



proNX Optical Director

User Guide



Modified: 2019-04-15

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

proNX Optical Director User Guide

Copyright © 2019 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <https://support.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

Chapter 1	Introduction	13
	proNX Optical Director Overview	13
	Logging in to the proNX Optical Director	16
	proNX Optical Director Page Layout	17
	Getting Started	19
	Changing Your (Local) User Settings	20
	Changing Your (Local) User Password	21
	Logging Out	22
	Working with Tables	22
	Supported Devices	23
Chapter 2	Dashboard	25
	About the Dashboard	25
	Tasks You Can Perform	25
	Field Descriptions	25
	Editing the Dashboard	29
Chapter 3	Monitor	31
	Network Map	31
	About the Network Map Page	31
	Tasks You Can Perform	32
	Navigating the Network Map Page	32
	Viewing Site Details	33
	Viewing Link Details	35
	Logical View	36
	About the Logical View Page	36
	Tasks You Can Perform	36
	Navigating the Logical View Page	37
	Viewing a Device or Device Group	38
	Viewing Link Details	39
	Current Alarms	40
	About the Current Alarms Page	40
	Tasks You Can Perform	40
	Field Descriptions	40
	Viewing Current Alarms	41
	Acknowledging or Unacknowledging an Alarm	43
	Historical Alarms	43
	About the Historical Alarms Page	44
	Tasks You Can Perform	44
	Field Descriptions	44
	Viewing Historical Alarms	44

	Events	46
	About the Events Page	46
	Tasks You Can Perform	46
	Field Descriptions	46
	Viewing Events	47
Chapter 4	Devices	49
	Devices Configuration	49
	About the Devices Configuration Page	49
	Tasks You Can Perform	49
	Field Descriptions	50
	Navigating the Device Tree	51
	Component Naming	52
	Creating a New Site	55
	Deleting a Site	55
	Site Management	56
	About the Site Config Page	56
	Tasks You Can Perform	56
	Field Descriptions	56
	Editing a Site's Parameters	57
	About the Site Location Page	57
	Tasks You Can Perform	58
	Field Descriptions	58
	Editing a Location Tree	58
	About the Site Devices Page	59
	Tasks You Can Perform	59
	Field Descriptions	59
	Viewing the List of Devices at a Site	60
	About the Site Operations Upgrade Page	60
	Tasks You Can Perform	60
	Field Descriptions	60
	Upgrading the Software on a Device	60
	About the Site Operations Backup Page	60
	Tasks You Can Perform	61
	Field Descriptions	61
	Backing Up the Device Configuration Database	61
	About the Site Operations Restart Page	61
	Tasks You Can Perform	61
	Field Descriptions	61
	Restarting All Devices at a Site	61
	About the Site Operations NTP Servers Page	62
	Tasks You Can Perform	62
	Field Descriptions	62
	About the Site Operations Date Time Page	62
	Tasks You Can Perform	62
	Field Descriptions	62

Device Management	63
About the Device Config Page	63
Tasks You Can Perform	64
Field Descriptions	64
Editing a Device's Parameters	64
About the Device NTP Servers Page	65
Tasks You Can Perform	65
Field Descriptions	65
Viewing the NTP Server List	66
Adding an NTP Server to the NTP Server List	66
Deleting an NTP Server from the NTP Server List	67
Enabling or Disabling NTP Servers	68
About the Device Datetime Page	68
Tasks You Can Perform	68
Field Descriptions	68
Setting the Date and Time	69
About the Device Security Page	69
Tasks You Can Perform	70
Field Descriptions	70
Adding or Deleting a RADIUS Server or Changing the RADIUS Security Options	70
About the Device Chassis View Page	71
Tasks You Can Perform	71
Field Descriptions	71
Navigating the Chassis View Page	72
About the Device Operations View Logs Page	74
Tasks You Can Perform	74
Field Descriptions	74
Viewing Logs for a Device	75
Log Collection	76
Automated Log Collection	76
Collecting Logs from a Device Manually	77
Metric Collection	77
Automated Metric Collection	78
Collecting Metrics from a Device Manually	79
About the Device Operations Upgrade Page	79
Tasks You Can Perform	79
Field Descriptions	79
Upgrading the Software on a Device	81
About the Device Operations Backup Page	82
Tasks You Can Perform	82
Field Descriptions	82
Device Configuration Database Backups	83
Automated Device Configuration Database Backups	83
Backing Up the Device Configuration Database Manually	84
About the Device Operations Restore Page	85
Tasks You Can Perform	85
Field Descriptions	85
Restoring the Device Configuration Database	86

About the Device Operations Restart Page	87
Tasks You Can Perform	87
Field Descriptions	87
Restarting a Device	88
Restoring a Device to Factory Defaults	88
Shelf Management	89
About the Devices Shelf Page	89
Tasks You Can Perform	89
Field Descriptions	89
Enabling or Disabling a Shelf	90
Adding a Multiplexer/Demultiplexer to a Shelf	91
Deleting a Multiplexer/Demultiplexer from a Shelf	92
Circuit Pack Management	92
About the Devices Circuit Pack Page	92
Tasks You Can Perform	92
Field Descriptions	92
Port Management	93
About the Devices Port Config Page	93
Tasks You Can Perform	93
Field Descriptions	93
Configuring a Port	101
About the Devices Port Threshold Page	101
Tasks You Can Perform	101
Field Descriptions	101
Configuring Threshold Crossing Alerts on Supported Tail Facility Ports	104
About the Devices Port Historical PMs (Metrics) Page	104
Tasks You Can Perform	104
Field Descriptions	104
Viewing Historical Performance Monitoring Metrics	105
About the Devices Port Telemetry Page	107
Tasks You Can Perform	107
Field Descriptions	107
Viewing Telemetry Metrics	108
Devices Discovery	109
Discovering a Device	109
Rediscovering a Device	112
Undiscovering a Device	112
Resynchronizing the Network	113
Moving a Discovered Device to a Different Site	114
Devices Inventory	114
About the Devices Inventory Page	114
Tasks You Can Perform	115
Field Descriptions	115
Viewing the Inventory	115

Chapter 5	Network	117
	Device Links	117
	Device Links Overview	117
	Provisioned Device Links	120
	Auto-Learned Device Links	120
	Device Link Validation	121
	About the Device Links Current Page	121
	Tasks You Can Perform	122
	Field Descriptions	122
	Viewing or Deleting a Link	124
	Editing the Fiber Type	124
	About the Device Links Create Link Page	125
	Tasks You Can Perform	125
	Field Descriptions	125
	Creating a Link	127
	Services	128
	Services Overview	128
	Optical Service and Tail Facility Endpoints	129
	Single Path Service	131
	Protected Service	131
	About the Services Provisioned Page	132
	Tasks You Can Perform	132
	Field Descriptions	132
	Orphan Service	134
	Viewing a Service	135
	Editing or Deleting a Service	137
	About the Services Create Page	138
	Tasks You Can Perform	138
	Field Descriptions	138
	Creating a Single Path Service	140
	Creating a Protected Service	142
Chapter 6	Administration	145
	Tasks	145
	About the Tasks Page	145
	Tasks You Can Perform	145
	Field Descriptions	145
	Viewing the Tasks List	147
	Users	147
	About the User Management Page	147
	Tasks You Can Perform	148
	Field Descriptions	148
	Viewing the List of Local Users	149
	Adding a Local User	149
	Editing a Local User	150
	Deleting a Local User	150
	Resetting a Local User's Password	151

	Activating or Deactivating a Local User	152
	About the User Tracker Page	153
	Tasks You Can Perform	153
	Field Descriptions	153
	Tracking Users in Real-Time	153
	File Servers	154
	About the File Servers Page	154
	Tasks You Can Perform	154
	Field Descriptions	154
	Viewing the File Server List	155
	Adding a File Server to the File Server List	156
	Editing a File Server	157
	Deleting a File Server from the File Server List	157
	Security	157
	About the Security Page	158
	Tasks You Can Perform	158
	Field Descriptions	158
	Authentication Process	159
	Local User Authentication	159
	Vendor-Specific Attribute (VSA) Requirements for Remote Authentication	160
	Viewing the Authentication Server List	161
	Adding an Authentication Server to the Authentication Server List	162
	Editing an Authentication Server	163
	Deleting an Authentication Server from the Authentication Server List	163
	Changing the Authentication Server Order in the Authentication Server List	164
	Reports	164
	About the Reports Page	164
	Tasks You Can Perform	164
	Field Descriptions	164
	Generating Reports	165
Chapter 7	Appendix	167
	Grafana	167
	Overview	167
	Viewing a PM Graph	169
	Creating a Multi-PM Dashboard (2 Metrics, 1 Entity, 1 Device)	172
	Creating a Multi-PM Dashboard (2 Metrics, 2 Entities, 2 Devices)	178

List of Figures

Chapter 1	Introduction	13
	Figure 1: Typical proNX Optical Director Deployment	15
	Figure 2: proNX Optical Director Page Layout	18
Chapter 4	Devices	49
	Figure 3: Port Telemetry Graph Example	108
Chapter 5	Network	117
	Figure 4: 2-Degree ROADM Node Example	119
	Figure 5: Optical Service and Tail Facility Endpoints	130
	Figure 6: Protected Service	131
	Figure 7: Service View Example	135
	Figure 8: Hovering on an Endpoint	136
	Figure 9: Service Telemetry Graph Example	137

List of Tables

Chapter 1	Introduction	13
	Table 1: Supported Devices	23
	Table 2: Supported Tail Facility Endpoints	24
Chapter 2	Dashboard	25
	Table 3: Widgets in the Dashboard	26
	Table 4: System Details	28
Chapter 3	Monitor	31
	Table 5: Link Colors and States	35
	Table 6: Multilink Colors	35
	Table 7: Link Colors and States	39
	Table 8: Link Weights	39
	Table 9: Fields for the Current Alarms Page	40
	Table 10: Fields for the Historical Alarms Page	44
	Table 11: Fields for the Events Page	46
Chapter 4	Devices	49
	Table 12: Fields in the Devices Configuration (Sites) Page	50
	Table 13: Fields in the Devices Configuration (Device Types) Page	50
	Table 14: TCX1000-RDM20 Component Naming	52
	Table 15: TCX1000-ILA Component Naming	53
	Table 16: FMD96 Component Naming	54
	Table 17: 2D8CMD Component Naming	54
	Table 18: Fields on the Site Config Page	56
	Table 19: Location Tree Hierarchy on the Site Location Page	58
	Table 20: Fields in the Site Devices Page	59
	Table 21: Fields on the Device Config Page	64
	Table 22: Fields in the Device NTP Servers Page	65
	Table 23: Fields in the Device Datetime Page	69
	Table 24: Fields in the Device Security Page	70
	Table 25: Fields in the Device Operations View Logs Page	74
	Table 26: JOC_LOG_COLLECTION_CRON Field Description	76
	Table 27: JOC_METRIC_COLLECTION_CRON Field Description	78
	Table 28: Fields in the Device or Site Operations Upgrade Page	80
	Table 29: Fields in the Device or Site Operations Backup Page	82
	Table 30: JOC_DEVICE_BACKUP_CRON Field Description	83
	Table 31: Fields in the Device Operations Restore Page	85
	Table 32: Fields in the Device or Site Operations Restart Page	87
	Table 33: Fields in the Devices Shelf Page	89
	Table 34: Fields in the Devices Circuit Pack Page	92

	Table 35: Fields in the Devices Port Config Page for Optical Ports	94
	Table 36: Fields in the Devices Port Optical Config (OCH) Page for Supported Tail Facility Ports	94
	Table 37: Fields in the Devices Port OTU Config Page for Supported Tail Facility Ports	96
	Table 38: Fields in the Devices Port ODU Config Page for Supported Tail Facility Ports	99
	Table 39: Fields in the Devices Port Page (for all other ports)	100
	Table 40: Fields in the Devices Port Optical Threshold (OCH) Page for Supported Tail Facility Ports	102
	Table 41: Fields in the Devices Port OTU Threshold Page for Supported Tail Facility Ports	102
	Table 42: Fields in the Devices Port ODU Threshold Page for Supported Tail Facility Ports	103
	Table 43: Fields in the Devices Port Historical PMs (Metrics) Page	105
	Table 44: Fields in the Devices Port Telemetry Page	107
	Table 45: Address Pattern	110
	Table 46: Fields in the Devices Inventory Page	115
Chapter 5	Network	117
	Table 47: Optical Network Glossary	118
	Table 48: Fields in the Device Links Current Page	122
	Table 49: Port State and Status Values	123
	Table 50: Valid Combinations for Auto-Learned and Provisioned Device Links	124
	Table 51: Fields in the Device Links Create Link Page	125
	Table 52: Supported Optical Links	127
	Table 53: Optical Service and Tail Facility Endpoints	130
	Table 54: Fields in the Services Provisioned Page	132
	Table 55: Fields in the Services Create Page	138
	Table 56: Port Selection Based on Type of Endpoint (Single Path)	141
	Table 57: Port Selection Based on Type of Endpoint (Protected)	143
Chapter 6	Administration	145
	Table 58: Fields in the Tasks Page	146
	Table 59: Fields in the User Management Page	148
	Table 60: Fields in the Create a New User Page and the Edit an Existing User Page	149
	Table 61: Fields in the User Tracker Page	153
	Table 62: Fields in the File Servers Page	155
	Table 63: Fields in the Security Page	158
	Table 64: Vendor-Specific Attribute (VSA) Requirements for RADIUS Authentication	160
	Table 65: Fields in the Reports Page	165
Chapter 7	Appendix	167
	Table 66: Historical PM Measurement Table (Simplified View)	168

CHAPTER 1

Introduction

- [proNX Optical Director Overview on page 13](#)
- [Logging in to the proNX Optical Director on page 16](#)
- [proNX Optical Director Page Layout on page 17](#)
- [Getting Started on page 19](#)
- [Changing Your \(Local\) User Settings on page 20](#)
- [Changing Your \(Local\) User Password on page 21](#)
- [Logging Out on page 22](#)
- [Working with Tables on page 22](#)
- [Supported Devices on page 23](#)

proNX Optical Director Overview



NOTE: This section is intended to provide a brief and general overview of the proNX Optical Director and might contain a description of features not found in the release that you are running. See the *TCX Series Optical Transport System Release Notes* for information on features for the release you are running.

The proNX Optical Director is a software controller and management system for open optical line systems (OLS), initially providing support for TCX1000 Series devices.

The proNX Optical Director provides the following functionality:

- Dynamic real-time control of optical links in OLS networks. This includes automatic span loss management, automatic nodal loss management, and automatic channel power control.

In traditional optical networks, this control function resides on the ROADMs themselves where the ROADMs exchange proprietary control messages with each other on an optical supervisory channel (OSC). This makes interworking across vendor equipment difficult and often leads to the deployment of single-sourced networks. Moving this function to a centralized software controller makes heterogeneous networks with equipment from multiple vendors possible.

- Network management of OLS networks including network topology, network visualization, and network monitoring and troubleshooting.

The proNX Optical Director displays the topology of the network and provides various visual indicators so that you can see the health of the network at a glance and deal with problem areas in a proactive manner.

- Device management of OLS elements including device configuration, device visualization, and device monitoring and troubleshooting.

The proNX Optical Director discovers OLS elements and reads and displays their configuration. You can change the configuration, view the equipment inventory, pull up a visual representation of the device, or view performance monitoring counters and alarm details.



NOTE: TCX Series devices do not support a built-in user interface such as a command line interface. You must use the proNX Optical Director to manage TCX Series devices.

- Service management of optical services across an OLS network including service provisioning, service activation, and service monitoring and troubleshooting.

The proNX Optical Director supports A-to-Z provisioning and activation of optical services. You select the two service endpoints and the proNX Optical Director provides you a list of paths that you can choose for that service. When you activate the service, the proNX Optical Director automatically configures the service across all the devices in the path.

- Endpoint management of supported transceivers on Juniper Networks equipment.

The OLS network provides optical service connectivity between endpoint transponders (typically). These transponders can be standalone or integrated within routers and switches. Although these endpoints are not technically part of the OLS network, you can use the proNX Optical Director to configure these endpoints on Juniper Networks equipment that supports coherent DWDM interfaces.

- Support for IPv4 and IPv6 networks. The proNX Optical Director can control and manage IPv4 and IPv6 devices.

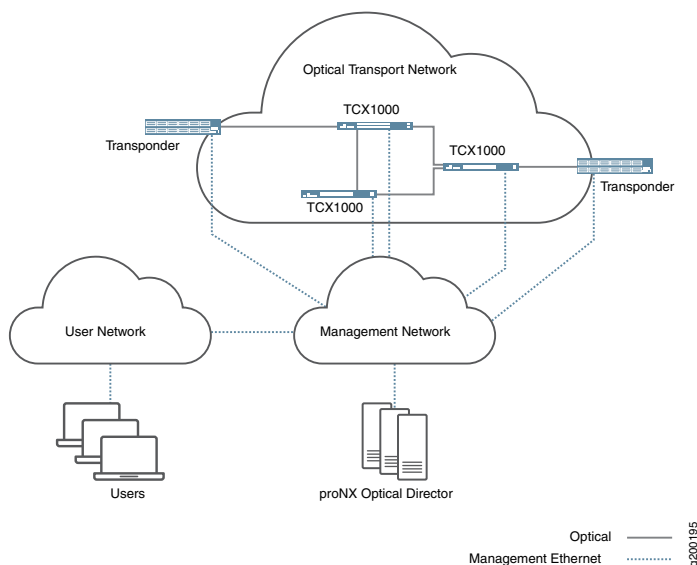
- Northbound RESTCONF interface for connecting to higher level management systems. See *Northbound Interface*.
- Web-based user interface. You can access the proNX Optical Director user interface from supported web browsers.

Figure 1 on page 15 shows a high level view of a typical deployment where the proNX Optical Director cluster controls and manages a TCX1000 Series optical transport network.

The proNX Optical Director runs on a cluster of three Linux servers. Within the cluster, one server acts as the master node. The master node is a regular node that is additionally responsible for orchestration and scheduling functions.

The proNX Optical Director connects to managed devices over a management network. Users connect to the proNX Optical Director using supported web browsers on their own computers.

Figure 1: Typical proNX Optical Director Deployment



Having network-wide visibility allows the proNX Optical Director to use advanced control algorithms that optimize optical transmission not only on a link but along the whole optical service path. The TCX1000 Series devices constantly send streams of real-time optical link measurements to the proNX Optical Director, which then uses the data to build an always current view of the optical links in the network. This allows the proNX Optical Director to make real-time control decisions on all aspects of optical link management, including the following:

- channel power control and equalization
- span loss compensation

- gain ripple and tilt compensation
- graceful ramp up and ramp down of channel powers as optical services (wavelengths) are added and removed

These control decisions are translated into commands that are communicated to the managed devices for execution. This ongoing control loop allows the proNX Optical Director to deliver optimal optical transmission performance for the managed devices by dynamically and automatically controlling all aspects of optical link output.

Logging in to the proNX Optical Director

Prerequisites

- The proNX Optical Director software is installed and running on the server cluster.
- The computer that you are logging in from has access to the server cluster and to the Internet. Internet access is required for displaying maps in the Network Map page.

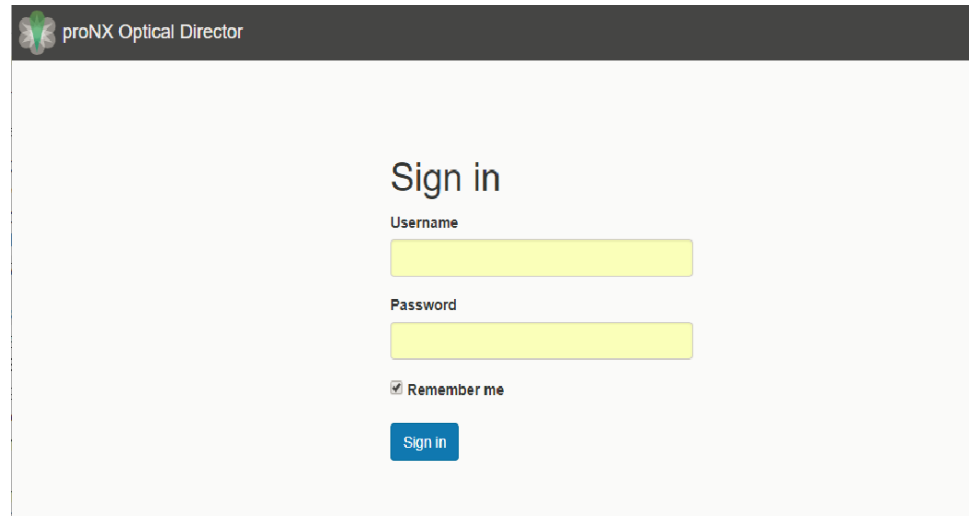
Use this procedure to log in to the proNX Optical Director.

1. Point your browser to the following URL:
 - Releases 2.2 and lower - <http://<server-vip-or-hostname>> where <server-vip-or-hostname> is the virtual IP address or resolvable hostname of the cluster
 - Releases 18.4 and higher - <https://<server-hostname>> where <server-hostname> is the resolvable and verifiable TLS hostname that you specified when you installed the cluster

You configure the virtual IP address and associated hostname for the cluster when you install the proNX Optical Director software.

The virtual IP address (and hostname) allows you and the devices under management to communicate with the proNX Optical Director using an IP address that remains fixed even if the master node changes within the cluster.

The proNX Optical Director login page appears:



2. Type your username and password and click **Sign in**.

When you log in, you are automatically placed in the dashboard.



NOTE: The default username is **admin** and the default password is **admin**. If this is the first time you are logging in, be sure to change the password from the default. For information on changing the password, see [“Changing Your \(Local\) User Password” on page 21](#).

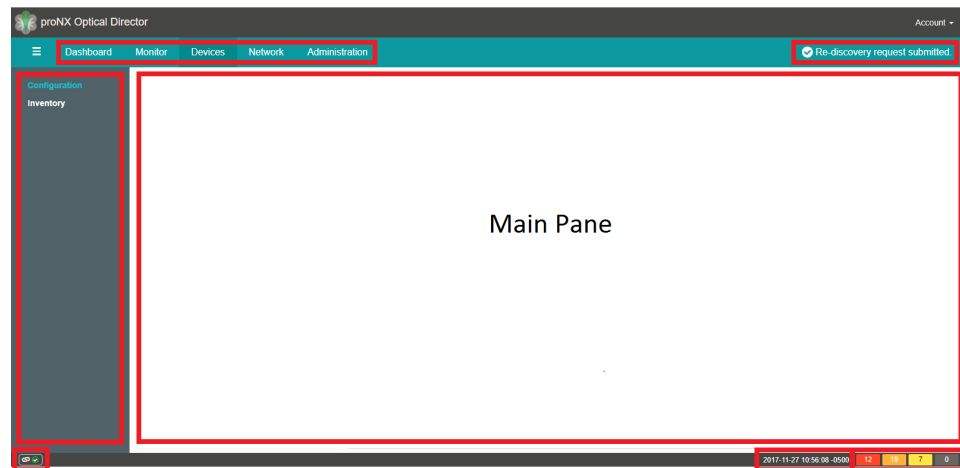
Release History Table

Release	Description
18.4	<a href="https://<server-hostname>">https://<server-hostname> where <server-hostname> is the resolvable and verifiable TLS hostname

proNX Optical Director Page Layout


Figure 2 on page 18 shows the general page layout of the proNX Optical Director.

Figure 2: proNX Optical Director Page Layout






At the top of the page is a row of tabs where you select one of the following areas:

- **Dashboard** - Displays a summary view of your network in graphical form. You can see an alarms count, the number of devices, software versions, available port capacity, and other summary information about your network.
- **Monitor** - Displays the topology of your network with visual indicators for problems and alarms. You can view your sites and the connectivity between sites as well as current and historical alarms tables and events tables.
- **Devices** - Provides site and device management. You can create sites, discover devices, view network device inventory, and configure devices including upgrading software, backing up and restoring device databases, and collecting and viewing performance monitoring metrics and logs.
- **Network** - Provides device links and service management. You can view and configure links and services.
- **Administration** - Provides various administrative functions such as user management, file and authentication server configuration, and viewing server tasks.


At the left of the page is the left-nav bar, which is placed in context based on the tab that you choose. You use the left-nav bar to further refine your selection. Not all tabs provide a left-nav bar. Click the  button to show or hide the left-nav bar.

The main pane is where you perform most of your tasks. It is placed in context based on your left-nav bar selection.

The top right corner of the page is the notification area. Notifications with an  are indications of abnormal behavior and require you to click the  to clear it. In general, you are not required to take any other action on notifications of abnormal behavior unless these indications persist, because the proNX Optical Director automatically tries to resolve the underlying issues that cause these notifications. Notifications with a  are informational and automatically clear after a few seconds.

The bottom right corner of the page displays the number of current alarms by severity. These counts are updated automatically as alarms are raised, cleared, and acknowledged in the network.

Immediately to the left of the alarms counts is the date, time, and time zone of the machine that your browser is running on. The time zone is displayed as a UTC offset.

The bottom left corner of the page displays the microservice connection status icon. Click it to show the status of the connectivity from the browser to the main microservices that make up the proNX Optical Director. A  indicates normal operation.

Getting Started

Setting up the proNX Optical Director to control and manage devices in your network consists of a set of basic steps.

Before using the proNX Optical Director, ensure that the devices in your network have been installed and that they can be reached from the proNX Optical Director. At a minimum, assign each device an IP address and connect it to the management network. As part of installation, you should also connect up the physical fibers that make up your optical network so that you do not have to return to connect them at a later date.

When you log in to the proNX Optical Director for the first time, you will find no devices under control or management. The first step you need to do is to discover the devices that make up your network. You can discover one device at a time or, more typically, you can discover multiple devices based on your discovery selection criteria. As part of device discovery, you will assign the device to a site. This allows the proNX Optical Director to accurately place the discovered device on the map. The proNX Optical Director supports a flexible set of discovery criteria to allow you to discover your devices and assign them to sites quickly and efficiently.

Devices are shipped from the factory with pre-loaded software. If the software version in the devices is not the software version that you want to run, then upgrade the software on the devices after you discover them.

Some devices such as optical multiplexer/demultiplexers are passive, which means the devices are not powered and do not run any software. Multiplexer/demultiplexers are modeled as modules that you explicitly configure and add to ROADM devices. Because multiplexer/demultiplexers are passive, they are not directly discoverable. The proNX Optical Director only becomes aware of their presence when you configure and add them to a ROADM device (or if you discover a ROADM device to which you had previously configured and added a multiplexer/demultiplexer).

Once you have discovered (and/or added) all your devices and assigned them to sites and upgraded the device software if needed, you can then configure the device links in your optical network. Device links represent the physical fibers connecting the devices together. In releases lower than release 2.2, you are required to configure all the device links manually. In releases 2.2 and higher, the proNX Optical Director supports automatic learning of all line spans in the network, so you are only required to configure the device links that are not line spans. It is important that you perform this step correctly because the proNX Optical Director uses the device links to build the ROADM topology of the

network. If the constructed topology does not match the actual topology, unexpected behavior can occur.

After the device links are configured and/or learned, the proNX Optical Director constructs an accurate view of the topology and can start supporting optical service creation. If the service you want to create includes the tail facility, then configure the tail facility endpoint before you create the service. The tail facility refers to the connectivity between the endpoint transponder and the optical network. The proNX Optical Director allows you to configure the tail facility endpoint if the tail facility endpoint resides on a supported port on Juniper Networks equipment. See [Table 2 on page 24](#) for information on supported tail facilities.

Once the tail facilities are configured, you can create the optical services.

The following steps summarize this workflow:

1. Install the hardware and connect it to the management network. See the *TCX1000 Programmable ROADM Hardware Guide* and the *TCX1000 Inline Amplifier Hardware Guide*.
2. Discover the devices (including the devices at the tail facility endpoints) and add them to sites. See [“Discovering a Device” on page 109](#).
3. Upgrade the software on the devices as necessary. See [“Upgrading the Software on a Device” on page 81](#) for information on upgrading the software on TCX Series devices. To upgrade the software on other devices, refer to the documentation for those other devices.
4. Add multiplexer/demultiplexers to ROADM devices as needed. See [“Adding a Multiplexer/Demultiplexer to a Shelf” on page 91](#).
5. Configure the device links. See [“Creating a Link” on page 127](#).
6. Configure the ports at the tail facility endpoints if you are creating services to supported tail facility endpoints. See [“Configuring a Port” on page 101](#).
7. Create the optical services. See [“Creating a Single Path Service” on page 140](#) and [“Creating a Protected Service” on page 142](#).

Changing Your (Local) User Settings

Use this procedure to change your user settings if you logged in using local user authentication. This procedure does not apply if you logged in using a remote authentication server. If you are unsure whether you logged in using local or remote user authentication, ask your network administrator.

1. Click **Account>Settings** in the top right corner of the page.

The User Settings page appears.

2. Update your **First Name** and **Last Name** as needed.

3. Update your **E-mail** address as needed. You must have an email address and the email address must be unique for all users.
4. Specify your **Language** from the drop-down list.
5. Specify the **Device Name Format** preference from the drop-down list:
 - System Name - Devices are shown by their system names.
 - IP Address - Devices are shown by their IP addresses.
 - Both - Devices are shown by both their system names and their IP addresses.
6. Click **Save**.

The UI allows you to save your changes only if you logged in using local user authentication.

Changing Your (Local) User Password

Use this procedure to change your user password if you logged in using local user authentication. This procedure does not apply if you logged in using a remote authentication server. If you are unsure whether you logged in using local or remote user authentication, ask your network administrator.

1. Click **Account > Password** in the top right corner of the page.

The Password page appears.

2. Change your password.

- Enter the **New password**. The password is assessed with a password strength indication.



NOTE: The password must be at least four characters long, but its assessed strength is not enforced.

- Retype the new password in the **New password confirmation** box.
3. Click **Save**. If the password and its confirmation do not match, re-enter the passwords.

Logging Out

Use this procedure to log out of the proNX Optical Director.

1. Click **Account>Sign Out** in the top right corner of the page.

You are logged out of the proNX Optical Director. If you have multiple pages open to the proNX Optical Director in your browser, you are logged out of all of them.

Working with Tables

The proNX Optical Director provides all tables with a common set of functions regardless of the data set being presented.

Here is an example of an Alarms table:

Show 10 entries	Display: All	View	Acknowledge	Copy	Print	Save	Search:
Device	Description	Source	Time Raised	Severity			
10.92.252.29	OTN Loss of signal	et-12/0/1	2017-08-18 10:10:39 -0400	Critical			
10.92.252.29	Link Down	et-8/0/13.0	2017-08-18 10:07:38 -0400	Critical			
10.92.252.29	Link Down	et-8/0/3.3	2017-08-18 10:07:38 -0400	Critical			
10.92.252.29	Link Down	et-8/0/9.1	2017-08-18 10:07:38 -0400	Critical			
10.92.252.31	Link Down	et-14/0/12.0	2017-08-18 10:34:32 -0400	Critical			
10.92.252.31	Link Down	et-14/0/17.3	2017-08-18 10:34:32 -0400	Critical			
10.102.220.11	Link Down	et-0/0/0	2017-08-18 09:38:23 -0400	Critical			
10.92.252.29	Link Down	et-8/0/16.3	2017-08-18 10:07:38 -0400	Critical			
10.92.252.29	Link Down	et-8/0/7.1	2017-08-18 10:07:38 -0400	Critical			
10.92.252.31	SIB 0 Absent	10.92.252.31	2017-08-18 10:02:55 -0400	Critical			

Showing 1 to 10 of 373 entries

Previous 1 2 3 4 5 ... 38 Next

1. To sort the table entries based a particular attribute, click the column heading for that attribute.

To reverse the order, click the column heading again.

2. To filter the table for any text string, type the text string into the **Search** box.

The table shows the filtered entries as you type. For example:

Show 10 entries	Display: All	View	Acknowledge	Copy	Print	Save	Search: 172.26.138.41
Device	Description	Source	Time Raised	Severity			
172.26.138.41	Device unreachable	172.26.138.41	2017-08-18 15:50:21 -0400	Critical			
172.26.138.41	Input LOS	connection 1/1/1/90	2017-08-18 05:40:54 -0400	Major			
172.26.138.41	Input LOS	connection 1/1/1/95	2017-08-18 05:30:53 -0400	Major			
172.26.138.41	Input LOS	channel1_1_LINE-R1_4	2017-08-18 07:30:46 -0400	Major			
172.26.138.41	Input LOS	channel1_1_LINE-R1_90	2017-08-18 07:30:46 -0400	Major			
172.26.138.41	Input LOS	channel1_1_LINE-R1_94	2017-08-18 07:30:46 -0400	Major			
172.26.138.41	Input LOS	channel1_1_LINE-R1_95	2017-08-18 07:30:46 -0400	Major			
172.26.138.41	Loss of Optical Output Signal	port 1/1/OSC1	2017-08-18 05:30:51 -0400	Minor			
172.26.138.41	Loss of Optical Input Signal	port 1/1/OSC0	2017-08-18 05:30:51 -0400	Minor			
172.26.138.41	Loss of Optical Input Signal	port 1/1/OSC1	2017-08-18 05:30:51 -0400	Minor			

Showing 1 to 10 of 14 entries (filtered from 373 total entries)

Previous 1 2 Next

3. If the table provides a **View** button, you can see more detailed information for a particular row by selecting a row and then clicking **View**.

A window appears showing more details for the selection. Here is an example of a **Current Alarm Details** window:

Current Alarm Details

Device 10.228.63.3
Description OTN Loss of signal
Source et-0/0/0
Time Raised 2018-01-04 01:43:46 -0500
Severity Critical
Acknowledged No
Probable Cause *Direction: Rx; Location: Far End;*

4. To copy (to clipboard), print, or save the table to a CSV file, click the **Copy**, **Print**, or **Save** buttons respectively.

This action applies to entries currently displayed in the table, after filtering has been applied.

Supported Devices

The proNX Optical Director can be used to manage the devices shown in [Table 1 on page 23](#).

Table 1: Supported Devices

Device	Support
TCX1000-RDM20	Full
TCX1000-ILA	Full
FMD96 (modeled as a circuit pack)	Full
2D8CMD (modeled as a circuit pack)	Full
BT17800	Basic
ACX6360-OR (router) or ACX6360-OX (transponder)	Basic

Table 1: Supported Devices (continued)

Device	Support
MX Series routers: MX200, MX240, MX480, MX960, MX2010	Basic
PTX Series routers: PTX3000, PTX5000	Basic
QFX Series switches: QFX10008, QFX100016	Basic
<p>NOTE: Basic support includes discovery and retrieval of system information, alarm management, inventory, log collection, performance monitoring, configuration database backup and restore, and more. See “Device Management” on page 63 for information on which management features are supported on which device. Basic support also includes configuration of the transceiver endpoint on the router, switch, or transponder if the transceiver is a supported tail facility endpoint (Table 2 on page 24).</p>	

Table 2: Supported Tail Facility Endpoints

Client Device	Supported Tail Facility Endpoints
BT17800	Ports on the UFM3 (BT8A78UFM3) 100G Coherent CFP-M05 transceiver (CFP-100GBASE-CHRT and BP3AMCTL) Ports on the UFM6 (BT8A78UFM6-I02) 400G Coherent MSA XCVR
ACX6360	Ports on the CFP2-DCO transceiver (CFP2-DCO-T-WDM-1)
MX Series router	Ports on the 100-Gigabit DWDM OTN MIC with CFP2-ACO (MIC3-100G-DWDM)
PTX Series router	Ports on the 100-Gigabit DWDM OTN PIC with CFP2-ACO (PTX-5-100G-WDM)
QFX Series switch	Ports on the QFX10K DWDM 1.2T Line Card (QFX10K-12C-DWDM)
<p>NOTE: For an explanation of tail facilities, see “Optical Service and Tail Facility Endpoints” on page 129.</p>	

CHAPTER 2

Dashboard

- [About the Dashboard on page 25](#)
- [Editing the Dashboard on page 29](#)

About the Dashboard

To access this page, click the **Dashboard** tab.

This is the first page you see when you log in to the proNX Optical Director. The dashboard is user-configurable and offers you a customized view of the health of your network through its widgets. You can add, remove, and rearrange widgets to meet your needs. The dashboard automatically adjusts the placement of the widgets to dynamically fit in your browser window.

Tasks You Can Perform

You can view the health of your network from this page. Additionally, you can customize the dashboard by adding, removing, and rearranging the widgets on a per user basis.

Field Descriptions

[Table 3 on page 26](#) describes the available widgets in the dashboard.

