

FG-750

Fiber Guardian



Copyright © 2012–2019 EXFO Inc. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form, be it electronically, mechanically, or by any other means such as photocopying, recording or otherwise, without the prior written permission of EXFO Inc. (EXFO).

Information provided by EXFO is believed to be accurate and reliable. However, no responsibility is assumed by EXFO for its use nor for any infringements of patents or other rights of third parties that may result from its use. No license is granted by implication or otherwise under any patent rights of EXFO.

EXFO's Commerce And Government Entities (CAGE) code under the North Atlantic Treaty Organization (NATO) is 0L8C3.

The information contained in this publication is subject to change without notice.

Trademarks

EXFO's trademarks have been identified as such. However, the presence or absence of such identification does not affect the legal status of any trademark.

Units of Measurement

Units of measurement in this publication conform to SI standards and practices.

Patents

This product incorporates the proprietary EXFO Link-Aware™ technology, employing spectrally-selective high-reflectance demarcation (HRD) filters to enable the attenuation of a specific branch of a P2MP (point-to-multipoint) network to be measured/monitored.

Feature(s) of this product is/are protected by one or more of: US patent 8,687,957 and equivalent patents pending and/or granted in other countries; US patent 8,576,389 and equivalent patents pending and/or granted in other countries; US patents 9,170,173; 9,571,186; 10,014,935; and 9,423,316.

Version number: 7.0.0.1

Microsoft End-User License Agreement

You have acquired a device ("DEVICE") that includes software licensed by EXFO Inc. (EXFO) from an affiliate of Microsoft Corporation ("MS"). Those installed software products of MS origin, as well as associated media, printed materials, and "online" or electronic documentation ("SOFTWARE") are protected by international intellectual property laws and treaties. Manufacturer, MS and its suppliers (including Microsoft Corporation) own the title, copyright, and other intellectual property rights in the SOFTWARE. The SOFTWARE is licensed, not sold. All rights reserved. The Microsoft EULA for the SOFTWARE can be found at: <https://www.microsoft.com/en-us/userterms>, by entering "Windows" as the Product Name, and "8" as the Version Number.

This EULA is valid and grants the end-user rights ONLY if the SOFTWARE is genuine and a genuine Certificate of Authenticity for the SOFTWARE is included. For more information on identifying whether your software is genuine, please see <https://www.microsoft.com/en-us/howtotell/default.aspx>.

IF YOU DO NOT AGREE TO THIS END USER LICENSE AGREEMENT ("EULA"), DO NOT USE THE DEVICE OR COPY THE SOFTWARE. INSTEAD, PROMPTLY CONTACT EXFO FOR INSTRUCTIONS ON RETURN OF THE UNUSED DEVICE(S) FOR A REFUND. ANY USE OF THE SOFTWARE, INCLUDING BUT NOT LIMITED TO USE ON THE DEVICE, WILL CONSTITUTE YOUR AGREEMENT TO THIS EULA (OR RATIFICATION OF ANY PREVIOUS CONSENT).

Software License Agreement (V.2016-02)

This Software License Agreement ("Agreement") shall apply to any Customer and its Users, for all its request for quotations and purchase orders, EXFO order acknowledgements and invoices and any delivery of Software by EXFO, for which there is no separate license agreement between you and the manufacturer or owner of the software, together with EXFO's Sales Terms and Conditions, available at <https://www.exfo.com/umbraco/surface/file/download/?ni=122228&cn=en-US> or on request, which are an integral part of this Agreement.

IMPORTANT: BY ORDERING, INSTALLING, DOWNLOADING, OR USING THE SOFTWARE OR OTHERWISE PROCEEDING WITH ANY TRANSACTION AFTER RECEIPT OF THE AGREEMENT, OR BY CLICKING ON THE ACCEPT BUTTON OR SIMILAR BUTTON, YOU, AS THE INDIVIDUAL OR SINGLE ENTITY ACQUIRING THE SOFTWARE (THE "CUSTOMER"), OR AS THE USER (AS HEREINAFTER DEFINED) SIGNIFY THAT YOU HAVE READ AND ACCEPTED THE TERMS AND CONDITIONS OF THIS AGREEMENT AS OF THE DATE ON WHICH YOU FIRST ORDER THE SOFTWARE, INSTALL, DOWNLOAD, USE OR CLICK THE ACCEPT BUTTON (THE "EFFECTIVE DATE"). IF YOU DO NOT ACCEPT THIS AGREEMENT, YOU SHOULD NOT ORDER, INSTALL, DOWNLOAD, NOR USE THE SOFTWARE AND CONTACT EXFO FOR A REFUND, IF APPLICABLE.

Terms and Conditions

1. DEFINITIONS

1.1 "Documentation" means EXFO's online or electronic information manual or other printed materials that (i) contain operating instructions and performance specifications for the Software and; (ii) EXFO delivers with the Software; and (iii) EXFO generally makes available to all users of its Software.

1.2 "Open Source Software" means individual software components that are provided with the Software, for which the source code is made generally available, and that are licensed under the terms of various published open source software license agreements or copyright notices accompanying such software components which include without limitation any software licenses approved as open source licenses by the Open Source Initiative or any substantially similar licenses.

1.3 "Product" means any hardware product developed by or on behalf of EXFO designed for use with the Software, as the case may be.

1.4 "Software" means the software programs and software components in object code, source code or other format and all modifications, updates, upgrades and enhancements that EXFO agrees to deliver or make available to Customer from time to time.

1.5 "Third Party" means any individual, corporation, partnership, association or other entity, other than the parties to this Agreement.

1.6 "Third Party Software" means the software programs distributed by EXFO as part of the Software which have been developed by Third Parties or their licensors and may include Open Source Software.

1.7 "Users" means Customer's officers, employees, and independent agents and contractors, who are bound by enforceable obligations to use the Software only on behalf of the Customer and only in accordance with this Agreement.

2. PROPRIETARY RIGHTS

2.1 The Customer acquiring a license to the Software is granted only those rights expressly conferred by the license grant set forth in Section 3 of this Agreement. The Software is licensed, not sold. Title to the Software and the Documentation shall not be passed to Customer, Users or to any other party. EXFO shall retain ownership of all rights, titles and interests, in and to the intellectual property rights related to the Software and the Documentation, including but not limited to, patent, trademark, copyrights, trade names, trade secrets, other similar rights, and intellectual property rights that could result from any alterations, attachments and improvements made by either party. Title in the Third Party Software or the Open Source Software remains with the Third Party licensors, as applicable. Customer and Users shall not, remove or modify any Software and Documentation markings or any notices of EXFO's or its Third Party licensors' proprietary rights.

3. LICENSE GRANT

3.1 License Grant. Subject to the terms and conditions of this Agreement, EXFO grants to Customer a personal, non-sublicensable, non-transferable and non-exclusive license to have Users install and use the Software in accordance with the Documentation and solely within Customer's own personal or business operations, as the case may be. EXFO's license grant is conditioned on Customer continuous compliance with all limitations and license restrictions described herein and in the Documentation and if Customer violates any of these limitations and restrictions or any other terms of this Agreement, the license grant will automatically and immediately terminate without notice from EXFO. Any usage of the Software outside one of the following scopes constitutes an infringement of EXFO's and/or its Third Party licensor's intellectual property and/or proprietary rights as well as a material breach of this Agreement.

3.1.1 Standard. The license grant of section 3.1 is granted solely to install the Software on either (i) one (1) EXFO designated Product; (ii) one (1) stand-alone computer; or (iii) one (1) mobile device, neither of which may be connected to a network in a manner that allows more than one (1) User to upload, access, run or generally use the Software concurrently.

3.1.2 Simulator Multi-User. In the case of Simulator Products, the license grant of section 3.1 is granted solely to use the Software in connection with one (1) EXFO designated Simulator Product and multiple Users may upload, access, run or generally use the Software concurrently subject to the hardware capabilities of the Simulator Product purchased by the Customer. Notwithstanding anything to the contrary herein, Users may customize or modify the Software standard package to meet Customer's specific needs as allowed by the script environment.

3.1.3 Server Access. For any Software that allows or grants access to a server, the license grant of section 3.1 is granted solely for the purpose of accessing the server that enables administration of User accounts and performs services as specified in the Documentation, such as data storage. Customer shall use the Software only with one (1) stand-alone Product or supported device within a server-configured time period or server access enablement, and shall be responsible for the administration of the User accounts and the Users' use of the Software. The Users may use the Software on behalf of the Customer for Customer's business activities as described in section 3.1 above, subject to the terms of this Agreement. The Customer shall purchase a license or subscription, as the case may be, for each User accessing the server. EXFO reserves the right to discontinue Server Access to Customer and its Users upon non-payment of appropriate and associated maintenance or subscription fees. Unless otherwise agreed in writing, the license grant for Server Access is limited to a period of 1 year from the date of purchase.

3.1.4 Service Assurance Licensed Hardware. In the case of Service Assurance Products, the license grant of section 3.1 is granted solely to use the EXFOWorx system (including where applicable other Service Assurance applications) in connection with the maximum number of verifier agents purchased by the Customer and identified by a verifier key provided by EXFO.

3.2 Copies. Unless otherwise agreed in writing, Customer may, when applicable with the type of Software, only make one (1) copy of the Software for backup and disaster recovery purposes provided that any copy or portion thereof must bear the same proprietary and/or copyright notices contained in or on the original copy.

4. LICENSE RESTRICTIONS

4.1 No right is granted (i) for the use of the Software for or in the interest of any Third Party, including, but not limited to, use for timesharing, service bureau, subscription service, hosting, outsourcing or other similar services; or (ii) to sell, transfer, export, license or sublicense any of the Software.

4.2 Customer shall not translate or create any derivative works based on the Software or Documentation or reverse engineer, decompile, disassemble or decode in whole or in part the Software or the Product or derive any source code or algorithms from the Software nor modify or alter the Software, the Product or the Documentation in any other manner whatsoever.

4.3 Customer shall not copy or use the Software or Documentation for any purpose or in any manner not expressly permitted in this Agreement.

4.4 Customer shall not remove or modify any program markings or any notice of EXFO's or its Third Party licensors' proprietary rights.

4.5 The validity of this Agreement is subject to the payment of all applicable license or maintenance fees by Customer to EXFO as the case may be and as indicated in the applicable EXFO invoice, if any.

4.6 The Third Party Software provided to Customer is distributed under the terms of the license agreements associated with that Third Party Software. Copies of these terms are included in the Documentation otherwise this Agreement shall govern the use of any Third Party Software by Customer. EXFO may designate any Third Party licensors as a third party beneficiary of this Agreement (the "Third Party Beneficiary") solely with regards to the distribution of such Third Party Software but this Agreement shall not be enforceable by the Third Party Beneficiary without a prior written agreement duly executed with EXFO. NOTWITHSTANDING ANYTHING ELSE TO THE CONTRARY IN THIS AGREEMENT, EXFO EXPRESSLY DISCLAIMS ANY WARRANTY, RESPONSIBILITY OR LIABILITY WITH REGARD TO THE THIRD PARTY SOFTWARE, INCLUDING THE DOWNLOADING AND INSTALLATION, IF APPLICABLE.

4.7 Software may contain Open Source Software. Open Source Software is composed of a variety of individual software components, each of which has its own copyright and its own applicable license conditions. Customer must review the licenses within the individual packages to understand its rights under them. The licenses can be found in each Software and/or the Documentation. NOTWITHSTANDING ANYTHING ELSE TO THE CONTRARY IN THIS AGREEMENT, EXFO EXPRESSLY DISCLAIMS ANY WARRANTY, RESPONSIBILITY OR LIABILITY WITH REGARD TO OPEN SOURCE SOFTWARE.

4.8 The Software may use Google Analytics, an analytics service provided by Google, Inc. ("Google") or any other similar analytics services. Anonymous information may be collected about Customer's use of the Software and such information will be transmitted to and stored on Google or third party servers. This information will be used for the purpose of compiling reports on the Software's activity. This information may also be transferred to other parties where required to do so by law, or where such parties process the information collected by the analytics services.

5. RESERVED RIGHTS

5.1 Title in the Software remains with EXFO. Title in the Third Party Software and Open Source Software remains with the Third Party providers.

5.2 EXFO reserves any rights not expressly granted in Section 3 and nothing in this Agreement constitutes a waiver of EXFO's rights under copyright laws or any other federal or state law or treaty. Without limiting the foregoing, EXFO reserves the right to license the Software to others on such terms as EXFO may establish in its sole discretion.

5.3 EXFO reserves the right, in any way and without notice, to revise, not to revise, update or modify the Software, or the information upon which the Software was based. Except as otherwise expressly set forth in this Agreement, EXFO assumes no responsibility, for (i) protecting the Software against obsolescence; (ii) providing any improvements to the Software; (iii) maintaining the Software; or (iv) providing other services with respect to the Software.

6. COOKIE AND PRIVACY POLICY

If the use of the Software allows connection to an EXFO Server, Customer and Users consent to EXFO's collection, use and disclosure of information associated with the Software solely in accordance with EXFO's Cookie and Privacy Policy, currently available at <https://www.exfo.com/en/user-privacy-notice/>, as it may be updated by EXFO from time to time.

7. AUDIT

When applicable, EXFO reserves its right to verify, upon reasonable notice, Customer's use of the Software in compliance with the terms of this Agreement and audit all books and financial records related to such use. Customer agrees to pay within 30 days of written notification any underpaid fees. If the Customer does not pay, EXFO can end Customer's support, licenses and this Agreement. EXFO shall have the right to disclose the result of such audit to its Third Party Software licensors to the extent that such audit results in findings concerning such Third Party Software licensor.

8. SUPPORT

EXFO shall only provide support for the Software to the extent set forth in a separate maintenance agreement or support program, if any, between EXFO and Customer.

9. CONFIDENTIAL INFORMATION

9.1 Customer shall hold the Software and the Documentation in strict confidence for the benefit of EXFO as confidential information.

9.2 Customer shall not make any disclosure of the Software (including methods or concepts utilized in the Software) to anyone other than its Users who have a need to know provided that Customer shall be responsible for the use of the Software by its Users. Customer shall notify its Users of their confidentiality obligations with respect to the Software and the Documentation and shall require its Users to comply with these obligations. The confidentiality obligations of Customer and its Users shall survive the termination of Customer's licenses and rights granted under this Agreement.

9.3 Customer shall not disclose results of any Software or Product benchmark tests without EXFO's prior written consent.

9.4 EXFO shall have the right to disclose, without Customer's consent, the terms of this Agreement to EXFO's Third Party Software licensors.

10. LIMITED WARRANTY AND EXCLUSIVE REMEDY

EXFO warrants that for a period of sixty (60) days from the date of delivery ("Warranty Period"), that the Software will operate and perform materially in conformance with the Documentation. If a breach of the warranty set forth in this Section 10 occurs, Customer's sole and exclusive remedy is that EXFO will provide reasonable efforts to correct non-conformances which are reproducible by EXFO during the Warranty Period. If the use of the Software allows connection to an EXFO Server, during any subscription term, EXFO will use commercially reasonable efforts to make the EXFO server generally available except for planned downtime or downtime caused by circumstances beyond EXFO's reasonable control.

11. DISCLAIMER

EXFO makes no representations and extends no warranties of any kind (other than those set forth in Section 10) with respect to (i) the use, sufficiency or accuracy of the Software; (ii) the sufficiency or accuracy of the reports or tests performed utilizing the Software; (iii) any Third Party Software and Open Source Software; (iv) any Third Party websites or links (including hyperlinks) thereto; or (v) the availability of the Software, the EXFO server or that the Software or the EXFO server performance will perform error-free and uninterrupted. TO THE EXTENT PERMITTED BY APPLICABLE LAW, THE FOREGOING WARRANTIES ARE IN LIEU OF ALL OTHER WARRANTIES, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE (EVEN IF EXFO KNOWS OR HAS BEEN MADE AWARE OF SUCH PURPOSE), AND THE WARRANTY AGAINST INFRINGEMENT OF PATENTS OR OTHER INTELLECTUAL PROPERTY RIGHTS. THE SOFTWARE IS NOT FAULT-TOLERANT AND IS NOT DESIGNED, MANUFACTURED, OR INTENDED FOR USE IN HAZARDOUS ENVIRONMENTS THAT REQUIRE FAILS-SAFE PERFORMANCE SUCH AS IN THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATIONS SYSTEMS, AIR TRAFFIC CONTROL, EMERGENCY RESPONSE, TERRORISM PREVENTION OR RESPONSE, LIFE SUPPORT OR WEAPONS SYSTEMS ("HIGH RISK ACTIVITIES") THE FAILURE OF WHICH COULD LEAD TO DEATH, PERSONAL INJURY, OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE. EXFO EXPRESSLY DISCLAIMS ANY WARRANTY OF FITNESS FOR HIGH RISKS ACTIVITIES.

12. LIMITATION OF LIABILITY

EXFO IS NOT LIABLE FOR ANY INDIRECT DAMAGES, LOST PROFITS, INCIDENTAL OR CONSEQUENTIAL DAMAGES, ARISING OUT OF THIS AGREEMENT OR THE FURNISHING OF THE SOFTWARE OR THIRD PARTY SOFTWARE, WEBSITES OR LINKS (INCLUDING HYPERLINKS) THERETO, INCLUDING THE USE OR INABILITY TO USE THE SOFTWARE OR THE THIRD PARTY SOFTWARE, WEBSITES OR LINKS (INCLUDING HYPERLINKS) THERETO, EVEN IF EXFO KNOWS OR HAS BEEN MADE AWARE OF THE POSSIBILITY OR LIKELIHOOD OF SUCH DAMAGES. EXFO IS NOT RESPONSIBLE FOR ANY COMPENSATION, REIMBURSEMENT, OR DAMAGES ARISING IN CONNECTION WITH: USERS INABILITY TO USE THE SOFTWARE AS A RESULT OF ANY UNANTICIPATED OR UNSCHEDULED DOWNTIME OF ALL OR A PORTION OF THE EXFO SERVER FOR ANY REASON, INCLUDING AS A RESULT OF POWER OUTAGES, SYSTEM FAILURES OR OTHER INTERRUPTIONS. EXFO'S LIABILITY UNDER THIS AGREEMENT, IF ANY, IS LIMITED TO I) THE ANNUAL LICENSE FEES FOR SUBSCRIPTION LICENSE OR (II) THE TOTAL LICENSE FEES ACTUALLY RECEIVED BY EXFO FOR THE SOFTWARE. IF ANY REMEDY HEREUNDER IS DETERMINED TO HAVE FAILED OF ITS ESSENTIAL PURPOSE, ALL LIMITATIONS OF LIABILITY, DISCLAIMERS AND EXCLUSIONS OF WARRANTY AND DAMAGES SET FORTH IN THIS AGREEMENT SHALL REMAIN IN EFFECT.

13. TERM AND TERMINATION

13.1 The term of this Agreement will commence on the Effective Date and will remain in effect until expiration of Customer's subscription licenses, if applicable, or until termination in accordance with Section 13.2.

13.2 This Agreement and the license and rights granted to Customer under this Agreement will automatically terminate without notice to Customer if (i) Customer assigns the license for the benefit of creditors; (ii) Customer admits in writing its inability to pay debts as they mature; (iii) a trustee or receiver is appointed for a substantial part of Customer's assets; (iv) a bankruptcy proceeding is instituted against Customer which is acquiesced in and is not dismissed within sixty (60) days, or results in an adjudication of bankruptcy; or (v) Customer breaches the license granted in Section 3 or breaches any of the restrictions of Section 4.

13.3 Without prejudice to any other rights, EXFO may terminate this Agreement if Customer fails to comply with any term or condition of this Agreement.

13.4 Upon termination of this Agreement, Customer shall return the Software and the Documentation, including all copies and, if requested, certify in writing to EXFO the return. Customer is bound by all obligations incurred prior to the termination; however, all of EXFO's obligations will automatically terminate upon termination. EXFO is under no obligation to refund any monies because of termination. These termination rights are in addition to all other rights and remedies available to EXFO.

14. GENERAL

14.1 Neither the execution of this Agreement or anything in it, or the Software, shall be construed as providing nor implying any arrangement or understanding that EXFO will make any purchase, lease, examination or test of, or give any approval with respect to, any product or service.

14.2 Customer may not assign, in whole or in part, this Agreement, or any license, rights or obligations granted, to any Third Party, including without limitation, any subsidiary, affiliate or entity owned or controlled by Customer, or pursuant to any merger, consolidation or other Customer reorganization, without the prior written consent of EXFO.

14.3 The failure of either party at any time to enforce any of the provisions of this Agreement or any right under this Agreement, or to exercise any option provided, will in no way be construed to be a waiver of the provisions, rights, or options, or in any way to affect the validity of this Agreement. The failure of either party to exercise any rights or options under the terms or conditions of this Agreement shall not preclude or prejudice the exercising of the same or any other right or option under this Agreement.

14.4 This Agreement must be construed and enforced according to the laws applicable in the province of Quebec, Canada, without regards to its conflict of laws provisions. The parties specifically exclude the application of the United Nations Convention on Contracts for the International Sale of Goods and the Uniform Computer Information Transactions Act.

14.5 If any provision or portion of a provision of this Agreement is held invalid or unenforceable, the remainder of the Agreement shall not be affected, and the remaining terms will continue in effect and be binding on the parties, provided that such holding of invalidity or unenforceability does not materially affect the essence of the Agreement.

14.6 EXFO and Customer agree to comply with all applicable laws. Specifically, Customer will comply with all applicable export and import control laws and regulations of the United States and any foreign jurisdiction in which the Software is used and, in particular, Customer will not export or re-export the Software without all required United States and foreign government licenses. Customer acknowledges and understands that the Software contains encryption technology that may require an export license from the U.S. State Department when exported or re-exported to government end-users, Internet or telecommunications service providers providing services specific to government end-users. Export of the Software to certain countries is prohibited. Customer will defend, indemnify, and hold harmless EXFO from and against any violation of such laws or regulations by Customer or any of its agents, officers, directors, or employees.

14.7 The provisions of this Agreement constitute the entire agreement between the parties with respect to the licensing of the Software and supersede (i) all prior agreements, oral or written; (ii) any conflicting terms in Customer's purchase order or EXFO's invoice; and (iii) all other communications relating thereto. All Sections that by their sense and context are intended to survive the execution, delivery, performance and termination of this Agreement, will survive and continue in effect.

14.8 Any references to information contained in a URL form an integral part of this Agreement and the Customer hereby confirms that it has access to the Internet and confirms that prior to entering into this Agreement has read and agrees with the terms and conditions set out in those documents.

14.9 U.S. GOVERNMENT END USERS. The Software and any other software covered under this Agreement is a "commercial item" as that term is defined at 48 C.F.R. 2.101, consisting of "commercial computer software" and "commercial computer software documentation" as such terms are used in 48 C.F.R. 12.212. Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4, all U.S. Government End User Customers acquire the Software with only those rights set forth therein.

END OF TERMS AND CONDITIONS

CONTACT INFORMATION: If you have any questions about this Agreement, please direct all correspondence to: EXFO Inc., 400 Godin Avenue, Quebec City, Quebec, G1M 2K2, Canada. Legal notice shall be sent to the attention of the EXFO Legal Department.

Third Party and Open Source License Notice

This product may include software developed by the following people and organizations with the following copyright notices:

- SLF4J (<http://www.slf4j.org>). Copyright © 2004-2017 QOS.ch. All rights reserved.
- Spring Framework Project (<http://www.spring.io>). Copyright © 2017 Pivotal Software Inc. All rights reserved.
- Node.js (<http://www.nodejs.org>). Copyright Node.js contributors. Copyright Joyent, Inc. All rights reserved.
- Express (<http://www.expressjs.com>). Copyright © 2009-2014 TJ Holowaychuk <tj@vision-media.ca>, Copyright © 2013-2014 Roman Shtylman <shtylman+expressjs@gmail.com>, Copyright © 2014-2015 Douglas Christopher Wilson <doug@somethingdoug.com>. All rights reserved.
- Express Session (<http://www.expressjs.com>). Copyright © 2010 Sencha Inc. Copyright © 2011 TJ Holowaychuk <tj@vision-media.ca>, Copyright © 2014-2015 Douglas Christopher Wilson <doug@somethingdoug.com>
- http-node-proxy (<https://github.com/nodejitsu/node-http-proxy>). Copyright © 2010-2016 Charlie Robbins, Jarrett Cruger & the Contributors.
- node-uuid (<https://github.com/kelektiv/node-uuid>). Copyright © 2010-2016 Robert Kieffer and other contributors.
- KeyCloak (<http://www.keycloak.org>).
- Apache Tomcat (<http://tomcat.apache.org>). Copyright © 1999-2017, The Apache Software Foundation.
- PostgreSQL (<https://www.postgresql.org>). Copyright © 1996-2017 The PostgreSQL Global Development Group.
- Redis (<https://redis.io>). Copyright © 2006-2015, Salvatore Sanfilippo and Pieter Noordhuis.
- Swagger (<https://swagger.io>). Copyright © 2017 SmartBear Software.
- Prometheus (<https://prometheus.io/>)
- MongoDB (<https://www.mongodb.com/>) © 2019 MongoDB, Inc.
- All other trademarks or service marks are the property of their respective owners.

Any third party software provided to you is distributed under the terms of the license agreements associated with that third party software. Where applicable, copies of the terms are included elsewhere in the documentation for this product.

The source code for some of these components is available upon request for three years from the date of your receipt of the product. Please submit requests to EXFO; some fees could be required to cover the cost of distribution.:

Oracle Java Commercial Features Notice

Use of the Commercial Features for any commercial or production purpose requires a separate license from Oracle. "Commercial Features" means those features identified Table 1-1 (Commercial Features In Java SE Product Editions) of the Java SE documentation accessible at <http://www.oracle.com/technetwork/java/javase/documentation/index.html>

Contents

Regulatory Information	xiv
1 Introducing the FG-750 Fiber Guardian	1
Main Features	3
Available Models	4
Available Optical Switch Cassette Configurations	9
Power Sources	12
Supported Web Browsers	12
Developing Your Own Test Applications	13
Technical Specifications	13
Conventions	14
2 Safety Information	15
General Safety Information	15
Other Safety Symbols on Your Unit	17
Laser Safety Information (Units with an OTDR)	18
Electrical Safety Information	20
3 Getting Started with Your Fiber Guardian	25
Preventing Electrostatic Discharge Damage	25
Preparing for Installation	26
Installing Your Unit in a Rack	27
Grounding Your Unit	30
Inserting or Removing Optical Switch Cassettes (FG-750EX Models Only)	32
Working with the Fiber (Patchcord) Management Tray	37
Connecting the Power and the Network Cables	45
Turning On or Off the Unit	48
Connecting a Monitoring Device to the Dry Contact Relays	50
Connecting an External Switch	52
Retrieving the IP Address of the Rear Ethernet Port (Host and Companion)	55
Preparing Your Unit for 3G/4G Access	59
Operating the RTU through SMS	67
Preparing to Access Your Unit via a WAN or the Internet	69
Connecting to the VPN	79
Cleaning and Connecting Optical Fibers	82
Working with the REST Commands (Certain Models Only)	84
Installing the Notification Agent on Your Computer	85
Understanding the Applications, User Accounts and Passwords	87

4	Managing Users	91
	Introduction	91
	Logging in to the Administration Console	91
	Realm Settings	93
	Roles	93
	Managing Users	94
	Managing Groups	104
	User Federation	105
5	Using the Host Web User Interface	109
	Accessing and Exiting the Host Web UI	109
	Viewing Host and Companion Information	111
	Configuring Network Settings	112
	Configuring the 3G/4G Settings	115
	Connecting as an NQMSfiber EMS Client (OTDR Mode Only)	117
	Configuring the E-Mail Server Settings	119
	Configuring SNMP	120
	Configuring the Time Server Settings	123
6	Setting Up Your RTU	125
	Detecting the Fibers Connected to the Optical Ports	125
	Changing a Cassette	129
	Configuring a Remote Switch (ROTAU)	131
	ROTAU Status	136
	Configuring Alerts	139
	Managing Alert Types	140
	Managing System Setting Values	146
	Editing Test On Demand Default Parameters	155
7	Operating Your RTU in OTDR Measuring Mode	157
	Managing Optical Routes	157
	Managing Test Setups	165
	Managing Test Programs	175
	Managing Threshold Sets	179
	Performing an Ad Hoc Test	183
	Performing a Test	190
	Managing Degraded Fibers	192
	Viewing Current and Scheduled Jobs	197
	Configuring the Notification Agent	198
	Managing Cable Templates	203

Contents

8 Analyzing Results	215
Viewing the Current Fault List	215
Searching and Displaying OTDR Results	222
Search Results for Test On Demand	226
9 Using the Line Configuration Web User Interface	231
Accessing the Line Configuration Web UI	231
Managing Remote OTAUs	235
Managing Ports and Lines	240
Performing an Injection Loss Test	244
Managing Configurations	246
10 Working With the Event Log	249
Viewing the Event Log	249
Customizing the Log View	250
Applying and Clearing Filters	251
Exporting Log Reports	253
11 Maintenance	255
Cleaning Switchable Connectors	256
Cleaning EUI Connectors	260
Cleaning Other Types of Connectors	262
Replacing the Air Filter	263
Replacing the Fan	267
Replacing the Power Supply Modules	275
Replacing the OTDR	279
Replacing an RTU or Changing the SSD (managed by EMS)	283
Backing Up the Database	287
Viewing the Installed Applications	289
Viewing the Firmware Version of the Companion	290
Managing Applications (Software Packages)	291
Recalibrating the Unit	295
Recycling and Disposal	296

12 Troubleshooting	297
Solving Common Problems	297
LED Indicators Description	300
Viewing System Status	304
Testing the Status of the Relays	304
Refreshing the Status of the LEDs	306
Connecting to Your Unit Using the KMV Remote Console	308
Resetting Configuration (Parameters)	312
Restoring Your Unit to Normal Operation (Windows 8)	313
Restoring Your Unit to Normal Operation (Windows 10)	317
Viewing Online Documentation	334
Contacting the Technical Support Group	335
Viewing Product Information	336
Transportation	336
13 Warranty	337
General Information	337
Liability	337
Exclusions	338
Certification	338
Service and Repairs	339
EXFO Service Centers Worldwide	340
A Fault Geolocalization Using a KML File	341
Index	345

Regulatory Information



IMPORTANT

Because of the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (that is, have errors) or be totally lost. Although significant delays or losses of data are rare when wireless devices such as your FG-750 are used in a normal manner with a well-constructed network, the unit should not be used in situations where failure to transmit or receive data could result in damage of any kind to the user or any other party, including but not limited to personal injury, death, or loss of property. EXFO accepts no responsibility for damaged of any kind resulting from delays or errors in data transmitted or received using the module, or for failure of the unit to transmit or receive such data.

Canada and USA Electromagnetic Interference Regulatory Statement

Electronic test and measurement equipment is exempt from FCC part 15, subpart B compliance in the United States of America and from ICES-003 compliance in Canada. However, EXFO Inc. makes reasonable efforts to ensure compliance to the applicable standards.

The limits set by these standards are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the user documentation, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

This product does not contain any user-serviceable components. Any product change or modification done by the user that is not expressly approved by the manufacturer will invalidate warranty and all applicable regulatory certifications and approvals and could void the user's authority to operate the equipment.

European Electromagnetic Compatibility Regulatory Statement

Warning: This is a class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures. Your product is suitable for use in industrial electromagnetic environments.

Canada and USA Wireless Compliance Related Information

If you purchased the 3G/4G option, your unit comes with an internal wireless module (adapter) and an antenna for which the information hereafter applies:

- This device complies with Part 15 of the FCC Rules.
- This device complies with Innovation, Sciences and Economic Development Canada license-exempt RSS standards.
- Operation is subject to the following two conditions:
 - (1) This device may not cause harmful interference
 - and
 - (2) this device must accept any interference received, including interference that may cause undesired operation.

Use in Specific Environments:

- The use of wireless products in hazardous locations is limited by the constraints posed by the safety directors of such environments.
- The use of wireless products in hospitals is restricted to the limits set forth by each hospital.
- Do not operate your unit in areas where blasting is in progress.
- Do not operate your unit where explosive atmospheres may be present including refuelling points, fuel depots, and chemical plants.
- Do not operate your unit near medical equipment, life support equipment, or any equipment which may be susceptible to any form of radio interference. In such areas, the unit *must be powered off*. Otherwise, the unit can transmit signals that could interfere with this equipment.

Radiation Exposure Statement:

- For compliance to RF exposure requirements, a minimum separation distance of 20 centimeters (8 inches) must be maintained between the FG-750 antenna and the user or bystanders when the unit is working.
- To comply with regulations limiting both maximum RF output power and human exposure to RF radiation, the maximum antenna gain including cable loss in a mobile-only exposure condition must not exceed the limits speculated in the table below:

Technology	Band	Frequency (MHz)	Maximum Antenna Gain (dBi)
LTE	2	1850–1910	6
	4	1710–1755	6
	5	824–849	6
	7	2500–2570	6
	12	699–716	6
	13	777–787	6
	25	1750–1915	6
	26	814–849	6
	30	2305–2315	(Disabled)
	41	2496–2690	9
UMTS	2	1850–1910	6
	4	1710–1755	6
	5	824–849	6

European Declaration of Conformity

The full text of the EU declaration of conformity is available at the following Internet address: www.exfo.com/en/resources/legal-documentation.

1 Introducing the FG-750 Fiber Guardian

The FG-750 Fiber Guardian is a multiple-port OTDR aimed at remote testing and continuous monitoring of lit/unlit optical fibers. The equipment can be used as a stand-alone unit or as an RTU (remote test unit), part of a centralized management system like EXFO NQMS*fiber*. An RTU contains an OTDR (optical time domain reflectometer) and an optical switch that allows the instrument to test and monitor multiple fibers from the same instrument.

In case you intend to or currently operate your FG-750 as part of an NQMS*fiber* system (centrally managed), Chapters 6 and 7 of this guide present functions centrally available from the EMS (Element Management System) Web User Interface, such as result viewing and creation/editing of test setups. Should you want to operate the unit as an autonomous *RFTS* (OTDR-based) unit, then all of this user guide is relevant in you becoming familiar with the how-to-use Fiber Guardian in a stand-alone installation, including how to setup e-mail and/or SMS alerts, and optional 3G/4G wireless interface.

The user guide also addresses a specialized usage of Fiber Guardian that is a fixed, remotely controlled, multi-port iOLM test equipment. This operation mode is available for example with a Node OTDR (OTM-700-Node) module.

Note: *If you purchased an FG-750ST/EX-Node iOLM and want to operate it as an iOLM product, you will first need to switch modes by choosing an application, before operating the equipment. By default, factory sets the operation mode to OTDR.*

- In OTDR mode, you can run basic functions such as triggering a manual OTDR test (ad-hoc), enabling standard fiber monitoring, and creating a cable template test campaign that allows for scheduled testing of one or multiple fibers, part of the same cable span for short or long periods of time.

Introducing the FG-750 Fiber Guardian

- In iOLM mode with a Node OTDR (OTM-700-Node), you can use the equipment as an intelligent Link-Aware™ probe and run your own tests through an API (REST services), fully documented and available standard with the product. With a Node iOLM Fiber Guardian, you can test through PON splitters with the help of HRD (high-reflectance demarkation) filters that provide the discrimination required to measure and monitor attenuation of a specific branch of a P2MP (point-to-multipoint) line.

Various applications are possible using Node iOLM (OTM-700-Node in iOLM mode):

- 24/7 surveillance of dark (no traffic) or lit (with traffic) optical fibers
- On-demand troubleshooting of P2P (point-to-point) and P2MP fiber lines
- Attenuation testing with HRD (termination filters) mainly in PON (passive optical network)
- Pass-fail testing on the transport fiber at time of installation
- Certification testing up to the customer port or drop terminal port
- Preventive maintenance testing and detection/localization of water intrusion or other slow varying phenomenon.

Main Features

Your unit includes the following:

- Stand-alone capabilities scalable to a centralized server application if required
- A main CPU (*host*), and a BMC (baseboard management controller) as a secondary controller unit (*companion*)
- OTDR measurement, fault finding, test scheduling, local storage, and event forwarding to external system or synchronization with centralized server application like EXFO NQMS*fiber*
- Optional built-in (first stage) or cassette switches (second stage)
- Possibility to connect external switches (remote OTAUs) for second and third stage switching capability
- Two USB 2.0 ports (host)
- Two Ethernet ports - local access and LAN/WAN connection
- Optional integrated communication module and external antenna for 3G/4G access (to take over automatically when the wired network is down, or to be used as primary network)
- Installation in a rack (rack-mounting brackets, front drawer for access to key parts and modules, and optional fiber management tray)
- Optional TAM (test access module) kits to couple transmit/receive OLT (optical line termination) port and test port to the line under test
- Optional patch panels to switch from multifiber cabling to single-fiber cabling without the WDMs (wavelength division multiplexers)
- Access to configure settings via the Fiber Guardian Host Web UI
- Ability to create a logical line based on the port numbers used, giving them a unique name or ID through the Line Configuration Web UI
- Open and fully documented API (REST interface) that enables you to develop your own system-level network test and management solution

Introducing the FG-750 Fiber Guardian

Available Models

- Can be managed from EMS (Element Management System)
- Fiber management tray (optional) that can be mounted on FG-750 front to better manage large quantity and/or extra length of jumper cables.

Available Models

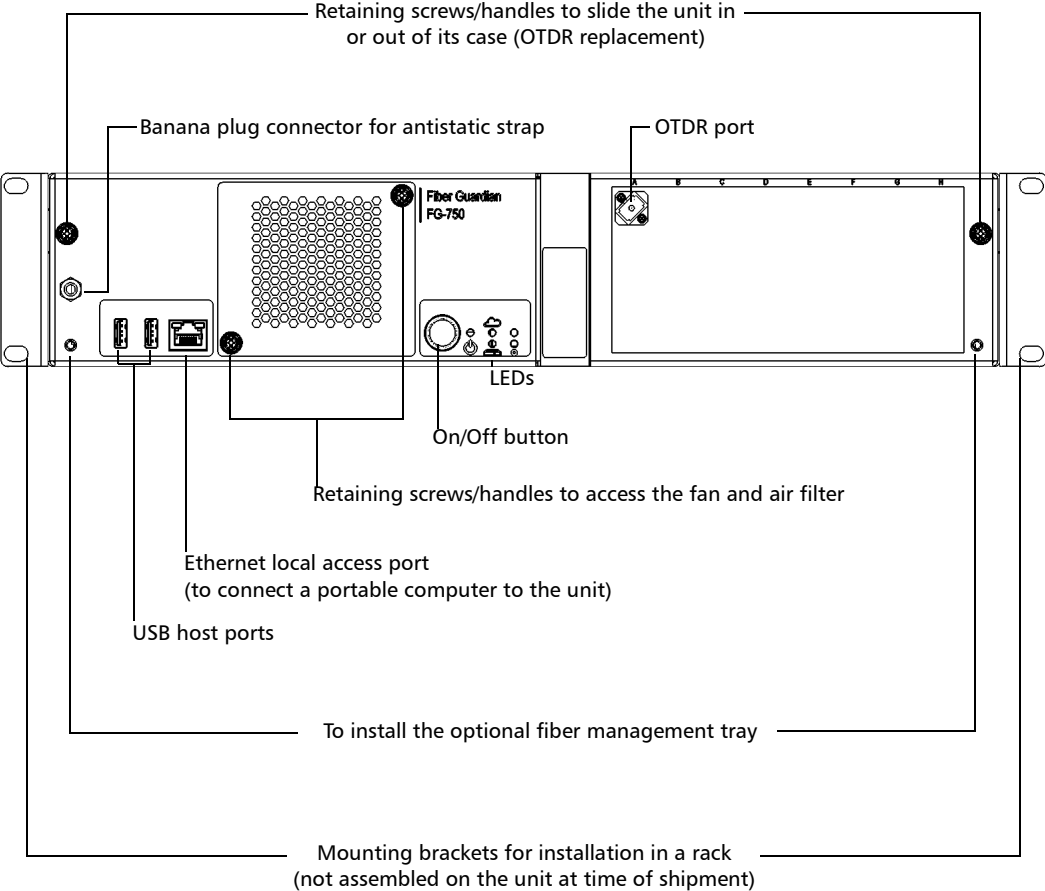
To better suit your testing needs, the following models are available:

- Single-port Fiber Guardian without an optical switch inside the unit (built-in or cassette type). Model: FG-750ST-XXXX-01 (ST:standard).
- Multiple-port Fiber Guardian with a built-in optical switch inside the unit. Model: FG-750ST-XXXX-N (N=4, 8, 12, 24, 32).
- Expandable multiple-port Fiber Guardian with optical switch cassettes that can be added/removed from an 8-port basic configuration. Model: FG-750EX.

Fiber Guardian without Switch Ports

FG-750ST single port model: FG-750ST-XXXX-01

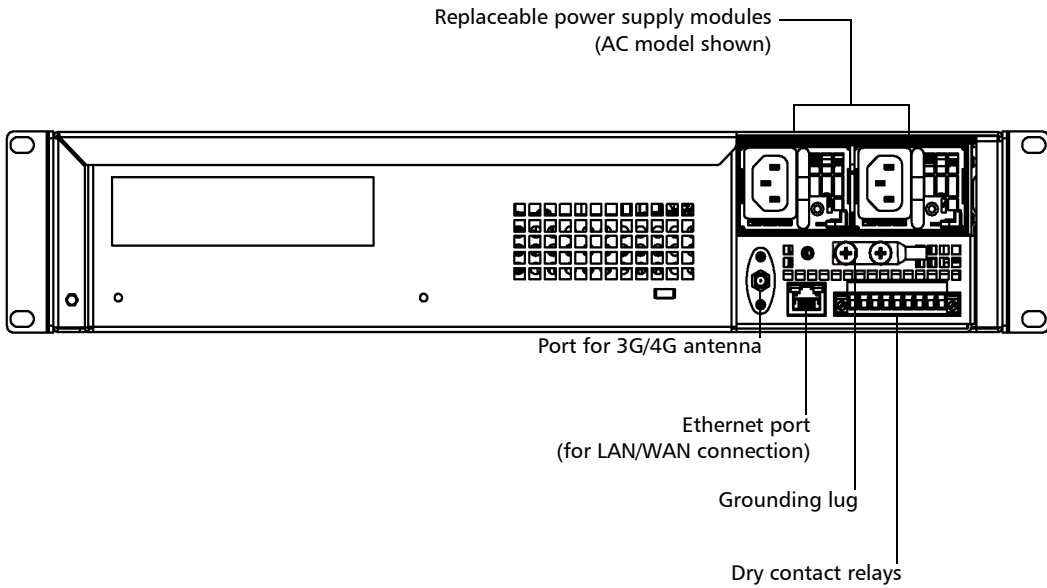
Front



Introducing the FG-750 Fiber Guardian

Available Models

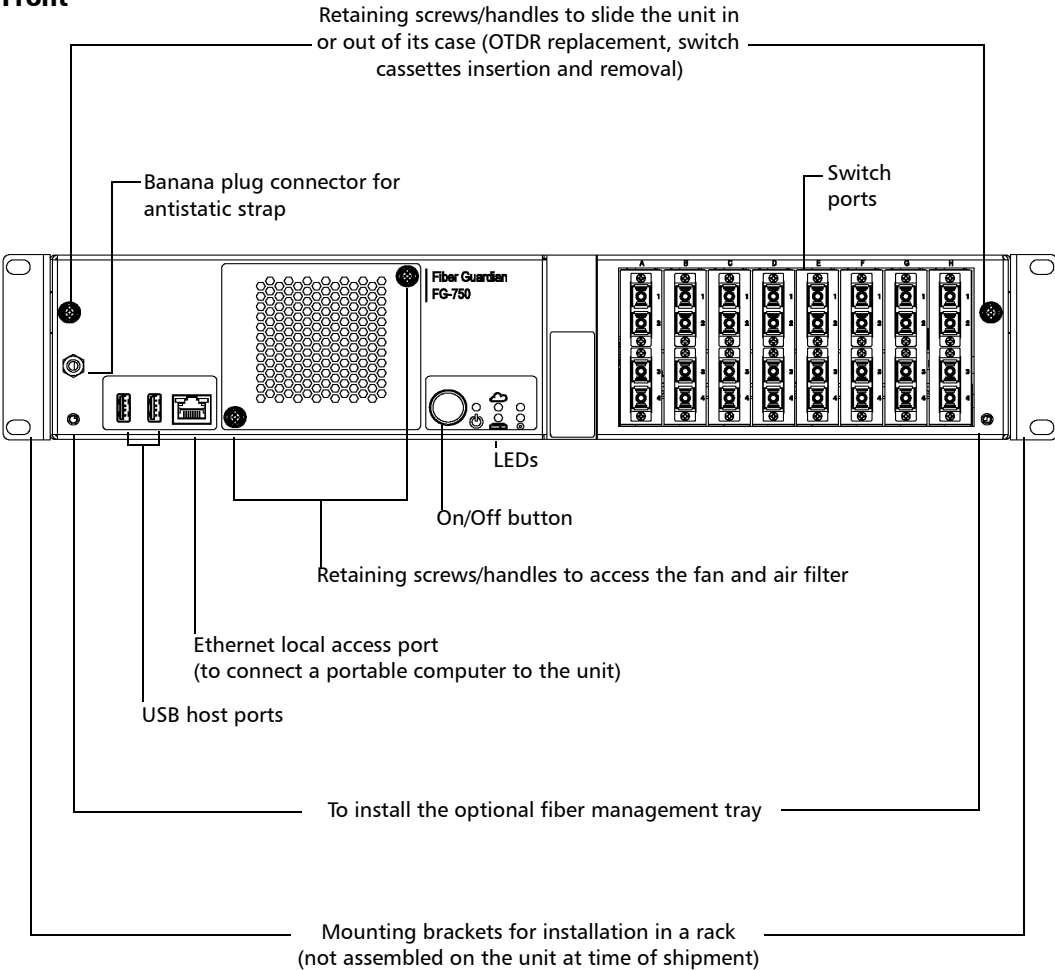
Back



Fiber Guardian with Switch Ports

Expandable Fiber Guardian with optical switch cassettes (shown below, fully loaded SC 32-port configuration)

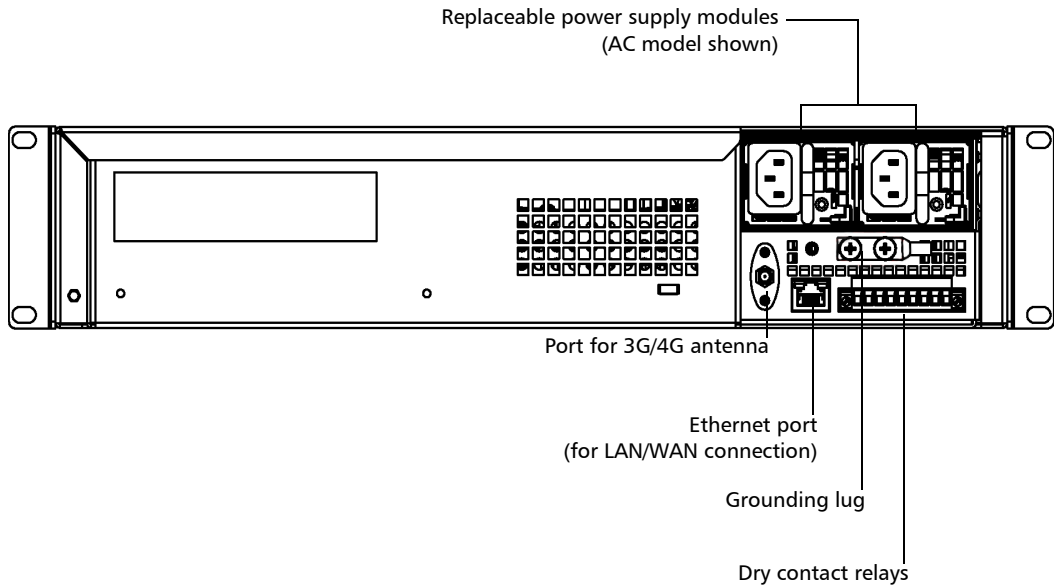
Front



Introducing the FG-750 Fiber Guardian

Available Models

Back



Available Optical Switch Cassette Configurations

When delivered with an optical switch, the minimum configuration for the FG-750 is 1x4 which is the size of optical switch cassette (OSC). The maximum is 1x96 with L1 (integrated first stage called L1) being a 1x8 connected to MTP 12-port cassettes at the second stage. Several possible configurations are available according to your needs.

Cassettes have various connector configurations to provide desirable port density or preferred connection standards. When the cassettes do not fill all the slots, you can use empty (short jumper) cassettes to avoid dust or other elements that could interfere with your testing.

Note: *Optical switch cassettes are all mounted with angled (APC) polished connectors.*

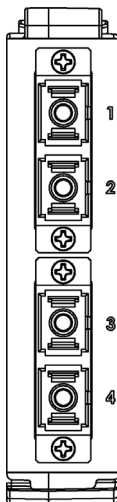


SC-Type Cassette (small jumper, no optical switch)

Introducing the FG-750 Fiber Guardian

Available Optical Switch Cassette Configurations

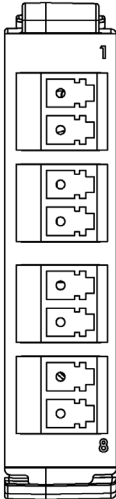
The one-port OSC is connected to the L1 stage and OTDR, and can be used for testing.



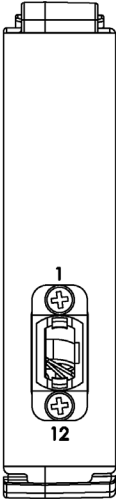
SC-type cassette (4-port optical switch)

Introducing the FG-750 Fiber Guardian

Available Optical Switch Cassette Configurations



LC-type cassette (8-port optical switch)



MTP-type cassette (12-port MTP optical switch)

Power Sources

Your unit operates with the following power sources:

- Replaceable power supply module (either AC or DC). Your unit needs only one power supply module to work, but it can house two of them. The second power supply provides redundancy. Your unit has been certified with two power supplies of the same type (two AC or two DC).

The power supply modules are hot-swappable, which means that you do not have to turn off your system to replace one of them. There is no need to disassemble the unit to replace such a power supply. For more information, see *Replacing the Power Supply Modules* on page 275.

- Rechargeable battery (for clock). This battery can keep the date and time for a very long time even if power is not connected to the unit.

Supported Web Browsers

The Host Web UI, the Line Configuration Web UI, the KVM remote console, and NQMS Web App support the following Web browsers:

- Internet Explorer 11 (IE11 mode only; compatibility mode not supported) or later.
- Google Chrome, version 49.0 or the last compatible version with Windows XP. Older versions are usually subject to vulnerabilities.
- Mozilla Firefox, version 52.0 or later.

Note: *If you want to work with the KVM remote console, you should ensure that Java 6 or later is installed on the computer that you will use to connect to this application.*

Developing Your Own Test Applications

In Link-Aware™ mode, you can build your own network test and management solution with the provided REST commands. For more information, see *Working with the REST Commands (Certain Models Only)* on page 84.

In OTDR mode, measurement API is based on REST, using the following commands:

- GET reads a known resource or a list of resources.
- PUT replaces the state and content of a known resource.
- POST changes the state of a resource that either doesn't yet exist (in creation) or its ID is unknown in advance.
- PATCH issues partial changes to a resource requiring existence of the changed resource.
- DELETE removes the known resource from storage.
- HEAD gets an HTTP response code when obtaining resources without any data.

Technical Specifications

To obtain this product's technical specifications, visit the EXFO Web site at www.exfo.com.

Conventions

Before using the product described in this guide, you should understand the following conventions:



WARNING

Indicates a potentially hazardous situation which, if not avoided, could result in *death or serious injury*. Do not proceed unless you understand and meet the required conditions.



CAUTION

Indicates a potentially hazardous situation which, if not avoided, may result in *minor or moderate injury*. Do not proceed unless you understand and meet the required conditions.



CAUTION

Indicates a potentially hazardous situation which, if not avoided, may result in *component damage*. Do not proceed unless you understand and meet the required conditions.



IMPORTANT

Refers to information about this product you should not overlook.

2 **Safety Information**

General Safety Information



WARNING

Do not install or terminate fibers while a light source is active. Never look directly into a live fiber and ensure that your eyes are protected at all times.



WARNING

The use of controls, adjustments and procedures, namely for operation and maintenance, other than those specified herein may result in hazardous radiation exposure or impair the protection provided by this unit.



WARNING

If the equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.



WARNING

Use only accessories designed for your unit and approved by EXFO. For a complete list of accessories available for your unit, refer to its technical specifications or contact EXFO.


Safety Information

General Safety Information



IMPORTANT




When you see the following symbol on your unit , make sure that you refer to the instructions provided in your user documentation. Ensure that you understand and meet the required conditions before using your product.



IMPORTANT



When you see the following symbol on your unit , it indicates that the unit is equipped with a laser source, or that it can be used with instruments equipped with a laser source. These instruments include, but are not limited to, modules and external optical units.














IMPORTANT

Other safety instructions relevant for your product are located throughout this documentation, depending on the action to perform. Make sure to read them carefully when they apply to your situation.






Other Safety Symbols on Your Unit

One or more of the following symbols may also appear on your unit.

Symbol	Meaning
	Direct current
	Alternating current
	The unit is equipped with an earth (ground) terminal.
	The unit is equipped with a protective conductor terminal.
	The unit is equipped with a frame or chassis terminal.
N	Neutral conductor
	On (Power)
	Off (Power)
	In position of a bistable push control
	Out position of a bistable push control
 OR 	On/off (Power)

Safety Information

Laser Safety Information (Units with an OTDR)

Symbol	Meaning
	Caution hot surface
	This slide rail mounted equipment is not to be used as a shelf or work space.
	Fuse
	Plus: positive polarity
	Minus: negative polarity

Laser Safety Information (Units with an OTDR)

Your instrument is in compliance with standards IEC 60825-1: 2007 and 2014.



WARNING

(IEC 60825-1: 2007) Viewing the laser output with certain optical instruments designed for use at a distance (for example, telescopes and binoculars) may pose an eye hazard.



WARNING

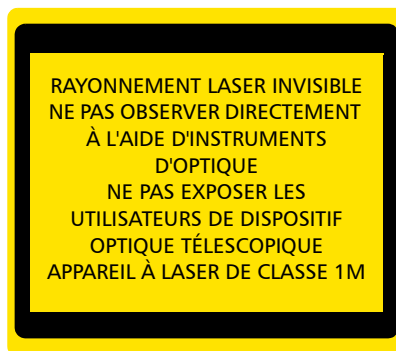
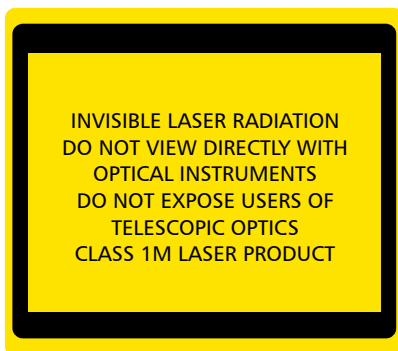
(IEC 60825-1: 2014) Viewing the laser output with telescopic optical instruments (for example, telescopes and binoculars) may pose an eye hazard and thus the user should not direct the beam into an area where such instruments are likely to be used.







Laser radiation may be encountered at the optical output port.

Safety Information

Laser Safety Information (Units with an OTDR)

The following labels indicate that the product contains a Class 1M source:



Wavelengths: / Longueur d'onde	Pulse width: / Largeur de l'impulsion	Max. peak power: / Puissance crête maximum
800 nm - 1300 nm	 $\leq 1 \mu s$	 $\leq 500 \text{ mW}$
1300 nm - 1400 nm	 $\leq 20 \mu s$	 $\leq 260 \text{ mW}$
1400 nm - 1700 nm	 $\leq 20 \mu s$	 $\leq 600 \text{ mW}$

Complies with standards 21 CFR 1040.10, except for deviations pursuant to Laser Notice No. 50, dated June 24, 2007.



CAUTION

Your unit contains a replaceable OTDR module.
To avoid damaging your FG-750 Fiber Guardian, use only EXFO
OTDR modules of the OTM-7xx Series with it.

Electrical Safety Information

This unit uses an international safety standard three-wire power cable. This cable serves as a ground when connected to an appropriate AC power outlet.



WARNING

- A readily accessible disconnect device must be installed on the mains (AC or DC circuits). The power cord of the AC/DC power adapter can be considered the disconnect device to the main power.
- If you intend to connect your FG-750 to AC power, use only the listed and certified AC/DC power adapter provided by EXFO with your unit. It provides reinforced insulation between primary and secondary, and is suitably rated for the country where the unit is sold.
- **DO NOT** connect the unit interfaces metallicity to OSP (Outside Plant) wiring. The unit interfaces are designed for use as intra-building surfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE) and require isolation from the exposed OSP cabling. The addition of Primary Protectors is not sufficient protection in order to connect these interfaces metallicity to OSP wiring.
- Use only the certified power cord that is suitably rated for the country where the unit is used.
- Replacing detachable MAINS supply cords by inadequately RATED cords may result in overheating of the cord and create a risk of fire.



WARNING

- Consideration should be given to the connection of the unit to the supply circuit, and the effect that overloading the circuits might have on over-current protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
- Ensure that your power supply is properly grounded and that the power cable and power supply are compatible with the unit.
- The power supply in this product contains no user-serviceable parts. There is more than one supply in this product. Refer servicing only to qualified personnel.
- Do not attempt to modify or use the supplied AC power cord if it is not the exact type required. A product with more than one power supply will have a separate AC power cord for each supply.

Note: *The AC power supply is not covered by the NEBS certification.*

Safety Information

Electrical Safety Information



WARNING

- Use this unit indoors only.
- Do not remove unit covers during operation.
- Operation of any electrical instrument around flammable gases or fumes constitutes a major safety hazard.
- To avoid electrical shock, do not operate the unit if any part of the outer surface (covers, panels, etc.) is damaged.
- Make sure both disconnect devices are turned off before servicing the unit.
- Only authorized personnel should carry out adjustments, maintenance or repair of opened units under voltage. A person qualified in first aid must also be present. Do not replace any components while the disconnect devices are turned on.
- Your unit is equipped with an internal rechargeable clock battery to keep time and date accurate. Only authorized personnel can replace this battery. Attempting to replace it yourself could seriously compromise your safety.
- Unless otherwise specified, all interfaces are intended for connection to Safety Extra Low Voltage (SELV) circuits only.
- Capacitors inside the unit may be charged even if the unit has been disconnected from its electrical supply.



CAUTION

Position the unit so that the air can circulate freely around it.

Equipment Ratings	
Temperature	
➤ Operation	➤ Node iOLM model: 0 °C to 40 °C (32 °F to 104 °F) ➤ Other models: -5 °C to 50 °C (23 °F to 122 °F)
➤ Storage	➤ -40 °C to 70 °C (-40 °F to 158 °F)
Heat release	300 W/m ²
Relative humidity	≤ 95 % non-condensing
Maximum operation altitude	3000 m (9843 ft)
Pollution degree	2
Installation category	II
Input Power	
➤ AC model ^a	➤ 100 - 240 V ~; 50/60 Hz; 2 A/1 A
➤ DC model ^b	➤ -48 V ---; 3 A

- a. Not exceeding ± 10 % of the nominal voltage.
b. Range: -40 - -72 V



CAUTION

- The use of voltages higher than those indicated on the label affixed to your unit may damage the unit.
- The operation and storage temperatures, as well as the altitude and relative humidity values of some modules may differ from those specified for your unit. In this case, always ensure that you comply with the most restrictive conditions (either module or unit).

3 **Getting Started with Your Fiber Guardian**

The installation process can be divided into the following main steps:

- Preparing for installation
- Installing the unit in a rack
- Connecting the devices
- Turning on the unit
- Connecting cables to the optical ports



WARNING

To avoid personal injuries and damages to the unit, you must perform the procedures detailed in this section in the order they are presented.

Preventing Electrostatic Discharge Damage

Electrostatic discharge (ESD) damage can cause complete or intermittent equipment failures. Always use an ESD-preventive wrist or ankle strap and ensure that it makes good skin contact. Connect the equipment end of the connection cord into the ESD connector located on the front of your unit (see *Available Models* on page 4).

All procedures for which the use of an antistatic strap is recommended will be identified as such throughout this documentation.

Preparing for Installation



WARNING

- The unit is designed to be installed in a limited access area, for example, Central Offices, Telecommunication Centers, computer rooms, wiring closet and similar type locations and in accordance with local codes.
- Only trained personnel can perform the unit installation and configuration tasks. These people have appropriate technical training and experience to be aware of the hazards to which a person can be exposed when performing these installation tasks.

Before installing your unit, you should take the following into consideration:

- The chosen location provides adequate clearance for maintenance procedures.
- The location is an environmentally-controlled area that meets the minimum operating parameters.
- The location is isolated from strong electromagnetic fields produced by electrical devices.
- The power cable and power supply are compatible with your power service.
- The power source is properly grounded and falls within the internal power supply rating.
- The location is in an ESD-safe work area.

Installing Your Unit in a Rack

- The rack (which is not included with the unit) should provide sufficient vertical clearance to insert the unit. The height of the unit is two rack units (2U) high or about 3 1/2 inches.
- All electrical cabling can be connected only through the back panel.



WARNING

- The equipment rack must be anchored to an unmovable support to prevent it from falling over when one or more servers are extended in front of the rack on slides. You must also consider the weight of any other device installed in the rack. A crush hazard exists should the rack tilt forward which could cause serious injury.
- Mounting of the unit in a rack or cabinet should be such that a hazardous condition is not achieved due to uneven mechanical loading. The fully-configured unit is heavy. Use caution when manipulating the unit. A lifting mechanism may be required for installation.

There mounting brackets are available in three formats:

- For 19-inch racks
- For 21-inch (ETSI) racks
- For 23-inch racks.



IMPORTANT

Ensure that you use the type of mounting brackets that corresponds to the width of your rack.

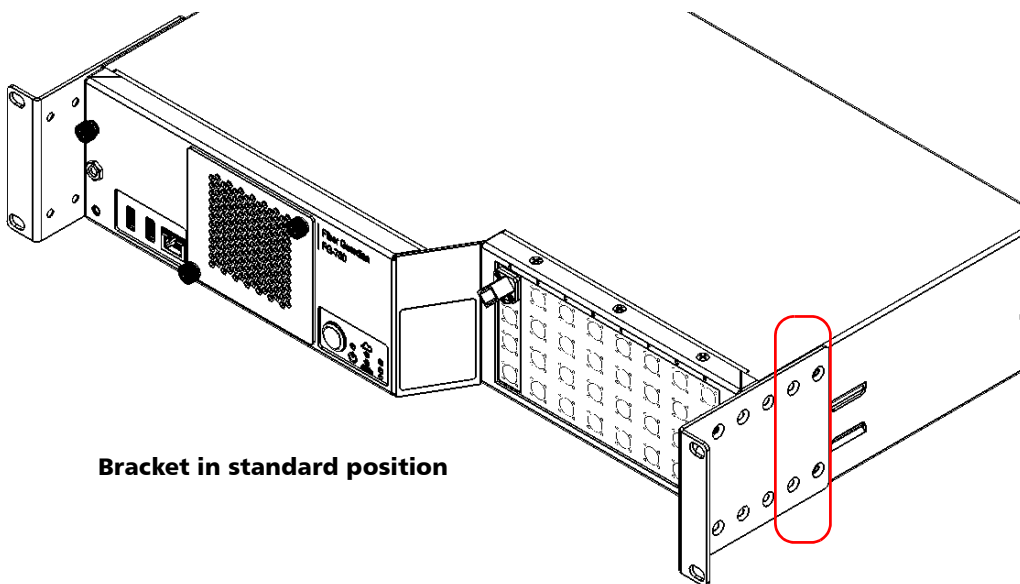
The brackets have several rows of holes for more installation versatility. You can install the unit with its front panel flush with the front of the rack, install it forward, or even recessed in the rack.

Getting Started with Your Fiber Guardian

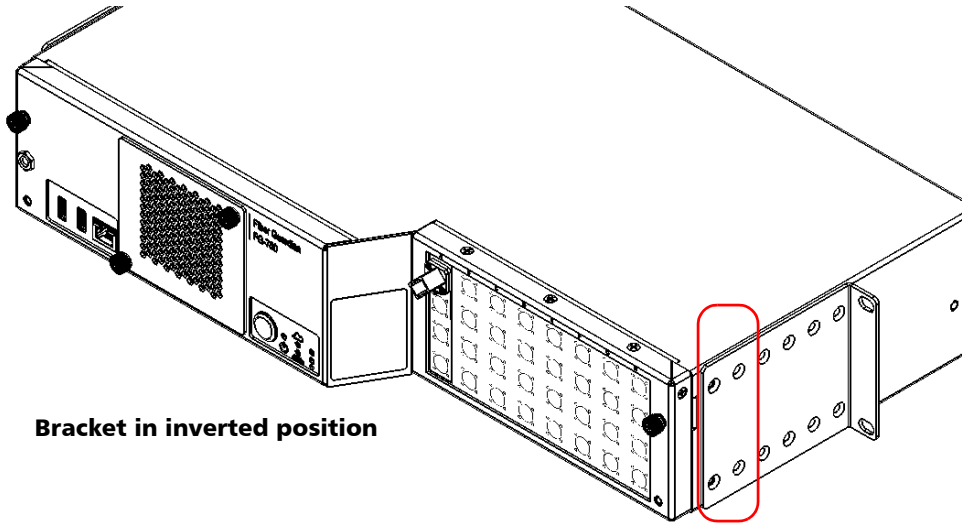
Installing Your Unit in a Rack

To install the mounting brackets on your unit:

- 1.** If necessary, turn off the unit and disconnect all optical fibers and electrical cables.
- 2.** Position the unit so that its bottom panel rests on a flat surface such as a table.
- 3.** Align the holes of the first bracket with the holes of the unit casing at the position that best suits your installation needs. You can even invert position of the mounting bracket if necessary.



