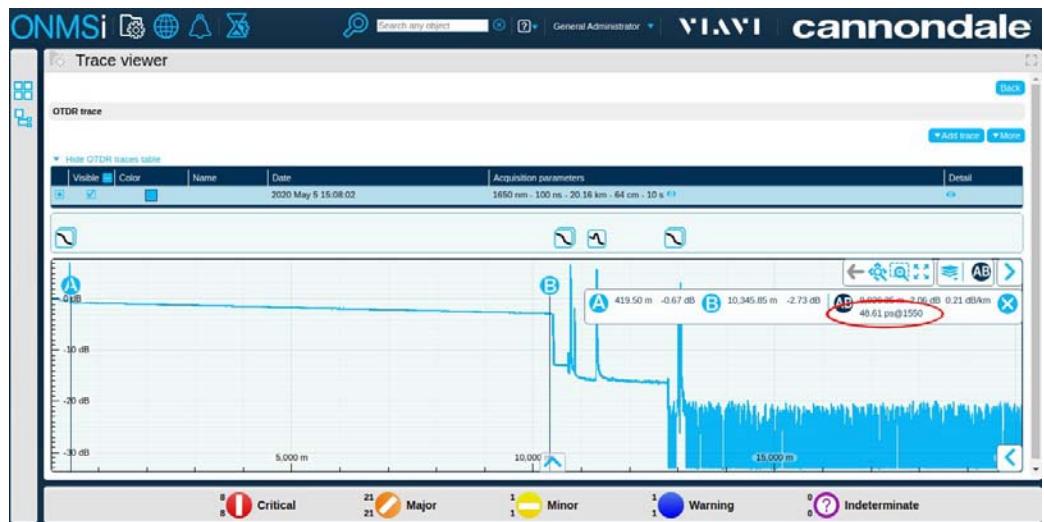
Optical events

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

Latency measurement

On the OTDR trace, the latency measurement is the distance between the 2 markers A & B, in time and not in distance, for the traffic wavelength, which can be different from the otdr measurement wavelength.

Figure 50 Latency measurement



To calculate this latency measurement, the ONMSi must be configured with the traffic wavelength (1500 nm by default) and the corresponding fiber index: see “[Point to Point General configuration](#)” on page 180).

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 51 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.

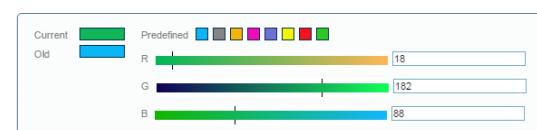
Figure 52 Event details



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

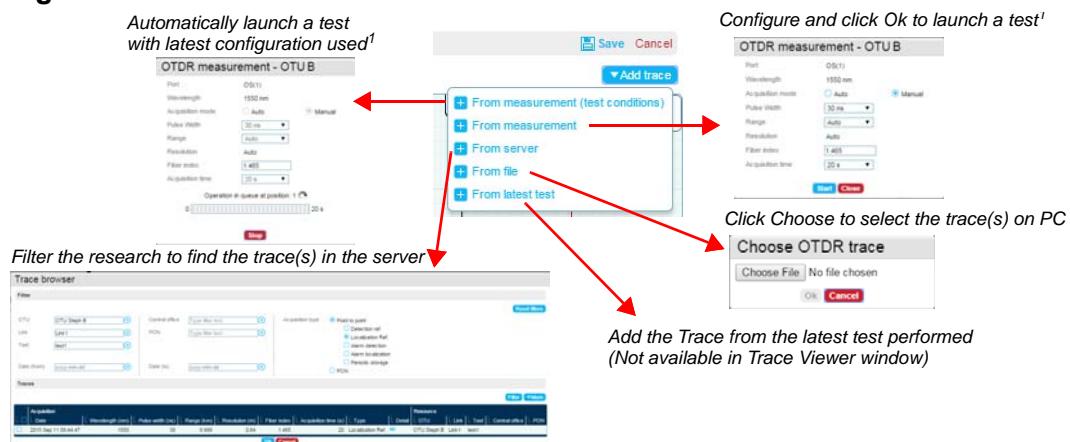
From the Trace Viewer or from a test result, you can add traces to the existing one, and then get several traces displayed in the same window.

Adding trace(s)

Once a trace is displayed, click on **Add trace** button

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

Figure 53 Add Traces sub-menu



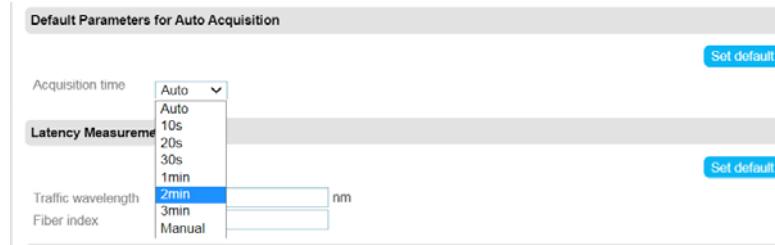
Note on OTDR acquisition time

The OTDR acquisition time can be defined to **Auto**, in which case the acquisition is defined to be performed for 20 seconds.

To modify the automatic acquisition time for otdr measurement:

- 1 Go to **System Settings > Point to Point** (see [Figure 210 on page 181](#))
- 2 Click on **Edit**.
- 3 In the **Default parameters for Auto acquisition** window:
 - Select a pre-defined acquisition time: **Auto / 10 s / 20 s / 30 s / 1 min / 2 min / 3 min**
 - or
 - Select **Manual** and define the automatic acquisition time: Min 5 seconds / Max: 5 minutes

Figure 54 Modification of the acquisition time



- 4 Click on **Save** to validate.

All the otdr acquisitions performed with acquisition time defined to **Auto** will be performed with the time defined in System Settings screen.

Multi-traces display

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

Figure 55 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 56 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 56
- “[Defining the system and domain roles for the user](#)” on page 60
- “[Changing the current user preferences](#)” on page 63
- “[Displaying the connected users](#)” on page 65

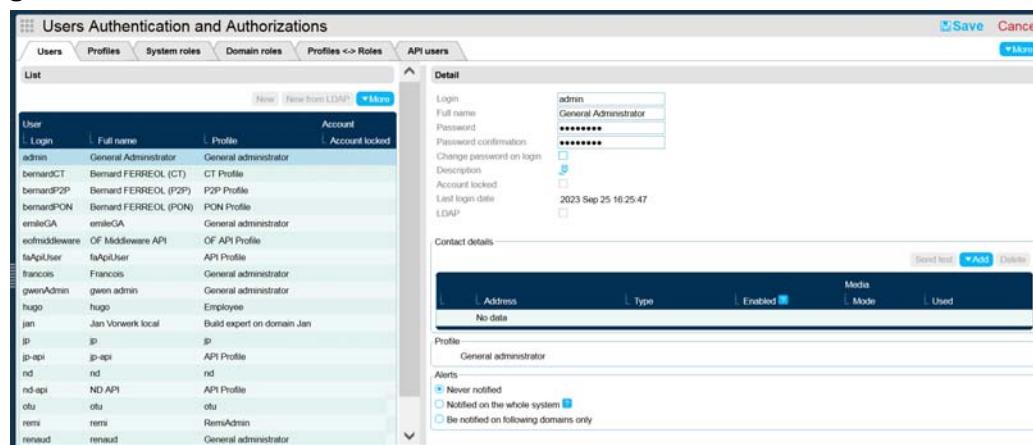
Adding a user

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 57 Creation of a «standard» user

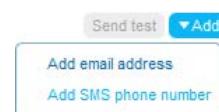


Details

- 1 Enter the parameters of the new user: **Login / Full name / Password confirmation**
- 2 If wished, click on the **Description** icon and enter a detailed description of the user in the dialog box.
- 3 Enter the password, and if necessary, select **Change password on login** to modify the password at first login of this user.
- 4 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 187).
- 5 Select if this user has an **Account Locked**: the user still exists but he cannot access anymore to the system.
- 6 Select the parameter **LDAP** to add this user to the LDAP and ONMSI server.

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 58 Contact details

Address	Type	Enabled	Media	Used
<input type="checkbox"/> jhondoe@viavisolution.com	Email	<input checked="" type="checkbox"/>	Use with default media	STE Exchange
<input type="checkbox"/> +33 626250174	SMS	<input checked="" type="checkbox"/>	Use with default media	▲

Profile

In the **Profile** window, click in the **Profile** text box and select the Profile to assign to the new user.

Alerts

Figure 59 Alerts

Alerts

- Never notified
- Notified on the whole system
- Be notified on following domains only

Domains	Available domains	Selected domains
	Alert test BPA Cust Domain V2 JP	

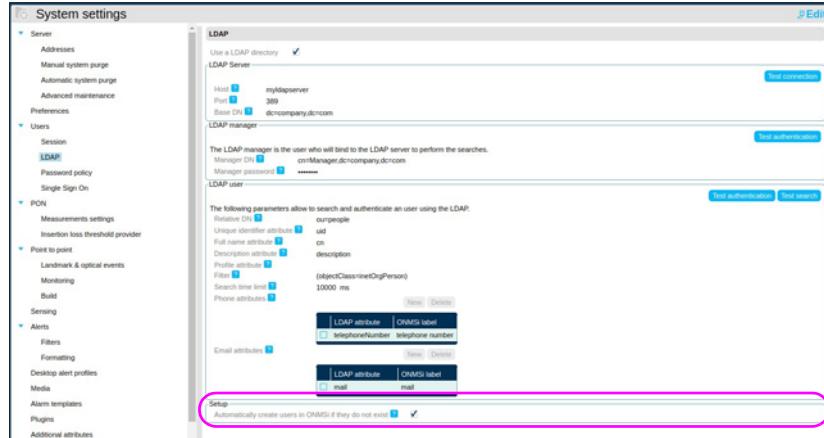
Filter Escalation user

- 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.

Automatic users' creation

If the checkbox "Automatically create users in ONMSI if they do not exist" is checked in the LDAP configuration screen:

Figure 60 «Automatically create users» parameter



when a user existing in LDAP connects to ONMSI for the first time and is not declared in ONMSI, he will be automatically created in ONMSI.

A profile will be assigned to the user from one of his LDAP attributes.

If the attribute is known to be unique for the user, its value can be used (with the default LDAP profile extractor) as the ONMSI profile name. The default LDAP extractor should be selected here

Figure 61 Default LDAP extractor



If that attribute can have multiple values for the user in the LDAP, then a custom profile extractor plugin must be used (please contact ONMSI support).

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)

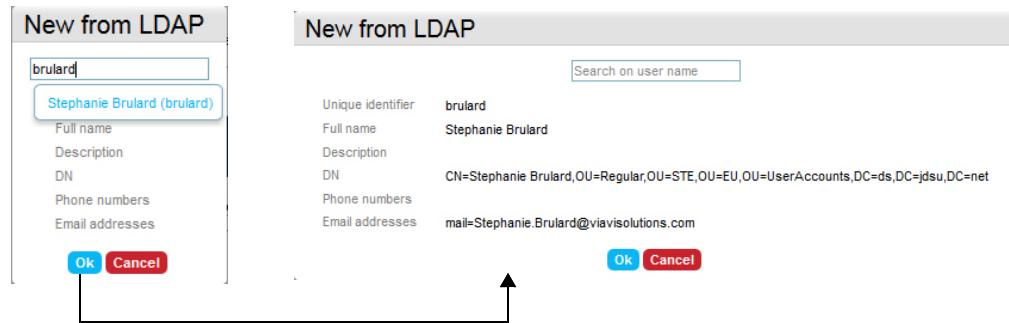
LDAP configuration details must be given by a person familiar with the directory. To get information on LDAP configuration, see "[Configuring the LDAP](#)" on page 170.

- 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 62 Adding a user from the LDAP



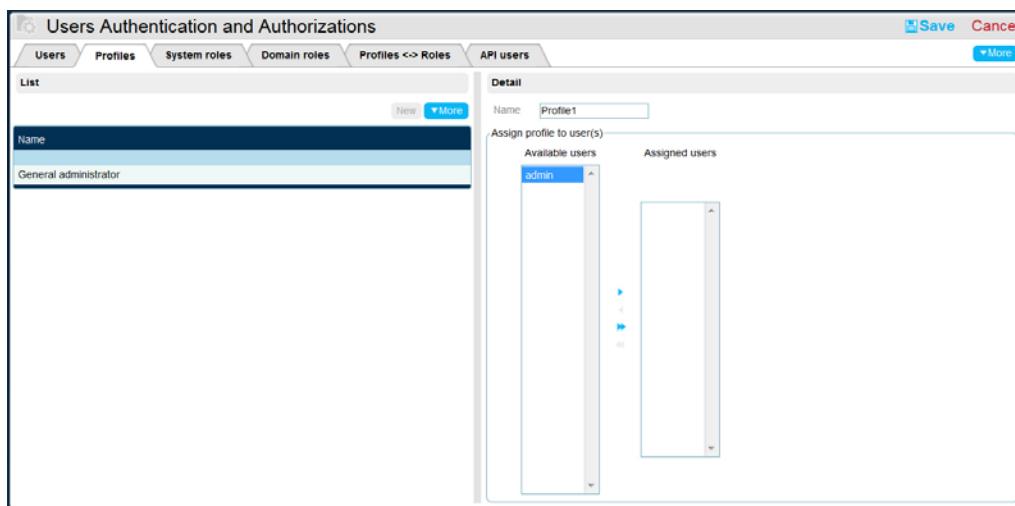
- 6 Click **Ok** to confirm the user to be added to ONMSI
- 7 The Details window is fulfilled with the user parameters used in its company.
- 8 In the Contact Details window, the e-mail and phone number will be automatically proposed if they are defined in the LDAP company directory.
- 9 Follow instructions from [step 1 to step 2 on page 57](#) to complete the addition of a user from LDAP.

Creating Profiles

Several profiles can be created, grouping roles on domains and on systems, so that users are assigned to a profile, and not only to one role.

To add a Profile 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 Select the **Profile** tab.
- 3 Press **New** button from the Profile tab to create a new Profile.

Figure 63 Creating a Profile

- 4 Enter a **Name** to this new profile
- 5 From the **Available users** list, select the user(s) to assign to the new profile. Maintain **Ctrl** key pressed to select several users.
- 6 Click on / to pass the selected user(s) to **Assigned users** box.
- 7 Click on **Save** to save the new Profile.

**CAUTION**

The Profile «General Administrator» must be defined with at least one user.

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
• API operator	• Domain administrator
• Data administrator	• Expert
• General administrator	• NOC

System built-in roles	Domain built-in roles
• P2P operator	• Observer
• PON operator	
• Test supervisor	

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 64 Create a System/Domain role

The screenshot displays the 'Users Authentication and Authorizations' screen with the 'System roles' tab active. The 'Detail' pane on the right shows the configuration for the 'API operator' role, listing its permissions under 'Built-in Permissions'. These permissions include various system and network management tasks such as managing domains, connecting to Web and API applications, and configuring system pinboards. The 'Included roles' section lists the 'Domain administ' role. The 'Domain roles' pane on the right lists several built-in roles: 'Domain administrator', 'Expert', 'NOC', 'Observer', and 'otu'. The 'Available roles' dropdown also lists these roles. The bottom of the screen includes a note about granting permissions to view all resources.

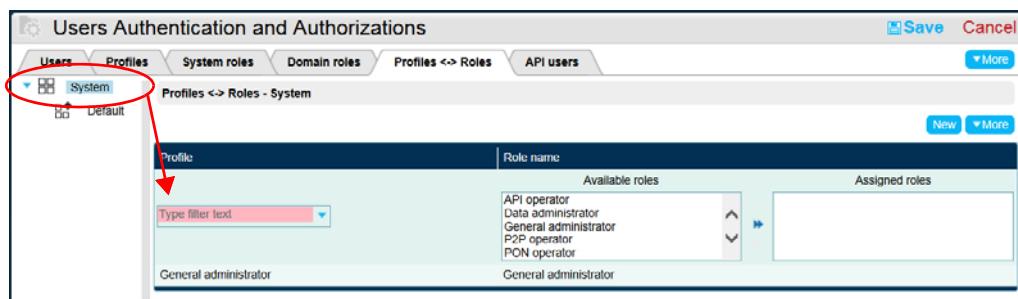
In the System roles, the “Manage domains” gives privileges on ALL domains. If you provide this privilege to a user, you do not need to assign domain roles to this user.

Assigning System roles to a Profile

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

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

Figure 65 Assign a System role



- 4 Select the Profile 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 profile 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.

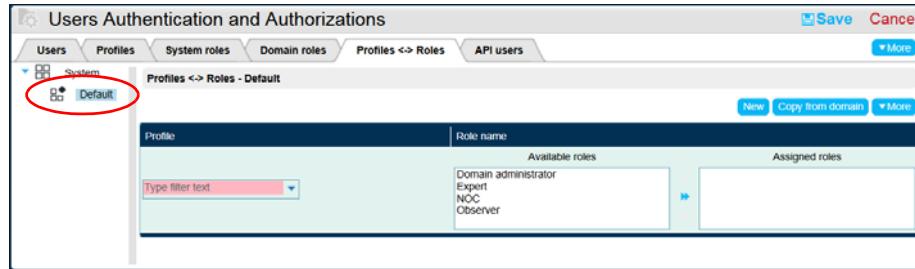
Assigning Domain roles to a profile

Once the profile, with user(s) assigned, is created, open the **Users Authentication and Authorization** page and:

- 1 Click on the tab **Profiles <-> Roles**.
- 2 Select a **domain** in the left screen.

- 3 Click on **New** button

Figure 66 Assign a Domain role



- 4 Select the **Profile 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 Domain roles assignation

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

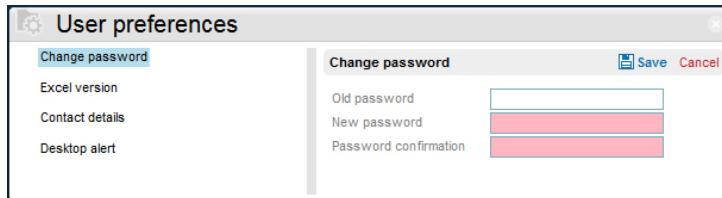
Changing the current user preferences

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 67 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**.
- 3 Select **Excel version** on the left of the screen
- 4 Press **Edit** to modify the version.

Figure 68 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.

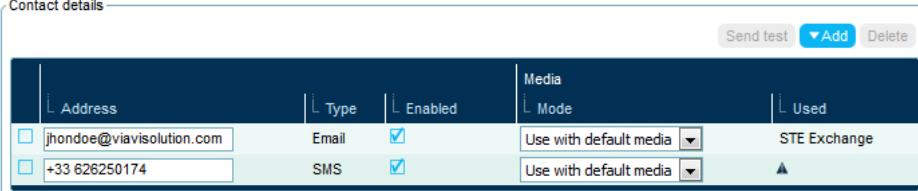
Modifying the notification address

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 69 Contact details



Address	Type	Enabled	Media	Used
jhondoe@viavisolution.com	Email	<input checked="" type="checkbox"/>	Use with default media	STE Exchange
+33 626250174	SMS	<input checked="" type="checkbox"/>	Use with default media	▲

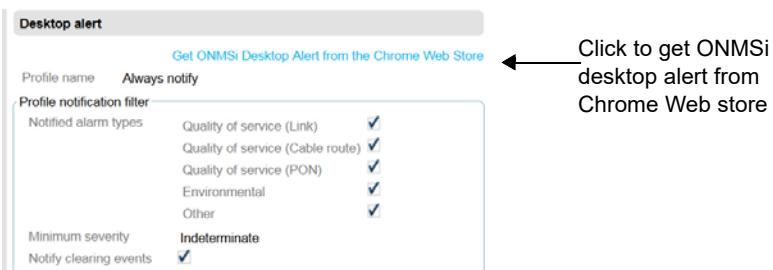
- 8 Select if the email / sms is enabled or not
- 9 In the **Mode** sub-menu, select if the address must be used:
 - with default media. The media is automatically displayed in the **Used** parameter
 - with specific media, in which case, the media will be modified in the **Used** parameter
- 10 Press **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 70 Desktop alert window



See “Configuring Desktop alert profiles” on page 187 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 71 List of connected user

The screenshot shows a window titled "Connected users". At the top, it displays "Remaining connections: 8". Below this is a table with the following data:

Login	Full name	IP address	Logged in since	Keep me connected
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	<input type="checkbox"/>

At the bottom right of the window are "Refresh" and "Disconnect" buttons.

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 68
- “[Creating a domain](#)” on page 68

Domain principle

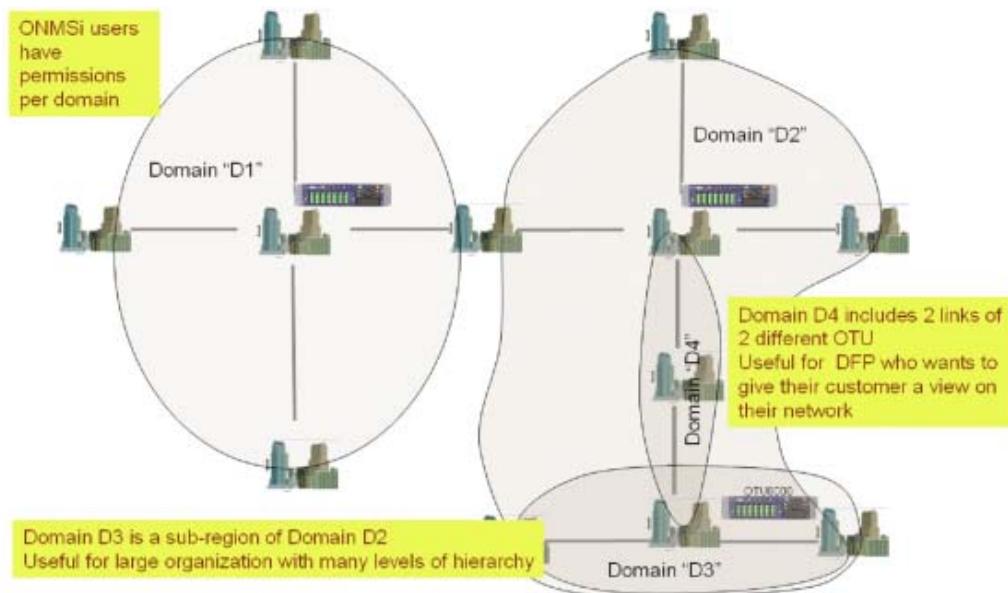
The ONMSi application allows to configure the flexible architecture of the network based on domains.

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 72 Domains architecture

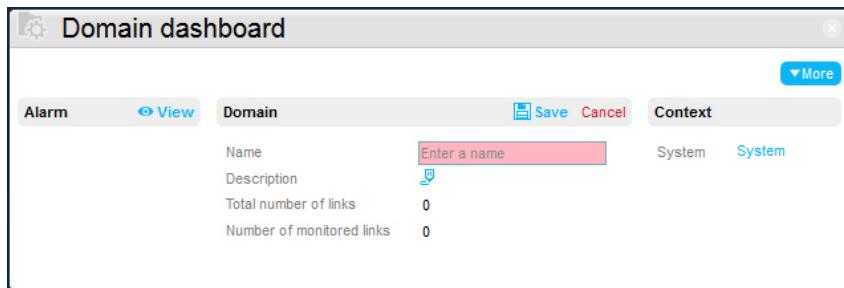


Creating a domain

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 73 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.

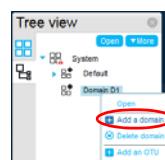
Figure 74 Domain created



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 69](#) 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.

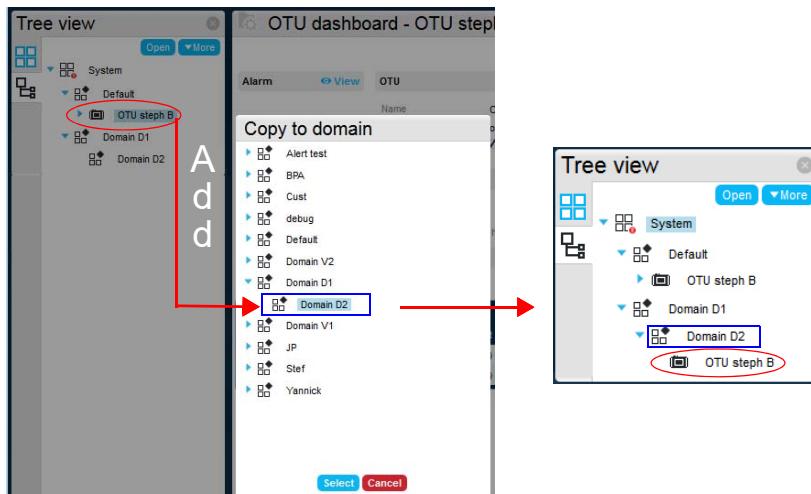
To add an existing OTU to a domain / sub-domain:

- 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 75 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

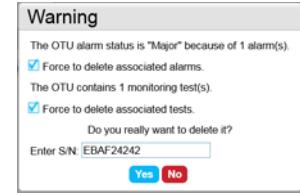
An OTU can be deleted from all the (sub-)domains it has been added:

- 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 Enter the Serial Number of the OTU to be deleted.
- 6 Click on **Ok**

The OTU is deleted from the system.



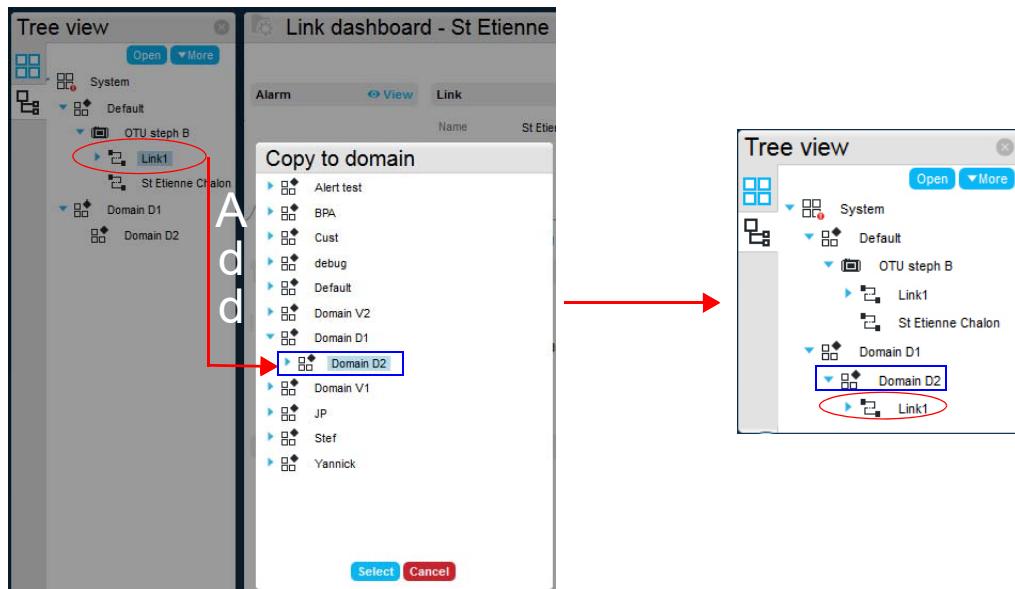
Copying a link to a domain

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 76 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 74
- “Advanced Monitoring” on page 78

Advanced Setup

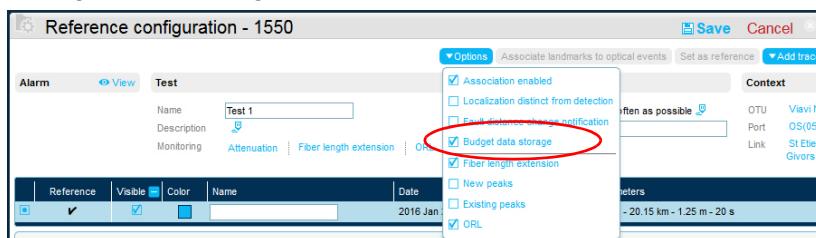
This chapter gives a description of the advanced parameters available for a link.

Downloading budget data (subject to license)

The data of the budget can be download in an Excel™ file.

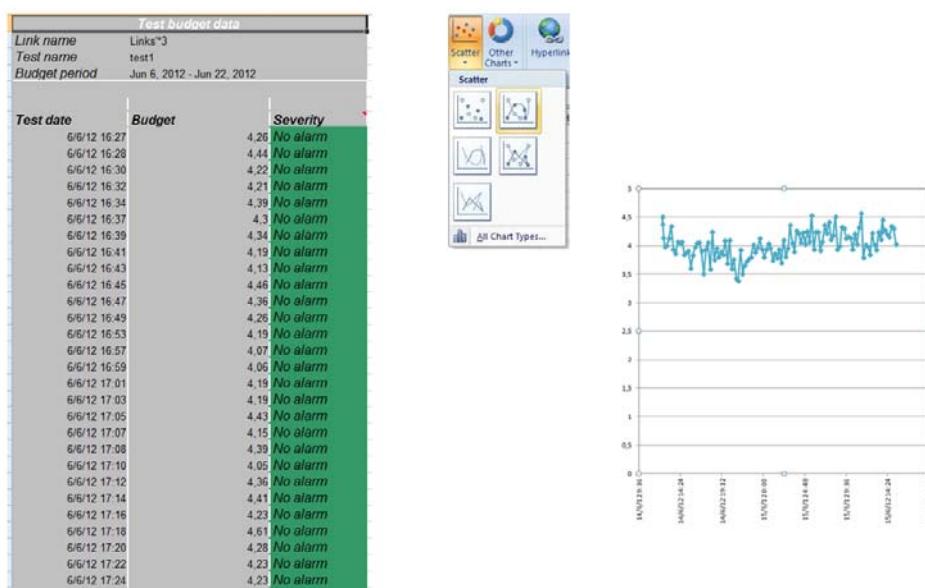
- 1 From the **Link dashboard** window, click on **Configuration & Reference** button.
- 2 In the Reference configuration window, click on **Edit**.
- 3 Select the parameter **Budget data storage**.
- 4 Press **Save** to confirm the selection.

Figure 77 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 78 Budget data in Excel format



Downloading landmark history

If the option **Periodical OTDR Trace storage** is available and configured with **txt format** for files saving (see “[Periodical OTDR Trace Storage option](#)” on page 77), reports can be generated, from the Landmarks available.

The report uses the txt files corresponding to the weekly maintenance trace.

It is saved outside the Database, in the path file defined in the configuration file of the option **Periodical OTDR Trace storage** (see “[Configuring the files path and name](#)” on page 77).



CAUTION

The tree structure in which the TXT/OTDR files are saved must not be modified, and the link names must remain the same.

- 1 From the Link Dashboard, click on the tab **Budget Graph**.
- 2 Click on **More**.
- 3 Click on **Download landmark history**.
- 4 In the dialog box opened, select the budget period or define it selecting the **Custom range...** parameter. In this case, enter the start/end dates for the report.
- 5 Click on **Ok** to validate

A txt report is generated and downloaded in the Web Browser.

The file can be opened using a spreadsheet program, such as Excel™, in order to get results in a table, using tab separator.

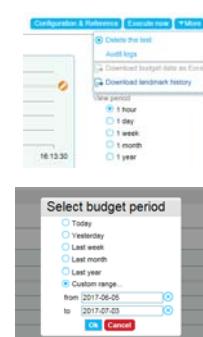


Figure 79 File open in Excel™

	A	B	C	D	E	F	G	H	I	J
1	OTU name	OTU HQ								
2	Link name	ViaVi2Sury Railway								
3	Wavelength (nm)		1625							
4	From	03/04/2016								
5	To	24/05/2016								
6										
7		05/04/2016	12/04/2016	19/04/2016	26/04/2016	03/05/2016	10/05/2016	17/05/2016	24/05/2016	
8	First Marker	-1,17	-1,17	-1,17	-1,17	-1,17	-1,17	-1,17	-1,17	
9	Last Marker	-8,3	-11	-10,9	-7,9	-8,3	-8,6	-8,5	-8,3	
10	Budget	-7,13	-9,83	-9,73	-6,73	-7,13	-7,43	-7,33	-7,13	
11										
12	VIAVI FR HQ	-10	-10	-10	-10	-10	-10	-10	-10	
13	Furan	-3,53	-3,59	-3,49	-3,53	-3,53	-3,83	-3,73	-3,53	
14	Bonson	-6,61	-6,6	-6,5	-6,21	-6,61	-6,91	-6,81	-6,61	
15	Sury	-8,4	-11,1	-11	-8	-8,4	-8,7	-8,6	-8,4	
16										



CAUTION

The application will NOT generate graphs. The user can select the lines he wants to create a graph under Excel for instance.

Scheduling a test

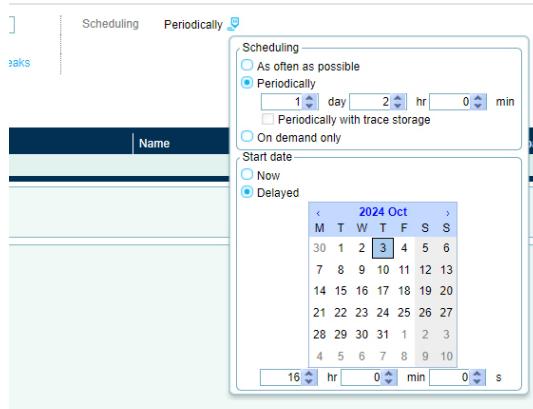
The **Scheduling** parameter allows to schedule the:

- 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 80 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



Periodical OTDR Trace Storage option

The license OTDR Trace Storage, available on option, allows to configure the storage of the OTDR traces scheduled periodically in another place than the ONMSI database:

- 1 Use Skipper to modify the configuration file settings.yaml

- 2 Add these lines:

```
onmsi:  
  trace-export:  
    path: /trace-export-path
```

where /trace-path-export is the absolute path on the server where the traces will be exported.

- 3 Run the following commands:

```
sudo rfts_configure  
sudo rfts_ctrl restart
```

- 4 Use Skipper to modify the configuration file /topaz/trace-export properties.

- 5 Configure the files saving

- 6 Save the file to validate the OTDR trace storage.

Configuring the files path and name

In the first part of the file, the path for files saving can be configured:

- Use one of the available template samples available and modify it as wished: remove the symbol # at the beginning of the sample and modify the path and the filenames, using the tags available.

Defining the files format

In the second part of the file, the format for files saving can be configured:

- Remove the symbol # at the beginning of the format(s) wished and keep the value as «true» to save the file with this format. If it is defined as «false» the files will not be saved to this format.



CAUTION

At least the path and the file format must be defined to get the parameter **Periodically with trace storage** in the **Scheduling** menu (see [Figure 81 on page 78](#)).

Modifying the Space management

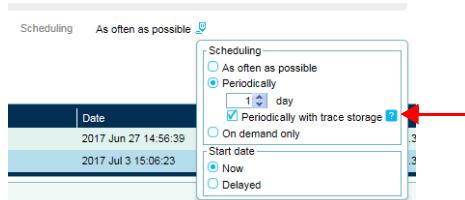
For the OTU name and Link name parameters only, the space can be managed from the file: the space can be replaced by the character «_» or the space can be removed (all characters will be attached)

- Remove the symbol # at the beginning of the space configuration wished.

- 7 From the Link dashboard, click on **Configuration & Reference**.

- 8 In the Reference configuration screen, click on **Edit**
- 9 In the **Scheduling** parameter, click on the icon  to modify the monitoring scheduling parameters.
- 10 In the **Scheduling** window, select:
 - **Periodically**: for a test at regular time interval
- 11 Select the parameter **Periodically with trace storage**.
- 12 Select the regular time interval:
 - Minimum period 1 day
 - Maximum period 999 days

Figure 81 Scheduling configured with OTDR traces saving



At each end of measurement, the otdr traces will be saved in the directory previously configured, with the file name previously defined.

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

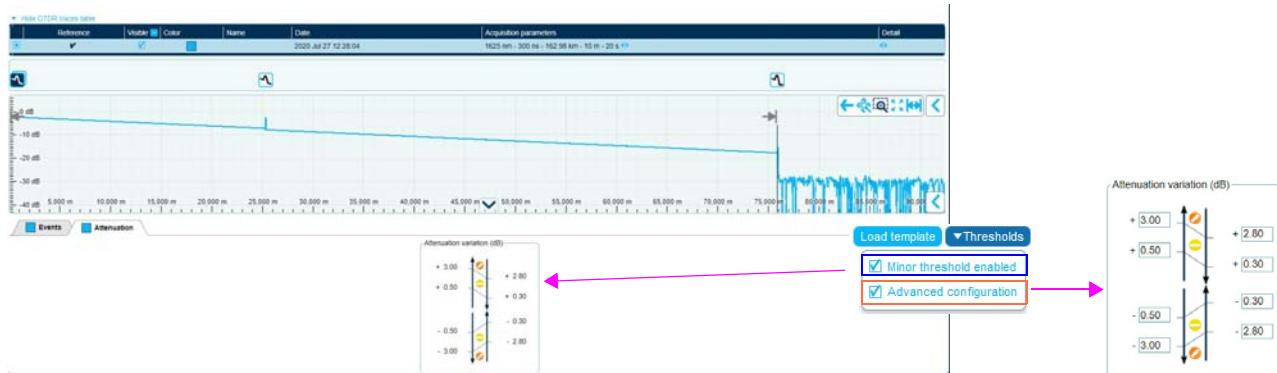
All those measurements can generate alarms except in case of critical alarms (fiber cut) or attenuation alarms.

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 82 Attenuation thresholds



- 4 Click on **Edit** to modify the attenuation parameters
- 5 Configure the threshold for the attenuation:
 - Define the maximum threshold for **Attenuation 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

Ref-Acq FM Level	Acq in noise	Ref – Acq Levels for all points between FM and LM	Severity	Type
< Minor	No	>= Minor (1dB) and < major (3dB)	Minor	Attenuation
	No	>= Major (3db) and < critical(6dB)	Major	Attenuation
	No	>= critical (6dB)	Critical	Attenuation
	Yes	>= critical (6dB)	Critical	Fiber Cut
>= Minor and < major	No	>= Minor (1dB) and < major (3dB)	Minor	Injection
	No	>= Major (3db) and critical(6dB)	Major	Attenuation
	No	>= critical (6dB)	Critical	Attenuation
	Yes	>= critical (6dB)	Critical	Fiber Cut

>= Major and < critical (6dB)	Any	Any	Major	Injection
>= Critical (6dB)	Any	Any	Critical	Injection



NOTE

With New monitoring and SmartAcq, FM is very close to the output of the OTU (few meters).

Alarm update conditions:

A new alarm localization is performed and an alarm update is triggered, on a link already in alarm, when:

- type of alarm changes
- or severity of alarm changes
- or alarm localization changes

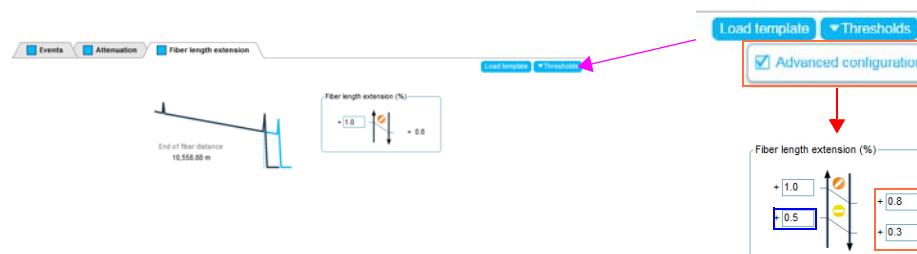
Fiber length extension

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.

Figure 83 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):
 - **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 84 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.

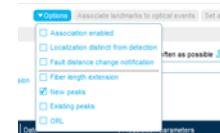
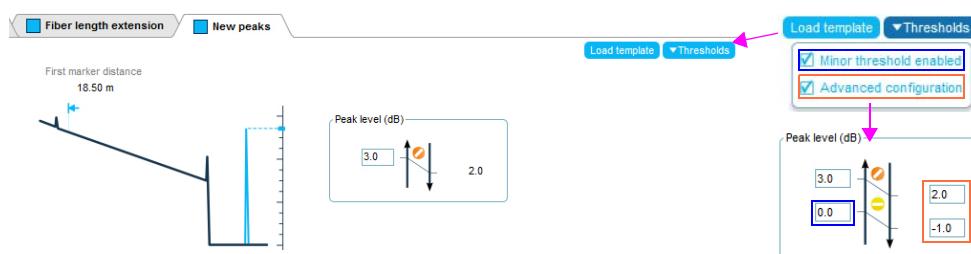


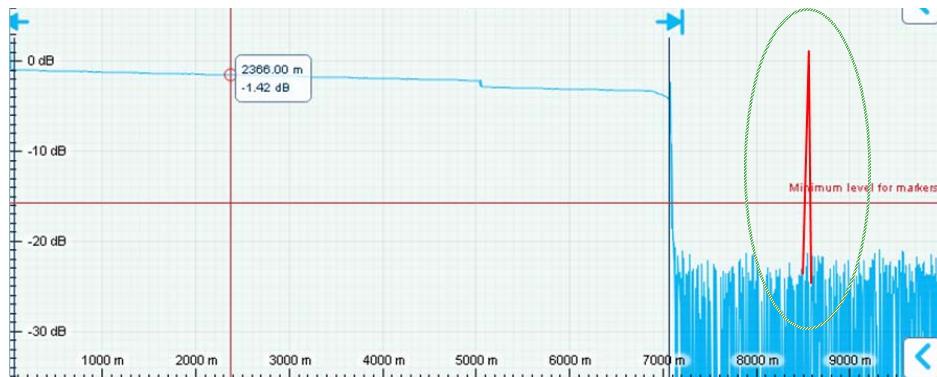
Figure 85 Thresholds for New Peaks



- 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 86 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 87 Alarm details for a new peak

Date	Alarm event	Severity	Ack.	User	Description/Comment	OTDR trace	Alerts and acknowledgments
2013 May 30 14:17:00	New peak	Major	No			See	0 / 0 / 0

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.

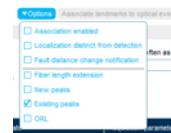
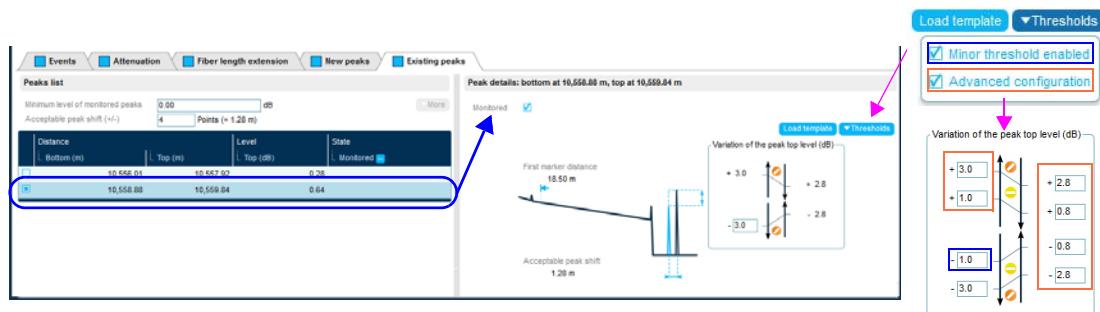


Figure 88 Thresholds for Existing Peaks



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

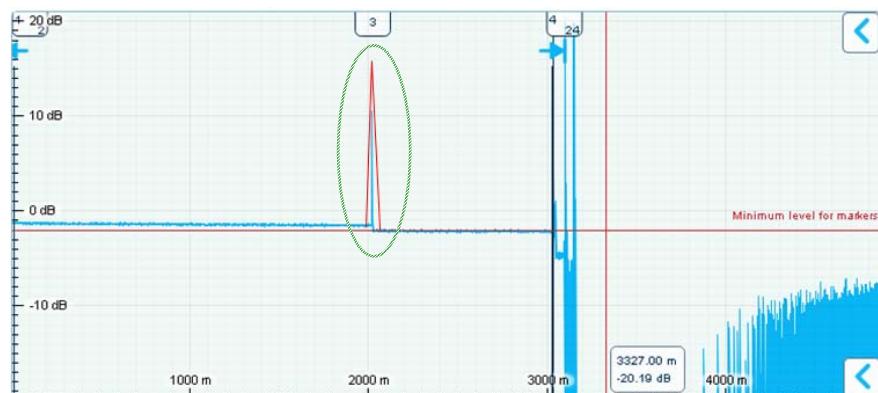
If necessary, modify this parameter in order to reduce/raise the list of peaks.

- 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 89 Existing peak



High Sensitivity Monitoring



NOTE

This function is available with an OTDR D Module (E81162D, E8115D) and the High Sensitivity license (E98-HS-MON) on OTU8000E.

The aim of this function is to detect faults of 0.1 dB or less. and locate very low attenuation change (0.1dB by default)

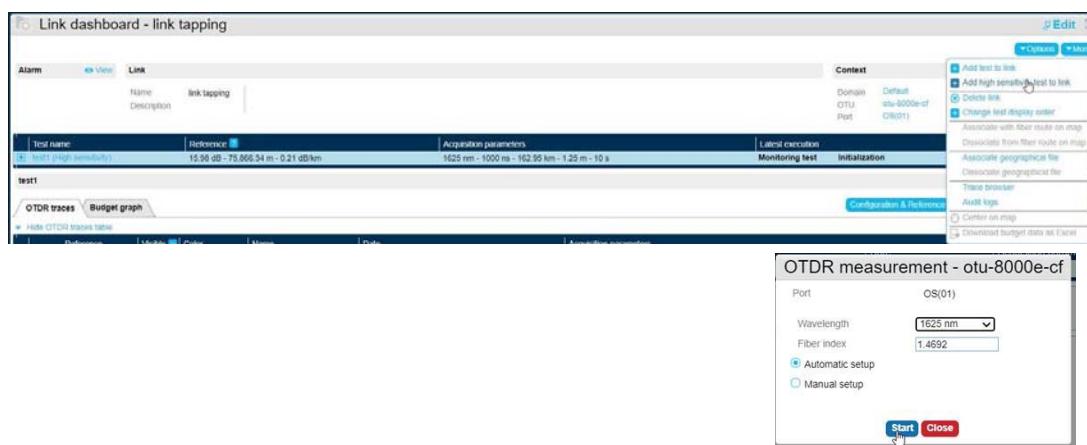
To configure the High Sensitivity monitoring test on a link:

1 Click on **Add high sensitivity test to link**.

A pop up window is displayed that proposes to setup the OTDR parameters automatically. Click on **Manual** to change it.

2 Click on **Start** to start the OTDR acquisition.

Figure 90 High Sensitivity monitoring test configuration



NOTE

For High sensitivity it is required to have the last marker 10dB above noise level. If it is not the case, a warning message is displayed and you should modify acquisition parameters (increase the pulse, example: 300ns -> 1μs, or decrease the resolution 1.20m -> 2.50m).

By default, with High Sensitivity monitoring, major threshold is set to 0.1 dB.

Figure 91 High sensitivity alarm thresholds



High sensitivity alarms have the same content as standard point to point monitoring alarms.

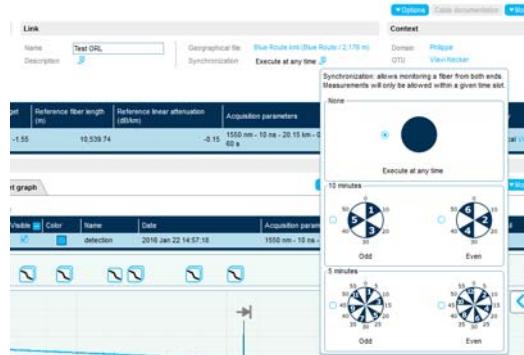
Figure 92 High sensitivity alarm details



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 93 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.



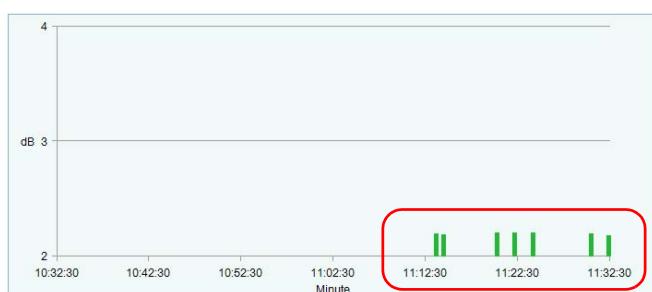
CAUTION

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 94 Budget with a time slot



Cable Documentation

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

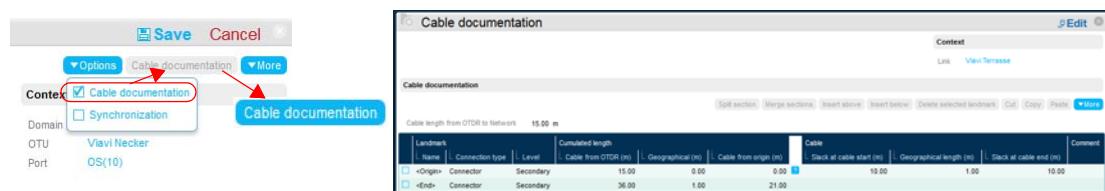
Activating the Cable documentation function

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 95 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**.

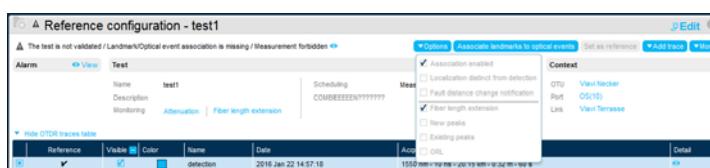
To validate the Association enabled parameter:

- 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 / Measurement forbidden** is displayed.

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

Figure 96 Option «Association enabled» selected



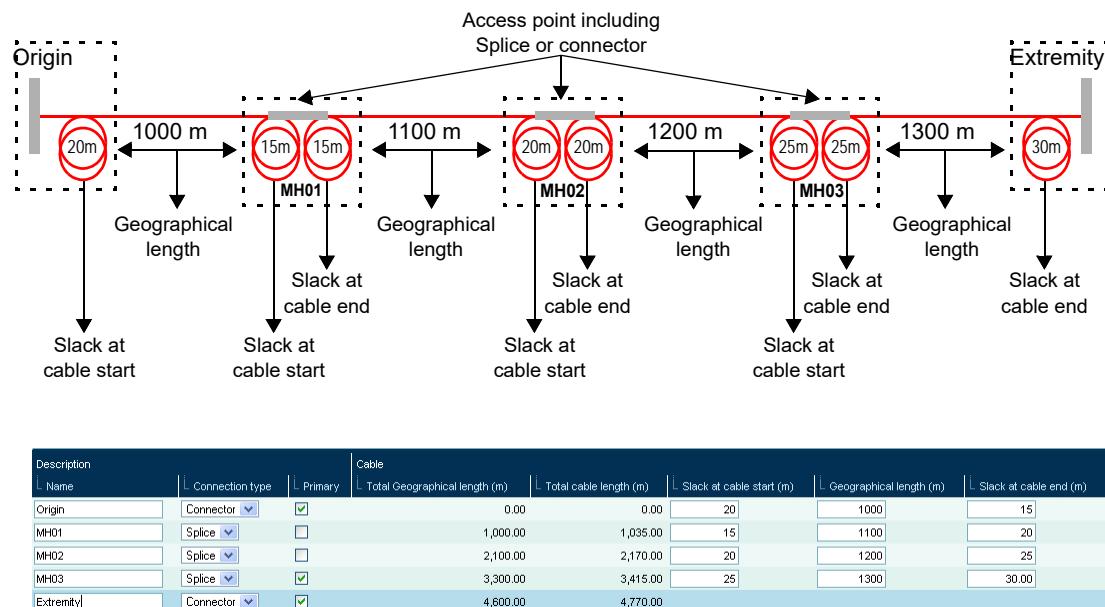
- 4 Click on the button to display the window «Associate landmarks to optical events» for the link selected.

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 97 Completing the landmark table according to the optical events

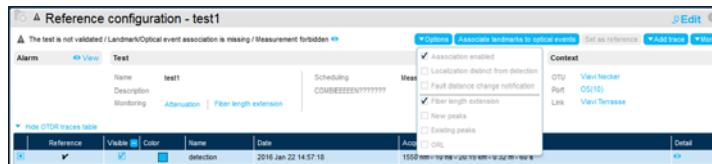


- 5 Click on **Save** to save the modifications.

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 98 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.

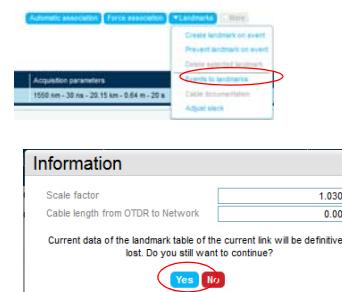
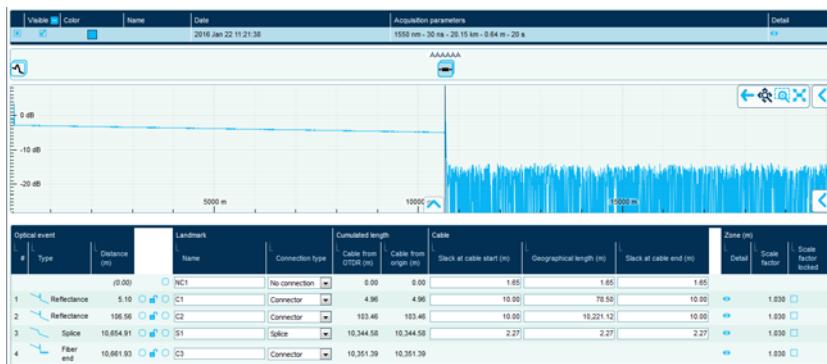


Figure 99 Landmark table and trace



- 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 100 Example of Excel file for landmark table

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

2 Upload the file from the Landmark table screen:

- a From the Link dashboard, click on Cable Documentation
- b In the Table window, click on **More > Upload from Excel**.
- c In the new dialog box select the excel file and click Ok to confirm.

The Upload results dialog box displays.

- d Click on **Close** to return to landmark table.



Upload result	
Added	4
Updated	0
Failed	0
Warnings	0

Associating Landmark and Optical Event

Once landmark table has been configured,

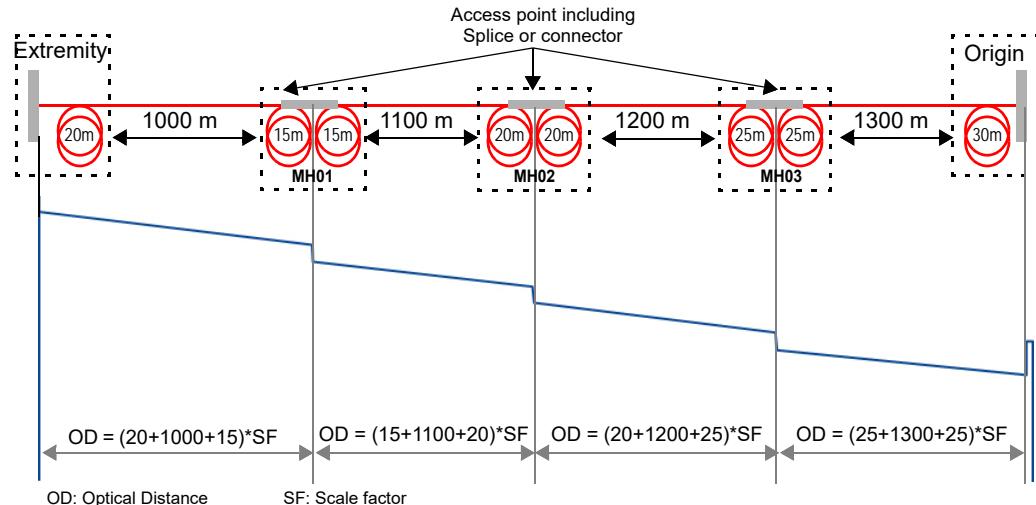
- 1 Return to Reference configuration window (for Link Dashboard, click on **Configuration & Reference** button).
- 2 Click on **Associate landmarks to optical events** button
- 3 Press **Edit** button

Figure 101 Table and trace before association



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

Figure 102 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 103 Force association

Associate landmarks to optical events									
Cable length from OTDR to Network <input type="text" value="10.00"/>			<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Adjust slack"/> <input type="button" value="Automatic association"/> <input style="outline: 2px solid red; border-radius: 10px; border: none; background-color: #e0e0e0; color: black; font-weight: bold; padding: 2px 10px; margin-right: 10px;" type="button" value="Force association"/> <input type="button" value="Dissociation"/> <input type="button" value="Create landmark"/> <input type="button" value="Delete selected landmarks"/> <input type="button" value="Landmark table"/> <input type="button" value="More"/>						
Optical event	#	Type	Distance (m)	Landmark	Name	Connection type	Cumulated length	Cable	Zone (m)
<input type="checkbox"/>				<input checked="" type="radio"/>	Origin	Connector	10.00	0.00	10.00
<input type="checkbox"/>				<input type="radio"/>	Extremity	Connector	31.00	21.00	1.00
<input type="checkbox"/>	1	Splice	5,046.85	<input checked="" type="radio"/>					10.00
<input type="checkbox"/>	2	Splice	7,011.36	<input type="radio"/>					1.00
<input type="checkbox"/>	3	Reflectance	7,065.07	<input type="radio"/>					10.00
<input type="checkbox"/>	4	Fiber end	8,078.03	<input type="radio"/>					1.00

Forced Association

Optical event	#	Type	Distance (m)	Landmark	Name	Connection type	Cumulated length	Cable	Zone (m)
<input type="checkbox"/>	1	Splice	5,046.85	<input checked="" type="radio"/>	Origin	Connector	10.00	0.00	10.00

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 91).

