



User Guide

PTP 820 NMS System Release R18A00



Accuracy

While reasonable efforts have been made to assure the accuracy of this document, Cambium Networks assumes no liability resulting from any inaccuracies or omissions in this document, or from use of the information obtained herein. Cambium reserves the right to make changes to any products described herein to improve reliability, function, or design, and reserves the right to revise this document and to make changes from time to time in content hereof with no obligation to notify any person of revisions or changes. Cambium does not assume any liability arising out of the application or use of any product, software, or circuit described herein; neither does it convey license under its patent rights or the rights of others. It is possible that this publication may contain references to, or information about Cambium products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that Cambium intends to announce such Cambium products, programming, or services in your country.

Copyrights

This document, Cambium products, and 3rd Party software products described in this document may include or describe copyrighted Cambium and other 3rd Party supplied computer programs stored in semiconductor memories or other media. Laws in the United States and other countries preserve for Cambium, its licensors, and other 3rd Party supplied software certain exclusive rights for copyrighted material, including the exclusive right to copy, reproduce in any form, distribute and make derivative works of the copyrighted material. Accordingly, any copyrighted material of Cambium, its licensors, or the 3rd Party software supplied material contained in the Cambium products described in this document may not be copied, reproduced, reverse engineered, distributed, merged or modified in any manner without the express written permission of Cambium. Furthermore, the purchase of Cambium products shall not be deemed to grant either directly or by implication, estoppel, or otherwise, any license under the copyrights, patents or patent applications of Cambium or other 3rd Party supplied software, except for the normal non-exclusive, royalty free license to use that arises by operation of law in the sale of a product.

Restrictions

Software and documentation are copyrighted materials. Making unauthorized copies is prohibited by law. No part of the software or documentation may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without prior written permission of Cambium.

License Agreements

The software described in this document is the property of Cambium and its licensors. It is furnished by express license agreement only and may be used only in accordance with the terms of such an agreement.

High Risk Materials

Cambium and its supplier(s) specifically disclaim any express or implied warranty of fitness for any high risk activities or uses of its products including, but not limited to, the operation of nuclear facilities, aircraft navigation or aircraft communication systems, air traffic control, life support, or weapons systems ("High Risk Use"). Any High Risk is unauthorized, is made at your own risk and you shall be responsible for any and all losses, damage or claims arising out of any High Risk Use.

© 2017 Cambium Networks Limited. All Rights Reserved.

Contents

About This User Guide	1
Contacting Cambium Networks	1
Purpose	2
Cross references	2
Feedback	2
Problems and warranty	3
Reporting problems.....	3
Repair and service	3
Hardware warranty	3
Security advice	4
Warnings, cautions, and notes.....	4
Warnings	4
Cautions.....	4
Notes	4
Caring for the environment	5
In EU countries	5
Disposal of Cambium equipment	5
Disposal of surplus packaging	5
In non-EU countries.....	5
Chapter 1: Before You Start	1-1
PTP 820 NMS functionality	1-2
Online Help	1-3
More information	1-4
Chapter 2: Getting Started	2-1
Logging in.....	2-1
Configuring PTP 820 NMS For Server High Availability.....	2-2
Configuring PTP 820 NMS for Database High Availability.....	2-3
Using the correct IP address format	2-4
Modifying connection templates.....	2-5
How to configure polling and traps in PTP 820 NMS	2-6
Discovering and managing elements.....	2-7
How to discover an NE.....	2-7
How to manage an element	2-9
How to unmanage/delete an element.....	2-9
Viewing and Configuring Alarms	2-10
How to customize the appearance of alarms	2-10
How to acknowledge an alarm.....	2-10

How to configure and receive alarm notifications	2-11
Viewing Alarm reports	2-12
Generating NG Alarm Reports	2-12
Viewing Legacy Alarm Reports	2-12
Viewing and Generating NG Inventory Reports	2-12
Viewing Legacy Inventory Reports	2-13
Analyzing Performance counters	2-14
How to collect Performance Monitoring (PM) counters information.....	2-14
Generating Performance Reports	2-14
Downloading new software or backing up and restoring configuration	2-16
Install and configure an FTP or SFTP server	2-16
How to download software to an NE	2-18
How to backup and restore NE configuration	2-19
Managing Security Groups and Users.....	2-20
How to create a new group	2-20
How to create a new user	2-20
How to change your password	2-20
Configuring Northbound Interface SNMP	2-21
Troubleshooting: how to solve port conflicts	2-22
Chapter 3: GUI overview	3-25
How to use the PTP 820 NMS GUI help system	3-26
The graphical user interface	3-27
How to reposition views	3-32
The objects in a perspective	3-39
The objects in a view.....	3-46
The objects in a view	3-46
Timeslider tool	3-51
Quick Search field	3-57
Search Options	3-58
Visualization of alarms	3-60
General dialogs and views	3-66
PTP 820 NMS Login dialog.....	3-66
Alarm dialog	3-67
Customize Columns dialog	3-68
Save Changes dialog	3-70
Export To File dialog	3-70
Columns	3-71
Format of values	3-72
Chapter 4: Predefined perspectives	4-73
Alarm Workflow perspective.....	4-73
Discover perspective	4-74
Geographical Surveillance perspective	4-74

Logical Surveillance perspective.....	4-76
Network Explorer perspective.....	4-77
Ethernet Services perspective	4-78
TDM Services perspective	4-78
Security Audit perspective	4-79
User Management perspective	4-80
Chapter 5: All views and dialogs.....	5-1
Fault	5-2
Active Alarms view	5-2
Active NMS Alarms view	5-7
Historical Alarms view	5-8
Alarm Summary view	5-14
Alarm Templates view	5-16
Alarm Templates Assignment view	5-20
Alarm Notifications view	5-23
Alarm Notification Table view	5-37
Alarm Notification table.....	5-37
Configuration	5-39
Hardware Inventory view	5-39
Software Inventory view	5-40
Transmission Inventory View	5-43
Element Software Management	5-44
Software Download Jobs view	5-47
Create Software Download Jobs wizard.....	5-49
Scheduling software download	5-53
Configuration File Management view	5-53
Connection Templates view	5-58
Connection Templates Assignment view	5-74
CLI Script Broadcast view	5-77
Performance	5-80
Current Performance view	5-80
Historical Performance view	5-84
Performance Collection Control view	5-94
Performance Templates view.....	5-98
Reset Cumulative Performance Counters dialog.....	5-102
Topology	5-103
Logical Map view	5-103
Geographical Map view.....	5-120
Network Explorer Map view.....	5-136
Domains.....	5-136
Network Elements (NE)	5-137
Relations between entities	5-137

Fields for a Topological link:	5-141
Managed Elements view	5-146
Logical Tree view	5-153
Geographical Tree view	5-162
Network Explorer Tree View	5-172
Element Explorer view	5-180
Available operations from the context menu of an element in the tree	5-180
Relation Overview view	5-180
Available operations	5-183
Topological Links view	5-183
Topological Links table	5-183
Available operations	5-184
Discover	5-185
Discover Settings view	5-185
Unmanaged Elements view	5-190
Unmanaged Elements table	5-190
Services - Ethernet and TDM	5-194
Service Management	5-194
Ethernet Services	5-197
TDM Services	5-210
Administration	5-226
Audit Log view	5-226
Group Administration view	5-228
User Administration view	5-232
Northbound Interface	5-236
Northbound SNMP Settings view	5-236
Reports	5-249
NG Performance Reports Generation	5-253
NG Inventory Reports Generation	5-271
Available operations	5-277
NG Alarm Reports Generation	5-290
Legacy Alarm Frequency Report grouped by Network Element	5-301
Legacy Alarm Frequency Report List	5-305
Legacy Network Element Types Overview Report	5-310
Legacy Inventory Report	5-313
Legacy Performance Overview Report	5-318
Legacy Performance Details Report	5-324
Scheduled Reports view	5-330
Other	5-334
Error Log view	5-334
Web Browser view	5-334
Progress view	5-335
Properties view	5-335

Filter Manager view.....	5-337
Ping/TraceRoute view	5-346
Open SNMP Interface	5-348
Open SNMP Interface.....	5-348
Open SNMP Interface view	5-350
Open SNMP Alias List	5-354
Current alarm table configuration.....	5-357
Current alarm list configuration	5-362
Preferences	5-365
Preferences: Fault Colors and Sounds.....	5-365
Preferences: Historical Alarms	5-371
Preferences: NE Configuration File Backup	5-372
Preferences: Network-wide PM Collection	5-372
Preferences: Network-wide Statistic Counters - RMON Collection.....	5-375
Preferences: External FTP/SFTP Server	5-377
Preferences: External Configuration Tools.....	5-377
Preferences: Server Connection.....	5-384
Preferences: Days to keep historic data.....	5-386
Preferences: Scheduled Reports	5-388
Preferences: Alarm Notifications - E-mail and Sound files.....	5-388
Preferences: Web Browser.....	5-392
Preferences: PTP 820 NMS Management Traps	5-393
Preferences: SNMP V3	5-395
Preferences: Password Settings	5-396
Preferences: RADIUS Server	5-398
Preferences: TDM Services VC Settings.....	5-400
Preferences: Network Explorer	5-402
Preferences: Open Street Map	5-403
Preferences: User Settings	5-404
System Tray Monitors	5-406
EMS Server monitor	5-406
PTP 820 NMS SNMP Agent monitor	5-411
Chapter 6: SNMP Agent	6-1
PTP 820 NMS SNMP Agent	6-2
SNMP Agent	6-2
Protocols Supported.....	6-2
MIBs Supported.....	6-2
MIB Overview	6-3
MIB Overview.....	6-3
Supported Standard MIBs	6-3
MIB-II	6-3
Entity-MIB.....	6-5

Microwave-specific MIBs	6-7
microwave-radio-2	6-8
MWRM2-NMS-MIB	6-8
Textual Conventions used	6-16
Configuration	6-18
License check.....	6-18
Creating a EMS SNMP agent user.....	6-18
Creating an NIF setting	6-18
Alarm Forwarding.....	6-18
Enabling heartbeat traps.....	6-19
Configuring the EMS SNMP agent.....	6-19
Potential port conflict.....	6-20
Verification.....	6-21
Test of MIB-2 attributes	6-21
Test of the entPhysicalTable	6-22
Test of PTP820 NMS specific attributes	6-22
Test of the ptp820nmsHWInventoryTable	6-23
Test of the ptp820nmsSWInventoryTable	6-23
Troubleshooting.....	6-25
Troubleshooting	6-25
SNMP agent fails to start.....	6-25
EMS server is not running	6-25
Invalid user or password	6-25
License is not valid.....	6-25
Cannot bind to UDP port 161	6-25
No traps are received	6-26
No hardware and software inventory data reported.....	6-26
No. of TRX count.....	6-26
Chapter 7: PTP 820 NMS Alarms	7-27
Chapter 8: System Manager	8-1
PTP 820 NMS System Manager.....	8-2
System Manager Logon	8-3
System Manager GUI Components Overview	8-4
Available System Manager views and wizards	8-8
General menu	8-10
Dashboard View	8-10
PTP 820 NMS HA State.....	8-13
PTP 820 NMS HA Configuration Status.....	8-14
Administration menu	8-17
Database Task View.....	8-17
Database Configurations View	8-18
Database Analysis View	8-22

PTP 820 NMS Initial Setup Wizard.....	8-24
Set Active User/Schema Wizard.....	8-44
Create User/Schema Wizard	8-51
Reinitialize User/Schema Wizard	8-57
Delete User/Schema Wizard	8-65
Upgrade User/Schema Wizard	8-73
Backup Active User/Schema Wizard	8-87
Backup User/Schema Wizard	8-93
Restore User/Schema Wizard	8-104
Optimize Active NMS User/Schema	8-113
Analyze User/Schema Wizard	8-114
License menu	8-121
License Administration View	8-121
Import License Wizard.....	8-123
Update Capabilities wizard.....	8-128
Settings menu	8-131
PTP 820 NMS Server View.....	8-131
NMS HA View - Configuring High Availability	8-134
System Manager View.....	8-137
Email Notification View	8-137
Database View.....	8-140
Other menu.....	8-143
Task Log View	8-143
PTP 820 NMS Log View.....	8-146
Scheduled Tasks View	8-147
System Manager maintenance	8-149
System Manager maintenance.....	8-149
System Manager troubleshooting.....	8-152
Windows version	8-153
Solaris version	8-153
Chapter 9: Abbreviations	CLV

List of Figures

Figure 1 Typical workspace view of PTP 820 NMS	3-27
Figure 2 PTP 820 NMS GUI objects	3-28
Figure 3 PTP 820 NMS main menu	3-28
Figure 4 PTP 820 NMS different views.....	3-29
Figure 5 PTP 820 NMS functionality views	3-30
Figure 6 PTP 820 NMS dialogs.....	3-31
Figure 7 PTP 820 NMS preference menus.....	3-32
Figure 8 PTP 820 NMS view classifications	3-39
Figure 9 Select dialog.....	3-41
Figure 10 Customize perspective dialog – Toolbar Visibility pane	3-42
Figure 11 Customize perspective dialog – Menu Visibility pane	3-43
Figure 12 Customize perspective dialog – commands pane	3-44
Figure 13 Typical snapshot of Geographical map	3-46
Figure 14 Geographical map close view.....	3-47
Figure 15 Timeslider tool	3-51
Figure 16 Historical alarms view with Timerslider tool.....	3-51
Figure 17 Timerslider tool view objects.....	3-52
Figure 18 Data and Time dialog.....	3-56
Figure 19 Search options	3-58
Figure 20 Alarm indicators in a topological map	3-62
Figure 21 Alarm workflow perspective	4-73
Figure 22 Discover and manage new elements.....	4-74
Figure 23 Geographical surveillance perspective.....	4-75
Figure 24 Logical surveillance perspective.....	4-76
Figure 25 Security audit perspective	4-80
Figure 26 User Management perspective.....	4-81
Figure 27 Active alarm view.....	5-2
Figure 28 Active alarm scope view.....	5-3
Figure 29 Alarm comment dialog.....	5-7
Figure 30 Active NMS Alarms	5-7
Figure 31 Historical alarm view.....	5-8
Figure 32 Alarm comments dialog.....	5-13
Figure 33 Alarm summary view	5-14
Figure 34 Active alarms view for a single alarm category	5-15
Figure 35 Alarm templates view.....	5-16
Figure 36 Create template dialog	5-19
Figure 37 Template Name dialog	5-19
Figure 38 Alarm template assignment view	5-20

Figure 39 Alarm template assignment view	5-23
Figure 40 Alarm notification rules tree	5-24
Figure 41 Alarm notification criteria definition	5-25
Figure 42 Audible notification definition area	5-27
Figure 43 Email notification definition area.....	5-28
Figure 44 General information	5-31
Figure 45 Criteria information	5-32
Figure 46 Select notification target	5-33
Figure 47 Audible notification configuration	5-34
Figure 48 Email notification configuration.....	5-35
Figure 49 Hardware inventory view	5-39
Figure 50 Software inventory view	5-40
Figure 51 Transmission inventory view	5-43
Figure 52 Element Software Management.....	5-44
Figure 53 Upload Software File to PTP 820 NMS Server.....	5-46
Figure 54 Software download jobs view	5-47
Figure 55 Software download jobs – basic inforamtion	5-50
Figure 56 Software download jobs – selecting elements	5-51
Figure 57 Software download jobs – selecting file to download	5-52
Figure 58 Schedule software download	5-53
Figure 59 Configuration file management view	5-54
Figure 60 Backup configuration dialog.....	5-56
Figure 61 Restore configuration dialog	5-57
Figure 62 Add configuration file.....	5-57
Figure 63 Connection templates view.....	5-58
Figure 64 Connection template of type “OpenSNMP”	5-60
Figure 65 Connection template	5-60
Figure 66 Connection template.....	5-64
Figure 67 Setting UTC offset	5-70
Figure 68 Create template dialog for connection type	5-72
Figure 69 Delete template dialog.....	5-73
Figure 70 Template name dialog	5-73
Figure 71 Confirm save of connection template dialog	5-74
Figure 72 Connection template assignment view	5-75
Figure 73 Current performance view	5-80
Figure 74 Historical performance view	5-84
Figure 75 Historical performance view.....	5-86
Figure 76 Historical performance graph.....	5-88
Figure 77 Line graph.....	5-91
Figure 78 Bar graph	5-91
Figure 79 Area graph.....	5-92
Figure 80 Performance collection control view	5-94

Figure 81	Assign performance templates	5-97
Figure 82	Performance templates view	5-98
Figure 83	New performance templates dialog	5-101
Figure 84	Rest cumulative performance counters dialog.....	5-102
Figure 85	Logical map view	5-103
Figure 86	NEs topological links	5-105
Figure 87	Background image dialog	5-109
Figure 88	Map overview tool	5-110
Figure 89	New topological link dialog.....	5-111
Figure 90	Edit topological link.....	5-114
Figure 91	New administrative domain dialog	5-115
Figure 92	Move resource dialog	5-116
Figure 93	Include managed elements dialog	5-117
Figure 94	Delete domain form model dialog.....	5-117
Figure 95	Delete network element form model dialog	5-118
Figure 96	Rename dialog	5-118
Figure 97	Save modified view dialog	5-119
Figure 98	Mute notifications dialog.....	5-119
Figure 99	Geographical map view	5-120
Figure 100	NEs topological links	5-122
Figure 101	Background image dialog.....	5-126
Figure 102	New topological link dialog.....	5-127
Figure 103	Edit topological link dialog.....	5-130
Figure 104	Map overview tool.....	5-131
Figure 105	New administrative domain dialog.....	5-131
Figure 106	Include managed element	5-132
Figure 107	Delete domain from model dialog.....	5-133
Figure 108	Delete network element from model dialog	5-133
Figure 109	Rename dialog	5-134
Figure 110	Save modified view dialog	5-135
Figure 111	Mute notifications dialog.....	5-135
Figure 112	Managed elements view.....	5-146
Figure 113	Managed elements configuration	5-148
Figure 114	Topology: geographical tree view.....	5-163
Figure 115	Topology: new administrative domain dialog	5-166
Figure 116	Topology: move resource dialog	5-166
Figure 117	Topology: Include manage elements dialog	5-168
Figure 118	Topology: delete domain from model dialog	5-168
Figure 119	Topology: delete network element from model dialog.....	5-169
Figure 120	Topology: rename dialog	5-170
Figure 121	Topology: Mute notifications dialog.....	5-170
Figure 122	Discover settings view	5-185

Figure 123	Setting for an SNMP range search	5-187
Figure 124	Unmanaged elements view	5-190
Figure 125	Managed elements dialogue	5-192
Figure 126	Confirm discovered element delete dialog.....	5-193
Figure 127	Service list	5-196
Figure 128	Ethernet flow domain navigator.....	5-198
Figure 129	Ethernet topology view	5-201
Figure 130	Topology overview	5-204
Figure 131	Ethernet Services view.....	5-204
Figure 132	Ethernet Service Path view	5-207
Figure 133	Ethernet Service Ports view.....	5-208
Figure 134	TDM Domains view	5-210
Figure 135	Topology Overview	5-216
Figure 136	TDM Services view.....	5-217
Figure 137	TDM Service Path view	5-219
Figure 138	TDM Service Ports view	5-219
Figure 139	TDM service trails	5-220
Figure 140	Audit log view	5-226
Figure 141	Customize columns dialog for audit log.....	5-228
Figure 142	Group administration view	5-229
Figure 143	Create security group dialog.....	5-230
Figure 144	Clone security group dialog	5-231
Figure 145	Confirm group delete dialog.....	5-231
Figure 146	User administration view.....	5-232
Figure 147	User administration view.....	5-233
Figure 148	Create new user dialog	5-234
Figure 149	Change password dialog.....	5-234
Figure 150	Verify password change dialog.....	5-235
Figure 151	Confirm user delete dialog	5-235
Figure 152	Northbound SNMP settings view	5-236
Figure 153	Create a new high level manager wizard.....	5-238
Figure 154	Set manager properties	5-239
Figure 155	Add communities.....	5-240
Figure 156	Add new community.....	5-240
Figure 157	Add V3 users	5-241
Figure 158	Add SNMP V3 Properties	5-242
Figure 159	Setting up a trap forwarder	5-243
Figure 160	Setting up a trap forwarder	5-244
Figure 161	Unmodified Trap Forwarding	5-245
Figure 162	Create high-level manager.....	5-246
Figure 163	Create an alarm forward view	5-247
Figure 164	Create an alarm forward configuration	5-247

Figure 165	Alarms to block	5-248
Figure 166	Other options.....	5-248
Figure 167	Report view.....	5-249
Figure 168	Alarm overview chart	5-250
Figure 169	Frequent alarms list	5-251
Figure 170	Export report dialog.....	5-253
Figure 171	NE type report	5-310
Figure 172	NE type report view	5-311
Figure 173	Export report dialog.....	5-312
Figure 174	Generating a inventory report.....	5-313
Figure 175	Hardware and software inventory report	5-314
Figure 176	Export report dialog.....	5-317
Figure 177	Performance report.....	5-318
Figure 178	Generating performance report	5-318
Figure 179	Performance report view.....	5-319
Figure 180	Performance time graph.....	5-321
Figure 181	Performance summarized graph	5-321
Figure 182	Performance report TOC	5-322
Figure 183	Export report dialog.....	5-323
Figure 184	Performance detailed report	5-324
Figure 185	Generating performance detailed report	5-324
Figure 186	Performance detailed report view	5-325
Figure 187	Performance details.....	5-326
Figure 188	Performance report TOC	5-328
Figure 189	Export report dialog.....	5-329
Figure 190	Exporting the performance details report to Excel	5-329
Figure 191	Schedule reports.....	5-331
Figure 192	Error log view.....	5-334
Figure 193	Progress view	5-335
Figure 194	Properties view	5-336
Figure 195	Discover and manage	5-349
Figure 196	Configuration view.....	5-349
Figure 197	SNMP NE configuration assign	5-350
Figure 198	SNMP interface view	5-351
Figure 199	Open SNMP alias list.....	5-354
Figure 200	Alias list validation	5-356
Figure 201	Current alarm table configuration	5-358
Figure 202	Active alarms view	5-359
Figure 203	Current alarm list	5-363
Figure 226	Preferences local colors	5-366
Figure 227	Preferences sounds.....	5-367
Figure 228	Preferences local connectivity colors.....	5-368

Figure 229	Preferences system colors.....	5-369
Figure 230	Preferences system connectivity colors.....	5-370
Figure 231	Preferences - Historical Alarms.....	5-371
Figure 232	Preferences - Network wide PM Collection	5-373
Figure 233	Preferences external tools.....	5-378
Figure 234	Create application group dialog.....	5-379
Figure 235	Confirm delete application group dialog.....	5-379
Figure 236	External tool paths.....	5-380
Figure 237	External tool assignments.....	5-381
Figure 238	Available external tools dialog.....	5-382
Figure 239	Web EMS	5-383
Figure 240	Preferences server connection.....	5-384
Figure 241	PTP 820 NMS login dialog	5-385
Figure 242	Preferences day to keep historic data	5-386
Figure 243	Preferences - email notification	5-389
Figure 244	Preferences - sound files	5-390
Figure 245	Preferences web browser	5-392
Figure 246	Preferences EMS heartbeat	5-394
Figure 247	Preferences SNMP V3	5-396
Figure 248	Preferences password settings.....	5-397
Figure 249	Preferences Radius server.....	5-399
Figure 250	Preferences user settings	5-401
Figure 251	Verify password change dialog	5-405
Figure 252	License information.....	5-407
Figure 253	Import license wizard - 1/3.....	5-408
Figure 254	Import license wizard - 2/3.....	5-408
Figure 255	Import license wizard - 3/3.....	5-409
Figure 256	SNMP agent parameters	5-411
Figure 258	License is not valid	6-22
Figure 259	ptp820nmsAlarmTable	6-23
Figure 260	ptp820nmsHWInventoryTable	6-23
Figure 261	ptp820nmsSWInventoryTable	6-24
Figure 262	System manager logon	8-3
Figure 263	System manager view	8-4
Figure 264	Scheduled tasks view	8-7
Figure 265	Dashboard view content.....	8-11
Figure 266	Dashboard view	8-11
Figure 267	Dashboard view	8-12
Figure 268	EMS server monitoring area	8-12
Figure 269	Active EMS database configuration area.....	8-15
Figure 270	Recent task area	8-16
Figure 271	Database task view content.....	8-17

Figure 272	Database configurations view content	8-18
Figure 273	Add database configurations	8-20
Figure 274	Database connection to admin user successful	8-21
Figure 275	Database connection to admin user failure	8-21
Figure 276	Delete a configuration warning	8-22
Figure 277	Delete a configuration not allowed warning	8-22
Figure 278	System manager logon	8-24
Figure 279	Initial setup wizard - 1/7	8-25
Figure 280	Initial setup wizard - 2/7	8-26
Figure 281	Selecting license file	8-27
Figure 282	Copying license file	8-28
Figure 283	Initial setup wizard - 3/7	8-29
Figure 284	Initial setup wizard - 3/7	8-30
Figure 285	Initial setup wizard - 4/7	8-31
Figure 286	Initial setup wizard - 5/7	8-32
Figure 287	Selecting database installation path	8-33
Figure 288	Initial setup wizard - 6/7	8-34
Figure 289	Initial setup wizard - 7/7	8-36
Figure 290	Initial setup wizard - 7/7 : statrt EMS server	8-37
Figure 291	Initial setup wizard - 7/7 : backup before upgrade fails	8-38
Figure 292	Error details reports	8-39
Figure 293	Initial setup wizard - 7/7: upgrade of database failed	8-40
Figure 294	Selecting backup file	8-41
Figure 295	Initial setup wizard - 7/7 : Schema upgrade failed	8-42
Figure 296	Initial setup wizard - 7/7 : Connection to the database failed	8-43
Figure 297	Initial setup wizard - 7/7	8-44
Figure 298	Set Active Wizard page 1 : Introduction	8-45
Figure 299	Set Active Wizard page 2 : Database Connection Parameters	8-46
Figure 300	Selecting exiting database connection	8-47
Figure 301	Set Active Wizard page 3 : User/Schema Parameters	8-48
Figure 302	Selecting user/schema	8-49
Figure 303	Set Active Wizard page 4 : Set Active	8-50
Figure 304	Set active user/schema	8-51
Figure 305	Create Wizard page 1 : Introduction	8-52
Figure 306	Create Wizard page 2 : Database Connection Parameters	8-53
Figure 307	Selecting a database connection	8-54
Figure 308	Create Wizard page 3 : User/Schema Parameters	8-55
Figure 309	Create Wizard page 4 : Create User/Schema	8-56
Figure 310	Create Wizard page 4 : creation process complete	8-57
Figure 311	Reinitialize Wizard page 1 : Introduction	8-58
Figure 312	Reinitialize Wizard page 2 : Database Connection Parameters	8-59
Figure 313	Selecting a database connection	8-60

Figure 314 Reinitialize Wizard page 3 : User/Schema Parameters.....	8-61
Figure 315 Selecting user/schema.....	8-62
Figure 316 Reinitialize Wizard page 4 : Reinitialize User/Schema.....	8-63
Figure 317 Reinitialize Wizard page 4 : Reinitialized	8-64
Figure 318 Reinitialize Wizard page 4 : Reinitialized	8-65
Figure 319 Delete Wizard page 1 : Introduction.....	8-66
Figure 320 Delete Wizard page 2 : Database Connection Parameters.....	8-67
Figure 321 Selecting a database connection	8-68
Figure 322 Delete Wizard page 3 : User/Schema Parameters	8-69
Figure 323 Selecting user/schema.....	8-70
Figure 324 Delete Wizard page 4 : Delete User/Schema.....	8-71
Figure 325 Deleting database	8-72
Figure 326 Upgrade Wizard page 1 : Introduction	8-73
Figure 327 Upgrade Wizard page 2 : Database Connection Parameters	8-74
Figure 328 Selecting a database connection	8-75
Figure 329 Upgrade Wizard page 3 : User/Schema Parameters	8-76
Figure 330 Select a user/schema.....	8-77
Figure 331 Upgrade Wizard page 4 : User/Schema backup	8-78
Figure 332 Selecting a database installation path	8-79
Figure 333 Upgrade Wizard page 5 : Upgrade User/Schema	8-80
Figure 334 Upgrade Wizard page 5 : Upgrade complete	8-81
Figure 335 Backup before upgrade fails	8-82
Figure 336 Error details report	8-83
Figure 337 Upgrade of database failed	8-84
Figure 338 Selecting a backup file	8-85
Figure 339 Database backup restore – retry	8-86
Figure 340 Restore database complete.....	8-87
Figure 341 Backup Active Wizard page 1 : Introduction.....	8-88
Figure 342 Backup Active Wizard page 2 : Backup Active User/Schema.....	8-89
Figure 343 Selecting a database path.....	8-90
Figure 344 Database backup	8-91
Figure 345 Schedule database backup	8-92
Figure 346 Schedule database backup complete	8-93
Figure 347 Backup Wizard page 1 : Introduction.....	8-93
Figure 348 Backup Wizard page 2 : Database Connection Parameters.....	8-95
Figure 349 Selecting a database connection	8-96
Figure 350 Backup Wizard page 3 : User/Schema Parameters	8-97
Figure 351 Select a user/schema.....	8-98
Figure 352 Backup Wizard page 4 : Backup User/Schema	8-99
Figure 353 Selecting a database installation path	8-100
Figure 354 Initiating backup process.....	8-101
Figure 355 Schedule of periodfic backup database.....	8-102

Figure 356 Schedule of periodfic backup database complete.....	8-103
Figure 357 Restore Wizard page 1 : Introduction	8-104
Figure 358 Restore Wizard page 2 : Database Connection Parameters.....	8-105
Figure 359 Selecting a database connection	8-106
Figure 360 Restore Wizard page 3 : User/Schema Parameters.....	8-107
Figure 361 Selecting user/schema.....	8-108
Figure 362 Restore Wizard page 4 : Restore User/Schema	8-109
Figure 363 Selecting a backup file	8-110
Figure 364 Selecting a database installation path	8-111
Figure 365 Restore of database file	8-112
Figure 366 Optimize Active User/Schema wizard	8-113
Figure 367 Analyze Wizard page 1 : Introduction.....	8-114
Figure 368 Analyze Wizard page 2 : Database Connection Parameters.....	8-115
Figure 369 Selecting a database connection	8-116
Figure 370 Analyze Wizard page 3 : User/Schema Parameters.....	8-117
Figure 371 Selecting a user/schema.....	8-118
Figure 372 Analyze Wizard page 4 : Analyze User/Schema.....	8-119
Figure 373 Analyze Wizard page 4 : Initiate analyze process	8-120
Figure 374 License administration.....	8-122
Figure 375 Import License Wizard page 1 : Introduction	8-123
Figure 376 Import License Wizard page 2 : Import License.....	8-124
Figure 377 Import License Wizard page 2 : selecting file	8-125
Figure 378 Import License Wizard page 2 : Import License.....	8-126
Figure 379 Import License Wizard page 3 : Restart server	8-127
Figure 380 Update Capabilities Wizard page 1 : Introduction.....	8-128
Figure 381 Update Capabilities Wizard page 2 : Update Capabilities	8-129
Figure 382 Update Capabilities Wizard page 3 : Update Capabilities	8-130
Figure 383 EMS server view content	8-131
Figure 384 NMS HA view	8-134
Figure 385 System manager contens.....	8-137
Figure 386 Email notification view content.....	8-138
Figure 387 Database view content	8-141
Figure 388 Database backup settings	8-142
Figure 389 Task log view content	8-143
Figure 390 Task details dialog.....	8-144
Figure 391 Second subtask details dialog.....	8-145
Figure 392 EMS log view content	8-146
Figure 393 Secheduled tasks view content	8-147
Figure 394 Multiple browser sessions	8-150
Figure 395 Windows services	8-151

List of Tables

Table 3 Alarm severity and node states.....	3-61
Table 4 Alarm information on topological objects.....	3-63
Table 5 Some examples of alarm states.....	3-64
Table 6 Active alarms list.....	5-4
Table 7 Historical alarms list.....	5-9
Table 8 Alarm template table.....	5-17
Table 9 Customized table.....	5-17
Table 10 Alarm edit template assignment table.....	5-21
Table 11 Alarm notification rule.....	5-24
Table 12 Alarm notification criteria.....	5-26
Table 13 Audible notification definition.....	5-28
Table 14 Email notification definition.....	5-29
Table 15 Hardware inventory table.....	5-39
Table 16 Software inventory table.....	5-41
Table 17 Transmission inventory view information.....	5-43
Table 18 Software Download Jobs.....	5-46
Table 19 Software Download Jobs Table.....	5-48
Table 20 Configuration file management table.....	5-55
Table 21 Connection templates table view area.....	5-59
Table 22 Attribute of “OpenSNMP”.....	5-60
Table 23 Connection template of type “PTP 820C” attributes.....	5-61
Table 24 Connection template of type “PTP820C, PTP820E, PTP820S, PTP820G” attributes.....	5-65
Table 25 Connection template assignment table.....	5-76
Table 26 NE name table.....	5-81
Table 27 Performance type table.....	5-81
Table 28 Current performance table.....	5-82
Table 29 NE name table.....	5-85
Table 30 Performance type table.....	5-85
Table 31 Historical performance table.....	5-87
Table 32 Historical data selection table.....	5-88
Table 33 Historical performance graph area.....	5-90
Table 34 Performamnce collection control attributes.....	5-95
Table 35 Performamnce template area attributes.....	5-99
Table 36 Template definition area attributes.....	5-100
Table 37 Fields for a topological link.....	5-112
Table 38 Fields for a topological link attributes.....	5-127
Table 39 Managed Elements table.....	5-147
Table 40 Discover settings table.....	5-185

Table 41	Fields for an SNMP range search	5-187
Table 42	Unmanaaged elements table	5-190
Table 43	Ethernet Services Ports view table.....	5-208
Table 44	TDM Services Ports view table	5-219
Table 45	Audit log table.....	5-227
Table 46	Alarm attributes	5-252
Table 47	HW inventory table	5-315
Table 48	SW inventory table	5-315
Table 49	SW inventory table	5-316
Table 50	Performance table attributes	5-326
Table 51	Open SNMP tree area attributes.....	5-352
Table 52	Open SNMP configuration area attributes	5-352
Table 53	Alias list table	5-354
Table 54	Current alarm table	5-359
Table 55	Current alarm list.....	5-364
Table 57	System group description.....	6-3
Table 58	SNMP group example	6-4
Table 59	entPhysicalTable description	6-6
Table 60	System manager menus.....	8-8
Table 61	EMS status buttons	8-13
Table 62	HA Configuration Status.....	8-14
Table 63	Database configuration buttons	8-19
Table 64	Database configuration attributes.....	8-20
Table 65	EMS server page attributes.....	8-132
Table 66	EMS server page attributes.....	8-135
Table 67	Field description:	8-148

About This User Guide

This guide contains the following chapters:

- Chapter 1: Before You Start
- **Error! Reference source not found.**Getting Started
- Chapter 3: GUI Overview
- Chapter 4: Predefined perspectives
- Chapter 5: All views and dialogs
- Chapter 6: SNMP Agent
- Chapter 7: PTP 820 NMS Alarms
- Chapter 8: System Manager
- Chapter 9: Abbreviations

Contacting Cambium Networks

Support website:	<ul style="list-style-type: none">• http://www.cambiumnetworks.com/support
Main website:	<ul style="list-style-type: none">• http://www.cambiumnetworks.com
Sales enquiries:	<ul style="list-style-type: none">• solutions@cambiumnetworks.com
Support enquiries:	<ul style="list-style-type: none">• support@cambiumnetworks.com
Repair enquiries:	<ul style="list-style-type: none">• rma@cambiumnetworks.com
Telephone number list:	<ul style="list-style-type: none">• http://www.cambiumnetworks.com/contact
Address:	Cambium Networks Limited, Linhay Business Park, Eastern Road, Ashburton, Devon, UK, TQ13 7UP

Purpose

Cambium's PTP 820 Network Management System (NMS) documents are intended to instruct and assist personnel in the operation, installation and maintenance of the Cambium equipment and ancillary devices. It is recommended that all personnel engaged in such activities be properly trained.