Bracket in standard position



Bracket in inverted position

- 4.** Fix the first bracket on the unit with the supplied screws (four screws per bracket).
- 5.** Repeat steps 3 and 4 with the other bracket, ensuring that you place the bracket at the exact same position (orientation of the bracket, set of holes on the bracket and on the unit's casing).
- 6.** Place the unit in the rack at the desired height.
- 7.** Fix the unit in place using four 10-32 x 1/2 in. screws (four M6 screws for the ETSI racks).
- 8.** For NEBs installation, use thread-forming type unit mounting screws that remove any paint or non-conductive coatings to establish a metal-to-metal contact.

Grounding Your Unit

To avoid the potential for an electrical shock hazard, you must reliably connect an earth grounding conductor to the unit (AC and DC models).

Note: *The DC units are intended for installation with an isolated DC return (DC-I) and are to be installed in a Common Bonding Network (CBN) per NEBS GR-1089.*



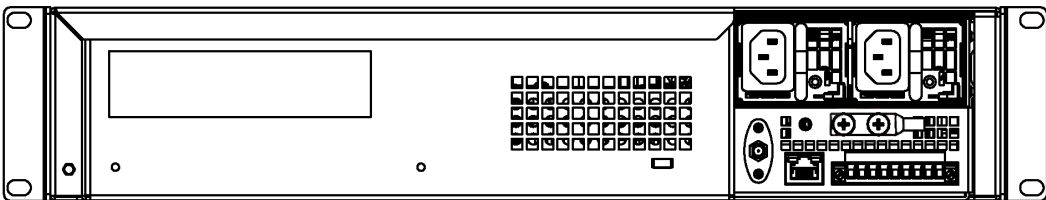
IMPORTANT

Ensure to ground the unit using a grounding method that complies with your local regulations.

If you are not sure on how to proceed, consult a certified electrician.

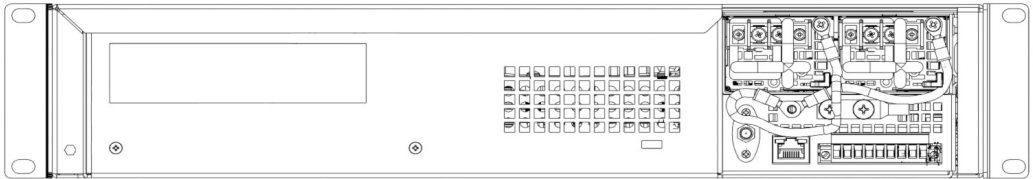
To ground your unit:

1. Remove the two Phillips screws, and remove the grounding lug from the rear panel of the unit.



2. Prepare the ground wire (minimum 12 AWG), and attach one of its ends to the unit's grounding lug using the appropriate crimping tool.
3. Use the two Phillips screws to attach the grounding and wire assembly to the rear panel of the unit.

4. Ground the other end of the wire as per your local regulation.
5. If a DC power supply is used, it needs to be grounded to the unit by using 2 green wires.



Your unit is now grounded properly.

Inserting or Removing Optical Switch Cassettes (FG-750EX Models Only)

If your unit features optical switch cassettes, you can change the configuration according to your test needs.

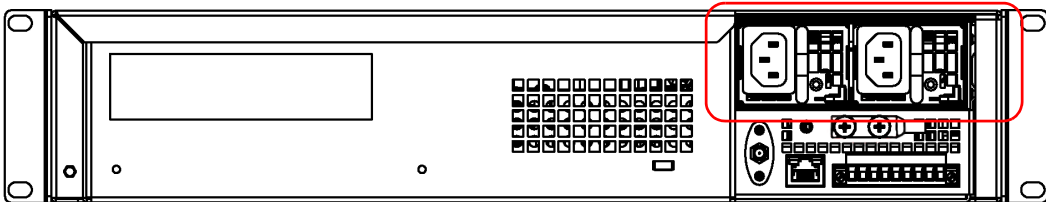


CAUTION

When removing a cassette, make sure to replace it with another one so that the front opening of the unit is always filled. Leaving empty spaces into the opening could allow dust and particles into the unit, and compromise its optimal operation.

To insert a cassette into the unit:

1. If you are using a fiber management tray, remove the protective window. For more information, see *Working with the Fiber (Patchcord) Management Tray* on page 37.
2. Turn off the unit and disconnect it completely from the power sources.

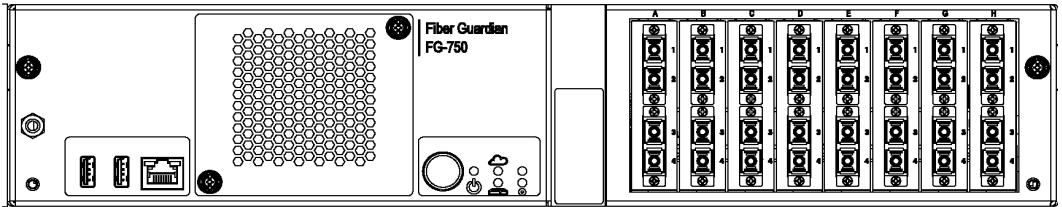


3. Put on an antistatic strap and connect it to the connector provided for that purpose on the front panel of the unit.

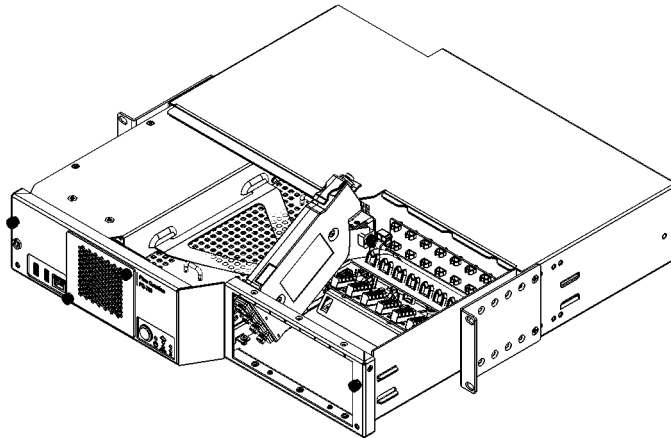
Getting Started with Your Fiber Guardian

Inserting or Removing Optical Switch Cassettes (FG-750EX Models Only)

4. Loosen the retaining screws on each side of the unit.



5. Pull the unit out of its casing.
6. If you have not done so already, clean the optical fiber connector located at the back of the cassette. For more information, see *Cleaning and Connecting Optical Fibers* on page 82.
7. Insert the cassette through the top opening.

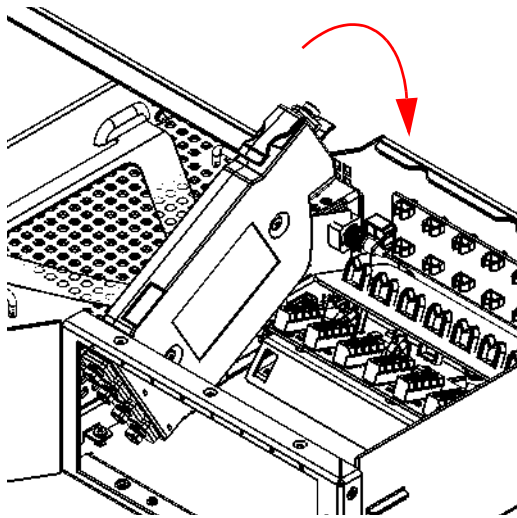


8. Connect the cassette to the unit using the optical connector at the back of the cassette and the corresponding optical fiber.

Getting Started with Your Fiber Guardian

Inserting or Removing Optical Switch Cassettes (FG-750EX Models Only)

9. Align the connector at the bottom of the cassette with the one inside the unit, and push down. The cassette will snap into place.



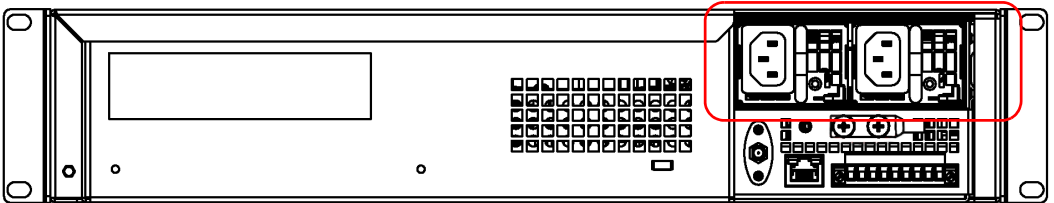
10. Push the unit back into its casing and retighten the retaining screws.
11. If you are using a fiber management tray, put the protective window back into place. For more information, see *Working with the Fiber (Patchcord) Management Tray* on page 37.

Getting Started with Your Fiber Guardian

Inserting or Removing Optical Switch Cassettes (FG-750EX Models Only)

To remove a cassette from the unit:

1. If you are using a fiber management tray, remove the protective window. For more information, see *Working with the Fiber (Patchcord) Management Tray* on page 37.
2. Turn off the unit and disconnect it completely from the power sources.



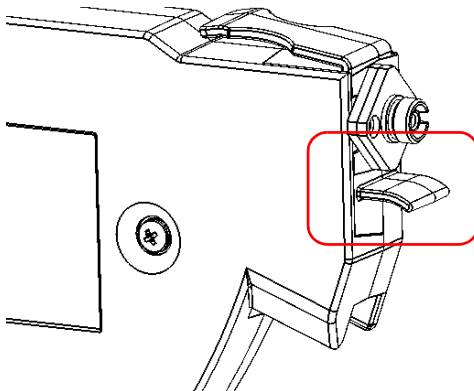
3. Put on an antistatic strap and connect it to the connector provided for that purpose on the front panel of the unit.
4. If you have not done so already, disconnect any fiber from the front of the cassette. Loosen the retaining screws on each side of the unit.
5. Pull the unit out of its casing.
6. Disconnect the optical fiber from the cassette and put the fiber back on the holder at the back of the unit.



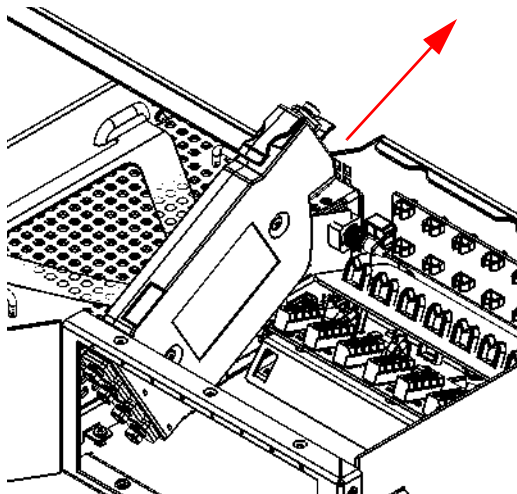
Getting Started with Your Fiber Guardian

Inserting or Removing Optical Switch Cassettes (FG-750EX Models Only)

7. Pull the module up using the tab located under the connector at the back of the cassette.



8. Pull the module out.



9. Push the unit back into its casing and retighten the retaining screws.
10. If you are using a fiber management tray, put the protective window back into place. For more information, see *Working with the Fiber (Patchcord) Management Tray* on page 37.

Working with the Fiber (Patchcord) Management Tray

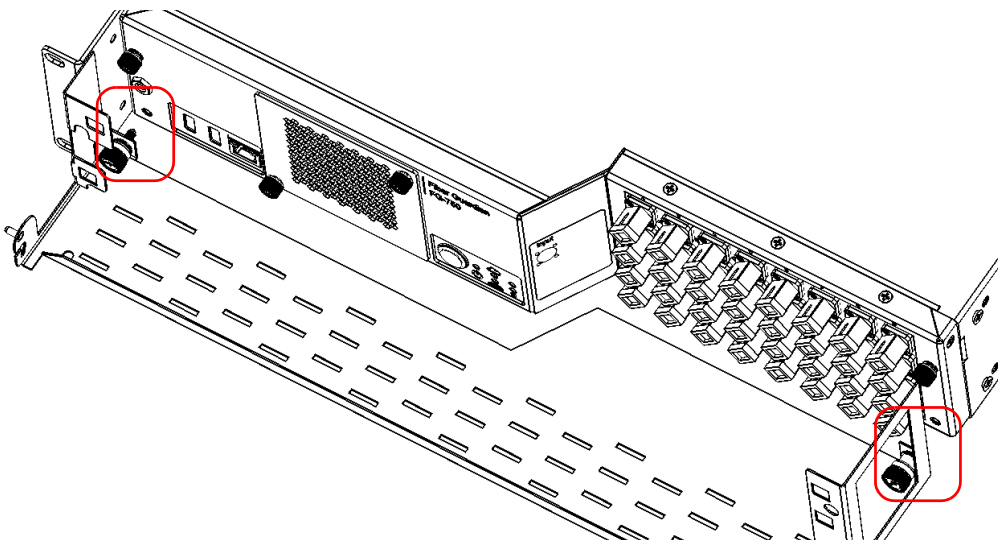
You can install an optional fiber management tray on your unit.

Note: *The fiber tray is not covered by the NEBS certification.*

The tray comprises a fixed part that you screw in place on your unit, and a mobile part (protective window). The protective window can be either folded down (access to the fan block or filter) or removed completely (insertion or removal of switch cassettes). As for the fiber management clips (into which you slide the fibers), there are five possible positions for more installation versatility.

To install the fiber management tray:

1. Carefully align the screws of the fiber management tray with the holes on the front of your unit.

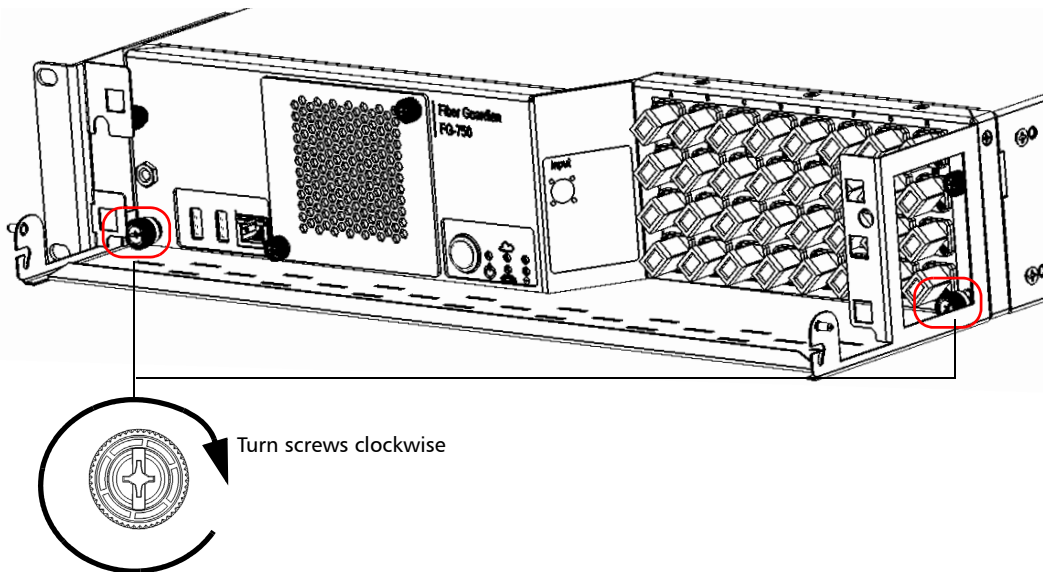


2. Slide the tray toward the unit until it makes contact with the casing of the unit.

Getting Started with Your Fiber Guardian

Working with the Fiber (Patchcord) Management Tray

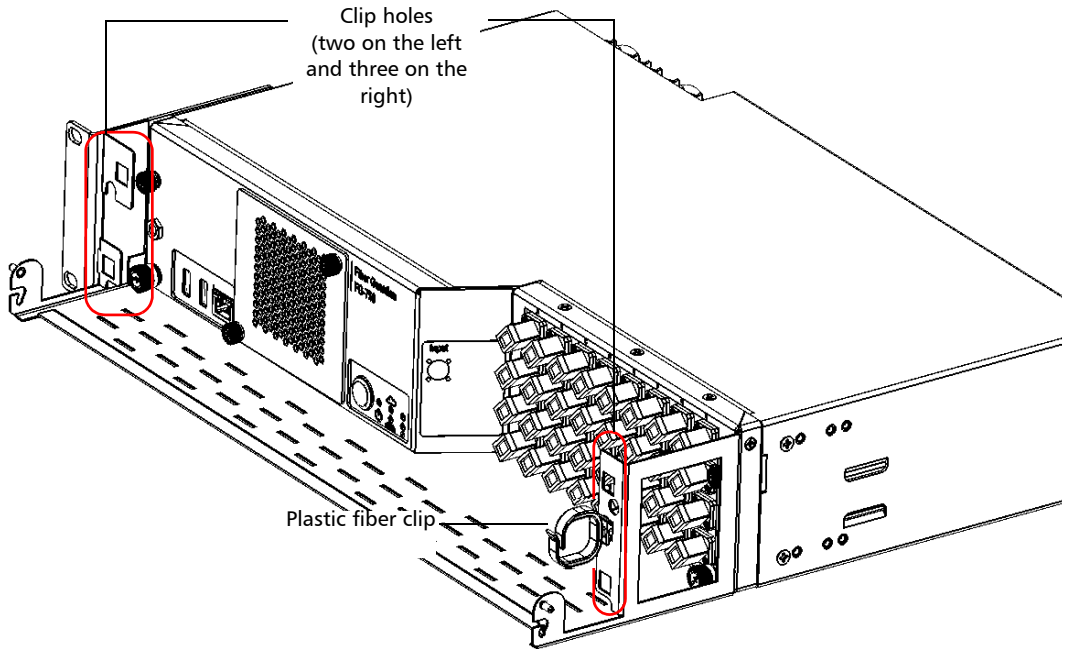
3. Using a Phillips screwdriver, turn the retaining screws clockwise until the tray is secured in place.



Getting Started with Your Fiber Guardian

Working with the Fiber (Patchcord) Management Tray

4. Position a plastic fiber clip as shown below, and snap it into the desired clip hole, depending on the configuration that you want to use.

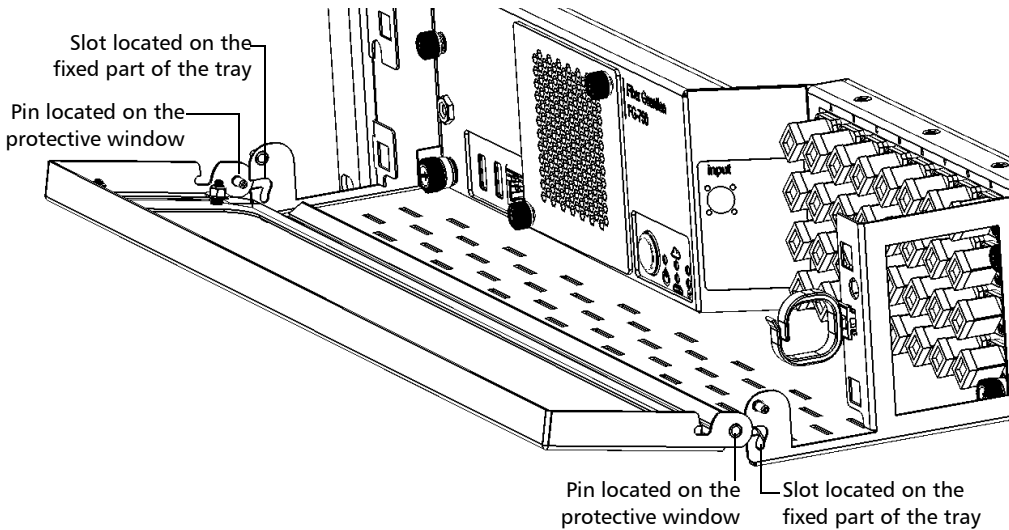


5. Repeat the previous step with all the fiber management clips that you want to install (maximum of five clips in all).

Getting Started with Your Fiber Guardian

Working with the Fiber (Patchcord) Management Tray

6. Install the protective window as follows:
 - 6a. Hold the protective window so that you see its flat side.
 - 6b. Carefully align the pins of the protective window with the slots on the fixed part of the tray.

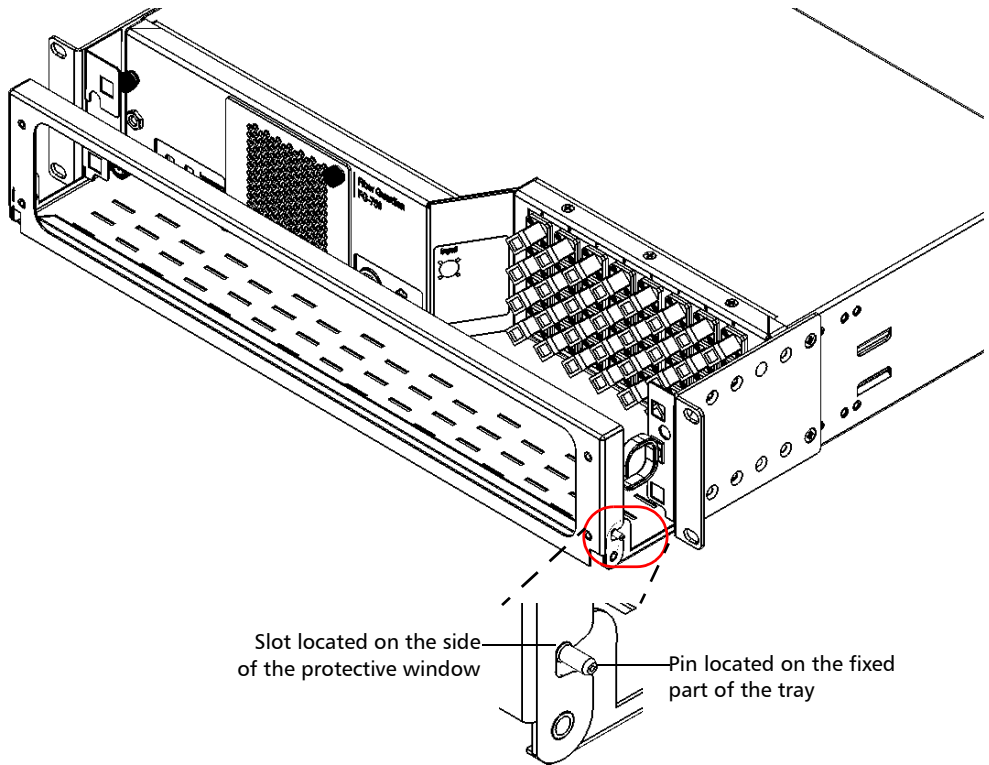


- 6c. Slide the pins of the protective window all the way down into the slots.

Getting Started with Your Fiber Guardian

Working with the Fiber (Patchcord) Management Tray

- 6d.** Position the protective window vertically, and push it slightly so that the slot on each side of the window rests on the corresponding pin on the tray.



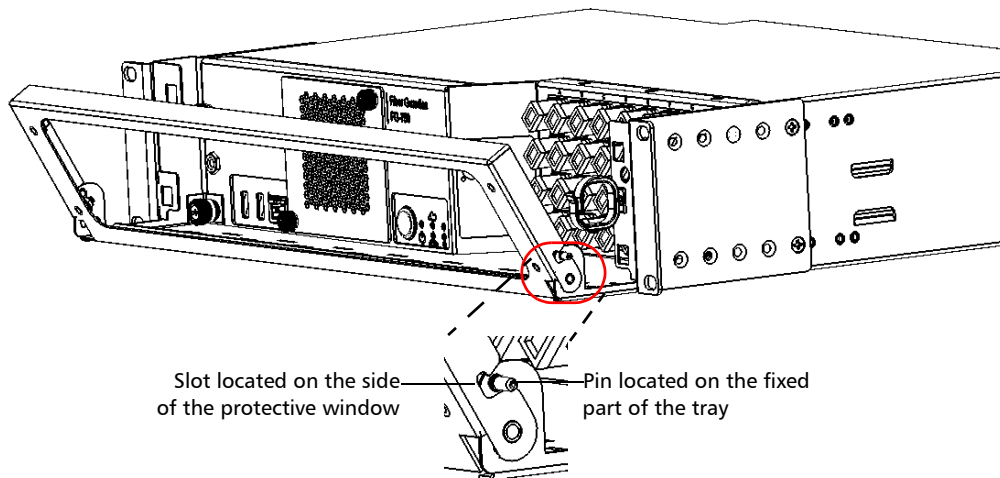
Your fiber management tray is now installed properly. You will simply need to slide the fibers into the fiber management clips when you are ready to use the tray.

Getting Started with Your Fiber Guardian

Working with the Fiber (Patchcord) Management Tray

To fold down the protective window:

1. Slightly pull the protective window upwards to release it from its seated position.



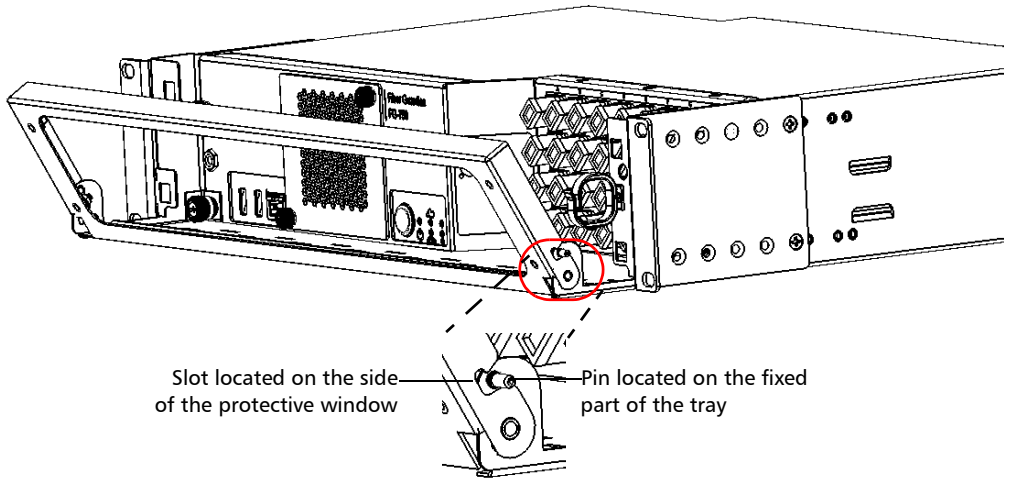
2. Once the protective window can move freely, fold it all the way down until it stops.

Getting Started with Your Fiber Guardian

Working with the Fiber (Patchcord) Management Tray

To remove the protective window:

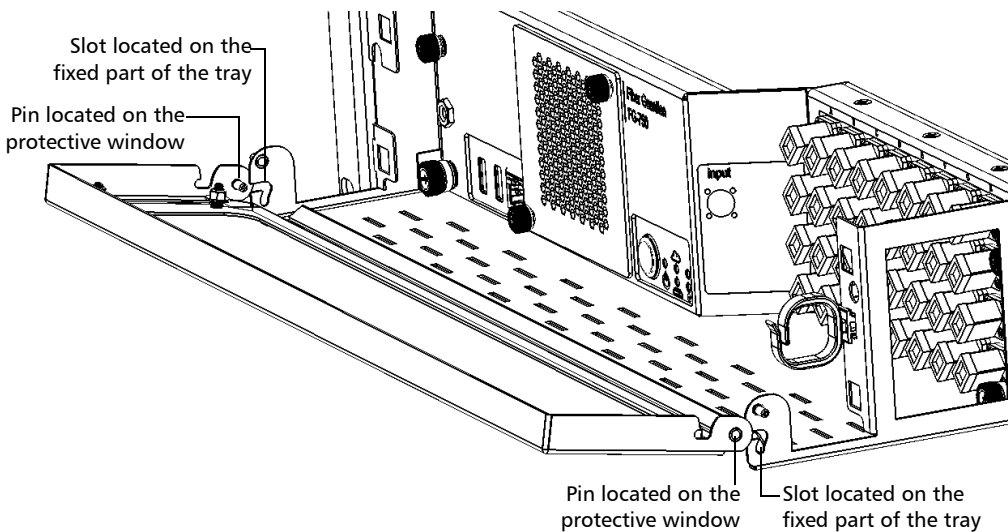
1. Slightly pull the protective window upwards to release it from its seated position.



Getting Started with Your Fiber Guardian

Working with the Fiber (Patchcord) Management Tray

2. Once the protective window can move freely, position the window so that you can slide the pins of the protective window all the way out of their slots.



Connecting the Power and the Network Cables

Before starting to work with your unit, you must connect the power. You may also wish to connect the LAN/WAN network cable, especially if you intend to install your unit in a rack. You can also connect a network cable for local access to the unit (front port).

The Fiber Guardian is available with either AC or DC power supplies. The unit has redundant AC or redundant DC power modules. To benefit from this redundancy, be sure to connect both power supplies, each to a separate circuit.



WARNING

- A certified over-current protecting device that is suitably rated must be installed at the source.
- All electrical installation and accessories must be done and selected as per local electrical code and regulation.

As soon as you connect the unit to a power source, the Baseboard Management Controller (BMC) starts its initialization. During this operation, the LEDs on the front panel will be lit in the following sequence:

- All LEDs will turn to yellow for about 40 seconds.
- All the LEDs will turn off for about 5 seconds.
- Finally, the power LED (🔌) will turn to blinking green, indicating that the BMC is now ready (unit is in standby).

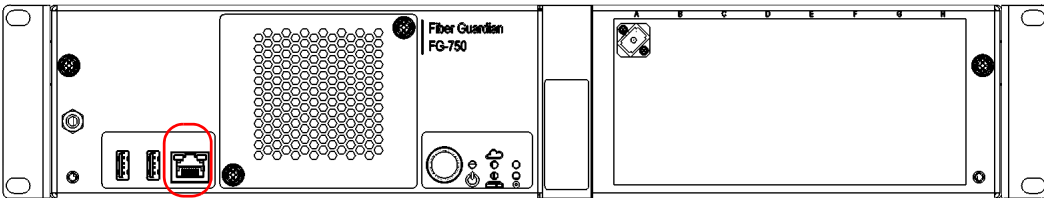
Note: *Your unit has been designed to restart automatically when the power comes back after a power outage. However, in this case, the initialization sequence will differ from the usual initialization sequence explained above. For detailed information about the LEDs, see LED Indicators Description on page 300.*

Getting Started with Your Fiber Guardian

Connecting the Power and the Network Cables

To connect the network cables:

1. To be able to operate the NQMS and REST commands via the LAN/WAN, connect one end of a network cable to the Ethernet port located at the back of your unit. Connect the other end of the cable to the network itself.
2. If you need a local access to the unit, connect one end of a network cable to the Ethernet port located at the front of your unit. Leave the other end of the cable free for future connections with a portable computer.



To connect the power to AC power supplies:

1. Connect the cords to the main power inlets located at the back of the unit.
2. Connect the other end of the cords to the power sources.

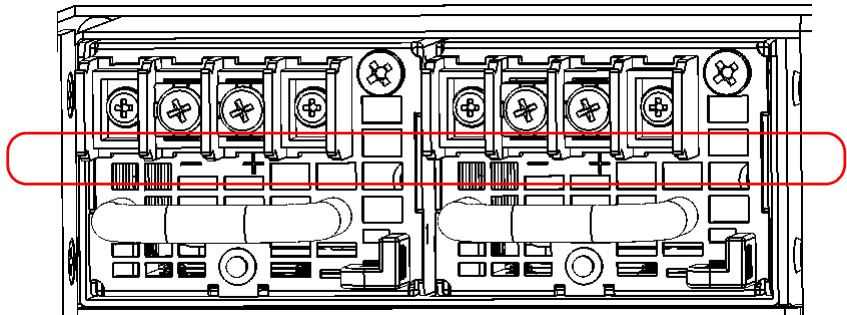
As soon as the initialization sequence is complete (power LED is blinking green), you are ready to turn on the unit (see *Turning On or Off the Unit* on page 48).

To connect the power to DC power supplies:

1. Ensure all power is off or disconnected at the source.

Note: *A certified over-current protection of 5 A must be installed at the power secondary distribution.*

2. Ensure that the unit is grounded properly. For more information, see *Grounding Your Unit* on page 30.
3. Crimp each power lead (minimum 14 AWG) with a UL-listed pressure terminal connector (ring type). The connector must be suitable for 14 AWG wires.
4. Pair the power leads with the appropriate power terminal (located at the back of the unit), respecting the polarity as indicated just below the terminal block.



5. Tighten the screws to attach the power leads to the unit.
6. Turn on the disconnect devices that are connected to the unit.

As soon as the initialization sequence is complete (power LED is blinking green), you are ready to turn on the unit (see *Turning On or Off the Unit* on page 48).

Getting Started with Your Fiber Guardian

Turning On or Off the Unit

Turning On or Off the Unit

As soon as you connect the unit to a power source, the companion starts its initialization. Once the initialization is complete, you can turn on the host. Once the host is on, the operating system will be started automatically. Several components must be initialized before you can actually send commands or connect to the unit.

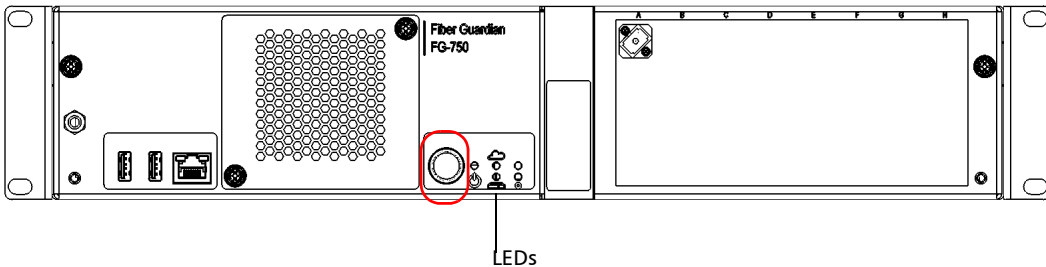
For detailed information about the LEDs, see *LED Indicators Description* on page 300.

Note: You can restart and turn off the host directly from the Host Web UI.

Note: Your unit has been designed to restart automatically when the power comes back after a power outage.

To turn on the host:

Press the power button until the power LED turns to green (non-blinking) and release it.





IMPORTANT

When the host is ready, the system LED turns to green (non-blinking).

When network cables are connected to the unit (front and rear ports), you must wait that the connection be established before the system can be accessed.

- Front port (Static-APIPA): about 60 seconds after the network cable is connected.
- Rear port (DHCP): a few seconds after the operating system is loaded.

There is no visual or audible sign that the connection on the front port is established.

To turn off the host “locally”:

When the unit is on, press the power button for one second and release it.

First, the system LED will turn to blinking green, and then turn off. Finally, the power LED will turn back to blinking green (standby mode), indicating that the host has been shut down properly.

Getting Started with Your Fiber Guardian

Connecting a Monitoring Device to the Dry Contact Relays

To restart the host from the Host Web UI:

1. Connect to the Host Web UI. For more information, see *Accessing and Exiting the Host Web UI* on page 109.
2. From the main menu, select **Actions > Restart Host**.
3. When the application prompts you to confirm the action, click **Yes**.

To turn off the host from the Host Web UI:

1. Connect to the Host Web UI. For more information, see *Accessing and Exiting the Host Web UI* on page 109.
2. From the main menu, select **Actions > Turn Off Host**.
3. When the application prompts you to confirm the action, click **Yes**.

Note: *Once the unit has been shut down, you will have to turn it on manually (by pressing the button on the front panel) to be able to use it.*

Connecting a Monitoring Device to the Dry Contact Relays

Your unit is equipped with dry contact relays that enable you to connect your own monitoring device if you wish to do so.

There are three dry contact relays (— 65 V; 0.46 A) on the back panel of the unit:

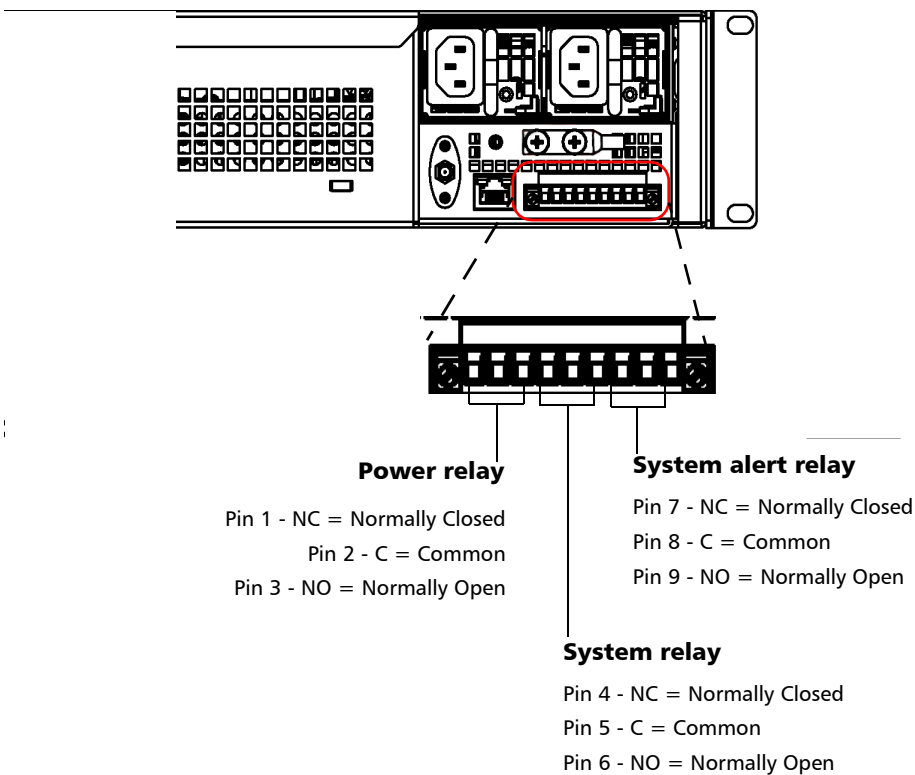
- **Power relay:** Activated when all components related to the host are turned on (the power LED is green and does not blink).
- **System relay:** Activated when the software and hardware (power, fan speed, temperature) are working normally.
- **User-defined relay:** Used for NQMS Optical Route monitoring and is activated when a fault is detected on an optical route.

Getting Started with Your Fiber Guardian

Connecting a Monitoring Device to the Dry Contact Relays

To connect a monitoring device to the dry contact relays:

See the diagram below to determine where you should connect the wires.



Connecting an External Switch

When you need extra switch ports, you can purchase an external switch that you will connect to your FG-750 unit.



WARNING

To avoid serious injuries, always follow all the connection and safety instructions provided with your external switch. If you are working with a Fiber Guardian remote OTAU, see *Safety Information* on page 15 and *Getting Started with Your Fiber Guardian* on page 25.



CAUTION

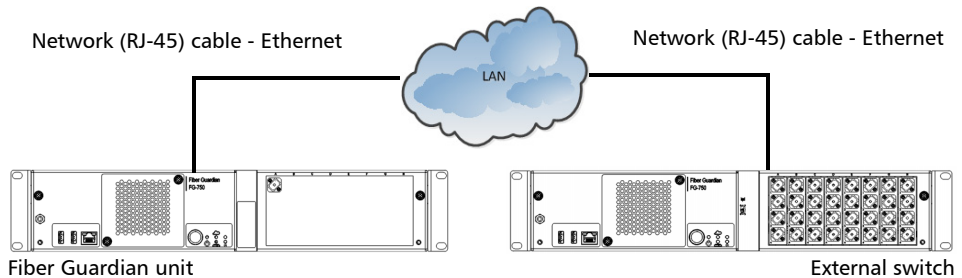
To avoid damaging your unit, use only external switches approved by EXFO with it.

For other models of external switches, if you need information on the connection procedures, the location of the various ports, or the configuration of the IP address, refer to the documentation that came with your switch.

To connect an external switch to your unit:

1. Connect one network cable to the rear Ethernet port of your unit, and one network cable to the LAN Ethernet port of the external switch.

Note: *If you are not sure which port to use, refer to the documentation that came with your external switch for the exact location of the LAN Ethernet port.*

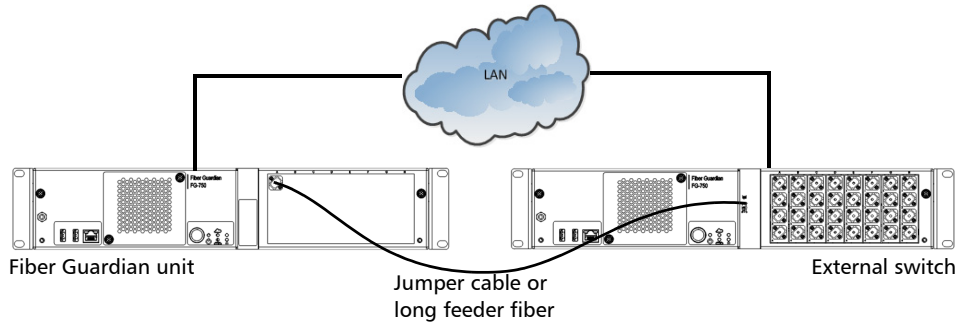


2. Connect both network cables to the same network (LAN).

Getting Started with Your Fiber Guardian

Connecting an External Switch

3. Connect one end of a jumper cable (or of a long feeder fiber) to the OTDR port (units without switch ports), or to any switch port of your choice on your Fiber Guardian unit.



4. Connect the other end of the jumper cable (or of the long feeder fiber) to the input port of the external switch.

Note: Depending on the external switch that you have, the input port may be labelled differently (master port, common port, etc.) or located at the back of the unit. Refer to the user documentation that came with your external switch for more information.

Note: Using a long feeder fiber will incur more attenuation, which will have to be taken into account when calculating the maximum OTDR reach.

Note: It is possible to cascade external switches. You would simply need to connect one port of an already connected switch to the input port of the external switch to add.

Retrieving the IP Address of the Rear Ethernet Port (Host and Companion)

Before starting to work with the Web user interfaces or the provided REST commands, you need to retrieve the IP address of the Ethernet port located on the back panel of the unit.



IMPORTANT

Keep the IP address of the rear Ethernet port to a safe location. You will need it later for most of the operations on your unit. While you retrieve the host IP address, it is a good idea to retrieve the address of the Companion as well to make sure that you have this information should you need to troubleshoot your system and temporarily lose access.

You will need to:

- Connect a portable computer to your unit via the Ethernet port located on its front panel.
- Enter the IP address of the front Ethernet port of the unit and provide it in the connection settings on the computer.
The (static) IP address is *https://169.254.10.10*.

Note: *Additional steps will be required because the SSL connection can not be trusted. The specific steps are different from Chrome to Firefox and IE.*

- Enter the appropriate user name when the Host Web UI prompts you.
 - The user name that you should enter is *Admin*.
 - The password is *Admin*.

The procedure below will guide you through the necessary steps.

Getting Started with Your Fiber Guardian

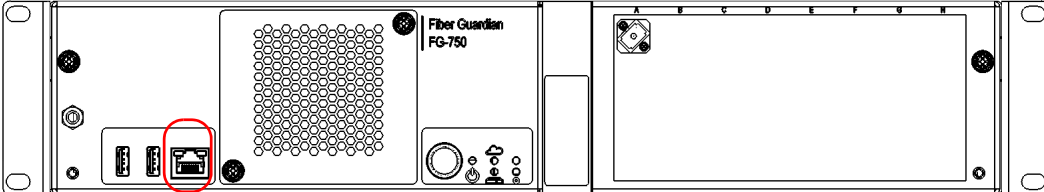
Retrieving the IP Address of the Rear Ethernet Port (Host and Companion)

To retrieve the IP address of the rear Ethernet port:

1. If necessary, turn on your unit. If the unit was not turned on yet, see *Turning On or Off the Unit* on page 48 for more information on the startup sequence and waiting time.

Note: *It may take a few minutes before your unit and the computer could “see” each other.*

2. Connect your portable computer to the front Ethernet port of the unit.
 - If you have already connected a network cable to your unit, simply connect the free end of the cable to your computer.
 - Otherwise, connect a network cable between the unit (front port) and your computer. You will have to wait about 60 seconds that the detection of the port is complete once the operating system is started.

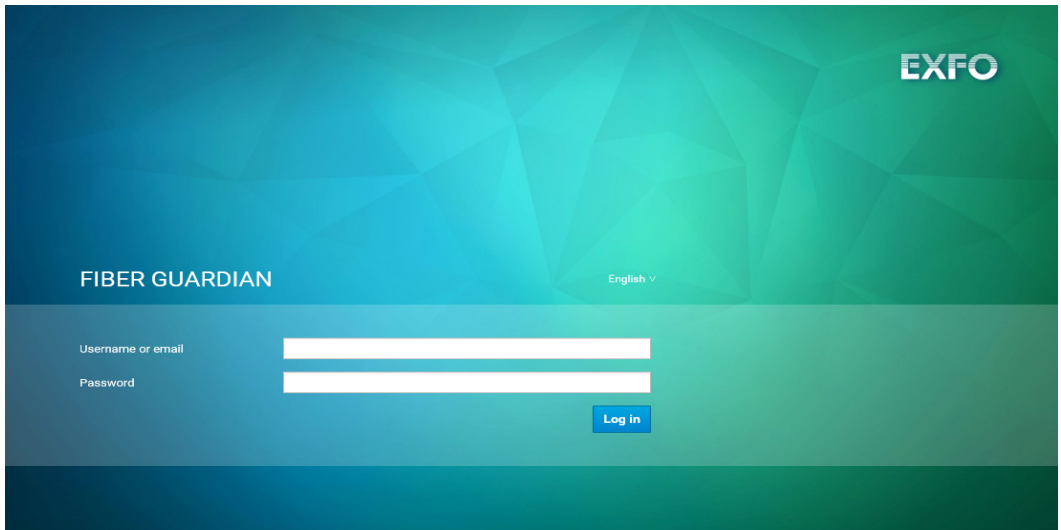


3. Turn on your computer.

Getting Started with Your Fiber Guardian

Retrieving the IP Address of the Rear Ethernet Port (Host and Companion)

4. Connect to the Host Web UI as follows:
 - 4a. From your computer, open a Web browser.
 - 4b. Go to the welcome page of the console URL at <https://169.254.10.10/HostWebUI>.

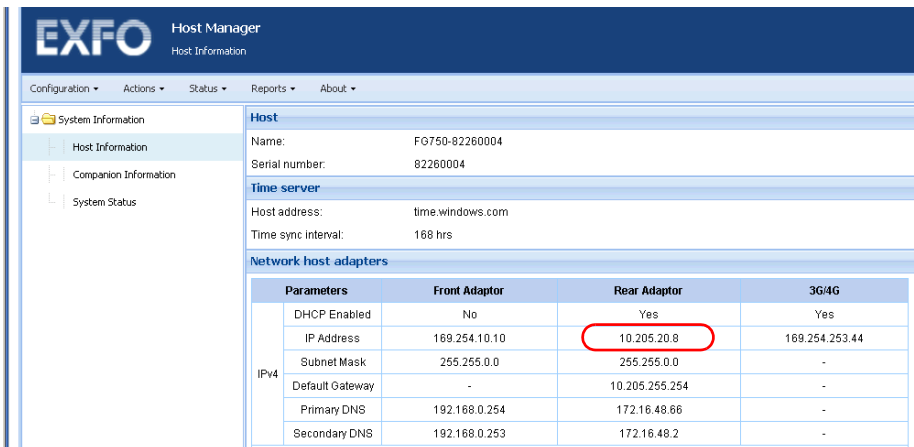


- 4c. Enter your **Username or email** and **Password**.
5. In the Host Web UI, from the main menu, select **Configuration**, then under **System Information**, select **Host Information**.

Getting Started with Your Fiber Guardian

Retrieving the IP Address of the Rear Ethernet Port (Host and Companion)

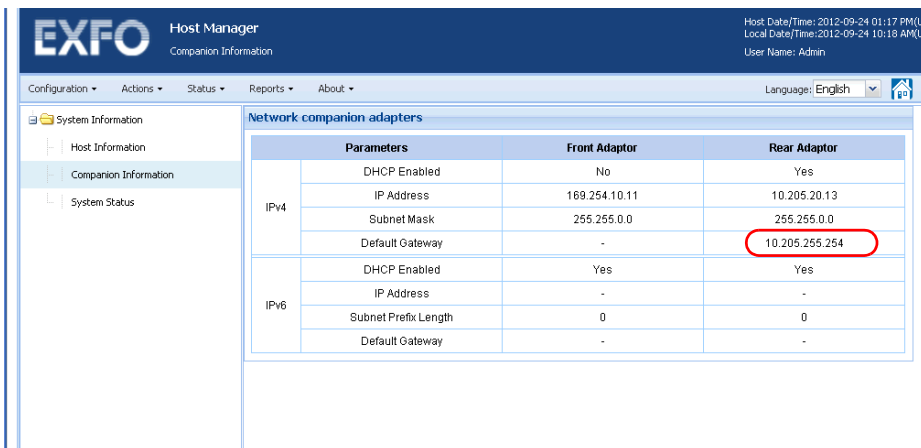
6. Go to the **Rear Adaptor** column and write down the IP address of the rear port.



The screenshot shows the EXFO Host Manager interface. The left sidebar contains 'System Information', 'Host Information', 'Companion Information', and 'System Status'. The main content area is titled 'Host Information' and includes sections for 'Host', 'Time server', and 'Network host adapters'. The 'Network host adapters' section contains a table with columns for 'Parameters', 'Front Adaptor', 'Rear Adaptor', and '3G4G'. The 'Rear Adaptor' column has the IP address '10.205.20.8' circled in red.

Parameters	Front Adaptor	Rear Adaptor	3G4G
DHCP Enabled	No	Yes	Yes
IP Address	169.254.10.10	10.205.20.8	169.254.253.44
Subnet Mask	255.255.0.0	255.255.0.0	-
Default Gateway	-	10.205.255.254	-
Primary DNS	192.168.0.254	172.16.48.66	-
Secondary DNS	192.168.0.253	172.16.48.2	-

7. Select **Companion Information**, then go to the **Rear Adaptor** column and write down the IP address of the rear port.



The screenshot shows the EXFO Host Manager interface with 'Companion Information' selected. The left sidebar contains 'System Information', 'Host Information', 'Companion Information', and 'System Status'. The main content area is titled 'Companion Information' and includes a section for 'Network companion adapters'. The 'Network companion adapters' section contains a table with columns for 'Parameters', 'Front Adaptor', and 'Rear Adaptor'. The 'Rear Adaptor' column has the IP address '10.205.255.254' circled in red.

Parameters	Front Adaptor	Rear Adaptor
DHCP Enabled	No	Yes
IP Address	169.254.10.11	10.205.20.13
Subnet Mask	255.255.0.0	255.255.0.0
Default Gateway	-	10.205.255.254
DHCP Enabled	Yes	Yes
IP Address	-	-
Subnet Prefix Length	0	0
Default Gateway	-	-

8. Once it is done, close the Web browser.
9. Disconnect the network cable from your computer.

Preparing Your Unit for 3G/4G Access

Wireless interface is offered for enabling remote access to the equipment over a VPN (one VPN software is proposed and tested working for this capability), but primary for receiving text messages (that is SMS) when used in OTDR mode. If your unit is equipped with the optional 3G/4G feature, it can switch to the wireless network automatically when the wired network is down. Depending on which type of optional package you have purchased, it includes:

- an internal wireless communication module and a remote low-profile antenna with extension cable
- an internal wireless communication module, an SMA Connector saver/extender and a dipole swivel antenna

Note: *If the 3G/4G signal is not strong enough where your unit is installed, the low-profile antenna will provide you with a stronger coverage.*

By default, your unit is configured to connect automatically to the wireless network but you can deactivate this feature if you prefer. You can also specify a maximum number of minutes during which the unit can remain connected to the wireless network. EXFO uses a generic firmware working on most opened wireless networks, or in roaming mode. Available interfaces are LTE, HSPA+ and UMTS.

When you receive your unit, it contains no Subscriber Identity Module (SIM) card and the antenna is not connected. This means that you will need to do the following:

- Purchase a compatible and unlocked SIM card from a provider offering 3G/4G services. If you need more information on the 3G/4G coverage in your area, contact your regional EXFO sales representative.
- Have the card activated (you must subscribe to a package of mobile services).
- Connect the antenna to your unit.

Getting Started with Your Fiber Guardian

Preparing Your Unit for 3G/4G Access

- Insert the SIM card in your unit.
- Configure the 3G/4G parameters via the Web UI.

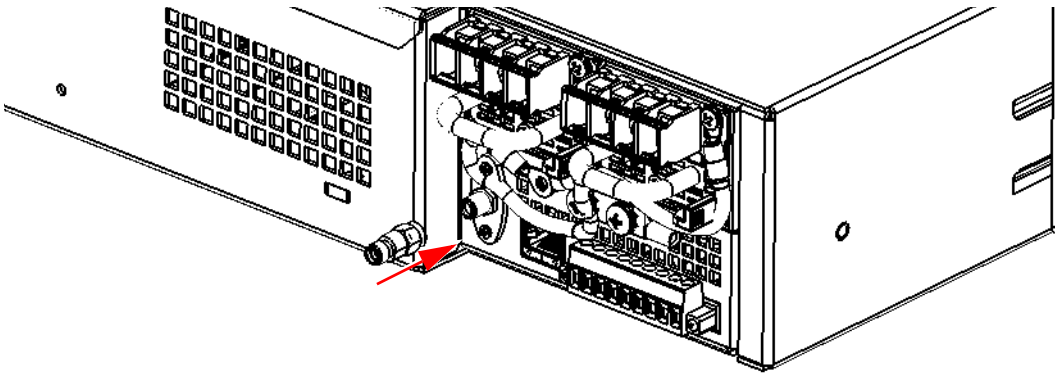
To connect the remote low-profile antenna to your unit:

1. Gently screw the antenna's connector to the 3G/4G port.
2. Position the antenna as needed for a maximum reception of the signal.

The antenna is ready to use.

To connect the dipole swivel antenna and SMA connector saver/extender to your unit:

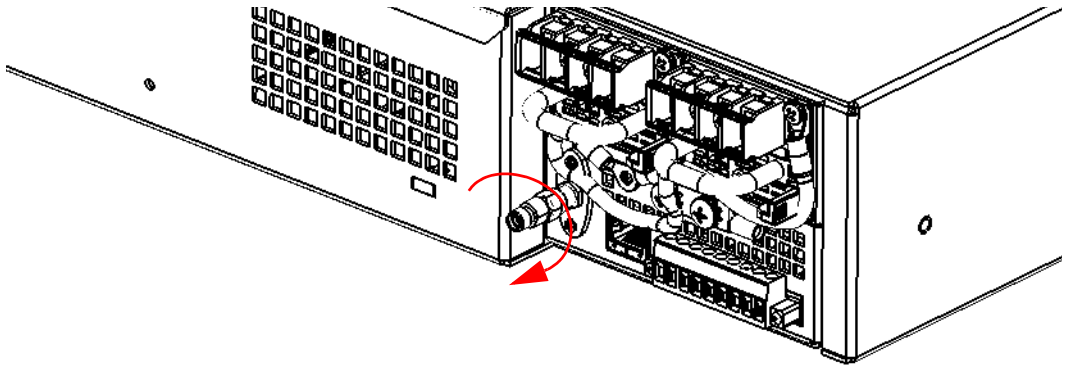
1. Gently screw the SMA connector saver/extender to the antenna's 3G/4G port. This will add clearance necessary for the antenna.



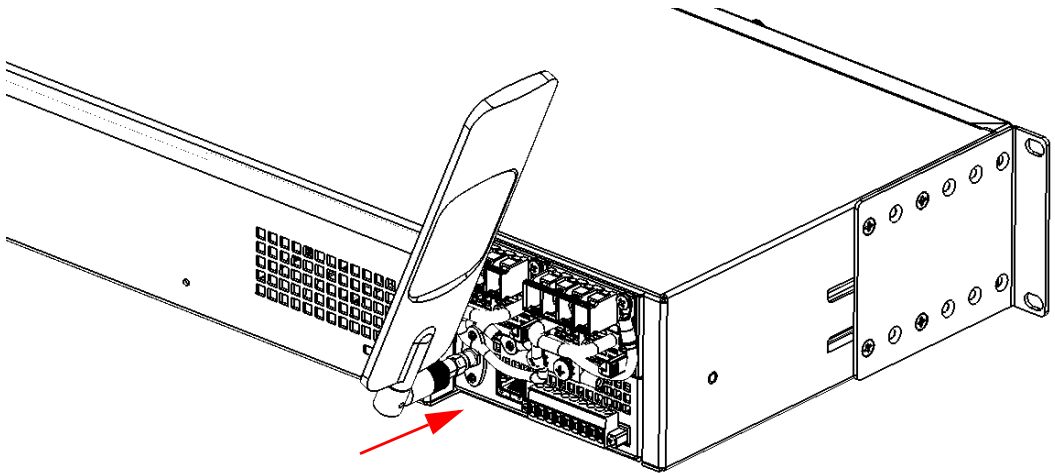
Getting Started with Your Fiber Guardian

Preparing Your Unit for 3G/4G Access

2. Firmly tighten the SMA connector saver/extender to the antenna's 3G/4G port.



3. Carefully align the connector of the antenna with the 3G/4G port on your unit and push the antenna gently towards the unit until it stops.



4. Gently screw the antenna's connector to the 3G/4G port.
5. Position the antenna as needed for a maximum reception of the signal.
The antenna is ready to use.

Getting Started with Your Fiber Guardian

Preparing Your Unit for 3G/4G Access



WARNING

To avoid serious injuries as well as irreparable damage to your unit, always remove both power cords before opening or servicing the unit.



CAUTION

To avoid damaging your unit or its components, you should wear an antistatic band during this maintenance operation. For more information, see *Preventing Electrostatic Discharge Damage* on page 25.



CAUTION

If you are using a 3G/4G antenna with cable, depending on your setup, you may have to install a lightning protection system between your Fiber Guardian unit and the cable's antenna. Failure to provide adequate lightning protection may lead to irreparable damage to your unit.

To insert the SIM card in your unit:



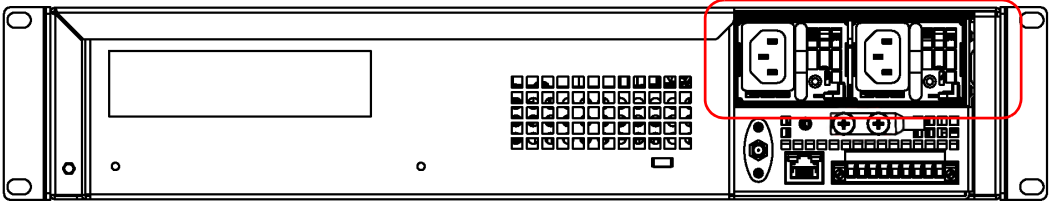
IMPORTANT

You **MUST** remove the power cord so that the hardware detects the SIM card. Rebooting the RTU (including the BMC) is *not* enough.

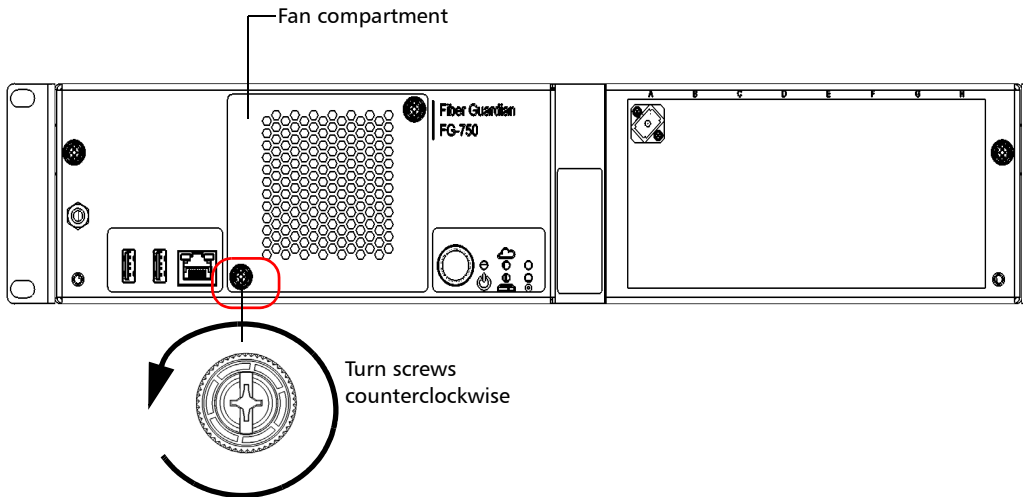
Getting Started with Your Fiber Guardian

Preparing Your Unit for 3G/4G Access

1. Turn off the unit and disconnect it completely from the power sources.



2. Put on an antistatic strap and connect it to the connector provided for that purpose on the front panel of the unit.
3. Turn the fan compartment screws counterclockwise until the compartment is loose. Since the screws are captive screws, you cannot remove them completely.



Getting Started with Your Fiber Guardian

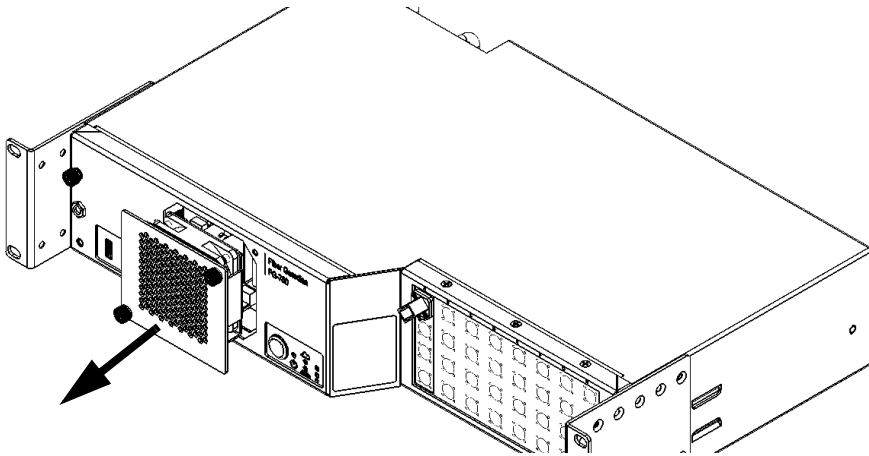
Preparing Your Unit for 3G/4G Access



CAUTION

To avoid dropping the fan compartment and damaging the unit, the fan, or the fan cord, hold the fan compartment firmly. Do not allow the fan compartment to hang over the edge of a rack or a table.

4. Using the screws as handles, gently pull away the fan compartment.



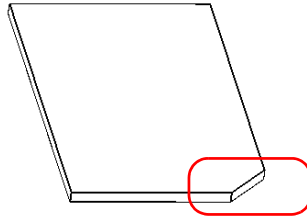
CAUTION

To prevent damage to your SIM card, avoid touching its gold area.

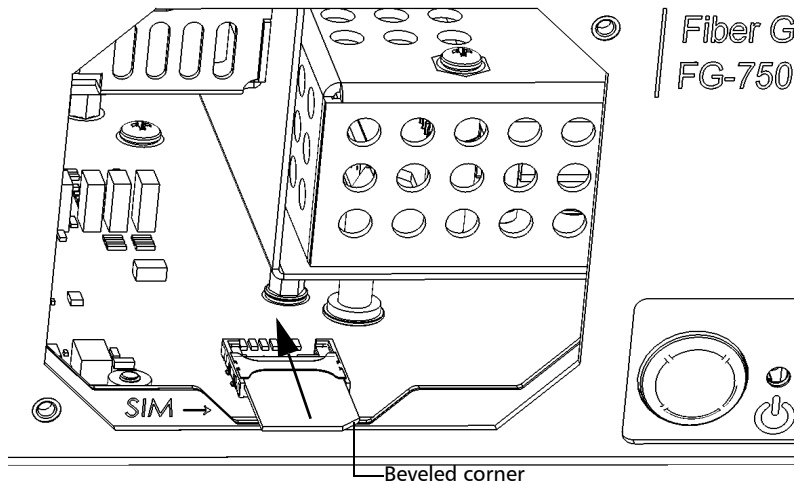
Getting Started with Your Fiber Guardian

Preparing Your Unit for 3G/4G Access

5. Hold the SIM card so that the gold area is facing down and that the beveled corner is on the right.



6. Slide the SIM card into the unit's SIM card slot, and push it all the way to the back of the card slot.



Getting Started with Your Fiber Guardian

Preparing Your Unit for 3G/4G Access

- 7.** Put the fan compartment back in its bay (it should be flush with the unit's front panel).
- 8.** Turn the fan compartment screws clockwise until the compartment is secured into place.
- 9.** Remove your antistatic strap.
- 10.** Reconnect the unit to its power sources (turn on both disconnected devices) and turn on your unit.

Note: *Successfully restarting your unit ensures that the SIM card is properly detected. You MUST remove the power cord and wait a few minutes for the capacitors to discharge before restarting your unit to ensure that the SIM card is properly detected. You will then be ready to configure the 3G/4G parameters.*

To configure the 3G/4G parameters:

Log on to the Web UI and configure the 3G/4G parameters. For more information on the configuration of these parameters, see *Configuring the 3G/4G Settings* on page 115.

Your unit is now ready to switch to the wireless network whenever the wired network is down.

Operating the RTU through SMS

The RTU can be operated by sending an SMS with appropriate commands in the SMS. The mobile number from which these commands are sent should be a valid mobile number of an existing RTU user. If the command is not valid then the RTU will send an SMS to the sender with the following text: <Command Text> is not a valid command. Messages are sent only to users in the system.