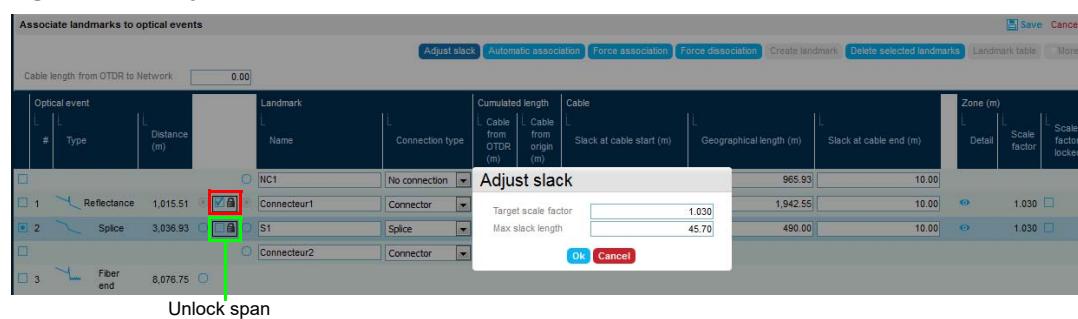
- If a landmark is still not matching properly, you can dissociate it:
 - Select both radio buttons
 - Click on **Force dissociation** to unlock the association

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 104 Adjust slack

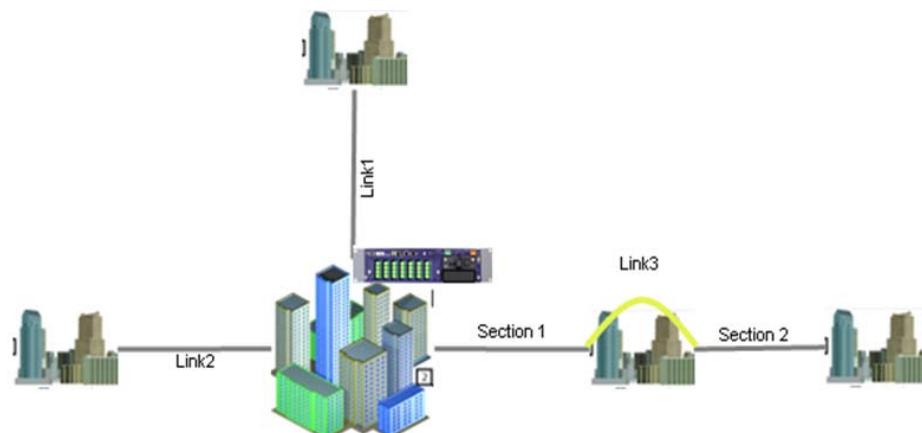


- 3 Adjust scale factor and max length if needed.
- 4 Click on **Ok** to validate.

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 105 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 106 Sections representation

Alarms on section

The section with alarm is displayed as faulty.

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

Figure 107 Alarm on section

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. KML 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.



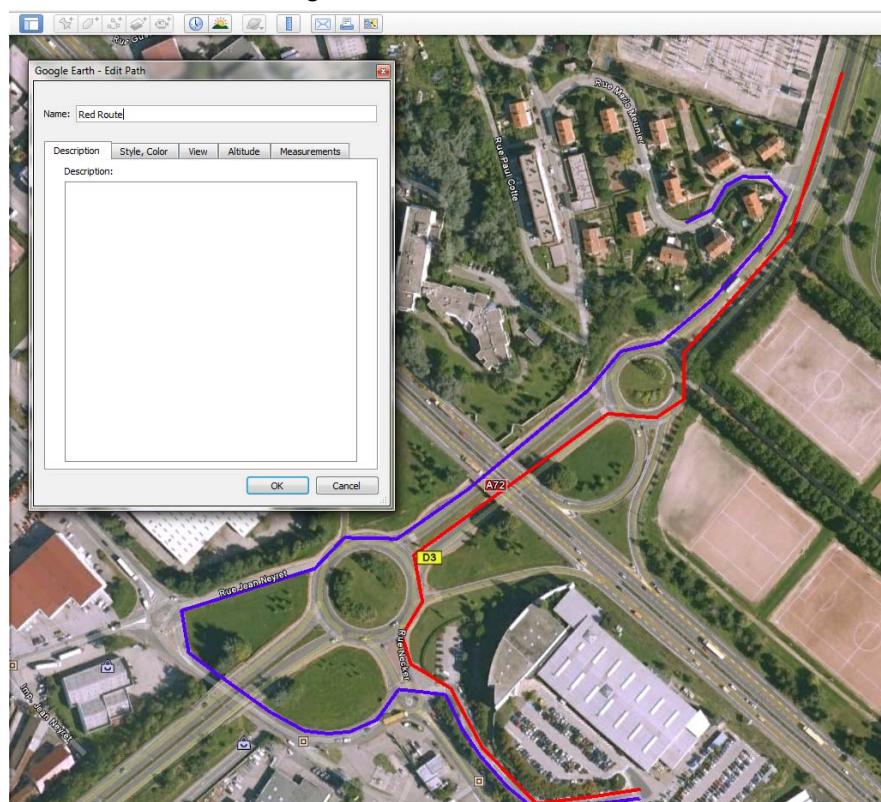
NOTE

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 108 Path drawn in Google Earth™



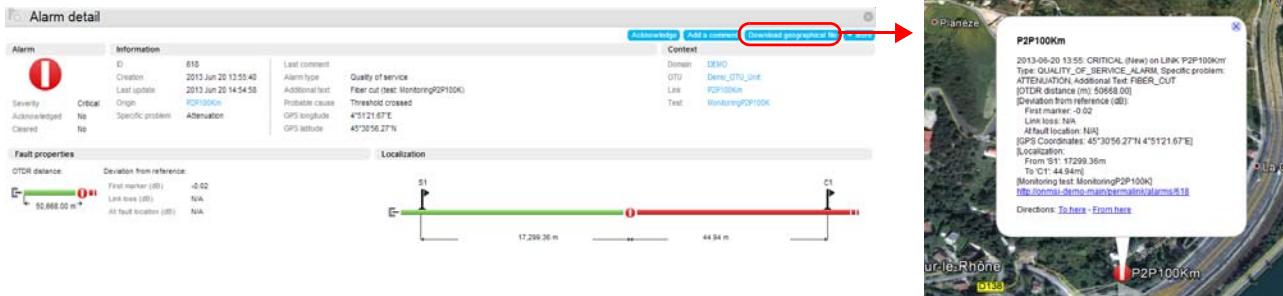
In the Link dashboard

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 109 Alarm details on map



Alarms management

This chapter provides a description of the Alarms management.

Topics discussed in this chapter include the following:

- “[Alarms Display](#)” on page 98
- “[Actions on alarms](#)” on page 99
- “[Actions on table display](#)” on page 102
- “[Notification by e-mail of an alarm](#)” on page 104
- “[Alarm Desktop alert](#)” on page 105

Alarms Display

Alarms Viewer

In the Alarm viewer, two tabs are available:

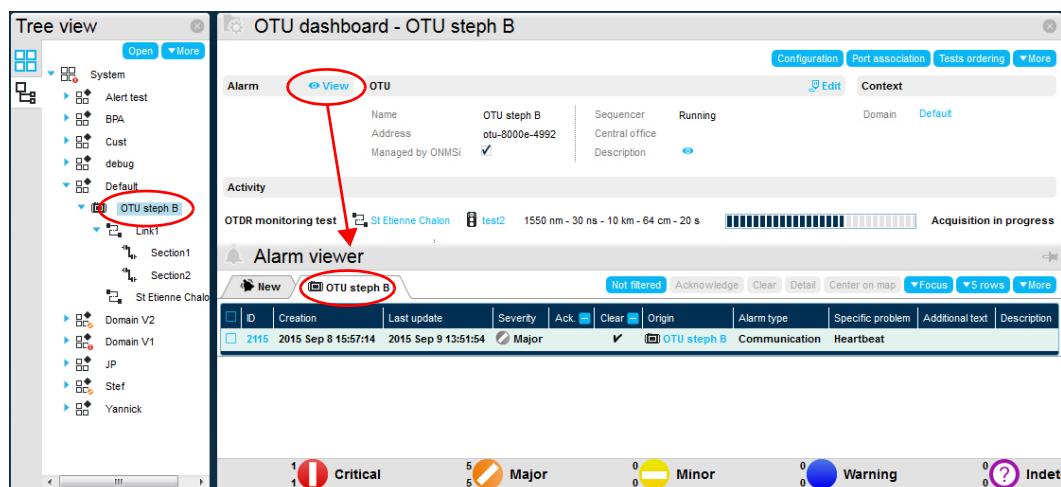
- The tab **New**, which shows the list of Non-acknowledged alarms.
From this tab, the alarms can be cleared and/or acknowledged (bulk)
- The tab «**Contextual**»: which content depends on the dashboard selected (system, domain, otu, port..).

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 110 List of alarms for a specific object



Alarms details

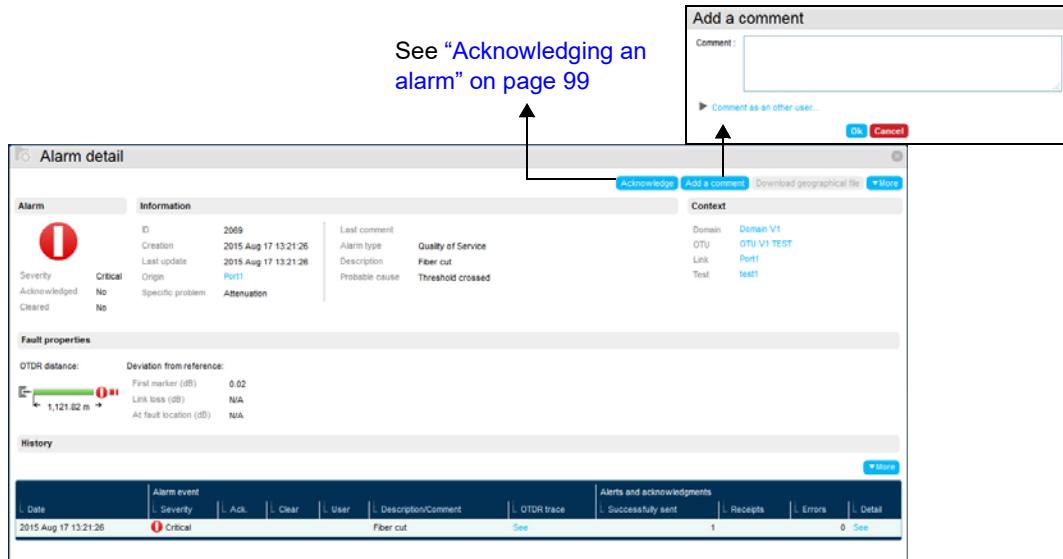
You can access to detail for any alarm (active or cleared).

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 111 Alarms details



Actions on alarms

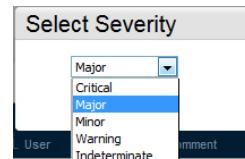
Changing the alarm severity

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 acknowledgment 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 acknowledgment of an alarm can be canceled.

- 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 canceled.

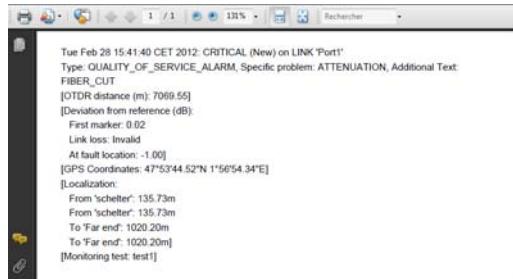
- 1 In the Alarm viewer, select the **ID** of the acknowledged alarm.
- 2 Click on **More** button
- 3 Click on **Unclear**.

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 112 Alarms Table in PDF

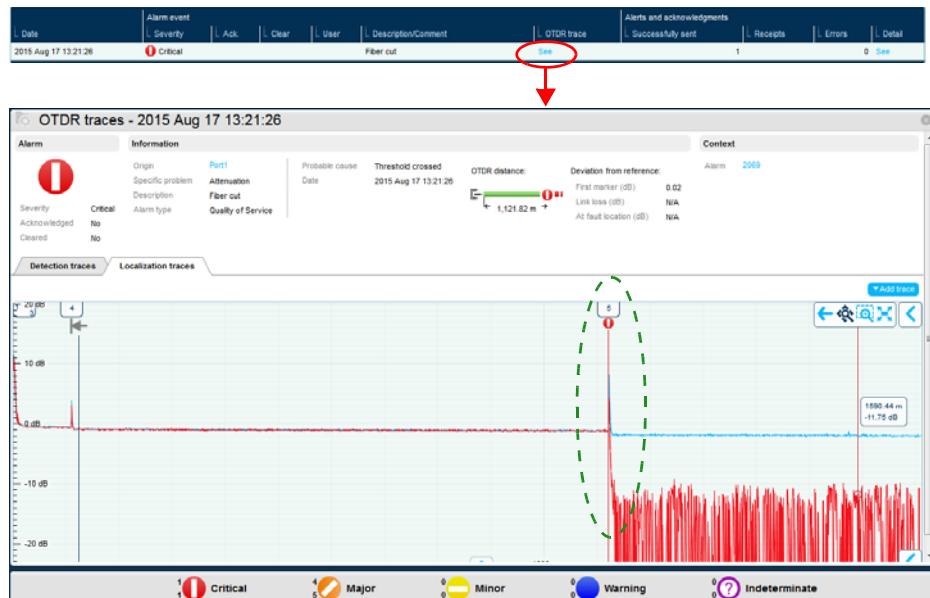


Alarm History (detail view)

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 113 Alarm details and trace



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 undone.

- 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.

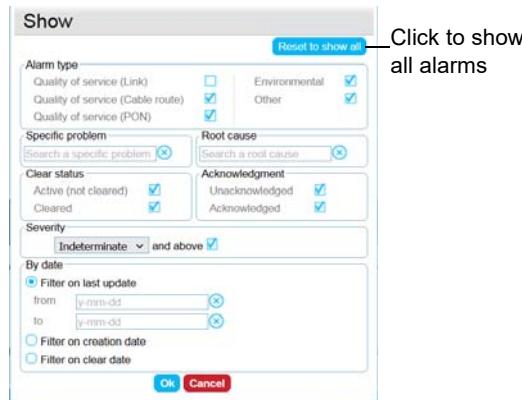
Actions on table display

Filtering the alarms in the table

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

- 1 Select the **System** alarms.
- 2 Click on **Filtered** button above the table
- 3 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 Acknowledgment window, select/deselect the alarm which have been acknowledged or not.
- 4 In the **Specific problems** window, enter the first letters of the specific problem to be displayed. This will show a list of the types of problem available. Select one from the list to display only the alarms with this specific problem.
- 5 In the **Root cause** window, enter the first letter in order to show a list of the root cause available. Select one from the list to display only the alarms with this specific problem.
- 6 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.
- 7 In the **By date** parameter, define the starting and end dates of the alarms to be displayed, according to last update, creation date or clear date.
- 8 Click on **Ok** to apply the Filters (or on **Cancel** to not apply filters).

Figure 114 Alarms filters



Configuring the alarms table

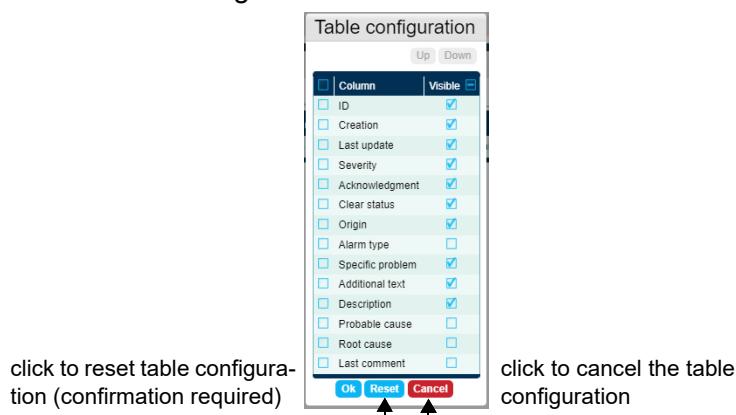
In the alarm viewer, configure the table:

- 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 115 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.

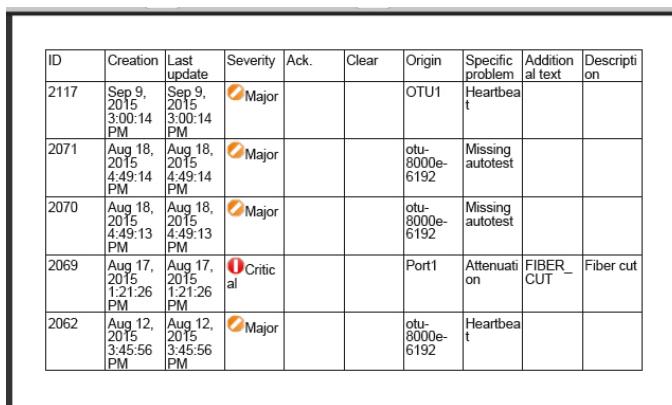
Downloading the alarms table

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 116 Alarms Table in PDF

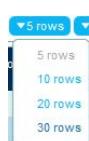


ID	Creation	Last update	Severity	Ack.	Clear	Origin	Specific problem	Additional text	Description
2117	Sep 9, 2015 3:00:14 PM	Sep 9, 2015 3:00:14 PM	Major			OTU1	Heartbeat		
2071	Aug 18, 2015 4:49:14 PM	Aug 18, 2015 4:49:14 PM	Major			otu-8000e-6192	Missing autotest		
2070	Aug 18, 2015 4:49:13 PM	Aug 18, 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.

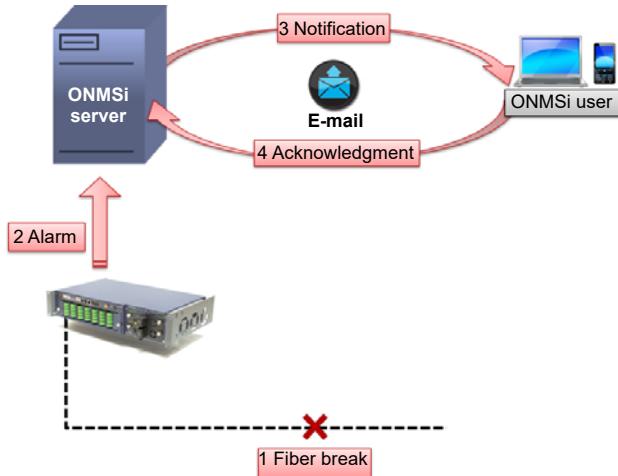


Rows: allows to configure the number of lines for the alarms table: from 5 to 30 rows.

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 117 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 184

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™



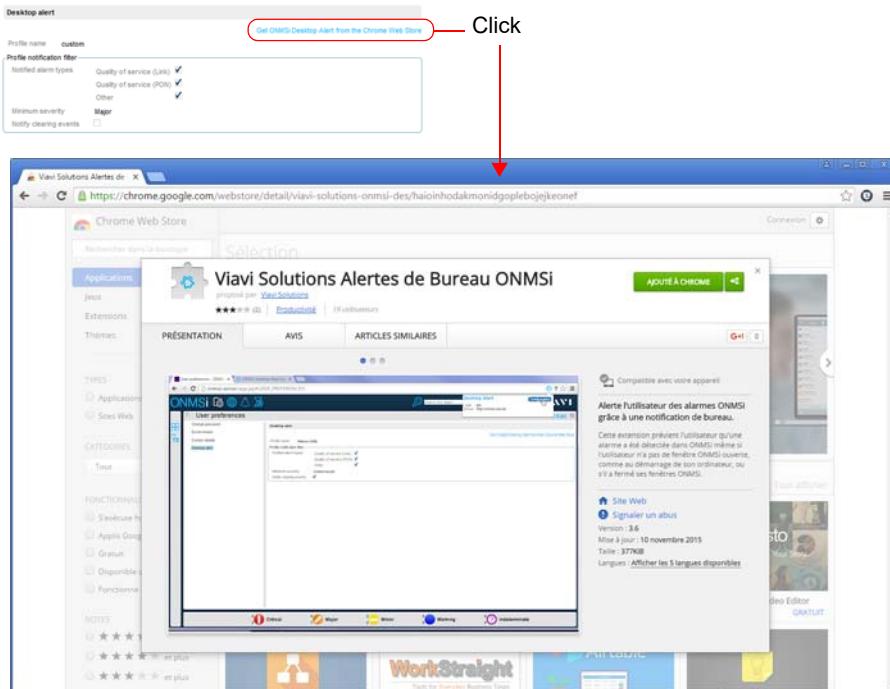
CAUTION

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.

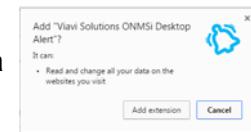


Figure 118 Desktop alert



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 task bar, a popup message informs the PC is «Listening to the ONMSI alarms».

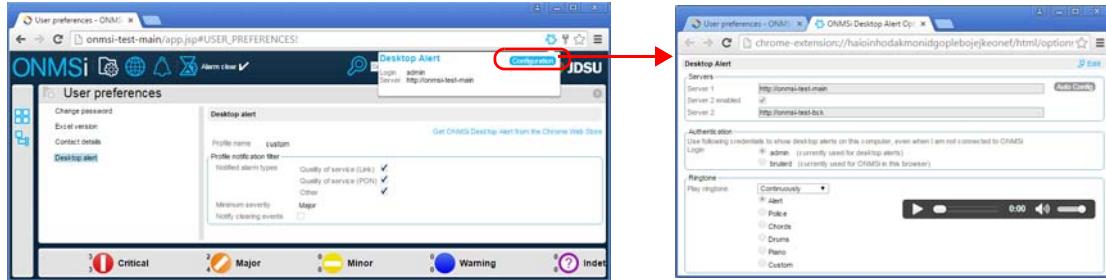


Configuring the desktop alerts

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 119 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 120 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:

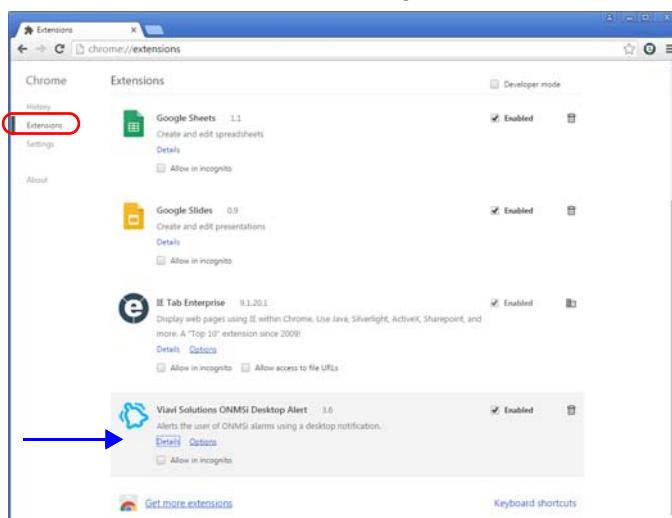
- 1 Click on the «Customize and control Google Chrome» button in the browser address bar and click on **Settings**.



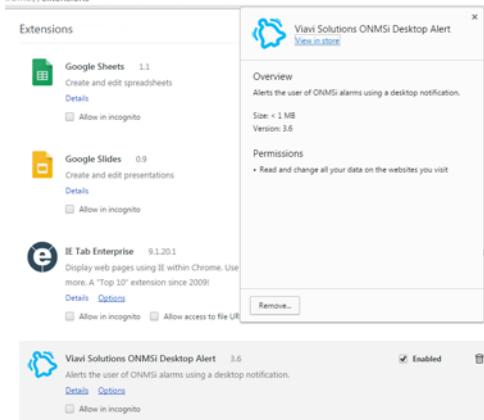
- 2 In the **Settings** page, click on **Extensions** on the left of the screen.

The ONMSI Desktop Alert extension is available among all the extensions enable.

Figure 121 List of extensions available in Google ChromeTM



- 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 106).
- Click on **Details** to display information on the extension



Tables, Reports and Pinboard 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 112
- “[Inventory Report](#)” on page 113
- “[Generating reports](#)” on page 114
- “[Managing Pinboard](#)” on page 116

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.

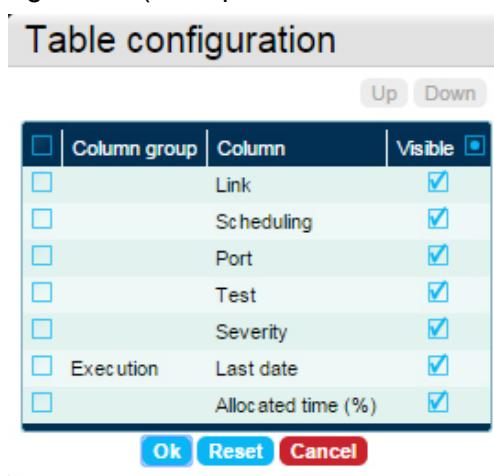
This configuration is kept in memory for downloading of tables in Excel or PDF.

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 122 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 123 Table from ONMSi in Excel and in PDF

ID	Creation	Last update	Severity	Ack.	Clear	Origin	Specific problem	Additional text	Description
2148	Sep 15, 2015 11:08:18 AM	Sep 15, 2015 11:51:16 AM	Major			CoAvec Attenuateur	Attenuation	ATTENUATION	Attenuation
2147	Sep 15, 2015 11:07:18 AM	Sep 15, 2015 11:29:33 AM	Critical			Contra	Attenuation	FIBER_CUT	Fiber cut
2140	Sep 15, 2015 7:36:00 AM	Sep 15, 2015 7:36:00 AM	Major			ONMSI-TEST-MAIN	Database backup	ERROR_CODE: AL	ERROR_CODE: AL
2069	Aug 17, 2015 1:21:26 PM	Sep 9, 2015 4:36:00 PM	Critical			Port1	Attenuation	FIBER_CUT	Fiber cut

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 124 Download inventory

Select inventory sections

Available sections

 OTUs
 ROTAU
 Links
 All
 None

6 Open the file on the PC.

Figure 125 Inventory in Excel

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	OTU	Name	Description	Managed by ONMSI	Address	Web Interface enabled	Domain	Hardware	OTDR module	Switches				Total OSU	
1	OTU - Sep 15, 2015 2:32:54 PM														
2	OTU														
3															
4															
5		OTU Steph B	Yes	Yes	otu-8000e-4992	Yes	Domain D1	Domain D2	OTU 8000E	4992	5.04	BOTTOM	8115 LR	40	
6		OTU V1 TEST	No	No	10.33.20.240	Yes	Domain V1	OTU 8000	1446	3.24	14492	TOP	8118 RLR 65		
7		otu-8000e-5334	Yannick/Yannick_1	Yes	otu-8000e-5334	Yes	Yannick/Yannick_1	OTU 8000E	5334	4.24	BETA 6	TOP	81162C		
8															
9															
10															
11															
12															

Generating reports

Creating a report

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

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

Name	Template	Frequency	Latest execution	Latest execution duration (min)	Latest status	Next execution	Send to
Missing template							
Active alarms			2023 Nov 9 09:15:50	0	Success		
Audit logs	Audit logs		2023 Feb 21 08:53:03	0	Success		
Audit Logs	Audit logs		2023 Jun 13 15:15:59	0	Success		
Latest PON tests	Latest PON test		2023 Aug 28 15:24:20	0	Success		
Links linear attenuation	Links linear attenuation		2023 Nov 10 09:32:02	0	Success		
PON test count per hour	PON test count per hour		2023 Aug 28 15:33:59	0	Success		

Detail

Name: Reports alarms **Latest execution:** **Next execution:**

Scheduling:
 Run report on demand
 Run report periodically
Delivery:
 None
 Email
 File

Content:
Template: Links alarm duration
Description: Oss alarm repartition per duration
Format: PDF
Language: English
Title: Report Alarms duration
Filter:
Minimum severity: Indeterminate
Minimum duration (min): 0
Date range: At run date and time (Full)
Scope:
Classes: Number of classes: 4
Class interval (Hours): 2

- 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 127 on page 115](#))
 - **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 `/opt/rfts_apps/export/topaz/report`.
 - 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 127 Reports available



Name	Template	Frequency	Latest execution	Latest execution duration (mn)	Latest status	Next execution	Send to
Report Steph	The active alarms		2015 Sep 15 15:42:00	0	Success		
Yannick_2_Daily_Alarms	The active alarms	Daily	2015 Sep 15 00:00:00	0	Success	2015 Sep 16 00:00:00	
Yannick_Weekly_Alarms	The active alarms	Weekly	2015 Sep 14 03:00:00	0	Success	2015 Sep 21 03:00:00	
Yannick_Past24h	The active alarms		2014 Sep 23 17:34:01	0	Success		
Attenuation	Links linear attenuation		2015 Sep 15 09:29:35	0	Success		Yannick

- 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 128 Example of report open in ExcelTM

The screenshot shows an Excel spreadsheet with the following data:

Column	Header	Content													
1	Execution date	September 13, 2015 3:51:44 PM													
2	Scope	System													
3	From	September 14, 2015 12:00:00 AM													
4	To	September 14, 2015 11:59:59 PM													
5	Minimum duration (min)	1													
6	Quality of service (L1)	Yes													
7	Quality of service (POH)	No													
8	Other														
9	Active (not cleared)	Yes													
10	Cleared	Yes													
11	Unacknowledged	Yes													
12	Acknowledged	Yes													
13	Indeterminate														
14	Minimum severity	Indeterminate													
15	Domain (OTU6) (Id)	Creation	Last update	Duration (DD HH:MM:SS)	Severity	Ack.	Clear	Origin	Alarm type	Specific problem	Additional text	Description	Probable cause	Last comment	
16	Domain: OTU6 (Id: 2066)	2066	August 17, 2015 10:39:56 AM	September 9, 2015 21:48:52 PM	28 13:20:3	26.35559201	Major	Yes	No	otu-8001 Communication	Heartbeat			Other	
17	Domain: OTU6 (Id: 2069)	2069	August 17, 2015 11:21:26 PM	September 9, 2015 21:48:52 PM	28 10:39:33	28.44343924	Critical	No	No	Port	FIBER_CUT	Fiber cut	Threshold crossed		
18	Domain: OTU6 (Id: 2070)	2070	August 17, 2015 11:21:26 PM	September 9, 2015 21:48:52 PM	28 10:39:33	28.44343924	Critical	No	No	Port	ATTENUATION	Other	Other		
19	Domain: OTU6 (Id: 2071)	2071	September 9, 2015 3:00:14 PM	September 9, 2015 5:05:34 PM	2 8:59:45	5.37482813	Major	Yes	No	OTU1	Communication	Heartbeat		Add a comment	
20	Domain: OTU1 (Id: 2117)	2117	September 9, 2015 3:00:14 PM	September 9, 2015 5:05:34 PM	2 8:59:45	5.37482813	Major	Yes	No	OTU1	Communication	Heartbeat			
21	Domain: OTU1 (Id: 2133)	2133	September 13, 2015 7:43:05 AM	September 14, 2015 7:40:36 AM	0 23:57:31	0.99827618	Warning	No	Yes	Server1	E_SAT (2GIG)	Attenuation	Other		
22	Domain: OTU1 (Id: 2134)	2134	September 13, 2015 7:43:05 AM	September 14, 2015 7:40:36 AM	0 23:57:31	0.99827618	Warning	No	Yes	Server1	ATTEN	Attenuation	Other		
23	Yannick: otu-8001 (Id: 2135)	2135	September 14, 2015 3:24:13 PM	September 15, 2015 9:09:42 AM	0 17:46:29	0.73991998	Minor	No	Yes	Coiveo	Quality of Service	ATTEN	Attenuation	Threshold crossed	
24	Yannick: otu-8001 (Id: 2136)	2136	September 14, 2015 3:24:13 PM	September 15, 2015 9:09:42 AM	0 17:46:29	0.73991998	Minor	No	Yes	Coiveo	Quality of Service	ATTEN	Attenuation	Threshold crossed	
25	Yannick: otu-8001 (Id: 2137)	2137	September 14, 2015 3:24:13 PM	September 15, 2015 9:09:42 AM	0 17:46:29	0.73991998	Minor	No	Yes	Coiveo	Quality of Service	ATTEN	Attenuation	Threshold crossed	
26	Domain: OTU6 (Id: 2138)	2138	September 14, 2015 5:43:34 PM	September 14, 2015 5:43:34 PM	0 0:0:11	0.00270502	Major	No	Yes	otu-8001	Equipment	Module compatibility	1		
27	Yannick: otu-8001 (Id: 2139)	2139	September 14, 2015 5:43:34 PM	September 14, 2015 5:42:33 PM	0 0:0:13	0.00270502	Major	No	Yes	otu-8001	Communication	Heartbeat			
28															

NOTE

If the customer logo is available in the User Interface, it will also be displayed in the report: see “[Adding a logo to the User Interface](#)” on page 13.

Managing Pinboard

The Pinboard tool allows to generate some graphics of different data, generated from the ONMSi, and to save all the graphics on a pinboard.

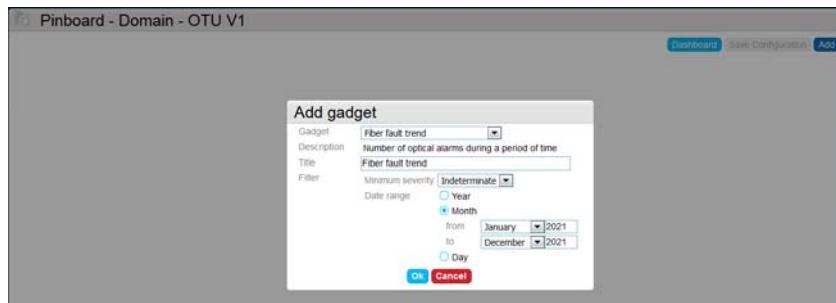
Configuring the pinboard

The Pinboard application can be launched from the System Dashboard or from a Domain dashboard:

- 1 Select the **System** or the **Domain** from which Data will be collected and displayed.
- 2 Click on **Pinboard** button from the System/Domain dashboard.
- 3 Click on **Add** to add a new data graphic (pie chart or bar chart).
- 4 In the **Add gadget** dialog box, define the parameters for the graphic to be displayed:
 - a In the **Gadget** menu, select the data templates for which a graphic must be generated:
 - **Alarm ageing:** Repartition by duration for all alarms that have been active (even momentarily) within the time range.
 - **Faults closed during last 24 hrs**
 - **Fiber fault trend:** Bar chart with number of optical alarms during a period of time
 - **MTTR Compliance:** Pie chart representation of alarm MTTR

- **Monitored fiber health:** Pie chart distribution of fiber health according to associated links linear attenuation
- **OTU status:** OTU availability (with and without alarms, unreachable, not managed)
- **Outstanding alarms:** Active alarms per severity
- **Port status:** Number of ports (unused, monitored with/without alarm)

Figure 129 Gadget configuration



b Configure the parameters available according to the Gadget selected.

In all types of gadget, you can modify the **Title** of the graphic.

c Click on **Ok** to validate.

After a few seconds, the graphic is automatically generated and displayed on the Pinboard screen.

- 5 Click on the bottom right corner to resize the window of the graphic (icon ↗).
- 6 Click on the title banner to move the graphic on the Pinboard page (icon ⇛).
- 7 Add as many graphics as necessary for the Pinboard.

By default, the new graphic is displayed on the left upper part of the Pinboard, above the existing one. Repeat steps 5 and 6 to fit the graphic and move it.

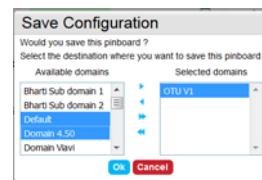
Figure 130 Example of Pinboards



Saving the Pinboard configuration

- 1 Once all the graphics wished are set-up and correctly positioned onto the Pinboard, click on **Save Configuration**.
- 2 If the Pinboard has been configured for a Domain or sub-domain, a dialog box displays allowing to save the current configuration for other domains than the one selected.

Figure 131 Save Pinboard configuration (Domain)



If wished, select other domains on the left column «**Available domains**» (press **Ctrl** to select several domains) and click on the right arrow to set those domains in «**Selected domains**» column.

- 3 Click on **Ok** to save the configuration.
- 4 If the Pinboard has been configured for the System, a confirmation is required: click on **Yes** to validate.

Other pinboard features

At any time, the pinboard can be modified: the graphics can be removed or their parameters can be modified:

- Click on ▾ and on **Edit** on the graphic to modify the parameters of this graphic.
- Click on **Remove** to remove the graphic from the pinboard.
- Don't forget to save the pinboard if modifications must be applied.

The parameters of a graphic can be displayed and the graphic refreshed:

- Click on the icon ⓘ to see the current parameters for the graphic.
Click on **Refresh** to Refresh the graphic.



NOTE

The graphics are refreshed automatically every 5 minutes, except the **Monitored Fiber Health** and **MTTR Compliance** graphics, which are refreshed every hour.

Fiber Sensing

This chapter provides a description of the Sensing monitoring function available with a DTSS Module installed onto the OTU.

Topics discussed in this chapter include the following:

- “Configuring the OTU with an OTDR Module connected to a DTSS Module” on page 120
- “DTSS Configuration Measurement” on page 121
- “DTSS Monitoring Test” on page 123
- “Zone Configuration” on page 125
- “Link Dashboard view” on page 128



CAUTION

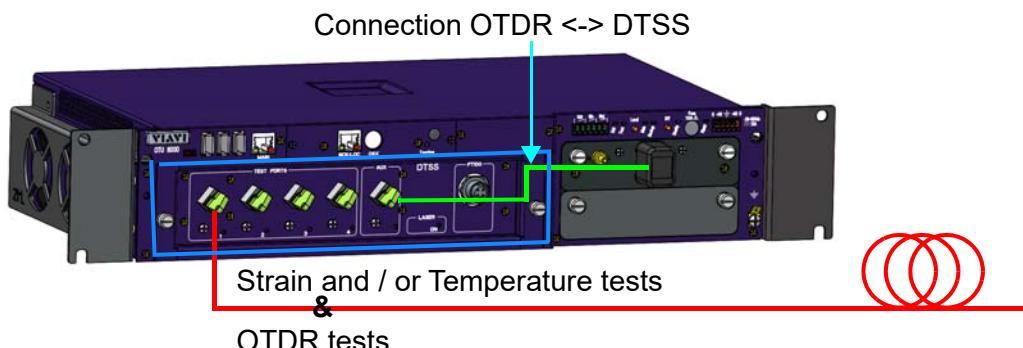
This function is available exclusively with a specific hardware configuration
For more information, contact your service center.

Configuring the OTU with an OTDR Module connected to a DTSS Module

The OTU can be equipped with DTSS Module and an OTDR module, which can be both connected, allowing to perform DTSS tests and OTDR tests on the same link.

The OTDR module output is then connected to the auxiliary input of the DTSS Module.

Figure 132 Links on the OTU equipped with a DTSS Module and OTDR

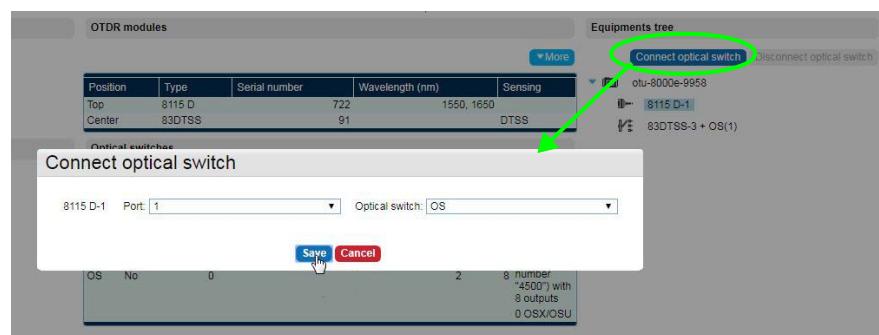


To link the OTDR to the DTSS Module

Once the DTSS Module and the OTDR Module have been added to the OTU configuration:

- 1 In the **OTU Dashboard**, in the **Equipment Tree**, select the DTSS Module.
The button **Connect optical switch** turns active.
- 2 Press the button.
The dialog box **Connect optical switch** opens.

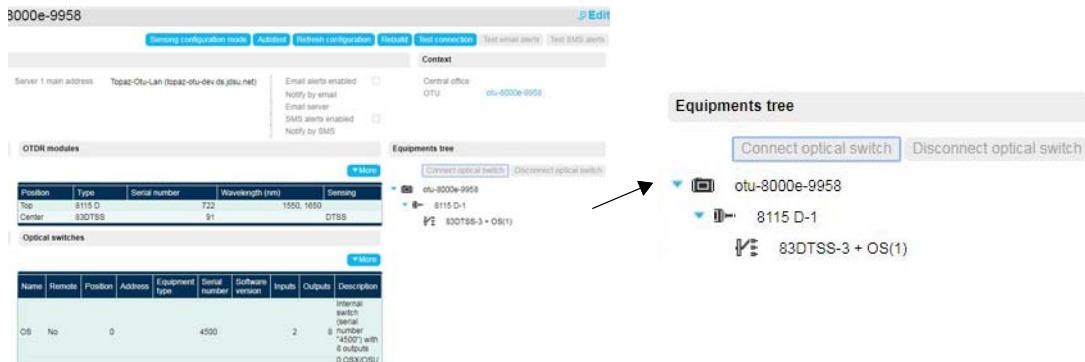
Figure 133 Connect Optical switch to DTSS Module



- 3 If necessary, modify port number and the optical switch port.
- 4 Click on **Save** to establish the connection.
- 5 Once completed, the OTDR output is connected to the auxiliary input of the DTSS Module.

- 6 The **Equipment tree** zone displays the DTSS Module, and the Optical Switch to which it is connected at a lower level.

Figure 134 Equipment tree: OTDR optical switch connected to DTSS



DTSS Configuration Measurement

Once the OTU is correctly configured with DTSS Module (and OTDR module if any), the DTSS Measurement must be configured.

The configuration must be done in *Sensing configuration mode* (instrument mode).

Once in *Sensing configuration mode*:

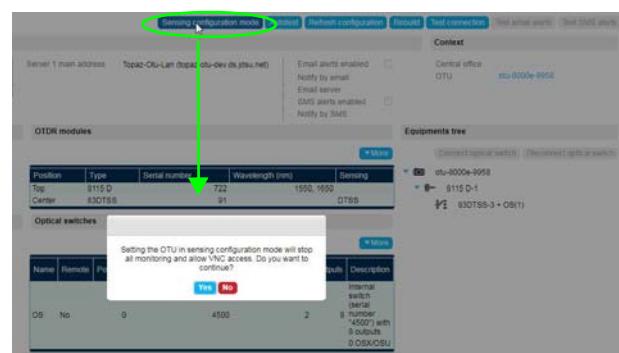
- the monitoring on OTU is stopped
- the user won't be able to perform any operation (measurements/tests on demand, configuration...) on this OTU via ONMSi.

However, he will still be able to navigate on the screens of this OTU or of this links/tests, which will be in read only mode.

- In the OTU Configuration screen; click on the **Sensing configuration mode** button **Sensing configuration mode**.

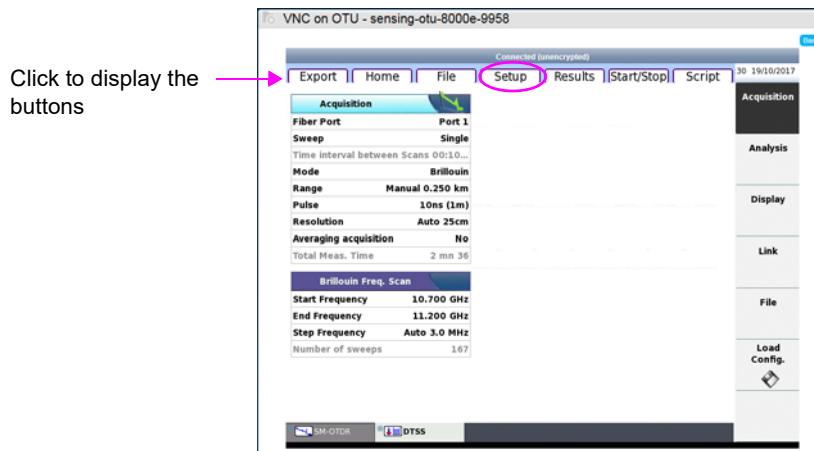
A warning message displays to indicate the monitoring will be stopped and the VNC allowed.

Figure 135 Warning message at start of Sensing configuration mode

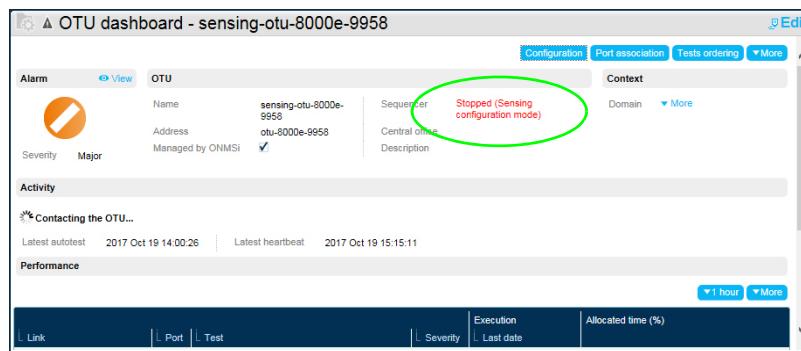


- 2 Press **Yes** to validate the Sensing configuration mode.
The screen displays the screen of the instrument.
- 3 If another screen than the Setup one is displayed, click on the upper banner and press **Setup** button.

Figure 136 Sensing configuration



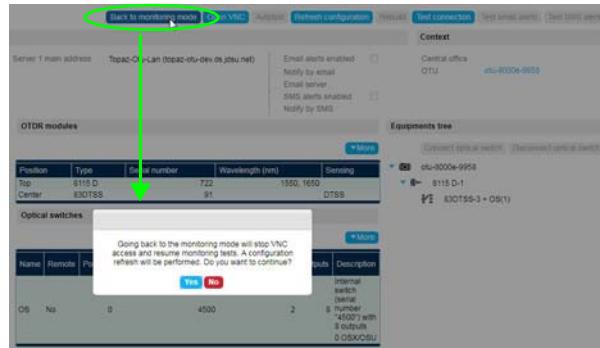
- 4 Refer to DTSS Module User Manual to configure the DTSS Measurement.
DTSS reference measurements are performed with VNC access to the OTU applications.
Measurement is automatically saved with the name: port<number>-<type measure>-<date-time>.dtss (port1_temp_strain_15_06_2017_13_54.dtss)
- 5 Once configuration is completed, click on **Back** to display the ONMSI application.
 - In this mode, the sensing configuration mode is still active, so the monitoring on OTU is stopped and the user won't be able to perform any operation (measurements/tests on demand, configuration...) on this OTU via ONMSI.
 - Only navigation on the screens of this OTU and of the links/tests, which will be in read only mode, are possible.



- If the VNC screen must be displayed back, click on **Open VNC** to return to configuration screen.
- 6 Click on **Back to Monitoring mode** Back to monitoring mode to return to monitoring mode once the configuration is completed and exit the sensing configuration mode.

A dialog box displays, informing the VNC access will be stopped and a refresh configuration performed.

Figure 137 Warning message when Sensing configuration mode is stopped



- 7 Click on **Yes** to confirm.

The configuration is refreshed (a bar graph displays on the shortcuts panel).



- All the acquisitions performed in Sensing configuration mode are saved onto the hard disk of the OTU.
- Once the user returns to Monitoring mode, the ONMSi refreshes the configuration in order to recover these acquisitions and save them in the database.
- This will allow to rebuild the OTU in case of failure.

DTSS Monitoring Test

Sensing monitoring is a relative monitoring. When the OTU performs a monitoring measurement, it compares it to the reference measurement to deliver a result trace, that is the difference between the monitoring and the reference measurement.

It therefore represents the variation of the temperature and/or strain from moment the reference was performed

Fiber segments will be defined as zones, on which thresholds will be applied to trigger alarms and locate faults .

For each zone:

- 1 Alarms thresholds will be defined
- 2 Alarms will be triggered
- 3 Defaults will be located

The monitoring results are **results of the difference between the measurement performed and the reference measurement = relative measurement**.

Reference measurement

Once references have been perform:

- 1 From the OTU dashboard, press **Port Association** button.
- 2 Select the port for which a link must be created.
- 3 Click on **More > Create Link**.
The Link Dashboard displays, in Edit mode.
- 4 Enter a name for the link.
- 5 Click on **Save** to save the link just created.
- 6 Click on **Add DTSS test** button to setup the test reference trace.

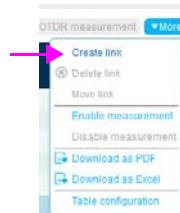
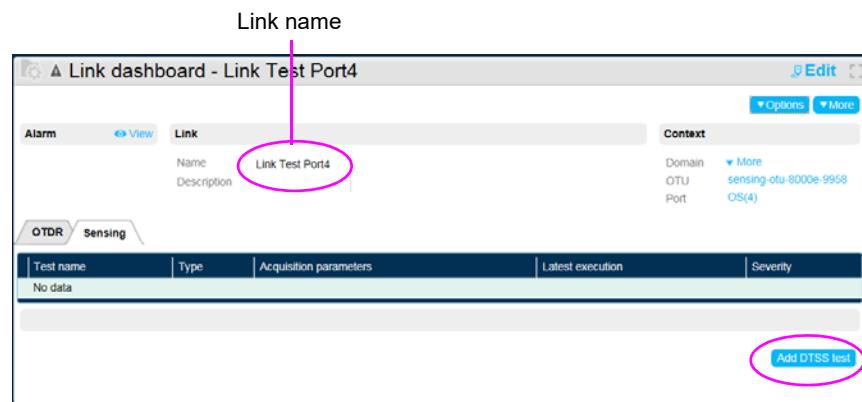
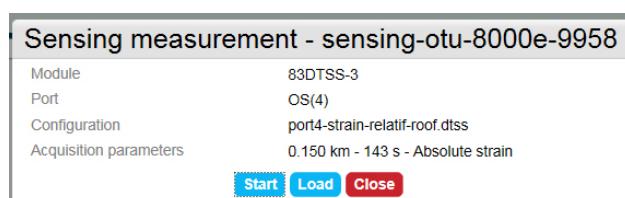


Figure 138 Add a DTSS test to a link



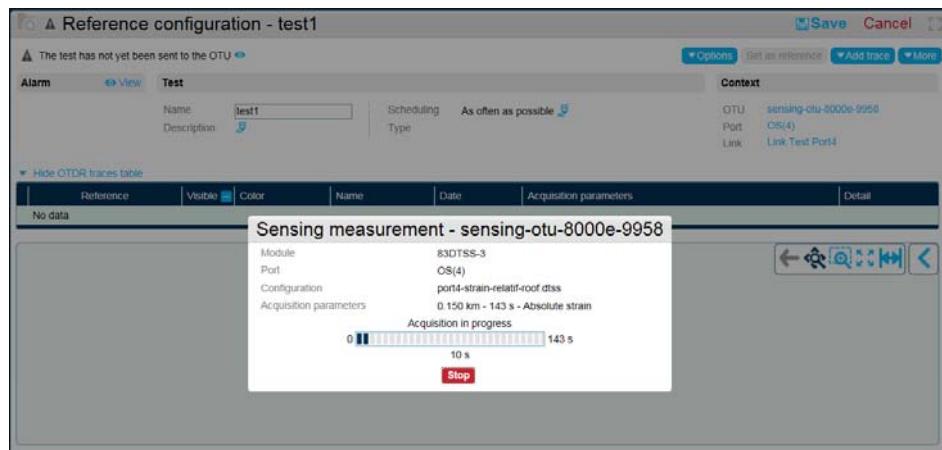
A dialog box displays, allowing to select a measurement performed onto the OTU when in sensing configuration mode, in order to either start a new measurement using the same parameters, or load it directly as reference.

Figure 139 Starting a DTSS Measurement



- 7 Click on **Start** to start a test using the same configuration as the one defined in the **Configuration** parameter
or
Click on **Load** to load the measurement selected in Configuration parameter.
- 8 If a new test has been launched (**Start**), a progress bar displays in the dialog box, with the elapsed time and the total acquisition time.

Figure 140 Sensing measurement in progress



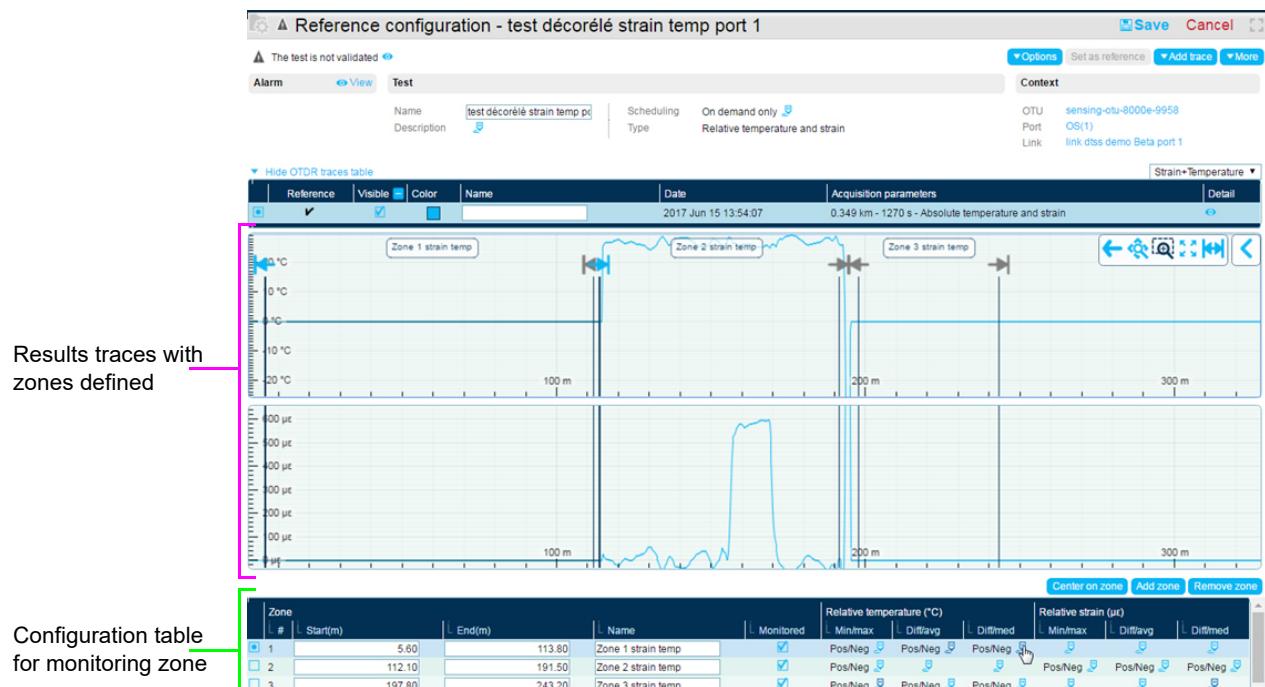
- Once acquisition is completed, the results trace displays as test reference.

Zone Configuration

If the measurement performed on the OTU in sensing configuration mode to setup the reference trace has been defined with zones, then those zones will be automatically imported as monitoring zones in the ONMSI application.