Cambium disclaims all liability whatsoever, implied or express, for any risk of damage, loss or reduction in system performance arising directly or indirectly out of the failure of the customer, or anyone acting on the customer's behalf, to abide by the instructions, system parameters, or recommendations made in this document.

Cross references

References to external publications are shown in italics. Other cross references, emphasized in blue text in electronic versions, are active links to the references.

This document is divided into numbered chapters that are divided into sections. Sections are not numbered but are individually named at the top of each page and are listed in the table of contents.

Feedback

We appreciate feedback from the users of our documents. This includes feedback on the structure, content, accuracy, or completeness of our documents. Send feedback to support@cambiumnetworks.com.

Problems and warranty

Reporting problems

If any problems are encountered when installing or operating this equipment, follow this procedure to investigate and report:

- 1 Search this document and the software release notes of supported releases.
- 2 Visit the support website.
- 3 Ask for assistance from the Cambium product supplier.
- 4 Gather information from affected units, such as any available diagnostic downloads.
- 5 Escalate the problem by emailing or telephoning support.

Repair and service

If unit failure is suspected, obtain details of the Return Material Authorization (RMA) process from the support website.

Hardware warranty

Cambium's standard hardware warranty is for one (1) year from date of shipment from Cambium Networks or a Cambium distributor. Cambium Networks warrants that hardware will conform to the relevant published specifications and will be free from material defects in material and workmanship under normal use and service. Cambium shall within this time, at its own option, either repair or replace the defective product within thirty (30) days of receipt of the defective product. Repaired or replaced product will be subject to the original warranty period but not less than thirty (30) days.

To register Cambium Networks products or activate warranties, visit the support website. For warranty assistance, contact the reseller or distributor.



Caution

Using non-Cambium parts for repair could damage the equipment or void warranty. Contact Cambium for service and repair instructions.

Portions of Cambium equipment may be damaged from exposure to electrostatic discharge. Use precautions to prevent damage.

Security advice

Cambium Networks systems and equipment provide security parameters that can be configured by the operator based on their particular operating environment. Cambium recommends setting and using these parameters following industry recognized security practices. Security aspects to be considered are protecting the confidentiality, integrity, and availability of information and assets. Assets include the ability to communicate, information about the nature of the communications, and information about the parties involved.

In certain instances, Cambium makes specific recommendations regarding security practices, however the implementation of these recommendations and final responsibility for the security of the system lies with the operator of the system.

Warnings, cautions, and notes

The following describes how warnings and cautions are used in this document and in all documents of the Cambium Networks document set.

Warnings

Warnings precede instructions that contain potentially hazardous situations. Warnings are used to alert the reader to possible hazards that could cause loss of life or physical injury. A warning has the following format:

**Warning**

Warning text and consequence for not following the instructions in the warning.

Cautions

Cautions precede instructions and are used when there is a possibility of damage to systems, software, or individual items of equipment within a system. However, this damage presents no danger to personnel. A caution has the following format:

**Caution**

Caution text and consequence for not following the instructions in the caution.

Notes

A note means that there is a possibility of an undesirable situation or provides additional information to help the reader understand a topic or concept. A note has the following format:

**Note**

Note text.

Caring for the environment

The following information describes national or regional requirements for the disposal of Cambium Networks supplied equipment and for the approved disposal of surplus packaging.

In EU countries

The following information is provided to enable regulatory compliance with the European Union (EU) directives identified and any amendments made to these directives when using Cambium equipment in EU countries.



Disposal of Cambium equipment

European Union (EU) Directive 2002/96/EC Waste Electrical and Electronic Equipment (WEEE)

Do not dispose of Cambium equipment in landfill sites. For disposal instructions, refer to

<http://www.cambiumnetworks.com/support>.

Disposal of surplus packaging

Do not dispose of surplus packaging in landfill sites. In the EU, it is the individual recipient's responsibility to ensure that packaging materials are collected and recycled according to the requirements of EU environmental law.

In non-EU countries

In non-EU countries, dispose of Cambium equipment and all surplus packaging in accordance with national and regional regulations.

Chapter 1: Before You Start

PTP 820 NMS is a comprehensive Network Management System offering centralized operation and maintenance capability for a range of network elements.

PTP 820 NMS offers full range management of network elements. It can perform configuration, fault, performance and security management. PTP 820 NMS is the user interface to transmission and access products and the key issue for the system is to present management networks in the simplest possible manner. The software has network auto-discovery and uses the configuration data in the network elements to automatically build the managed network. The various elements and their attributes may be accessed using the intuitively graphical presentation of the element and its components. PTP 820 NMS has a continuously updated display of network status and network events are reported from the elements using notifications. An extensive database and context sensitive help facilities enable the user to analyze and report network events.

PTP 820 NMS provides the following network management functionality:

- Fault Management
- Configuration Management
- Performance Monitoring
- Security Management
- Graphical User Interface with Internationalization
- Network Topology using Perspectives and Domains
- Automatic Network Element Discovery
- HW and SW Inventory
- Software Download jobs
- Northbound interface to higher order OSS
- Report Generator

Functionality is maintained during network growth, with solutions covering the entire range of radio networks from a single hop to nationwide multi-technology networks. High availability and reliability is obtained through various redundancy schemes.

PTP 820 NMS functionality

The PTP 820 NMS system is scalable both in size and functionality. The PTP 820 NMS Server is the basis for any PTP 820 NMS system, providing basic functionality within the Fault, Configuration, Performance and Security (FCPS) management areas. The PTP 820 NMS Server is by itself an advanced tool for the user to perform operations and monitor network elements for the whole operational network in real time. The flexible client/server architecture gives the operators easy access to all network elements and full control of the system from many different locations.

By selecting among a set of optional features, the PTP 820 NMS system can be enhanced and tailored to each operator's individual needs and requirements. With all optional features installed, PTP 820 NMS system provides the operator with an advanced and sophisticated network management system that will highly increase the efficiency of operations and maintenance in the network.

For easy integration to external higher-level management systems, a Northbound SNMP interface can be provided.

Online Help

This is the online help system for the PTP 820 NMS network management system. Click [here](#) to read more about how to use the online user manual, and how to launch the manual from different parts of the application.

The manual can provide you with help about how to install and [how to configure the application](#). As soon as you know [how to discover and manage a network element](#), you can start [designing your network](#) as desired.

Reading the definitions about the [different graphical objects in the application](#) will help you understand more about this manual. The manual contains a wide selection of "how-to's" (e.g. [How to download software to an NE](#)), and a detailed description of each perspective (e.g. the [Geographical Surveillance](#) perspective) and view (e.g. the [Geographical Tree](#) view).


More information

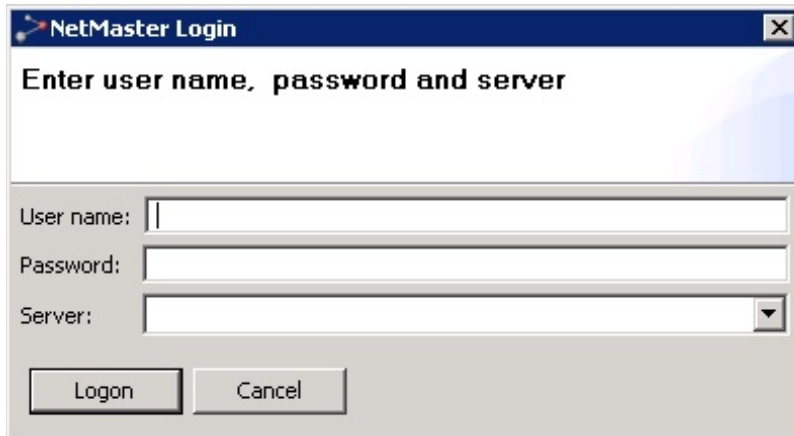
Install the unit in accordance with the instructions in this manual.

If you cannot find the answer to your question in the user manual, contact your responsible support person.

Chapter 2: Getting Started

Logging in

- 1 Launch the PTP 820 NMS Client application  from the Start menu. The login dialog appears.



The image shows a Windows-style dialog box titled "NetMaster Login". It has a blue header bar with the title and a close button. Below the header, the text "Enter user name, password and server" is displayed. There are three input fields: "User name:" with a text box, "Password:" with a text box, and "Server:" with a text box and a dropdown arrow. At the bottom, there are two buttons: "Logon" and "Cancel".

- 2 Enter a **User name** and **Password**. The initial credentials are:

- User name: **root**
- Password: **pw**



Note: It is strongly recommended to change the password as soon as possible to prevent unauthorized access (refer to [How to change your password](#)).

- 3 In **Server**, enter one of the following:
 - Network name of a PTP 820 NMS server
 - IP-address of a PTP 820 NMS server
 - The value **localhost**, if the server is running on the same computer as the client. Leaving the field blank, has the same effect.

Configuring PTP 820 NMS For Server High Availability

Server High Availability is intended to ensure continuous PTP 820 NMS operation. For instructions on how to configure a server High Availability setup, refer to the PTP 820 NMS Server High Availability chapter in the PTP 820 NMS.

Configuring PTP 820 NMS for Database High Availability

PTP 820 NMS also offers a Database High Availability option, which can be implemented if Server High Availability is implemented. For instructions on how to configure a database High Availability setup, refer to the PTP 820 NMS Database High Availability chapter in the PTP 820 NMS Installation Guide.

Using the correct IP address format

PTP 820 NMS can communicate with the NEs using either IPv4 or IPv6, but not a mix of the two. Therefore you must decide prior to installation in which format the network will be managed

Modifying connection templates

A connection template contains a list of attributes (SNMP and HTTP parameters) for defining communication between the NEs and PTP 820 NMS. It can also contain a set of configurable parameters (Trap Management, NTP, UTC) that are enforced on the devices assigned to this connection template.

Each type of NE (such as PTP 820C, PTP 820G, etc.) has a default connection template, which can be edited. Different connection templates can be configured for different sets of elements. A device can have only one connection template assigned to it at a given moment.

The templates can be assigned to NEs at different stages of the discover process:

- Prior to discovery: In the New discover settings window accessed from the [Discover Settings](#) view, you can select for each device type the connection template to use for device discovery. Data in the connection template will be used to scan the network. Only devices that match the selected connection template credentials will be discovered.
- After discovery but prior to device management: In the [Unmanaged Elements](#) view you can reassign connection templates for discovered elements. This determines which connection template is applied to the device once it is managed. If the connection template contains also configuration parameters, these will be set on the device upon device management.
- After a device is managed: Connection templates can be reassigned in the the [Connection Template Assignment](#) view. If the connection template contains also configuration parameters, these will be set on the device at the next polling interval.
- At a minimum, the parameters that need to be configured in order to manage a device are SNMP and HTTP (for devices that support HTTP) version and authentication parameters. They need to have the same value as on the device.
- For full details about how to configure connection templates, see [Connection Templates view](#).

Template Definition

Modify details of selected template

[This template is currently assigned to 4 network elements.](#)

Connection Polling: 1200

Configuration Reconcile: 24

File transfer protocol: FTP

Hypertext protocol: HTTP

Hypertext User: admin [Set Password...](#)

IP Address Family

IP Address Family: Disabled

SNMP Configuration Management

SNMP Version: v2c

SNMP User: admin [Set Password...](#)

Authentication Algorithm: MD5

Encryption Mode: DES

Read Community: public

Write Community: private

Trap Receiver Management

Trap Receiver Strategy: Disabled

IP List:

Scheduled Backup of Network Element Configuration

☐ Enable Run every 2 days at time 12:00 AM

NTP Configuration Management

NTP Configuration Strategy: Disabled

NTP Admin State: Disabled

NTP Version: NTPv4

NTP Server:

UTC Configuration Management

UTC Configuration Strategy: Disabled

UTC Offset Hours: 0

UTC Offset Minutes: 0

DST Start Month: 1

DST Start Day: 1

DST End Month: 1

DST End Day: 1

DST Offset (Hours): 1

How to configure polling and traps in PTP 820 NMS

PTP 820 NMS uses a polling mechanism towards all network elements to check if the NE is "alive" and to check if there are any alarms or configuration changes on the NE. The frequency of this polling should be configured depending on:

- The available bandwidth for network management in your network
- The CPU load on the PTP 820 NMS server
- The CPU load on the NEs
- What response time is accepted for surveillance of the NEs

SNMP network elements

SNMP is a connectionless protocol. Even if notifications/traps are received from an SNMP NE, PTP 820 NMS still needs to poll the element for lost traps and to verify that connection is ok.

As a general rule, the polling interval should be:

- lengthened (relative to the default) if DCN network bandwidth is limited or processing load is too high.
- shortened if traps are not configured but faster response time is desired.

The intervals for polling SNMP NEs are configurable in PTP 820 NMS using connection templates **polling interval**

A connection template contains a list of attributes used when setting up connections for this NE type. Some of these attributes are user configurable, including passwords. For some NE types the polling intervals are also available for configuration. This attribute can be defined in [Connection Polling](#) field in the [Connection Templates](#) view. Because different connection templates can be configured for different sets of elements, polling can be configured differently for different parts of the network.

About SNMP trap handling: traps and polling

When PTP 820 NMS server is set up as trap receiver/listener in the SNMP agent on the NEs in your network, PTP 820 NMS will receive and process traps immediately as they appear on the NEs.

If PTP 820 NMS is not set up as trap receiver on some NEs, PTP 820 NMS will only check alarm status when polling these NEs. Whenever alarm status is updated due to polling, changes in alarm status will only be reported at the end of every polling interval.

Please note that port 162 must be open in the firewall on the PTP 820 NMS server, in order to receive traps.

Discovering and managing elements

The discovery process is the process by which PTP 820 NMS identifies new network elements so it can manage them. The following sub-sections describe the process in detail. Essentially, the flow is as follows:




The operator defines IP-address-based search ranges for discovering new elements. The elements discovered in the defined search-ranges automatically appear in the *Unmanaged elements* view.

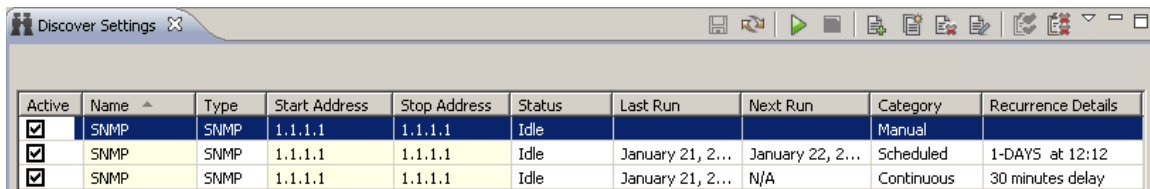
From the *Unmanaged elements* view, you can decide which elements to manage. These elements are turned into managed elements by moving them into the preferred domain in the [Geographical Tree](#) view or [Logical Tree view](#).

How to discover an NE

To discover an NE:

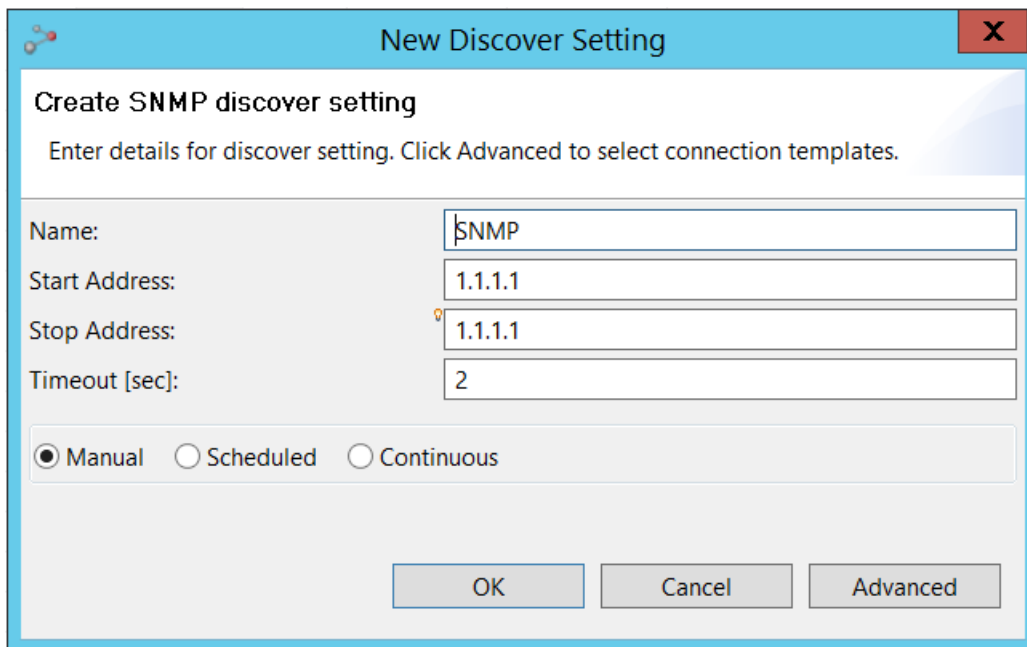
- 1 Navigate to **Perspective > Open Perspective > Discover** to open the Discover perspective.

- 2 In the [Discover Settings view](#), click  to create a new search task for discovering the NE(s) you want to manage. Alternatively, select a row and click  to edit or  to clone an existing search task.



Active	Name	Type	Start Address	Stop Address	Status	Last Run	Next Run	Category	Recurrence Details
<input checked="" type="checkbox"/>	SNMP	SNMP	1.1.1.1	1.1.1.1	Idle			Manual	
<input checked="" type="checkbox"/>	SNMP	SNMP	1.1.1.1	1.1.1.1	Idle	January 21, 2...	January 22, 2...	Scheduled	1-DAYS at 12:12
<input checked="" type="checkbox"/>	SNMP	SNMP	1.1.1.1	1.1.1.1	Idle	January 21, 2...	N/A	Continuous	30 minutes delay

- 3 Define the search range by entering the desired IP addresses in the **Start Address** and **Stop Address** fields. Make sure that:
 - The IP range includes the NE you want to discover. Make sure to use the correct [IP address format](#).
 - You are using the correct [connection template](#) for your NE-type.



New Discover Setting

Create SNMP discover setting

Enter details for discover setting. Click Advanced to select connection templates.

Name:




Start Address:

Stop Address:

Timeout [sec]:

☒ Manual
 ☐ Scheduled
 ☐ Continuous

OK Cancel Advanced

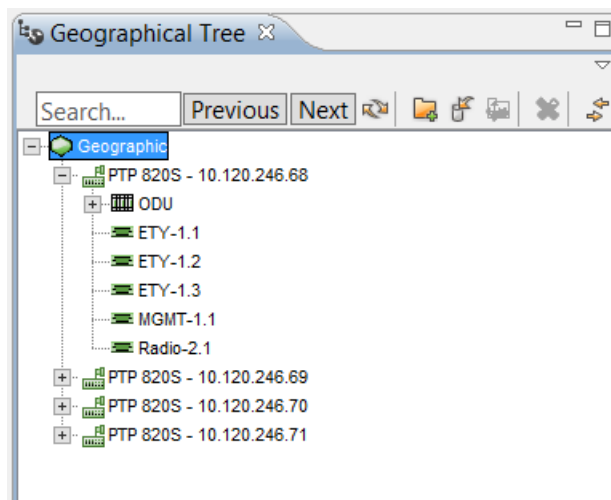
- 4 Set the discovery process type to one of the following:
 - **Manual** – a discovery process that runs only when the Run Manual Now  icon is clicked. This is the default option.
 - **Scheduled** – a discovery process that is scheduled to run on a daily or weekly basis.
 - **Continuous** – a discovery process that is scheduled to run an endless number of discovery cycles, with a configurable delay between cycles.
- 5 Click **OK**.
- 6 In the Discover Settings view:
 - i Enable your search by checking the **Active** checkbox in the row corresponding to the discovery task you defined.
 - ii Click  to save your changes.
 - iii Click  to start a **Manual Discover** process and wait for it to finish. Search progress is displayed in the **Status** column of the **Discover Settings view**.
- 7 The discovered NEs are displayed in the **Unmanaged Elements** table.

Unmanaged Elements						
Drag selected elements into a domain to manage.						
Discovered by	NE Name	Product Name	Address	Connection Template	Status	Description
SNMP	PTP 820S - 10.120.246.71	PTP 820S	10.120.246.71	PTP-820S		High capacity packet radio outdo...
SNMP	PTP 820S - 10.120.246.69	PTP 820S	10.120.246.69	PTP-820S		High capacity packet radio outdo...
SNMP	PTP 820S - 10.120.246.70	PTP 820S	10.120.246.70	PTP-820S		High capacity packet radio outdo...
SNMP	Microwave radio	PTP 820G	10.120.200.76	PTP-820G		PTP 820G 1RU, 2 radio, 6 GbE, 16 ...
SNMP	PTP 820C - 10.120.246.72	PTP 820C	10.120.246.72	PTP-820C		High capacity packet radio outdo...
SNMP	Microwave radio	PTP 820G	10.120.200.67	PTP-820G		PTP 820G 1RU, 2 radio, 6 GbE, 16 ...
SNMP	PTP 820S - 10.120.246.68	PTP 820S	10.120.246.68	PTP-820S		High capacity packet radio outdo...
SNMP	PTP 820C - 10.120.246.62	PTP 820C	10.120.246.62	PTP-820C		High capacity packet radio outdo...
SNMP	Microwave radio	PTP 820G	10.120.200.74	PTP-820G		PTP 820G 1RU, 2 radio, 6 GbE, 16 ...
SNMP	PTP 820C - 10.120.246.73	PTP 820C	10.120.246.73	PTP-820C		High capacity packet radio outdo...
SNMP	Microwave radio	PTP 820G	10.120.200.75	PTP-820G		PTP 820G 1RU, 2 radio, 6 GbE, 16 ...

How to manage an element



The NEs discovered in the Discover process are displayed in the [Unmanaged Elements](#) view.

To manage an element, select it in the **Unmanaged Elements** table (as shown below) and [drag it into the domain](#) you want in the [Geographical Tree](#) view (shown in the left pane) or Logical Tree view. Alternatively, right-click the element in the **Unmanaged Elements** table, select **Manage Element(s)**, and select where you want the element in the [Geographical Tree](#) view (shown in the left pane) or Logical Tree view



How to unmanage/delete an element

To unmanage or delete an NE:

- 1 Select the NE in the Geographical or Logical or Ethernet or TDM Tree or Map, or in the [Managed Elements](#) view.
- 2 Click the Delete button , or right-click the NE and select **Delete**. The NE will now appear in the [Unmanaged Elements](#) view.
- 3 Optionally, in the [Unmanaged Elements](#) view, select the NE and click the Delete button , or right-click the NE and select **Delete Discovered Element(s)**. Upon confirmation, the NE will be removed completely from the application.

Viewing and Configuring Alarms

Currently raised alarms on the device can be viewed in the [Active Alarms](#) view, and alarms that were cleared can be viewed in the [Historical Alarms view](#). If you acquire an *Alarm to Service Correlation* license, you can also view all the related confirmed end to end services that are associated with an alarm, as described in [Viewing alarm-to-service correlation](#).

Alarms can be received as SNMP traps, or retrieved by the PTP 820 NMS server through the synchronization mechanisms ([Connection Polling](#), [Configuration Reconcile](#) or [Manual Reconcile](#)). Refer to the [Connection Templates](#) view for more details.

How to customize the appearance of alarms

You can optionally customize the appearance of incoming NE alarms. This is done by creating alarm templates in the [Alarm Templates](#) view, and then assigning alarm templates to NEs in the [Alarm Templates Assignment](#) view.

Alarm templates are used for changing alarm severities, changing alarm text, or blocking certain incoming alarms from a set of NEs.

To create and use an alarm template:

1. Create an alarm template as described in [Creating a new alarm template](#).
2. Assign an alarm template to devices as described in [Assigning an alarm template to an NE](#).

For full details about how and when to use alarm templates, refer to the [Alarm Templates view](#) chapter.

How to acknowledge an alarm

Fault conditions on NE are [visualized in different views](#). Whenever a [new alarm](#) is discovered, it is recommended that this error condition is followed up by someone. This involves identifying and fixing the error on the equipment (solving the "root-cause problem"), and solving potential consequences of the error condition for users of your network.

A new fault condition that has been followed up can be flagged by setting an "Acknowledged" flag on the alarm.

To acknowledge an alarm:

1. Open an [Active Alarms](#) view containing the new alarm.
2. Select the line containing the new alarm and use the [Acknowledge Alarms](#) operation.
3. In the [Alarm Comments](#) dialog, enter a sufficient description of how this alarm is being followed up, and press **OK**.

The alarm is now acknowledged and no longer considered as a "new" alarm, and the [alarm indicators in the topological views](#) are updated to reflect the new alarm status for the most severe new and active alarms.

The same procedure can be followed on cleared alarms in the [Historical Alarms](#) view, except that acknowledging alarms will not influence the topological views.

If you wish, you can [unacknowledge an acknowledged alarm](#) so it will be considered again a “new” alarm.

How to configure and receive alarm notifications

In the [Alarm Notifications view](#), you can optionally configure and enable [Alarm Notifications Rules](#) for generating [sounds](#), [e-mails](#) or [On-screen Notifications](#) when certain alarms occur in your network.

In the [Alarm Notification Table view](#) you can view the alarm notifications for alarms that meet the [On-screen Notifications](#) criteria of the [Alarm Notifications Rules](#).

Viewing Alarm reports

PTP 820 NMS records information about active and cleared device alarms. The information can be viewed in various PTP 820 NMS views and generated reports, using the legacy Alarm Reports mechanism or the Next Generation (NG) Alarm Reports mechanism.

The information can also be exported to file, such as a CSV file, for further processing.

Generating NG Alarm Reports

You can generate the following types of NG alarm reports using the `alarmreport` CLI command.

- [Alarm Log Report](#) - Lists current and historical alarms
- [Current Alarms Report](#) - Lists current alarms
- [Alarmed NEs Report](#) - Lists NEs ordered by the number of alarms on the NE
- Alarm Frequency Report - Lists the most frequent logged alarms in the specified period
- Alarm Frequency by NE Report - Lists the most frequent logged alarms in the specified period, by NE

The report is generated as soon as the CLI command is given, and saved to the specified location, as described in [Generating Alarms reports using a CLI command](#).

Viewing Legacy Alarm Reports

You can view the following types of legacy alarm reports from **Views > Reports** in the GUI:

- [Legacy Alarm Frequency Report grouped by Network Element](#) - Lists the 100 most frequent logged alarms in the entire network during the last 7 days, by NE.
- [Legacy Alarm Frequency Report List](#) - Lists the 100 most frequent logged alarms in the entire network during the last 7 days.

Viewing and Generating NG Inventory Reports

You can instruct PTP 820 NMS to generate various inventory reports either through the GUI or using the `inreport` command line interface (CLI) command.

- To generate NG inventory reports via CLI, refer to [Generating Inventory reports using a CLI command](#).
- To generate NG inventory reports using the GUI, refer to [Generating Inventory reports via the GUI](#).

You can generate any of the following types of inventory reports:

- [Ethernet Ports Report](#) - provides information about the devices' Ethernet ports, including cascading ports
- [Frequency Change Report](#) - Provides information about changes in Tx and Rx frequency of radio ports in network elements
- [Full Link Report](#) - Provides up-to-date information regarding the link as well as 24 hours of link PM counters

- [Network Element Report](#) – provides status information and data about network elements
- [Radio Report](#) – Provides information about radio interfaces
- [Link report](#) – Provides data about links, such as transmit and receive frequencies and slot number locations
- [Licensing Report](#) – Provides data about the licenses enabled for each network element
- [Versions Report](#) – Provides data about the software and firmware versions installed on network elements
- [SFP Inventory Report](#) – Provides static SFP information for each electrical and optical Ethernet port of the specified network elements
- [Serial Numbers Report](#) – Displays the serial number for each network element

Viewing Legacy Inventory Reports

Inventory information can be viewed in the following GUI views:

- [Software Inventory](#) view – Displays all available software memory banks for the selected NEs. Each line displays the status of a memory bank and details about the software stored on this bank. You can also select a memory bank in the table to activate idle software or reset active software.
- [Hardware Inventory](#) view – Displays an overview of the currently available hardware elements of the selected NEs. "Hardware elements" refers to physical equipment in the NE, such as cards, interfaces, modules, boards and chips.
- [Transmission Inventory](#) view – Displays transmission information for the selected NEs

In each of these views, inventory data can be viewed for an individual node in the topology views by right-clicking the node, selecting **Configuration**, and then selecting **Hardware Inventory** or **Software Inventory** or **Transmission Inventory**. Alternatively, you can view inventory data for the entire network, by selecting from the main menu **Views > Configuration** and then selecting **Hardware Inventory** or **Software Inventory** or **Transmission Inventory**. You can schedule periodic generation of a hardware, software, or transmission inventory report in the [Scheduled Reports](#) view.

You can also generate from the GUI a [Legacy Inventory Report](#) that displays hardware, software and transmission inventories for all the managed elements within the scope of the report. The report can be generated for an individual node in the topology views by right-clicking the node and selecting **Reports > Inventory Report**. Alternatively, you can generate the inventory report for the entire network by selecting **Views > Reports > Inventory Report** from the **main** menu.

Finally, you can generate from the GUI a [Legacy Network Element Types Overview Report](#) that summarizes the NE types and configurations for all the managed elements within the scope of the report. The report can be generated for an individual node in the topology views by right-clicking the node and selecting **Reports > Network Element Types Overview Report**.

Alternatively, you can generate the inventory report for the entire network by selecting **Views > Reports > Network Element Types Overview Report** from the main menu.

Analyzing Performance counters

NE performance can be analyzed using the various performance reports. Performance data collection and display is available through two mechanisms: legacy performance reports generation, and NG performance reports generation.

The information in the reports can also be exported to file, such as a CSV file, for further processing.

How to collect Performance Monitoring (PM) counters information

Enabling NG PM collection

As a prerequisite to generating NG PM reports, you need to enable NG PM data collection, as follows:

- 1 Enable network-wide collection of PM counters by checking the **Enable Network-wide PM Collection** option in the [Network-wide PM Collection](#) Preferences page.
- 2 Enable network-wide collection of RMON counters by checking the **Enable RMON Collection** checkbox option in the [Network-wide Statistic Counters](#) Preferences page.
- 3 Enable collection of network-wide traffic queue data by checking the **Enable Network-wide Traffic Queue Collection** checkbox option in the [Network-wide PM Collection](#) Preferences page.
- 4 Restart the PTP 820 NMS server, in the [Dashboard View](#) of the [System Manager](#).

Enabling Legacy PM collection

As a prerequisite to generating legacy PM reports, you need to enable legacy PM data collection, as follows:

1. In the [Performance Templates](#) view, configure a performance template for collecting performance data from network elements.
2. Assign a performance templates to NEs as described in [assigning performance templates](#).

Generating Performance Reports

Generating NG PM reports

You can instruct PTP 820 NMS to generate various NG performance reports either through the GUI or using the **pmreport** command line interface (CLI) command

- To generate NG PM reports via CLI, refer to [Generating Performance reports using a CLI command](#).
- To generate NG PM reports using the GUI, refer to [Generating Performance reports via the GUI](#).

You can generate the following types of NG performance reports:

- [Ethernet Radio](#)
- [Interface Performance report - E1 / DS1](#)

- [Interface Performance report - STM1 / OC3](#)
- [Interface Performance report - XC Carrier](#)
- [Radio Performance Report](#)
- [RMON Report](#)
- [Enhanced Radio Performance Report](#)
- [Enhanced Radio Ethernet Performance Report](#)
- [Trails Performance Report](#)
- [SFP Optical Power Performance Report](#)
- [Input Voltage Performance Report](#)
- [Traffic Queue Performance Report](#)

Viewing and Generating Legacy PM reports

Performance information can be viewed in the following GUI views.

- [Current Performance](#) view – This view presents performance measurements as read from NEs each time you select the [Start Performance Reading](#) operation.
- [Historical Performance](#) view – This view presents stored historical performance data that PTP 820 NMS collected from NEs.

In both these views, performance data can be viewed for an individual node in the topology views by right-clicking the node, selecting **Performance**, and then selecting **Current Performance** or **Historical Performance**. Alternatively, you can display performance data for the entire network, by selecting from the main menu **Views > Performance** and then selecting **Current Performance** or **Historical Performance**.

You can also generate in the GUI the following legacy performance reports:

- [Performance Overview Report](#) – Displays a summary of the performance measurement points matching a filter you specify. The report is generated by selecting **Views > Reports > Performance Overview Report**.
- [Performance Details Report](#) – Displays the performance measurement points matching a filter you specify. The report is generated by selecting **Views > Reports > Performance Details Report**. You can schedule periodic generation of a performance report in the [Scheduled Reports](#) view.

Downloading new software or backing up and restoring configuration

Install and configure an FTP or SFTP server

Several tasks, such as software upgrade and configuration backup and restore, require the use of FTP or SFTP. If you wish to use FTP/SFTP, you must install FTP/SFTP server software on the same machine as the PTP 820 NMS server.

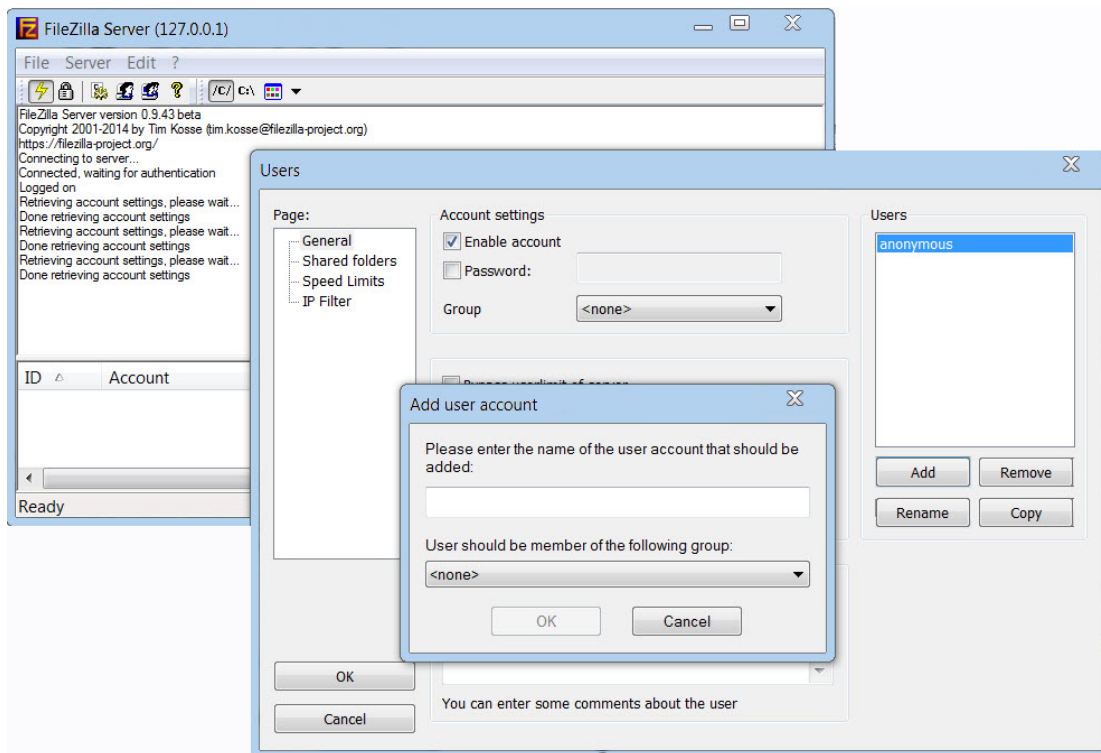


Note: For FTP, it is recommended to use FileZilla_Server software that can be downloaded from the web (freeware).