SMS Command Format to Resume/Suspend an OR (Optical Route)

P[OR-Port Name]R[ROTAU-Port Number][C or X]

For example:

- To Resume OR - on port A,2: PA,2C
- To Suspend OR - on port A,2: PA,2X
- To Resume OR - on port A,2 R005: PA,2R5C
- To Suspend OR - on port A,2 R005: PA,2R5X
- To Suspend all ORs: X
- To Resume all ORs: C

SMS Command Format for Running an OnDemand Test

P[OR-Port Name]R[ROTAU-Port Number]T[Test Setup-Index if test setups are sorted in alphabetical order for an Optical Route]

For example:

If 2 test setups exist, for example, Monitoring and Proactive maintenance on port - A,2 - then the commands are as follows:

- Command to start an OnDemand Test on a test setup Proactive maintenance:

PA,2T2

Note: *The index of a test setup is the sequence number of a test setup when all test setups of an Optical Route are sorted by **Testsetup Name**. Here the index for Proactive maintenance is 2.*

- Command to start an OnDemand Test on a test setup Proactive maintenance if it belongs to ROTAU port - A,2 R004:

PA,2R4T2

Preparing to Access Your Unit via a WAN or the Internet

When your computer and your unit are connected to a same WAN or to the Internet, you can access your unit remotely with your computer. The connection is made possible by the use of a Virtual Private Network (VPN). If you have purchased the 3G/4G option, the unit will also use a VPN to connect to the wireless network when the wired network is down.



IMPORTANT

EXFO does not provide licenses for any VPN client or server applications. You can use any VPN application supporting data transfer over a 3G/4G wireless network.

The information hereafter is for guidance purposes only. The installation and use may differ for VPN applications other than LogMeIn Hamachi. If you are not sure how to proceed, contact your network administrator.

Contact Hamachi to ensure that you can use a free version of the LogMeIn Hamachi application or to purchase a license.

Before being able to work with a VPN, you must:

- Install the LogMeIn Hamachi VPN client application on your computer.
- Create your own VPN on the Hamachi server.
- Install the LogMeIn Hamachi client on your unit.

The VPN that you will create will serve as a “connection” point between your computer and your unit. You will need to use the Hamachi VPN client application to connect to this new VPN.

Your unit must have access to the Internet to be able to configure it on the Hamachi server.

Getting Started with Your Fiber Guardian

Preparing to Access Your Unit via a WAN or the Internet



IMPORTANT

You cannot install the VPN client on the unit via a WAN or the Internet. You must either connect a portable computer (DHCP adapter) to the front port of the unit, or connect both the unit and a computer to a same LAN.

To install the LogMeIn Hamachi VPN client on your computer:

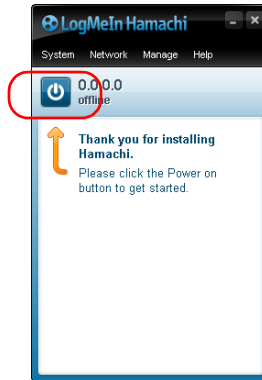
1. On your computer, open a Web browser and go to <https://secure.logmein.com/products/hamachi/download.aspx>.
2. Download (save) the LogMeIn Hamachi VPN client application (installation file) to your computer.
3. Double-click the installation file that you have just downloaded to start the installation.
4. From the first window, select the desired language and click **Next**. Follow the on-screen instructions.



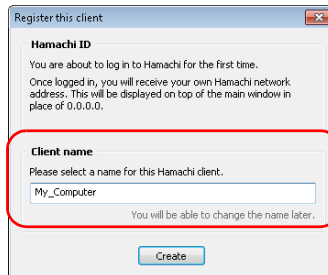
Getting Started with Your Fiber Guardian

Preparing to Access Your Unit via a WAN or the Internet

5. When the installation is complete, from the **LogMeIn Hamachi** window, click the *Power on* button to establish a connection with the Hamachi server.



6. Under **Client name**, enter a name that will enable you to easily identify your computer later.



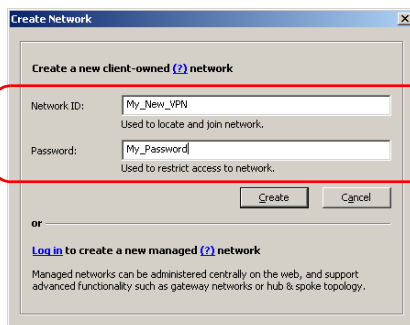
Getting Started with Your Fiber Guardian

Preparing to Access Your Unit via a WAN or the Internet

7. Click **Create** to confirm the name and send a request for an address on the Hamachi server.
8. Since no VPN has been created yet, create one as follows:
 - 8a. Click **Create a new network**.



- 8b. Enter a network ID and a password for your VPN.

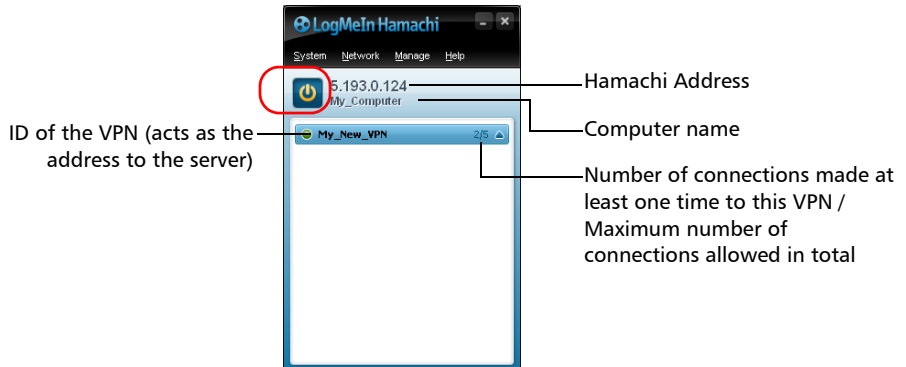


Getting Started with Your Fiber Guardian

Preparing to Access Your Unit via a WAN or the Internet

8c. Click **Create** to complete the process.

8d. Once the VPN is created, click the *Power off* button and close the window.



Note: *Even though the VPN has been created from your computer, it is hosted on the Hamachi server, not on your computer directly.*

Getting Started with Your Fiber Guardian

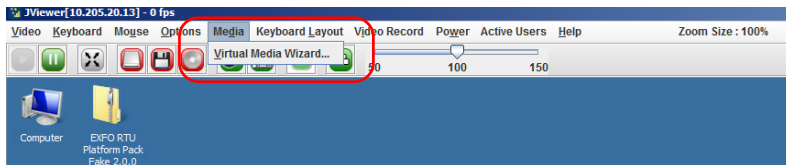
Preparing to Access Your Unit via a WAN or the Internet

To install the LogMeIn Hamachi VPN client on your unit:

1. Transfer the installation file to your unit from your computer.

Note: *Once the transfer is complete, you can go to step 2.*

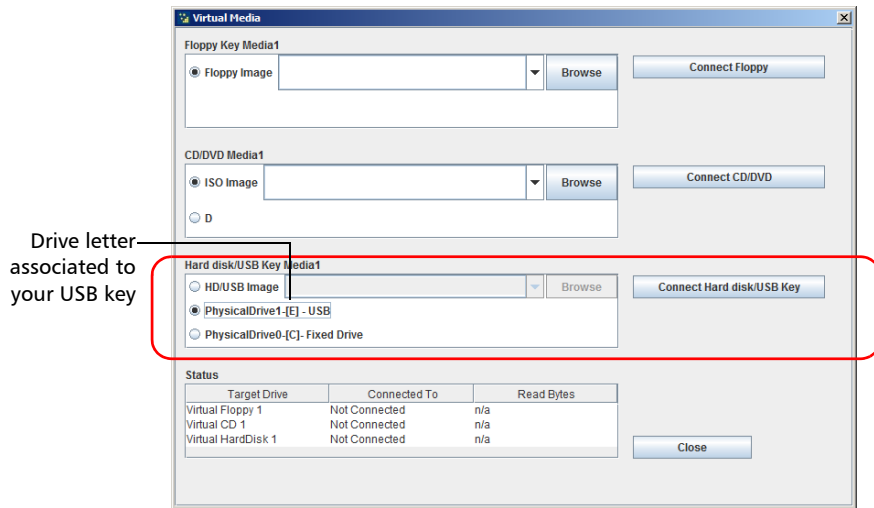
- 1a. Connect a USB key to your computer and copy the LogMeIn Hamachi installation file to your key.
- 1b. From your computer, connect to your unit using the KVM remote console. For more information, see *Connecting to Your Unit Using the KVM Remote Console* on page 308.
- 1c. In the Remote Console, from the main menu, select **Media > Virtual Media Wizard**.



Getting Started with Your Fiber Guardian

Preparing to Access Your Unit via a WAN or the Internet

- 1d.** Under **Hard disk/USB Key Media 1**, select your USB key from the list. The drive letter associated with your USB key in this application should be exactly the same as you could see under Windows if you would open a file explorer on your computer.



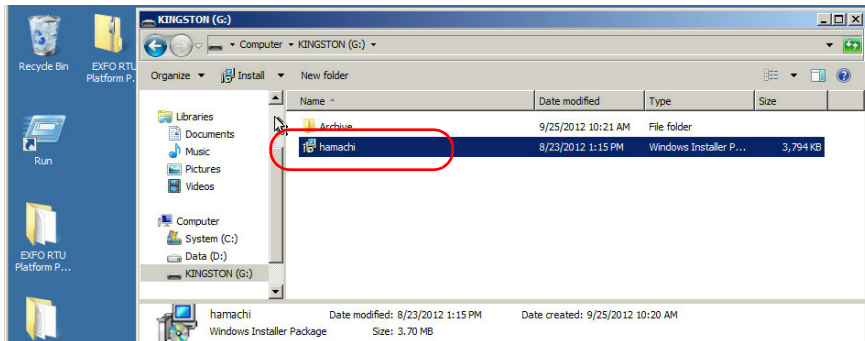
- 1e.** Click **Connect Hard disk/USB Key**.

- 1f.** Click **Close**.

Getting Started with Your Fiber Guardian

Preparing to Access Your Unit via a WAN or the Internet

- 1g.** In the Remote Console, from **Computer**, double-click the USB key to view its content.
- 1h.** Copy the LogMeIn Hamachi installation file and paste it to the desktop (or the folder of your choice) of your unit.



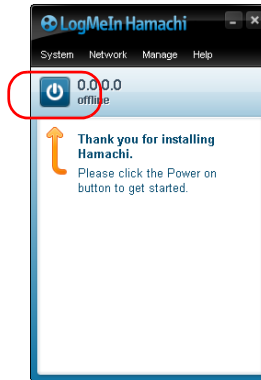
- 2.** Double-click the installation file that you have just copied to start the installation.
- 3.** From the first window, select the desired language and click **Next**. Follow the on-screen instructions.



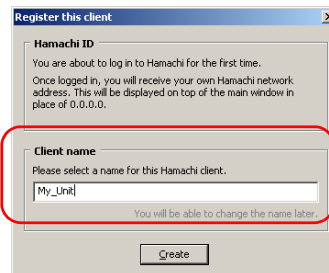
Getting Started with Your Fiber Guardian

Preparing to Access Your Unit via a WAN or the Internet

4. When the installation is complete, from the **LogMeIn Hamachi** window, click the *Power on* button to establish a connection with the Hamachi server.



5. Under **Client name**, enter a name that will enable you to easily identify your unit later.



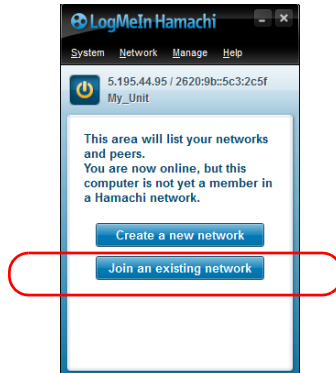
6. Click **Create** to confirm the name and send a request for an address on the Hamachi server.

Getting Started with Your Fiber Guardian

Preparing to Access Your Unit via a WAN or the Internet

7. Once the connection is established, from the **LogMeIn Hamachi** window, connect to the VPN that you have created earlier.

7a. Click the **Join an existing network** button.



7b. Enter the ID of your VPN and the corresponding password.

7c. Confirm with **Join**.



IMPORTANT

Do not leave the VPN (network) and do not log off from the Hamachi server from your unit.
Do not close the LogMeIn Hamachi window with the *Power off* button. Otherwise, you will not be able to access your unit from a WAN or the Internet later.

7d. Close the window with the  button (not the *Power off* button).

You are now able to access your unit from your computer via a WAN or the Internet.

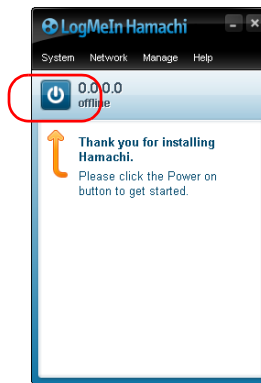
Connecting to the VPN

When your computer and unit are both connected to a WAN or the Internet, you need to join the VPN from your computer and to retrieve the LogMeIn address of your unit before being able to connect to the Host Web UI or the Line Configuration Web UI.

The VPN client must be installed on both your computer and your unit already. For more information on how to install the VPN client, see *Preparing to Access Your Unit via a WAN or the Internet* on page 69.

To connect to the VPN:

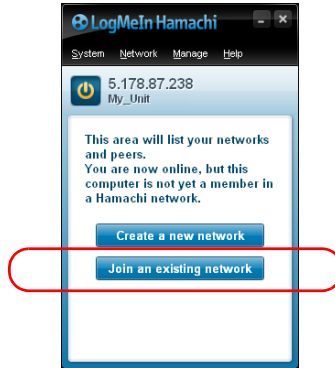
1. From your computer, start the LogMeIn Hamachi client application.
2. Click the *Power on* button to establish a connection with the Hamachi server.



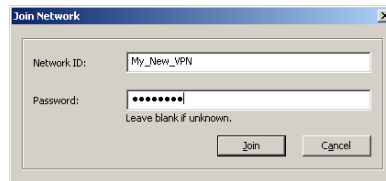
Getting Started with Your Fiber Guardian

Connecting to the VPN

3. Click the **Join an existing network** button.

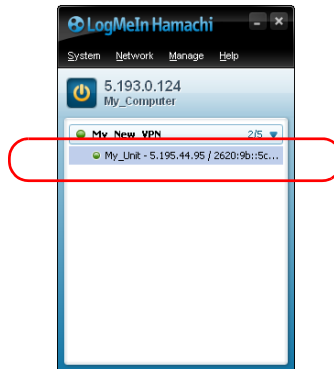


4. Enter the ID of your VPN and the corresponding password.



5. Confirm with **Join**.

6. Write down the Hamachi address (which begins with 5.x) that has been assigned to the unit.



You are now ready to connect to the desired application.

Cleaning and Connecting Optical Fibers



IMPORTANT

To ensure maximum power and to avoid erroneous readings:

- Always inspect fiber ends and make sure that they are clean as explained below before inserting them into the port. EXFO is not responsible for damage or errors caused by bad fiber cleaning or handling.
- Ensure that your patchcord has appropriate connectors. Joining mismatched connectors will damage the ferrules.

To connect the fiber-optic cable to the port:

- 1.** Inspect the fiber using a fiber inspection probe. If the fiber is clean, proceed to connecting it to the port. If the fiber is dirty, clean it as explained below.
- 2.** Clean the fiber ends as follows:
 - 2a.** Gently wipe the fiber end with a lint-free swab dipped in optical-grade liquid cleaner.
 - 2b.** Use a dry swab to dry the connector completely.
 - 2c.** Visually inspect the fiber end to ensure its cleanliness.

3. Carefully align the connector and port to prevent the fiber end from touching the outside of the port or rubbing against other surfaces.

If your connector features a key, ensure that it is fully fitted into the port's corresponding notch.

4. Push the connector in so that the fiber-optic cable is firmly in place, thus ensuring adequate contact.

If your connector features a screw sleeve, tighten the connector enough to firmly maintain the fiber in place. Do not overtighten, as this will damage the fiber and the port.

Note: *If your fiber-optic cable is not properly aligned and/or connected, you will notice heavy loss and reflection.*

EXFO uses good quality connectors in compliance with EIA-455-21A standards.

To keep connectors clean and in good condition, EXFO strongly recommends inspecting them with a fiber inspection probe before connecting them. Failure to do so will result in permanent damage to the connectors and degradation in measurements.

Working with the REST Commands (Certain Models Only)

You can build your own test applications with the provided REST commands. You can refer to the *Using iOLM Measurement Services* and *Using FG-700 Series REST Services* documentation for detailed information.



IMPORTANT

- ▶ The computer that you intend to use to send commands must be connected to the same network as the unit.
- ▶ You must know the IP address of the rear Ethernet port. If you do not know the IP address of the port, see *Retrieving the IP Address of the Rear Ethernet Port (Host and Companion)* on page 55.

It is possible to test the link to the rear Ethernet port by trying to access the REST documentation on the unit.

To access the REST documentation:

1. Connect to the Host Web UI. For more information, see *Accessing and Exiting the Host Web UI* on page 109.
2. From the main menu, select **Actions** > **Applications**.
3. Click the link corresponding to the document that you want to view.

Installing the Notification Agent on Your Computer

The Notification Agent is an application that you can install on any computer that can “view” the RTUs, which usually means that the computer and RTUs are connected to the same network. It monitors one or several RTUs and warns you whenever faults are detected.

To install the Notification Agent on your computer:

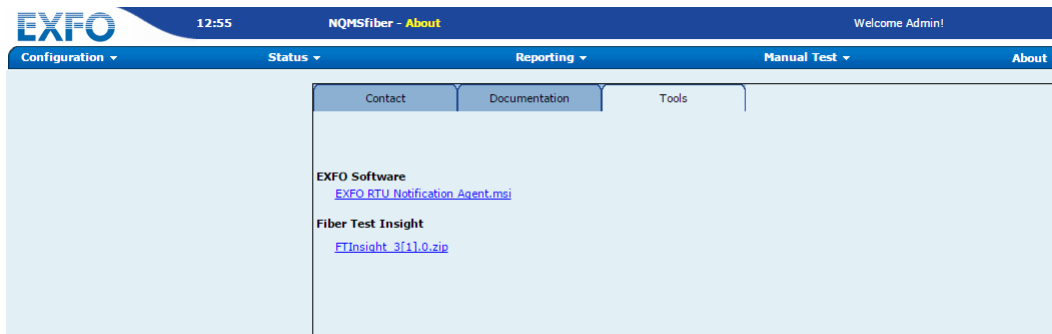
- 1.** Verify if you need to install the .NET Framework 4.0 or higher on your computer as follows:
 - 1a.** From your computer, go to the Control Panel.
 - 1b.** Start Add/Remove Programs.
 - 1c.** From the list of programs that are already installed on your computer, try to locate *Microsoft .NET Framework 4.0* or higher.

If this item is on the list, you do not need to install .NET Framework 4.0 or higher; otherwise, you will need to install it.
- 2.** Start the RTU application (see *Setting Up Your RTU* on page 125).
- 3.** Install the Notification Agent as follows:
 - 3a.** From the main menu of the NqmsWebOtdr2 application, select **About > Tools**.

Getting Started with Your Fiber Guardian

Installing the Notification Agent on Your Computer

- 3b.** Under **EXFO Software**, click the hyperlink to retrieve the necessary file.



- 3c.** Save the file to a location of your choice on your computer.
- 3d.** Double-click the *.msi* file to start the installation and follow the instructions on the screen.

You are now ready to use the Notification Agent. For more information, see *Configuring the Notification Agent* on page 198.

Understanding the Applications, User Accounts and Passwords

There are several ways to interact with your Fiber Guardian unit.

The table below summarizes the information about the different applications as well as the corresponding user names and passwords.

Application	Connection	User Name and Default Password
<p>HostWebUI:</p> <ul style="list-style-type: none"> ➤ To configure the host and companion settings ➤ To monitor the system (event log) 	<ul style="list-style-type: none"> ➤ Computer connected directly to the unit (front port): From your computer, in a Web browser, type: <i>https://Front_Port_IP_Address/HostWebUI</i> ➤ LAN connection: From your computer, in a Web browser, type: <i>https://Rear_Port_IP_Address/HostWebUI</i> ➤ WAN or Internet connection: From your computer (already connected to the VPN), in a Web browser, type: <i>https://LogMeIn_Hamachi_Address/HostWebUI</i> 	<ul style="list-style-type: none"> ➤ User name: Admin ➤ Password: Admin

Getting Started with Your Fiber Guardian

Understanding the Applications, User Accounts and Passwords

Application	Connection	User Name and Default Password
Fiber Guardian (OTDR mode)	<ul style="list-style-type: none">➤ Computer connected directly to the unit (front port): From your computer, in a Web browser, type: <i>https://Front_Port_IP_Address</i>➤ LAN connection: From your computer, in a Web browser, type: <i>https://Rear_Port_IP_Address</i>➤ WAN or Internet connection: From your computer (already connected to the VPN), in a Web browser, type: <i>https://LogMeIn_Hamachi_Address</i>	<ul style="list-style-type: none">➤ User name: Admin➤ Password: Admin

Getting Started with Your Fiber Guardian

Understanding the Applications, User Accounts and Passwords

Application	Connection	User Name and Default Password
<p>Optical lines test Web UI: To link your lines and switch ports according to your tests (in iOLM mode)</p>	<p>In the Host Web UI, from the main menu, select Actions > Applications. Click the link corresponding to the Line Configuration Web UI. OR</p> <ul style="list-style-type: none"> ➤ Computer connected directly to the unit (front port): From your computer, in a Web browser, type: <i>//Front_Port_IP_Address/LineConfiguration</i> ➤ LAN connection: From your computer, in a Web browser, type: <i>//Rear_Port_IP_Address/LineConfiguration</i> ➤ WAN or Internet connection: From your computer (already connected to the VPN), in a Web browser, type: <i>https://LogMeIn_Hamachi_Address/LineConfiguration</i> 	<ul style="list-style-type: none"> ➤ User name: Admin ➤ Password: Admin
<p>List of the REST commands</p>	<p>In the Host Web UI, from the main menu, select Actions > Applications. Click the link corresponding to the list that you want to view.</p>	<ul style="list-style-type: none"> ➤ User name: Admin ➤ Password: Admin
<p>REST documentation</p>	<p>In the Host Web UI, from the main menu, select About > Help. Click the link corresponding to the document that you want to view.</p>	<ul style="list-style-type: none"> ➤ User name: Admin ➤ Password: Admin

Getting Started with Your Fiber Guardian

Understanding the Applications, User Accounts and Passwords

Application	Connection	User Name and Default Password
Your own application using the REST commands	The user name and password must be sent with each command as a “basic authentication” header.	<ul style="list-style-type: none">➤ User name: WebServicesUser➤ Password: WebServicesUser
Direct connection to the unit (in Windows) for troubleshooting and installation of VPN client application.	Via the KVM application (see <i>Connecting to Your Unit Using the KVM Remote Console</i> on page 308).	<ul style="list-style-type: none">➤ User name: Administrator➤ Password: RTUEXFO123

Note: *If you do not know the IP address of the rear Ethernet port, see Retrieving the IP Address of the Rear Ethernet Port (Host and Companion) on page 55.*

Note: *If you do not know the LogMeIn Hamachi address of your unit, or how to connect to the VPN, see Preparing to Access Your Unit via a WAN or the Internet on page 69 and Connecting to the VPN on page 79. If you are using a VPN client application other than LogMeIn Hamachi, see with your network administrator for the specific connection procedure.*

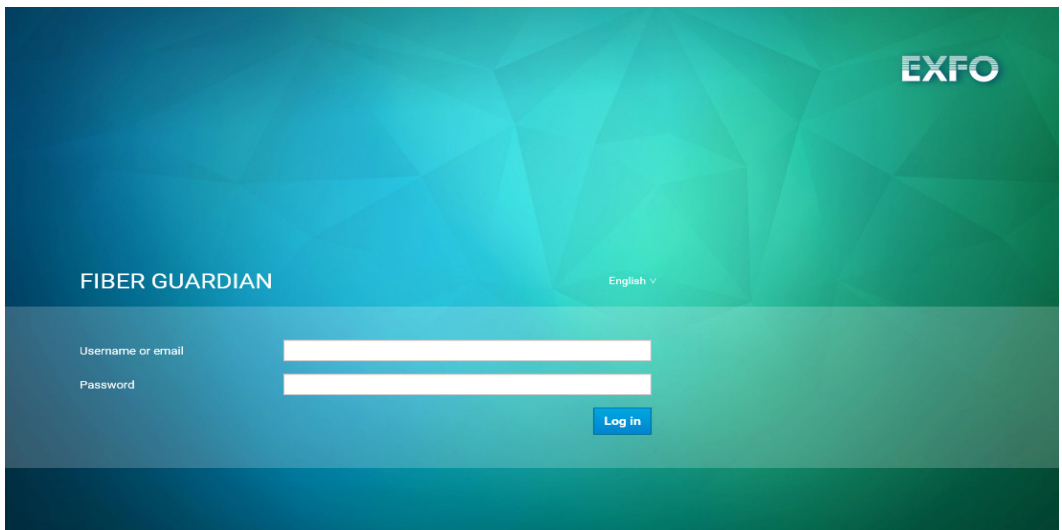
4 *Managing Users*

Introduction

The Fiber console module is an open-source enterprise-class Identity and Access Management (IAM) solution which EXFO has customized and integrated to its Fiber Guardian/NQMSfiber products. It offers simple, secured, and extensive authentication and auditing functions. As a user in a centrally managed installation, you are now authenticated through a single sign-on/out instance which can itself be connected to your existing LDAP (Lightweight Directory Access Protocol) service. For centrally managed solutions, it means one log-on to move from one application (for example, central) to another (for example, local).

Logging in to the Administration Console

1. Go to the welcome page of the console URL at https://RTU_IPAddress.
2. To access the console, use the **Users** menu item in the navigation bar once logged in.



Managing Users

Logging in to the Administration Console

3. Enter your **Username or email** and **Password**. The user Admin Console page opens.

The screenshot shows the EXFO Administration Console interface. The top navigation bar is blue with the EXFO logo on the left and the user 'Admin Admin' on the right. A left sidebar contains a menu with categories: 'Configure' (Realm Settings, Clients, Client Templates, Roles, Identity Providers, User Federation, Authentication), 'Manage' (Groups, Users, Sessions, Events, Import), and 'Fiber' (selected). The main content area is titled 'Fiber' and has a trash icon. Below the title are tabs for 'General', 'Login', 'Keys', 'Email', 'Themes', 'Cache', 'Tokens', 'Client Registration', and 'Security Defenses'. The 'General' tab is active, showing configuration fields: 'Name' (Fiber), 'Display name' (Fiber Guardian), 'HTML Display name' (Fiber Guardian), 'Enabled' (ON), and 'Endpoints' (OpenID Endpoint Configuration). 'Save' and 'Cancel' buttons are at the bottom.

Note: *If you are curious about a certain feature, button, or field within the Admin Console, hover your mouse over the question mark ? icon. This will pop up tooltip text to describe the area of the console you are interested in.*

Realm Settings

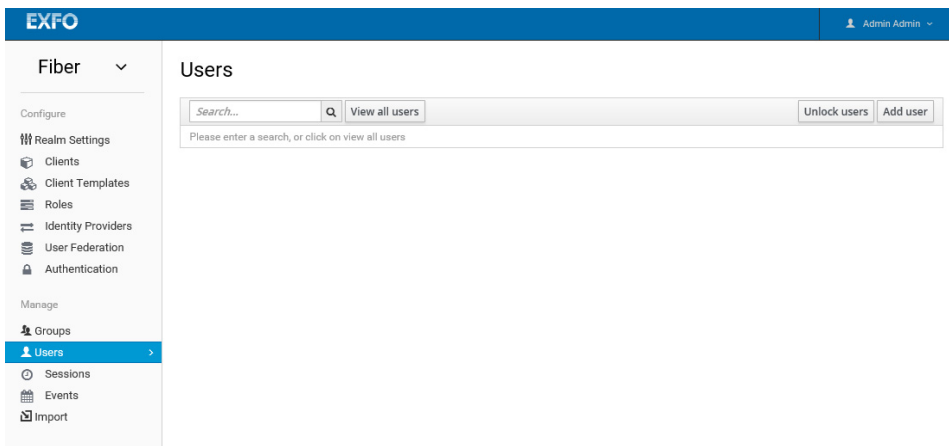
A realm manages a set of users, credentials, roles, and groups. A user belongs to and logs into a default realm named **fiber**, display name **Fiber Guardian Management System**. Realms are isolated from one another and can only manage and authenticate the users that they control. For all standard installs, only one realm is to be used.

Roles

Roles are configured at the realm level and identify a type or category of user. Admin, user, manager, and employee are all typical roles that may exist in an organization. For example, the Admin Console has specific roles which give permission to users to access parts of the Admin Console UI and perform certain actions. There is a global namespace for roles and each user also has its own dedicated namespace where roles can be defined.

Managing Users

If you need to manage a specific user, click **Users** in the left menu bar. This menu option brings you to the user list page.



To search for users:

1. In the search box, type in a full name, last name, or email address you want to search for in the user database. The query will bring up all users that match your criteria. The **View all users** button will list every user in the system. This will search just the local user database and not the federated database (LDAP) because some LDAP does not have a way to page through users.
2. So if you want the users from federated backend to be synced into the user database you need to either:
 - 2a. Adjust search criteria. That will sync just the backend users matching the criteria into the user database.
 - 2b. Go to **User Federation** tab and click **Sync all users** or **Sync changed users** in the page with your federation provider. See *User Federation* on page 105 for more details.

To create new users:

1. From the user list page, on the right side of the empty user list, click the **Add User** button to start creating your new user.

The screenshot shows the 'Add user' form in the EXFO interface. The form is titled 'Add user' and is located in the 'Users' section. The form contains the following fields and controls:

- ID**: Text input field.
- Created At**: Text input field.
- Username***: Text input field (mandatory).
- Email***: Text input field (mandatory).
- First Name***: Text input field (mandatory).
- Middle Name**: Text input field.
- Last Name***: Text input field (mandatory).
- Telephone Number**: Text input field.
- User Type***: Dropdown menu (mandatory).
- Time Zone***: Dropdown menu (mandatory).
- Language***: Dropdown menu (mandatory).
- Units***: Dropdown menu (mandatory).
- Mobile Number**: Text input field.
- Trap receiver address**: Text input field.
- Http post URL**: Text input field.
- User Interface Access**: Three toggle switches for **AW**, **RTU**, and **MOBILE**, all currently set to **OFF**.
- Address**: Text input field.
- Comments**: Text input field.
- User Enabled**: Toggle switch, currently set to **ON**.
- Email Verified**: Toggle switch, currently set to **OFF**.
- Required User Actions**: Dropdown menu with the text 'Select an action...'.

At the bottom of the form, there are **Save** and **Cancel** buttons.

2. Enter the mandatory fields highlighted with an asterisk.

Managing Users

Managing Users

3. Click **Save**. This will bring you to the management page for your new user.

The screenshot shows the EXFO user management interface. The top navigation bar is blue with the EXFO logo on the left and 'Admin Admin' on the right. Below the navigation bar, there is a breadcrumb trail 'Users > user'. The main content area is titled 'User' and has several tabs: 'Details' (selected), 'Attributes', 'Credentials', 'Role Mappings', 'Groups', 'Consents', and 'Sessions'. The 'Details' tab contains a form for user configuration. The form includes fields for ID, Created At, Username, Email, First Name, Middle Name, Last Name, Telephone Number, User Type, Time Zone, Language, Units, Mobile Number, Trap receiver address, Http post URL, User Interface Access (AW, RTU, MOBILE), Address, Comments, User Enabled, Email Verified, Required User Actions, and Impersonate user. At the bottom of the form are 'Save' and 'Cancel' buttons.

EXFO Admin Admin

Users > user

User

Details Attributes Credentials Role Mappings Groups Consents Sessions

ID e7b1e22d-15d4-4c9a-bd73-2e8ff4fd8b73

Created At 8/4/17 4:17:34 PM

Username user

Email user@user.ca

First Name user

Middle Name

Last Name userLastName

Telephone Number

User Type Regular User

Time Zone (UTC) GMT - Greenwich Mean Time

Language English

Units Metric

Mobile Number

Trap receiver address

Http post URL

User Interface Access AW OFF RTU OFF MOBILE OFF

Address

Comments

User Enabled ON

Email Verified OFF

Required User Actions Select an action...

Impersonate user Impersonate

Save Cancel

The user management page allows you to manage and view user information, by selecting the desired tab.

- The **Details** tab displays all the data relevant to the user, including the following:

- **User Type** is either **Regular User** or **Customer**.

Regular User refers to a person who uses the system to provide Quality of Service (QoS) data for the customer. Regular users do not receive alerts according to the fault position, as they are not associated with the optical route sections. However, they receive alerts for each alarm defined in the alarm type.

Customer refers to an individual, a partner, an association, a joint stock company, a trust, a corporation, or a governmental entity that subscribes to telecommunications services offered by the company operating the NQMSfiber system. Customers are different from regular users because they cannot access the system (neither EMS nor RTU) through the administrative workstation (AW) but can receive alerts and automatically generated reports through emails. However, they are mostly interested in faults that occur on the sections of an optical route that belong to them. Thus, different customers can be defined for different sections of each optical route.

Note: *If you are not part of a region in which the RTU is located, you will not see the alarms coming from that RTU as well as the status and the results associated. You will not be able to access that RTU and change its configurations.*

- **Time Zone** is the preferred time zone used to display the date and time in the AW windows.
- **Language** is the preferred language for the user interface: English, French, Spanish, or Russian.

Managing Users

Managing Users

- **Units** can be either **Metric** or **Imperial**.
- **Mobile Number** is the number of the user's mobile device.
- **Trap receiver address** is for the RTU (remote test unit) only. The default is the manager IP address/DNS name of the SNMP manager. You can change the value when you configure a user. For existing users, this value is configured under Configuration > Host > Northbound Settings > SNMP. Provide the HTTP post URL where the JSON (JavaScript Object Notation) object for an event will be posted if the HTTP post notification channel is configured.
- **HTTP post URL:** Parameters in a post are either in the body (default) or directly in the string. You can also have parameters in the string like this:
`https://example.com/page?parameter=value&also=another.`

Include the names of the desired fields with a \$ in front. For example,

`https://example.com/page?param1=$FaultGroupDate¶m2=$Position.` In this example, the values of FaultGroupDate and Position would go in param1 and param2.

Available values are as follows (case insensitive):

FaultIdOnRtu, FaultResultIdonRTU, FirstReferenceIdonRTU, LastLearningIdonRTU, FaultType, Confirmations, Position, MinPosition, MaxPosition, Loss, ThresholdType, ThresholdValue, AppliedThreshold, EventType, OpticalRoute, TestSetupId, TestSetupName, TestType, RTUName, RTUIP and OTDRSerialNumber.

- **User Interface Access** allows you to select **ON** or **OFF** for the following:
 - AW** (administrative workstation) which is required to view the EMS web interface.
 - RTU** (remote test unit) for access from the EMS.
 - MOBILE** for mobile app access.
- **User Rights for RTU** is **View** or **Edit**, allowing you to grant viewing or editing rights for the RTU application.
- **Credentials** are pieces of data that are used to verify the identity of a user. Examples are passwords, OTP (one-time-passwords), digital certificates, or even fingerprints. This tab allows you to create, disable, and reset passwords.

The screenshot shows the EXFO user management interface. The top navigation bar is blue with the EXFO logo on the left and 'Admin Admin' on the right. A left sidebar contains a 'Fiber' dropdown and a 'Configure' section with options like 'Realm Settings', 'Clients', 'Client Templates', 'Roles', 'Identity Providers', 'User Federation', and 'Authentication'. Below this is a 'Manage' section with 'Groups' and 'Users' (selected). The main content area shows 'Users > user' and a 'User' profile with a trash icon. The 'Credentials' tab is active, showing fields for 'New Password', 'Password Confirmation', and a 'Temporary' toggle set to 'ON'. Below these are sections for 'Disable Credentials' (with a 'Disable' button) and 'Credential Reset' (with a 'Send email' button).

To change a password:

- 1.** Enter a new password. A **Reset Password** button will pop up that you click, after you've typed everything in. If the **Temporary** switch is **ON**, this new password can only be used once and will need to be changed after login.
- 2.** Alternatively, if you have email set up in **Realm Settings**, you can send an email to the user that asks them to reset their password. Choose **Update Password** from the **Reset Actions** list box and click **Send email**. The sent email contains a link that will bring the user to the update-password screen.
- 3.** Like passwords, you can send an email to the user that asks them to reset their OTP (one-time password) generator. Choose **Configure OTP** in the **Reset Actions** list box and click the **Send email** button. The sent email contains a link that will bring the user to the OTP setup screen.

Required Actions

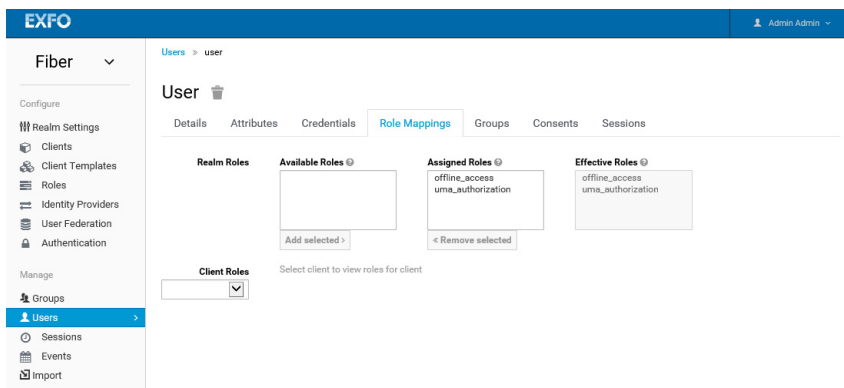
Required actions are tasks that a user must finish before they are allowed to log in. A user must provide their credentials before required actions are executed. Once a required action is completed, the user will not have to perform the action again. Here are explanations of some of the built-in required action types:

- **Update Password:** When set, a user must change their password.
- **Configure OTP:** When set, a user must configure a one-time password generator on their mobile device using either the Free OTP or Google Authenticator application.

- **Verify Email:** When set, a user must verify that they have a valid email account. An email will be sent to the user with a link they have to click. Once this workflow is successfully completed, they will be allowed to log in.
- **Update Profile:** This required action asks the user to update their profile information, that is, their name, address, email, and/or phone number.

Admins can add required actions for each individual user within the user's **Details** tab in the Admin Console.

- User **Role Mappings** can be assigned individually to each user and defines a mapping between a role and a user. A user can be associated with zero or more roles. This role mapping information can be encapsulated into tokens and assertions so that applications can decide access permissions on various resources they manage.

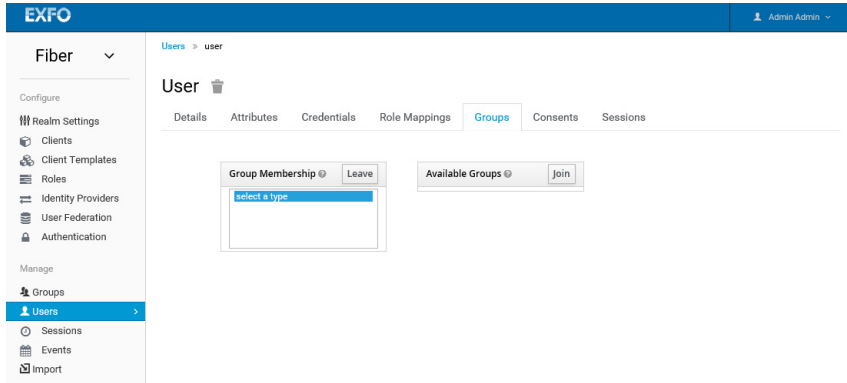


Roles are configured at the realm level. For more information, see *Roles* on page 93.

Managing Users

Managing Users

- **Groups** manage groups of users. Attributes can be defined for a group. You can map roles to a group as well. Users that become members of a group inherit the attributes and role mappings that group defines.



Select a group from the **Available Groups** tree and click the **Join** button to add the user to a group. Vice versa to remove a group. If you go to **Groups** and the detail page for that group, and select the **Members** tab, the user list has been updated.

- **Sessions** are created when a user logs in. A session manages the login session and contains information like when the user logged in and what applications have participated within single-sign on during that session. Both admins and users can view session information.

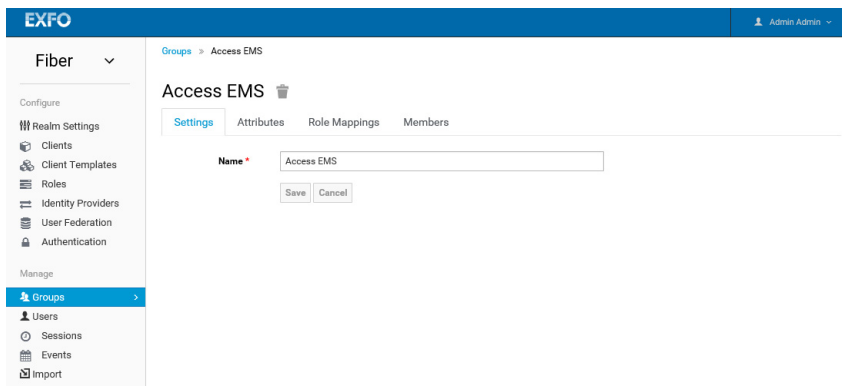
The screenshot shows the EXFO Fiber Guardian web interface. The top navigation bar is blue with the EXFO logo on the left and a user profile 'Admin Admin' on the right. A left sidebar contains a menu with categories like 'Configure', 'Manage', and 'Users'. The 'Users' menu item is highlighted. The main content area shows the breadcrumb 'Users > user' and the title 'User' with a trash icon. Below the title are tabs for 'Details', 'Attributes', 'Credentials', 'Role Mappings', 'Groups', 'Consents', and 'Sessions'. The 'Sessions' tab is active, displaying a table with columns for 'IP Address', 'Started', 'Last Access', 'Clients', and 'Action'. A 'Logout all sessions' button is located in the top right corner of the table area.

IP Address	Started	Last Access	Clients	Action
Logout all sessions				

Managing Groups

Groups allow you to manage a common set of attributes and role mappings for a set of users. Users can be members of zero or more groups. Users inherit the attributes and role mappings assigned to each group. To manage groups go to the Groups left menu item.

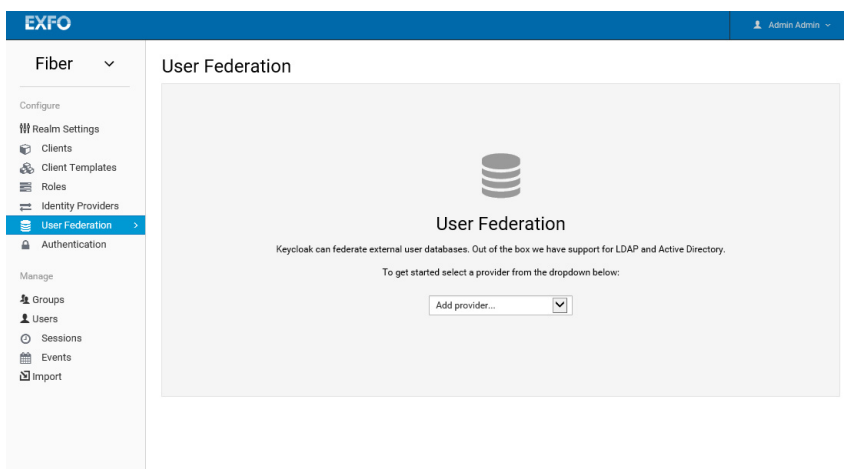
Groups are hierarchical. A group can have many subgroups, but a group can only have one parent. Subgroups inherit the attributes and role mappings from the parent. This applies to the user as well. So, if you have a parent group and a child group and a user that only belongs to the child group, the user inherits the attributes and role mappings of both the parent and child. To add a group, click on the parent you want to add a new child to and click **New** button. Select the Groups icon in the tree to make a top-level group. Entering in a group name in the **Create group** screen and hitting **Save** will bring you to the individual group management page.



Any attributes and role mappings you define will be inherited by the groups and users that are members of this group. To add a user to a group you need to go back to the user detail page and click the **Groups** tab there. For more information, see page 102.

User Federation

Users can federate existing external user databases with support for LDAP and Active Directory by using the User Storage SPI. Once you log in, the internal user store searches to find you. If you can not be found, an iteration over every User Storage provider configured for the realm will be performed until a match is found. Data from the external store is mapped into a common user model that is consumed by the runtime. This common user model can then be mapped to OIDC token claims and SAML assertion attributes.



To add a storage provider:

1. Click on **User Federation** in the left menu of the Admin Console.
2. Click in the **Add provider...** list box and choose the desired provider. The configuration page of that provider will open.

Managing Users

User Federation

LDAP and Active Directory

The user management console comes with a built-in LDAP/AD provider. It is possible to federate multiple different LDAP servers in the same user realm where you can map LDAP user attributes into the common user model. By default, it maps username, email, first name, and last name, but you are free to configure additional mappings. The LDAP provider also supports password validation via LDAP/AD protocols and different storage, edit, and synchronization modes.

Selecting **ldap** as the desired provider from the **User Federation** page will bring you to the LDAP configuration page.

Configure

- Realm Settings
- Clients
- Client Templates
- Roles
- Identity Providers
- User Federation**
- Authentication

Manage

- Groups
- Users
- Sessions
- Events
- Import

Add user federation provider

Required Settings

Console Display Name

Priority

Edit Mode

Sync Registrations

* Vendor

* Username LDAP attribute

* RDN LDAP attribute

* UUID LDAP attribute

* User Object Classes

* Connection URL [Test connection](#)

* Users DN

* Authentication Type

* Bind DN

* Bind Credential [Test authentication](#)

Custom User LDAP Filter

Search Scope

Use Truststore SPI

Connection Pooling

Connection Timeout

Read Timeout

Pagination

Kerberos Integration

Allow Kerberos authentication

Use Kerberos For Password Authentication

Sync Settings

Batch Size

Configuring LDAP Settings

- **Console Display Name** is used when this provider is referenced in the admin console.
- **Priority** denotes the priority of this provider when looking up users or for adding registrations.
- **Edit Mode** allows users, through the User Account Service, and admins, through the Admin Console, to have the ability to modify user metadata. Depending on your setup you may or may not have LDAP update privileges. The Edit Mode configuration option defines the edit policy you have with User Documentation LDAP/AD Integration 314 in your LDAP store.
 - **READ_ONLY** does not allow changes to username, email, first name, last name, and other mapped attributes. An error will be displayed anytime anybody tries to update these fields. Also, password updates will not be supported.
 - **WRITABLE** allows for updates to username, email, first name, last name, other mapped attributes and passwords. All will be synchronized automatically with your LDAP store.
 - **UNSYNCED** allows any changes to username, email, first name, last name, and passwords to be stored in the user local storage. It is up to you to figure out how to synchronize back to LDAP. This allows user deployments to support updates of user metadata on a read-only LDAP server. This option only applies when you are importing users from LDAP into the local user database.
- **Sync Registrations** enables/disables your LDAP adding new users. Click **ON** if you want new users created in the admin console or the registration page to be added to LDAP.
- **Allow Kerberos authentication** allows you to select **ON/OFF** for Kerberos/SPNEGO authentication in realm with users data provisioned from LDAP.

Managing Users

User Federation

- **Sync Settings** allows you to sync all LDAP users into the user database, by configuring and enabling the following settings:
 - **Batch Size** is the number of LDAP users to be imported from LDAP in a single transaction.
 - **Periodic Full Sync** will synchronize all LDAP users when **ON** is selected. Those LDAP users, which already exist and were changed in LDAP directly will be updated.
 - **Periodic Changed Users Sync** will update and/or import only those users that were created or updated after the last sync, when **ON** is selected.

Storage Mode

By default, users from LDAP will be imported into the local user database. This copy of the user is either synchronized on demand, or through a periodic background task. The one exception to this is passwords. They are not imported and password validation is delegated to the LDAP server. The benefits to this approach is that all features will work, while any extra per-user data that is needed can be stored locally. This approach also reduces load on the LDAP server as uncached users are loaded from the user database the second time they are accessed. The only load your LDAP server will have is password validation. The downside to is that when a user is first queried, this will require a user database insert. The import will also have to be synchronized with your LDAP server as needed.

Alternatively, you can choose not to import users into the user database. In this case, the common user model that the runtime uses is backed only by the LDAP server. This means that if LDAP doesn't support a piece of data that a feature needs, that feature will not work. The benefit to this approach is that there is no overhead of importing and synchronizing a copy of the LDAP user into the user database.

5 **Using the Host Web User Interface**

You need to configure different settings from the Host Web UI before you can start working with your unit.

Accessing and Exiting the Host Web UI

The Host Web UI allows you to perform various operations on the host and companion of your unit.

For a complete list of supported Web browsers, see *Supported Web Browsers* on page 12.

The steps that you will need to follow to access the Web UI will depend on the type of connection that you have: computer connected locally to the unit, computer and unit connected to a same LAN, or computer and unit connected to a WAN or the Internet. In the latter case, you will need to connect your computer to the VPN and to retrieve the LogMeIn address of your unit before being able to connect to the Web UI.

To start the Host Web UI:

- 1.** If you intend to connect to your unit via a WAN or the Internet, connect to the VPN (see *Connecting to the VPN* on page 79); otherwise, go directly to step 2.
- 2.** From your computer, open a Web browser.
- 3.** In the address bar, type the appropriate information.
 - Computer connected directly to the unit (front port), type `https://169.254.10.10/HostWebUI`
 - For LAN connection, type `https://Rear_Port_IP_Address/HostWebUI`
 - For WAN or Internet connection, type `https://Unit_LogMeIn_Hamachi_Address/HostWebUI`

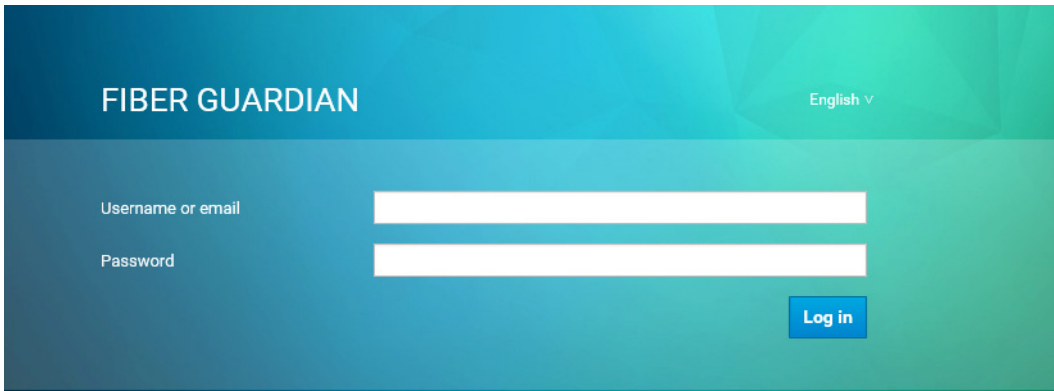
Using the Host Web User Interface

Accessing and Exiting the Host Web UI

Note: If you do not know the IP address of the rear Ethernet port, see Retrieving the IP Address of the Rear Ethernet Port (Host and Companion) on page 55.

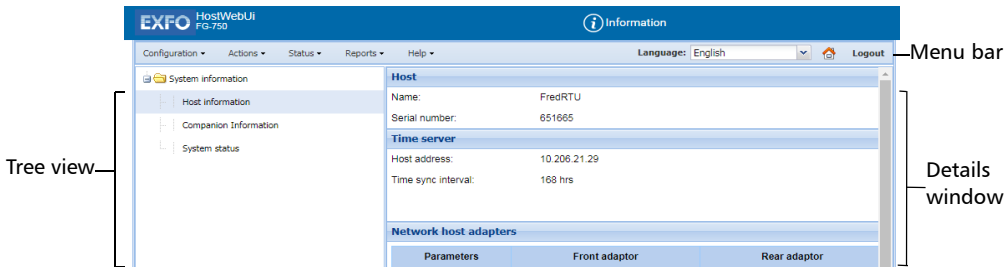
Note: If you do not know the LogMeIn Hamachi address of your unit, see Connecting to the VPN on page 79.

4. When the application prompts you, enter *Admin* as the user name and *Admin* as the password.



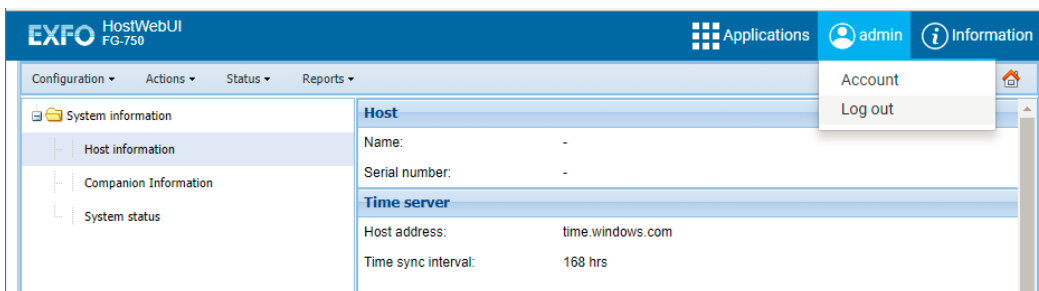
5. Click **OK** to open the session.

The main window is displayed.



To exit the Host Web UI:

Click **Log out** found under **admin** in the navigation bar.



Viewing Host and Companion Information

You can view the following information about your Fiber Guardian host and companion, from the Web UI:

- Host Information:
 - Name and serial number of the host
 - Address of the time server and the sync interval
 - IPv4 and IPv6 configurations of the host network adapters
- Companion Information: IPv4 and IPv6 configurations of the companion network adapters.

To view host and companion information:

1. Start the Host Web UI. For more information, see *Accessing and Exiting the Host Web UI* on page 109.
2. From the **Status** menu, select **System Information**.
3. Select either **Host Information** or **Companion Information**, depending on the type of information that you need to retrieve.

Configuring Network Settings

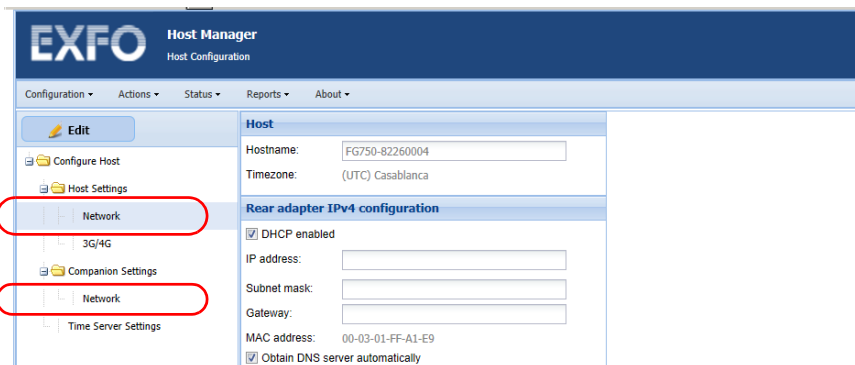
You can configure various network settings for the host and the companion. These settings include the host name, and the IP addresses of the rear adapter (IPv4 and IPv6). By default, the IP addresses of both the host and companion are assigned dynamically (automatically) by a DHCP server on your LAN. However, if you prefer, you can define your own static IP addresses.

Note: *If you are not sure on how to proceed or need more information about the configuration, see with your network administrator.*

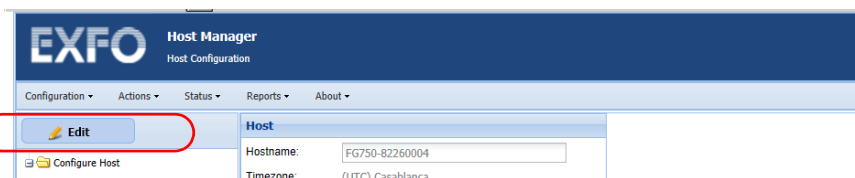
To configure the network settings:

- 1.** Start the Host Web UI. For more information, see *Accessing and Exiting the Host Web UI* on page 109.
- 2.** From the **Configuration** menu, select **Host**.

3. Depending on the type of parameters that you wish to modify, under **Host Settings** or **Companion Settings**, select **Network**.



4. To modify the displayed information, click **Edit**.



5. Depending on your needs, go to the **Rear adapter IPv4 configuration** or **Rear adapter IPv6 configuration** section.

Using the Host Web User Interface

Configuring Network Settings

6. Configure the parameters as needed.

The screenshot shows the 'Host' configuration window with the following sections and annotations:

- Host:** Host name: FG750-82260004 (Annotation: Corresponds to the computer name; must be unique on the network.)
- Timezone:** (UTC) Casablanca
- Rear adapter IPv4 configuration:**
 - DHCP enabled (Annotation: To let the system assign the IP address dynamically)
 - IP address: [] (Annotation: To configure a static IP address)
 - Subnet mask: []
 - Gateway: []
 - MAC address: 00-03-01-FF-A1-E9
 - Obtain DNS server automatically (Annotation: To let the system define the address to the DNS server (option not available for the companion))
 - Primary DNS: [] (Annotation: To define static DNS addresses)
 - Secondary DNS: []
- Rear adapter IPv6 configuration:**
 - DHCP enabled
 - IP address: []
 - Subnet prefix length: 0
 - Gateway: []
 - MAC address: 00-03-01-FF-A1-E9
 - Obtain DNS server automatically
 - Primary DNS: []
 - Secondary DNS: []
- Front adapter configuration:**
 - DHCP enabled: No

Buttons: Apply, Cancel

Copyright © 2012, EXFO Inc. All rights reserved.

- If you want the system to automatically assign IP addresses for the rear adapter, ensure that the **DHCP enabled** and **Obtain DNS server automatically** check boxes are selected.
- If you prefer to define static IP addresses for the rear adapter, clear both the **DHCP enabled** and **Obtain DNS server automatically** check boxes, and set the extra parameters.

Note: The **Obtain DNS server automatically** option and the related parameters are available for the host only.

7. Click **Apply** to confirm the changes.

Configuring the 3G/4G Settings

Once you have prepared your unit for wireless access, you are ready to configure the 3G/4G network settings via the Web UI. For more information on the preparation of your unit, see *Preparing Your Unit for 3G/4G Access* on page 59.

You can configure the unit to use a 3G/4G wireless network when the LAN is not available. To do so, you will need to specify an access point name (APN), a user name, and a password for the connection to the 3G/4G network.

Note: *Not all service providers require a user name and a password to authorize the connection to the 3G/4G network.*

By default, your unit is configured to connect automatically to the wireless network, but you can deactivate this feature if you prefer. You can also specify a maximum number of minutes during which the unit can remain connected to the wireless network.

You can also specify the type of security (authentication) that you want to use for the 3G/4G connection.

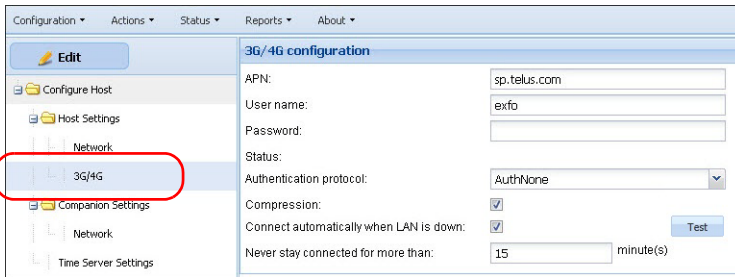
Note: *If you need more information about the connection parameters or the configuration, see with your service provider.*

Using the Host Web User Interface

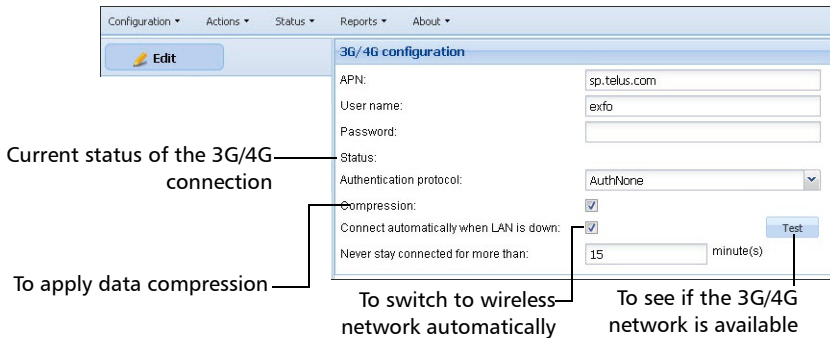
Configuring the 3G/4G Settings

To configure the 3G/4G settings:

1. Start the Host Web UI. For more information, see *Accessing and Exiting the Host Web UI* on page 109.
2. From the **Configuration** menu, select **Host**.
3. Under **Host Settings**, select **3G/4G**.



4. Click **Edit**.
5. Configure the parameters as needed.



6. Click **Apply** to confirm the changes.

Connecting as an NQMSfiber EMS Client (OTDR Mode Only)

The **EMS Server** configuration page is available from the **Configuration > Host** tab.

To configure the EMS Server:

1. Click **EMS Server** under **Northbound Settings** to open the **EMS Server** page.
 - 1a. Enter the **IP Address/Host Name**.
 - 1b. Enter the **Polling Frequency** number of hours, from 0 to 720 (which is about a month). Default is 24 hrs.
 - 1c. Select a **Network Topology** value, either **LAN** (default) or **Lowbandwidth**.

The screenshot shows the 'EMS Server' configuration page. The left sidebar contains a tree view with 'EMS Server' selected under 'Northbound Settings'. The main content area has the following fields and buttons:

- IP Address/Host Name:**
- Polling Frequency (hrs.):**
- Network Topology:**
- Last successful synchronization:** 2014-09-12 15:40:07
- Buttons:** Test Connection, Start Synchronization, Recovery Configuration, Detach from EMS

2. Click **Apply** to confirm your changes, or **Cancel**.
3. Click **Test Connection** to ping the **Host Name**. If successful, a confirmation popup appears.

Using the Host Web User Interface

Connecting as an NQMSfiber EMS Client (OTDR Mode Only)

4. Click **Start Synchronization** to call the EMS SOAP 'getRtuStatus'. If the EMS response is online and the RTU's request for synchronization was sent, a confirmation popup appears.

Once a synchronization is done, a message displaying the date and time of the last successful synchronization is added. This text is updated with every successful synchronization and is removed when detaching from the EMS or changing the value of the Host Name.

5. Click **Recovery Configuration** to open a popup **Recovery** window. Type in the **Old Mac Address** and click **recover** to revert to the previous EMS parameters.
6. Click **Detach from EMS** to clear the RTU from all information about the EMS. All created users, EMS and LDAP configurations are deleted.

Error messages occur when:

- the values for the Host Name or synchronization frequency are empty,
- trying to detach an RTU that was never synchronized to an EMS.

Configuring the E-Mail Server Settings

The **E-Mail** configuration page is available from the **Configuration > Host** tab. Click **E-Mail Server** under **Northbound Settings** to open the following **E-Mail Server** page.

The screenshot shows the configuration page for the E-Mail Server. The interface includes a top navigation bar with 'Configuration', 'Actions', 'Status', 'Reports', and 'About' menus. A left sidebar contains a tree view of settings: 'Configure Host', 'Host Settings', 'Companion Settings', 'Northbound Settings', and 'Time Server Settings'. Under 'Northbound Settings', 'E-Mail Server' is selected. The main content area is titled 'E-Mail Server' and contains the following fields:

- Server Address: EmailServerExfo
- Port: 3680
- Server message type: SMTP
- Sender: fred@exfo.com
- Authentication Required
- User Name: fred
- Password: [masked]
- Retype password: [masked]

To configure the E-Mail Server settings:

1. Click **Edit** to set the following parameters:
 - 1a. **Server Address** is the IP or Host Name.
 - 1b. **Port** is the number value higher than 0.
 - 1c. **Server message type** is a fixed value of **SMTP**.
 - 1d. **Sender** is the e-mail address used to send e-mails.

Using the Host Web User Interface

Configuring SNMP

1e. Authentication Required allows you to enable the following fields by checking the box:

User Name is the name of the user permitted to connect to the SMTP server.

Password of the accredited user.

Retype password to confirm the correct password.

2. Click **Apply** to save changes, or **Cancel** to discard them.

Configuring SNMP

SNMP (Simple Network Management Protocol) is a set of protocols for managing complex networks. SNMP consists of the following:

- An SNMP manager
- An SNMP agent
- A database of management information
- Managed SNMP devices
- The network protocol

The SNMP manager provides an interface between a network manager and the management system. The SNMP agent provides an interface between the manager and the physical devices being managed. The agent sends a Trap when a specific event occurs.

You can use SNMP to run a test to check the health of a fiber. This test is called Test on Demand (TOD), as it can be run as per your requirement. Test on Demand can be run on RTU, using SNMP from a third party SNMP manager or any third party application.

To configure SNMP:

1. Click **SNMP** under **Northbound Settings** to open the **SNMP** page.

OR (for standalone units)

From the main menu, select **Configuration > System Settings**. Then, from the tree view, select **Other Settings, then SNMP**.

2. Click **Edit**.

The screenshot shows the EXFO Host Manager web interface. The top navigation bar includes 'Configuration', 'Actions', 'Status', 'Reports', and 'About'. The left sidebar shows a tree view with 'SNMP' selected under 'Northbound Settings'. The main panel displays the 'SNMP' configuration form with the following fields:

- Version: V3 (dropdown)
- SNMP Manager IP/Hostname: (text input)
- Remote Port: 162 (dropdown)
- User Name: (text input)
- SNMP Engine ID: (text input)
- Password: (text input)
- Authentication Algorithm: SHA (dropdown)
- Encryption Password: (text input)
- Encryption Algorithm: DES (dropdown)

Buttons for 'Apply' and 'Cancel' are located at the bottom of the form.

3. Select the SNMP version.
4. For Version V3 (default), enter the following parameters:
 - 4a. User Name
 - 4b. SNMP Engine ID is read only.
 - 4c. Password
 - 4d. Authentication Algorithm for the password encryption type: MD5 or SHA.