In any case, the user will then be able to add, modify or remove monitoring zones.

Figure 141 Sensing Test Configuration



Zones

Monitoring zones are defined per test.

If several tests are created on the same link, each test will independently manage its own monitoring zone setup.

Modifying the position of a zone

If a zone must be moved:

- 1 If the screen is not in Edit mode, click **Edit**.
- 2 Enter the **Start** and/or **End** position in the Zone table under trace.
or
Click on the icon  and move horizontally to modify the start and end position of the zone directly from the trace.

Adding/Removing a zone

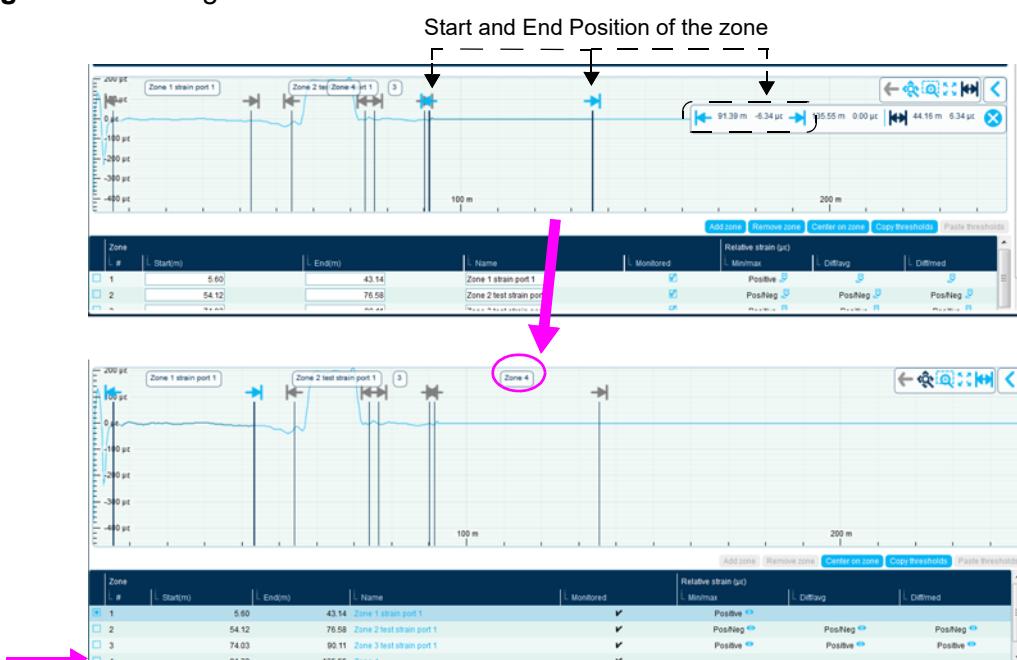
To add a zone, or remove an existing one:

- 1 Press **Edit** to enter the edit mode
- 2 To add a zone, select the zone after which the new one will be added.
To remove a zone, select it in the table.
- 3 Press **Add zone** or **Remove zone** button.

The new zone displays in the table and is identified on the trace.

If a zone is removed, press **Yes** in the dialog box displayed to validate the deletion

Figure 142 Adding a zone



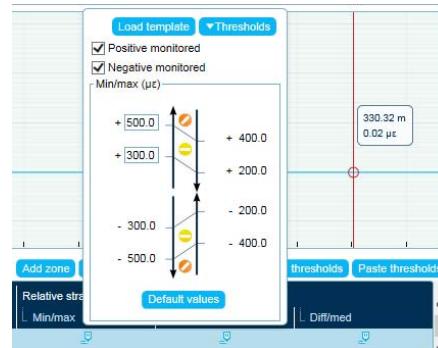
Zone thresholds

By default, the Monitored parameter is selected to enable all monitoring configured on the zone, and can be unselected to disable them globally.

To monitor a zone, and define the elements to be monitored, from the Reference configuration screen:

- 1 Press **Edit** to enter the edit mode.
- 2 Select **Monitored** parameter for the zone to be monitored.
- 3 Click on the icon  of the monitoring for which thresholds must be defined, either for Strain, Temperature or both:
 - **Min/Max**: Monitors the values of the lowest and highest points of the zone (allow to detect defaults when the zone varies homogeneously)
 - **Diff/avg**: Monitors the differences between the lowest/highest point and the average of the zone (allows to detect spot defaults)
 - **Diff/med**: Monitors the differences between the lowest/highest point and the median of the zone (allows to detect spot defaults)
- 4 You can choose to monitor high and/or low values using the **Positive monitored** and **Negative monitored** check-boxes.

Figure 143 Defining alarm thresholds



- 5 Click on **Load Template** to load a thresholds configuration defined in the **Settings** screen.
- 6 Click on **Threshold** and select:
 - **Minor threshold enabled**: to display and modify of necessary the minor thresholds for the parameter selected.
 - **Advanced configuration**: to manually define the hysteresis; if not selected the hysteresis is calculated automatically.
- 7 Click on **Default values** to define the threshold with values available by default.
- 8 Click outside of the alarm threshold configuration box to exit this box.

The monitored elements are defined with **Pos** and / or **Neg** parameter in the table according to the configuration (**Positive monitored** and / or **Negative monitored** defined).

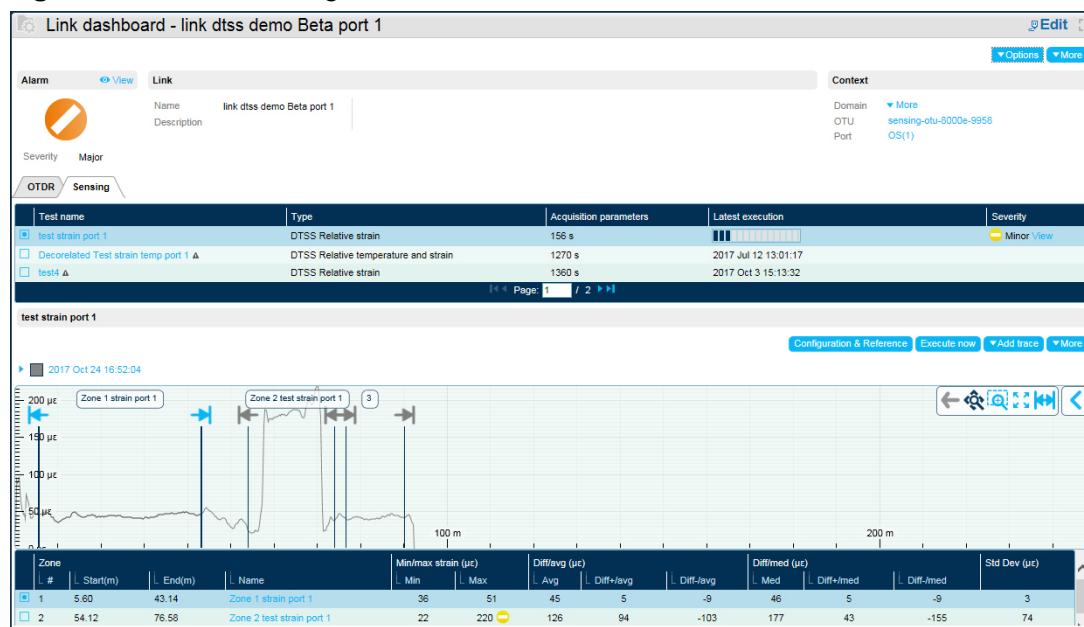
Figure 144 Alarm thresholds defined

Relative temperature (°C)			Relative strain ($\mu\epsilon$)		
Min/max	Diff/avg	Diff/med	Min/max	Diff/avg	Diff/med
Pos/Neg	Pos/Neg	Pos/Neg	Positive		
Pos/Neg	Pos/Neg	Pos/Neg	Pos/Neg	Pos/Neg	Pos/Neg

Link Dashboard view

The **Link Dashboard** displays the numerical values of each measurement on the trace.

Figure 145 Fiber Sensing: Link Dashboard view



Zone Dashboard

From the **Link dashboard**, click on the **Name** of one zone to display the **Sensing Zone** window.

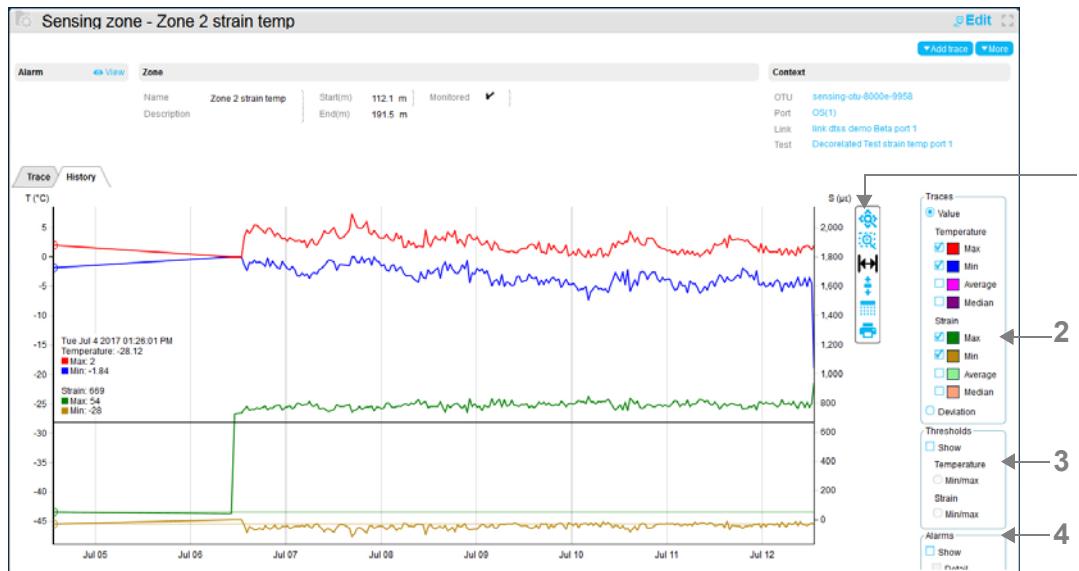
The Sensing zone is to be used only for exploitation.

Click on the **History** tab to display a view of the evolution of zone measurement in time.

The Y axis displays the temperature on left, and the strain on right. If both are defined, both values are available.

Under the graph is displayed the severity of each type of monitoring.

Figure 146 Zone; History



The thresholds displayed are those applied at the time of acquisition. They are not applied in the history if they are modified after.

- 1
-
- Pan and Zoom on double click (hold Shift key to zoom out)
 - Zoom in a Zone (hold Shift key to zoom out)
 - Zoom in a selected time range (hold Shift key to zoom out; the current screen will be displayed in the selected range)
 - Adjust the vertical axis to fully display the graph
 - Define the time range for the graph display (from 1 year to 1 day)
 - Print the graph as it is currently displayed: with the current zoom level, the current information selected (thresholds...)

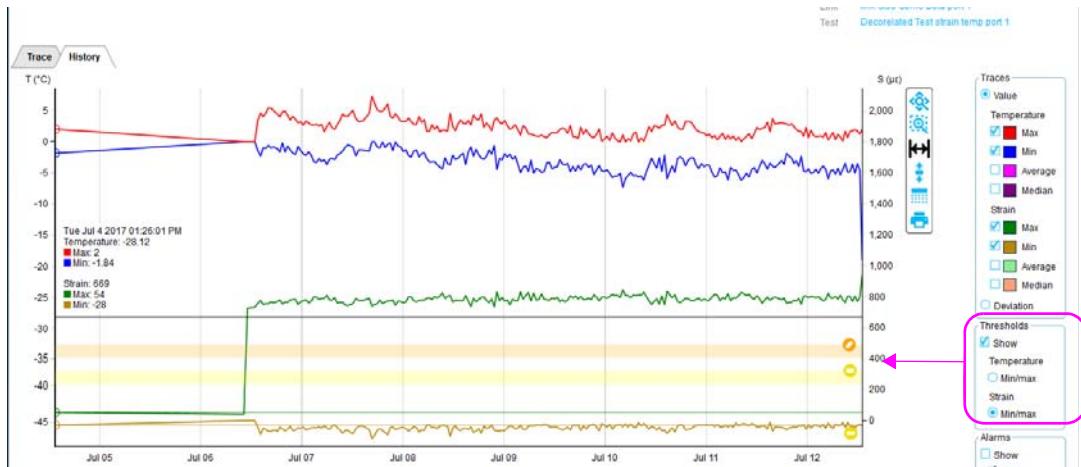
- 2
-
- Define if the graph must be displayed with the **Values** or the **Deviation**
If Values is selected, define the values to be displayed for **Temperature** and/or **Strain: Min, Max, Average, Median**
If Deviation is selected, define the results to be displayed for **Temperature** and/or **Strain: Diff+/avg, Diff-/avg, Diff+/med, Diff-/med**

3

Thresholds

 Show
 Temperature
 Min/max
 Strain
 Min/max

Define if **Thresholds** must be displayed, either for Temperature, or for Strain.
Select **Show** parameter to display the alarm thresholds exceeded, with the icon  and/or .



4

Alarms

 Show
 Detail

Define if **Alarms** must be displayed under the graph.
Select **Show** parameter to display the alarms history, and select **Detail** to display the alarms history according to alarm type for **Temperature** on the left and/or **Strain** on the right (Max, Min, Diff+avg, Diff-/avg, Diff+/med, Diff-/med).



Alarms details

To display the details of an alarm detected on a fiber sensing results trace, click on the alarm:

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

Figure 147 Alarm Detail

The screenshot shows the 'Alarm detail' interface. On the left, there's a yellow circular icon labeled 'Alarm detailed information.' A blue arrow points from this text to the yellow icon. Below it, a green box highlights the 'Fault properties' section. Another blue arrow points from the text 'Detail description of the fault: see "Fault Properties"' to this green box. To the right of the properties, a red arrow points from the text 'Click to display the sensing trace see Figure 148.' to the 'History' table. The 'History' table lists several entries with columns for Date, Severity, Ack., Clear, User, Description/Comment, Sensing traces, Successfully sent, Receipts, Errors, and Detail.

Date	Severity	Ack.	Clear	User	Description/Comment	Sensing traces	Successfully sent	Receipts	Errors	Detail
2017 Oct 24 14:10:20	Minor				Min/max	See	0	0	0	See
2017 Oct 24 11:58:57	Major				Min/max	See	0	0	0	See
2017 Oct 24 08:35:59	Major				Multiple causes	See	0	0	0	See
2017 Oct 23 18:29:35	Major				Multiple causes	See	0	0	0	See
2017 Oct 23 10:05	Minor				Multiple causes	See	0	0	0	See

Fault Properties

The Fault Properties displays a detailed description of the fault. One line displays the minimum values and one line the maximum values.

The Position column displays the highest and the lowest point of the zone.

	Value of the highest point	Distance interval onto which the threshold has been exceeded	Value of the average	Value of the median
Position	190με	[57.44m 70.71m]	114με	167με
Maximum	67.90m	190με	76με	22με
Minimum	71.48m	11με	-102με	-156με

Annotations explain the data:

- Value of the highest point: Points to the '190με' value.
- Value of the lowest point: Points to the '11με' value.
- Distance interval onto which the threshold has been exceeded: Points to the '[57.44m 70.71m]' range.
- Value of the difference between the highest point and the average: Points to the '-102με' value.
- Value of the average: Points to the '114με' value.
- Value of the median: Points to the '167με' value.

Click on **See** in the **Sensing trace** column to display the sensing trace of the alarm selected.

Figure 148 Sensing Trace for selected alarm



ONMSi PON System

This chapter provides a description for the creation and configuration of ONMSi PON system.

Topics discussed in this chapter include the following:

- “Manual PON Creation” on page 134
- “Home Browser page” on page 138
- “Associating Central Office to OTU” on page 139
- “PON Calibration” on page 140
- “PON Test” on page 143
- “ONMSi PON Topology” on page 148
- “ONMSi PON Field application” on page 152
- “VIP Permanent Monitoring” on page 158

Manual PON Creation

Uploading / Downloading Data

ONMSi PON Data requires information from network inventory in order to:

- tie the test result to Network inventory data,
- provide reports with names and identifier that are understood by all the users
- facilitate the field technician work.

Uploading data is mandatory and is to be done **PRIOR** to associating the OTU to Central Office.

- CO, PON and HOME are created only via the Upload tool.

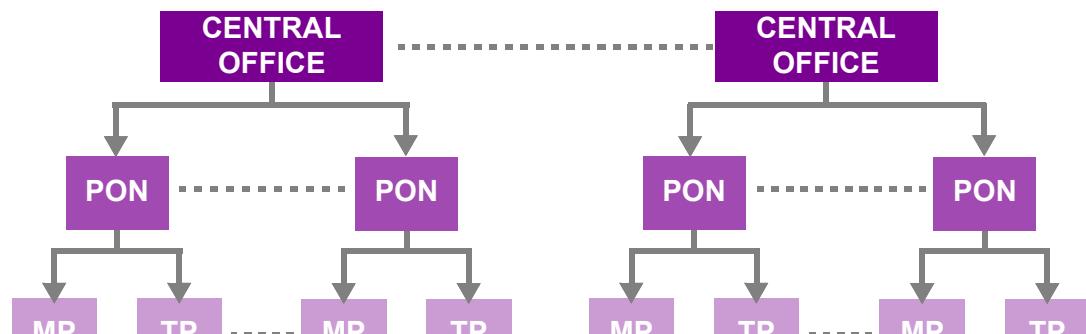
The **first level** of ONMSi PON Data structure is the **Central Offices** (exchanges) where the test head is installed.

The **second level** is composed of **PON**. One PON is connected to one single test head port (Switch port). A PON is composed of a feeder (one fiber) connected to a splitter (1x32). The splitter has 32 branches connected to CBT. A PON refers to one central office.

The **third level** is composed of two different set of data:

- Monitored Points (MP) with reflector = **Home**.
- **Test Points:** Different PON points tested from the splitter.

Figure 149 ONMSi PON



MP: Monitored Point (Reflector is left)

TP: Test Point (Reflector is removed after the test)

- 1 In the **System Dashboard**, click on **More**.
- 2 Click on:
 - **Download central office** to download the file template for Central offices.
 - **Download PONs** to download the file template for the PON.
 - **Download homes** to download the file template for the Monitored points.



NOTE

Columns **in bold** are mandatory.

Central Office Data

The central office data contains 4 fields:

- **Central Office name** (mandatory)
- Description: Free text to add information
- **External key**: it is the column identifying the CO (used when uploading PON). External Key can be the same as Name. This key must be unique in the whole application.
- ONMSi key (read-only): auto-generated number given by ONMSi.

Central office data can be pushed to ONMSi by using Excel™ Template or by the API.

Figure 150 Central Office data

	A	B	C	D
1			<i>Central offices</i>	
2				<i>Additional attributes</i>
3				
4	Name	Description	Internal key	External key
5	CO1	MyCentralOff1		CO1_K
6	CO2	MyCentralOff2		CO2_K
7				
8				

PON Data

The PON data contains the following fields:

- **Pon name** (mandatory). It must be a name identifying the fiber. It must be unique. It is composed of Splitter ID and SASA Number (Example: "TMALAPJ1")
- Description: Free text to add information
- Internal key (read-only): auto-generated number given by ONMSI.
- **PON Type**: This field indicates the OTDR measurement configuration. It can be left with "Default" or "Module C" at Day 1. PON type can also be optimized later.
- OTU/Test Head Name: This field can be used for the association between optical switch port and PON. It must indicate the Test Head name used for testing this PON. If it is not provided, this association can be made by the user interface.
- **OTU optical switch name** (Mandatory if **OTU Name** is given): In the case of BTOR, this field must contain "OS".
- **OTU Port Number** (Mandatory if **OTU Name** is given): The port number which the PON is connected to.
- **Central Office External Key**: It is used to tie it to the central office data. It must contain the external key given for the central office.
- **External key**: This key is used to tie ONMSi data to customer data. It is used for the relationship between PON and monitoring points. This key must be unique in the whole application.

PON data can be pushed to ONMSi by using Excel™ Template or by the API.

Figure 151 PON Data

Pons		OTU		External identifier		Additional attributes				
Name	Description	Internal key	PON Type	Name	Optical switch name	Port number	CO.External key	External key	Port Id	Validated by
C02-01	3310	POH_HR_ots-8000e-10548	05		2 CO_C02	C02-01				
C02-02	3345	POH_HR_ots-8000e-10548	05		2 CO_C02	C02-02				
C02-03	3389	POH_HR_ots-8000e-10548	05		3 CO_C02	C02-03				
C02-04	3415	POH_HR_ots-8000e-10548	05		26 CO_C02	C02-04				
C02-05	3450	POH_HR_ots-8000e-10548	05		27 CO_C02	C02-05				
C02-06	3485	POH_HR_ots-8000e-10548	05		28 CO_C02	C02-06				

Monitored Point Data (called Home in the user interface)

The monitored point data contains the following fields:

- **Name:** Name given to this monitored point.
- **Identifier:** It must be unique for the whole application. It is entered by the Field Tech when the reflector is connected. From this identifier, the test head and the switch port to be used for the measurement are known. It is often the same as the name.
- Description: Free text
- Upstream test point: The parent test point for this monitored point.
- VIP: VIP flag to indicate that this monitored point is permanently monitored.
- Internal key (read-only): Given by ONMSi.
- Termination Type: It contains an item of a list of texts defined by the user. It can be for example “passed”, “connected” or “Terminated” for home termination. This field can be changed later from the user interface.
- **PON External Key:** It is used to tie it to the PON data. It must contain the external key given for the PON.

Figure 152 Monitored Point data

Homes		Home		Termination		External identifier	
Name	Home Identifier	Description	Upstream test point	VIP	Internal key	Termination type	PON.External key
toto	toto			false	5661	pon jp 2	
tutu	tutu			false	5662	pon jp 2	
tata	tata			false	5663	pon jp 2	
Maison1	Maison1			false	19127	Passed	pon test 1 Ex. key
Maison2	Maison2			false	19128	Passed	pon test 1 Ex. key
Maison3	Maison3			false	19129	Connected	pon test 1 Ex. key

Test Points data

Test point data contains the following fields:

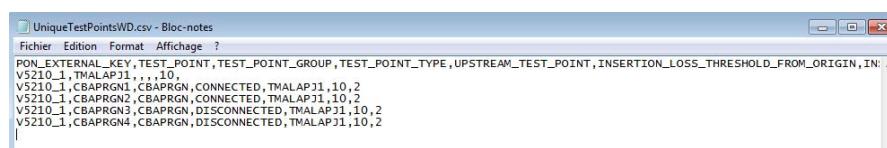
- **PON_EXTERNAL_KEY:** Name of the PON the test points refer to.
- **TEST_POINT:** Name of test point (Ex: <Splitter ID>P1 for the port 1 of the splitter).
- **TEST_POINT_GROUP:** If multiple test points belong to the same optical component like the splitter ports, the name of the splitter can be given for the name of the group. This field is not used with the current mobile application. In the future it will be used to facilitate user input by grouping test points.

- **TEST_POINT_TYPE:** The value must be "CONNECTED". Later it will also be possible to put "DISCONNECTED" in order to test the not connected ports when this feature is available with the mobile application. The TEST_POINT_TYPE could be freely modified by user.
- **UPSTREAM_TEST_POINT:** Test point which is before (Origin: OTDR) the test point. It is empty if it is the first test point (splitter output)
- **INSERTION_LOSS_THRESHOLD_FROM_ORIGIN:** This data is used for the mobile application. The test passes if the insertion loss measured from OTDR is below the given threshold. If it is empty the measurement result is only displayed. There is no pass/fail.
- **INSERTION_LOSS_THRESHOLD_FROM_UPSTREAM_TEST_POINT** (Optional): This data is used for the mobile application. The test passes if the insertion loss measured from the upstream test point is below the given threshold. If it is empty the measurement result is only displayed. There is no pass/fail. The threshold must take into account the measurement uncertainties (+/-0.5dB) and the variant between reflectors. Insertion loss between test points being low (few tenths of dB), The threshold must be the sum of the estimated insertion loss and total uncertainties (measurement and reflectors variant).
- **LOW LOSS:** LOW LOSS must be enabled («true») if the insertion loss at the Test POINT is expected to be low. It is typically for test points after a first splitter (connected to the feeder) having a split ratio of less than 32.

Figure 153 Test Points Data

PON_EXTERN AL_KEY	TEST_POINT TEST_POINT_GROUP	TEST_POINT_TYPE	UPSTREAM_TEST_POINT	INSERTION_LOSS_THRESHOLD_FROM_ORIGIN	INSERTION_LOSS ON_UPSTREAM_TEST_POINT
TMALAPJ1	CBAPRGN1	CBAPRGN	CONNECTED	TMALAPJ1	25
TMALAPJ1	CBAPRGN2	CBAPRGN	CONNECTED	TMALAPJ1	25
TMALAPJ1	CBAPRGN3	CBAPRGN	DISCONNECTED	TMALAPJ1	25
TMALAPJ1	CBAPRGN4	CBAPRGN	DISCONNECTED	TMALAPJ1	25

Files must be in CSV format. Separator must be ','



CAUTION

If test points are already existing, they are updated and associated measurements are deleted.

Uploading data

Once the data have been entered for each object, they can be imported from Excel:

- 1 In the System Dashboard, click on **More > Upload from Excel (CO, PONs, Homes)**.

- 2 Click on **Browse**.
- 3 Select the first xls files to be imported and press **Open**.
- 4 Click on **Ok** to validate the import.
- 5 Once completed, a dialog box displays the data added, updated, failed or a warning. Click **Close** to close the window.
- 6 Proceed the same way for the other data files.

Upload result	
Added	0
Updated	3
Failed	0
Warnings	0

Home Browser page

From the **System Dashboard**, click on **Home Browser** to retrieve a filtered list of Homes along with their status and main information.

Figure 154 Home Browser

Name	ID	Termination	Attachment date	Severity	Measurement Detail	Attached to PON	CO
Home 1/03	Home 1/03		2020-Jan-15 18:47:15			PON 1	CO for vOTU
Home 2/04	Home 2/04		2020-Jan-10 17:46:56			PON 2	CO for vOTU
Home 1/04	Home 1/04		2019-Dec-12 17:40:07			PON 1	CO for vOTU
Home 1/09	Home 1/09		2019-Dec-11 11:18:51			PON 1	CO for vOTU
Home 1/07	Home 1/07		2019-Dec-11 11:10:55			PON 1	CO for vOTU
Home 1/08	Home 1/08		2019-Dec-11 11:07:41			PON 1	CO for vOTU
Home 1/01	Home 1/01		2019-Dec-9 15:52:30			PON 1	CO for vOTU
Home 1/49	Home 1/49		2019-Dec-5 09:49:33			PON 1	CO for vOTU
Home 1/02	Home 1/02					PON 1	CO for vOTU
Home 1/05	Home 1/05					PON 1	CO for vOTU
Home 1/06	Home 1/06					PON 1	CO for vOTU
Home 1/10	Home 1/10					PON 1	CO for vOTU

- Click on the **PON Id** to display the PON details

Figure 155 PON details

PON - PON FTH-9000_CHR-01										Edit	
Alarm			PON							Start test Topology More	
Name	Description	Type	Calibration status	VIP scheduling	Enable feeder test	As often as possible	Port Id	Domain	Link	OTU	Port
PON FTH-9000_CHR-01	PON_FTH_9000_CHR_01	PON_HR_Ins [Build_Auto_New]	Calibrated	test pan Feeder 01	✓	Other attributes		CO FTH-9000_CHR	PON-9000-00019 CHR	OS001	
Tests history											
Test result	Run on	CO level (dB)	Calibration run on	Peak status	New/Missing from reference peaks			OTDR trace	More		
2023 Aug 30 23:38:41	2023 Aug 30 23:32:25	0.49 dB	CO calibration values	-0.39 dB from 6.50 to 9.50 m							
2023 Aug 30 23:31:09	2023 Aug 30 23:29:55										
2023 Aug 30 23:28:42	2023 Aug 30 23:24:23										
2023 Aug 30 23:23:09	2023 Aug 30 23:22:24										
2023 Aug 30 23:20:39	2023 Aug 30 23:19:25										
2023 Aug 30 23:18:09	2023 Aug 30 23:17:23										
2023 Aug 30 23:16:37	2023 Aug 30 21:56:12										
Distance from CO	Compensated deviation (m)	Measurements	Alarm	Reference peak	Attached home						
Distance from CO (m)	Compensated deviation (m)	Level (dB)	Level deviation (dB)	Insertion loss (dB)	Insertion loss deviation (dB)	Severity	Changed	Detail	Level (dB)	Type	Termination
10.619.27	2.16	2.98	-3.91	33.86	3.91	✓			6.89	Home	FBO-0dB
10.622.93	2.07	5.36	-1.99	31.48	1.99				7.35	Home	FBO-0dB
10.681.90	2.07	16.70	-1.39	20.14	1.39				18.09	Home	FBO-0dB
10.752.91	2.07	20.85	-1.38	15.99	1.38				22.23	Home	FBO-0dB
10.883.04	2.07	-1.60	-1.58	38.44	1.58				-0.02	Home	FBO-0dB
11.228.75	2.08	21.69	-1.26	15.15	1.26				22.95	Home	FBO-0dB

- Click on one **Home Id** to display the Home page description, with all the measurement results for this Home: distance from Central Office, Level, Level deviation and Alarm severity.

Figure 156 Home details

Date	Measurements	Alarm		
	Distance from CO (m)	Level (dB)	Level deviation (dB)	Severity
2020 Jan 21 17:22:06	2,212.38	6.45	(6.52)	-0.07
2020 Jan 21 16:26:32	2,212.38	6.45	(6.52)	-0.07
2020 Jan 21 16:25:05	(2,212.38)	(6.52)	(6.52)	Missing peak Critical
2020 Jan 21 16:16:09	(2,212.38)	(6.52)	(6.52)	Missing peak Critical
2020 Jan 21 16:14:43	(2,212.38)	(6.52)	(6.52)	Missing peak Critical
2020 Jan 21 16:13:07	(2,212.38)	(6.52)	(6.52)	Missing peak Critical
2020 Jan 21 16:10:42	(2,212.38)	(6.52)	(6.52)	Missing peak Critical
2020 Jan 21 16:06:44	(2,212.38)	(6.52)	(6.52)	Missing peak Critical
2020 Jan 21 14:47:00	(2,212.38)	(6.52)	(6.52)	Missing peak Critical

Adding Filters

- If the a PON or a CO is entered in the search field, the list of Homes belonging to that PON or CO will be displayed.
- Click on **Add Filter** On to apply specific filters to the current list:
 - **Severity:** Not Set / Indeterminate / Warning / Minor / Major / Critical
 - **Termination:** Not set / Passed / Terminated / Connected

Deleting Home or PON Data from the System

- 1 In the Home or PON description page (see [Figure 156 on page 139](#) and [Figure 155 on page 138](#)) click on **More > Delete home** or **Delete PON**.

A confirmation dialog box displays:

- For Home deletion, it indicates the home deletion will also delete its history.
- For PON, the system asks if the attached Homes must be deleted: select **Force to delete associated homes** if wished.

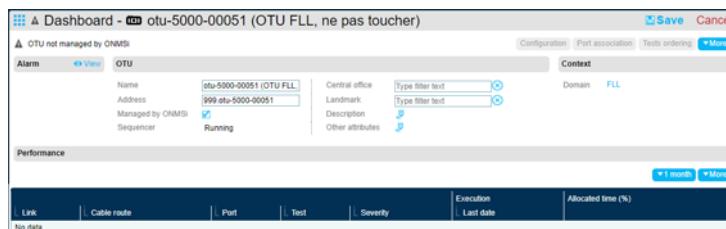
- 2 Click on **Yes** to confirm (or Cancel to cancel the deletion).

Associating Central Office to OTU

The Central Office where the OTU is located is to be selected in a list box in the OTU Dashboard:

- 1 Open the OTU Dashboard.
- 2 Click on **Edit** to add the Central office.
- 3 Select in the Central Office list, the one to be associated to the OTU.
- 4 Press **Save** to confirm the association.
Wait for the association to be completed.

Figure 157 Association of the Central Office to the OTU



CAUTION

Once a Central Office has been associated, it cannot be modified.

PON Calibration

PON calibration is necessary before reflectors are installed. It is composed of 2 steps:

- Calibration: This step defines a zone from which the insertion loss (IL) is measured. It also allows the IL measurement to be independent from OTDR and switch loss
- Non reflector peaks: this step ignores the peaks not corresponding to reflectors (splitter, open fiber, etc)

Associate PON to Optical Switch port



NOTE

The PON to associate to the port must have been previously created and uploaded (see “[Uploading data](#)” on page 137).

Each port of the optical switch is associated to a PON.

- 1 From the OTU Dashboard, click on **Port Association**.
- 2 In the Port association page, click on **Edit** to associate a PON to a port.
- 3 Select from the **PON Name** list box, the PON to be associated to the corresponding port.
The **Link Type** is automatically updated according to the PON selected.
- 4 Select or deselect the calibration if it has already be done for one port.
- 5 Press **Save** to validate the association.

Figure 158 Association switch port and PON

Port association - fth-9000-00016							Save	Cancel
Port association							Context	
Total number of ports	192	Central office	CO CO4					
Number of unused ports	179	OTU	fth-9000-00016					
OTU ports								
Port	Link Name	Type	PON Name	PON calibration	Calibrated	Zone (m)	Level (dB)	Deviation (dB)
OS(001)	link_test_splitter	Build_Splitter_1x4	link port 3 23.64	9.72 - 12.75	-1.52	0.04	See	
OS(002)	link port 2	Build_Auto_Launch15m						
OS(003)	link port 3 23.64	Build_Auto_Splitter1x4						
OS(004)	CO4-04	Default	CO4-04	12.91 - 15.94	-2.17	0.03	See	
OS(005)	fth-9000-00016 OS(005)	0 PON JSON	fth-9000-00016 OS(005)					
OS(006)	fth-9000-00016 OS(006)	PON 1:8 x 1:8	fth-9000-00016 OS(006)					
OS(007)	None							

Calibration Principle

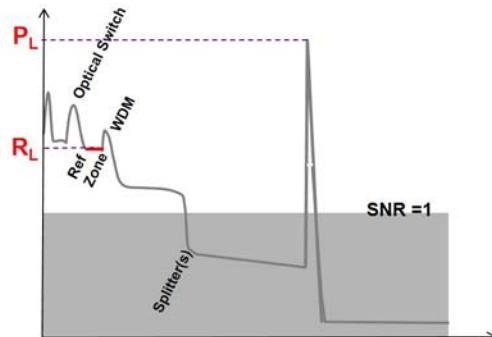
The calibration is the process to measure a reference level (R_L) on the OTDR trace

This reference level allows the insertion level measurement (see principle)

The peak level is corrected with the reference level in order not to be dependent on OTDR power and switch loss.

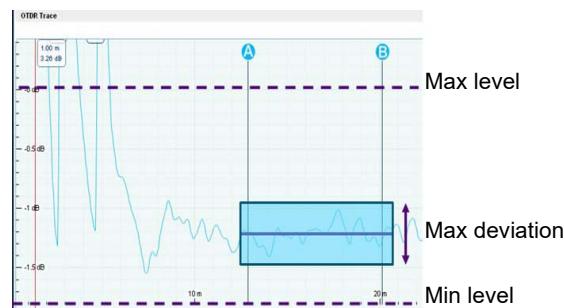
In the Figure below, the reference zone, also called Calibration, is taken between the switch and the WDM. It can also be between the WDM and the ODF, or after the ODF.

Figure 159 Insertion Loss measurement principle



This zone must be stable for accurate measurement. It is the reason the deviation (see picture below) must be within limits.

Figure 160 Deviation within limits



This zone is also used to check if the fiber is connected correctly to the test unit. This is the reason why there are the Max and min level.

Calibration process

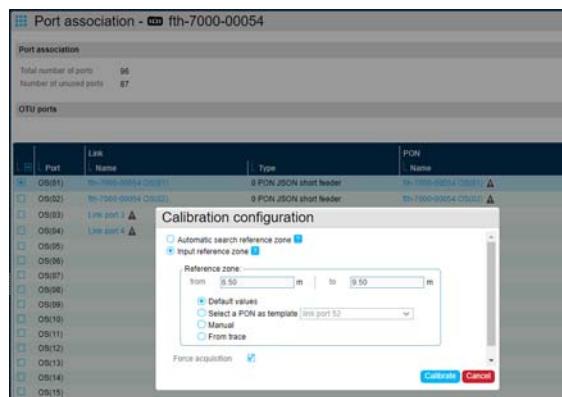
The calibration is available from Port association - OTU page.

1 Select the Port(s) to be calibrated.

2 Press **Calibration**.

The Calibration Configuration window displays.

Figure 161 Calibration Configuration



3 Define the reference zone:

- **Automatic search**: the OTU/FTH is searching for the reference zone conforming to the PON calibration acceptance thresholds of the PON type.

or

- **Input reference zone**: specify the reference zone.

- **Default values** sets the acquisition to use values defined in System settings/PON (see “PON configuration” on page 179).
- **Select a PON as Template** allows the user to select a previously-calibrated PON: Use this option when the WDM are at the same distance
- **Manual** lets the user enter his own values
- **From Trace** allows the user to place the cursors directly on the trace (an acquisition must have been done previously).

4 Select **Force Acquisition** option if you want the System to make an OTDR measurement even if an OTDR measurement already exists.

5 Press **Calibrate** to launch the calibration.

Once completed, if the calibration fails, the values are in red.

The calibration fails if a value is out of the limits define from System /settings /PON / Measurement setting (see “PON configuration” on page 179).

The reasons can be the fiber connection is not good or the zone is not appropriate

PON Test

Tag Not Homes

After the calibration is done, this function allows for a bulk of ports to tag all the peaks present on the OTDR "Not Home". This avoids that these peaks are displayed with the field app.

Figure 162 PON Test results

The screenshot shows the 'PON - PON 1' test results page. At the top, there are three annotations:

- A yellow circle icon with 'PON' next to it is labeled 'PON alarm severity Highest severity among PON homes'.
- A text box containing 'A test can be executed only if the PON is calibrated' is positioned above the 'Test result' table.
- A text box containing 'A link test is executed if peaks are missing' is positioned to the right of the table.

The 'Test result' table has columns for 'Run on', 'CO level (dB)', 'Calibration run on', 'CO calibration values', 'reference level', 'Distance from CO', 'Measurements', 'Level (dB)', 'Level deviation (dB)', 'Insertion loss (dB)', 'Alarm', 'Severity', 'Changed', 'Reference peak', 'Attached home', 'Termination', 'Reflector', 'ID (Name)', and 'Description'. A specific row is highlighted in green, showing a 'New peak' at 2.212.38 m with a level of 6.52 dB.

Below the table, a callout box points to a specific entry in the history: '2019 Dec 23 16:20 2019 Dec 18 16:14: 2019 Dec 18 15:26'. The text next to this entry states: 'The history contains all the PON tests including those launched from the field application or via the API'.

Table 5 Results table

	This symbol indicates that this test was used for referencing this peak
Distance from CO (m)	Peak distance. It can be different from the reference peak as the system tolerates a deviation because of OTDR resolution and temperature adjustments
Level (dB)	This level is the absolute peak level minus the reference level.
Insertion Loss (dB)	Insertion loss (IL) is calculated from the peak level, the reference level and the reflector reflectance. After a peak is associated, a new test must be executed to have the IL calculated because it is calculated by the OTU8000
Deviation (dB)	Peak level deviation from the reference for reference peaks (Home or Not Home) or from the previous test for other peaks. Missing Peak if the peak could not be found or New Peak if the did not exist before. Deviation is updated for non referenced peak only if System settings > PON > PON Test is set to Previous Measurement .

Table 5 Results table

Severity	Severity level of the PON alarm
Changed	This symbol indicates that this test changed the severity of the associated home.
Detail	Show details on the reference peak. Value of the reference peak
Type	The reference peak type can be Home when it is associated, Not home when it is referenced but it does not correspond to a PON termination.
Attached Home Id	Click on the Home Id to display the Home details (see Figure 156 on page 139)

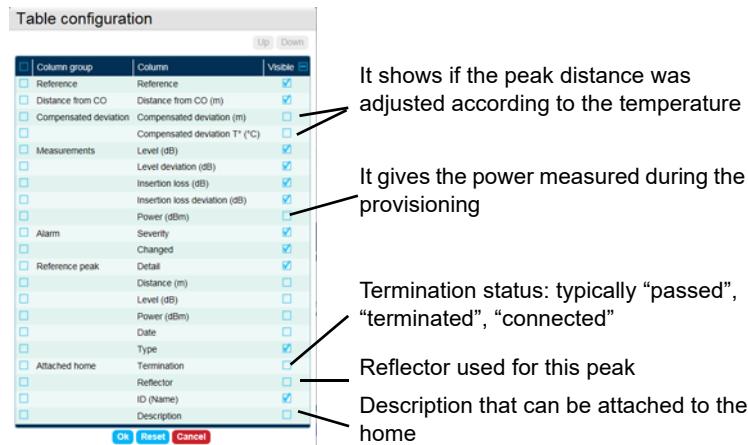
If wished, click on **More > Download as PDF** or **Download as Excel** to save the results table in a pdf or xls file.

PON test results table customization

The table can be customized:

- 1 Click on **More > Table Configuration**.
- 2 Select / deselect the columns which must be visible / hided on the results table.

Figure 163 Table configuration



Modifying some table parameters

- 1 Click on **Edit** to get the fields changeable in the table
 - In Reference Peak **Type**, select not home for a new peak not corresponding to a PON termination.
 - In **Reflector**, select the type of reflector used for the new peak.
 - In **ID (Name)**, select the Home Id corresponding to the new peak.
- 2 Click on **Save** to validate the modifications.

Automated PON creation

If a link type is configured with a PON topology (see “[Link types](#)” on page 175), with splitters and templating, the PON is automatically created accordingly.

The test points, corresponding to the first and second splitters, can also be configured manually if the 1st splitter ratio and the splitter labellings are defined in the Link type (see “[OTDR Link type configuration](#)” on page 176).

Moreover, when a measurement is performed on a link with PON, the PON calibration automatically starts if the calibration was not valid in previous tests.

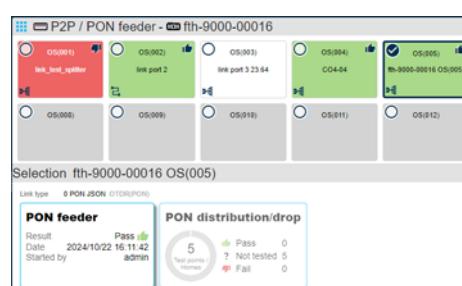
The instrument will now automatically find the calibration zone, if the configuration of the PON type in the link type includes this research, and if the OTU support this zones’ research. Otherwise, the calibration zone may be defined according the defined distances.

After this calibration, if succeeded,

- the tag Not homes is automatically launched, and it will only tag the new peaks as “not home” (see “[Tag Not Homes](#)” on page 143).
- a PON test is automatically launched and the peaks are automatically defined as “not home”, so that the PON is ready to use.

- 1 From the **Port association** page, click on the icon and select **P2P / PON feeder** sub-menu
- 2 Select the link(s) to be measured and click on the icon .
Several links can be selected in order to measure links in bulk.
- 3 In the dialog box, select the Link type to be used (define a PON type).
- 4 Define if the measurement must be performed **Periodically** and/or **Later**.
- 5 Click on **Start measurement**.
The OTU activity bar will display the measurement in progress.
- 6 Once completed, the **PON Feeder** view is displayed, with different cards are displayed under the selected links.

Figure 164 PON results (PON feeder view)



PON feeder view

PON feeder card

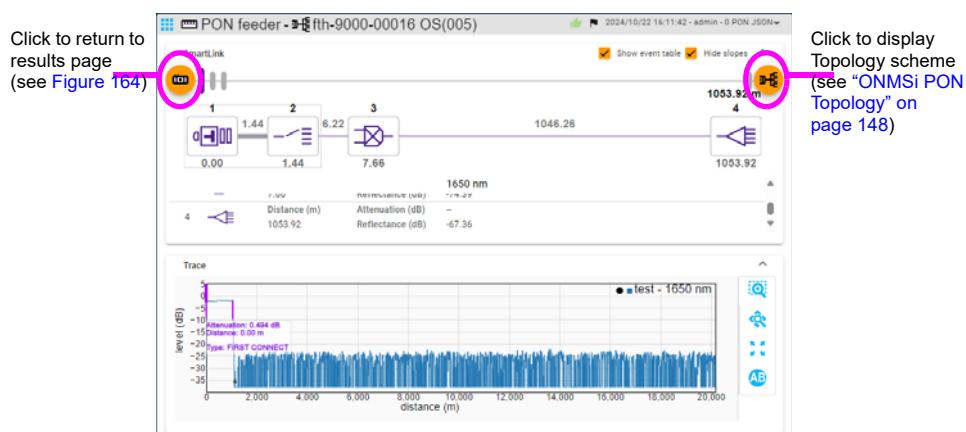
The PON feeder cards displays the PON feeder status.

- 1 Click on the **PON feeder** card to display the results trace and/or SLM view.

or

If the PON distribution /drop screen is displayed, click on the icon and switch to P2P PON feeder.

Figure 165 PON feeder SLM view and trace

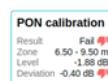


PON Calibration card

- If the PON is not calibrated, the card is displayed

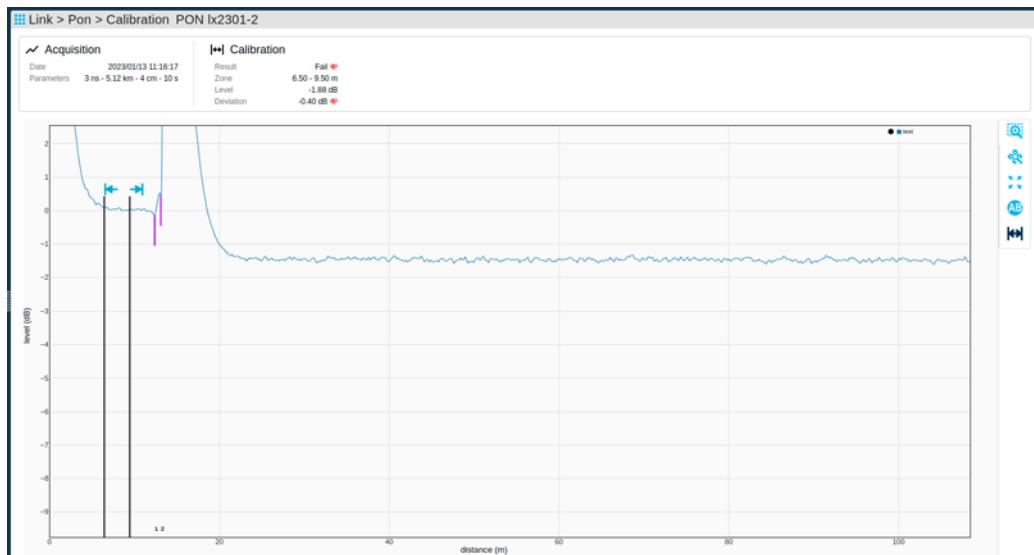


- If Calibration failed, the card is displayed



Click on this card to display the calibration screen, showing the trace and the calibration results:

Figure 166 Calibration trace



To perform manually the calibration, return to **Ports association** view and follow instructions “[Calibration process](#)” on page 142.

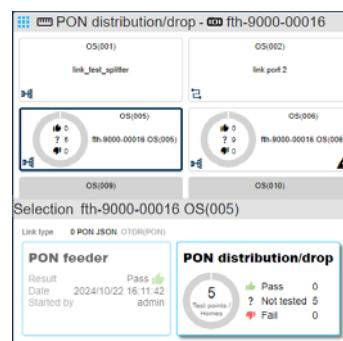
PON distribution/drop card

- 1 Directly click on the card to display the PON Topology (see “[ONMSi PON Topology](#)” on page 148).

PON distribution/drop view

- 1 Click on the icon to open the sub-menu and click on **PON distribution/drop**.

Figure 167 PON distribution/drop view



The main table display, for the links, the total number of Homes/Test points, with the number of passed, failed and not tested homes/test points, depending on whether they have been associated to a reflector peak measurement, and if the calculated insertion loss lies within the thresholds, or not.

Click on the card **PON distribution/drop** to display the Topology (see “[ONMSi PON Topology](#)” on page 148).

ONMSi PON Topology

This function gives a graphical view of the PON status. It shows the PON topology according to the info contained in Test point and Homes.

1 To access the PON Topology:

a Click on **PON distribution/drop**.

or

b Select a link from the OTU or Cable Head page in Construction view, and click on the **PON distribution/drop** card at the bottom of the screen. You can also open Topology screen clicking on the PON icon  in the SLM graphical view (see [Figure 165 on page 146](#)).

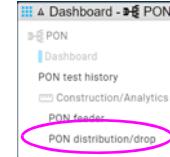
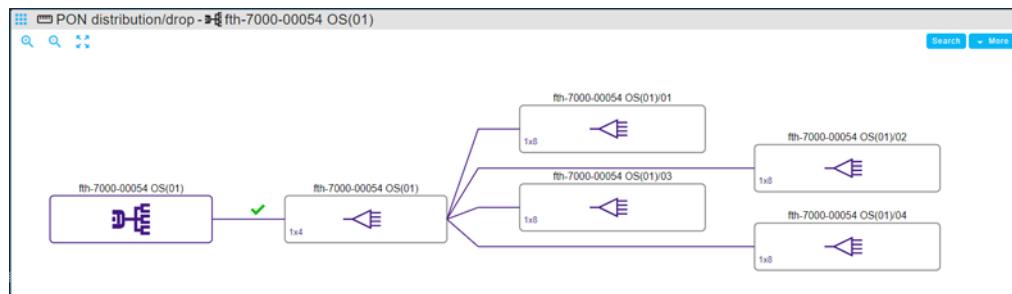


Figure 168 PON Topology

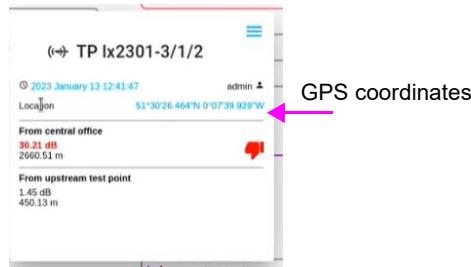


Between the OTU and the first splitter, a check, pass () or fail (), is displayed: it indicates the pass or fail measurement of the feeder. Click on it to display the SLM view and trace for this measurement.

1 Click on one object icon to open the information about this object.

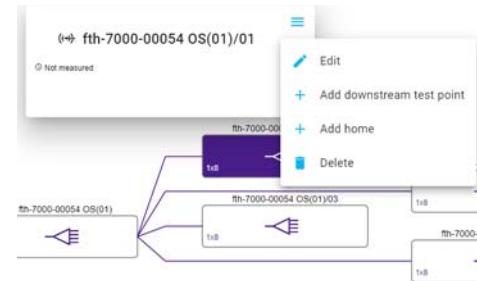
If alarms are defined for the object, the alarm information are displayed.

Figure 169 Information for Test Point in alarm



When a reflector is associated to a test point via the Field Application, this last one is able to generate the GPS coordinates for this test point. Those coordinates are then displayed in Topology: click on those coordinates to display the test point onto a map (previously configured in ONMSi).

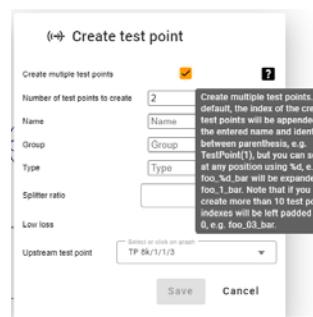
- 2 Click on the icon to open a menu into which you can:
 - **Edit** (modify) the object name,
 - **Add downstream test point**
 - **Add home**
 - **Delete** the element



Adding Downstream test point(s)

Click on **Add downstream test point** to open a new box and configure the new test point(s):

Figure 170 Create test point(s)



Select **Create multiple test points** parameter to define several test points in bulk using a naming convention; click on the **?** icon to display the help information.

Press **Save** once test point(s) is/are created.

Creating Home(s)

Click on **Add Home** and configure the new Home(s) to be added to the PON:

Figure 171 Create Home(s)

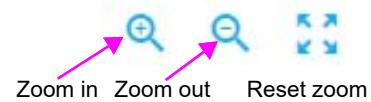


Select **Create multiple homes** parameter to define several homes in bulk using a naming convention; click on the **?** icon to display the help information.

Press **Save** once Home(s) is/are created.

Zoom function

Zooming is available with the zoom tools available on the upper left part of the Topology screen.

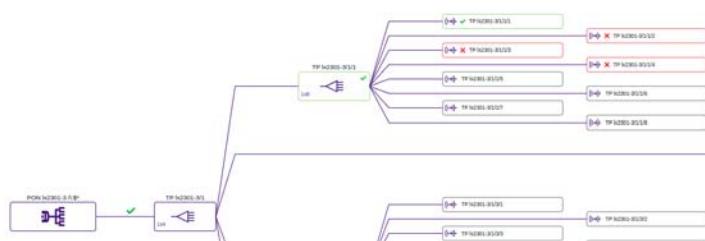


Colors

The colors of the PON depends of the view for the Topology:

In **Construction** view, the pass/fail status is defined on peaks association:

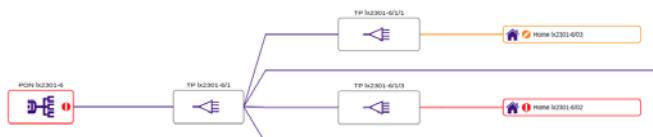
Figure 172 Construction view with alarms



- Grey: Not tested
- Green: Successfully tested
- Red: failed Test

In **Monitoring** view, where only the homes and their parent test points/splitters) the alarm status is displayed:

Figure 173 Monitoring view with alarms



- Grey: not monitored/not associated to a reflector peak
- Violet: monitored and normal
- Orange: failed test after a maintenance test (severity major)
- Red: failed test after a maintenance test (severity critical)

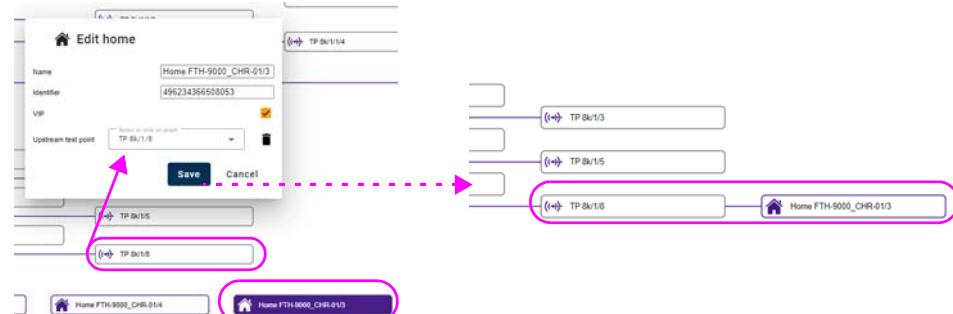
Associate / Dissociate

To associate/disassociate Test Point and home.

To associate a home and a test point:

- 1 Select the **Home** and click on **Edit**
- 2 Click then on the **Test point** you want to connect directly on the Topology scheme, or select the Test Point on the list **Upstream test point** from the Edition menu.
- 3 Click on **Save** button.

Figure 174 Home - Test point association



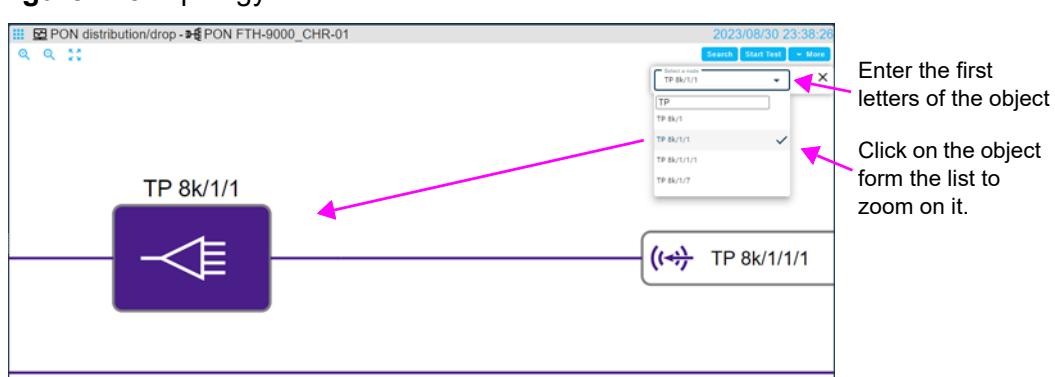
To dissociate a home, you just need to **Edit** the Home and press to remove the Test Point.