Table 3: Widgets in the Dashboard
















Widget	Description
Available Ports - Optical	<p>View the number of available optical ports in your network as a percentage of the total number of optical ports. This gives an approximate indication of client port usage. A high percentage usually indicates that you need to add more multiplexer/demultiplexers to your network.</p> <p>The total number of optical ports at each ROADM node is the number of universal ports on the ROADM(s), plus the number of client ports on attached multiplexer/demultiplexers, less the number of multiplexers/demultiplexers. For example, a ROADM node consisting of a single TCX1000-RDM20 and a single FMD96 has 20 universal ports plus 96 multiplexer/demultiplexer client ports less 1 port used to connect to the multiplexer/demultiplexer, which results in 115 optical ports. The total number of optical ports in the network is the sum of the total number of optical ports at each ROADM node in the network.</p> <p>The number of available optical ports at each ROADM node is the total number of optical ports less the number of channels added/dropped at that node. For example, if the above ROADM node has 15 channels added/dropped (regardless of whether the channels are added/dropped directly on the universal ports or through the FMD96), then the number of available optical ports is the 115 total ports less the 15 channels, which results in 100 available ports. The number of available ports in the network is the sum of the number of available ports at each ROADM node in the network.</p> <p>See “Device Links Overview” on page 117 for an explanation of ROADM nodes.</p> <p>This widget is a snapshot. To refresh the counts, click the  icon.</p>
Available Ports - Packet	<p>View the number of supported tail facility ports available as a percentage of the total number of supported tail facility ports. A tail facility port is considered available if its operational status is Down.</p> <p>See “Services Overview” on page 128 for an explanation of tail facilities.</p> <p>This widget is a snapshot. To refresh the counts, click the  icon.</p>
Current Alarms	<p>View the number of current alarms in your network categorized by severity.</p> <p>Click a severity to bring up the Current Alarms table filtered for the string “Critical”, “Major”, or “Minor” depending on the severity selected.</p> <p>This widget is updated automatically as alarms are raised, cleared, or acknowledged.</p>
Device Types	<p>View the number of devices in your network categorized by device type.</p> <p>Select the device types to display by toggling the selection boxes in the legend.</p> <p>This widget is a snapshot. To refresh the counts, click the  icon.</p>
Historical Alarms	<p>View the top ten devices with the highest historical alarm counts.</p> <p>Select the devices to display by toggling the selection boxes in the legend. If a device has a count that is much higher than the others, the scale on the graph might not provide sufficient resolution for you to see the counts for the other devices. In this case, simply uncheck the devices with the higher counts to see the counts for the other devices on a more useful scale.</p> <p>This widget is a snapshot. To refresh the counts, refresh the page.</p>

Table 3: Widgets in the Dashboard (continued)

Widget	Description
Historical Events	<p>View the top ten devices with the highest historical event counts.</p> <p>Select the devices to display by toggling the selection boxes in the legend. If a device has a count that is much higher than the others, the scale on the graph might not provide sufficient resolution for you to see the counts for the other devices. In this case, simply uncheck the devices with the higher counts to see the counts for the other devices on a more useful scale.</p> <p>This widget is a snapshot. To refresh the counts, click the  icon.</p>
Hourly Event Count	<p>View the number of events that have occurred in the network over each of the last 24 hours.</p> <p>This widget is a snapshot. To refresh the counts, click the  icon.</p>
Site Alarms	<p>View the alarm counts by severity by site.</p> <p>Select the site to display from the drop-down list.</p> <p>This widget is updated automatically as alarms occur.</p>
Software Versions	<p>View software versions running on devices in the network (including supported devices at the tail facility endpoint).</p> <p>Select the software versions to display by toggling the selection boxes in the legend.</p> <p>This widget is a snapshot. To refresh the counts, click the  icon.</p>
System Details	See Table 4 on page 28 .
Task Statistics	<p>View the counts of successful (green) and failed (red) tasks launched by the proNX Optical Director. The failed task count includes tasks with a status of Failure or Finished. (A Finished task is a task where one or more subtasks have failed.)</p> <p>Click a status inside the graph to bring up the Administration Tasks table filtered for the Success status or the Failure or Finished status depending on the status selected.</p> <p>NOTE: This widget is applicable for counts of tasks and not subtasks.</p> <p>This widget is a snapshot. To refresh the counts, click the  icon.</p>
Unreachable Devices	<p>View the list of unreachable devices in your network. These are the devices that are discovered but are no longer reachable. The proNX Optical Director rediscovers all devices periodically. If the proNX Optical Director does not receive a response from a device after a number of tries, the proNX Optical Director declares the device unreachable. You will not be able to configure or create links or services on unreachable devices.</p> <p>This widget is a snapshot. To refresh the list, click the  icon.</p>

NOTE: You can refresh all widgets simultaneously by clicking the  icon in the top right corner of the page.

Table 4: System Details

System Details	Description
Cluster Nodes	
Uptime	The time the node has been running since the last reset.
CPU Count	The number of CPUs on the node.
Memory	The amount of memory on the node.
Kernel	The kernel version running on the node.
OS Image	The OS version running on the node.
Kublet Version	The Kublet version running on the node.
OutOfDisk	<p>An OutOfDisk condition on the node. This condition is set when the node has insufficient disk space for creating pods.</p> <p>A green  indicates there is no OutOfDisk condition. Contact JTAC if this attribute is shown with any other indication.</p>
MemoryPressure	<p>A MemoryPressure condition on the node. This condition is set when available memory on the node has fallen below the low memory threshold.</p> <p>A green  indicates there is no MemoryPressure condition. Contact JTAC if this attribute is shown with any other indication.</p>
DiskPressure	<p>A DiskPressure condition on the node. This condition is raised when available disk space on the node has fallen below the low disk space threshold.</p> <p>A green  indicates there is no DiskPressure condition. Contact JTAC if this attribute is shown with any other indication.</p>
Ready	A green  indicates the node is running normally.
Cluster Pods	Contact JTAC if any item does not appear with a green  .
Cluster Services	Contact JTAC if any item does not appear with a green  .
Service Connections	Contact JTAC if any item does not appear with a green  .

Release History Table


Release	Description
18.4	Task Statistics

Editing the Dashboard

Use this procedure to customize what widgets you see in the dashboard.

1. Click the **Dashboard** tab.

The dashboard is displayed.

2. Click the  icon in the top right corner of the page.

The Edit pane appears at the top of the dashboard.



3. In the Edit pane, double click the widget you want to add to the dashboard.

The selected widget is moved to the first available spot that can accommodate its size in the dashboard . Repeat until all desired widgets are moved to the dashboard.

4. To remove a widget from the dashboard, click the  icon for that widget.

The removed widget appears in the Edit pane.

5. To reposition a widget in the dashboard, drag and drop the widget to the desired location.

6. To resize a widget, place your mouse over the widget until the  icon appears in the lower right corner. Click the  icon and drag until the widget is at the desired size and then release.

7. When you are finished editing the dashboard, click the  icon to close the Edit pane.

CHAPTER 3

Monitor

- [Network Map on page 31](#)
- [Logical View on page 36](#)
- [Current Alarms on page 40](#)
- [Historical Alarms on page 43](#)
- [Events on page 46](#)


Network Map

- [About the Network Map Page on page 31](#)
- [Navigating the Network Map Page on page 32](#)
- [Viewing Site Details on page 33](#)
- [Viewing Link Details on page 35](#)

About the Network Map Page

To access this page, click the **Monitor** tab and then select **Network Map** from the left-nav bar.

The Network Map page lets you view the topology of your network. The map shows sites and the connectivity between sites. A site represents a geographic location shared by colocated devices. You associate a device to a site during device discovery. The placement of a site on the map is dictated by the site's latitude and longitude coordinates. If no devices have been discovered, the map is unpopulated.

The  icon includes an alarm indication. The presence of a dot in the upper right corner of the icon indicates the existence of active unacknowledged alarms. Red indicates the existence of active unacknowledged critical alarms. Amber indicates the existence of active unacknowledged major alarms. Yellow indicates the existence of active unacknowledged minor alarms. When multiple levels of alarm severity exist, the color reflects the level of the most severe alarm, with red being the most severe and yellow being the least severe. The absence of a dot indicates no active unacknowledged alarms, which implies one of the following:

- all active alarms have been acknowledged, or
- there are no active alarms

The color of the link indicates whether the link is up or down. Green indicates that the link is up. Red indicates that the link is down.

Tasks You Can Perform


You can perform the following tasks from this page:


- View the topology of your network.
- View site details for a particular site.
- View link details for a particular link.

Navigating the Network Map Page




Use this procedure to navigate the Network Map page. When you first open the Network Map page, the sites are centered on the map and the map is automatically set to a level of magnification that allows all sites to be displayed.

1. To pan around the map, click and hold anywhere in the map background and drag the map until the desired part of the map comes into view.
2. To zoom in and out:

To zoom in, click the  in the lower right corner. Alternatively, you can zoom in by double clicking anywhere in the map background or by using your mouse scroll wheel.

To zoom out, click the  in the lower right corner. Alternatively, you can zoom out by using your mouse scroll wheel.



NOTE: If you zoom out such that two or more sites are on top of each other, a single  icon is displayed. To see the sites represented by the  icon, click the  icon.

3. To view information for a site, see [“Viewing Site Details” on page 33](#).
4. To view information for a link, see [“Viewing Link Details” on page 35](#).
5. To search for a site, type the name of the site in the search box. The search is case-insensitive. As you type, a list of matching entries is shown. Continue typing to narrow down the list or move your mouse over the desired entry to highlight it. Once the desired entry is highlighted, click or press Enter to select it.

The map zooms in and centers on the selected site, and a window appears in the top left corner showing details for the selected site.
6. To search for a device, type the name or IP address of the device in the search box. The search is case-insensitive. As you type, a list of matching entries is shown. Continue

typing to narrow down the list or move your mouse over the desired entry to highlight it. Once the desired entry is highlighted, click or press Enter to select it.

The map zooms in and centers on the site containing the selected device, and a window appears in the top left corner showing details for the selected site and device.

7. To reset the view, click the reset  icon.

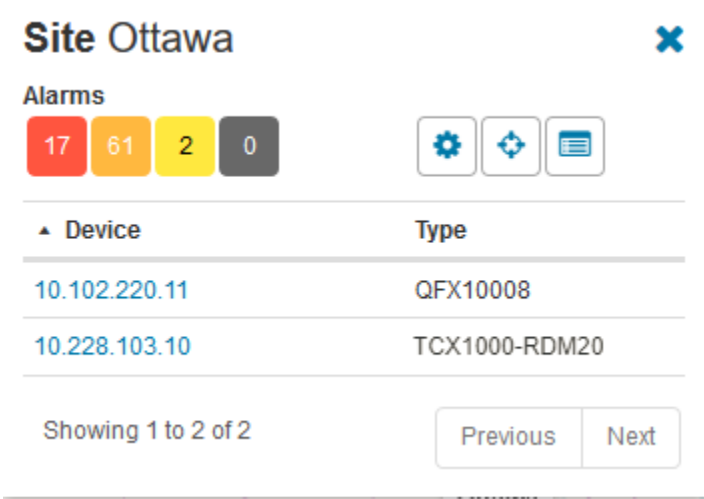
Viewing Site Details

Use this procedure to view information on a site.

The information includes a listing of the devices found at that site. From here, you can see details on the devices including any outstanding alarms.

1. To see information for a site, click the site.

The Site window appears in the upper left corner, for example:




The screenshot shows a window titled "Site Ottawa" with a close button (X) in the top right corner. Below the title, there is an "Alarms" section with four colored boxes containing the numbers 17 (red), 61 (orange), 2 (yellow), and 0 (grey). To the right of these boxes are three icons: a gear (Settings), a location pin (Location), and a list (Devices). Below this is a table with two columns: "Device" and "Type". The table contains two rows of data. At the bottom of the table, it says "Showing 1 to 2 of 2" and there are "Previous" and "Next" buttons.

Device	Type
10.102.220.11	QFX10008
10.228.103.10	TCX1000-RDM20

The following information is shown:

- The name of the site.
 - A visual indication of the number of alarms raised at each severity for all devices at that site.
 - A list of devices that belong to that site. Click a column heading to sort the list by that column. If the list is long, use the Next and Previous buttons to page through the list.
 - Shortcut buttons are provided at the top right to go to the Site Config page, the Site Location page, and the Site Devices page.
2. To see information on a device within a site, click a device from the device list.

The Site window is extended to display the following information in a Device pane:

- The name and/or IP address of the device, depending on user preferences. See [“Changing Your \(Local\) User Settings” on page 20](#).
 - A visual indication of the number of alarms at the different severities for that device.
 - The type of device.
 - The software version running on the device.
 - Shortcut buttons are provided at the top right of the Device pane to go to the Device Config page, the Devices Inventory page, the Device Chassis View page, and the Device Security page.
3. To see the alarms raised on that device, click the alarm severity that you would like to see.
- To see critical alarms, click the number within the red indicator.
 - To see major alarms, click the number within the amber indicator.
 - To see minor alarms, click the number within the yellow indicator.
- The Current Alarms table appears, filtered for that device and for the string that matches the selected severity. For information on the Current Alarms table, see [“Current Alarms” on page 40](#).
4. To close the Site window, click .

See Also • [Site Management on page 56](#)

Viewing Link Details

Use this procedure to view information on a link. The color and state of a link are derived from the administrative state and operational status at each endpoint of the link ([Table 5 on page 35](#)).

Table 5: Link Colors and States

Endpoint 1		Endpoint 2		Link Color	Link State
Administrative State	Operational Status	Administrative State	Operational Status		
Out of Service	Down	Out of Service	Down	Black	OOS-Down
In Service	Down	In Service	Down	Red	IS-Down
In Service	Down	Out of Service	Down	Red	IS-Down, OOS-Down
In Service	Up	In Service	Up	Green	IS-Up
All other combinations				Gray	–

When more than one link exists between two sites, a single multilink is displayed. The color of the multilink is derived from the colors of the individual links ([Table 6 on page 35](#)).

Table 6: Multilink Colors

Individual Link Colors	Multilink Color
All individual links are green.	Green
All individual links are black.	Black
All individual links are red.	Red
All individual links are gray.	Gray
At least one individual link is green but not all individual links are green.	Amber
No individual link is green and at least one individual link is red, but not all individual links are red.	Red
No individual link is green or red, and at least one individual link is black, but not all individual links are black.	Black

1. To see information on a link, click the link.

The Links window appears in the upper left corner, for example:

Links Between BOS and AUS ✕			
▲ Source	Destination	State	Fiber Type
10.228.4.122, port: 1/1/LINE	10.228.4.36, port: 1/1/LINE	IS-Up	Single Mode Fiber
Showing 1 to 1 of 1		Previous	Next

The following information is displayed:

- The source and destination site names.
- The source and destination device names and/or IP addresses, depending on user preferences.
- The source and destination port endpoints.
- The link state.
- The fiber type (applicable to links on ROADM line ports only).

If multiple links are present between sites, information on all links is displayed.

2. To close the Links window, click **✕**.

See Also • [Device Links on page 117](#)

Logical View

- [About the Logical View Page on page 36](#)
- [Navigating the Logical View Page on page 37](#)
- [Viewing a Device or Device Group on page 38](#)
- [Viewing Link Details on page 39](#)

About the Logical View Page

To access this page, click the **Monitor** tab and then select **Logical View** from the left-nav bar.

The Logical View page lets you view the logical grouping and logical connectivity in your network.

Tasks You Can Perform


You can perform the following tasks from this page:

- View the logical groups (such as ROADM nodes) in your network.

- View the connectivity between and within logical groups.
- Show or hide different elements from the view.

Navigating the Logical View Page

Use this procedure to navigate the Logical View page. The Logical View page displays connectivity between and within ROADM nodes.

A ROADM node is displayed generically as a device group , which is a collection of one or more devices. The number of devices contained inside the device group is shown by a number in the upper left corner of the device group icon. Currently, the only device group that can hold more than one device is a ROADM node.


When you first open the Logical View page, the device groups are centered on a blank background and set to a level of magnification that allows all device groups to be displayed.


1. Use the **Select** drop-down list to include or exclude specified entities from view:
 - **Show Mux/Demux** - Check to show multiplexers/demultiplexers, uncheck to hide multiplexers/demultiplexers.
 - **Show ILAs** - Check to show ILAs, uncheck to hide ILAs. If ILAs are hidden, the links that go through the ILAs are displayed between the ROADM endpoints.
 - **Show Transponders** - Check to show transponders, uncheck to hide transponders.
 - **Show Un-Connected** - Check to show unconnected devices, uncheck to hide unconnected devices. An unconnected device is a device with no configured or learned links. Note that a connected device can appear unconnected when the device at the other end of the connection is hidden. In other words, if you hide unconnected devices, you might still see devices that appear unconnected if they are connected to a hidden device.




NOTE: In general, when a device is hidden, any links that connect to the device are also hidden. The exception to this is the ILA device, where a connection that spans hidden ILAs is shown as a link between the two ROADM endpoints. This allows you to view ROADM to ROADM connectivity without cluttering the view with amplifiers. A connection that spans hidden ILAs is called an amplified link.

2. To pan around the page, click and hold anywhere in the background, and drag until the desired part of the page comes into view.
3. To zoom in and out:

To zoom in, click the  in the lower right corner. Alternatively, you can zoom in by using your mouse scroll wheel.

To zoom out, click the  in the lower right corner. Alternatively, you can zoom out by using your mouse scroll wheel.

4. To view information for a device or device group, see [“Viewing a Device or Device Group” on page 38](#).
5. To view information for a link, see [“Viewing Link Details” on page 39](#).
6. To reset the view, click the reset  icon.

Viewing a Device or Device Group

Use this procedure to view information on a device or a device group.


1. To see information for a device group, click the device group.

An information window appears in the upper left corner. The following information is shown:

- The number of devices within the device group.



NOTE: A multiplexer/demultiplexer is part of a ROADM device and is not counted as a separate device.

- A visual indication of the number of alarms collectively raised at each severity for all devices in that device group.
 - A list of devices that belong to that device group. Click a column heading to sort the list by that column. If the list is long, use the Next and Previous buttons to page through the list.
 - To see information on a device within the list, click a device in the device list. The information window is extended to display device information. Alarm counts are displayed and a shortcut is provided to allow you to click to the Device Config page for that device.
 - To close the information window, click .
2. To show the contents of a device group, double click the device group. The device group is expanded and the contained devices are shown within a shaded device group box. The size of the device group box is automatically set and cannot be changed.
 - To see information on a device within the group, hover over the device with your mouse.
 - To bring up an information window for a device, click the device. An information window appears in the upper left corner showing the alarm counts for the device. From here, you can click a shortcut to go to the Device Config page for that device.

- To move a device within a device group box, click and drag the device within the device group box.
- To hide the contents of a device group, double click the shaded device group box.

Viewing Link Details

Use this procedure to view information on a link. The color and state of a link are derived from the administrative state and operational status at each endpoint of the link ([Table 7 on page 39](#)).

Table 7: Link Colors and States

Endpoint 1		Endpoint 2		Link Color	Link State
Administrative State	Operational Status	Administrative State	Operational Status		
Out of Service	Down	Out of Service	Down	Black	OOS-Down
In Service	Down	In Service	Down	Red	IS-Down
In Service	Down	Out of Service	Down	Red	IS-Down, OOS-Down
In Service	Up	In Service	Up	Green	IS-Up
All other combinations				Gray	–

Links are drawn with different weights, as shown in [Table 8 on page 39](#):

Table 8: Link Weights

Link	Weight
Links between ROADM nodes	Heavy
Links between TCX1000-RDM20 devices within a ROADM node	Medium
All other links	Light

1. To see information on a link, click the link.

The Links window appears in the upper left corner. The following information is displayed:

- The source and destination device names and/or IP addresses, depending on user preferences. For amplified links, the source and destination refer to the ROADM device endpoints.
- The source and destination port endpoints. For amplified links, the source and destination refer to the ROADM line port endpoints.

- The link state. For amplified links, the link state is derived from the state of the ROADM port endpoints.
 - The fiber type (applicable to line spans only).
2. To close the Links window, click **X**.

Release History Table

Release	Description
18.4	The Logical View page lets you view the logical grouping and logical connectivity in your network.

Current Alarms

- [About the Current Alarms Page on page 40](#)
- [Viewing Current Alarms on page 41](#)
- [Acknowledging or Unacknowledging an Alarm on page 43](#)

About the Current Alarms Page

To access this page, click the **Monitor** tab and then select **Alarms>Current** from the left-nav bar.

The Current Alarms page displays the table of outstanding alarms in your network. You can filter the table to see alarms for a specific device or a subset of devices, and you can acknowledge an alarm. Acknowledging an alarm allows you to indicate to other users that this alarm is being addressed.

See the *TCX Series Optical Transport System Feature Guide* for information on all alarms.

Tasks You Can Perform

You can perform the following tasks from this page:

- View current alarms in the network or on a device.
- Acknowledge or unacknowledge alarms.

Field Descriptions

[Table 9 on page 40](#) explains the headings in the Current Alarms page.

Table 9: Fields for the Current Alarms Page

Field	Description
Device	The IP address of the device.
Description	The alarm description as reported by the device for alarms generated by the device or as provided by the proNX Optical Director for alarms generated by the proNX Optical Director.
Source	The component that raised the alarm.

Table 9: Fields for the Current Alarms Page (continued)

Field	Description
Time Raised	<p>The date and time when the alarm was raised, in the following format:</p> <p>YYYY-MM-DD HH:MM:SS ZZZZ</p> <ul style="list-style-type: none"> • YYYY is the year • MM is the month • DD is the day • HH is the hour • MM is the minute • SS is the second • ZZZZ is the time zone represented as a UTC offset (for example, Eastern Daylight Time is specified as -0400)
Severity	<p>Critical, major, or minor.</p> <p>For alarms raised by the TCX Series elements, the following definitions apply:</p> <ul style="list-style-type: none"> • Critical - service-affecting hardware failure • Major - service-affecting abnormal condition • Minor - non-service-affecting abnormal condition

Viewing Current Alarms

Use this procedure to view current alarms for a device.

1. Click the **Monitor** tab and then select **Alarms>Current** from the left-nav bar.

The Current Alarms table is displayed:

Show 10

▼ entries

Display:

☒ All

☐ View

☐ Acknowledge

☐ Copy

☐ Print

☐ Save

Search:

Device	Description	Source	Time Raised	Severity
10.92.252.29	OTN Loss of signal	et-12/0/1	2017-08-18 10:10:39 -0400	Critical
10.92.252.29	Link Down	et-8/0/13.0	2017-08-18 10:07:38 -0400	Critical
10.92.252.29	Link Down	et-8/0/3.3	2017-08-18 10:07:38 -0400	Critical
10.92.252.29	Link Down	et-8/0/9.1	2017-08-18 10:07:38 -0400	Critical
10.92.252.31	Link Down	et-14/0/12.0	2017-08-18 10:34:32 -0400	Critical
10.92.252.31	Link Down	et-14/0/17.3	2017-08-18 10:34:32 -0400	Critical
10.102.220.11	Link Down	et-0/0/0	2017-08-18 09:38:23 -0400	Critical
10.92.252.29	Link Down	et-8/0/16.3	2017-08-18 10:07:38 -0400	Critical
10.92.252.29	Link Down	et-8/0/7.1	2017-08-18 10:07:38 -0400	Critical
10.92.252.31	SIB 0 Absent	10.92.252.31	2017-08-18 10:02:55 -0400	Critical

Showing 1 to 10 of 373 entries

Previous

1

2

3

4

5

...

38

Next

By default, the alarms are sorted first by **Severity** then by **Time Raised**.



NOTE: This table is updated automatically as alarms occur.

2. To see all alarms, all acknowledged alarms, or all unacknowledged alarms, select **All**, **Acknowledged**, or **Un-Acknowledged** respectively from the **Display** drop-down list.

By default, all alarms are displayed.

3. To see alarms for a particular device, use the standard table search function. See [“Working with Tables” on page 22](#).

The following example shows the table filtered for the specified IP address:

Show 10
▼
entries
Display:
☒ All -
☐ View
☐ Acknowledge
☐ Copy
☐ Print
☐ Save -
Search:
172.26.138.41

Device	Description	Source	Time Raised	Severity
172.26.138.41	Device unreachable	172.26.138.41	2017-08-18 15:50:21 -0400	Critical
172.26.138.41	Input LOS	connection 1/1/1/90	2017-08-18 05:40:54 -0400	Major
172.26.138.41	Input LOS	connection 1/1/1/95	2017-08-18 05:30:53 -0400	Major
172.26.138.41	Input LOS	channel 1_1_LINE-R_4	2017-08-18 07:30:46 -0400	Major
172.26.138.41	Input LOS	channel 1_1_LINE-R_90	2017-08-18 07:30:46 -0400	Major
172.26.138.41	Input LOS	channel 1_1_LINE-R_94	2017-08-18 07:30:46 -0400	Major
172.26.138.41	Input LOS	channel 1_1_LINE-R_95	2017-08-18 07:30:46 -0400	Major
172.26.138.41	Loss of Optical Output Signal	port 1/1/OS/C1	2017-08-18 05:30:51 -0400	Minor
172.26.138.41	Loss of Optical Input Signal	port 1/1/OS/C0	2017-08-18 05:30:51 -0400	Minor
172.26.138.41	Loss of Optical Input Signal	port 1/1/OS/C1	2017-08-18 05:30:51 -0400	Minor

Showing 1 to 10 of 14 entries (filtered from 373 total entries)
Previous
1
2
Next

4. To see more details on an alarm, select an alarm and then click **View**.

The **Current Alarm Details** window appears:

Current Alarm Details	
Device	10.228.63.3
Description	OTN Loss of signal
Source	et-0/0/0
Time Raised	2018-01-04 01:43:46 -0500
Severity	Critical
Acknowledged	No
Probable Cause	Direction: Rx; Location: Far End;

The Probable Cause field indicates the direction in which the problem is likely occurring and the possible location of the problem. For example, the Probable Cause field in the above Loss of Signal alarm indicates that the Loss of Signal is in the receive direction and that the device at the far end of the fiber is where you should start troubleshooting.

5. To acknowledge or unacknowledge an alarm, see [“Acknowledging or Unacknowledging an Alarm” on page 43](#).
6. To sort, filter, copy, print, or save table entries, see [“Working with Tables” on page 22](#).


Acknowledging or Unacknowledging an Alarm

Use this procedure to acknowledge or unacknowledge an alarm.

You can use alarm acknowledgment in different ways, but typical usage is for you to use alarm acknowledgment to distinguish between alarms that someone is addressing (acknowledged) and alarms that still require someone to examine and triage (unacknowledged).

The color of the acknowledged alarm turns gray to reduce its visual impact and to allow you and other users to focus on the alarms that still need to be examined and assigned.

Acknowledging an alarm does the following:

- the alarm turns gray in the Current Alarms table
- the alarm is removed from consideration when determining the alarm indication color to display in the  icon in the Network Map



NOTE: Acknowledging an alarm does not change the severity of the alarm, nor does it change the alarm count for that severity. For example, if there are ten critical alarms and you acknowledge one of them, the acknowledged alarm count increases by one and the critical alarm count remains at ten.

1. Click the **Monitor** tab and then select **Alarms>Current** from the left-nav bar.

The Current Alarms table is displayed.

2. To acknowledge an alarm, select an alarm and click **Acknowledge**.

The alarm is acknowledged and the alarm row turns gray.

3. To unacknowledge an acknowledged alarm, select an alarm that has been acknowledged and click **Un-acknowledge**.

The alarm is unacknowledged and the alarm row turns back to the color of its severity.

Historical Alarms

- [About the Historical Alarms Page on page 44](#)
- [Viewing Historical Alarms on page 44](#)

About the Historical Alarms Page

To access this page, click the **Monitor** tab and then select **Alarms>Historical** from the left-nav bar.

The Historical Alarms page displays the table of historical alarms in your network. Historical alarms are alarms that have been cleared and are no longer outstanding. You can filter the table to see historical alarms for a specific device or a subset of devices.

Historical alarms provide you with a clear view of the history of a device so that you can spot any issues or trends that require attention. For example, historical alarms can reveal link flapping or other regularly-occurring issues.

Tasks You Can Perform

You can view historical alarms in the network or on a device from this page.

Field Descriptions

Table 10 on page 44 explains the headings in the Historical Alarms page.

Table 10: Fields for the Historical Alarms Page

Field	Description
Device	See Table 9 on page 40.
Description	See Table 9 on page 40.
Source	See Table 9 on page 40.
Time Raised	See Table 9 on page 40.
Time Cleared	<p>The date and time when the alarm was cleared, in the following format:</p> <p>YYYY-MM-DD HH:MM:SS ZZZZ</p> <ul style="list-style-type: none"> • YYYY is the year • MM is the month • DD is the day • HH is the hour • MM is the minute • SS is the second • ZZZZ is the time zone represented as a UTC offset (for example, Eastern Daylight Time is specified as -0400)
Severity	See Table 9 on page 40.

Viewing Historical Alarms

Use this procedure to view historical alarms for a device.

1. Click the **Monitor** tab and then select **Alarms>Historical** from the left-nav bar.

The Historical Alarms table is displayed:

Show 10 entries

View Copy Print Save Search:

Device	Description	Source	Time Raised	Time Cleared	Severity
10.92.252.31	OTN Loss of signal	et-2/0/0	2017-08-21 10:04:41 -0400	2017-08-21 10:05:41 -0400	Critical
172.26.138.41	Device unreachable		2017-08-17 20:49:14 -0400	2017-08-17 20:49:44 -0400	Critical
172.26.138.41	Device unreachable		2017-08-17 16:28:14 -0400	2017-08-17 16:28:51 -0400	Critical
10.92.252.29	Link Down	et-8/0/15.2	2017-08-19 10:05:01 -0400	2017-08-19 21:07:35 -0400	Critical
172.26.138.41	Device unreachable		2017-08-17 15:38:14 -0400	2017-08-17 15:38:54 -0400	Critical
10.92.252.31	Link Down	et-14/0/13.1	2017-08-21 21:33:31 -0400	2017-08-22 10:07:31 -0400	Critical
10.92.252.31	Link Down	et-14/0/18.2	2017-08-21 10:17:47 -0400	2017-08-21 10:18:01 -0400	Critical
10.92.252.31	Link Down	et-14/0/8.0	2017-08-19 10:16:11 -0400	2017-08-19 21:08:15 -0400	Critical
10.92.252.31	Link Down	et-14/0/23.2	2017-08-21 10:18:13 -0400	2017-08-21 21:30:25 -0400	Critical
10.92.252.29	Link Down	et-8/0/18.2	2017-08-20 10:05:00 -0400	2017-08-21 07:10:22 -0400	Critical

Showing 1 to 10 of 4,811 entries

Previous 1 2 3 4 5 ... 482 Next

By default, the alarms are sorted first by **Severity** then by **Time Raised**.



NOTE: This table is updated automatically as alarms are cleared.



NOTE: It is normal to see the occasional duplicate alarm in this list.

2. To see alarms for a particular device, use the standard table search function. See [“Working with Tables”](#) on page 22.

The following example shows the table filtered for the specified IP address:

Show 10 entries

View Copy Print Save Search: 10.92.252.29

Device	Description	Source	Time Raised	Time Cleared	Severity
10.92.252.29	Link Down	et-8/0/16.3	2017-08-18 10:07:38 -0400	2017-08-18 21:07:20 -0400	Critical
10.92.252.29	Link Down	et-14/0/1	2017-08-19 10:04:28 -0400	2017-08-19 10:09:16 -0400	Critical
10.92.252.29	Link Down	et-8/0/6.0	2017-08-20 10:05:00 -0400	2017-08-21 07:10:22 -0400	Critical
10.92.252.29	Link Down	et-8/0/22.0	2017-08-20 10:05:00 -0400	2017-08-21 07:10:22 -0400	Critical
10.92.252.29	Link Down	et-8/0/19.0	2017-08-21 10:05:41 -0400	2017-08-22 07:07:17 -0400	Critical
10.92.252.29	OTN Loss of signal	et-12/0/1	2017-08-21 10:10:34 -0400	2017-08-22 07:07:17 -0400	Critical
10.92.252.29	OTN Loss of signal	1365	2017-08-18 21:07:18 -0400	2017-08-19 10:04:30 -0400	Critical
10.92.252.29	Link Down	et-8/0/18.2	2017-08-20 10:05:00 -0400	2017-08-21 07:10:22 -0400	Critical
10.92.252.29	Link Down	et-8/0/15.2	2017-08-19 10:05:01 -0400	2017-08-19 21:07:35 -0400	Critical
10.92.252.29	Link Down	et-8/0/17.3	2017-08-19 10:05:01 -0400	2017-08-19 21:07:35 -0400	Critical

Showing 1 to 10 of 1,042 entries (filtered from 4,812 total entries)

Previous 1 2 3 4 5 ... 105 Next

3. To see more details on an alarm, select an alarm row and then click View.

The **Historical Alarm Details** window appears:

Historical Alarm Details



Device 10.228.4.141
Description Topology link has FE=port:1_1_U0 at 10.228.4.47. Device not found
Source port:1/1/U0
Time Raised 2018-04-12 12:53:25 -0400
Time Cleared 2018-04-12 12:54:25 -0400
Severity Major
Acknowledged No
Probable Cause Direction: Tx; Location: Far End;

Close

4. To sort, filter, copy, print, or save table entries, see [“Working with Tables” on page 22](#).

Events

- [About the Events Page on page 46](#)
- [Viewing Events on page 47](#)

About the Events Page

To access this page, click the **Monitor** tab and then select **Events** from the left-nav bar.

You can use the Events page to view the events in your network. Events are SNMP traps or NETCONF events received from managed devices, and can include alarms, non-alarmed conditions such as threshold crossing alerts, as well as notifications of routine transactions and behavior. A high event count does not necessarily indicate errors in the network but should warrant further investigation. You can filter the table to see events for a specific device or a subset of devices, and you can expand an event to view additional details for that event.

Tasks You Can Perform

You can view SNMP and NETCONF events in the network or on a device from this page.

Field Descriptions

[Table 11 on page 46](#) explains the headings in the Events page.

Table 11: Fields for the Events Page

Field	Description
Device	The IP address of the device.
Description	The OID of the SNMP trap or the name of the NETCONF notification.

Table 11: Fields for the Events Page (continued)

Field	Description
Time Received	<p>The date and time when the event was received, in the following format:</p> <p>YYYY-MM-DDTHH:MM:SS.SSS</p> <ul style="list-style-type: none"> • YYYY is the year • MM is the month • DD is the day • T is the delimiter • HH is the hour • MM is the minute • SS.SSS is the second

Viewing Events

Use this procedure to view events for a device.

1. Click the **Monitor** tab and then select **Events** from the left-nav bar.

The Events table is displayed:

Device	Description	Time Received
10.228.61.1	1.3.6.1.4.1.2636.4.5.1	2018-03-07T08:50:46.915
10.228.61.1	1.3.6.1.4.1.2636.1.1.1.2.69.0	2018-03-07T03:49:05.951
10.228.61.1	1.3.6.1.6.3.1.1.5.4	2018-03-07T03:59:47.714
10.228.61.1	1.3.6.1.4.1.2636.4.1.1	2018-03-07T04:36:43.436
10.228.61.1	1.3.6.1.4.1.2636.4.5.0.1	2018-03-06T17:52:21.412
10.228.61.1	1.3.6.1.4.1.2636.4.5.0.1	2018-03-06T15:52:05.247
10.228.61.1	1.3.6.1.4.1.2636.1.1.1.2.69.0	2018-03-07T04:15:05.704
10.228.61.1	1.3.6.1.4.1.2636.4.21.2	2018-03-07T04:15:05.593
10.228.61.1	1.3.6.1.4.1.2636.3.73.1.3.0.2	2018-03-07T03:59:02.106
10.228.61.1	1.3.6.1.4.1.2636.4.21.0.2	2018-03-07T04:15:00.116



NOTE: This table is updated automatically as events are raised.

2. To see events for a particular device, type the IP address of the device in the search box. See [“Working with Tables” on page 22](#).
3. To see more details on an event, select an event row and then click **View**.

The **Event Details** window appears:

Event Details



Netconf Details

```
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2018-03-06T17:41:45Z</eventTime>
  <netconf-session-end xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-notifications">
    <username>netconf</username>
    <session-id>1112</session-id>
    <source-host>::ffff:127.0.0.1</source-host>
    <termination-reason>closed</termination-reason>
  </netconf-session-end>
</notification>
```

Close

4. To sort, filter, copy, print, or save table entries, see [“Working with Tables” on page 22](#).

CHAPTER 4

Devices

- [Devices Configuration on page 49](#)
- [Site Management on page 56](#)
- [Device Management on page 63](#)
- [Shelf Management on page 89](#)
- [Circuit Pack Management on page 92](#)
- [Port Management on page 93](#)
- [Devices Discovery on page 109](#)
- [Devices Inventory on page 114](#)

Devices Configuration

- [About the Devices Configuration Page on page 49](#)
- [Navigating the Device Tree on page 51](#)
- [Component Naming on page 52](#)
- [Creating a New Site on page 55](#)
- [Deleting a Site on page 55](#)

About the Devices Configuration Page

To access this page, click the **Devices** tab and select **Configuration** in the left-nav bar.

The Devices Configuration page is the top level page where you manage sites and devices in your network. It consists of a mini-left-nav bar that displays the device tree and a main pane that is in context with the selection in the device tree. The device tree is a hierarchical representation of the device's component model.