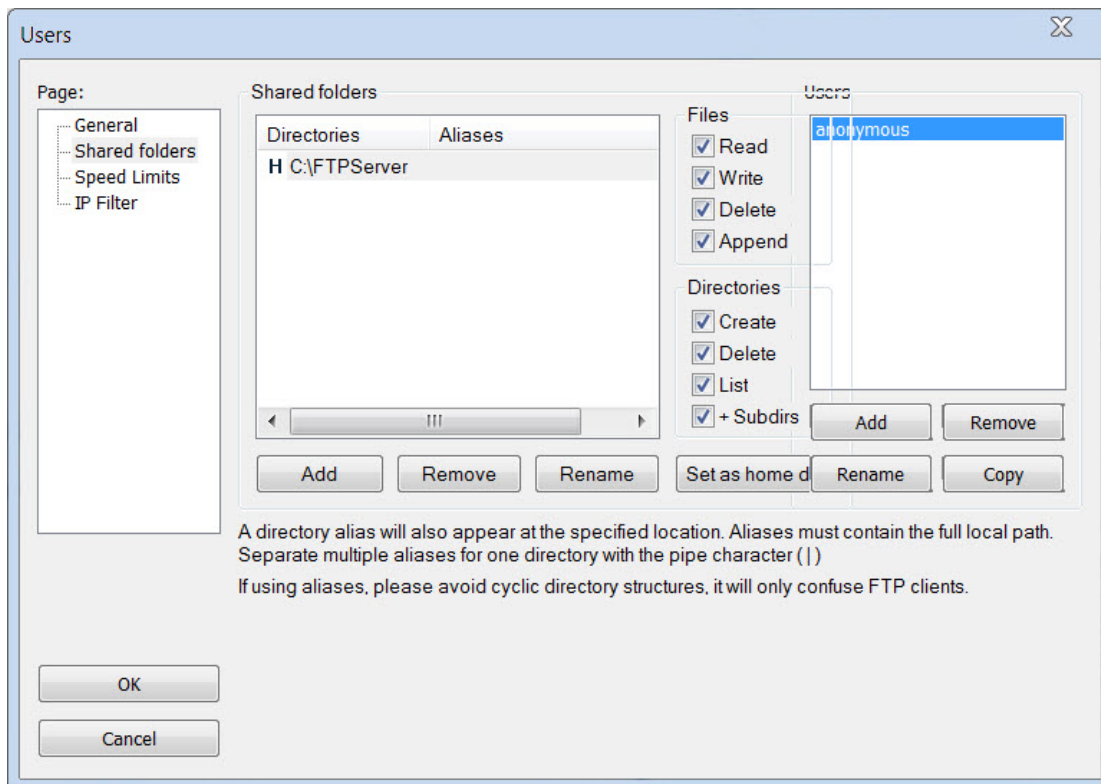
For SFTP, it is recommended to use SolarWinds SFTP/SFCP server (freeware).

To install and configure FTP or SFTP server software on the PTP 820 NMS server machine:

- 1 Create a user and (optional) password on the FTP/SFTP server. For example, in FileZilla Server, perform the following:
 - i From the **Edit** menu, select **Users**.
 - ii In the Users window, click **Add**.
 - iii In the Add user account window, enter a user name and click **OK**.
 - iv In the Users window, select **Enable account** and, optionally, select **Password** and enter a password.
 - v In the Users window, click **OK**.



- 2 Create a shared FTP/SFTP folder on the machine you are using to perform the software upgrade, or configuration backup, export and import, etc. (for example, `C:\FTPServer`). In some cases, this folder serves the FTP application as a temporary memory for the files until PTP 820 NMS moves the files to an internal folder.
- 3 In the FTP/SFTP server, set up the permissions for the shared FTP/SFTP folder. For example, in FileZilla Server:
 - i From the **Edit** menu, select **Users**.
 - ii In the Users window, select **Shared folders**.
 - iii Underneath the Shared folders section, click **Add** and browse for your shared FTP folder.
 - iv Select the folder and click **OK**.
 - v In the Shared folders section, select your shared FTP folder.
 - vi In the Files and Directories sections, select all of the permissions.
 - vii Click **Set as home directory** to make the Shared folder the root directory for your FTP server.
 - viii Click **OK** to close the Users window.



- 4 Enter the settings of the FTP/SFTP server in the [Preferences: External FTP/SFTP Server](#) Preferences page.

High Availability considerations

The FTP/SFTP server settings defined in the Preferences pages (see [Preferences: External FTP/SFTP Server](#)) are stored in the database, and are therefore always synchronized between the Primary and the Secondary servers in a [Server High Availability](#) setup.

However, you must ensure that the FTP/SFTP servers themselves are configured identically on both machines.

IPv6 address format considerations

If you want the FTP/SFTP server to communicate with the NE using the IPv6 address format, you need to set the [IP Address Family](#) in the corresponding connection template to **IPv6**. Alternatively, set the NE's **IP Address Family** to **IPv6** using the EMS user interface or a CLI command.


How to download software to an NE

The views needed in this process can be opened from **Views > Configuration** or by using the context menu of a selected NE in any of the topological views.

Before you start downloading, you might want to check the current software versions on the NE you want to download software to. This can be done as follows:

- 1 Open the [Software Inventory](#) view for the NE (i.e., by selecting the NE in one of the topological views, and using the **Configuration > Software Inventory** context menu).
- 2 Study the Software Name and Version of the memory banks on the unit for which you want to upload new software.
 - If the correct version is already running (on the ACTIVE memory bank), no action needs to be taken.
 - If the correct version is already stored on a memory bank in the unit (on an IDLE memory bank) but has not been activated, you can activate the software by selecting **Activate Software** in the view. No further action needs to be taken.
 - If no correct version is found on this unit, you need to download new software, so that this procedure can be continued.


The following procedure can be followed when downloading software for one single NE and when downloading for several at the same time.

- 1 Start the [Create Software Download Jobs](#) wizard for the NE for which you want to upload new software, by selecting a domain containing this NE in one of the topological views and then selecting **Configuration > Create Software Download Job** in the menu. (Alternatively: if you want to download software to several NEs in different topological models, you should start the wizard directly from the [Software Download Jobs](#) view).
- 2 In the first page in the wizard, **Basic Information**, enter a job name (and a description if needed).
- 3 In the second page in the wizard, **Selecting Elements**, use the **Element Type** dropdown menu to select an NE type.
- 4 Then browse the tree in the **Elements** area and select the NE you want upload new software to:
 - if you want to download to more than one NE, check several checkboxes.
 - if you want to download software to NEs in different topological models, use the Model dropdown menu to switch between the Logical and Geographical Model in the Elements area (this dropdown menu is only available when the wizard is opened directly from the Software Download Jobs view).
- 5 In the third page in the wizard, **Select file to download**, select which software files to download. The window displays all the files uploaded to the PTP 820 NMS server using the Upload Software File  option in the Element Software Management view. Then exit the wizard by using the **Finish** button.
- 6 The [Software Download Jobs](#) view will now open. Select the new job in the table and start the job by using the **Start Job** menu option.
- 7 Monitor the download progress for each of the NEs in the job by expanding the job in the **Software Download Job** view. When the state of the job changes to DONE, the download has completed successfully for this element.

- 8 In the [Software Inventory](#) view, the new software should now be available in one of the memory banks with IDLE status. You might have to press **Refresh** to retrieve the latest status from the NE. You can now activate the new software version by selecting the memory bank in the table and selecting the **Activate Software** menu option. If this software is activated successfully, the memory bank's status will change to ACTIVE, while the previously active memory bank becomes IDLE.

Please note that steps 3 and 4 can be skipped if a single NE was selected when opening the wizard, as this will skip the **Selecting Elements** page in the wizard.

How to schedule a software download job

It is also possible to schedule a software download job for a future date and time. This option is enabled by selecting  Schedule Job in the menu of the [Software Download Jobs](#) view. Refer to [Scheduling Software Download](#).

How to backup and restore NE configuration

You can at any time manually backup the configuration of NEs, and/or schedule automatic backups. You can also restore an NE's configuration from a configuration backup.

Both manual and scheduled configuration backups can be viewed in the [Configuration File Management view](#), and restored from that view.

- To manually backup an NE's configuration file, use the [Backup Configuration](#) option available in the [Configuration File Management view](#).
- To schedule automatic backup of NEs' configuration files, use the [Scheduled Backup](#) option available in PTP 820 connection templates.
- To restore an NE's configuration, use the [Restore Configuration](#) option available in the [Configuration File Management view](#).

Managing Security Groups and Users

How to create a new group

Only users who are defined as Administrators or Security Officers are allowed to create or modify new security groups.

The views needed here are found in the [User Management](#) perspective.

To create a new group:

- 1 In the [Group Administration](#) view select the Create new security group operation.
- 2 In the Create Security Group dialog enter group name and optionally description. Press OK to finish.
- 3 Select the new security group in the [Groups](#) table and then select any appropriate permissions in the Permissions detail part.

How to create a new user

Only users who are defined as Administrators or Security Officers are allowed to create new or modify new users.

The views needed here are found in the [User Management](#) perspective:

- 1 In the [User Administration](#) view select the [Create User Account](#) operation.
- 2 In the [Create New User](#) dialog enter User name, Password and optionally enter additional user data. Press **OK** to finish. Note that the password must comply with the password definition rules specified in the [Password Settings](#) Preferences page.
- 3 Select the new user in the [Users](#) table and then select an appropriate group in the [Groups](#) table.



Note: A user may be assigned to a maximum of one group.

How to change your password

This procedure can be used for all users whenever they want to change their own password. As password change involves logging off the server, all ongoing tasks in the client should be saved and finished before running this procedure.

If you try to define a password that does not comply with the security rules, an appropriate error message is displayed, with instructions for defining a compliant password. The password security rules are set by a user having the appropriate permissions, in the [Password Settings](#) Preferences page.

To change your password:

- 1 Open the [User Settings](#) preference page.
- 2 Enter your current password in the **Current Password** field.
- 3 Enter a new password in the **New Password** field.
- 4 Retype this password in the **Confirm New Password** field.
- 5 If you have retyped the new password correctly, you can now press **OK**.

- 6 The [Verify Password Change](#) dialog will now appear, with a warning that password is changed, and that you will be logged off the server. Close this dialog by pressing **OK**.
- 7 The [PTP 820 NMS Login](#) dialog will now appear. Finish the task, by entering your Login parameters, including your new password and press **OK**.

Please note that a user with [administrator privileges](#) is allowed to change password for other users at any time, e.g. when the user has lost the password. This is done by using the [Change Password](#) operation on a selected user in the [User Administration](#) view. The administrator should use this operation with care, as the selected user's ongoing work is aborted when the server automatically logs off all client sessions for this user.

Note also that in a Database High Availability configuration, if a user password was changed but a switchover to the Standby database occurred before the Active database was backed up, the new password may be lost and the user may need to login with the old password.

Configuring Northbound Interface SNMP

Configuration of Northbound SNMP is a process that involves both configuration of the [Northbound Interface SNMP Settings](#) in the PTP 820 NMS Client as well as properties of the [PTP 820 NMS Agent monitor](#) service:

- 1 Configure Northbound SNMP Settings in the PTP 820 NMS Client:
 - i [Create a new user](#) and add this user to the predefined user group "SNMP Agent".
 - ii Open [Northbound Interface SNMP Settings](#) view by selecting from the menu Views | Northbound Interface | SNMP Settings.
 - iii Press the **Create a new High Level Manager** button to start the [Create High-Level Manager wizard](#).
 - iv Open the [PTP 820 NMS Management Traps](#) preference menu to enable and configure PTP 820 NMS **management trap** settings.
 - v If you want SNMP v3 on the Northbound interface, open the [SNMP V3](#) Preferences page to configure SNMP v3 settings.
- 2 Configure the PTP 820 NMS SNMP Agent:
 - For Windows version, do the following:
 - i Right-click the [SNMP Agent Service](#) icon in the Windows taskbar system tray and select **Configuration**.
 - ii Enter the user name and password for the SNMP Agent user that shall log on to the PTP 820 NMS server as defined in step 1a.
 - iii Enter the URL for the PTP 820 NMS Server to be monitored.
 - iv Stop the SNMP Agent service by right-clicking the PTP 820 NMS SNMP Agent Service **icon** and select **Stop**.
 - v Start the SNMP Agent service by right-clicking the PTP 820 NMS SNMP Agent monitor **icon** and **Start**.
 - For Solaris version, do the following:
 - i Setup username, password and server URL by editing the file:

```
<install-dir>/Northbound SNMP/bin/conf/logininfo.properties
```

Example content of [logininfo.properties](#) (this is just an example, other values for username, password and serverurl are recommended):

```
#NIF login props
#Tue May 18 14:19:24 CEST 2010
username=root
```

```
password=passwd
serverurl=jnp://localhost:1099
```

- ii After the `logininfo.properties` has been set up properly, stop the Northbound SNMP Agent service by running:

```
svcadm disable ngNIFService
```

- iii Then enable the Northbound SNMP Agent service by running:

```
svcadm enable ngNIFService
```

- iv If you want to check the status of the Northbound SNMP Agent service:

```
svcs ngNIFService
```

For detailed information about PTP 820 NMS's northbound interface, see [SNMP Agent](#).



Note: If you configure a High Level Manager using SNMP v2c or v3, you can initiate SNMP queries (GET operations) from the OSS to PTP 820 NMS.

Troubleshooting: how to solve port conflicts

Identify port conflict

By default the PTP 820 NMS SNMP agent will try to bind to UDP port 161. If other SNMP agents shall run in parallel, the port for PTP 820 NMS agent must be changed in order to avoid port conflict.

To identify port conflicts with other processes, see:

```
<install-dir>/Northbound SNMP/bin/logs/nif.log
```

If this log contains entries like this:

```
2010-05-19 11:30:23,671 FATAL Bind Exception : Port 161 is in use. See
PTP 820 NMS installation guide on how to change SNMP agent port.
2010-05-19 11:30:25,756 INFO PTP 820 NMS SNMP agent stopped
```

it means that there is a port conflict.

Solve port conflict

There are two alternative methods to solve port conflicts:

Alternative 1- let PTP 820 NMS SNMP Agent use another port:

- 1 Edit the file

```
<install-dir>/Northbound SNMP/bin/conf/wrapper.conf
```

- 2 Find the line containing

- Windows version:

```
wrapper.app.parameter.2=-p 161
```

- Solaris version:

```
wrapper.app.parameter.3=161
```

- 3 Change the number to another (port) number.

Alternative 2 - Stop the processes that occupy the needed port

Note: Please note that this procedure only applies to Solaris version.

See also [how to identify the processes that occupy a port](#). (Standard for Solaris is that snmpdx and snmpd are running, using port 161)

To stop snmpdx:

```
svcadm disable snmpdx
```

To stop snmpd:

```
svcadm disable sma
```

For more details about stopping snmpd, see

<http://docs.sun.com/app/docs/doc/817-3000/6mikgnghb?a=view>

How to identify a process that occupy a port on Solaris

One way to identify a process that occupy a port, is by looking in `/etc/services`, e.g.:

```
grep -w 161 /etc/services
```

Another way is to create a script 'port2pid' :

```
pids=$(ps -e | sed 1d | awk '{print $1}')
port=$1
if [ "$port" == "" ]; then
    echo "Missing port number parameter"
    exit 1
fi

for f in $pids
do
    /usr/proc/bin/pfiles $f 2>/dev/null | /usr/xpg4/bin/grep -wq "port:
$port"
    if [ $? -eq 0 ]; then
        echo "-----"
        echo "Port $port is being used by PID:"
        ps -ef -o pid -o args | egrep -v "grep|pfiles" | grep $f
    fi
done
```

Then run the script : (set runnable: `chmod +x port2pid`)





```
./port2pid 161
```

Chapter 3: GUI overview

This chapter includes:

- [The graphical user interface](#)
- [The objects in a view](#)
- [Timeslider tool](#)
- [Quick Search field](#)
- [Visualization of alarms](#)

How to use the PTP 820 NMS GUI help system

- Browse topics in the **Contents** frame on the left side of this online help. Click on a topic to be displayed. Use the **Back** and **Forward** buttons to navigate within the history of viewed topics.
-  Use the **Search** frame to display the **Search** view. To quickly locate topics on a particular subject in the documentation, enter a query in the **Search** area. You can narrow the scope of your search by selecting only the sections you are interested in.
-  Click the **Refresh / Show Current Topic** button after you run a search and find a topic you were looking for.
-  Click the **Show in Table of Contents** button to match the navigation tree with the current topic. You might also find it useful to synchronize after following in-topic links.
-  Select the **Show All Topics** button to show documentation about capabilities that are disabled in the application. When you choose to show all topics in the table of contents, the headings for documentation about any disabled activities are shown in the table of contents and also appear in search results.

A text in **italic** identifies the name of a single [GUI](#) object in the application: a [perspective](#), [view](#), [dialog](#), [area](#), field, icon, menu-item, etc.

How to launch the PTP 820 NMS

help system

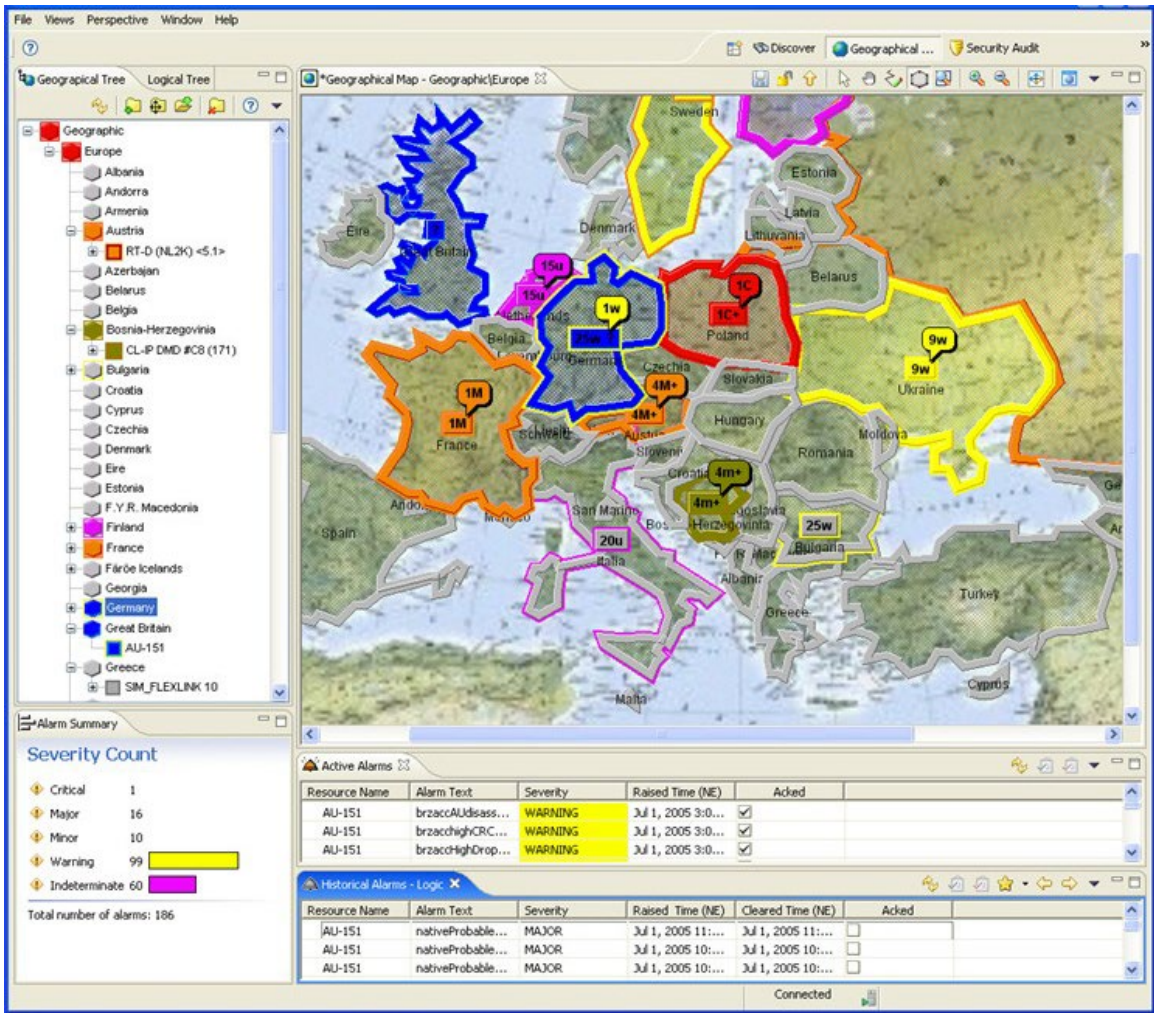


Click the **Help** icon on the top toolbar to launch the manual with this start page.

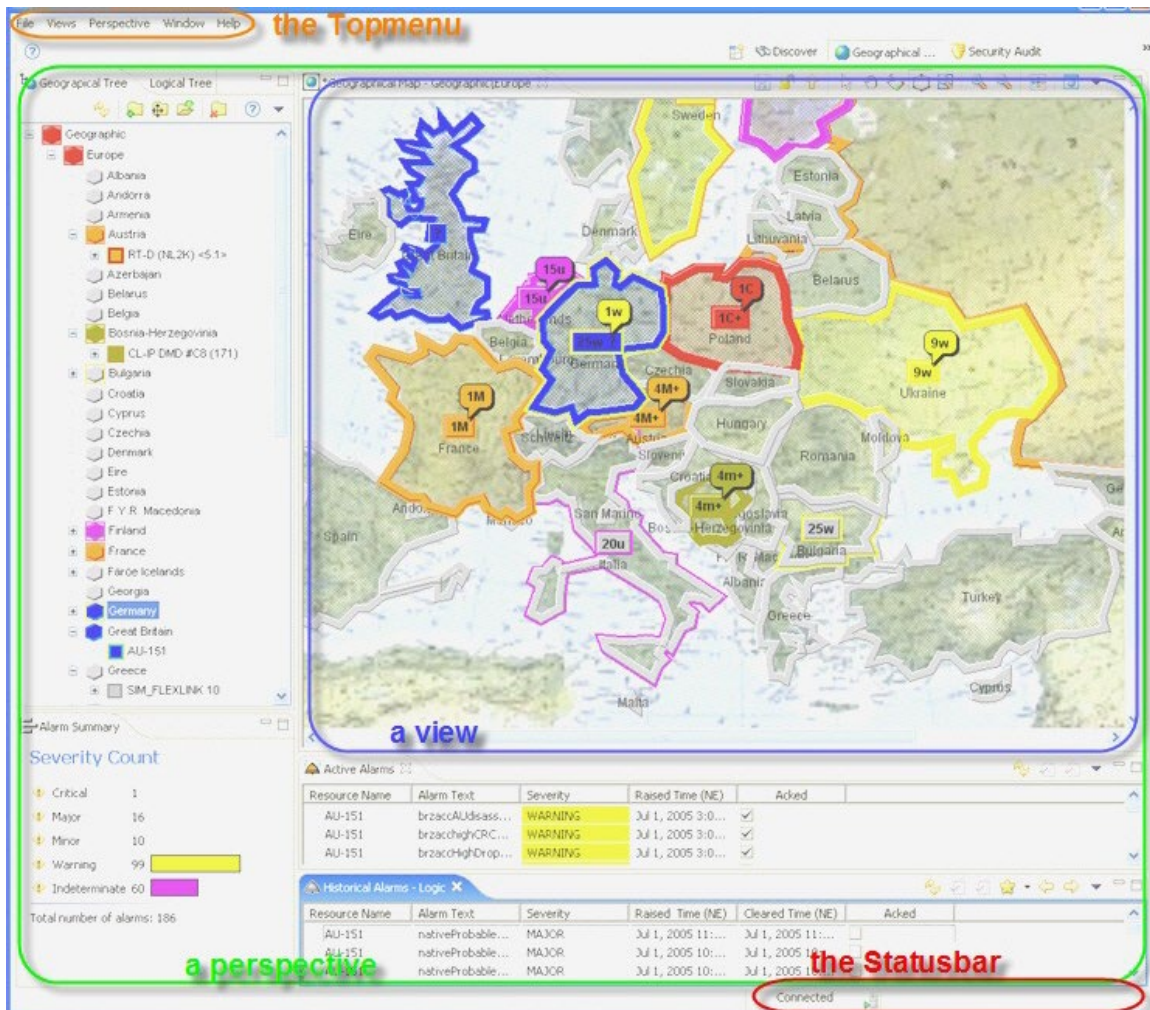
The graphical user interface

PTP 820 NMS is an application built on the Eclipse platform. This platform offers a graphical user interface (GUI) which differs slightly from the standard Microsoft Windows GUI. A snapshot of a typical workspace in the PTP 820 NMS client application might look like this:

Figure 1 Typical workspace view of PTP 820 NMS



If we take a closer look at the picture, we can see that the application is built from several standard objects which will always be present in the application:

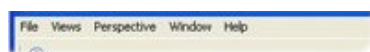
Figure 2 PTP 820 NMS GUI objects

Understanding these objects and how they behave will help you understand the other chapters in this manual.

In addition to the objects in this figure, PTP 820 NMS contains several [dialogs](#), [context menus](#), [view dropdown menus](#) and a set of [preference menus](#). (Please note that some of the functionality described in the user manual will only be visible if the user has sufficient [permissions](#) for using the application).

Main menu

On the top left side of the application you will always find the main menu (marked with orange in the above [Figure 2](#)).

Figure 3 PTP 820 NMS main menu

This is a group of dropdown menus which is used to activate different parts of the application. From this menu, you can:

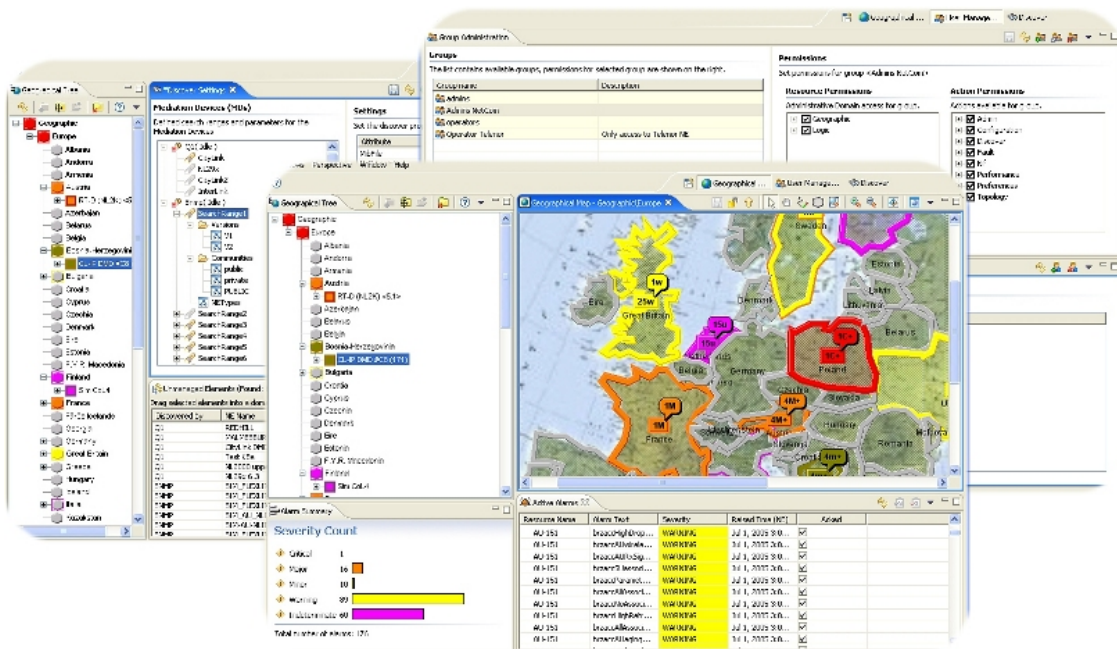
- log off and exit the application
- open most views (not the views that needs data-input to open: these views can only be opened from another view or dialog)
- open and manage all perspectives
- open the program preferences
- open the help system

See chapters about each perspective, about each view or about the program preferences for more details.

Perspectives

A perspective is a collection of views (marked with green in the above [Figure 2](#)), which reflects a certain working situation. Here are a few examples:

Figure 4 PTP 820 NMS different views



Within a perspective, you can open and reposition all the different views you need. When you install PTP 820 NMS, it comes with a set of predefined perspectives that should help you get started when using the application for the first time.

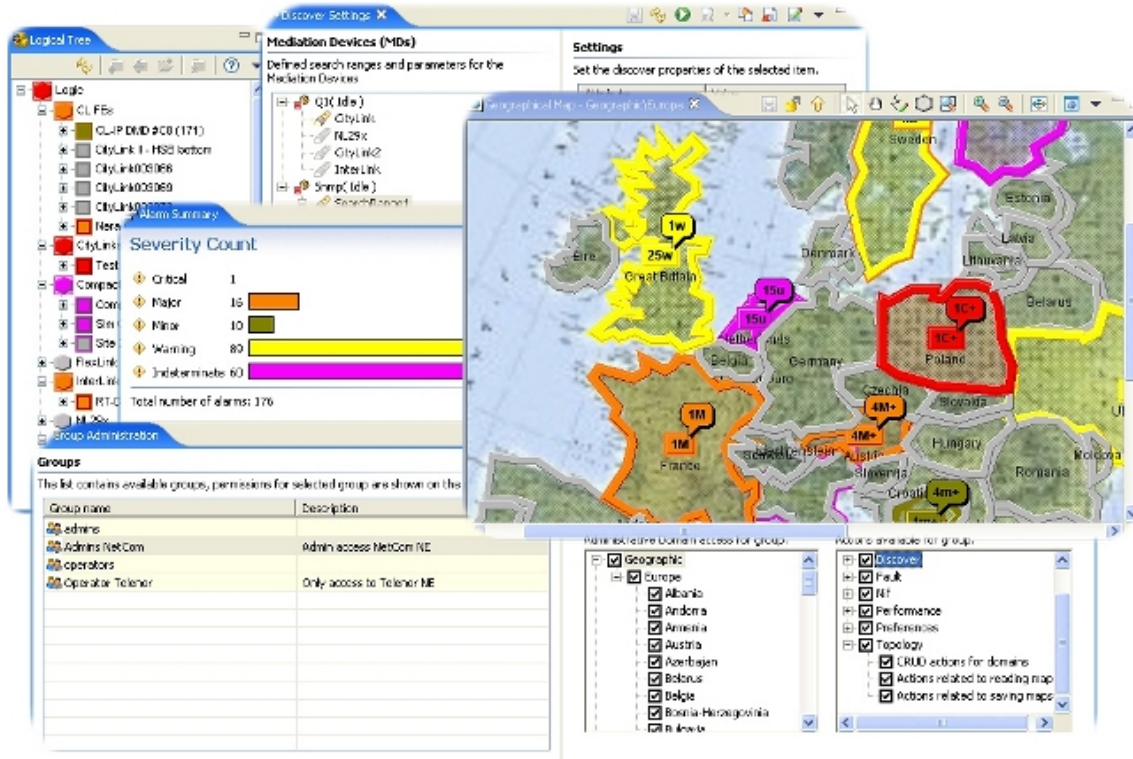
When you open a perspective, all the views belonging to this perspective are displayed. The views will appear with the same position and scope as when you last opened the perspective.

The idea behind perspectives is that they provide you with a fast way of moving between different working situations. You can always reset a perspective to its default, and you can create your own set of perspectives. For more information about opening, moving between and managing perspectives, please see the chapter about [objects in perspectives](#).

Views

A view is a "window" within the application (marked with blue in the above [Figure 2](#)). PTP 820 NMS offers a wide range of functionality available within views, and you can open all your views in the application at the same time. Here are a few examples:

Figure 5 PTP 820 NMS functionality views



The views can be opened, [closed](#), [resized](#), [moved](#) or [detached from the application](#) as you want.

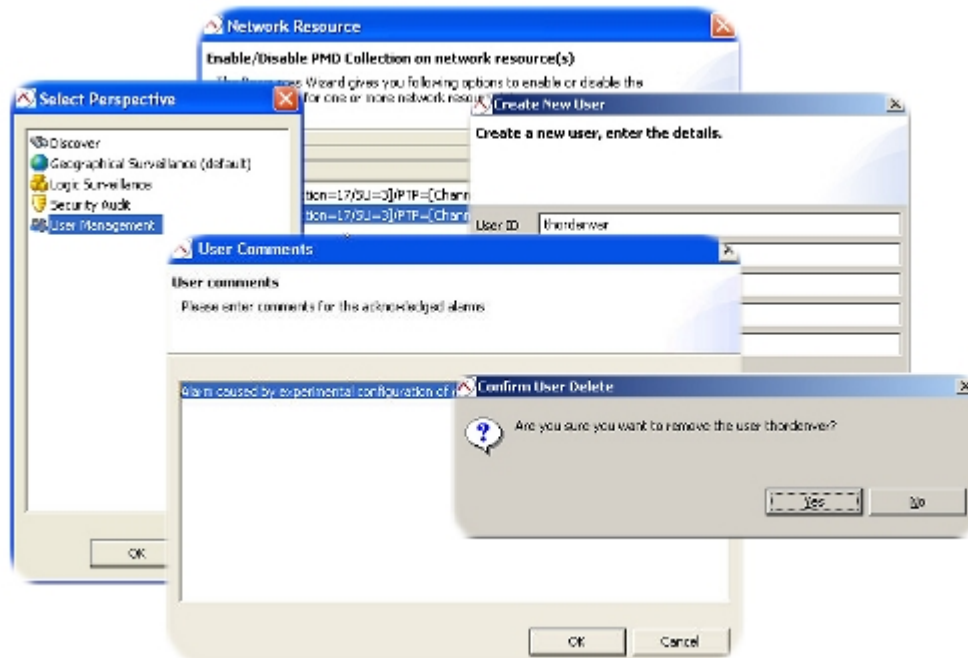
For more information about how to use views, please see the chapter about [objects in views](#) or [how to reposition views](#) within a perspective.

When you open a perspective, a set of views will be displayed. You can open more views by selecting *Views* from the [main menu](#), or by using [context menus](#) or [dropdown menus](#) within the views that are already open.

Dialogs

A dialog is a window that requests information from the user - and must be closed before the user can take further action (as distinct from views - where you can operate all views in the perspective at the same time). The dialog appears on top of the application, and all other controls in the application become unavailable until the tasks in the dialog have been completed and/or the dialog closed. Here are a few examples:

Figure 6 PTP 820 NMS dialogs



Some dialogs are opened from the [main menu](#), while others are opened from [objects in views](#): [context menus](#), [dropdown menus](#) or from the [view toolbars](#). For more information about the operations available in each dialog, see the section of the user manual that describes each view or dialog.

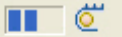
Statusbar

The **statusbar** can be seen at the bottom of the application.