Searching an object in the Topology

To easily find any object from the Topology (home, test points...);

- 1 Click on **Search** button and enter the first letters of the searched object.
 - 2 Select the object to be found in the list.
- The display is zoomed on the searched object, which is highlighted.

Figure 175 Topology - Search tool



Downloading CSV file

Click on **More** button in Topology screen, and click on **Download CSV** to save a CSV file for the PON.

The generated file will give access, for one PON, to all the Test points and Homes construction information.

This file can be opened using a spreadsheet program (Excel™...)

ONMSi PON Field application

The ONMSi PON Field application can be used for:

- Testing a test point where the reflector is plugged
- Associating a home to a peak where the reflector is left
- Testing Home where the reflector is left

The field application is available from the URL: <https://<server address>/m/>

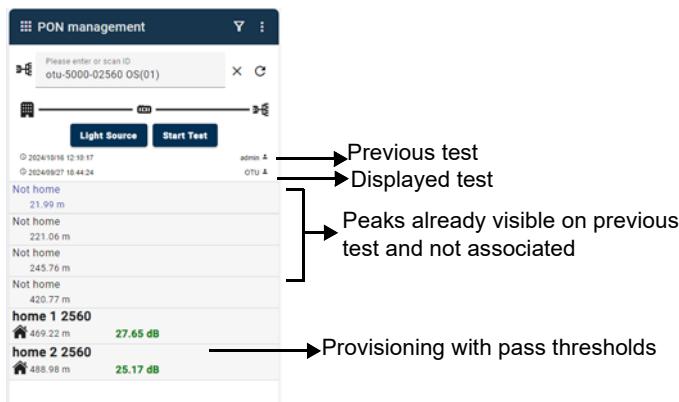
The user must have the appropriate permissions for using the field app.

After login:

- 1 Click on **PON management**.
- 2 Enter the first letters of the PON name for which you want to display the results.

The [Figure 176](#) shows the details of the display:

Figure 176 Test result display



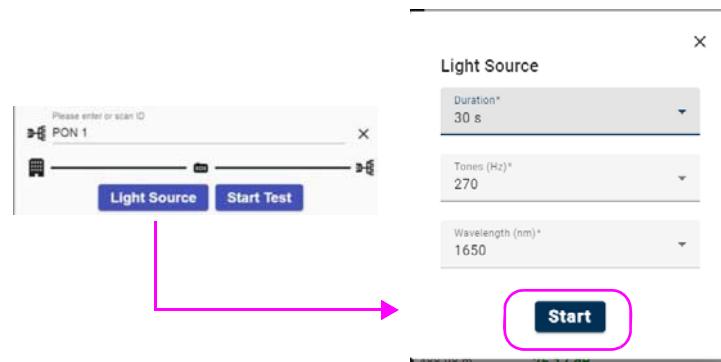
Display of Missing/New according to PON Setting

The peak status depends on the settings defined in the ONMSi System Settings screen: see "[“PON Test” on page 179](#)".



Light Source

If available on the OTDR, a light source can be started. Click to configure the Light source (Duration / Tones / Wavelength) and press **Start**:



Calibration

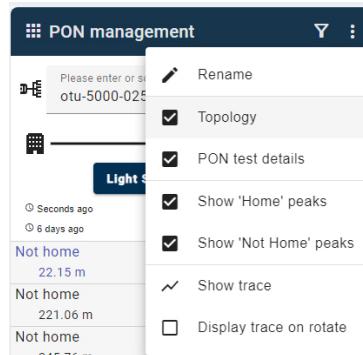
If the PON is not calibrated, a calibration is run by clicking on **Calibrate** displayed instead of start test if the auto calibration is disabled.

Calibrate

Configuration of the PON field application

Click on the icon to open the PON menu and perform several actions on display and on test points:

Figure 177 PON configuration



Rename

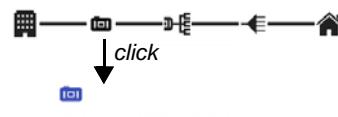
Rename the Home, PON or Test Point displayed: Name / Identifier (Home) / Additional Attributes

Create new test point (if a Splitter is selected)

Enter a Name and Additional Attributes to create a new test point

Select to display the graphical representation of the selected component:

Topology



OTU: otu-8000e-10548

Click on one element (turns blue) to display its name under the topology representation.

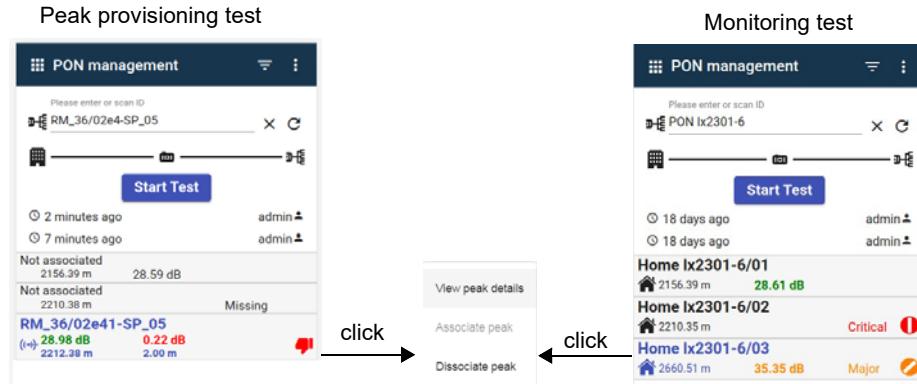
PON test details	Display the history of PON tests under Start button:	<input type="radio"/> 2 minutes ago <input type="radio"/> 7 minutes ago	admin
Show «Home» peaks & Show «No Home» peaks	Select those parameters to display the Home and/or the other peaks type on the results screen		
Show trace (active if a PON is displayed)	Display the results trace of the tested peak.		
Display trace on rotate	Select to rotate the trace when the instrument is rotate.		

Performing an OTDR test

- 1 An OTDR test can be triggered by selecting **Start Test**.

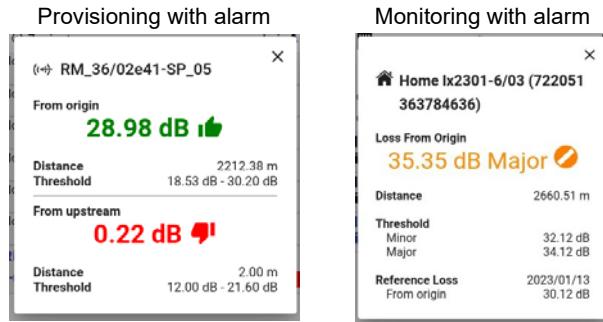
The test result displays the list of the peak with distance, peak level and Insertion loss.

Figure 178 Peak results



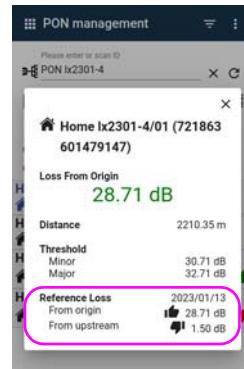
The test point displays:

- The Insertion Loss from the Origin, and the distance.
 - The Insertion Loss on the Upstream test, if any, and the distance.
 - The alarm status if alarm thresholds are defined:
 - test does not exceed alarm thresholds
 - test exceeds alarm thresholds
- 1 Click on one peak to open a sub-menu and click on:
 - **View peak details** to display the details of the selected peak.

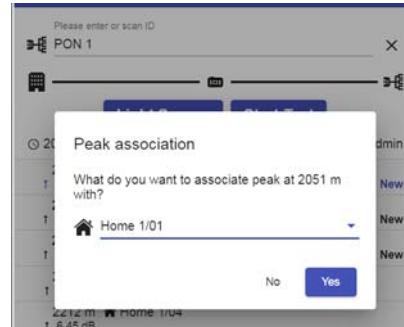


In case the provisioning for the monitored peak was defined with thresholds, the pass/fail status is displayed:

Figure 179 Monitored peak details with provisioning status



- **Associate peak / Dissociate peak:** It is asked to select the test point or the home to be associated if the test was triggered from the PON.



Once the association is performed, an icon displays:

- the Insertion Loss measurement lies within the thresholds
- the Insertion Loss measurement exceeds the thresholds

A confirmation is required when a dissociation is performed.

GPS coordinates

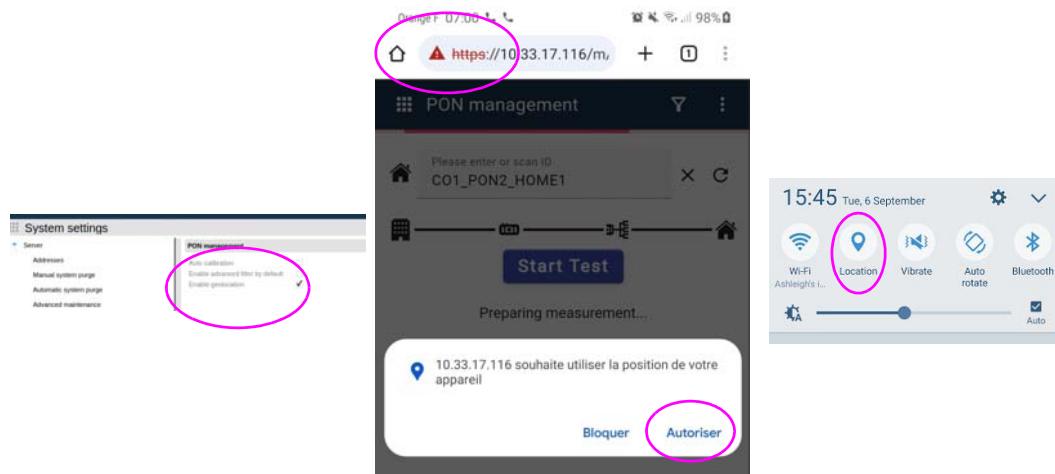
In the Filed application, the GPS coordinates can be indicated in order to be sure the technician performing the measurements is at the good location.

Pre-requisites to use GPS coordinates in Field application

The use of the GPS coordinates in the Field application is possible exclusively if:

- Server is in https
- System settings "Enable geolocation" is flagged (see Field Application settings page 192)
- User has authorized localization on his mobile: this will be asked as soon as the user triggers a measurement from the Field application.
- "Location" is enabled on the user mobile phone

Figure 180 GPS authorizations

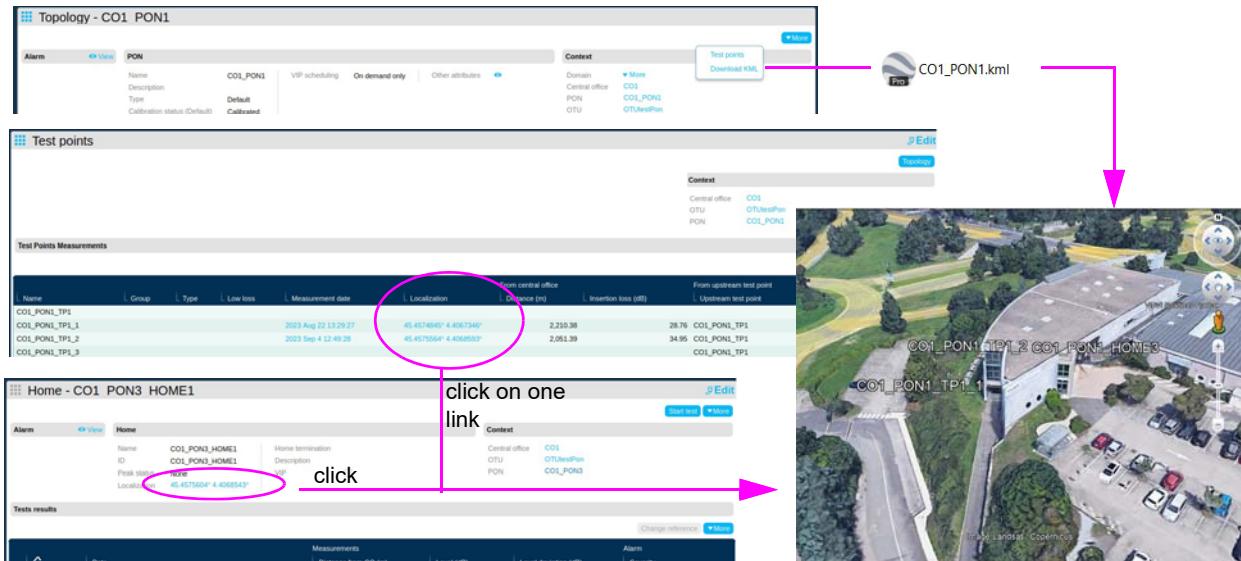


GPS information in ONMSi

Once a measurement is performed from Field application, the GPS information is available in several screen on the ONMSi:

- From the **PON Topology** screen, the KML file with all recorded test points, can be downloaded: click on **More > Download KML**.
- From the **Home** dashboard, and from the **Test Point** dashboard, a link toward the location map is available:
 - In **Test point** dashboard, a new column **Localization** is available and display a link for each test point
 - In **Home** dashboard, the link is available in the details window, on the upper part of the screen.

Figure 181 Links to location on map



NOTE

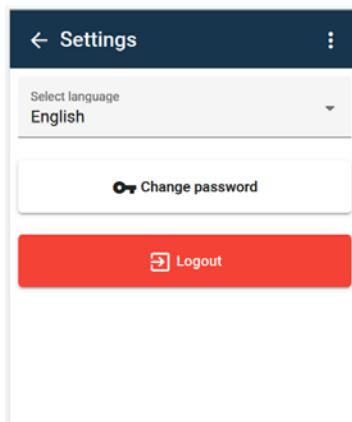
GPS coordinates are stored in Fiber Analytics.

Modifying the application settings

To modify the settings of the ONMSi Field application:

- 1 Click on the icon on the upper banner and click on **Settings** Settings .

Figure 182 ONMSi Field settings



- 2 Modify the **Language** of the application.
- 3 Click on **Change password** to modify the password for connection: enter the current password and twice the new password, then confirm clicking on **Change password**.
- 4 Click on **Logout** to exit from the current session.

VIP Permanent Monitoring

Associated to the Point to multiple point (P2MP) solution, commercial software option 'E9iVIPMON100' allows to add monitoring and demarcation feature.

To know if this software is validated and to know how many VIP can be declared, please check under your ONMSi license page.

Figure 183 License view

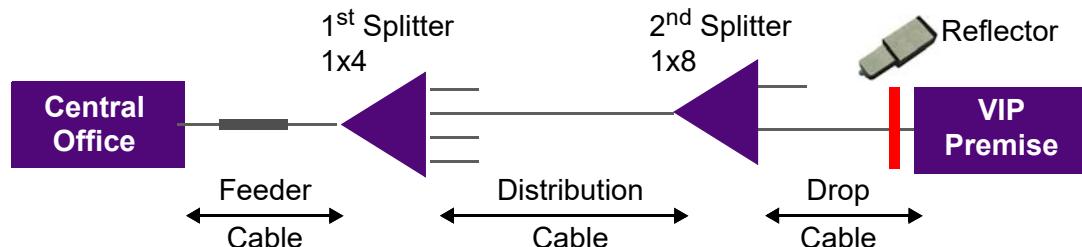


The number written in front of VIP homes provides the number of homes which can be declared as VIP.

This software option offers two features:

- 1 **VIP monitoring:** allows to identify 'Home' with a reflector permanently installed. The associated reflectance peak is monitored 24/7 and an alarm is generated in case of fiber break appears along the fiber route from central office (OLT) to home (ONT), affecting this VIP customer.
- 2 **Demarcation:** associated to the VIP monitoring feature, demarcation helps to identify the affected section of the network (Feeder, distribution, drop) and to locate the fiber break in terms of distance if it's located in feeder or in distribution.

Figure 184 PON Network with VIP Monitoring option



- Feeder up to 10 km
- Up to 16 VIP per OLT/ Switch port
- 2 stages of splitters
- Max 1 to 64 splitting ratio
- First Splitter: 1 by 4 or 1 by 8
- Distribution up to 2 km
- Drop up 200 m
- 1 reflector at VIP premise

Limits of the software

VIP Monitoring has been designed with the limit of up to 50 PON (OLT) per OTU. Demarcation has been designed with the following assumptions:

- PON architecture of two stages of splitters (1x4 following by 1x8)
- All the fibers belong to the same optical core cable

- Only complete cable break is considered, meaning all the fibers belong to the cable are cut. Partial degradation or partial cable break can introduce diagnostic error.
- The second splitters (mainly the farthest) can be identified with a reflector

Identifying the Home pass

The VIP Monitoring/Demarcation is a complementary feature of P2MP function, the following explanation starts when an OLT/PON is defined, set up and calibrated: see “[PON Calibration](#)” on page 140.

Identifying the home pass as VIP can be done in two way:

- 1 When home associated to PON OLT is imported, Home can be identified as VIP, from the datasheet file.

Figure 185 Identifying the Home as VIP

Name	Home identifier	Description	Upstream test point	VIP	Internal key	Termination type	PON External key
VIP 01	V 01,ODN 01					ODN 001	
VIP 02	V 02,ODN 01					ODN 001	
VIP 03	V 03,ODN 01					ODN 001	
VIP 04	V 04,ODN 01					ODN 001	
VIP 05	V 05,ODN 01					ODN 001	
VIP 06	V 06,ODN 01					ODN 001	
VIP 07	V 07,ODN 01					ODN 001	
VIP 08	V 08,ODN 01					ODN 001	
Distribution Leg 1	L 01,ODN 01					ODN 001	

- 2 At any time, a home can be identified a VIP by checking its associated VIP box on the ONMSi application: click on **Edit** in the PON page, and in the **Test result** box, select the box **VIP** of the **Home** which must be identified as VIP.

Figure 186 Home identification

The screenshot shows the ONMSi interface for managing a PON port named 'TMAPRLE/2'. The 'Topology' tab is selected, displaying a table of optical nodes (ONUs). The last column of the table is labeled 'VIP' with a checkbox. One row in the table has the 'VIP' checkbox checked, indicated by a pink arrow. Other columns include 'ID (Name)', 'Reflector', 'Termination', 'Type', 'Attached home', 'Reference peak', 'Detail', 'Severity', 'Changed', 'Measurements', 'Distance from CO (m)', and 'Level (dB)'. The table also lists various test results and calibration details.

When a VIP is added, ONMSi page shows the number of VIP tokens already used based on the quantity allowed by license.

Starting VIP Monitoring

As soon as one VIP associated to PON /OLT is declared and saved, the associated PON test is added to the monitoring cycle of the existing OTU.

Every day, 24 hours a day, the PON/OLT test is continuously done checking if the reflectance peak associated to the declared VIPs are still here or not.

Figure 187 PON Monitoring Test

Line	Test	Severity	Execution Last date	Allocated time (%)
Example of Fiber Cut at near end ▲	Pass		2020 May 14 21:26:39	
Example of Injection Fault ▲	Pass		2020 May 15 00:21:33	
OTU NORTH_01 (PON) ▲	Pass		2020 May 14 21:26:39	
VIAVI APV HQ to VIAVI APV Exchange ▲	Pass		2020 May 14 21:23:00	
VIAVI APV HQ to VIAVI Industrial Park ▲	Pass		2020 Apr 14 23:57:26	
VIAVI APV HQ to VIAVI Industrial Park ▲	Pass		2020 Apr 14 00:40:40	

At this stage, if a complete cable break appears, an alarm is going to be generated identifying the VIPs who are impacted by this incident.

Figure 188 Alarm on a VIP

Alarm

Name: PON_PON_UHR_2-2, Type: VIP scheduling, Status: Calibrated, Severity: Critical

Tests History

Date	Time	Calibration last run	Calibration value	Severity
2020 May 20 20:42:33	2020 May 20 20:42:33	2020 May 20 20:42:33	0.20 dB from 400.00 to 500.00 dB	Critical

Measurements

Measurement	Level (dB)	Level deviation (dB)	Delta	Sensitivity	Changed	Demarcation peak	Attached Name	Type	Termination	Refactor	ID (Name)	Description
Distance from CO	-0.28	New peak	0.28	Not referenced								
Distance from CO	-0.34	New peak	0.34	Not referenced								
Distance from CO	-0.21	New peak	0.21	Not referenced								
Distance from CO	-0.40	New peak	0.40	Not referenced								
(13.002.00)	0.00	Outside limits (-1.00)	1.00	Missing peak	Critical		Home	PBG-00B			20201704121204_Phone	
(13.048.00)	0.00	Outside limits (0.07)	0.07	Missing peak	Critical		Home	PBG-00B			20201704121204_Phone	

Alarm viewer

ID	Creation	Last update	Sensitivity	Ack	Clear	Log	Specific problem	Additional info	Description	Probable cause	Last cause
3108	2020 May 20 20:42:33	2020 May 20 20:42:33	Critical				PON		2 VIP down	Threshold crossed	

To activate the demarcation feature, an associated test (P2P) must be created. This test will be automatically triggered when an optical issue impacting one of declared VIPs is reported. The purpose of this test will be to identify the section of network (feeder, distribution, drop) creating the issue.

NOTE

As soon as a VIP is declared, if there is an existing test (P2P) is declared on the PON/OLT OTU's port, the schedule of this test will be set up as 'Test on Demand'.

In conclusion, the PON test is scheduled 'as often as possible' and the Demarcation test is scheduled 'On demand only'.

Setting up demarcation

As described above, the purpose of this test is to identify the section of network (feeder, distribution, drop) impacting at least one VIP.

As associated with PON Test, this demarcation test is triggered in case of VIP is affected by an alarm.

- 1 Create a link on the same port as the PON TEST:

In the Port association page, select the port, then click on **More > Create a Link**.

Figure 189 Creating a link

Port	Link Name	PON Name	Type	PON calibration	Zone (m)	Level (dB)	Deviation (dB)
OS(1)	Link PON_PON_UHR_2-1	PON_PON_UHR_2-1	MOD C 10ns 8cm	Calibrated	495.00 - 505.00	-0.27	
OS(2)	Link PON_PON_UHR_2-2	PON_PON_UHR_2-2	MOD C 10ns 8cm	Calibrated	495.00 - 505.00	-0.20	

- 2 Define the OTDR measurement which will be used as reference:

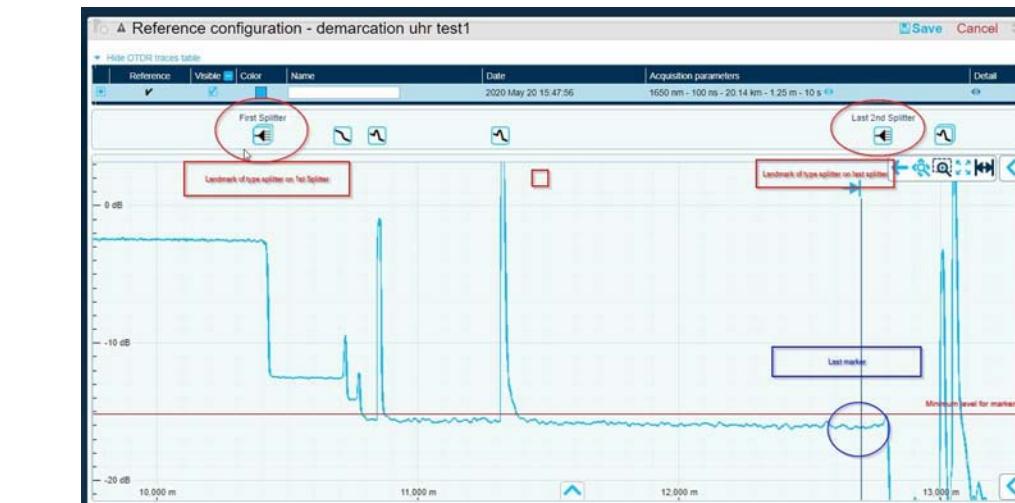
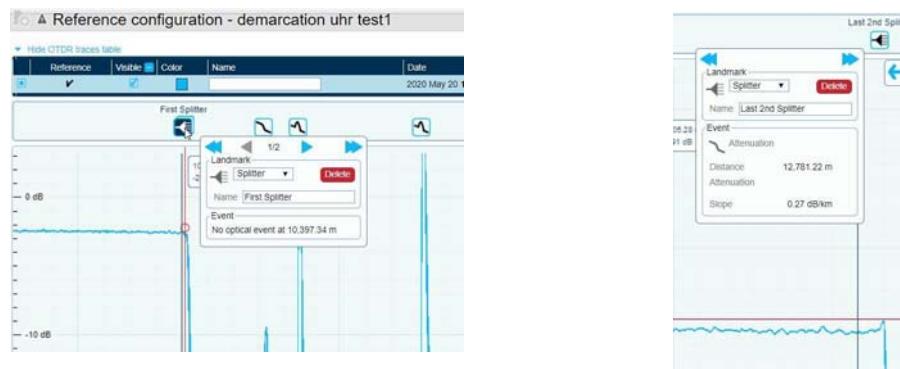
- The OTDR parameters must be manually selected with the purpose to be able to identify the farthest second splitter. Don't use auto-provisioning or automatic setup.
- The parameters depend on the type of your OTDR module and the topology of your PON

Figure 190 OTDR Measurement parameters

- 3 Along the OTDR trace, the first splitter and the farthest second splitter must be identified as landmark:
 - Select the optical event on the OTDR trace which corresponds to the first splitter, identify it as **Landmark**, set up it as splitter type and name it as 'first splitter'.
 - Use the arrows to select the optical event on the OTDR trace which corresponds to the farthest second splitter, identify it as **Landmark**, set up it as splitter type and name it as 'second splitter'. Having a reflector installed at this splitter is a real help.

First splitter must be identified for demarcation between feeder and distribution

Farthest second splitter must be identified for demarcation between distribution and drop



NOTE

Don't hesitate to break the 6 dB rule above the noise floor to position the last marker associated to the farthest second splitter.

In this case for demarcation test, ignore the warning message.



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

This test will be scheduled 'on demand only' and is triggered when at least one of VIP associated to this PON/OLT is in alarm.

Alarms Viewer

Demarcation

The P2P test previously defined and associated to the PON/OLT test helps to identify the section (feeder, distribution, drop) which affects the VIP in alarm.

Except for drop section, the location of the fault is provided if possible.

Demarcation: Drop section

In alarm viewer, the alarm identifies affected PON/OLT, the section (DROP) and the number of VIPs impacted (2).

Figure 191 Alarm Viewer: Drop section

ID	Creation	Last update	Severity	Ack	Clear	Origin	Specific problem	Additional info	Description	Probable cause	Root cause
3119	2020 May 20 17:16:57	2020 May 20 17:16:57	Critical			PON PON_UHR_2-3	DROP_CABLE	DROP_CABLE - 2 VIP down	Threshold crossed	Other	
3118	2020 May 20 17:15:54	2020 May 20 17:17:13	Critical			PON PON_UHR_2-4	DROP_CABLE	DROP_CABLE - VIP 205846475314370 down	Threshold crossed	Other	

1 Open the alarm to identify the VIP.

Figure 192 Alarm details on Drop section

Alarm detail		Information		Context			
	Critical	ID: 3119	Creation: 2020 May 20 17:15:57	Last comment:	Domain: Default		
Severity: Critical	Acknowledged: No	Last update: 2020 May 20 17:15:57	Origin: PON PON_UHR_2-1	Alarm type: Quality of Service	OTU: stu-6000e-adt_18_68		
Cleared: No	Specific problem: PON	Probable cause: DROP_CABLE - 2 VIP down	PON: PON PON_UHR_2-1	Description: Threshold crossed			
		Duration (DD HHMM.SS): 00:02:07.42					
Demarcation		Localization					
OTDR distance: N/A	Demarcation: DROP_CABLE	OTDR trace:		Fault in drop cable			
VIP homes in alarm							
VIP: 2058007781124761 (Home PON_UHR_2-1)		VIP: 2058007781124761 (Home PON_UHR_2-1)					
History							
Date: 2020 May 20 17:15:57	Alarm event: Critical	Ack.: Clear	User: Description:Comment: DROP_CABLE	Charges: 2 peaks	PON test: Success: 1		
				See:	Alerts and acknowledgments: Receipts: 1 Errors: 0 Date:		

At any time, you can access to the associated PON test and OTDR trace.

Demarcation: Distribution section

In alarm viewer, the alarm identifies affected PON/OLT, the section (Distribution), plus the distance of fault location and the number of VIPs impacted (2).

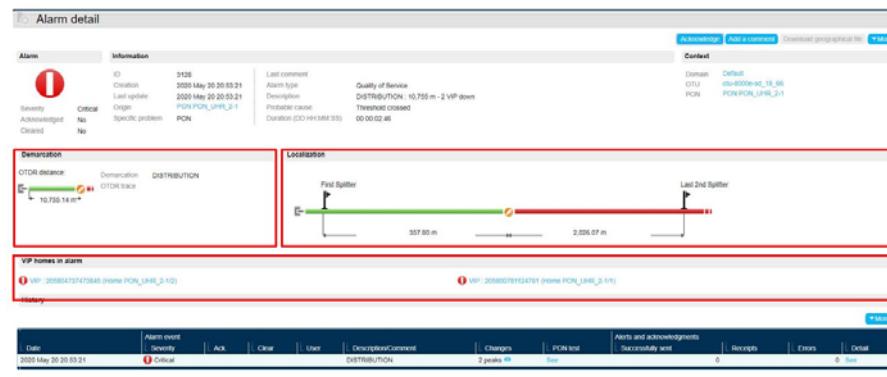
Figure 193 Alarm Viewer: Distribution section

Alarm viewer											
ID	Creation	Last update	Severity	Ack	Clear	Origin	Specific problem	Additional text	Description	Probable cause	Root cause
3128	2020 May 20 20:53:21	2020 May 20 20:53:21	Critical			PON PON_UHR_2-1	PON	DISTRIBUTION	DISTRIBUTION : 10.755 m - 2 VIP down	Threshold crossed	
3127	2020 May 20 20:52:58	2020 May 20 20:53:21	Critical			LINK PON PON_UHR_2-1	Attenuation	FIBER_CUT	Fiber cut - 10.755.14 m	Threshold crossed	Fiber Break

Open the alarm window and access to 3 major information:

- to identify the VIPs affected by the optical issue
- to identify the section (Distribution) and to locate the optical fault from OLT,
- to locate the fault from the first splitter.

Figure 194 Alarm details on Distribution section



Demarcation: Feeder section

In alarm viewer, the alarm identifies affected PON/OLT, the section (Feeder), plus the distance of fault location and the number of VIPs impacted (2).

Figure 195 Alarm Viewer: feeder section

Alarm viewer											
ID	Creation	Last update	Severity	Ack	Clear	User	Specific problem	Additional text	Description	Probable cause	Root cause
3129	2020 May 20 21:04:19	2020 May 20 21:04:19	Critical				LINK power level value < 0.1	AMPLIFIER	FIBER_CUT	FIBER CUT - 10.742.89 m	Threshold crossed
3131	2020 May 20 21:04:12	2020 May 20 21:04:12	Critical				PON PON_UHR_2-1	PON	FEEDER	FEEDER : 10.763 m - 2 VIP down	Threshold crossed

Open the alarm window:

- to identify the VIPs affected by the optical issue
- to identify the section (feeder) and to locate the optical fault from OLT,
- to locate the fault from the OLT and to first splitter.

Figure 196 Alarm details on Feeder section

The screenshot displays two main windows from the ONMSi PON System:

- Alarm detail** window (top):

Alarm		Information				Context	
Severity: Critical	Origin: PON	ID: 3131	Creation: 2020 May 20 21:04:12	Last comment: PON_PON_UHR_2-1	Alarm type: Quality of Service	Domain: Default	
Acknowledged: No	Specific problem: PON	Last update: 2020 May 20 21:04:12	Description: FEEDER 10.753m - 2 VIP down	Probable cause: Threshold crossed	OTU: ub-400Ww-ct_1E_08		
Closed: No			Duration (DD HH:MM:SS): 00:00:39:24		PON: PON_PON_UHR_2-1		

 A fiber map shows a green line segment labeled "FEEDER" with a length of 10.752 59 m. A red vertical line segment labeled "first splitter" is located at 9.721 48 m.
- Alarm viewer** window (bottom):

ID	Creation	Last update	Severity	Ack.	Clear	Origins	Specific problem	Additional test	Description	Probable cause	Root cause
3130	2020 May 20 21:04:12	2020 May 20 21:04:12	Critical			PON_PON_UHR_2-1	FIBER_CUT	Fiber cut - 10.752 59 m	Threshold crossed		
3131	2020 May 20 21:04:12	2020 May 20 21:04:12	Critical			PON_PON_UHR_2-1	PON	FEEDER	FEEDER : 10.753 m - 2 VIP down	Threshold crossed	Fiber break

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 168
- “Configuring an automatic purge” on page 168
- “Configuring the unit preferences” on page 169
- “Users” on page 170
- “Links configuration” on page 175
- “Point to Point Configuration” on page 180
- “Configuring e-mail/sms alert profiles” on page 184
- “Configuring Desktop alert profiles” on page 187
- “Configuring the Media servers” on page 188
- “Additional Attributes” on page 191
- “Field application” on page 192

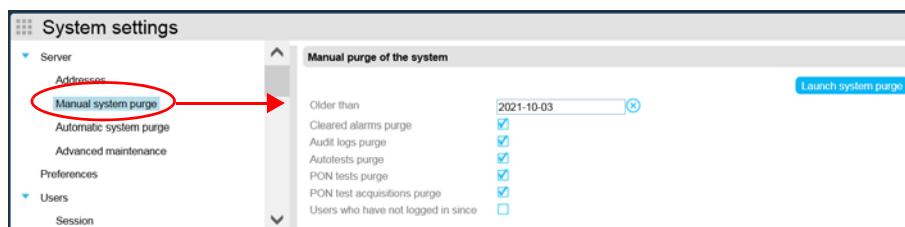
Configuring and launching a manual purge

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 Select **Users who have not logged in since**: this will delete users not logged since the date defined above, keeping the connection of the last user available.
- 5 Click on **Launch system purge** to start the process.

Figure 197 Manual system purge



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



CAUTION

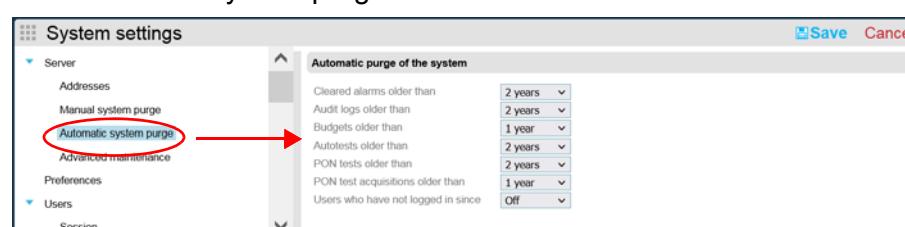
The user must have the system purge permission to launch the process.

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 198 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 199 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.

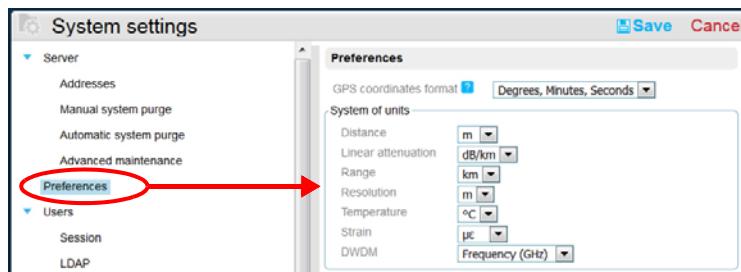
Configuring the unit preferences

From the System Settings screen, the units can be modified.

Once **System settings** page is opened:

- 1 Click on **Preferences**.
- 2 Click on **Edit** to modify the current parameters
 - For **GPS coordinates format**, select **Signed Decimal Degrees**, **Decimal Degrees** or **Degrees, Minutes, Seconds**.
 - For **System of units**, define the unit for **Distance**, **Linear attenuation**, **Range**, **Resolution**, **Temperature**, **Strain** and **DWDM**.

Figure 200 Preferences



Users

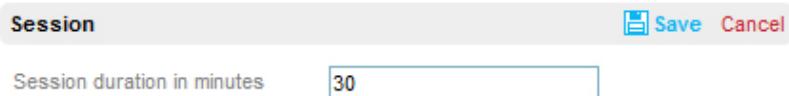
The **Users** page allows to define parameters for Session, LDAP and password policy.

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 201 Session duration



Configuring the LDAP



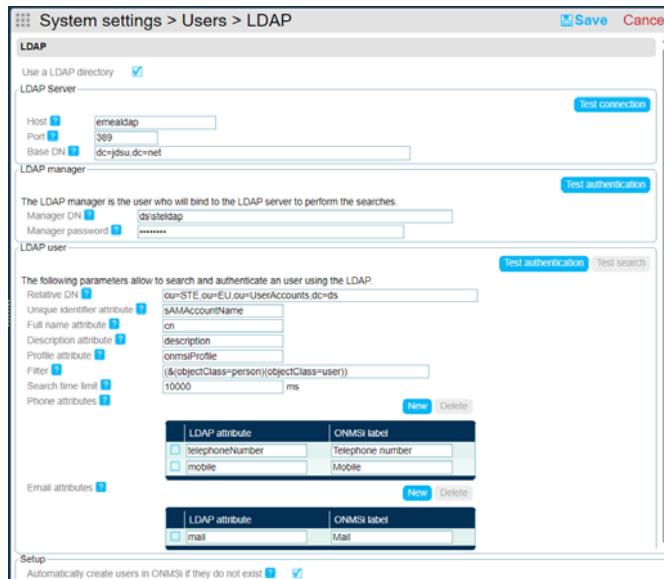
CAUTION

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 202 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

- 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
- 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.
- Enter/modify the parameter of the LDAP manager:
 - Manager DN: Manager domain name
 - Manager password: Password to access to the domain
 - Press **Test Authentication** before going to **LDAP User**

LDAP User configuration

Contact your IT to complete the LDAP user fields.

Configuring the password policy

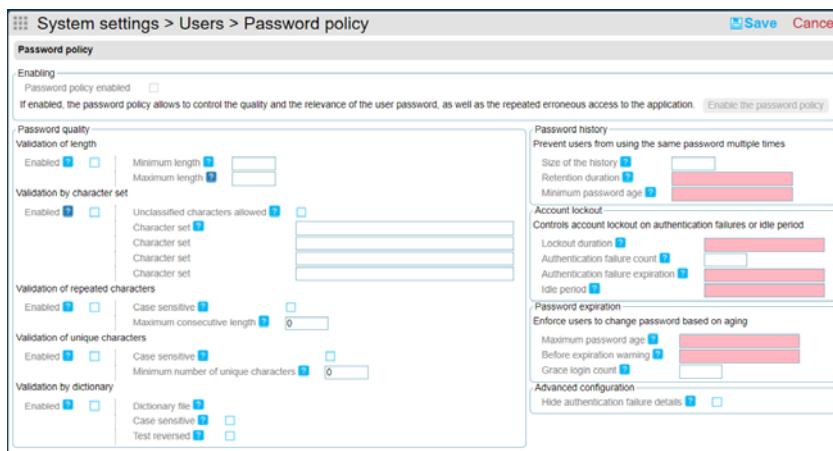
The password policy available in ONMSi allows to add restrictions and control the quality and relevance of user passwords for the System, as well as the repeated erroneous access to the application.

- 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 203 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), ms (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
- The location of the file used as dictionary is: /opt/rfts_apps/conf/opendj/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 can 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).

Single Sign On screen

Once **System settings** page is opened:

1 Click on **Users > Single Sign On**.

The right window displays the Template used for extracting data.

Figure 204 Single Sign On



Links configuration

The **Links** page allows to define the Link types and to configure the PON.

Link types

Click on **Link types** to set a link type, for every links.

This link types allow to define the parameters in order to provide the instrument the measurement configuration, but also for the PONs configuration.

Figure 205 Links type configuration

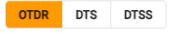
The screenshot shows the 'Link type' configuration page. The 'Name' field is 'P2P_Link_SS'. The 'Usage' tab is selected. In the 'Topology' section, 'PON' is checked. The 'PON type' section includes 'Acquisition conditions for new calibration' (Wavelength: 1650 nm, Range: 20 nm, Resolution: 16 pm, Pulse width: 10 ps, Dispersion index: 1.4695, Backscattering level: -81 dB), 'Calibration' (Automatic search reference zone, Input reference zone, Min level threshold: -4 dB, Max level threshold: 0.5 dB, Min deviation threshold: 0.5 dB, Max deviation threshold: 0.5 dB), and 'Insertion loss' (Chirp ID: 0). The 'Reflectors for field provisioning' section lists FBG-0dB and UBR-10dB. The 'Peak thresholds' section shows a graph with peak levels of -2.0, -1.9, -3.9, and -4.0 dB. The 'Feeder test conditions' section has 'All' selected, with 'Number of missing homes' set to 2 and 'Max central office level deviation (dB)' set to 3.

- 1 Select the link type to be used from the list.
Take care of the type: CFG or JSON.
- 2 Click on **Duplicate** to set a new link type according to an existing one.
or
Click on **Edit** and modify the current link type.
CAUTION: the type of **Usage** (OTDR, DTS or DTSS) cannot be modified.
- 3 Enter a **Name** for the link type.
 - Click on  if necessary to enter a description.
- 4 Once the configuration is defined (see “OTDR Link type configuration” on page 176 or “DTS or DTSS Link type configuration” on page 179), press **Save** to apply the new parameters.

Press **Export** to export either a configuration file or a JSON file.

According to the measurement defined, the configurable parameters are different.

OTDR Link type configuration

Define the link type for **OTDR** usage  :

Topology

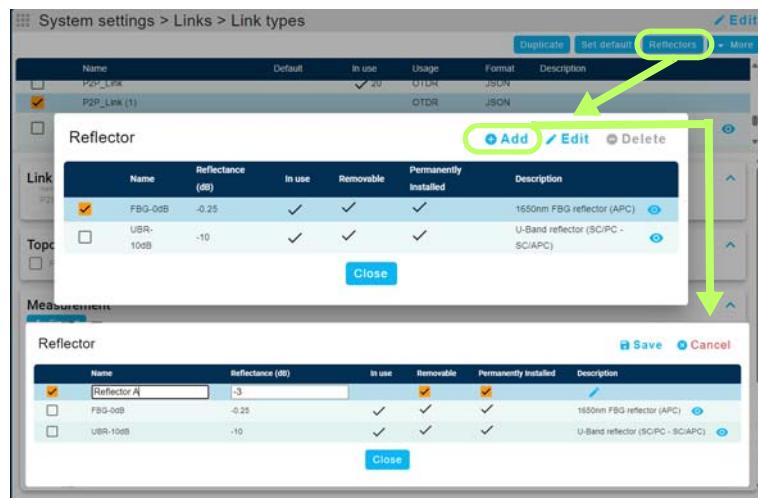
- 1 In **Topology** window, define whether the link is
 - a P2P link
 - a PON link: select PON and configure the PON type.
- 2 If an OTDR link is set, define if the link is **In service** or not.
- 3 If **PON** is selected, click on the PON type arrow and define the PON in the sub-menu:
 - a Define the **1st splitter** ratio (and the second splitter): from 1:2 to 1:28 or select **Unknown** if it is not known.
 - b Define the **1st splitter labeling**: use %L to insert the link name at any position (e.g.: foo_%L_test, will be expanded to foo_mylink_test. If the parameter is left empty, the 1st splitter creation will be disabled).
 - c The measurement settings can be changed in **Acquisition conditions for new calibration** window.
The measurement setting is applied during calibration. These settings are kept for all the PON test even if measurement setting is modified. The application of the new setting requires to re-do the calibration.
Select **Use shortest pulse width** to use the shortest pulse supported by the OTDR module. If the parameter is not selected, define the pulse width in the text box.
 - d Define new **Calibration thresholds**: Min and Max levels and Max deviation.

Define the calibration section in **Begin/End position from origin**.

- e **Insertion Loss Offset:** depending on the configuration, the calibration may be taken on a patchcord located before the WDM and ODF. In order to have an accurate Insertion Loss, an offset can be added – Per PON type - to take into the WDM and ODF loss.
- f **Reflectors for field provisioning** are listed here. If there is more than one reflector, the field tech will have to select the used reflector.

To add new reflector, leave the edition mode, and click on **Reflectors** on the top right. Click on **Edit** to modify an existing reflector or click on **Add** to configure the new reflector: Name, Reflectance, Removable or not, Permanently installed or not and a description. Press **Save** to validate.

Figure 206 Adding a reflector



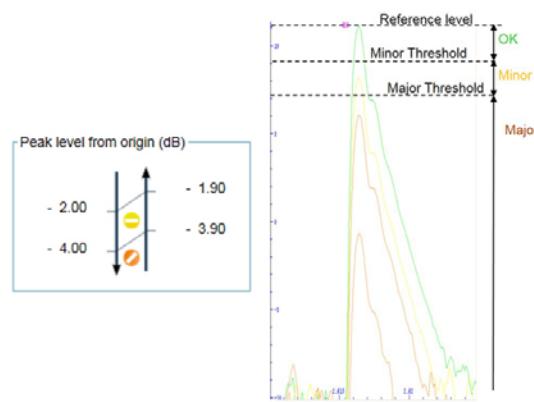
- g Define the **Peak thresholds**:

New Peak threshold: This value allows to fix a limit to determine if a peak has to be considered as a new one or ignored

Missing position: indicates the deviation allowed. In [Figure 206](#) if the peak has moved of more than three acquisition points, it is considered missing

Alarm raised in new peak: select the parameter if only peaks above “New peak threshold” are displayed.

Peak level from origin (dB): modify if necessary the alarm severity.



h Configure the **Feeder test conditions**:

Select **All** to test all feeders and define the **Max central office level deviation (dB)**.

or

Select **X** and define the **Number of missing homes** and the **Max central office level deviation (dB)**.

- 4 In the **Measurement** window, if a CFG file format has been selected (and duplicated), click on **Import** and import the configuration file to be used.
- 5 Click on **Switch to JSON** to change the CFG file format to JSON format, and configure the **Acquisition setup** and **Alarm thresholds** tabs:
In Acquisition Setup tab, configure the Acquisition Mode (SmartAcq or Auto), adjust the Averaging time and configure the Fiber Index (click on **+** to create a new one).
In Alarm thresholds tab, configure thresholds for **Splice (dB)**, **Connector (dB)** and **Link linear attenuation (dB/km)**.



The JSON configuration file support depends on the equipment used (for example, this configuration is not available with our OTU 8000) and of its software version.

Figure 207 OTDR Link type - JSON file configuration

DTS or DTSS Link type configuration

- Check the link type for **DTS** or **DTSS** usage is selected

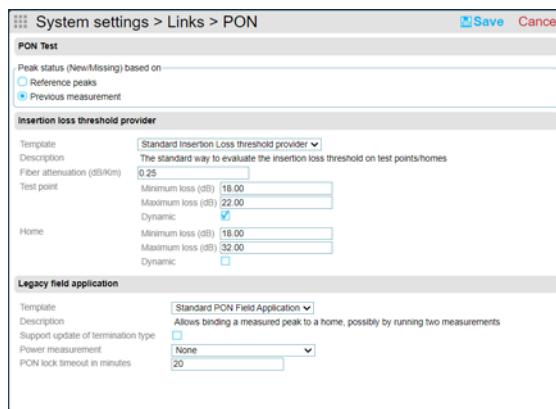
Usage OTDR DTS **DTSS**

- Click on **Import** to import a configuration file (.fo_cfg).

PON configuration

Click on **PON** to start the PON configuration.

Figure 208 PON Settings



PON Test

The peaks resulting from a PON test are compared with the reference for Home and not Home peaks. In addition, the other peaks are compared with the previous measurement if it is selected. This setting is used to show the results displayed by the PON Field Application or by the Web UI PON Test.

Insertion Loss threshold provider

The Insertion Loss threshold provider screen allows to define some alarm thresholds for Test Points and Home of the PON.

None is selected by default.

Click on **Edit** to modify the configuration:

- In **Template** parameter, select **Standard Insertion Loss threshold provider**.
- Define the **Fiber attenuation** value, in db/km.
- For **Test Point** and **Home**, define the **Minimum** and **Maximum Loss** values (in dB).
- Select **Dynamic** parameter to modify the threshold detection according to the distance of the point.

Legacy Field application

Kept for backward compatibility.

Insertion Loss Threshold plug-ins

Some plug-ins can be created to calculate the dynamic thresholds.

Figure 209 Example of thresholds for Test points and Home

The screenshot displays two interface panels. The top panel, titled 'Test Points Measurements', lists test points with their names, groups, types, low-loss values, measurement dates, distances from the central office, and insertion losses. A tooltip indicates a threshold exceeded at 22.20 dB. The bottom panel, titled 'PON Measurement Topology', shows a tree view of test results for today and yesterday, with a detailed view of a specific measurement showing its distance from CO, level, deviation, and insertion loss.

NOTE

For more information, contact your local service center.

Point to Point Configuration

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

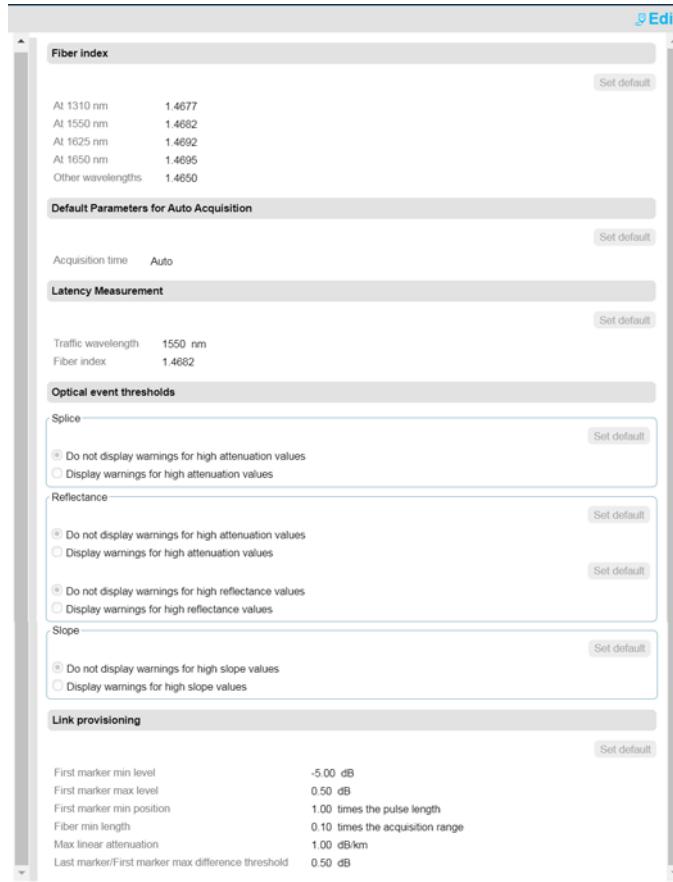
Point to Point General configuration

- 1 Click on **Point to Point** in the System settings window

The current configuration for Fiber Index, Default parameters for Auto Acquisition, Latency measurement, Optical event Thresholds and Link provisioning is displayed.

- 2 Click on **Edit** and modify the wished parameters.
- 3 Click on **Save** to save the new configuration.

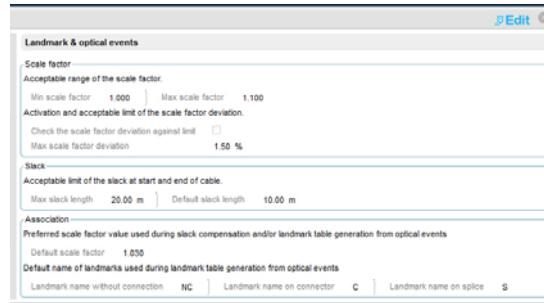
Figure 210 Point to Point: general configuration



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.

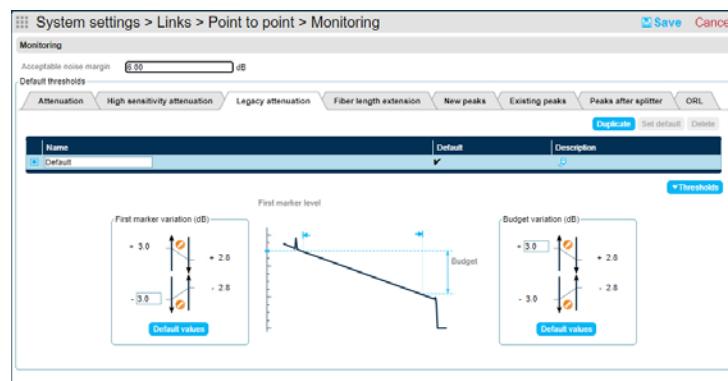
Figure 211 Configuration for Landmarks and optical events



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 / High sensitivity attenuation / Legacy attenuation / Fiber length extension / New peaks / Existing peaks / Peaks after splitter / ORL.
- 4 Click on **Save** to save the new configuration.

Figure 212 Configuration for Monitoring



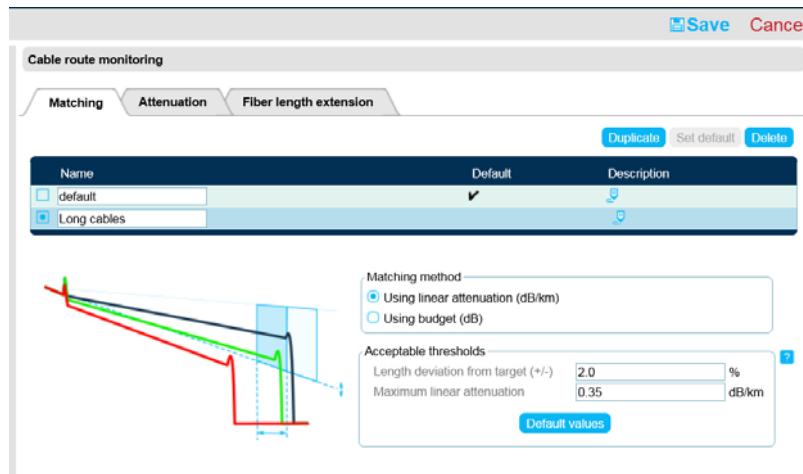
Cable route Monitoring configuration

- 1 Click on **Point to Point** in the System settings window
- 2 Click on **Cable Route Monitoring**.
The current configurations for Tolerance margins in cable route are displayed.
- 3 Click on **Edit**.
- 4 Select an existing configuration and modify the values
or

Select an existing configuration and click on **Duplicate** to copy the configuration and create a new one based on the selected one.

- 5 Modify the wished thresholds for: **Matching / Attenuation / Fiber length extension**.
- 6 Click on **Save** to save the selected configuration.

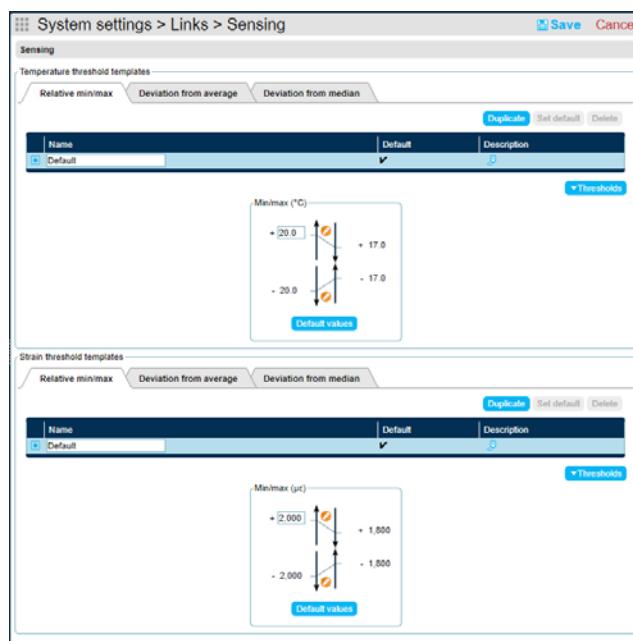
Figure 213 Configuration for Cable Route Monitoring



Sensing Configuration

The Sensing menu allows to modify the parameters for sensing configuration.