The device tree can be categorized by device type or by site. When you categorize the device tree by site, the Devices Configuration (Sites) page appears. When you categorize the device tree by device type, the Devices Configuration (Device Types) page appears.

Tasks You Can Perform

You can perform the following tasks from this page:

- View a list of sites or device types in your network.

- Create a new site.
- Delete a site.

Field Descriptions

Table 12 on page 50 and Table 13 on page 50 describe the fields in the Devices Configuration (Sites) page and the Devices Configuration (Device Types) page. To switch between these two pages, see [“Navigating the Device Tree” on page 51](#).

Table 12: Fields in the Devices Configuration (Sites) Page

Field	Description
Site Name	The name of the site. You configure the name when you create the site.
Description	The description of the site. You add the description when you create the site.
Devices	The number of devices at that site. Passive equipment such as a multiplexer/demultiplexer is not included in this count. Passive equipment is modeled as a circuit pack on an active device.

Table 13: Fields in the Devices Configuration (Device Types) Page

Field	Description
Model Name	The model name of the device. This information is retrieved from the device.
Manufacturer	The manufacturer of the device. This information is retrieved from the device.
Devices	The number of devices for that device type. Passive equipment such as a multiplexer/demultiplexer is not associated with a device type and is therefore not included in this count. Passive equipment is modeled as a circuit pack on an active device.

Navigating the Device Tree

Use this procedure to navigate the device tree. When you go to the Devices Configuration page, the mini-left-nav bar shows a collapsed device tree categorized by either device type or site depending on how it was last categorized.

The tree is arranged hierarchically as follows:

- Device type or site (highest level)
- Device
- Shelf
- Circuit pack (one or more levels)
- Port (lowest level)

In order to provide a consistent look-and-feel, the proNX Optical Director maps all devices into the above hierarchy.

Where needed, the hierarchy is extended to include additional levels. For example, an MX Series router has a chassis that contains FPCs that in turn contain MICs that in turn contain transceivers and ports. The proNX Optical Director represents this as a device containing a shelf containing an FPC circuit pack containing a MIC circuit pack containing a transceiver circuit pack containing a port.

In contrast, TCX Series devices do not have shelves or circuit packs, so the proNX Optical Director represents TCX Series devices as devices containing a single shelf that contains a single circuit pack.

1. To view the device tree categorized by site, click the **Sort** icon below the device tree and select **Site**. To view the device tree categorized by device type, click the **Sort** icon and select **Device Type**.
2. To expand an entry in the device tree, click the expansion arrow to the left of the entry. Only entries that contain branches have expansion arrows. To collapse an entry, click the expansion arrow again.
3. To select an entry, expand the device tree and click the entry you want to select. The main pane shows information in context with the selected entry.
4. To select multiple entries, press the Ctrl key (or Cmd key in Mac OS X) before selecting each entry.
5. To search for an entry by name or IP address, click the **Search** icon beneath the device tree and type the search string in the search box. As you type, a list of matching entries is shown. Continue typing to narrow down the list or move your mouse over the desired entry to highlight it. Once the desired entry is highlighted, click or press Enter to select it.

The device tree expands and highlights the selected entry.

To close the search box, click the **Search** icon again.

6. To collapse the entire tree, click the **Collapse** icon below the device tree.

Component Naming

The proNX Optical Director displays components in the device tree and elsewhere using names that are native to the device being managed. For example, pic:2/0/0 represents a PIC in FPC 2, MIC 0, and PIC 0.

For the TCX Series devices, see [Table 14 on page 52](#) to [Table 17 on page 54](#).

Table 14: TCX1000-RDM20 Component Naming

Component	Name	Description
Device	Assigned by user	This is the name that you configure as part of the system information.
Shelf	TCX1000-RDM20	This is the name used for the TCX1000-RDM20 shelf. There is one shelf per device.
Circuit Pack	roadm:1/1	<p>The ROADM capability in the TCX1000-RDM20 is modeled as a circuit pack using a <chassis>/<index> format.</p> <p>There is one ROADM per shelf. The <chassis> is always 1 and the <index> is always 1.</p>

Table 14: TCX1000-RDM20 Component Naming (continued)

Component	Name	Description
Port	port:1/1/U0-U19	Universal ports for add/drop access and to connect to other ROADM elements within the same ROADM node.
	port:1/1/LINE	Line port for connecting to another ROADM node.
	port:1/1/OSC0	OSC 0 port for add/drop access to one of the two OSC wavelengths. For information on usage, see the TCX1000 Programmable ROADM Hardware Guide.
	port:1/1/OSC1	OSC 1 port for add/drop access to the second of the two OSC wavelengths. For information on usage, see the TCX1000 Programmable ROADM Hardware Guide.
	port:1/1/OSC	OSC port for connecting to the OSC 0 or OSC 1 port to select which OSC wavelength to add/drop. For information on usage, see the TCX1000 Programmable ROADM Hardware Guide.
	port:1/1/ETHCRAFT	Ethernet craft interface for local craft access. For information on usage, see the TCX1000 Programmable ROADM Hardware Guide.
	port:1/1/DCN0-DCN1	DCN ports to connect to the management network.

Table 15: TCX1000-ILA Component Naming

Component	Name	Description
Device	Assigned by user	This is the name that you configure as part of the system information.
Shelf	Chassis	This is the name used for the TCX1000-ILA shelf. There is one shelf per device.
Circuit Pack	ILA	This is the name used for the TCX1000-ILA circuit pack. There is one circuit pack per shelf.
Port	LINE-A	Line port for the span in one direction.
	LINE-B	Line port for the span in the other direction.

Table 16: FMD96 Component Naming

Component	Name	Description
Device	Assigned by user	This is the name of the TCX1000-RDM20 that the multiplexer/demultiplexer belongs to.
Shelf	TCX1000-RDM20	This is the shelf that the multiplexer/demultiplexer belongs to.
Circuit Pack	md:0/<index>	<p>The multiplexer/demultiplexer is modeled as a circuit pack using a <chassis>/<index> format.</p> <p>The <chassis> is always 0 for a passive device. The <index> is the index that you assign when you create the multiplexer/demultiplexer.</p>
Port	port:0/<index>/C1-C96	<p>Client ports for add/drop access to individual wavelengths.</p> <p>Each client port is associated with a specific wavelength. See the TCX1000 Programmable ROADM Hardware Guide for the client port to wavelength mapping.</p>
	port:0/<index>/L1	<p>Line port for connecting to the ROADM device.</p> <p>The FMD96 has a single line port to connect to a single degree.</p>

Table 17: 2D8CMD Component Naming

Component	Name	Description
Device	Assigned by user	This is the name of the TCX1000-RDM20 that the multiplexer/demultiplexer belongs to.
Shelf	TCX1000-RDM20	This is the shelf that the multiplexer/demultiplexer belongs to.
Circuit Pack	cmd:0/<index>	<p>The multiplexer/demultiplexer is modeled as a circuit pack using a <chassis>/<index> format.</p> <p>The <chassis> is always 0 for a passive device. The <index> is the index that you assign when you create the multiplexer/demultiplexer.</p>
Port	port:0/<index>/C0-C7	<p>Client ports for add/drop access to individual wavelengths.</p> <p>The 2D8CMD is 'colorless'. Each client port has access to all wavelengths.</p>
	port:0/<index>/L0-L1	<p>Line ports for connecting to the ROADM devices.</p> <p>The 2D8CMD has two line ports to connect to two degrees.</p>

Creating a New Site

Use this procedure to create a new site. There are different ways to create a new site. This procedure describes how to do this from the Devices Configuration (Sites) page.

1. Click the **Devices** tab, select **Configuration** in the left-nav bar, and sort the device tree by site.


2. Click **New** to create a new site.

The Create a Site window depicting a map of the world appears.




3. To pan around the map, click and hold anywhere in the map background and drag the map until the desired part of the map comes into view.

4. To zoom in and out:

To zoom in, click the  in the lower right corner. Alternatively, you can zoom in by using your mouse scroll wheel.

To zoom out, click the  in the lower right corner. Alternatively, you can zoom out by using your mouse scroll wheel.



NOTE: If you zoom out such that two or more sites are on top of each other, a single  icon is displayed. To see the sites represented by the  icon, click the  icon.

5. To create a new site, click the spot on the map where you want to create the site. For better accuracy, zoom in on the map to get better location resolution.

The New Site dialog appears.

6. Type the **Site Name** of the new site and click **Save**.

The site appears on the map.

7. Repeat steps 5 and 6 to create another site. When you are finished creating sites, click **OK** to close the Create a Site window.

Deleting a Site

Use this procedure to delete a site. There are different ways to delete a site. This procedure describes how to do this from the Devices Configuration (Sites) page.

1. Click the **Devices** tab, select **Configuration** in the left-nav bar, and sort the device tree by site.

2. Select a site from the table of sites and click **Delete**.

You can only delete a site that does not contain any devices.

3. Click **Delete** in the confirmation dialog.

The deleted site is removed from the table of sites and from the device tree.

Site Management

- [About the Site Config Page on page 56](#)
- [Editing a Site's Parameters on page 57](#)
- [About the Site Location Page on page 57](#)
- [Editing a Location Tree on page 58](#)
- [About the Site Devices Page on page 59](#)
- [Viewing the List of Devices at a Site on page 60](#)
- [About the Site Operations Upgrade Page on page 60](#)
- [Upgrading the Software on a Device on page 60](#)
- [About the Site Operations Backup Page on page 60](#)
- [Backing Up the Device Configuration Database on page 61](#)
- [About the Site Operations Restart Page on page 61](#)
- [Restarting All Devices at a Site on page 61](#)
- [About the Site Operations NTP Servers Page on page 62](#)
- [About the Site Operations Date Time Page on page 62](#)

About the Site Config Page

To access this page, click the **Devices** tab and select **Configuration** in the left-nav bar. Then sort the device tree by site and click the site that you want to edit. By default, this page starts in the Config tab.

The Site Config page displays information for the selected site. A site represents a geographic location shared by colocated devices.

Tasks You Can Perform

You can edit or delete the selected site from this page.

Field Descriptions

[Table 18 on page 56](#) explains the fields in the Site Config page.

Table 18: Fields on the Site Config Page

Field	Description
Site Name	The site's name. This name must be unique.

Table 18: Fields on the Site Config Page (continued)

Field	Description
Latitude	The site's latitude in degrees. This can only be edited if the site does not contain any devices.
Longitude	The site's longitude in degrees. This can only be edited if the site does not contain any devices.
Contact	The site's contact information. Enter the contact information for the person administering the site. This is optional.
Address	The site's civic address. Enter the address of the site. This is optional.
Description	A description of the site. Add text to further describe the site. This is optional.

Editing a Site's Parameters

Use this procedure to edit an existing site's parameters.

1. Click the **Devices** tab, select **Configuration** in the left-nav bar, and sort the device tree by site. Then, click the site you want to edit.
2. Edit the site's parameters as desired by clicking inside each text box and typing the new string. See [Table 18 on page 56](#) for a description of the parameters.
3. To save your changes, click **Save**.
4. To discard your changes, click **Reset**.
5. To delete the site, click **Delete**. You can only delete a site if the site does not contain any devices.

See Also • [Creating a New Site on page 55](#)

About the Site Location Page

To access this page, click the **Devices** tab and select **Configuration** in the left-nav bar. Then sort the device tree by site, click the site that you want to edit, and select the **Location** tab.

The Site Location page displays the location tree for the selected site. The location tree is optional and provides a structured way for you to specify additional location information (such as building, room, and rack) for devices at a site. Once you set up the tree, you can associate devices to a location in the location tree during device discovery. After you discover the device, the location information is shown as a text string in the Device Config page (see [“About the Device Config Page” on page 63](#)).

Tasks You Can Perform

You can edit the location tree for the selected site.

Field Descriptions

Table 19 on page 58 explains the location tree hierarchy in the Site Location page.

Table 19: Location Tree Hierarchy on the Site Location Page

Field	Description
Site	The name of the site.
Building	The name of the building.
Room	The name of the room.
Rack	The name of the rack.

Editing a Location Tree

Use this procedure to edit a location tree for a site. Every site has a default location tree that you can edit to serve your needs.

1. Click the **Devices** tab and select **Configuration** in the left-nav bar. Then sort the device tree by site, click the site that you want to edit, and select the **Location** tab.

The location tree appears. If this is the first time you are editing the location tree for this site, the default tree is shown.

2. To expand or hide location information for branches beneath a node in the tree, double-click the box at that node.
3. To add a building to a site:
 - a. Select the site box and click **New**.

The Create New Building dialog appears.
 - b. Enter the **Name** of the building and click **Submit**.

The dialog closes and the building you just added is shown in the location tree under the site.
 - c. When you add a building, a default room and rack are added as well. Double-click the building to see the default room and rack.
4. To add a room to a building:
 - a. Select the building box and click **New**.

The Create New Room dialog appears.
 - b. Enter the **Name** of the room and click **Submit**.

The dialog closes and the room you just added is shown in the location tree under the building.

- c. When you add a room, a default rack is added as well. Double-click the room to see the default rack.

5. To add a rack to a room:

- a. Select the room box and click **New**.

The Create New Rack dialog appears.

- b. Enter the **Name** of the rack and click **Submit**.

The dialog closes and the rack you just added is shown in the location tree under the room.

6. To edit the name of a building, room, or rack, select the building, room, or rack and click **Edit**.

Change the **Name** in the ensuing dialog and click **Submit**

7. To delete a building, room, or rack, select the building, room, or rack and click **Delete**.

You cannot delete the last rack in a room or the last room in a building, nor can you delete the building that is part of the default tree.

8. Click **Save** to save your changes.

About the Site Devices Page

To access this page, start from the Devices Configuration page, categorize the device tree by site, and click the site that you want to edit. This places you in the Site Config page. From here, select the **Devices** tab.

The Site Devices page lists the devices found at the selected site.

Tasks You Can Perform

You can view the list of devices found at the selected site.

Field Descriptions

Table 20 on page 59 explains the fields in the Site Devices page.

Table 20: Fields in the Site Devices Page

Field	Description
Device	The IP address of the device.
Model	The model or device type.
Vendor	The vendor of the device.

Table 20: Fields in the Site Devices Page (continued)

Field	Description
Software Version	The software version that the device is running.

Viewing the List of Devices at a Site

Use this procedure to view the list of devices at a site.

1. Start from the Devices Configuration page, categorize the device tree by site, click the site that you want to view, and select the **Devices** tab.

A table displaying the list of devices found at the site is shown. See [Table 20 on page 59](#) for an explanation of the table headings.

2. To search, copy, print, or save the table, see [“Working with Tables” on page 22](#).

About the Site Operations Upgrade Page

To access this page, start from the Devices Configuration page, categorize the device tree by site, and click the site that you want to edit. This places you in the Site Config page. From here, select **Operations>Upgrade**.

The Site Operations Upgrade page is where you go to simultaneously upgrade the software of all devices at a site.

Tasks You Can Perform

If all the devices at the site are of the same type, then you can perform a software upgrade on all devices at the selected site simultaneously. If the devices are not all of the same type, or if you only want to perform a software upgrade on a subset of devices, see [“About the Device Operations Upgrade Page” on page 79](#).

Field Descriptions

See [“Field Descriptions” on page 79](#).

Upgrading the Software on a Device

See [“Upgrading the Software on a Device” on page 81](#).

About the Site Operations Backup Page

To access this page, start from the Devices Configuration page, categorize the device tree by site, and click the site that you want to back up. This places you in the Site Config page. From here, select **Operations>Backup**.

The Site Operations Backup page displays the list of devices that you can back up from the selected site.

Tasks You Can Perform

You can back up the configuration database for all devices found at the selected site. If you only want to back up a subset of devices at the selected site, see [“About the Device Operations Backup Page”](#) on page 82.



NOTE: You can only back up devices that support the same file transfer protocol (FTP or SFTP). If some devices at the site can only use FTP while others can only use SFTP, then you must back up these devices separately.

Field Descriptions

See [“Field Descriptions”](#) on page 82.

Backing Up the Device Configuration Database

See [“Backing Up the Device Configuration Database Manually”](#) on page 84.

About the Site Operations Restart Page

To access this page, start from the Devices Configuration page, categorize the device tree by site, and click the site that you want to restart. This places you in the Site Config page. From here, select **Operations>Restart**.

The Site Operations Restart page displays the list of devices that you can reboot from the selected site starting in release 18.4.

Tasks You Can Perform

You can perform a warm or cold reboot of all devices at the selected site. If you only want to reboot a subset of devices at the selected site, see [“About the Device Operations Restart Page”](#) on page 87.



NOTE: You can reboot all devices at a site only if all devices support the type of restart that you want to perform.

Field Descriptions

See [“Field Descriptions”](#) on page 87.

Restarting All Devices at a Site

See [“Restarting a Device”](#) on page 88.

About the Site Operations NTP Servers Page

To access this page, start from the Devices Configuration page, categorize the device tree by site, and click the site that you want to back up. This places you in the Site Config page. From here, select **Operations>Set NTP Servers**.

The Site Operations NTP Servers page displays the list of devices that you can back up from the selected site.

Tasks You Can Perform

You can back up the configuration database for all devices found at the selected site. If you only want to back up a subset of devices at the selected site, see [“About the Device Operations Backup Page” on page 82](#).



NOTE: You can only back up devices that support the same file transfer protocol (FTP or SFTP). If some devices at the site can only use FTP while others can only use SFTP, then you must back up these devices separately.

Field Descriptions

See [“Field Descriptions” on page 82](#).

About the Site Operations Date Time Page

To access this page, start from the Devices Configuration page, categorize the device tree by site, and click the site that you want to back up. This places you in the Site Config page. From here, select **Operations>Set Date and Time**.

The Site Operations Date Time page displays the list of devices that you can back up from the selected site.

Tasks You Can Perform

You can back up the configuration database for all devices found at the selected site. If you only want to back up a subset of devices at the selected site, see [“About the Device Operations Backup Page” on page 82](#).



NOTE: You can only back up devices that support the same file transfer protocol (FTP or SFTP). If some devices at the site can only use FTP while others can only use SFTP, then you must back up these devices separately.

Field Descriptions

See [“Field Descriptions” on page 82](#).

Device Management

- [About the Device Config Page on page 63](#)
- [Editing a Device's Parameters on page 64](#)
- [About the Device NTP Servers Page on page 65](#)
- [Viewing the NTP Server List on page 66](#)
- [Adding an NTP Server to the NTP Server List on page 66](#)
- [Deleting an NTP Server from the NTP Server List on page 67](#)
- [Enabling or Disabling NTP Servers on page 68](#)
- [About the Device Datetime Page on page 68](#)
- [Setting the Date and Time on page 69](#)
- [About the Device Security Page on page 69](#)
- [Adding or Deleting a RADIUS Server or Changing the RADIUS Security Options on page 70](#)
- [About the Device Chassis View Page on page 71](#)
- [Navigating the Chassis View Page on page 72](#)
- [About the Device Operations View Logs Page on page 74](#)
- [Viewing Logs for a Device on page 75](#)
- [Log Collection on page 76](#)
- [Metric Collection on page 77](#)
- [About the Device Operations Upgrade Page on page 79](#)
- [Upgrading the Software on a Device on page 81](#)
- [About the Device Operations Backup Page on page 82](#)
- [Device Configuration Database Backups on page 83](#)
- [About the Device Operations Restore Page on page 85](#)
- [Restoring the Device Configuration Database on page 86](#)
- [About the Device Operations Restart Page on page 87](#)
- [Restarting a Device on page 88](#)
- [Restoring a Device to Factory Defaults on page 88](#)

About the Device Config Page

To access this page, start from the Devices Configuration page, expand the device tree to see the list of devices, and click the device that you want to edit. By default, this page starts in the Config tab.

The Device Config page displays system information for the selected device.

Tasks You Can Perform

You can view and edit information for the selected device from this page.

Field Descriptions

Table 21 on page 64 explains the fields in the Device Config page.

Table 21: Fields on the Device Config Page

Field	Description
Name	The device's name. This name does not need to be unique.
IP Address	The device's IP address. This is read-only.
Location	The device's location. This is optional.
Uptime	The time since the last device restart. This is read-only.
Software Version	The software version running on the device. This is read-only.
Model	The device model or type. This is read-only.
Contact	The device's contact information. Enter the contact information for the person administering the device. This is optional.
Physical Location	The device's physical location as specified in the location tree. This is read-only.

Editing a Device's Parameters

This procedure applies to the following devices:

- ACX6360
- BTI7800 devices
- MX Series routers
- PTX Series routers
- QFX Series switches
- TCX1000-ILA
- TCX1000-RDM20

Use this procedure to edit the system information for a device.

1. Start from the Devices Configuration page, expand the device tree to see the list of devices, and click the device that you want to edit.
2. Edit the device's parameters as desired by clicking inside each text box and typing the new string. See [Table 21 on page 64](#) for a description of the parameters.

3. To save your changes, click **Save**.
4. To discard your changes, click **Reset**.

About the Device NTP Servers Page

To access this page, start from the Devices Configuration page, expand the device tree to see the list of devices, and click the device that you want to edit. From here, select the **Date Time>NTP** tab.



NOTE: If the NTP selection does not appear for the device that you select, you cannot use the proNX Optical Director to configure NTP for that device.

The Device NTP Servers page displays the NTP servers that the selected device is configured to use. To ensure proper timestamps on performance monitoring metrics (PMs), all managed devices must be configured to use NTP servers.

Tasks You Can Perform

You can perform the following actions on this page:

- View the list of NTP servers that the device is currently using.
- Specify a new NTP server for the device.
- Remove an existing NTP server from the list of servers that the device is using.

Field Descriptions

Table 22 on page 65 explains the fields in the Device NTP Servers page.

Table 22: Fields in the Device NTP Servers Page

Field	Description
IP Address	The IP address of the NTP server.
Port	The protocol port to use. This field is hardcoded to the standard port 123 and cannot be changed.
Preferred	An indication of whether the specified server is preferred. A preferred NTP server is used before an NTP server that is not preferred.
State	Specify whether use of NTP servers is enabled or disabled.

Viewing the NTP Server List

This procedure applies to the following devices:

- ACX6360
- BT17800 devices
- MX Series routers
- PTX Series routers
- QFX Series switches
- TCX1000-ILA
- TCX1000-RDM20

Use this procedure to view the list of NTP servers that the selected device is configured to use.

1. Start from the Devices Configuration page, expand the device tree to see the list of devices, and click the device that you want to edit. From here, select the **Date Time>NTP** tab.

A table displaying the list of NTP servers is displayed. See [Table 22 on page 65](#) for an explanation of the fields.

2. To search, copy, print, or save the table, see [“Working with Tables” on page 22](#).

Adding an NTP Server to the NTP Server List

This procedure applies to the following devices:

- ACX6360
- BT17800 devices
- MX Series routers
- PTX Series routers
- QFX Series switches
- TCX1000-ILA
- TCX1000-RDM20

Use this procedure to add an NTP server to the list.

1. Start from the Devices Configuration page, expand the device tree to see the list of devices, and click the device that you want to edit. From here, select the **Date Time>NTP** tab.

A table displaying the list of NTP servers is displayed.

2. Click **New** to add an NTP server to this list. The Create a New NTP Server dialog appears.

3. Specify the IPv4 or IPv6 **IP address** of the server you want to add.
4. Specify whether the server is **Preferred** or not.
5. Click **Add** to add the specified NTP server.

The dialog closes and the server you just specified is shown in the NTP server list.

6. To save and activate your changes, click **Save**.
7. To discard your changes, click **Reset**.

Deleting an NTP Server from the NTP Server List

This procedure applies to the following devices:

- ACX6360
- BT17800 devices
- MX Series routers
- PTX Series routers
- QFX Series switches
- TCX1000-ILA
- TCX1000-RDM20

Use this procedure to delete an NTP server from the list.

1. Start from the Devices Configuration page, expand the device tree to see the list of devices, and click the device that you want to edit. From here, select the **Date Time>NTP** tab.
A table displaying the list of NTP servers is displayed.
2. Select the NTP server you want to delete and click **Delete**.
3. To save and activate your changes, click **Save**.
4. To discard your changes, click **Reset**.

Enabling or Disabling NTP Servers

This procedure applies to the following devices:

TCX1000-RDM20

Use this procedure to enable or disable the use of NTP servers for a device.

1. Start from the Devices Configuration page, expand the device tree to see the list of devices, and click the device that you want to edit. From here, select the **Date Time>NTP** tab.

A list of NTP servers is displayed.

2. To enable the use of NTP servers, select **Enabled** from the **State** drop-down list.
3. To disable the use of NTP servers, select **Disabled** from the **State** drop-down list.
4. To save and activate your changes, click **Save**.
5. To discard your changes, click **Reset**.

About the Device Datetime Page

To access this page, start from the Devices Configuration page, expand the device tree to see the list of devices, and click the device that you want to edit. From here, select the **Date Time>Manual** tab.

The Device Datetime page displays the dialog where you set the date and time on the device.

Tasks You Can Perform

You can perform the following actions on this page:

- Change the date on the device.
- Change the time on the device.



NOTE: If the device is configured to use NTP servers, then using this page to change the date or time has no effect.

Field Descriptions

Table 23 on page 69 explains the fields in the Device Datetime page.

Table 23: Fields in the Device Datetime Page

Field	Description
Date	The date on the device.
Time	The time on the device.

Setting the Date and Time

This procedure applies to the following devices:	ACX6360
	MX Series routers
	PTX Series routers
	QFX Series switches
	TCX1000-ILA
	TCX1000-RDM20

Use this procedure to manually set the date and time on a device.

1. Start from the Devices Configuration page, expand the device tree to see the list of devices, and click the device that you want to edit. From here, select the **Date Time>Manual** tab.
2. Click the calendar icon to set the date.
3. Use the arrows to set the hour and minute. The time is specified in 24-hour format.
4. Click **Save**.



NOTE: If the device is configured to use NTP servers, then using this page to change the date or time has no effect.

About the Device Security Page

To access this page, start from the Devices Configuration page, expand the device tree to see the list of devices, and click the device that you want to edit. From here, select the **Security** tab.

The Device Security page displays the RADIUS servers that the selected device is configured to use.

Tasks You Can Perform

You can perform the following actions on this page:

- View the list of RADIUS servers that the device is currently using.
- Specify a new RADIUS server for the device.
- Remove an existing RADIUS server from the list of servers that the device is using.

Field Descriptions

Table 24 on page 70 explains the fields in the Device Security page.

Table 24: Fields in the Device Security Page

Field	Description
Server Name	The name of the RADIUS server
IP Address	The IP address of the RADIUS server
Authentication Port	The protocol port to use

Adding or Deleting a RADIUS Server or Changing the RADIUS Security Options

This procedure applies to the following devices:	BTI7800 Series devices
	MX Series routers
	PTX Series routers
	QFX Series switches
	TCX1000-ILA
	TCX1000-RDM20

NOTE: The TCX1000-ILA supports a maximum of two RADIUS servers.

Use this procedure to add or delete a RADIUS server to or from the list of RADIUS servers that the device is using, or to change the RADIUS security options. The RADIUS security options specify how long to wait for a response from a RADIUS server and how many times to attempt contact.

1. Start from the Devices Configuration page, expand the device tree to see the list of devices, and click the device that you want to edit. From here, select the **Security** tab.
2. To add a new RADIUS server:

- a. Click **New**. The Create a New Security Server dialog appears.
 - b. Use the drop-down list to select the RADIUS server you want to add. You can only add servers that have been created in **Administration > Security**. See [“Security” on page 157](#) for information on using remote authentication.
 - c. Enter the shared secret. This is the shared secret between the selected device (RADIUS client) and the RADIUS server.
 - d. Click **Add**. The Create a New Security Server dialog closes and the added server is shown in the list of servers.
 - e. Set the **Attempts** and **Timeout**. These attributes apply to all servers in the list. For information on how these attributes are used, see [“Authentication Process” on page 159](#).
 - f. Click **Save**.
3. To change the RADIUS security options, set the **Attempts** and **Timeout** and click **Save**.
The RADIUS security options apply to all servers in the authentication server list and only appear if there is at least one server in the list. For information on how these attributes are used, see [“Authentication Process” on page 159](#).
 4. To delete a RADIUS server from the list:
 - a. Select the RADIUS server you want to delete.
 - b. Click **Delete**. The deleted server is removed from the list of servers.
 - c. Click **Save**.

About the Device Chassis View Page

To access this page, start from the Devices Configuration page, expand the device tree to see the list of devices, and click the device that you want to view. From here, select the **Chassis View** tab.

The Device Chassis View page displays a visual representation of the selected device along with information on the device, circuit packs, and ports. You have a choice of multiple views.

Tasks You Can Perform

You can see a visual representation of the selected device:

- front, rear, and rotatable perspective views
- device, circuit pack, and port information

Field Descriptions

The Chassis View page depicts a visual representation of the selected device.

Navigating the Chassis View Page

This procedure applies to the following devices:	ACX6360
	BT17800 devices
	MX Series routers
	PTX Series routers
	QFX Series switches
	TCX1000-ILA
	TCX1000-RDM20

NOTE: The BT17800 Series devices support the front and rear views only.


Use this procedure to navigate the Chassis View page.


1. Start from the Devices Configuration page, expand the device tree to see the list of devices, and click the device that you want to view. From here, select the **Chassis View** tab.



A visual representation of the selected device appears.

2. To pan around the chassis view, click and hold anywhere in the background and drag until the desired part of the chassis comes into view.

3. To zoom in and out:

To zoom in, click the  in the lower right corner. Alternatively, you can zoom in by double clicking anywhere in the map background or by using your mouse scroll wheel.

To zoom out, click the  in the lower right corner. Alternatively, you can zoom out by using your mouse scroll wheel.

4. Use your mouse to hover over different components to see the names of the components.
5. Click the  icon in the top right corner and select from the following views:
 - Pan-Zoom Front View
 - Pan-Zoom Rear View
 - Perspective View
6. To rotate the device in perspective view, click the  icon in the lower right corner.
7. To see information on the device, click the device.



The device information window appears displaying some or all of the following information:



NOTE: Information displayed varies per device.

- Device type
- IP address
- Alarms (with an indication of the number of alarms at each severity for that device)
- Product code
- Model number
- Hardware version
- Manufacture date
- Description

Additionally, you can navigate to the following pages:

- To go to the Device Config page, click the  icon.
 - To go to the Inventory page filtered for the IP address of the device, click the  icon.
8. To see information on a circuit pack, click the circuit pack.

A circuit pack information window appears displaying some or all of the following information:



NOTE: Information displayed varies per device.

- Type of circuit pack
 - Alarms (with an indication of the number of alarms at each severity for that circuit pack)
 - Product code
 - CLEI code
 - Hardware version
9. To see information on a port, click the port.

A port information window appears displaying some or all of the following information:






NOTE: Information displayed varies per port type.

- Port name
- Alarms (with an indication of the number of alarms at each severity for that port)

- Interface name along with administrative state and operational status
- Port type

Additionally, you can navigate to the following pages for some ports. If the respective icon does not appear in the port information window, then the feature is not supported for that port.

- To go to the Devices Port Config page, click the  icon.
 - To go to the Devices Port Thresholds page, click the  icon.
 - To go to the Devices Port Metrics page, click the  icon.
10. To reset the chassis view, click the **Reset** icon.

About the Device Operations View Logs Page

To access this page, start from the Devices Configuration page, expand the device tree to see the list of devices, and click the device that you want to view. From here, select **Operations>View Logs**.

The Device Operations View Logs page displays the logs that have been collected for the selected device.

Tasks You Can Perform

You can perform the following actions on this page:

- View the logs collected for the specified device.
- Launch the Kibana data visualization tool to further analyze the logs.

Field Descriptions

Table 25 on page 74 explains the fields in the Device Operations View Logs page.

Table 25: Fields in the Device Operations View Logs Page

Field	Description
Timestamp	The timestamp of the log record.
Facility	<p>The facility of the log record.</p> <p>The TCX1000-RDM20 devices support the following values:</p> <ul style="list-style-type: none"> • equipment • netconf • oamevent
Level	<p>The severity level of the log record.</p> <p>The TCX1000-RDM20 devices support the following values:</p> <ul style="list-style-type: none"> • info

Table 25: Fields in the Device Operations View Logs Page (continued)

Field	Description
Event Type	<p>The type of event.</p> <p>The TCX1000-RDM20 devices support the following values:</p> <ul style="list-style-type: none"> • restart • alarm-notification • maint-state-change - a change in the administrative state
Message	A description of the event.
<p>NOTE: These fields are device-specific. Not all devices supply information for all fields. Fields that have no information supplied are left empty.</p>	

Viewing Logs for a Device

This procedure applies to the following devices:

- ACX6360
- BTI7800 devices
- MX Series routers
- PTX Series routers
- QFX Series switches
- TCX1000-ILA
- TCX1000-RDM20

Prerequisites

- You have collected log records for the device. See [“Log Collection” on page 76](#).

Use this procedure to view the collected logs for a device.

1. Start from the Devices Configuration page, expand the device tree to see the list of devices, and click the device that you want to view. From here, select the **Operations>View Logs** tab.

A table displaying the log records for the selected device is displayed. See [Table 25 on page 74](#) for an explanation of the fields.

2. To view details of a specific log record, select the log record and click **View**. The selected log record appears in a new window.
3. To view logs using Kibana, click **Analyze**.



NOTE: How to use of Kibana is outside the scope of this document.

4. To search, copy, print, or save the table, see [“Working with Tables” on page 22](#).

Log Collection

The proNX Optical Director collects logs from managed devices automatically on a predefined schedule. The proNX Optical Director also supports manual log collection on demand.

For both automated and manual log collection, the proNX Optical Director collects log files from most devices directly, but for some devices, the proNX Optical Director uses a file server for intermediate staging of log files.

Specifically, the TCX1000-ILA and BT17800 devices require the use of a file server for transfer and temporary storage of log files. Once the log file is uploaded to the file server by the device, the proNX Optical Director collects and then deletes the log file from the file server. The file server used for this purpose is configured to be the default SFTP Staging server. You configure a file server to be the default SFTP Staging server when you add (or edit) the file server. Once you configure the default SFTP Staging server, the use of this server for intermediate staging is transparent to the user.

For information on adding a file server, see [“Adding a File Server to the File Server List” on page 156](#). If you do not configure any file server to be the default SFTP Staging server, then automated and manual log collection cannot be run for the TCX1000-ILA and BT17800 devices.

Automated Log Collection

By default, the proNX Optical Director automatically collects logs from all devices in the network every 12 hours, which allows you time to correct any retrieval failures while minimizing unnecessary processing.

The log collection schedule is specified by the `JOC_LOG_COLLECTION_CRON` variable in the `/etc/kubernetes/apps/joc/joc-config-map.yml` file on the master node. For example:

```
JOC_LOG_COLLECTION_CRON: "0 15 1,13 * * ?"
```

The scheduling format is based on the Quartz scheduler and is explained in [Table 26 on page 76](#).

Table 26: JOC_LOG_COLLECTION_CRON Field Description

Fields						Meaning
seconds	minutes	hours	day	month	day of week	
0	15	1,13	*	*	?	Every day of every month at 1:15:00 and 13:15:00



NOTE: Changing the collection schedule is beyond the scope of this document.

Collecting Logs from a Device Manually

This procedure applies to the following devices:	ACX6360
	BT17800 devices
	MX Series routers
	PTX Series routers
	QFX Series switches
	TCX1000-ILA
	TCX1000-RDM20

NOTE: For the TCX1000-ILA and BT17800 devices, you must configure a default SFTP Staging server in the file server list before you can use this procedure. See [“Log Collection” on page 76](#).

Use this procedure to collect logs on demand from the specified device.

1. Start from the Devices Configuration page, expand the device tree to see the list of devices, and click the device that you want to view. From here, select **Operations>Collect Logs**.

The proNX Optical Director retrieves logs from the selected device. Depending on the amount of logs, this might take a few minutes to complete. You can monitor progress by viewing the task. See [“Viewing the Tasks List” on page 147](#).

Once the task completes, follow the procedure described in [“Viewing Logs for a Device” on page 75](#) to view the logs.

Metric Collection

The proNX Optical Director collects historical performance monitoring metrics (PMs) from managed devices automatically on a predefined schedule. The proNX Optical Director also supports manual metric collection on demand.

Historical PMs are PMs that are collected and binned (aggregated over a measurement interval, timestamped, and discretely stored) by the device.

For both automated and manual metric collection, the proNX Optical Director collects metrics from most devices directly, but for some devices, the proNX Optical Director uses a file server for intermediate staging of metric files.

Specifically, the TCX1000-ILA and BT17800 devices require the use of a file server for transfer and temporary storage of metric files. Once the metric file is uploaded to the file server by the device, the proNX Optical Director collects and then deletes the metric file from the file server. The file server used for this purpose is configured to be the default

SFTP Staging server. You configure a file server to be the default SFTP Staging server when you add (or edit) the file server. Once you configure the default SFTP Staging server, the use of this server for intermediate staging is transparent to the user.