This bar gives you the following information:

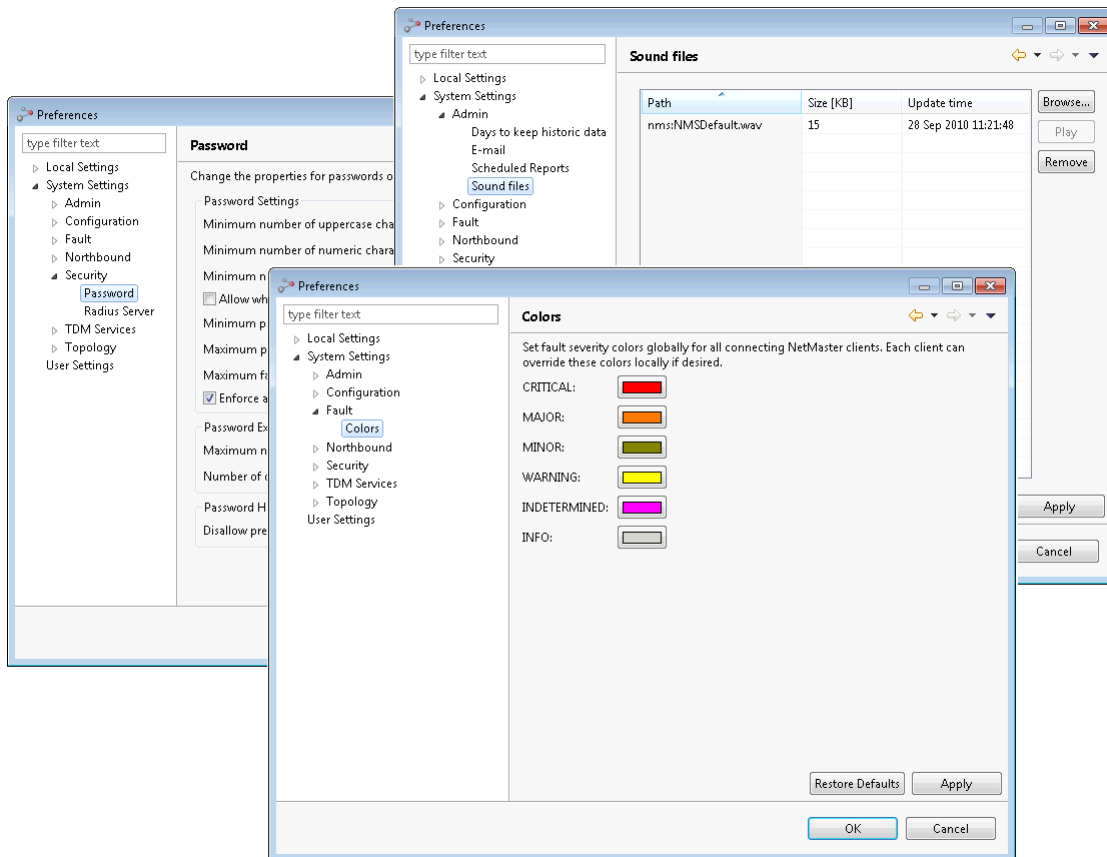
- Notifications 37** The **Notifications** area on the **statusbar** appears in red if there are un-viewed alarms in the [Alarm Notification Table view](#). The number of un-viewed alarms is also listed.
- Clicking this Alarm Notification button opens the [Alarm Notification Table view](#). The icon appears yellow if there are un-viewed alarms in the table.
- Clicking this icon opens the [Alarm Notifications view](#).
- User: johan** The **User** area on the **statusbar** displays the **User name** that is logged on.
- License: BS** The **License** area on the **statusbar** displays info about the current license on server.
- Connected: localhost** This **Connection Status** area on the **statusbar** will always tell you status of the connection to the server. See the chapter about [Server Connection](#) preferences for more details.

-  The **Progress** area on the **statusbar** displays if the server is busy with a background process. Double-click this area anytime to open the [Progress view](#).

Preference menus

The preference pages can be found under **Window > Preferences** in the [main menu](#). Here are a few examples:

Figure 7 PTP 820 NMS preference menus



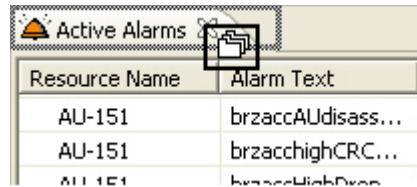
For more information about the settings in the preference menus, see the section about the different areas covered by preference menus in the user manual.

How to reposition views

Drag the [View tab](#) to reposition the view. Depending on how you drag the view, it will be positioned in different ways.

Stack

If you drag a view on top of another pane or into the middle of a view, the cursor will change to resemble a stack of folders (before dropping the view):



Resource Name	Alarm Text
AU-151	brzaccAUdisass...
AU-151	brzacchighCRC...
AU-151	brzacchighCRC...

When you place a view in a "stack" the view will appear "on top" of one or more views – all with the same size and coordinates.

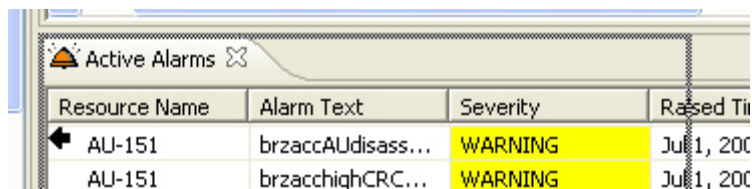
Several views in a stack are displayed like this:



Click a view name to bring this view to the front

Place left

If you drag a view to the left edge of another view, the cursor will look like this (before dropping):



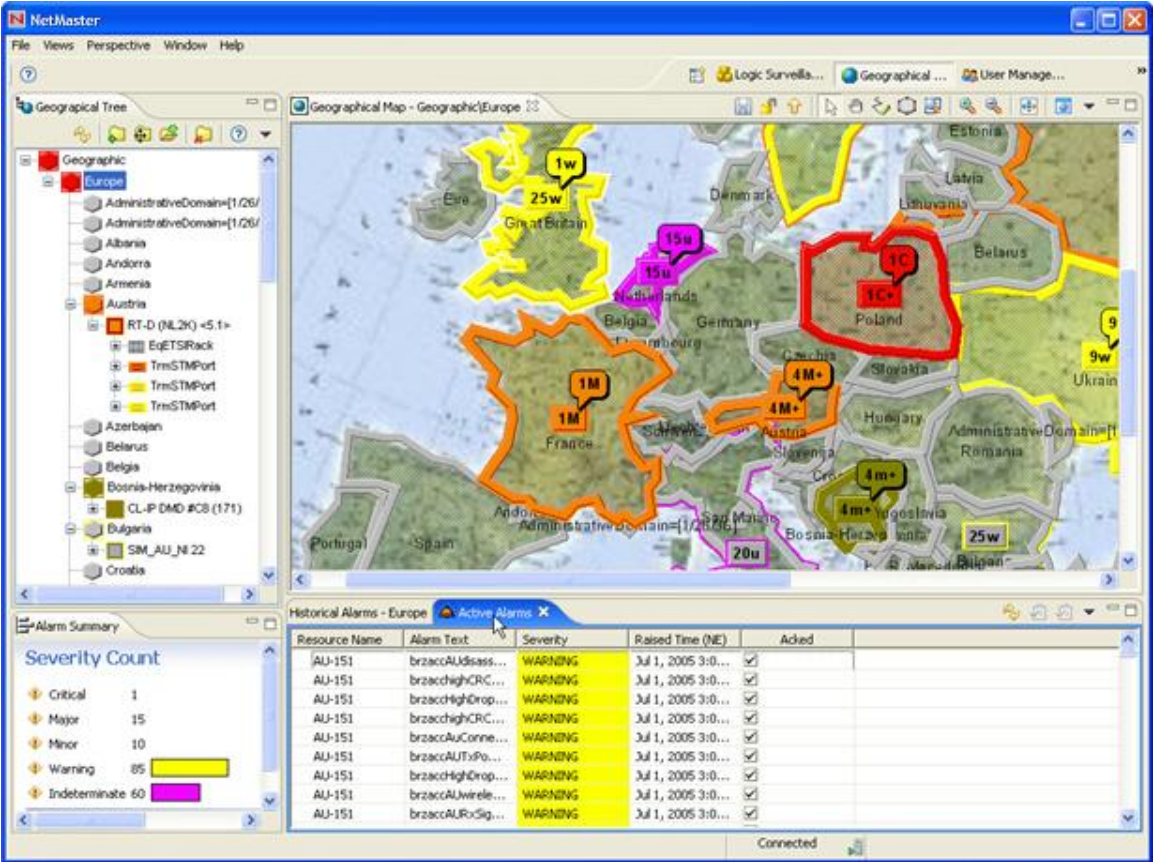
Resource Name	Alarm Text	Severity	Raised Time
AU-151	brzaccAUdisass...	WARNING	Jul 1, 200
AU-151	brzacchighCRC...	WARNING	Jul 1, 200

When you place a view to the left the space for two views will be split equally, with the moved view to the left.

Step by step example - drag left

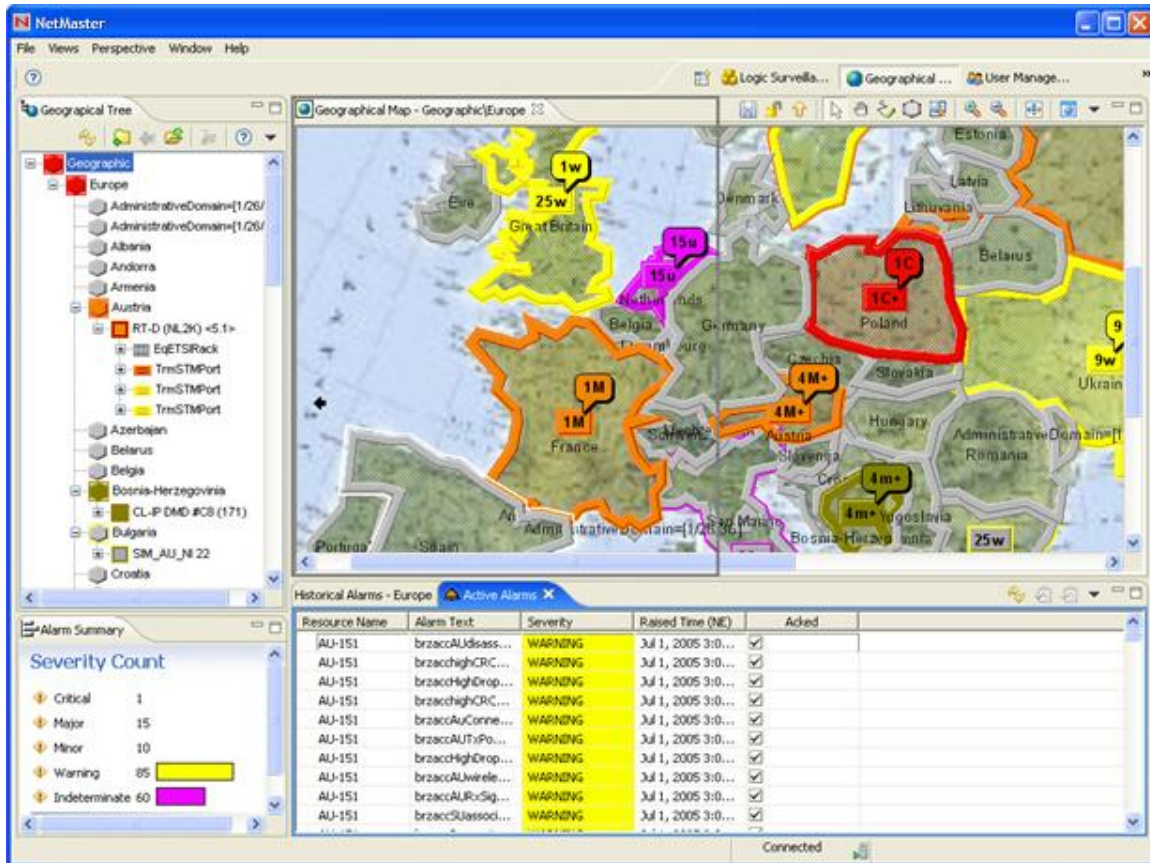
Here you can see an example of how to drag a view to the left of another. We now want to place the **Active Alarms** view to the left of the **Geographical Map** view.

1 Before we start dragging



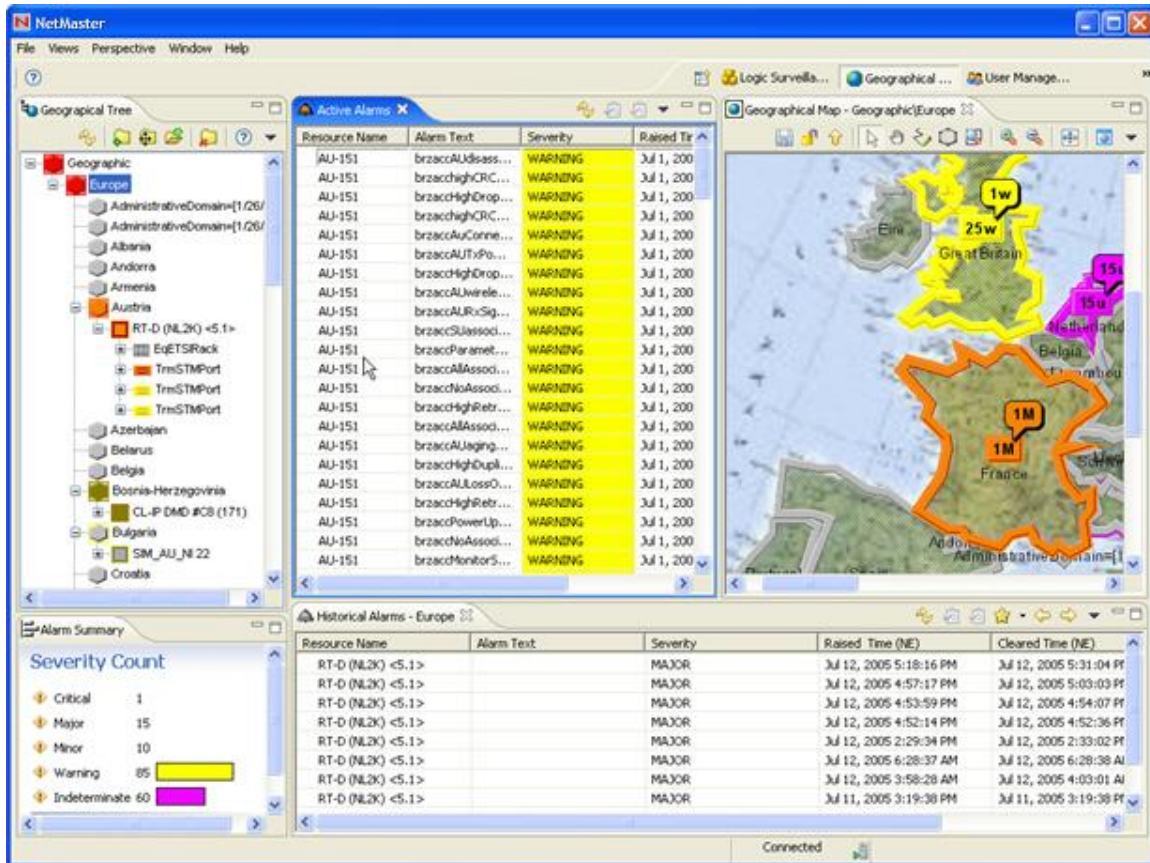
We start by moving the mouse cursor to the **Active Alarm** view's [tab](#).

2 While dragging



Then we drag the view tab to the left edge of the **Geographical Map** view. Please note how the cursor now changes to a left arrow, and how a grey frame indicates what the new position of the dragged view will be.

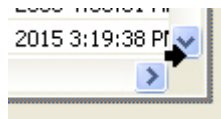
3 After positioning left



Then we drop the view at the left edge of the view. Please note the new position of the **Active Alarms** view and the new size of the **Geographical Map** view.

Place right

If you drag a view to the right edge of another view, the cursor will look like this:



The result is similar to [the step-by-step example](#) above (except that the view is now placed to the right of the other view).

Place top

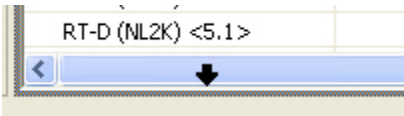
If you drag a view to the top edge of another view, the cursor will look like this:



The result is similar to [the step-by-step example](#) above (except that the view is now placed above the other view).

Place bottom

If you drag a view to the bottom edge of another view, the cursor will look like this:



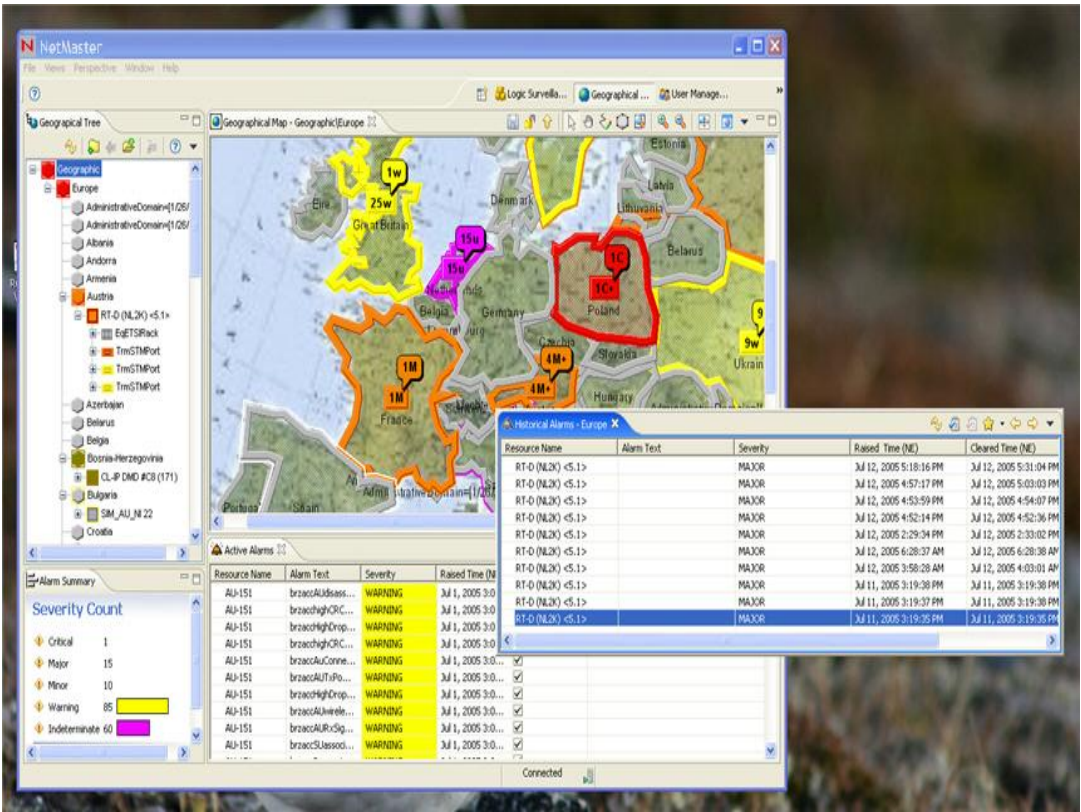
The result is similar to [the step-by-step example](#) above (except that the view is now placed below the other view).

Detach

When dragging a view outside the perspective (only possible when the PTP 820 NMS client is not maximized), the cursor will look like this:



The view then will become "detached" from the application, i.e. it will become a "floating" window on top of the application like this:



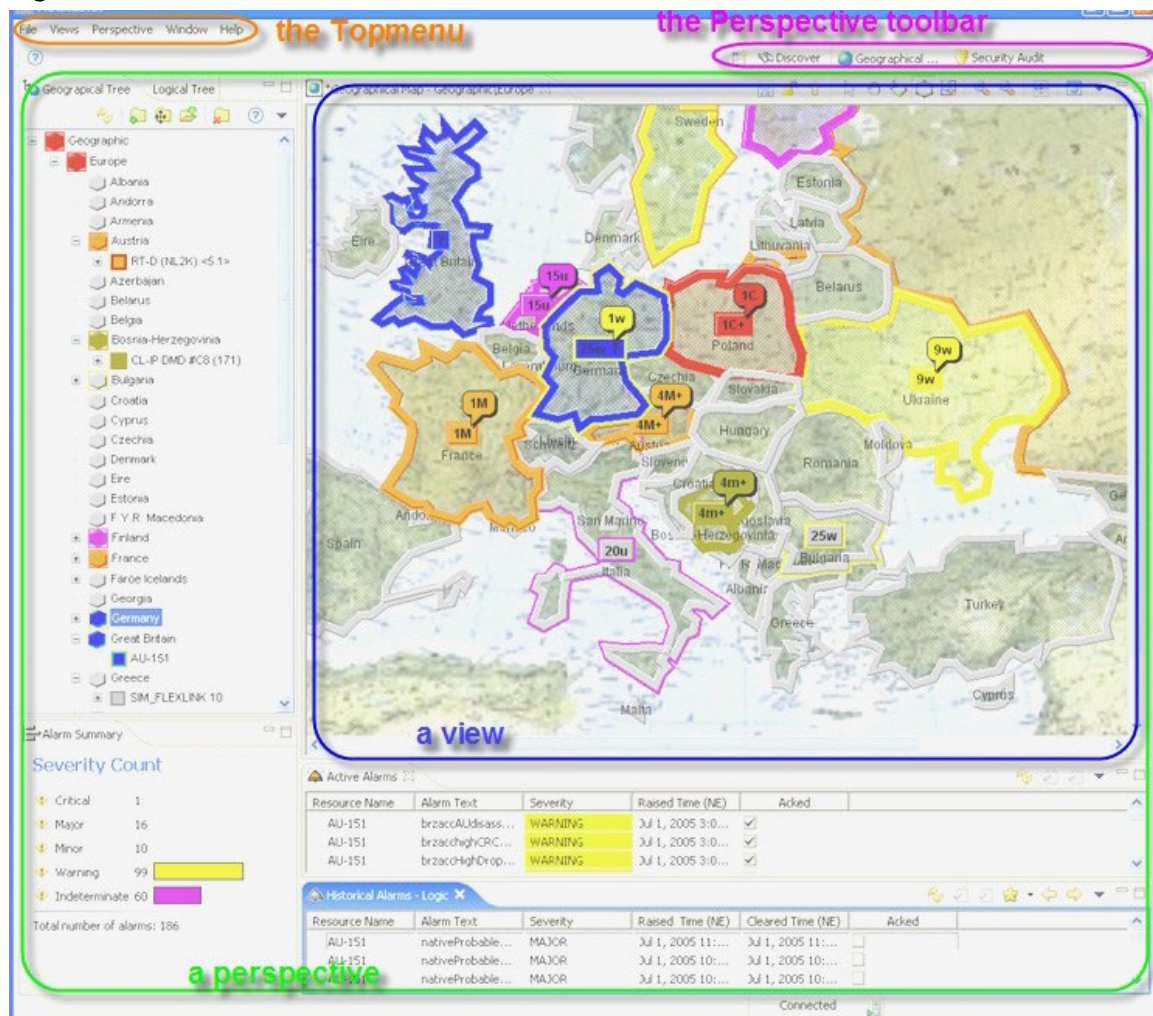
You can always move the view back to a position within the PTP 820 NMS perspective by dragging the view-pane somewhere inside the application.

The objects in a perspective

A perspective is a collection of views which reflects a certain working situation, e.g. surveillance of elements, discovery of new elements or managing users. When changing to another working situation, you can easily switch to another perspective that reflects this situation and then switch back to the previous perspective and continue your work there. The user can change or modify each perspective by opening and closing views, changing the coordinates and data scope for the views. The user can manage perspectives by creating, renaming, saving and deleting perspectives.

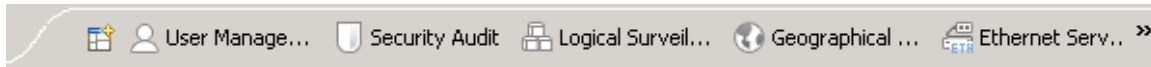
Please note the following areas, menus and toolbars which will always be present in PTP 820 NMS:

Figure 8 PTP 820 NMS view classifications







The Perspective toolbar

The Perspective toolbar is ([normally](#)) found on the upper right corner (marked with pink in the [figure](#) above), and may look like this:



This bar displays a list of all currently open perspectives and enhances the currently active perspective.

Available operations

-  Click the **Perspective Picker** icon to open a list of available perspectives, where you can pick the one you want to open. When selecting **Other...** you can select from all perspectives using the [Select Perspective](#) dialog.
-  Click one of the other perspective icons on the toolbar to switch to another open perspective. The icon in this example will open the **Discover** perspective.
-  Click the **More Perspectives** icon to pick another open perspective from a list. This icon will only be displayed when there is not sufficient space for all open perspectives on the **Perspective** toolbar.
-  Drag the left edge of the **Perspective** toolbar to resize it. Resizing is indicated by a "double arrow" cursor, as shown here.

The **Perspective** toolbar also has a [context menu](#) where you can:

- **dock...** : re-locate the perspective toolbar to different areas of the application. The icon bar can be docked top-left (default), top-right or to the left (vertical).
- **show text**: hide/unhide the name tags for the perspective icons on the toolbar.
- **close one** or **all** perspectives (this menu-option is only available when the context menu is opened on one of the perspective icons).

Perspective main menu

From the [main](#) menu (marked with orange in the [figure](#) above) under "Perspective", you can:

- **Reset** a perspective.
- create a new perspective by **saving** a perspective with a new name.
- **Save** the current perspective so that all views will appear in the current state next time you reset this perspective.
- **Reset** a perspective. All views will now appear the same as when the perspective was saved.
- **Close** the **current** perspective or **all** perspectives.
- **Customize** perspectives. Customization is carried out from the [Customize Perspective](#) dialog.
- **Delete** a perspective.

Please note that only user-defined perspectives can be overwritten or deleted. The predefined perspectives [Geographical Surveillance](#), [Logical Surveillance](#), [Discover](#), [User Management](#) and [Security Audit](#) are protected, and should be considered as templates for making user-defined perspectives.

Select Perspective dialog

This dialog appears when selecting **Other...** from the dropdown menu on the [Perspective Picker](#) icon or under **Perspective > Open Perspective > Other...** in the main menu.

Figure 9 Select dialog



Select one of the perspectives in the list and press the **OK** button to open it, or press the **Cancel** button to ignore.

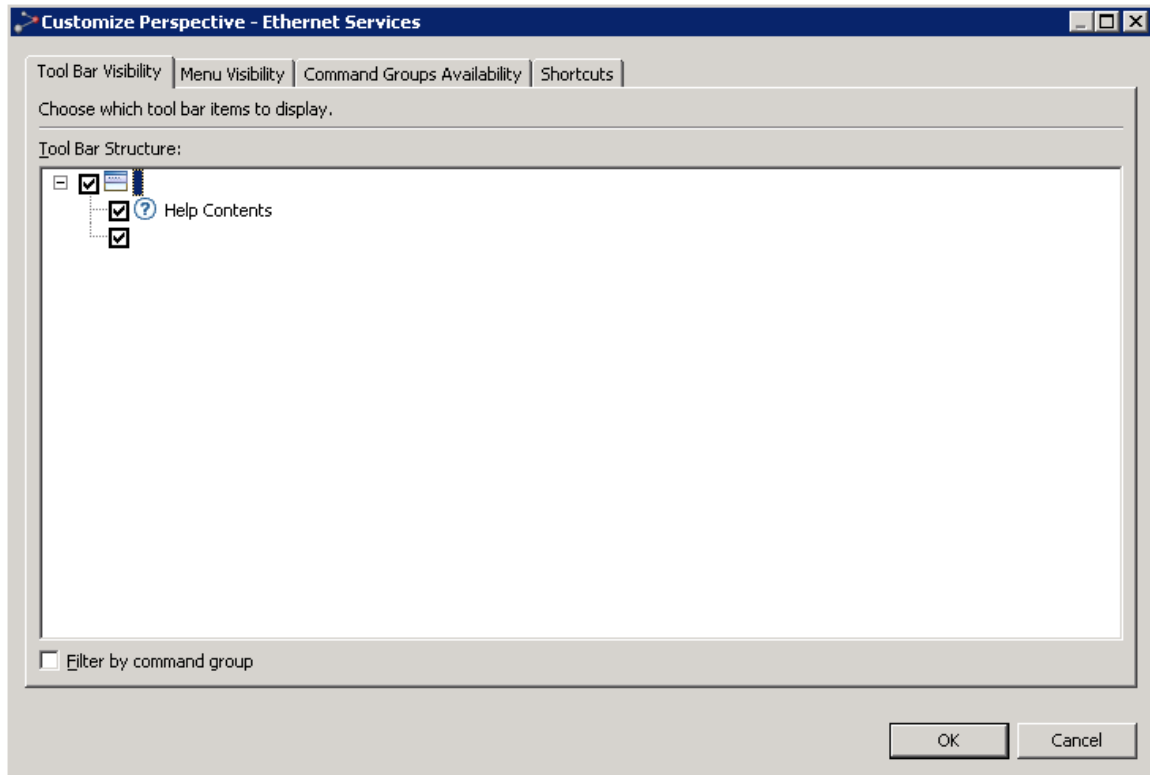
Customize Perspective dialog

The **Customize Perspective** dialog is opened by selecting Perspective > **Customize Perspective...** from the main menu and offers some customization of the currently active perspective.

The dialog has several different panes.

Customize Perspective dialog – Toolbar Visibility pane

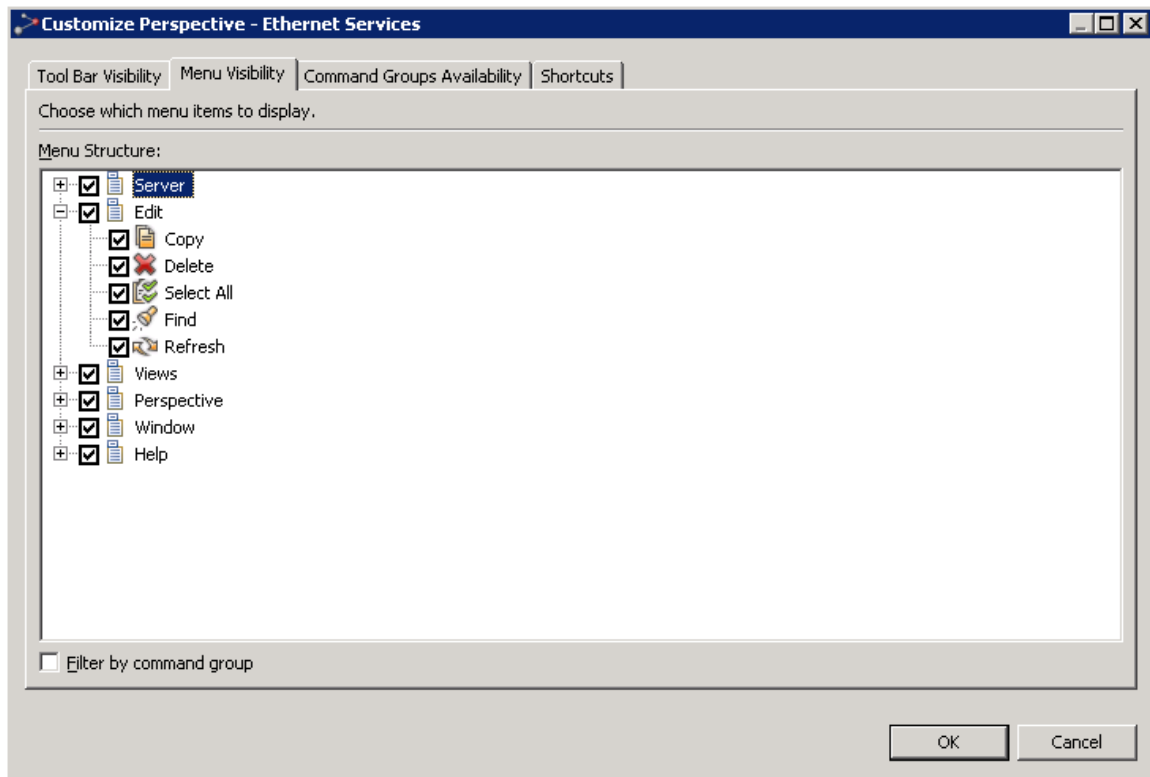
Figure 10 Customize perspective dialog – Toolbar Visibility pane



In this pane you can choose which toolbar items to display in the current perspective.

Customize Perspective dialog - Menu Visibility pane

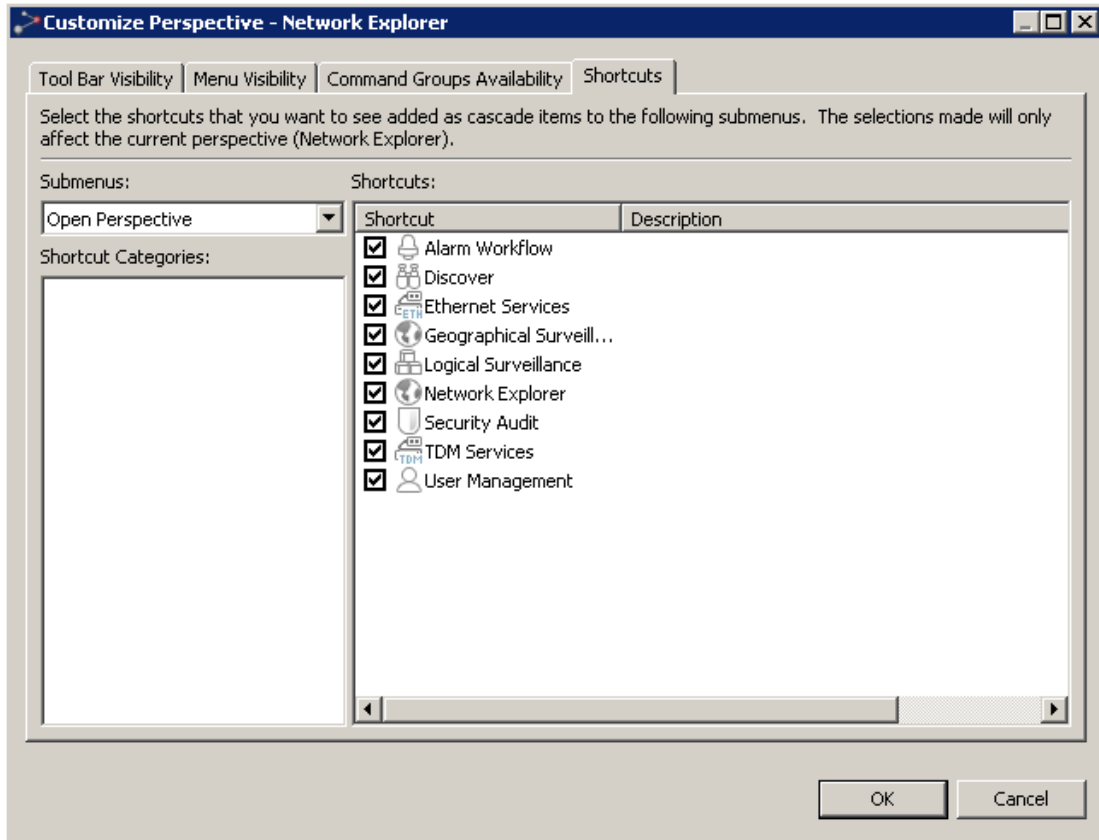
Figure 11 Customize perspective dialog - Menu Visibility pane



In this pane, you can select which menu items to display when opening the currently active perspective.

Customize Perspective dialog - Shortcuts pane

Figure 12: Customized Perspective-Network Explorer



In this pane you can select which shortcuts will be available from certain shortcuts.