Figure 214 Sensing configuration



- 1 Click on **Edit**.

- 2 Select an existing configuration and modify the values
or
Select an existing configuration and click on **Duplicate** to copy the configuration and create a new one based on the selected one.
- 3 For both **Temperature threshold templates** and **Strain threshold templates**, modify the wished thresholds: **Relative min/max / Deviation from average / Deviation from media**,
- 4 Click on **Save** to save the selected configuration.

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 215 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.

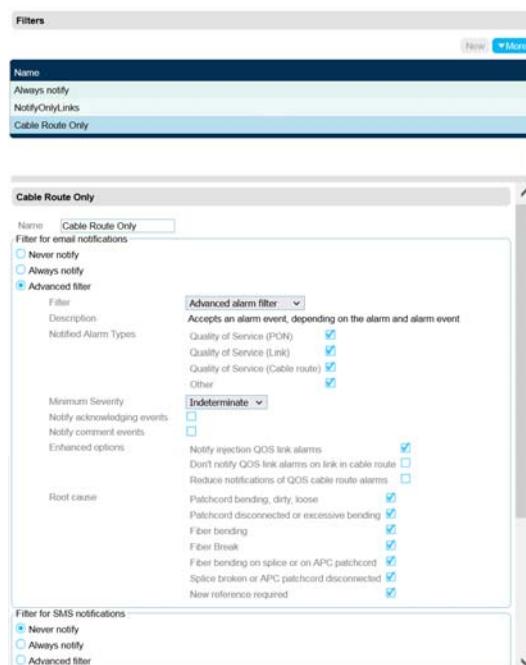
Defining filters for the e-mail notifications

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 216 Alerts > Filters



- 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) / Quality of Service (Cable Route) / Other.
 - In **Enhanced options**, select or deselect the available parameters:
 - **Notify injection QOS link alarms**: select to get notifications when alarms occur on injection of the link.
 - **Don't notify QOS link alarms on link in cable route**: select it if no alarm notification must be sent when the link belongs to a cable route, as an alarm is sent when the Cable Route is in alarm.
 - **Reduce notifications of QOS cable route alarms**: select it to only get information on start and end of the scan. If not selected, all the information during the In progress status of the scan are notified.
 - In **Root Cause**, select or deselect the root cause of the alert.
- 4 Click on **Save** to save the new profile / the modifications of the existing profile.

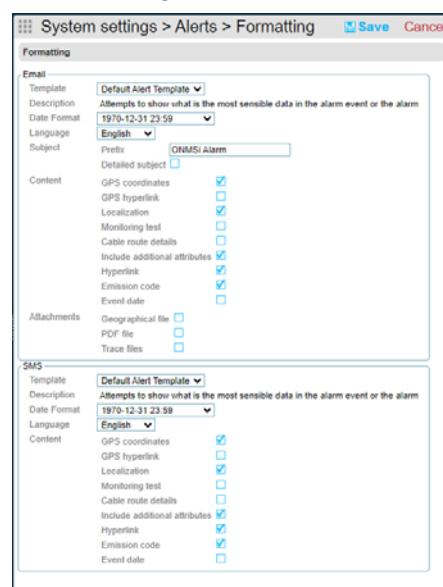
Configuring the e-mail format

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.

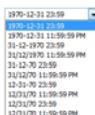
Figure 217 Alerts > e-mail Formatting



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 Select if the Detailed subject must be specified or not.

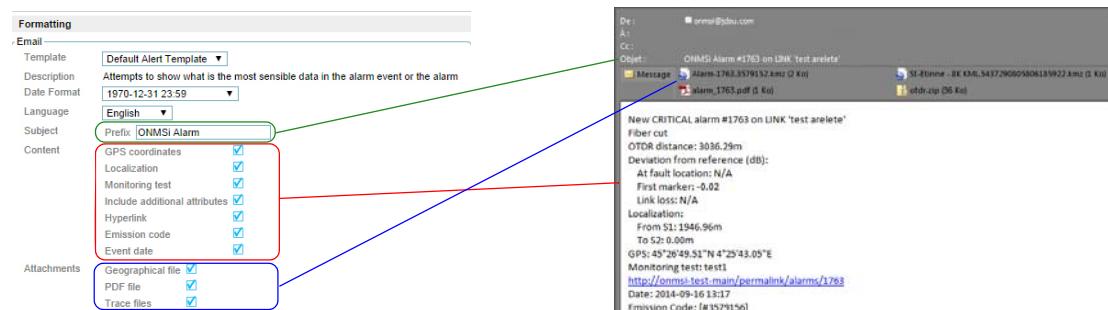
8 In the Content parameter, select the information to be contained in the e-mail.

9 In the Attachments parameter, select the type of file(s) to be attached to the e-mail: Geographical file / PDF file / Trace files.

10 Click on Save to save the e-mail format.

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

Figure 218 Example of e-mail according to formatting configured



Configuring Desktop alert profiles

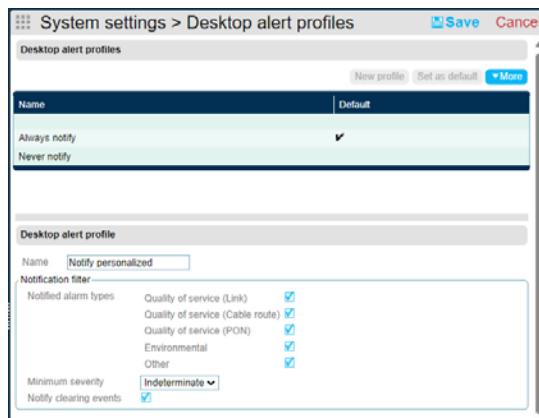
Different profile can be created to receive only specific alarm on PC.

See “[Alarm Desktop alert](#)” on page 105 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 alert notifications.**
The dialog box to create a new profile displays.

Figure 219 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 (Cable Route)** / **Quality of service (PON)** / **Environmental** / **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 188](#) 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.

Configuring the Media servers

Click on **Media** to start the configuration of the servers for e-mail and sms sending and receiving.

Configuring the e-mail server

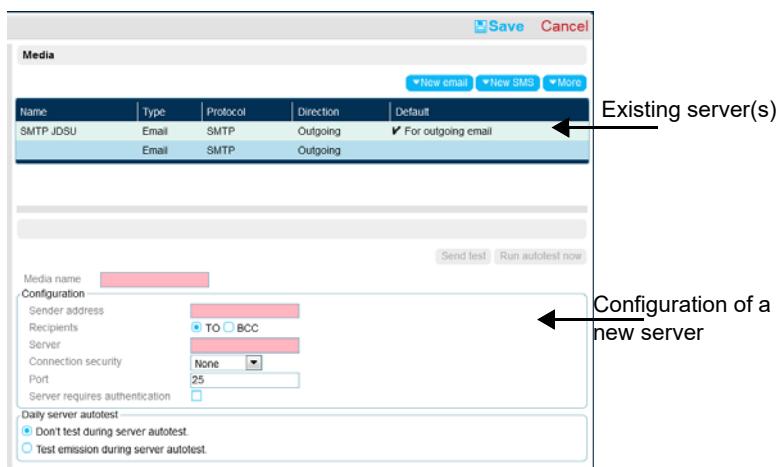
In the Media Window:

- 1 Click on **New email**.
- 2 Click on **Email using SMTP server (outgoing)** to configure the server for sending e-mail.
or
Click on **Email using POP server (incoming)** to configure the server for receiving e-mails.
- 3 Configure the server as wished.
- 4 Click on **Save** to save the new server configuration.

NOTE

Fields in red are mandatory.

Figure 220 Media > E-mail Server configuration



Configuring the sms server

In the Media Window:

- 1 Click on **New SMS**.
- 2 Click on **SMS using SMPP server (outgoing)** to configure the server for sending messages.
or
Click on **SMS using script (outgoing)** to configure the server for sending messages using a script.
- 3 Configure the server as wished.
- 4 Click on **Save** to save the new server configuration.



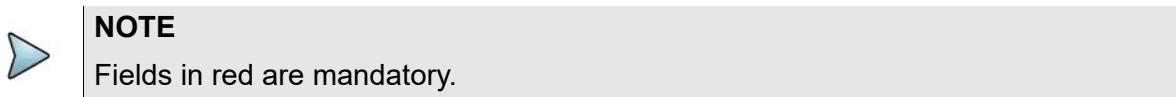


Figure 221 Media > SMS Server configuration

The screenshot shows the "Media > SMS Server configuration" page. At the top, there is a table titled "Media" with columns: Name, Type, Protocol, Direction, and Default. Two rows are listed: "SMTP JOSU" (Email, SMTP, Outgoing, checked for default) and "SMS" (SMS, SMPP, Outgoing). Below the table, there is a form for "Configuration". The "Media name" field is highlighted in red. The "Version" dropdown has "3.3" selected. Other fields include "Port" (0), "System type" (Tranceiver), "Bind Address IONI" (Unknown (0)), "Bind Address NPI" (Unknown (0)), "Sender address" (checkboxes), "Use custom source address configuration" (checkbox), "Use custom destination address configuration" (checkbox), "Maximum number of concatenated messages" (256), and "Daily server autotest" (radio buttons for "Don't test during server autotest" and "Test emission during server autotest"). Arrows point from the text "Existing server(s)" to the table header and from "Configuration of a new server" to the "Media name" field.

Plugins

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

Once **System settings** page is opened:

1 Click on **Plugins**.

The Plugins table displays.

Figure 222 Plugins

The screenshot shows the "Plugins" table. The columns are "Type", "Name", and "Description". The table lists various plugins: Alarm download template (Default Formatter), Alert notification filter (Advanced alarm filter, Wavelength alarm filter), Alert receipt handler (Default handling of alert receipts), Alert template (Default Alert Template, Raw Alert Template), Build cdm extractor (DefaultBuildCdmExtractor), Dynamic Application (Standard PON Field Application), GPS provider (FNM GPS coordinates provider), Gadget (Alarm ageing, Faults closed during last 24 hrs, Fiber fault trend, MTTR Compliance, Monitored fiber health, OTU status, Outstanding alarms, Port status). Descriptions provide details for each plugin's function.

Type	Name	Description
Alarm download template	Default Formatter	Formats an alarm with default content.
Alert notification filter	Advanced alarm filter	Accepts an alarm event, depending on the alarm and alarm event
Alert notification filter	Wavelength alarm filter	Accepts an alarm event, depending on the alarm, the alarm event, and the wavelength of the test
Alert receipt handler	Default handling of alert receipts	Finds a string like #123456 or #123456 in the subject then in the body and extracts 123456 as the receipt ID
Alert template	Default Alert Template	Attempts to show what is the most sensible data in the alarm event or the alarm
Alert template	Raw Alert Template	Shows the raw content of the alarm event without much interpretation
Build cdm extractor	DefaultBuildCdmExtractor	The default way to extract build test data from CDM.
Dynamic Application	Standard PON Field Application	Allows binding a measured peak to a home, possibly by running two measurements
GPS provider	FNM GPS coordinates provider	Provides GPS coordinates from FNM
Gadget	Alarm ageing	Repartition by duration for all alarms that have been active (even momentarily) within the time range.
Gadget	Faults closed during last 24 hrs	Repartition of faults closed during last 24 hrs
Gadget	Fiber fault trend	Number of optical alarms during a period of time
Gadget	MTTR Compliance	Pie chart representation of MTTR compliance according to service level agreement (SLA)
Gadget	Monitored fiber health	Pie chart distribution of fiber health according to associated links linear attenuation
Gadget	OTU status	OTU availability (with and without alarms, unreachable, not managed)
Gadget	Outstanding alarms	Active alarms per severity
Gadget	Port status	Port status: Number of ports (unused, monitored with/without alarm)

2 Click on **Refresh** to refresh the scripts; this can take few minutes.

Click on **More** and download the plugins on the PC (see “[Downloading data from a table / list](#) on page 112).

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 223 Additional Attributes configuration screen

Name	Type	List	Always display
domainAA	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Date		

Detail

Name: Domain1

Type: Date

Description:

Always display (unchecked)

Unique (unchecked)

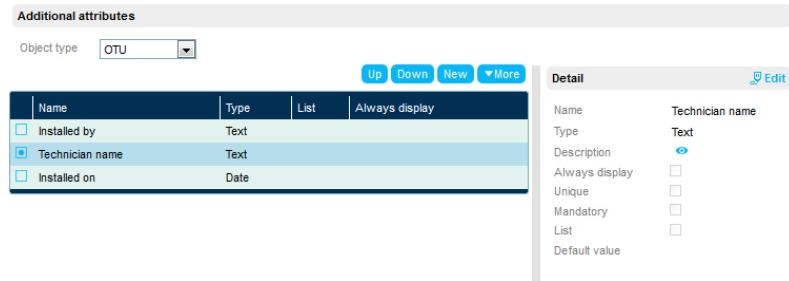
Mandatory (unchecked)

List (unchecked)

Default value: y-mm-dd

- 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 224 Additional Attributes created (for OTU)

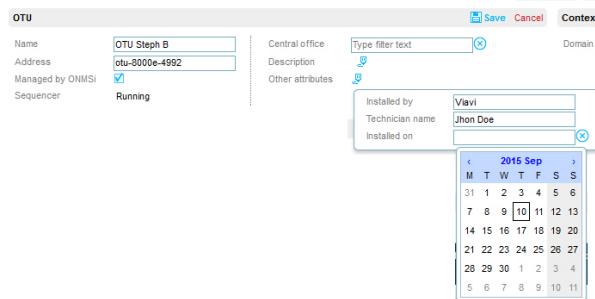


Displaying and completing the attribute

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 225 Additional Attribute in the Object dashboard (for OTU)



Field application

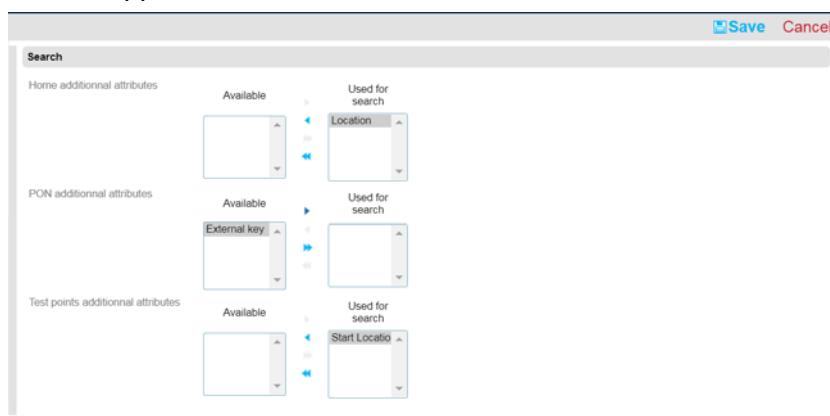
From the System settings window, dedicated zone for Field applications is available

Once **System settings** page is opened:

- 1 Click on **Field application**.
- 2 Select a category: PON Management / Scanner / Search.

- 3 In **PON Management**, click on **Edit** and
 - select **Auto Calibration** to enable auto calibration in PON application. Click on **Save** to validate.
 - select **Enable Advanced filters by default** to enable the advanced filters in PON application
 - select **Enable geolocation** to enable the function to gather geolocation during measurements, in the PON application.
- In **Scanner**, click on **Edit**, select the Current Scanner and select/deselect the formats wished. Click on **Save** to validate.
- In **Search**, define the Additional Attributes that can be Used for search, for the Home, PON and Test points (see “[Additional Attributes](#)” on page 191).

Figure 226 Field application > Search



- 4 Click on **Save** to validate the parameters.

Measurements

Topics discussed in this chapter include the following:

- “Principle” on page 196
- “Display of the measurement page” on page 196
- “Domain Management” on page 197
- “Connecting links to the OTU/FTH or to the Cable Head” on page 200
- “Starting measurements on links” on page 203
- “Results screen from measurement tests” on page 206
- “Generating a report for the links” on page 217
- “Exporting Trace, pdf and / or json data” on page 218
- “Construction/Analytics Field Application” on page 219

Principle

The Construction/Analytics view allows to manage domains (add resources), to use Cable management and to validate the network construction.

It allows to use the OTU as a measurement instrument, using the functionalities of the instrument. It allows to perform measurement tests in series.

Display of the measurement page

The page can be displayed from the sub-menu by clicking on the icon of the **System**, **OTU/FTH** or **PON Dashboard**:

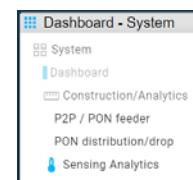
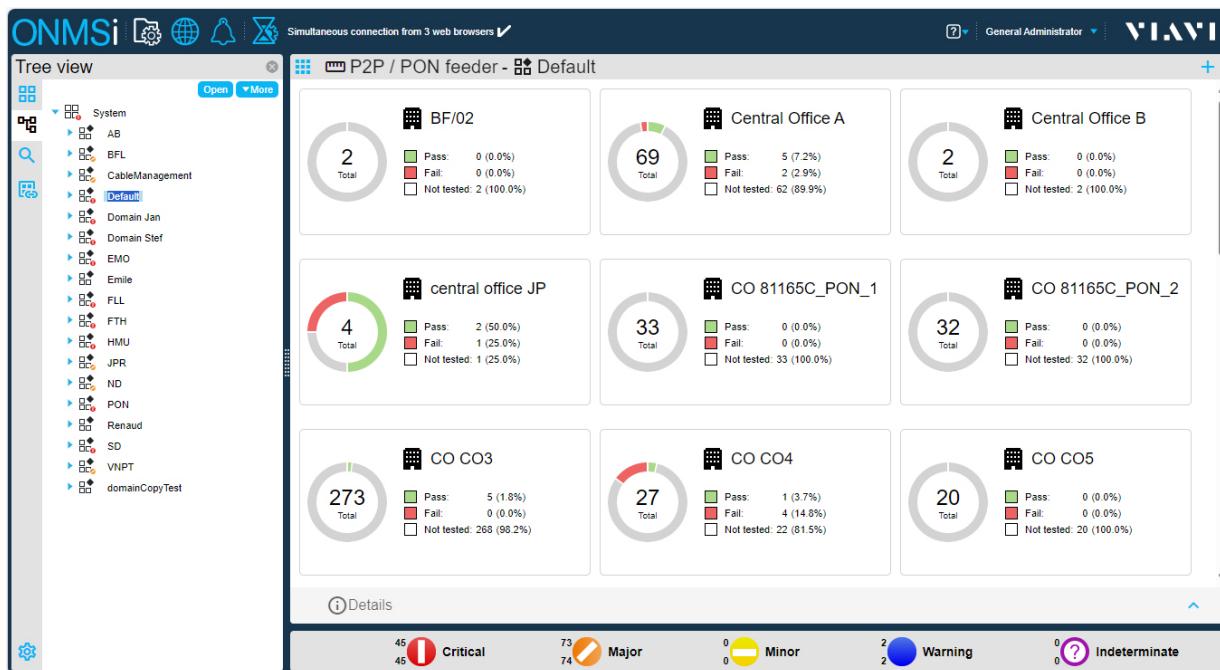


Figure 227 Construction / Analytics view

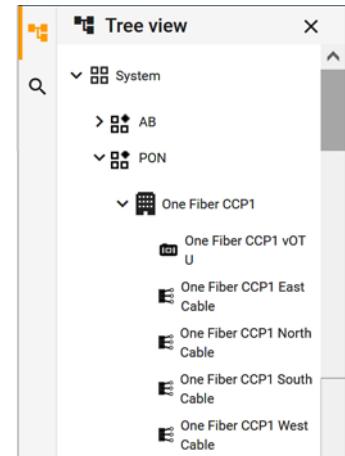


Domain Management

The Domain can be composed of:

- Sub-domains
- Central Offices
- OTU/FTH
- Cable Heads (cable incoming or outgoing from/to the central office and made of a group of fibers)
- Orphan Links: links that are not connected to any OTU and not belonging to any cable head.

Once in the selected domain, the user can add a Central Office and define its components (OTU/FTH and Cable Head).

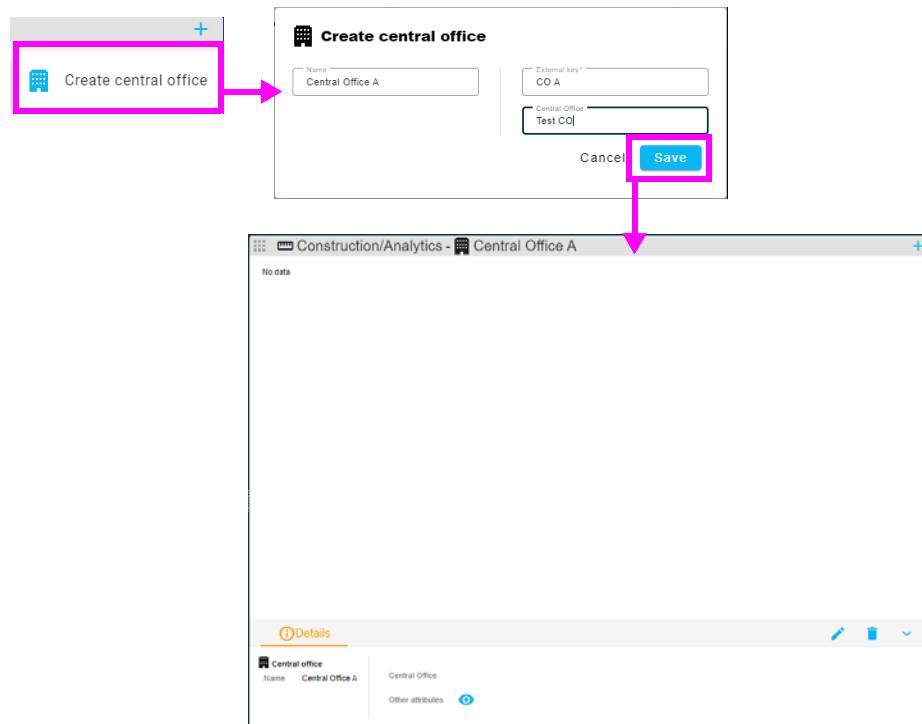


Adding a Central Office to the domain

- 1 From **System** dashboard, click on the domain into which the Central Office must be added
- 2 Click on «+» > **Create central office**.
A new window opens.
- 3 Enter a **Name** for the Central Office and define an **External key**.
- 4 If other additional attributes have been defined, they can be entered here (see “[Additional Attributes](#)” on page 191).
- 5 Click on **Save** to validate.

The new Central Office is added to the System dashboard.

Figure 228 Creating a new Central Office



- Click on **Details** tab, at the bottom of the window to display/hide the detailed information of the Central Office.
- Click on to modify the information regarding the Central Office (Name/ External key).
- Click on to delete the Central Office.



CAUTION

To delete a Central Office, all the elements linked to it must be deleted/removed first (OTU/FTH, Cable Heads, Links).

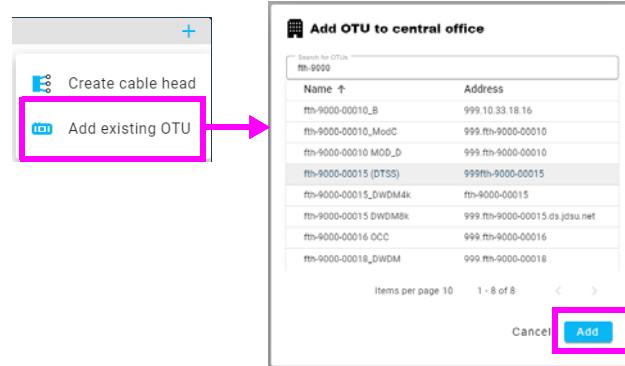
Once created, the components of the Central Office can be added.

Adding an existing OTU/FTH

To add an existing OTU/FTH or FTH-9000/-7000 to the Central Office:

- 1 From the Central Office dashboard, click on > **Add existing OTU**.
- 2 In the new window, select the OTU/FTH from the list.
- 3 Click on **Add**.

Figure 229 Adding an OTU to the Central Office



The OTU/FTH is added to the Central Office.

Figure 230 OTU dashboard

- Click on **Details** tab, at the bottom of the window to display/hide the detailed information of the OTU.
- Click on to modify the OTU/FTH name and additional attributes if any (see “Additional Attributes” on page 191).
- Click on to remove the OTU/FTH from the Central Office. A confirmation is required.



CAUTION

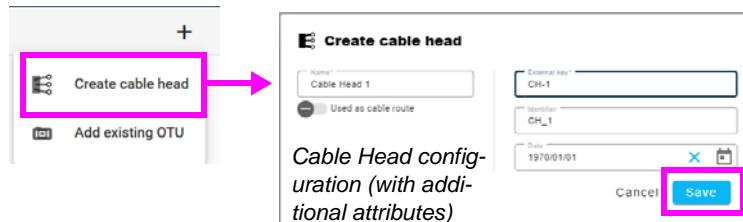
To remove an OTU/FTH from a Central Office, all the connected links must be disconnected first. They will remain accessible from their cable heads, or the central office's orphan links.

Adding a Cable Head to the Central Office

- From the Central Office dashboard, click on > **Create cable head**.

- 2 In the new window, enter a **Name** for the new cable head.
- 3 If necessary, define an **External key** for this cable head, as well as the additional attributes, if any (see “Additional Attributes” on page 191).
- 4 Select the parameter **Used as cable route** to define this cable head as a cable route (see “Cable Management” on page 29).
- 5 Click on **Save**.

Figure 231 Adding a Cable Head to the Central Office



The Cable head is added to the Central Office.

Figure 232 Cable Head dashboard

	Boolean AA	Date AA	Datetime mand AA	Float AA	Int mand AA	Text AA	Unique AA	URL AA	List text AA	List Datetime mand AA
Cable head	2022/07/29	2022/07/29 17:29:00		0.123	1234	AAA	B	http://localhost:8080/app.jsp#configuration	A1	2022/07/27 00:00:00
Name										
Central office										
Used as cable route	✓									

- Click on **Details** tab, at the bottom of the window to display/hide the detailed information of the Cable Head.
- Click on to modify the Cable head name, and the additional attributes, if any (see “Additional Attributes” on page 191).
- Click on to delete the Cable head from the Central Office. A confirmation is required.

If the links are not attached to OTU ports, select the option «Delete the links associated to the cable head». to also delete the links from cable head.

Connecting links to the OTU/FTH or to the Cable Head

Once the OTU/FTH or the Cable Head has been added to the Central Office, one or several links can be associated to it.

Two methods can be used to associate links to OTU/Cable Head:

- Applying label
- Adding manually a link

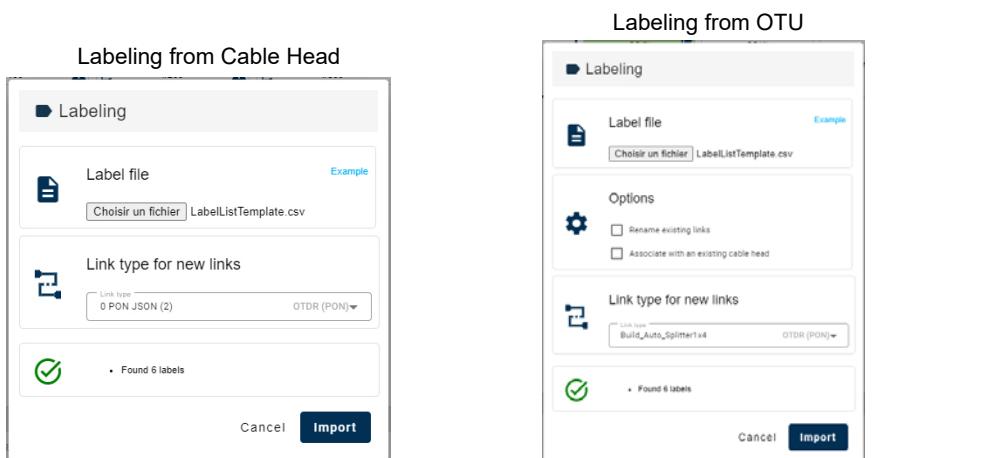
Applying a label to create links in bulk

In order to test fibers, links must be created on their ports. This can be done in bulk by using the labeling feature.

To apply a labeling to the tested fibers:

- 1 On the OTU/FTH dashboard only, select the first port from which labeling must be defined.
- 2 Click on  > **Labeling**.
- 3 Click on **Browse** button to select a labeling file.
or
Click on **Example** to download an example of csv file and use it as template.
- 4 If necessary select **Rename existing links** to define the existing links according to the new labeling.
- 5 If necessary, for the OTU, select **Associate with an existing cable head** and define the existing cable head name, in order to add the links in the cable head.
- 6 Select the **Link type (used) for new links** to be measured from the list.
- 7 Press **Import** to apply the labeling to the number of fibers defined in the csv file.
Example: if in the labeling file, 6 links/fibers have been defined from 7 to 12, and are applied from the port 13: link 7 will be set on Port 13, link 8 will be set on Port 14...

Figure 233 Labeling



Once the labels are successfully transferred, a pop up message displays at the bottom of the screen and in the Notification panel.

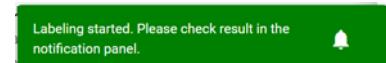
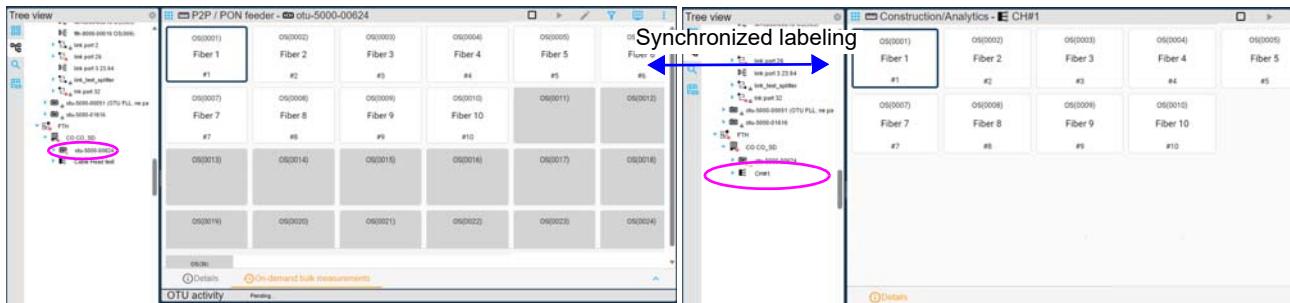


Figure 234 Labeling results



Adding manually a link

If some links have been disconnected from an OTU and don't belong to a cable head, they are still displayed in their central office's **Orphan Link** view. They can be connected to OTU ports from the OTU view, or added to a cable head from the Cable Head view.

- 1 From the OTU/FTH dashboard, select the port onto which a link must be connected.
- 2 In the OTU/FTH or Cable Head dashboard, click on > **Connect Link** (for OTU/FTH) / **Add Link** (for Cable Head).
- 3 Enter at least the first 3 letters of the link name to find it in the list
- 4 Select it in the list.
- 5 For the OTU, if necessary, select **Associate with an existing cable head** and define the cable head name, and fiber number in order to add the link in the cable head.
- 6 Press **Add**.

Once the link is successfully added, a pop up message displays at the bottom of the screen and in the Notification panel.



Editing multiple links

Whether links are already tested or not (but at least connected), the links'information can be edited and modified if necessary (link type, periodic measurement...).

- 1 Select several links (tested and/or connected).
- 2 Click on .
The **Edit multiple links** window opens
- 3 Click on the icon of each parameter to be modified and enter
- 4 Enter the information wished.

Figure 235 Edit multiple links

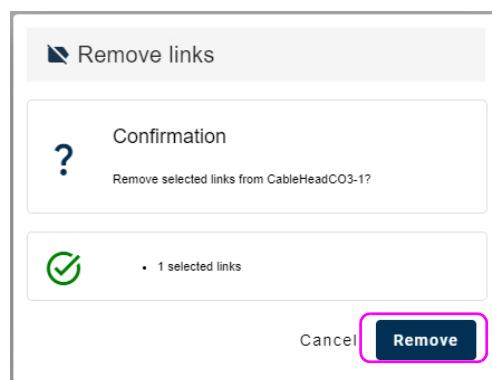


- 5 Press **Save** to validate
- 6 All the parameters defined will be applied for all the links selected.

Disconnecting a link

- 1 Select one or several links from the dashboard.
- 2 Click on > Disconnect links (with OTU) / Remove links (with Cable head).
- 3 In the dialog box open, click on **Disconnect** / **Remove** to confirm the deletion.

Figure 236 Link removal



CAUTION

If some links are in alarm, the alarms will be cleared if links are disconnected.

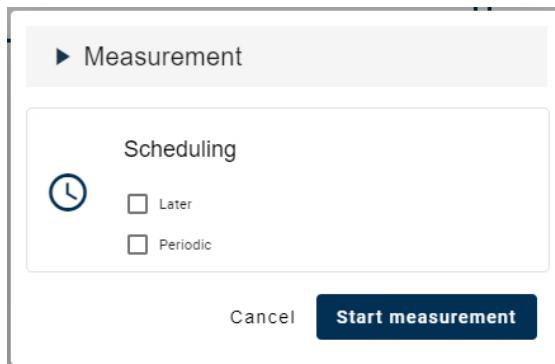
Starting measurements on links

- 1 From OTU/FTH or Cable Head dashboard, select the link(s) for which a test must be performed in series.
Multiple selection can be eased by applying filter to display only the relevant ports (see “Filtering the display” on page 208), then select all the visible ports by clicking on the square on the right of the upper banner.



Click on  to open the Measurement window.

Figure 237 Start Measurement



- 2 Press **Start measurement** button.

By default, the test is started as soon as possible. It can be delayed by clicking on the **Later** option and selecting the start date by clicking the calendar icon.

If **Later** has been defined, the measurement will be launched at the defined date/hour.

If **Periodic** is selected, the link measurement is performed with the interval corresponding to the **Days / Hours** defined, but will stop when the periodic measurement is deactivated.

During the test, the OTU activity bar displays the link measurement in progress:

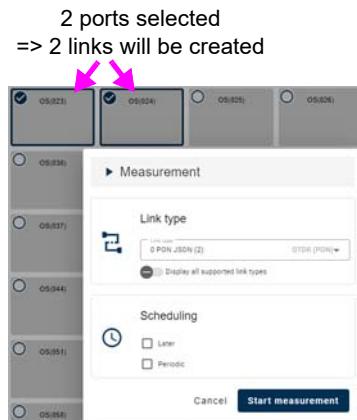


Creating and measuring automatically a link

From the OTU ports screen, the link can be automatically created and measured:

- 1 In the OTU panel, select the port(s) onto which the link(s) must be tested.
- 2 Click on .
- 3 In the **Measurement** window, define the Link type to be used for link measurement
- 4 If necessary, define if the measurement must be scheduled (**Later** and **Periodic** parameters).

Figure 238 Measurement for automatic links



The link name by default will be: *the otu/fth name [space] the port number*.
For example: *FTH-9000 OS(023)*.

PON link type

If the link type is defined with a PON topology, the instrument will try to detect the first splitter, the WOTDM and detect the switches.

Canceling a test

If a test is in progress or has been defined later, and must be canceled, proceed as follows:



NOTE

Links with planned tests are identified with an icon



Links with test in progress are identified with an icon



- 1 Open the measurements window at the bottom of the screen clicking on **On-demand bulk measurements** tab.
- 2 In the list of tests (planned or completed), the planned tests are represented by a **cross**.
- 3 Click on the cross of the planned test to be deleted.

Figure 239 List of tests

User	Start	End	Status
admin	2024/10/16 14:30:00		Complete: 0, remaining: 1
admin	2024/10/16 14:11:00	2024/10/16 14:12:02	Complete: 1, total: 1
admin	2024/10/16 12:12:00	2024/10/16 12:12:01	Complete: 1, total: 1

- 4 A confirmation window displays: click on **Yes** to validate the cancellation of the measurement starting
In the list, the End date is filled and the Status of the test is updated.



CAUTION

For periodic tests, edit the links and deselect the **Periodic** parameter (see [page 204](#)).

Results screen from measurement tests

Once all the links are tested, the OTU/Cable dashboard displays as follow:

Figure 240 Example of OTU dashboard after measurement tests



- The square is grey if no link is associated to the port.
- The square is white if a link is associated to the port, but no test has been performed, or if no test has been correctly performed.
- The pass tests (with results which not exceed the defined thresholds) are displayed with a green background and with the icon .
- The fail tests (with results exceeding the defined thresholds) are displayed with a red background and with the icon .

The icons displayed on the bottom of each square correspond to the link type parameters:

- the icon  indicates an OTDR test, without PON (a standard Point to Point)
- the icon  indicates an OTDR test, with PON topology
- the icon  indicates a DTS or DTSS link type

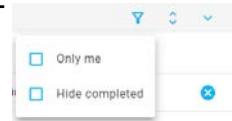


On-demand bulk measurement window

The **On-demand bulk measurements** window allows to display the status for measurements that have already been performed on this OTU/FTH, the last 60 days.

Click on **Filter** icon  and filter the list selecting only the measurement you made or hiding the measurements completed.

Click on  to display the list on the entire window. Click again to display it under the ports view.



Actions on display

Overriding the result

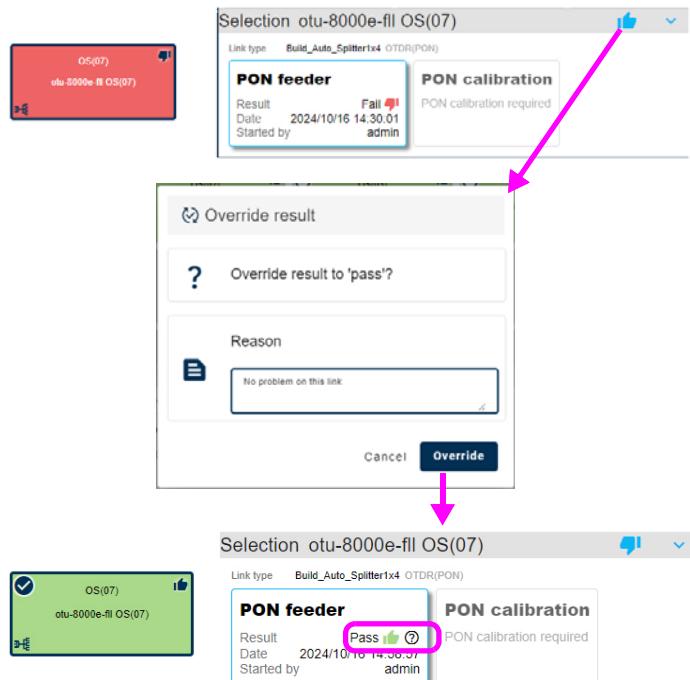
Once a link has been measured, the results can be modified, and overridden from fail to pass.

To override a result:

- 1 Click on the result to be modified in the links list.
- 2 Open the **Details** window, at the bottom of the screen.
- 3 Click on the icon  to modify the current result and turns it to «pass».
- 4 In the dialog box, a reason for this modification can be added (optional).
- 5 Click on **Override** to validate.

The link turns green and the status «pass» is displayed in the **Details** view, with the date of the override action.

Figure 241 Overriding the link status



- Drag the mouse on the icon to display the reason for this modification, if any (see [step 4](#)).
- Click on the icon to restore the link to fail status. A validation is required.

Overriding with DTS Module

On a link of a DTS module, which can also perform OTDR measurement, a link type OTDR is defined, a measurement is launched.

Then, the same link is defined with a DTS link type and a DTS measurement is launched.

Both OTDR Construction Analytics and Sensing Analytics cards are displayed (see [Figure 246 on page 211](#)).

The overriding is done for each link:

- go to **P2P /PON feeder** view to override result for OTDR measurement.
- go to **Sensing Analytics** view to override result for Sensing measurement.

Filtering the display

To apply a filter on the display, whatever is the dashboard displayed (OTU, Cable Head or Orphan Links):

- 1 Click on the icon of the banner.

- 2 Enter the filter parameter in the Search text zone: for example, display only the link containing «AAA», and/or display only the ports (for OTU) or fibers (for Cable Head) from 1 to 5 (1 - 5) and press **Enter** to validate.

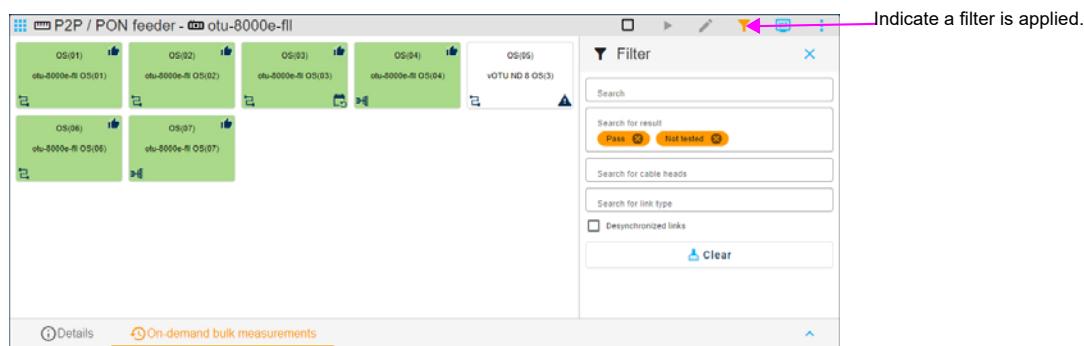
And/Or

Click on **Result** and select the result type(s) to be displayed (several results can be selected) in the dialog box and press **Enter** to validate.

And/or

Click on **Search for cable heads** (for OTU) or on **Search for OTUs** (on Cable Head) and enter the cable head(s)/OTUs to be found and press **Enter** to validate

Figure 242 Filtered results



Click on **Clear** to remove filters and display all ports.

Filter: Desynchronized links

From the Filter screen, select the parameter **Desynchronized links**.

Once a link type is defined for a link, the parameters are used at each measurement. For periodic measurement, those parameters are sent to the OTU, which will perform the measurement according to those parameters.

However, if the parameters of a link type are modified, the OTU will not be updated and will continue performing periodic measurements with previous parameters.

In this case, the links are defined as **Desynchronized links**.

The desynchronization information is displayed in overview screens, (System, Domain, Central Office), allowing to reach the OTU affected with desynchronized links. To apply the new link type parameters, the periodic measurement needs to be started again.

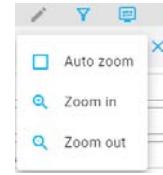
Figure 243 Desynchronized links



Zooming on display

The Links view can be zoomed in or out:

- 1 Click on to open the Zoom menu.
 - 2 Click on **Zoom in** as many times as necessary to enlarge the links display to the zoom level wished.
Click on **Zoom out** as many times as necessary to reduce the links display.
- Click on **Auto zoom** to apply an automatic zoom on links display.



NOTE

The maximum zoom level is reached when one link fits to the window width

Figure 244 Example of max zoom



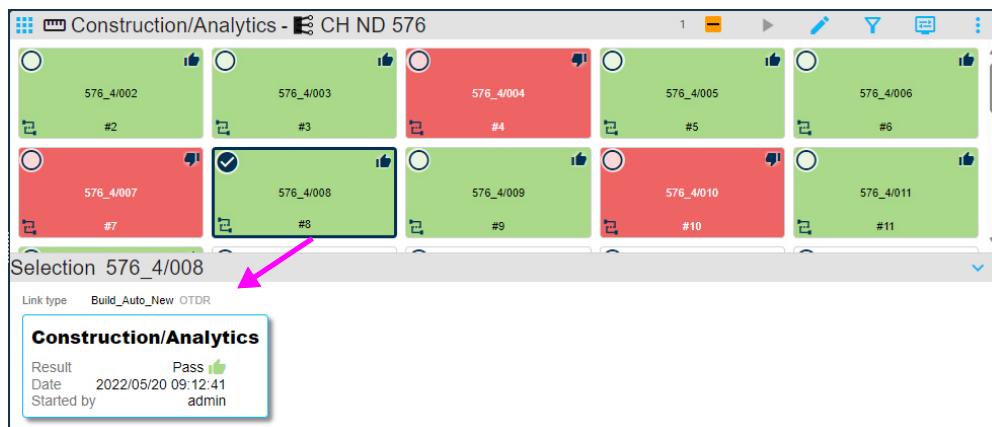
Displaying results for measured link(s)

Once a link measurement is completed, click on the corresponding frame to access the different views available for this link..

Details of the Link

- Once a Link is selected, the general information are displayed above the links list.
The box displays a summary of the Link.

Figure 245 Link details



Click on Construction/Analytics box to open the Smart Link view of the link, and also access to the results table and the trace.

Display for the same links with different “link type” types

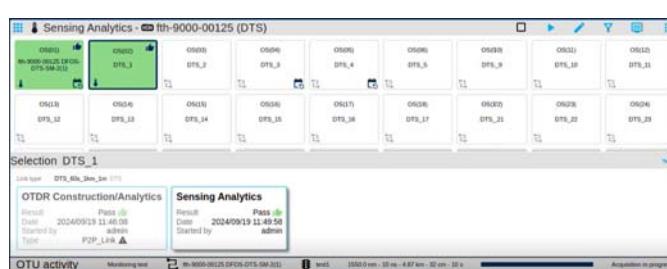
If a first measurement was performed with a link type, and then other measurements are performed with a different link type, then both are displayed at the bottom of the screen.

For example, if a link type was defined as OTDR for measurement, and then modified as DTSS link type, then both cards are displayed:

- Click on the **Dashboard** icon and select **Sensing Analytics**.



Figure 246 Measurement results otdr and dtss for the same link



The **OTDR construction/Analytics** card is displayed, next to the **Sensing Analytics** card.

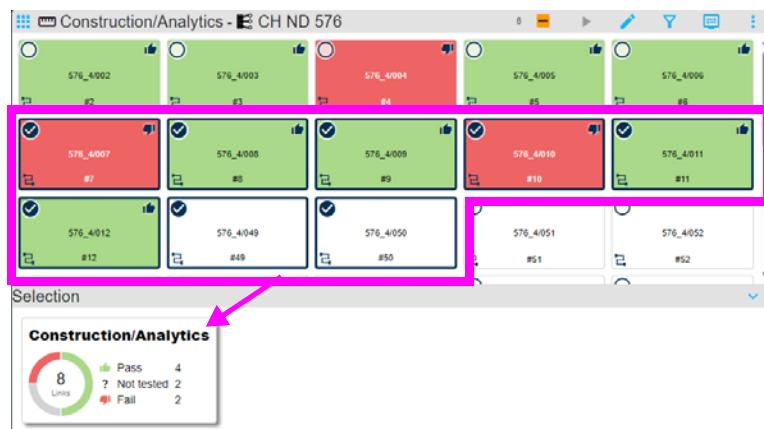
- 2 Click on one card to display the corresponding results.

Details for several selected Link

Select several links from the list to display a summary card of the selection: the total number of links selected, with:

- the number of measured links with pass status.
- the number of connected links but not measured.
- the number of measured links with failed status

Figure 247 Summary card for several selected links

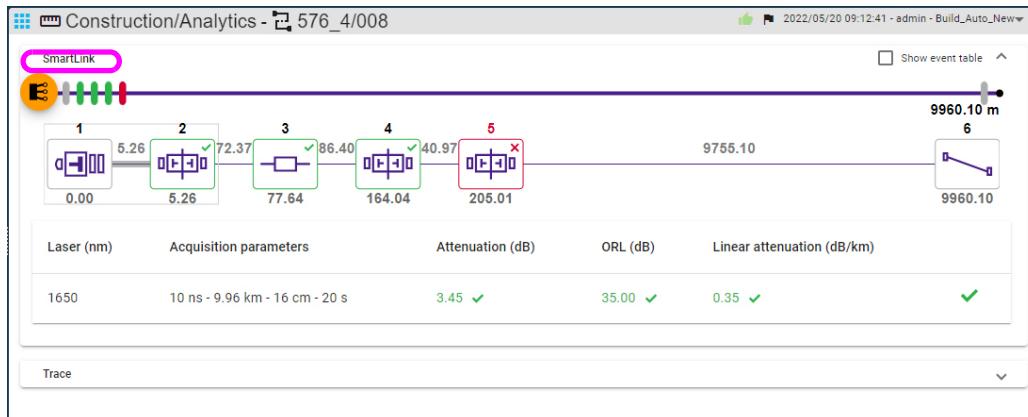


OTDR results

SmartLink view

- 1 Click on the **Construction/Analytics** card to directly attend the SmartLink view.
The SmartLink view displays a graphical representation of the link and the measurement results (Link loss / Linear Attenuation / ORL).

Figure 248 SmartLink View



- Icons are framed in green when results are within the thresholds.
- They are framed in red if the results exceed the thresholds.

NOTE

In **SmartLink** view, as well as in **Events** or **Trace** view, the 3 latest measurements of the link are available on the right of the box: click on the scrolling menu and select a measurement to be displayed according to the date/time of this measurement.



The icon indicates the last measurement performed on the link.

SmartLink: details of an event or of a section

In the graphical representation, click on one event or one section between 2 events to display the detailed values for this event/section under the graphic:

Figure 249 Event details

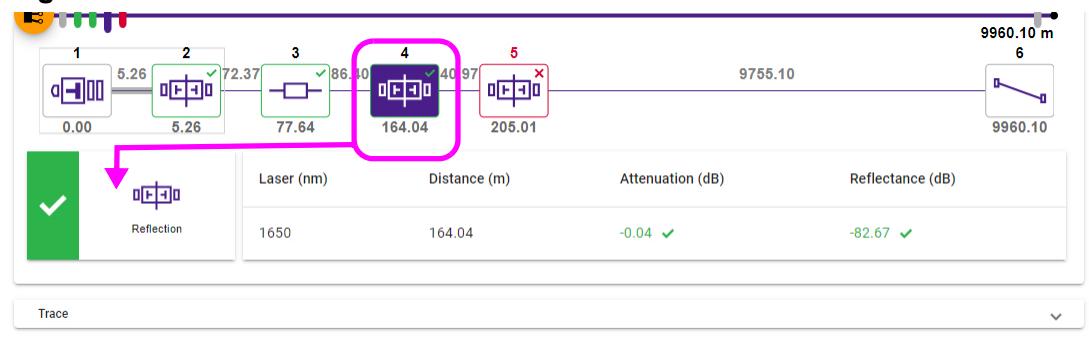
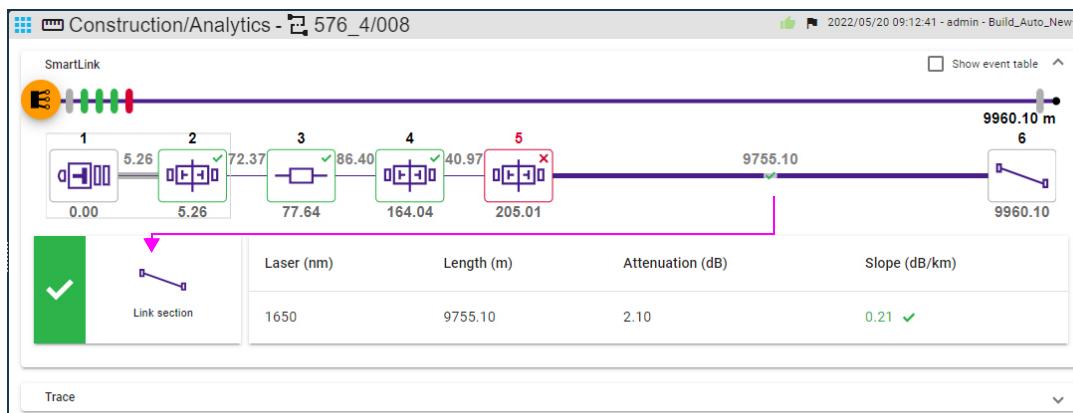


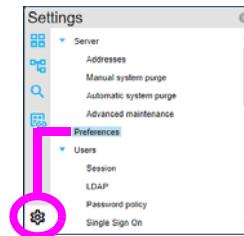
Figure 250 Link section details



Notes on unit

The units defined in the Construction/Analytics view depend on the units defined in the ONMSi application: the units can be modified on ONMSi, and the modifications will be applied in the Construction/Analytics view.

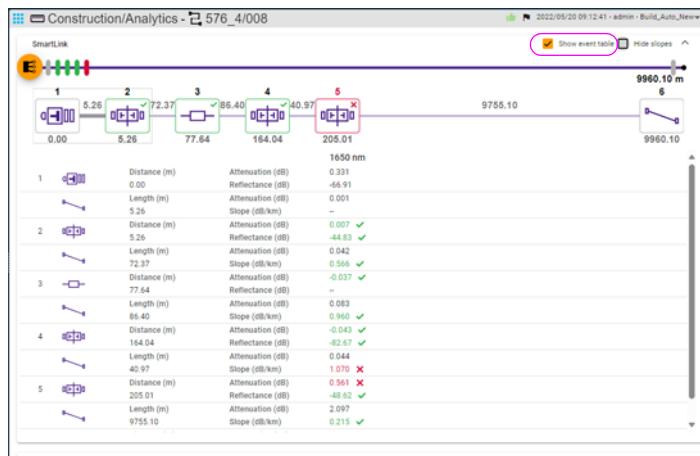
- 1 Click on **Settings** icon at the bottom of the screen
- 2 Click on **Preferences**.
- 3 See “Configuring the unit preferences” on page 169 to modify the units.
- 4 To apply the new unit preferences, you will have to log out and log back
- 5 Return to **Construction/Analytics** view and check the new units are defined in one of the Link views (SmartLink, Traces...)



Event Table

- 1 Select **Show event table** to display the events table for the measurement, under the SLM view.

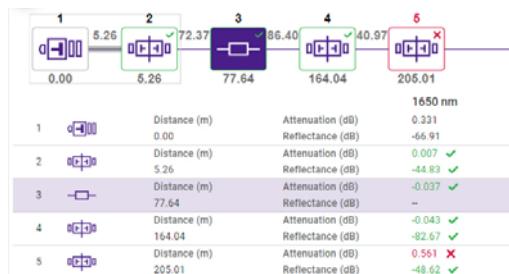
Figure 251 Events table



The slopes between events can be hidet in the table, selecting **Hide slopes** parameter.

Click on one event on the table to highlight it in the **SmartLink** graphic and vice-versa.

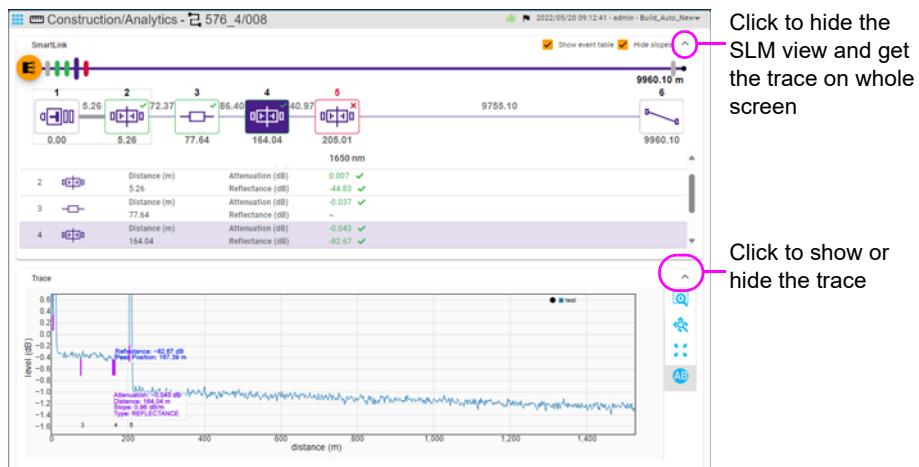
Figure 252 Event selected in SLM view and event table



Trace view

- 1 Click on **Trace** arrow to display the trace under the SLM view.
The measured link is represented by a trace.

Figure 253 Trace view



To visualize the trace on whole screen, just hide the SLM clicking on the arrow.

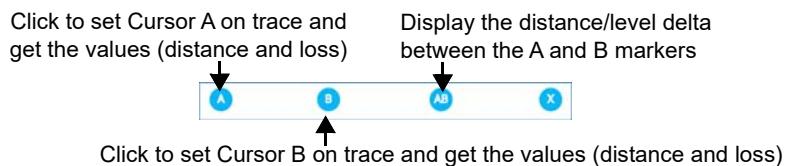
Zoom on trace

- Click on and draw a rectangle on trace to zoom in.
- Click on and use the mouse roll to zoom in/out on the trace.
- Click on to reset zoom and display the full trace.

Cursors A and B

- Click on to open the Cursors menu

Figure 254 Cursors menu



Multi-traces view

In case of multi-wavelengths measurements, the traces are displayed in overlay.