For information on adding a file server, see [“Adding a File Server to the File Server List” on page 156](#). If you do not configure any file server to be the default SFTP Staging server, then automated and manual metric collection cannot be run for the TCX1000-ILA and BT17800 devices.

Automated Metric Collection

By default, the proNX Optical Director automatically collects historical performance monitoring metrics (PMs) from all devices in the network every 12 hours, which allows you time to correct any retrieval failures while minimizing unnecessary processing.

The metric collection schedule is specified by the `JOC_METRIC_COLLECTION_CRON` variable in the `/etc/kubernetes/apps/joc/joc-config-map.yml` file on the master node. For example:

```
JOC_METRIC_COLLECTION_CRON: "0 20 1,13 * * ?"
```

The scheduling format is based on the Quartz scheduler and is explained in [Table 27 on page 78](#).

Table 27: JOC_METRIC_COLLECTION_CRON Field Description

Fields						Meaning
seconds	minutes	hours	day	month	day of week	
0	20	1,13	*	*	?	Every day of every month at 1:20:00 and 13:20:00



NOTE: Changing the collection schedule is beyond the scope of this document.

Collecting Metrics from a Device Manually

This procedure applies to the following devices:	ACX6360
	BT17800 devices
	MX Series routers
	PTX Series routers
	QFX Series switches
	TCX1000-ILA
	TCX1000-RDM20

NOTE: For the TCX1000-ILA and BT17800 devices, you must configure a default SFTP Staging server in the file server list before you can use this procedure. See [“Metric Collection” on page 77](#).

Use this procedure to collect historical performance monitoring metrics (PMs) on demand from the specified device.

1. Start from the Devices Configuration page, expand the device tree to see the list of devices, and click the device that you want to view. From here, select **Operations>Collect Metrics**.

The proNX Optical Director retrieves metrics from the selected device. Depending on the amount of data, this might take a few minutes to complete. You can monitor progress by viewing the task. See [“Viewing the Tasks List” on page 147](#).

Once the task completes, follow the procedure described in [“Viewing Historical Performance Monitoring Metrics” on page 105](#) to view the metrics.

About the Device Operations Upgrade Page

To access this page, start from the Devices Configuration page, expand the device tree to see the list of devices, and click the device that you want to upgrade. From here, select **Operations>Upgrade**.

The Device Operations Upgrade page is used to perform a software upgrade on the selected device.

Tasks You Can Perform

You can perform a software upgrade on the selected device.

Field Descriptions

The following table explains the fields in the Device Operations Upgrade page and in the Site Operations Upgrade page.

Table 28: Fields in the Device or Site Operations Upgrade Page

Field	Description
Device	See Table 20 on page 59 .
Model	See Table 20 on page 59 .
Vendor	See Table 20 on page 59 .
Software Version	See Table 20 on page 59 .
File Server	The file server where you can download the software from.
Software	The file name of the software package you want to download.

Upgrading the Software on a Device

This procedure applies to the following devices starting in release 2.2:

- BT17800 devices
- TCX1000-ILA
- TCX1000-RDM20

This procedure applies to the following devices starting in (proNX Optical Director) release 18.4:

- MX Series routers
- PTX Series routers

NOTE: VMHost software image upgrades are not supported for any device.

Use this procedure to perform a software upgrade on one or more devices or on all devices within a site.

1. Select the device or site that you want to upgrade.
 - To upgrade a specific device, start from the Devices Configuration page, expand the device tree to see the list of devices, and click the device that you want to upgrade.

To select multiple devices to upgrade, once you select a single device, use the Ctrl key (Cmd key in Mac OS X) to multi-select other devices. Only select devices that are of the same type.

After you pick your device or devices, select **Operations>Upgrade**.
- To upgrade all devices at a site, start from the Devices Configuration page, categorize the device tree by site, click the site that you want to upgrade, and select **Operations>Upgrade**. You can only upgrade all devices at a site if all devices are of the same type.

The Software Upgrade page appears displaying the list of devices that you are upgrading.

2. Select the file server where you want to download the software package from. If the file server that you want to use is not listed, you have to add it first. See [“Adding a File Server to the File Server List” on page 156](#).



NOTE: If the device that you want to upgrade only supports FTP, then only FTP servers are listed. If your device only supports SFTP, then only SFTP servers are listed. TCX1000 Series devices only support SFTP.

3. Click **Browse** to browse the files on the file server. By default, you are placed into the directory that you specified when you added the file server.

Browse to the software load you want to use and click **Select**.

4. To stage the software load, select **Stage**. This downloads the software load to the device.



NOTE: If you are staging software on a TCX1000-RDM20 device and you encounter an error, select **Device Reset** to reset the software upgrade state machine and then **Stage** the software load again. This reset does not affect traffic.

5. To activate the software load, select **Activate**.

About the Device Operations Backup Page

To access this page, start from the Devices Configuration page, expand the device tree to see the list of devices, and click the device that you want to back up. From here, select **Operations>Backup**.

The Device Operations Backup page is used to back up the configuration database from the specified device or devices.

Tasks You Can Perform

You can back up the configuration database from a specific device or devices.

Field Descriptions

The following table explains the fields in the Device Operations Backup page and the Site Operations Backup page.

Table 29: Fields in the Device or Site Operations Backup Page

Field	Description
Device	See Table 20 on page 59 .
Model	See Table 20 on page 59 .
Vendor	See Table 20 on page 59 .
Software Version	See Table 20 on page 59 .
File Server	<p>The file server where you want to upload the backed-up configuration database.</p> <p>NOTE: If you are manually backing up multiple devices and some devices only support FTP while others only support SFTP, then you will not be able to select a file server. You will need to run the backup twice, once for FTP devices and once for SFTP devices.</p>
Backup File	<p>The backup file name suffix.</p> <p>The backup file name is automatically constructed from the device's IP address followed by the specified suffix, as shown:</p> <p><device-ip>-<suffix></p>

Device Configuration Database Backups

The proNX Optical Director backs up the configuration database from managed devices automatically on a predefined schedule. The proNX Optical Director also supports manual backups on demand.

Both automated and manual backups require the use of a file server to store the backup files.

Furthermore, automated backups require you to configure one of the file servers to be the default Backup server. If you do not configure any file server to be the default Backup server, then automated backups cannot be run.

Manual backups do not require you to set up a default Backup server because you select the server explicitly as part of the manual backup procedure.

Automated Device Configuration Database Backups

By default, the proNX Optical Director automatically backs up the configuration of all devices in the network once a day. For devices that support FTP, the backup files are uploaded to the default FTP Backup server. For devices that support SFTP, the backup files are uploaded to the default SFTP Backup server.

You configure a file server to be the default when you add the file server. For information on adding a file server, see [“Adding a File Server to the File Server List” on page 156](#).

If you do not configure any file server to be the default backup server, then automated backups do not run.

The backup schedule is specified by the `JOC_DEVICE_BACKUP_CRON` variable in the `/etc/kubernetes/apps/joc/joc-config-map.yml` file on the master node. For example:

```
JOC_DEVICE_BACKUP_CRON: "0 15 04 * * ?"
```

The scheduling format is based on the Quartz scheduler and is explained in [Table 30 on page 83](#)).

Table 30: JOC_DEVICE_BACKUP_CRON Field Description

Fields						Meaning
seconds	minutes	hours	day	month	day of week	
0	15	04	*	*	?	Every day of every month at 04:15:00



NOTE: Changing the backup schedule is beyond the scope of this document.

Backing Up the Device Configuration Database Manually

This procedure applies to the following devices:

- ACX6360
- BT17800 devices
- MX Series routers
- PTX Series routers
- QFX Series switches
- TCX1000-ILA
- TCX1000-RDM20

Use this procedure to manually back up the configuration database from one or more devices or from all devices within a site.

1. Select the device or site that you want to back up.
 - To back up a device, start from the Devices Configuration page, expand the device tree to see the list of devices, and click the device that you want to back up.

To select multiple devices to back up, once you select a single device, use the Ctrl key (Cmd key in Mac OS X) to multi-select other devices. Select only devices that can support the same file transfer protocol (FTP or SFTP). If some selected devices can only use FTP while others can only use SFTP, then you must run the backup twice, once for FTP devices and once for SFTP devices.

After you pick your device or devices, select **Operations>Backup**.
 - To back up all devices at a site, start from the Devices Configuration page, categorize the device tree by site, click the site that you want to back up, and select **Operations>Backup**. You can only back up all devices at a site if they all support the same file transfer protocol.

The Backup page appears.

2. Select the file server where you want to upload the backed-up configuration database. If the file server that you want to use is not listed, you have to add it first. See [“Adding a File Server to the File Server List” on page 156](#).



NOTE: If the device that you want to back up only supports FTP, then only FTP servers are listed. If your device only supports SFTP, then only SFTP servers are listed. TCX1000 Series devices only support SFTP.

3. In the Select Backup Directory and File text box, click **Browse** to specify the file name suffix and the directory that you want to use, or use the suggested suffix.
4. To start the backup, select **Backup**.

The device configurations for the selected devices are backed up to the file server.

About the Device Operations Restore Page

To access this page, start from the Devices Configuration page, expand the device tree to see the list of devices, and click the device that you want to restore. From here, select **Operations>Restore**.

The Device Operations Restore page is used to restore the configuration database from a backup.

Tasks You Can Perform

You can restore the configuration database from a backup.

Field Descriptions

Table 31 on page 85 explains the fields in the Device Operations Restore page.

Table 31: Fields in the Device Operations Restore Page

Field	Description
File Server	The file server where you can retrieve the backed-up configuration database.
Restore File	The name of the backup to restore.

Restoring the Device Configuration Database

This procedure applies to the following devices:	ACX6360
	BT17800 devices
	MX Series routers
	PTX Series routers
	QFX Series switches
	TCX1000-ILA
	TCX1000-RDM20

NOTE: When restoring a configuration database to an ACX6360 router or transponder or MX Series or PTX Series router or QFX Series switch, the prnX Optical Director downloads the configuration to the device as the candidate version. The prnX Optical Director does not perform the commit. You have to log in to the device CLI to perform the commit.

Use this procedure to restore the configuration database from a backup.

1. Select the device to which you want to restore the database. Start from the Devices Configuration page, expand the device tree to see the list of devices, and click the device that you want to restore. From here, select **Operations>Restore**.

The Restore page appears.

2. Select the file server where you want to retrieve the backup from. If the file server that you want to use is not listed, you have to add it first. See [“Adding a File Server to the File Server List” on page 156](#).



NOTE: If the device that you want to restore only supports FTP, then only FTP servers are listed. If your device only supports SFTP, then only SFTP servers are listed. TCX1000 Series devices only support SFTP.

3. Click **Browse** to browse the files on the file server. By default, you are placed into the directory that you specified when you added the file server.

Browse to the backup configuration file you want to restore and click **Select**.

4. To start the restore, select **Restore**.

About the Device Operations Restart Page

To access this page, start from the Devices Configuration page, expand the device tree to see the list of devices, and click the device that you want to restart. From here, select **Operations>Restart**.

The Device Operations Restart page is used to perform a warm or cold reboot of a device starting in release 18.4.

Tasks You Can Perform

You can perform a warm or cold reboot of the selected device.

Field Descriptions

Table 32 on page 87 explains the fields in the Device Operations Restart page.

Table 32: Fields in the Device or Site Operations Restart Page

Field	Description
Device	See Table 20 on page 59.
Model	See Table 20 on page 59.
Vendor	See Table 20 on page 59.
Software Version	See Table 20 on page 59.
Restart Type	<p>The type of restart.</p> <p>The definitions of warm and cold restart depend on the device. The following definitions apply to the TCX1000-RDM20 and the TCX1000-ILA devices:</p> <ul style="list-style-type: none"> • Warm - The processor is reset, causing the software to be restarted, but the hardware is not reset. Provisioning data and operational settings are maintained. Traffic on optical modules is not affected. • Cold - Both the processor and the hardware (including optical modules) are reset. Provisioning data is maintained but operational settings such as the EDFA target gain and target power are reset to default values. <p>NOTE: Traffic is affected during a cold restart.</p> <p>For the restart behavior of other products, consult the respective documentation for those other products.</p>

Restarting a Device

This procedure applies to the following devices starting in (proNX Optical Director) release 18.4:

ACX6360
MX Series routers
PTX Series routers
QFX Series switches
TCX1000-ILA
TCX1000-RDM20

NOTE: The ACX6360 router or transponder, the MX Series and PTX Series router, and the QFX Series switch support cold restart only.

Use this procedure to perform a warm or cold reboot of a device.

1. Select the device or site that you want to reboot.
 - To reboot a device, start from the Devices Configuration page, expand the device tree to see the list of devices, and click the device that you want to reboot.

To select multiple devices to reboot, once you select a single device, use the Ctrl key (Cmd key in Mac OS X) to multi-select other devices. Select only devices that support the type of restart that you want to perform.

After you pick your device or devices, select **Operations>Restart**.
 - To reboot all devices at a site, start from the Devices Configuration page, categorize the device tree by site, click the site that you want to reboot, and select **Operations>Restart**. You can reboot all devices at a site only if they all support the same restart type.

The Restart page appears.
2. Select the **Restart Type**.
3. Click **Restart** and then click **Confirm** in the ensuing confirmation dialog.

Restoring a Device to Factory Defaults

This procedure applies to the following devices starting in (proNX Optical Director) release 18.4:

TCX1000-ILA
TCX1000-RDM20

Use this procedure to restore a device to factory defaults.

1. Start from the Devices Configuration page, expand the device tree to see the list of devices, and click the device that you want to restore to factory defaults.

2. Select **Operations>Factory Restore**.
3. Click **Restore** in the ensuing confirmation dialog.

Release History Table

Release	Description
18.4	Use this procedure to perform a warm or cold reboot of a device.
18.4	Use this procedure to restore a device to factory defaults.

Shelf Management

- [About the Devices Shelf Page on page 89](#)
- [Enabling or Disabling a Shelf on page 90](#)
- [Adding a Multiplexer/Demultiplexer to a Shelf on page 91](#)
- [Deleting a Multiplexer/Demultiplexer from a Shelf on page 92](#)

About the Devices Shelf Page

To access this page, start from the Devices Configuration page, expand the device tree to see the list of devices, expand a device to see the shelf, and click the shelf.

The Devices Shelf page displays information on the shelf including any passive equipment associated with that shelf (such as multiplexer/demultiplexers).

Tasks You Can Perform

You can use the Devices Shelf page to perform the following actions:

- View the shelf state and status.
- See the list of multiplexer/demultiplexers attached to the shelf.
- Add multiplexer/demultiplexers to the shelf.
- Delete multiplexer/demultiplexers from the shelf.

Field Descriptions

[Table 33 on page 89](#) explains the fields in the Devices Shelf page.

Table 33: Fields in the Devices Shelf Page

Field	Description
Administrative State	The shelf's administrative state.
Operational Status	The shelf's operational status. This is read-only.
Device	The IP address of the device containing this shelf.

Table 33: Fields in the Devices Shelf Page (continued)

Field	Description
Model	The model of the shelf.
Product Code	The product equipment code of the shelf.
Mux/Demux Modules (ROADM nodes only)	
Name	The name and index of the multiplexer/demultiplexer module. This is read-only. The name and index are set when you add the multiplexer/demultiplexer.
Product Code	The product equipment code (PEC) of the multiplexer/demultiplexer module. This is read-only. The PEC is set when you add the multiplexer/demultiplexer.
Connected Port	The port on the ROADM module that the multiplexer/demultiplexer module connects to. This is read-only. The connected port is specified when you create a link between the multiplexer/demultiplexer line port and a universal port on the ROADM module. See “Creating a Link” on page 127 .
Cross Connections (ACX6360-OX only)	
Cross Connection Number	The optical interface and index of the individual line interfaces.
Client Interface	The client interface of the cross connection.
Line Interface	The line interface of the cross connection.
NOTE: Not all fields appear for every device.	

Enabling or Disabling a Shelf

Use this procedure to enable or disable a shelf on a TCX1000-RDM20.

1. Start from the Devices Configuration page, expand the device tree to see the list of devices, expand a device to see the shelf, and click the shelf. The Devices Shelf page appears.
2. To enable the shelf, select **In-Service** from the Administrative State drop-down list.
The shelf is brought into service immediately.
3. To disable the shelf, select **Out-of-Service** from the Administrative State drop-down list.
The shelf is taken out of service immediately.

Adding a Multiplexer/Demultiplexer to a Shelf

Use this procedure to add a multiplexer/demultiplexer to a TCX1000-RDM20.

When you are adding and dropping a large number of wavelengths at a ROADM node, you typically install the ROADM node with a multiplexer/deemultiplexer. The multiplexer/demultiplexer is a passive device that allows you to increase the wavelength fanout by providing access to all 96 wavelengths in the fiber.

1. Start from the Devices Configuration page, expand the device tree to see the list of devices, expand a device to see the shelf, and click the shelf. The Devices Shelf page appears.

2. Click **New** in the Mux/Demux Modules pane.

The New Mux/Demux Module dialog appears.

3. Specify the **Module Index** from the drop-down list.

The fixed multiplexer/demultiplexer is automatically named md:0/<index> and the colorless multiplexer/demultiplexer is automatically named cmd:0/<index>.

You can assign any index you want as long as it's unique within this ROADM node.

4. Specify the **Mux/Demux Type** from the drop-down list.

5. Specify the **Product Code** from the drop-down list.

6. Optionally, create the device links for this device.

- a. In the **Create Links** box, click **show**.
- b. Use the drop-down list to specify the **Line Port**.
- c. Use the drop-down list to specify the **Universal Port**.
- d. If you are adding a 2D8CMD, use the drop-down list to specify the second **Line Port**, **Partner RDM**, and second **Universal Port**.

If you choose not to add the device links now, you can always add the device links later.

7. Click **Add**.

The multiplexer/demultiplexer at the specified index is added and appears in the Mux/Demux Modules list and in the device tree.

You can now create a link from the multiplexer/demultiplexer line port to a universal port on the ROADM module (if you did not already created the link above), and from the multiplexer/demultiplexer client ports to supported tail facility endpoints.

Deleting a Multiplexer/Demultiplexer from a Shelf

Use this procedure to delete a multiplexer/demultiplexer from a shelf.

1. Start from the Devices Configuration page, expand the device tree to see the list of devices, expand a device to see the shelf, and click the shelf. The Devices Shelf page appears.
2. Select the multiplexer/demultiplexer that you want to delete and click **Delete**. You can only delete the multiplexer/demultiplexer if it does not have a link configured on the Connected Port.

The selected multiplexer/demultiplexer is immediately deleted and removed from the list.

Circuit Pack Management

- [About the Devices Circuit Pack Page on page 92](#)

About the Devices Circuit Pack Page

To access this page, start from the Devices Configuration page, expand the device tree to see the list of devices, expand a device to see the shelf, expand the shelf to see the circuit packs, and click the circuit pack.

The Devices Circuit Pack page displays information on the circuit pack.

Tasks You Can Perform

You can view circuit pack information on this page.

Field Descriptions

[Table 34 on page 92](#) explains the fields in the Devices Circuit Pack page.

Table 34: Fields in the Devices Circuit Pack Page

Field	Description
Device	The name and/or IP address of the device containing this circuit pack. This is read-only.
Name	The name of the circuit pack. This is read-only.
Type	The type of circuit pack. This is read-only.
Model	The model of circuit pack. This is read-only.
Product Code	The product equipment code (PEC) of the circuit pack. This is read-only.

Port Management

- [About the Devices Port Config Page on page 93](#)
- [Configuring a Port on page 101](#)
- [About the Devices Port Threshold Page on page 101](#)
- [Configuring Threshold Crossing Alerts on Supported Tail Facility Ports on page 104](#)
- [About the Devices Port Historical PMs \(Metrics\) Page on page 104](#)
- [Viewing Historical Performance Monitoring Metrics on page 105](#)
- [About the Devices Port Telemetry Page on page 107](#)
- [Viewing Telemetry Metrics on page 108](#)

About the Devices Port Config Page

To access this page, start from the Devices Configuration page, expand the device tree to see the list of devices, expand a device to see the shelf, expand the shelf to see the circuit packs, expand the circuit pack hierarchy to see the ports, and click the port.

The contents of the Devices Port Config page vary depending on the port. In general, ports in the optical network have fewer parameters while transponder ports (tail facility endpoints) have more parameters because transponders operate at both the optical layer and the physical layer.

Tasks You Can Perform

You can use the Devices Port Config page to perform the following actions:

- View port parameters on TCX1000-RDM20 and TCX1000-ILA devices and on supported tail facility endpoints.
- Configure parameters on optical ports on TCX1000-RDM20 devices and on supported tail facility endpoints.
- Enable or disable a port on TCX1000-RDM20 devices and on supported tail facility endpoints.

Field Descriptions

[Table 35 on page 94](#) through [Table 39 on page 100](#) show a superset of the fields displayed for the different kinds of ports and transceivers. Not all fields are displayed or are configurable for all ports and transceivers. If a field is grayed out in the user interface page or does not appear at all, then that attribute is not supported for the specified port or transceiver.



NOTE: This document only gives cursory treatment to the various configuration parameters on tail facility ports. Consult the appropriate Junos OS or BT17800 documentation to see a fuller description of the parameters along with allowed values.

Table 35: Fields in the Devices Port Config Page for Optical Ports

Field	Description
Administrative State	<p>The port's administrative state:</p> <ul style="list-style-type: none"> • In-Service - laser is enabled • Out-of-Service - laser is disabled <p>NOTE: The only effect of setting a TCX1000-RDM20 Ux port out of service is to mask alarms for that port. The laser is not disabled.</p> <p>You can change the administrative state of TCX1000-RDM20 ports only. You cannot change the administrative state of TCX1000-ILA ports. TCX1000-ILA ports are controlled exclusively by the optical control layer of the proNX Optical Director.</p>
Operational Status	<p>The port's operational status:</p> <ul style="list-style-type: none"> • Up - port is operating normally • Down - port has detected a problem (for example, loss of signal on input) or is no longer processing the incoming signal due to automatic line shutdown (ALS) procedures <p>This attribute is read-only.</p>
Label	<p>The port label for TCX1000-RDM20 ports.</p> <p>This is a character string that you can configure to further describe the port. This string is not used by the proNX Optical Director.</p>

Table 36: Fields in the Devices Port Optical Config (OCH) Page for Supported Tail Facility Ports

Field	Description
NOTE: This table contains attributes for the optical channel (OCH). The optical channel represents the optical signal, which, in some transceivers, can contain one or more constituent OTU4 signals.	
<i>Port State</i>	
Administrative State	The administrative state.
Operational Status	The operational status. This is read-only.
<i>Loopbacks</i>	
Local Loopback	Enable or disable local loopback.
Line Loopback	Enable or disable line loopback.
<i>Configuration</i>	
Interface Name	The interface name displayed in the format used by the device. This is read-only.

Table 36: Fields in the Devices Port Optical Config (OCH) Page for Supported Tail Facility Ports (continued)

Field	Description
Modulation Format	<p>The modulation format specifies how an optical channel modulates its constituent OTU4 signal(s).</p> <p>When you configure an optical service between two transponder endpoints, the modulation format must match between the two endpoints.</p>
Wavelength	<p>The wavelength is specified in the following format:</p> <p><wavelength> / <frequency> (<channel>)</p> <p>where <channel> is the mutliplexer/demultiplexer channel number.</p>
Wavelength Spacing	The wavelength spacing (grid).
FEC Mode	<p>The FEC mode for the optical channel.</p> <p>When you configure an optical service between two transponder endpoints, the FEC Mode must match between the two endpoints.</p>
Encoding	<p>The encoding for the optical channel.</p> <p>When you configure an optical service between two transponder endpoints, the Encoding must match between the two endpoints.</p>
Laser Enable	Enables or disables the laser.
Tx Power	Sets the transmit power (dBm) of the laser.
CPRWS	Carrier phase recovery window size used for coherent transceivers.
LOS Alarm Threshold	<p>Sets the Loss-of-Signal alarm threshold.</p> <p>When the received signal power drops below this threshold, an LOS alarm is raised.</p>
LOS Warning Threshold	<p>Sets the Loss-of-Signal warning threshold.</p> <p>When the received signal power drops below this threshold, an LOS warning is raised.</p>
<i>Signal Degrade Config</i>	
Signal Degrade Interval	<p>Specify the interval (ms) over which the BER must stay above the BER Raise Threshold value for the Signal Degrade alarm to be raised.</p> <p>After the alarm is raised, if the BER returns below the BER Clear Threshold value for the specified interval, the alarm is cleared.</p>

Table 36: Fields in the Devices Port Optical Config (OCH) Page for Supported Tail Facility Ports (continued)

Field	Description
BER Raise Threshold	Specify the BER threshold at which the Signal Degrade alarm is raised (subject to the Signal Degrade Interval requirement).
BER Clear Threshold	Specify the BER threshold at which the Signal Degrade alarm is cleared (subject to the Signal Degrade Interval requirement).
<i>Auto-In-Service</i>	
Enable	Enables or disables auto-in-service (AINS) on the interface.
Timer	The AINS countdown timer on the interface.
<i>Custom Settings</i>	
Custom Setting 1, 2, 3	Optional customizable text fields for you to enter additional information for the port. These fields are displayed but are otherwise not used by the device.

Table 37: Fields in the Devices Port OTU Config Page for Supported Tail Facility Ports

Field	Description
<i>Port State</i>	
Administrative State	The administrative state.
Operational Status	The operational status. This is read-only.
<i>Information</i>	
Interface Name	The interface name displayed in the format used by the device. This is read-only.
Interface Type	The interface type. This is read-only.
<i>Configuration</i>	
Wavelength	The wavelength is specified in the following format: <wavelength> / <frequency> (<channel>) where <channel> is the mutliplexer/demultiplexer channel number.
Wavelength Spacing	The wavelength spacing (grid).
OTU Rate	This is read-only.

Table 37: Fields in the Devices Port OTU Config Page for Supported Tail Facility Ports (continued)

Field	Description
FEC Mode	<p>The FEC mode for the OTU signal.</p> <p>When you configure an optical service between two transponder endpoints, the FEC mode must match between the two endpoints.</p> <p>If the transceiver requires you to configure the FEC Mode on the optical channel, then the FEC Mode cannot be set for the OTU signal.</p>
Loopback Type	The type of loopback.
PRBS Mode	Configures PRBS (pseudorandom binary sequence) signal generation.
Laser Enable	Enables or disables the laser.
<i>Signal Degrad Config</i>	
Backward FRR	<p>Enable or disable backward fast reroute insertion.</p> <p>When enabled, the local end embeds BER status information into transmitted OTN frames. This allows the far end router or switch to detect and react to signal degrade conditions more quickly.</p> <p>Enable only if the far end supports this feature.</p>
Signal Degrad	<p>Enable or disable signal degrade monitoring.</p> <p>Signal degrade monitoring allows the router or switch to detect and react to signal degrade conditions.</p>
Signal Degrad Interval	<p>Specify the interval (ms) over which the BER must stay above the BER Raise Threshold value for the Signal Degrad alarm to be raised.</p> <p>After the alarm is raised, if the BER returns below the BER Clear Threshold value for the specified interval, the alarm is cleared.</p>
BER Raise Threshold	Specify the BER threshold at which the Signal Degrad alarm is raised (subject to the Signal Degrad Interval requirement).
BER Clear Threshold	Specify the BER threshold at which the Signal Degrad alarm is cleared (subject to the Signal Degrad Interval requirement).
Seconds Degraded For Fault	The number of consecutive degraded intervals required to raise a signal degrade fault. When the value is set to 0, signal degrade monitoring is disabled.

Table 37: Fields in the Devices Port OTU Config Page for Supported Tail Facility Ports (continued)

Field	Description
Degraded Threshold Per Second	The threshold used to evaluate whether a 1-second interval is considered a degraded interval. The threshold is the percentage of errored blocks in a 1-second interval. If the percentage of errored blocks detected in a 1-second interval exceeds this threshold, the interval is considered degraded.
<i>TTI Config</i>	
TTIM Action	<p>Enable or disable OTU trail trace identifier mismatch verification.</p> <p>When enabled, the local end compares the received trace identifier with the expected trace identifier. If the expected trace identifier does not match the actual received trace identifier, an alarm is raised. A mismatch might indicate that the fiber is connected to the wrong destination.</p> <p>The trace identifier consists of a Source Access Point Identifier (SAPI) followed by a Destination Access Point Identifier (DAPI).</p> <p>Enable only if the far end supports this feature.</p>
SAPI Tx Trace Config	Sets the SAPI value in the transmitted trace identifier.
SAPI Rx Trace Config	Displays the SAPI value from the received trace identifier. This is read-only.
SAPI Expected Rx Trace	Sets the expected SAPI value for the received trace identifier.
DAPI Tx Trace Config	Sets the DAPI value in the transmitted trace identifier.
DAPI Rx Trace Config	Displays the DAPI value from the received trace identifier. This is read-only.
DAPI Expected Rx Trace	Sets the expected DAPI value for the received trace identifier.
Transmit Trace	Sets the transmitted trace identifier.
Receive Trace	Displays the received trace identifier. This is read-only.
Expected Trace	Sets the expected received trace identifier.
<i>Auto-In-Service</i>	
Enable	Enables or disables auto-in-service (AINS) on the interface.
Timer	The AINS countdown timer on the interface.
<i>Custom Settings</i>	

Table 37: Fields in the Devices Port OTU Config Page for Supported Tail Facility Ports (continued)

Field	Description
Custom Setting 1, 2, 3	Optional customizable text fields for you to enter additional information for the port. These fields are displayed but are otherwise not used by the device.

Table 38: Fields in the Devices Port ODU Config Page for Supported Tail Facility Ports

Field	Description
<i>Configuration</i>	
Interface Name	The interface name displayed in the format used by the device. This is read-only.
Multiplex Mode	Specifies whether the ODU interface consists of multiplexed subinterfaces.
<i>Signal Degrade Config</i>	
Backward FRR	<p>Enable or disable backward fast reroute insertion.</p> <p>When enabled, the local end embeds BER status information into transmitted OTN frames. This allows the far end router or switch to detect and react to signal degrade conditions more quickly.</p> <p>Enable only if the far end supports this feature.</p>
Signal Degrade	<p>Enable or disable signal degrade monitoring.</p> <p>Signal degrade monitoring allows the router or switch to detect and react to signal degrade conditions.</p>
Signal Degrade Interval	<p>Specify the interval (ms) over which the BER must stay above the BER Raise Threshold value for the Signal Degrade alarm to be raised.</p> <p>After the alarm is raised, if the BER returns below the BER Clear Threshold value for the specified interval, the alarm is cleared.</p>
BER Raise Threshold	Specify the BER threshold at which the Signal Degrade alarm is raised (subject to the Signal Degrade Interval requirement).
BER Clear Threshold	Specify the BER threshold at which the Signal Degrade alarm is cleared (subject to the Signal Degrade Interval requirement).
<i>TTI Config</i>	

Table 38: Fields in the Devices Port ODU Config Page for Supported Tail Facility Ports (continued)

Field	Description
TTIM Action	<p>Enable or disable ODU trail trace identifier mismatch verification.</p> <p>When enabled, the local end compares the received trace identifier with the expected trace identifier. If the expected trace identifier does not match the actual received trace identifier, an alarm is raised. A mismatch might indicate that the fiber is connected to the wrong destination.</p> <p>The trace identifier consists of a Source Access Point Identifier (SAPI) followed by a Destination Access Point Identifier (DAPI).</p> <p>Enable only if the far end supports this feature.</p>
SAPI Tx Trace Config	Sets the SAPI value in the transmitted trace identifier.
SAPI Rx Trace Config	Displays the SAPI value from the received trace identifier. This is read-only.
SAPI Expected Rx Trace	Sets the expected SAPI value for the received trace identifier.
DAPI Tx Trace Config	Sets the DAPI value in the transmitted trace identifier.
DAPI Rx Trace Config	Displays the DAPI value from the received trace identifier. This is read-only.
DAPI Expected Rx Trace	Sets the expected DAPI value for the received trace identifier.
Transmit Trace	Sets the transmitted trace identifier.
Receive Trace	Displays the received trace identifier. This is read-only.
Expected Trace	Sets the expected received trace identifier.
<i>Auto-In-Service</i>	
Enable	Enables or disables auto-in-service (AINS) on the interface.
Timer	The AINS countdown timer on the interface.

Table 39: Fields in the Devices Port Page (for all other ports)

Field	Description
Device	The name of the device containing this port. This is read-only.
Name	The name of the port. This is read-only.
Administrative State	The port's administrative state. This is read-only.

Table 39: Fields in the Devices Port Page (for all other ports) (continued)

Field	Description
Operational Status	The port's operational status. This is read-only.

Configuring a Port

Use this procedure to configure an optical port on a TCX1000-RDM20 or a port on a supported tail facility endpoint.

1. Start from the Devices Configuration page, expand the device tree to see the list of devices, expand a device to see the shelf, expand the shelf to see the circuit packs, expand the circuit pack to see the ports, and click the port.
2. Configure the port parameters as described in [Table 35 on page 94](#) through [Table 38 on page 99](#).
3. To save your changes, click **Save**.
4. To discard your changes, click **Reset**.

About the Devices Port Threshold Page

To access this page, start from the Devices Configuration page, expand the device tree to see the list of devices, expand a device to see the shelf, expand the shelf to see the circuit packs, expand the circuit pack to see the ports, and click the port. From here, select the interface (**OCH**, **OTU**, **ODU**) from the drop-down list and click **Threshold**.



NOTE: Not all devices support configurable thresholds. Devices that do not support configurable thresholds do not have the **Threshold** tab.

The Devices Port Threshold page displays the threshold crossing alert (TCA) configuration for the port. A threshold crossing alert is a configurable warning that triggers when its associated performance monitoring metric exceeds the configured threshold value. TCAs can be configured for both the 15-minute bin and the 24-hour bin. Typically only a subset of the performance monitoring metrics can be controlled using TCAs.

Tasks You Can Perform

You can view and configure the threshold crossing alerts for the selected port and interface.

Field Descriptions

[Table 40 on page 102](#) through [Table 42 on page 103](#) explain the fields in the Devices Port Threshold page.



NOTE: This document only gives cursory treatment to router and switch configuration parameters. Consult the appropriate Junos OS documentation to see a fuller description of the parameters along with usage tips and exceptions.

Table 40: Fields in the Devices Port Optical Threshold (OCH) Page for Supported Tail Facility Ports

Field	Description
Carrier Frequency Offset (MHz)	Set the maximum and minimum thresholds for the carrier frequency offset in the 15-minute and 24-hour bins, and select the check box to enable them. You can enable the maximum and minimum TCAs separately.
Module Temperature (°C)	Set the maximum and minimum thresholds for the module temperature in the 15-minute and 24-hour bins, and select the check box to enable them. You can enable the maximum and minimum TCAs separately.
Rx-Power (dBm)	Set the maximum and minimum thresholds for the receive power in the 15-minute and 24-hour bins, and select the check box to enable them. You can enable the maximum and minimum TCAs separately.
Tx-Power (dBm)	Set the maximum and minimum thresholds for the transmit power in the 15-minute and 24-hour bins, and select the check box to enable them. You can enable the maximum and minimum TCAs separately.
FEC-BER	Set the threshold for the FEC bit error rate in the 15-minute and 24-hour bins, and select the check box to enable the TCA.

Table 41: Fields in the Devices Port OTU Threshold Page for Supported Tail Facility Ports

Field	Description
<i>Near End</i>	
BBE	Set the threshold for background block errors in the 15-minute and 24-hour bins, and select the check box to enable the TCA.
ES	Set the threshold for errored seconds in the 15-minute and 24-hour bins, and select the check box to enable the TCA.
SES	Set the threshold for severely errored seconds in the 15-minute and 24-hour bins, and select the check box to enable the TCA.
UAS	Set the threshold for unavailable seconds in the 15-minute and 24-hour bins, and select the check box to enable the TCA.
<i>Far End</i>	

Table 41: Fields in the Devices Port OTU Threshold Page for Supported Tail Facility Ports (continued)

Field	Description
BBE	Set the threshold for background block errors in the 15-minute and 24-hour bins, and select the check box to enable the TCA.
ES	Set the threshold for errored seconds in the 15-minute and 24-hour bins, and select the check box to enable the TCA.
SES	Set the threshold for severely errored seconds in the 15-minute and 24-hour bins, and select the check box to enable the TCA.
UAS	Set the threshold for unavailable seconds in the 15-minute and 24-hour bins, and select the check box to enable the TCA.
<i>FEC-BER</i>	
FEC-BER	Set the threshold for the FEC bit error rate in the 15-minute and 24-hour bins, and select the check box to enable the TCA.