Using the Host Web User Interface

Configuring SNMP

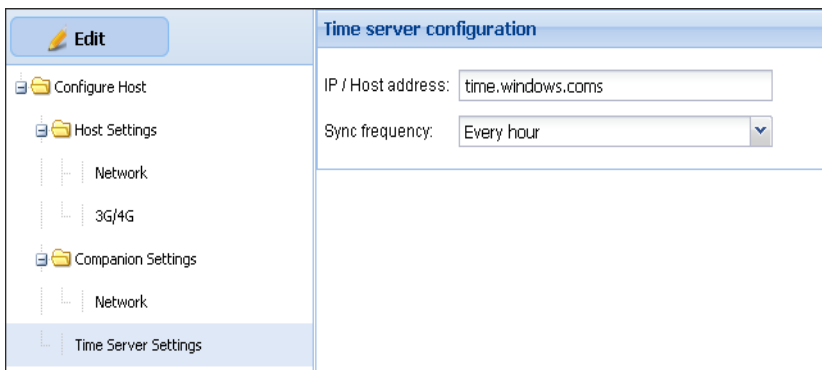
- 4e.** Encryption Password used for the data.
- 4f.** Encryption Algorithm also used for the data: DES (default), AES, or 3DES.
- 5.** For versions **V1** and **V2c**, enter the following parameters:
 - 5a.** The SNMP Manager IP/Hostname can either be IPv4, IPv6, or the hostname of the SNMP listener. A port can also be set for the destination like this: 127.0.0.1:6001 or FG750777777:6002.
 - 5b.** Remote Port is a numerical value only, over 0 and is by default 162.
- 6.** Click **Apply** to save changes, or **Cancel** to discard them.

Configuring the Time Server Settings

You can configure time server settings of the host from the Host Web UI.

To configure the time server settings:

1. Start the Host Web UI. For more information, see *Accessing and Exiting the Host Web UI* on page 109.
2. From the **Configuration** menu, click **Host**.
3. Click **Time Server Settings**.
4. To modify the displayed information, click **Edit**.
5. In the **IP / Host address** field, enter the IP address or the host address of the time server that you are using.



Edit	
Configure Host	
Host Settings	
Network	
3G/4G	
Companion Settings	
Network	
Time Server Settings	

Time server configuration	
IP / Host address:	<input type="text" value="time.windows.coms"/>
Sync frequency:	<input type="text" value="Every hour"/>

Note: For your unit to be synchronized with a time server, ensure that you specify the address (or the name) of an NTP server that your unit can reach.

Note: A Fiber Guardian unit cannot be used as a time server.

6. From the **Sync frequency** list, select the time frame that the host should synchronize with the time server.
7. To confirm the changes, click **Apply**.

6 Setting Up Your RTU

Detecting the Fibers Connected to the Optical Ports

You must perform the detection of the optical ports in the following cases:

- when you install a new RTU.
- when you connect optical fiber to previously unused ports to activate testing (see *Cleaning and Connecting Optical Fibers* on page 82).

The RTU must first detect the fibers connected to the ports. It will automatically create the optical routes, test setups and test programs (for more information, see *Managing Optical Routes* on page 157).

Once the detection is completed, you can configure a remote switch (ROTAU) if you want. The RTU will only take into account (detect) ports to which fibers of at least 50 meters are connected.

To detect new ports:

1. From the main menu, select **Configuration > Remote Test Unit**.
2. Under **OTAU**, click **Detect**.

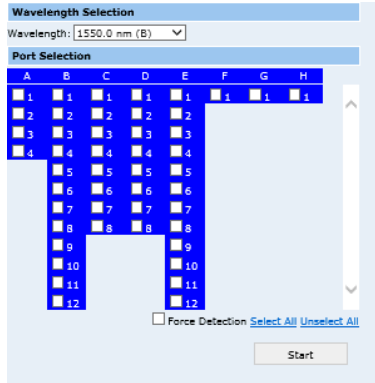
The screenshot shows the EXFO NQMSFiber - Remote Test Unit web interface. The interface is divided into several sections:

- Configuration:** Includes a sidebar with "Remote Test Unit", "Connected Optical Routes", and "Controlled ROTAUs".
- Status:** Shows "Name: S/N: 783009" and "Comments:".
- Reporting:** Shows "Status: Responding".
- Manual Test:** Includes "OTDR" section with "Serial number: 783009", "Model name: OTH-740-DIMET", and "Wavelength: 1550 nm on singlemode B fiber".
- About:** Includes "OTAU" section with "Serial number: 776324" and "Number of ports: 47".
- Port status:** A table with columns A, B, C, D, E, F, G, H and rows 1 through 12. The table is currently empty.
- Buttons:** "Detect", "Backup Database", "Reset to Factory Settings", and "Edit".

Setting Up Your RTU

Detecting the Fibers Connected to the Optical Ports

- From the displayed dialog box, select a wavelength.



Note: The wavelength used to detect a series of ports will be used as the default monitoring test wavelength. You may therefore start monitoring on certain ports at a certain wavelength and on other ports with another wavelength.

- Select the ports you want to use at this wavelength.

Note: To quickly select or clear the check boxes, use respectively **Select All** and **Unselect All**.

- Click **Start** to start the automatic detection of the ports. The RTU will generate test setups for the new wavelengths.
- Repeat the previous steps with other wavelengths and ports if necessary.

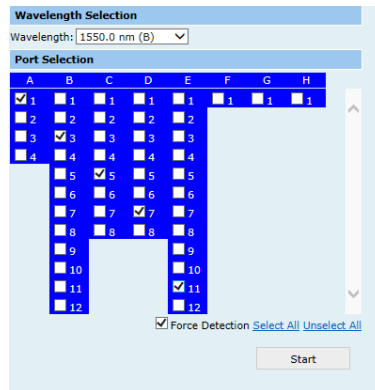
The status of the ports (detected or not) is indicated in the **OTAU** section.

You can now configure the remote switch, if you have one (see *Configuring a Remote Switch (ROTAU)* on page 131).

Note: Once the manual detection of fiber ports is done there is a chance that ports remain undetected though the fiber is connected, these ports can be detected forcefully by selecting force detection of fiber.

To use Force Detection of fiber:

1. From the main menu, select **Configuration > Remote Test Unit**.
2. From the tree view, select the optical test head to which the optical routes are connected.
3. Under **OTAU**, click **Detect**.
4. From the displayed dialog box, select a wavelength.



5. Select the ports you want to use at this wavelength.

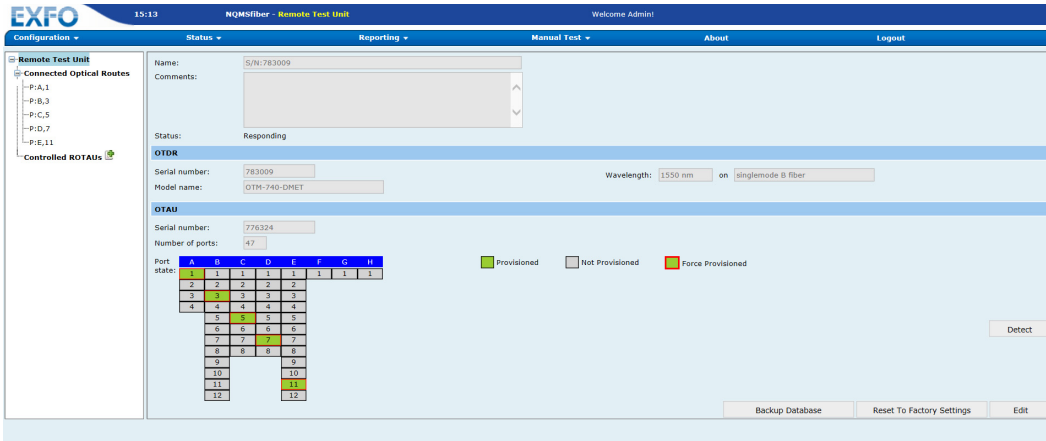
Note: To quickly select or clear the check boxes, use respectively **Select All** and **Unselect All**.

6. Check **Force Detection** and click **Start** to start the force detection of the ports.

Setting Up Your RTU

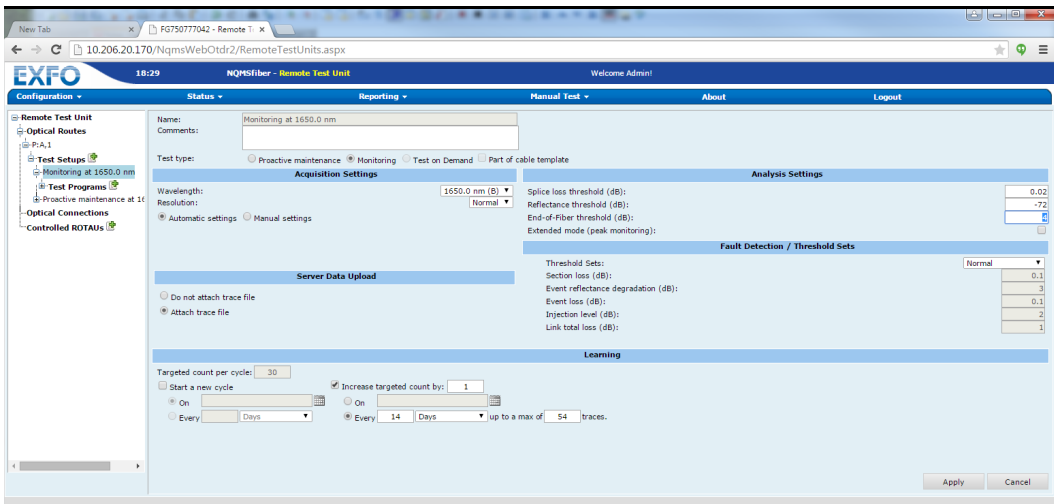
Detecting the Fibers Connected to the Optical Ports

7. The forcibly detected ports will be outlined in red.



8. You can configure the ROTAU with the force detected fibers.

9. As the force detection of fiber has been done because of the poor quality of the fiber, the end of fiber threshold may need to change manually to get test results.



Changing a Cassette

When a cassette change is detected in your RTU, you are automatically redirected to the **Optical Connections** assignment page. Here, a list of affected optical routes not linked to ports is displayed and must be reassigned to a *Not provisioned* port on the RTU, or deleted. You cannot navigate elsewhere on the website (redirection) unless you take action on this page which is in edit mode.

The screenshot shows the EXFO NQMSfiber - Remote Test Unit interface. The top navigation bar includes 'Configuration', 'Status', 'Reporting', 'Manual Test', 'About', and 'Logout'. The left sidebar shows a tree view with 'Remote Test Unit', 'Optical Routes', 'P:C,1', 'P:H,1', 'Optical Connections', and 'Controlled ROTAs'. The main content area displays a table titled 'Optical Connections' with the following data:


Connection	Name	Status	Action
Optical route @ C,1	P:C,1	Decoupled	Assign to C,1
Optical route @ H,1	P:H,1	Decoupled	Assign to H,1

To assign a route to the new cassette:

1. From the new cassette layout, select a port by clicking on .
 - 1a. If the route's original port still exists on the new cassette layout, the same port is suggested under the **Action** column.
 - 1b. If the route's original port does not exist anymore, is displayed indicating that the route is unassigned and requires more information. All routes must be reassigned before you can resume monitoring. If some routes cannot be reassigned to a port, you must delete them.

Setting Up Your RTU

Changing a Cassette






- When you click , a port selection window is displayed. Select a column and port number to assign the route.

Port Selection							
A	B	C	D	E	F	G	H
1	1	1	1	1	1	1	1
2			2	2	2		2
3			3	3	3		3
4			4	4	4		4
5			5	5			5
6			6	6			6
7			7	7			7
8			8	8			8
9			9				
10			10				
11			11				
12			12				

- Delete a route by clicking . All routes can be deleted at once by clicking the delete all button .

This is useful for the following:

- ▶ If you just want access again to the website to start over.
- ▶ If there is a long list of routes to delete.
- ▶ If you just want to keep some routes, for example delete all, then assign 2-3 routes.

Action		
Assign to C,1		
Assign to H,1		

- Click **Apply** to confirm your selections.

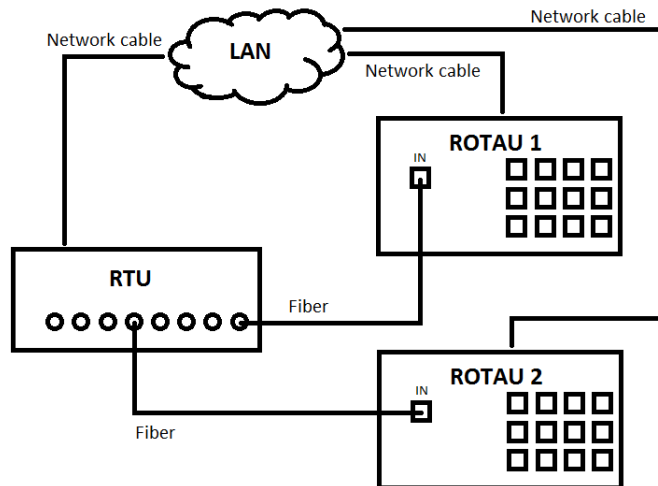
Configuring a Remote Switch (ROTAU)

For more information on port configuration, see *Detecting the Fibers Connected to the Optical Ports* on page 125.

You can also remove a ROTAU if it is no longer used.

To configure a ROTAU:

1. Ensure that your ROTAU is connected as follows.



2. From the main menu, select **Configuration > Remote Test Unit**.

Setting Up Your RTU

Configuring a Remote Switch (ROTAU)

To add a ROTAU

1. Under **Controlled ROTAUs**, click the listed ROTAU to open the information page.
2. Click **Create Optical Routes** button to open a popup window.
3. Enter the ports for which you would like to create the routes.

The screenshot shows the EXFO NQMSfiber - Remote Test Unit web interface. The top navigation bar includes the EXFO logo, the time 16:24, the page title 'NQMSfiber - Remote Test Unit', and a 'Welcome Admin!' message. The main navigation menu has tabs for Configuration, Status, Reporting, Manual Test, About, and Logout. The left sidebar shows a tree view with 'Remote Test Unit' expanded to 'Controlled ROTAUs', where 'ROTAU:A,1' is selected. The main content area displays the configuration for 'ROTAU:A,1'. The 'Name' field is 'ROTAU:A,1' and the 'Status' is 'Operational'. A 'Create Optical Route' dialog box is open in the foreground, titled 'Create Optical Route - Internet Explorer'. It has two sections: 'Wavelength Selection' with a checked checkbox for '1550.0 nm (B)' and 'Port Selection' with instructions: 'Type port numbers and/or port ranges separated by semicolons. For example, type 5; 7; 24-30'. The dialog box has 'Create' and 'Cancel' buttons. At the bottom right of the main interface, there are buttons for 'Create Optical Routes', 'Edit', and 'Delete'.

To edit a ROTAU:

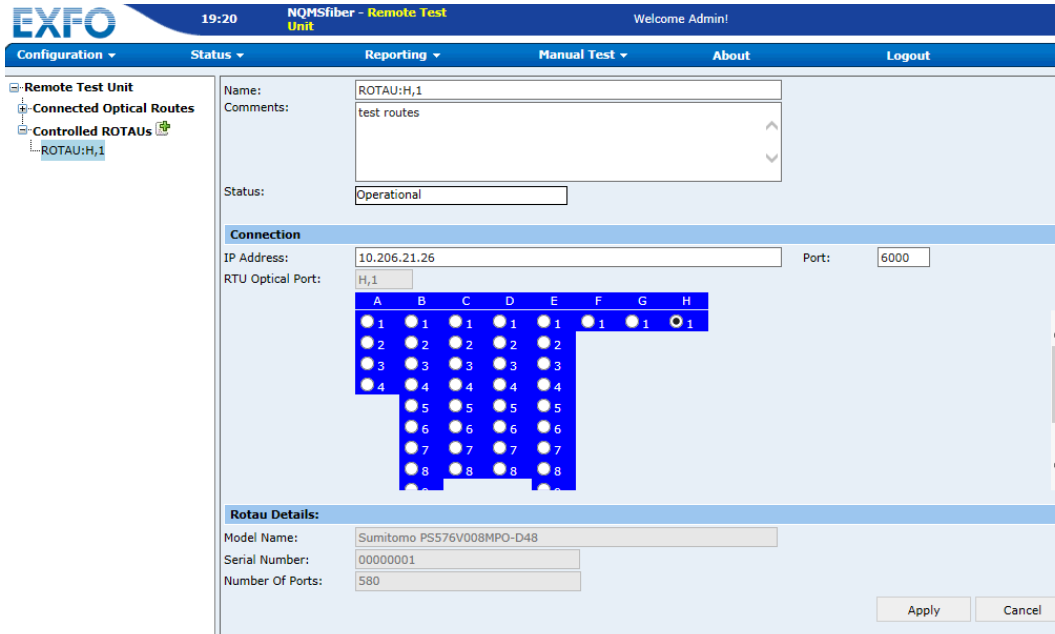
1. Under **Controlled ROTAUs**, click the listed ROTAU to open the information page.
2. Click the **Edit** button corresponding to the port to which the ROTAU is connected.

The screenshot shows the EXFO NQMSfiber Remote Test Unit configuration interface. The top navigation bar includes 'Configuration', 'Status', 'Reporting', 'Manual Test', 'About', and 'Logout'. The main content area is divided into a left sidebar and a main panel. The sidebar shows a tree view with 'Remote Test Unit' expanded to 'Controlled ROTAUs', where 'ROTAU:A,1' is selected. The main panel displays the configuration for 'ROTAU:A,1'. The 'Name' field is 'ROTAU:A,1'. The 'Status' is 'Operational'. The 'Connection' section shows 'IP Address: 10.206.20.186' and 'RTU Optical Port: A,1'. The 'Rotau Details' section shows 'Model Name: DiCon MS1X8', 'Serial Number: 19A0E10D0020', and 'Number Of Ports: 8'. At the bottom right, there are buttons for 'Create Optical Routes', 'Edit', and 'Delete'.

Setting Up Your RTU

Configuring a Remote Switch (ROTAU)

3. Set the parameters for the ROTAU.



The RTU will delete the optical route that was defined for the local port as well as its related test setups and test programs. It will also create optical routes and test setups (according to the system setting parameters) for each of the ROTAU's ports.

If the ROTAU is not responding, an error message will appear. See *Viewing the Event Log* on page 249 for information about troubleshooting the error.

4. Click **Apply** to update the changes, or **Cancel** to discard them.

Note: ROTAU configuration with normal detection fiber and force detected fiber, has not any difference.

To remove a ROTAU:

- 1.** From the main menu, select **Configuration > Remote Test Unit**.
- 2.** Under **Controlled ROTAUs**, click the **Delete** button corresponding to the port to which the ROTAU is connected.
- 3.** When the application prompts you, click **OK** to confirm deletion.




The RTU will delete the optical routes and test setups that were created for each of the ROTAU's ports. It will create a single optical route (corresponding to the local port) and the related test setups (according to the system setting parameters).

ROTAU Status

The ROTAU status validation relies on two configuration items which are defined in system settings:

- ROTAU Polling time which periodically checks if each configured ROTAU is reachable. It is defined in seconds and its default value is 300 seconds.
- ROTAU Number of failed polls before alert is used as a threshold before sending an alarm. It is defined as a count and its default value is 3 successive failed polls.

Each ROTAU has one of the following states:

- **Operational**  when
 - the configured **IP Address** is reachable
 - the linked OSC Port is provisioned
- **Unreachable**  when
 - the configured **IP Address** is unreachable
 - the ROTAU has just been created
 - the ROTAU IP Address has just been changed
- **Decoupled**  when
 - the linked OSC Port is not provisioned
 - the linked OSC Port is a virtual port

When **Decoupled**, the port image is replaced by a red X.

A change in ROTAU status from **Operational** to **Unreachable** launches a system warning on the event when the number of failed polls, defined in the configuration, is reached. The minimum time an alert is launched is 15 minutes.

The status is displayed under **Controlled ROTAUs** for the selected **ROTAU**.

The screenshot shows the EXFO NQMSfiber Remote Test Unit interface. The top navigation bar includes 'Configuration', 'Status', 'Reporting', 'Manual Test', and 'About'. The left sidebar shows a tree view with 'Remote Test Unit' expanded to 'Controlled ROTAUs', where 'ROTAU:B,1' is selected. The main content area displays the configuration for 'ROTAU:B,1' with the following details:

- Name: ROTAU:B,1
- Comments: (empty text area)
- Status: ✔ Operational
- Connection section:
 - IP Address: 10.206.20.188
 - Port: (empty)
 - RTU Optical Port: B,1

In the **Controlled ROTAUs** list, the status is also displayed.

The screenshot shows the EXFO NQMSfiber Remote Test Unit interface. The top navigation bar includes 'Configuration', 'Status', 'Reporting', 'Manual Test', and 'About'. The left sidebar shows a tree view with 'Remote Test Unit' expanded to 'Controlled ROTAUs', where 'ROTAU:B,1' is selected. The main content area displays a table titled 'Controlled ROTAUs' with the following data:

Name	Connected RTU Port	Status
✔ ROTAU:B,1	B,1	Operational

Setting Up Your RTU

ROTAU Status

Consolidated ROTAU Status

The Consolidated ROTAU status represents a global status of all configured ROTAUs on the system. A ROTAU status is reported when at least 1 ROTAU status is changed. The consolidated status has one of the following states:

- Normal - all ROTAU are operational
- Unreachable - at least 1 ROTAU is unreachable
- Decoupled - at least 1 ROTAU is decoupled
- Unreachable or Decoupled - at least 1 ROTAU is decoupled and 1 is unreachable, or 1 ROTAU is decoupled and unreachable

To view the Consolidated ROTAU Status:

From the main menu, select **Status > System**.

The screenshot shows the EXFO NQMSfiber - System Status interface. The top navigation bar includes the EXFO logo, the time 18:35, the system name NQMSfiber - System Status, and the user name Welcome Admin!. Below the navigation bar, there are several tabs: Configuration, Status, Reporting, Manual Test, About, and Logout. The Status tab is selected, and the Consolidated ROTAUs status is displayed as Normal. The interface also shows a tree view of Remote Test Units (RTUs) on the left, including P:A,1, P:A,2, and P:C,1, each with sub-items for Monitoring at 1550.0 nm and Proactive maintenance at 1550.

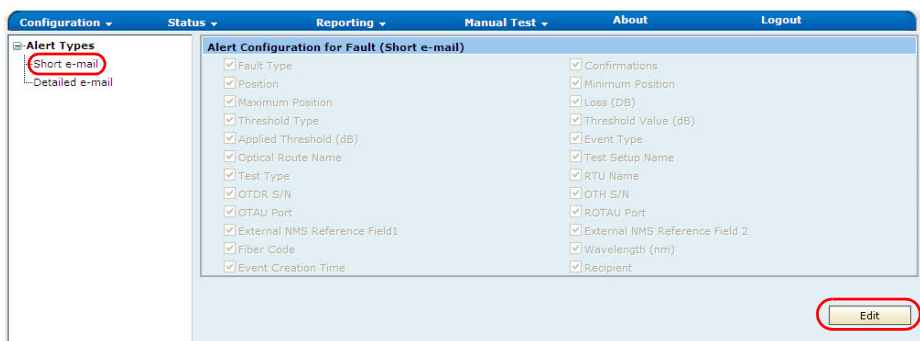
Attribute	Value
Number of skipped optical routes	2
Results with errors count	0
Results with errors since last synchronization count	0
Consolidated ROTAUs status	Normal

Configuring Alerts

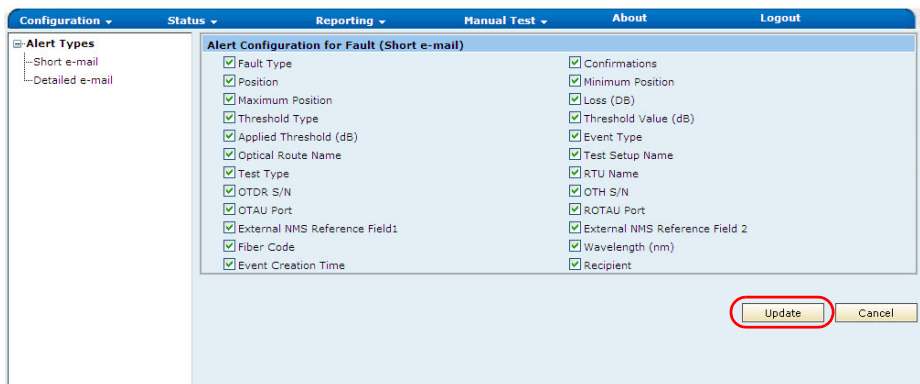
The alerts are generated when certain events occur. This application allows you to configure the alert for the fault. Here you can configure **Short e-mail** alert and **Detailed e-mail** alert.

To configure alert:

1. From the main menu select **Configuration > Alert Configuration**.
2. From the tree view, select desired e-mail option and click **Edit**.



3. Select the required options and click **Update** to apply the changes.



Managing Alert Types

The application can alert users when certain events, or combinations of events, occur. To generate the alerts, the application uses predefined templates called *alert types*.

The following alert types are created automatically at time of installation:

- Fiber fault
- System fault
- Fiber fault (for OSS/GIS system)
- Life signal

You can also create your own alert types. You can modify and delete any alert type, including those that were created at time of installation.

Note: *You must be logged in as Admin user to be able to create, modify or delete alert types.*

Each of the alert types includes the following items:

- Channel type: format of the message that will be sent to the specified users when the application generates an alert. The channel type includes:
 - the short e-mail to send a brief message, in plain text.
 - the detailed e-mail to send complete information in html format with the OTDR trace in attachment.
 - the xml e-mail, like the detailed e-mail, is sent to the configured e-mail account of the user. The GIS system can use the physical route information from the xml mail present on the mail server to find the precise location of the fault. For more information, see *Managing Optical Routes* on page 157.
 - the SNMP (Simple Network Management Protocol) to send alerts in the form of SNMP, trap.
 - the RTU can be set to send event data — change in the status of a fault, life signal of the RTU, errors, and warnings — to external applications as a JavaScript Object Notation (JSON) object through HTTP to the configured HTTP Post URL. The HTTP Post URL can be configured from the user page. For more information, see *Managing Users* on page 91.
- E-mail addresses of the people to whom the alert messages must be sent.



IMPORTANT

You must activate the alert types you intend to use. Otherwise, the application will not take them into account.

Setting Up Your RTU

Managing Alert Types

To view an alert type:

1. From the main menu, select **Configuration > Alerting Types**.
2. From the tree view, select the desired alert type.

Information on the selected alert type

The screenshot shows the EXFO web interface for configuring alerting rules. The top navigation bar includes 'Configuration', 'Status', 'Reporting', 'Manual Test', 'About', and 'Logout'. The left sidebar shows a tree view with 'Alerting Types' selected and circled in red. The main content area displays the configuration for a selected alert rule, including fields for Name, Channel type, Comments, and a list of destinations.

Alerting Rule Details

Name: Channel type: Short e-mail

Comments:

Is active Use this rule if server is not available


Apply this rule to the following events:

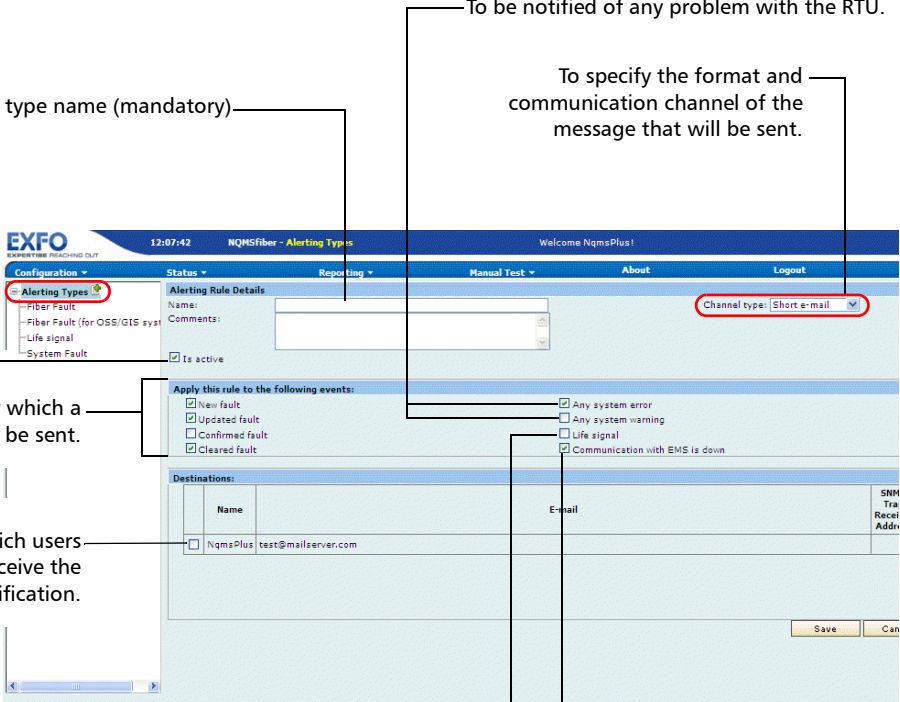
<input checked="" type="checkbox"/> New fault	<input checked="" type="checkbox"/> Any system error
<input checked="" type="checkbox"/> Updated fault	<input type="checkbox"/> Any system warning
<input type="checkbox"/> Confirmed fault	<input type="checkbox"/> Life signal
<input checked="" type="checkbox"/> Cleared fault	<input checked="" type="checkbox"/> Communication with EMS is down

Destinations:

Receiver Address
<input type="checkbox"/> J w
<input type="checkbox"/> J w
<input type="checkbox"/> NqmsPlus test@mailserver.com
<input type="checkbox"/> prajakta p.

To add alert types

1. From the main menu, select **Configuration > Alerting Types**.
2. From the tree view, click the  icon that appears next to **Alerting Types**.



The screenshot shows the 'Alerting Rule Details' configuration page. The left sidebar has 'Alerting Types' selected. The main area contains fields for 'Name', 'Comments', and 'Is active'. Below these are checkboxes for 'Apply this rule to the following events' and a 'Destinations' table. Annotations with lines pointing to specific UI elements provide the following information:

- Alert type name (mandatory):** Points to the 'Name' input field.
- To ensure the application takes this alert type into account:** Points to the 'Alerting Types' menu item in the sidebar.
- Events for which a message will be sent:** Points to the 'Apply this rule to the following events' section.
- To indicate which users will receive the notification:** Points to the 'Destinations' table.
- To receive a confirmation that the RTU is operational (every 12 hours):** Points to the 'Life signal' checkbox.
- To be notified of any problem with the RTU:** Points to the 'Any system error' checkbox.
- To specify the format and communication channel of the message that will be sent:** Points to the 'Channel type' dropdown menu.
- Not used with stand-alone RTU:** Points to the 'SNMP Trap Address' column in the 'Destinations' table.

Note: If the SNMP channel type is selected, the machine address is displayed for the destination table.

Setting Up Your RTU

Managing Alert Types

3. Enter the parameters according to your needs.
4. Click **Save** to create the alert type or **Cancel** to discard them.

To modify alert types:

1. From the main menu, select **Configuration > Alerting Types**.
2. From the tree view, select the alert type you want to modify.

The screenshot shows the EXFO configuration interface for Alerting Types. The top navigation bar includes 'Configuration', 'Status', 'Reporting', 'Manual Test', 'About', and 'Logout'. The left sidebar shows a tree view with 'Alerting Types' selected. The main content area is titled 'Alerting Rule Details' and contains the following fields and sections:

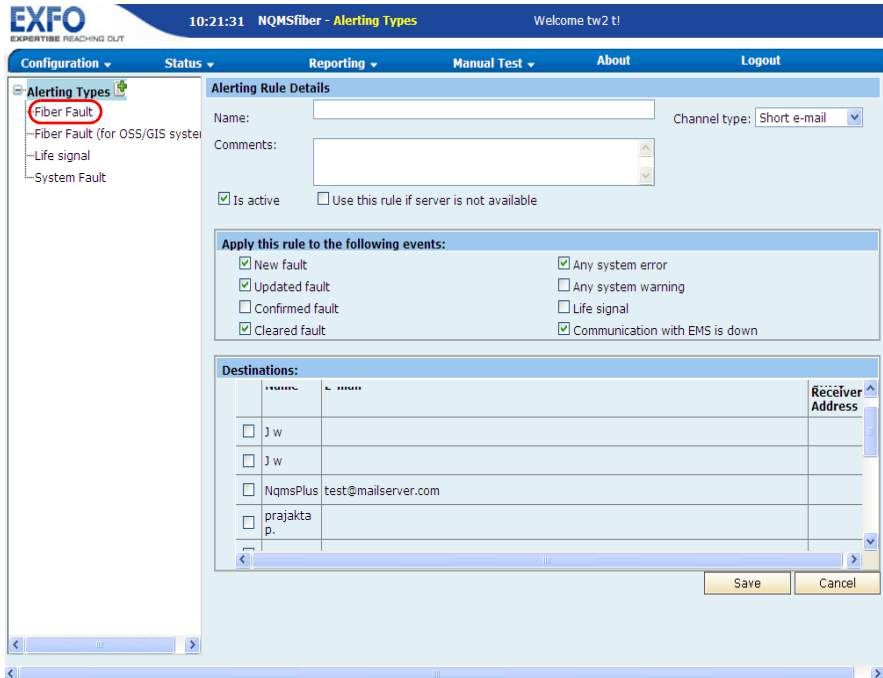
- Name:** Fiber Fault
- Channel type:** Short e-mail
- Comments:** (empty text area)
- Is active
- Use this rule if server is not available
- Apply this rule to the following events:**
 - New fault
 - Updated fault
 - Confirmed fault
 - Cleared fault
 - Any system error
 - Any system warning
 - Life signal
 - Communication with EMS is down
- Destinations:**

		Receiver Address
<input type="checkbox"/>	3 w	
<input type="checkbox"/>	3 w	
<input type="checkbox"/>	NqmsPlus test@mailserver.com	
<input type="checkbox"/>	prajakta p.	

3. Click **Edit**.
4. Modify the parameters according to your needs.
5. Click **Apply** to update changes or **Cancel** to discard them.

To delete alert types:

1. From the main menu, select **Configuration > Alerting Types**.
2. From the tree view, select the alert type you want to delete.



3. Click **Delete**.
4. When the application prompts you, click **OK** to confirm deletion.

Managing System Setting Values

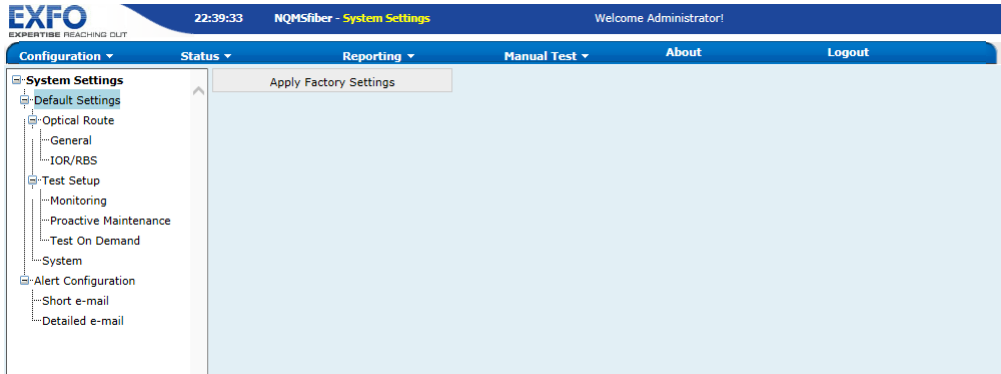
There are two types of default values: factory values (used when you need to revert to factory values) and current default values (used currently to operate the RTU).

The default values are grouped into categories:

- **Optical route:** to define the IOR (group index), RBS coefficient and helix factor that the RTU will use when it creates the optical routes. For more information on these parameters, see *Modifying Optical Routes* on page 160.
- **Test setup:** to define, for monitoring and proactive maintenance (two distinct sets of parameters), test settings such as resolution, acquisition type (automatic or manual), range, etc. and learning settings such as the targeted learning count, reset and expand parameters. For more information on these parameters, see *Managing Test Setups* on page 165).
- **System:** to define “global” parameters such as the number of test setups that will be created automatically, the way fiber breaks will be. You cannot modify factory default values.

To revert to factory default values for Default Settings:

- 1.** From the main menu, select **Configuration > System Settings**.
- 2.** From the tree view, select **Default Settings**.
- 3.** Click **Apply Factory Settings**.



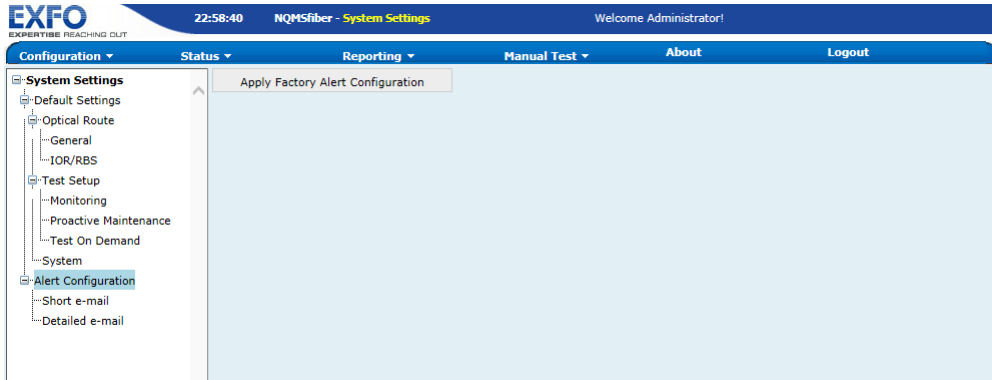
- 4.** The application displays a prompt to confirm that the default factory settings will be applied. Click **OK** to apply the **Default Settings** parameters to default, or **Cancel** to keep the current values.

Setting Up Your RTU

Managing System Setting Values

To revert to factory default values for Alert Configuration:

1. From the main menu, select **Configuration > System Settings**.
2. From the tree view, select **Alert Configuration**.
3. Click **Apply Factory Alert Configuration**.



4. The application displays a prompt to confirm that the other factory settings will be applied. Click **OK** to revert the **Alert Configuration** parameters to default, or **Cancel** to keep the current values.

Defining Default Helix Factor, IOR, and RBS Values

You can define the IOR (group index), RBS coefficient and helix factor that the RTU will use when it creates the optical routes.

- The *index of refraction (IOR)* value (also known as group index) is used to convert time-of-flight to distance. Having the proper IOR is crucial for all OTDR measurements associated with distance (event position, attenuation, section length, total length, etc.). IOR is provided by the cable or fiber manufacturer.

The test application determines a default value for each wavelength. You can set the IOR value for each available wavelength.

- The *Rayleigh backscatter (RBS) coefficient* represents the amount of backscatter in a particular fiber. The RBS coefficient is used in the calculation of event loss and reflectance, and it can usually be obtained from the cable manufacturer.

The test application determines a default value for each wavelength. You can set the RBS coefficient for each available wavelength.

- The *helix factor* takes into consideration the difference between the length of the cable and the length of the fiber inside the cable. Fibers within a cable are spiraling around the cable core. The helix factor describes the pitch of that spiral.

By setting the helix factor, the length of the OTDR distance axis is always equivalent to the physical length of the cable (not the fiber).

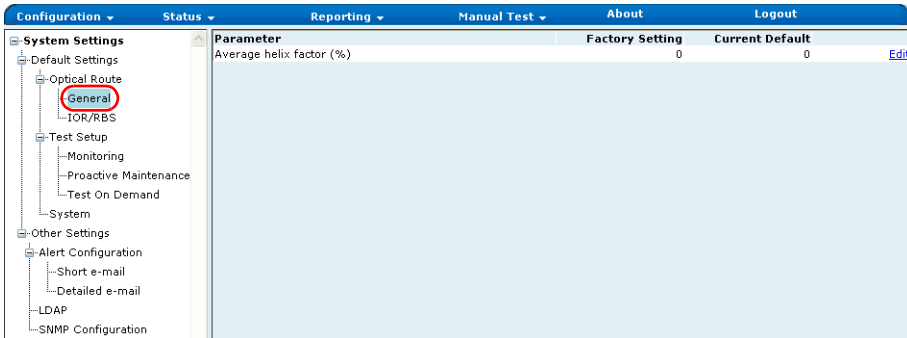
Setting Up Your RTU

Managing System Setting Values

To modify the current helix factor, IOR, or RBS values:

1. From the main menu, select **Configuration > System Settings**.
2. From the tree view,
 - For helix factor, select **General**.

The parameters for helix factor are displayed.

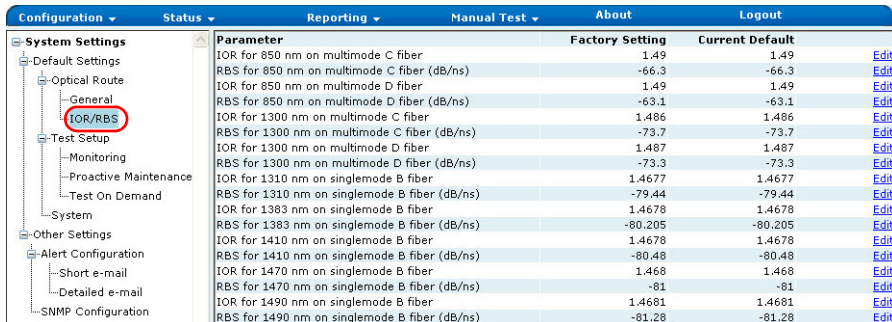


The screenshot shows the RTU configuration interface. The left sidebar displays a tree view under 'System Settings' with 'Optical Route' expanded and 'General' selected. The main panel shows a table with the following data:

Parameter	Factory Setting	Current Default	
Average helix factor (%)	0	0	Edit

- For IOR and RBS, select **IOR/RBS**.

The parameters for IOR and RBS are displayed.



The screenshot shows the RTU configuration interface with 'IOR/RBS' selected in the tree view. The main panel displays a table of parameters:

Parameter	Factory Setting	Current Default	
IOR for 850 nm on multimode C fiber	1.49	1.49	Edit
RBS for 850 nm on multimode C fiber (dB/ns)	-66.3	-66.3	Edit
IOR for 850 nm on multimode D fiber	1.49	1.49	Edit
RBS for 850 nm on multimode D fiber (dB/ns)	-63.1	-63.1	Edit
IOR for 1300 nm on multimode C fiber	1.486	1.486	Edit
RBS for 1300 nm on multimode C fiber (dB/ns)	-73.7	-73.7	Edit
IOR for 1300 nm on multimode D fiber	1.487	1.487	Edit
RBS for 1300 nm on multimode D fiber (dB/ns)	-73.3	-73.3	Edit
IOR for 1310 nm on singlemode B fiber	1.4677	1.4677	Edit
RBS for 1310 nm on singlemode B fiber (dB/ns)	-79.44	-79.44	Edit
IOR for 1383 nm on singlemode B fiber	1.4678	1.4678	Edit
RBS for 1383 nm on singlemode B fiber (dB/ns)	-80.205	-80.205	Edit
IOR for 1410 nm on singlemode B fiber	1.4678	1.4678	Edit
RBS for 1410 nm on singlemode B fiber (dB/ns)	-80.48	-80.48	Edit
IOR for 1470 nm on singlemode B fiber	1.468	1.468	Edit
RBS for 1470 nm on singlemode B fiber (dB/ns)	-81	-81	Edit
IOR for 1490 nm on singlemode B fiber	1.4681	1.4681	Edit
RBS for 1490 nm on singlemode B fiber (dB/ns)	-81.28	-81.28	Edit

3. Click the **Edit** button appearing next to the parameter you want to modify.
4. Click **Apply** to update changes or **Cancel** to discard them.
5. Repeat the previous steps with all the parameters you want to modify.

Defining Default Values for Test Setups

You can define, for monitoring and proactive maintenance (two distinct sets of parameters), test settings such as resolution, acquisition type (automatic or manual), range, etc. and learning settings such as the targeted learning count, reset and expand parameters.

- *Resolution*: By selecting the high-resolution feature (“high”), you will obtain more data points per acquisition. This way, the data points will be closer to each other, which will result in a greater distance resolution for the trace.
- *Acquisition settings*: With automatic settings, the application will determine the most appropriate range, pulse width and duration for you. If you prefer to specify these values yourself when you define a test setup, you should select the manual settings.
- *Range*: Corresponds to the distance range of the fiber span to be tested, in kilometers.
- *Pulse width*: A longer pulse allows you to probe further along the fiber, but results in lower resolution. A shorter pulse width provides higher resolution, but less distance range.
- *Duration*: Corresponds to the acquisition duration (period during which results will be averaged). Generally, longer acquisition times generate cleaner traces (this is especially true with long-distance traces) because as the acquisition time increases, more of the noise is averaged out. This averaging increases the signal-to-noise ratio (SNR) and the OTDR’s ability to detect small events.

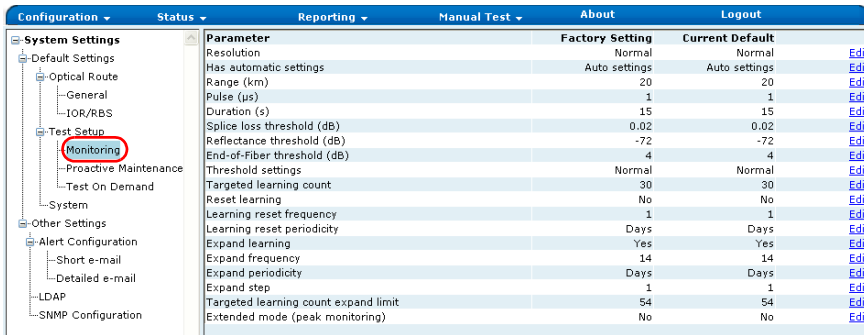
Setting Up Your RTU

Managing System Setting Values

- **Splice loss threshold:** Setting for detecting small non-reflective events during trace analysis and when establishing the test setup reference.
- **Reflectance threshold:** Setting for detecting small reflective events during trace analysis and when establishing the test setup reference.
- **End-of-fiber threshold:** Setting for detecting important event loss that could compromise signal transmission during trace analysis and when establishing the test setup reference.
- **Fault threshold settings:** The threshold set that will be used during tests. For more information, see *Managing Threshold Sets* on page 179.

To modify the default values for test setups:

1. From the main menu, select **Configuration > System Settings**.
2. From the tree view, select the set of settings you want to modify (**Monitoring** or **Proactive Maintenance**).



Configuration	Status	Reporting	Manual Test	About	Logout
System Settings					
Default Settings					
Optical Route					
General					
IOR/RBS					
Test Setup					
Monitoring					
Proactive Maintenance					
Test On Demand					
System					
Other Settings					
Alert Configuration					
Short e-mail					
Detailed e-mail					
LDAP					
SNMP Configuration					
Parameter	Factory Setting	Current Default			
Resolution	Normal	Normal			Edit
Has automatic settings	Auto settings	Auto settings			Edit
Range (km)	20	20			Edit
Pulse (µs)	1	1			Edit
Duration (s)	15	15			Edit
Splice loss threshold (dB)	0.02	0.02			Edit
Reflectance threshold (dB)	-72	-72			Edit
End-of-Fiber threshold (dB)	4	4			Edit
Threshold settings	Normal	Normal			Edit
Targeted learning count	30	30			Edit
Reset learning	No	No			Edit
Learning reset frequency	1	1			Edit
Learning reset periodicity	Days	Days			Edit
Expand learning	Yes	Yes			Edit
Expand frequency	14	14			Edit
Expand periodicity	Days	Days			Edit
Expand step	1	1			Edit
Targeted learning count expand limit	54	54			Edit
Extended mode (peak monitoring)	No	No			Edit

3. Click the **Edit** button appearing next to the parameter you want to modify.
4. Click **Apply** to update changes or **Cancel** to discard them.
5. Repeat the previous steps with all the parameters you want to modify.

Defining Default Values for System Parameters

You can define “global” parameters such as the number of test setups that will be created automatically, the way fiber breaks will be managed, the maximum database size, etc.

- You can specify which data will be uploaded to the EMS server (not applicable when RTU is used in stand-alone mode).

The table below shows which information will be stored on RTU and uploaded to the server, in each case.

Type of upload	Faults and data acquired during the first reference of the learning period	Data acquired with monitoring	Data acquired with Proactive maintenance
Do not attach trace file	Uploaded	Not stored	<ul style="list-style-type: none"> ➤ Stored ➤ Uploaded
Attach trace file	Uploaded, along with .trc file	Not stored	<ul style="list-style-type: none"> ➤ Stored ➤ Uploaded, along with .trc file

- Degraded fiber handling strategy, when enabled, skips an optical route if the fiber is degraded. The selection for this option is enabled, by default.
- The maximum number of fiber result entries is 5 000, by default. You can increase this number up to 100 000 entries. However, this maximum value will never be reached if the database size exceeds 80% of the maximum database size.

Setting Up Your RTU

Managing System Setting Values

To modify the default values for system parameters:

1. From the main menu, select **Configuration > System Settings**.
2. From the tree view, select **System**.

Parameter	Factory Setting	Current Default	
Break strategy	Skip	Skip	Edit
Degraded fiber handling strategy	Enabled	Enabled	Edit
Test setup definition strategy	Both	Both	Edit
Server data upload policy	Attach trace file	Attach trace file	Edit
ROTAU control delay (s)	5	5	Edit
ROTAU communication frequency (s)	300	300	Edit
ROTAU failed communication attempts before alert	3	3	Edit
Maximum log entries in database	50000	50000	Edit
Maximum result entries in database	5000	5000	Edit
Maximum fault entries in database	1000	1000	Edit
Maximum database size (Gb)	10	10	Edit

3. Click the **Edit** button appearing next to the parameter you want to modify.
4. Click **Apply** to update changes or **Cancel** to discard them.
5. Repeat the previous steps with all the parameters you want to modify.

Editing Test On Demand Default Parameters

The default input parameters for test on demand are listed on the **Test On Demand** screen.

To edit test on demand parameters:

1. From the main menu, select **Configuration > System Settings**.
2. From the tree view, select **Default Settings > Test Setup**.
3. Select **Test On Demand**.

The screenshot shows the EXFO NQMSfiber System Settings interface. The left sidebar contains a tree view with 'Test On Demand' highlighted. The main area displays a table of parameters with their Factory Setting and Current Default values, and an Edit link for each row.

Parameter	Factory Setting	Current Default	
Resolution	Normal	Normal	Edit
Has automatic settings	Auto settings	Auto settings	Edit
Range (km)	20	20	Edit
Pulse (µs)	1	1	Edit
Duration (s)	15	15	Edit
Splice loss threshold (dB)	0.02	0.02	Edit
Reflectance threshold (dB)	-72	-72	Edit
End-of-Fiber threshold (dB)	4	4	Edit
Threshold settings	Normal	Normal	Edit
Targeted learning count	50	50	Edit
Extended mode (peak monitoring)	No	No	Edit

The **Test On Demand** page lists the parameters with their **Factory Setting** values and **Current Default** values.

4. Click **Edit** corresponding to the parameter.
5. Enter the appropriate value.
6. Click **Apply** to update changes or **Cancel** to discard them.

7 Operating Your RTU in OTDR Measuring Mode

Managing Optical Routes

By default, once the detection of the fibers (that are connected to the ports) is complete, the application creates the following items automatically:

- An optical route for each of the ports the RTU has detected, that is one per port to which a fiber is connected.
- Two default test setups for each route at the wavelengths selected during fiber detection. If you prefer, you can modify this behavior (see *Managing System Setting Values* on page 146).
- One test program for each of the test setup.

Each optical route can have one or more test setups and each test setup can have one or more test programs.

The screenshot displays the Fiber Guardian configuration interface. On the left, a tree view shows the hierarchy: 'Optical routes created by the RTU' (containing 'OTH:1 P001'), 'Test setups associated with a specific route' (containing 'Monitoring at 1550.0 nm'), and 'Test program associated with a specific test setup' (containing 'Proactive maintenance at SNMPTOD1'). The main panel shows the configuration for the 'Monitoring at 1550.0 nm' test setup. The 'Name' field is 'Monitoring at 1550.0 nm' and the 'Test type' is 'Monitoring'. The 'Acquisition Settings' include 'Wavelength: 1550.0 nm (B)' and 'Resolution: Normal'. The 'Analysis Settings' include 'Splice loss threshold (dB): 0.02', 'Reflectance threshold (dB): -72', and 'End-of-Fiber threshold (dB): 4'. The 'Fault Detection' section has 'Use standard set of thresholds: Normal' and various threshold values. The 'Server Data Upload' section has 'Normal' selected. The 'Learning' section has 'Targeted count per cycle: 30' and 'Increase targeted count by: 1'. The 'Start Test' button is highlighted with a red circle.

Operating Your RTU in OTDR Measuring Mode

Managing Optical Routes

Even if the optical routes are created automatically by the RTU, you can view, modify, duplicate, and delete these routes.

From the optical routes window, you can:

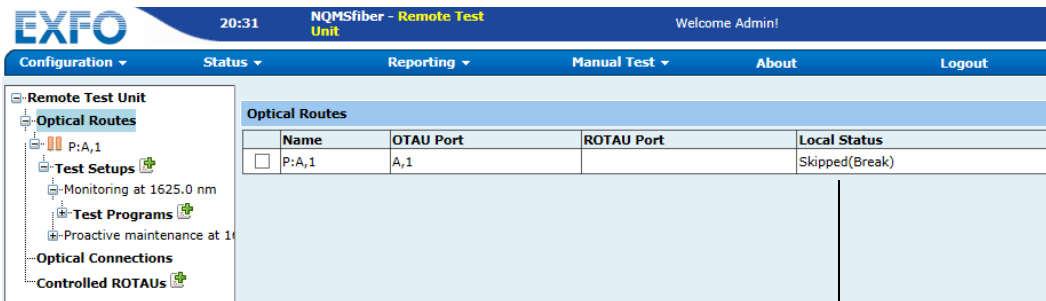
- view, edit, copy, and delete routes (deleted routes can be re-created later by a new port detection).
- suspend or resume scheduled jobs on one or several routes.
- view, add, modify, and delete test setups (see *Managing Test Setups* on page 165).
- view, add, modify, and delete test programs (see *Managing Test Programs* on page 175).

Viewing Optical Routes

To view optical routes:

From the main menu, select **Configuration > Remote Test Unit > Optical Routes**.

The application lists all the optical routes that have been detected.



Status of the route:

Not configured: no jobs are scheduled

Active: at least one job is scheduled

Skipped (and the reason): even if jobs are scheduled, no test will be performed on this route

Modifying Optical Routes

The RTU creates the optical routes automatically with settings based on the defined default values. For more information on the parameters, see *Managing System Setting Values* on page 146.

- You can specify whether the link is made of dark or live fiber.
- You can modify the helix factor, the IOR, and RBS values.
- You can specify one or two additional IDs to your route (cable ID and tube, or fiber color) to complete the information about this route. It can also help documenting the start and finish sites of the route. This information is part of the xml e-mail that will be sent according to the alert rules that you have defined (see *Managing Alert Types* on page 140).

To modify optical routes:

1. From the main menu, select **Configuration > Remote Test Unit > Optical Routes**.
2. From **Optical Routes** tree view, select the optical route you want to modify.
3. Click **Edit**.

The screenshot displays the EXFO NQMSfiber Remote Test Unit configuration interface. The top navigation bar includes 'Configuration', 'Status', 'Reporting', 'Manual Test', 'About', and 'Logout'. The left sidebar shows a tree view under 'Remote Test Unit' with 'Optical Routes' selected. The main configuration area is titled 'P:B,1' and contains the following fields and sections:

- Name:** P:B,1
- Comments:** (empty text area)
- OTDR:** OTDR 1550 nm (SM)
- OTAU port:** B,1
- ROTAU port:** (empty)
- Settings:**
 - Test Ready:
 - Type: Dark Live
 - Average helix factor: 0 %
- Physical Network Reference:** Physical Route ID: (empty)
- External NMS Reference:** Field 1: (empty), Field 2: (empty)
- Correction Factors:**

Wavelength	IOR	RBS
1550.0 nm	1.4683	-81.87

Buttons for 'Apply' and 'Cancel' are located at the bottom right of the configuration area.

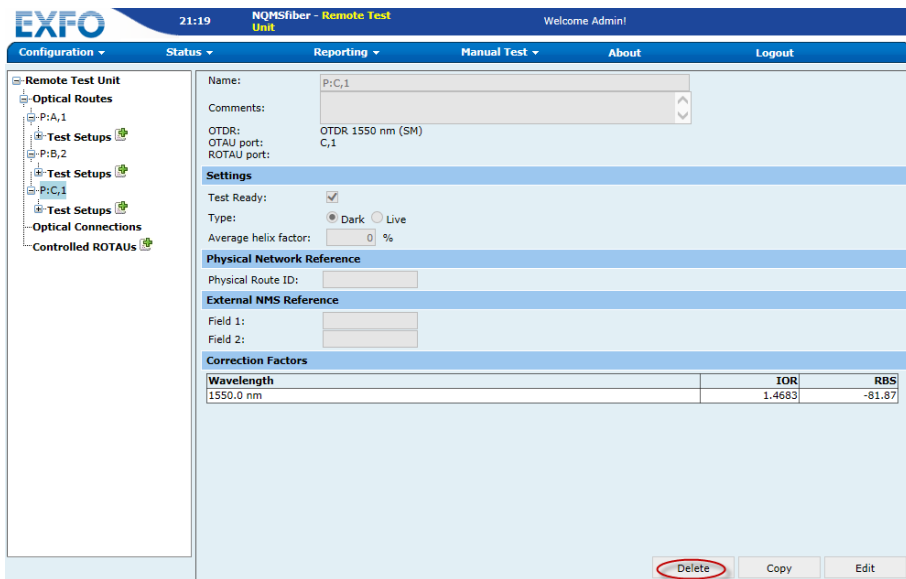
4. Set the parameters according to your needs.
5. Click **Apply** to update changes or **Cancel** to discard them.

Deleting Optical Routes

You can “recover” deleted routes by performing a port detection (see *Detecting the Fibers Connected to the Optical Ports* on page 125).

To delete optical routes:

1. From the main menu, select **Configuration > Remote Test Unit > Optical Routes**.
2. From the **Optical Routes** tree view, select the optical route you want to delete.



3. Click **Delete**.
4. When the application prompts you, click **OK** to confirm deletion.

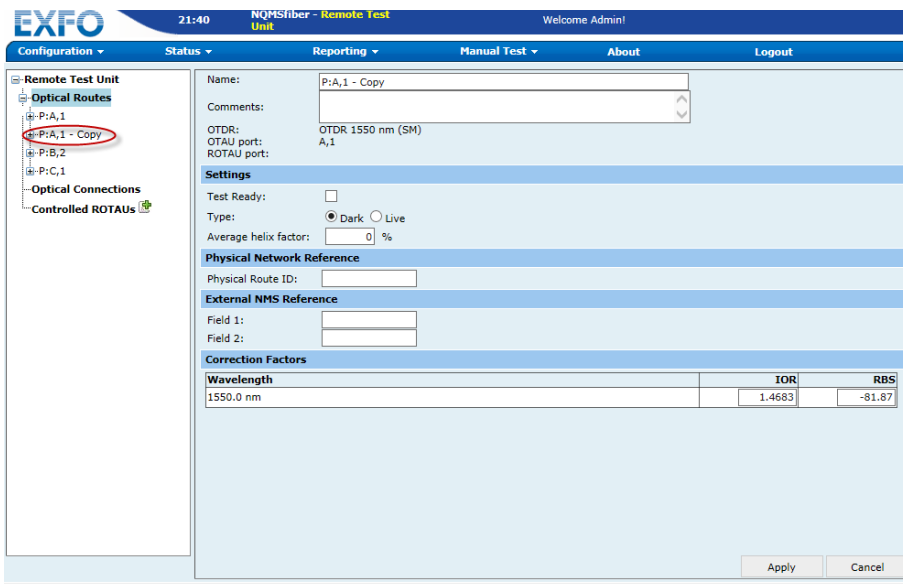
Copying Optical Routes

In the optical route view, you can duplicate the current optical route. The route copied will have exactly the same properties and test on the same port, but will not retain **Test Setups** and trace data. Also, the name generated will be the same name as the copied route but appended with **- Copy**.

To copy an optical route:

1. From the main menu, select **Configuration > Remote Test Unit > Optical Routes**.
2. From the **Optical Routes** tree view, select the optical route you want to copy.
3. Click **Copy**.

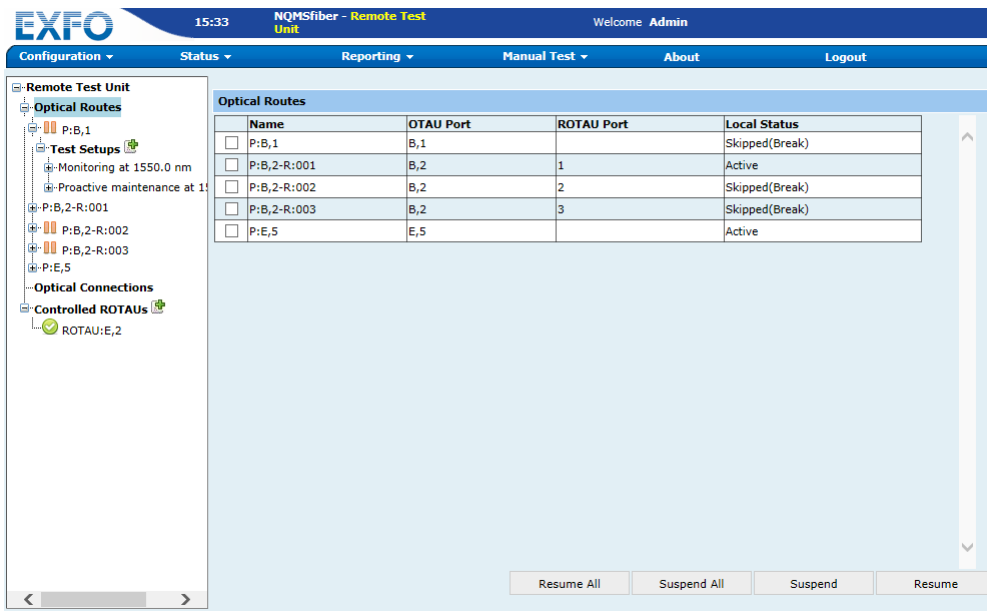
After copying, the optical route edit screen containing the copied route is listed in edit mode.



Suspending or Resuming Scheduled Jobs on Optical Routes

To suspend or resume scheduled jobs:

1. From the main menu, select **Configuration > Remote Test Unit**. A list of **Optical Routes** is displayed.



2. Click **Resume All** or **Suspend All** depending on your needs.
OR
3. Select the specific optical routes for which you want to suspend or resume tests.
4. Click **Suspend** or **Resume**.

The route status will change accordingly.

Managing Test Setups

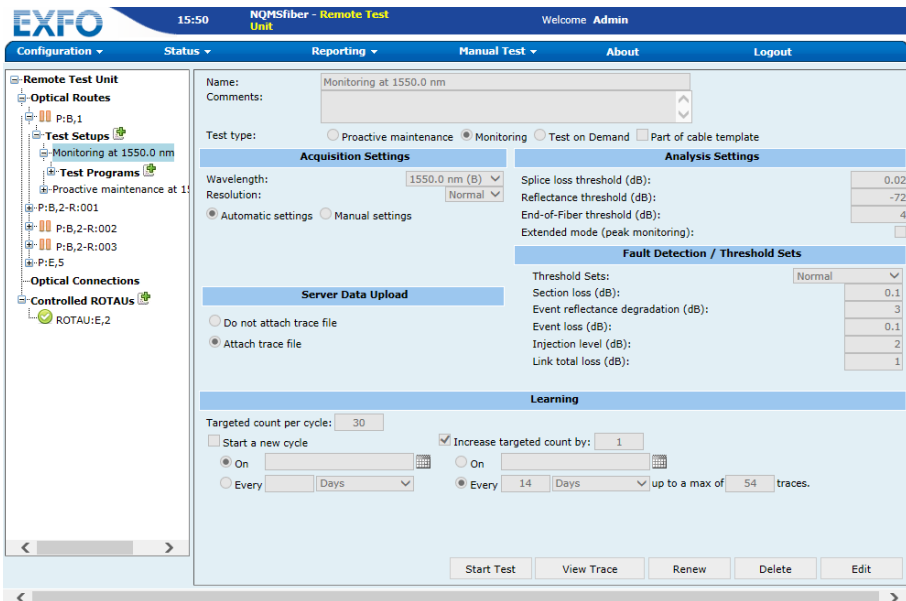
Test setups describe the method of analysis by defining wavelength, pulse settings, thresholds, reference data, etc. They contain one or more test programs.

Once the port detection is complete, the application creates three default test setups (that is, one per test type) for each of the detected optical routes:

- **Monitoring:** This type of test is ideal for a 24/7 surveillance of cable cuts or major degradation that affects QoS. In this case, reference, learning data, and optical fault trace results are stored in the EMS. Automatic test setup configuration for this type is 15 seconds as the target test time per port. It can be set at any other value. For this test setup, the test manager can select the fault detection threshold from three predefined alarming sensitivities: Coarse, Normal, or Sensitive.
- **Proactive Maintenance:** This type of test is ideal for running weekly or daily tests on a route to detect degradations that do not yet affect QoS. In case of proactive maintenance, all the results, including reference data, are stored into the EMS. This test detects faults and alerts when degradation level is above a specified set of fault detection thresholds. By default, the test time is 45 seconds and can be changed. Proactive maintenance is used for medium to long-term analysis of the network or to build historical trend results for the route automatically.
- **Test on Demand:** This type of test is conducted to check the health of fibers when required.

Operating Your RTU in OTDR Measuring Mode

Managing Test Setups



You can view, add, modify, and delete test setups.

- There are three types of tests. If you select **Proactive maintenance**, the results of the tests will *always* be saved.
- If you select **Monitoring**, the results will be saved only if they contain fault information.
- If you select **Test on Demand**, the **Server Data Upload** section and **Targeted count per cycle** field in the **Learning** section are disabled.
- You can select the high-resolution feature to obtain more data points per acquisition. This way, the data points will be closer to each other, which will result in a greater distance resolution for the trace.