Select **Open Perspective** in the **Submenus** dropdown to hide/display perspectives. This will influence the list of perspectives available in the following shortcuts:

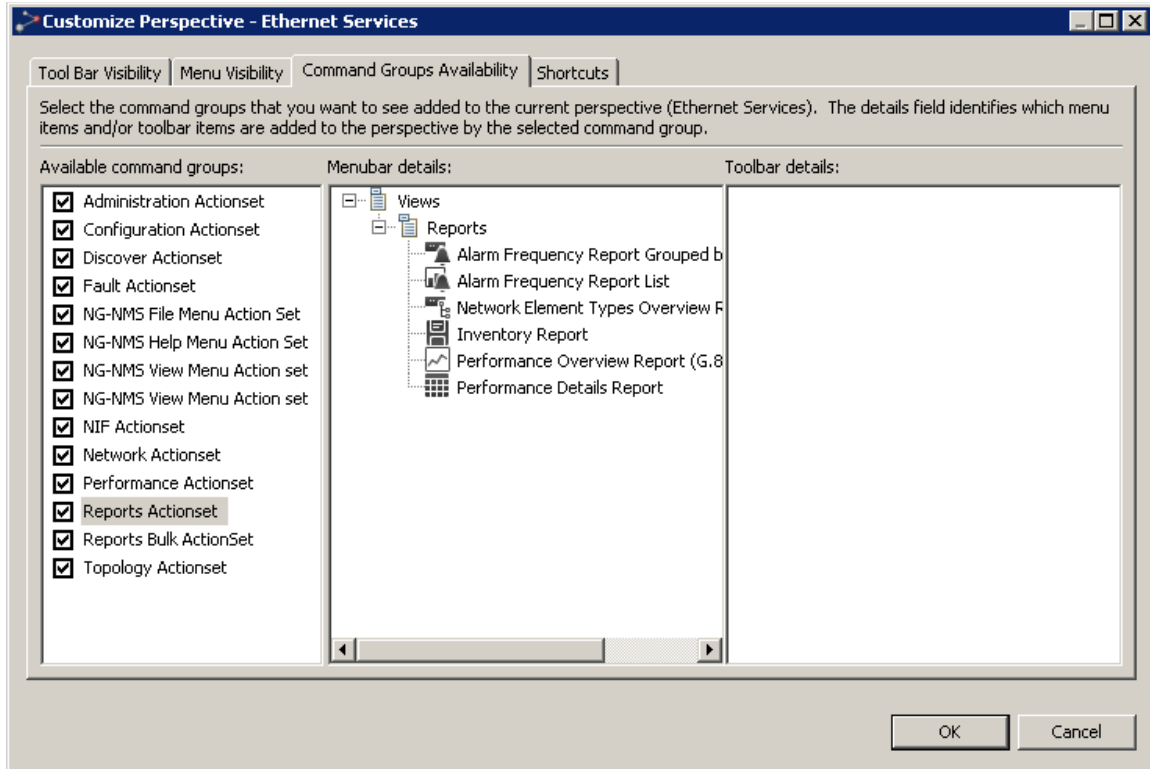
- in the main menu by selecting **Perspective >Open Perspective**, and
- when clicking the [Perspective Picker](#) icon on the **Perspective** toolbar.

Changes in this dialog will only be applied to the currently active perspective. This can be useful when you have designed your own set of preferred perspectives and your list of perspectives is growing.

All hidden perspectives will still be available in the **Select Perspective** dialog, which can be opened from the same menus.

Customize Perspective dialog - Command Groups Availability pane

Figure 12 Customize perspective dialog – commands pane



In this pane you can hide a set of views and dialogs from the **Views** submenu in the main menu. Changes made in this dialog will only be applied to the currently active perspective.

Please note that hiding views/dialogs in the **Customize Perspective** dialog does not affect how you open views from [context menus](#) or [dropdown menus](#) from within other views.

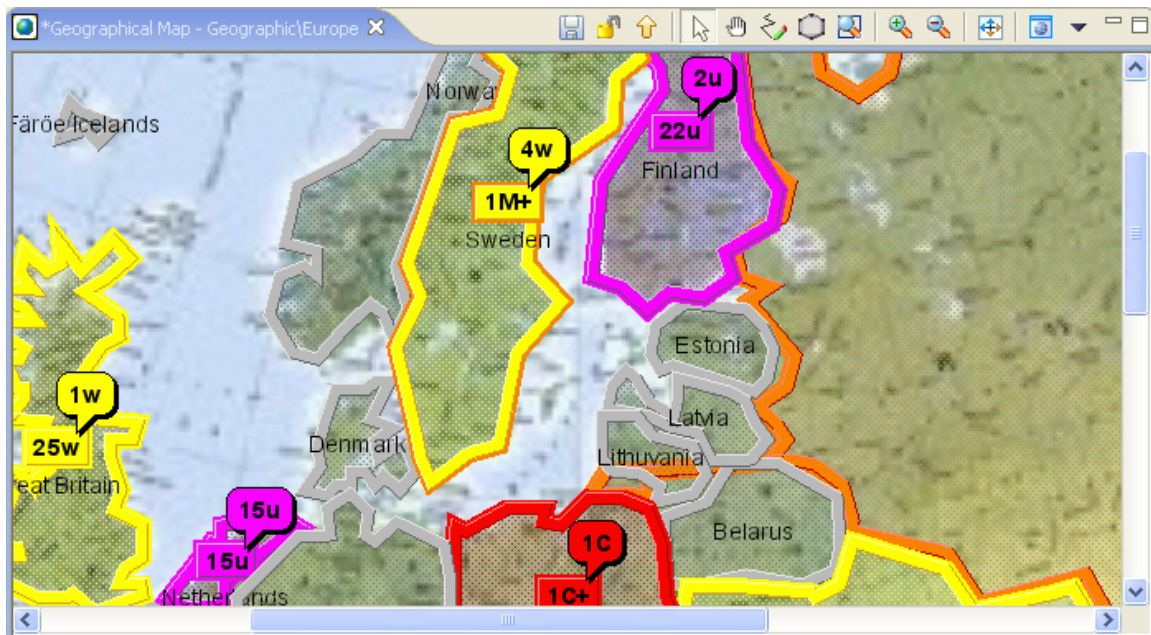
The objects in a view

You will find views whenever you start the application and open a (non-empty) [perspective](#). You can open more views by selecting **Views** from the [main menu](#), or by using [context-menus](#) or [dropdown](#) menus within the views that are already open.

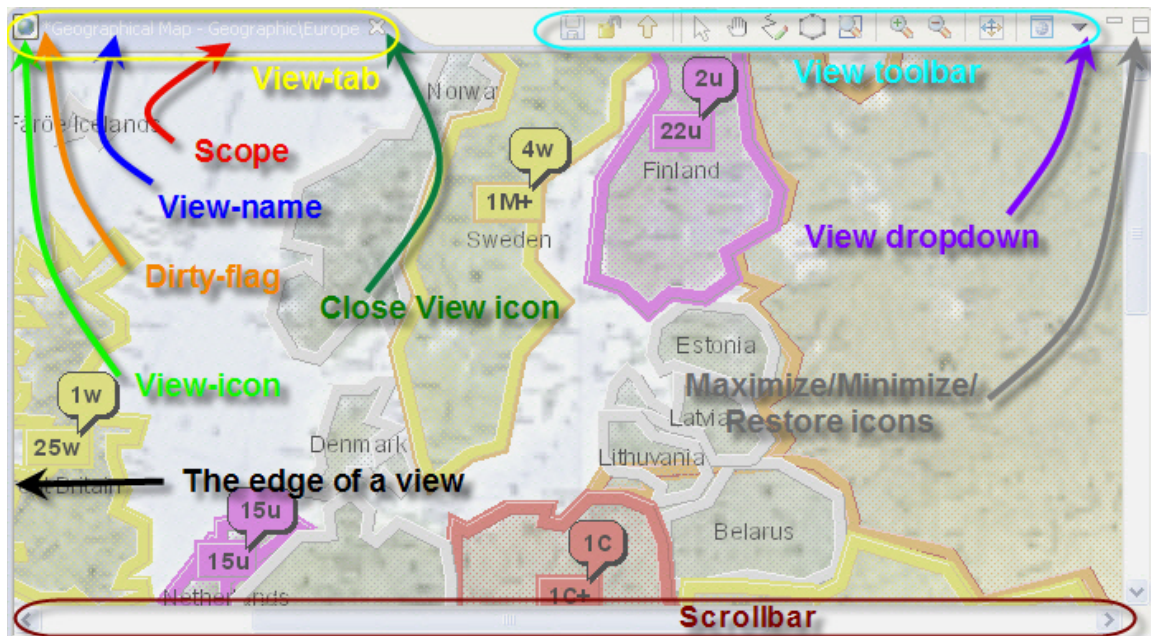
The objects in a view

This is a typical snapshot of a view in this case the **Geographical Map** view:

Figure 13 Typical snapshot of Geographical map



Some of the objects in this view are found in (almost) all views. Take a closer look at this example:

Figure 14 Geographical map close view

The Data area


In the background of the above example, you can see a map of Europe with several alarm indicators. This area contains the main functionality of the view - where the data is presented and/or utilized. Every view will contain one or more areas like this. The data area can contain a graphical map, a table, a graph or a set of controllers. Each view and its different data areas and controllers are described in the GUI overview section of this manual.


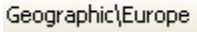

The View tab

View tab is found on the upper left edge of any view (marked with yellow in the above [example](#)).



The tab consists of the following objects:

-  A **View** icon, which is located on the left of the View tab. (marked with bright green in the above [example](#)). This icon helps you uniquely identify each view by view type, and the same icon can be found in all menus where you can open this view.
- * A **Dirty** flag, which appears only when there is unsaved data in the view (marked with orange in the above [example](#)). This little asterisk to the left of the view name indicates that your changes to the view have not yet been applied, and that the Save icon on the [View](#) toolbar can be used. If you try to close a view with dirty flag without saving data, the [Save Changes](#) dialog will be opened. You will only find a Dirty flag in views where data is modified in a Data area on the client and is saved to the server in a separate operation.


-  A **View name** (marked with blue in the above [example](#)). As with the View icon, it uniquely identifies each view by view type. The same name is used in all menus where this view can be opened.
-  A **Scope**, which can be found only when the view is opened with a particular selection of data (the scope **Geographic\Europe** is marked with red in the above [example](#)). The **Scope** is text that follows the **View name** and describes the data selected in the **Data** area. If the **Scope** is changed while a view is open, this text will be updated dynamically.
-  A **Close View** icon (marked with dark green in the above [example](#)). If the view contains any unsaved data (indicated by the [Dirty](#) flag), the [Save Changes](#) dialog will let you decide whether to save changes or not.

Available operations on the View tab

- Click the tab and drag the view to reposition it. This can be done several ways, read [How to reposition views](#) to find out more about repositioning views.
- Use the [Close View](#) icon to close the view
- Use the Viewtab's own [context menu](#). This menu contains shortcuts for **Close**, **Maximize/Minimize/Restore**, and several variants of **Resize** and **Move** a view.




Edge of a view

The **edge** indicates where a view ends and another starts (marked with a black arrow in the above [example](#)).

-  Drag the **View edge** to resize the view. When you move the cursor over this edge, it will change shape to a "double arrow", indicating that resizing is possible.

The Scrollbar

A **scrollbar** will appear whenever a view has more data than there is space for within the size of a view (marked with brown in the above [example](#))

-  Click the arrows to scroll the view in the desired direction
-  Click outside the scrollbar to scroll one page
-  Drag the scrollbar to quickly scroll the view in either direction

The View toolbar

The **View** toolbar is a list of icons found in the upper right corner of all views (marked with bright blue in the above [example](#)).

This toolbar will look different for each view. Below is another example of the **View** toolbar for the **Group Administration** view:




Each icon on the toolbar represent an operation on the data in the view, which can be activated by clicking the icon. Only the most common operations for the view, and operations on the view's main data, are normally found on the **View** toolbar. Other operations for the view can be found in a [view dropdown](#), in a [context menu](#) or as controllers in the view's [Data area](#).

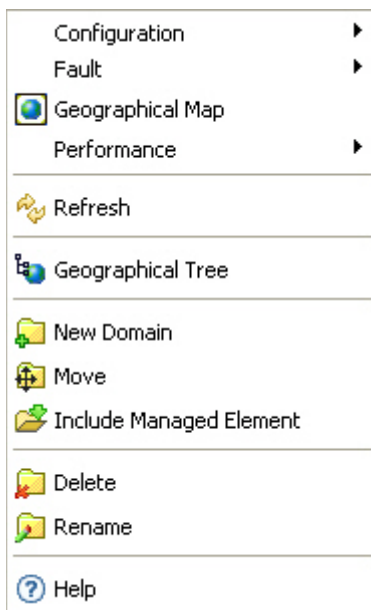
Some operations are used in several views (e.g. Refresh and Save), while others are not. For more details about operations available from the **View** toolbar, see the section on that view in the user manual.

The View dropdown

Every view has its own dropdown menu to the right of the toolbar (marked with purple in the above [example](#)). All operations available for that views' main data can be found here. Please note that some views have several levels of datasets and several sets of controllers (e.g. Alarm Templates view). Only operations on the views' main data are normally found on the **View** dropdown.


-  Click the View Dropdown icon to open a dropdown menu for a view

The View dropdown menu will look different for each view. This is an example for the Geographical Map view:



Selecting an item on the menu will in some cases apply changes to the (selected) data in the view, and in other cases open a view or a dialog. Depending on the state of the currently selected data, some menu options will become disabled/enabled (e.g. you cannot block a user who has already been blocked)




Some menu items are common for several views:

-  Select a menu with a **More Submenus** menu indicator to see more submenu items within this category. A menu item containing this icon does not activate an operation but can be considered as a header for a new sub-menu.

For more details about operations available from the [View](#) dropdown, see the section on that view in the user manual.

Maximize/Minimize/Restore icons

All views can have three different states, all of which can be enabled using the following icons (marked with grey in the above [example](#)) to the right of the View toolbar:

-  **Maximize** the view - the view is placed on top of all the other views. This is useful when you want to study a large amount of data in the view.
-  **Minimize** the view - the view becomes hidden at the bottom/top of the perspective. This is useful when you have a lot of views open.
-  **Restore** the view - the view returns to its previous state. This is the normal placement during surveillance.

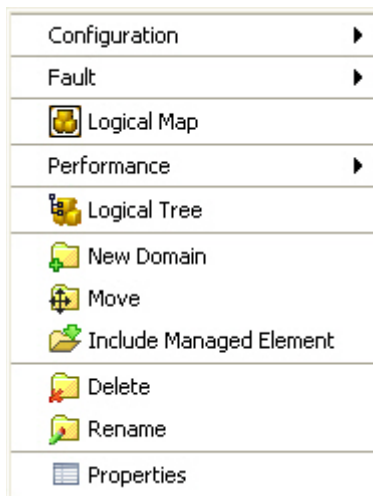
Another way to restore a minimized view, is to click its view tab.

Please note that when several views are [stacked](#), minimizing one view will also minimize the other views in this stack.


The Context menu

In most places in the application, it is possible to right-click (or left-click, if you are using a left-handed mouse) and open a special menu. This menu is called a context menu and is required in order to access a lot of functionality provided in the application.

The context menu will look different for each view. Below is an example from the Logical Map view:



The **context menu** and its available menu options will vary for each view, each area within a view, and each object in a area. Selecting a menu item will in some cases open a view or a dialog, in other cases apply changes to the selected data in the view. Some menu options will be disabled/enabled depending of the currently selected data in the view.

-  Select a menu with a **More Sub-menus** menu indicator to see more submenu items within this category. A menu item containing this icon does not activate an operation, but can be considered as a header for a new sub-menu.

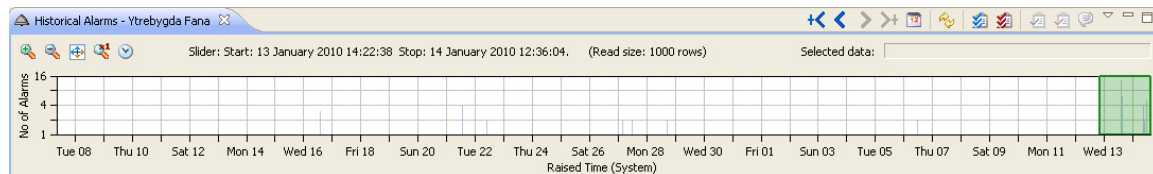
For more details about operations available from the [Context menu](#), see the section of the user manual describing all objects in each view.

Timeslider tool

The **Timeslider** tool is available in the [Historical Alarms view](#) and the [Historical Performance view](#), and can be enabled by selecting [Show Timeslider](#) on the [View dropdown](#).

The Timeslider is a tool that makes it easier to navigate the contents of a view with large amounts of data in a table (or a graph). Whenever the Timeslider tool is enabled, it is possible to navigate the [Slider](#) to filter the content in the main view.

Figure 15 Timeslider tool

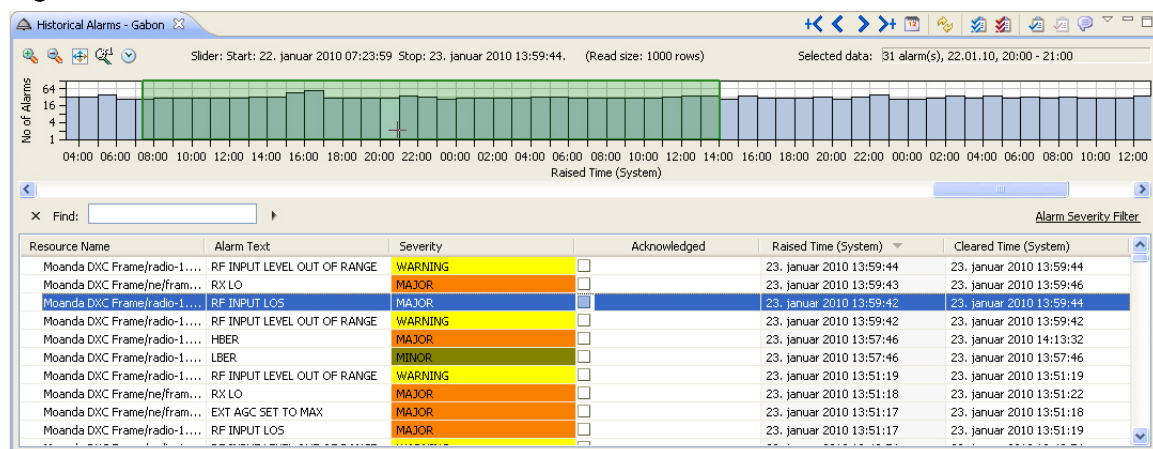


The contents of the table in the main view changes dynamically while the Slider is navigated in the [Timeslider bar](#) (assumed there are any changes in the result set). When navigation has been done with the Slider, the content of the table in the main view is updated, so that only entries satisfying the navigation are shown in the table.

Due to the possibility of vast amount of data in the database, the Timeslider tool will not be fully populated. The initial setup will show the Slider on top of the data bars for the newest data available. The data amount shown is one [read size](#). When navigating the Slider, the Timeslider bar graph will be dynamically populated with data corresponding to the read size.

Example: Historical Alarms view, with Timeslider tool enabled:

Figure 16 Historical alarms view with Timerslider tool

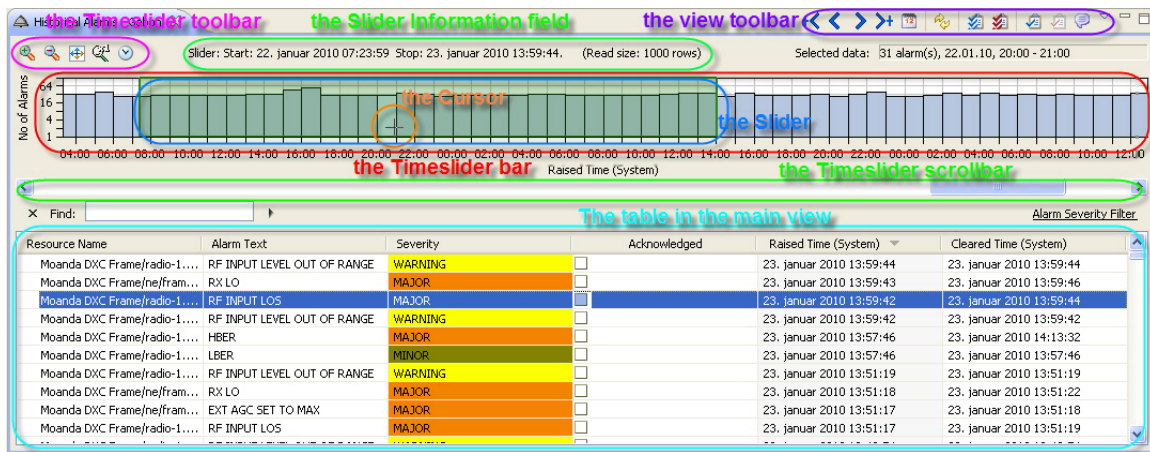


This example shows 1000 alarms displayed in the [Historical Alarms table](#), distributed from 22. januar 2010 07:23:59 to 23. januar 2010 13:59:44.

Each column in **Timeslider bar** graph represents the amount of alarms within an hour. This example shows that cursor has currently selected the interval 20:00-21:00, with 31 alarms.

The objects in a view with Timeslider tool

Figure 17 Timerslider tool view objects



Slider Information field

Slider: Start: November 26, 2015 12:50:12 PM Stop: November 30, 2015 7:48:17 AM.

The exact start and stop position of the **Slider** is given in the **Slider Information** text field above the **Timeslider bar**.

Read size

The **Slider Information** field also shows the current read size. The read size for the Historical Performance view is 24h. The default read size for the Historical Alarms view is 1000 alarms and can be modified in the Historical Alarms preference menu.

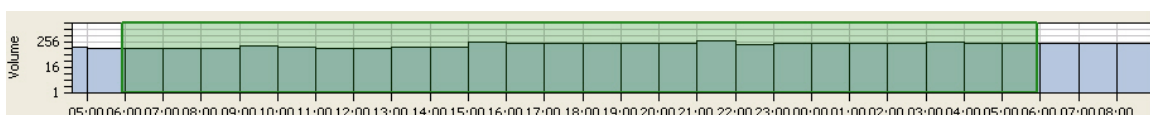
Selected Data information field

Selected data: 8 alarm(s), 11/21/15, 7:00

The amount of data in the interval currently selected by the cursor in the **Timeslider bar**, is given in the text field to the right of the [Slider Information field](#).

Whenever moving the cursor to another interval in the **Timeslider bar**, the amount of data in this interval will be displayed. When cursor is moved away from an interval in the Timeslider bar area, the Selected Data information field becomes empty.

Timeslider bar






The **Timeslider bar** provides a visualization of the amount of data that is available and currently presented in the table. The bar can be clicked and used for navigation of data in the table.

The area contains a column graph with time interval along the x-axis, and amount of data in the PTP 820 NMS database along the y-axis. The y-axis uses an exponential scale, so that both small and big values can be presented in the same graph.

Slider

The green frame in the **Timeslider bar** indicates the **Slider** area, which corresponds to the data currently in the table in the main view.






can be done by clicking with the mouse in the **Slider**. The different operations are indicated by the cursor:

-  Click in the middle of the **Slider** and drag the **Slider** to a new position where you want to analyze the available data. The **Slider** read size settles the amount of data that is read from the start position of the slider.
-  Click on the left border of the **Slider** and drag further to the left, to increase the area by the amount of one read size. The exact position of the left border will be determined by the oldest data in the read.
-  Click on the right border of the **Slider** and drag further to the right, to increase the area by the amount of one read size. The exact position of the right border will be determined by the oldest data in the read.









For more details about how to use the **Slider**, see the [examples](#) at the end of this chapter.

Timeslider toolbar and available operations

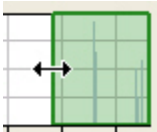
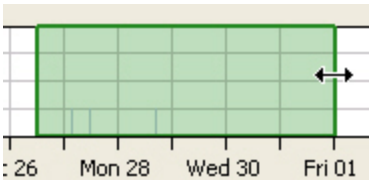
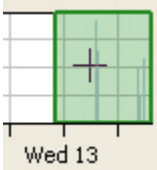

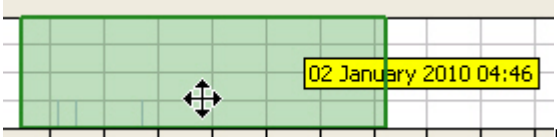
In the upper left corner of the Timeslider tool, there is a toolbar with a set of operations to the Timeslider tool. These operations may be used to navigate more accurately based on the timeline and read size.

-  - Reset the Timeslider to the basic zoom. This is calculated from the oldest alarm in the database up to present.
-  - Zoom in on the Timeslider bar
-  - Zoom out on the Timeslider bar
-  - Zoom to fit contents of slider
-  - Group bar in chart by minutes. Default is grouped by hours.

View toolbar and view dropdown and available operations

- In the views supporting the **Timeslider** tool, there are several operations on the [View toolbar](#) and [View dropdown](#) that will operate the **Timeslider** tool.
-  Extend previous read. This button extends the Slider to the left and adds a full read to the existing data already listed. If the read size was 10, then the table would contain 20 entries after the operation. Each consecutive action will add an extra data to the data table based on read size. Start position will be calculated based on oldest data read. The stop position is kept as before.
-  Get previous read. This button moves the Slider one read size to the left. The accurate start position is calculated based on the oldest data in the new data read from the database. The stop position is the previous start position.
-  Get next read. This button moves the Slider one read size to the right. The accurate stop position is calculated based on the newest data in the new data read from the database. The start position is the previous stop position.
-  Extend next read. This button extends the Slider to the right and adds a full read to the existing data already listed. If the read size was 10, then the table would contain 20 entries after the operation. Each consecutive action will add an extra data to the data table based on read size. Stop position will be calculated based on newest data read. The start position is kept as before.
-  Go to selected time and date. This button opens the [Date and Time dialog](#). The entry will be the new starting point for the **Slider**. Data will be read from this starting point up to read size. The new right border will be calculated based on the newest data in the read.
-  Refresh the view.
-  Show Timeslider - **Show/hide the Timeslider tool.**
-  Show Timeslider scrollbar Show/hide the **Timeslider scrollbar** at the bottom of the **Timeslider** tool. Whenever the Timeslider is [zoomed](#), the scrollbar can be used for navigating Timeslider bar along the time axis.

Examples of Slider operations

- 
 Double arrow cursor is active when you move over the **Slider** edge. Click and drag will move the edge of the slider. A pop-up will indicate the date/time alignment of the edge.
- 
 Double arrow cursor is active when you move over the **Slider** edge. Click and drag will move the edge of the **Slider**. A pop-up will indicate the date/time alignment of the edge.
- 
 Cross cursor indicates that you are inside the **Slider**. Single click will re-read data within the **Slider**. Click and drag will move the **Slider**.
- 
 Move slider right. The pop-up indicates the date and time alignment of the left edge of the slider.
- 
 Move slider left. The pop-up indicates the date and time alignment of the right edge of the **Slider**.

Date and Time dialog

This dialog appears whenever selecting [Go to selected time and date](#) on the View toolbar.

Figure 18 Data and Time dialog

Date and Time

Select the desired interval.

Select the start date and time of the interval

May 2016							June 2016						
Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat
24	25	26	27	28	29	30				1	2	3	4
1	2	3	4	5	6	7	5	6	7	8	9	10	11
8	9	10	11	12	13	14	12	13	14	15	16	17	18
15	16	17	18	19	20	21	19	20	21	22	23	24	25
22	23	24	25	26	27	28	26	27	28	29	30	1	2
29	30	31					3	4	5	6	7	8	9

2:21:21 PM

Select the end date and time of the interval

May 2016							June 2016						
Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat
24	25	26	27	28	29	30				1	2	3	4
1	2	3	4	5	6	7	5	6	7	8	9	10	11
8	9	10	11	12	13	14	12	13	14	15	16	17	18
15	16	17	18	19	20	21	19	20	21	22	23	24	25
22	23	24	25	26	27	28	26	27	28	29	30	1	2
29	30	31					3	4	5	6	7	8	9

2:21:21 PM

OK Cancel

Pick a start date and time and an end date and time and press **OK** to select a new time interval for the **Slider**.


Quick Search field

The **Quick Search** field makes it possible to search the contents of a table view.

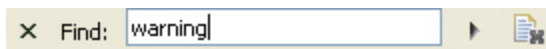
The **Quick Search** field is available in the following views:

- [Active Alarms](#) view
- [Historical Alarms](#) view
- [Current Performance](#) view
- [Historical Performance](#) view
- [Managed Elements](#) view
- [Unmanaged Elements](#) view
- [Software Inventory](#) view
- [Hardware Inventory](#) view
- [CPE Inventory](#) view
- [CPE Radio Statistics](#) view
- [Performance Collection Control](#) view

The **Quick Search** field can be enabled by selecting **Show Quick Search** on the [view dropdown](#) :

 Show Quick Search

Whenever the Quick Search field is enabled in a table view, it is possible to specify text string to search for within the table content.

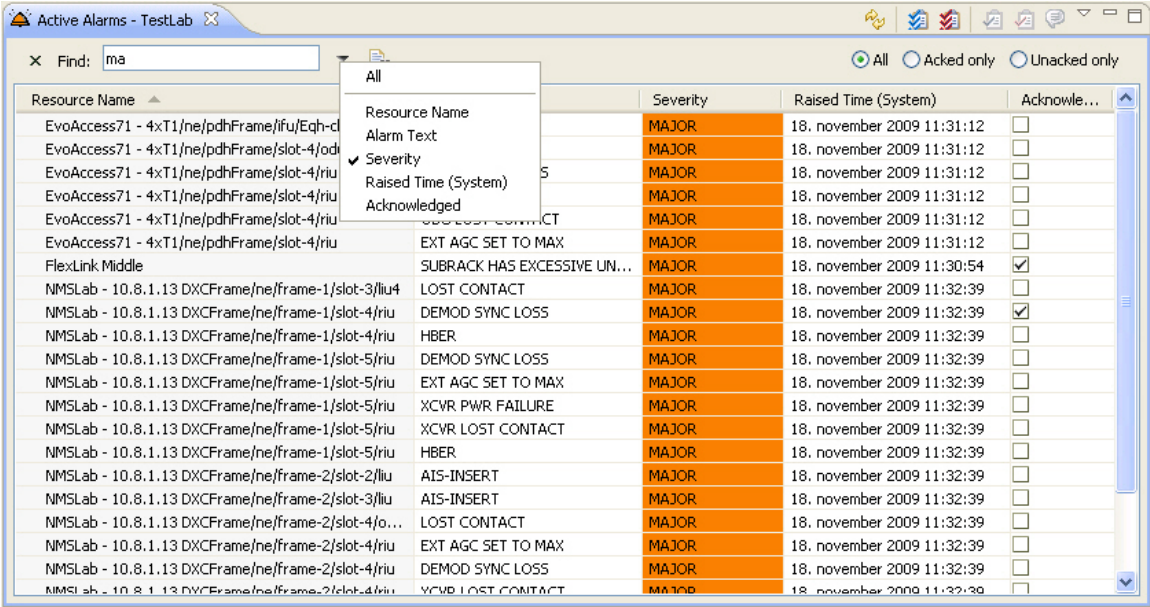


The contents of the view changes dynamically while the search string is typed in the [text field](#) (assumed there are any changes in the result set). No explicit search button must be pressed. Only entries satisfying the search string will be shown in the table.

Search Options

This example shows an **Active Alarms** view, with **Quick Search** field enabled:

Figure 19 Search options



Search scope

All visible columns in a table can be searched. To add/remove columns in the table, use the [Customize Columns](#) dialog.

The quick search functionality searches only among occurrences in the view, not among occurrences that are already hidden.

Example: if only **Acked only** is selected in an **Active Alarms view**, a specified text string in the **Quick Search field** will only search among the acknowledged alarms.

Column Selector attribute

It is possible to narrow the search scope by using the [Column Selector attribute](#), to specify columns to search among.

In the above [example](#), only the column **Severity** is used for searching in an **Active Alarms view**. The default attribute is **All**, which enables a search within all visible columns.

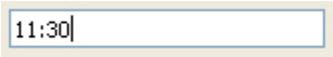



Valid search strings

All rows will be displayed if no quick search string is specified.

Some columns contain non-string values, like checkboxes.

- The string "Y" applies on selected checkboxes.
- The string "N" applies on unselected checkboxes.

Available operations

-  Type a search string in the **text field**.
-  Close the **Quick Search** field.
-  Open the **Column Selector** attribute.
-  Clear the content of the **text field**.

Visualization of alarms

An alarm is a fault indication sent from an NE in your network to the network manager. The purpose of alarms is to indicate to the operator that action might be needed, for example that equipment needs maintenance, the network needs to be set up differently or that users must be warned about low quality of the traffic in the network.

The alarm status of the different parts of your network is visualized in the topology views (**Geographical** or **Logical Map**, or **Tree**) using colors, alarm counts, codes and symbols.

Whenever an alarm is raised somewhere in the network, domains and NEs in the view will change color reflecting the updated alarm status of the most severe alarms – including both new alarms and all active alarms.

Alarm states

The life-cycle of an alarm in PTP 820 NMS can be described with the states as follows:








- **Active:** When a clearable alarm is raised for the NE, we call the alarm "active". These alarms can be found in the [Active Alarms](#) view and [Alarm Summary](#) view.
- **Acked:** When a clearable alarm is being followed up, the operator can acknowledge the alarm by setting it to "acked" and adding a comment to the alarm. Acked alarms are a subset of the alarms.
- **New:** A clearable alarm which is currently active and has not been acked is called a "new alarm". New alarms are also a subset of the active alarms.
- **Cleared:** When the fault condition disappears from the NE the alarm becomes "cleared" and the NE sends a "clear" signal to the network manager. As soon as the network manager receives information that an alarm has cleared, its alarm indicators in the topological view are removed. Please note that the "non-clearable" alarms (all alarms with the parameter Is Clearable = "N") also are considered as "cleared" in PTP 820 NMS, because they cannot be cleared at a later time. The cleared alarms can be found in the [Historical Alarms](#) view.


Only active alarms are visualized with colors in the topological views.

Alarm severities and node states

The alarm severities and node states are indicated as follows:

Table 1 Alarm severity and node states

Priority	Severity*	Severity Color*	Severity Code*	Description
1	Loss of Connectivity	 Blue	?	Indicates that no contact has been made with the network element. The communication settings should be checked in order to obtain contact with the element. We cannot determine the correct status of the alarms on the NE, as alarms are currently no longer being received.
2	Critical	 Red	C	The most severe alarm. It signifies that a condition affecting the service has occurred and immediate corrective action is required.
3	Major	 Orange	M	Indicates that a condition affecting the service has occurred and urgent corrective action is required.
4	Minor	 Olive green	m	Indicates the existence of a condition not affecting the service, but that requires corrective action in order to prevent a more serious fault.
5	Warning	 Yellow	w	Indicates the detection of a potential or impending fault that will affect the service, before any significant effects have been felt. Action should be taken to further diagnose and correct the problem in order to prevent it from becoming a more serious fault that will affect the service.
6	Indeterminate	 Pink	u	The network manager cannot determine the severity of an alarm.
7	Info	 Gray	i	A notice from the NE, which is not connected to any error-situation, e.g. a confirmation.

Priority	Severity*	Severity Color*	Severity Code*	Description
8	Normal	 Light green	(no text)	No alarms or warnings have been reported from the network element.

*Please note that "Severity", "Severity Color" and "Severity Code" are inaccurate terms for "Loss of Connectivity" and "Normal", because they do not have an alarm severity as they refer to "node states" determined by the PTP 820 NMS server and not alarms.