Table 42: Fields in the Devices Port ODU Threshold Page for Supported Tail Facility Ports

Field	Description
<i>Near End</i>	
BBE	Set the threshold for background block errors in the 15-minute and 24-hour bins, and select the check box to enable the TCA.
ES	Set the threshold for errored seconds in the 15-minute and 24-hour bins, and select the check box to enable the TCA.
SES	Set the threshold for severely errored seconds in the 15-minute and 24-hour bins, and select the check box to enable the TCA.
UAS	Set the threshold for unavailable seconds in the 15-minute and 24-hour bins, and select the check box to enable the TCA.
<i>Far End</i>	
BBE	Set the threshold for background block errors in the 15-minute and 24-hour bins, and select the check box to enable the TCA.
ES	Set the threshold for errored seconds in the 15-minute and 24-hour bins, and select the check box to enable the TCA.
SES	Set the threshold for severely errored seconds in the 15-minute and 24-hour bins, and select the check box to enable the TCA.
UAS	Set the threshold for unavailable seconds in the 15-minute and 24-hour bins, and select the check box to enable the TCA.

Configuring Threshold Crossing Alerts on Supported Tail Facility Ports

Use this procedure to configure threshold crossing alerts for a port and interface.

1. Start from the Devices Configuration page, expand the device tree to see the list of devices, expand a device to see the shelf, expand the shelf to see the circuit packs, expand the circuit pack to see the ports, and click the port. From here, select the interface (**OCH**, **OTU**, **ODU**) from the drop-down list and click **Threshold**.

The TCAs for the selected port and interface are displayed.

2. Configure the TCAs as desired and select the **Enable** check box to enable them.
3. To save your changes, click **Save**.
4. To discard your changes, click **Reset**.
5. Repeat for the other interfaces on this port as desired.

About the Devices Port Historical PMs (Metrics) Page

To access this page, start from the Devices Configuration page, expand the device tree to see the list of devices, expand a device to see the shelf, expand the shelf to see the circuit packs, expand the circuit pack to see the ports, and click the port. From here, click **Metrics** (in releases 2.2 and lower) or **Metrics>Historical PMs** (in releases 18.4 and higher).

The Devices Port Historical PMs (Metrics) page allows you view selected metrics.



NOTE: To ensure that the metrics are displayed with the correct timestamps, ensure that the devices are configured to use NTP servers. See [“About the Device NTP Servers Page”](#) on page 65.

Tasks You Can Perform

You can use the Devices Port Historical PMs (Metrics) page to perform the following actions:

- View the performance monitoring metrics for the port.
- Analyze the metrics using Grafana.

Field Descriptions

[Table 43 on page 105](#) explains the fields in the Devices Port Historical PMs (Metrics) page.

Table 43: Fields in the Devices Port Historical PMs (Metrics) Page

Field	Description
Time Series	Set the time series or bin length for which you want to display the counters. The counters are collected in 1-minute, 15-minute, and 24-hour bins. NOTE: Not all devices support the 1-minute bin.
Time Range	Specify the time period that you want to view.
Entity	Specify the interface from the drop-down list.
Metric	Specify the metric from the drop-down list.

Viewing Historical Performance Monitoring Metrics

Prerequisites

- You have collected the metrics for the device you want to view. See [“Metric Collection” on page 77](#).



NOTE: Management network instability might cause the proNX Optical Director to lose one or more historical PM bins. If you see that some PM bins are missing, you can wait for the next scheduled PM collection or you can perform a manual PM collection to retrieve all bins from the device again. See [“Collecting Metrics from a Device Manually” on page 79](#).

Use this procedure to view historical performance monitoring metrics (PMs) for a port.

The proNX Optical Director stores collected PMs in a database for 30 days and makes them available for viewing. PM data points older than 30 days are purged from the database. The proNX Optical Director supports the collection and display of 1-minute, 15-minute, and 1-day bins. The actual bins collected and displayed depend on what the device supports. PM points in 15-minute bins are timestamped on the hour and at every 15 minutes thereafter. PM points for the 1-day bin are timestamped at midnight (local time of the machine running the web browser accessing the GUI).

- Start from the Devices Configuration page, expand the device tree to see the list of devices, expand a device to see the shelf, expand the shelf to see the circuit packs, expand the circuit pack to see the ports, and click the port. From here, click **Metrics** (in releases 2.2 and lower) or **Metrics>Historical PMs** (in releases 18.4 and higher).

The metrics for the port are displayed in table form.

- Select the **Time Series** from the drop-down list. The available options are **1 Minute**, **15 Minute**, and **24 Hours**.



NOTE: Not all devices support the 1 Minute bin. If the 1 Minute bin option does not appear in the drop-down list, then the 1 Minute bin option is not supported for the selected device.

3. Specify the time range.


Click inside the **Time Range** box to open a calendar where you can select the time range. You can choose one of the quick selections (**Today**, **Yesterday**, **Last 7 Days**, **Last 30 Days**) or you can fully customize your range. Ensure that you specify the correct time in addition to the date.

When you finish specifying the time range, click **Apply**.

4. Specify the **Entity** (typically the interface) from the drop-down list.

5. Specify the **Metric** from the drop-down list.

6. Click the  button.

The table displays a snapshot of the selected metric. To refresh the table at any time, click the  button.



NOTE: The graph displays the selected metric without units. To obtain the units for the selected metric, consult the MIB where the selected metric is found.

7. To analyze the metrics using Grafana, select the **Analyze** button. To get started with Grafana, see ["Grafana" on page 167](#).

See the *TCX Series Optical Transport System Feature Guide* for the list of performance monitoring metrics supported.

About the Devices Port Telemetry Page

To access this page, start from the Devices Configuration page, expand the device tree to see the list of devices, expand an optical device to see the shelf, expand the shelf to see the circuit packs, expand the circuit pack to see the ports, and click an optical port. From here, click **Metrics>Telemetry**.

The Devices Port Telemetry page allows you view and graph real-time telemetry metrics starting in release 18.4.

Tasks You Can Perform

You can use the Devices Port Telemetry page to graph real-time telemetry data from an optical port.

Field Descriptions

Table 44 on page 107 explains the fields in the Devices Port Telemetry page.

Table 44: Fields in the Devices Port Telemetry Page

Field	Description
Duration	Set the duration in which you want to view and graph the selected telemetry metric(s).
Metrics	Select the metric(s) you want to view.
Progress	This field shows the progress of the telemetry metric collection relative to the specified duration.

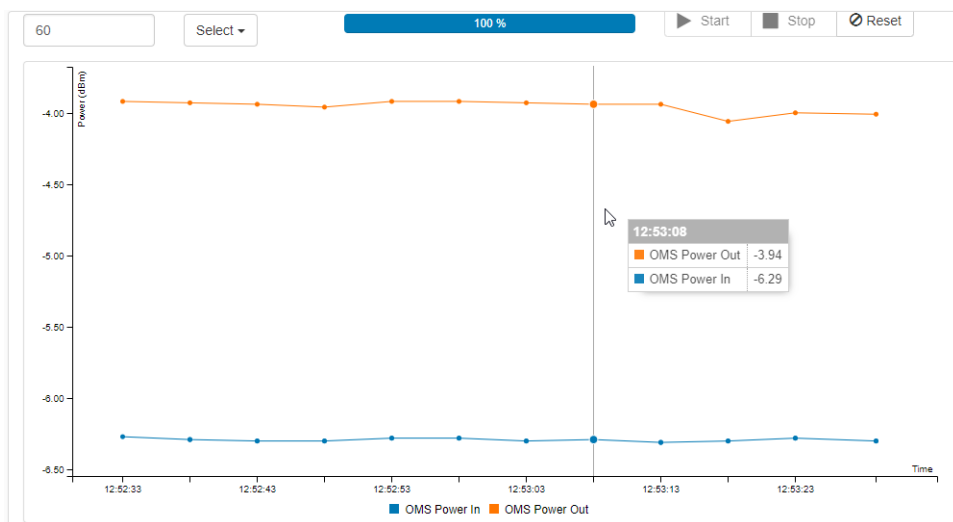
Viewing Telemetry Metrics

Use this procedure to view real-time telemetry data from an optical port.

The proNX Optical Director receives streams of telemetry data from optical devices in the network. This data is used by the Optical Control Layer to manage the optical controls of the optical ports on the devices. A subset of this data is available for viewing using the procedure in this section.

Figure 3 on page 108 shows an example of the type of graph you can generate:

Figure 3: Port Telemetry Graph Example



1. Start from the Devices Configuration page, expand the device tree to see the list of devices, expand an optical device to see the shelf, expand the shelf to see the circuit packs, expand the circuit pack to see the ports, and click an optical port. From here, click **Metrics>Telemetry**.

The Devices Port Telemetry page appears.

2. Specify the time **Duration** that you want to view and graph the telemetry data.
3. Select the telemetry **Metric** from the drop-down list. You can select more than one metric.
4. Click **Start** to start telemetry data collection and graphing.
5. Click **Pause** to pause the graphing of telemetry data. Telemetry data continues to be collected when paused. To continue graphing, click **Start**.

6. Click **Stop** to stop telemetry data collection and graphing prior to duration expiry.
7. Click **Reset** to clear the graph.

See the *TCX Series Optical Transport System Feature Guide* for the list of telemetry metrics supported.

Release History Table

Release	Description
18.4	Metrics>Historical PMs (in releases 18.4 and higher)
18.4	Use this procedure to view real-time telemetry data from an optical port

Devices Discovery

- [Discovering a Device on page 109](#)
- [Rediscovering a Device on page 112](#)
- [Undiscovering a Device on page 112](#)
- [Resynchronizing the Network on page 113](#)
- [Moving a Discovered Device to a Different Site on page 114](#)

Discovering a Device

Use this procedure to discover a new device.

In order to control and manage devices, you have to let the proNX Optical Director know which devices you want to control and manage. This is called device discovery, and is typically the first step you perform when using the proNX Optical Director. You can discover one device at a time or, more typically, you can discover multiple devices based on your discovery selection criteria. As part of device discovery, you will assign the device to a site. This allows the proNX Optical Director to accurately place the discovered device on the map.

1. Start from the Devices Configuration page.
2. If you want to discover a new device for an existing site, categorize the device tree by site and select the site.

3. Click **Discovery** and select **Device Discovery** from the drop-down list.

The Device Discovery dialog appears.

4. Specify the IP address or IP address pattern in the **Address Pattern** box.

You can enter a single IP address or an IP address pattern representing multiple IP addresses. See [Table 45 on page 110](#).

Table 45: Address Pattern

Address Pattern	Example
Full IPv4 or IPv6 address	10.228.103.4
List of IPv4 or IPv6 addresses separated by commas	10.228.103.4, 10.228.145.8
A range of IPv4 or IPv6 addresses	10.228.103.1-10
All IPv4 or IPv6 addresses in a subnet	10.228.103.255

- Specify the **NETCONF Username** and **NETCONF Password**. These are the read-write login credentials for the device.


If you are discovering multiple devices, you must ensure that the login credentials are the same across the devices you want to discover. If the login credentials are not the same, then you will have to limit each discovery to the group of devices that share the same login credentials.


The user that you specify must have read-write privileges for all attributes on the device. Devices are shipped with a default read-write username and password that you can use to log in for the first time. For information on the default username and password for a device, see the respective device documentation. Specifically, for the TCX1000-RDM20, see the *TCX1000 Programmable ROADM Hardware Guide*. For the TCX1000-ILA, see the *TCX1000 Inline Amplifier Hardware Guide*.

- Specify the site.
 - If you selected the site in step 2, then the **Site Name**, **Latitude**, and **Longitude** are automatically populated. You can proceed to step 13.
 - If you did not select the site earlier, then proceed to step 7
- Click **Select Site**.




The Create or Select a Site window depicting a map of the world appears.

- To pan around the map, click and hold anywhere in the map background and drag the map until the desired part of the map comes into view.
- To zoom in and out:

To zoom in, click the  in the lower right corner. Alternatively, you can zoom in by using your mouse scroll wheel.

To zoom out, click the  in the lower right corner. Alternatively, you can zoom out by using your mouse scroll wheel.



NOTE: If you zoom out such that two or more sites are on top of each other, a single  icon is displayed. To see the sites represented by the  icon, click the  icon.

10. If you want to create a new site, click the location on the map where you want to create the new site. Zoom in to get better resolution.

The New Site dialog appears. Type the **Site Name** of the new site and click **Save**.

The site appears on the map.

11. Click the site in which you want to add the new device and click **Select**.

The Create or Select a Site window closes and the selected site is populated in the **Site Name**, **Latitude**, and **Longitude** boxes.

12. Optionally, set the **Physical Location**. The location is set using the location tree for the site. The location tree provides a structured way for you to place a device at a location within a site.

- To specify the **Physical Location** of the new device, click **Select**. This brings up the Select Location dialog.
- If you want to edit the tree to create a new building, room, or rack, see [“Editing a Location Tree” on page 58](#).
- Select the rack where you want to place the device and click **Select**. The Select Location dialog closes.

Your selection is now shown in the **Physical Location** field.

13. Click **show** in **Advanced Settings** to see additional configuration parameters.

Parameter	Description
Automatically Configure JUNOS	<p>If the device to be discovered is a Juniper Networks router or switch, select yes to automatically configure that router or switch for NETCONF and SNMP access from the proNX Optical Director. This feature requires Telnet access to be enabled on the router or switch.</p> <p>When selected, the proNX Optical Director configures the router or switch as follows:</p> <ul style="list-style-type: none"> enables the router or switch to accept NETCONF requests destined for the port you specify in NETCONF Port creates an SNMP read-only community called "public" if it doesn't already exist creates an SNMP read/write community that you specify in SNMP Community
SNMP Community	<p>Specify the SNMP read/write community string used by the proNX Optical Director to write to the device. By default, the proNX Optical Director uses the "private" community string.</p> <p>You do not need to configure SNMP when discovering TCX1000-RDM20 devices.</p>

Parameter	Description
SNMP Port	<p>Specify the SNMP port to use for SNMP requests to the device. By default, the proNX Optical Director uses the standard port 161.</p> <p>You do not need to configure SNMP when discovering TCX1000-RDM20 devices.</p>
NETCONF Port	<p>Specify the NETCONF port to use for NETCONF requests to the device. By default, the proNX Optical Director uses the standard port 830, which is the default used by many Juniper Networks devices including the TCX1000-RDM20.</p> <p>NOTE: The BTI7800 Series device uses a different NETCONF port number. See the <i>BTI7800 Series Software Configuraiton Guide</i> for more information.</p>

- Click **Discover** to start the discovery task. To monitor the progress of this task, see [“Viewing the Tasks List” on page 147](#).

Rediscovering a Device

Use this procedure to rediscover a device or multiple devices.

Rediscovering a device causes the proNX Optical Director to refresh its view by performing a full data retrieval from the device. You do not normally need to rediscover a device because the proNX Optical Director regularly synchronizes with all devices under management. However, if you suspect the proNX Optical Director has a stale view of a device, you can rediscover it to speed up the synchronization.

- You can rediscover a single device, multiple devices, or all devices at a site.
 - To select all devices at a site, start from the Devices Configuration page, categorize the device tree by site, and click the site that you want to rediscover.
 - To select a single device, start from the Devices Configuration page, expand the device tree to see the list of devices, and click the device that you want to rediscover.
 - To select multiple devices, once you select a single device or site, use the Ctrl key (Cmd key in Mac OS X) to multi-select other devices or sites. You can select a combination of sites, a combination of devices, or a combination of sites and devices.
- Once you have selected the devices you want to rediscover, click **Discovery>Re-discover Selected**. To monitor the progress of this task, see [“Viewing the Tasks List” on page 147](#).

Undiscovering a Device

Use this procedure to undiscover a device or multiple devices.

Undiscovering a device removes the device from proNX Optical Director management. The proNX Optical Director deregisters itself from the device and removes the device from view.

- You can undiscover a single device, multiple devices, or all devices at a site.

- To select all devices at a site, start from the Devices Configuration page, categorize the device tree by site, and click the site that you want to undiscover.
 - To select a single device, start from the Devices Configuration page, expand the device tree to see the list of devices, and click the device that you want to undiscover.
 - To select multiple devices, once you select a single device or site, use the Ctrl key (Cmd key in Mac OS X) to multi-select other devices or sites. You can select a combination of sites, a combination of devices, or a combination of sites and devices.
2. Once you have selected the devices you want to undiscover, click **Discovery>Un-discover Selected**.

When you undiscover a device, it is normal to see transient error notifications as the proNX Optical Director receives messages from the device that has been undiscovered. These messages will stop once the undiscovery is complete.

Resynchronizing the Network

Use this procedure to resynchronize the proNX Optical Director with all devices in the network.

Resynchronizing with the network causes the proNX Optical Director to rediscover all devices under management. You do not normally need to resynchronize with the network because the proNX Optical Director regularly synchronizes with all devices under management. However, if you suspect the proNX Optical Director has a stale view of many devices in the network, you can use this procedure to speed up the synchronization.

1. Start from the Devices Configuration page.
2. To resynchronize the proNX Optical Director with all devices in the network, click **Discovery>Resync Network**.

To monitor the progress of this task, see "[Viewing the Tasks List](#)" on page 147.

Moving a Discovered Device to a Different Site

Use this procedure to move a discovered device to a different site. You normally specify the site when you discover a device, but if you specified the wrong site or if you simply want to change the site that the device was originally associated with, then you can use this procedure to do that.

1. You can move a single device, multiple devices, or all devices at a site.
 - To move all devices at a site, start from the Devices Configuration page, categorize the device tree by site, and click the site that you want to move.
 - To move a single device, start from the Devices Configuration page, expand the device tree to see the list of devices, and click the device that you want to move.
 - To move multiple devices, once you select a single device or site, use the Ctrl key (Cmd key in Mac OS X) to multi-select other devices or sites. You can select a combination of sites, a combination of devices, or a combination of sites and devices.
2. Once you have selected the devices you want to move, click **Discovery>Move Selected to Site**.

The Move Selected to Site window appears.

3. From the Site drop-down list, select the site where you want to move the selected devices.
4. Optionally, set the **Physical Location** for the device at the new site. The location is set using the location tree for the site. The location tree provides a structured way for you to place a device at a location within a site.
 - To specify the **Physical Location** of the new device, click **Select**. This brings up the Select Location dialog.
 - If you want to edit the tree to create a new building, room, or rack, see [“Editing a Location Tree” on page 58](#).
 - Select the rack where you want to place the device and click **Select**. The Select Location dialog closes.
5. Click **Save**.

Devices Inventory

- [About the Devices Inventory Page on page 114](#)
- [Viewing the Inventory on page 115](#)

About the Devices Inventory Page

To access this page, click the **Devices** tab and select **Inventory** in the left-nav bar.

The Devices Inventory page lists the equipment inventory in your network.

Tasks You Can Perform

You can view a list of inventory in your network from this page.

Field Descriptions

Table 46 on page 115 describes the fields in the Devices Inventory page.

Table 46: Fields in the Devices Inventory Page

Field	Description
Device	The name and/or IP address of the device.
Type	The type of component within the device: <ul style="list-style-type: none"> • module • chassis • XCVR
Name	The name of the component.
Model	The model or component type.
Product Code	The product equipment code of the component.
Serial Number	The serial number of the component.

Viewing the Inventory

Use this procedure to view the inventory in your network.

1. Click the **Devices** tab and select **Inventory** in the left-nav bar.

The list of inventory in your network is displayed in a table.

Devices / Inventory

Show 100 entries

View Copy Print Save Search:

Device	Type	Name	Model	Product Code	Serial Number
10.228.234.14	Module	midplane	CHAS-BP3-MX240-S	750-047865	xxxxxxxxxx
10.228.234.14	Module	fpm:board	CRAFT-MX240-S	760-021392	xxxxxxxxxx
10.228.234.14	Module	pem:0	PWR-MX480-2400-DC-S	740-063045	xxxxxxxxxx
10.228.234.14	Module	pem:2	PWR-MX480-2400-DC-S	740-063045	xxxxxxxxxx
10.228.234.14	Module	routing:engine:0	RE-S-1800X4-16G-S	740-031116	xxxxxxxxxx
10.228.234.14	Module	cb:0	SCBE2-MX-S	750-062572	xxxxxxxxxx
10.228.234.14	Module	fpc:1	MPC-3D-16XGE-SFPP	750-062581	xxxxxxxxxx
10.228.234.22	Chassis	roadm	TCX1000 20 PORT ROADM SYSTEM	TCX1000-RDM20	xxxxxxxxxx
10.228.234.22	Module	md:0/7		BT8A96MD03	xxxxxxxxxx

2. To see details on a particular device or equipment, click the row for that device or equipment and select **View**.
3. To sort, filter, copy, print, or save table entries, see “Working with Tables” on page 22.

CHAPTER 5

Network

- [Device Links on page 117](#)
- [Services on page 128](#)

Device Links

- [Device Links Overview on page 117](#)
- [Device Link Validation on page 121](#)
- [About the Device Links Current Page on page 121](#)
- [Viewing or Deleting a Link on page 124](#)
- [Editing the Fiber Type on page 124](#)
- [About the Device Links Create Link Page on page 125](#)
- [Creating a Link on page 127](#)

Device Links Overview

The proNX Optical Director must have a view of the topology of the network in order to create and manage optical services. With an accurate view of the topology, the proNX Optical Director can dynamically control the optical links in your network and determine the available service paths for the services that you subsequently create. In order to build the topology, the proNX Optical Director needs to know how devices are connected together, including:

- the device links within a ROADM node (must be configured)
- the device links between ROADM nodes (can be configured or learned)
- the device links between amplifier sites (can be configured or learned)
- the device links between ROADM nodes and amplifier sites (can be configured or learned)
- the device links between ROADM nodes and transponder endpoints (must be configured)

See [Table 47 on page 118](#) for definitions of terms used in this section.

Table 47: Optical Network Glossary

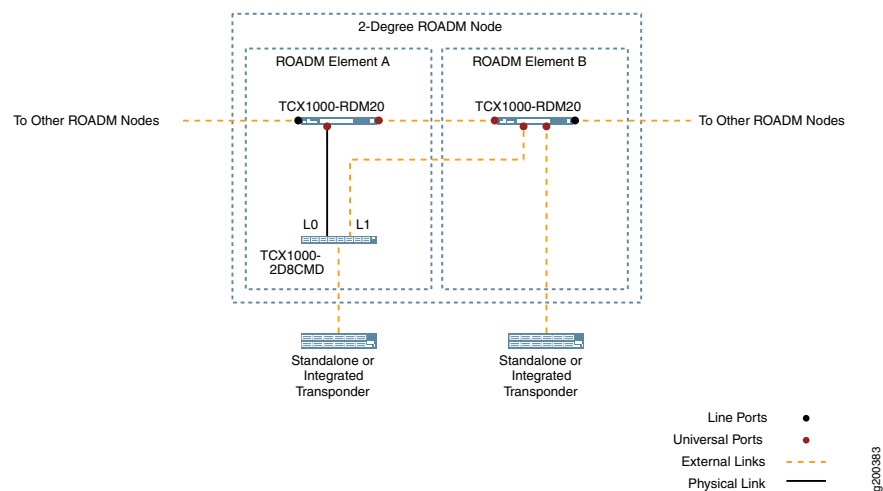
Term	Definition
Amplifier site	A site containing a line amplifier device providing amplification of the incoming composite DWDM signals. An example of a line amplifier device is the TCX1000-ILA, which is an inline amplifier that provides amplification in both directions.
Device link	A link between any two managed devices. Device links represent the actual fibers installed between devices in your network.
Line span	A device link connecting the line ports of two devices together.
ROADM element	<p>A TCX Series ROADM device that provides a wavelength switching function for a single degree in a ROADM node. This function can include switching wavelengths to another degree (that is, to another ROADM element for pass-through) and switching wavelengths for local add/drop access. An example of a ROADM element is the TCX1000 Programmable ROADM (TCX1000-RDM20), which is a 20-port ROADM device that provides wavelength switching between its 20 universal ports and its line port.</p> <p>Additionally, there exist passive multiplexer/demultiplexer devices such as the 96-Channel Fixed Mux/Demux (FMD96) and the TCX1000 2-Degree 8-Channel Colorless Mux/Demux (2D8CMD), which attach to a TCX Series ROADM device to provide higher fan-out add/drop access to the individual wavelengths. While multiplexer/demultiplexers are physically distinct from the TCX Series ROADM devices they attach to, they are not logically standalone. For this reason, the proNX Optical Director models the multiplexer/demultiplexer device as an extension (that is, as a circuit pack) of a ROADM element.</p>
ROADM node	<p>A configuration of ROADM elements that together provide a specific role in an optical network. A ROADM node is conceptual only, and exists purely to convey the type of role that the constituent ROADM elements provide. Examples of ROADM nodes are single-degree terminal nodes and multi-degree add/drop nodes.</p> <p>A ROADM node consists of as many ROADM elements as there are degrees. For example, a single-degree node consists of a single ROADM element. A four-degree node consists of four ROADM elements.</p> <p>A ROADM node can be split between two or more sites. A split ROADM node is a highly survivable configuration where ROADM elements comprising a ROADM node are located at separate sites. A failure or outage at one site affects traffic at that site only. Add/drop traffic on the same ROADM node but at another site is not affected if the traffic is not configured to pass through the failed ROADM element.</p> <p>Like a regular ROADM node, a split ROADM node is conceptual, and cannot be explicitly created or deleted. A ROADM node becomes a split ROADM node once you configure a device link between a universal port of a ROADM element at one site and a universal port of a ROADM element at a different site (subject to nodal loss constraints). See the <i>TCX Series Optical Transport System Feature Guide</i> for information on the maximum nodal loss that is allowed to occur on the fiber between ROADM elements within a ROADM node.</p>
Tail facility	The link from the optical network edge to the client transponder. See “Optical Service and Tail Facility Endpoints” on page 129 .
Topology	<p>The ROADM topology, which is the topology concerned with how ROADM nodes are connected together, and consequently, how wavelengths are allocated in the network.</p> <p>NOTE: The ROADM topology models an amplifier site as part of a line because line amplifiers operate on the composite DWDM signal and not on the individual wavelengths.</p>

Figure 4 on page 119 shows an example of how devices can be connected together in a 2-degree ROADM node. A 2-degree ROADM node contains two ROADM elements, with each ROADM element connected to a line (or degree). These ROADM elements are labelled A and B in the example.

ROADM Element A consists of a TCX1000-RDM20 and a 2D8CMD. The 2D8CMD connects to a universal port on the TCX1000-RDM20 in ROADM Element A and can optionally connect to a universal port on the TCX1000-RDM20 in ROADM Element B. By connecting to both TCX1000-RDM20 devices, the 2D8CMD has add/drop access to wavelengths on both degrees, which is a prerequisite to setting up a service with working and protection paths.

In contrast, ROADM Element B just consists of a TCX1000-RDM20, so it only has add/drop access to wavelengths on the line that it is attached to. The reason for this is that the TCX1000-RDM20 can only switch wavelengths between its universal ports and its line port. It cannot switch wavelengths from one universal port to another.

Figure 4: 2-Degree ROADM Node Example



The endpoint or client transponder can be a standalone device or integrated within a router or a switch. The endpoint transponder can connect to the ROADM node in a couple of different ways. One way is to connect the endpoint transponder to a client port on the 2D8CMD in ROADM Element A to provide add/drop access to both degrees. By doing this, you can then set up a service with both working and protection paths through the network. The second way is to connect the endpoint transponder directly to a universal port on the TCX1000-RDM20 in either ROADM Element A (not shown) or ROADM Element B to provide add/drop access to the degree to which the TCX1000-RDM20 is attached.

The device links to the endpoint transponders are known as tail facilities, which are the connections between the optical network edge and the client device. The proNX Optical Director can be used to provision tail facility links to supported ports on Juniper Networks equipment as well as to provision the endpoints themselves. See [Table 2 on page 24](#) for the list of the tail facility endpoints that the proNX Optical Director can configure.

Device links within a ROADM node and from a ROADM node to a tail facility endpoint must be manually provisioned.

Device links between ROADM nodes, between amplifier sites, and between ROADM nodes and amplifier sites, can be learned depending on which release of the proNX Optical

Director and TCX1000-RDM20 you are running. These device links are called line spans because they connect to the line ports of the devices.

Provisioned Device Links

A provisioned device link is a device link that you explicitly create. A provisioned device link where both endpoints are within the same ROADM element is called a physical link. A provisioned device link where one endpoint resides outside the ROADM element is called an external link. For more information on external and physical links, see <http://www.openroadm.org>.



NOTE: In Juniper Networks' implementation, only device links that are provisioned have a physical or external type designation. Auto-learned device links are not associated with a link type.

It is important that your configured device links match the actual device links or unexpected behavior can occur.



NOTE: When you provision a device link to a ROADM port, the ROADM port is automatically placed in-service administratively. You do not need to manually place the port in-service.

Auto-Learned Device Links

Automatic learning of line spans is supported if you are running proNX Optical Director release 2.2 or higher and the devices in your network are running the following releases:

- TCX1000-RDM20 running release 3.1 or higher
- TCX1000-ILA running any release

The proNX Optical Director learns about the existence of line spans based on the Link Layer Discovery Protocol (LLDP) neighbor information that the devices report. While the proNX Optical Director can determine the neighbors from this data, it cannot determine the type of fiber used for the span because the type of fiber used cannot be automatically detected. Instead, the proNX Optical Director assumes a default fiber type for all line spans in the network.



NOTE: If this default fiber type is different from the actual fiber type for a particular span, you will need to manually configure the fiber type for that span.

To change the fiber type, you have to create an external link based on the auto-learned link and then change the fiber type of the external link. The proNX Optical Director does not allow you to change the fiber type of an auto-learned device link directly because auto-learned data originates from the device and is read-only. For convenience, the

proNX Optical Director user interface lets you perform this task as if you are editing the fiber type. See [“Editing the Fiber Type” on page 124](#).

Nevertheless, it is important for you to be aware that when you change the fiber type of an auto-learned device link, you are actually creating a separate external link and assigning a fiber type to that external link. When the proNX Optical Director sees an external link and an auto-learned link sharing the same two endpoints, the proNX Optical Director uses the fiber type provisioned for the external link.

If you later physically unplug the fiber associated with the auto-learned device link, the auto-learned designation disappears from the table (in the Device Links Current page), but the entry remains to represent the newly created external link. You can delete this external link just like you can delete any other external link.



NOTE: Unlike a provisioned link, an auto-learned link to a ROADM port does not automatically place the ROADM port administratively in-service. You will need to manually place the port in-service or create the external link for the line span. One way of creating the external link is to edit the fiber type.

Device Link Validation

The proNX Optical Director validates device links for network-wide consistency. The following provisioning inconsistencies are detected and alarmed:

- Two or more device links share the same endpoint (that is, a port has a link to more than one device). The proNX Optical Director displays the inconsistent links in the table in the Device Links Current page. The inconsistent links are considered invalid and are not considered part of the topology.
- An auto-learned line span does not match the provisioned (expected) line span. The proNX Optical Director displays the inconsistent links in the table in the Device Links Current page. The auto-learned line span is considered valid and part of the topology. The provisioned (expected) line span is considered invalid and is therefore not part of the topology.

See the *TCX Series Optical Transport System Feature Guide* for information on all alarms.

About the Device Links Current Page

To access this page, click the **Network** tab and select **Device Links>Current** in the left-nav bar.



NOTE: In releases 2.1 and lower, this page is known as the Topology Provisioned page.

This page displays all the physical, external, and auto-learned device links on the discovered devices in your network. Note that the physical and external device links displayed are configured and might not represent the actual connectivity. When debugging

link problems, you should first verify that the configured device links match the actual connectivity. To assist in the debugging, the proNX Optical Director raises an alarm if it is able to detect a misconfigured link. See the *TCX Series Optical Transport System Feature Guide* for information on all alarms.

Tasks You Can Perform

You can perform the following tasks from this page:

- View a list of device links in your network.
- Delete a provisioned device link.
- Change the fiber type of an auto-learned device link by adding a provisioned external link based on the auto-learned device link.

Field Descriptions

Table 48 on page 122 explains the fields in the Device Links Current page.



NOTE: A single row in the table in the Device Links Current page can represent two links. A provisioned external link that is also auto-learned is displayed as a single row.

Table 48: Fields in the Device Links Current Page

Field	Description
Source Site	The name of the site where the source device is located.
Source Device	The name and/or IP address of the device at the source end of the link. A device is assigned as a source or a destination when you create the link.
Source Port	The name of the port at the source device.
Source State	The state of the port at the source device. The format is <i>operational-status (administrative-state)</i> . See Table 49 on page 123.
Destination Site	The name of the site where the destination device is located.
Destination Device	The name and/or IP address of the device at the destination end of the link. A device is assigned as a source or a destination when you create the link.
Destination Port	The name of the port at the destination device.
Destination State	<p>The state of the port at the destination device. The format is <i>operational-status (administrative-state)</i>. See Table 49 on page 123.</p> <p>The destination state is not displayed if the destination device is undiscovered or if the destination port does not exist.</p>

Table 48: Fields in the Device Links Current Page (continued)



Field	Description
Auto Learned (via LLDP)	<p>An indication of whether the link is auto-learned or not. Only line spans can be auto-learned.</p> <p>A  indicates that the link is auto-learned. A  indicates that the link is not auto-learned. An N/A indicates that the auto-learned designation does not apply because the device link is not a line span. See Table 50 on page 124.</p>
Provisioned Type	<p>The type of provisioned link:</p> <ul style="list-style-type: none"> Physical, for a device link where both endpoints are within the same ROADM element External, for a device link where one endpoint is outside of the ROADM element <p>The proNX Optical Director automatically determines the type based on the link endpoints. You do not explicitly provision the type.</p> <p>NOTE: An Incomplete designation is displayed for links on ROADM or ILA line ports when the far end of a link cannot be reconciled. This can occur when the far end port does not exist or when the far end port is an endpoint for another link.</p> <p>NOTE: This field can be empty for auto-learned line spans. See Table 50 on page 124.</p>
Provisioned Fiber Type	<p>The fiber type is one of the attributes used by the Optical Control Layer control algorithm. All common fiber types are supported:</p> <ul style="list-style-type: none"> Single Mode Fiber LS (SMF-LS) E-LEAF Dispersion Shifted Fiber TRUEWAVE Reduced Slope TRUEWAVE Classic NZ-DSF <p>This attribute is applicable to line spans only. The fiber type for universal port and client connections is Not Applicable.</p> <p>NOTE: The fiber type for an auto-learned line span is set to Single Mode Fiber by default. It is grayed out to indicate that it is a default setting and not a provisioned value. See Table 50 on page 124.</p>
Loopback	A loopback indication is shown if the source and destination link endpoints are the same.

Table 49: Port State and Status Values

Port State / Status	Valid Values
Administrative State	<ul style="list-style-type: none"> In-Service - laser is enabled Out-of-Service - laser is disabled
Operational Status	<ul style="list-style-type: none"> Up - port is operating normally Down - port has detected a problem (for example, loss of signal on input) or is no longer processing the incoming signal due to automatic line shutdown (ALS) procedures

Table 50: Valid Combinations for Auto-Learned and Provisioned Device Links

Auto Learned	Provisioned Type	Provisioned Fiber Type	Description
N/A	Physical	<empty>	Refers to a provisioned physical link.
N/A	External	<empty>	Refers to a provisioned external link that is not a line span.
✗	External	<any>	Refers to a line span that is provisioned.
✓	<empty>	Single Mode Fiber (gray font)	Refers to a line span that is auto-learned. The Fiber Type is set to Single Mode Fiber by default. It is grayed out to indicate a default setting and not a provisioned value.
✓	External	<any>	Refers to a line span that is both auto-learned and provisioned.

Viewing or Deleting a Link

Use this procedure to view a list of all links or to delete a specific link.

1. Click the **Network** tab and select **Device Links>Current** in the left-nav bar.
A table listing all provisioned and auto-learned links in the network is displayed.
2. If you want to delete a provisioned link, select the link (row) and click **Delete**. You can only delete a provisioned link. You cannot delete an auto-learned link.
A confirmation dialog appears. Click **Delete** to confirm.

When you delete a link, you should remove the physical fiber that the deleted link represents. This ensures that the configured topology matches the actual topology.



NOTE: Deleting a link that is provisioned and not auto-learned removes that link from proNX Optical Director control and management. This is service affecting for all services that traverse the link. You should not delete such a link if there are services that traverse the link. Additionally, if the deleted link has an endpoint on a TCX1000-RDM20 port, the port is automatically taken out of service (administratively).

Editing the Fiber Type

Use this procedure to change the fiber type of an auto-learned device link.

Note that you are not actually changing the fiber type. You are creating a new External link based on the auto-learned link and setting the fiber type of the newly created link.

If the line span being edited has an endpoint on a TCX1000-RDM20 port, that port is placed in service as a consequence of this task (because this task is equivalent to creating a device link).

1. Click the **Network** tab and select **Device Links>Current** in the left-nav bar.
A table listing all provisioned and auto-learned links in the network is displayed.
2. To change the fiber type for an auto-learned link, select the link (row) and click **Edit**.
You can only edit a link that has the auto-learned **X** designation.
The Edit Fiber Type dialog appears.
3. Specify the **Fiber Type** using the drop-down list.
4. Click **Save**.

This creates an External link based on the auto-learned link and sets the **Fiber Type** of the newly created link to the specified fiber type. If there are any endpoints on TCX1000-RDM20 ports, those ports are automatically placed in service (administratively).