On the right of the trace display, click on the trace selection box to select the trace.

Click on the trace description to hide the trace.

selected trace → test - 1310 nm
unselected hidden trace → test - 1550 nm
 test - 1625 nm

Sensing results

- In **Sensing Analytics view**, click on one card to display the corresponding results trace.
- Click on the arrow to show the **Zones** table under the trace.



NOTE

The zones must be configured in the configuration file (*.fo_cfg*), and at least one zone must be defined.

Figure 255 Sensing trace and Zones table



Generating a report for the links



NOTE

The report generation is available exclusively for OTDR measurements.

The links results can be exported in a report:

- in csv (to be usable with a spreadsheet program such as Excel™ ...) to get a list of events
- in pdf, to get a summary of the measurements.

1 Select the links to be included in the report.

2 Click on and click on **Reporting**.

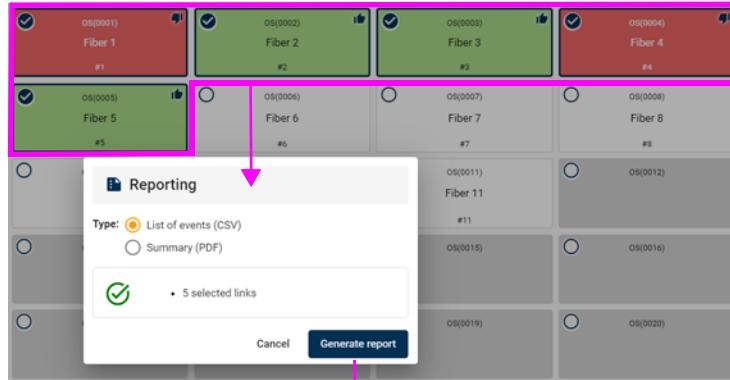
3 Select the report: list of events (CSV) or summary (PDF). Click on **Generate Report**.

A pop up window and a notification on the right of the screen are displayed during the report generation.

In the Notifications window, click on to just close it, or on to remove the completed Notification and close the window.

The report is saved on your computer, in csv or pdf format and the filename is:
`measurements_yyyy-mm-dd_hhmmss.csv`

Figure 256 Report



example of pdf report

Port #	Cable head Id	Fiber #	Link	Laser (nm)	Loss (dB)	ORL (dB)	Length (m)	Status	Date	Technician
OS(0001)	Cable Head 1	1	Fiber 1	1650	3.45	35	9960.1	Fail	2022-05-16 16:42:45	admin
OS(0002)	Cable Head 1	2	Fiber 2	1650	3.45	35	9960.1	Pass	2022-05-16 16:43:05	admin
OS(0003)	Cable Head 1	3	Fiber 3	1650	3.45	35	9960.1	Pass	2022-05-16 16:43:25	admin
OS(0004)	Cable Head 1	4	Fiber 4	1650	3.45	35	9960.1	Fail	2022-05-16 16:43:46	admin
OS(0005)	Cable Head 1	5	Fiber 5	1650	3.45	35	9960.1	Pass	2022-05-16 16:44:06	admin

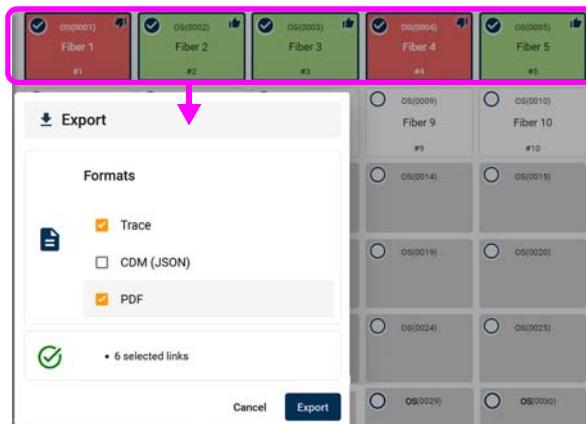
Exporting Trace, pdf and / or json data

The test results trace (.sor, .csor or .msor format) and/ or cdm file used by the instrument (json file) can be exported:

- 1 Select the tested links for which the results trace, pdf and/or json data must be exported.
- 2 Click on and click on **Export**.
- 3 Select the format for the exportation: **Trace, CDM (JSON) or PDF**.
- 4 Click on **Export**.

A pop up window is displayed during the export process.

Figure 257 Export box (for OTDR measurement)



The export file is saved on your computer, in a zip file and the zip name is: acquisitions-yyyymmdd_hhmmss.zip.

The filename is: linkname-yyyymmdd_hhmmss.sor/.json/.pdf.



NOTE

The pdf export (generated by the OTU/FTH) for each link measurement, is only available for OTDR measurements. For Sensing measurements, only the trace and CDM (JSON) can be exported.

Construction/Analytics Field Application

The Construction/Analytics view is available on the ONMSI Field Application and can be used to:

- Perform tests
- Perform Reporting and exports
- Modify the display: zoom in and out, apply filters...

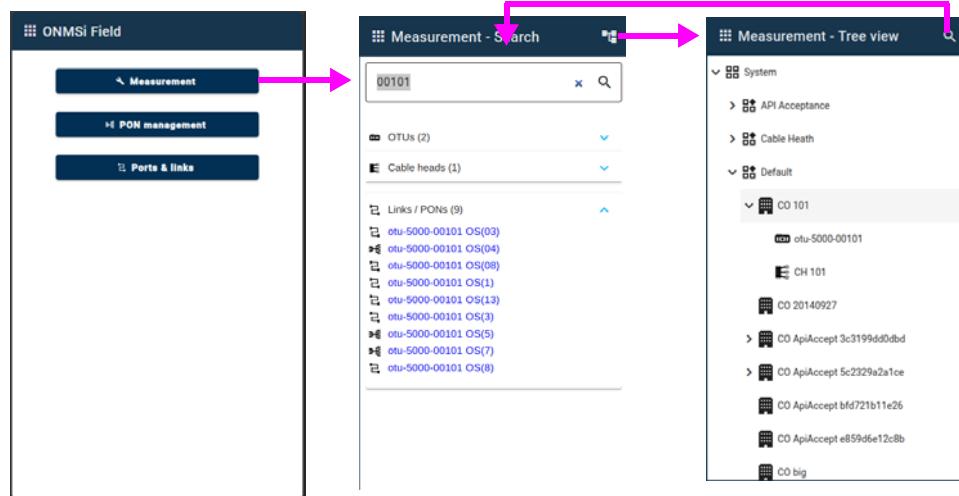
The Field application does not allow to create, edit or remove/delete resources (OTU, Cable heads or Orphan Links).

Opening the field application

The field app is available from the URL: <https://<server address>/m/>.

- 1 In the **Home** page, press **Measurement**.
- 2 In the search toolbar, search the resource to be displayed, or click on the icon  to open the System tree and find the resource.

Figure 258 Measurement application

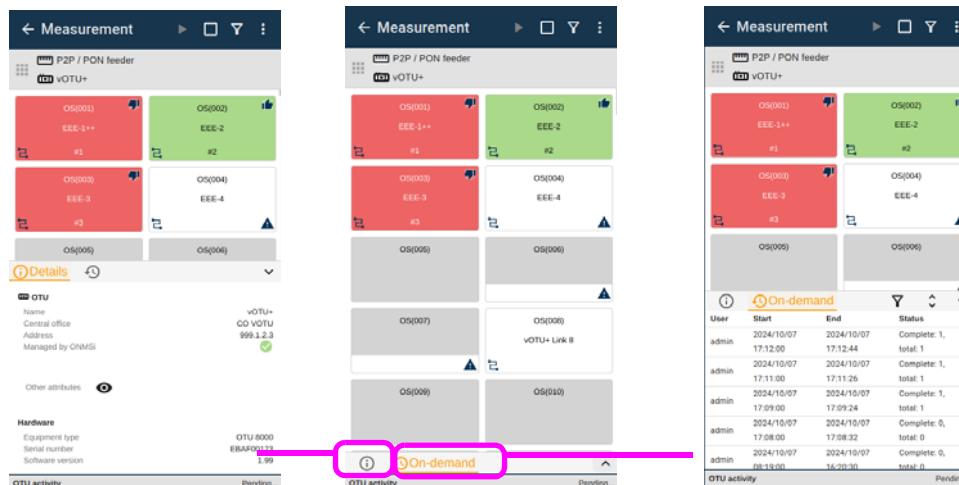


Once a resource is open, the functionalities are the same as in the ONMSi application.

OTU/FTH or Cable Head view

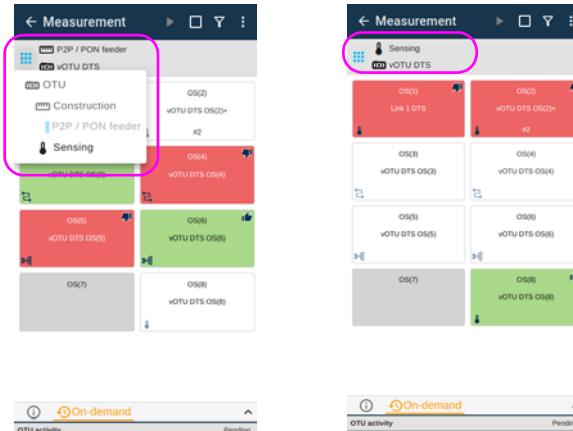
- Click on the OTU/FTH or Cable Head to visualize available links.

Figure 259 OTU view



- Click on **Details** icon to display the details regarding the OTU/FTH.
- Click on the **On demand** icon to open the list of measurement tests at the bottom of the screen.

- If the resource has both OTDR measurements and sensing measurements, swap from one view to the other clicking on the left upper part.

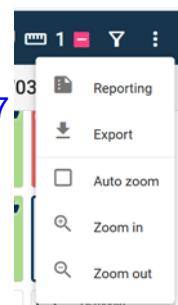


On the upper banner of the field application, the icons are similar to the ONMSI application:

- (active exclusively if at least one link is selected): launch tests - see “[Starting measurements on links](#)” on page 203.
- : select all the links
- : filter the links display - see “[Filtering the display](#)” on page 208

Click on to open the menu and to:

- Generate a report of the results (active exclusively if at least one link is selected) - see “[Generating a report for the links](#)” on page 217
- Export data (active exclusively if at least one link is selected) - see “[Exporting Trace, pdf and / or json data](#)” on page 218
- Zoom in and zoom out - see “[Zooming on display](#)” on page 210.

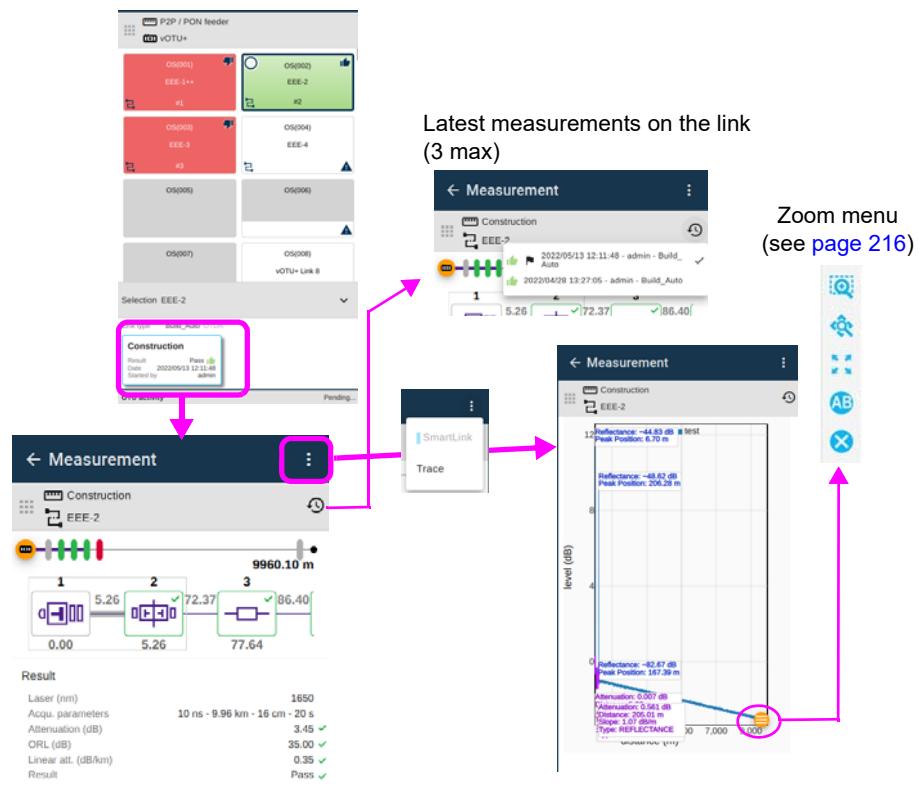


Measured link view

Select one measured link to access to the link information

- Click on to reduce the Details / Selection window.
 - Click on to filter the list of measurement tests, and on to display the list in full screen (see “[On-demand bulk measurement window](#)” on page 207).
- Select one measured link to display the corresponding card at the bottom of the screen.
 - Click on this card to open the SLM results screen.

Figure 260 Measured Link view



- Click on to override the result to pass: see “Overriding the result” on page 207.

Cable health monitoring

This chapter provides a general description of the cable health monitoring, furnished in standard with ONMSi V5.10 and higher.

Topics discussed in this chapter are as follow:

- “[Cable health monitoring principle](#)” on page 224
- “[Starting with the cable health monitoring](#)” on page 225
- “[Launching the cable health monitoring and analyzing results](#)” on page 226
- “[Cable route dashboard](#)” on page 229

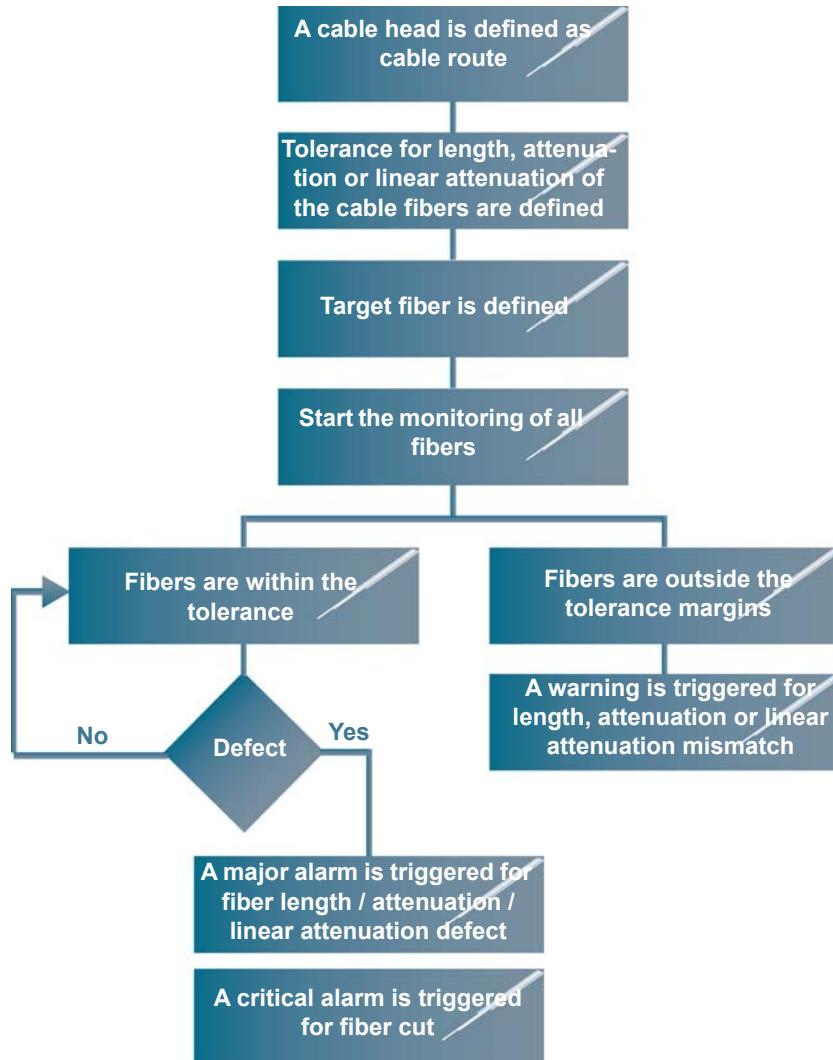
Cable health monitoring principle

The cable health is used to monitor all the fibers from all the cables, without the need to redo references.

A fiber is used as reference (target fiber) and all the other fibers from a cable are tested according to this target fiber, in length, attenuation or linear attenuation.

The cable health monitoring works as follows:

Figure 261 Principle of the cable health monitoring



All measurement made will be stored in ONMSi, who keep track of the latest measurement made on a cable route and measurement made if defect has been detected.

On the other side, measurements are captured into Fiber Analytics (keep history of all measurement made in cable route).

Starting with the cable health monitoring

Once the cable route has been created:

- 1 In the cable route dashboard, click on **Configuration** to reach the cable route Configuration screen.
- 2 Click on **Enable monitoring of all links**.

The cable route is put in monitoring.

The OTU will create all the tests on all the links of the cable. It will measure the length and budget at each fiber.

Defining the Length and Attenuation Tolerance

To launch the cable health monitoring, first, define the tolerance margins for the fiber length and the attenuation

From **Cable Route monitoring Configuration** screen:

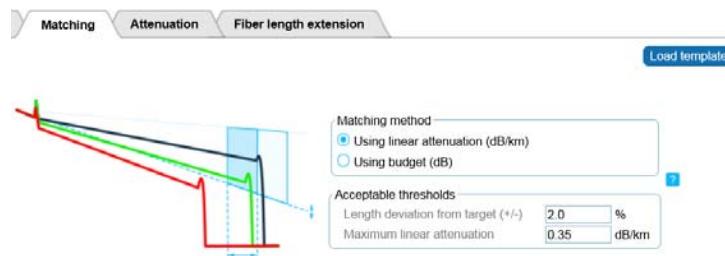
- 1 Click on the tab **Matching**:

First, define the **Matching method**: either **Using linear attenuation (dB/km)** or **Using budget (dB)**.

Then, define the thresholds used to accept or reject a fiber from the cable route monitoring inside a cable route. Two thresholds are required:

- **Length deviation**: this is the acceptable drift, in percent, around the target length of the cable route.
By default, the value is defined to +/- 2% in length around the length of the target.
- **Budget deviation (if Using budget has been defined as Matching Method)**: this is the acceptable drift, in dB, around the target budget of the cable route. By default, the attenuation tolerance is 4dB.
Or
- **Maximum linear attenuation (if Using linear attenuation has been defined as Matching Method)**: this is the maximum acceptable linear attenuation, in dB/km, of the cable route. By default, the linear attenuation tolerance is 0.35 dB/km.

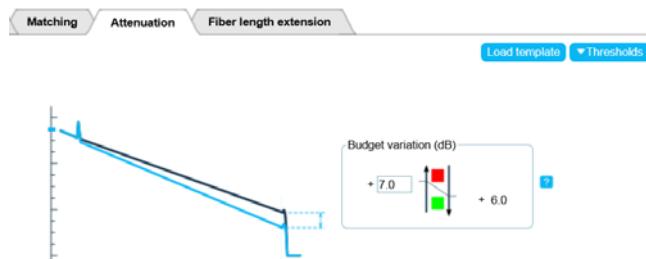
Figure 262 Matching configuration



2 Click on the tab Attenuation:

Define the threshold used to detect a loss in the fiber budget during the cable route monitoring. The drift of the End of Monitoring is specified in dB.

Figure 263 Attenuation configuration

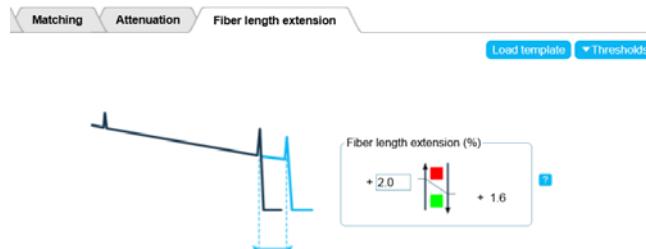


If necessary, click on **Thresholds** and select **Advanced configuration** to be able to configure the min. budget (+6.0 dB in the figure above)

3 Click on the tab Fiber length extension:

Define the threshold used to detect a fiber length extension during the cable route monitoring. The drift of the End of Monitoring is specified in percentage.

Figure 264 Fiber length extension configuration

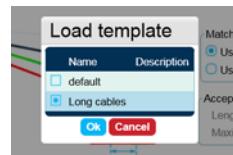


Downloading templates for Tolerance margins

To apply the configuration saved in the template previously created (see XXX), one for each parameter:

- 1 Click on **Load template** in the tab wished.
- 2 Select the template and click **OK**.

The values are automatically updated in the select tab, with the values defined in the template.



Launching the cable health monitoring and analyzing results

Once the tolerance margins are defined, a test is launched and a fiber is automatically suggested as target.

Figure 265 Links of the cable

Link	Fiber #	Name	OTU	Monitoring	Enabled	Target	Reference	Date	Length (m)	Budget (dB)	Linear attenuation (dB/km)	Latest state	Date	Length (m)	Budget (dB)	Linear attenuation (dB/km)	Status
1	LNK#1F#1	1			✓			2023 Sep 25 10:31:59	10,044.45	2.12	0.21	2023 Sep 25 10:31:09	10,045.09	2.03	0.20	No target	
2	LNK#2F#2	2			✓			2023 Sep 25 10:31:21	10,045.73	2.03	0.20	2023 Sep 25 10:31:34	10,045.73	1.99	0.20	No target	
3	LNK#3F#3	3			✓			2023 Sep 25 10:31:46	10,045.09	1.91	0.19					No target	
8	LNK#4F#8	8			✓	Suggested											No target
9	LNK#4F#9	9			✓												No target

The suggested target of the cable route is the longest fiber with the lowest attenuation (with logic to minimize switching when several fibers are digitized).

This fiber is usually the longest fiber with the lowest attenuation.

To validate a fiber as target

- Select, in the **Link** tab, the fiber to be defined as Target fiber (not necessarily the Suggested one).
- Click on **Monitoring** and click on **Set target link**.
The target column displays a notch on the target fiber.

Link	Fiber #	Name	OTU	Monitoring	Enabled	Target
1	LNK#1F#1	1			✓	
2	LNK#2F#2	2			✓	
3	LNK#3F#3	3			✓	
8	LNK#4F#8	8			✓	✓
9	LNK#4F#9	9			✓	

Measurements of the other links will then be performed according to the length of the target fiber.

If a fiber is outside tolerance margins (in length or attenuation), it is displayed in red in the Links Monitoring table with status “Match length shorter” or “Match Attenuation”.

NOTE

All the measurements made in cable health monitoring will be stored in ONMSi, which keep track of the latest measurement made on cable route.

Moreover, measurements are captured by Fiber Analytics (keep history of all the measurements made in Cable Route).

Fibers status

Figure 266 Cable route monitoring - Links results table

Cable route monitoring configuration - CH#1													Edit				
Information													Context				
Cable route	CH#1	Description	Target length (m)	from 9,844.19 to 10,245.99	Target budget (dB)	from 0.00 to 9.97	Scheduling	As often as possible	Domain	Central office	CodeManagement	OTU	otu-5000-00024	Dashboard			
Links	Matching	Attenuation	Fiber length extension														
Link	Fiber #	Name	OTU	Monitoring	Enabled	Target	Reference	Date	Length (m)	Budget (dB)	Linear attenuation (dB/km)	Latest state	Date	Length (m)	Budget (dB)	Linear attenuation (dB/km)	Status
1	LNK#1F#1	1		✓	✓	✓	2023 Sep 25 10:44:08	10,045.09	1.97	0.20	2023 Sep 25 10:51:35	10,044.45	2.06	0.20	Pass	Pass	
2	LNK#2F#2	2		✓	✓		2023 Sep 25 10:44:20	10,044.45	2.05	0.20	2023 Sep 25 10:51:48	10,047.01	2.11	0.21	Pass	Pass	
3	LNK#3F#3	3		✓	✓		2023 Sep 25 10:44:33	10,044.45	1.93	0.19	2023 Sep 25 10:50:54	10,045.73	2.03	0.20	Pass	Pass	
8	LNK#4F#8	8		✓	✓		2023 Sep 25 10:44:39	10,045.09	2.12	0.21	2023 Sep 25 10:51:07	1,500.00	10.00	6.67	Length too short	Length too short	
9	LNK#4F#9	9		✓	✓		2023 Sep 25 10:44:59	10,045.09	2.12	0.21	2023 Sep 25 10:51:22	10,047.01	2.07	0.21	Pass	Pass	

According to the fibers' status, the information regarding those fibers are different:

Status	Fiber measured?	Fiber monitored?	Comment
Waiting...	No	No	
No target	Yes	No	No fiber defined as target. As long as no target is defined, no alarm is raised.
Pass	Yes	Yes	Fiber lie within the thresholds for length, attenuation and linear attenuation
Length too short	Yes	No	Outside tolerance margin for length
Length too long	Yes	No	
Budget too low	Yes	No	Outside tolerance margin for budget if Matching method is by budget
Budget too high	Yes	No	
Linear attenuation too high	Yes	No	Outside tolerance margin for budget if Matching method is by linear attenuation
Attenuation	Yes	Yes	A major alarm is triggered
Fiber cut	Yes	Yes	A critical alarm is triggered
Fiber length extension	Yes	Yes	A major alarm is triggered

Other actions in Configuration screen

- Click on **More > Refresh tests on OTU** to send all tests to OTU.
- Select one or several fiber(s) from the **Links** table and click on **OTDR traces** to display traces in overlay (up to 8 traces can be displayed in the same window).

Figure 267 OTDR traces from cable monitoring



- Select one fiber from the **Links** table and click on **Execute now** to launch a test of the fiber immediately, and then stop the sequence.

Cable route dashboard

Click on **Dashboard** button to exit the configuration screen and return to the Cable Route dashboard.

- The list of tested fibers displays, with alarm status

Figure 268 Cable route dashboard

The screenshot shows the 'Cable route dashboard - CH#1' interface. At the top, there's an 'Information' section with details like 'Cable route: CH#1', 'Scan activity: In progress...', and various target and budget parameters. Below this is a 'Links, monitoring states and alarms' table. The table has columns for Link ID, Fiber #, Name, Standard monitoring & Alarm, Enabled, Date, Length (m), Budget (dB), Linear attenuation (dB/km), Status, Severity in cable route, Fault position (m), and Fault attenuation (dB). The data shows 9 entries, with the last entry (Link 9) having a 'Length too short' severity.

Link	Fiber #	Name	Standard monitoring & Alarm	Enabled	Date	Length (m)	Budget (dB)	Linear attenuation (dB/km)	Status	Severity in cable route	Fault position (m)	Fault attenuation (dB)
1	UNKHF#1			✓	2023 Sep 25 11:10:54	10,046.37	2.15	0.21	Pass			
2	UNKHF#2			✓	2023 Sep 25 11:10:41	10,045.00	2.04	0.20	Avg	Attenuation	Major	10,024.73
3	UNKHF#3			✓	2023 Sep 25 11:09:49	10,046.37	2.03	0.20	Pass			
4	UNKHF#4			✓	2023 Sep 25 11:10:02	1,500.00	10.00	6.67	Pass			
5	UNKHF#5			✓	2023 Sep 25 11:10:14	10,045.73	1.97	0.20	Pass			
6	UNKHF#6											
7	UNKHF#7											
8	UNKHF#8											
9	UNKHF#9			✓					Pass			

- Click on **More > Table Configuration** to modify the table view (add/remove columns).

Figure 269 Table Configuration

The screenshot shows the 'Table configuration' dialog box. It lists various columns grouped under 'Column group' and allows selecting which columns are visible. The columns include Link, Fiber #, Name, Enabled, OTU, Port, Standard monitoring & Alarm, Last update, Severity, Section, Specific problem, Additional text, Description, Cable route monitoring & latest states, Enabled, Target, Date, Length (m), Budget (dB), Linear attenuation (dB/km), Status, Severity in cable route, Fault position (m), and Fault position (dB). The 'Visible' column contains checkboxes for each item. The right side of the dialog shows a preview of the table with some data rows.

Column group	Column	Visible
Link	Fiber #	<input checked="" type="checkbox"/>
	Name	<input checked="" type="checkbox"/>
OTU	Name	<input type="checkbox"/>
	Port	<input type="checkbox"/>
Standard monitoring & Alarm	Enabled	<input checked="" type="checkbox"/>
	ID	<input checked="" type="checkbox"/>
	Last update	<input type="checkbox"/>
	Severity	<input checked="" type="checkbox"/>
	Section	<input type="checkbox"/>
	Specific problem	<input type="checkbox"/>
	Additional text	<input type="checkbox"/>
	Description	<input type="checkbox"/>
Cable route monitoring & latest states	Enabled	<input checked="" type="checkbox"/>
	Target	<input checked="" type="checkbox"/>
	Date	<input checked="" type="checkbox"/>
	Length (m)	<input checked="" type="checkbox"/>
	Budget (dB)	<input checked="" type="checkbox"/>
	Linear attenuation (dB/km)	<input checked="" type="checkbox"/>
	Status	<input checked="" type="checkbox"/>
	Severity in cable route	<input checked="" type="checkbox"/>
	Fault position (m)	<input checked="" type="checkbox"/>
	Fault position (dB)	<input checked="" type="checkbox"/>

- As in Configuration screen:
 - Select one or several Fibers and click on **OTDR traces** to display the traces in the viewer.
 - Select one fiber and click on **Execute now** to launch a test of the fiber immediately, and then stop the sequence.

- Click on **More > Enable /Disable measurement** to enable or disable measurement on a port - See “[Provisioning the link](#)” on page 24.
- In the upper part of the screen, click on **Scan now** to launch a scan of the cable route. Click **OK** to validate.
If a fiber is monitored, any defect will trigger an alarm. See “[OTU Scans](#)” on page 32.
- Click on **More > Audit logs** to display the Audit logs screen - See “[Once this option is enabled, it is kept after a logout/login on the same web browser.](#)” on page 6.

GeoView

This chapter provides a description of the possible actions on map, using the GeoView option. The goal of the GeoView option is to display on a map, geographical files and alarms of links.

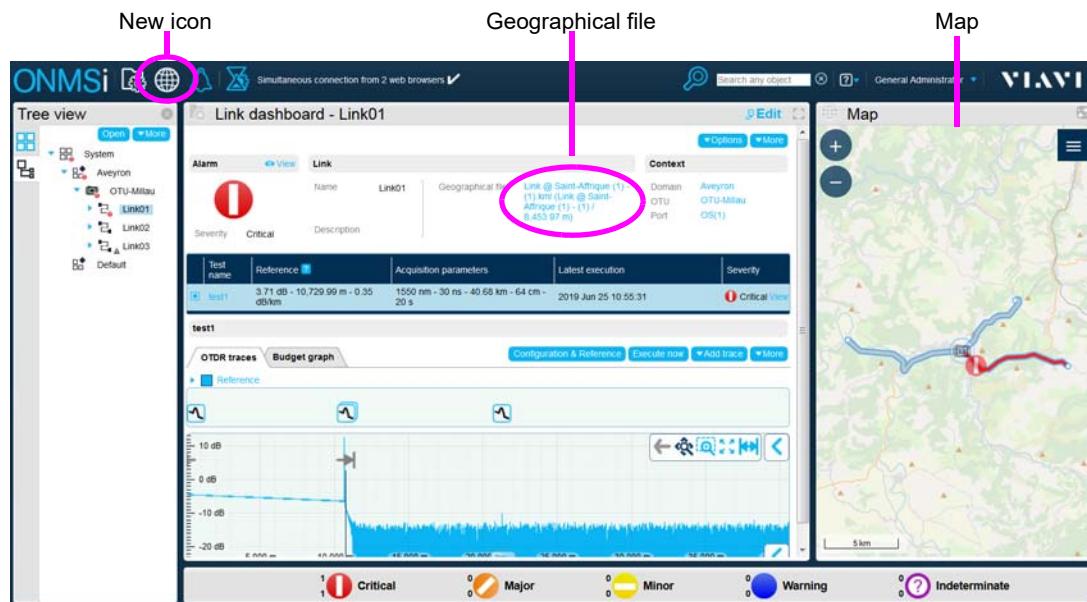
Topics discussed in this chapter include the following:

- “Pre-requisites” on page 232
- “Interaction with the map” on page 232
- “Interaction on map” on page 235

Pre-requisites

- Once the license is activated, the icon **Map** is displayed on the upper banner and a new window dedicated to mapping displays on the right.
- Associate a geographical file to a link: see “[Associating a geographical file to a link](#)” on page 93.

Figure 270 Geographical file associated to a link



Interaction with the map

Once a file is associated to a link, you can visualize:

- the OTU linked to the link
- the link itself
- the alarms on that link, if any.

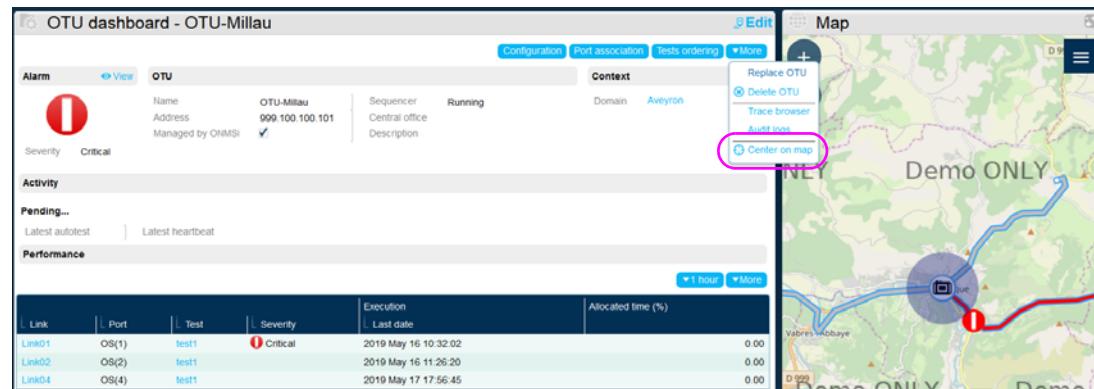
Centering the map on the OTU

To display the OTU centered on map:

- 1 Go to the **OTU dashboard**.
- 2 Click on **More**.
- 3 Click on **Center on Map**.

The OTU is highlighted and centered on the map.

Figure 271 OTU centered on map



Centering the map on the Link

To display the link centered on map:

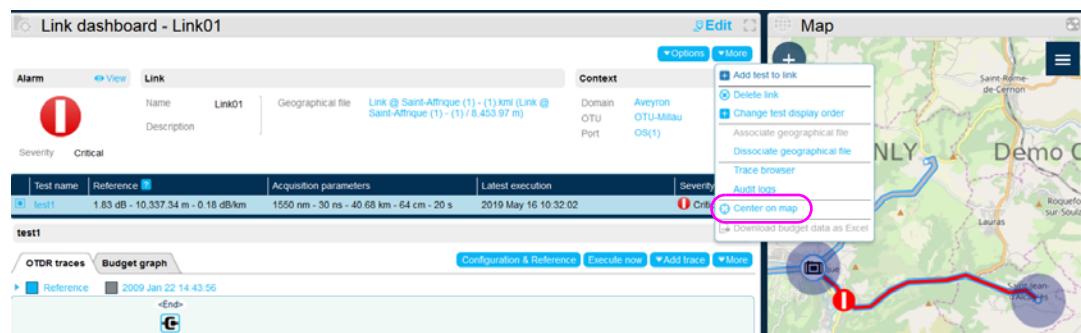
- 1 Go to the **Link dashboard**.
- 2 Click on **More**.
- 3 Click on **Center on Map**.

The Link is highlighted  and centered on map.

Once centering process is completed:

- the link is displayed in grey, without alarm on the link
- it is displayed in red/orange if an alarm is present on the link.

Figure 272 Link centered on map



Centering the map on the Alarm

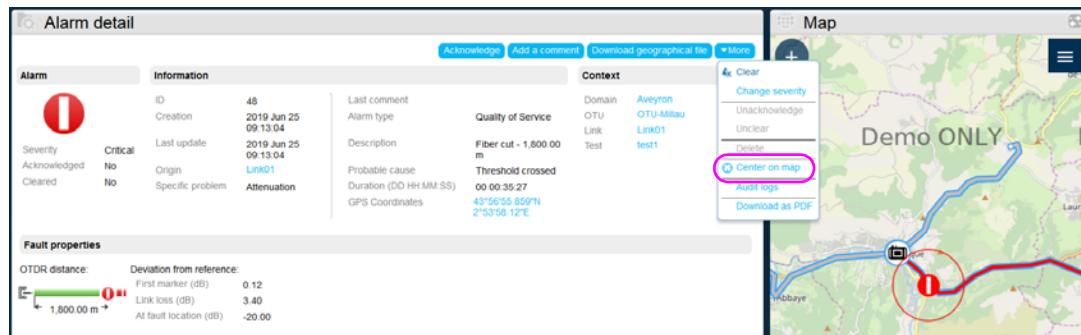
To display the Alarm centered on map:

- 1 Go to the **Alarm dashboard**.

- 2 Click on **More**.
- 3 Click on **Center on Map**.

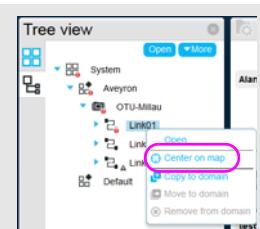
The alarm is highlighted and centered on map.

Figure 273 Alarm centered on map



NOTE

- The **OTU** and **Link** can be centered on map from the Tree view:
- Right click on the OTU / Link and click on **Center on Map**.



Trace viewer and map

Once the GeoView is installed, a new tool **Trace tracking** is available on the trace viewer.

This tool allows to locate from the otdr trace a point on the map link.

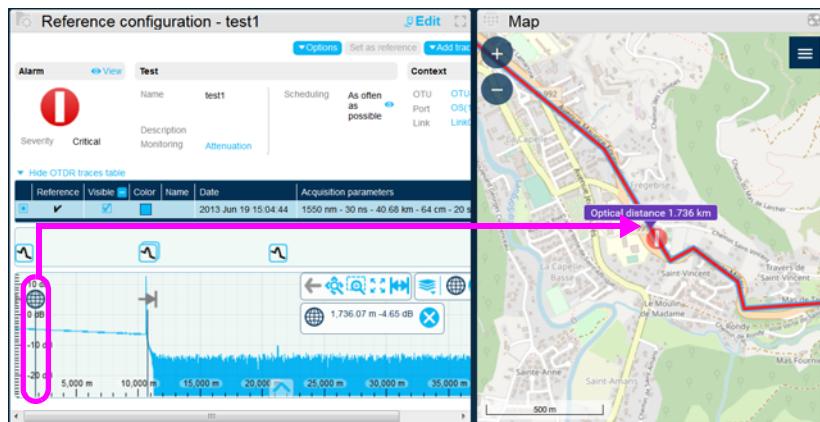
- 1 Open the Trace viewer (see [Chapter 7 on page 45](#))
- 2 On the trace view, click on the tool **Trace Tracking**.
- 3 Set the cursor on the trace, at the position wished.



The trace displays with a vertical line with the icon

The corresponding point is represented on the map by a purple mark indicating the optical distance.

Figure 274 Trace tracking



Click on to hide the trace tracking tool and representation on trace and on map.

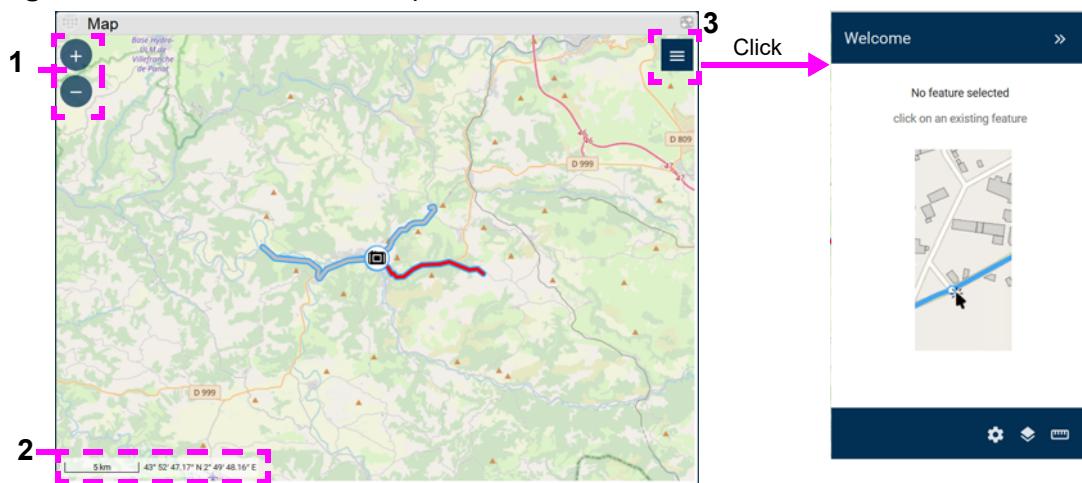
If you click again on Trace tracking tool, the last tracking defined will display back.

Interaction on map

The map window contains the following element:

- 1 On the upper left part of the map, the + and - buttons, allowing to zoom in / out on the map.
To navigate on map, you can also:
 - Zoom in / out on the map using the mouse roll.
 - Displace on the map, maintaining the mouse left button pressed and dragging the mouse.
- 2 At the bottom of the map, display the scale and the mouse tracker (gps coordinates of the mouse position).
- 3 On the upper right part of the map, click to display the Tools and Details panel.

Figure 275 General view on map



Tools and Details panel

Once the Tool and details panel is opened, three tools are available at the bottom of the dialog box:

- the Settings tools
- the Layers visibility tools
- the measure tool

Setting tools

The settings tools allow to display information available for the map (not changeable).

Click on **Settings** icon to display the different elements described:

Figure 276 Settings menu



- **Projection:** display the information on geographical projection.
- **Bounds:** display the limits if the map
- **Background layer:** displays the URL allowing to access to the map image (advanced settings)

Layers Tools

The layer tools window is dedicated to the objects visibility on map.

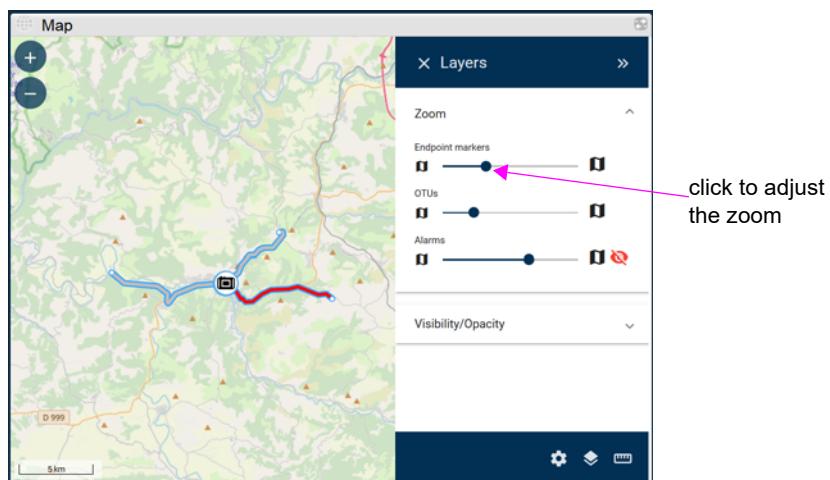
Click on **Layers** icon  to display the 2 sub-menus available: **Zoom** or **Visibility/Opacity**.

Zoom

The **Zoom** sub-menu allows to define the objects visibility according to the zoom level defined for the map.

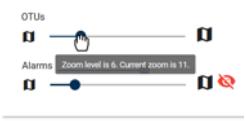
Navigate on the object bar pressing the button to adapt the zoom level.

Figure 277 Adjusting Objects Zoom



The icon  indicates the object is not visible on map with the current map zoom level.

Maintain the cursor on the button of an object to have an indication of the zoom level selected.

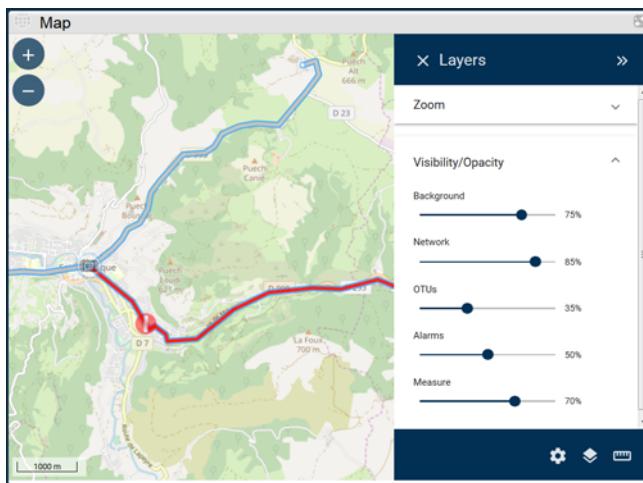


Visibility/Opacity

The **Visibility/Opacity** sub-menu allows to adjust the visibility of the objects: Background / Network / OTUs / Alarms / Measure.

Click on the button of one object to make it more or less visible on the map.

Figure 278 Visibility of the objects

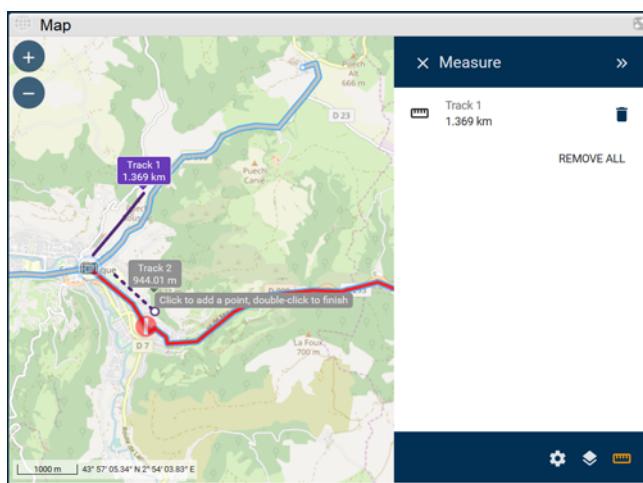


Measure Tools

The measure tools window allows to measure tracks on map.

- 1 Click on **Measure** icon
 - 2 Click on the map at the starting point of the tracks
 - 3 Click once on the following point(s) of the track.
 - 4 Double click to finish the track.
- The track created is indicated on the right, with its length.
- Click on the icon
 - Click on **REMOVE ALL** to remove all the tracks of the map
 - Open the **Layers > Visibility/Opacity** window to adjust the visibility of all the tracks (see "["Visibility/Opacity" on page 237](#)).

Figure 279 Measure Tool

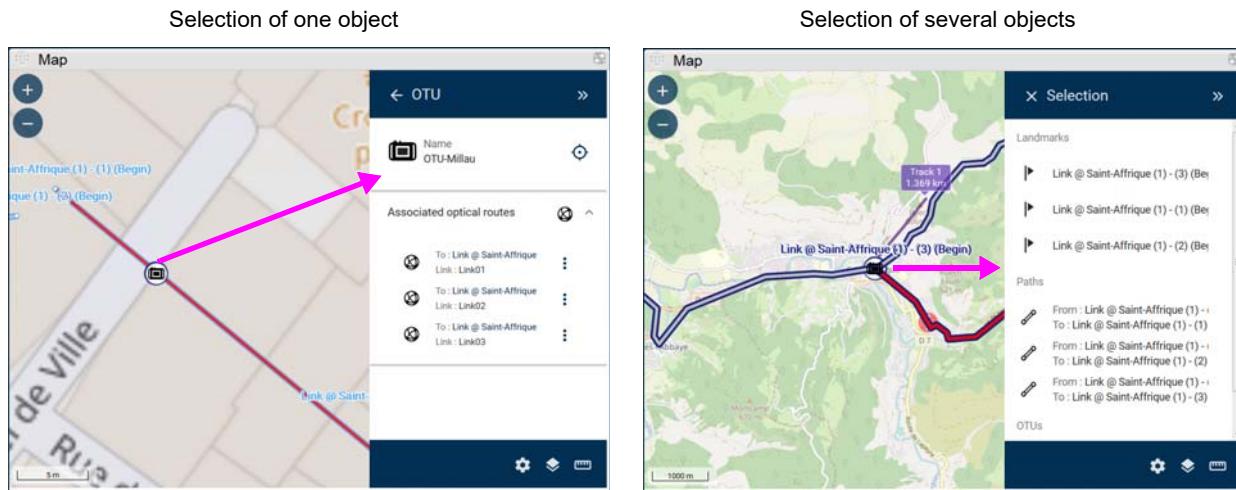


Object selection

On the Map view, the objects can be selected in two different ways:

- for the selection of one single object, click once to display the information related to this object
- if several objects are set on the same zone of the map, click once to display the list of objects available on the right and click on the object wished.

Figure 280 Object(s) selection



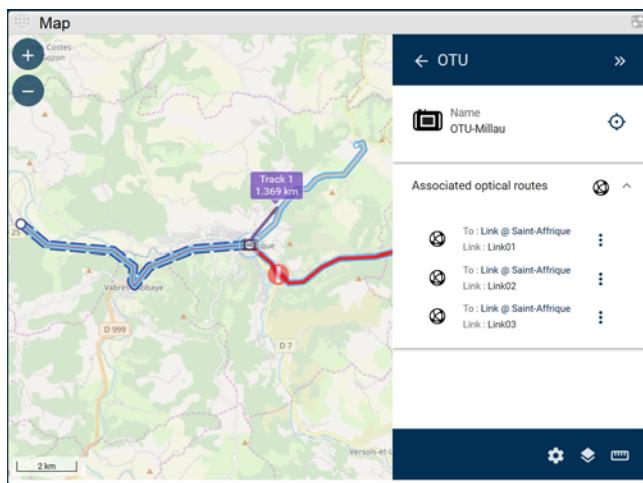
Three types of objects, for which information are available, can be selected:

- Path
- Landmark (path end points)
- OTU

In the object description window:

- the first part displays the path length (for path) and the name for OTU and landmark.
 - the second part displays the objects relation:
 - for the path -> the landmarks
 - for the landmark -> the path to which it belongs
 - for the OTU -> its links
 - the third part displays the optical route(s) associated with the object.
- Click on **:** and than on **Highlight** to highlight the optical route on the map (dotted line).

Figure 281 Path highlighted



GeoDesign

This chapter provides a description of the possible actions on map, using the GeoDesign option. The goal of the GeoDesign option is to create on a map, all the geographical objects of a system.

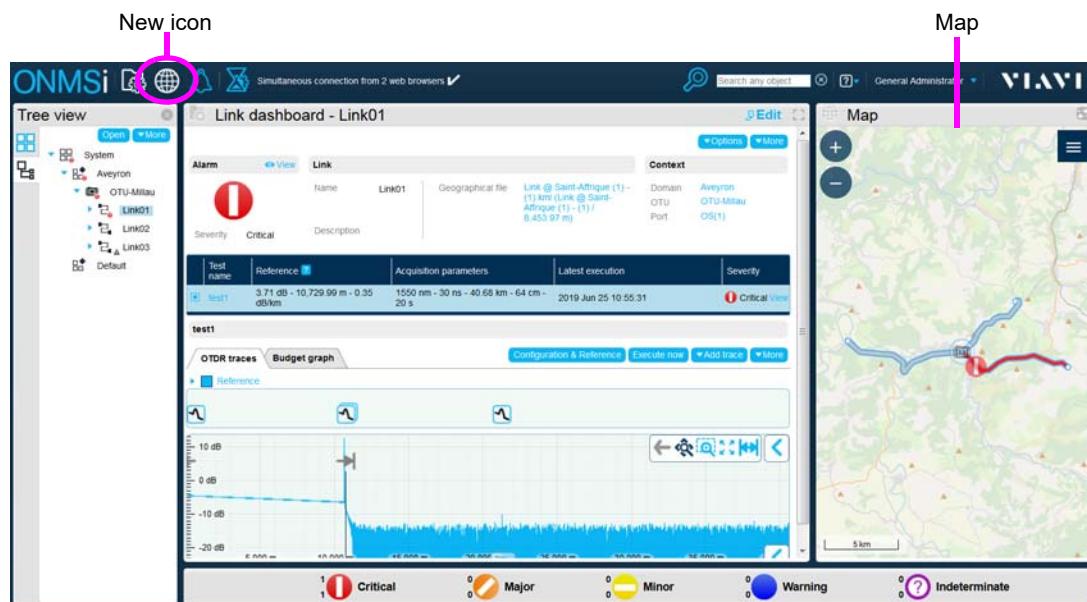
Topics discussed in this chapter include the following:

- “Pre-requisites” on page 242
- “Creating an object” on page 243
- “Importing/Exporting KML file” on page 253
- “Interaction with the map” on page 261
- “Interaction on map” on page 264

Pre-requisites

- Once the license is activated, the icon **Map** is displayed on the upper banner and a new window dedicated to mapping displays on the right.

Figure 282 GeoDesign installed

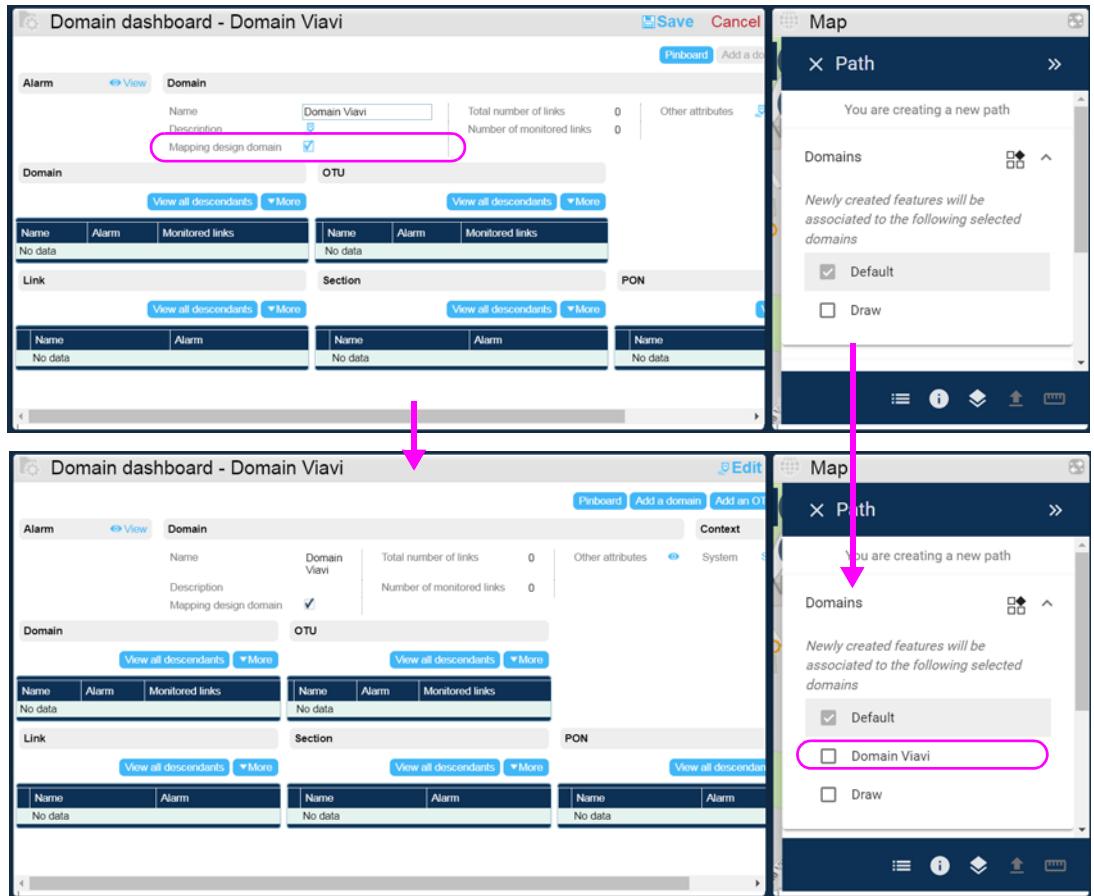


Adding a domain to the mapping design

- On the ONMSi system, double click on the Domain wished to display the Domain dashboard.
- Click on **Edit** to modify the domain configuration.
- Select the parameter **Mapping design domain**.
- Click on **Save** to validate.

The new domain is automatically available for mapping. It is displayed, and selectable, at the creation of a path or landmark.