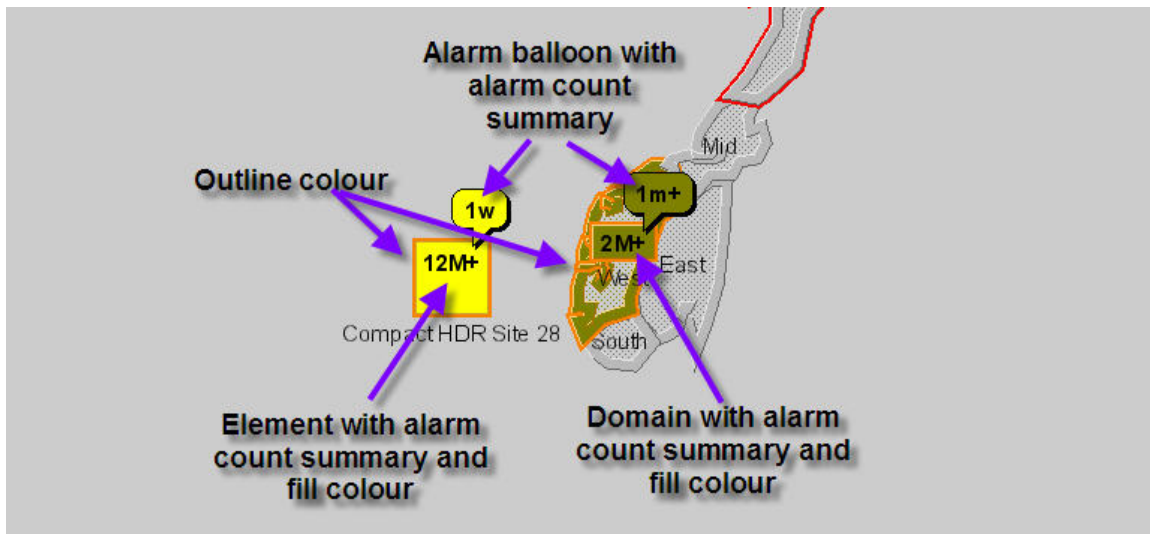
The severity of a node will always reflect the highest severity among its children. This means that if a domain contains two NEs containing different alarm severities, only the "highest" alarm severity will be displayed for the domain ("highest" as defined in the Priority column in the table above, including the node-states "Normal" and "Loss of Connectivity"). Similarly an NE will have the highest severity of all the equipment contained in the NE.

Please note that the severity colors presented in the above table can be changed from their default colors using the [Preferences](#) pages. This can be done both globally on the server using system fault settings, or on a client using local fault settings. In the Preferences pages you can also [prevent the Loss of Connectivity](#) state from being displayed anywhere other than the NE.

Alarm indicators in a topological map

If we take a closer look at a map view, we can see that NEs and domains contain several indicators which are used to visualize active alarms:

Figure 20 Alarm indicators in a topological map

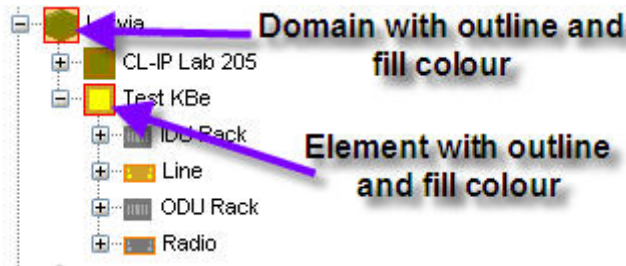


In the NE called "Compact HDR Site 28" in the above example, we can see that active alarms are indicated by the following properties on the NE: an orange outline, a element alarm count summary "12M+", a yellow fill color, a yellow alarm balloon and an alarm balloon count summary "1w".

On the domain called "West", we can see that active alarms are indicated by the following properties on the domain: an orange outline, a domain alarm count summary "2M+", a brown domain fill color, a brown alarm balloon and an alarm balloon count summary "1m+".

Alarm indicators in a topological tree

If we take a closer look at a tree view, we can see that active alarms are indicated for NEs and domains in the tree using similar objects with individual properties:



In the above example, in the domain called "Latvia" we can see that alarms are indicated by the following properties in the domain: a red outline and a brown fill color.

We can also see that the NE called "Test KBe" has the following alarm indicators in the tree: a red outline and a yellow fill color.

Under the node "Test KBe" we can also see several nodes representing the different items of equipment in the NE. Some are colorless, others have a colored outline, while others have both a fill color and an outline color.

Alarm information on topological objects

The colors and summary for these objects give you the following information:



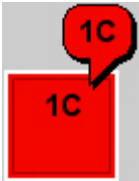

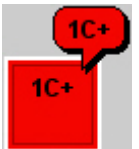

Table 2 Alarm information on topological objects





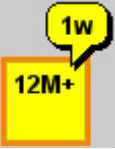

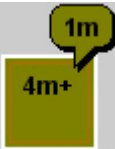

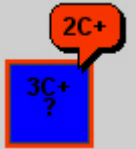



Object	Where	Information
Balloon alarm summary	NE and domains in map	A count and severity code for the most severe new alarm A plus sign indicates that there are also less severe new alarms.
Element/domain fill color	NE and domains in map and tree	The color of the most severe new alarm/state. This color will normally be the same as the severity color for the alarm balloon summary, but will turn blue when the node has the state "Loss of Connectivity". The fill color for the node in a tree is the same as the element/domain fill color of this object in a map.

Object	Where	Information
Alarm balloon color	NE and domains in map	The color of the most severe new alarm. This color will normally be the same as the element/domain fill color, but will remain this color if the node changes to "Loss of Connectivity" state.
Element/domain alarm summary	NE and domains in map	A count and severity code for the most severe active alarm. A plus sign indicates that there are also less severe active alarms.
Element/domain outline color	NE and domains in map and tree	The color of the most severe active alarm. This color will always be the same as the severity color for the element/domain alarm summary. The outline color for the node in a tree is the same as the outline color of this object in a map. As the outline color only differs from the fill color when the most severe active alarm is different from the most severe new alarm, a different outline color indicates the highest severity of the acked alarms.

Some examples of alarm states

Table 3 Some examples of alarm states

Alarm State Values	Map view	Tree view	Comment
Normal			The resource has no alarms.
New Critical			The resource has one new critical alarm
New Critical and Less Severe			The resource has one new critical alarm, plus other less severe new alarms

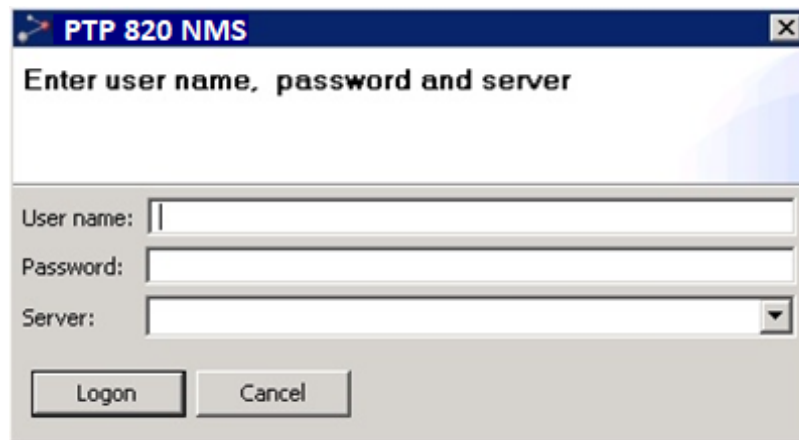
Alarm State Values	Map view	Tree view	Comment
Acked Major			The resource has one acknowledged major alarm
Acked Critical and Less Severe			The resource has one acknowledged critical alarm, plus other less severe acknowledged alarms
New Warning and Acked Major			The resource has one new Warning alarm, twelve acknowledged Major alarms plus other less severe active alarms (including the one new Warning).
New and Acked Minor			The resource has one new Minor alarm, plus three acknowledged Minor alarms (in total, four active Minor alarms).
Loss of Connectivity, new and acknowledged Critical			<p>The resource has Loss of Connectivity, has two new Critical alarm plus other less severe new alarms, has one acknowledged Critical alarm (in total, three active Critical alarms) plus other less severe active alarms (including the less severe new alarms).</p> <p>As alarms no longer are being received from the NE, alarm counts are not reliable.</p>
Muted element with Critical and Less Severe			The resource is currently muted , resulting that alarms from this element will currently not trigger Alarm Notifications . It has 6 new critical alarms, plus other less severe new alarms

General dialogs and views

PTP 820 NMS Login dialog

This dialog appears whenever starting PTP 820 NMS client application.

The dialog will also appear if the user logs off the client by selecting **File > Log Off** from the main menu, or when the connection between server and client is broken – e.g. when the [password is changed](#).



Type values for **User name** and **Password** in this fields. Use a user name as defined for this user in the [User Administration](#) view. Password can be updated both in the **User Administration** view and in the [User Settings](#) preference page.

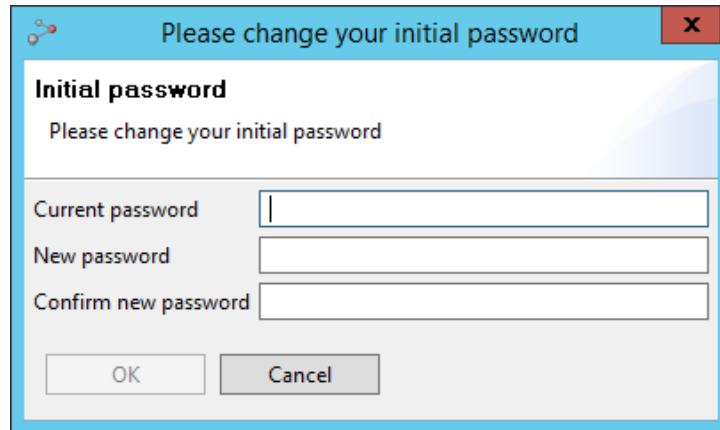
In the field **Server**, you can type

- Network name of a PTP 820 NMS server
- IP-address of a PTP 820 NMS server
- the value **localhost**, if the server is running on the same computer as the client. (leaving the field blank, has the same effect)
- alternatively you may also specify the port number on the server, by adding a colon (:) and the port number to the server. If not specifying a port number, the default port number (1098) will be used. (for example 10.100.3.54:1098 or PTP 820 NMS server:1098)

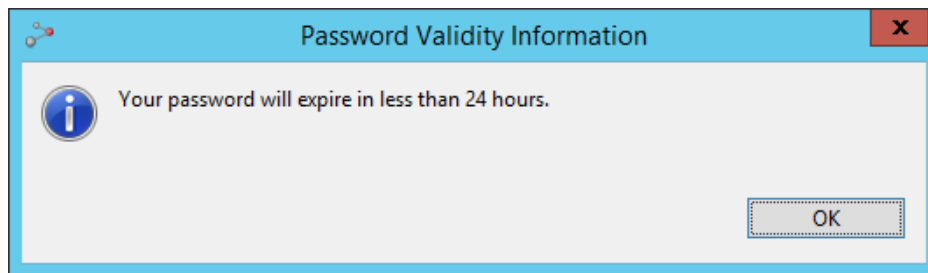
Alternatively use the dropdown in the **Server** field, to select from a list of the last 5 used server connection strings.

Click **Logon** when finished, or **Cancel** to abort.

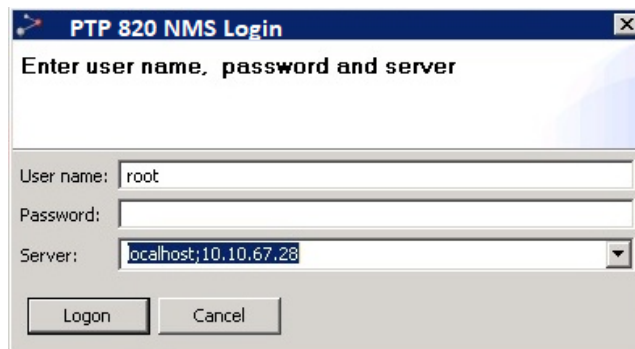
If **Enforce a password change upon first login** is selected in the **Error! Reference source not found.** page, then upon first login the following appears:



If your password is about to expire, then upon login a password expiration warning is displayed:



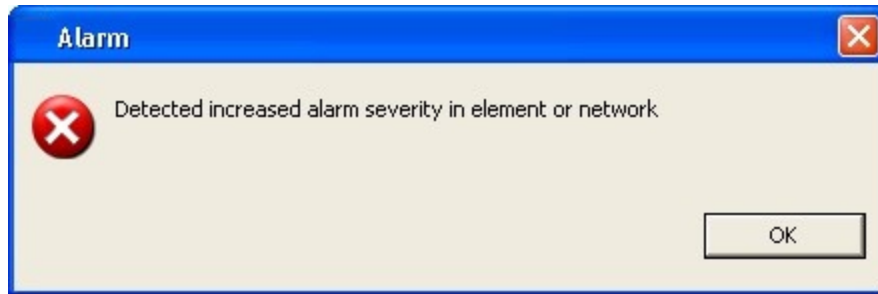
If High Availability is configured (refer to [Error! Reference source not found.](#)), you must specify in the *Server* field the addresses of both the Primary and the Secondary servers, separated by a semicolon, as shown in the following example.



If the Active and Standby servers are in the process of performing a switchover, a message appears with a request to click the **Reconnect** button.

Alarm dialog

This dialog appears whenever you receive an alarm which increase severity on a node-type with **Loop** enabled in the [Sounds](#) preferences page.



When this dialog appears PTP 820 NMS will generate a notification sound as defined in the **Sounds** preferences page. The sound notifications can be enabled

- On NE-level - generating sounds whenever receiving alarms that increase the severity on any managed NE node
- or on Network level - generating sounds whenever receiving alarms that increase the severity on top-level node of either [Geographical model](#) or [Logical model](#)

The **Alarm** dialog will appear on top of all other GUI in PTP 820 NMS - independent of what [dialog](#), [view](#) or [perspective](#) that currently is open in PTP 820 NMS.

Click the **OK** button to close dialog and stop the notification sound.

Customize Columns dialog

The purpose of the **Customize Columns** dialog is to select

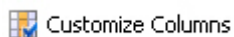
- visible columns
- column order

in the table in the view where you opened this dialog.

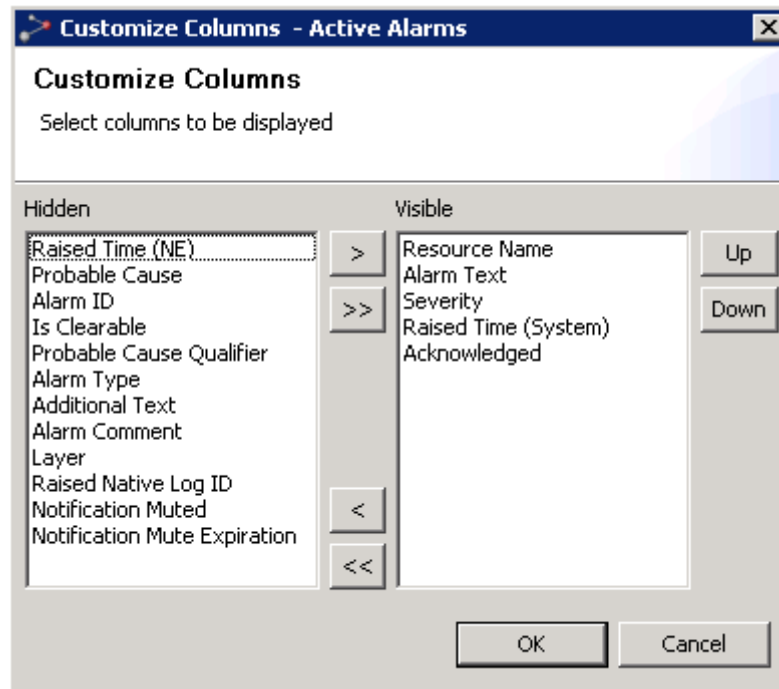
The dialog can be opened from the following views:

- [Active Alarms](#) view
- [Historical Alarms](#) view
- [Hardware Inventory](#) view
- [Software Inventory](#) view
- [Performance Collection Control](#) view
- [Historical Performance](#) view
- [Current Performance](#) view
- [Audit Log](#) view
- [Discover Settings](#) view
- [Unmanaged Elements](#) view
- [Managed Elements](#) view

The dialog can be enabled by selecting **Customize Columns** on the [view dropdown](#) :



A table similar to the following will be opened:



Please note that the content of the **Customize Columns** dialog will depend on which view you have opened this dialog from. The above example is a customization of the **Historical Alarms** table.







The Visible area

The **Visible** area contains a list of columns to be visible in the corresponding table. The item at the top of this list will be the leftmost column in the table and the item at the bottom of the list will be the rightmost column. You can select one or more items in this area to move up/down or left (to **Hidden**).

The Hidden area

The **Hidden** area contains a list of header names for all columns are to be invisible in the corresponding table. You can select one or more items in this area to move right (to **Visible**).

Available operations

-  Show the selected hidden columns
-  Show all hidden columns
-  Hide the selected column
-  Hide all columns
-  Move the selected visible column one place left in the table
-  Move the selected visible column one place right in the table

Pressing the **OK** button will close the dialog and apply all your changes to the corresponding table. Pressing the **Cancel** button will close the dialog without applying any changes.

Save Changes dialog

This dialog is opened whenever you try to close a view which contains unsaved data. This can happen in any view where you are required to save data to the server, and the title of the dialog will depend on the name of the view that caused the dialog to open.

This example displays the **Save Changes** dialog for the **Alarm Templates** view:



Click the **Yes** button to save the changes and close the view. Click the **No** button to close the view without saving changes.

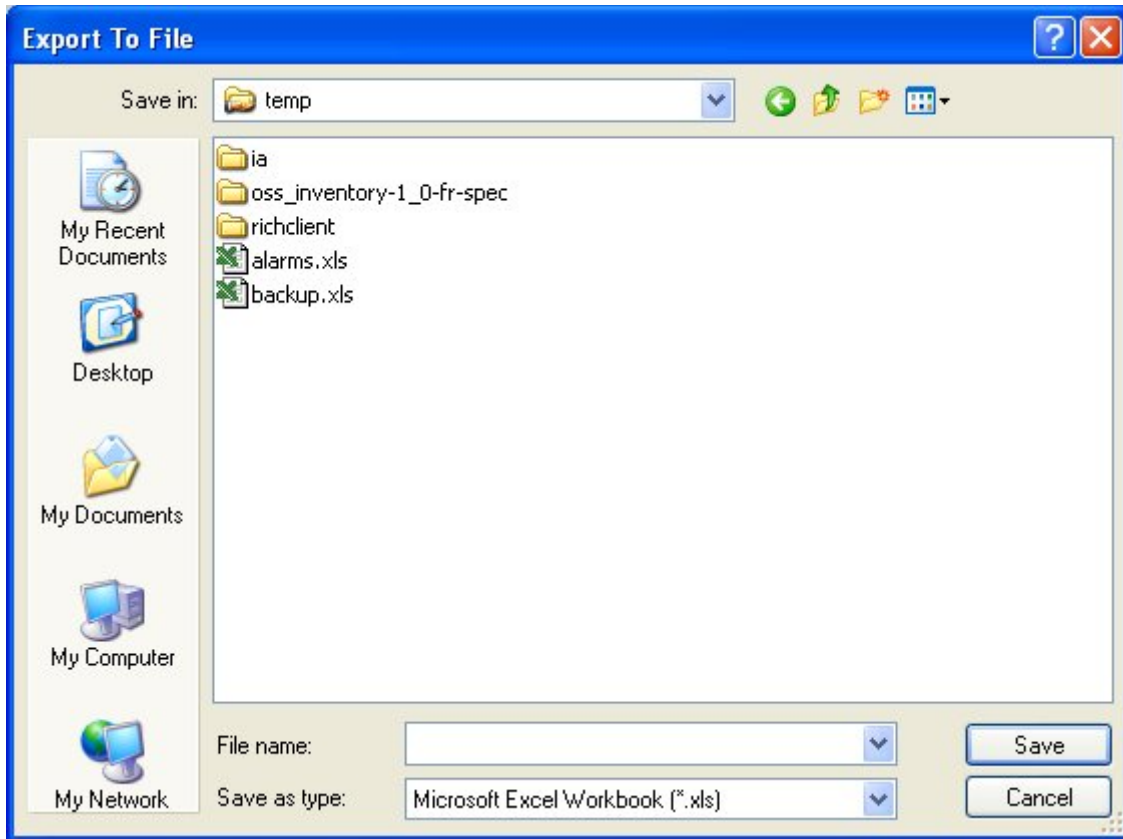
Export To File dialog

This dialog can be opened from all views presenting data in a tabular fashion, i.e. [Active Alarms](#) view, [Hardware Inventory](#) view, [Software Inventory](#) view, etc.



Export to File...

Click this icon in the dropdown menu of one of the tabular views if you want to export the content of the table to disk. A dialog similar to this will be opened (on Microsoft Windows):



The purpose of this dialog is to export the content of the view's table to file for further processing or printing. The dialog box lets the user specify the drive, directory, and name of a file to save.

File types supported are Microsoft Excel Workbook (xls), Comma Delimited (csv), and eXtensible Markup Language (xml).

Content of exported file

Rows

Depending on the view, rows in the table might be filtered using the [Quick Search](#) field, the [Timeslider](#) tool, the current [filter](#) or the current [scope](#) of the view. For all views, all the visible rows in the tabular view will be exported (E.g. If there are 30000 rows in the view the result file will contain 30000 rows). Please note that when exporting to Microsoft Excel format file, the max number of rows is 65533.

The ordering of the rows will be the same as the original view.

Columns

Only the visible columns will be exported. Columns can be set to hidden/visible using the **Customize Columns** dialog.

Format of values

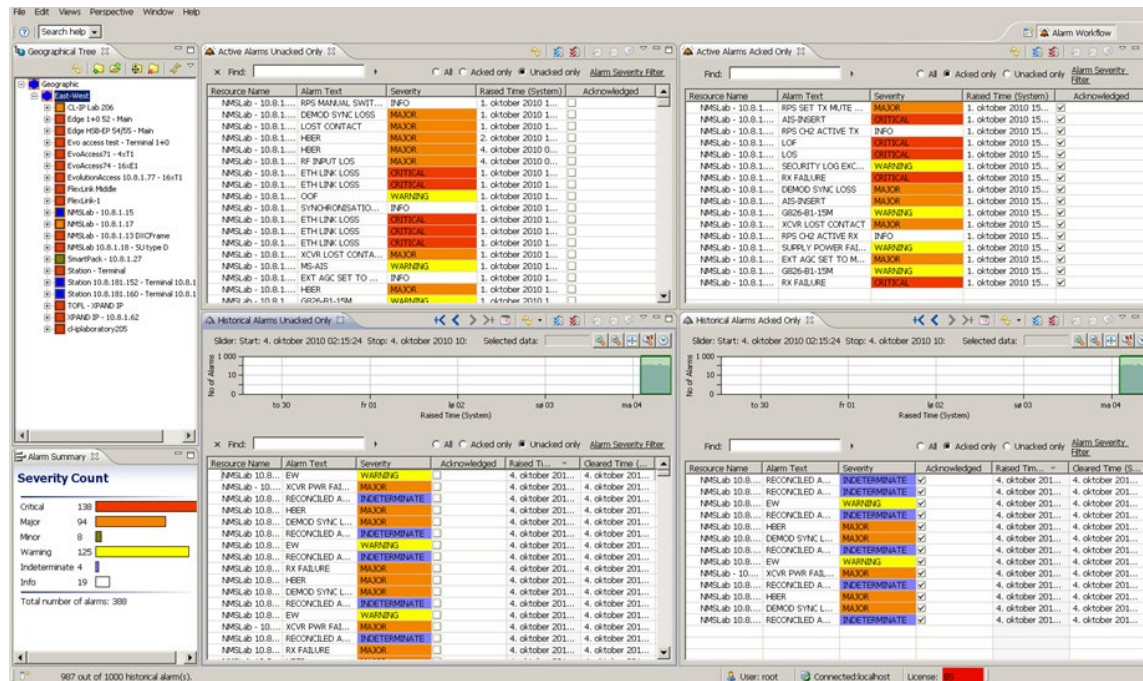
The format of the values in the result file will be the same as in the view (e.g. regional options for time and numbers).

Chapter 4: Predefined perspectives

Alarm Workflow perspective

This is a perspective for surveillance of NEs in the system.

Figure 21 Alarm workflow perspective



The perspective consists of the following views:

- The [Geographical Tree view](#) provides a hierarchical overview based on geography of the elements and equipment.
- The [Alarm Summary view](#) provides summaries of all alarms within different severities for your entire network.
- Details of each [active](#) alarm can be found in the [Active Alarms views](#):
 - Active Alarms Unacked Only: Lists all active alarms that are [unacked](#) in the system
 - Active Alarm Acked Only: Lists all active alarms that are [acked](#) in the system.
- Details of each [historical](#) alarm can be found in the [Historical Alarms views](#):
 - Historical Alarms Unacked Only: Lists all historical alarms that are unacked in the system.
 - Historical Alarms Acked Only: Lists all historical alarms that are acked in the system.

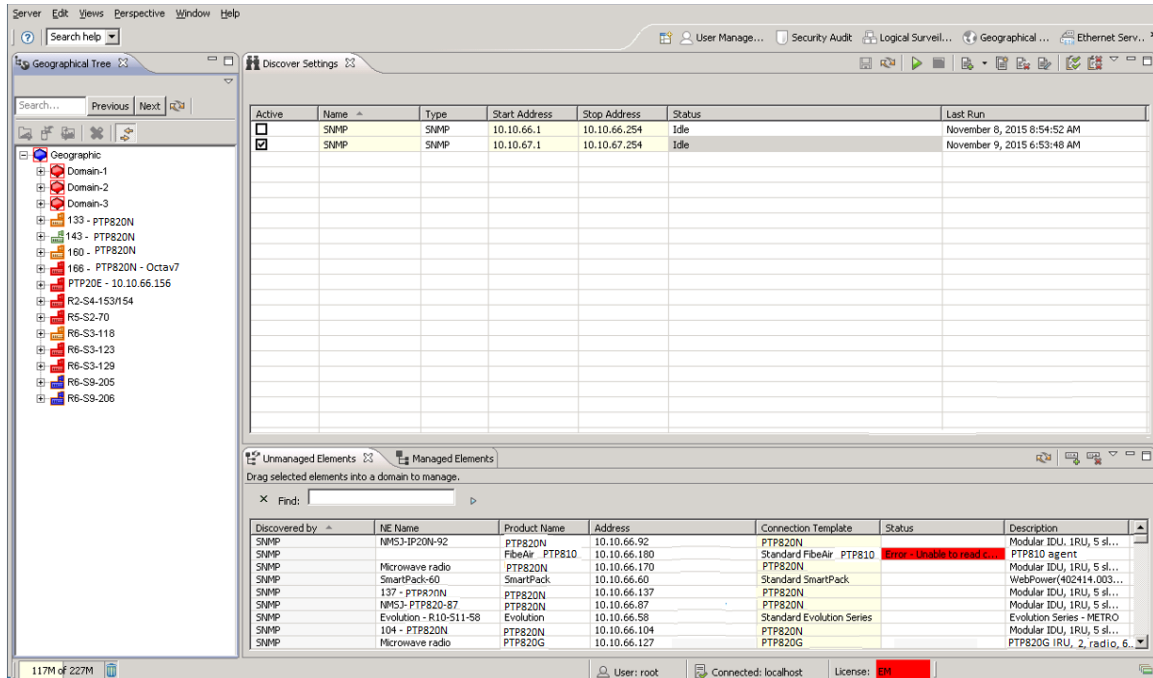
See also:

- [Opening several instances of alarm views with same scope](#)
- [How to acknowledge an alarm](#)
- [Visualization of Alarms](#)

Discover perspective

This is a perspective where you can discover and manage new elements.

Figure 22 Discover and manage new elements



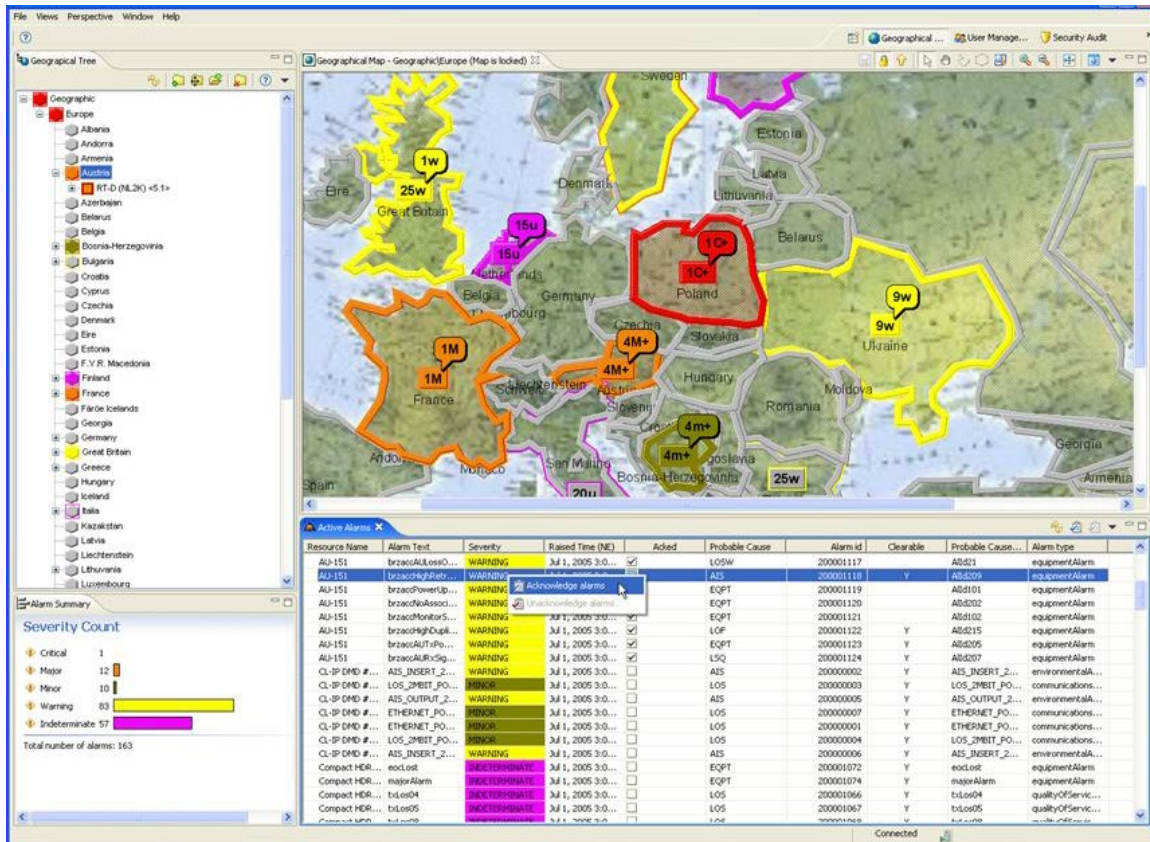
Prepare your discover parameters in the [Discover Settings](#) view, save the settings and then start the discover process. New elements are found in the [Unmanaged Elements](#) view and can be managed by dragging directly into the preferred domain in the [Geographical Tree](#) view. Managed elements are found in the Managed Elements view.

See also:

- [How to discover and manage an NE](#)

Geographical Surveillance perspective

This is a perspective for surveillance and management of NEs based on a geographical model.

Figure 23 Geographical surveillance perspective

The [Alarm Summary](#) view provides summaries of all alarms within different severities for your entire network. Details of each alarm can be found in the [Active Alarms](#) view.

It is recommended that you use the [Geographical Map](#) view to create/design the domain objects on the different levels in the geographical model. This view gives you a good picture of the alarm status in different geographical regions, and in the [Geographical Tree](#) view you can also see details of the alarm status on the NE's equipment. Both these views are good starting points for several maintenance and surveillance tasks regarding configuration and performance of the NE.

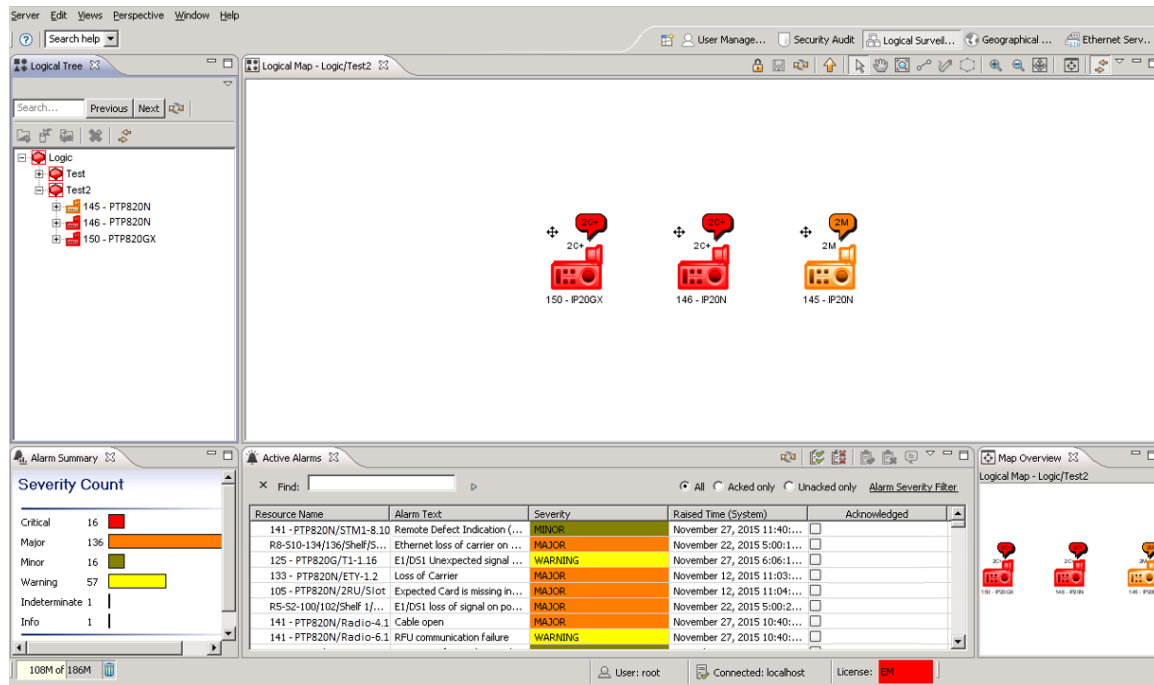
See also:

- [Visualization of Alarms](#)
- [How to acknowledge an alarm](#)
- [How to configure polling and traps](#)
- [How to use the performance reports](#)
- [How to download software on NE](#)
- [How to synchronize clock on a NE](#)

Logical Surveillance perspective

This is a perspective for monitoring and managing NEs based on a user-defined Logical Model. For details about how to organize a logical model, see the chapters about the [Logical Tree](#) view.

Figure 24 Logical surveillance perspective



The [Alarm Summary](#) view provides summaries of all alarms of the different severities in your entire network. Alarm details can be found in the [Active Alarms](#) view.

Both the [Logical Map](#) view and [Logical Tree](#) view provide a picture of the alarm status in different areas of your logical model, and in the tree view you can also browse to see details about the alarm status of the NE's equipment. Both views are good starting points for other maintenance and surveillance tasks, e.g. regarding configuration and performance on the NE. In both views you can create logical domains for your NE, and it is recommended that you organize the logical model so that the maintenance and surveillance tasks are carried out smoothly.