About the Device Links Create Link Page

To access this page, click the **Network** tab and select **Device Links>Create Link** in the left-nav bar.

This page displays fields that you fill in to create a device link in your network.

Tasks You Can Perform

You can create device links from this page.

Field Descriptions

Table 51 on page 125 explains the fields in the Device Links Create Link page.

Table 51: Fields in the Device Links Create Link Page

Field	Description
Source ¹	
Site	The site of the source endpoint of the link.
Device	The name and/or IP address of the ROADM or ILA device at the source site.

Table 51: Fields in the Device Links Create Link Page (continued)

Field	Description
Circuit Pack	This can be one of the following at the source site: <ul style="list-style-type: none"> the name of the ROADM device within the ROADM node if the source is a ROADM device, or ILA, if the source is an ILA device, or the name of the circuit pack on the tail facility endpoint if the source is a tail facility endpoint
Port	The port on the above Circuit Pack at the source site.
Destination ¹	
Site	The site of the destination endpoint of the link.
Device	The name and/or IP address of the ROADM or ILA device at the destination site.
Circuit Pack	This can be one of the following at the destination site: <ul style="list-style-type: none"> the name of the ROADM device within the ROADM node if the source is a ROADM device, or ILA, if the source is an ILA device, or the name of the circuit pack on the tail facility endpoint if the source is a tail facility endpoint
Port	The port on the above Circuit Pack at the destination site.
Fiber Type	The type of fiber being used on a ROADM or ILA line port. It is not applicable for links on other ports. The fiber type is one of the attributes used by the Optical Control Layer control algorithm.
Loopback	This sets the destination link endpoint to be the same as the source link endpoint. This is not supported for live deployments and is for future use.

¹ The source and destination assignments are used only to distinguish between the two endpoints and can be assigned arbitrarily.

Creating a Link

Use this procedure to create a new link. [Table 52 on page 127](#) shows the allowed link endpoint combinations.

Table 52: Supported Optical Links

Source Link Endpoint ¹	Destination Link Endpoint ¹	Type ²
A line port on a TCX1000-RDM20 or a TCX1000-ILA	A line port on a TCX1000-RDM20 or a TCX1000-ILA	External
A universal port on a TCX1000-RDM20	A line port on an FMD96	Physical
A universal port on a TCX1000-RDM20	A line port on a 2D8CMD	Physical if the 2D8CMD belongs to the TCX1000-RDM20 External otherwise
A universal port on a TCX1000-RDM20	A supported tail facility endpoint on Juniper Networks equipment. See Table 2 on page 24 .	External
A client port on an FMD96 ³ or on a 2D8CMD	A supported tail facility endpoint on Juniper Networks equipment. See Table 2 on page 24 .	External

¹ The source and destination designations are used only to distinguish between the two link endpoints. They are assigned arbitrarily and are interchangeable.

² The proNX Optical Director implicitly determines the type based on the endpoints being interconnected. You do not explicitly provision the type.

³ The FMD96 is a fixed channel multiplexer/demultiplexer, which means that each client port is associated with a hardcoded fixed wavelength. When you create a link between an FMD96 client port and a tail facility endpoint, you must ensure that the tail facility endpoint is configured with a wavelength that matches the wavelength of the client port on the FMD96.

1. Click the **Network** tab and select **Device Links>Create Link** in the left-nav bar.
The Device Links Create page appears.
2. Use the drop-down lists to populate the source **Site**, **Device**, **Circuit Pack**, and **Port**.
When you select the **Site**, the **Device** drop-down list only shows the devices at that site. When you select the **Device**, the **Circuit Pack** drop-down list only shows the circuit packs on that device. When you select the **Circuit Pack**, the **Port** drop-down list only shows the ports on that circuit pack.
3. Use the drop-down lists to populate the destination **Site**, **Device**, **Circuit Pack**, and **Port**.

Only those destinations that can be connected to the source are available for selection. See [Table 52 on page 127](#) for details.

4. Use the drop-down list to select the **Fiber Type**.
5. Click **Create** to create the link or **Reset** to discard your changes.

When you create a link on a TCX1000-RDM20 port, the proNX Optical Director places the port in service (administratively) and places the link under proNX Optical Director control.



NOTE: Once the link is created, the link endpoint ports will no longer be available for selection in the drop-down lists. It might take a minute or two before the port availability in the drop-down list is updated. If you try to create another link before the drop-down list is updated, be careful not to select a port that is already in use as a link endpoint.

Services

- [Services Overview on page 128](#)
- [About the Services Provisioned Page on page 132](#)
- [Orphan Service on page 134](#)
- [Viewing a Service on page 135](#)
- [Editing or Deleting a Service on page 137](#)
- [About the Services Create Page on page 138](#)
- [Creating a Single Path Service on page 140](#)
- [Creating a Protected Service on page 142](#)

Services Overview

An optical service provides wavelength connectivity between optical service endpoints and exists as a series of individual optical cross-connects that route the service wavelength through the multiplexers/demultiplexers, ROADMs, and line amplifiers that make up the optical network. The proNX Optical Director encapsulates this series of cross-connects into a single entity and displays it as an end-to-end light path.

Attached to each end of the optical service is the endpoint transponder. The endpoint transponder can be a standalone transponder or a transponding function integrated on packet equipment.

The connection between the endpoint transponder and the optical network edge is called the tail facility. The tail facility endpoint (that is, transponder) is not part of the optical network, but you can use the proNX Optical Director to configure the tail facility endpoint if the tail facility terminates on a supported transceiver port on Juniper Networks equipment. This is called a supported tail facility endpoint.

If the tail facility does not terminate on a supported transceiver port, the tail facility endpoint is known as an external or alien endpoint. You can connect an alien endpoint to the optical network but you will need to configure the alien endpoint using the external equipment's management system.

When you create an optical service using the proNX Optical Director, you specify the wavelength and the two endpoints that the wavelength interconnects. The endpoint that you specify can be an optical service endpoint (that is, an optical port at the optical network edge) or a supported tail facility endpoint:

- If the service connects to a supported tail facility endpoint, then you can specify the tail facility endpoint directly when you create the service. The proNX Optical Director automatically determines where the optical service endpoints are based on the configured device links and sets up the optical service between the optical service endpoints.
- If the service connects to an alien endpoint, then the endpoint you specify is the optical port that attaches to the alien endpoint at the optical network edge. This can be a topologically-unconnected universal port on a TCX1000-RDM20 if the alien device is attached directly to that port, or a universal port on a TCX1000-RDM20 that is topologically connected to a multiplexer/demultiplexer. In this latter case, the alien device is attached to a client port on the multiplexer/demultiplexer.

Optical Service and Tail Facility Endpoints

This document describes two types of endpoints: the optical service endpoint and the tail facility endpoint.

The optical service endpoint refers to the port at the optical network edge that connects to the client transponder. This endpoint is part of the optical network.

The tail facility endpoint is the port on the client transponder that connects to the optical network edge. This endpoint is a client or a user of the optical network.

[Figure 5 on page 130](#) and [Table 53 on page 130](#) describe the allowed endpoints when you create a service. You can create a service from endpoints A, B, C, or D to endpoints E, F, G, or H.

Figure 5: Optical Service and Tail Facility Endpoints

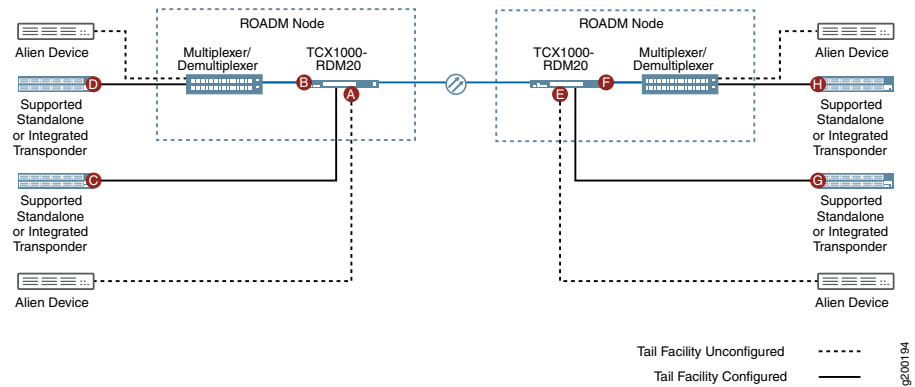


Table 53: Optical Service and Tail Facility Endpoints

Endpoint	Label	Usage
<p>An optical service endpoint where the endpoint is a topologically-unconnected universal port on a TCX1000-RDM20.</p> <p>This is a universal port that does not have a link associated with it.</p>	A or E	<p>You typically use this endpoint when you set up a service to an alien device that is attached directly to a universal port on the TCX1000-RDM20.</p>
<p>An optical service endpoint where the endpoint is a universal port on a TCX1000-RDM20 that is topologically connected to a multiplexer/demultiplexer.</p> <p>This is a universal port that has a link to a multiplexer/demultiplexer.</p>	B or F	<p>You typically use this endpoint when you set up a service to an alien device that is attached to a client port on the multiplexer/demultiplexer.</p>
<p>A supported tail facility endpoint where the endpoint is topologically connected to a universal port on a TCX1000-RDM20.</p> <p>This is a transceiver port at the supported tail facility endpoint.</p>	C or G	<p>You typically use this endpoint when you set up a service to a supported tail facility endpoint that is attached directly to a universal port on the TCX1000-RDM20.</p>
<p>A supported tail facility endpoint where the endpoint is topologically connected to a client port on a multiplexer/demultiplexer.</p> <p>This is a transceiver port at the supported tail facility endpoint.</p>	D or H	<p>You typically use this endpoint when you set up a service to a supported tail facility endpoint that is attached to a client port on the multiplexer/demultiplexer.</p>

The TCX1000-RDM20 has a pool of 20 universal ports that you can use to connect to other ROADM elements and/or to client transponders. For lower wavelength fan-out, you can deploy the TCX1000-RDM20 without a multiplexer/demultiplexer and use any available universal ports to connect directly to client transponders (labels A, C, E, G). For larger wavelength fan-out, you can deploy the TCX1000-RDM20 alongside a multiplexer/demultiplexer to give access to more wavelengths (labels B, D, F, H).

When creating a service to an alien tail facility endpoint, the endpoint you specify resides in the optical network (labels A, B, E, F) and does not include the tail facility itself. It is your responsibility to ensure that the alien endpoint is configured properly to connect to the optical network at those points.

When creating a service to a supported tail facility endpoint, the endpoint that you specify is the supported port on Juniper Networks equipment (labels C, D, G, H). See [Table 2 on page 24](#) for the list of supported tail facility endpoints.

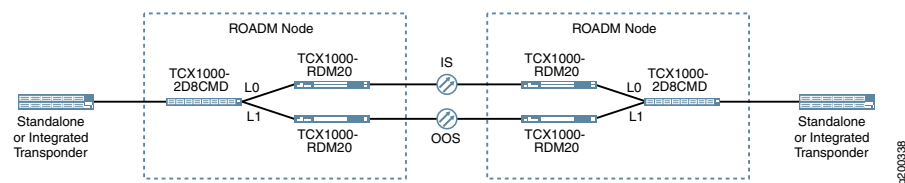
Single Path Service

A single path service is a service that has a single path set up between the two service endpoints. A fault on the path might cause the service to go down.

Protected Service

[Figure 6 on page 131](#) shows a protected service using a pair of two-degree ROADM nodes connected in a basic two-node ring. More complex ring and mesh configurations are possible as well.

Figure 6: Protected Service



A protected service is a service that has a pair of paths set up between the two service endpoints. One path is placed administratively in-service (IS) and the other path is placed administratively out-of-service (OOS). Under normal conditions, the IS path provides the optical connectivity. If a fault occurs in the current IS path, you can manually restore service by administratively disabling the current IS path and administratively enabling the current OOS path so that the current OOS path becomes the new IS path. This is called manual restoration. See [“Editing or Deleting a Service” on page 137](#) for instructions on how to change a service’s administrative state.



NOTE: It is up to the operator to ensure that one path is administratively in-service and the other path is administratively out-of-service. The prnX Optical Director does not enforce this but will raise an alarm if both paths are in-service.

A multi-degree colorless multiplexer/demultiplexer such as the TCX1000 2-Degree 8-Channel Colorless Mux/Demux (2D8CMD) is required at each end as the common endpoint for the protected service. The 2D8CMD has two line ports (L0 and L1) that connect to the two different degrees in the ROADM node, thereby supporting two paths between the endpoints.

A protected service is modeled as a pair of services where each service in the pair takes a different path across the network. The individual services in the pair are effectively single path services that share a common wavelength and common endpoints.

There are two ways to set up a protected service in the proNX Optical Director:

- You can configure the IS path and let the proNX Optical Director determine and configure the OOS path. This is the easier method.
- You can configure a single path service for the IS path and separately configure a single path service for the OOS path. The proNX Optical Director is then able to determine that you have created a protected service because the single path services that you created share the same wavelength and the same endpoints.

About the Services Provisioned Page

To access this page, click the **Network** tab and select **Services>Provisioned** in the left-nav bar.

This page lists all the provisioned optical services in the network.

Tasks You Can Perform

In addition to seeing the list of optical services in the network, you can view a specific optical service, edit a specific optical service including changing its administrative state, and delete a specific optical service from this page.

Field Descriptions

Table 54 on page 132 explains the fields in the Services Provisioned page.

Table 54: Fields in the Services Provisioned Page

Field	Description
Name	The name of the service. The name is set when you create the service.
Frequency	The optical frequency of the service. To see the corresponding wavelength and channel number, hover over the frequency value.

Table 54: Fields in the Services Provisioned Page (continued)

Field	Description
State	<p>The end-to-end state of the service. The format is <i>operational-status (administrative-state)</i>.</p> <p>The <i>operational-status</i> includes the port status at the tail facility endpoints but the <i>administrative-state</i> does not.</p> <p>The following are the valid values for the operational status:</p> <ul style="list-style-type: none"> • Up - All ports along the service path are up. • Down - At least one port along the service path is down. <p>The following are the valid values for the administrative state:</p> <ul style="list-style-type: none"> • In-Service - When you set the administrative state of an optical service to In-Service, all cross-connects along the service path are administratively placed in service. • Out-of-Service - When you set the administrative state of an optical service to Out-of-Service, all cross-connects along the service path are administratively placed out of service. • Degraded - The administrative state is displayed as Degraded if one or more TCX1000-RDM20 devices in the service's path has a cross-connect configured for the light path in one direction but not the other. This is a configuration issue and typically indicates a service activation failure. Check the current alarms as well as the task history. This value cannot be set directly by the user.
Source Site	The name of the site where the source device is located.
Source Device	<p>The name and/or the IP address of the device at the source.</p> <p>The source device can be an endpoint transponder attached to the optical network, or a ROADM element at the optical network edge.</p> <p>NOTE: The prnX Optical Director might display a device as a source or as a destination differently from how you assigned the device when you created the service.</p>
Source Port	<p>The port on the source device.</p> <p>If the source device is an endpoint transponder, then this field refers to a port on that transponder.</p> <p>If the source device is a ROADM element, then this field refers to a universal port on that ROADM.</p>
Destination Site	The name of the site where the destination device is located.
Destination Device	<p>The name and/or the IP address of the device at the destination.</p> <p>The destination device can be an endpoint transponder attached to the optical network, or a ROADM element at the optical network edge.</p> <p>NOTE: The prnX Optical Director might display a device as a source or as a destination differently from how you assigned the device when you created the service.</p>
Destination Port	<p>The port on the destination device.</p> <p>If the destination device is an endpoint transponder, then this field refers to a port on that transponder.</p> <p>If the destination device is a ROADM element, then this field refers to a universal port on that ROADM.</p>

Table 54: Fields in the Services Provisioned Page (continued)

Field	Description
Critical	The number of critical alarms on devices along the service path. ¹
Major	The number of major alarms on devices along the service path. ¹
Minor	The number of minor alarms on devices along the service path. ¹
SA	If the SA indicator is present, then service affecting alarms exist.
¹ This is a count of the following alarms in optical network equipment along the service path (including alarms at the tail facility endpoints): <ul style="list-style-type: none"> • port and EDFA alarms in the service path • connection and channel alarms in the service path 	

Orphan Service

An orphan service is a service without two add/drop endpoints. If you see an orphan service displayed, it is an indication that you have misconfigured the ROADM topology or otherwise altered the ROADM topology (such as unplugging and plugging fibers to different devices when LLDP is enabled) after the service is created.

The proNX Optical Director only allows you to create an optical service if a path exists between the two add/drop endpoints at the time that you create the service. If, after you create the service, you change the ROADM topology (such as by deleting links or undiscovering ROADM devices) such that the original path no longer exists between the two endpoints, the proNX Optical Director shows the service as two orphan services, one for each endpoint.

The reason for this is that, after the ROADM topology change, the proNX Optical Director cannot reconcile the intended service path with the new ROADM topology and therefore cannot display the full service path. It is only able to display the path from each endpoint to where the topology is broken. Note that this behavior can be different for a cut fiber. In the case of a cut fiber on a line span, the proNX Optical Director still knows where the intended path is as long as the associated external link is provisioned. In this case, the service is shown with a link that is down, and not as a pair of orphan services.

When you fix the ROADM topology, the proNX Optical Director will display the service correctly once again.

To prevent this from happening, ensure you do not change the ROADM topology after you create the service.

Viewing a Service

Use this procedure to view a provisioned service.

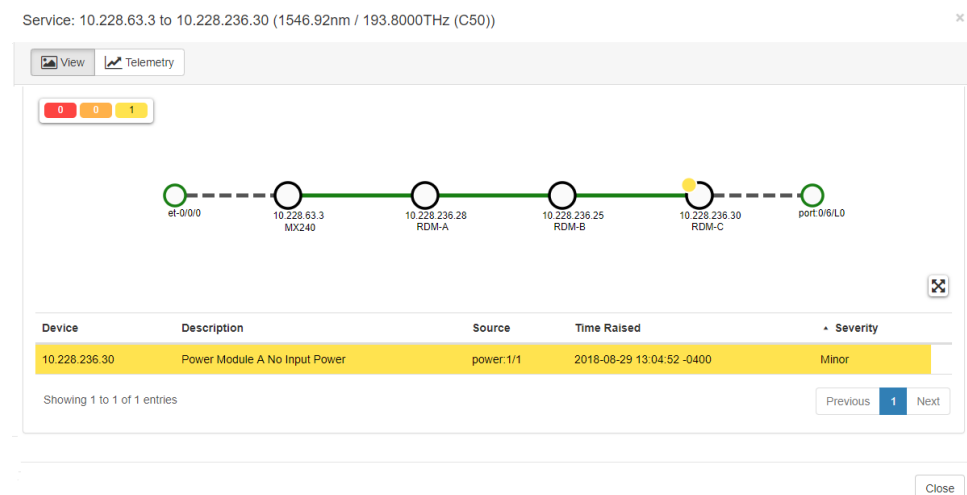
1. Click the **Network** tab and select **Services>Provisioned** in the left-nav bar.

A list of services in your network appears.

2. Select the service you want to view and click **View**.

The service appears in a new window. The window shows a visual representation of the service and the list of alarms associated with the devices that are part of the service. [Figure 7 on page 135](#) shows an example of the service view:

Figure 7: Service View Example



At the top is the title that indicates the source and destination devices and the wavelength used to connect them. The upper left corner of the main service view area shows a count of the number of alarms on the devices that are part of the service. In this case, there is one minor alarm. Below the alarm counts is a visual representation of the service, which shows the service endpoints connected to each other through two or more devices.

An endpoint of a service is displayed as follows:

- If the endpoint is a supported tail facility endpoint, then the endpoint is shown as an interface on the supported tail facility device.
- If the endpoint is an alien endpoint attached to a universal port on a TCX1000-RDM20, then the endpoint is shown as a universal port on the TCX1000-RDM20.
- If the endpoint is an alien endpoint attached to a client port on an FMD96, then the endpoint is shown as a client port on the FMD96.
- If the endpoint is an alien endpoint attached to a client port on a 2D8CMD, then the endpoint is shown as a line port on the 2D8CMD. The reason for displaying the

endpoint as a line port is that the 2D8CMD is colorless, so the wavelength is seen by all client ports (and not exclusively by a single client port) on the multiplexer/demultiplexer.



NOTE: The proNX Optical Director does not keep track of which 2D8CMD client port is physically connected to the alien endpoint. You will need to keep track of that physical connection yourself.

In this example, the service view shows a service with an endpoint on an MX Series router on the left connecting across ROADM elements to an alien endpoint on the right. You can see that this is an alien endpoint because the service view shows the endpoint as a port on a ROADM element, in this case, a line port on a 2D8CMD, which you can confirm by hovering over the endpoint to see the endpoint details (see [Figure 8 on page 136](#)).

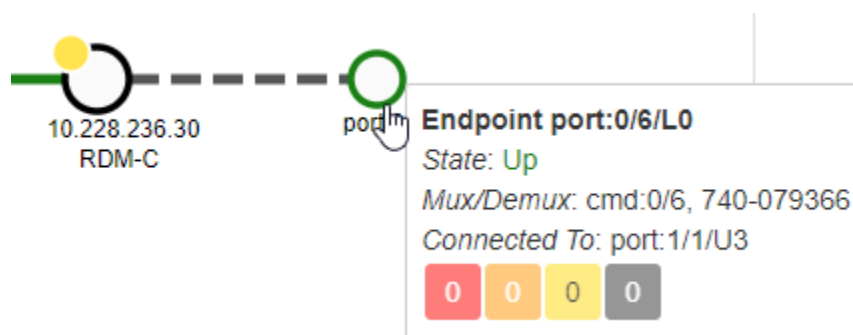
The service representation is color-coded as follows:


- An endpoint is green if the port that it represents is administratively in-service. An endpoint is red if the port that it represents is administratively out-of-service.
- Links between devices are shown with solid lines. The line is green if the link is operationally up. The line is red if the link is operationally down.

Below the service view is an alarms table showing the current alarms on the devices that are part of the service. See [“Field Descriptions” on page 40](#) for a description of the table headings.

3. Hover over links, devices, and ports to see more information on a link, device, or port.
For example:

Figure 8: Hovering on an Endpoint

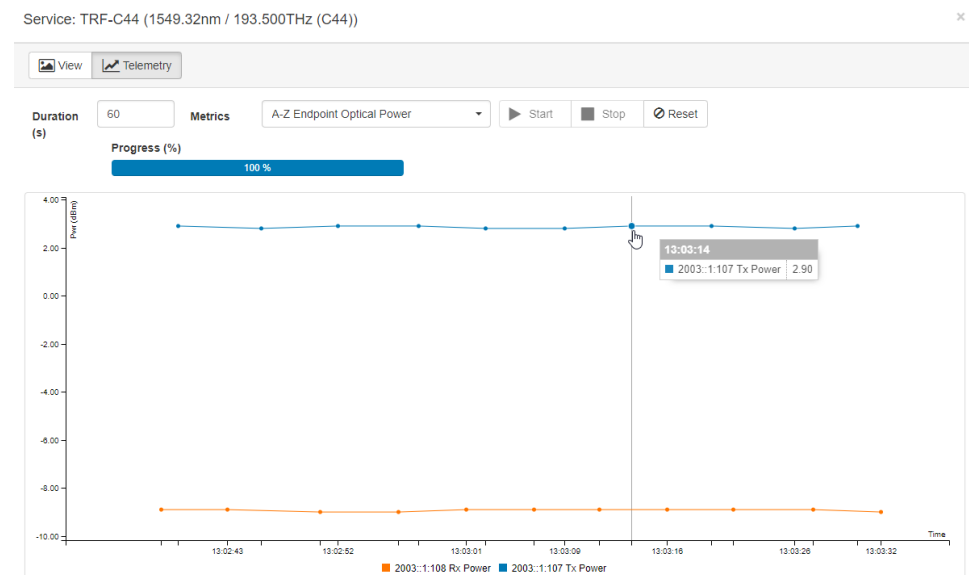


4. You can pan the service view and zoom in and out using the scroll wheel as desired.
To reset the view, click the **Reset View**  icon.
5. To view and graph telemetry data, click the **Telemetry** button. The Telemetry panel appears.

- Specify the time **Duration** that you want to view and graph the telemetry data.
- Select the telemetry **Metric** from the drop-down list. You have the option of selecting the transmit and receive power pairs in each direction. You can only select one direction at a time.
- Click **Start** to start telemetry data collection and graphing.
- Click **Pause** to pause the graphing of telemetry data. Telemetry data continues to be collected when paused. To continue graphing, click **Start**.
- Click **Stop** to stop telemetry data collection and graphing prior to duration expiry.
- Click **Reset** to clear the graph.

Figure 9 on page 137 shows an example of the type of graph you can generate:

Figure 9: Service Telemetry Graph Example



- Click **Close** to close the service window.

Editing or Deleting a Service

Use this procedure to view, edit (including changing the administrative state), or delete a provisioned service.

- Click the **Network** tab and select **Services>Provisioned** in the left-nav bar.
A list of services in your network appears.
- To edit a service, select a service and click **Edit**.
The Edit Service dialog appears.
 - To change the **Service Name**, type the new service name in the box.

- To change the **Admin State**, use the drop-down list to specify the new administrative state. When you change the state to **IS**, the proNX Optical Director sets all cross-connects along the service path to In-Service. When you change the state to **OOS**, the proNX Optical Director sets all cross-connects along the service path to Out-of-Service.

Click **Save** to save your changes or **Cancel** to discard them.

3. To delete a service, select a service and click **Delete**.

A confirmation dialog appears. Click **Delete** to confirm.

About the Services Create Page

To access this page, click the **Network** tab and select **Services>Create Service** in the left-nav bar.

This is the main page where you create an optical service.

Tasks You Can Perform

You can create an optical service between specified endpoints. See [Table 53 on page 130](#) for the different endpoints that you can specify. As part of service creation, the proNX Optical Director automatically configures the cross-connects on all the devices along the service path.

Field Descriptions

[Table 55 on page 138](#) explains the fields in the Services Create page.

Table 55: Fields in the Services Create Page

Field	Description
Service Type	<p>Specify whether the service is Single Path or Protected.</p> <p>A single path service is a service that has only a single path set up between the two service endpoints.</p> <p>A protected service is a service that has a pair of paths set up between the two service endpoints. When you create a protected service, you specify the in-service (IS) path, and the proNX Optical Director automatically determines and configures the out-of-service (OOS) path.</p>
Source	
Site	The name of the site where the source device is located.
Device	<p>The name and/or the IP address of the source device.</p> <p>The source device can be an endpoint transponder attached to the optical network, or a ROADM element at the optical network edge.</p> <p>NOTE: A multiplexer/demultiplexer is modeled as part of a ROADM element.</p>

Table 55: Fields in the Services Create Page (continued)

Field	Description
Endpoint	<p>The port on the source device.</p> <p>If the source device is an endpoint transponder, then this field specifies a port on that transponder.</p> <p>If the source device is a ROADM element, then this field specifies a universal port on that ROADM.</p> <p>In both cases, the drop-down list shows entries with annotations that further describe the entries:</p> <ul style="list-style-type: none"> • If the endpoint is a port on a transponder, the annotations show which universal port(s) the transponder port is connected to and whether the connection is going through a multiplexer/demultiplexer. • If the endpoint is a port on a ROADM element, the annotations show which universal ports are not connected, which universal ports are connected to a multiplexer/demultiplexer, and which universal ports are connected directly to an endpoint transponder.
Destination	
Site	The name of the site where the destination device is located.
Device	<p>The name and/or IP address of the destination device.</p> <p>The destination device can be an endpoint transponder attached to the optical network, or a ROADM element at the optical network edge.</p> <p>NOTE: A multiplexer/demultiplexer is modeled as part of a ROADM element.</p>
Endpoint	<p>The port on the destination device.</p> <p>If the destination device is an endpoint transponder, then this field specifies a port on that transponder.</p> <p>If the destination device is a ROADM element, then this field specifies a universal port on that ROADM.</p> <p>In both cases, the drop-down list shows entries with annotations that further describe the entries:</p> <ul style="list-style-type: none"> • If the endpoint is a port on a transponder, the annotations show which universal port(s) the transponder port is connected to and whether the connection is going through a multiplexer/demultiplexer. • If the endpoint is a port on a ROADM element, the annotations show which universal ports are not connected, which universal ports are connected to a multiplexer/demultiplexer, and which universal ports are connected directly to an endpoint transponder.
Details	
Wavelength	The wavelength of the service.

Table 55: Fields in the Services Create Page (continued)

Field	Description
Admin State	The administrative state of the service. For a protected service, this is the administrative state of the IS path.
Name	Optional, the name of the service.
Computed Path Options	
Index	An index assigned by the proNX Optical Director for this entry. This index is only used on this page. It is not referred to or displayed on other pages.
Service Name	A name assigned by the proNX Optical Director to describe the service. This name is only used on this page. It is not referred to or displayed on other pages.
Path Description	The path that the service takes across the network.
Service Preview	A visual preview of the service. The service is shown from universal port to universal port. The tail facility and the multiplexer/demultiplexer ports (if applicable) are not displayed.

Creating a Single Path Service

Prerequisites

- The topology has been configured such that a service path can be set up between the desired endpoints.
- All ports along the service path are administratively enabled. Ports on the TCX1000-RDM20 are administratively enabled automatically if a link is configured on that port. If a link is not configured on that port, such as if your service endpoint is on a TCX1000-RDM20 universal port (to connect to alien equipment), then be sure to administratively enable that port manually. See [“Configuring a Port” on page 101](#) for information on how to do this.

Use this procedure to create a new single path optical service.

1. Click the **Network** tab and select **Create Service** in the left-nav bar.

The Services Create page appears.

2. Set the **Service Type** to **Single Path**.
3. Use the drop-down lists to specify the source and destination **Site**, **Device**, and **Endpoint**. Once you select the **Site**, the **Device** drop-down list only shows the devices at the selected site. Once you select the **Device**, the **Endpoint** drop-down list only shows the ports on the selected device.



NOTE: The source and destination assignments are used only to distinguish between the two endpoints and can be assigned arbitrarily.

How you select the Endpoint from the drop-down lists differs slightly depending on the type of endpoint (see [Table 56 on page 141](#)).

Table 56: Port Selection Based on Type of Endpoint (Single Path)

Type of Endpoint	Port Selection
Supported Tail Facility Endpoint	<p>Select the tail facility endpoint directly using the drop-down lists by selecting the tail facility device and port. This is the easiest method.</p> <p>Alternatively, you can proceed as follows:</p> <ul style="list-style-type: none"> • If the supported tail facility endpoint is topologically connected to a universal port on a TCX1000-RDM20, select the universal port. To help you select the correct universal port, the Endpoint drop-down list shows annotations that identify the tail facility endpoint connected to that universal port. • If the supported tail facility endpoint is topologically connected to a client port on a multiplexer/demultiplexer, select the universal port on the TCX1000-RDM20 that is connected to the multiplexer/demultiplexer. To help you select the correct universal port, the Endpoint drop-down list shows entries with annotations that identify the tail facility endpoints reachable from that universal port. There can be more than one tail facility endpoint displayed for the same universal port because different tail facility endpoints can connect to different client ports on the same multiplexer/demultiplexer. Pick the entry with the annotation to the desired tail facility endpoint. <p>NOTE: If you are setting up a service to a supported tail facility endpoint attached to a 2D8CMD, the Endpoint drop-down list might show multiple entries to the same tail facility endpoint because there might be multiple paths to that endpoint (via line port L0 or L1). Look through the annotated entries to pick the entry that uses the desired line port on that device.</p>
Alien Endpoint	<p>Select the universal port on the TCX1000-RDM20 as follows:</p> <ul style="list-style-type: none"> • If the alien device is attached directly to the TCX1000-RDM20, select the universal port on the TCX1000-RDM20 that is attached to the alien device. This port is topologically unconnected. • If the alien device is attached to a client port on a multiplexer/demultiplexer, select the universal port on the TCX1000-RDM20 that is topologically connected to the multiplexer/demultiplexer. To help you select the correct universal port, the Endpoint drop-down list shows annotations that identify the multiplexer/demultiplexer connected to that universal port. <p>NOTE: The same multiplexer/demultiplexer might have a mix of client ports, with some attached to alien endpoints and others attached to supported tail facility endpoints. In this case, the Endpoint drop-down list shows multiple annotated entries for the universal port connecting to that multiplexer/demultiplexer. Select the entry for the port and not the entries with the annotated supported tail facility endpoints.</p> <p>NOTE: The proNX Optical Director does not keep track of which 2D8CMD client port is physically connected to the alien endpoint. You will need to keep track of that physical connection yourself.</p>

4. Specify the **Wavelength**.

You cannot change the wavelength if the endpoints that you specify are already associated with a wavelength. For example, if you specify a tail facility endpoint that is already configured for a specific wavelength, the proNX Optical Director uses that wavelength for the service.

5. Set the **Admin State** of the service.

6. Optionally, specify the **Name** of the service.

7. Scroll down to verify the Computed Path Options.

The Computed Path Options consist of a list of all possible paths and a service preview. The proNX Optical Director chooses one of the paths to display in the preview.

Use the scroll wheel to zoom in or out in the service view. To reset the view, click the

Reset View  icon.

8. Select the path you want to create (if multiple paths exist) and click **Create** to create the service. Otherwise, click **Reset** to discard your changes and start over.

The proNX Optical Director sets up the service by configuring the cross-connects on all devices along the service path. To monitor the progress of this task, see [“Viewing the Tasks List” on page 147](#).

Creating a Protected Service

Prerequisites

- The topology has been configured such that more than one service path can be set up between the desired endpoints.
- The tail facility endpoint (whether supported or alien) must be attached to a client port on a multi-degree colorless multiplexer/demultiplexer such as the TCX1000 2-Degree 8-Channel Colorless Mux/Demux (2D8CMD).

Use this procedure to create a new protected optical service between endpoints attached to client ports on 2D8CMD multiplexer/demultiplexers.

1. Click the **Network** tab and select **Create Service** in the left-nav bar.

The Services Create page appears.

2. Set the **Service Type** to **Protected**.

When you set the **Service Type** to **Protected**, you configure the IS path in the steps below. You do not need to explicitly configure the OOS path. The proNX Optical Director automatically determines and configures the OOS path for you. The Computed Path Options for both the IS path and the OOS path are displayed at the bottom of the page.

3. Use the drop-down lists to specify the source and destination **Site**, **Device**, and **Endpoint** for the IS path. Once you select the **Site**, the **Device** drop-down list only shows the devices at the selected site. Once you select the **Device**, the **Endpoint** drop-down list only shows the ports on the selected device.



NOTE: The source and destination assignments are used only to distinguish between the two endpoints and can be assigned arbitrarily.

How you select the Endpoint from the drop-down lists differs slightly depending on the type of endpoint (see [Table 57 on page 143](#)).

Table 57: Port Selection Based on Type of Endpoint (Protected)

Type of Endpoint	Port Selection
Supported Tail Facility Endpoint	<p>Select the tail facility endpoint directly using the drop-down lists by selecting the tail facility device and port.</p> <p>NOTE: If you set up the topology correctly, the Endpoint drop-down list shows multiple entries to the same tail facility endpoint because there are multiple paths to that endpoint (via line port L0 or L1). Look through the annotated entries to pick the entry that corresponds to the desired IS path.</p>
Alien Endpoint	<p>Select the L0 or L1 port on the 2D8CMD that corresponds to the desired IS path.</p> <p>NOTE: The proNX Optical Director does not keep track of which 2D8CMD client port is physically connected to the alien endpoint. You will need to keep track of that physical connection yourself.</p>

4. Specify the **Wavelength**.

You cannot change the wavelength if the endpoints that you specify are already associated with a wavelength. For example, if you specify a tail facility endpoint that is already configured for a specific wavelength, the proNX Optical Director uses that wavelength for the service.

5. Set the **Admin State** of the service. This is the administrative state of the IS path.

You cannot set the administrative state of the OOS path. It is always OOS when you create the service.

6. Optionally, specify the **Name** of the service.

7. Scroll down to verify the Computed Path Options for both the IS and OOS paths. The proNX Optical Director automatically determines and configures the OOS path based on the wavelength and endpoints you select for the IS path.

Use the scroll wheel to zoom in or out in the service view. To reset the view, click the

Reset View  icon.

8. Select the path you want to create (if multiple paths exist) and click **Create** to create the service. Otherwise, click **Reset** to discard your changes and start over.

The proNX Optical Director sets up the service by configuring the cross-connects on all devices along the IS and OOS service paths. To monitor the progress of this task, see [“Viewing the Tasks List” on page 147](#).

CHAPTER 6

Administration

- [Tasks on page 145](#)
- [Users on page 147](#)
- [File Servers on page 154](#)
- [Security on page 157](#)
- [Reports on page 164](#)

Tasks

- [About the Tasks Page on page 145](#)
- [Viewing the Tasks List on page 147](#)

About the Tasks Page

To access this page, select the **Administration** tab and click **Tasks** in the left-nav bar.