Figure 283 Adding a domain to GeoDesign



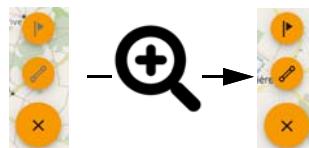
Creating an object

Both types of objects can be created from the map: a **Landmark** or a **Path**.

Before creating an object

- The zoom level on the map must be high enough to be able to create an object. If the map is not enough zoom-in, the objects are not activated (icons are grayed out). Zoom-in to activate the objects creation (icons turns black).

Figure 284 Tools activation



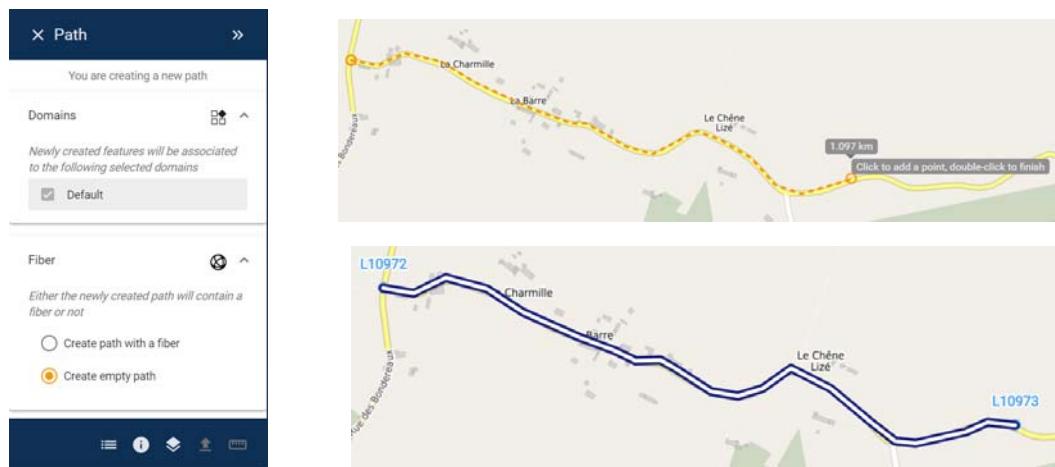
Creating a path

- 1 Click on  , on the map.
- 2 Click on the icon  to start designing a Path on the map.
The dialog box Path displays and indicates, in the first part, the Domain to which the new path will be associated.
- 3 Define if the new path will contain a fiber, selecting **Create a path with a fiber**, or not, selecting **Create empty path** (defined by default).

Designing a path without fiber

- 1 Click on the starting point of the path on the map.
The dialog box is hided.
- 2 Draw the path, clicking step by step to add a point.
- 3 Double click to define the end point of the path.

Figure 285 Designing an empty path



Designing a path with fiber

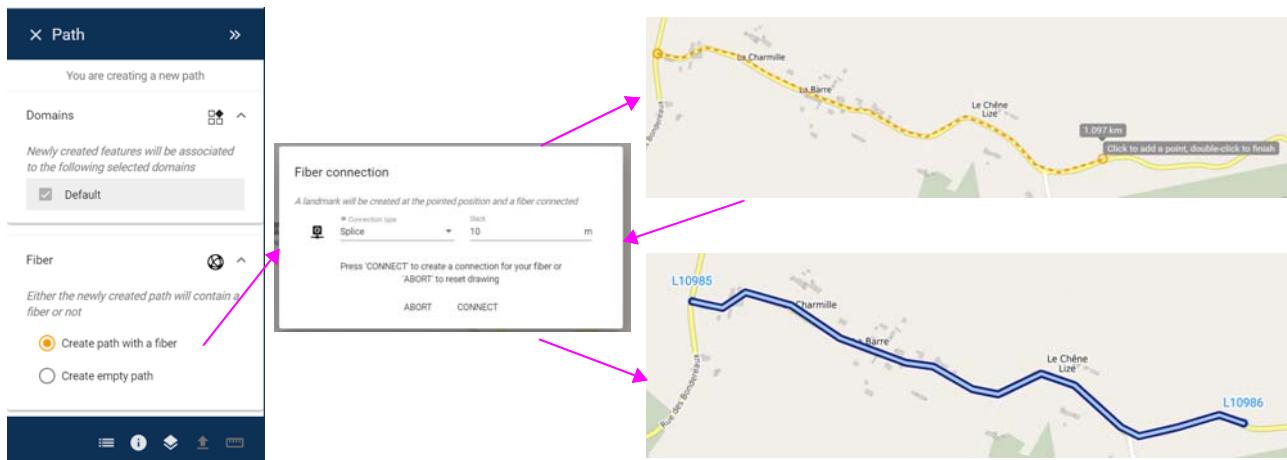
- 1 Click on the starting point of the path on the map.
The dialog box is hided.
The Fiber connection box displays.

Figure 286 Fiber connection box



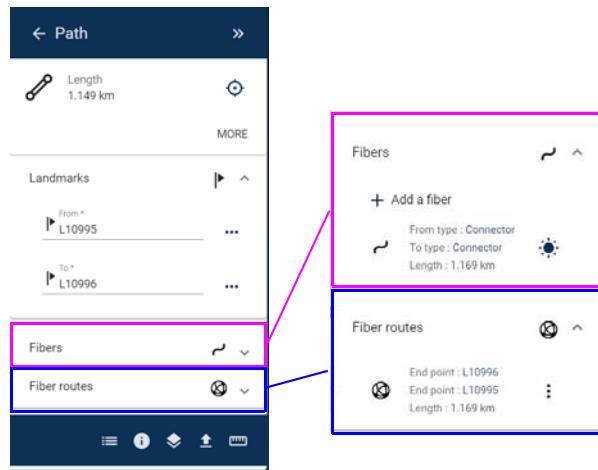
- 2 Define the **Connection type** of the fiber, at the starting point of the path: **Splice / Connector / Direct**.
- 3 Define the **Slack** (in meter).
- 4 Click on **CONNECT** to validate the fiber connection at the path starting point.
- 5 On the map, draw the path, clicking step by step to add a point.
- 6 Double click to define the end point of the path.
The Fiber connection box displays.
- 7 Define the **Connection type** of the fiber, at the starting point of the path: **Splice / Connector / Direct**.
- 8 Define the **Slack** (in meter).
- 9 Click on **CONNECT** to validate the fiber connection at the path ending point.
The path is designed with one landmark at each extremity.

Figure 287 Designing a path with fiber



- 10 Click on the icon and on the path to display the details of the path

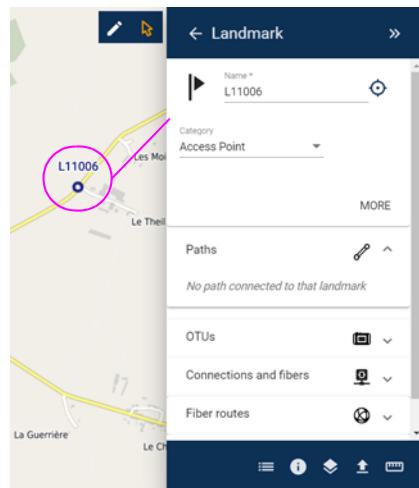
Figure 288 Path details



Creating a landmark

- 1 Click on on the map.
- 2 Click on the icon to start designing a Landmark on the map.
The dialog box Landmark displays and indicates, in the first part, the Domain to which the new landmark will be associated.
- 3 Click on the map, at the position of the landmark.
The Landmark dialog box displays

Figure 289 Landmark dialog box



- 4 In the **Name** parameter, click on the current name to modify it (for example, enter the road name).
- 5 If necessary modify the landmark **Category: Access Point or Building**.

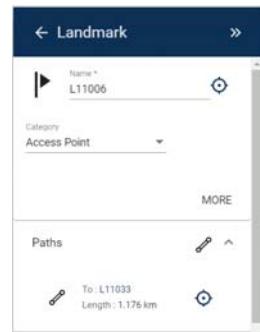
Connecting a Path to a landmark

Once a Landmark has been added on the map, a path can be associated to it.

In the **Landmark** window, open the **Path** sub-menu.

- 1 Click on the icon  and click on the path icon .
- 2 Click on the map, and design the path, starting or ending the path with the landmark previously created, clicking exactly on the landmark .

Once created, a path is associated to the Landmark.

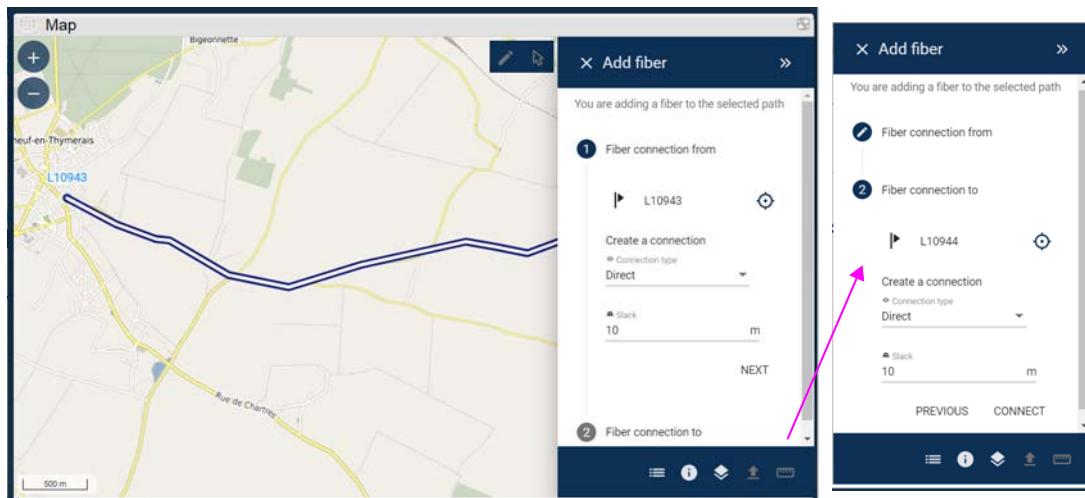


Adding a fiber to a path

Once a path has been designed, a fiber can be added, whether the path has been created with or without fiber.

- 1 Select the path using the tool .
- 2 In the **Fibers** sub-menu, click on  Add a fiber. The box **Add fiber** displays
- 3 In the **Fiber connection from** window, define the **Connection Type** (Splice / Connector / Direct) and the **Slack** (in meter) for the origin of the fiber.
- 4 Click on **NEXT**.
- 5 In the Fiber connection to window, define the same parameters for the extremity of the fiber.
- 6 Click on **CONNECT** to validate the fiber connection to the path.

Figure 290 Adding a fiber to a path



If the path was empty (white with dark blue borders), it is represented in light blue to indicate a fiber has been added.

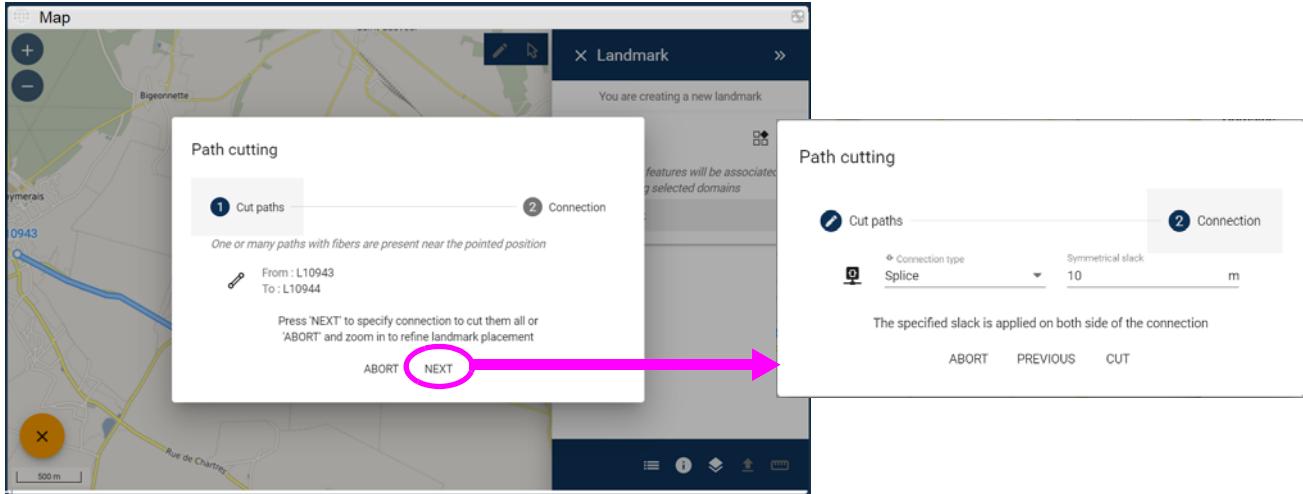
Adding a landmark

Adding a landmark on the path with fiber

Once a path has been created, even with one connector at each extremity, landmarks can be added on this path, creating a path cut:

- 1 Click on on the map.
- 2 Click on the icon to start designing a Landmark on the path.
- 3 Click on the path, at the position of the landmark must be.
The Path cutting box displays.
- 4 The first box indicates the path, with its position, which will be cut if a landmark is created.
- 5 Click on **CUT** to confirm the landmark onto the path.
- 6 In the second box, define the type of connector of the landmark (**Connector**, **Splice** or **Direct**).
- 7 Define the **Symmetrical slack** position (in meter).
- 8 Click on **CUT** to validate the path cutting.
Click on **PREVIOUS** to return to Cut paths box
Click on **ABORT** to cancel the path cutting.

Figure 291 Path cutting

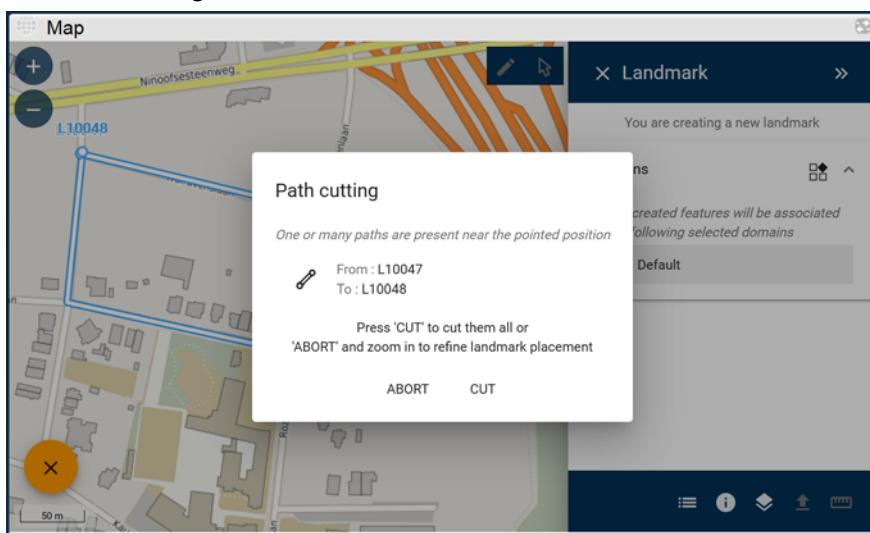


Adding a landmark on the path without fiber

Once a path has been created, even with one connector at each extremity, landmarks can be added on this path, creating a path cut:

- 1 Click on on the map.
- 2 Click on the icon to start designing a Landmark on the path.
- 3 Click on the path, at the position of the landmark must be.
The Path cutting box displays.
- 4 Click on **CUT** to confirm the landmark onto the path.
Click on **ABORT** to cancel the path cutting.

Figure 292 Path cutting



Adding an OTU

The OTU can be added from the GeoDesign or from the OTU page of the ONMSi system.

Adding an OTU from GeoDesign

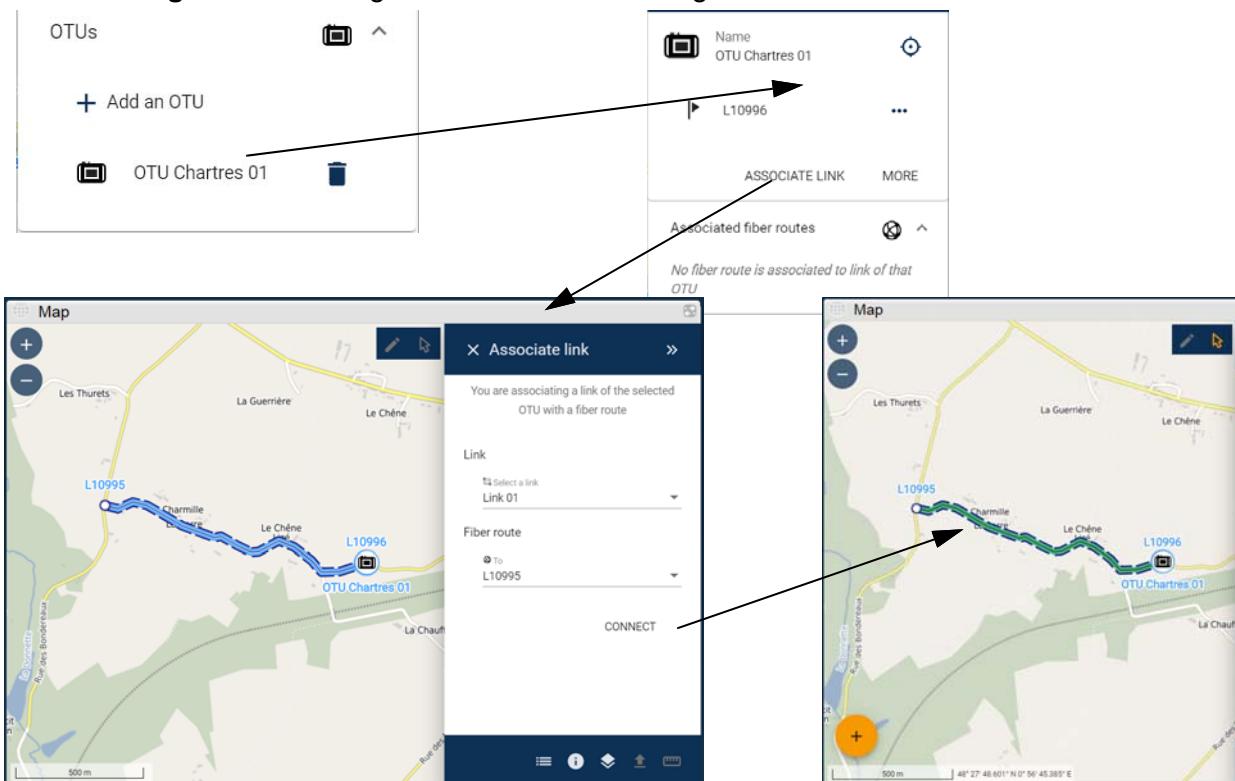
From a landmark, an OTU Can be added to the GeoDesign map:

Select the landmark.

- 1 Click on **OTU** to open the sub-menu
- 2 Click on **Select an OTU** to display the list of all the unused OTU of the ONMSi system.
- 3 Select the OTU to be added to the landmark.
- 4 Click on **ADD OTU** to confirm the OTU adding.
- 5 Click to show the OTU details: the landmark and the fiber route to which it can be associated.
- 6 Click on **ASSOCIATE LINK** to associate a link of the OTU with a fiber route.
The path is represented with a dotted blue line.
- 7 Define a link and the end point to be associated to the OTU.

Once association is completed, the fiber route is represented on the map with a green line (and a dotted blue line when object is selected).

Figure 293 Adding an OTU and associating a link



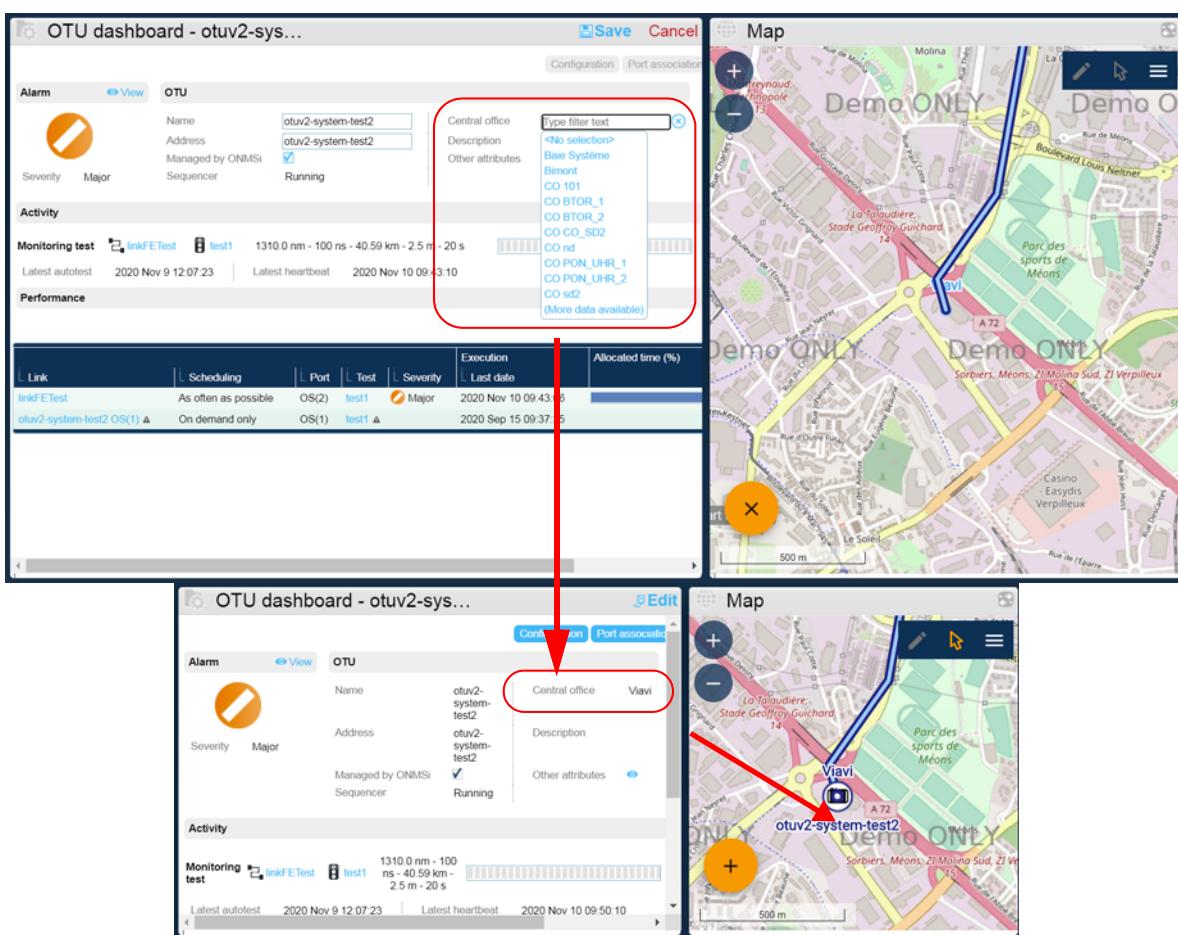
Adding an OTU from the ONMSI

The OTU can be added on the map from the ONMSI system:

- 1 From the OTU page, click on **Edit**.
- 2 In **Central Office** parameter, the list of existing landmarks is displayed, among which are the OTU.
- 3 Select the OTU or enter the first letters to easily find it in the list.
- 4 Click on **Save**.

The OTU is displayed on the map.

Figure 294 OTU added from OTU page

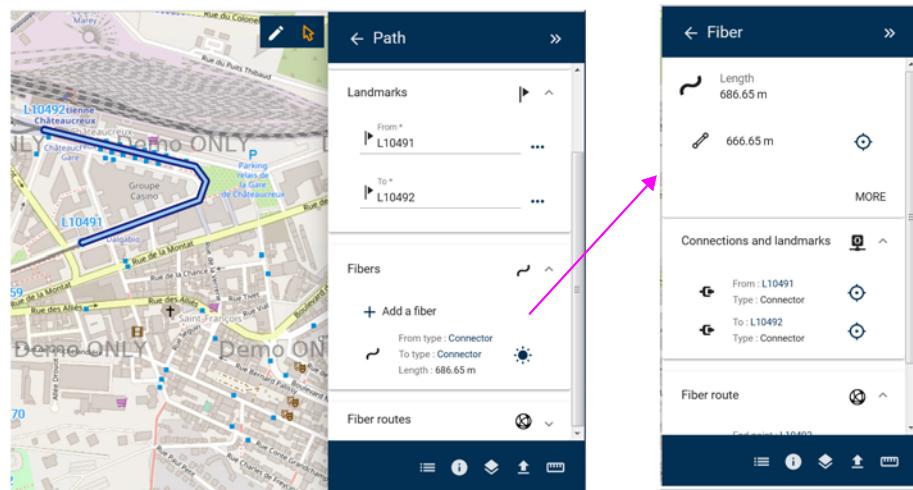


Visualizing a fiber details

To see the details of a fiber and of a connection

- 1 Click on the path onto which a fiber is defined.
- 2 In the **Fibers** box, click on the fiber description to display the fiber details

Figure 295 Fiber details



NOTE

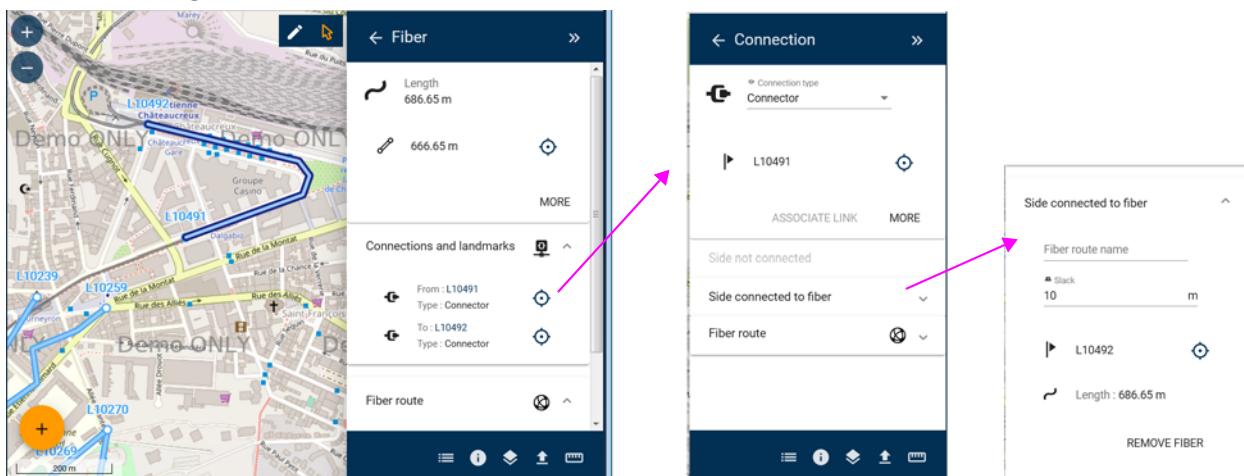
To remove a fiber, open the Connection box: see “[Visualizing a connection details](#)” on page 252.

Visualizing a connection details

The connection of a fiber can detailed in the right frame:

- 1 In the **Fiber** box, click on one **Connection** to display the details for this connection.
or
From **Landmark** box, open **Connection and fibers** box and click on one connector to display the details.

Figure 296 Connection details



- 2 Open the **Side (not) connected to fiber** to display and enter name of the route at that end point and the Slack.

- 3 From the **Connection** box, the fiber to which it is connected can be removed clicking on **REMOVE FIBER**.

A confirmation is required, and the dialog box informs you the fiber route will be modified.

Importing/Exporting KML file

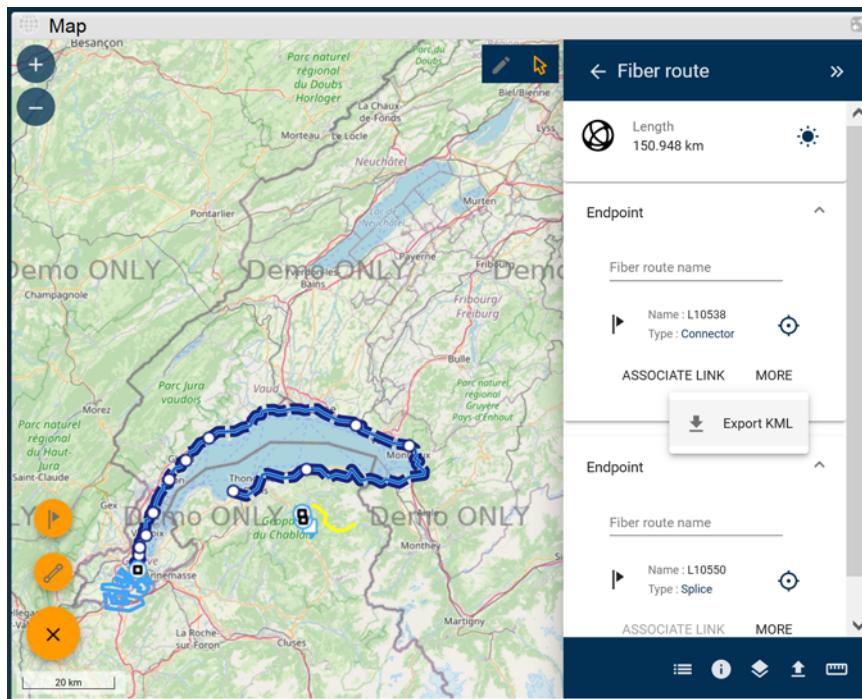
The GeoDesign option allows to import or export a KML file from/toward a mapping software (such as Google EarthTM).

Exporting a fiber route

Once a fiber route has been designed in GeoDesign, whether it is monitored or not, it can be exported toward a KML file and downloaded in a mapping software:

- 1 Select the Fiber route on the map.
- 2 Click on **Fiber route** to display the details.
- 3 Click on **More > Export KML**.

Figure 297 Export fiber route



Importing a KML file

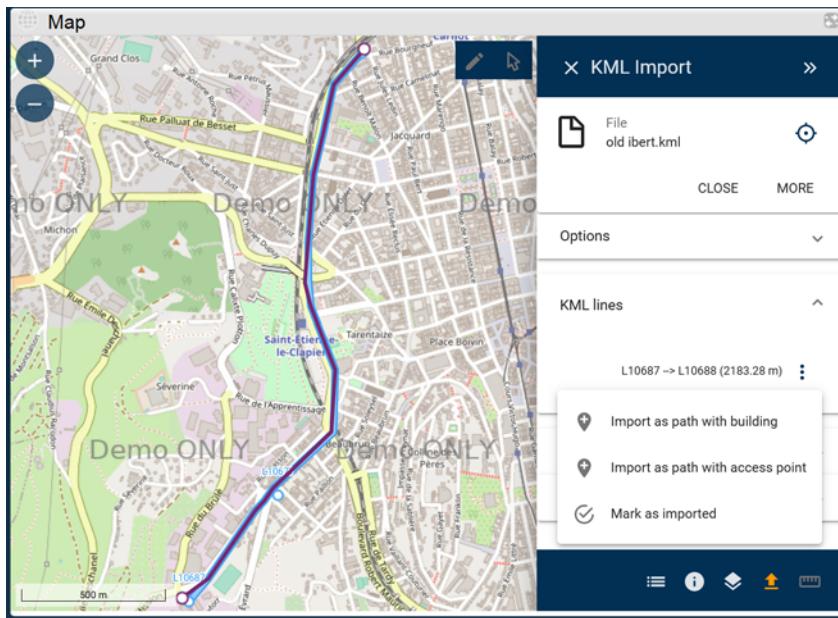
Once a fiber route has been designed with a mapping software, and saved in a KML file, it can be imported manually or automatically into the GeoDesign map.

Manual import of the KML file

- 1 On the Map view, zoom in around the area of the fiber route drawn in the mapping software.
 - 2 Open the Main panel clicking on .
 - 3 At the bottom of the Panel, click on the icon  to open the Import KML window.
 - 4 Select **Manual Import** and click on the grey frame to browse a file or drag it on the zone.
 - 5 Select the file and click **Open**.
- The fiber route is drawn on the map, in purple.
If necessary, click on  to locate route on the map.
- 6 Open the **KML lines** menu and click on **Import as path with building/access point** to import the path with one building/access point at each extremity.
If, on the mapping software, the path was drawn with points, open the **KML points** menu and define the points as buildings or paths.



Figure 298 Fiber route manually imported



- Select **Mark as imported** to move that KML feature to import history.
- 7 If necessary, click on **Options** and modify the **Overlap margin**: specify the distance used to detect overlap between KML features and network features (see “Path close to an existing one” on page 260).
 - 8 Click on **Create new path** to validate the path imported from KML file.

To retrieve the KML features before the path creation, open the **Import history** menu and click on the icon  to reset report history.

Import history
KML lines

 L10687 -> L10688 (2183.28 m) 

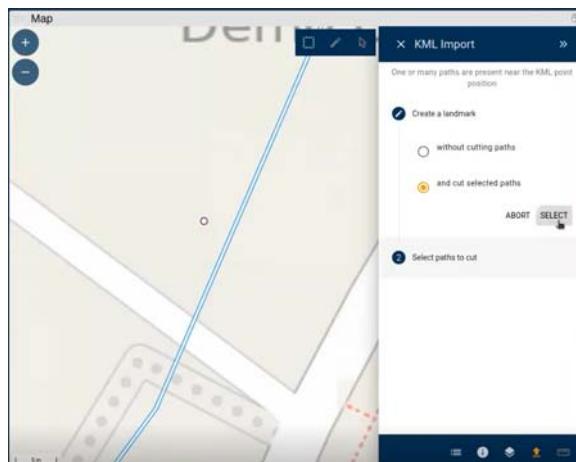
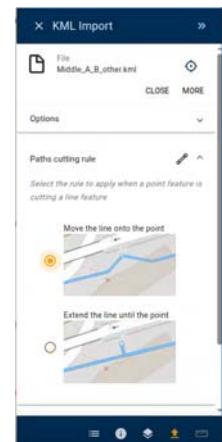
Cutting a path by a landmark

Once a KML file with a path is imported, this path can be cutting in 2 different methods:

- move the last segment of the path to the new landmark
- make' an “extra line” to go to the landmark

To cut a path manually imported:

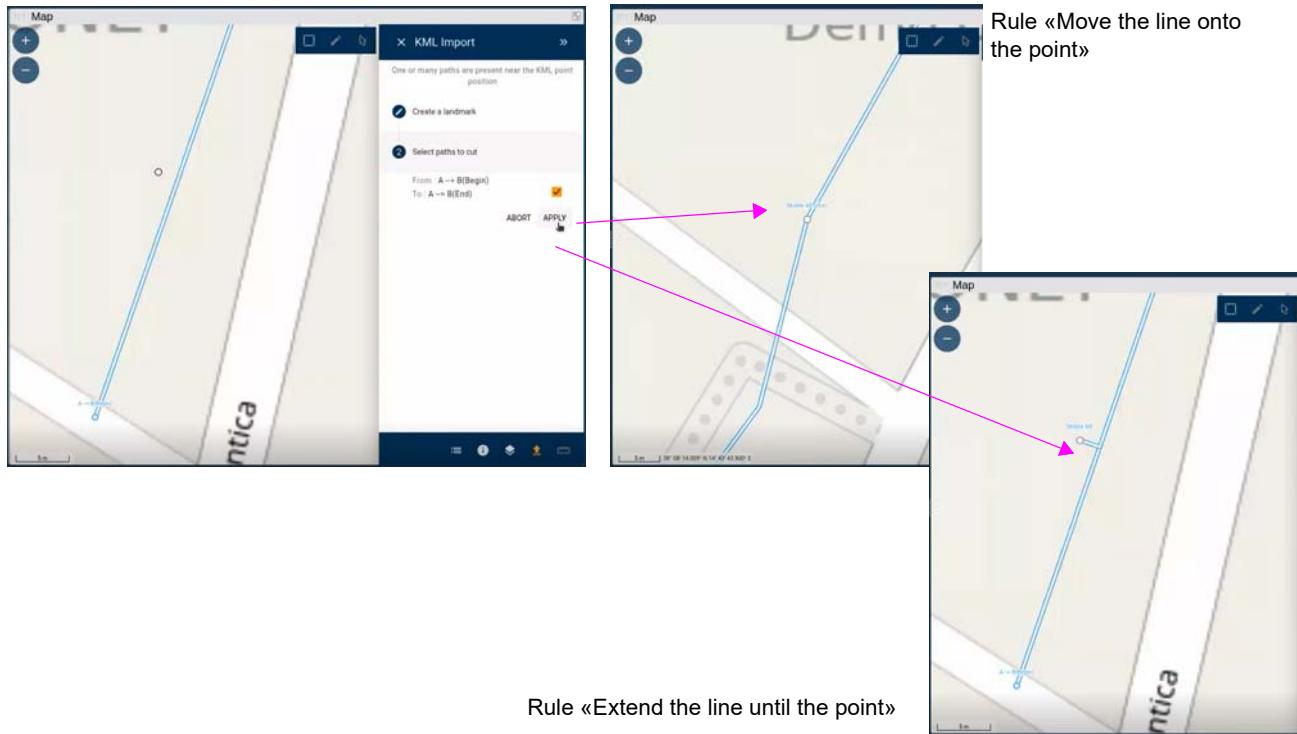
- 1 Once the path is created, import a KML file with only one point.
- 2 In **Path cutting rule** menu, select **Move the line onto the point**, to move the last segment to the new landmark.
or
Select **Extend the line until the point**, to create an “extra line” to reach the new landmark.
- 3 Open KML points sub-menu, and open the point menu and click on Import as access point
- 4 In **Create a landmark**, select “**and cut selected path**” and click on **SELECT**.



- 5 In **Select paths to cut**, select the path to cut with the access point and click on **APPLY**.

The path is modified according to the rule previously defined.

Figure 299 Cut path with a landmark



Automatic import of the KML file

The KML file, exported from the mapping software, can contain multiple paths and landmarks (size < 10Mb).

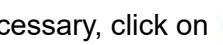
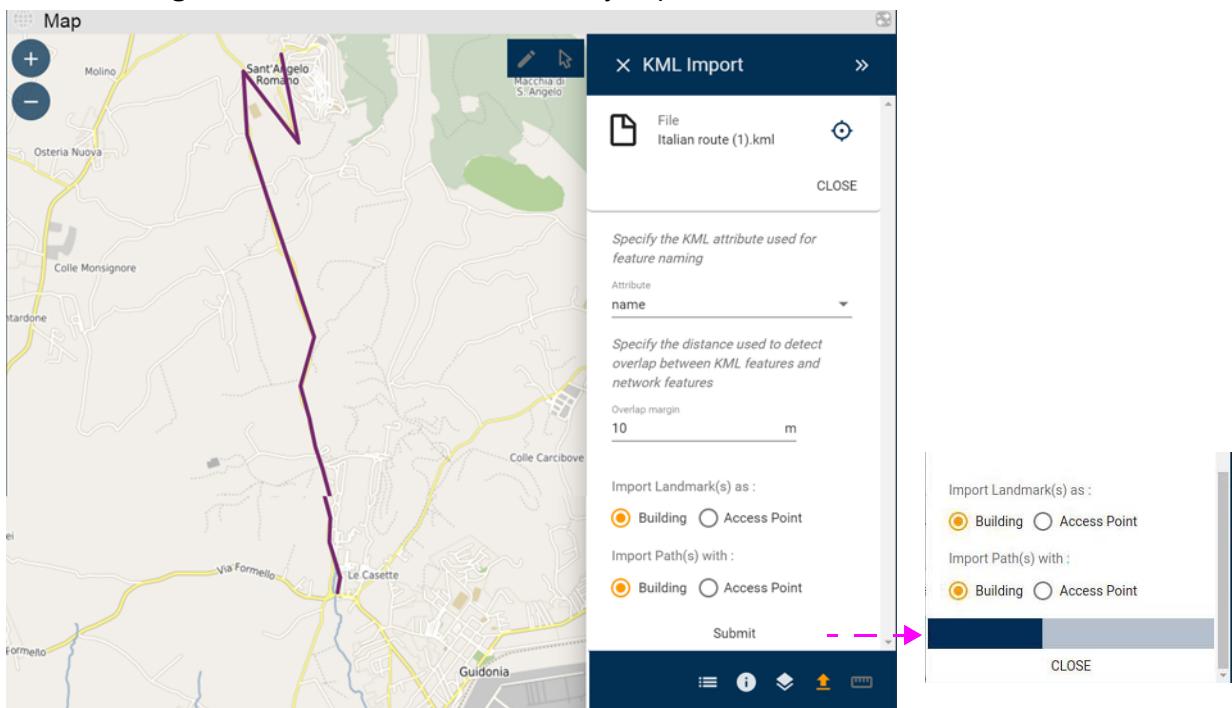
- 1 Open the Main panel clicking on .
- 2 At the bottom of the Panel, click on the icon  to open the Import KML window.
- 3 Select **Auto Import** and click on the grey frame to browse a file or drag it on the zone.
- 4 Select the file and click **Open**.
The fiber routes are drawn on the map, in purple.
If necessary, click on  to locate routes on the map.
- 5 Specify the KML **Attribute** used for landmarks naming.
- 6 If necessary, modify the **Overlap margin**: specify the distance used to detect overlap between features (if features overlap, the existing one or the first created is kept).
- 7 If, landmarks were exported from mapping software, in **Import Landmark(s) as**, define the points as **Buildings** or **Access Points**.
In the **Import Path(s) with**, select the landmark type **Building** or **Access Point** to import the path with one Building/Access Point at each extremity.

Figure 300 Fiber route automatically imported



- 8 Click on **Submit** to validate the paths and landmarks imported from KML file.
- A progress bar is displayed during the import.

Geodesign is automatically refreshed at the end of the processing.

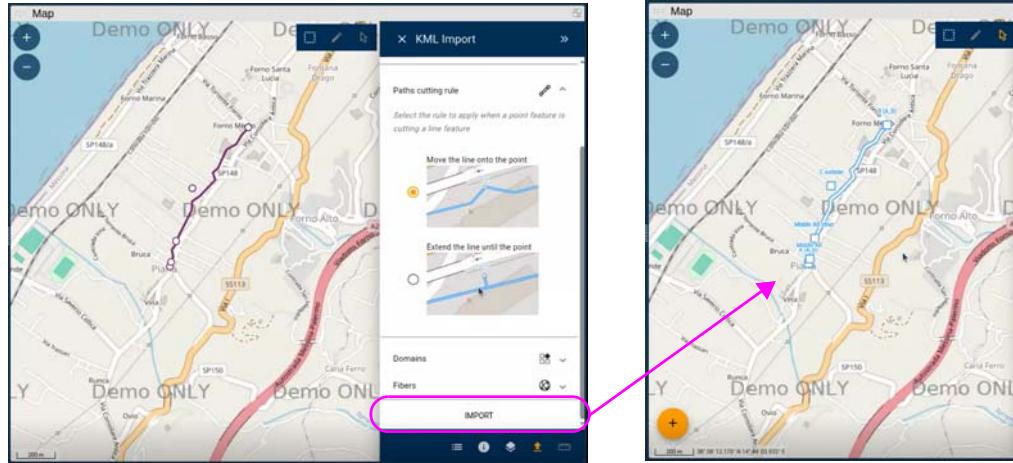
Cutting a path by a landmark

The path automatically import can be cut in 2 different methods, as in manual import (see [page 254](#)).

To cut a path automatically imported:

- 1 Once the path is created, import a KML file with only one point.
- 2 In **Path cutting rule** menu, select **Move the line onto the point**, to move the last segment to the new landmark.
or
Select **Extend the line until the point**, to create an “extra line” to reach the new landmark.
- 3 Click on **IMPORT**.

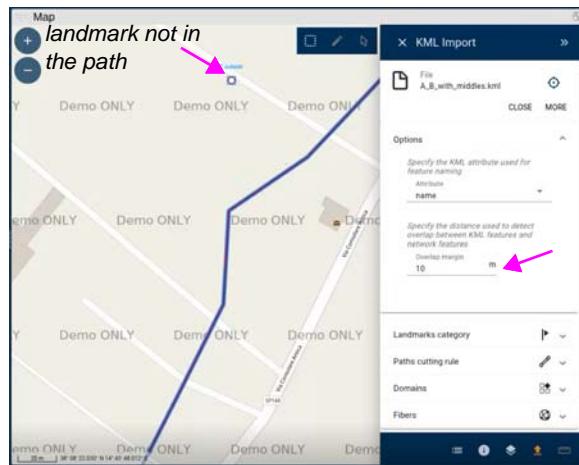
Figure 301 Automatic import with cut path



The path is cut with the landmark(s) close to this path.

If a landmark does not cut the path, it is due to the distance between the path and the landmark, which is higher than the overlap margin, defined in the **KML Import > Options** menu.

Figure 302 Overlap margin



Automatic import of a KML file with a fiber

- Once the KML file is imported automatically, open **Fibers** sub-menu.

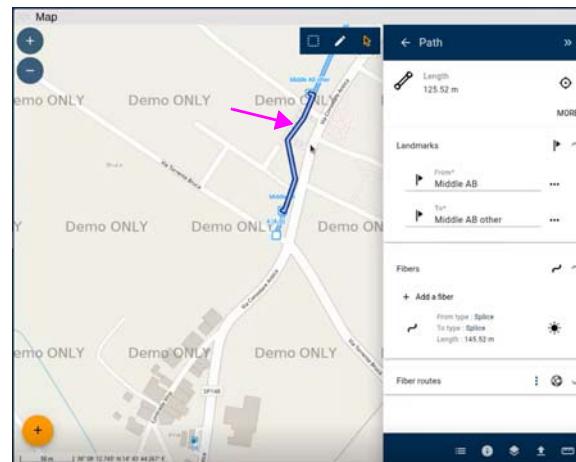
Figure 303 Adding a fiber to a path



- 2 Select the option **Check to create a fiber in the path**.
- 3 Define the connector type for the fiber: **Connector**, **Splice** or **Direct**.
All the paths and all the landmarks of this KML file will be defined with this connector type.
- 4 If necessary, modify the **Slack** to apply around the connections.
- 5 Click on **Import**.

The fiber is designed onto the path.

Figure 304 Fiber added to a path



Resetting the KML file history

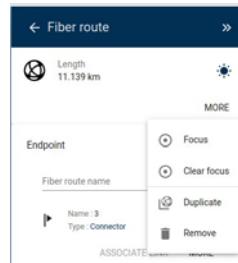
To import a KML file that had already been automatically imported, from the KML window, press **More** and click on **Reset history**.

This will reset the filename: it will remove it from the database so that you can import it again.

Deleting a Fiber Route

A route and its objects (fiber and connections) can be deleted from the **More** menu.

To be able to remove a route, it must not be associated with a link: see “[Dissociating a link](#) on page 270.

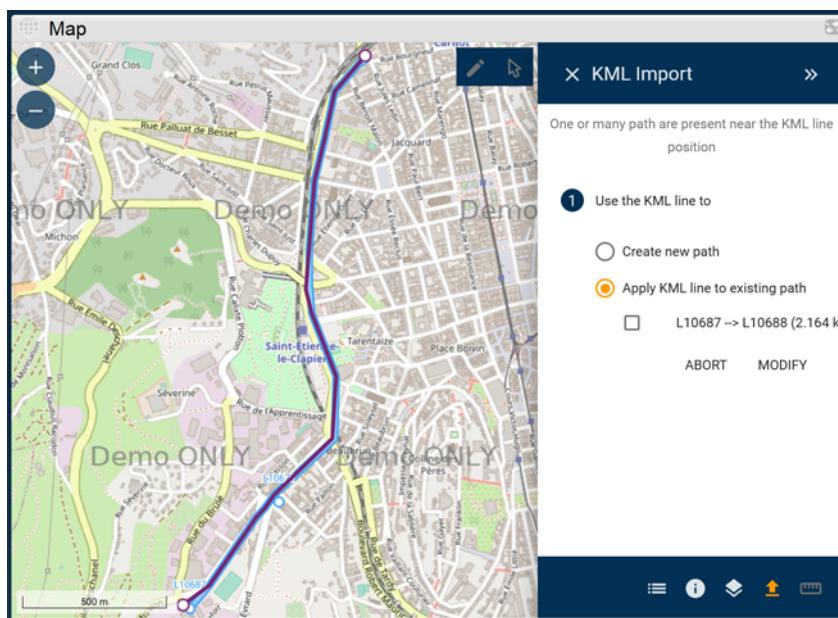


Path close to an existing one

If the imported path is very close and similar to an existing one in GeoDesign, then the dialog box allows to choose whether the path is a new one or if it replaces the existing one:

If the imported path is inside the area defined in **Overlap margin**, then it is considered as similar (see [step 7](#)).

Figure 305 Creating a path close to an existing one



Click on **Apply KML line to existing path**, select the path, and click on **Modify** to replace the existing path with the new one imported.

NOTE

If the imported path is longer/shorter than the existing one, it is not consider as similar.

Interaction with the map

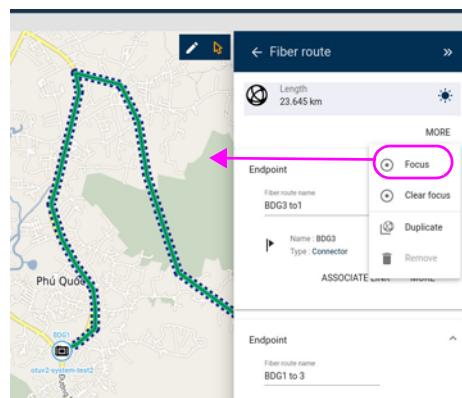
From the map, you can visualize:

- the OTU linked to the link
- the link itself
- the alarms on that link, if any.

Focus on a fiber route

From the **More** menu, a route can be selected (Focus) in order to help identifying its object (its objects gets highlighted on the Panel,) and the route is clearly identified on the map.

Figure 306 Focused route



- Only one route at a time can be focused
- And the **Focus** is cleared by the user by selection **Clear focus** for the corresponding route.

Duplicating a fiber route

To speed up the process when several routes are identical (for ex in case of several fibers monitored in a same cable), a route can be duplicated from the **More** menu \ **Duplicate**.

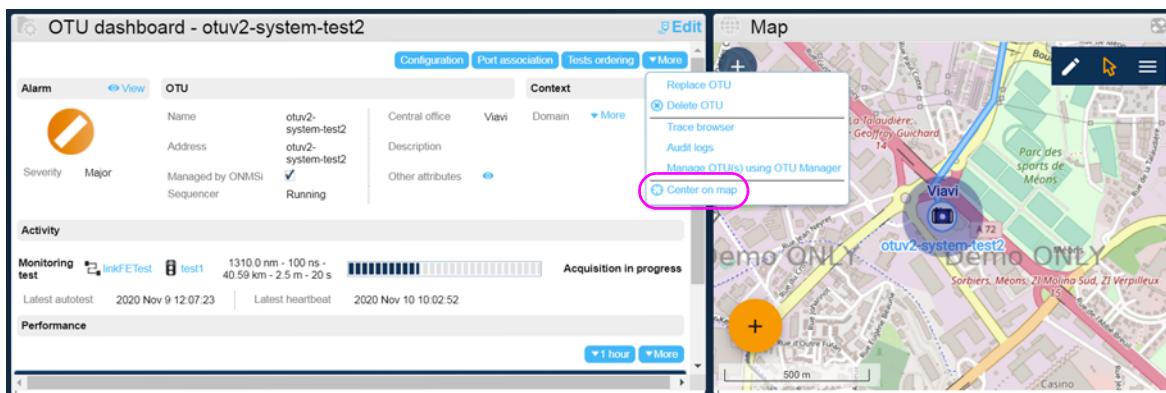
Centering the map on the OTU

To display the OTU centered on map:

- 1 Go to the **OTU dashboard**.
- 2 Click on **More**.
- 3 Click on **Center on Map**.

The OTU is highlighted and centered on the map.

Figure 307 OTU centered on map



Centering the map on the Link

To display the link centered on map:

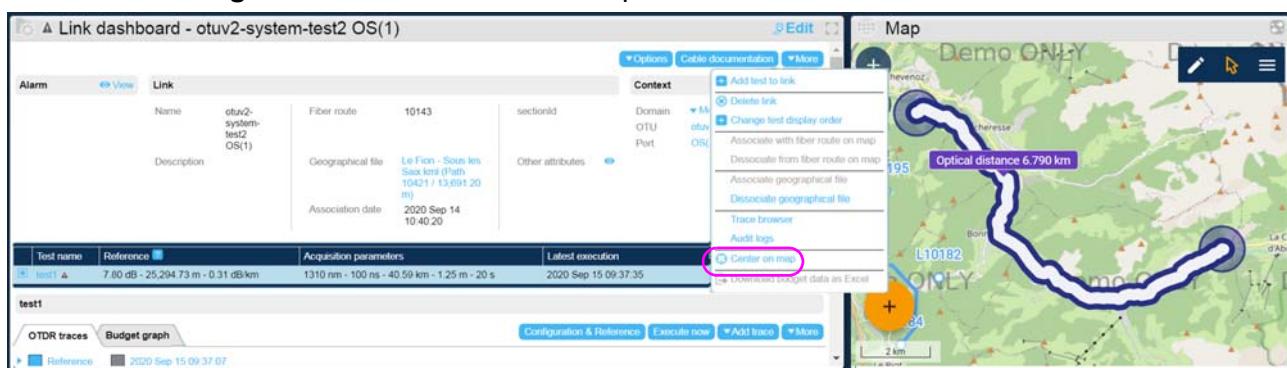
- 1 Go to the **Link dashboard**.
- 2 Click on **More**.
- 3 Click on **Center on Map**.

The Link is highlighted  and centered on map.

Once centering process is completed:

- the link is displayed in grey, without alarm on the link
- it is displayed in red/orange if an alarm is present on the link.

Figure 308 Link centered on map



Centering the map on the Alarm

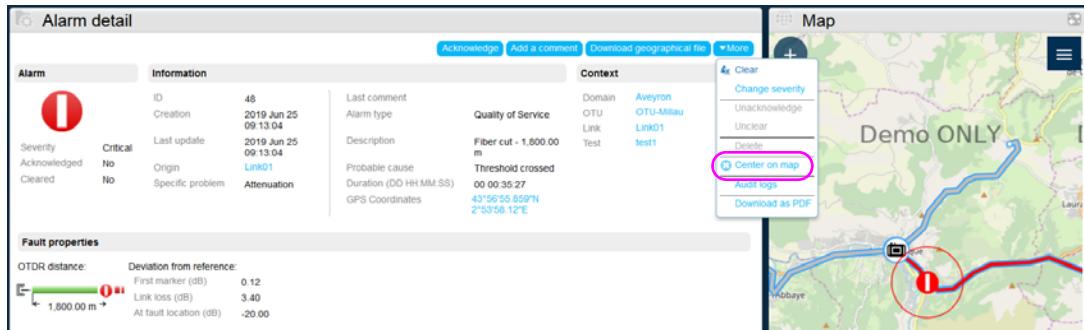
To display the Alarm centered on map:

- 1 Go to the **Alarm dashboard**.
- 2 Click on **More**.

3 Click on Center on Map.

The alarm is highlighted and centered on map.

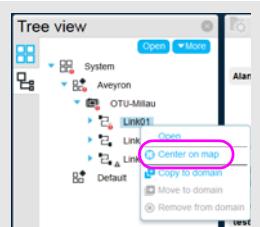
Figure 309 Alarm centered on map



NOTE

The **OTU** and **Link** can be centered on map from the Tree view:

- Right click on the OTU / Link and click on **Center on Map**.



Trace viewer and map

Once the GeoDesign is installed, a new tool **Trace tracking** is available on the trace viewer.

This tool allows to locate from the otdr trace a point on the map link.

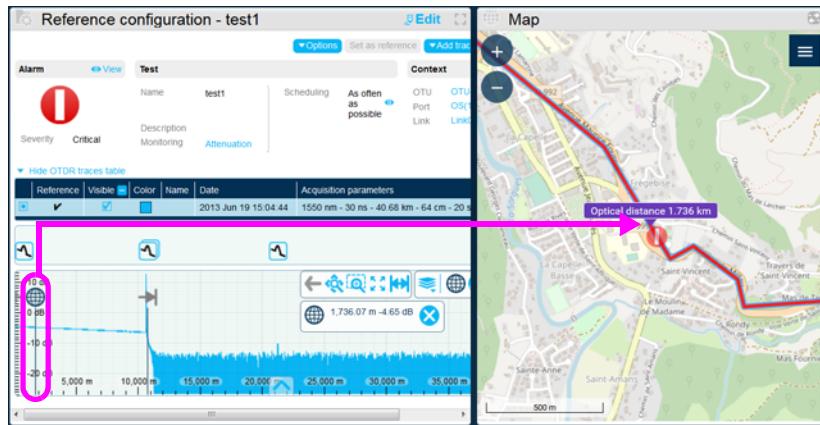
- Open the Trace viewer (see [Chapter 7 on page 45](#))
- On the trace view, click on the tool **Trace Tracking**.
- Set the cursor on the trace, at the position wished.