IMPORTANT

EXFO does not recommend to test in high resolution if the acquisition time is less than 15 seconds. It may be impossible to obtain acceptable performance with this combination of settings.

- You can either set the acquisition parameters (range, pulse, duration) yourself or let the application determine the most appropriate values. In the latter case, the application will automatically evaluate the best settings according to the fiber link currently connected to the unit.
- To optimize event detection, you can set the following analysis detection thresholds:
 - **Splice loss threshold (dB):** To detect small non-reflective events during trace analysis.
 - **Reflectance threshold (dB):** To detect small reflective events during trace analysis.
 - **End-of-Fiber threshold (dB):** To detect important event loss that could compromise signal transmission during trace analysis.
- If you select the **Extended mode (peak monitoring)** option, the application will search the “noisy” portion of the OTDR trace to detect strong reflective events (such as those caused by UPC connectors) and set the monitoring range up to this point. The reflective peak level will be used as an indicator for link loss between end of fiber (RBS) and this point.

Note: *The application will take the option into account only if there is a significant reflective event located after the end of analysis.*

- You can set the fault detection thresholds. The application uses these thresholds when comparing the current measurement with reference trace to determine if there is a fault or not.

Operating Your RTU in OTDR Measuring Mode

Managing Test Setups

You can either select one of the predefined threshold sets (default or your own) or set the parameters manually. For information on how to create your own threshold sets, see *Managing Threshold Sets* on page 179.

If, after performing tests, you find that the fault detection is too sensitive, you can do one of the following:

- Select a less sensitive threshold set.
- Create a threshold set with custom values, and select it in the test setup. In this case, you will also need to perform a new reference.
- You can specify which data will be uploaded to the EMS server (not applicable when RTU is used in stand-alone mode). For more information, see *Defining Default Values for System Parameters* on page 153.

Normal is selected by default, but you can set the application to use another option by default (see *Managing System Setting Values* on page 146).

- You can define parameters for the learning process.

A learning phase is a key provisioning function in NQMSfiber. This function provides information about the fiber under test. It creates a series of statistics on the stability of the link loss and every event of the fiber reference trace. Stable events or sections can then be monitored more closely. The less stable events, such as the very far end portion of the trace, are obtained from the system with the best possible fault detection thresholds. The learning process consists of at least one cycle during which the application will perform the specified number of acquisitions to establish the fault detection parameters (limits, mean value). These parameters take into account the environmental variations occurring on the fiber during the learning process.

The first reference is created when you apply the changes from the RTU configuration window (gear icon). If a first reference has been created already, you can also create a new first reference using the

renew feature. If you modify the acquisition or analysis parameters, the application will prompt you to perform a new reference. For more information, see *Creating the Reference Traces* on page 174.

During the tests, each result will be compared to those of the reference trace.

You can specify the number of acquisitions that will be performed during a learning cycle.

You can also set the application to start new learning cycles when desired. The application can start the new cycle on a specific date or periodically (for example, every 2 weeks).

Note: *The application will only be able to start a new learning cycle if the previous one has at least started.*

You can even set the application to perform extra acquisitions when the learning cycle is complete (extend). The application can start the new acquisitions on a specific date or periodically until a certain number of acquisitions is reached. This maximum value corresponds to the number of acquisitions defined for a cycle plus the number of extra acquisitions.

The learning process will be performed only if at least one test program has been activated (enabled).

Operating Your RTU in OTDR Measuring Mode

Managing Test Setups

To view test setups:

1. From the main menu, select **Configuration > Remote Test Unit**.
2. From the tree view, select the **Optical Route** for which you want to view the test setups.

Status of test setup:


- Ready for reference:** setup is complete, but reference has not been performed yet (see *Creating the Reference Traces* on page 174)
- Reference complete:** reference performed and waiting for the learning cycle to begin
- Learning:** learning cycle is underway
- Testing:** learning cycle is complete and tests are performed
- Invalid parameters:** wavelength or pulse is invalid for the test setup
- Configuration change:** reference should be renewed by the user. If the optical route is resumed, all test setups which have a configuration change status will be set back to their previous state.(Learning, Testing, Referenced).

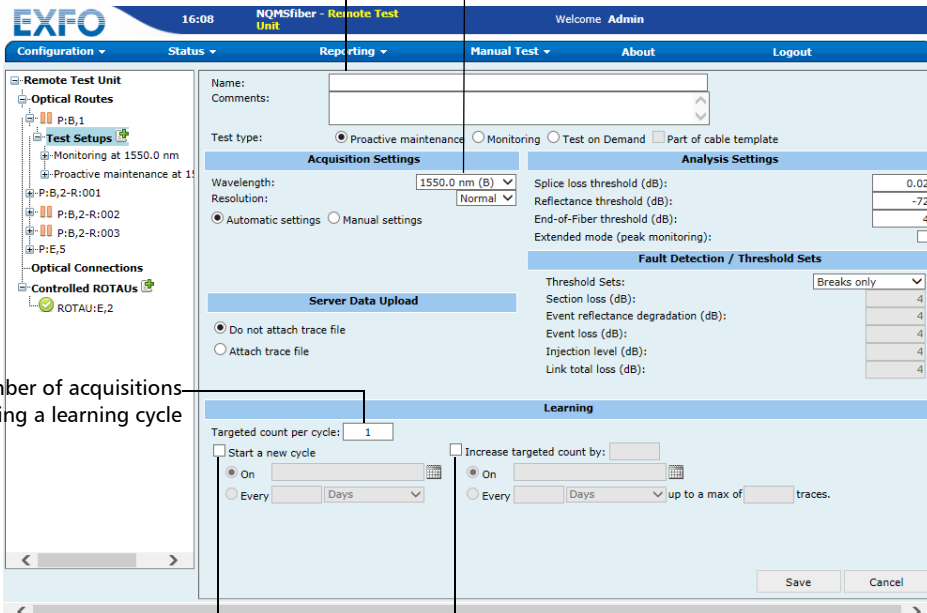
Name	Type	Status	OTAU Port	ROTAU Port
Monitoring at 1625.0 nm	Monitoring	Learning	A,1	
Proactive maintenance at 1625.0 nm	Proactive maintenance	Reference complete	A,1	

3. From the tree view, select **Test Setups**.

The application lists all the existing test setups.

To add test setups:

1. From the main menu, select **Configuration > Remote Test Unit**.
2. From the tree view, select an **Optical Route** and click the  icon that appears next to **Test Setups**.



Test setup name (mandatory)

Test wavelength (fiber code is indicated in parentheses)

Number of acquisitions during a learning cycle

To start a new learning cycle

To perform extra acquisitions when the learning cycle is complete

3. Enter the parameters according to your needs.
4. Click **Save** to create the test setup or **Cancel** to discard them.

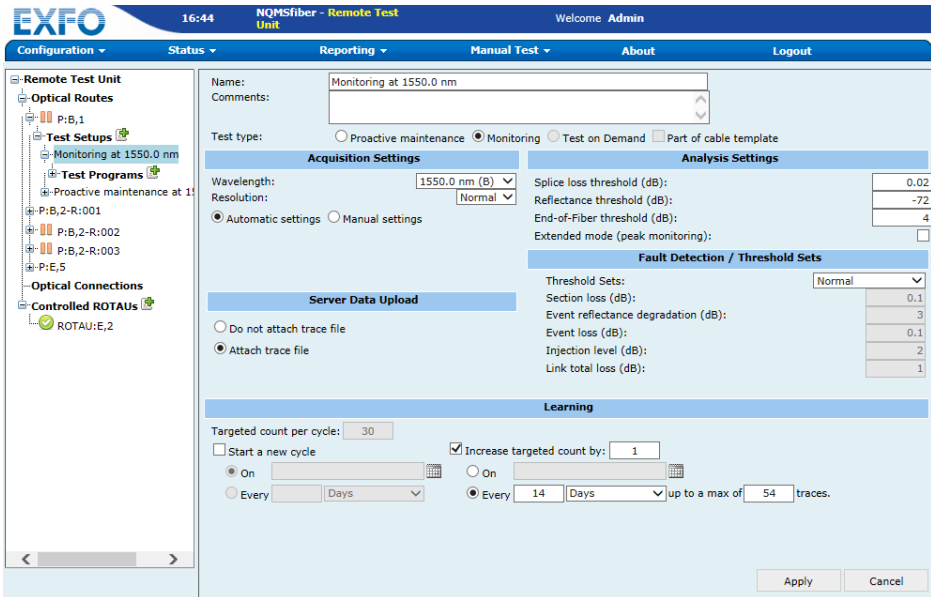
The application creates a **Test Programs** branch under the new test setup automatically. You can add test programs from this branch.

Operating Your RTU in OTDR Measuring Mode

Managing Test Setups

To modify test setups:

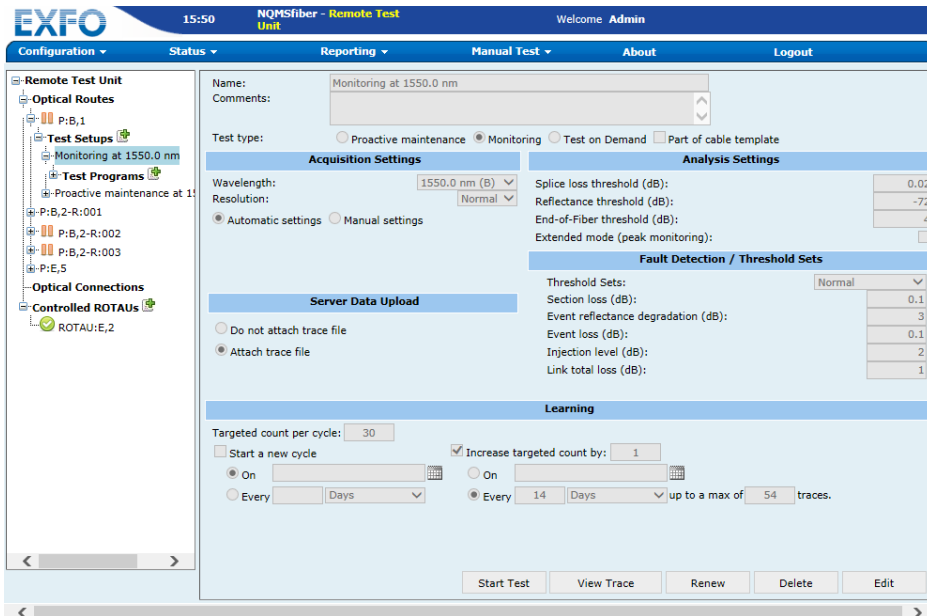
1. From the main menu, select **Configuration > Remote Test Unit > Optical Routes**.
2. From the **Optical Routes** tree view, select the optical route you want to modify.
3. Select **Test Setups** and the test.
4. Click **Edit**.



5. Modify the parameters according to your needs. For more information on the various parameters, see *Managing Test Setups* on page 165.
6. Click **Apply** to update changes or **Cancel** to discard them.

To delete test setups:

1. From the main menu, select **Configuration > Remote Test Unit > Optical Routes**.
2. From the **Optical Routes** tree view, select the optical route containing the test setup you want to delete.



3. Click **Delete**.
4. When the application prompts you, click **OK** to confirm deletion.



IMPORTANT

Except for default test setups that can be re-created by performing a new port detection, deleted test setups cannot be recovered. The associated test programs and results will be deleted as well.

Creating the Reference Traces

Before starting the learning process, the application must create the reference traces. They are created automatically just after a fiber detection, after a renew, and when a test setup is added or updated.

If you modify the acquisition or analysis parameters, the application will prompt you to perform a new reference. This reference will be independent from the previous one and a new learning process, based on this new reference, will also be scheduled. It is also possible to re-create a reference trace afterwards, if you have made a repair, for instance.

To re-create the reference trace for a specific test setup (acquisition and analysis settings unchanged):

- 1.** From the main menu, select **Configuration > Remote Test Unit > Optical Routes**.
- 2.** From the tree view, select the route containing the test setup for which you want to create a new reference.
- 3.** Select **Test Setups** and the test setup for which you want to create a new reference.
- 4.** Click **Renew**.

Managing Test Programs

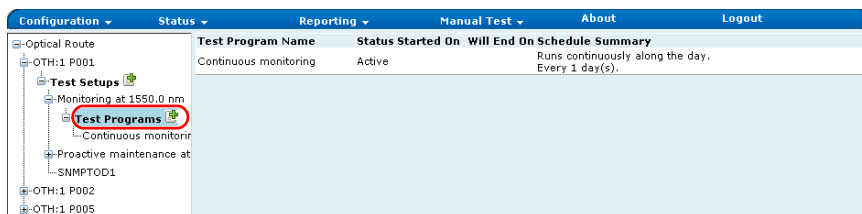
Test programs are part of test setups. They describe the start and end dates and periodicity of jobs, and this, either for continuous or scheduled monitoring, or periodic data acquisition (in proactive maintenance).

Once the port detection is complete, the application creates default test setups and test programs.

You can view, add, modify, and delete test programs. (Disabled when synchronized with an EMS.)

To view test programs:

1. From the main menu, select **Configuration > Remote Test Unit > Optical Routes**.
2. From the tree view, select the route containing the test setup for which you want to view the test programs.




3. Select **Test Setups**.
4. Then select the test for which you want to view the test programs, and select **Test Programs**.

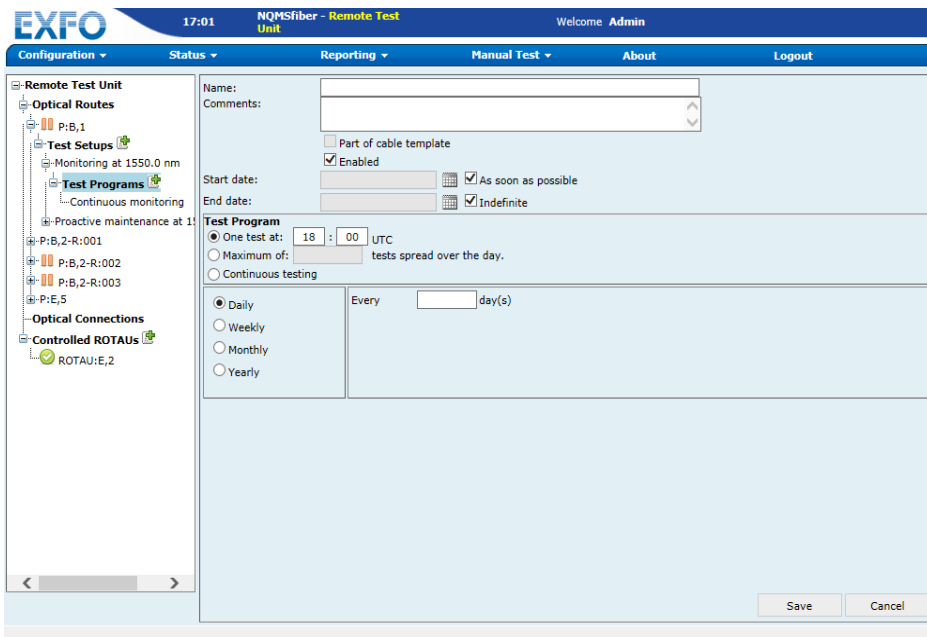
The application lists all the existing test programs for the selected test setup.

Operating Your RTU in OTDR Measuring Mode

Managing Test Programs

To add test programs:

1. From the main menu, select **Configuration > Remote Test Unit > Optical Routes**.
2. From the tree view, select the route containing the test setup for which you want to add test programs.
3. Select **Test Setups**.
4. Then select the test for which you want to add **Test Programs**.
5. Click the  icon that appears next to **Test Programs**.



The screenshot shows the EXFO NQMSfiber - Remote Test Unit configuration interface. The interface is divided into a left sidebar and a main configuration area. The sidebar shows a tree view of the configuration structure, including 'Remote Test Unit', 'Optical Routes', 'P:B,1', 'Test Setups', 'Monitoring at 1550.0 nm', 'Test Programs', and 'Controlled ROTAUs'. The main configuration area is titled 'Remote Test Unit' and contains the following fields and options:

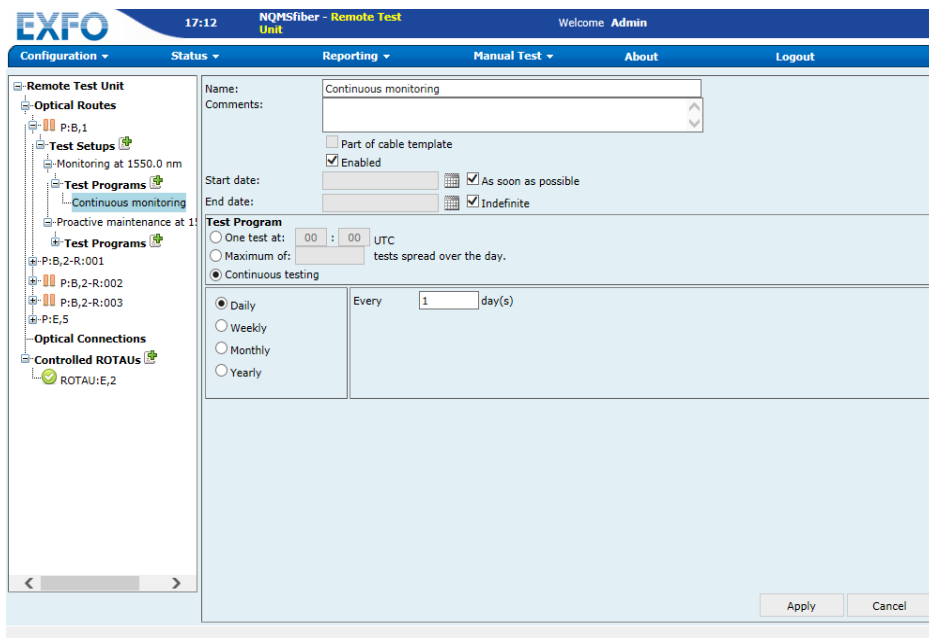
- Name:** A text input field.
- Comments:** A text input field.
- Part of cable template
- Enabled
- Start date:** A date picker field.
- As soon as possible
- End date:** A date picker field.
- Indefinite
- Test Program:**
 - One test at: 18 : 00 UTC
 - Maximum of: [] tests spread over the day.
 - Continuous testing
- Daily Every [] day(s)
- Weekly
- Monthly
- Yearly

At the bottom right of the configuration area, there are 'Save' and 'Cancel' buttons.

6. Enter the parameters according to your needs.
7. Click **Save** to create the test program or **Cancel** to discard them.

To modify test programs:

1. From the main menu, select **Configuration > Remote Test Unit > Optical Routes**.
2. From the tree view, select the route containing the test setup for which you want to modify test programs.
3. Expand the **Test Setups** branch and select the test setup for which you want to modify test programs.
4. Under **Test Programs**, select the item to modify.
5. Click **Edit**.



6. Modify the parameters according to your needs.
7. Click **Apply** to update changes or **Cancel** to discard them.

Operating Your RTU in OTDR Measuring Mode

Managing Test Programs

To delete test programs:

- 1.** From the main menu, select **Configuration > Remote Test Unit > Optical Routes**.
- 2.** From the tree view, select the route containing the test setup for which you want to delete test programs.
- 3.** Expand the **Test Setups** branch and select the test setup for which you want to delete test programs.
- 4.** Under **Test Programs**, select the item to delete.
- 5.** Click **Delete**.
- 6.** When the application prompts you, click **OK** to confirm deletion.



IMPORTANT

Except for default test programs that can be re-created by performing a new port detection, deleted test programs cannot be recovered.

Managing Threshold Sets

The RTU application comes with default threshold sets that you can use to define test setups. You can also create your own threshold sets, modify and delete them.

Note: You cannot modify or delete the default threshold sets.

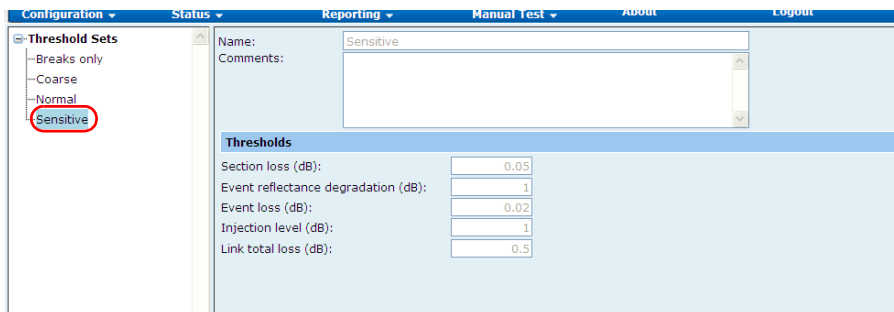
Note: You must be logged in as **Admin** username to be able to create threshold sets.

If, after performing tests, you find that the fault detection is too sensitive, you can do one of the following:

- Select a less sensitive threshold set.
- Create a threshold set with custom values, and select it in the test setup. In this case, you will also need to perform a new reference.

To view the threshold sets:

1. From the main menu, select **Configuration > Threshold Sets**.
2. From tree view, select the threshold set you want to view.




Note: You can only add, modify and delete software packages when the RTU is used in stand-alone mode.

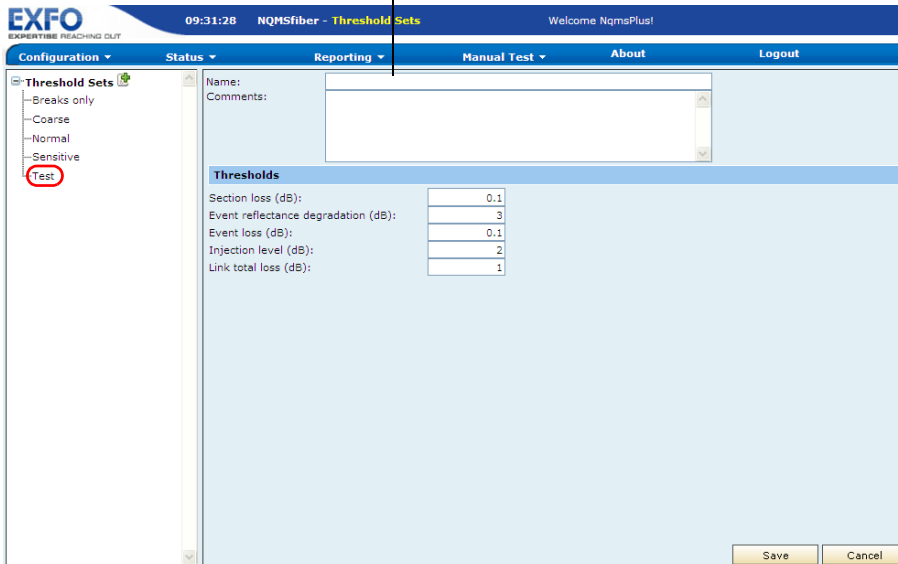
Operating Your RTU in OTDR Measuring Mode

Managing Threshold Sets

To add threshold sets:

1. From the main menu, select **Configuration > Threshold Sets**.
2. From the tree view, click the  icon that appears next to **Threshold Settings**.

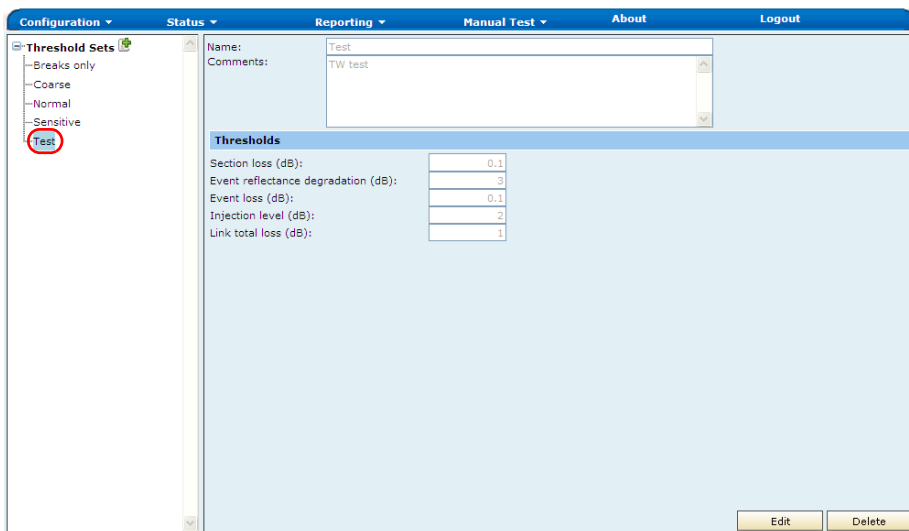
Threshold set name (mandatory)



3. Enter the parameters according to your needs.
4. Click **Save** to create the test setup or **Cancel** to discard it.

To modify threshold sets:

1. From the main menu, select **Configuration > Threshold Sets**.
2. From the tree view, select the threshold set you want to modify.



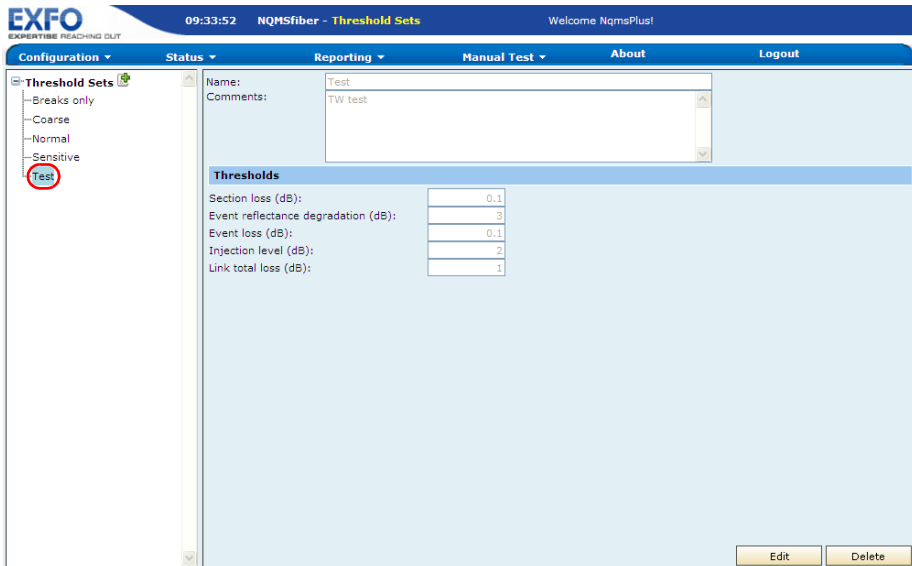
3. Click **Edit**.
4. Modify the parameters according to your needs.
5. Click **Apply** to update changes or **Cancel** to discard them.

Operating Your RTU in OTDR Measuring Mode

Managing Threshold Sets

To delete threshold sets:

1. From the main menu, select **Configuration > Threshold Sets**.
2. From the tree view, select the threshold set you want to delete.



3. Click **Delete**.
4. When the application prompts you, click **OK** to confirm deletion.

Performing an Ad Hoc Test

An ad hoc test is a manual test where you select the test parameters. The ad hoc test is useful when you want to perform a standard OTDR test on a specific port that is not detected. Such a test is also useful when you install a new RTU to ensure acquisitions are performed normally. The test is performed immediately after you start it.

When the RTU is used within a system, ad hoc test results are stored in the database, but not transferred to the EMS server.

The ad hoc test acquisition settings can be automated, where the pulse and range are automatically calculated, or manually set, where you enter your own values.

You can select the high-resolution feature to obtain more data points per acquisition. This way, the data points will be closer to each other, which will result in a greater distance resolution for the trace.



IMPORTANT

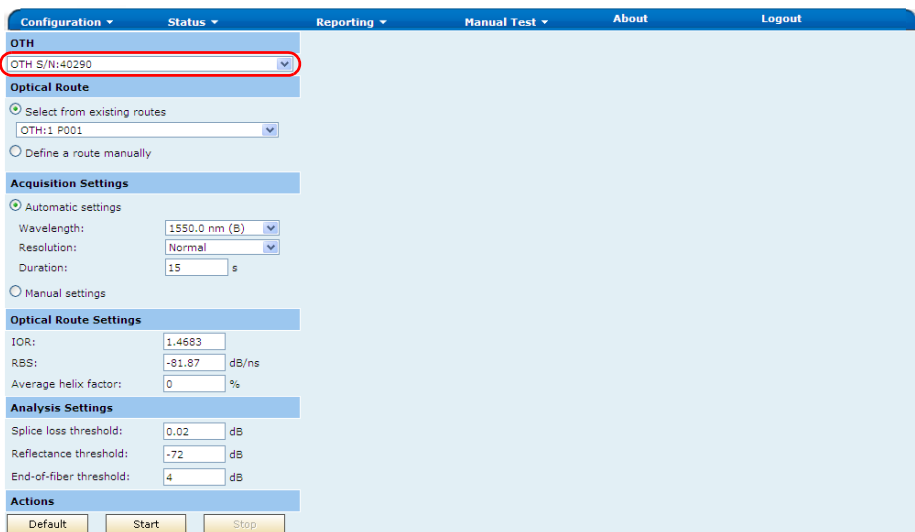
EXFO does not recommend to test in high resolution if the acquisition time is less than 15 seconds. It may be impossible to obtain acceptable performance with this combination of settings.

Operating Your RTU in OTDR Measuring Mode

Performing an Ad Hoc Test

To perform an ad hoc test:

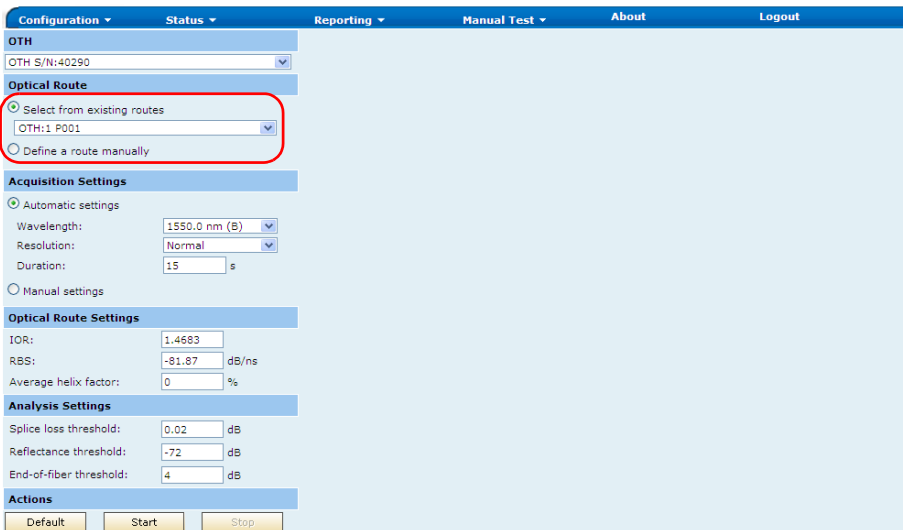
1. From the main menu, select **Manual Tests > Ad Hoc**.



2. Select an optical route in the **Select from existing routes** list. This option is available only if fiber detection has already been performed.

OR

Click **Define a route manually** and select a port from corresponding list.



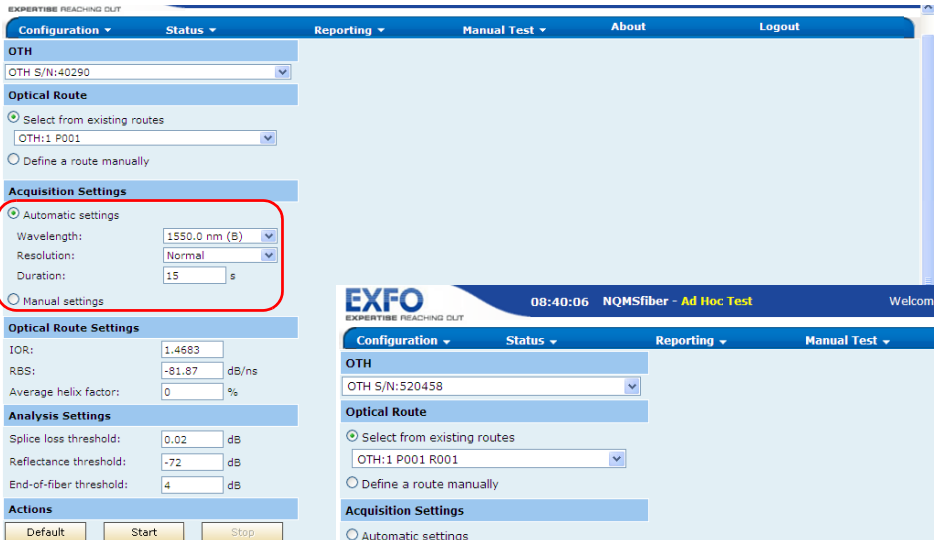
The screenshot displays the configuration interface for the OTDR Measuring Mode. The interface is organized into several sections:

- Configuration:** Includes a dropdown menu for 'OTH S/N:40290'.
- Optical Route:** This section is highlighted with a red box. It contains two radio button options: 'Select from existing routes' (which is selected) and 'Define a route manually'. Below the selected option is a dropdown menu showing 'OTH:1 P001'.
- Acquisition Settings:** Contains a radio button for 'Automatic settings' (selected) and 'Manual settings'. Under 'Automatic settings', there are three fields: 'Wavelength: 1550.0 nm (B)', 'Resolution: Normal', and 'Duration: 15 s'.
- Optical Route Settings:** Contains three input fields: 'IOR: 1.4683', 'RBS: -81.87 dB/ns', and 'Average helix factor: 0 %'.
- Analysis Settings:** Contains three input fields: 'Splice loss threshold: 0.02 dB', 'Reflectance threshold: -72 dB', and 'End-of-fiber threshold: 4 dB'.
- Actions:** Contains three buttons: 'Default', 'Start', and 'Stop'.

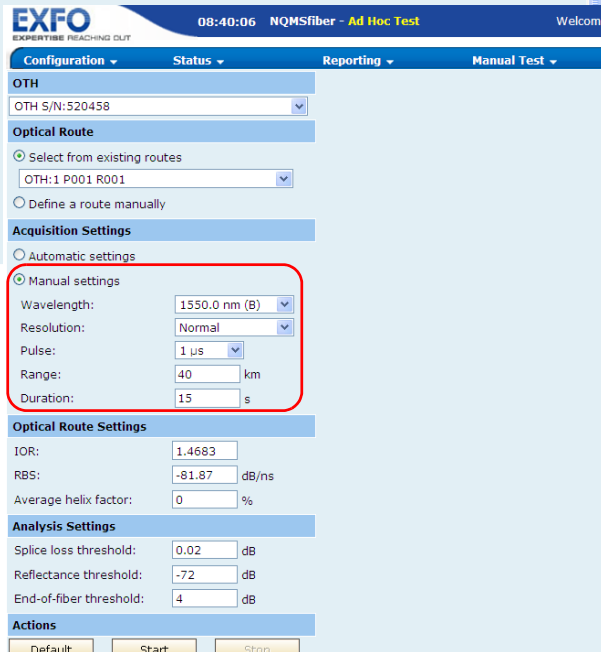
Operating Your RTU in OTDR Measuring Mode

Performing an Ad Hoc Test

3. Select the acquisition type. Depending on what you have selected, fill out the required values.



Automatic settings



Manual settings

4. Select the optical route settings required for your test.

The screenshot displays the configuration interface of an RTU. The top navigation bar includes 'Configuration', 'Status', 'Reporting', 'Manual Test', 'About', and 'Logout'. The main content area is divided into several sections:

- OTH**: A dropdown menu showing 'OTH S/N:40290'.
- Optical Route**: Two radio buttons. The first, 'Select from existing routes', is selected, with a dropdown menu showing 'OTH:1 P001'. The second, 'Define a route manually', is unselected.
- Acquisition Settings**: Two radio buttons. 'Automatic settings' is selected. Below it are three fields: 'Wavelength: 1550.0 nm (B)', 'Resolution: Normal', and 'Duration: 15 s'. 'Manual settings' is unselected.
- Optical Route Settings**: This section is highlighted with a red box. It contains three input fields: 'IOR: 1.4683', 'RBS: -81.87 dB/ns', and 'Average helix factor: 0 %'.
- Analysis Settings**: Three input fields: 'Splice loss threshold: 0.02 dB', 'Reflectance threshold: -72 dB', and 'End-of-fiber threshold: 4 dB'.
- Actions**: Three buttons: 'Default', 'Start', and 'Stop'.

Operating Your RTU in OTDR Measuring Mode

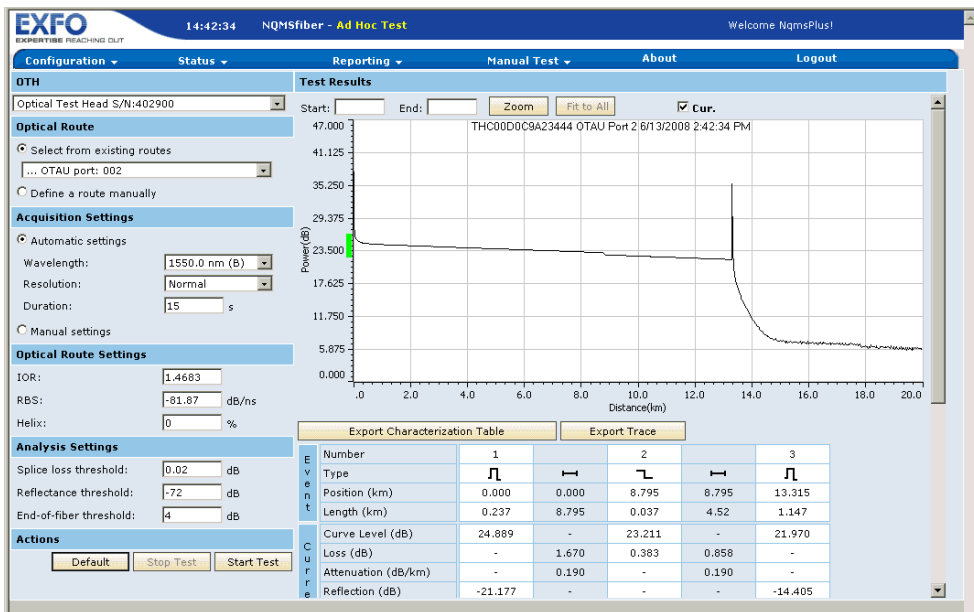
Performing an Ad Hoc Test

5. Enter the threshold values for your analysis.

The screenshot shows a web-based configuration interface for an OTDR. The interface is divided into several sections: OTH, Optical Route, Acquisition Settings, Optical Route Settings, Analysis Settings, and Actions. The Analysis Settings section is highlighted with a red box, indicating the focus of the task. The Analysis Settings section contains three input fields: Splice loss threshold (0.02 dB), Reflectance threshold (-72 dB), and End-of-fiber threshold (4 dB). The Actions section at the bottom contains three buttons: Default, Start, and Stop.

Section	Parameter	Value	Unit
Analysis Settings	Splice loss threshold	0.02	dB
	Reflectance threshold	-72	dB
	End-of-fiber threshold	4	dB

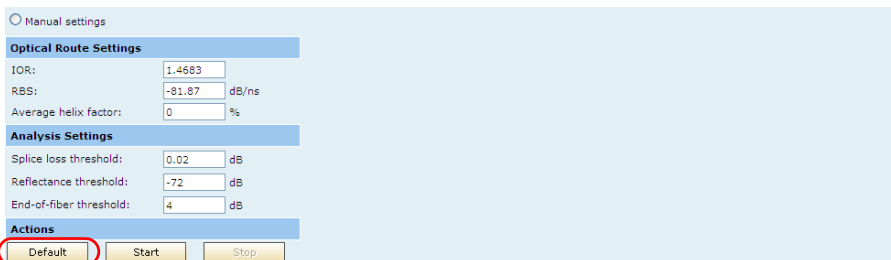
6. Click Start Test.



The application displays the results as soon as the test is complete.

To revert the test options to their default values:

1. On the **Manual Tests** menu, select **Ad Hoc**.



2. Click **Default**.

Performing a Test

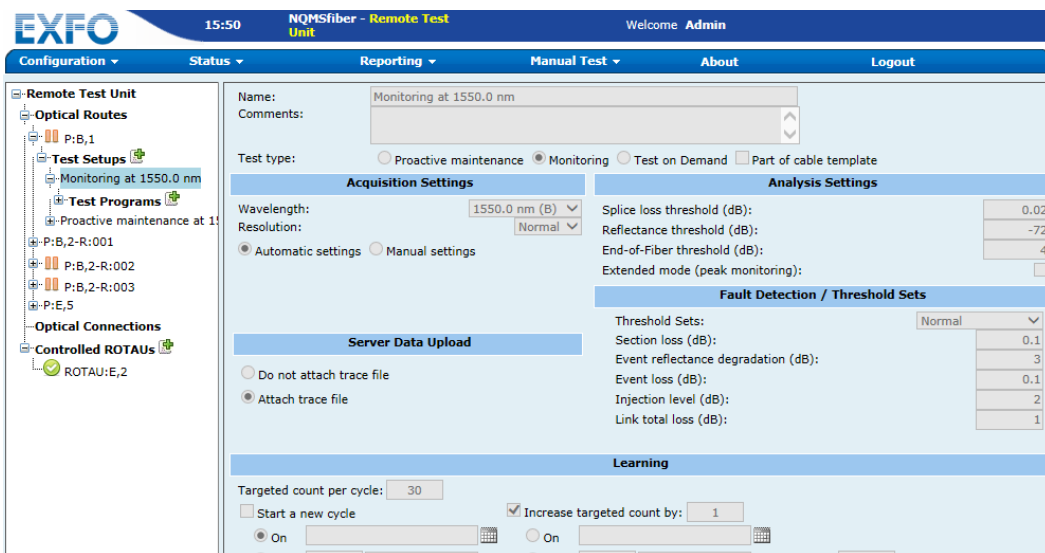
You can perform a test for optical routes that the RTU has created. This type of test is performed on a specific test setup. It is similar to a test program, except that it is not “scheduled” at a later time.

Only the test setups for which a reference has been created can be used to perform a test. For information on references, see *Creating the Reference Traces* on page 174.

You can also start a test from the current fault list window (see *Viewing the Current Fault List* on page 215).

To perform a test:

1. From the main menu, select **Configuration > Remote Test Unit > Optical Routes**.
2. From the tree view, select the route containing the test setup you want to use for your test.
3. Select **Test Setups** and the test setup you want to use for your test.



4. Click **Start Test**.

The test is sent to the test queue, waiting to be performed.

Note: *If there was a fault before you started the test, this fault will be cleared and re-created (fault status will be set as New) if it is still present.*

Managing Degraded Fibers

The degraded fiber handling strategy feature allows you to capture unstable fiber conditions which were not captured on existing learning processes, such as a fast reflectance change, or a mechanical stress that can make loss to change on a minute or so time frame. If degradation (fluctuating link) is observed continuously in a test setup of an optical route, the link is skipped and no further tests are performed on it. This process reduces the number of fault sync requests and improves performance.

Note: *The degraded fiber handling strategy can be disabled to capture fast transient conditions. It is recommended to enable it for higher performance and elimination of spurious faults (RTU) and alarms (EMS). The degraded fiber handling strategy applies to test setup of monitoring type only.*

To enable/disable degraded fiber handling strategy:

1. From the main menu, select **Configuration > System Settings > Default Settings**.
2. From the tree view, select **System**.

Parameter	Factory Setting	Current Default	
Break strategy	Skip	Skip	Edit
Degraded fiber handling strategy	Enabled	Enabled	Edit
Test setup definition strategy	Both	Both	Edit
Server data upload policy	Attach trace file	Attach trace file	Edit
ROTAU control delay (s)	5	5	Edit
ROTAU communication frequency (s)	300	300	Edit
ROTAU failed communication attempts before alert	3	3	Edit
Maximum log entries in database	50000	50000	Edit
Maximum result entries in database	5000	5000	Edit
Maximum fault entries in			

3. Click **Edit** to enable or disable the degraded fiber handling strategy.

Enabling or disabling degraded fiber handling strategy from the EMS updates the factory settings on the RTU and not the individual current default for each RTU.

If the degraded fiber handling strategy is enabled on the RTU and a fault is in any of the following states on EMS: New, Still There, or Changed, then the optical routes are skipped and the alarm remains open on the EMS side.

If the fault is manually cleared from the RTU, the alarm will be resolved.

If the alarm is resolved from the EMS and the fault is still present, a new alarm is opened in the next planned synch.

Note: *The degraded fiber handling strategy settings should be changed on each RTU application.*

4. Click **Apply** to update the changes or **Cancel** to discard them.

Operating Your RTU in OTDR Measuring Mode

Managing Degraded Fibers

The fiber is classified as degraded under the following criteria:

Criterion 1: Three jobs are observed. The link is disabled if any of the following conditions are satisfied:

- There are two new jobs and one cleared job.

Date	Job ID	Description	Monitoring	OTAU	ROTAU	Duration	Status	Link
2012-11-27 07:15:53	OTH:1 P004 R059	Monitoring at 1625.0 nm	Monitoring	4	59	40 s	Failed	Still there
2012-11-27 07:15:07	OTH:1 P004 R056	Monitoring at 1625.0 nm	Monitoring	4	66	40 s	Failed	Still there
2012-11-27 07:13:53	OTH:1 P004 R059	Monitoring at 1625.0 nm	Monitoring	4	59	40 s	Failed	New
2012-11-27 07:12:53	OTH:1 P004 R056	Monitoring at 1625.0 nm	Monitoring	4	66	40 s	Failed	New
2012-11-27 07:11:57	OTH:1 P004 R059	Monitoring at 1625.0 nm	Monitoring	4	59	44 s	Failed	Cleared
2012-11-27 07:10:54	OTH:1 P004 R056	Monitoring at 1625.0 nm	Monitoring	4	56	41 s	Failed	New
2012-11-27 07:09:52	OTH:1 P004 R059	Monitoring at 1625.0 nm	Monitoring	4	59	40 s	Failed	New
2012-11-27 07:08:53	OTH:1 P004 R056	Monitoring at 1625.0 nm	Monitoring	4	56	43 s	Failed	Still there

- Three consecutive jobs bear the changed state.

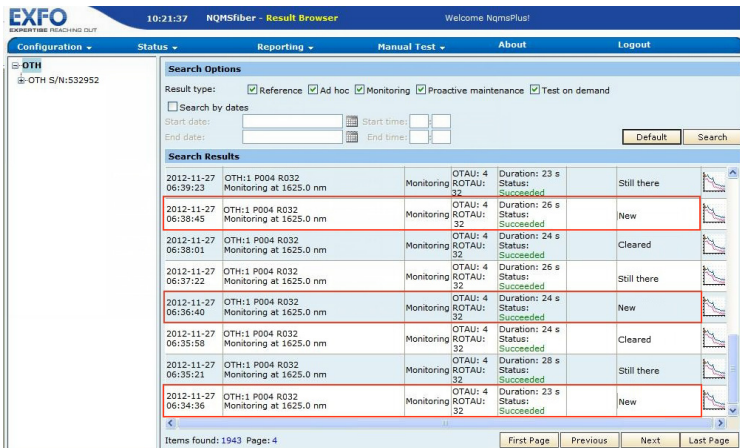
Date	Job ID	Description	Monitoring	OTAU	ROTAU	Duration	Status	Link
2012-11-27 06:39:23	OTH:1 P004 R032	Monitoring at 1625.0 nm	Monitoring	4	32	23 s	Failed	Changed
2012-11-27 06:38:45	OTH:1 P004 R032	Monitoring at 1625.0 nm	Monitoring	4	32	26 s	Failed	Changed
2012-11-27 06:38:01	OTH:1 P004 R032	Monitoring at 1625.0 nm	Monitoring	4	32	24 s	Failed	Changed
2012-11-27 06:37:22	OTH:1 P004 R032	Monitoring at 1625.0 nm	Monitoring	4	32	26 s	Failed	Changed
2012-11-27 06:36:40	OTH:1 P004 R032	Monitoring at 1625.0 nm	Monitoring	4	32	24 s	Failed	Still there
2012-11-27 06:35:58	OTH:1 P004 R032	Monitoring at 1625.0 nm	Monitoring	4	32	24 s	Failed	Still there
2012-11-27 06:35:21	OTH:1 P004 R032	Monitoring at 1625.0 nm	Monitoring	4	32	28 s	Failed	Still there
2012-11-27 06:34:36	OTH:1 P004 R032	Monitoring at 1625.0 nm	Monitoring	4	32	23 s	Failed	New

Operating Your RTU in OTDR Measuring Mode

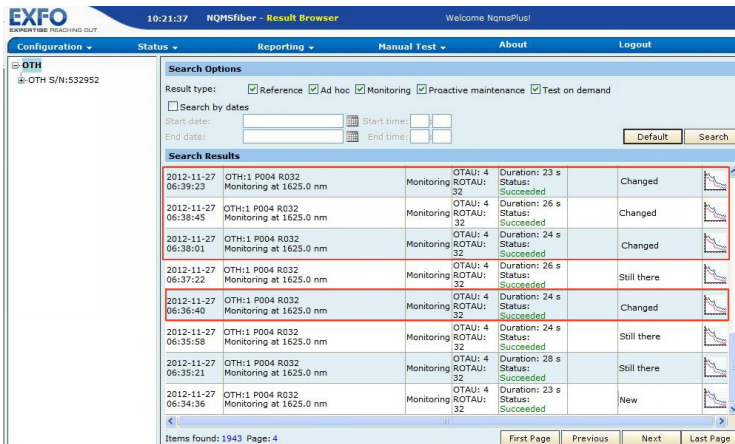
Managing Degraded Fibers

Criterion 2: If Criterion 1 is not satisfied, then ten jobs are observed. The link is disabled if any of the following conditions are satisfied:

- There are three or more new jobs over ten jobs.



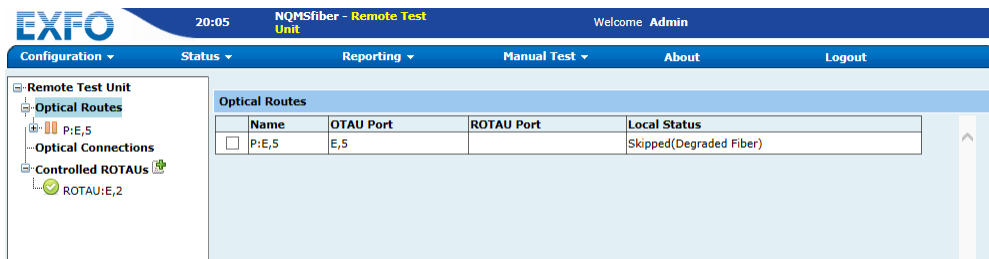
- The state of more than three job has changed.



Operating Your RTU in OTDR Measuring Mode

Managing Degraded Fibers

If any of the above criterion is satisfied, the status of the optical route is changed to Skipped due to degraded fiber on the **Configuration > Optical Routes** page and no tests are performed.



The screenshot displays the EXFO NQMSfiber - Remote Test Unit interface. The top navigation bar includes the EXFO logo, the time 20:05, the unit name NQMSfiber - Remote Test Unit, and the user name Admin. Below the navigation bar, there are several tabs: Configuration, Status, Reporting, Manual Test, About, and Logout. The left sidebar shows a tree view with the following items: Remote Test Unit, Optical Routes (selected), Optical Connections, and Controlled ROTAs. The main content area displays the Optical Routes table.

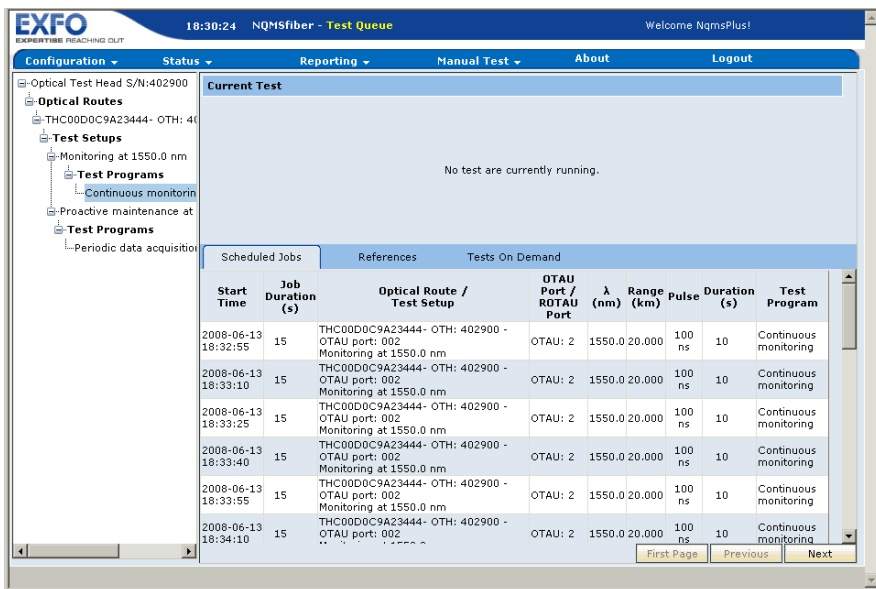
	Name	OTAU Port	ROTAU Port	Local Status
<input type="checkbox"/>	P:E,5	E,5		Skipped(Degraded Fiber)

Viewing Current and Scheduled Jobs

The test queue allows you to view the test that is underway, the scheduled jobs, the references, and the tests on demand that are waiting to be performed. You can view all of the jobs or only those associated with a specific test setup.

To view current and scheduled jobs:

1. From the main menu, select **Status > Test Queue**.
2. If you want to narrow down your search, from the tree view, select the desired test setup.



3. Click the tab corresponding to the type of jobs for which you want to see the status.

Configuring the Notification Agent

The Notification Agent is an application that you can install on any computer that can “view” the RTUs, which usually means that the computer and RTUs are connected to the same network. It monitors one or several RTUs and warns you whenever faults are detected.

From the Notification Agent, you can switch directly to the RTU login window to access the RTU Web application. Once you are connected to the RTU application, the list of recent faults is automatically displayed, allowing you to retrieve some more information about the detected faults.

You can specify the frequency (in seconds) at which the Notification Agent communicates with the monitored RTUs to retrieve the number of faults. You can also specify for how long the notification messages should be displayed.




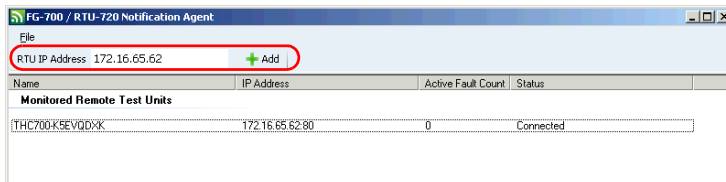
IMPORTANT

By exiting the application (from the File menu or with the ) , the Notification Agent will stop monitoring the listed RTUs.

Before proceeding with the Notification Agent, ensure that it has been installed on your computer. For more information on the installation, see *Installing the Notification Agent on Your Computer* on page 85.

To add an RTU to the list of monitored units:

1. If necessary, from the computer's desktop, double-click the  icon to open the Notification Agent.
2. In the **RTU IP address** box, enter the IP address of the RTU to be monitored.



3. Click **Add**. The application will verify the connection with the RTU.
4. When the application displays a message indicating that the diagnostic was completed successfully, click **OK**.

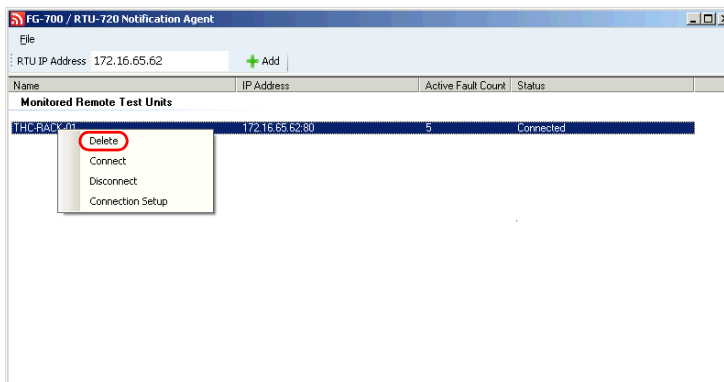
The RTU will now be monitored automatically.

Operating Your RTU in OTDR Measuring Mode

Configuring the Notification Agent

To remove an RTU from the list of monitored units:

1. Right-click the row corresponding to the RTU to be removed.



IMPORTANT

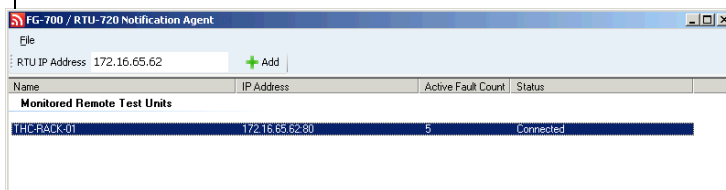
Once you click Delete, the RTU is removed from the list without any further confirmation or warning.

2. Click **Delete**.

To switch to the RTU application for more information about the detected faults:

1. Double-click the row corresponding to the RTU for which faults have been detected.

Icon in the title bar and in the Windows status bar turns to red to indicate that faults have been detected



Note: You can also double-click any notification message while it is displayed to open the RTU logon window.

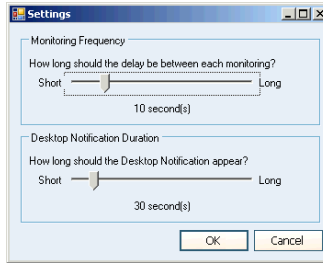
2. When the RTU logon window is displayed, enter your user name and password.

Operating Your RTU in OTDR Measuring Mode

Configuring the Notification Agent

To adjust the monitoring and notification parameters:

1. From the **File** menu, select **Settings**.
2. Use the sliders to adjust the monitoring and notification parameters to your needs.



3. Click **OK** to confirm the changes or **Cancel** to discard them.

Managing Cable Templates

The cable templates feature is particularly useful if you want to test many fibers that are all part of a same cable, using the same parameters. Instead of having to define test setups and test programs on each of the optical routes with the desired parameters, you can simply define one template per wavelength.

The application will schedule the tests automatically according to the parameters that you have set.

You can retrieve all the results acquired with a cable template at the same time and export them if desired.

Once you have modified the acquisition or analysis parameters, the application will prompt you to perform a new reference. This reference measurement will be performed on each of the selected ports with the defined parameters. As long as the reference has not been performed, the template will not be used.

You can view, add, copy, modify and delete templates.

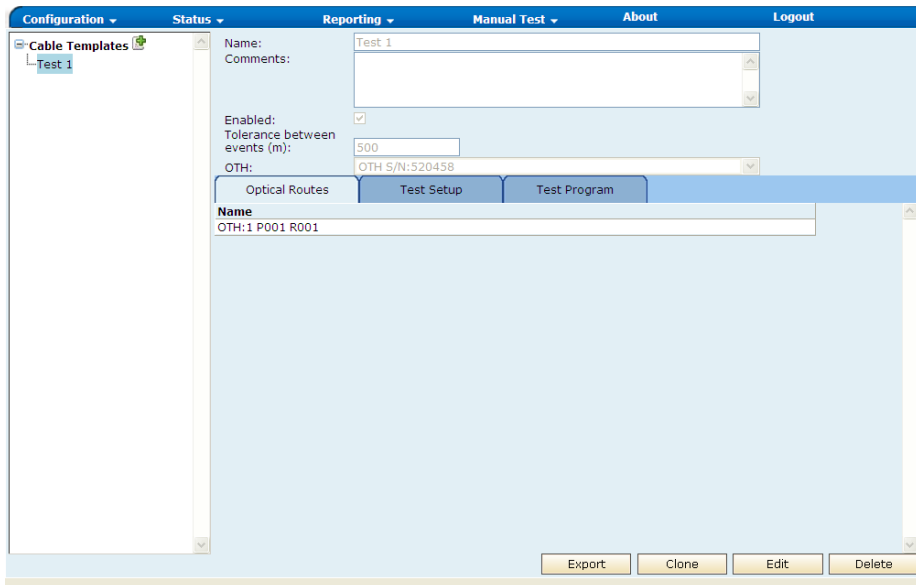
Viewing Cable Templates

You can view all the cable templates that have already been defined.

To view cable templates

From the main menu, select **Configuration > Cable Templates**.

The application lists all the cable templates that have been defined.



Adding Cable Templates

For each template, you have to specify the following items:


- Tolerance between events, in meters (for fibers to be considered as identical).
- Optical routes on which the tests will be performed.
- Parameters related to the test setup (see *Managing Test Setups* on page 165).
 - You can specify only one wavelength per template.
 - The provided values correspond to the default values associated with the proactive maintenance test setup (see *Defining Default Values for Test Setups* on page 151).
- Parameters related to the test program (see *Managing Test Programs* on page 175).

If you modify the acquisition or analysis parameters, the application will prompt you to perform a reference. For more information, see *Creating the Reference Traces* on page 174.

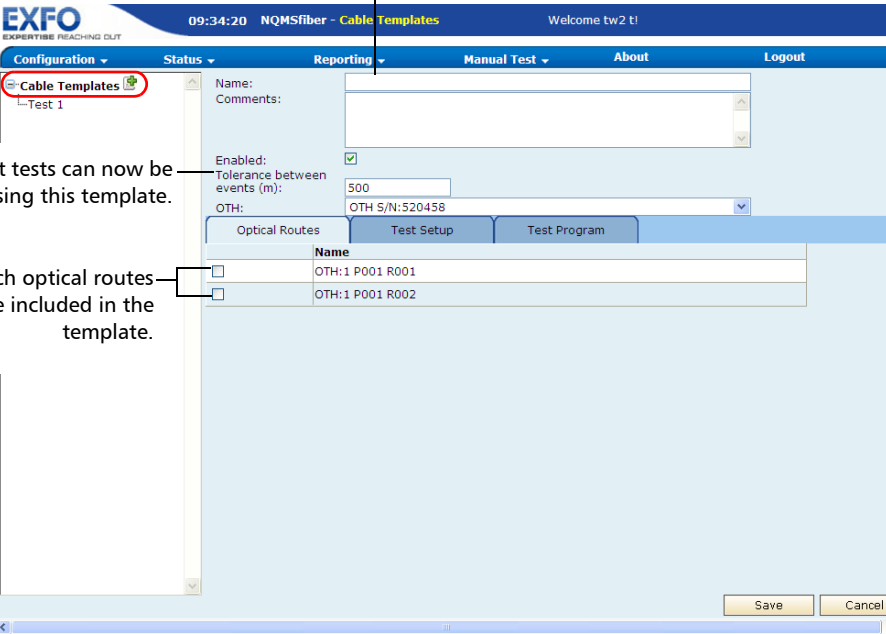
Operating Your RTU in OTDR Measuring Mode

Managing Cable Templates

To add cable templates:

1. From the main menu, select **Configuration > Cable Templates**.
2. From the tree view, click the  icon that appears next to **Cable Templates**.

Cable template name (mandatory)



To indicate that tests can now be performed using this template.

To specify which optical routes must be included in the template.

3. Enter the general parameters according to your needs.
4. Specify the optical routes that you want to include in the cable template.

5. Define the test setup parameters as follows:

5a. Select the **Test Setup** tab.

5b. Enter the parameters according to your needs.



IMPORTANT

EXFO does not recommend to test in high resolution if the acquisition time is less than 15 seconds. It may be impossible to obtain acceptable performance with this combination of settings.

Test wavelength (one wavelength per template).
Fiber code is indicated between parentheses.

To use default threshold sets or your own threshold sets (see *Managing Threshold Sets* on page 179)

To specify which data will be transferred to the server (not used with stand-alone RTU)

To define the fault detection parameters manually

Operating Your RTU in OTDR Measuring Mode

Managing Cable Templates

6. Define the test program parameters as follows:
 - 6a. Select the **Test Program** tab.
 - 6b. Enter the parameters according to your needs.

The screenshot displays the 'Test Program' configuration window for a cable template named 'Test 1'. The window has a blue header with menu options: Configuration, Status, Reporting, Manual Test, About, and Logout. On the left, a tree view shows 'Cable Templates' with 'Test 1' selected. The main area contains the following fields and options:

- Name: Test 1
- Comments: (empty text area)
- Enabled:
- Tolerance between events (m): 500
- OTH: OTH S/N:520458
- Start date: (calendar icon)
- End date: (calendar icon)
- One test at: 16 : 00 GMT
- Frequency: Weekly
- Every: 1 week(s)
- On days: Sunday Monday Tuesday Wednesday Thursday Friday Saturday
- Options: As soon as possible, Indefinite

At the bottom right, there are 'Apply' and 'Cancel' buttons.

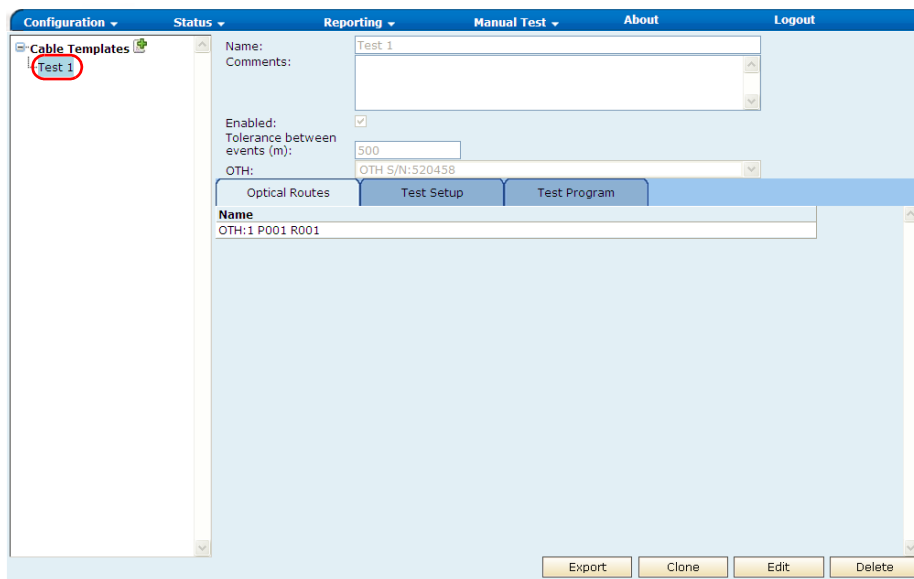
7. Click **Apply** to create the cable template or **Cancel** to discard it.