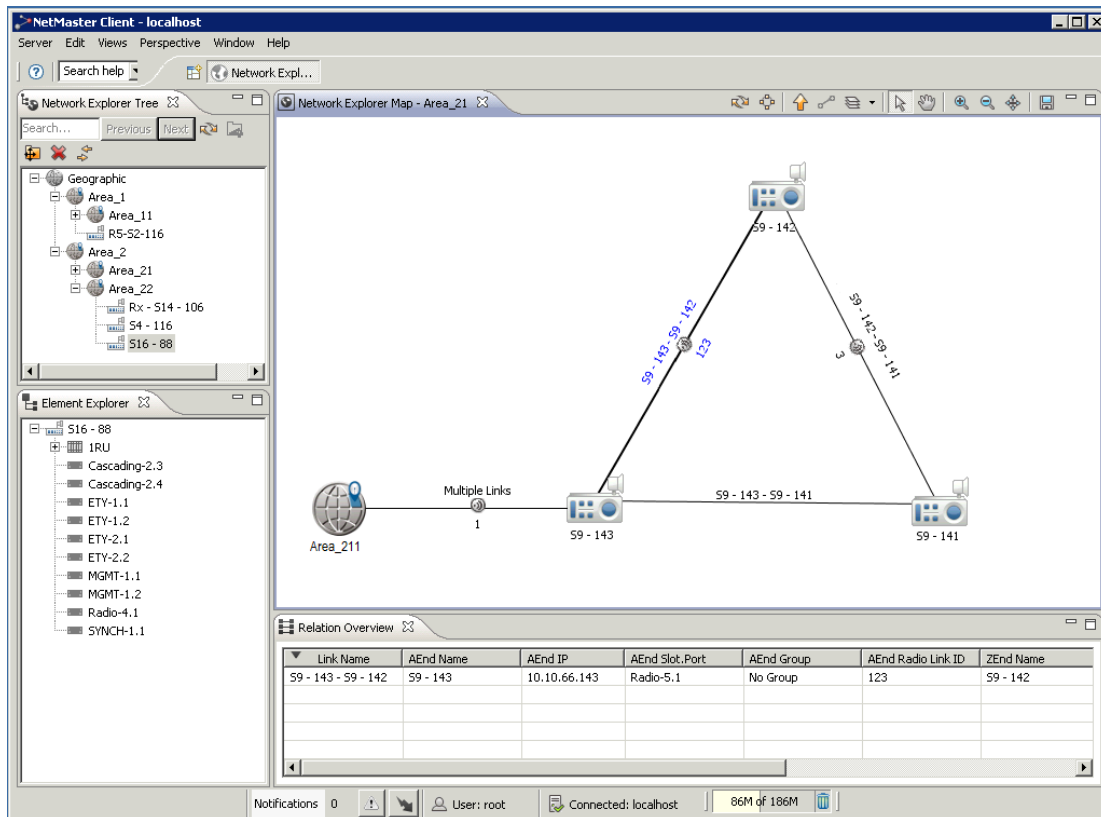
See also:

- [Visualization of Alarms](#)
- [How to acknowledge an alarm](#)
- [How to configure polling and traps](#)
- [How to use the performance reports](#)
- [How to download software on NE](#)
- [How to synchronize clock on a NE](#)

Network Explorer perspective

This is a perspective for monitoring and managing NEs based on either the [Geographical](#) model or the [Logical](#) model. The choice of which model to link to this perspective, is set in the [Network Explorer](#) Preferences page.

Any change done to domains and NEs (such as managing, deleting, renaming, etc.) in this **Network Explorer** perspective, is automatically reflected in the model to which this **Network Explorer** perspective is linked, and vice versa.



It is recommended that you use the [Network Explorer Map](#) view to create/design the domain objects on the different levels, corresponding to the NEs' actual physical location. This view gives you a good picture of the relations between elements in different geographical regions, as well as displaying the link names and the radio link IDs directly on the map.

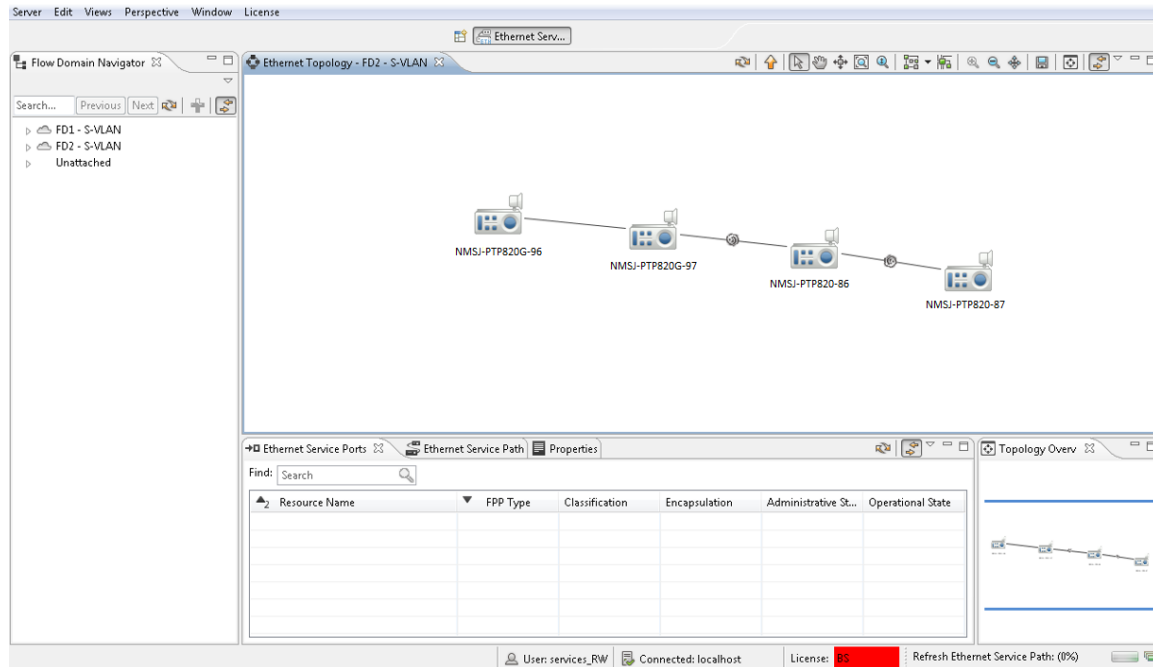
The [Network Explorer Map](#) view, together with the [Network Explorer Tree](#) view, are good starting points for various maintenance and surveillance tasks regarding configuration and performance of NEs.

See also:

- [Viewing and Configuring Alarms](#)
- [How to acknowledge an alarm](#)
- [How to configure polling and traps in PTP 820 NMS](#)
- [Analyzing Performance](#)
-

Ethernet Services perspective

This is a perspective for managing the provisioning of end-to-end Ethernet services, which gives you full control of the Ethernet services across the entire Ethernet network.



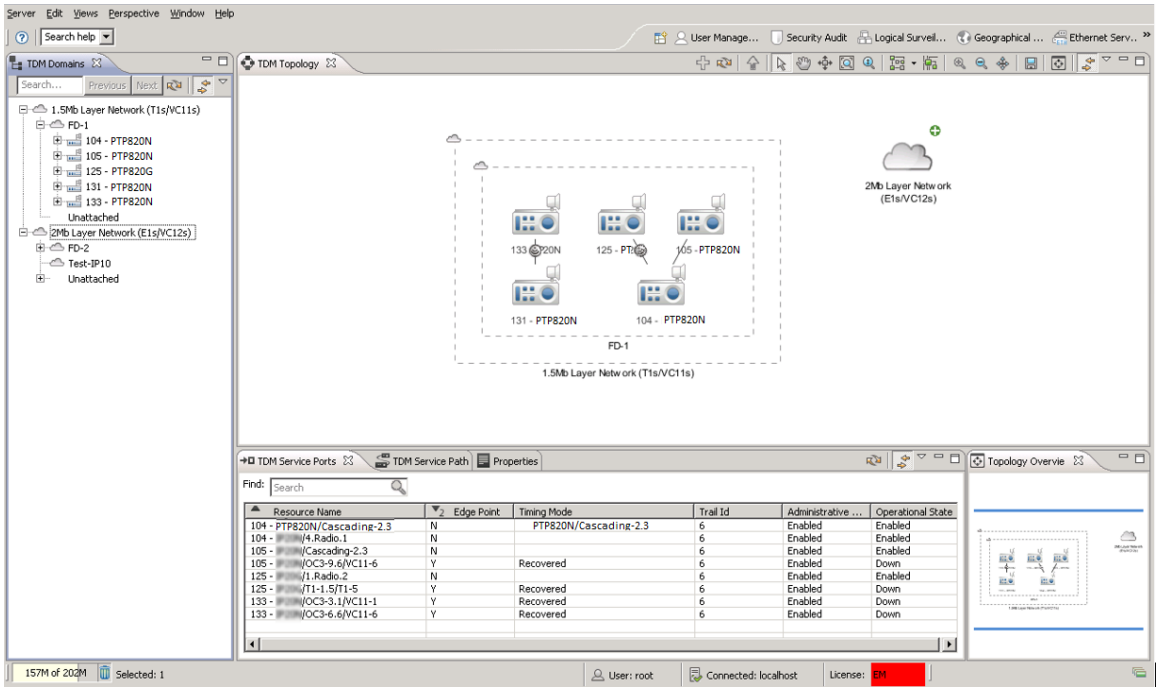
The first step in managing Ethernet services is to define the connectivity of the Ethernet network by creating Ethernet flow domains, using the Create Flow Domain wizard. Services that are already provisioned on the devices are discovered automatically by PTP 820 NMS.

Flow domains can then be managed in the Flow Domain Navigator view as well as the Ethernet Topology view, which displays flow domains, managed elements, and Ethernet links.

To create an Ethernet service, use the Create Ethernet Service wizard. You can manage the services and view detailed service information in the scoped Ethernet Services view and its corresponding Ethernet Service Path and Ethernet Service Ports views.

TDM Services perspective

This is a perspective for managing the provisioning of end-to-end TDM trails, which gives you full control of the TDM services across the entire TDM network.



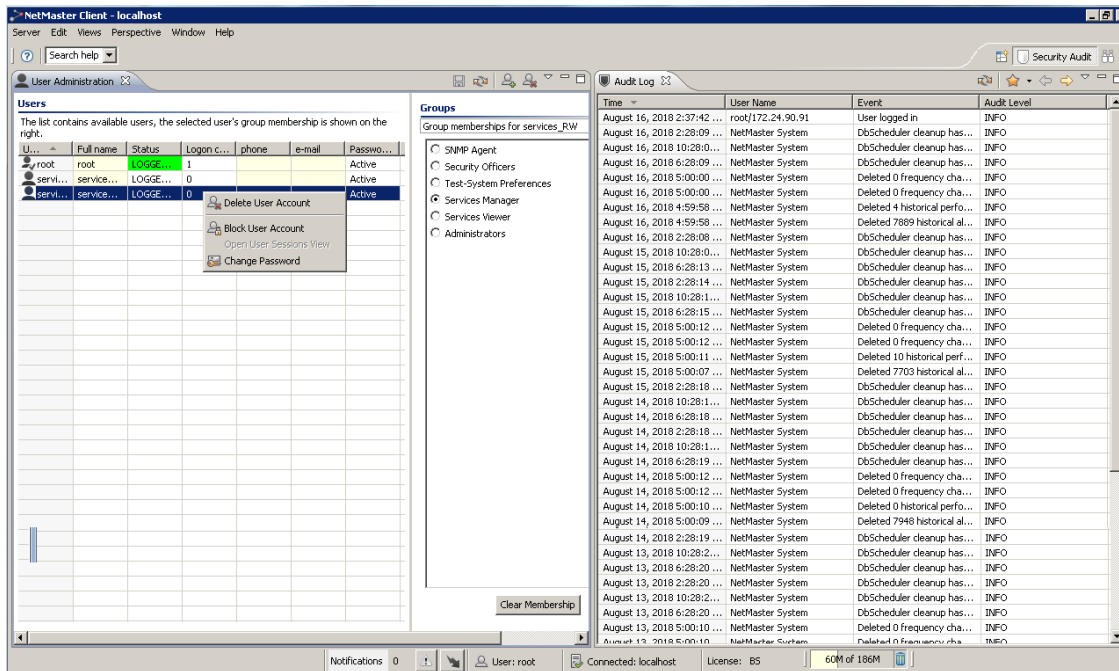
Elements are grouped into TDM domains based on connectivity and by making initial use of the grouping in the Ethernet Flow Domain Navigator. You can view the TDM subnetworks using the TDM Domains view as well as the TDM Topology view, which displays TDM domains, managed elements, and their TDM connections.

It is recommended that you enter information about existing STM-1/OC-3 links using the Create STM-1/OC-3 User Link wizard, because these links cannot be automatically discovered by PTP 820 NMS.

To create a TDM service, use the TDM Services wizard. You can manage the services and view detailed service information in the scoped TDM Services view and its corresponding TDM Service Path and TDM Service Ports views.

Security Audit perspective

This is a perspective for detecting undesirable behavior among users.

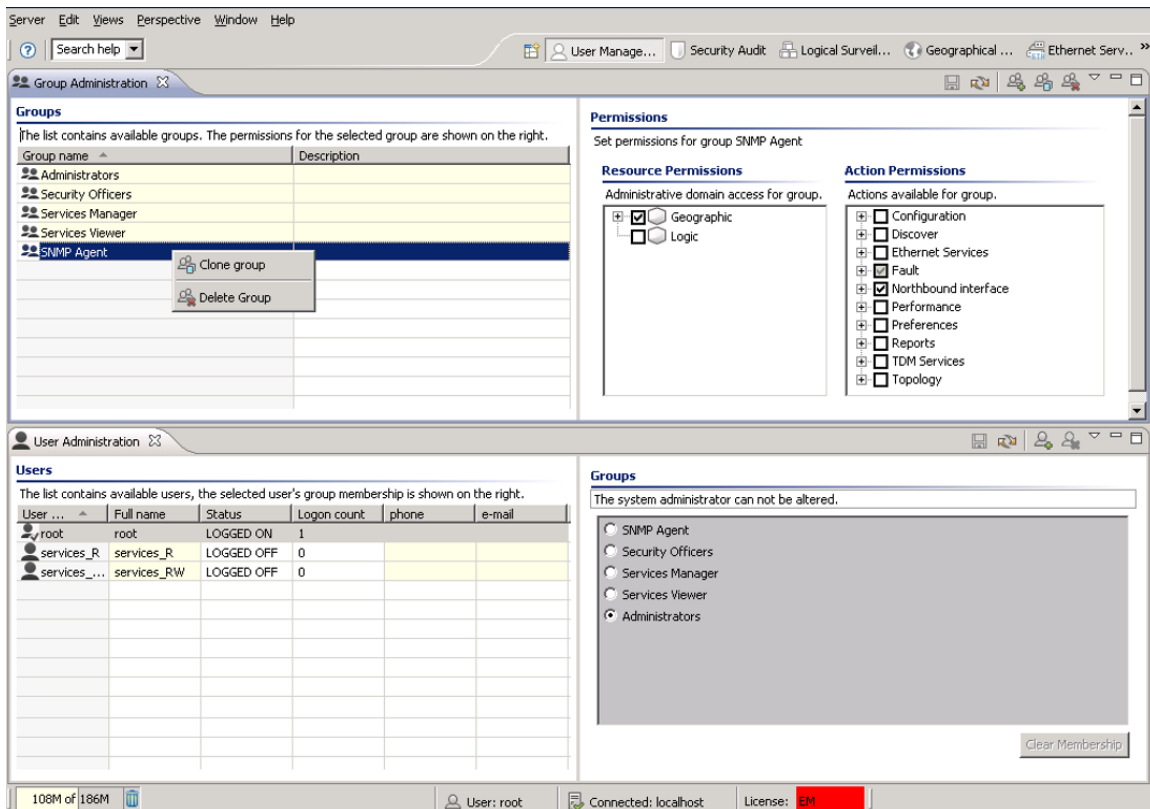
Figure 25 Security audit perspective

Use the [User Audit](#) view to investigate all events performed by users. If unwanted behavior is detected, suspicious user accounts can be blocked or deleted in the [User Administration](#) view.

Use the [Filter Manager](#) view to manage filters for the Audit Log view, the **Performance Overview** Report view and the **Performance Details** Report view.

User Management perspective

This is a perspective for creating new users and assigning/restricting permissions to the different user groups.

Figure 26 User Management perspective

Use the [User Administration](#) view to manage users: create new users, change passwords, block, delete and allocate permissions by assigning users to different groups. In the [Group Administration](#) view you can create user groups and assign permissions for each group. You can modify permissions regarding access to geographical and logical domains, and regarding usage of different actions in the applications.

See also:

- [How to create a new user](#)
- [How to create a new user-group](#)
- [How to change your password](#)

Chapter 5: All views and dialogs

This chapter includes:

- [Fault](#)
- [Configuration](#)
- [Performance](#)
- [Topology](#)
- [DiscoverServices - Ethernet and TDM](#)
- [Administration](#)
- [Northbound Interface](#)
- [Reports](#)
- [Other](#)
- [Open SNMP Interface](#)
- [General dialogs and views](#)
- [Preferences](#)
- [System Tray Monitors](#)

Fault

Active Alarms view

This view is found in both the [Geographical Surveillance](#) perspective and [Logical Surveillance](#) perspective.

This view is opened "non-scoped" from the main menu under Views | Fault | Active Alarms, as shown below:

Figure 27 Active alarm view

Resource Name	IP	Alarm Text	Severity	Raised Time (System)	Acknowledged
IP-20E - 10.1...	10.10.66.174	Loss of Carrier	MAJOR	July 27, 2017 11:52:50 AM	<input type="checkbox"/>
IP-20E - 10.1...	10.10.66.174	RFU RX level out of range	WARNING	July 27, 2017 11:52:50 AM	<input type="checkbox"/>
IP-20E - 156/...	10.10.66.156	Loss of Carrier	MAJOR	August 2, 2017 9:28:21 PM	<input type="checkbox"/>
IP10G - S5 - ...	10.10.67.135	E1/D51 unexpected signal on port #9	WARNING	July 31, 2017 4:42:00 PM	<input type="checkbox"/>
Rx - S14 - 10...	10.10.68.109	Under voltage	MAJOR	July 20, 2017 3:25:57 PM	<input type="checkbox"/>
IP10G - S5 - ...	10.10.67.135	E1/D51 unexpected signal on port #14	WARNING	July 31, 2017 4:42:00 PM	<input type="checkbox"/>
IP10G - S5 - ...	10.10.67.135	E1/D51 unexpected signal on port #15	WARNING	July 31, 2017 4:42:00 PM	<input type="checkbox"/>
IP10G - S5 - ...	10.10.67.135	E1/D51 unexpected signal on port #3	WARNING	July 31, 2017 4:42:00 PM	<input type="checkbox"/>
Rx - S14 - 98...	10.10.68.98	RFU communication failure	WARNING	August 2, 2017 4:59:26 AM	<input type="checkbox"/>
Rx - S14 - 11...	10.10.68.110	Loss of Carrier	MAJOR	July 27, 2017 11:51:00 AM	<input type="checkbox"/>
Rx - S14 - 11...	10.10.68.110	RFU communication failure	WARNING	July 27, 2017 11:51:00 AM	<input type="checkbox"/>
IP-20ER2 - 1...	10.10.66.173	Loss of Carrier	MAJOR	July 27, 2017 11:53:02 AM	<input type="checkbox"/>
IP-20E - 10.1...	10.10.66.174	Loss of Carrier	MAJOR	July 27, 2017 11:52:50 AM	<input type="checkbox"/>
Rx - S14 - 10...	10.10.68.109	Expected Card is missing in slot	MAJOR	June 22, 2017 6:13:14 PM	<input type="checkbox"/>
IP10G - S5 - ...	10.10.67.135	Too many non-edge ports	WARNING	July 31, 2017 4:42:00 PM	<input type="checkbox"/>
IP-20E - 156/...	10.10.66.156	Loss of Carrier	MAJOR	August 2, 2017 9:28:21 PM	<input type="checkbox"/>
Rx - S14 - 11...	10.10.68.110	Expected Card is missing in slot	MAJOR	July 27, 2017 11:51:00 AM	<input type="checkbox"/>

The Active Alarms view presents active alarms for the current scope, and allows you to acknowledge alarms which have been followed up.

An "[active](#)" alarm is a clearable alarm in the "raised" state and which has not been "cleared". Whenever an alarm is cleared, it will be removed from the table, but can still be found in a corresponding scope in the [Historical Alarms](#) view.

Active Alarms view with a scope

The view can also be opened by selecting any node in one of the topology views (Geographical or Logical Map or Tree) and then selecting Fault | Active Alarms in the Context or Dropdown menu. The view will then open with the selection as a [scope](#) - presenting only those alarms for the currently selected NEs/nodes/subdomain, as shown below:

Figure 28 Active alarm scope view

Resource Name	Alarm Text	Severity	Raised Time (System)	Acknowledged
141 - 7.7	E1/DS1 Unexpected signal ...	WARNING	November 9, 2015 6:55:36 ...	<input type="checkbox"/>
150 - ascending-...	Loss of Carrier	MAJOR	November 8, 2015 9:37:37 ...	<input type="checkbox"/>
150 - radio-1.1	Radio loss of frame	CRITICAL	November 8, 2015 9:37:37 ...	<input type="checkbox"/>
141 - 7.3	E1/DS1 Unexpected signal ...	WARNING	November 9, 2015 6:55:36 ...	<input type="checkbox"/>
NMSJ- /Radio-1....	RFU communication failure	WARNING	November 9, 2015 6:55:52 ...	<input type="checkbox"/>
141 - dio-4.1	RFU communication failure	WARNING	November 9, 2015 6:55:36 ...	<input type="checkbox"/>
NMSJ- /IDU/Pow...	Under voltage	MAJOR	November 9, 2015 6:55:52 ...	<input type="checkbox"/>

In the above example, the Active Alarms view presents alarms, restricted to a scope containing one single domain called "Domain-1".

The Active Alarms view can also be opened from the [Alarm Summary](#) view by clicking a bar in the graph Severity Count area. In this case the scope will be restricted to the selected severity, but contain alarms from your entire network.

Opening several instances of alarm views with same scope

The normal behaviour when opening a view in PTP 820 NMS is that it is possible to open max 1 instance of a given view with a given scope. If you try to open a given view with a scope that is already open, PTP 820 NMS will shift focus to the already opened view.

For the alarms views it is however possible to open several instances of a view with the same scope. Each time an alarm view is opened, a new instance of the view is opened, even if a view with similar scope already is open. In this way you may have open several instances of Active and Historical Alarms view. This offers a flexible way of working with different quick search and filter settings. To distinguish between similar instances, each alarm view can be [renamed](#).

See the [Alarm Workflow perspective](#) on a suggestion on how to work with the alarm views.

Please note that max 1 instance of the **Active Alarms** view can be opened by [clicking a Severity Count bar](#) in the **Alarm Summary** view. It is however possible to open several **Active Alarms** view unscoped, and then use the [Alarm Severity filter](#).

Active alarms table

The table displays the following fields for each alarm:

Table 4 Active alarms list












Name	Explanation
Resource Name	Source of alarm - the network resource that generated the alarm.
Alarm Text	Gives the most likely reason for the alarm. Similar to "Native Probable Cause", as defined in TMF608. This is a textual description of the cause of the alarm, displayed exactly as sent from the NE or portrayed in the PTP 820 NMS user interface. The text can be customized using the Alarm Templates view.
Severity	One of the possible alarm severities: CRITICAL, MAJOR, MINOR, WARNING, INDETERMINATE or INFO. The severities of incoming alarms can be altered using the Alarm Templates view.
Raised Time (NE)	The time on the NE when the alarm was raised.
Acknowledged	Checked if the alarm has been acknowledged .
Probable Cause	Probable Cause shows the likely cause of this alarm. The value is predefined in the TMF608.
Alarm ID	A number which identifies the instance of this alarm.
Is Clearable	Has the value " Y" if the alarm/event represents a condition that can be cleared at a later time (otherwise blank). Always "Y" for Active alarms.
Probable Cause Qualifier	A code for identifying the alarm, e.g. used in the Alarm Templates view.
Alarm type	<p>A text which identifies the type of alarm. Used internally to map the alarm to a corresponding name.</p> <p>Value is one of the following (as defined in TMF608 and specified by X.733: EventType):</p> <ul style="list-style-type: none"> - COMMUNICATIONS_ALARM - ENVIRONMENTAL_ALARM - EQUIPMENT_ALARM - PROCESSING_ERROR_ALARM - QUALITY_OF_SERVICE_ALARM - SECURITY_ALARM

Name	Explanation
Raised Time (System)	The time on the PTP 820 NMS server when the alarm was raised.
Additional Text	Free form text description of the alarm (not interpreted by server)
Alarm comment	An optional text added by a user in the Alarm Comment dialog.
Layer	Identifies the layer of the node reporting the event/alarm. "N/A" if not relevant.
Raised Native Log Id	Element specific alarm id for the raised alarm event. May be used to trace the alarm in the element alarm log. PTP 820 NMS will only record Raised/Cleared Native Log Ids for element types that support it. There are also some situations where it may not be recorded even for element types that support it
Notification Muted	Has the value " Y" if the NE containing this alarm currently is muted . Only alarms from unmuted elements can trigger alarm notifications .
Notification Mute Expiration	The time on the PTP 820 NMS server when muting on this element will automatically expire . Will have the value "Never" if element is muted without Notifications Mute Expiration enabled, and will be blank if element is not muted.

The color of the Severity field in the table will by default correspond to the severity of the alarm. For more details about alarms, including severities and colors, see the chapter about [visualization of alarms](#).

The [Alarm Templates](#) view can be used to customize the Alarm Text and Severity for selected alarms, or to prevent certain alarms from appearing in the Active Alarms view.

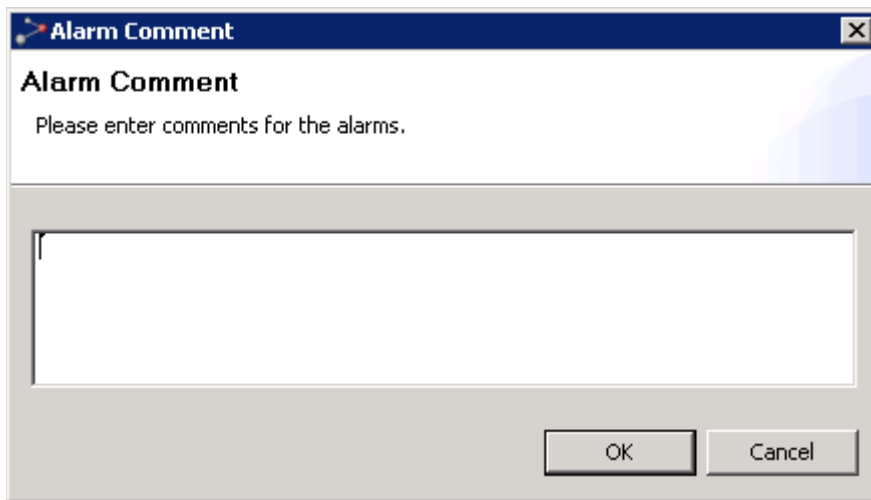
Available operations

-  **Refresh View** Refresh the entire table and update the status of all available alarms: new/raised alarms are received, and cleared alarms disappear from the Active Alarms view.
-  **Acknowledge All Alarms...** Acknowledge all alarms in the view and open the Alarm Comment dialog, where you can add a comment to the alarms.
-  **Unacknowledge All Alarms...** Remove the acknowledgement of all alarms in the view and open the Alarm Comment dialog, where you can add a comment to the alarms.
-  **Acknowledge alarms** Acknowledge the currently selected alarm (or alarms) and open the [Alarm Comment](#) dialog, where you can add a comment to this alarm. If the currently selected alarm has already been acknowledged, this operation will be disabled.
-  **Unacknowledge alarms** Remove the acknowledgement of an alarm and open the [Alarm Comment](#) dialog. If the currently selected alarm has not been acknowledged, this operation will be disabled.
-  **Alarm Comment...** Open the [Alarm Comment](#) dialog, where you can view and change an alarm comment.
-  **Rename View** Use Rename view to change the view title from the default "[view name](#) - [scope](#)" to something suitable for your purpose. It is convenient to do this to distinguish between views, when [several instances of the same view with same scope](#) are opened.
-  **Show Quick Search** Enable the [Quick Search](#) field in the Active Alarms view. The quick search functionality makes it possible to search the contents of the view. All visible columns can be searched.
-  **Export to File...** Use the [Export](#) function to save your current data to file. You are allowed to save the table as an Excel spreadsheet (.xls), comma separated file (.csv) or extended markup language (.xml). A standard Save dialog will appear (as defined by your operating system)
-  **Customize Columns** Open the [Customize Columns](#) dialog for the Active alarms view. In this dialog you can select which columns will be displayed in the table, and the order in which they appear.
- ☒ **All** ☐ **Acked only** ☐ **Unacked only** Click the Acked Filter radio buttons to quickly view all alarms or acknowledged/unacknowledged alarms only. By default, this filter is set to All.
-  **Alarm Severity Filter** Use the Alarm Severity Filter dropdown to select showing alarms with specific Alarm severity (or alarms severities). By default, this filter is set to All.

Alarm Comment dialog

This dialog is opened when editing a comment. A similar dialog is opened whenever acknowledging or unacknowledging an alarm.

Figure 29 Alarm comment dialog



Add a comment in the text field, and press the OK button when finished.

Active NMS Alarms view

This view is opened "non-scoped" from the main menu under **Views > Fault > Active NMS Alarms**. The view displays active alarms related to Server High Availability only. Thus, the alarms shown in this view are a subset of all [Active Alarms](#).

For a description of the fields displayed for each alarm, refer to Active alarms table. For a description of the operations available in this view, refer to Available operations.

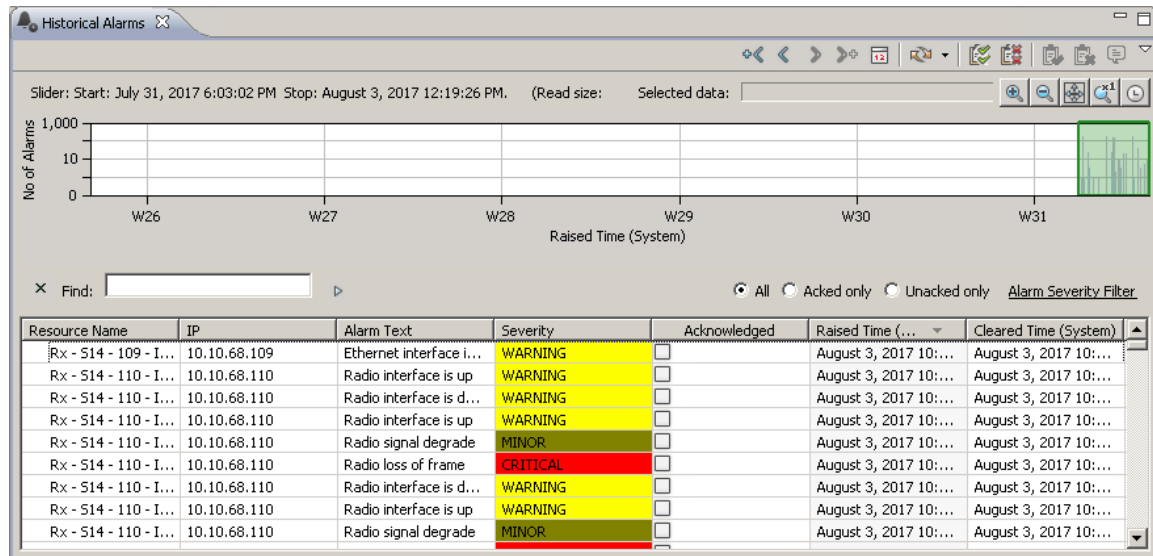
Figure 30 Active NMS Alarms

[illegible]

Historical Alarms view

The view is opened by selecting any node in one of the topology views (Geographical or Logical Map or Tree) and then selecting Fault | Historical Alarms in the Context or Dropdown menu. This will open the Historical Alarms view with this selection as a scope - displaying only those alarms for the currently selected NE/nodes/subdomain.

Figure 31 Historical alarm view



The view is also opened by selecting any node in one of the topology views (Geographical or Logical Map or Tree) and then selecting Fault | Historical Alarms in the Context or Dropdown menu. This will open the Historical Alarms view with this selection as a [scope](#) - displaying only those alarms for the currently selected NE/nodes/subdomain.

The view displays a table of all historical alarms for the current selection. A "historical" alarm is any alarm that is "cleared" (see [definition of "cleared alarms"](#)). Whenever an alarm disappears from any table in the [Active Alarms](#) view, it will appear in any Historical Alarms table with the same scope.

The Historical Alarms view can help you when analyzing situations with errors or poor performance in your network. By studying other errors and the order they appeared for the NE, this view can help you identify and solve the ["root cause problem"](#).

Opening several instances of alarm views with same scope

The normal behaviour when opening a view in PTP 820 NMS is that it is possible to open max 1 instance of a given view with a given scope. If you try to open a given view with a scope that is already open, PTP 820 NMS will shift focus to the already opened view.

For the alarms views it is however possible to open several instances of a view with the same scope. Each time an alarm view is opened, a new instance of the view is opened, even if a view with similar scope already is open. In this way you may have open several instances of Active and Historical Alarms view. This offers a flexible way of working with different quick search and filter settings. To distinguish between similar instances, each alarm view can be [renamed](#).

See the [Alarm Workflow perspective](#) on a suggestion about how to work with the alarm views.

Historical Alarms table

The table displays the following values for each alarm:

Table 5 Historical alarms list

Name	Explanation
Resource Name	Source of alarm - the network resource that generated the alarm
Alarm Text	Gives the most likely reason for the alarm. Similar to "Native Probable Cause", as defined in TMF608. This is a textual description of the cause of the alarm, displayed exactly as sent from the NE or portrayed in the PTP 820 NMS user interface. The text can be customized using the Alarm Templates view.
Severity	One of the possible alarm severities: CRITICAL, MAJOR, MINOR, WARNING, INDETERMINATE or INFO. Severities can be customized using the Alarm Templates view.
Raised Time (NE)	The time on the NE when the alarm was raised.
Cleared Time (NE)	The time on the NE when the alarm was cleared.
Acked	Checked if the alarm has been acknowledged
Probable Cause	A mapping of the Probable Cause Qualifier and/or Native Probable Cause with a set of predefined Probable Causes as defined in TMF608
Probable Cause Qualifier	A code for uniquely identifying the alarm, e.g. used in the Alarm Templates view.
Alarm type	A text which identifies the type of alarm. Used internally to map the alarm to a corresponding name. Value is one of the following (as defined in TMF608 and specified by X.733: EventType): - COMMUNICATIONS_ALARM - ENVIRONMENTAL_ALARM - EQUIPMENT_ALARM - PROCESSING_ERROR_ALARM - QUALITY_OF_SERVICE_ALARM - SECURITY_ALARM
Raised Time (System)	The time on the PTP 820 NMS server when the alarm was raised.