The trace displays with a vertical line with the icon

The corresponding point is represented on the map by a purple mark indicating the optical distance.



Figure 310 Trace tracking



Click on to hide the trace tracking tool and representation on trace and on map.

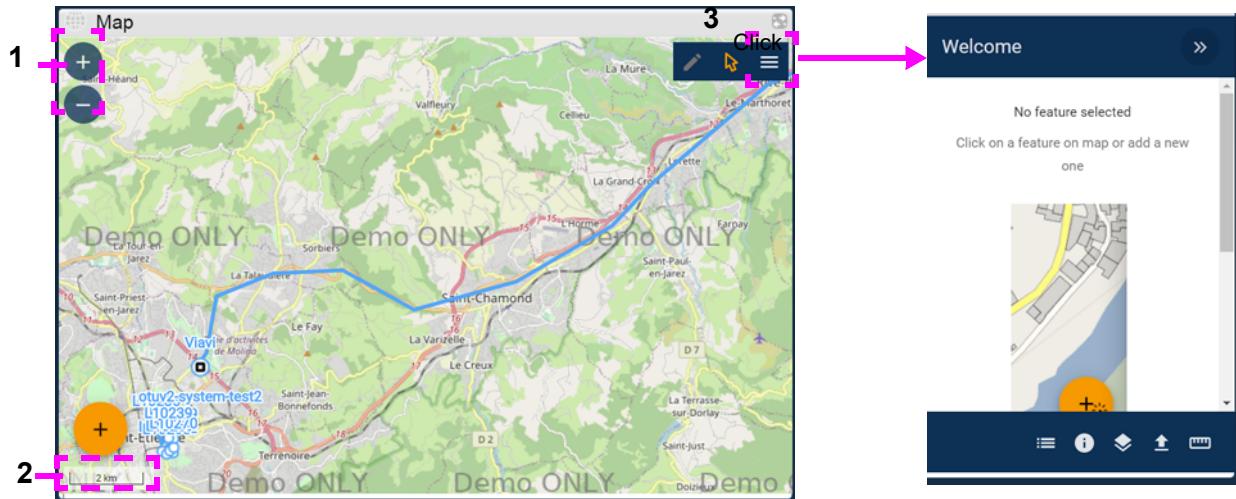
If you click again on Trace tracking tool, the last tracking defined will display back.

Interaction on map

The map window contains the following element:

- 1 On the upper left part of the map, the + and - buttons, allowing to zoom in / out on the map.
To navigate on map, you can also:
 - Zoom in / out on the map using the mouse roll.
 - Displace on the map, maintaining the mouse left button pressed and dragging the mouse.
- 2 At the bottom of the map, display the scale and the mouse tracker (gps coordinates of the mouse position).
- 3 On the upper right part of the map, click on to display main Panel and Tools.

Figure 311 General view on map



Tools and Detail panel

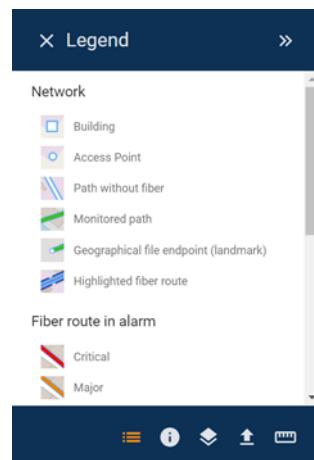
Once the Tool and detail panel is opened, four tools are available at the bottom of the dialog box:

- the Legend tool
- the Information tool
- the Layers setting tool
- the Measure tool

Legend tool

Click on the icon  to display the legend of all the elements available on GeoDesign map.

Figure 312 Legend

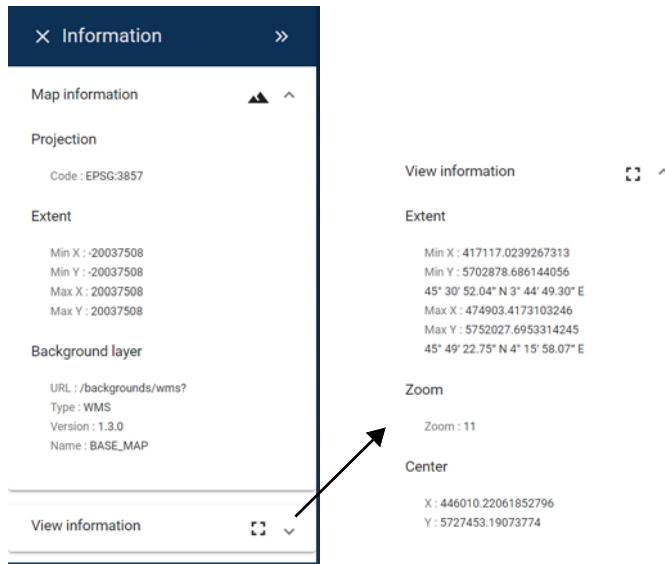


Information tool

The information tool allow to display information available for the map and for the current view (not changeable).

Click on **Information** icon  to display the different elements described:

Figure 313 Settings menu



- **Projection:** display the information on geographical projection.
- **Bounds:** display the limits if the map
- **Background layer:** displays the URL allowing to access to the map image (advanced settings)

The **View** window displays the information relative to the current view of the map (Extent / Zoom / Center).

Layers Tool

The layer tool window is dedicated to the objects visibility on map.

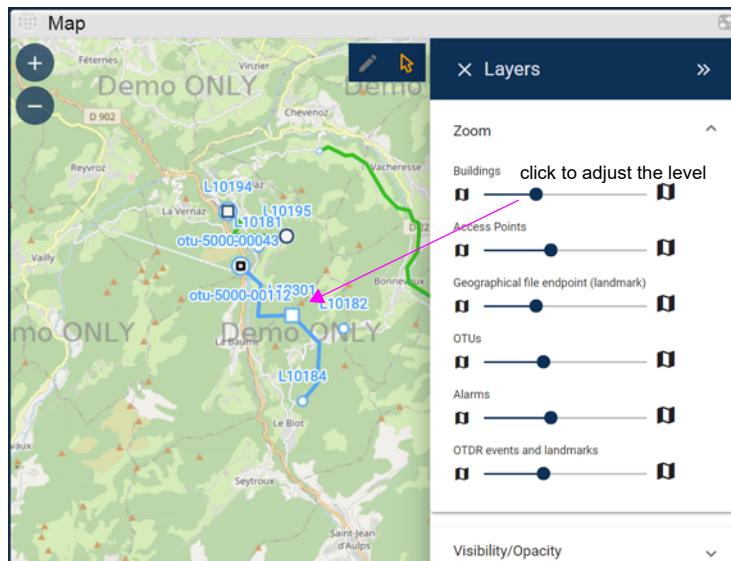
Click on **Layers** icon  to display the 2 sub-menus available: **Zoom** or **Visibility/Opacity**.

Zoom

The **Zoom** sub-menu allows to define the objects visibility according to the zoom level defined for the map.

Navigate on the object bar pressing the button to adapt the zoom level.

Figure 314 Adjusting Objects Zoom



The icon indicates the object is not visible on map with the current map zoom level.

Maintain the cursor on the button of an object to have an indication of the zoom level selected.

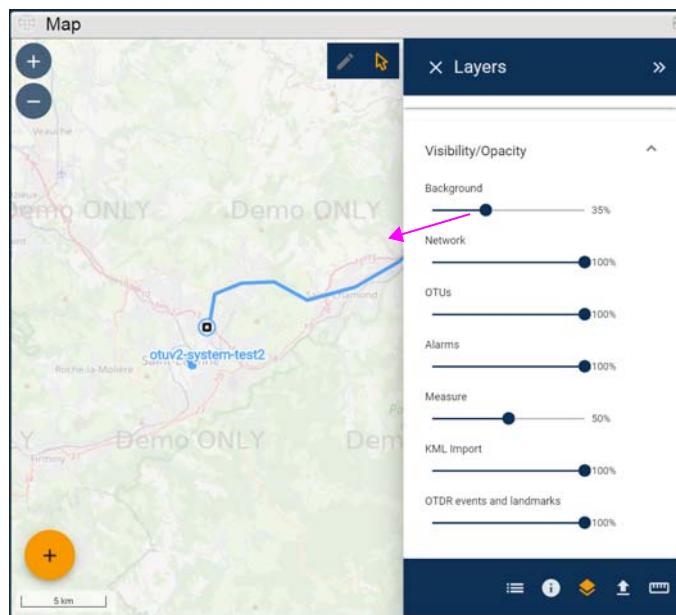


Visibility/Opacity

The **Visibility/Opacity** sub-menu allows to adjust the visibility of the objects: Background / Network / OTUs / Alarms / Measure.

Click on the button of one object to make it more or less visible on the map.

Figure 315 Visibility of the objects

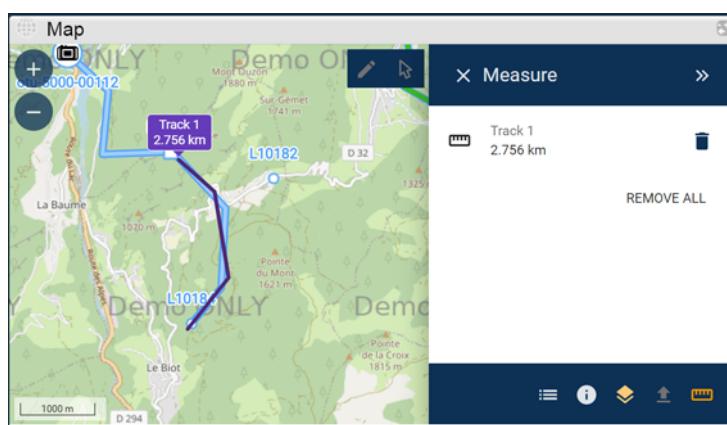


Measure Tool

The Measure tool window allows to measure tracks on map.

- 1 Click on **Measure** icon 
- 2 Click on the map at the starting point of the tracks
- 3 Click once on the following point(s) of the track.
- 4 Double click to finish the track.
The track created is indicated on the right, with its length.
 - Click on the icon  to remove the track.
 - Click on **REMOVE ALL** to remove all the tracks of the map
 - Open the **Layers > Visibility/Opacity** window to adjust the visibility of all the tracks (see "[Visibility/Opacity](#)" on page 267).

Figure 316 Measure Tool



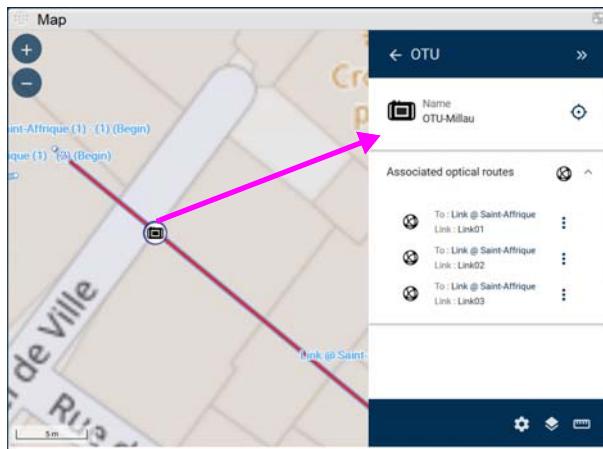
Object selection and details

On the Map view, the objects can be selected in two different ways:

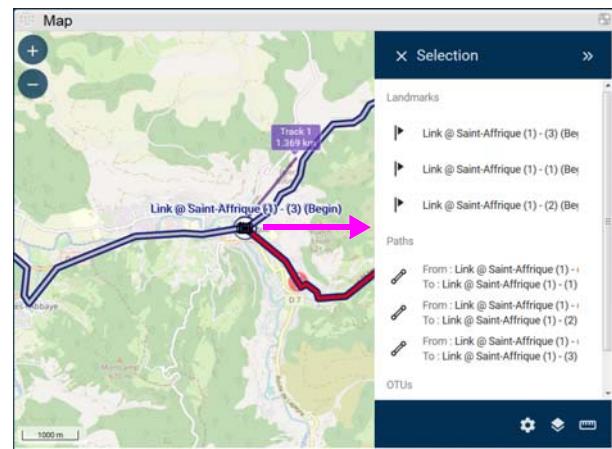
- for the selection of one single object, click once to display the information related to this object
- if several objects are set on the same zone of the map, click once to display the list of objects available on the right and click on the object wished.

Figure 317 Object(s) selection

Selection of one object



Selection of several objects



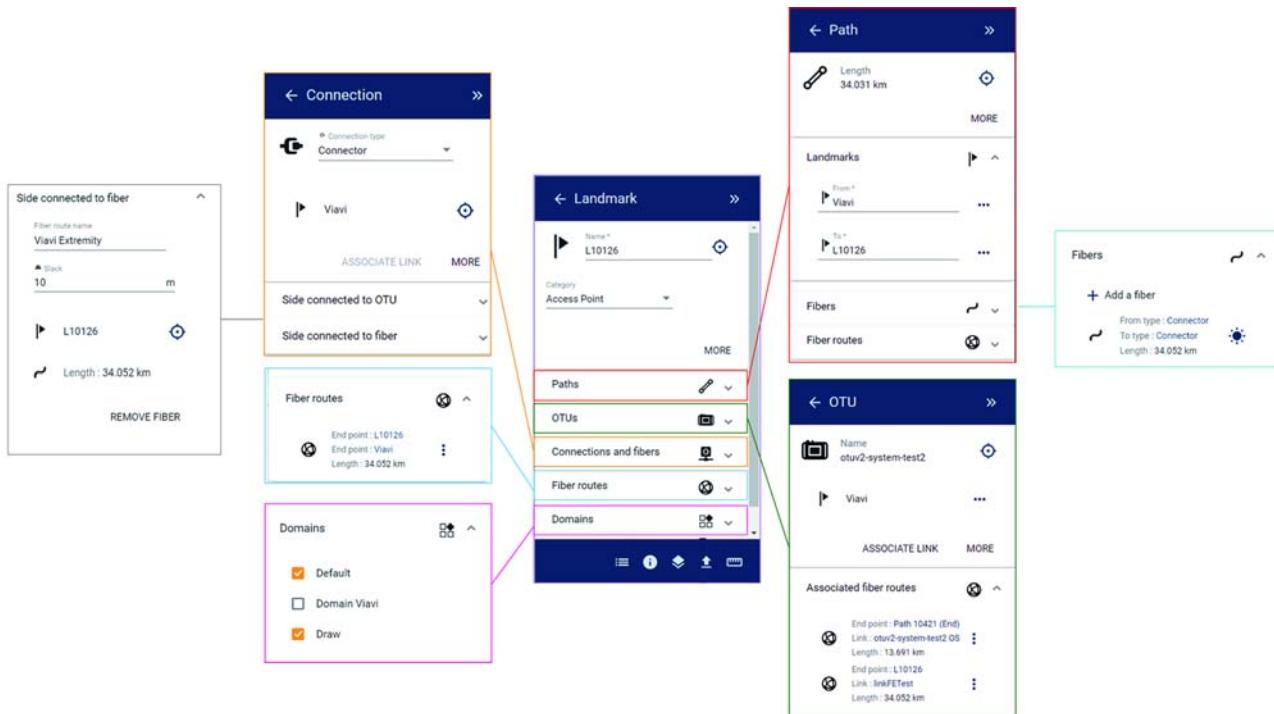
Three types of objects, for which information are available, can be selected:

- Path
- Landmark (path end points)
- OTU

In the object description window:

- the first part displays:
 - the **Paths** length
 - the name for **OTUs** and associated links.
 - the **Landmark** name and Category.
- the following parts display the object relations:
 - for the **Paths** -> the **Landmarks** defined on this path and the **Fibers** available on this path.
 - for the **Landmark** -> the **Paths** on which it is defined, the **OTUs** associated to this landmark and the **Connections and fibers** on which is defined this landmark.
 - for the **OTU** -> its associated links
- the third part displays the optical **Fiber route(s)** associated with the object.

Figure 318 ONMSi object details



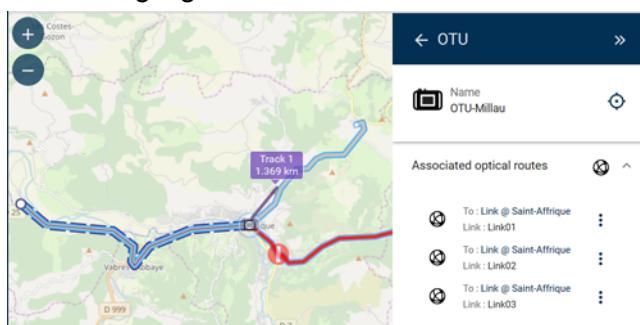
Dissociating a link

- From the **Fiber route** window, a link can be dissociate from the fiber route.
- The link can also be dissociated from the **Connection** window, from a connection side, if it is the link connector.

Highlighting an object

- Click on in **Connections and fibers** window to highlight a fiber or connection on the map.
- Click on in **Landmark** or **Paths** window to highlight a landmark or a path on the map.
- Click on and than on **Highlight** to highlight the optical route on the map (dotted line).

Figure 319 Optical route highlighted



Single Sign On (SSO) configuration

This chapter provides a description of the SSO configuration.

Topics discussed in this chapter include the following:

- “[Purpose](#)” on page 272
- “[Prerequisites](#)” on page 272
- “[Connection to Keycloak](#)” on page 272
- “[User fields extractors](#)” on page 273

Purpose

Optionally, ONMSi can be configured so that users are authenticated using Single Sign On (SSO) if your company has Keycloak set up (see <https://www.keycloak.org/>)

Prerequisites

- Your IT organization uses Keycloak and is willing to do some required changes, for instance to allow the ONMSi server URLs.
- SSO is an optional feature in ONMSi, so an adequate license must be obtained.
- The following configurations need to be performed

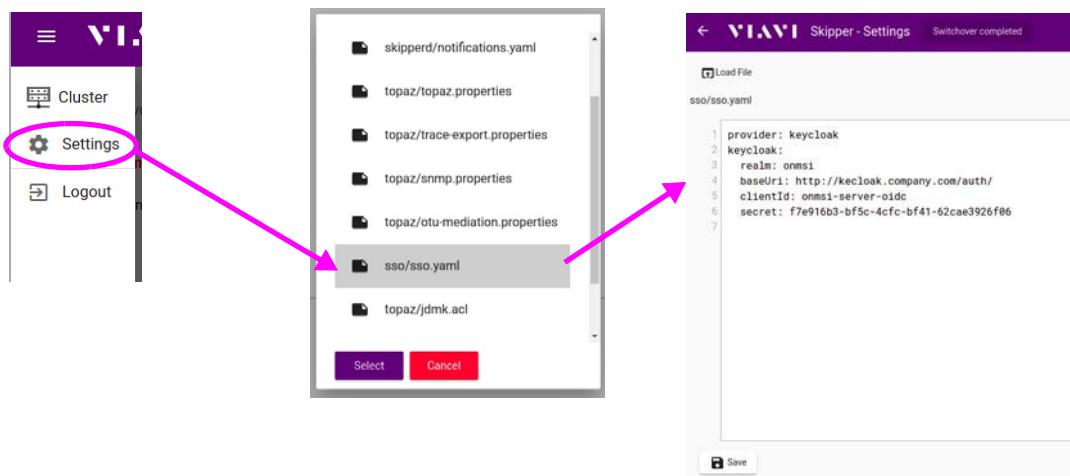
Connection to Keycloak

The connection from ONMSi to Keycloak is configured in a file, which can be edited from the Skipper UI (highly recommended because it includes a syntax checker) or using a text editor on the server.

If you opt for the text editor, the file is located on disk under `/opt/rfts_apps/conf/sso/sso.yaml`.

Otherwise, use Skipper to open the `sso/sso.yaml` file

Figure 320 Opening yaml file



Perform any required changed and save.

These settings are only read at ONMSi startup so any change here will require a fresh start of ONMSi, for instance using:

```
rfts_ctrl restart -c onmsi
```

Configuration of Keycloak is complex and outside of the scope of this user manual.

However, ONMSi interfaces to Keycloak using two clients:

- one for the regular web application and
- another for the field application

Here is a list of parameters supported in the sso.yaml file.

provider		string	"None" or "keycloak"
keycloak			
	realm	string	The realm of the SSO
	baseUri	string	The base URL of the keycloak server
	secret	string	The authentication secret
	clientId	string	The client ID for the regular web app
	fieldClientId	string	The client ID for the field web app
	localeAttribute	string	The name of the attribute specifying the locale to use
	defaultLocaleValue	string	The default locale to use in the event that the locale is not found in the JSON claims (only the language is used)
	maxClockSkewSeconds	integer	Maximum clock drift allowed between the ONMSi and the Keycloak servers.

User fields extractors

When interfacing with an LDAP or a Keycloak system, these authentication systems can provide information about the connected user, such as the username obviously, but also the full name, the e-mail address or the granted authorizations.

These granted authorizations should be configured as a profile (such as "General administrator" or "Expert in department 42", ...) that can be mapped to a user profile in ONMSi.

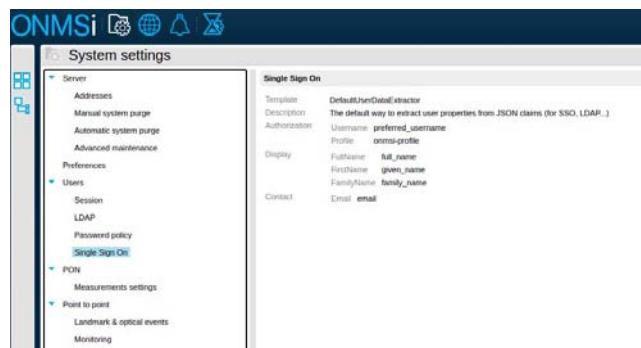
This mapping can be configured in the system settings of ONMSi (see figure below) and can even be customized using plugins.

By default, when interfacing with a Keycloak system, ONMSi will expect an attribute called "onmsi-profile" in the JSON claims returned by Keycloak.



The value of this attribute will be used as a user profile name any user who authenticates with Keycloak.

Figure 321 ONMSi Single Sign On





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 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 Soft-

ware 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 equity

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.

OTU Manager

This chapter provides a description of the OTU Manager

Topics discussed in this chapter are as follows:

- “[Introduction to OTU Manager](#)” on page 282
- “[Starting OTU Manager](#)” on page 282
- “[Using the OTU Manager](#)” on page 283
- “[Manager repository \(libraries\)](#)” on page 284
- “[Maintenance operations](#)” on page 286
- “[Support operations](#)” on page 288

Introduction to OTU Manager

The OTU Manager replaces legacy OTU toolkit. OTU Manager operations include:

- OTUs/FTHs maintenance operations:
 - Update the OTUs / FTHs firmware
 - Update the OTUs / FTHs licenses
 - Update the OTUs / FTHs SSH keys
 - List the OTUs / FTHs main information: versions, licenses...
- OTUs/FTHs advanced support operations:
 - Download the OTUs/FTHs logs
 - Reboot the OTUs / FTHs
 - Cleanup the OTUs / FTHs
 - Test the remote access to the OTUs / FTHs



NOTE

For legacy OTU 8000 and OTU 8000E with firmware before 7.22, please use legacy OTU Toolkit to upgrade them. To use OTU toolkit, replace “otu-manager” in browser URL by “otutk”.

Starting OTU Manager

- 1 From the system dashboard, click on **More**.
- 2 Click on **Manage OTUs using OTU Manager** menu.

Figure 1 Open OTU Manager



CAUTION

The user must have the **Manage OTUs** permission on at least one domain to access this menu.

Using the OTU Manager

The OTU manager is opened in a new tab of the browser. It displays the list of all the OTUs/FTHs visible in ONMSi by the logged user. To add manually a new OTU or FTH (not yet in ONMSi) click the button on bottom right.

On top banner, in the search field, you can search an OTU or FTH of the list, by its name or IP address.

Figure 2 OTU Manager

	OTU Name	Type	Version	Status
otu-8000e-cf	OTU 8000E	V18.86		
otu-8000e-sd	OTU 8000E	V18.86		
otu-8000e-10548	OTU 8000E	V18.88	SSH key not installed ⚠	

To display the OTU / FTH main information click on it in the list. To refresh OTU / FTH information, click on **Refresh** button.

Figure 3 OTU main information

Detail	Value
Last Refresh	Jul 21, 2020, 9:28:39 AM
Serial No	0002
Rescue	V18.79
Firmware	V18.86
Address	otu-8000e-cf
OTU Interface	http://otu-8000e-cf
Options	High sensitivity... Peak Monitoring... Rest API Smart Access ...

Remove an OTU or an FTH from OTU Manager (not from ONMSi):

From the OTU Manager window:

- 1 Select the OTU / FTH to be removed.
- 2 Click on **More** and click on **Remove OTU**.

Figure 4 Removing an OTU from OTU Manager



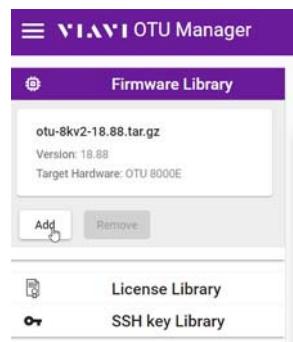
Manager repository (libraries)

Firmwares, licenses and SSH keys libraries to be applied on OTUs / FTHs are accessible on left panel.

Firmware library

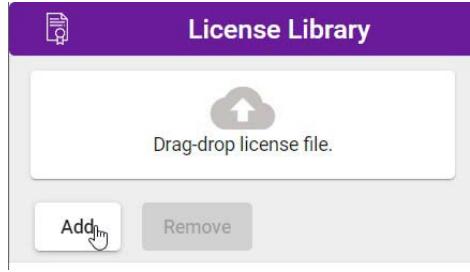
To add a new OTU/FTH firmware from your disk to the repository:

- 1 Click on “Add”.
- 2 Select the file to upload.
- 3 Wait for the upload starting



License library

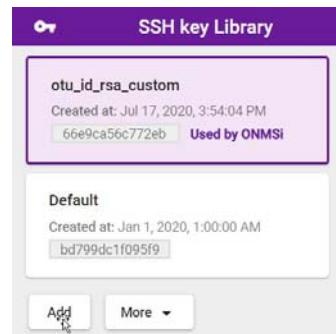
OTU/FTH requires licenses for advanced features (Enhanced_Security, Light_Source, High_Sensitivity...). Those OTU/FTH licenses are grouped in license files (one license file can contain licenses for several OTUs or FTHs) and can be uploaded to the license repository.



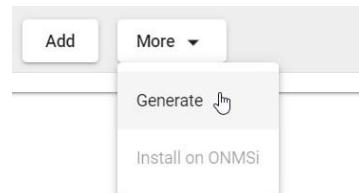
SSH Keys library

ONMSI uses SSH keys to communicate to OTUs/FTHs. Those SSH keys can be changed from OTU Manager:

- Either you can add your own custom key by clicking on "Add" button:



- Or a new key can be randomly generated:

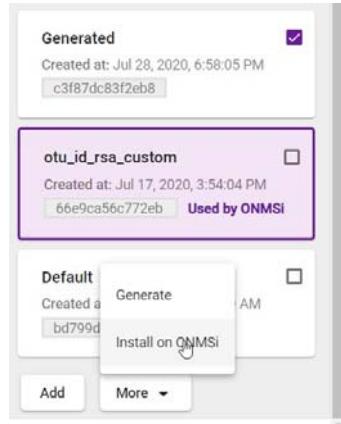


NOTE

Once the new key is generated, or once your own key is added, it must be installed on ONMSI and installed on all OTUs/FTHs (cf Update SSH keys).

To install the new key on ONMSI (that SSH key becomes the current key used by ONMSI), select the key and click on **Install on ONMSI**.

Figure 5 Install New generated ssh key on ONMSi



NOTE

OTUs and FTHs with a previous key will no longer be accessible by ONMSi until the key used by ONMSi is installed on them (cf Update SSH keys).

Maintenance operations

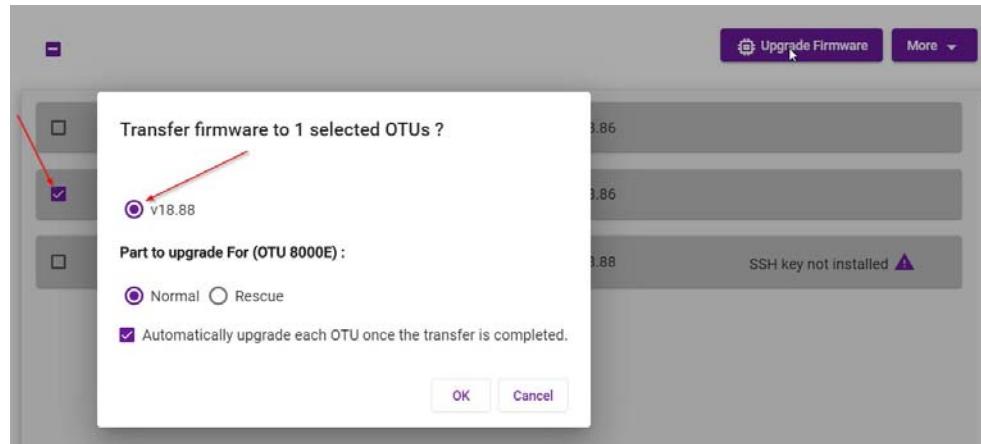
Firmware upgrade

OTU/FTH upgrade uses the OTU/FTH firmware versions available on the server, and visible in the firmware library (see “[Firmware library](#)”).

Upgrade process:

- 1 Select the OTUs / FTHs to upgrade on the list (check box), and click on “**Upgrade Firmware**” on upper right
- 2 Select the firmware version to use on the dialog box (only possible versions for the given OTU type are proposed)
- 3 Start the upgrade by clicking the “**OK**” button.

Figure 6 Upgrade OTU 8000E



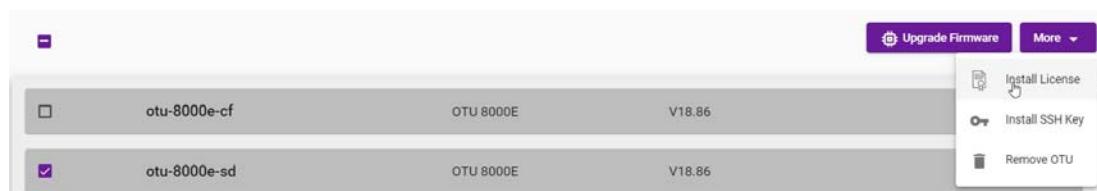
NOTE

For OTU 8000E, upgrade first the normal partition, then once done, upgrade the rescue partition.

License update

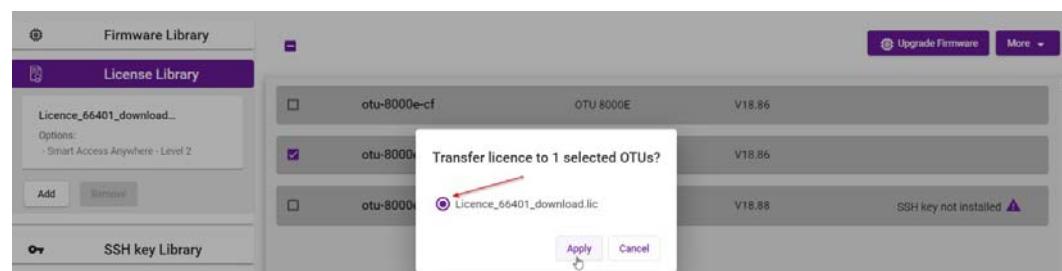
OTU/FTH uses licenses for advanced features; licenses must be uploaded first to the license library on the server (see “[Manager repository \(libraries\)](#)”) and then they can be applied to OTUs / FTHs.

Figure 7 Install License



Select the license file and apply it on OTU/FTH:

Figure 8 Apply selected License



SSH key update

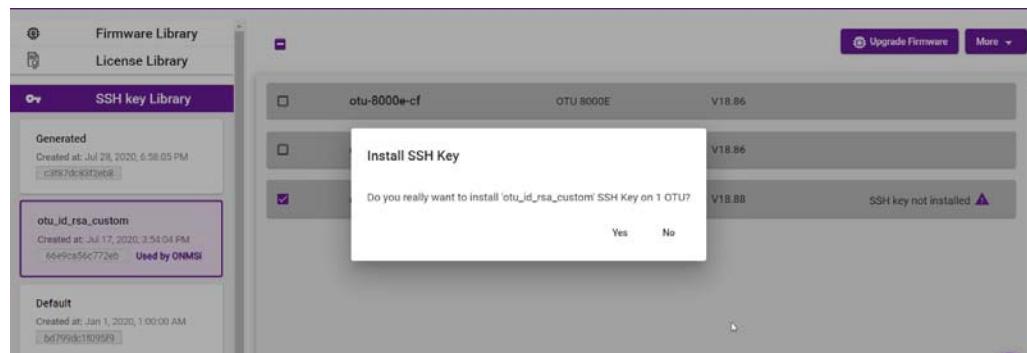
SSH key must be available on the "SSH key library" before being applied on OTUs/FTHs (see “[Firmware library](#)”).

Figure 9 Install new SSH key



Apply the current ssh key used by ONMSi on the OTU/FTH:

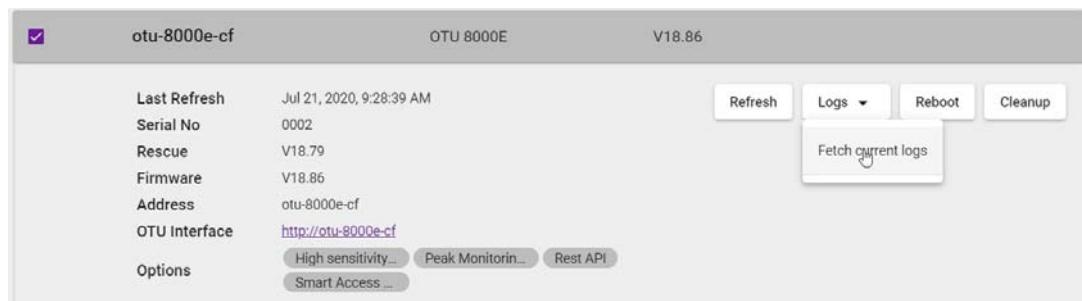
Figure 10 Apply current ssh key on OTU



Support operations

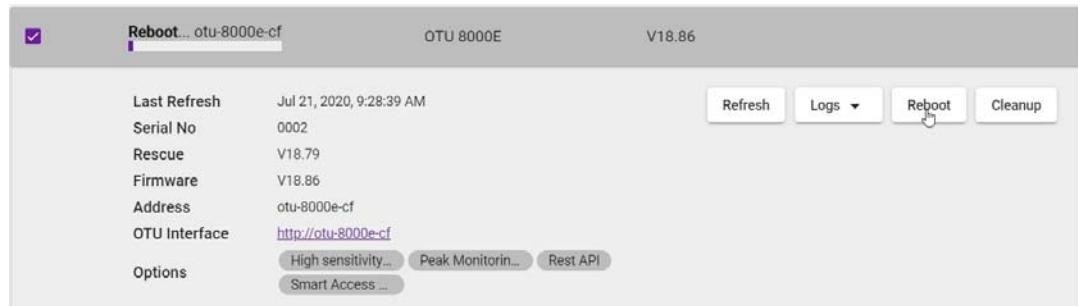
Download log files

Figure 11 Download logs



Reboot OTU / FTH

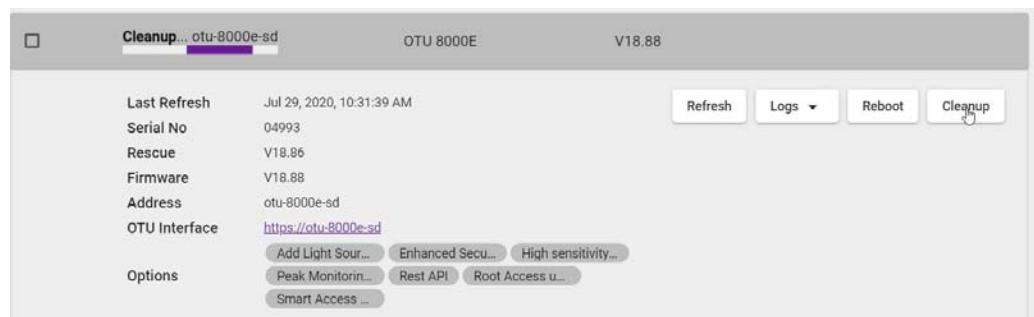
Figure 12 OTU Reboot



Cleanup OTU / FTH

This operation removes all alarms, monitoring tests.

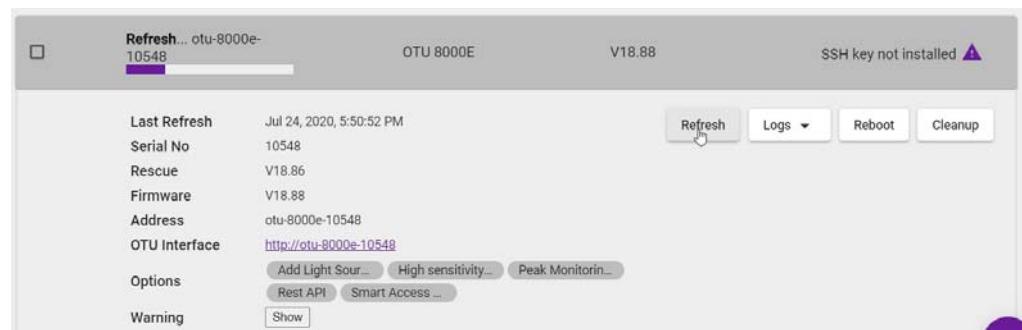
Figure 13 Cleanup OTU



Test the remote access to the OTUs / FTHs

Click on **Refresh** button. If an error occurs, a dialog explains the issue and detail is available with **Show** button.

Figure 14 Test Remote access



OTU Toolkit

This chapter provides a description of the OTU toolkit.

The OTU Toolkit is deprecated and has been replaced by the OTU Manager (see [Appendix B](#))

If for some reason, you still need to use it, it first needs to be installed on the system,
Please ask your system administrator to turn it on.

Once the OTU Toolkit is installed and runs properly, you need to edit the URL in your web browser to access it. Once connected to ONMSi, open another browser tab and add the following path to the URL: /otutk

This would lead to something like: `http://onmsi-server-name/otutk`

Topics discussed in this chapter are as follows:

- “[Introduction to OTU toolkit](#)” on page 292
- “[Using the OTU Toolkit](#)” on page 293
- “[Downloading the logs files for an OTU](#)” on page 294
- “[Rebooting OTUs](#)” on page 294
- “[Updating the OTU firmware](#)” on page 294
- “[Cleaning OTUs](#)” on page 296
- “[Checking the OTU hard disk](#)” on page 296
- “[Testing the OTU network access](#)” on page 296
- “[Uploading a license on the OTU](#)” on page 297
- “[Applying a software patch on the OTU](#)” on page 297

Introduction to OTU toolkit

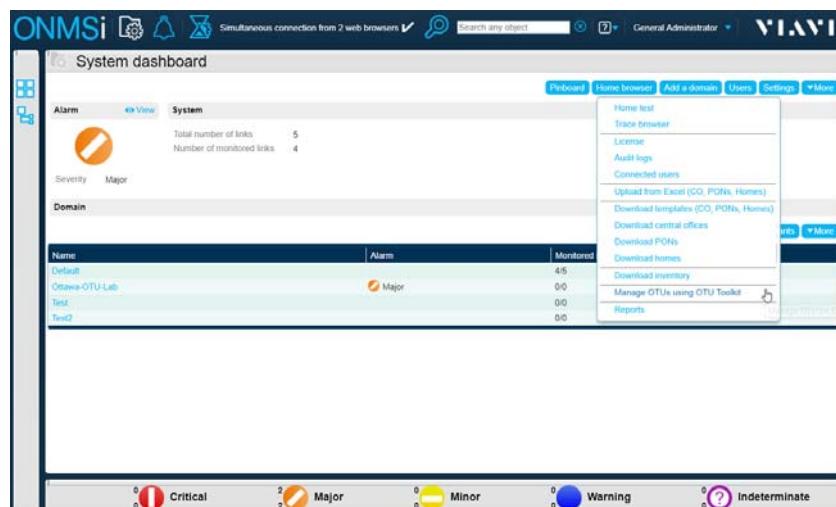
The OTU toolkit allows to perform OTUs operations like:

- Display the OTU(s) versions
- Reboot the OTU(s)
- Update the OTUs firmware
- Download the OTU(s) logs
- Test the remote access to the OTU(s)
- Test the OTU(s) hard disk.

To open the OTU toolkit:

- 1 From the system dashboard, click on **More**
- 2 Click on **Manage OTUs using OTU toolkit** menu.

Figure 15 Open OTU Toolkit



OTU Manager is opened in a new tab, to access OTU Toolkit replace "otu-manager" in the web browser url by "otutk".



CAUTION

The user must have the **Manage OTUs** permission on at least one domain to access this menu.

Using the OTU Toolkit

The OTU toolkit is opened in the browser in a new tab. It displays the list of OTUs visible in ONMSi by the logged user.

Figure 16 List of visible OTUs

OTU details								Firmware				
Operation	Name	Address	Serial number	Hardware type	Version	Run mode	Boot	Otu	Rescue	Tar(s)	Licenses	Last refresh
<input type="checkbox"/> success	otu-8000e-cf.ds.jdsu.net	otu-8000e-cf.ds.jdsu.net	2	OTU 8000E	7.27	normal	8.71	7.27	7.27	otu-8kv2-7.27qui.tar.gz		Mon Jan 28 16:33:43 CET 2019
<input type="checkbox"/> success	otu-5000-00006	otu-5000-00006	EBAJ0000666	OTU 5000	17.06	normal	10.28	17.10	17.10	otu-5000-17.10.tar		Mon Jan 28 16:34:00 CET 2019
<input type="checkbox"/>	otu-8000e-7467	10.14.152.133	?	?	?							

The data displayed in the **OTU details** columns are coming from ONMSi.

To reload the list of OTUs:

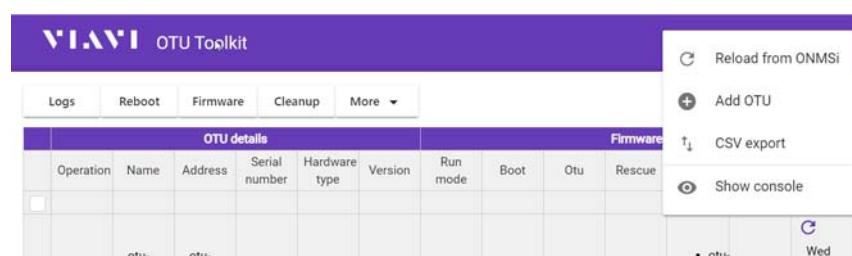
- 1 In the menu
- 2 Click on **Reload from ONMSi**

To add manually a new OTU (not coming from ONMSi)

- 1 In the menu
- 2 Click on **Add OTU**.

A popup dialog is displayed to enter the new OTU address.

Figure 17 Reload the OTUs List / Add an OTU



The data displayed in the **Firmware** columns need to be retrieved from the OTUs.

To refresh data for **one** OTU:

- 1 Select the OTU, you want to query
- 2 Press the refresh button

To refresh data for **all** OTUs:

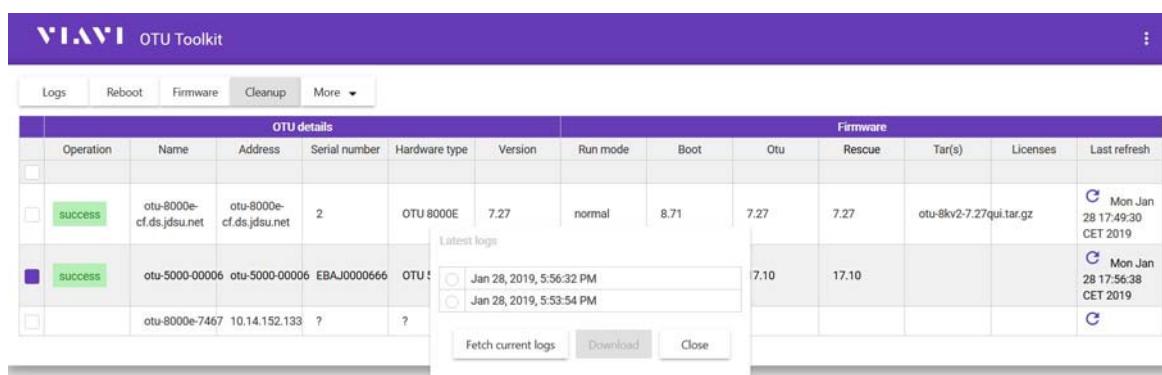
- 1 Open the **More** menu
- 2 Click on the **Refresh** menu

Downloading the logs files for an OTU

From the list of OTUs:

- 1 Select one OTU
- 2 Click on **Logs**
A popup window displays the list of the latest logs available on the server (maximum 5 logs).
- 3 To retrieve a new logs file from the OTU:
 - a Click on the **Fetch current logs** button.
- 4 To download a logs file:
 - a Select a logs file.
 - b Then click on the **Download** button.

Figure 18 Downloading log files



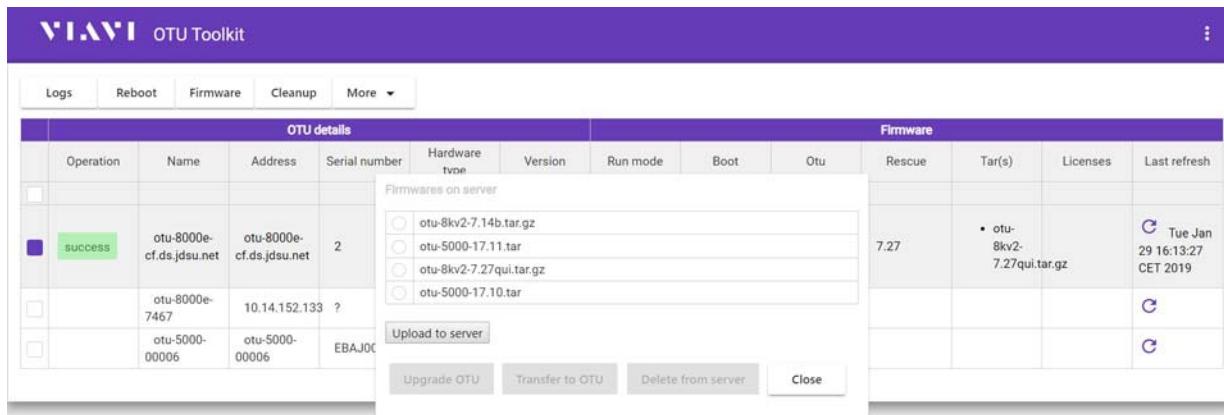
Rebooting OTUs

- 1 Select one or more OTUs
- 2 Click on **Reboot**.
A confirmation dialog box is displayed
- 3 Click on **OK** to reboot the OTU(s)

Updating the OTU firmware

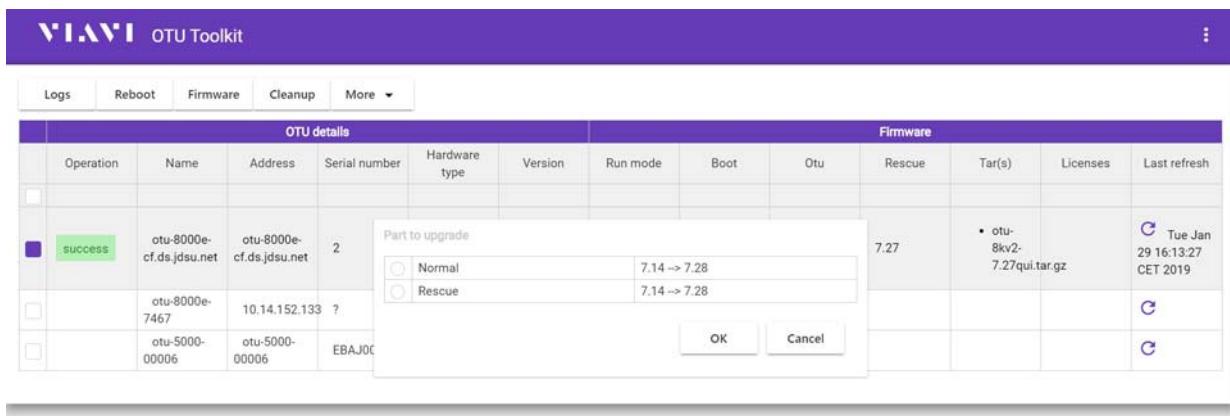
- 1 Select one or more OTUs
- 2 Click on **Firmware**
A popup window displays the list of the latest OTU firmwares available on the server.

Figure 19 Firmwares list



- 3 If the firmware is not yet available on the server, the user can click on **Upload to server** button to upload a new firmware to the server.
- 4 The user can select one firmware in the list and:
 - a Click on the **Upgrade OTU** button to upgrade the selected OTUs with the selected firmware.
 - i A new dialog box shows the current and new firmware versions
 - ii Select the firmware to be updated and click on the **OK** button to launch the upgrade

Figure 20 Select the firmware to be updated



If the firmware is not on the OTU, it is first transferred to the OTU before the upgrade.

- b Click on the **Transfer to OTU** button to transfer the firmware to the selected OTUs
- c Click on the **Delete from Server** button to delete the selected firmware from the Server.

Cleaning OTUs

- 1 Select one or more OTUs
- 2 Click on **Cleanup**.
- 3 A confirmation dialog box is displayed
- 4 Click on **OK** to cleanup the OTU(s)

Checking the OTU hard disk

From the list of OTUs:

- 1 Select one OTU.
- 2 Click on the **More** menu and then on the **Check hard disk** menu.

At the end of the test, in the operation column, it displays **success** if the hard disk is working fine and **failure** in case of problem.

Figure 21 OTU hard disk checked

OTU details												Firmware		
Operation	Name	Address	Serial number	Hardware type	Version	Run mode	Boot	Otu	Rescue	Tar(s)	Licenses	Last refresh		
<input type="checkbox"/>	success	otu-8000e-cf.ds.jdsu.net	otu-8000e-cf.ds.jdsu.net	2	OTU 8000E	7.27	normal	8.71	7.27	7.27	• otu-8kv2-7.27qui.tar.gz			Tue Jan 29 18:25:08 CET 2019
<input type="checkbox"/>	otu-8000e-7467	10.14.152.133	?	?	?									
<input type="checkbox"/>	otu-5000-00006	otu-5000-00006	EBAJ0000666	OTU 5000	17.06									

Testing the OTU network access

From the list of OTUs:

- 1 Select one OTU
- 2 Click on the **More** menu and then on the **Check Network** menu.

At the end of the test a report displays the test results.

Figure 22 Network Test results

OTU details										Firmware					
Operation	Name	Address	Serial number	Hardware type	Version	Run mode	Boot	Otu	Rescue	Tar(s)	Licenses	Last refresh			
success	otu-8000e-cf.ds.jdsu.net	otu-8000e-cf.ds.jdsu.net	2	OTU 8000E	7.27	normal	8.71	7.27	7.27			Tue Jan 29 18:23:03 CET 2019			
Check network result															
Name	Address	Serial number	SSH port opened	SSH accessstatus	HTTP port opened	HTTP access status	Small sync bw up	Small sync bw down	Small checksum status	Big sync bw up	Big sync bw down	Big checksum status			
otu-8000e-cf.ds.jdsu.net	otu-8000e-cf.ds.jdsu.net	2	true	true	true		5.34Mb/s	16.00Mb/s	true	32.00Mb/s	22.86Mb/s	true			

Uploading a license on the OTU

- 1 Select one or more OTUs.
- 2 Click on **Licensing**
A popup window displays the list of available licenses on the server.
- 3 Click on **Upload license** button to upload a new license to the server.
- 4 Select on license in the list and click on **Apply**.

Applying a software patch on the OTU

- 1 Select one or more OTUs
- 2 Click on **Patches**
A popup window displays the list of available patches on the server.
- 3 Click on **Upload patch** button to upload a new patch to the server.
- 4 Select on patch in the list and click on **Apply**.

Index

A

About ONMSI 11
Account lockout 174
Action list 10
Add Trace 51
Additional attributes 191
Alarm 184
 acknowledge 99, 102
 attenuation 79
 clean 100
 clear 102
 delete 101
 details 98, 99
 download pdf 100
 history 101
 ID 44, 100
 list 98
 pdf 100
 peak 82
 purge 168
 section 93
 severity 99
 table 102, 103
 viewer 12, 98
Attenuation 27, 48, 78, 79
Audit log 168
Authentication 56, 58, 59, 62, 171, 174
Automatic fail-over 16

B

Backup server 16
Both end measurement 85
Budget
 data download 74
 graph 29
 time slot 86

C

Connection test 19
Contact details 64
Contextual help 11, 13

D

Dashboard 46
 system 8
Desktop Alert
 disable 108
Desktop alert 65, 105
 configure 106
 display 107
 installation 105
 profile 187
 remove 108
Domain
 add 68
 copy a link 71
 delete otu 71
 remove otu 70
Domain role 60, 61
Download 112
 alarm 100
 alarm table 104
E-mail 57, 64, 105, 184, 185, 186
 formatting 186
Escalation 184
Events table 49, 50
Excel 7, 64, 74, 104, 112, 114, 116, 190
 landmarks table 89

F

Fail-over 16
Fiber Length extension 80
Filters 46, 51, 102, 185
 audit log 7
 e-mail 185
First Marker (FM) 26, 47
Formatting 186

G

Geographical file 93

H

History 101

I

Inventory report 113

IP Address

 OTU 18

IP address 7, 16, 171

 server 6

K

KLM 93

L

LAN 16

Landmarks 86–92

 association 91
 force association 91

Last Marker (LM) 26, 47

LDAP 58–59, 170–171

 Manager 171

M

Main server 16

Manual fail-over 16

Marker A & B 47

N

Notification 56, 64, 104, 106, 174, 185

Notifications 57

O

Online help 11

Optical events 48

 landmarks 90

OTDR 2, 76, 82, 93, 101
 reference trace 27

OTU 70

 add 18–19

 connection test 19

 delete from domain 71

 ping test 19

 recall test 19

 remove from domain 70

 run test 18

 test connection 18

P

Password 6

 expiration 174
 history 174
 policy 172
 quality 172
 user 56, 63

PDF 7, 100, 104, 112, 187, 190

Peak 81–82

Ping test 19

Ports association 24, 25

Purge 168

R

Rebuild (OTU) 19

Recall test 19

Refresh

 config. (OTU) 19

Report

 create 114
 excel 116
 execute 115

Ringtone 107

S

Scale factor (Landmarks) 92

Section 12

Server

 address 15–16, 107
 backup & main 16
 IP address 6
 LDAP 171
 name 6

Severity 99

Slacks (Landmarks) 92

Splitting section (Landmarks) 92

Sub-domains 69

Synchronization 86–??

System dashboard 68

System role 60–61

T

Table

 configuration 112
 download 112
 events 50
 landmarks 87–90

Test

 connection 18
 on demand 78
 purge 168
 schedule 75
 stop 76

Time slot 86

Trace

 add 51

color [50](#)
multi- [51](#)

Trace Browser [46](#)

Trace viewer [46](#)

U

User
add [56](#)
alerts [57](#)
API [172](#)
connected [65](#)
contact details [56](#)
details [56](#)
disconnect a [66](#)
domain [60](#)
domain role [62](#)
LDAP [58–59](#), [170–171](#)
password [6](#), [63](#)
preferences [11](#)
session duration [170](#)
system [60](#)
system role [62](#)

Z

Zoom [27](#), [47](#)



70ONMSI10
Rev. 016, June 2025
English



VIAVI Solutions

North America:	1.844.GO VIAVI / 1.844.468.4284
Latin America	+52 55 5543 6644
EMEA	+49 7121 862273
APAC	+1 512 201 6534
All Other Regions:	viavisolutions.com/contacts
email	TAC@viavisolutions.com
address	6001 America Center Drive, San Jose, CA, 95002, USA