Modifying Cable Templates

You can enable or disable a specific template, modify the target learning count value and the parameters related to the test program (time and frequency at which the test will be performed). For any other parameter (wavelength, optical route, etc.), you will have to build a new template.

To modify cable templates:

1. From the main menu, select **Configuration > Cable Templates**.
2. From the tree view, select the cable template that you want to modify.



3. Click **Edit**.
4. Modify the parameters according to your needs.
5. Click **Apply** to apply changes, or **Cancel** to discard them.

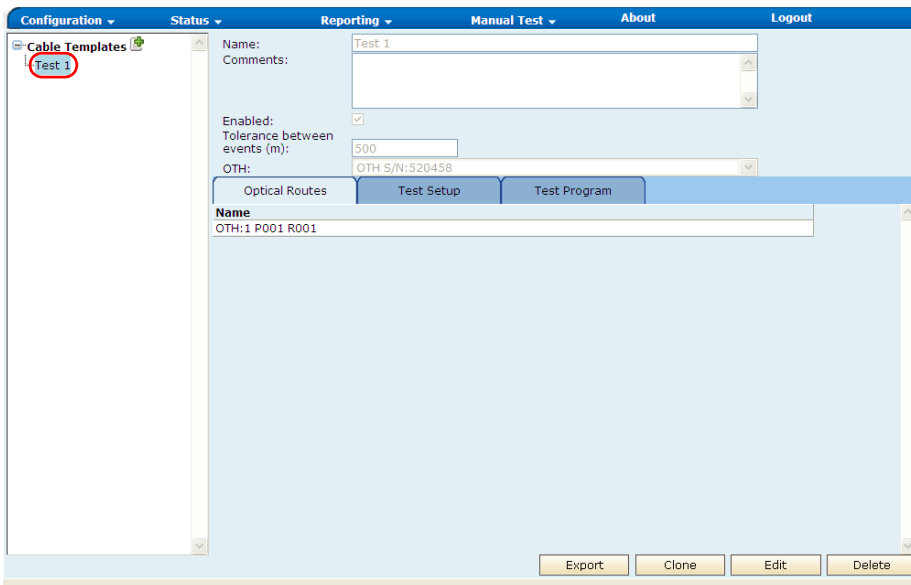
Copying Cable Templates

To speed up the creation of cable templates, you can duplicate existing templates and only have to modify a few parameters.

If you modify the acquisition or analysis parameters, the application will prompt you to perform a reference. For more information, see *Creating the Reference Traces* on page 174.

To copy cable templates:

1. From the main menu, select **Configuration > Cable Templates**.
2. From the tree view, select the cable template that you want to duplicate.



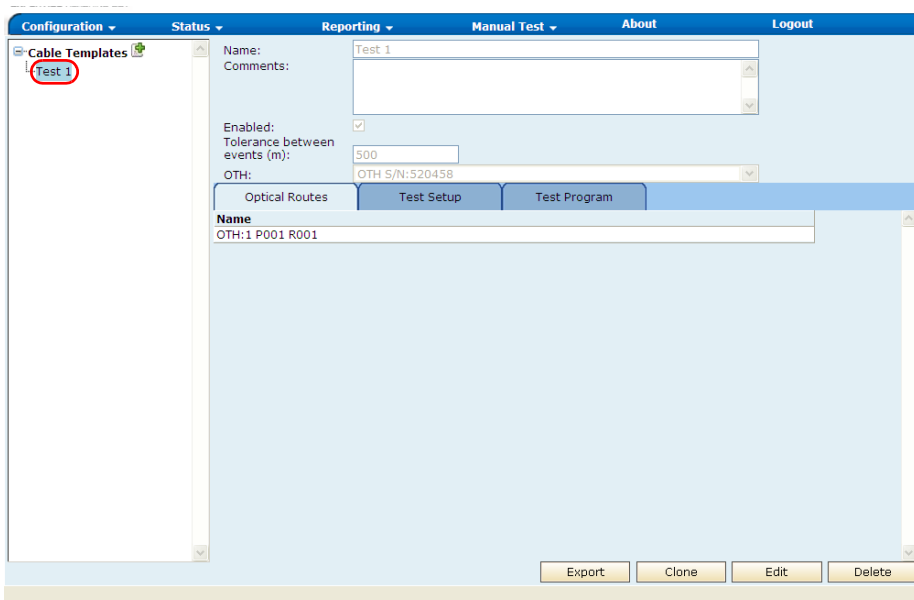
3. Click **Clone**.
4. Modify the parameters according to your needs.
5. Click **Save** to apply changes, or **Cancel** to discard them.

Deleting Cable Templates

You can delete cable templates at any time.

To delete cable templates:

1. From the main menu, select **Configuration > Cable Templates**.
2. From the tree view, select the template you want to delete.



3. Click **Delete**.
4. When the application prompts you, click **OK** to confirm deletion.

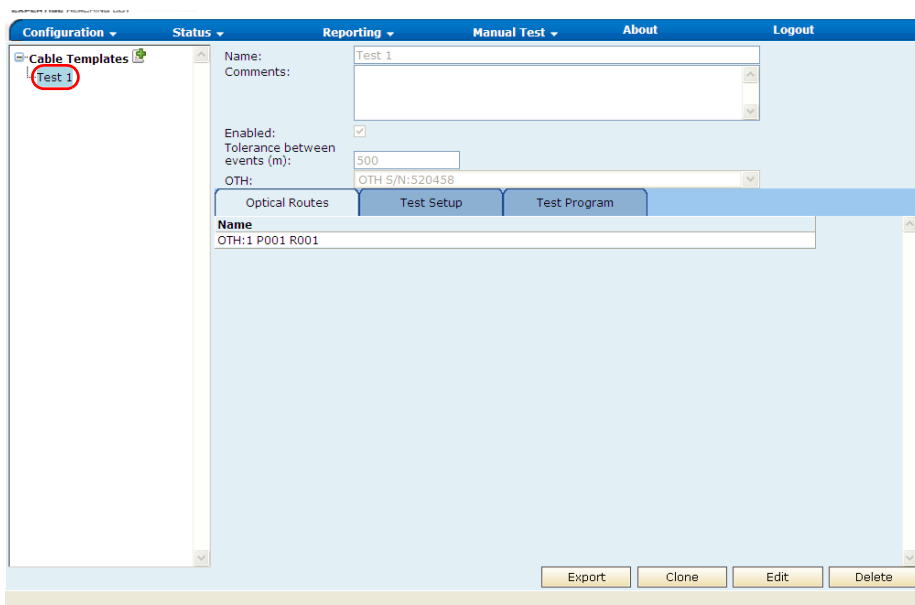
Exporting Cable Template Results


You can either view the cable template results in Microsoft Excel or save them in a .csv format. This could be useful if you prefer to work with raw data and build your own reports.

By default, the start date corresponds to the date on which the first measurement has been performed. Similarly, the end date corresponds to the date on which the last measurement has been performed.

To export cable templates results:

1. From the main menu, select **Configuration > Cable Templates**.
2. From the tree view, select the template for which you want to export the results.



- 3.** Click **Export**.
- 4.** If you wish to limit the results to a specific period of time, from the displayed dialog box, specify the start and end dates using the  buttons.
- 5.** When the application prompts you, you can either open the results directly in Microsoft Excel or save them.

8 **Analyzing Results**

The RTU application is a Web interface for accessing each RTU directly using a Web browser. The RTU application can provide access to each RTU locally via a LAN, or remotely via a dialup connection.

Viewing the Current Fault List

By default, the current fault list is displayed when you start the RTU application.

You can export the list of faults, clear faults and start a test (test on demand) from the current fault list window (see *Viewing, Exporting and Clearing Faults* on page 216).

For each of the faults, you can view the corresponding OTDR trace and characterization table for advanced analysis (see *Analyzing the OTDR Trace and Characterization Table* on page 217).

Analyzing Results

Viewing the Current Fault List

Viewing, Exporting and Clearing Faults

You can export the list of faults to a .csv (comma separated values) file and clear faults from the current fault list window.

To view the current fault list:

From the main menu, select **Status > Current Faults**.

A summary of the current faults is displayed.

The screenshot displays the EXFO NQMSfiber - Current Faults interface. The top navigation bar includes 'Configuration', 'Status', 'Reporting', 'Manual Test', 'About', and 'Logout'. The main content area is titled 'Recent Faults' and contains a table with the following data:

Last Update	Status	Type	Degradation (dB)	Position (km)	Position (km) (Min./Max.)	Optical Route/Test Setup
<input checked="" type="checkbox"/> 2010-10-04 07:17:59	New	Break	14.423	8.804	Min.: 8.788 Max.: 8.825	OTH:1 P001 Monitoring at 1550.0 nm

At the bottom of the interface, there are three buttons: 'Export All', 'Clear', and 'Start Test'.

To export the list of *all* recent faults to a .csv file

To clear (remove) the selected faults

To start tests using the test setups for which the selected faults occurred (equivalent to performing a test on demand on the route whose test setup created the event)

Analyzing the OTDR Trace and Characterization Table

If you are an experienced user, you will find the Trace Viewer particularly useful. With this utility, you can make a complementary analysis of the optical fiber link. By comparing the current OTDR measurement to the four other results provided (reference, minimum, maximum, and average), you may be able to give a more complete evaluation of the optical link's state than what the application achieves by itself.

- The reference corresponds to the OTDR measurement that was made the very first time the test setup was run. The analysis of this first OTDR measurement determined the structure of the event characterization table that is associated to the test setup.
- During the learning period, many measurements are made on the test setup. At each distance position of the OTDR measurement, the application keeps the minimum value measured. The *Min* trace corresponds to a “reconstruction” of an OTDR measurement, using the minimum value measured at each distance position.
- In a very similar way, the *Max* trace displays a “reconstruction” of an OTDR measurement, using the maximum value measured at each distance position.
- Finally, during the learning period, at each distance position of the OTDR measurement, the application keeps the average value. The *Avg* trace corresponds to a “reconstruction” of an OTDR measurement, using the average value calculated at each distance position.

Analyzing Results

Viewing the Current Fault List

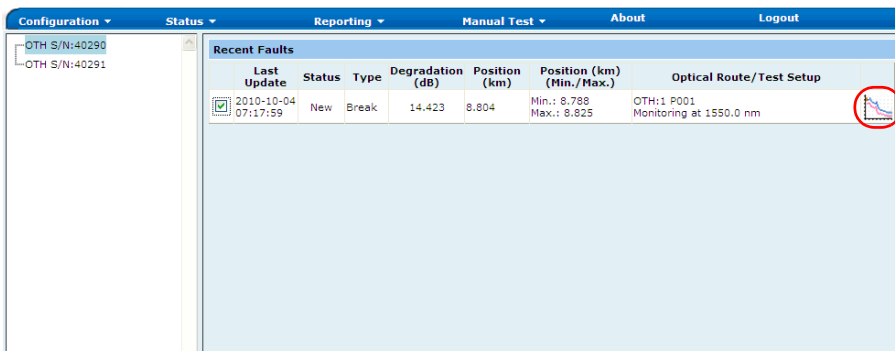
You can zoom in on a specific portion of the graph. You can also quickly return to the complete graph view.

You can save (export) the OTDR trace in native .trc format. You will be able to open the trace with applications that support this format of file, such as EXFO's FastReporter.

You can also either view the characterization table in Microsoft Excel or save it in a .csv format. This could be useful if you prefer to work with raw data and build your own reports.

To view the OTDR trace and the characterization table:

1. From the main menu, select **Status > Current Faults**.
2. On the row corresponding to the fault for which you want to view the OTDR graph and event table, click the graph icon.



The screenshot shows the application interface with a navigation bar at the top containing 'Configuration', 'Status', 'Reporting', 'Manual Test', 'About', and 'Logout'. On the left, there is a sidebar with 'OTH S/N:40290' and 'OTH S/N:40291'. The main area displays a table titled 'Recent Faults' with the following data:

Last Update	Status	Type	Degradation (dB)	Position (km)	Position (km) (Min./Max.)	Optical Route/Test Setup
2010-10-04 07:17:59	New	Break	14.423	8.804	Min.: 8.788 Max.: 8.825	OTH:1 P001 Monitoring at 1550.0 nm

A small graph icon in the rightmost column of the table is circled in red.

The application displays the OTDR graph and the characterization table.

To define the first (Start) and last (End) points of the zoom area, in kilometers.

To select which trace will be displayed on the graph.

Information on events

Current trace results

Reference trace results (expand the items for detailed information)

Event List		1	1.1	1.2	2	3	4	5
Type	Σ	Π	Π	Π	Π	Π	Π	Π
Position (km)	0.000	0.000	0.006	0.000	2.239	2.239	4.473	4.970
Length (km)	0.013	0.006	-	2.239	0.007	2.234	0.02	0.496
Curve Level (dB)	16.206	-	-	-	15.709	-	15.213	-
Loss (dB)	-	-	-	0.497	-0.008	0.503	-	-
Attenuation (dB/km)	-	-	-	0.222	-	0.225	-	-
Reflection (dB)	-66.550	-66.583	-68.439	-	-54.017	-	-40.288	-
Reflective Peak (dB)	22.317	22.317	21.818	-	22.771	-	29.057	-
Cumulative Loss (dB)	0.000	0.000	0.000	0.497	0.490	0.993	0.993	-
Curve Level (dB)	16.212	-	-	-	15.722	-	15.223	-
Loss (dB)	-	-	-	0.490	-0.011	0.510	-	0.908
Attenuation (dB/km)	-	-	-	0.219	-	0.228	-	-
Reflection (dB)	-66.539	-66.539	-68.394	-	-54.045	-	-40.290	-
Reflective Peak (dB)	22.320	22.320	21.829	-	22.771	-	29.065	-
Cumulative Loss (dB)	0.000	0.000	0.000	0.490	0.479	0.990	0.990	-

Test Properties		Result Properties	
Property	Value	Property	Value
Wavelength (nm)	1650.0	Actual range (km)	10.0
Auto settings	Yes	Actual pulse (ns)	30
Resolution	Normal	Actual duration (s)	10
Fiber code	B	Extended range (km)	4.494
Average helix factor (%)	0	RBS range (km)	4.473
ICR	1.4689	Resolution (m)	0.6377912
RBS (dB/ns)	-82.821	Expected injection (dB)	20.428
Splice loss threshold (dB)	0.02	Minimum injection (dB)	16.428
Reflectance threshold (dB)	-72	Maximum injection (dB)	20.928
End-of-Fiber threshold (dB)	4	Learning cycle	1
Targeted learning count	30	Reference learning cycle	1
		Learning count	30
		Reference learning count	29

To export the characterization table:

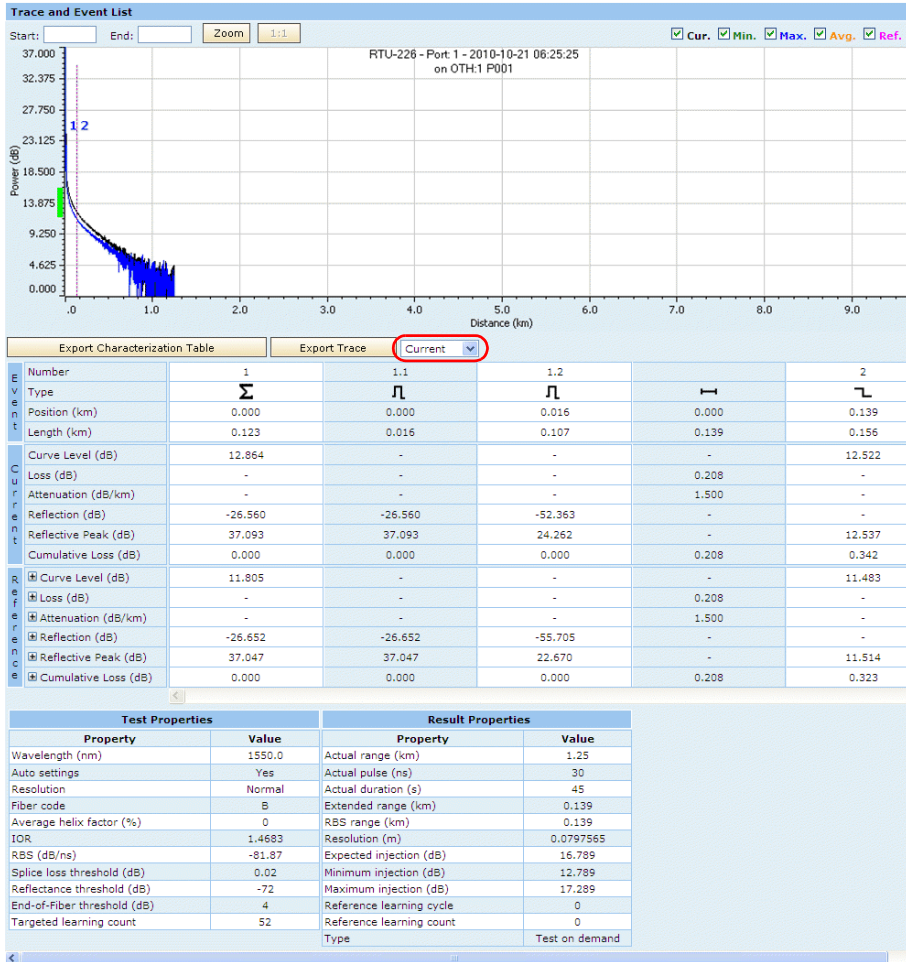
Click the **Export Characterization Table** button. When the application prompts you, you can either open the table directly in Microsoft Excel or save it.

Analyzing Results

Viewing the Current Fault List

To export the OTDR trace:

1. From the list of trace types, select the desired trace.



2. Click the **Export Trace** button.

The **File Download** dialog box is displayed.

3. Click **Find** to search for an appropriate program online to open the .trc file.

OR

Click **Open** to open the .trc file.

OR

Click **Save** to save the .trc file.

To zoom in on a specific area of the trace:

1. In the **Start** and **End** boxes, enter the desired values, in kilometers.
2. Click the **Zoom** button.

To revert to the complete graph view:

Click the **1:1** button.

Searching and Displaying OTDR Results

The result browser allows you to search the OTDR results, then view them directly or save them for future reference.

You can search among all the available results or narrow down your search to a specific test setup. You can also filter the results by type (ad hoc tests, references, etc.) and by date.

You can save (export) the OTDR trace in native .trc format. You will be able to open the trace with applications that support this format of file, such as EXFO's FastReporter.

You can also save both the results table and the data points of the OTDR trace (x and y coordinates) in a .csv format. This is useful if you prefer to work with raw data and build your own reports.

If you want, you can clear the results from the results window. This will not delete them from the database.

To search OTDR results:

1. From the main menu, select **Reporting > Result Browser**.

The screenshot shows the EXFO NQMSfiber - Result Browser interface. The left sidebar contains a tree view with the following items: **Optical Test Heads** (circled in red), Optical Test Head S/N: 402900, Optical Routes, and Test Setups (Monitoring at 1550.0 nm, Proactive maintenance). The main area is titled 'Search Options' and includes a 'Search by dates' section with start and end date/time pickers. Below this is a 'Search Results' table with columns: Date / Time, Optical Route / Test Setup, Type, Ports, Job Information, Learning, and Fault Status / Information. The table contains two rows of results, both for 'Reference' tests on 'OTAU: 2' ports, with a 'Succeeded' status. At the bottom, it indicates 'Items found: 2 Page: 1' and has navigation buttons for 'First Page', 'Previous', and 'Next'.

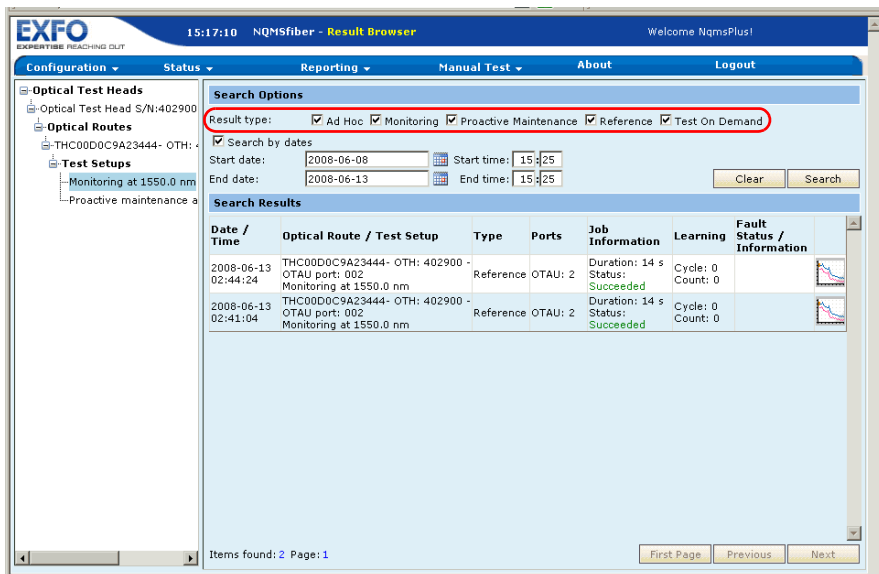
Date / Time	Optical Route / Test Setup	Type	Ports	Job Information	Learning	Fault Status / Information
2008-06-13 02:44:24	THC00D0C9A23444- OTH: 402900 - OTAU port: 002 Monitoring at 1550.0 nm	Reference	OTAU: 2	Duration: 14 s Status: Succeeded	Cycle: 0 Count: 0	
2008-06-13 02:41:04	THC00D0C9A23444- OTH: 402900 - OTAU port: 002 Monitoring at 1550.0 nm	Reference	OTAU: 2	Duration: 14 s Status: Succeeded	Cycle: 0 Count: 0	

2. If you want to narrow down your search to a specific test setup, from the tree view, select the desired test setup. If you do not select any, the search will be performed on all of them.

Analyzing Results

Searching and Displaying OTDR Results

3. Select which type of results you want to include in your search by selecting the corresponding options.





The screenshot shows the EXFO NQMSfiber - Result Browser interface. The top navigation bar includes Configuration, Status, Reporting, Manual Test, About, and Logout. The left sidebar shows a tree view with Optical Test Heads, Optical Routes, and Test Setups. The main area is divided into Search Options and Search Results.

Search Options:



- Result type: Ad Hoc Monitoring Proactive Maintenance Reference Test On Demand
- Search by dates
- Start date: 2008-06-08 Start time: 15:25
- End date: 2008-06-13 End time: 15:25
- Buttons: Clear, Search

Search Results:

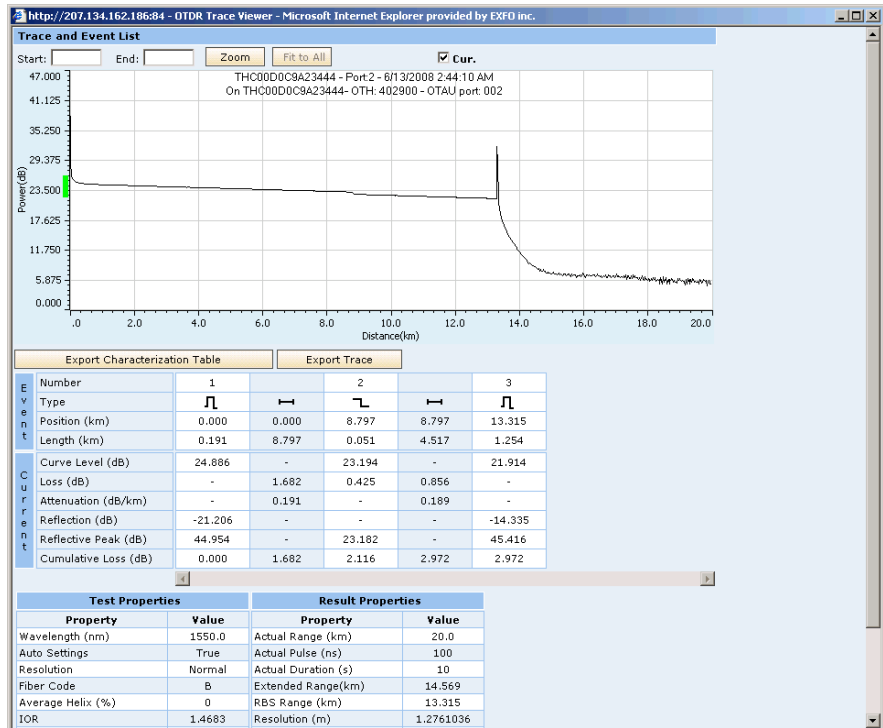
Date / Time	Optical Route / Test Setup	Type	Ports	Job Information	Learning	Fault Status / Information
2008-06-13 02:44:24	THC00D0C9A23444- OTH: 402900 - OTAU port: 002 Monitoring at 1550.0 nm	Reference	OTAU: 2	Duration: 14 s Status: Succeeded	Cycle: 0 Count: 0	
2008-06-13 02:41:04	THC00D0C9A23444- OTH: 402900 - OTAU port: 002 Monitoring at 1550.0 nm	Reference	OTAU: 2	Duration: 14 s Status: Succeeded	Cycle: 0 Count: 0	

Items found: 2 Page: 1

Buttons: First Page, Previous, Next

4. If you wish to limit the search to specific dates and time, use the **From** and **To** boxes. The date in the **From** and **To** boxes is in MM/DD/YYYY format (you can also select a date using the  button) and the time format is HH:MM in 24-hour format.
5. Click **Search**.
6. Once your search is completed, locate the result you wish to view and click .

- If you wish to export the trace or the characterization table at this point, click the corresponding button.



- Select whether you want to view directly the file, or save it. If you select the latter, indicate the location where you want to save the file.

To clear results from the results window:

From the **Result Browser** window, click the **Clear** button.

Analyzing Results

Search Results for Test On Demand

Search Results for Test On Demand

The search results for **Test on demand** are displayed:

- When you are using a physical RTU.
- When test type is selected as **Test on demand**.

Note: *For the search results of **Test on demand**, RTU may or may not be in sync with EMS.*

To view the search result:

- 1.** From the main menu, select **Reporting > Result Browser**.
- 2.** In the **Search Options** section, select the **Test on demand** check box.
OR
Select the **Search by dates** check box.
- 3.** If you select the **Search by dates** check box, enter the date and time range in the **Start date**, **Start time**, **End date**, and **End time** fields.

4. Click Search.

The screenshot shows the EXFO NQMSfiber Result Browser interface. The top navigation bar includes 'Configuration', 'Status', 'Reporting', 'Manual Test', 'About', and 'Logout'. The main content area is titled 'Search Options' and contains several checkboxes for search criteria: Reference, Ad hoc, Monitoring, Proactive maintenance, and Test on demand. Below these are fields for 'Search by dates', 'Start date', 'End date', 'Start time', and 'End time'. A 'Search' button is located at the bottom right of the search options section.

The 'Search Results' section displays a table with the following columns: Date / Time, Optical Route / Test Setup, Type, Ports, Test Information, Learning, and Fault Status. The table contains five rows of data, each representing a test result. Each row includes a small icon in the rightmost column, which is a line graph showing signal quality over time.

Date / Time	Optical Route / Test Setup	Type	Ports	Test Information	Learning	Fault Status
2011-02-21 11:29:11	OTH:1 P001 Monitoring at 1550.0 nm	Monitoring	OTAU: 1	Duration: 14 s Status: Succeeded		Cleared
2011-02-21 11:28:52	OTH:1 P001 Monitoring at 1550.0 nm	Monitoring	OTAU: 1	Duration: 15 s Status: Succeeded		Still there
2011-02-21 11:28:30	OTH:1 P001 Monitoring at 1550.0 nm	Monitoring	OTAU: 1	Duration: 14 s Status: Succeeded		New
2011-02-21 09:44:10	OTH:1 P001 Monitoring at 1550.0 nm	Monitoring	OTAU: 1	Duration: 14 s Status: Succeeded	Cycle: 1 Count: 30	
2011-02-21 09:43:52	OTH:1 P001 Monitoring at 1550.0 nm	Monitoring	OTAU: 1	Duration: 15 s Status: Succeeded	Cycle: 1 Count: 29	

5. The search results display the following details: **Date/Time, Optical Route/Test Setup, Type, Ports, Test Information, Learning, and Fault Status.**

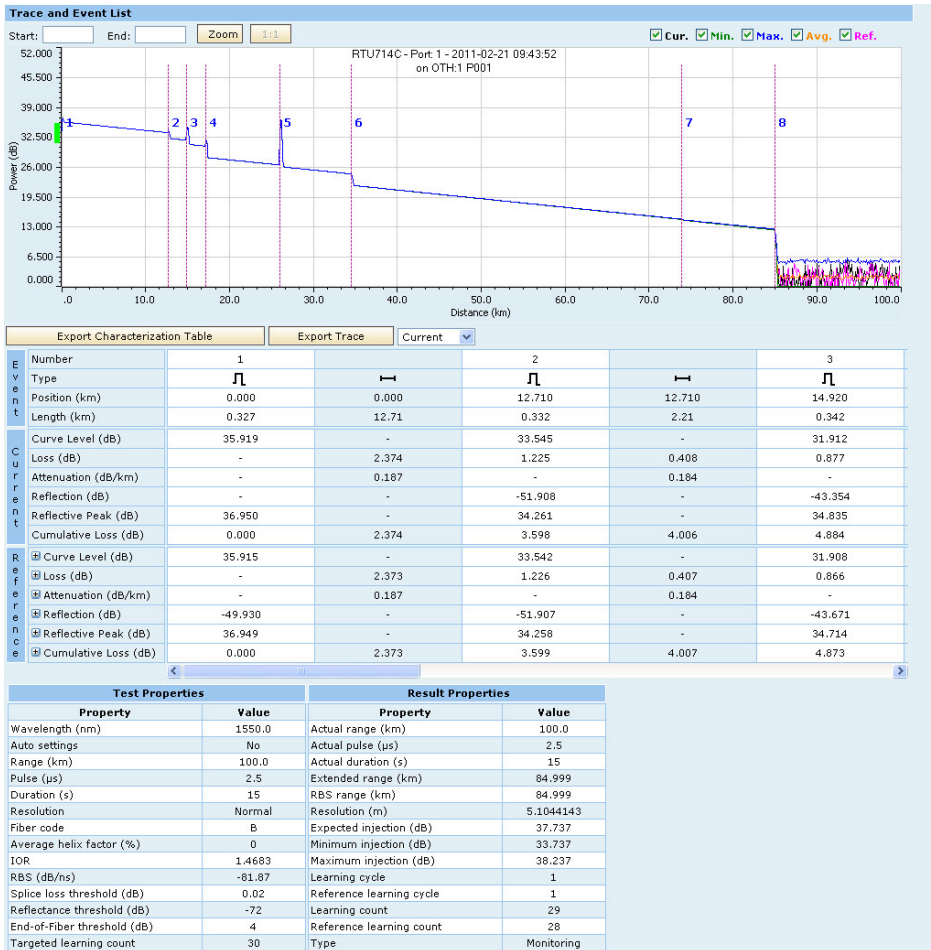
6. Click the **Details**  icon. The **Trace and Event** list screen displays the **Test Properties, Result Properties, and Fault Properties** sections.

Note: During search results, if any fault is detected, it is listed under **Fault Properties**. If no fault is detected, then the results are displayed under **Test Properties and Result Properties**.

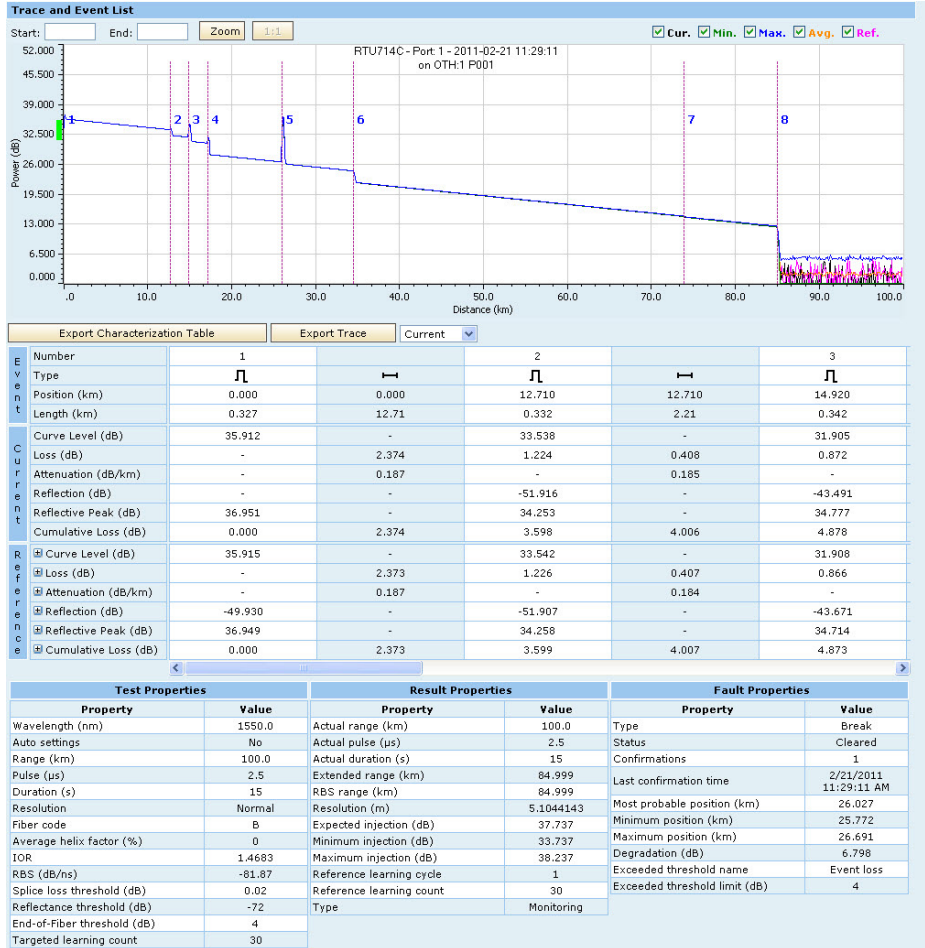
Analyzing Results

Search Results for Test On Demand

- Trace and Event list with **Test Properties** and **Result Properties** sections.



- Trace and Event list with **Test Properties**, **Result Properties**, and **Fault Properties** sections.



9 **Using the Line Configuration Web User Interface**

The Line Configuration Web UI is a tool used to create test lines (network logic with name or ID) corresponding to a test port number based on the unit optical switching configuration and number of ports available. It also allows continuity checks between the OTDR and switch ports, ensuring both communication and optical connections are present and working. The Web interface automatically detects if you have an OTDR, OTAUs, allows you to add remote OTAUs, and enables you to name the connections (lines) accordingly. The Line Configuration UI is available only in iOLM/Link-Aware™ mode.

The date and time in the header of the application are updated every minute. The format used is yyyy-MM-dd hh:mm (UTC +- hh:mm).

Accessing the Line Configuration Web UI

You can access the application directly from the **Actions > Applications** menu of the Host Web UI.

Note: *If you access the Line Configuration directly from the Host Web UI, you do not need to reenter your login credentials.*

You can also access the application directly from a Web browser and swap the enabled software with Host Web UI.

Using the Line Configuration Web User Interface

Accessing the Line Configuration Web UI

To connect directly using a Web Browser:

1. From your computer, open a Web browser.
2. In the address bar, type the appropriate information.
 - Computer connected directly to the unit (front port), type
`//169.254.10.10/LineConfiguration`
 - For LAN connection, type
`https://Rear_Port_IP_Address/LineConfiguration`
 - For WAN or Internet connection, type
`https://Unit_LogMeIn_Hamachi_Address/LineConfiguration`

Note: *If you do not know the IP address of the rear Ethernet port, see Retrieving the IP Address of the Rear Ethernet Port (Host and Companion) on page 55.*

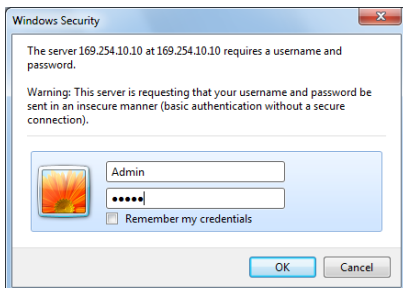
Note: *If you do not know the LogMeIn Hamachi address of your unit, see Preparing to Access Your Unit via a WAN or the Internet on page 69.*

For information about the supported browsers for your application, see *Supported Web Browsers* on page 12.

Using the Line Configuration Web User Interface

Accessing the Line Configuration Web UI

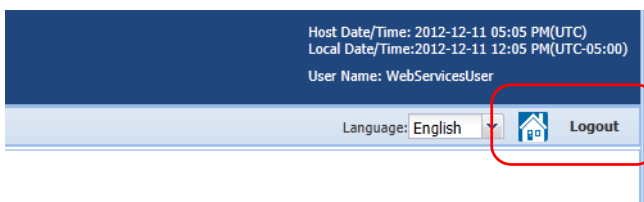
3. Once you have accessed the application, use your Host Web UI credentials to log in.



For more information about login credentials for your applications, see *Understanding the Applications, User Accounts and Passwords* on page 87.

To log out:

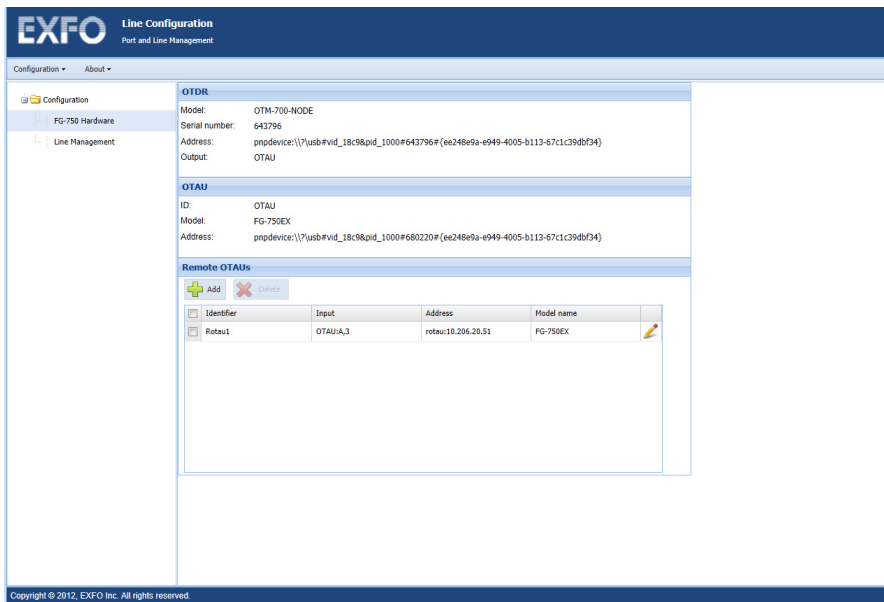
Click the **Logout** button on the top right corner of the window.



Using the Line Configuration Web User Interface

Accessing the Line Configuration Web UI

The main configuration window is where you can manage lines and hardware components for your system (OTDR, OTAU's and remote OTAU's). The application automatically detects if you have an OTDR and internal switches (OTAU), and retrieves the relevant information on-screen. Remote OTAU's are added and managed by the user, and the related settings are saved in the configuration file.



To access the main window:


Select the **Configuration** menu, then **Ports and Line Management**. In the tree view, you can see the items below:

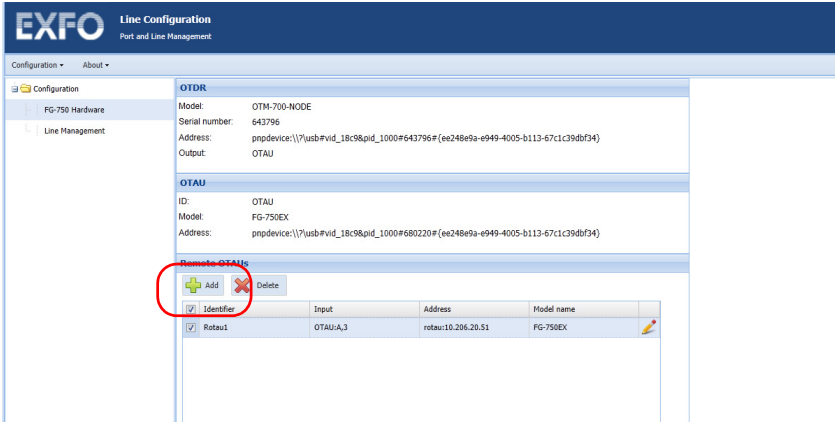
- **FG-750 Hardware** is used to manage OTAU's and Remote OTAU's.
- **Line Management** is to manage ports and lines. This is also where you can view the injection loss test results for your lines.

Managing Remote OTAU's

Remote OTAU's are external switches that you connect to your system to add ports.

To add a Remote OTAU:

1. From the **FG-750 Hardware** section, under **Remote OTAU's**, click  .



The screenshot displays the EXFO Line Configuration web interface. The main content area is titled "Remote OTAU's" and contains a table with columns for Identifier, Input, Address, and Model name. A red circle highlights the "Add" button (a green plus sign) located above the table. The table contains one entry: "Rotau1" with Input "OTAU-A_3", Address "rotau:10.206.20.51", and Model name "FG-756EX".

Identifier	Input	Address	Model name
<input checked="" type="checkbox"/>	OTAU-A_3	rotau:10.206.20.51	FG-756EX

Using the Line Configuration Web User Interface

Managing Remote OTAU's

2. Enter the information for your new Remote OTAU.

The screenshot shows a dialog box titled "Add Remote OTAU". It contains the following fields and values:

- OTAU ID: Rotau2
- IP address: 10.206.20.200
- Input signal comes from: Rotau1 (dropdown menu)
- Input port: A,1
- Specifications section (expanded):
 - Switch model: FG-750EX (dropdown menu)
 - Communication port: (empty)
 - Serial number: Unit Serial Number

At the bottom right of the dialog are two buttons: "Add" and "Cancel".

- The OTAU ID is limited to 30 characters and is case-sensitive.
- The **Add** button will become active when you have added a valid IP address. However, the reachability of the address is not tested until you run an injection loss test. See *Performing an Injection Loss Test* on page 244 for more information.

- The input signal selections include the available switches in the network.
- The input port is limited to 20 alphanumeric characters.

Note: *If the switch is an FG-750, the port name is usually the slot the switch module is in, and the port, separated by a comma. For example if your switch is in slot C, and you are using the second port, then the port name will be C,2. If the switch is an external model (576-port and 720-port Node OTAU's, identified as "Sumitomo"), then the port will be only the corresponding number.*


- Two switch models are supported: FG-750EX and Node OTAU (Sumitomo).
- The communication port is a numeric value ranging from 1 to 65535.

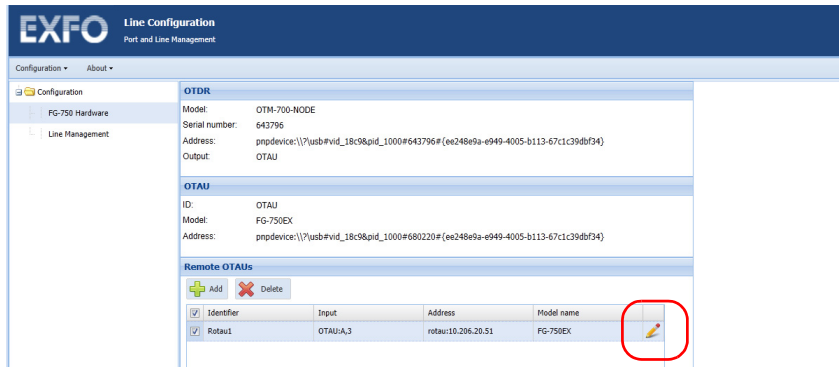
3. Click **Add** to add the Remote OTAU.

Using the Line Configuration Web User Interface

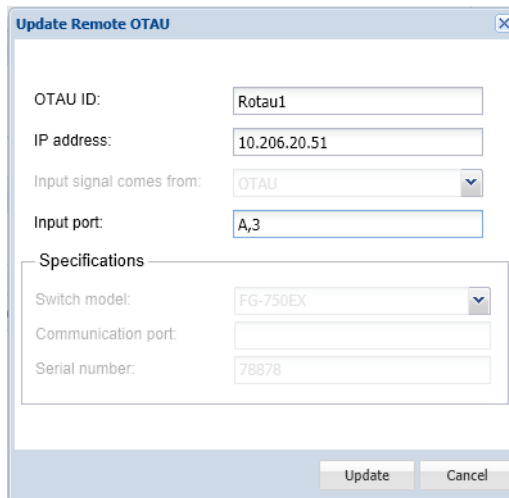
Managing Remote OTAU's

To edit an existing Remote OTAU entry:

1. From the **FG-750 Hardware** section, click the  button next to the Remote OTAU that you want to modify.



2. Change the information as needed. Only the OTAU ID, IP address and Communication port information can be changed at this point.



3. Click **Update** once your changes are complete.

To delete a Remote OTAU from the list:

1. From the **FG-750 Hardware** section, select the Remote OTAU or OTAU(s) that you want to delete.




IMPORTANT

Deleting the selected remote OTAU(s) will also delete all associated lines and cascaded remote OTAU(s).

The screenshot shows the EXFO Line Configuration web interface. The main content area is divided into three sections: OTDR, OTAU, and Remote OTAUs. The OTDR section displays details for a device with Model: OTM-700-NODE, Serial number: 643796, and Address: pnpdevice:\\?usb#vid_18c9&pid_1000#643796#(ee248e9a-4949-4005-b113-67c1c39df94). The OTAU section displays details for a device with ID: OTAU, Model: FG-750EX, and Address: pnpdevice:\\?usb#vid_18c9&pid_1000#680220#(ee248e9a-4949-4005-b113-67c1c39df94). The Remote OTAUs section contains a table with columns for Identifier, Input, Address, and Model name. The table has two rows: one for 'Rotau' with Input 'OTAU-A_3' and Address 'rotau:10.206.20.51'. A red circle highlights the 'Delete' button in the Remote OTAUs section.

Identifier	Input	Address	Model name
<input checked="" type="checkbox"/>	OTAU-A_3	rotau:10.206.20.51	FG-750EX

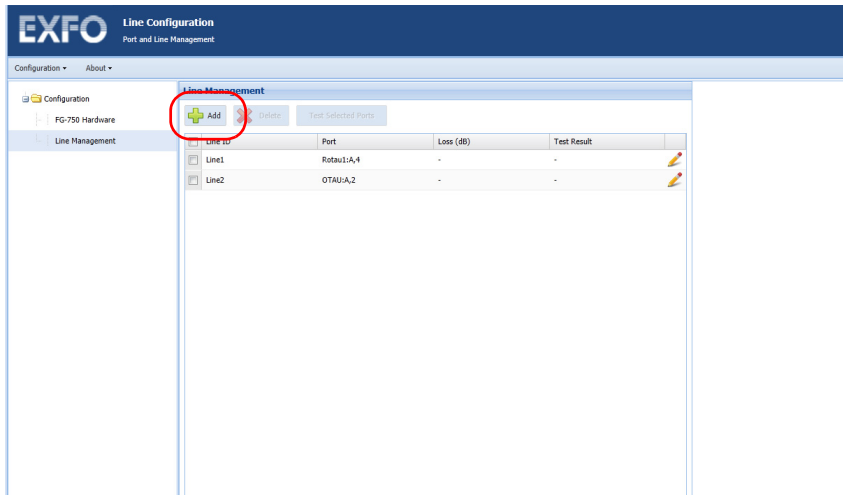
2. Click the  **Delete** button.
3. Confirm your choice.

Managing Ports and Lines

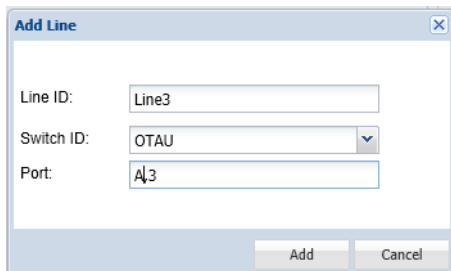
You can simply add, edit or delete lines from the **Line Management** window. By default, the list is empty (no line “pre-configured”).

To add a line:

1. From the tree view, select **Line Management**, then click  .



2. Enter the identification information for the new line, and associated port.



The screenshot shows a dialog box titled "Add Line" with a close button (X) in the top right corner. It contains three input fields: "Line ID" with the text "Line3", "Switch ID" with a dropdown menu showing "OTAU", and "Port" with the text "A3". At the bottom right of the dialog are two buttons: "Add" and "Cancel".

- The Line ID will be checked for uniqueness and is case sensitive. The maximum length is 50 characters. An automatically generated name is proposed, with an incrementation to avoid overwrites.
- If the line is to be matched to a switch port, select the switch in the list of available choices. If no switches are available, you can only select the OTDR. In the case of cascading switches, select the last switch in the link to match the line and port.
- Once the switch is selected, you can select the port you want to associate to the line. The maximum length is 50 characters, and the name is case sensitive. If you only have an OTDR in your system, this field is disabled.

Note: *If the switch is an FG-750, the port name is usually the slot the switch module is in, and the port, separated by a comma. For example if your switch is in slot C, and you are using the second port, then the port name will be C,2. If the switch is an external model (Node OTAU, identified as “Sumitomo”), then the port will be only the corresponding number.*

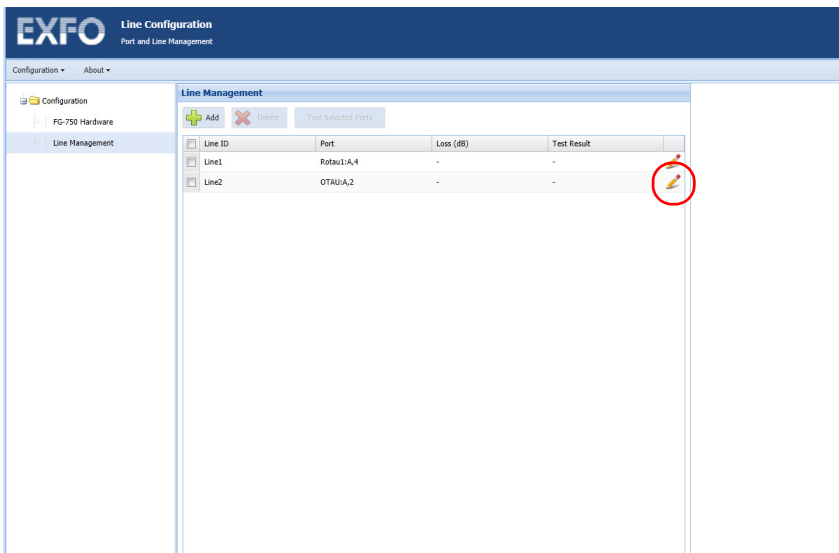
3. Click **Add** to add the line.

Using the Line Configuration Web User Interface

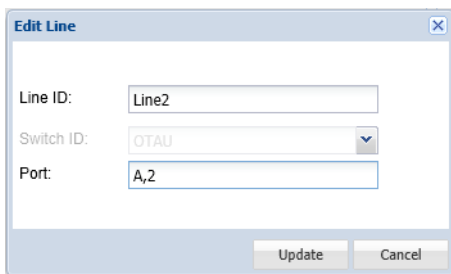
Managing Ports and Lines

To edit a line:

1. From the tree view, select **Line Management**, then click the  button next to the line that you want to modify.



2. Change the information as needed.

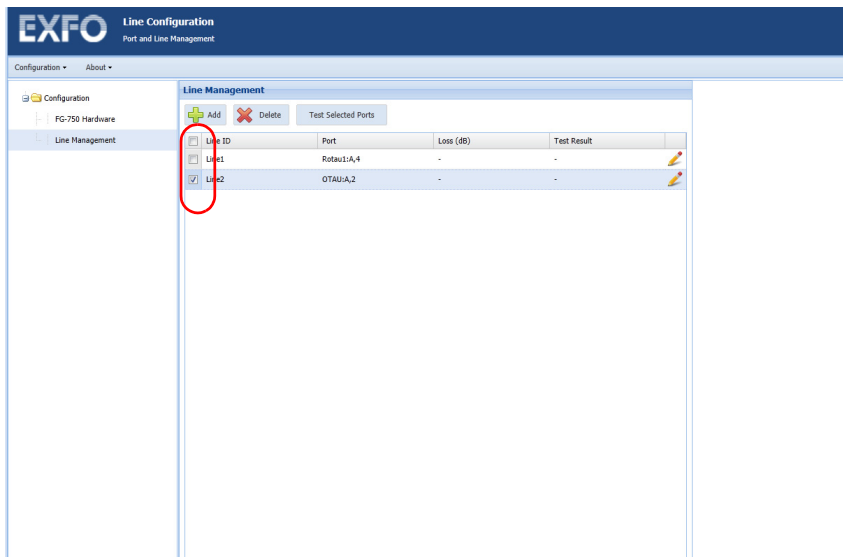



Note: The switch ID item is not available in edit mode.

3. Click **Update** to confirm your changes.

To delete a line:

1. From the tree view, select **Line Management**, then select the line or lines that you want to delete.



2. Click the  **Delete** button.
3. Confirm your choice.

Performing an Injection Loss Test

The injection loss test is used to confirm that your switches are properly connected. The test can be performed on one or several ports at a same time.

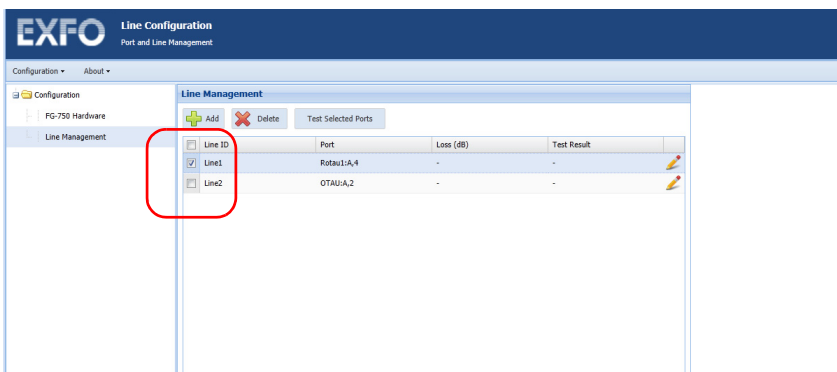


IMPORTANT

The injection lost test results are not persistent. They will be erased if you exit the application, or refresh your window.

To perform an injection loss test:

1. From the **Line Management** section, select which lines you want to test. To quickly select or deselect all entries, use the check box in the list header.



2. Click **Test Selected Ports**.

Using the Line Configuration Web User Interface

Performing an Injection Loss Test

3. Once the test is complete, you can view individual, detailed results by clicking **Show Result** in the line that you want to view. If there was a problem with the line, the **Diagnostic** section provides details to help with the troubleshooting.



4. Once you are done viewing the details, click **Close Window**.

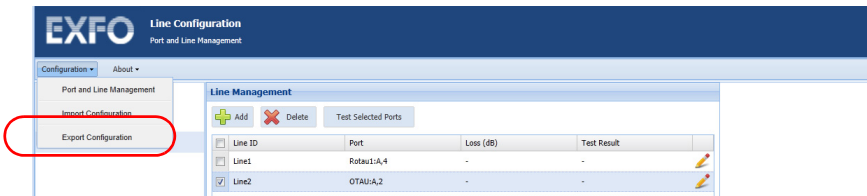
Managing Configurations

Configuration files can be particularly useful when you want to reuse information and have uniform testing over your units. The file is in XML format and can be modified or updated even if you are not directly on the unit.

Manually saving your configuration files is strongly recommended to ensure the safekeeping of your setups in case of problems.

To export, or save, a configuration:

1. From the main window, select the **Configuration** menu, then **Export Configuration**.



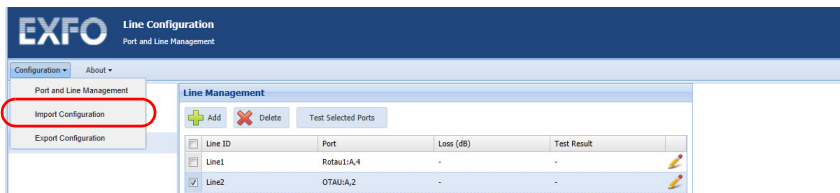
2. Select **Save**, then select the location for the file.
3. The default name for the file is Line_Configuration_ddMMMyy.xml. Change the name if required.

Note: In the file name, dd stands for day, MMM for month, and yy for year. For example, a file name could be Line_Configuration_10Dec12.xml.

4. Click **Save** to complete the export.

To import, or load, a configuration file:

1. From the main window, select the **Configuration** menu, then **Import Configuration**.



2. Locate the XML file that you want to use as the configuration.
3. Click **Open**.

The page is refreshed automatically to reflect this new configuration file. If the XML provided by the configuration file is not compliant with a supported configuration format, you will be notified.

10 Working With the Event Log

From the Host Web UI, you can:

- View a log of all the events that occur on the host or companion, including measurement entries.
- Customize your view of the logs.
- Apply filters to refine the log view.
- Export logs to an XML file.

Viewing the Event Log

You can view a log of the events that occur on the host or companion, such as the OTDR measurements, software updates, problems, etc.

To view the event log:

1. Connect to the Host Web UI. For more information, see *Accessing and Exiting the Host Web UI* on page 109.
2. From the **Reports** menu, click **Event Log**.
3. Click the calendar icons and the time drop-down menus in the **From** and **To** boxes to select the time period for which you want to view the log of events.
4. Click **Refresh**.

The application displays a list of all the events from the selected time period. The **Total Logs** value indicates the number of entries found to a maximum of 2000 at a time.

Configuration ▾ Actions ▾ Status ▾ Reports ▾ About ▾ Language: English ▾ Logout

Event Logs

From: 2014-10-27 12:04 To: 2014-10-28 12:05 Refresh Clear Filters Export XML Delete All Logs Total Logs: 2

Information Warnings Errors Communication errors with the server

Event Source	Description	EventType	Date and Time
Fiber Guardian Host Service	Cmd failed on: Return code : 255, NetFun : Exfo, Command : 96, prop.RequestData 02-01-FF-FF We will retry in 3 sec... (2)	Information	Host: 2014-10-27 22:19:51(UTC) Local: 2014-10-27 18:19:51(UTC-04:00)
Fiber Guardian Host Service	Cmd failed on: Return code : 255, NetFun : Exfo, Command : 96, prop.RequestData 02-01-FF-FF We will retry in 3 sec... (1)	Information	Host: 2014-10-27 22:19:43(UTC) Local: 2014-10-27 18:19:43(UTC-04:00)

Customizing the Log View

The **Event Log** page also displays the following columns:

- **Event Source** is the Fibre Guardian Host/App.
- **Description** displays detailed information about the event.
- **Event Type** can be log entries displaying information, warnings, or errors.
- **Date and Time** allows you to select a time period for the event logs.

You can customize the Host Web UI to display or hide these columns.

To customize the log view:

- 1.** Connect to the Host Web UI. For more information, see *Accessing and Exiting the Host Web UI* on page 109.
- 2.** From the **Reports** menu, click **Event Log**.
- 3.** Click any of the column names to display a drop-down menu.
- 4.** From the drop-down menu, go to **Columns**.
- 5.** From the **Columns** menu, clear the check boxes corresponding to the columns that you want to hide.

Select the check boxes of the columns that you want to display.

Applying and Clearing Filters

You can further customize the log view by applying the filters on the **Event Log** page. Selecting the corresponding check box enables a filter and clearing the check box disables that particular filter. Multiple filters can be enabled at the same time. Filter data is displayed in the **Description** and **Event Type** columns. Available filters are as follow:

- **Information** displays a list of all the information log entries for the selected time period.
- **Warnings** display a list of all the warning log entries for the selected time period.
- **Errors** display a list of all the error log entries for the selected time period.
- **Communication errors with the server** display log entries only for the OTDR measurements.

In addition to choosing which columns to display, the following 2 columns also display the following filters:

Column Name	Available Filter	Description
Event Source	Fiber Guardian App	Displays log entries only from the companion.
	Fiber Guardian Host	Displays log entries only from the host.
Date and Time	Before	Displays a list log entries (if any) for a time period before the selected date.
	After	Displays a list log entries (if any) for a time period after the selected date.
	On	Displays a list log entries (if any) for the time period selected.

Working With the Event Log

Applying and Clearing Filters

To apply filters to the Event Source or Date and Time columns:

- 1.** Connect to the Host Web UI. For more information, see *Accessing and Exiting the Host Web UI* on page 109.
- 2.** From the **Reports** menu, click **Event Log**.
- 3.** If you want to apply filters on the type of source:
 - 3a.** Click the **Event Source** column.
 - 3b.** From the **Event Source** drop-down menu, click **Filters**.
 - 3c.** From the **Filters** menu, select the desired criteria.
- 4.** If you want to apply filters on the time period of the event:
 - 4a.** Click the **Date and Time** column.
 - 4b.** From the **Date and Time** drop-down menu, click **Filters**.
 - 4c.** From the **Filters** menu, select the desired criteria.
- 5.** Click **Refresh**.

To clear all the currently applied filters:

- 1.** Go to **Reports > Event Log**.
- 2.** Click **Clear Filters**.

Exporting Log Reports

If you wish, you can export a log report to an XML file.

To export a log report:

- 1.** Connect to the Host Web UI. For more information, see *Accessing and Exiting the Host Web UI* on page 109.
- 2.** From the **Reports** menu, click **Event Log**.
- 3.** Select the time period and the appropriate filter to view the log that you want to export.
- 4.** Click **Export XML** to export the displayed log to an XML file.

11 Maintenance

To help ensure long, trouble-free operation:

- Always inspect fiber-optic connectors before using them and clean them if necessary.
- Keep the unit free of dust.
- Clean the unit casing and front panel with a cloth slightly dampened with water.
- Store unit at room temperature in a clean and dry area. Keep the unit out of direct sunlight.
- Avoid high humidity or significant temperature fluctuations.
- Avoid unnecessary shocks and vibrations.
- If any liquids are spilled on or into the unit, turn off the power immediately, disconnect from any external power source, remove the batteries and let the unit dry completely.



WARNING

The use of controls, adjustments and procedures, namely for operation and maintenance, other than those specified herein may result in hazardous radiation exposure or impair the protection provided by this unit.

Cleaning Switchable Connectors

Regular cleaning of switchable connectors will help maintain optimum performance. There is no need to disassemble the unit.



IMPORTANT

If any damage occurs to internal connectors, the module casing will have to be opened and a new calibration will be required.



WARNING

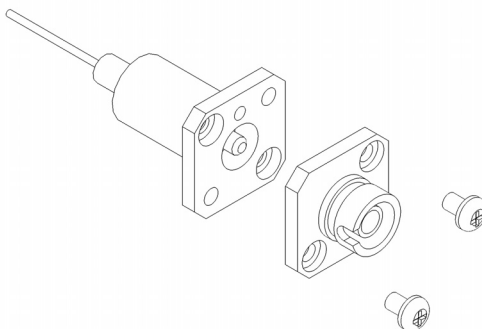
Before cleaning the connectors, you should suspend the tests on all optical routes to avoid hazardous radiation exposure. Refer to the procedure below for instructions.

To suspend the tests on all optical routes:

1. Log in on the RTU application if you have not already done so.
2. From the main menu, select **Configuration > Optical Routes**.
3. Click **Suspend All**. The route status will change to *Skipped*.

To clean switchable connectors:

- 1.** Use a small Phillips screwdriver to remove the two screws on the connector and expose the connector baseplate and ferrule.

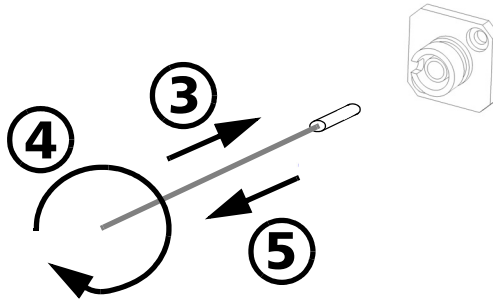


- 2.** Moisten a 2.5 mm cleaning tip with *one drop* of optical-grade liquid cleaner.

Maintenance

Cleaning Switchable Connectors

3. Slowly insert the cleaning tip into the adapter until it comes out on the other side (a slow clockwise rotating movement may help).



4. Gently turn the cleaning tip one full turn, then continue to turn as you withdraw it.
5. Repeat steps 3 to 4 with a dry cleaning tip.

Note: Make sure you do not touch the soft end of the cleaning tip.

6. Clean the ferrule in the connector port as follows:
 - 6a. Deposit *one drop* of optical-grade liquid cleaner on a lint-free wiping cloth.



IMPORTANT

Avoid contact between the tip of the bottle and the wiping cloth, and dry the surface quickly.

- 6b. Gently wipe the connector and ferrule.

- 6c.** With a dry lint-free wiping cloth, gently wipe the same surfaces to ensure that the connector and ferrule are perfectly dry.
- 6d.** Verify connector surface with a fiber inspection probe (for example, EXFO's FIP).



WARNING

Verifying the surface of the connector WHILE THE UNIT IS ACTIVE WILL result in permanent eye damage.

- 7.** Fix the connector back onto the connector baseplate with the two screws.
- 8.** Throw out cleaning tips and wiping cloths after one use.

Cleaning EUI Connectors

Regular cleaning of connectors will help maintain optimum performance. There is no need to disassemble the unit.



IMPORTANT

If any damage occurs to internal connectors, the module casing will have to be opened and a new calibration will be required.

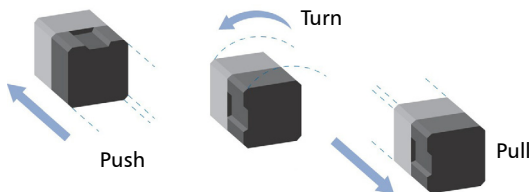


WARNING

Looking into the optical connector while the light source is active **WILL** result in permanent eye damage. EXFO strongly recommends to **TURN OFF** the unit before proceeding with the cleaning procedure.