The Tasks page shows you the list of tasks that the proNX Optical Director is running. The displayed tasks relate to interactions between the proNX Optical Director and the devices under management. It can consist of tasks that are internally generated to control the devices and tasks that you create as part of device and network management.

Tasks You Can Perform

You can view the list of proNX Optical Director tasks and their status. You can also view additional details for a specific task or view any subtasks if applicable.

Field Descriptions

[Table 58 on page 146](#) explains the fields in the Tasks page.

Table 58: Fields in the Tasks Page

Field	Description
Type	<p>The type of task or subtask:</p> <ul style="list-style-type: none"> • Device Edit - editing a device • Discovery - discovering a device • Historic Metric Collection - retrieving PM metrics from a device • Interface Edit - editing an interface on the device • Log Collection - retrieving logs from a device • NE Backup - backing up the configuration database from a device • NE Restore - restoring a configuration database to a device • Service Edit - editing a service • Software Upgrade - upgrading software on a device • System Info Edit - editing the system information on a device • Telemetry Subscription - configuring a device for OTI connectivity (created and launched by the system) • Un-discovery - unregistering a device from control and management
Create Time	The start time of the task or subtask.
End Time	The end time of the task or subtask. If the task is not yet complete, this field is blank.
Owner	<p>The entity that launched the task or subtask. Tasks launched by the system are labelled as system. Tasks launched by a user are labelled by username.</p> <p>Users with the User role can only see tasks that they launch themselves. Users with the Administrator role can see all tasks including system tasks and tasks launched by other users.</p>
Status	<p>The status of the task or subtask:</p> <ul style="list-style-type: none"> • Pending - The task or subtask has been created. • Received - The task or subtask has been received by the microservice that will execute it. • Started - The task or subtask has started but has not finished. • Success - The task or subtask has finished successfully. • Finished - The task has finished but at least one subtask has failed. • Failure - The task or subtask has failed. <p>NOTE: The proNX Optical Director has no control over how long a device takes to complete a task. In some situations, the proNX Optical Director might time out and mark a task as failed. Since the proNX Optical Director does not cancel a task when it times out, the device can continue to complete the task successfully. If the task details of a failed task indicate the failure is due to a timeout, be sure to double check to determine whether the task has indeed failed or not.</p>
Details	An explanation of the task or subtask.

Viewing the Tasks List

Use this procedure to view the list of tasks that the proNX Optical Director has launched.

1. Select the **Administration** tab and click **Tasks** in the left-nav bar.

A table displaying the list of tasks is displayed. See [Table 58 on page 146](#) for an explanation of the fields.

2. To see details for a task, click a task and select **View**.

A Task Details window appears for the selected task. Click **Close** to close the window.

3. Some tasks have subtasks.

- To see the subtasks for a task, click a task and select **Subtasks**. The Subtasks window appears listing the subtasks for the selected tasks.
- To see details for a subtask, click the subtask in the Subtasks window and select **View**. The Subtask Details window appears for the selected subtask. Click **Close** to close the window.

4. To search, copy, print, or save the table, see [“Working with Tables” on page 22](#).

Users

- [About the User Management Page on page 147](#)
- [Viewing the List of Local Users on page 149](#)
- [Adding a Local User on page 149](#)
- [Editing a Local User on page 150](#)
- [Deleting a Local User on page 150](#)
- [Resetting a Local User's Password on page 151](#)
- [Activating or Deactivating a Local User on page 152](#)
- [About the User Tracker Page on page 153](#)
- [Tracking Users in Real-Time on page 153](#)

About the User Management Page

To access this page, select the **Administration** tab and click **Users>User Management** in the left-nav bar.

The User Management page displays the users that are allowed to log in to the proNX Optical Director with local user authentication.



NOTE: You must have Administrator privileges to access the User Management page.

Tasks You Can Perform

You can perform the following actions on this page:

- View the list of local users.
- Create a new local user.
- Edit the information for an existing local user.
- Reset a local user's password.
- Activate or deactivate a local user.

Field Descriptions

Table 59 on page 148 explains the fields in the User Management page.

Table 59: Fields in the User Management Page

Field	Description
Login	The login name of the user
Email	The email address of the user
Activated or Deactivated	<p>Users who are activated are shown with an Activated indication. An Activated user is allowed to log in and use the proNX Optical Director.</p> <p>Users who are deactivated are shown with a Deactivated indication. A Deactivated user is not allowed to log in and use the proNX Optical Director.</p> <p>NOTE: A deactivated user can still be logged in to the proNX Optical Director. See “Activating or Deactivating a Local User” on page 152 for information on when a deactivation takes effect.</p>
Reset	<p>Users whose passwords should be reset are shown with a Reset indication. This indication allows you to see which users still need to set their passwords. This indication is automatically set for new users and can be set for existing users. See “Resetting a Local User's Password” on page 151 for more information on setting the Reset indication and resetting passwords.</p> <p>NOTE: An existing user displayed with the Reset indication can still log in to the proNX Optical Director using his or her current password.</p>
Language	The language for the user
Role	<p>The role (privilege) of the user:</p> <ul style="list-style-type: none"> • Administrator – access to all proNX Optical Director functions • User – access to all proNX Optical Director functions except Users and File Servers selections in the Administration tab. Additionally, users with the User role can only see tasks that they launch themselves. They cannot see system tasks or tasks launched by other users.

Table 60: Fields in the Create a New User Page and the Edit an Existing User Page

Field	Description
Login	Specify the login name if you are creating a new user. You cannot change the login name if you are editing an existing user.
First name	Specify the first name of the user. This is optional.
Last name	Specify the last name of the user. This is optional.
Email	Specify the email address of the user. This email address must be unique.
Activated	This indicates whether the user has been activated or not. When creating a new user, this check box is unchecked. A new user is automatically activated once you finish creating the new user.
Language	Select the language from the drop-down list: <ul style="list-style-type: none"> • en - English • it - Italian
Role	Select the role from the drop-down list: <ul style="list-style-type: none"> • Administrator - access to all proNX Optical Director functions • User - access to all proNX Optical Director functions except Users and File Servers selections in the Administration tab.

Viewing the List of Local Users

Use this procedure to view the list of local users that are allowed to log in to the proNX Optical Director.

1. Select the **Administration** tab and click **Users>User Management** in the left-nav bar.
A table displaying the list of users is displayed. See [Table 59 on page 148](#) for an explanation of the fields.
2. To search, copy, print, or save the table, see “[Working with Tables](#)” on [page 22](#).

Adding a Local User

Use this procedure to add a local user.

1. Select the **Administration** tab and click **Users>User Management** in the left-nav bar.
A table displaying the list of users is displayed.
2. Click **New** to add a user. The Create a New User dialog appears.
See [Table 60 on page 149](#) for an explanation of the fields.
3. Specify the **First Name** and **Last Name** of the user.

4. Specify the **Email** address of the user.
5. Select the **Language** from the drop-down list.
6. Specify the **Role** for the user.
7. Click **Save** to add the user.

The dialog closes and the user you just added is shown in the user list with both the **Activated** and **Reset** indications. This indicates that the user has been activated and that the user's password should be reset.

8. If you do not want the new user to be activated, click the **Activated** button to toggle its setting. See [“Activating or Deactivating a Local User” on page 152](#) for more information.
9. Reset the user's password. See [“Resetting a Local User's Password” on page 151](#).
The new user cannot log in until his or her password is set.

Editing a Local User

Use this procedure to edit information for a local user.

1. Select the **Administration** tab and click **Users>User Management** in the left-nav bar.
A table displaying the list of users is displayed.

2. Select the user you want to edit and click **Edit**.

The Edit an Existing User dialog appears. See [Table 60 on page 149](#) for an explanation of the fields.

3. Update the **First name**, **Last name**, **Email**, **Language**, and **Role** as needed.
You cannot change the **Login** name.

4. Check or uncheck the **Activated** check box to activate or deactivate the user.
5. Click **Update** to save your changes.

The dialog closes and the user is updated.

Deleting a Local User

Use this procedure to delete a user.

1. Select the **Administration** tab and click **Users>User Management** in the left-nav bar.
A table displaying the list of users is displayed.

2. Select the user you want to delete and click **Delete**.

A confirmation dialog appears.

3. Click **Delete** to confirm.

The deleted user is removed from the user list.



NOTE: If the deleted user is currently logged in, the deletion does not take effect until the user logs out.

Resetting a Local User's Password

Use this procedure to reset a local user's password. You cannot use this procedure to reset your own password (that is, the password of the current user). To reset your own password, see ["Changing Your \(Local\) User Password" on page 21](#).

1. Select the **Administration** tab and click **Users>User Management** in the left-nav bar.

A table displaying the list of users is displayed.

2. Set the **Reset** indication for the user whose password you want to reset if the **Reset** indication is not already displayed

In order to reset a user's password, the user must be displayed with a **Reset** indication.

- For new users, the **Reset** indication is automatically displayed.
- For existing users, select the user and click **Reset** to turn on the **Reset** indication.

3. Select the user and click **View**.

The User Details window appears.

4. To change the password on behalf of the user, click **Reset Password**.

The Reset Password page appears.

- Enter the **New password**. The password is assessed with a Password strength indication.



NOTE: The password must be at least four characters long, but its assessed strength is not enforced.

- Retype the new password in the **New password confirmation** box.
- Click **Validate new password**. If the password and its confirmation do not match, re-enter the passwords.

After the password is validated, you will see a "Your password has been reset. Please sign in." message. This message is intended for the user when the user changes his or

her own password. You can ignore this message if you are changing the password on behalf of the user. You remain signed in to your current user session.

5. To let the user change his or her own password, click **Copy to Clipboard**.

This copies the Reset Password link to the clipboard where you can paste it in an email to send to the user. The link is saved to the clipboard with proper formatting. When you paste the link, you must paste it with the formatting included. Do not paste the link as plain text.

Click **Close** to close the User Details window.



NOTE: The user must change the password within 24 hours. If the password is not reset within a 24-hour period, the Reset Password link becomes invalid. Then, the administrator should delete and recreate the user account.

If you changed the password on behalf of the user, the user is now shown without the **Reset** indication. If you are letting the user change the password, the **Reset** indication continues to be shown until the user changes the password.

Activating or Deactivating a Local User

Use this procedure to activate or deactivate a user directly from the User Management page. When a user is activated, the user is allowed to log in to the proNX Optical Director. When a user is deactivated, the user is not allowed to log in to the proNX Optical Director.

1. Select the **Administration** tab and click **Users>User Management** in the left-nav bar.

A table displaying the list of users is displayed.

2. Select the user that you want to activate or deactivate.

If the user is currently activated, the user is shown with an **Activated** indication. If the user is currently deactivated, the user is shown with a **Deactivated** indication.

3. Toggle the **Activated** or **Deactivated** indications as desired.



NOTE: If you are deactivating a user and the user is currently logged in, the deactivation does not take effect until the user logs out.

About the User Tracker Page



NOTE: This feature has been deprecated starting in release 18.4.

To access this page, select the **Administration** tab and click **Users>User Tracker** in the left-nav bar.



NOTE: You must have Administrator privileges to access the User Tracker page.

The User Tracker provides you a real-time view of what other users are actively doing. The User Tracker maintains no history and therefore the User Tracker is empty when you first access the page. As users navigate the proNX Optical Director UI while you remain on the User Tracker page, the User Tracker starts to display which pages the active users are currently loading. Only those users who are actively loading pages appear in the list. Users who are logged in but are not active do not appear in the list because the User Tracker has no way of knowing what page an inactive user is on.

Tasks You Can Perform

You can perform the following actions on this page:

- View the list of active users currently logged in to the proNX Optical Director.
- See which page each active user has most recently viewed in real time.

Field Descriptions

Table 61 on page 153 explains the fields in the User Tracker page.

Table 61: Fields in the User Tracker Page

Field	Description
User	The login name of the user
IP Address	The IP address of the machine that the user has logged in from.
Current Page	The page that the user has most recently viewed.
Time	The time that the page was loaded.

Tracking Users in Real-Time

Use this procedure to track users in real-time.

1. Select the **Administration** tab and click **Users>User Tracker** in the left-nav bar.
An empty User Tracker page appears.

2. Remain on this page and wait for active users to appear.

This page is populated as active users navigate the proNX Optical Director UI. If you wait long enough, you will be able to see all the active users in the system. If a user logs out and closes his browser, the user is removed from the list.



NOTE: If you exit and reenter or refresh the User Tracker page, the User Tracker will be empty because the User Tracker does not maintain a history.

File Servers

- [About the File Servers Page on page 154](#)
- [Viewing the File Server List on page 155](#)
- [Adding a File Server to the File Server List on page 156](#)
- [Editing a File Server on page 157](#)
- [Deleting a File Server from the File Server List on page 157](#)

About the File Servers Page

To access this page, select the **Administration** tab and click **File Servers** in the left-nav bar.

The File Servers page lists the file servers that the proNX Optical Director is configured to use. The proNX Optical Director uses file servers for device software upgrades and device backup and restore operations.

Each file server entry is associated with a single protocol (FTP or SFTP). If you want the file server that you are configuring to be used for both FTP and SFTP access, then create two file server entries, one for each protocol.

Tasks You Can Perform

You can perform the following actions on this page:

- View the list of file servers that the proNX Optical Director can currently use.
- Specify a new file server for the proNX Optical Director to use.
- Edit the information for an existing file server.
- Remove an existing file server from the list of servers that the proNX Optical Director can use.

Field Descriptions

[Table 62 on page 155](#) explains the fields in the File Servers page.

Table 62: Fields in the File Servers Page

Field	Description
Server Name	The name of the FTP or SFTP server.
Protocol	<p>Supported protocols are FTP and SFTP. Only one protocol can be selected. If you want the server to support both protocols, create a separate file server entry for each.</p> <p>NOTE: The TCX1000-RDM20, TCX1000-ILA, and BTI7800 devices connect using SFTP.</p> <p>NOTE: The MX Series and PTX Series routers, the QFX Series switches, and the ACX6360 devices connect using FTP.</p>
IP Address	The IP address of the file server.
Username	The user login name for the file server.
Directory	The directory where you store and retrieve your files.
Operation Supported	<p>Indicates whether the server is the default server for the specified operation:</p> <ul style="list-style-type: none"> • DEFAULT_SFTP_STAGING - SFTP protocol, default for staging of files for log and metric collection • DEFAULT_SFTP_DB_BACKUP - SFTP protocol, default for device configuration backup • DEFAULT_FTP_STAGING - FTP protocol, default for staging of files for log and metric collection • DEFAULT_FTP_DB_BACKUP - FTP protocol, default for device configuration backup <p>If the entry is blank, then the server is not the default server for any operation.</p> <p>The default server is used for operations where you do not explicitly specify the server to use. These operations include automated backups, automated log and metric collection, and manual log and metric collection for some devices. See “Device Configuration Database Backups” on page 83, “Log Collection” on page 76, and “Metric Collection” on page 77.</p>
Description	The description of the server.

Viewing the File Server List

Use this procedure to view the list of file servers that the proNX Optical Director is configured to use.

1. Select the **Administration** tab and click **File Servers** in the left-nav bar.

A table displaying the list of file servers is displayed. See [Table 62 on page 155](#) for an explanation of the fields.

2. To search, copy, print, or save the table, see [“Working with Tables” on page 22](#).

Adding a File Server to the File Server List

Use this procedure to add a file server to the list.

1. Select the **Administration** tab and click **File Servers** in the left-nav bar.
A table displaying the list of file servers is displayed.
2. Click **New** to add a file server to this list. The Create a New File Server dialog appears.
3. Specify the **Server Name** of the server you want to add.
4. Specify the **Protocol** to use.
5. Specify the IPv4 or IPv6 **IP address** of the server you want to add.
6. Specify the protocol **Port** to use.
7. Specify the **Username** and **Password** to use to log in to the server.
8. Specify the **Directory** on the server where you will store and retrieve files. The directory path is relative to the (S)FTP user's login directory.

You can specify the directory directly or you can **Browse** to it. When you click **Browse**, the Select Directory dialog displaying a directory tree appears. Double-click a directory to see its contents. Highlight a directory and click **Select** to select it.
9. Specify the default operation(s), if any, that you want the server to support:
 - SFTP Staging - SFTP protocol, default for staging of files for log and metric collection
 - SFTP Backup - SFTP protocol, default for device configuration backup
 - FTP Staging - FTP protocol, default for staging of files for log and metric collection
 - FTP Backup - FTP protocol, default for device configuration backup



NOTE: The operation(s) you choose must be consistent with the Protocol you specify in 4 above.

10. Optionally, add a **Description** to describe this server.
11. Click **Save** to add the specified file server.

The dialog closes and the server you specify is shown in the file server list.

Editing a File Server

Use this procedure to edit a file server in the file server list.

1. Select the **Administration** tab and click **File Servers** in the left-nav bar.
A table displaying the list of file servers is displayed.
2. Select the file server you want to edit and click **Edit**.
The Edit an Existing File Server dialog appears.
3. Update the **Server Name**, **Protocol**, **IP address**, **Port**, **Username**, **Password**, and/or **Directory** as needed.
4. Click **Update** to save your changes.
The dialog closes and the server is updated.

Deleting a File Server from the File Server List

Use this procedure to delete a file server from the list.

1. Select the **Administration** tab and click **File Servers** in the left-nav bar.
A table displaying the list of file servers is displayed.
2. Select the file server you want to delete and click **Delete**.
A confirmation dialog appears.
3. Click **Delete** to confirm.

Security

- [About the Security Page on page 158](#)
- [Authentication Process on page 159](#)
- [Local User Authentication on page 159](#)
- [Vendor-Specific Attribute \(VSA\) Requirements for Remote Authentication on page 160](#)
- [Viewing the Authentication Server List on page 161](#)
- [Adding an Authentication Server to the Authentication Server List on page 162](#)
- [Editing an Authentication Server on page 163](#)
- [Deleting an Authentication Server from the Authentication Server List on page 163](#)
- [Changing the Authentication Server Order in the Authentication Server List on page 164](#)

About the Security Page

To access this page, select the **Administration** tab and click **Security** in the left-nav bar.



NOTE: Remote authentication is supported only using RADIUS servers in this release.

The Security page lists the remote authentication servers configured for proNX Optical Director user authentication.

The servers in this same list are also available to be selected for device user authentication. Device user authentication is used when you use the proNX Optical Director to discover a device. When you discover a device, you enter the login credentials in the Device Discovery dialog. These credentials are then authenticated by the device either locally on the device or by using a remote authentication server. To select a remote authentication server from this list for device user authentication, see [“About the Device Security Page” on page 69](#).

The servers are listed in alphabetical order in both lists. The order that the servers are listed is relevant. See [“Authentication Process” on page 159](#).

Tasks You Can Perform

You can perform the following actions on this page:

- View the list of remote authentication servers.
- Specify a new remote authentication server for this list.
- Edit the information for an existing remote authentication server.
- Remove an existing remote authentication server from this list.
- Change the order of remote authentication servers in this list. The order of the servers in this list dictates the authentication order.

Field Descriptions

[Table 63 on page 158](#) explains the fields in the Security page.

Table 63: Fields in the Security Page

Field	Description
Server Name	The name of the authentication server.
IP Address	The IP address of the authentication server.
Port	The protocol port to use.
Authorization Type	The type of authorization to use. Only radius-pap is supported.

Table 63: Fields in the Security Page (continued)

Field	Description
Attempts	The number of attempts to reach each server in the list during authentication.
Timeout	The number of seconds to wait for a response from each server during authentication.

Authentication Process

The authentication process is similar regardless of whether the authentication client is the proNX Optical Director or the device. For proNX Optical Director user authentication, the authentication client is the proNX Optical Director. For device user authentication, the authentication client is the device.

The order that the authentication servers are listed affects the authentication order. The server list for proNX Optical Director user authentication is shown in [“About the Security Page” on page 158](#). The server list for device user authentication is shown in [“About the Device Security Page” on page 69](#).

The servers are listed in alphabetical order in both lists. To change the position of a server in the list, change the server name by deleting and re-adding the server using a name that alphabetically positions the server in the desired position.

The authentication client tries to authenticate with the first server in the list. If the authentication client does not receive a response after **Timeout** seconds, the authentication client tries the next server in the list, and so on. If the authentication client goes through the whole list without receiving a response from any server, the authentication client cycles through the list again. The authentication client goes through the list for the number of times specified by the **Attempts** attribute.

If one of the authentication servers rejects the authentication request, or if none of the authentication servers responds to the authentication request within the period specified by the **Timeout** and **Attempts** attributes, local user authentication is performed.



NOTE: Set the **Timeout** and **Attempts** values such that the maximum time that authentication can take is under 5 seconds (for example, 3 attempts with a timeout of 1 second). This allows local authentication to take place in the unlikely event that the authentication servers are unreachable.

Local User Authentication

Local user authentication allows you to log in if the remote authentication servers are unreachable or if a misconfiguration causes the remote authentication servers to reject the login request. In these situations, the user is authenticated locally.

The credentials for local user authentication are stored in the local database. For the proNX Optical Director user, this is the proNX Optical Director database administered using **Administration > Users > User Management** (see [“About the User Management Page”](#))

on page 147). For the device user, this is the database stored on the device (see the respective device documentation).

The local and remote authentication databases are independent of each other. You can have the same or different usernames and you can have the same or different passwords in each database. The same username and password can be rejected by the remote authentication server but accepted by local user authentication, and vice versa. There is no correlation between the two databases.

Vendor-Specific Attribute (VSA) Requirements for Remote Authentication

Some authentication clients require vendor-specific attributes to be returned from the remote authentication server during the authentication process. These attributes can include an indication of the privilege level for the user being authenticated (Table 64 on page 160).

Table 64: Vendor-Specific Attribute (VSA) Requirements for RADIUS Authentication

Authentication Client	Requirement on the RADIUS Server	Required Attribute Values	Example Configuration (FreeRADIUS ¹)
proNX Optical Director	<p>Requires the RADIUS server to return the Juniper-Local-User-Name VSA in the Access-Accept message.</p> <p>This VSA is encapsulated within attribute 26 with the vendor ID set to the Juniper Networks ID number, 2636.</p> <p>The attribute value indicates the privilege level.</p>	Juniper-Local-User-Name (string): super-user	<p>dictionary file:</p> <pre> VENDOR Juniper 2636 BEGIN-VENDOR Juniper ATTRIBUTE Juniper-Local-User-Name 1 string END-VENDOR Juniper </pre> <p>users file:</p> <pre> Juniper-Local-User-Name := "super-user" </pre>

Table 64: Vendor-Specific Attribute (VSA) Requirements for RADIUS Authentication (continued)

Authentication Client	Requirement on the RADIUS Server	Required Attribute Values	Example Configuration (FreeRADIUS ¹)
TCX1000-RDM20	<p>Requires the RADIUS server to return both the Lumentum-CLI-Priv VSA and the Lumentum-SFTP-Priv VSA in the Access-Accept message.</p> <p>This VSA is encapsulated within attribute 26 with the vendor ID set to the Lumentum ID number, 46184.</p> <p>The attribute value indicates the privilege level.</p>	<p>Lumentum-NACM (string): read-write-exec</p> <p>Lumentum-CLI-Priv (string): admin</p> <p>Lumentum-SFTP-Priv (string): read-write</p>	<p>dictionary file:</p> <pre> VENDOR Lumentum 46184 BEGIN-VENDOR Lumentum ATTRIBUTE Lumentum-NACM 1 string ATTRIBUTE Lumentum-CLI-Priv 2 string ATTRIBUTE Lumentum-SFTP-Priv 3 string END-VENDOR Lumentum </pre> <p>users file:</p> <pre> Lumentum-NACM := read-write-exec Lumentum-CLI-Priv := "admin" Lumentum-SFTP-Priv := "read-write" </pre>
TCX1000-ILA	<p>Requires the RADIUS server to return the User-Role VSA in the Access-Accept message.</p> <p>This VSA is encapsulated within attribute 26 with the vendor ID set to the Oplink ID number, 7483.</p> <p>The attribute value indicates the privilege level.</p> <p>Alternatively, instead of using the User-Role VSA, the TCX1000-ILA can process the same attribute value (privilege level) in the Reply-Message attribute.</p>	<p>User-Role (integer): 2</p>	<p>dictionary file:</p> <pre> VENDOR Oplink 7483 BEGIN-VENDOR Oplink ATTRIBUTE User-Role 1 integer END-VENDOR Oplink </pre> <p>users file:</p> <pre> User-Role := 2 </pre>

¹ These examples are provided to illustrate the concepts only. Consult your RADIUS server vendor's documentation for proper configuration of the vendor-specific attributes.

NOTE: For RADIUS server requirements for devices not listed in the table, see the documentation for those devices.

Viewing the Authentication Server List

Use this procedure to view the list of remote authentication servers.

1. Select the **Administration** tab and click **Security** in the left-nav bar.

A table displaying the list of file servers is displayed in alphabetical order. See [Table 63 on page 158](#) for an explanation of the fields.

2. To search, copy, print, or save the table, see [“Working with Tables” on page 22](#).

Adding an Authentication Server to the Authentication Server List

Use this procedure to add an authentication server to the list.

1. Select the **Administration** tab and click **Security** in the left-nav bar.

A table displaying the list of authentication servers is displayed.

2. Click **New** to add an authentication server to this list. The Create a New Authentication Server dialog appears.

3. Specify the **Server Name** of the server you want to add.

Since the remote authentication servers are listed alphabetically, the name you give the server dictates where that server is placed in the list, which consequently influences the authentication order.

4. Specify the IPv4 or IPv6 **IP address** of the server you want to add.

5. Specify the **Secret** that the authentication client uses to communicate with the authentication server.

6. Specify the protocol **Port** to use.

7. Select the **Authorization Type** from the drop-down list.

8. Specify the **Attempts** and **Timeout** values.

For convenience, the product of these two values is shown in the **Delay** field. The **Delay** field indicates the maximum time in seconds that the RADIUS client waits for remote user authentication to complete. This field is informational and represents the time delay encountered when the remote authentication servers are unreachable. Keeping this delay under 5 seconds allows local user authentication to take place.

9. Click **Save** to add the specified authentication server.

The dialog closes and the server you just specified is shown in the server list.

Editing an Authentication Server

Use this procedure to edit an authentication server in the authentication server list.

1. Select the **Administration** tab and click **Security** in the left-nav bar.
A table displaying the list of authentication servers is displayed.
2. Select the authentication server you want to edit and click **Edit**.
The Edit an Existing Authentication Server dialog appears.
3. Update the **IP address**, **Secret**, **Port**, **Authorization Type**, **Attempts**, and/or **Timeout** as needed.
4. Click **Update** to save your changes.
The dialog closes and the server is updated.



NOTE: If you are currently using this server for device user authentication, the changes that you make are not automatically propagated to the device. In order to propagate the changes to the device, you have to delete and re-add this server from the Device Security page (see [“Adding or Deleting a RADIUS Server or Changing the RADIUS Security Options”](#) on page 70).

Deleting an Authentication Server from the Authentication Server List

Use this procedure to delete an authentication server from the list.

1. Select the **Administration** tab and click **Security** in the left-nav bar.
A table displaying the list of file servers is displayed.
2. Select the authentication server you want to delete and click **Delete**.
A confirmation dialog appears.



NOTE: If you are currently using this server for device user authentication, the confirmation dialog offers you the ability to delete the server from all device user authentication lists as well. This saves you the extra step of having to remove this server from all device user authentication lists.

3. Click **Delete** to confirm.

Changing the Authentication Server Order in the Authentication Server List

Use this procedure to change the order that the remote authentication servers are listed. The order is relevant for user authentication.

To change the placement of a particular server in the list, delete the server and add it back with a different name.

1. Select the authentication server you want to move and follow the procedure in [“Deleting an Authentication Server from the Authentication Server List” on page 163](#) to delete that server. It is recommended that you choose the option to delete the server from all device user authentication lists.
2. Follow the procedure in [“Adding an Authentication Server to the Authentication Server List” on page 162](#) to re-add the deleted server, but choose a server name that places the server in the desired position in the alphabetically ordered list.
3. If you are using this server for device user authentication, add the server back to the device user authentication lists. See [“About the Device Security Page” on page 69](#).

Reports ---

- [About the Reports Page on page 164](#)
- [Generating Reports on page 165](#)

About the Reports Page

To access this page, select the **Administration** tab and click **Reports** in the left-nav bar.

The Reports page is where you select the report(s) to generate on various aspects of the network in releases 18.4 and higher.

Tasks You Can Perform ---

You can generate one or more reports on various aspects of the network.

Field Descriptions ---

[Table 65 on page 165](#) explains the fields in the Reports page.

Table 65: Fields in the Reports Page

Field	Description
Available Categories	<p>The following types of reports are available:</p> <ul style="list-style-type: none"> • Optical Services • Sites • Users • AAA Servers • Devices • File Servers • Historical Alarms • Inventory • Device Links • Active Alarms • IETF Links • IETF Nodes
Selected Categories	The report(s) to be generated

Generating Reports

Use this procedure to generate reports for your network in releases 18.4 and higher.

1. Select the **Administration** tab and click **Reports** in the left-nav bar.
2. Select the reports to be generated. Use the **Add**, **Add All**, **Remove**, and/or **Remove All** buttons to move report types between the Available Categories and the Selected Categories columns.
3. Click **Report** to generate reports from the selected categories.

The reports are generated and downloaded as (.xlsx) files.

Release History Table

Release	Description
18.4	Use this procedure to generate reports for your network in releases 18.4 and higher.

CHAPTER 7

Appendix

- [Grafana on page 167](#)

Grafana

- [Overview on page 167](#)
- [Viewing a PM Graph on page 169](#)
- [Creating a Multi-PM Dashboard \(2 Metrics, 1 Entity, 1 Device\) on page 172](#)
- [Creating a Multi-PM Dashboard \(2 Metrics, 2 Entities, 2 Devices\) on page 178](#)

Overview

The proNX Optical Director software comes packaged with Grafana, a popular open platform used for analytics. You can use Grafana to query and visualize performance monitoring metrics from the proNX Optical Director's historical PM database to debug issues and observe trends on devices and links in your network.

The proNX Optical Director collects performance monitoring metrics from managed devices and stores the metrics in the proNX Optical Director's historical PM database. Performance monitoring metrics include a variety of counts and gauges that devices commonly measure and monitor to give indications of health and performance for components in the system. Most devices collect these metrics in 15-minute and 24-hour bins, and some devices collect them in 1-minute bins as well. A bin is a collection period over which the measurement samples are summarized (maximum/minimum/average), and the summaries are timestamped and stored.

The proNX Optical Director stores PM metrics in an Influx database. Each PM metric is stored in the database as a measurement. In Influx database terminology, a measurement is a container that holds the data being stored. A measurement is identified by a string. It is convenient to think of a measurement as a table and the string as the name of the table. In the historical PM database, a measurement is identified by a string in the following format:

```
<bin>/<ip_address>/<entity_type>/<metric_type>
```

An example of a measurement is **FIFTEEN_MIN/10.228.107.23/port/band-input-power**, which is the band-input-power metric in the 15-minute bin on a port on the device with the IP address specified.

Within each measurement, the data is organized as a table, as follows:

Table 66: Historical PM Measurement Table (Simplified View)

time	id	avg	max	min	value
This is the timestamp of the bin. For the 15-minute bins, the timestamps are every 15 minutes. Similarly, for the 24-hour bins, the timestamps are every 24 hours, and for the 1-minute bins, the timestamps are every minute.	This is the entity identifier where the metric was captured. For example, if the entity type was a port, then this identifier would specify the exact port on the device.	This is the average value of all samples of the metric within the bin period.	This is the maximum value of all samples of the metric within the bin period.	This is the minimum value of all samples of the metric within the bin period.	This is the value of the last sample of the metric within the bin period.

NOTE: The sampling frequency varies from device to device.

For example, here is a simplified view of a typical table stored in the historical PM database:

```

name: FIFTEEN_MIN/10.228.107.26/port/band-output-power
time      avg    id      max    min    value
----
2018-06-18T14:45:00Z 1.5    port:1_1_LINE_osc1 1.51  1.49  1.51
2018-06-18T14:45:00Z -50.72 port:1_1_LINE_osc2 -50.72 -50.72 -50.72
2018-06-18T14:45:00Z 6.24   port:1_1_LINE_total 6.31  6.18  6.27
2018-06-18T15:00:00Z -50.72 port:1_1_LINE_osc2 -50.72 -50.72 -50.72
2018-06-18T15:00:00Z 6.23   port:1_1_LINE_total 6.3    6.16  6.23
2018-06-18T15:00:00Z 1.5    port:1_1_LINE_osc1 1.51  1.5    1.5
2018-06-18T15:15:00Z 6.23   port:1_1_LINE_total 6.29  6.17  6.2
2018-06-18T15:15:00Z 1.5    port:1_1_LINE_osc1 1.51  1.5    1.5
2018-06-18T15:15:00Z -50.72 port:1_1_LINE_osc2 -50.72 -50.72 -50.72

```

Grafana allows you to create custom queries of the historical PM database and to graph the result. Examples of this are shown in the following sections. Note that the following sections are presented for your convenience to help you get started with Grafana. These sections are cursory and are not intended to replace official Grafana documentation. For official Grafana documentation, see docs.grafana.org. For more information on the Influx database, see <https://www.influxdata.com>.



NOTE: The screenshots used in the following sections are from the Grafana software packaged with proNX Optical Director release 2.1.

Viewing a PM Graph

Use this procedure to view a graph of a performance monitoring metric plotted over time. This procedure displays a metric from the 15-minute bin as an example, but the same procedure can be used to view metrics in other bins by simply selecting the appropriate dashboard.

Prerequisites

- You are using the proNX Optical Director to monitor your network and you have collected the metrics you want to display. The proNX Optical Director automatically collects metrics from managed devices every 12 hours. You can also collect metrics on demand. For information on collecting metrics on demand, see [“Collecting Metrics from a Device Manually” on page 79](#).

1. Access Grafana from your web browser.

- Releases 2.2 and lower - go to <http://<server-ip-or-hostname>:3000>
- Releases 18.4 and higher - go to <https://<server-hostname>/graphs>

This places you in the Home dashboard. You can also access Grafana from the proNX Optical Director UI by clicking on the **Analyze** button in the Devices Port Metrics page. See [“Viewing Historical Performance Monitoring Metrics” on page 105](#).

2. Click on the Home drop-down list to see the list of preconfigured dashboards. In addition to the Home dashboard, the proNX Optical Director software comes packaged with the following:

- 15min Metrics - a dashboard that displays the average, minimum, maximum, and last value of a metric from the 15-minute bin over a specified time period
- 1min Metrics - a dashboard that displays the average, minimum, maximum, and last value of a metric from the 1-minute bin over a specified time period
- 24h Metrics - a dashboard that displays the average, minimum, maximum, and last value of a metric from the 24-hour bin over a specified time period
- Cluster - a dashboard that displays usage information for the proNX Optical Director server cluster
- Pods - a dashboard that displays usage information for a selected pod

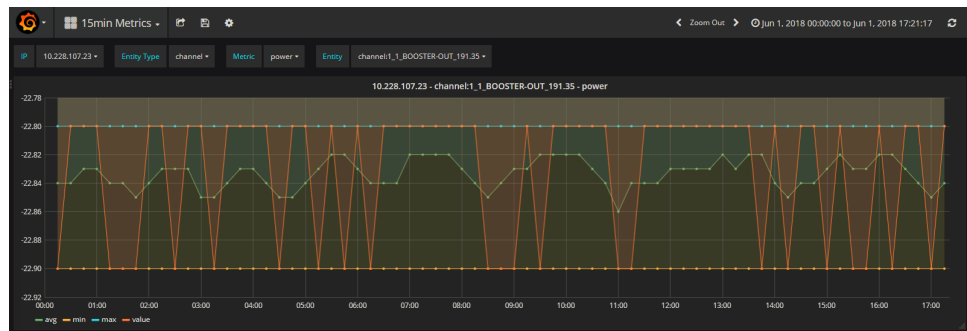
3. Select the **15min Metrics** dashboard (for example).

The 15min Metrics dashboard is displayed. The dashboard has a row of tabs at the top where you can select the entity and metric you want to view. These are called variables.