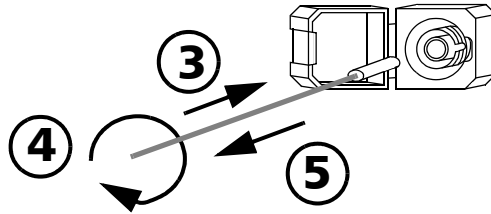
To clean EUI connectors:

1. Remove the EUI from the instrument to expose the connector baseplate and ferrule.



2. Moisten a 2.5 mm cleaning tip with *one drop* of optical-grade liquid cleaner.

3. Slowly insert the cleaning tip into the EUI adapter until it comes out on the other side (a slow clockwise rotating movement may help).



4. Gently turn the cleaning tip one full turn, then continue to turn as you withdraw it.
5. Repeat steps 3 to 4 with a dry cleaning tip.

Note: *Make sure you don't touch the soft end of the cleaning tip.*

6. Clean the ferrule in the connector port as follows:
 - 6a. Deposit *one drop* of optical-grade liquid cleaner on a lint-free wiping cloth.



IMPORTANT

Avoid contact between the tip of the bottle and the wiping cloth, and dry the surface quickly.

- 6b. Gently wipe the connector and ferrule.
- 6c. With a dry lint-free wiping cloth, gently wipe the same surfaces to ensure that the connector and ferrule are perfectly dry.
- 6d. Verify connector surface with a fiber inspection probe (for example, EXFO's FIP).
7. Put the EUI back onto the instrument (push and turn clockwise).
8. Throw out cleaning tips and wiping cloths after one use.

Maintenance

Cleaning Other Types of Connectors

Cleaning Other Types of Connectors

Connectors that do not fall under the EUI or switchable connector categories can be cleaned using a mechanical cleaner. Depending on the type of connector, you will use a different cleaner.



Single-fiber mechanical cleaner (FC, SC, LC)

Multifiber mechanical cleaner (MTP/MTO)



WARNING

Verifying the surface of the connector with a fiber-optic microscope **WHILE THE UNIT IS ACTIVE WILL result in permanent eye damage.**

To clean a connector using a mechanical cleaner:

1. Insert the mechanical into the optical adapter, and push the outer shell into the cleaner.

Note: *The cleaner makes a clicking sound that indicates that the cleaning is done.*

2. Verify connector surface with a portable fiber-optic microscope (for example, EXFO's FOMS) or fiber inspection probe (for example, EXFO's FIP).

When you have finished cleaning the connectors and have reconnected the optical fibers, you can resume all optical route testing.

Replacing the Air Filter

There is one 62 x 62 mm filter located at the front of the unit. This type of filter cannot be cleaned. You must replace it with a new one, typically every 90 days (or after about 2000 hours) of operation. This interval may vary, depending on the environment into which the unit is operated. Dirty air filters can cause the unit's internal temperature to rise.



WARNING

To avoid serious injuries as well as irreparable damage to your unit, always remove both power cords before opening or servicing the unit.



CAUTION

To avoid damaging your unit or its components, you should wear an antistatic band during this maintenance operation. For more information, see *Preventing Electrostatic Discharge Damage* on page 25.



CAUTION

Use only air filters designed for your unit and approved by EXFO. You can purchase new filters from EXFO.



IMPORTANT

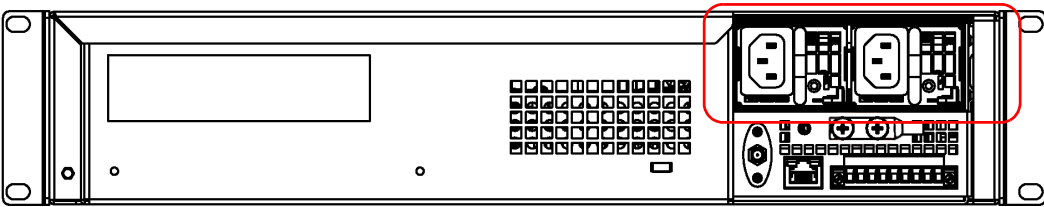
Replacing the air filter at the recommended intervals may prolong the life of the fan.

Maintenance

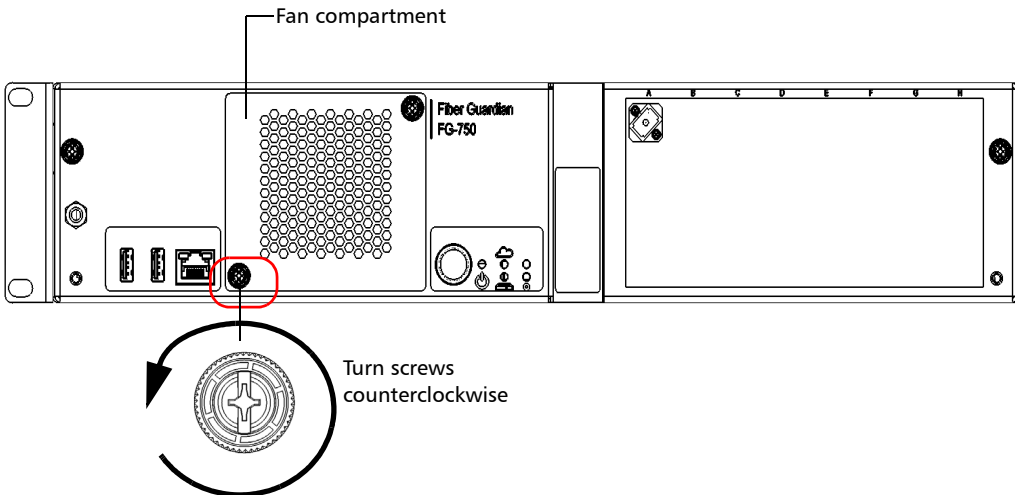
Replacing the Air Filter

To replace the air filter:

1. If you are using a fiber management tray, fold down the protective window. For more information, see *Working with the Fiber (Patchcord) Management Tray* on page 37.
2. Turn off the unit and disconnect it completely from the power sources.



3. Put on an antistatic strap and connect it to the connector provided for that purpose on the front panel of the unit.
4. Turn the fan compartment screws counterclockwise until the compartment is loose. Since the screws are captive screws, you cannot remove them completely.

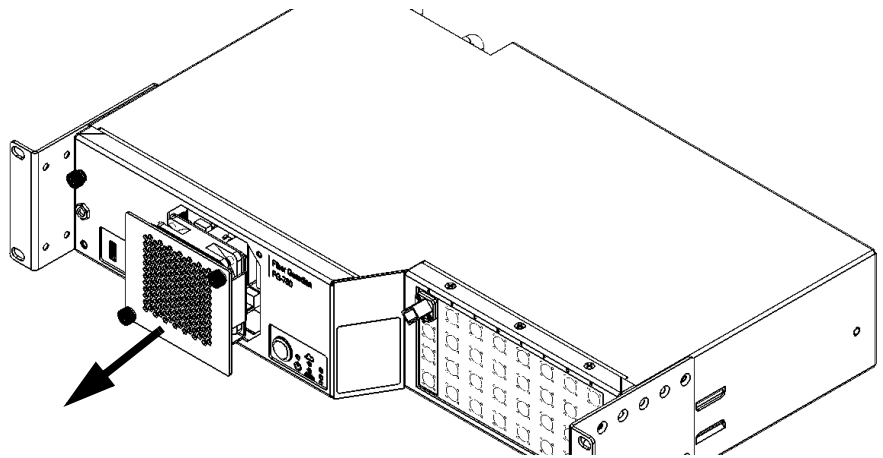




CAUTION

To avoid dropping the fan compartment and damaging the unit, the fan, or the fan cord, hold the fan compartment firmly. Do not allow the fan compartment to hang over the edge of a rack or a table.

5. Using the screws as handles, gently pull away the fan compartment.



6. Position the fan compartment vertically so that you see the top of the filter.
7. Lift the filter with two fingers to remove it.
8. Slide a new filter back into place.

Maintenance

Replacing the Air Filter

- 9.** Put the fan compartment back in its bay (it should be flush with the unit's front panel).
- 10.** Turn the fan compartment screws clockwise until the compartment is secured into place.
- 11.** Remove your antistatic strap.
- 12.** Reconnect the unit to its power sources (turn on both disconnected devices) and turn on your unit.
- 13.** If you are using a fiber management tray, put the protective window back into place. For more information, see *Working with the Fiber (Patchcord) Management Tray* on page 37.

Replacing the Fan

Your unit is equipped with one fan located at the front of the unit's casing. If you ever need to replace the fan, you must purchase a new one from EXFO.



WARNING

To avoid serious injuries as well as irreparable damage to your unit, always remove both power cords before opening or servicing the unit.



CAUTION

To avoid damaging your unit or its components, you should wear an antistatic band during this maintenance operation. For more information, see *Preventing Electrostatic Discharge Damage* on page 25.



CAUTION

Use only fans designed for your unit and approved by EXFO.



IMPORTANT

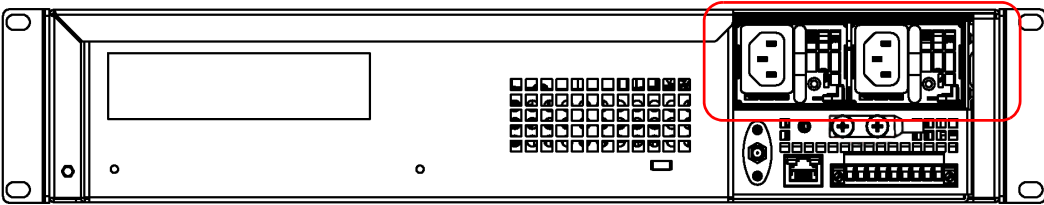
Replacing the air filter at the recommended intervals may prolong the life of the fan.

Maintenance

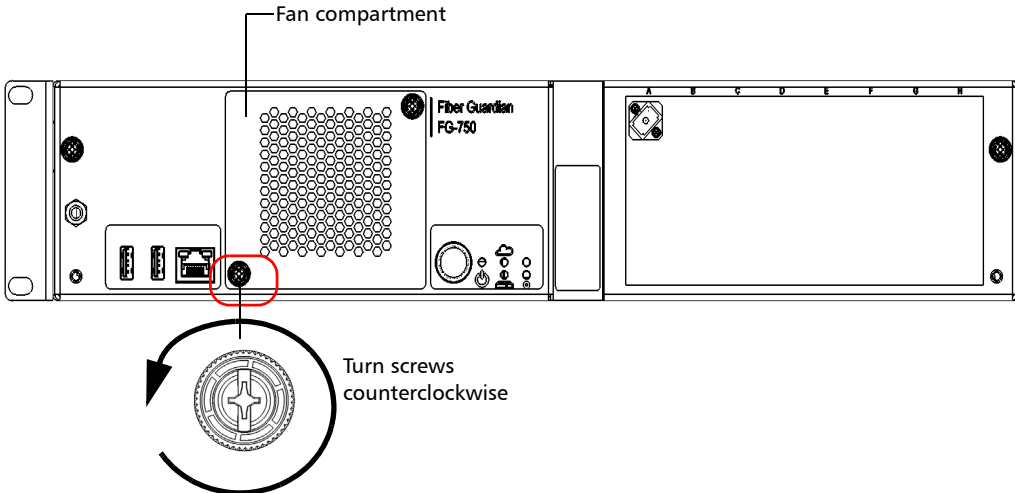
Replacing the Fan

To replace the fan:

1. If you are using a fiber management tray, fold down the protective window. For more information, see *Working with the Fiber (Patchcord) Management Tray* on page 37.
2. Turn off the unit and disconnect it completely from the power sources.



3. Put on an antistatic strap and connect it to the connector provided for that purpose on the front panel of the unit.
4. Turn the fan compartment screws counterclockwise until the compartment is loose. Since the screws are captive screws, you cannot remove them completely.

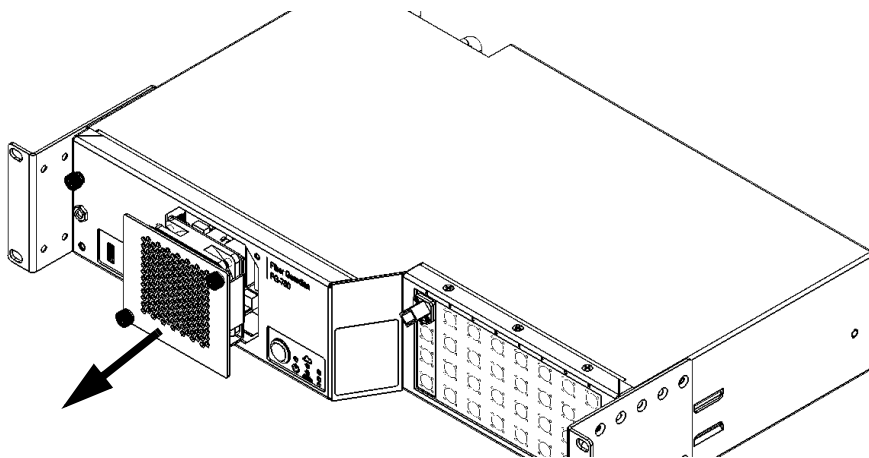




CAUTION

To avoid dropping the fan compartment and damaging the unit, the fan, or the fan cord, hold the fan compartment firmly. Do not allow the fan compartment to hang over the edge of a rack or a table.

5. Using the screws as handles, gently pull away the fan compartment.



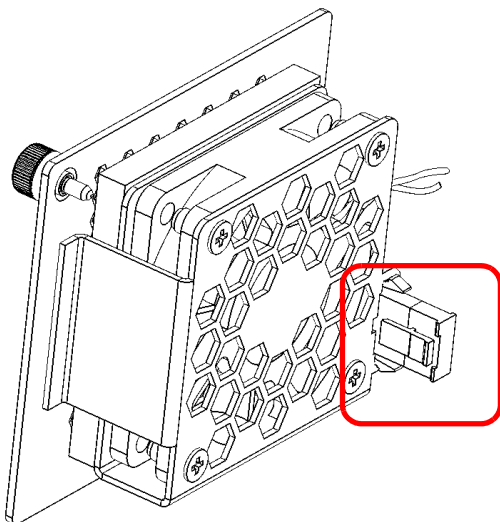
CAUTION

Do not disconnect the cord linking the fan to the motherboard when you want to disconnect the power from the fan. Disconnect the fan using the connector located on the fan compartment instead.

Maintenance

Replacing the Fan

6. Position the fan block so that you see its connector.

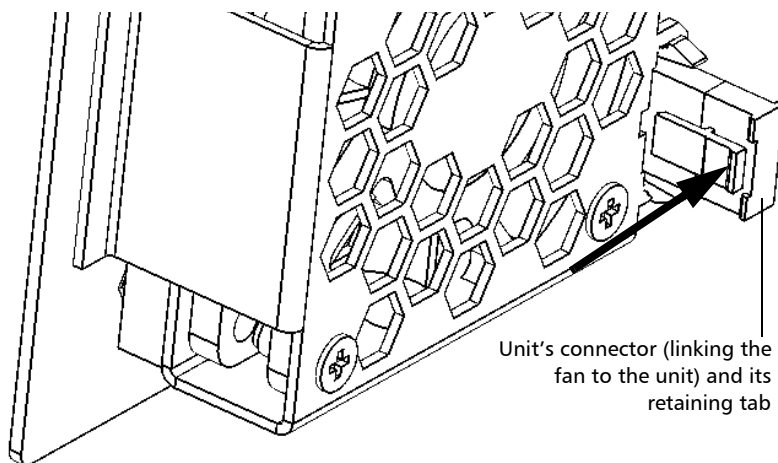




CAUTION

To avoid damaging the connector linking the fan to the unit, never pull on the unit's connector without pushing the retaining tab first.

7. Disconnect the power to the fan as follows:
 - 7a. Push the retaining tab against the connector linking the fan to the unit and hold it firmly.

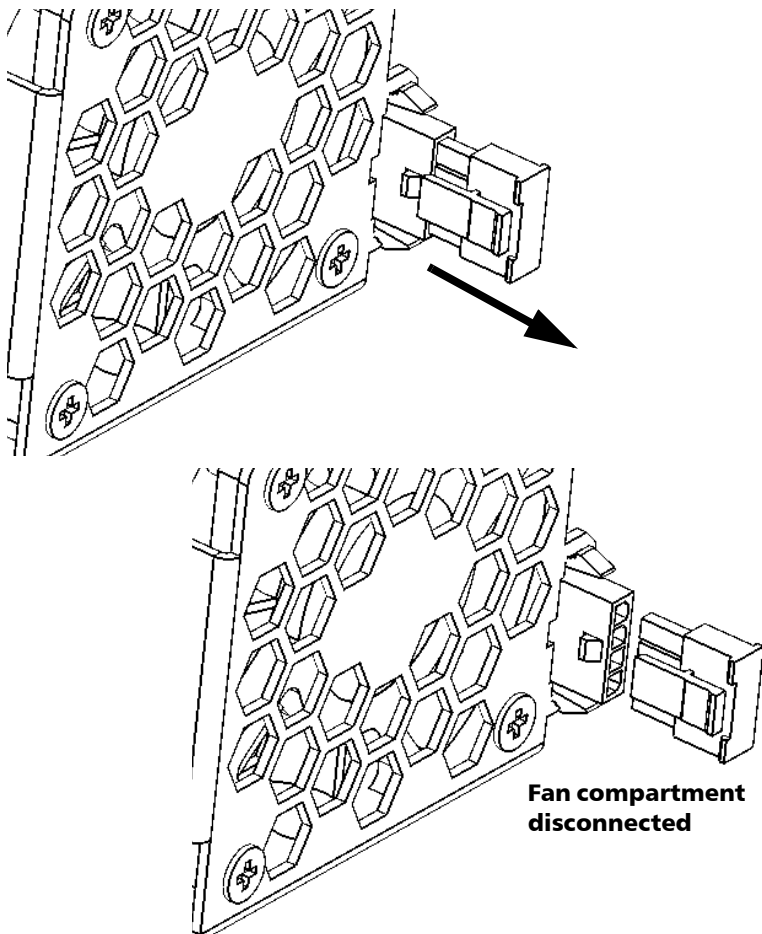


Unit's connector (linking the fan to the unit) and its retaining tab

Maintenance

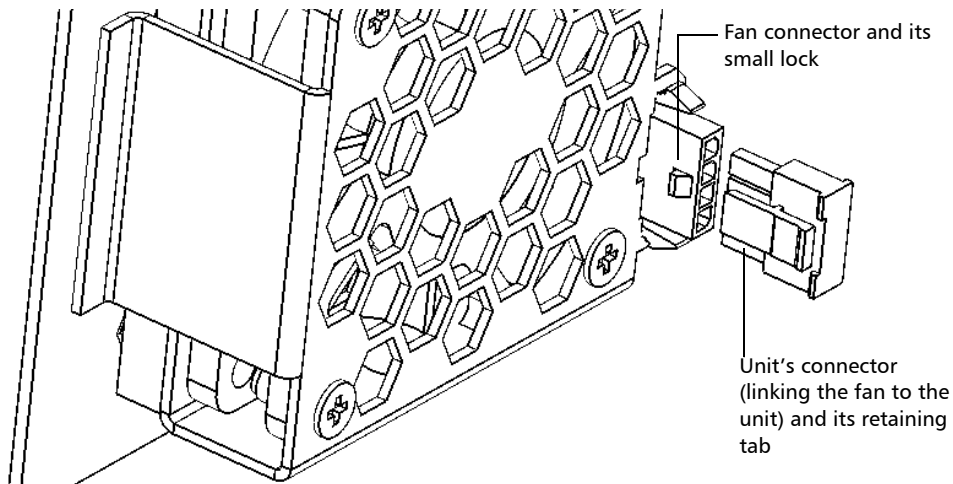
Replacing the Fan

- 7b.** Pull the connector away to remove the old fan completely.



- 8.** Position the new fan block so that you see its connector.

- 9.** Connect the power to the fan as follows:
- 9a.** Ensure that the fan connector and the connector linking the fan to the unit are well aligned. The retaining tab on the unit's connector should be on the same side as the small lock on the fan connector.



- 9b.** Connect the unit's connector to the fan.

Note: *You may find useful to hold the bottom of the fan connector while you push in the unit's connector.*

Maintenance

Replacing the Fan

- 10.** Put the fan compartment back in its bay (it should be flush with the unit's front panel).
- 11.** Turn the fan compartment screws clockwise until the compartment is secured into place.
- 12.** Remove your antistatic strap.
- 13.** Reconnect the unit to its power sources (turn on both disconnected devices) and turn on your unit.

Note: *If you are using a fiber management tray, put the protective window back into place. For more information, see Working with the Fiber (Patchcord) Management Tray on page 37.*

Replacing the Power Supply Modules

Your unit is powered by two replaceable power supply modules (either AC or DC). Your unit needs only one power supply module to work, but it can house two of them. The second power supply provides redundancy.

The power supply modules are hot-swappable, which means that you do not have to turn off your system to replace one of them. There is no need to disassemble the unit to replace such a power supply.

Ensure that you replace the defective power supply with a new one of the same type (AC or DC).

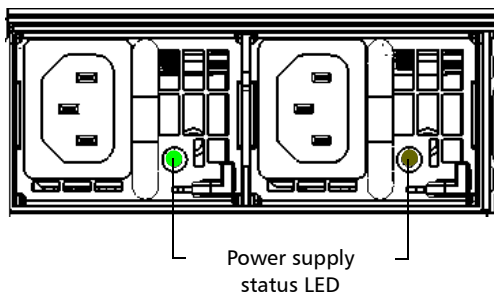


WARNING

To avoid serious injuries, ALWAYS TURN OFF THE DISCONNECT DEVICE THAT IS CONNECTED TO THE DEFECTIVE POWER SUPPLY before replacing the power supply.

To replace an AC power supply:

1. Position the unit so that its back panel is facing you.
2. Locate the defective power supply (its LED will be off).

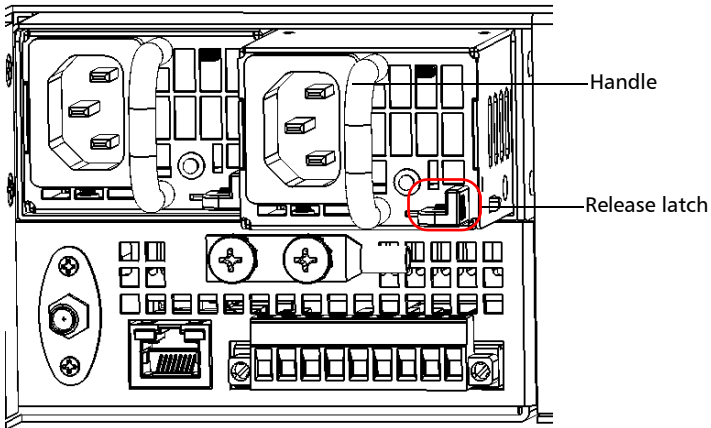


3. Disconnect the power cord from the defective power supply.

Maintenance

Replacing the Power Supply Modules

4. While pushing the release latch of the defective power supply to the left, gently pull the module toward you with the handle.



Note: As soon as the module can slide freely in its bay, there is no need to keep holding the release latch.

5. Pull the power supply module completely out of its bay.



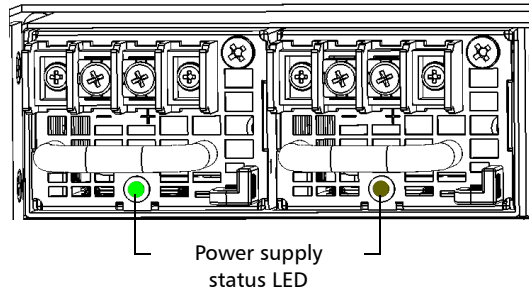
CAUTION

To avoid damaging the new power supply module, do not touch the gold connector located at the back and be careful not to hit it either.

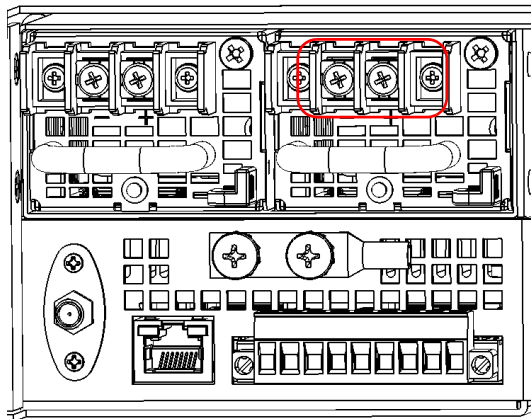
6. Position the new power supply so that its release latch is at the right of the handle.
7. Slide the new power supply into the empty bay until it stops (the module will not be flush with the edge of the bay).
8. While pushing the release latch to the left, gently push the module in its bay until it clicks into place.
9. Connect the power cord to the new power supply.

To replace a DC power supply:

1. Position the unit so that its back panel is facing you.
2. Locate the defective power supply (its LED will be off).



3. Turn off the disconnect device that is connected to the defective power supply.
4. Loosen the screws from the power terminals to disconnect the power leads from the defective power supply module.

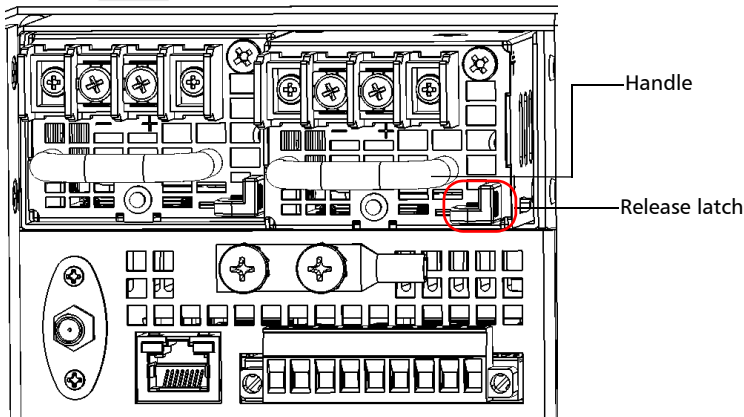


5. Unplug the earth strap wires from the defective power supply module.

Maintenance

Replacing the Power Supply Modules

6. While pushing the release latch of the defective power supply to the left, gently pull the module toward you with the handle.



Note: As soon as the module can slide freely in its bay, there is no need to keep holding the release latch.

7. Pull the power supply module completely out of its bay.



CAUTION

To avoid damaging the new power supply module, do not touch the gold connector located at the back and be careful not to hit it.

8. Connect the earth strap wires to the new power supply if you do not have spare earth strap wires with new power supply.
9. Position the new power supply so that its release latch is at the right of the handle.
10. Slide the new power supply into the empty bay until it stops (the module will not be flush with the edge of the bay).
11. While pushing the release latch to the left, gently push the module in its bay until it clicks into place.

- 12.** Pair the power leads with the appropriate power terminal (located at the back of the unit), respecting the polarity.
- 13.** Tighten the screws to attach the power leads to the unit.
- 14.** Turn on the disconnect device that is connected to the new power supply module.

Replacing the OTDR

You may need to replace the OTDR for maintenance purposes.



WARNING

To avoid serious injuries as well as irreparable damage to your unit, always remove both power cords before opening or servicing the unit.



CAUTION

To avoid damaging your unit or its components, you should wear an antistatic band during this maintenance operation. For more information, see *Preventing Electrostatic Discharge Damage* on page 25.

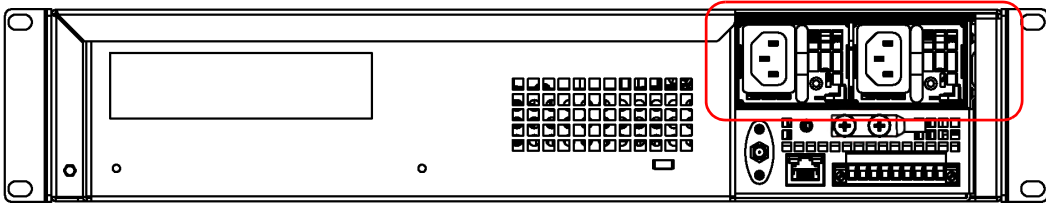
To replace the OTDR:

- 1.** If you are using a fiber management tray, remove the protective window. For more information, see *Working with the Fiber (Patchcord) Management Tray* on page 37.

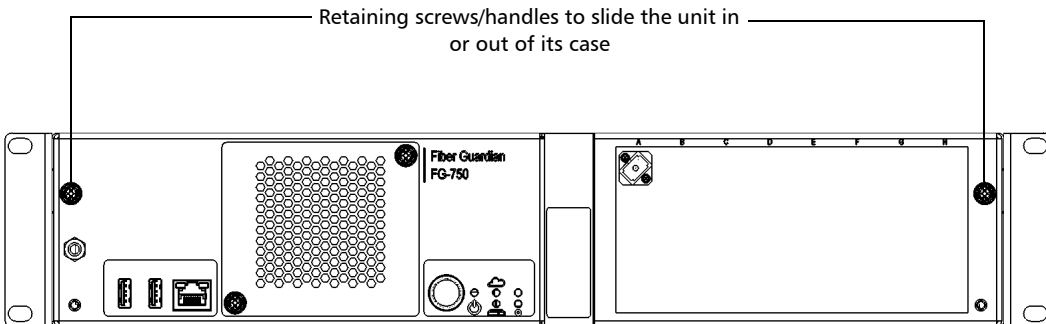
Maintenance

Replacing the OTDR

2. Turn off the unit and disconnect it completely from the power sources.

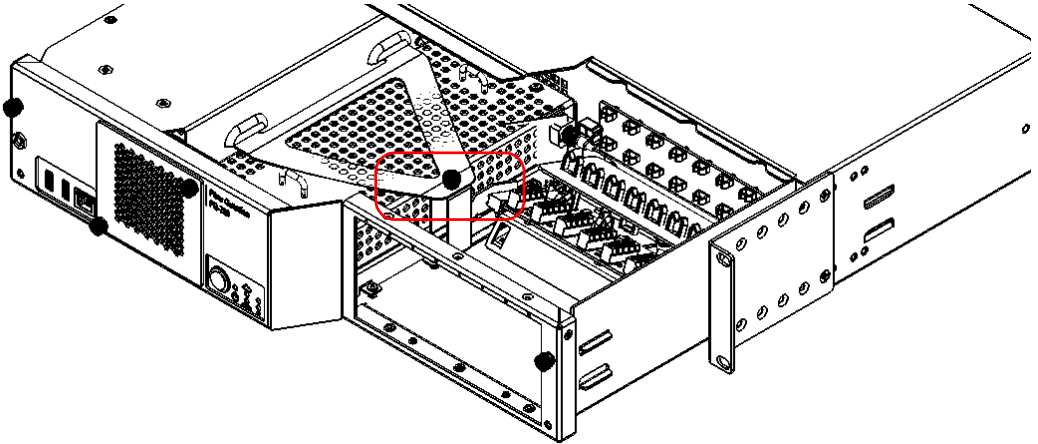


3. Put on an antistatic strap and connect it to the connector provided for that purpose on the front panel of the unit.
4. Turn the unit's main compartment screws counterclockwise until the compartment is loose. Since the screws are captive screws, you cannot remove them completely.



5. Using the screws as handles, gently pull the compartment towards you to open the unit.

6. Turn the screw of the OTDR's retaining tab counterclockwise until the tab is loose. Since the screw is a captive screw, you cannot remove it completely.



7. Remove the retaining tab to access the OTDR.



CAUTION

To avoid damaging the fiber or the module, proceed with caution when connecting or disconnecting the fiber from the OTDR's port.

8. Unscrew the optical fiber's connector to disconnect the fiber from the OTDR's port.
9. Using the two handles on the module, pull up the module to remove it from the unit's casing.
10. Clean the port of the new OTDR.
11. Clean the optical fiber connector (see *Cleaning and Connecting Optical Fibers* on page 82).
12. Carefully align the module with the anchoring pins at the bottom of the unit's casing.

Maintenance

Replacing the OTDR

- 13.** Insert the new module, ensuring that it lays flat on the bottom of the unit's casing.
- 14.** Connect the optical fiber to the module (see *Cleaning and Connecting Optical Fibers* on page 82).
- 15.** Place the retaining tab back into place, over the OTDR.
- 16.** Turn the screw of the retaining tab clockwise until the tab is secured in place.
- 17.** Using the screws as handles, gently push the unit's main compartment to close it.
- 18.** Turn the unit's main compartment screws clockwise until the compartment is secured in place.
- 19.** Remove your antistatic strap.
- 20.** Reconnect the unit to its power sources (turn on both disconnected devices) and turn on your unit.
- 21.** If you are using a fiber management tray, put the protective window back into place. For more information, see *Working with the Fiber (Patchcord) Management Tray* on page 37.

Your new OTDR is ready to be used.

Replacing an RTU or Changing the SSD (managed by EMS)

To replace an RTU:

1. Start the HostWebUI application.
 - 1a. Select **Host** from the **Configuration** menu.
 - 1b. Under **Northbound Settings**, select **EMS Server**.

The screenshot displays the EXFO Host Manager web interface. The top navigation bar includes the EXFO logo, the text "Host Manager Host Configuration", and system information: "Host Date/Time: 2015-06-16 16:06(UTC)", "Local Date/Time: 2015-06-16 12:06(UTC-04:00)", and "Username: Admin". Below the navigation bar are tabs for "Configuration", "Actions", "Status", "Reports", and "About". A language dropdown is set to "English" and a "Logout" button is present. The main content area is divided into a left sidebar and a central panel. The sidebar shows a tree view with categories: "Configure Host", "Host Settings" (containing Network, 3G/4G, Log), "Companion Settings" (containing Network), "Northbound Settings" (containing EMS Server, E-Mail Server, SNMP, LDAP), and "Edit". The central panel is titled "EMS Server" and contains the following fields and buttons: "IP address/host name:" (text input), "Polling frequency (hrs.):" (text input with value "24"), "Network topology:" (text input with value "LAN"), and four buttons: "Test Connection", "Start Synchronization", "Recovery Configuration", and "Detach From EMS".

Maintenance

Replacing an RTU or Changing the SSD (managed by EMS)

2. Note the MAC address of the old RTU from the EMS.
 - 2a. Select **Network** from the **Configuration** menu.
 - 2b. Note the MAC address displayed under the **Rear adapter** section.

The screenshot shows the EXFO Host Manager interface. The top navigation bar includes 'Configuration', 'Actions', 'Status', 'Reports', and 'About'. The right side of the header displays 'Host Date/Time: 2015-03-05 19:16(UTC)', 'Local Date/Time: 2015-03-05 14:16(UTC-6)', and 'Username: Admin'. The left sidebar contains a tree view with categories like 'Edit', 'Configure Host', 'Host Settings', 'Companion Settings', and 'Northbound Settings'. The 'Network' option under 'Host Settings' is selected. The main content area is divided into sections: 'Host' (Hostname: FG750801305, Timezone: (UTC) Casablanca), 'BMC' (System version: 1.1.2.0), 'Rear adapter IPv4 configuration' (DHCP enabled, IP address, Subnet mask, Gateway, MAC address: 00-03-01-FF-C2-A8), and 'Rear adapter IPv6 configuration' (DHCP enabled). The MAC address '00-03-01-FF-C2-A8' is circled in red.

3. Turn ON RTU. (Do not detect any port).

4. Test the RTU connection with EMS.
 - 4a. Select **EMS Server** from the HostWebUI > **Configuration** > **Host** menu.
 - 4b. Click the **Edit** button.
 - 4c. Enter the EMS **IP address/host name** in the **EMS Server** configuration section.
 - 4d. Click the **Apply** button.

The screenshot displays the EXFO Host Manager web interface. The top navigation bar includes the EXFO logo, 'Host Manager Host Configuration', and system information: 'Host Date/Time: 2015-03-05 19:29(UTC)', 'Local Date/Time: 2015-03-05 14:29(UTC-0)', and 'Username: Admin'. Below the navigation bar are tabs for 'Configuration', 'Actions', 'Status', 'Reports', and 'About'. A language dropdown is set to 'English'. The left sidebar shows a tree view of configuration options, with 'EMS Server' selected under 'Northbound Settings'. The main content area is titled 'EMS Server' and contains the following configuration fields:

- IP address/host name: 10.206.21.102
- Polling frequency (hrs.): 24
- Network topology: LAN

Below the fields are five buttons: 'Test Connection' (highlighted in blue), 'Start Synchronization', 'Recovery Configuration', and 'Detach From EMS'.

5. Click the **Test Connection** button. The application will ask you if you want to synchronize the configuration now. Click **No** to this.

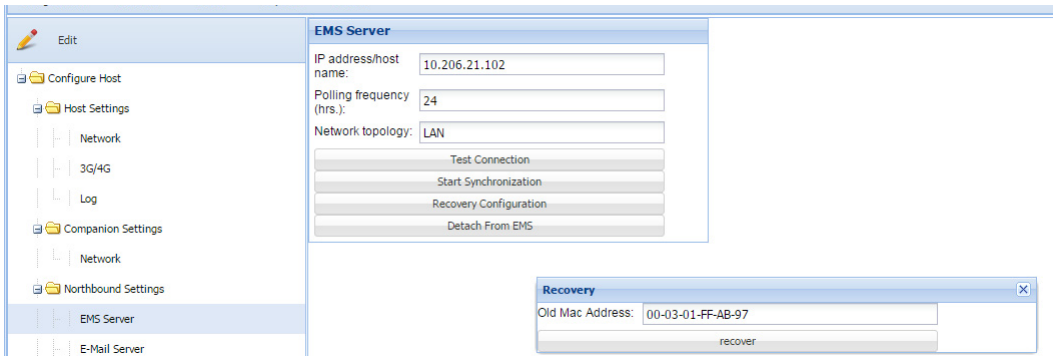
Maintenance

Replacing an RTU or Changing the SSD (managed by EMS)

6. Perform **Recovery Configuration**:

6a. Click the **Recovery Configuration** button.

6b. Enter the **Old MAC Address** (previously noted in step 2) in the **Recovery** text box and click the **recover** button.



7. On EMS web UI, select the RTU and then clear the **Offline** check box.

8. After completion of successful recovery, check the RTU status on EMS; it should be in **Not connected** and **Synchronized** state.

Backing Up the Database

When you are using the+ RTU in stand-alone mode, you must perform backups of the database for additional security in case of a major system failure.

Note: *When the RTU is used with the EMS server, there is no need for manual backups, because the system configuration is copied on the EMS server.*

Depending on the database size, the backup process can take from a few seconds to a about 10 minutes.

The backup file includes *all* the database entries, such as:

- Optical routes, test setups, test programs
- Custom thresholds
- Default values
- Results

The application names the backup files as follows:

Year Day Minute
 YYYYMMDDHHMM.NqmsOtdr.BAK
 Month Hour file name extension

You can find the backup file in the *D:\DatabaseBackup* folder, on your RTU.

Note: *Only the most recent backup is kept.*

If you ever need to recover the database, contact EXFO (see *Contacting the Technical Support Group* on page 335).

Maintenance

Backing Up the Database

To back up the database:

1. From the main menu, select **Configuration > Remote Test Unit**.
2. Click **Backup Database**.

The screenshot shows the EXFO NQMSfiber - Remote Test Unit web interface. The top navigation bar includes 'Configuration', 'Status', 'Reporting', 'Manual Test', 'About', and 'Logout'. The left sidebar shows a tree view with 'Remote Test Unit' selected, containing 'Connected Optical Routes' and 'Controlled ROTAUs'. The main content area displays the following information:

- Name:** S/N:792338
- Comments:** (Empty text area)
- Status:** Responding
- OTDR Section:**
 - Serial number:** 792338
 - Model name:** OTM-740-CD16
 - Wavelength:** 1610 nm on singlemode B1
- OTAU Section:**
 - Serial number:** 801305
 - Number of ports:** 22
 - Port state:** Provisioned Not Provisioned Force Pro

At the bottom right of the interface, there are two buttons: 'Backup Database' and 'Reset T'.

Viewing the Installed Applications

You can view a list of all the applications installed on the host as well as their versions. If you need to retrieve the firmware (system) version of the companion, see *Viewing the Firmware Version of the Companion* on page 290.

To view a list of the installed applications:

- 1.** Connect to the Host Web UI. For more information, see *Accessing and Exiting the Host Web UI* on page 109.
- 2.** From the **Configuration** menu, click **Software Packages**.

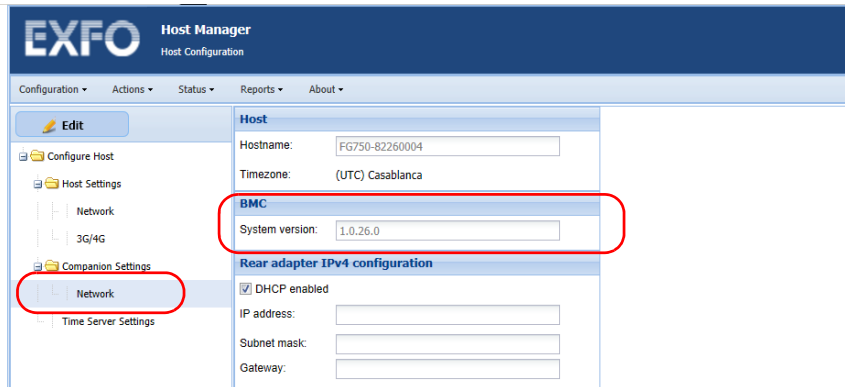
The Web UI displays a list of all the installed applications.

Viewing the Firmware Version of the Companion

You can retrieve the firmware (system) version of the companion from the Host Web UI.

To view the firmware version of the companion:

1. Connect to the Host Web UI. For more information, see *Accessing and Exiting the Host Web UI* on page 109.
2. From the main menu, select **Configuration > Host**.
3. Under **Companion Settings**, select **Network**.



The version number is displayed under **BMC**.

Managing Applications (Software Packages)

You can add, modify, or delete software packages from the host directly in Host Web UI or from the EMS if the RTU is linked to one.

You can modify the settings (name, transfer and installation dates, etc.) for a specific package that has already been added, or even delete a package that you no longer need. Deleting a software package removes the application from the host. However, the edition and deletion are not allowed for all the software packages.

The edition and deletion operations can be performed according to the following table.

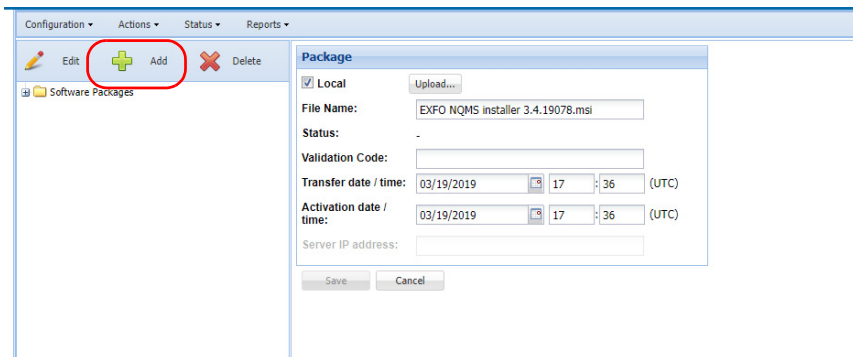
Possible States for Software Packages	Allowed Operations
Scheduled	Edit, delete
Downloaded	Edit, delete
Download failed	Edit, delete, retry
Activated	Delete
Activation failed	Delete, retry
Cancel failed	Delete, retry
History (was replaced by a more recent one)	Delete

Maintenance

Managing Applications (Software Packages)

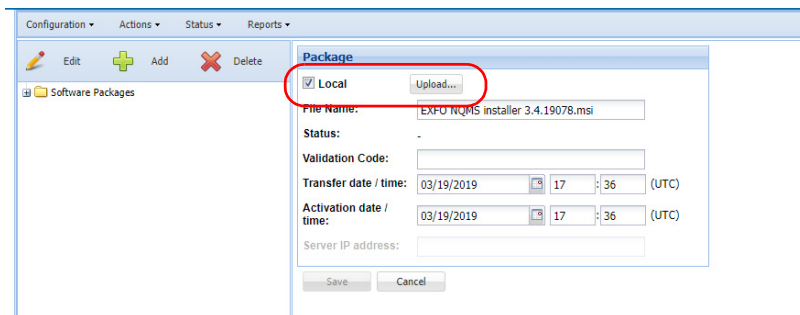
To add a software package:

1. If you intend to connect to your unit via a WAN or the Internet, connect to the VPN (see *Connecting to the VPN* on page 79); otherwise, go directly to the next step.
2. Connect to the Host Web UI. For more information, see *Accessing and Exiting the Host Web UI* on page 109.
3. From the **Configuration** menu, click **Software Packages**.
4. Click **Add**.



The screenshot shows the Host Web UI interface. At the top, there are navigation menus: Configuration, Actions, Status, and Reports. Below these, there are icons for Edit, Add, and Delete. The 'Add' icon is highlighted with a red circle. The main content area shows a folder icon for 'Software Packages'. On the right side, there is a 'Package' form with the following fields: Local (checked), File Name (EXFO NQMS installer 3.4.19078.msi), Status (-), Validation Code (empty), Transfer date / time (03/19/2019 17:36 UTC), Activation date / time (03/19/2019 17:36 UTC), and Server IP address (empty). There are 'Save' and 'Cancel' buttons at the bottom of the form.

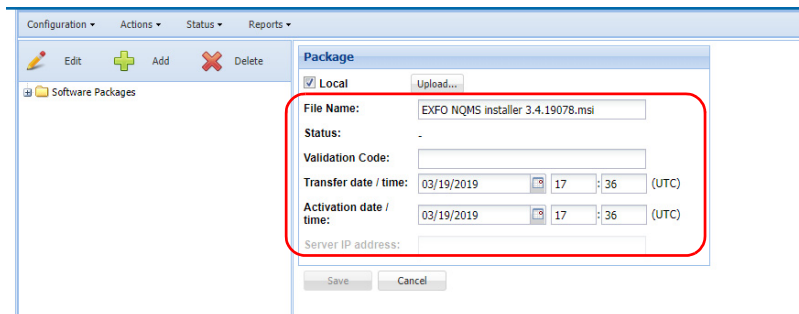
5. Upload the package:
 - 5a. Select the **Local** option, then click **Upload**.



The screenshot shows the Host Web UI interface, similar to the previous one. The 'Local' checkbox is checked and highlighted with a red circle. The 'Upload...' button is also highlighted with a red circle. The rest of the form fields and buttons are the same as in the previous screenshot.

- 5b.** Locate the desired software package in the browser window, then click **Open**.

Once the operation is complete, the file name, and transfer and activation dates will be provided automatically. You can modify the transfer and activation dates if they do not suit your needs.



The screenshot shows a web-based interface for managing software packages. The main window has a menu bar with 'Configuration', 'Actions', 'Status', and 'Reports'. Below the menu is a toolbar with 'Edit', 'Add', and 'Delete' buttons. The left sidebar shows a tree view with 'Software Packages'. The main content area displays a 'Package' configuration dialog. The dialog has a 'Local' checkbox checked and an 'Upload...' button. The 'File Name' field contains 'EXFO NQMS installer 3.4.19078.msi'. The 'Status' field is empty. The 'Validation Code' field is empty. The 'Transfer date / time' field is set to '03/19/2019 17:36 (UTC)'. The 'Activation date / time' field is also set to '03/19/2019 17:36 (UTC)'. The 'Server IP address' field is empty. At the bottom of the dialog are 'Save' and 'Cancel' buttons. A red rectangle highlights the 'File Name', 'Status', 'Validation Code', 'Transfer date / time', and 'Activation date / time' fields.

Note: The upload operation can take several minutes.

Note: If you enter a past date or time, the transfer or activation will start right away.

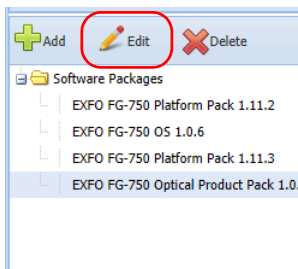
- 6.** Click **Save**.

Maintenance

Managing Applications (Software Packages)

To edit a software package:

1. Connect to the Host Web UI. For more information, see *Accessing and Exiting the Host Web UI* on page 109.
2. From the **Configuration** menu, click **Software Packages**.
3. From the list of the installed software packages, click the package that you want to edit.
4. Click **Edit**.



5. Modify the information as needed.
6. Click **Save**.

To delete a software package:

1. Connect to the Host Web UI. For more information, see *Accessing and Exiting the Host Web UI* on page 109.
2. From the **Configuration** menu, click **Software Packages**.
3. From the list of the installed software packages, click the package that you want to delete.
4. Click **Delete**, then confirm your choice.

Recalibrating the Unit

EXFO manufacturing and service center calibrations are based on the ISO/IEC 17025 standard (*General Requirements for the Competence of Testing and Calibration Laboratories*). This standard states that calibration documents must not contain a calibration interval and that the user is responsible for determining the re-calibration date according to the actual use of the instrument.

The validity of specifications depends on operating conditions. For example, the calibration validity period can be longer or shorter depending on the intensity of use, environmental conditions and unit maintenance, as well as the specific requirements for your application. All of these elements must be taken into consideration when determining the appropriate calibration interval of this particular EXFO unit.

Under normal use, the recommended interval for your FG-750 Fiber Guardian is: three years.

For newly delivered units, EXFO has determined that the storage of this product for up to six months between calibration and shipment does not affect its performance (EXFO Policy PL-03).

Maintenance

Recycling and Disposal

To help you with calibration follow-up, EXFO provides a special calibration label that complies with the ISO/IEC 17025 standard and indicates the unit calibration date and provides space to indicate the due date. Unless you have already established a specific calibration interval based on your own empirical data and requirements, EXFO would recommend that the next calibration date be established according to the following equation:

Next calibration date = Date of first usage (if less than six months after the calibration date) + Recommended calibration period (three years)

To ensure that your unit conforms to the published specifications, calibration may be carried out at an EXFO service center or, depending on the product, at one of EXFO's certified service centers. Calibrations at EXFO are performed using standards traceable to national metrology institutes.

Recycling and Disposal



This symbol on the product means that you should recycle or dispose of your product (including electric and electronic accessories) properly, in accordance with local regulations. Do not dispose of it in ordinary garbage receptacles.

For complete recycling/disposal information, visit the EXFO Web site at www.exfo.com/recycle.

12 Troubleshooting

Solving Common Problems

Problem	Possible Cause	Solution
The unit has restarted unexpectedly.	<ul style="list-style-type: none">▶ There was a problem with the host while you were working or at startup of the unit.▶ There was a problem with the companion.▶ There has been a power failure.	Any problem that could have occurred should be solved once the unit has restarted. If the problem persists, contact EXFO.
You have waited 10 minutes after starting the installation of the Platform package, but you are still unable to connect to the Host Web UI.	There was a problem during the installation process.	Try restarting the unit through the KVM console, or manually (by pressing the button on the front panel); ensure that the Host Web UI is accessible, and that the right version has been installed properly. If the new version has not been installed, try reinstalling the Platform package. If you are not able to reconnect to the Host Web UI or if the new package cannot be installed, contact EXFO.

Troubleshooting

Solving Common Problems

Problem	Possible Cause	Solution
The Host Web UI stops responding in the “Loading” state.	The IP address or the host name of the host machine has changed.	Check the IP address of the host, and correct if necessary.
	The host machine is restarting.	Wait for the host machine to start.
	The host machine is not reachable.	Contact your network administrator for network-related troubleshooting.
	The Web browser that is used is not supported.	Use one of the supported browsers see <i>Supported Web Browsers</i> on page 12. If none of the solutions mentioned above solves the problem, contact EXFO.
Network settings are not properly applied on the host machine.	Wrong IP address, subnet mask, or gateway.	Check if the IP address, subnet mask and gateway that you have specified for the host are valid.
The Web interface is not loaded or not rendered properly in the Web browser.	Browser-specific issue. The browser might not support HTML5.	Refresh the Web page. If the interface still does not load properly, check the version of your browser. The Web browser must support HTML5. For the complete list of supported Web browsers, see <i>Supported Web Browsers</i> on page 12.

Problem	Possible Cause	Solution
Web browser is not prompting the user for login credentials.	Login credentials are saved in the Web browser cache.	If you have enabled the browser to save passwords, disable the setting and clear the browser cache.
Impossible to connect to the KVM remote console.	Java may not be installed on your computer.	Ensure that Java 6 or later is installed on the computer that you intend to use to connect to remote console.
	The Web browser that is used is not supported.	Use one of the supported browsers see <i>Supported Web Browsers</i> on page 12. If none of the solutions mentioned above solves the problem, contact EXFO.
The unit is not responding.	---	Try restarting the host through the KVM console, or manually by pressing and holding down the power button for 5 seconds. If this does not solve the problem, try restarting both the host and the companion, by pressing and holding down the power button for 10 seconds. If the problem persists, contact EXFO.

Troubleshooting


LED Indicators Description


LED Indicators Description

The LEDs on your unit help you determine its current status. They are located on the front panel.

For the power and system LEDs, if more than one error is detected at the same time, the color of the LED will be set according to the most severe error (red as the most severe, followed by yellow).


The table below presents the possible statuses once the initial startup sequence is complete.




LED	Status	Meaning and Possible Solution
 Power	Green	The unit is on and there are no voltage problems.
	Yellow	Non-critical voltage error detected. You can look in the Host Web UI for more information (see <i>Viewing System Status</i> on page 304). One of the power supply module could be missing or defective. Ensure that both power supply modules are present and functioning properly. If necessary, replace the defective power supply (see <i>Replacing the Power Supply Modules</i> on page 275). If the problem persists, contact EXFO.
	Red	Critical voltage error detected. Contact EXFO.
	Off	The unit has been disconnected from all its power sources.

LED	Status	Meaning and Possible Solution
 System	Green	The unit is working properly. There are no software or hardware problems.
	Yellow	<p>Non-critical hardware error detected. You can look in the Host Web UI for more information (see <i>Viewing System Status</i> on page 304).</p> <ul style="list-style-type: none"> ➤ The air filter could be dirty. Inspect and replace the air filter if necessary (see <i>Replacing the Air Filter</i> on page 263). ➤ The temperature of the room where the unit is located, could be slightly too low or too high. Ensure that the temperature falls within the specified operating temperature range (see <i>Electrical Safety Information</i> on page 20). Once the problem is solved, refresh the LEDs status (see <i>Refreshing the Status of the LEDs</i> on page 306). <p>If the problem persists, contact EXFO.</p>
	Yellow, blinking	<p>Non-critical software error detected.</p> <ul style="list-style-type: none"> ➤ Consult the Event log to find the cause of the problem and try to solve it (see <i>Viewing the Event Log</i> on page 249). ➤ Once the problem is solved, refresh the LEDs status (see <i>Refreshing the Status of the LEDs</i> on page 306). <p>If the problem persists, contact EXFO.</p>

Troubleshooting

LED Indicators Description

LED	Status	Meaning and Possible Solution
 System (continued)	Red	<p>Critical hardware error detected. You can look in the Host Web UI for more information (see <i>Viewing System Status</i> on page 304).</p> <ul style="list-style-type: none">➤ The fan could be defective. Replace the fan (see <i>Replacing the Fan</i> on page 267).➤ The temperature of the room where the unit is located, is critically too low or too high. Ensure that the temperature falls within the specified operating temperature range (see <i>Electrical Safety Information</i> on page 20). Once the problem is solved, refresh the LEDs status (see <i>Refreshing the Status of the LEDs</i> on page 306). <p>If the problem persists, contact EXFO.</p>
	Red, blinking	<p>Critical software error detected.</p> <ul style="list-style-type: none">➤ Consult the Event log to find the cause of the problem and try to solve it (see <i>Viewing the Event Log</i> on page 249).➤ Once the problem is solved, refresh the LEDs status (see <i>Refreshing the Status of the LEDs</i> on page 306). <p>If the problem persists, contact EXFO.</p>
	Off	<p>The host is off.</p>

LED	Status	Meaning and Possible Solution
 Communication	Green	The LAN is up (on the rear Ethernet port).
	Green, blinking	The LAN is down, but the unit has automatically switched to 3G.
	Yellow	<ul style="list-style-type: none"> ▶ The LAN is down and the 3G network is down, or there is a problem with the configuration of the 3G settings (ex.: wrong APN). ▶ The unit is not equipped with the 3G option.
 Measurement in progress	Green	An OTDR acquisition is underway.
	Off	No acquisition is underway.
 Measurement status	Green	At least one optical route is detected.
	Green, blinking	At least one route is in the skipped status. No fault is present.
	Yellow	A fiber fault with degradation type is present.
	Red	At least a fiber fault with break type is present.

Viewing System Status

You can view the current status on your system under three views: host, companion and system. The status information includes the host name and serial number, the address of the time server and synchronization interval, the IPv4 and IPv6 configuration for the rear adapters for both the host and companion, as well as information such as the LED and relay statuses, processor usage and system temperature.

To view system status:

1. Connect to the Host Web UI.
2. From the **Status** menu, click **System Information**.
The interface displays the **Host Information** window.
3. If you want to view the companion status, click **Companion Information**.
4. If you want to view the system status, click **System Status**.

Testing the Status of the Relays

You can test the status of the power, system, and user-defined relays directly from the Host Web UI.

To test the status of the relays:

1. Start the Host Web UI. For more information, see *Accessing and Exiting the Host Web UI* on page 109.
2. From the **Status** menu, click **System Information**.

3. Click **System Status**.

The screenshot shows a software interface with a menu bar (Configuration, Actions, Status, Reports, About) and a sidebar with 'System Information' expanded to 'System Status'. The main content area displays 'Host uptime: -' and two tables: 'LED status' and 'Relay status'.

LED	Status
Power	(Yellow)
System	(Red Blinking)
Communication	(Green)
Measurement in progress	(Red Blinking)
Measurement status	(Red)

Relay	Status	Symbol	Test
Power	Active		<input type="button" value="Test"/>
System	InActive		<input type="button" value="Test"/>
User-defined	Active		<input type="button" value="Test"/>

4. Under **Relay status**, click the **Test** button corresponding to the relay that you want to test.

The relay status changes from its current status to the other (from “Active” to “InActive”, or from “InActive” to “Active”); and then comes back to its initial status.

Refreshing the Status of the LEDs

When power or system errors occur, the corresponding LED switches from green to another color, depending on the type of problem that has been detected (see *LED Indicators Description* on page 300). For troubleshooting purposes, the status of the LEDs is kept until you refresh it.

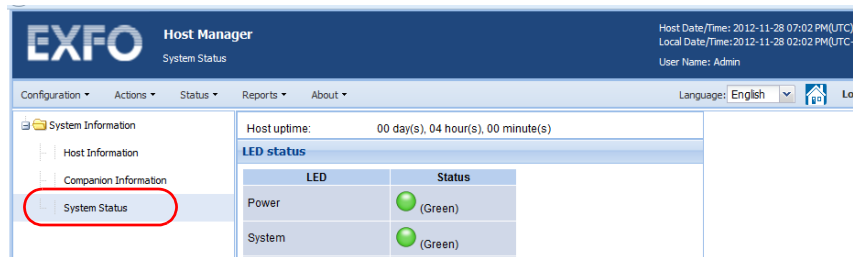
You can refresh the status of the power or system LEDs using one of the following methods:

- Send a request to refresh the status, via the Fiber Guardian Web user interface, or by using the *LedStateChangeRequest* REST command. This method is particularly useful when you do not need to turn off the unit (for example, after you corrected software errors). For more information on the REST commands, see *Working with the REST Commands (Certain Models Only)* on page 84.
- Shut down and restart the unit. For more information, see *Turning On or Off the Unit* on page 48.

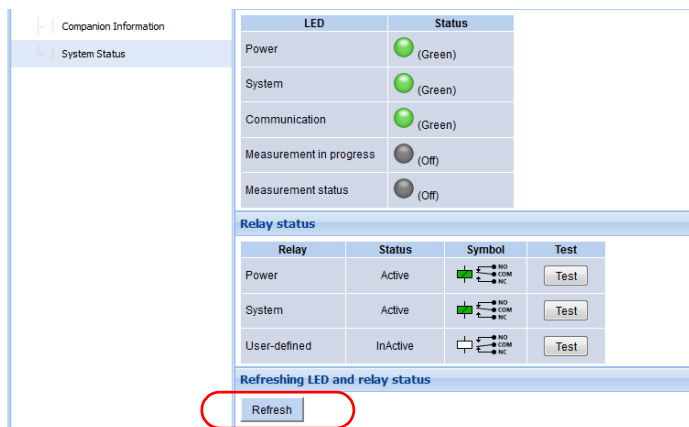
Normally, you will only need to refresh the status of the LEDs in the case of software errors. For hardware errors that require a replacement of material (power supply, fan, filter), the status will be refreshed automatically after you restart your unit.

To refresh the status of the LEDs via the Host Web UI:

1. Connect to the Host Web UI. For more information, see *Accessing and Exiting the Host Web UI* on page 109.
2. From the main menu, select **Status > System Information**.
3. From the tree view, select **System Status**.



4. Under **Refreshing LED and relay status**, click the **Refresh** button.



The LEDs will blink three times, indicating that the refresh operation is underway. After that, the status of the LEDs will have been updated.

Connecting to Your Unit Using the KVM Remote Console

Most of the configuration and monitoring tasks on your FG-750 unit can be performed via the Host Web UI. However, you may need to access your unit directly in certain cases such as advanced troubleshooting or when you need to install a VPN client.



IMPORTANT

You cannot access the KVM remote console via a WAN or the Internet. You must either use a portable computer (DHCP adapter) connected to the front port of the unit, or a computer connected to a same LAN as the unit. This is due to a limitation of the Internet, not of your system and applications.

For a complete list of supported Web browsers, see *Supported Web Browsers* on page 12.

To connect to your unit using the KVM remote console:

1. Ensure that your computer is equipped with Java 6 or later. If it is not the case, install it on your computer (www.java.com) first.
2. Connect to the Host Web UI. For more information, see *Accessing and Exiting the Host Web UI* on page 109.
3. From the main menu, select **Status > System Information**.

4. From the tree view, select **Companion Information**.

The screenshot shows the EXFO Host Manager interface. In the left-hand tree view, the 'Companion Information' item is highlighted with a red circle. The main content area displays the 'Network companion adapters' table.

	Parameters	Front Adaptor	Rear Adaptor
IPv4	DHCP Enabled	No	Yes
	IP Address	169.254.10.11	10.205.20.13
	Subnet Mask	255.255.0.0	255.255.0.0
	Default Gateway	-	10.205.255.254

5. Go to the **Rear Adaptor** column and write down the IP address of the rear port.

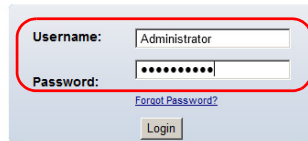
The screenshot shows the EXFO Host Manager interface. In the left-hand tree view, the 'Companion Information' item is selected. The main content area displays the 'Network companion adapters' table. The IP address '10.205.20.13' in the 'Rear Adaptor' column is circled in red.

	Parameters	Front Adaptor	Rear Adaptor
IPv4	DHCP Enabled	No	Yes
	IP Address	169.254.10.11	10.205.20.13
	Subnet Mask	255.255.0.0	255.255.0.0
	Default Gateway	-	10.205.255.254

Troubleshooting

Connecting to Your Unit Using the KMV Remote Console

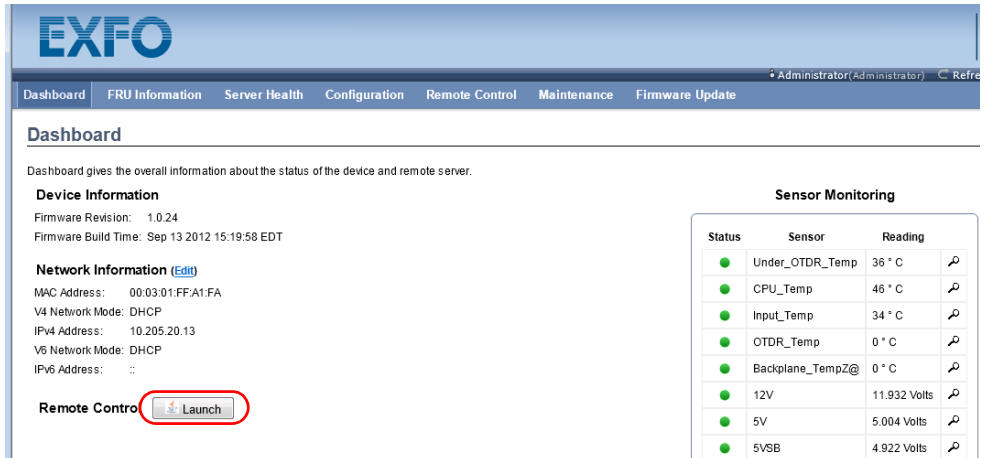
6. From your computer, open a Web browser, and then type `https://Companion_Rear_Port_IP_Address`, where the *Companion_Rear_Port_IP_Address* corresponds to the address that you have retrieved at step 5.
7. When the application prompts you, enter *Administrator* as the user name and *RTUEXFO123* as the password.



A screenshot of a web-based login form. The form is enclosed in a light blue rounded rectangle. It contains two input fields: 'Username:' with the text 'Administrator' and 'Password:' with ten black dots. Below the password field is a blue link that says 'Forgot Password?'. At the bottom center is a 'Login' button.

8. Click the **Login** button.

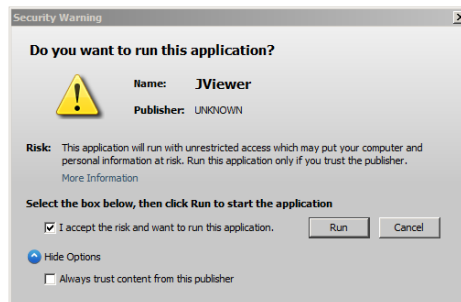
- From the **Dashboard** tab, click the **Launch** button.



The screenshot shows the EXFO dashboard interface. The top navigation bar includes tabs for Dashboard, FRU Information, Server Health, Configuration, Remote Control, Maintenance, and Firmware Update. The main content area is titled "Dashboard" and provides an overview of the device and remote server status. It is divided into three sections: Device Information, Network Information, and Remote Control. The Remote Control section contains a "Launch" button, which is circled in red. To the right, there is a "Sensor Monitoring" table with columns for Status, Sensor, and Reading.

Status	Sensor	Reading	
●	Under_OTDR_Temp	36 ° C	↻
●	CPU_Temp	46 ° C	↻
●	Input_Temp	34 ° C	↻
●	OTDR_Temp	0 ° C	↻
●	Backplane_TempZ@	0 ° C	↻
●	12V	11.932 Volts	↻
●	5V	5.004 Volts	↻
●	5VSB	4.922 Volts	↻

- When the application prompts you to confirm that you want to start the KVM remote console, select the **I accept the risk and want to run this application** check box.



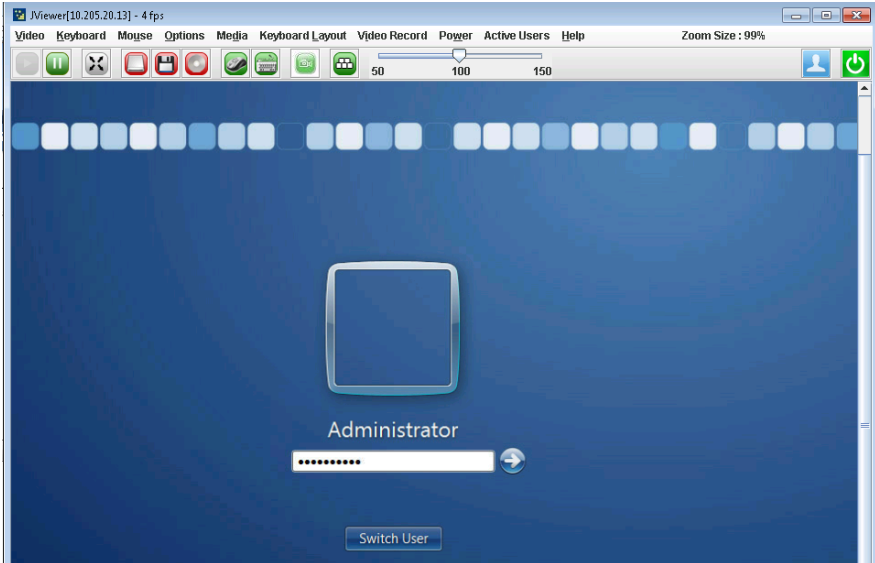
- Click **Run**.

Note: *If you never be prompted again for such applications, select the **Always trust content from this publisher** check box.*

Troubleshooting

Resetting Configuration (Parameters)

12. If necessary, log on to Windows using *Administrator* as the user account and *RTUEXFO123* as the password.



The KVM remote console displays the host's desktop.

Resetting Configuration (Parameters)

You can reset the Fiber Guardian host configuration to its factory default values. The following procedure describes how to reset host its default settings.

To reset the configuration of the host:

1. Connect to the Host Web UI. For more information, see *Accessing and Exiting the Host Web UI* on page 109.
2. From the **Actions** menu, click **Reset Configuration**.
3. When the application prompts you to confirm the operation, click **Yes**.

Restoring Your Unit to Normal Operation (Windows 8)

Your FG-750 unit comes with integrated emergency system tools with which you can:

- verify the integrity of the storage device
- revert your unit to its initial state (as it was when you purchased it) or restore it with a specific Windows image (WIM) that could have been provided to you by EXFO customer service, for example.



IMPORTANT

Restoring the system partition replaces what is currently installed on your unit with the image you choose. You can stop the process at any time, but you will still need to perform the recovery operation. Otherwise, your unit will not function properly.

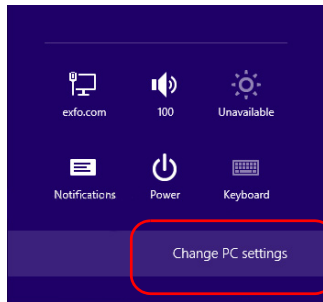
If you have installed new software, product packs and updates, you must reinstall them; otherwise, they will no longer be available.

Troubleshooting

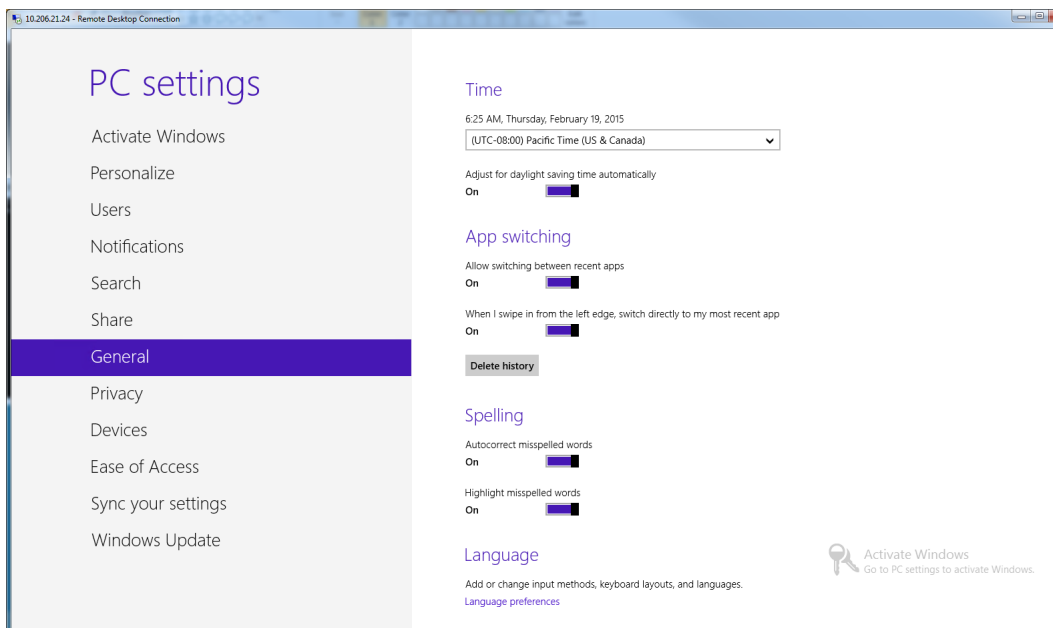
Restoring Your Unit to Normal Operation (Windows 8)

To restore the system partition:

1. Connect to the KVM remote console, but do not log in to Windows. For more information, see *Connecting to Your Unit Using the KVM Remote Console* on page 308.
2. From the remote console, go to the bottom-right corner of the screen with your mouse to make the Windows charm bar appear.
3. Select **Settings**, then, **Change PC settings**.



4. Select **General**.



Troubleshooting

Restoring Your Unit to Normal Operation (Windows 8)

5. Finally, click the **Get started** button for one of the two last options, either **Refresh your PC without affecting your files** or **Remove everything and reinstall Windows**. The second option reboots the computer and restores the original Windows.

Refresh your PC without affecting your files

If your PC isn't running well, you can refresh it without losing your photos, music, videos, and other personal files.

Get started

Remove everything and reinstall Windows

If you want to recycle your PC or start over completely, you can reset it to its factory settings.

Get started

Restoring Your Unit to Normal Operation (Windows 10)

Your FG-750 unit comes with integrated emergency system tools with which you can:

- verify the integrity of the storage device
- revert your unit to its initial state (as it was when you purchased it) or restore it with a specific Windows image (WIM) that could have been provided to you by EXFO customer service, for example.



IMPORTANT

Restoring the system partition replaces what is currently installed on your unit with the image you choose. You can stop the process at any time, but you will still need to perform the recovery operation. Otherwise, your unit will not function properly.

If you have installed new software, product packs and updates, you must reinstall them; otherwise, they will no longer be available.

You can create your own WIM files directly from your unit and store them on a USB key for future use.



IMPORTANT

The WIM files that you create are based on the serial number of your unit. This means that the WIM files created on one unit are only valid to restore this particular unit.

Troubleshooting

Restoring Your Unit to Normal Operation (Windows 10)



IMPORTANT

The creation of a WIM file implies a compression of the files that are currently installed on your unit. The size of the files after compression cannot be estimated beforehand.

For this reason, the application **WILL NOT PROMPT YOU AT THE BEGINNING** of the operation if the storage capacity (or the file system) of your USB key is not appropriate.



CAUTION

- ▶ **DO NOT TURN OFF** your unit while the recovery operation is underway. Doing so may severely damage your unit. Damaged units will need to be sent back to EXFO for repair.

When you want to restore your unit, there are several options. The table below gives an overview of the possibilities.

Method	Description
Restore	<ul style="list-style-type: none">▶ The unit will be reverted to the state in which it was when the WIM file was created.▶ All data files will be lost once the operation is complete.▶ If you have installed products and updates since the WIM file was created, you will have to reinstall them.
Reset to factory settings	<ul style="list-style-type: none">▶ The unit will be reverted to its initial state.▶ All data files will be lost once the operation is complete.▶ If you have installed products and updates since you purchased your unit, you will have to reinstall them.



IMPORTANT

To avoid problems, always use the wizard provided by EXFO to revert your unit to a previous state, not the recovery tools provided by Microsoft.





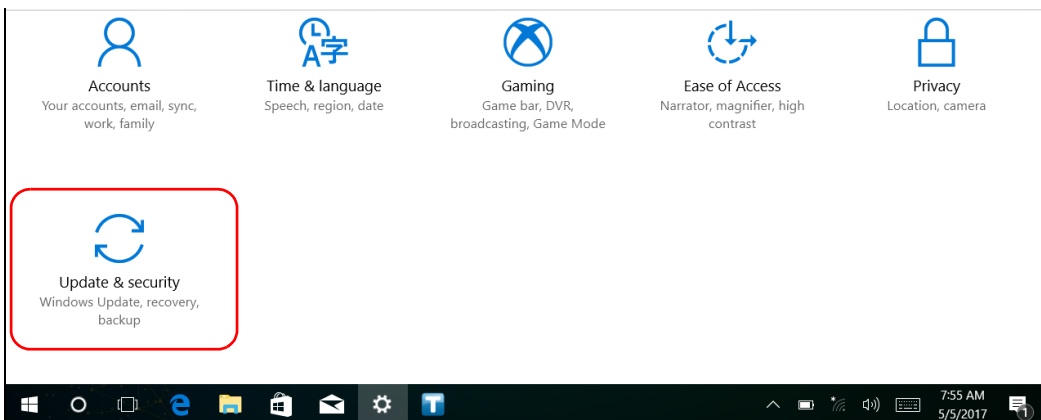
IMPORTANT

The size of the WIM will depend on the disk space that is currently used on your unit.

To avoid problems, always use a USB key with an NTFS file system, and a minimum of 16 GB of free disk space.

To create a WIM file for your unit:

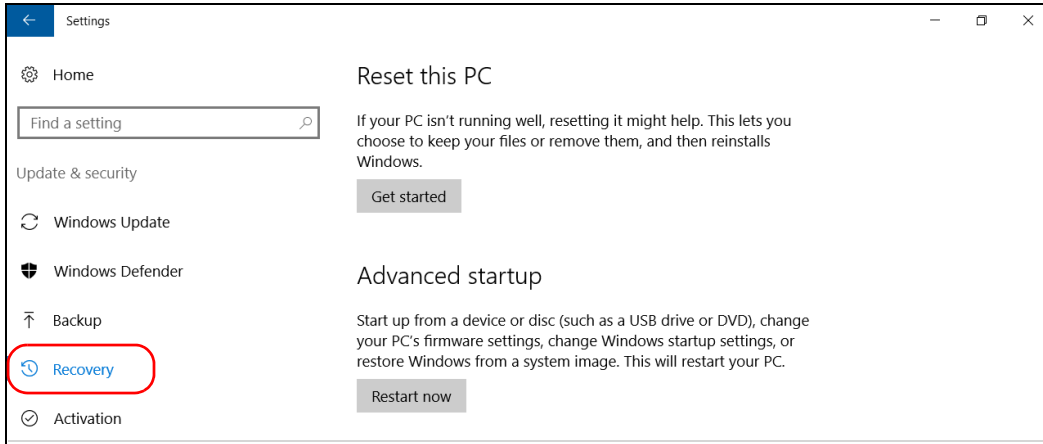
1. From the task bar, click the **Start** button (), and then **Settings** ().
2. Click **Update & security**.



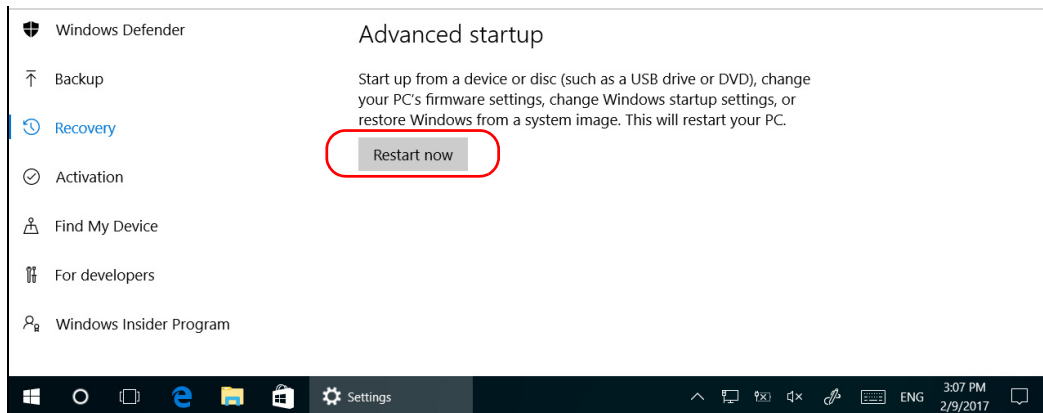
Troubleshooting

Restoring Your Unit to Normal Operation (Windows 10)

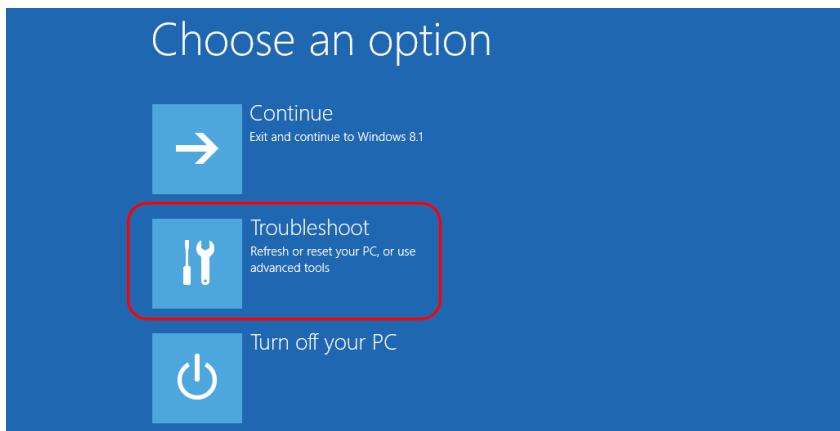
3. Select **Recovery**.



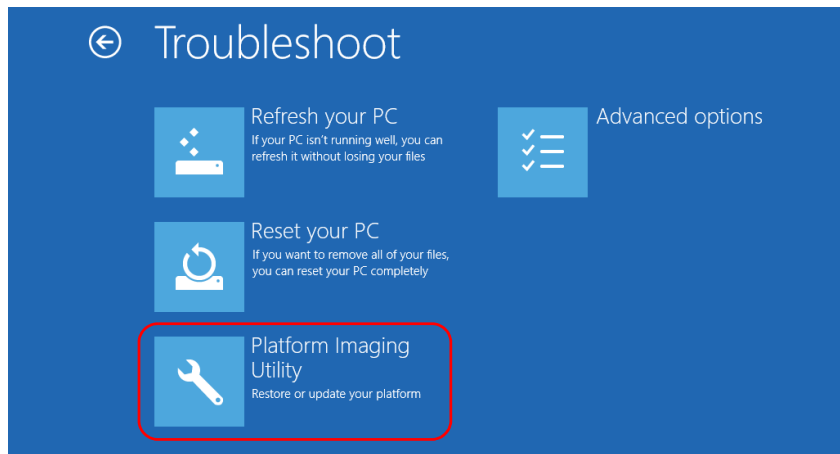
4. Under **Advanced Startup**, click **Restart now**.



5. Under **Choose an option**, click **Troubleshoot**.



6. Click **Platform Imaging Utility** to display the corresponding application.

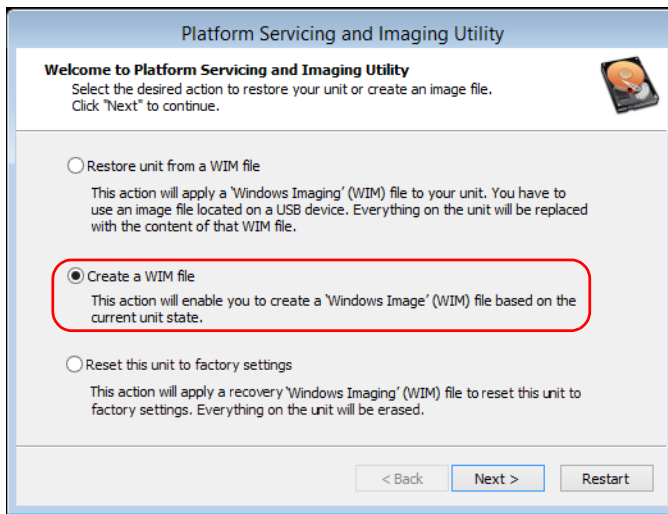


7. Connect a USB key to your unit.

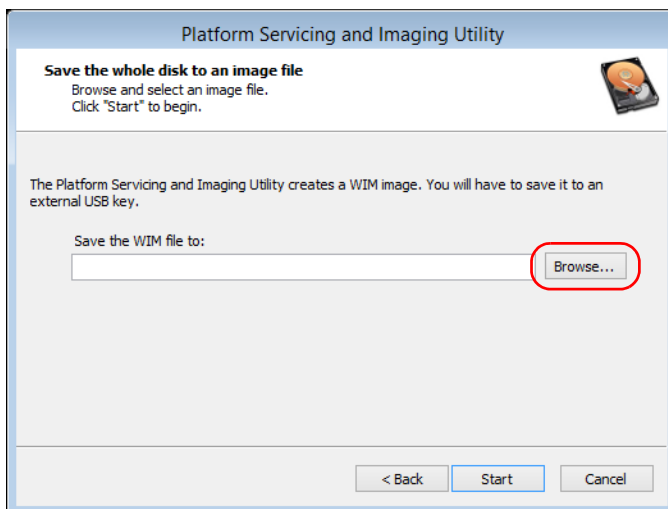
Troubleshooting

Restoring Your Unit to Normal Operation (Windows 10)

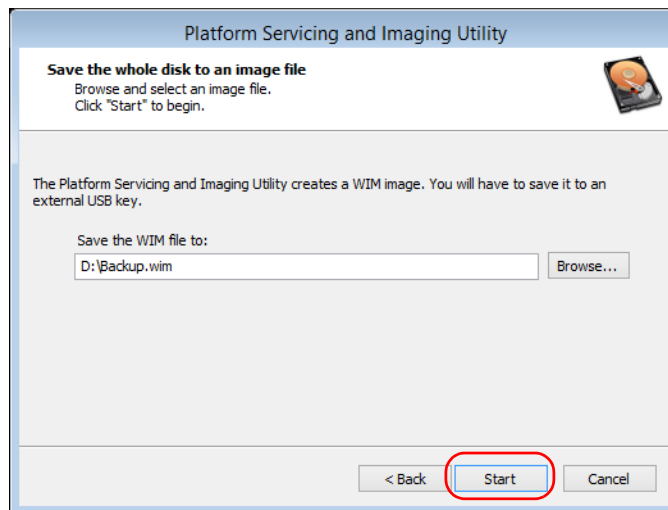
- From the Platform Servicing and Imaging Utility wizard, select **Create a WIM file**, and then click **Next**.



- Click **Browse**.



- 10.** Locate the USB key, and then double-click its identifier to access the contents.
- 11.** Select the desired folder.
- 12.** Enter a file name, and then click **Save**.
- 13.** Click **Start**.



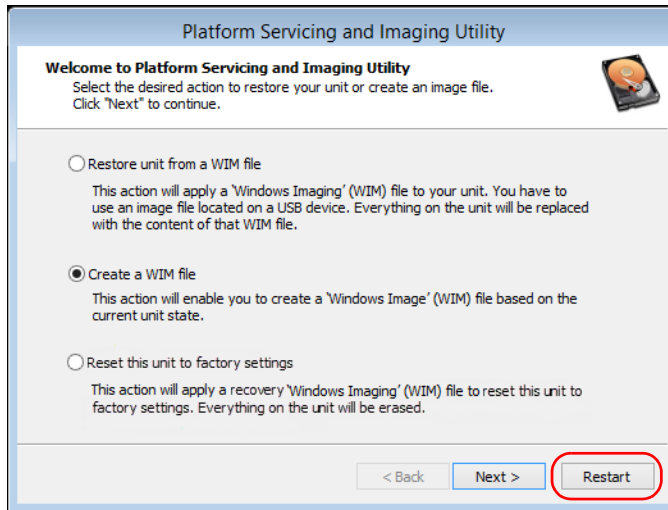
Note: *The time required to create the image varies with the configuration of your unit.*

- 14.** When the operation is complete and the application prompts you, click **OK**.
- 15.** Disconnect the USB key.
- 16.** Click **Cancel** to return to the Welcome window of the utility.

Troubleshooting

Restoring Your Unit to Normal Operation (Windows 10)

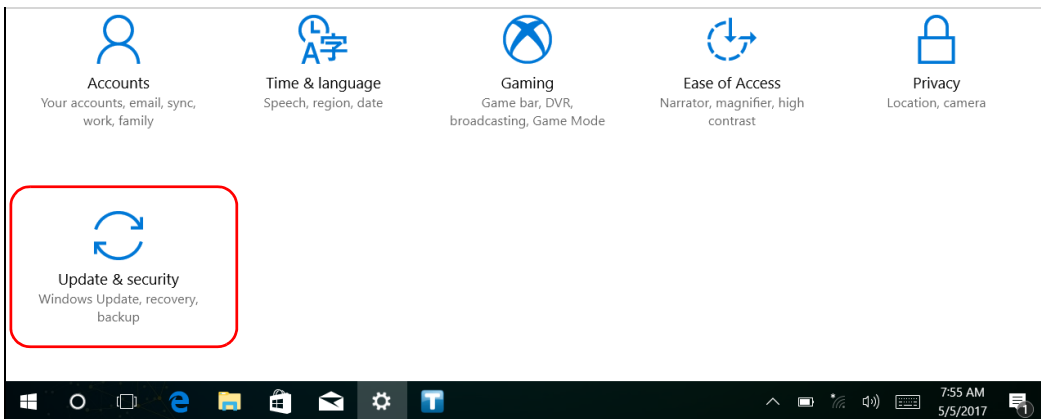
17. Click **Restart**.



The WIM file is ready for future use.

To revert your unit to a previous state with a WIM file:

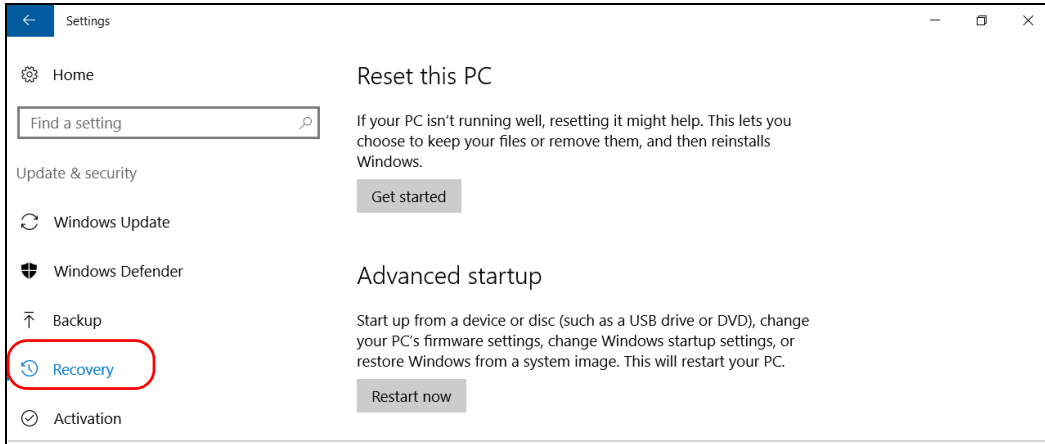
1. If desired, back up your data.
2. From the task bar, click the **Start** button (), and then **Settings** ().
3. Click **Update & security**.



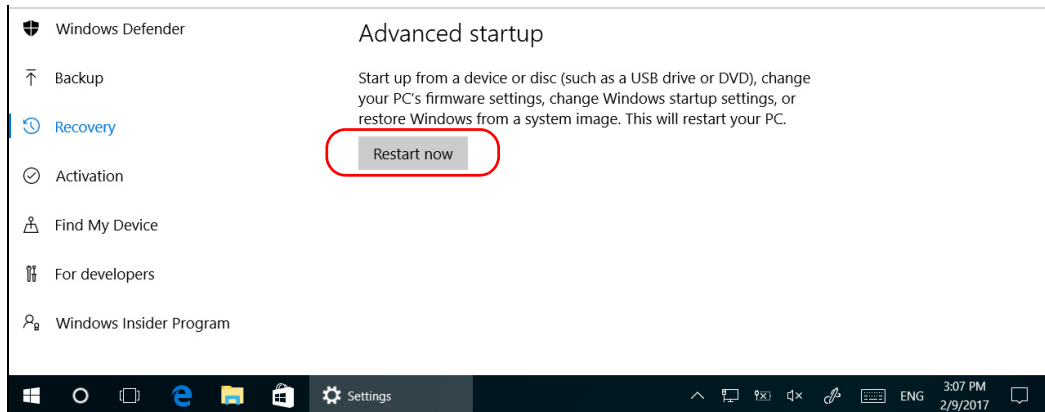
Troubleshooting

Restoring Your Unit to Normal Operation (Windows 10)

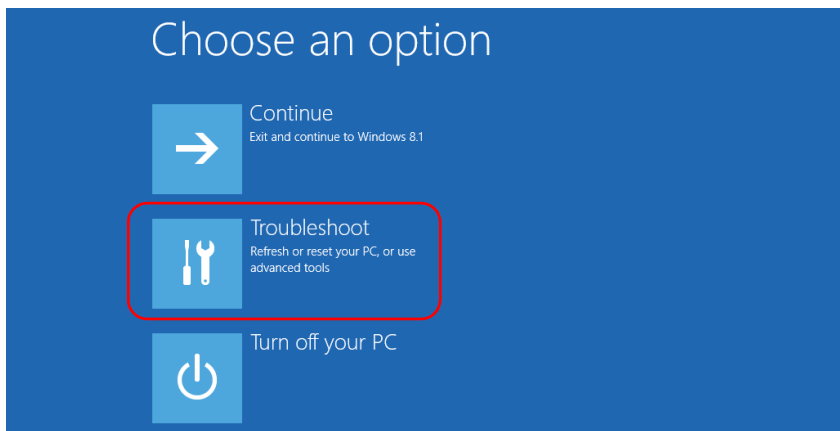
4. Select **Recovery**.



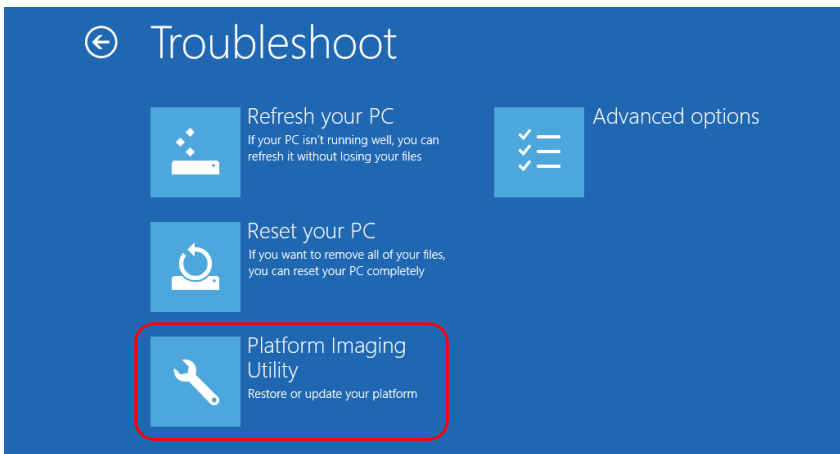
5. Under **Advanced Startup**, click **Restart now**.



- Under **Choose an option**, click **Troubleshoot**.



- Click **Platform Imaging Utility** to display the corresponding application.

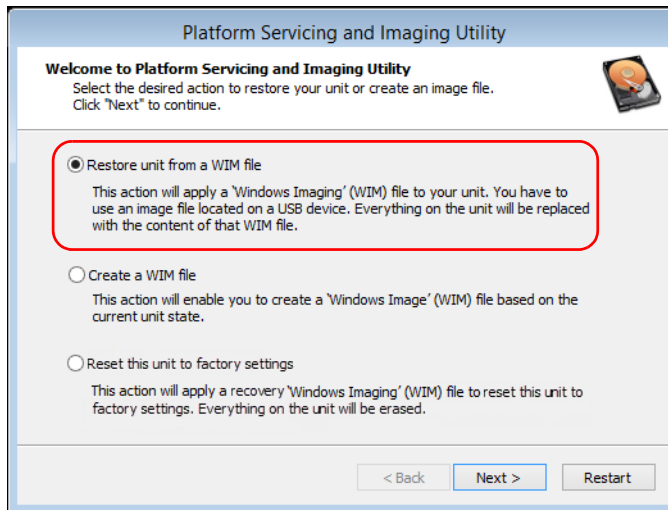


- Connect the USB key with the desired WIM file to your unit.

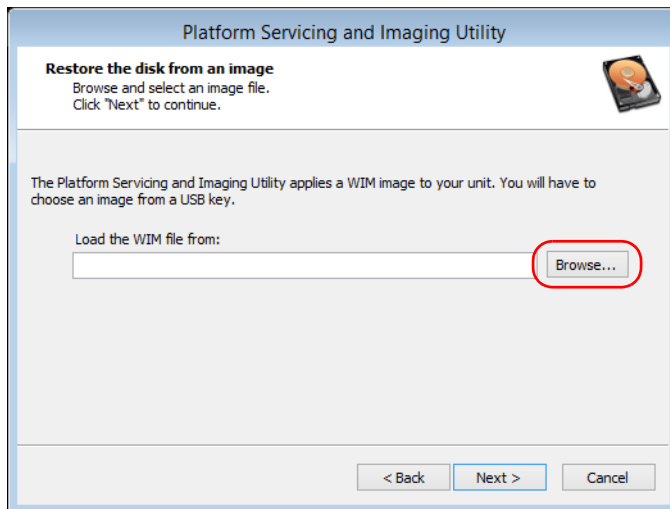
Troubleshooting

Restoring Your Unit to Normal Operation (Windows 10)

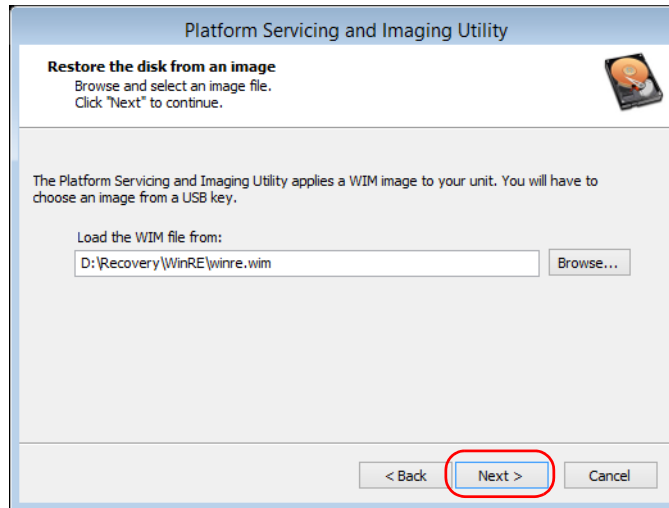
- From the Platform Servicing and Imaging Utility wizard, select **Restore unit from a WIM file**, and then click **Next**.



- Click **Browse**.



11. Locate the USB key, and then double-click its identifier to access the contents.
12. Select the desired WIM file.
13. Click **Next**.



14. Read the warning, and then click **Start** to restore the unit with the selected image.
15. When the operation is complete and the application prompts you, disconnect the USB key, and then click **OK**.

The unit will restart.

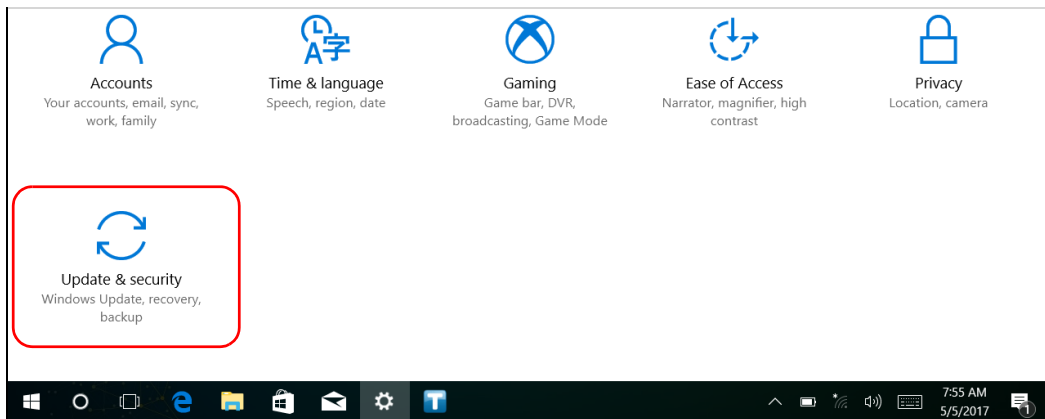
To reset your unit to its factory settings:

1. If desired, back up your data.
2. From the task bar, click the **Start** button (), and then **Settings** ().

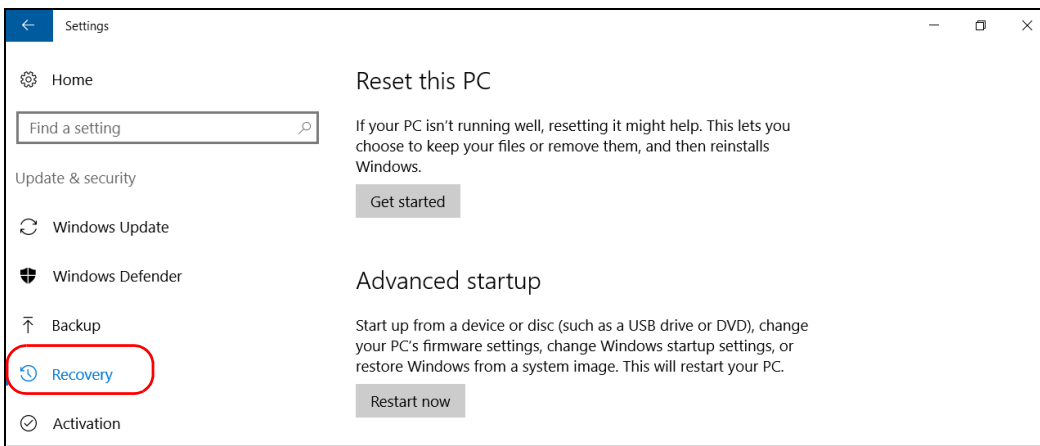
Troubleshooting

Restoring Your Unit to Normal Operation (Windows 10)

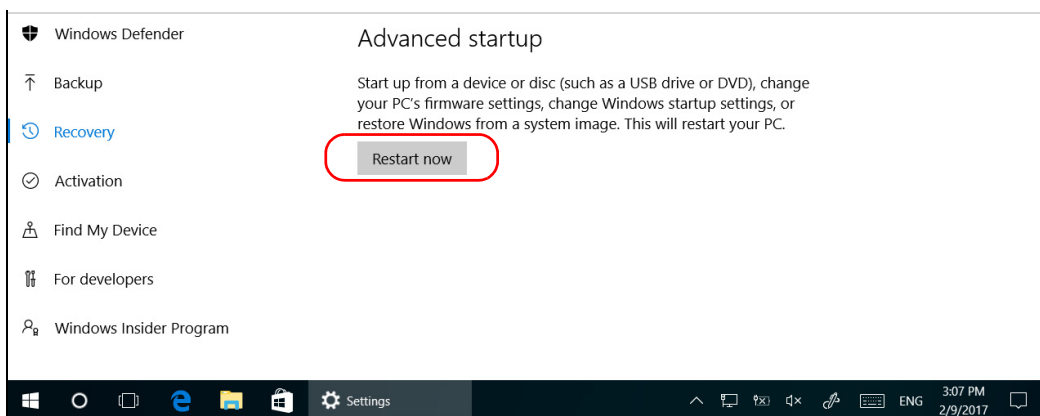
3. Click **Update & security**.



4. Select **Recovery**.



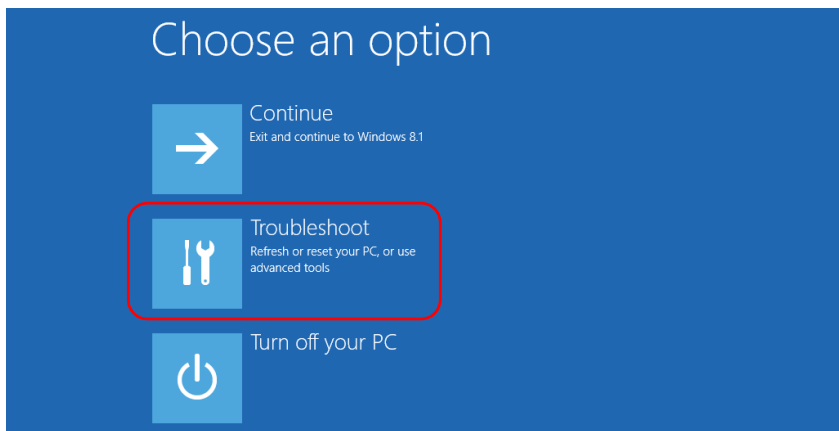
5. Under **Advanced Startup**, click **Restart now**.



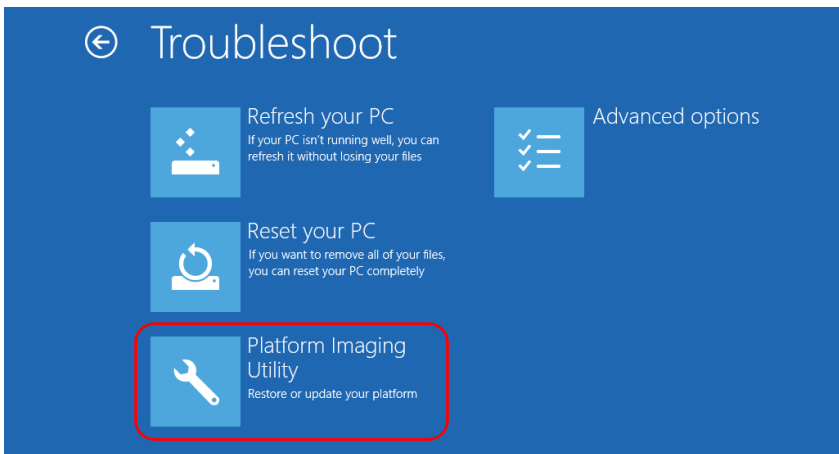
Troubleshooting

Restoring Your Unit to Normal Operation (Windows 10)

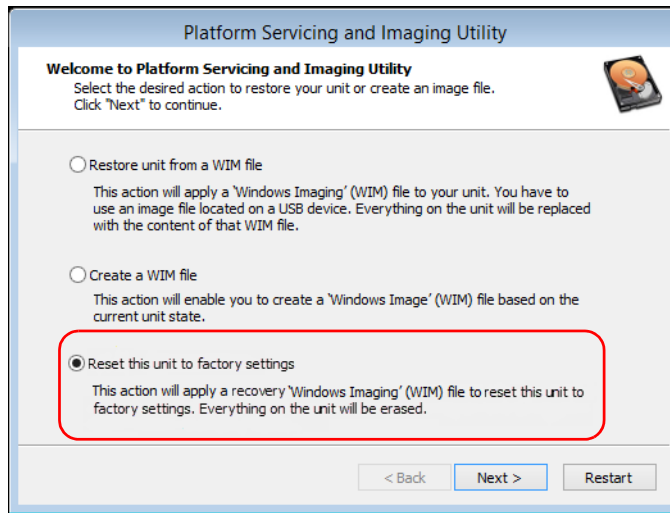
- Under **Choose an option**, click **Troubleshoot**.



- Click **Platform Imaging Utility** to display the corresponding application.



- From the Platform Servicing and Imaging Utility wizard, select **Reset this unit to factory settings**, and then click **Next**.



- Read the warning, and then click **Start** to restore the unit with the selected image.
- When the operation is complete and the application prompts you, click **OK**.
The unit will restart.
- Configure the regional parameters, and accept the license agreements as you did when you first received your unit.

Viewing Online Documentation

An online version of the Fiber Guardian user guide is available at all times from the Host Web UI.

To view the online documents

- 1.** Start the Host Web UI. For more information, see *Accessing and Exiting the Host Web UI* on page 109.
- 2.** From the **About** menu, click **Help**.
- 3.** Click the user guide that you want to view.

Contacting the Technical Support Group

To obtain after-sales service or technical support for this product, contact EXFO at one of the following numbers. The Technical Support Group is available to take your calls from Monday to Friday, 8:00 a.m. to 7:00 p.m. (Eastern Time in North America).

Technical Support Group

400 Godin Avenue
Quebec (Quebec) G1M 2K2
CANADA

1 866 683-0155 (USA and Canada)
Tel.: 1 418 683-5498
Fax: 1 418 683-9224
support@exfo.com

For detailed information about technical support, and for a list of other worldwide locations, visit the EXFO Web site at www.exfo.com.

If you have comments or suggestions about this user documentation, you can send them to customer.feedback.manual@exfo.com.

To accelerate the process, please have information such as the name and the serial number (see the product identification label), as well as a description of your problem, close at hand.



IMPORTANT

If you require quick assistance specific to your fiber monitoring solution, use support.nqmsfiber@exfo.com instead.

Viewing Product Information

If you need any assistance regarding your Fiber Guardian, you can contact EXFO.

To view EXFO contact information:

1. Connect to the Host Web UI. For more information, see *Accessing and Exiting the Host Web UI* on page 109.
2. From the **About** menu, click **Contact EXFO**.

Transportation

Maintain a temperature range within specifications when transporting the unit. Transportation damage can occur from improper handling. The following steps are recommended to minimize the possibility of damage:

- Pack the unit in its original packing material when shipping.
- Avoid high humidity or large temperature fluctuations.
- Keep the unit out of direct sunlight.
- Avoid unnecessary shocks and vibrations.

13 **Warranty**

General Information

EXFO Inc. (EXFO) warrants this equipment against defects in material and workmanship for a period of one year from the date of original shipment. EXFO also warrants that this equipment will meet applicable specifications under normal use.

During the warranty period, EXFO will, at its discretion, repair, replace, or issue credit for any defective product, as well as verify and adjust the product free of charge should the equipment need to be repaired or if the original calibration is erroneous. If the equipment is sent back for verification of calibration during the warranty period and found to meet all published specifications, EXFO will charge standard calibration fees.

THIS WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES EXPRESSED, IMPLIED, OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL EXFO BE LIABLE FOR SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES.

Liability

EXFO shall not be liable for damages resulting from the use of the product, nor shall be responsible for any failure in the performance of other items to which the product is connected or the operation of any system of which the product may be a part.

EXFO shall not be liable for damages resulting from improper usage or unauthorized modification of the product, its accompanying accessories and software.

Warranty

Exclusions

Exclusions

EXFO reserves the right to make changes in the design or construction of any of its products at any time without incurring obligation to make any changes whatsoever on units purchased. Accessories, including but not limited to fuses, pilot lamps, batteries and universal interfaces (EUI) used with EXFO products are not covered by this warranty.

This warranty excludes failure resulting from: improper use or installation, normal wear and tear, accident, abuse, neglect, fire, water, lightning or other acts of nature, causes external to the product or other factors beyond the control of EXFO.

Certification

EXFO certifies that this equipment met its published specifications at the time of shipment from the factory.

Service and Repairs

EXFO commits to providing product service and repair for five years following the date of purchase.

To send any equipment for service or repair:

- 1.** Call one of EXFO's authorized service centers (see *EXFO Service Centers Worldwide* on page 340). Support personnel will determine if the equipment requires service, repair, or calibration.
- 2.** If equipment must be returned to EXFO or an authorized service center, support personnel will issue a Return Merchandise Authorization (RMA) number and provide an address for return.
- 3.** If possible, back up your data before sending the unit for repair.
- 4.** Pack the equipment in its original shipping material. Be sure to include a statement or report fully detailing the defect and the conditions under which it was observed.
- 5.** Return the equipment, prepaid, to the address given to you by support personnel. Be sure to write the RMA number on the shipping slip. *EXFO will refuse and return any package that does not bear an RMA number.*

Note: *A test setup fee will apply to any returned unit that, after test, is found to meet the applicable specifications.*

After repair, the equipment will be returned with a repair report. If the equipment is not under warranty, you will be invoiced for the cost appearing on this report. EXFO will pay return-to-customer shipping costs for equipment under warranty. Shipping insurance is at your expense.

Routine recalibration is not included in any of the warranty plans. Since calibrations/verifications are not covered by the basic or extended warranties, you may elect to purchase FlexCare Calibration/Verification Packages for a definite period of time. Contact an authorized service center (see *EXFO Service Centers Worldwide* on page 340).

Warranty

EXFO Service Centers Worldwide

EXFO Service Centers Worldwide

If your product requires servicing, contact your nearest authorized service center.

EXFO Headquarters Service Center

400 Godin Avenue
Quebec (Quebec) G1M 2K2
CANADA

1 866 683-0155 (USA and Canada)
Tel.: 1 418 683-5498
Fax: 1 418 683-9224
support@exfo.com

EXFO Europe Service Center

Winchester House, School Lane
Chandlers Ford, Hampshire S053 4DG
ENGLAND

Tel.: +44 2380 246800
Fax: +44 2380 246801
support.europe@exfo.com

EXFO Telecom Equipment (Shenzhen) Ltd.

3rd Floor, Building C,
FuNing Hi-Tech Industrial Park, No. 71-3,
Xintian Avenue,
Fuhai, Bao'An District,
Shenzhen, China, 518103

Tel: +86 (755) 2955 3100
Fax: +86 (755) 2955 3101
support.asia@exfo.com

To view EXFO's network of partner-operated Certified Service Centers nearest you, please consult EXFO's corporate website for the complete list of service partners:

<http://www.exfo.com/support/services/instrument-services/exfo-service-centers>.

A Fault Geolocalization Using a KML File

This chapter describes finding a fault's geographical position using a KML/KMZ file. These files are custom and need a specific standard. For information on file formatting, contact EXFO (see *Contacting the Technical Support Group* on page 335).

See *Accessing and Exiting the Host Web UI* on page 109 to login to the Host Web UI. Configure the SMTP settings to send e-mails (see *Configuring the E-Mail Server Settings* on page 119) and setup an **Alerting Type** (see *Managing Alert Types* on page 140) to send an e-mail when faults occur.

To upload a KML file:

1. Enter `https:// RTU_IP /api/topology/importkml.html`. This opens the following web page:

Topology KML Import

Not secure | `https://10.28.224.23/api/topology/importkml.html`

Browse...

Import

KML Import Status:

ImportedObjectid	Name	Type	Action	Time Stamp	Status
------------------	------	------	--------	------------	--------

2. Click on the **Browse** button and select your KML/KMZ file.

Note: The `.kml/.kmz` file must have the same name as the Optical Route created on the FG-750 (in the `NqmsWebOtdr2` web page).

Fault Geolocation Using a KML File

3. Click on the **Import** button.

After a couple of seconds, the following summary of Imported Object IDs is displayed:

Topology KML Import

C:\fakepath\Hack.kmz Browse...

100%

Import

KML Import Status:

File uploaded ...

ImportedObjectId	Name	Type	Action	TimeStamp
4911	QC QCCT01-000S01-ENTOURAGE	site	CREATED	2018-05-15 19:51:17.104+0000
4928	QC QCCT01-8877-Henri-Bourassa	site	CREATED	2018-05-15 19:51:17.217+0000
4945	QC QCCT03-Bar-Orsainville	site	CREATED	2018-05-15 19:51:17.294+0000
4962	QCCS-2230-LACBEAUPORT	cableSegment	CREATED	2018-05-15 19:51:17.415+0000
4970	QCCS-2231-Henri-Bourassa-Bar-Orsainville	cableSegment	CREATED	2018-05-15 19:51:17.497+0000
4978	Hack	opticalRoute	CREATED	2018-05-15 19:51:17.681+0000

To view the geolocalization of a fault:

Under **Configuration/Remote Test Unit**, select the **Name** of the optical route with the same name as the KML file:

The screenshot displays the EXFO OTDR FG-750 web interface. The top navigation bar includes 'Applications', 'admin', and 'Information'. The main menu has 'Configuration', 'Status', 'Reporting', 'Manual Test', and 'About'. The left sidebar shows a tree view with 'Remote Test Unit' expanded, containing 'Optical Routes' (with 'ExampleRoute' selected), 'Test Setups', 'Optical Connections', and 'Controlled ROTAs'.

The main content area shows the configuration for 'ExampleRoute':

- Name: ExampleRoute
- Comments: (empty text box)
- OTDR: OTDR 1650 nm (SM)
- OTAU port: D,1
- ROTAU port: (empty text box)

Settings

- Test Ready:
- Type: Dark Live
- Average helix factor: %

Physical Network Reference

- Physical Route ID:

External NMS Reference

- Field 1:
- Field 2:

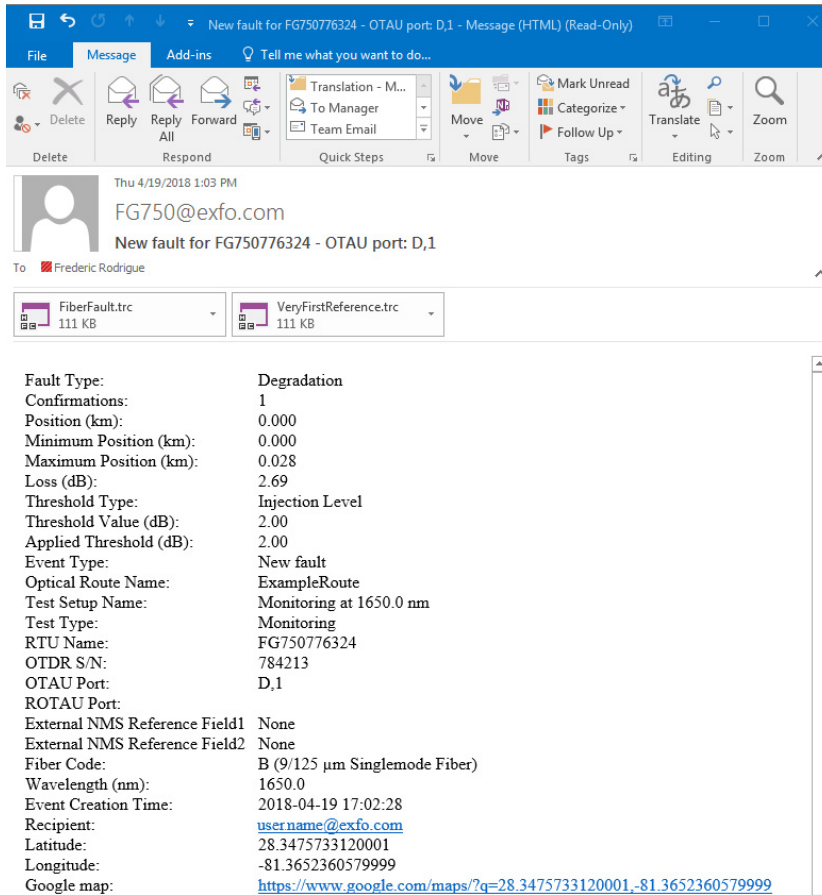
Correction Factors

Wavelength	IOR	RBS
1650.0 nm	1.4689	-82.821

At the bottom right, there are three buttons: 'Delete', 'Copy', and 'Edit'.

Fault Geolocation Using a KML File

When a fault occurs, an e-mail is sent listing 3 new values: **Latitude**, **Longitude**, and **Google map** hyperlink which represent the geolocation of the fault.



The screenshot shows an email client interface. The message is from FG750@exfo.com, titled "New fault for FG750776324 - OTAU port: D,1". The email body contains a list of fault details:

Fault Type:	Degradation
Confirmations:	1
Position (km):	0.000
Minimum Position (km):	0.000
Maximum Position (km):	0.028
Loss (dB):	2.69
Threshold Type:	Injection Level
Threshold Value (dB):	2.00
Applied Threshold (dB):	2.00
Event Type:	New fault
Optical Route Name:	ExampleRoute
Test Setup Name:	Monitoring at 1650.0 nm
Test Type:	Monitoring
RTU Name:	FG750776324
OTDR S/N:	784213
OTAU Port:	D,1
ROTAU Port:	
External NMS Reference Field1	None
External NMS Reference Field2	None
Fiber Code:	B (9/125 µm Singlemode Fiber)
Wavelength (nm):	1650.0
Event Creation Time:	2018-04-19 17:02:28
Recipient:	username@exfo.com
Latitude:	28.3475733120001
Longitude:	-81.3652360579999
Google map:	https://www.google.com/maps/?q=28.3475733120001,-81.3652360579999

All message formats including HTTP Post contain these 3 new values for a **Fiber Fault** except for SNMP (Simple Network Management Protocol) and SMS. see *Channel type page* 141 to select the desired alert message format.

Index

3G/4G access	59
A	
AC	
adapter	20
power	12, 30, 45
requirements	23
AC requirements	23
accessing unit directly	308
acquisition	
distance	151
duration.....	151
range	151
setting analysis detection thresholds...	167
setting pulse	151
activation time, changing.....	294
ad hoc test	
default values	189
performing	183
adding	
lines	240
remote OTAU.....	235
tray	37
address of time server	123
after-sales service	335
air filter, replacing	263
allowed operations on packages	291
antenna, connecting	60
applications	
add	292
delete	294
edit packages.....	294
Fiber Guardian	109
KVM remote console	308
Line Configuration	231
manage	291
view	289
applying filters.....	252
automatic	
connection to network.....	59
IP address.....	112
available models	4
B	
backup connection	59
battery, clock.....	12
blinking LED	300
browsers, supported.....	12
building applications	84
C	
cabinet installation	27
capacitors	22
cassette	
insertion and removal	32
types	9
caution	
of personal hazard	14
of product hazard	14
changing	
AC power supply.....	275
DC power supply.....	277
OTDR module.....	279
power supply	275
characterization table	218
checking storage device integrity	313, 317
cleaning	
fiber ends.....	82
front panel.....	255
other connectors.....	262
switchable connectors	256
clearing log filters.....	252
clock battery.....	12

Index

- closing application
 - Fiber Guardian 109
 - Line Configuration 231
 - common problems 297, 300
 - communication LED 303
 - companion
 - configure network 112
 - status 304
 - version 290
 - view information 111
 - computer
 - installing VPN client 70
 - modifying name 112
 - configuring
 - 3G/4G 115
 - network 112
 - SNMP 120
 - time server 123
 - connecting
 - a switch 52
 - antenna 60
 - power and network 45
 - to applications 12
 - to unit 308
 - to VPN 79
 - via WAN or Internet 69
 - connectors, cleaning 256
 - conventions, safety 14
 - covers, unit 22
 - creating reports 253
 - current, electrical 23
 - customer service 339
- D**
- data, sorting 251
 - DC power 12, 30, 45
 - default values for ad hoc test 189
 - defective fan 267
 - deleting
 - faults 215
 - filters 252
 - lines 243
 - remote OTAU 239
 - DHCP 112
 - disconnecting unit 20
 - displaying
 - log columns 250
 - log entries 251
 - distance range 151
 - DNS server 112
 - documentation, REST 84
 - dry contact relays 50
- E**
- editing
 - lines 242
 - remote OTAU 238
 - software packages 294
 - test on demand 155
 - electrostatic discharge damage. *see* ESD 25
 - emergency
 - connection 59
 - system tools 313, 317
 - equipment returns 339
 - errors 300
 - ESD, preventing 25
 - Ethernet ports, address 55
 - ETSI racks 27
 - event log
 - customize 250
 - export 253
 - filters 251
 - view 249
 - Event Source column 251
 - Event Type column 251
 - events, exporting 253
 - exiting application
 - Fiber Guardian 109, 111
 - Line Configuration 231

-
- exporting
 - event log 253
 - fault list 215
 - line configuration 246
 - external
 - power supply 20
 - switches 52, 235
 - F**
 - fan
 - filter 263
 - replacing 267
 - FC connector cleaner 262
 - fiber ends, cleaning 82
 - Fiber Guardian
 - services 84
 - starting 109
 - fiber management tray 37
 - filter, replacing 263
 - firmware version 290
 - front and back panels 5
 - front panel, cleaning 255
 - G**
 - gateway, defining 112
 - generating reports 253
 - H**
 - helix factor
 - admissible values 149
 - setting 146, 149
 - hiding
 - log columns 250
 - log entries 251
 - host
 - configure 3G/4G 115
 - configure network 112
 - modifying name 112
 - reset defaults 312
 - restarting 50
 - status 304
 - turning off/restarting 48
 - view information 111
 - I**
 - identification label 335
 - importing line configuration 247
 - indoor use 22
 - information, system 304
 - injection loss test 244
 - inlets 20
 - input
 - current 23
 - input current 23
 - inserting
 - cassette 32
 - SIM card 62
 - installation of unit in rack 27
 - installing VPN client
 - general information 69
 - on computer 70
 - on unit 74
 - iOLM commands 84
 - IOR
 - obtaining 149
 - setting 146, 149
 - J**
 - java version 12
 - L**
 - label, identification 335
 - launching application 109, 231
 - LC connector cleaner 262
 - LED
 - communication 303
 - description 300
 - measurement in progress 303
 - measurement status 303
 - power 300

Index

- resetting the status..... 306
- system 301
- Line Configuration application 231
- line configurations
 - exporting 246
 - importing 247
- lines
 - adding 240
 - deleting 243
 - editing 242
 - managing 240
- log view, customizing 250
- loss test 244

M

- main features 3
- maintenance
 - front panel 255
 - general information 255
 - switchable connectors 256
- managing
 - fibers 37
 - line configurations 246
 - lines 240
 - remote OTAUs 235
 - switches 235
- maximum
 - input current 23
- maximum input current 23
- measurement in progress LED 303
- measurement status LED 303
- mechanical connector cleaning 262
- models offered 4
- modifying package settings 294
- module
 - OTDR 279
 - power supply 12
 - switch 9
- monitoring device 50
- monitoring test setup 165
- mounting brackets 27

- MTP/MTO connector cleaner 262
- multifiber cleaner 262

N

- network cables, connecting 45
- new power supply 275
- notification agent
 - configuration 198
 - installation 85
- number of ports 9

O

- opening protective window 42
- OTDR
 - laser class 18
 - replacing 279
- overview of applications 87

P

- packages, software 291
- panels, front and back 5
- parameters
 - fiber, setting default values 149
 - helix factor 146, 149
 - IOR 146, 149
 - Rayleigh backscatter coefficient... 146, 149
 - resetting 312
- passwords of all applications 87
- patchcord management tray 37
- pinout of the relays 50
- plugging unit 45
- ports, switch 9
- power
 - cable 20
 - connecting 45
 - LED 300
 - plug 20
 - relay 50
 - sources 12, 23
 - supply 20

-
- power supply module
 - AC..... 275
 - DC 277
 - defective..... 275
 - general information..... 275
 - preventing ESD..... 25
 - proactive maintenance test setup 165
 - problems, solving..... 297
 - product
 - identification label..... 335
 - specifications..... 13
 - programming guide..... 84
 - protective window 37
 - folding down..... 42
 - removing 43
 - pulse width 151
- R**
- rack dimensions 27
 - RBS (Rayleigh backscatter)
 - obtaining..... 149
 - setting 146, 149
 - rear port address..... 55
 - rebooting host 48
 - recovery mode..... 313, 317
 - red LED..... 300
 - regulatory information..... xiv, xv
 - relays
 - dry contact 50
 - viewing status..... 304
 - remote console 308
 - remote OTAUs..... 235
 - adding 235
 - deleting 239
 - editing 238
 - managing 235
 - removing
 - column filters..... 252
 - protective window..... 43
 - switch cassette 32
 - repairing unit 22
- replacing
 - AC power supply..... 275
 - air filter 263
 - DC power supply..... 275, 277
 - fan 267
 - OTDR..... 279
 - report, generating 253
 - requirements for installation 26
 - resetting
 - configuration 312
 - status of LEDs 306
 - REST commands 84
 - restarting host 48, 50
 - restoring unit..... 313, 317
 - result browser 223
 - retrieving rear port address 55
 - return merchandise authorization (RMA) .. 339
- S**
- safety
 - caution..... 14
 - conventions 14
 - general info 15
 - grounding unit..... 30
 - laser 18
 - power cable 20
 - warning 14
 - SC connector cleaner..... 262
 - search results test on demand..... 226
 - selecting log columns..... 250
 - service and repairs 339
 - service centers 340
 - shipping to EXFO..... 339
 - showing log columns 250
 - SIM card 62
 - single-fiber cleaner 262
 - software packages
 - general information 291
 - operations..... 291
 - solving problems 297, 300
 - sorting data..... 251

Index

- specifications, product 13
- starting application
 - Fiber Guardian 109
 - Line Configuration 231
- states, software packages 291
- static IP address 112
- status, system 304
- storage device integrity 313, 317
- storage requirements 255
- supported browsers 12
- switch
 - cassettes 32
 - configurations 9
- switchable connectors, cleaning 256
- switching to wireless network 59
- symbols, safety 14
- synchronization frequency 123
- system
 - emergency tools 313, 317
 - LED 301
 - relay 50
 - status 304
 - version 290

T

- technical specifications 13
- technical support 335
- temperature for storage 255
- test on demand
 - editing 155
 - search results 226
 - test setup 165
- test setup
 - monitoring 165
 - proactive maintenance 165
 - test on demand 165
- testing relays 304
- tests
 - ad hoc 183
 - injection loss 244
 - starting 215

- threshold
 - analysis detection 167
 - end-of-fiber detection 152, 167
 - reflectance detection 152, 167
 - splice loss detection 152, 167
- time server 123
- tools system, emergency 313, 317
- transportation requirements 255, 336
- tray installation 37
- turning off unit 48, 50
- turning on unit 48
- types of cassettes 9

U

- unit
 - covers 22
 - disconnecting 20
 - features 3
 - grounding 30
 - installation 26
 - repairing 22
 - turning on 48
- user names 87

V

- verify disk integrity 313, 317
- version, firmware 290
- viewing
 - relay status 304
 - results 223
- VPN
 - client installation 69
 - connection 79

W

- WAN connection 69
- warranty
 - certification 338
 - exclusions 338

general 337
liability 337
Web
 browsers 12
 connection 69
 user interface 109
wim file 313, 317
wireless network 59

X

xml file 253

Y

yellow LED 300

CHINESE REGULATION ON RESTRICTION OF HAZARDOUS SUBSTANCES (RoHS)

中国关于有害物质限制的规定

NAMES AND CONTENTS OF THE TOXIC OR HAZARDOUS SUBSTANCES OR ELEMENTS
CONTAINED IN THIS EXFO PRODUCT

包含在本 EXFO 产品中的有毒有害物质或元素的名称及含量

Part Name 部件名称	Lead 铅 (Pb)	Mercury 汞 (Hg)	Cadmium 镉 (Cd)	Hexavalent Chromium 六价铬 (Cr(VI))	Polybrominated biphenyls 多溴联苯 (PBB)	Polybrominated diphenyl ethers 多溴二苯醚 (PBDE)
Enclosure 外壳	O	O	O	O	O	O
Electronic and electrical sub-assembly 电子和电气组件	X	O	X	O	X	X
Optical sub-assembly ^a 光学组件 ^a	X	O	O	O	O	O
Mechanical sub-assembly ^a 机械组件 ^a	O	O	O	O	O	O

Note:

注:

This table is prepared in accordance with the provisions of SJ/T 11364.

本表依据 SJ/T 11364 的规定编制。

O: Indicates that said hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement of GB/T 26572.

O: 表示该有害物质在该部件所有均质材料中的含量均在 GB/T 26572 标准规定的限量要求以下。

X: indicates that said hazardous substance contained in at least one of the homogeneous materials used for this part is above the limit requirement of GB/T 26572. Due to the limitations in current technologies, parts with the "X" mark cannot eliminate hazardous substances.



X: 表示该有害物质至少在该部件的某一均质材料中的含量超出 GB/T 26572 标准规定的限量要求。

标记 "X" 的部件, 皆因全球技术发展水平限制而无法实现有害物质的替代。

a. If applicable.

如果适用。

MARKING REQUIREMENTS
标注要求

Product 产品	Environmental protection use period (years) 环境保护使用期限 (年)	Logo 标志
This EXFO product 本 EXFO 产品	10	
Battery ^a 电池	5	

a. If applicable.
如果适用。

P/N:1075297

www.EXFO.com · info@EXFO.com

CORPORATE HEADQUARTERS 400 Godin Avenue

Quebec (Quebec) G1M 2K2 CANADA
Tel.: 1 418 683-0211 · Fax: 1 418 683-2170

TOLL-FREE (USA and Canada)

1 800 663-3936

© 2019 EXFO Inc. All rights reserved.
Printed in Canada (2019-03)

The logo for EXFO, featuring the letters 'EXFO' in a bold, blue, sans-serif font. The letters are composed of horizontal lines, giving it a modern, digital appearance.