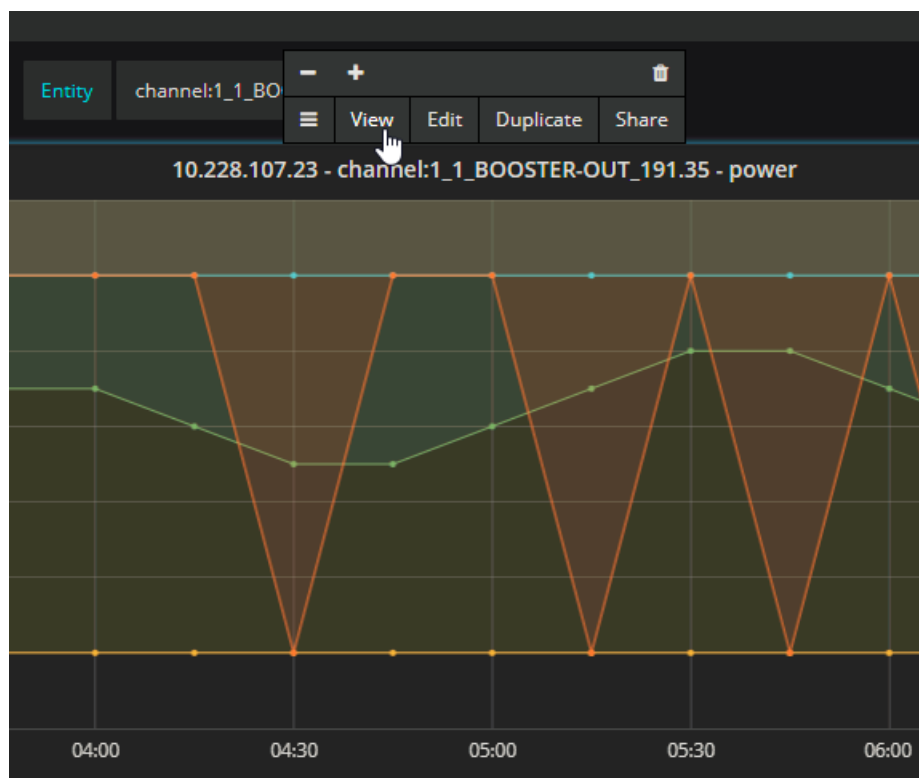
4. Select the date range from the upper right corner of the page. You have the option of selecting from predefined ranges or you can specify a custom range.

5. Select the IP address of the device from the **IP** variable drop-down list. This is the IP address of the device that you want to view.
6. Select the entity type from the **Entity Type** variable drop-down list. This is the type of entity or component that you want to view.
7. Select the metric from the **Metric** variable drop-down list. This is the metric you want to view.
8. Select the entity from the **Entity** variable drop-down list. This is the specific entity or component that you want to view.

A graph of the selected PM is displayed, for example:



9. To focus on a specific time range on the graph, click on the graph and drag your mouse horizontally to encompass the desired time range. When you release your mouse, the graph is redrawn with the new time range.
10. To view the graph in a full browser page, click the graph title and then select **View** in the ensuing pop-up, for example:



To return to the dashboard from the full browser view, click **Back to dashboard** at the top of the page.

Creating a Multi-PM Dashboard (2 Metrics, 1 Entity, 1 Device)


Use this procedure to create a dashboard that graphs two metrics from one entity on a device.

This procedure creates a dashboard that displays two metrics from the 15-minute bin as an example, but the same general procedure can be used to create a dashboard that displays metrics from other bins.

Prerequisites

- You are using the proNX Optical Director to monitor your network and you have collected metrics for the devices you want to analyze. The proNX Optical Director automatically collects metrics from managed devices every 12 hours. You can also collect metrics on demand. For information on collecting metrics on demand, see [“Collecting Metrics from a Device Manually” on page 79](#).
 - Familiarize yourself with the terminology and constructs described in [“Overview” on page 167](#).
- Follow the procedure in [“Viewing a PM Graph” on page 169](#) to bring up the 15min Metrics dashboard.


You will use this dashboard to create the new one. This approach allows you to reuse the same variables without having to recreate them.

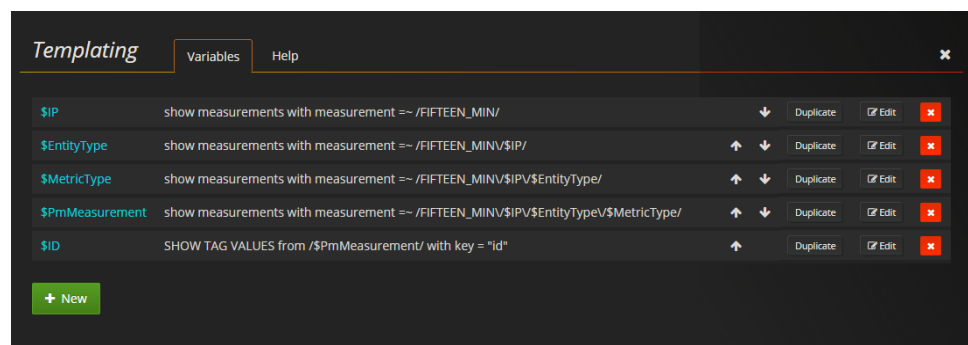
- Click the  icon at the top of the page and then select **Save As...**

Enter the new name for the dashboard and click **Save**.

You are now placed into the new dashboard. Since you have not made any changes yet, this dashboard is the same as the 15min Metrics dashboard.

- List the variables that are defined for this dashboard. Variables allow you to dynamically select which metric you want to graph when you view the dashboard.

Click the  icon at the top of the page and then select **Templating**. The Templating panel appears listing the variables that have been defined.



An explanation of these constructs is provided in the steps that follow.

4. Create a new metric type variable that allows you to select the second metric to graph. This new variable will appear in the variables row in the dashboard. For expediency, you will create the new variable from the existing variable.
 - a. Find the row for the **\$MetricType** variable and click **Duplicate**. The duplicated variable (**\$copy_of_MetricType**) is added to the bottom of the list of variables.
 - b. Click **Edit** for the duplicated variable. The Edit panel appears.
 - c. In the **Name** box in the Variable section, change the variable name to something more meaningful (for example, **MetricType2**).

The screenshot shows the 'Templating' interface with the 'Edit' tab selected. Under the 'Variable' section, the 'Name' field contains 'MetricType2' and is highlighted with a red circle. The 'Label' is 'Metric', 'Type' is 'Hide', and 'Query' is a dropdown menu. Below this is the 'Query Options' section, which includes a 'Data source' dropdown set to 'historic_metrics', a 'Refresh' dropdown set to 'On Dashboard Load', a 'Query' text field containing 'show measurements with measurement =~ /FIFTEEN_MINV\$IPV\$EntityType/', a 'Regex' text field containing '/FIFTEEN_MIN.*V([w-]+)/', and a 'Sort' dropdown set to 'Alphabetical (asc)'.

You do not need to make any changes to the Query Options section because this second metric type variable has the same characteristics as the first metric type variable. Here is an explanation of the query options:

- Query - Search through all measurements and look for measurements matching FIFTEEN_MIN/<IP address>/<Entity Type>. These represent the measurements in the 15-minute bins for the IP address and entity type that you specify in the IP variable and Entity Type variable drop-down lists in the dashboard.
- Regex - Additionally, from the results of the query, capture the last string containing word characters (a-z, A-Z, 0-9, _) and hyphens (-). The last string in a measurement is the metric type. In other words, this query looks through the database for all 15-minute bins matching the specified IP address and entity type, and presents all metric types found to the user through the Metric variable drop-down list.

- d. Scroll down and click **Update**. The new variable name is now shown in the list of variables.
5. Create a new PM measurement variable that uses the second metric. The PM measurement variable represents the measurement containing the metric being graphed. You will refer to this variable later when you define the graph. For expediency, you will create the new variable from the existing variable.

- a. Find the row for the **\$PmMeasurement** variable and click **Duplicate**. The duplicated variable (**\$copy_of_PmMeasurement**) is added to the bottom of the list of variables.
- b. Click **Edit** for the duplicated variable. The Edit panel appears.
- c. In the **Name** box in the Variable section, change the variable name to something more meaningful (for example, **PmMeasurement2**).
- d. In the Query Options section, change the query to use the new metric type. You accomplish this by clicking in the **Query** box and changing **\$MetricType** to **\$MetricType2**.

The screenshot shows the 'Templating' interface with the 'Edit' tab selected. Under the 'Variable' section, the 'Name' field is 'PmMeasurement2' (circled in red). Below it, the 'Label' is 'PmMeasurement'. In the 'Query Options' section, the 'Query' field contains the text 'show measurements with measurement =~ /FIFTEEN_MIN/\$IPV\$EntityTypeV\$MetricType2/' (where '\$MetricType2' is circled in red). Other options include 'Data source' as 'historic_metrics', 'Refresh' as 'On Dashboard Load', 'Regex' as '/^-(.*)-.*\$', and 'Sort' as 'Disabled'.

Here is an explanation of the query options:

- Query - Search through all measurements and look for the measurement matching FIFTEEN_MIN/<IP address>/<Entity Type>/<Metric Type>. This represents the measurement in the 15-minute bins for the IP address, entity type, and metric type that you specify in the IP variable, Entity Type variable, and second Metric variable drop-down lists in the dashboard.

- e. Scroll down and click **Update**. The new variable name and definition are now shown in the list of variables.
6. The order of the variables in the list dictates how the variables are displayed in the variables row in the dashboard. Use the arrow buttons for each variable to move them up or down. How you order them is a personal preference. In this example, the final order is as follows:

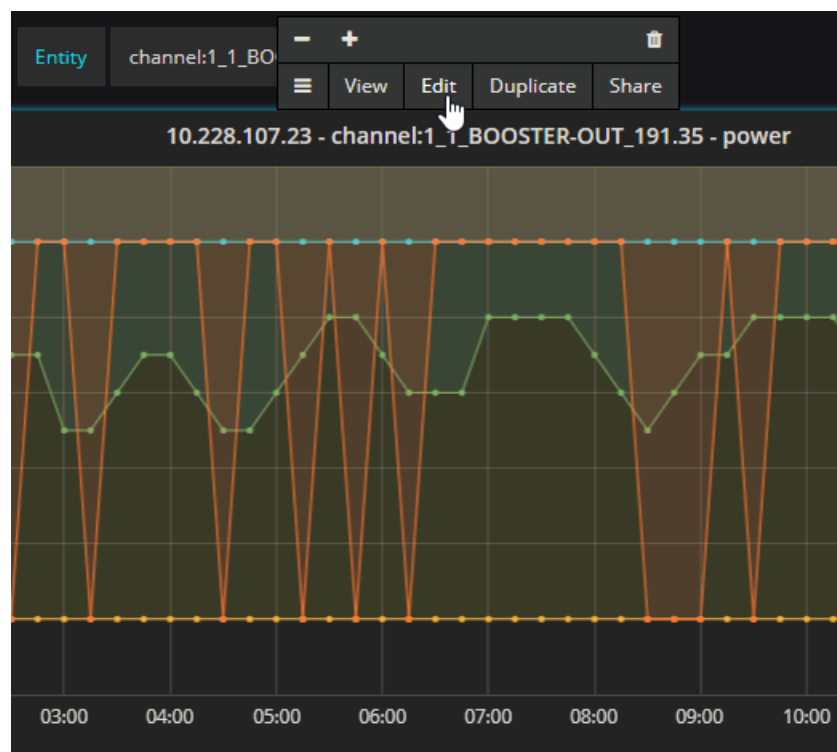
Templating			Variables	Help			
\$IP	show measurements with measurement =~ /FIFTEEN_MIN/	↓	Duplicate	✓ Edit	✕		
\$EntityType	show measurements with measurement =~ /FIFTEEN_MINV\$IP/	↑ ↓	Duplicate	✓ Edit	✕		
\$ID	SHOW TAG VALUES from /\$PmMeasurement/ with key = "id"	↑ ↓	Duplicate	✓ Edit	✕		
\$MetricType	show measurements with measurement =~ /FIFTEEN_MINV\$IPV\$EntityType/	↑ ↓	Duplicate	✓ Edit	✕		
\$MetricType2	show measurements with measurement =~ /FIFTEEN_MINV\$IPV\$EntityType/	↑ ↓	Duplicate	✓ Edit	✕		
\$PmMeasurement	show measurements with measurement =~ /FIFTEEN_MINV\$IPV\$EntityTypeV\$MetricType/	↑ ↓	Duplicate	✓ Edit	✕		
\$PmMeasurement2	show measurements with measurement =~ /FIFTEEN_MINV\$IPV\$EntityTypeV\$MetricType2/	↑	Duplicate	✓ Edit	✕		



NOTE: The \$PmMeasurement and \$PmMeasurement2 variables are configured as hidden in the variables row, and therefore their order is not important. These variables are used in defining the graph.

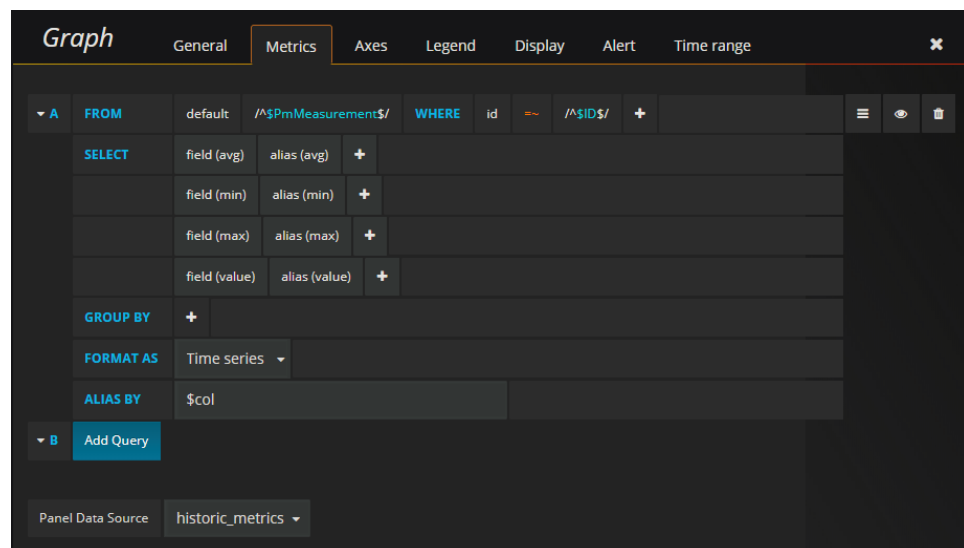
- Click the ✕ in the upper right corner to close the Templating panel.
- Now that you have defined the new variables, you can edit the graph to use the new variables.

Click the graph title and then select **Edit** in the ensuing pop-up, for example:




The Graph panel appears below the graph.

9. Click the **Metrics** tab in the Graph panel if it has not already been selected.



Here is an explanation of the graph query options:

- FROM - Find the measurement matching the measurement specified in the \$PmMeasurement variable. The \$PmMeasurement variable contains a string consisting of your selections for IP address, entity type, and metric type from the respective variable drop-down lists in the dashboard.
 - WHERE - From the matching measurement, search through the table for the entry that matches the \$ID variable. The \$ID variable contains your selection from the Entity drop-down list in the dashboard.
 - SELECT - From the matching entry, select the avg, min, max, and value fields to display and graph.
10. Create a new query for the second metric. For expediency, you will create the new query from the existing query.
- a. Click the  icon in Query A and select **Duplicate**. The duplicated query is shown in Query B.
 - b. In Query B in the FROM row, click the `/$PmMeasurement$` box and select `/$PmMeasurement2$` from the drop-down list.
- Query B is the same as Query A except that you are using the measurement specified in the \$PmMeasurement2 variable. The \$PmMeasurement2 variable contains a string consisting of your selections for the IP address, entity type, and second metric type from the respective variable drop-down lists in the dashboard.
11. Adding the second query puts the second metric on the graph. So that you can discern one metric from the other metric on the graph, edit the alias to add information to distinguish between the two metrics.
- a. In Query A, in the SELECT row, click in each of the alias fields and add **\$MetricType**.
 - b. In Query B, in the SELECT row, click in each of the alias fields and add **\$MetricType2**.

For example:

The screenshot shows the 'Graph' configuration panel with tabs for General, Metrics, Axes, Legend, Display, Alert, and Time range. The 'Metrics' tab is active, showing two metric groups, A and B. Group A has a 'FROM' clause with 'default' and '/^\$PmMeasurement\$/', a 'WHERE' clause with 'id' and '/^\$ID\$/', and a 'SELECT' clause with 'field (avg)' and 'alias (\$MetricType avg)'. Group B has a 'FROM' clause with 'default' and '/^\$PmMeasurement2\$/', a 'WHERE' clause with 'id' and '/^\$ID\$/', and a 'SELECT' clause with 'field (avg)' and 'alias (\$MetricType2 avg)'. Both groups have 'GROUP BY' and 'FORMAT AS' options set to 'Time series'.

Group	FROM	WHERE	SELECT	GROUP BY	FORMAT AS
A	default / [^] \$PmMeasurement\$/	id / [^] \$ID\$/	field (avg) alias (\$MetricType avg)		Time series
B	default / [^] \$PmMeasurement2\$/	id / [^] \$ID\$/	field (avg) alias (\$MetricType2 avg)		Time series

12. Change the graph title so that the title matches the graph.
 - a. Click the **General** tab.
 - b. In the Info section, click in the **Title** box and specify the variable for the second metric.

For example: **\$IP - \$ID - \$MetricType - \$MetricType2**

13. Click the **X** in the upper right corner to close the Graph panel.
14. Save your new dashboard.

Here is an example of the new graph showing two metrics for the same entity on the same device:



Creating a Multi-PM Dashboard (2 Metrics, 2 Entities, 2 Devices)


Use this procedure to create a dashboard that graphs two metrics from two different entities on two different devices. This is useful, for example, to compare metrics at the output of one device with the input of another.

This procedure creates a dashboard that displays two metrics from the 15-minute bin as an example, but the same general procedure can be used to create a dashboard that displays metrics from other bins.

Prerequisites

- You are using the proNX Optical Director to monitor your network and you have collected metrics for the devices you want to analyze. The proNX Optical Director automatically collects metrics from managed devices every 12 hours. You can also collect metrics on demand. For information on collecting metrics on demand, see [“Collecting Metrics from a Device Manually” on page 79](#).
 - Familiarize yourself with the terminology and constructs described in [“Overview” on page 167](#).
- Follow the procedure in [“Viewing a PM Graph” on page 169](#) to bring up the 15min Metrics dashboard.


You will use this dashboard to create the new one. This approach allows you to reuse the same variables without having to recreate them.

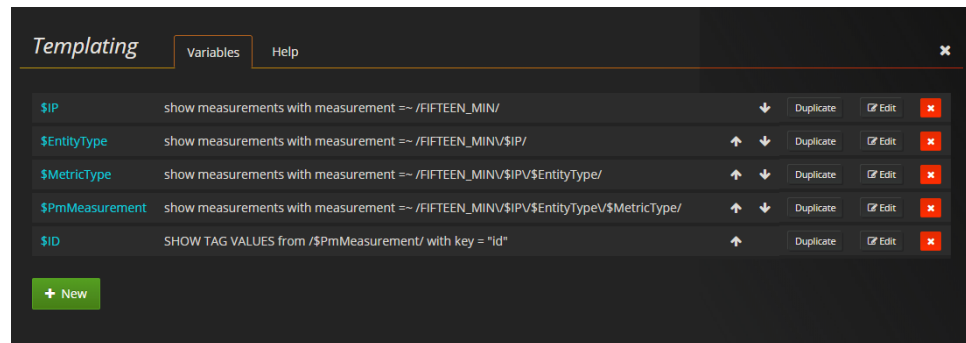
- Click the  icon at the top of the page and then select **Save As...**

Enter the new name for the dashboard and click **Save**.

You are now placed into the new dashboard. Since you have not made any changes yet, this dashboard is the same as the 15min Metrics dashboard.

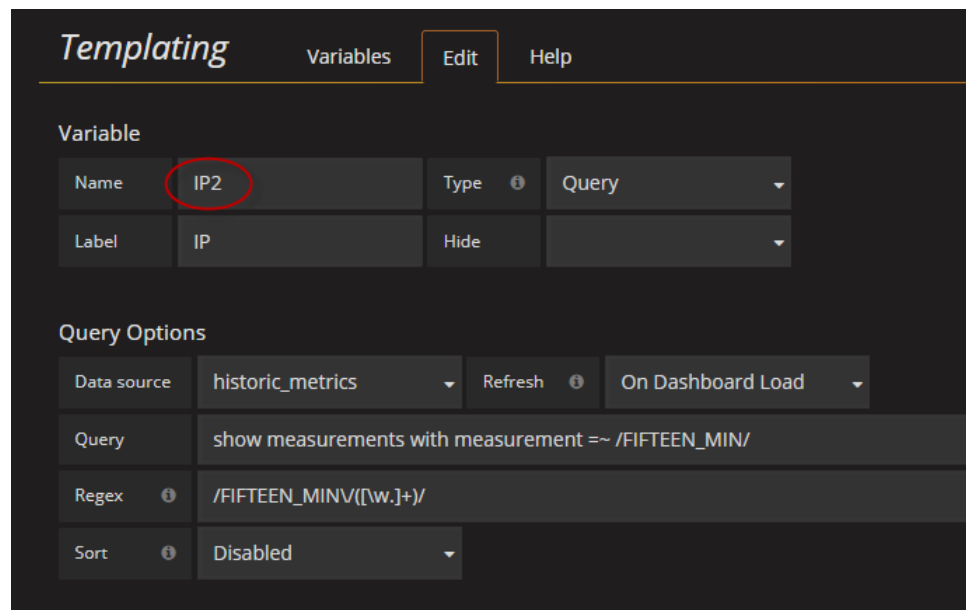
- List the variables that are defined for this dashboard.

Click the  icon at the top of the page and then select **Templating**. The Templating panel appears listing the variables that have been defined.



An explanation of these constructs is provided in the steps that follow.

4. Create a new IP variable that allows you to select the IP address of the second device. This new variable will appear in the variables row in the dashboard. For expediency, you will create the new variable from the existing variable.
 - a. Find the row for the **\$IP** variable and click **Duplicate**. The duplicated variable (**\$copy_of_IP**) is added to the bottom of the list of variables.
 - b. Click **Edit** for the duplicated variable. The Edit panel appears.
 - c. In the **Name** box in the Variable section, change the variable name to something more meaningful (for example, **IP2**).



You do not need to make any changes to the Query Options section because this second IP variable has the same characteristics as the first IP variable. Here is an explanation of the query options:

- Query - Search through all measurements and look for measurements matching FIFTEEN_MIN. These represent the measurements for all the 15-minute bins.

- **Regex** - Additionally, from the results of the query, capture the string immediately following FIFTEEN_MIN. This string contains word characters and dots (such as an IP address in dotted decimal form). In other words, this query looks through all 15-minute bins in the database and presents all IP addresses found to the user through the IP variable drop-down list.
- d. Scroll down and click **Update**. The new variable name is now shown in the list of variables.
5. Create a new entity type variable that allows you to select the entity type for the second metric. This new variable will appear in the variables row in the dashboard. For expediency, you will create the new variable from the existing variable.
 - a. Find the row for the **\$EntityType** variable and click **Duplicate**. The duplicated variable (**\$copy_of_EntityType**) is added to the bottom of the list of variables.
 - b. Click **Edit** for the duplicated variable. The Edit panel appears.
 - c. In the **Name** box in the Variable section, change the variable name to something more meaningful (for example, **EntityType2**).
 - d. In the Query Options section, change the query to use the new IP variable. You accomplish this by clicking in the **Query** box and changing **\$IP** to **\$IP2**.

The screenshot shows the 'Templating' interface with the 'Edit' tab selected. The 'Variable' section shows a table with the following data:

Variable	Name	Type	Query
	EntityType2		
	Entity Type	Hide	

The 'Query Options' section shows the following settings:

Query Options	Data source	Refresh	On Dashboard Load
	historic_metrics		
Query	show measurements with measurement =~ /FIFTEEN_MIN/\$IP2/		
Regex	/(band-name card channel roadm total edfa connection fru port)+/		
Sort	Alphabetical (asc)		

Here is an explanation of the query options:

- **Query** - Search through all measurements and look for measurements matching FIFTEEN_MIN/<IP address>. These represent the measurements in the 15-minute bins for the IP address that you specify in the second IP variable drop-down list in the dashboard.
- **Regex** - Additionally, from the results of the query, capture the key words from the measurement (band-name, card, channel, roadm, total, edfa, connection, fru, port). These key words represent the entity type. In other words, this query

looks through the database for all 15-minute bins matching the second specified IP address, and presents all entity types found to the user through the Entity Type variable drop-down list.

- e. Scroll down and click **Update**. The new variable name and definition are now shown in the list of variables.
6. Create a new metric type variable that allows you to select the second metric. This new variable will appear in the variables row in the dashboard. For expediency, you will create the new variable from the existing variable.
 - a. Find the row for the **\$MetricType** variable and click **Duplicate**. The duplicated variable (**\$copy_of_MetricType**) is added to the bottom of the list of variables.
 - b. Click **Edit** for the duplicated variable. The Edit panel appears.
 - c. In the **Name** box in the Variable section, change the variable name to something more meaningful (for example, **MetricType2**).
 - d. In the Query Options section, change the query to use the new variables. You accomplish this by clicking in the **Query** box and changing the query as follows:
 - change **\$IP** to **\$IP2**
 - change **\$EntityType** to **\$EntityType2**

Templating Variables Edit Help

Variable

Name	MetricType2	Type	Query
Label	Metric	Hide	

Query Options

Data source	historic_metrics	Refresh	On Dashboard Load
Query	show measurements with measurement =~ /FIFTEEN_MIN\'\$IP2\'\$EntityType2\'		
Regex	/FIFTEEN_MIN.*V([w-]+)/		
Sort	Alphabetical (asc)		

Here is an explanation of the query options:

- Query - Search through all measurements and look for measurements matching FIFTEEN_MIN/<IP address>/<Entity Type>. These represent the measurements in the 15-minute bins for the IP address and entity type that you specify in the second IP variable and second Entity Type variable drop-down lists in the dashboard.
- Regex - Additionally, from the results of the query, capture the last string containing word characters (a-z, A-Z, 0-9, _) and hyphens (-). The last string

in a measurement is the metric type. In other words, this query looks through the database for all 15-minute bins matching the second specified IP address and the second specified entity type, and presents all metric types found to the user through the Metric variable drop-down list.

- e. Scroll down and click **Update**. The new variable name and definition are now shown in the list of variables.
7. Create a new PM measurement variable that uses the new variables. The PM measurement variable represents the measurement containing the metric being graphed. You will refer to this variable later when you define the graph. For expediency, you will create the new variable from the existing variable.
 - a. Find the row for the **\$PmMeasurement** variable and click **Duplicate**. The duplicated variable (**\$copy_of_PmMeasurement**) is added to the bottom of the list of variables.
 - b. Click **Edit** for the duplicated variable. The Edit panel appears.
 - c. In the **Name** box in the Variable section, change the variable name to something more meaningful (for example, **PmMeasurement2**).
 - d. In the Query Options section, change the query to use the new variables. You accomplish this by clicking in the **Query** box and changing the query as follows:
 - change **\$IP** to **\$IP2**
 - change **\$EntityType** to **\$EntityType2**
 - change **\$MetricType** to **\$MetricType2**

The screenshot shows the 'Templating' interface with the 'Edit' tab selected. The 'Variable' section contains a table with the following data:

Variable	Name	Type	Query
	PmMeasurement2		
	PmMeasurement	Hide	Variable

The 'Query Options' section contains the following fields:

- Data source: historic_metrics
- Refresh: On Dashboard Load
- Query: show measurements with measurement == /FIFTEEN_MIN/\$IP2/\$EntityType2/\$MetricType2/
- Regex: /.^.(*)-.*
- Sort: Disabled

Here is an explanation of the query options:

- Query - Search through all measurements and look for the measurement matching FIFTEEN_MIN/<IP address>/<Entity Type>/<Metric Type>. This represents the measurement in the 15-minute bins for the IP address, entity type, and metric type that you specify in the second IP variable, second Entity Type variable, and second Metric variable drop-down lists in the dashboard.
- e. Scroll down and click **Update**. The new variable name and definition are now shown in the list of variables.
 8. Create a new ID variable that allows you to select the entity for the second metric. This new variable will appear in the variables row in the dashboard. For expediency, you will create the new variable from the existing variable.
 - a. Find the row for the **\$ID** variable and click **Duplicate**. The duplicated variable (**\$copy_of_ID**) is added to the bottom of the list of variables.
 - b. Click **Edit** for the duplicated variable. The Edit panel appears.
 - c. In the **Name** box in the Variable section, change the variable name to something more meaningful (for example, **ID2**).
 - d. In the Query Options section, change the query to use the new PM measurement variable. You accomplish this by clicking in the **Query** box and changing **\$PmMeasurement** to **\$PmMeasurement2**.

The screenshot shows the 'Templating' interface with the 'Edit' tab selected. The 'Variable' section contains a table with the following data:

Name	Type	Query
ID2		

Below the table, the 'Label' is set to 'Entity' and the 'Hide' checkbox is unchecked. The 'Query Options' section includes the following fields:

- Data source:** historic_metrics
- Refresh:** On Dashboard Load
- Query:** SHOW TAG VALUES from: /\$PmMeasurement2/ with key = "id"
- Regex:** /.*(-.*)-.*/
- Sort:** Alphabetical (asc)

Here is an explanation of the query options:

- Query - Search through the table corresponding to the measurement specified by the \$PmMeasurement2 variable and show all id values. These id values represent the entities in the 15-minute bins for the IP address, entity type, and metric type that you specify in the second IP variable, second Entity Type variable, and second Metric variable drop-down lists in the dashboard. These id values are presented to the user through the second Entity variable drop-down list.
- e. Scroll down and click **Update**. The new variable name and definition are now shown in the list of variables.
9. The order of the variables in the list dictates how the variables are displayed in the variables row in the dashboard. Use the arrow buttons for each variable to move them up or down. How you order them is a personal preference. In this example, the final order is as follows:

Templating

Variables

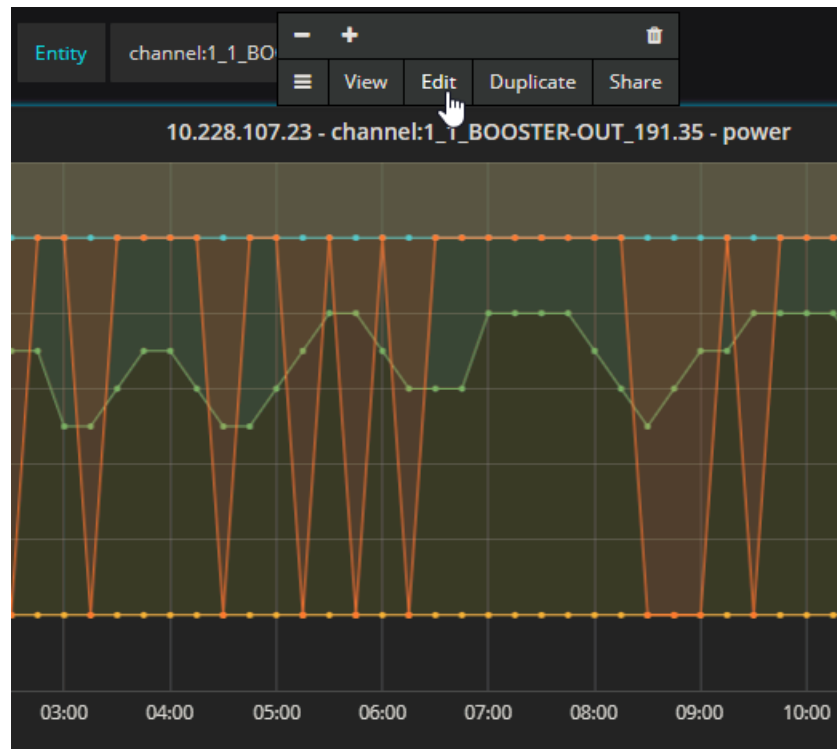
Help

\$IP	show measurements with measurement =~ /FIFTEEN_MIN/	↓	Duplicate	✎ Edit	✖
\$EntityType	show measurements with measurement =~ /FIFTEEN_MIN/\$IP/	↑ ↓	Duplicate	✎ Edit	✖
\$ID	SHOW TAG VALUES from /\$PmMeasurement/ with key = "id"	↑ ↓	Duplicate	✎ Edit	✖
\$MetricType	show measurements with measurement =~ /FIFTEEN_MIN/\$IP/\$EntityType/	↑ ↓	Duplicate	✎ Edit	✖
\$PmMeasurement	show measurements with measurement =~ /FIFTEEN_MIN/\$IP/\$EntityType/\$MetricType/	↑ ↓	Duplicate	✎ Edit	✖
\$IP2	show measurements with measurement =~ /FIFTEEN_MIN/	↑ ↓	Duplicate	✎ Edit	✖
\$EntityType2	show measurements with measurement =~ /FIFTEEN_MIN/\$IP2/	↑ ↓	Duplicate	✎ Edit	✖
\$ID2	SHOW TAG VALUES from /\$PmMeasurement2/ with key = "id"	↑ ↓	Duplicate	✎ Edit	✖
\$MetricType2	show measurements with measurement =~ /FIFTEEN_MIN/\$IP2/\$EntityType2/	↑ ↓	Duplicate	✎ Edit	✖
\$PmMeasurement2	show measurements with measurement =~ /FIFTEEN_MIN/\$IP2/\$EntityType2/\$MetricType2/	↑	Duplicate	✎ Edit	✖



NOTE: The \$PmMeasurement and \$PmMeasurement2 variables are configured as hidden in the variables row, and therefore their order is not important. These variables are used in defining the graph.

10. Click the ✕ in the upper right corner to close the Templating panel.
11. Now that you have defined the new variables, you can edit the graph to use the new variables.
- Click the graph title and then select **Edit** in the ensuing pop-up, for example:



The Graph panel appears below the graph.

12. Click the **Metrics** tab in the Graph panel if it has not already been selected.

Graph General **Metrics** Axes Legend Display Alert Time range

▼ A FROM default /[^]\$PmMeasurement\$/ WHERE id [~] /[^]\$ID\$/ +

SELECT field (avg) alias (avg) +

field (min) alias (min) +

field (max) alias (max) +

field (value) alias (value) +

GROUP BY +

FORMAT AS Time series ▼

ALIAS BY \$col

▼ B Add Query

Panel Data Source historic_metrics ▼


Here is an explanation of the graph query options:

- FROM - Find the measurement matching the measurement specified in the \$PmMeasurement variable. The \$PmMeasurement variable contains a string

consisting of your selections for IP address, entity type, and metric type from the respective variable drop-down lists in the dashboard.

- WHERE - From the matching measurement, search through the table for the entry that matches the \$ID variable. The \$ID variable contains your selection from the Entity drop-down list in the dashboard.
- SELECT - From the matching entry, select the avg, min, max, and value fields to display and graph.

13. Create a new query for the second metric. For expediency, you will create the new query from the existing query.

- a. Click the  icon in Query A and select **Duplicate**. The duplicated query is shown in Query B.
- b. In Query B in the FROM row, change the query as follows:
 - click the `/^$PmMeasurement$` box and select `/^$PmMeasurement2$` from the drop-down list
 - click the `/^ID` box and select `/^$ID2$` from the drop-down list

Query B is the same as Query A except that you are using the measurement specified in the \$PmMeasurement2 variable. The \$PmMeasurement2 variable contains a string consisting of your selections for the second IP address, second entity type, and second metric type from the respective variable drop-down lists in the dashboard. Additionally, Query B is looking for the entry identified by the entity specified in the \$ID2 variable. The \$ID2 variable contains your selection for the entity from the second Entity drop-down list in the dashboard.

14. Adding the second query puts the second metric on the graph. So that you can discern one metric from the other metric on the graph, edit the alias to add information to distinguish between the two metrics.

- a. In Query A, in the SELECT row, click in each of the alias fields and add \$IP.
- b. In Query B, in the SELECT row, click in each of the alias fields and add \$IP2.

For example:

Graph										General	Metrics	Axes	Legend	Display	Alert	Time range	
▼ A	FROM	default	/^\\$PmMeasurement\$		WHERE	id	=	/^\\$ID\$		+							
	SELECT	field (avg)	alias (\$IP avg)		+												
		field (min)	alias (\$IP min)		+												
		field (max)	alias (\$IP max)		+												
		field (value)	alias (\$IP value)		+												
	GROUP BY	+															
	FORMAT AS	Time series ▼															
	ALIAS BY	\$col															
▼ B	FROM	default	/^\\$PmMeasurement2\$		WHERE	id	=	/^\\$ID2\$		+							
	SELECT	field (avg)	alias (\$IP2 avg)		+												
		field (min)	alias (\$IP2 min)		+												
		field (max)	alias (\$IP2 max)		+												
		field (value)	alias (\$IP2 value)		+												
	GROUP BY	+															
	FORMAT AS	Time series ▼															



NOTE: In this example, the IP address is used to distinguish between the two metrics, the assumption being that you will only use this graph to display metrics from different devices. If this assumption is incorrect, then update the alias fields with a more appropriate distinction.

15. Change the graph title so that the title matches the graph.
 - a. Click the **General** tab.
 - b. In the Info section, click in the **Title** box and specify the variable for the second metric.
 For example: \$ID - \$IP - \$MetricType - \$IP2 - \$MetricType2
16. Click the ✕ in the upper right corner to close the Graph panel.
17. Save your new dashboard.

Here is an example of the new graph showing two metrics for two entities on two different devices:



Release History Table

Release	Description
18.4	<a href="https://<server-hostname>/graphs">https://<server-hostname>/graphs