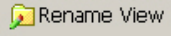




Name	Explanation
Cleared Time (System)	The time on the PTP 820 NMS server when the alarm was cleared .
Is Clearable	Has the value " Y" if the alarm/event represents a condition that can be cleared at a later time (otherwise blank).
Alarm ID	A number which identifies the instance of this alarm.
Additional Text	Free form text description of the alarm (not interpreted by server)
Alarm Comment	An optional text added by a user in the Alarm Comment dialog.
Layer	Identifies the layer of the node reporting the event/alarm. "N/A" if not relevant.
Raised Native Log Id	Element specific alarm id for the raised alarm event. May be used to trace the alarm in the element alarm log. PTP 820 NMS will only record Raised/Cleared Native Log Ids for element types that support it. There are also some situations where it may not be recorded even for element types that support it
Cleared Native Log Id	Element specific alarm id for the cleared alarm event. May be used to trace the alarm in the element alarm log.
Notification Muted	Has the value "Y" if the NE containing this alarm currently is muted . Only alarms from unmuted elements can trigger alarm notifications .
Notification Mute Expiration	The time on the PTP 820 NMS server when muting on this element will automatically expire . Will have the value "Never" if element is muted without Notifications Mute Expiration enabled, and will be blank if element is not muted.
Duration (System)	Duration of the alarm on the PTP 820 NMS server. Corresponds to: Cleared Time (System) - Raised Time (System)
Duration (NE)	Duration of the alarm on the NE. Corresponds to: Cleared Time (NE) - Raised Time (NE). Blank if any of these columns are blank







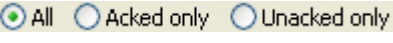

For more details about alarms and definition of severities, see the chapter about [visualization of alarms](#). The alarm-text and severity of incoming alarms for an NE can be customized by creating a template in the [Alarm Templates view](#) and applying the template to the NE in the [Alarm Templates Assignment view](#).

Please note that the table displays a query of data selection defined in the [Timeslider](#) tool. Default is a query of the last 1000 historical alarms. In addition the data currently presented in the view can be filtered using the [Quicksearch](#) field, [Acked Filter](#) radiobuttons and [Alarm Severity Filter](#) dropdown.

Available operations

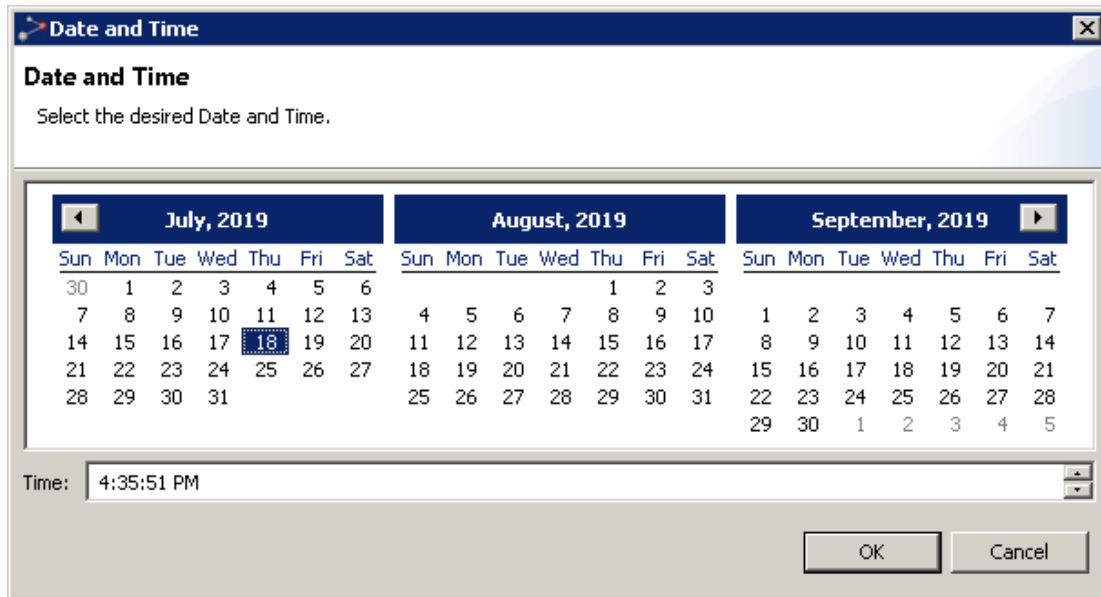
The following operations are available in the table:

-  Manual Refresh. Refresh the entire table and update the status of all available alarms - displays new, cleared alarms. Press arrow down to switch between Manual and Automatic Refresh.
-  Automatic Refresh. Refresh the entire table and update the status of all available alarms - displays new, cleared alarms. Can be set to auto refresh every 1 min, 5 min and 10 min. Note that Timeslider functionality is not available when in auto refresh mode. Press arrow down to switch between Manual and Automatic Refresh.
-  Acknowledge All Alarms... Acknowledge all alarms in the view and open the Alarm Comment dialog, where you can add a comment to the alarms.
-  Unacknowledge All Alarms... Remove the acknowledgement of all alarms in the view and open the Alarm Comment dialog, where you can add a comment to the alarms.
-  Acknowledge alarms Acknowledge the currently selected alarm (or alarms) and open the [Alarm Comment](#) dialog, where you can add a comment to this alarm. If the currently selected alarm has already been acknowledged, this icon/operation will be disabled.
-  Unacknowledge alarms Remove the acknowledgement of an alarm, and open the [Alarm Comment](#) dialog. If the currently selected alarm has already been acknowledged, this icon/operation will be disabled.
-  Alarm Comment... Open the [Alarm Comments dialog](#), where you can view and change an alarm comment.
-  Rename View Use Rename View to change the title from the default "[view name - scope](#)" to something suitable for your purpose. It is convenient to do this to distinguish between the views, when [several instances of the same view with same scope](#) are opened.
-  Extend previous read. This operation does a query of data corresponding to adding one [read size](#) to the left in the [Timeslider](#) tool.
-  Get previous read. This operation does a query of data corresponding to moving one read size to the left in the Timeslider tool.
-  Get next read. This operation does a query of data corresponding to adding one read size to the right in the Timeslider tool.
-  Extend next read. This operation does a query of data corresponding to moving one read size to the right in the Timeslider tool.

-  Go to selected time and date. This button opens the [Date and Time dialog](#). The entry will be the new starting point for the Slider. Data will be read from this starting point up to read size. The new right border will be calculated based on the newest data in the read.
-  Show Timeslider - Show/hide the [Timeslider](#) in the Historical Alarms view. The Timeslider is a tool that makes it easier to navigate the contents of a view with large amounts of data in the table. Whenever the Timeslider tool is enabled, it is possible to navigate the [Slider](#) to do a query for the content in the main view.
-  Show Timeslider scrollbar Show/hide the Timeslider scrollbar at the bottom of the Timeslider tool. Whenever the Timeslider is [zoomed](#), the scrollbar can be used for navigating Timeslider bar along the time axis.
-  Show Quick Search Enable the [Quick Search](#) field in the Historical Alarms view. The quick search functionality makes it possible to search the contents of the view. All visible columns can be searched.
-  Export to File... Use the Export function to save your current data to file. You are allowed to save the table as an Excel spreadsheet (.xls), comma separated file (.csv) or extended markup language (.xml). A standard [Export To File](#) dialog will appear (as defined by your operating system).
-  Customize Columns Open the [Customize Columns](#) dialog for the Historical Alarms view. In this dialog you can select which columns will be displayed in the table, and the order in which they appear.
-  ☒ All ☐ Acked only ☐ Unacked only Click the Acked Filter radiobuttons to quickly view all alarms or acknowledged/unacknowledged alarms only. By default this filter is set to All.
-  Alarm Severity Filter Use the Alarm Severity Filter dropdown to select showing alarms with specific Alarm severity (or alarms severities). By default this filter is set to All.

Date and Time dialog

This dialog appears whenever selecting **Go to selected time and date** on the **Historical Alarms View** toolbar.

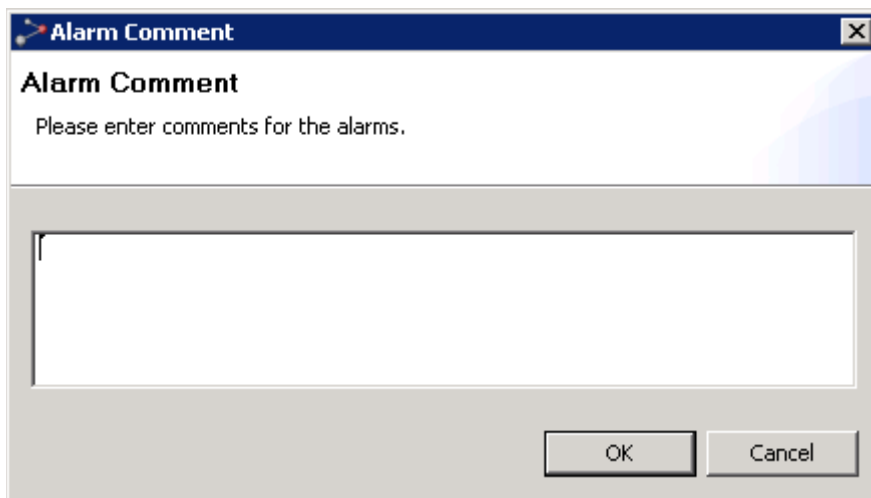


Pick a new start date and time for the **Slider** and press **OK**.

Alarm Comments dialog

This dialog is opened whenever acknowledging or unacknowledging an alarm, or when viewing a comment.

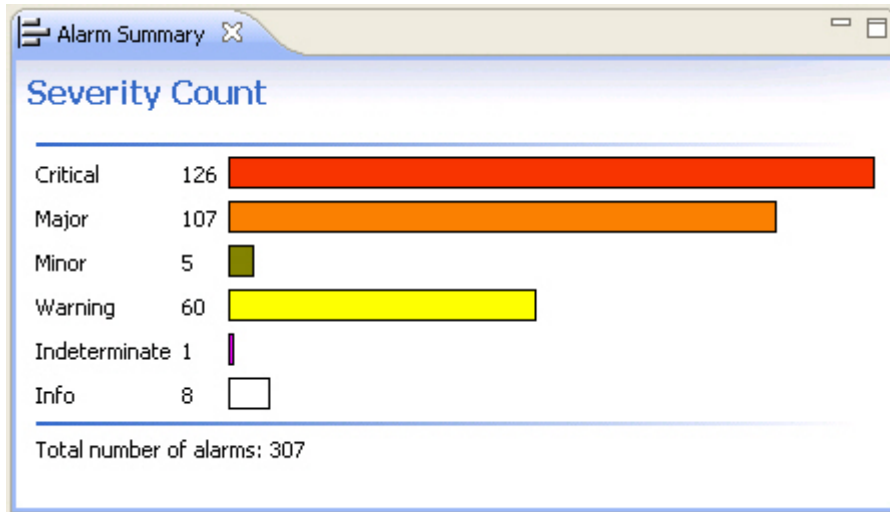
Figure 32 Alarm comments dialog



Add a comment in the text field, and press the OK button when finished.

Alarm Summary view

Figure 33 Alarm summary view




The **Alarm Summary** view shows an overview of all alarms for all your managed NEs, and provides a quick overview of the alarm status in your entire network.

The view displays the **Severity Count** graph: a graphical presentation of alarms of each severity in the entire network. The graph includes a bar for each of the categories: Critical, Major, Minor, Warning, Indeterminate and Info.

The view will only present "[active](#)" alarms: clearable alarms in a "raised" state, and not those that have been "cleared". The same alarm state is presented in the [Active Alarms](#) view. Whenever an alarm is "cleared" on the equipment, it will disappear from the **Alarm Summary** view, but can be found in the [Historical Alarms](#) view. For more details about alarms, alarm states and severities, see the chapter about [visualization of alarms](#).

Available operations

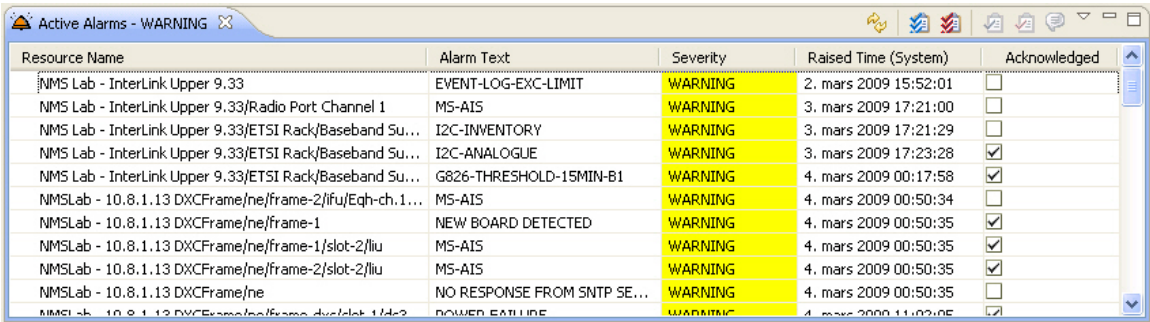
-  Click any of the bars in the Severity Count graph to study the alarms of this severity. This will open the [Active Alarms](#) view, with the selected severity as the [scope](#).

Please note that max 1 instance of the Active Alarms view can be opened by clicking a Severity Count bar. It is however possible to open several Active Alarms view unscoped, and then use the [Alarm Severity filter](#).

Active Alarms view for a single alarm category

The example below shows the Active Alarms view, opened by clicking the Warning bar in the Severity Count graph:

Figure 34 Active alarms view for a single alarm category

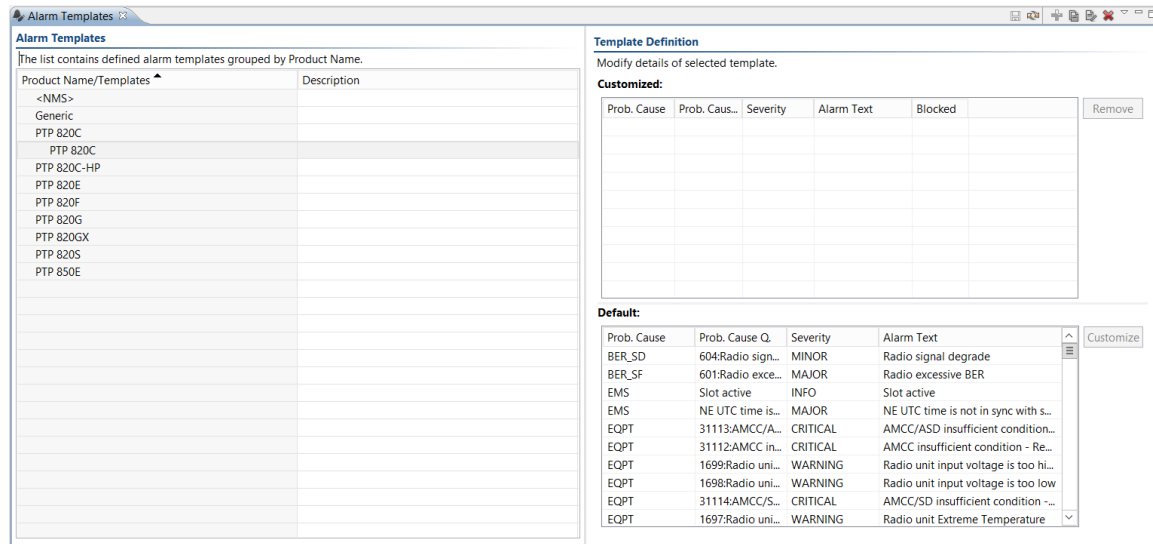


Resource Name	Alarm Text	Severity	Raised Time (System)	Acknowledged
NMS Lab - InterLink Upper 9.33	EVENT-LOG-EXC-LIMIT	WARNING	2. mars 2009 15:52:01	<input type="checkbox"/>
NMS Lab - InterLink Upper 9.33/Radio Port Channel 1	MS-AIS	WARNING	3. mars 2009 17:21:00	<input type="checkbox"/>
NMS Lab - InterLink Upper 9.33/ETSI Rack/Baseband Su...	I2C-INVENTORY	WARNING	3. mars 2009 17:21:29	<input type="checkbox"/>
NMS Lab - InterLink Upper 9.33/ETSI Rack/Baseband Su...	I2C-ANALOGUE	WARNING	3. mars 2009 17:23:28	<input checked="" type="checkbox"/>
NMS Lab - InterLink Upper 9.33/ETSI Rack/Baseband Su...	G826-THRESHOLD-15MIN-B1	WARNING	4. mars 2009 00:17:58	<input checked="" type="checkbox"/>
NMSLab - 10.8.1.13 DXCFRame/ne/frame-2/ifu/Eqh-ch.1...	MS-AIS	WARNING	4. mars 2009 00:50:34	<input type="checkbox"/>
NMSLab - 10.8.1.13 DXCFRame/ne/frame-1	NEW BOARD DETECTED	WARNING	4. mars 2009 00:50:35	<input checked="" type="checkbox"/>
NMSLab - 10.8.1.13 DXCFRame/ne/frame-1/slot-2/liu	MS-AIS	WARNING	4. mars 2009 00:50:35	<input checked="" type="checkbox"/>
NMSLab - 10.8.1.13 DXCFRame/ne/frame-2/slot-2/liu	MS-AIS	WARNING	4. mars 2009 00:50:35	<input checked="" type="checkbox"/>
NMSLab - 10.8.1.13 DXCFRame/ne	NO RESPONSE FROM SNTP SE...	WARNING	4. mars 2009 00:50:35	<input type="checkbox"/>
NMSLab - 10.8.1.13 DXCFRame/ne/frame-due/slot-1/de2	POWER FAILURE	WARNING	4. mars 2009 11:02:05	<input checked="" type="checkbox"/>

Alarm Templates view

This view is opened from the main menu under **Views > Fault > Alarm Templates**.

Figure 35 Alarm templates view



In this view you can create templates for redefining the appearance your alarms. Each template contains mapping between a set of alarms and severities, and/or an alarm filter, and/or an alarm text. The changes in this view will apply for NEs which have a template assigned in the [Alarm Templates Assignment](#) view and will apply to your incoming alarms (not for alarms that is already active or cleared). For more details about alarms and severities, see the chapter about [visualisation of alarms](#). The templates created in this view are used by the [Alarm Templates Assignment](#) view and might influence all views displaying incoming alarms (existing alarms will not be influenced).

Alarm templates are used when you (or your organization) consider an alarm to have a different severity from the default alarms. This can typically be:

- When your organization is using NEs from several vendors, and want to use a company-specific set of severities instead of the vendors' default severities. In this case you might want to permanently assign severity mappings and alarm texts for all NEs in the network.
- When you want to continue using equipment with a known error. In this case you might want to temporarily assign a filter ignoring the alarm on the NE until the NE-defect is rectified.
- When a certain error situation on NE must be monitored especially closely, e.g. when you have guaranteed extra high quality for a customer. In this case you might want to assign a template increasing the severity of some alarms indicating certain error situations.

We use the term "assign a template to the NE", even though no change is actually made to the NE when assigning an alarm template - the template is solely a mapping within PTP 820 NMS of the incoming alarm from this NE.

The view consists of an Alarm Templates area containing a table of alarm templates, and a Template Definition area containing details about the currently selected alarm template.

Alarm Templates table

The **Alarm Templates** area consists of a table containing the following columns:

Table 6 Alarm template table

Name	Explanation
Product Name/Templates	Each NE type can have several associated alarm templates. Click the Expand icon to the left of the NE type to expand a list of all templates which have currently been created for that NE type. Note that if no templates are created the list will be empty and it will not be possible to expand the list. New templates are created with the Add Template icon on the toolbar. Click a template to view details about that template.
Description	Text entered by the user describing a template.

Each line in the table contains either an NE type or a template. Select an NE-Type in the **NE-Type/Template** column in the to create a new alarm template or select a template to view its properties.

Template Definition area

This area only appears when a template is selected in the Alarm Templates table. In the Default area you can select alarms that you wish to customize. In the Customized area, for each alarm you can define a new alarm-text, severity and decide whether the alarm should be blocked.

Customized table

The Customized area consists of a table containing the following columns:

Table 7 Customized table

Name	Explanation
Prob. Cause	Gives the most likely reason for the alarm This is a code which can help describe the cause of the alarm, displayed exactly as sent from the NE.
Prob. Cause Q.	A code for identifying the alarm, e.g. used in the Active Alarm view and the Historical Alarm view.
Severity	Changes the severity in the Customized table if you want PTP 820 NMS to use a different severity.
Alarm Text	Write your own text in the Customized table if you want PTP 820 NMS to present a different text for this alarm.











Update alarm-texts change severities and change blocking by clicking and writing directly in the table. Remove customization of an alarm by selecting the alarm in the table and then moving it back to the [Default](#) table with the [Move To..](#) context menu or one of [Move](#) buttons.




Default table

The Default area consists of a Default table containing the same columns as the [Customized](#) table, but contains the default values for each alarm. The Default table contains all available alarms for the currently selected NE-type that is not yet customized in this template.

Select one or more alarms in the Default area and move it by dragging it into the Customized area or by using the [Move To..](#) context menu or one of [Move](#) buttons.

Available operations

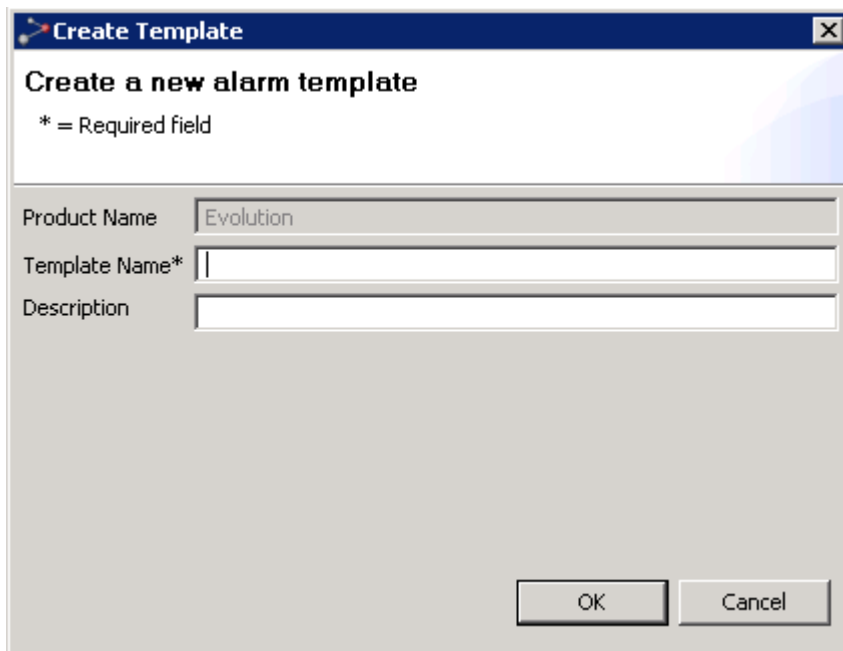
-  **Save** Save all changes made to the templates in this view. When changes have been saved, the updates in the alarm templates can influence the incoming alarms. Alarms that is already active (or cleared) before pressing Save will not be influenced by your latest change.
-  **Create Template** Add a new template. The [Create Template](#) dialog will be opened. This menu item will only be available if an NE type is selected in the NE type/Template table.
-  **Refresh View** Refresh the view to receive the newest data from server.
-  **Clone** Clone the selected template. The [Template Name](#) dialog will be opened. This menu item will only be available if a template is selected in the NE type/Template table.
-  **Delete** Delete the selected template. This menu item will only be available if a template is selected in the NE type/Template table.
-  **Rename** Change the name of the selected template. The [Template Name](#) dialog will be opened. This menu item will only be available if a template is selected in the NE type/Template table.
-  **Horizontal** Arrange the view horizontally.
-  **Vertical** Arrange the view vertically.
-  **Move To customized table** Use this context-menu in the Default table to move an available alarm from the Default table to the Customized table. This will allow you to change the severity, alarm text and/or filtering for this alarm .
-  **Move To Default table** Use this context menu in the Default table to move an available alarm from the Customized table to the Default table. The alarm will no longer be customized with this template, and its default severity, alarm text and filtering will be used.

-  This button can be used similarly to the Move To Customized Table context menu.
-  This button can be used similarly to the Move To Default Table context menu.
-  click a NE-Type to expand a list of all templates associated to the NE-Type in the Alarm Templates table.

Create Template dialog

This dialog is opened when using Create New Template with an Product Name/Templates selected in the Product Name/Template table.

Figure 36 Create template dialog



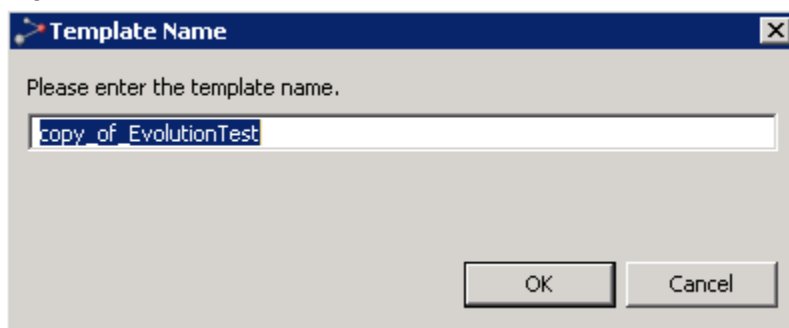
The 'Create Template' dialog box has a title bar with a close button. The main area contains the text 'Create a new alarm template' and a legend '* = Required field'. Below this are three input fields: 'Product Name' with the value 'Evolution', 'Template Name*' which is empty, and 'Description' which is empty. At the bottom right are 'OK' and 'Cancel' buttons.

Enter a name and description of the new template. After pressing OK, you will see the template in the Product Name/Template table under your chosen NE Name.

Template Name dialog

This dialog is opened when using Clone or Rename on an alarm template.

Figure 37 Template Name dialog



The 'Template Name' dialog box has a title bar with a close button. The main area contains the text 'Please enter the template name.' and a single input field with the text 'copy_of_EvolutionTest'. At the bottom right are 'OK' and 'Cancel' buttons.

Enter the name of the new alarm template (if Clone was used) or enter the new name of the existing template (if Rename was used).

Creating a new alarm template

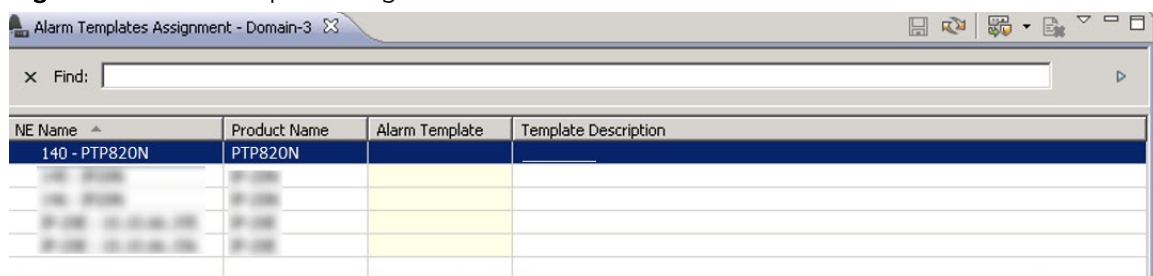
You can create an alarm template anytime, and assign it to a device.

- 1 Open the [Alarm Templates](#) view from the [main](#) menu, by selecting **Views > Fault > Alarm Templates**.
- 2 In the [Alarm Templates](#) table; select the NE-type you want to create a template for, and use the operation [Create Template](#).
- 3 In [the Create Template](#) dialog; enter a **Template Name** (and optionally a **Description**) and then close the dialog by pressing **OK**.
- 4 The new alarm template can now be found in the **Alarm Templates** table in the **Alarm Templates** view. You might need to [expand](#) the NE Type in the table to see the new template.
- 5 Select the new template in the **Alarm Templates** table. Details about the template can now be seen in the [Template Definition](#) area.
- 6 In [the Default](#) table, select each of the alarms you want to modify, and [move](#) to the **Customized** table.
- 7 In the Customized table, for each of the alarms you want to modify, do one or more as follows:
 - Select a new **Severity** from the dropdown
 - Enter a new **Alarm Text**.
 - Block the Alarm by checking the **Blocked** checkbox
- 8 When you have finished updating Alarms, press **Save** to store the updates in the **Alarm Templates** view. The new template is now available for NEs of this NE-type in the [Alarm Templates Assignment](#) view. To assign an alarm template, refer to [Assigning an alarm template to an NE](#)

Alarm Templates Assignment view

This view is opened "[scoped](#)" by selecting any NE or domain in one of the topology views (Geographical or Logical Map or Tree) and selecting **Fault > Alarm Templates Assignment** in the Context or Dropdown menu, or non-scoped by selecting **Views > Fault > Alarm Templates Assignment** from the main menu.

Figure 38 Alarm template assignment view



NE Name	Product Name	Alarm Template	Template Description
140 - PTP820N	PTP820N		

The view is dependent on templates created in the [Alarm Templates](#) view, and the templates assigned to an NE in this view might influence all views where alarms and severities from this NE are displayed.

In this view you can assign alarm templates to all your selected NEs. The templates created in the [Alarm Templates](#) view contain mappings between a set of alarms and severities, alarm text and/or filter conditions. For more details about alarms and severities, see the chapter about [visualization of alarms](#).

We use the term "assign a template to the NE", even though no change is actually made to the NE when assigning an alarm template, the template is solely a mapping within PTP 820 NMS of the incoming alarm from this NE.

Alarm Edit Template Assignment table






The table contains the following columns:

Table 8 Alarm edit template assignment table

Name	Explanation
NE Name	Names of the NEs to which you want to assign a new template to.
Product Name	Type of equipment.
Alarm Template	The short name for the currently selected alarm template. Click the dropdown list to select one of the available alarm templates.
Template Description	A user-defined text describing the purpose of this template.

The table includes all NEs available for the node from which you opened the dialog.

Available operations

-  Click the dropdown menu in the Alarm Template column to select a template for the NE on this line in the table.
-  **Assign Template** Use the context menu in the table to assign an alarm template to one or more NE currently selected in the table.
-  **Clear Assignment** Use the context menu in the table to remove alarm templates from one or more NEs currently selected in the table.
-  **Refresh** Refresh the view so that it is updated with the latest current template assignments from the server.
-  **Save** Apply and save all changes made to template assignments in this view. If this view is closed without saving data, the [Save Changes](#) dialog will appear.

Assigning an alarm template to an NE

To assign an alarm template to an NE:

- 1 Open the [Alarm Templates Assignment](#) view by selecting your NE (or a domain containing this NE) in one of the topology views (**Geographical** or **Logical Map** or **Tree**), and using the menu **Fault > Alarm Template Assignment**.
- 2 On the line containing your NE in the **Alarm Templates Assignment** view; select the new template from the dropdown in the **Alarm Template** column.

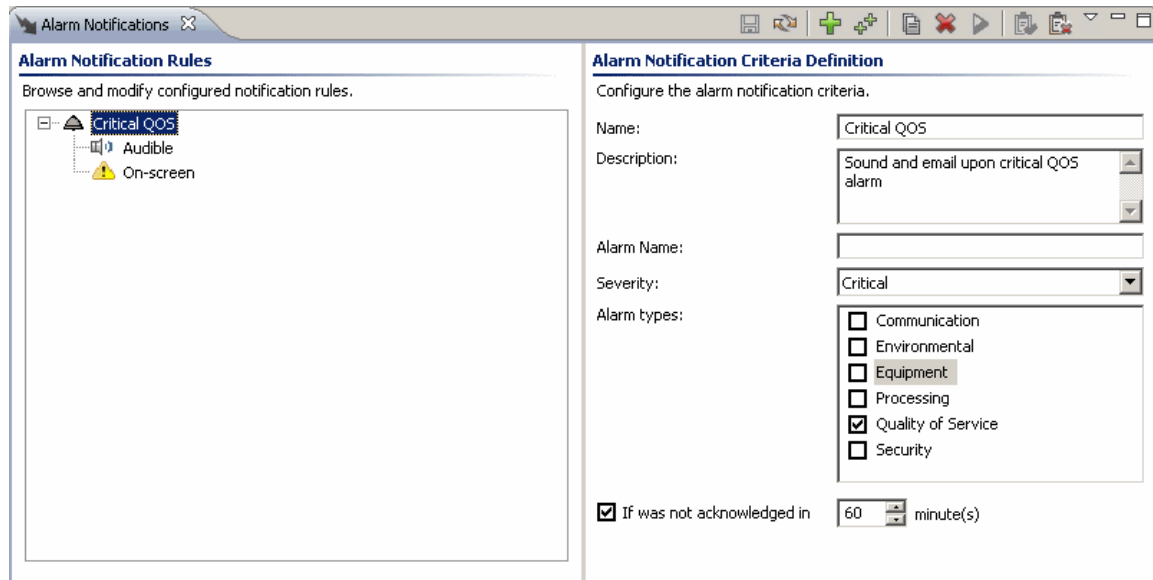
Save your changes in the view.

All affected incoming alarms for this NE will now appear as defined in the assigned alarm template (being blocked, or appearing with a user defined alarm text and/or severity). The result of this alarm customization can be observed in the [Historical Alarms](#) view, [Active Alarms](#) view and all other views where alarms are [visualized](#).

Alarm Notifications view

This view is opened from the main menu under **Views > Fault > Alarm Notifications**.

Figure 39 Alarm template assignment view



In the Alarm Notifications view, you can configure and enable rules for generating [sounds](#) and [e-mails](#) when certain alarms occur in your network. Each alarm notification rule consist of a criterion and a set of targets.

An active alarm notification can be turned off in several ways:

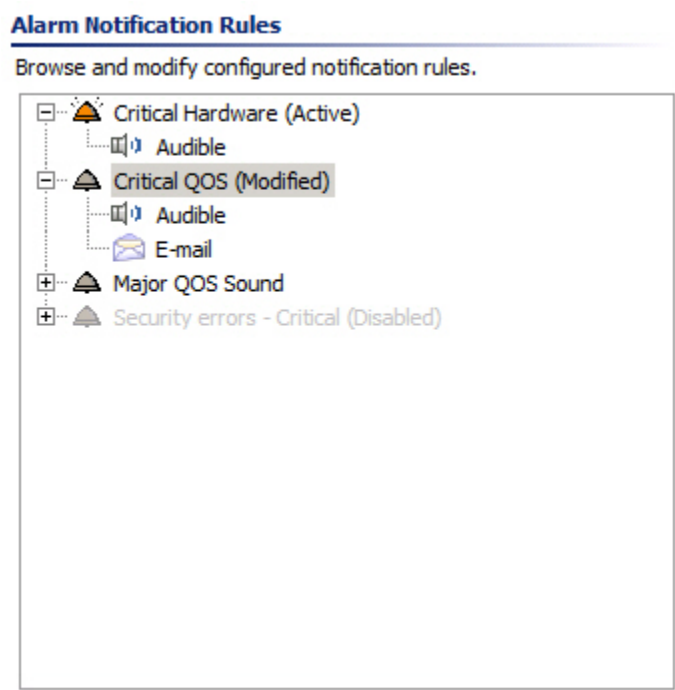
- on the NE/ in the network: make the alarm condition cleared on the element, by removing the (root) cause for the alarm
- in the Active or Historical Alarms view: by [acknowledging](#) the alarm(s) triggering this alarm notification
- in the Geographical or Logical Tree view : by (temporarily) [muting](#) the NE that sent the alarm triggering this alarm notification
- in the Alarm Notification view: by (temporarily) disabling the alarm notification rule, or by deleting or any other way modifying the rule

The view consists of an Alarm Notifications Rules tree containing all the notification rules, and a [Definition area](#) containing the detailed configuration for the currently selected notification criterion or target.

Alarm Notification Rules tree

The tree view lists all alarm notification rules, made from configured notification criteria along with attached notification targets.

Figure 40 Alarm notification rules tree






The tree can contain the following objects:

- An alarm notification criterion.
- An Audible notification target.
- An e-mail notification target.

An alarm notification rule can have different states:

Table 9 Alarm notification rule

Name	Icon	Explanation
Enabled, Inactive		<p>This rule is enabled, but currently not sending any alarms to any targets. An enabled inactive rule is marked by a dark grey node in the Alarm Notification Rules tree. There is several reasons for an enabled rule to be inactive:</p> <p>no alarms are currently fulfilling the criteria defined for this rule, i.e. everything is "normal"</p> <p>no target is currently assigned this rule</p> <p>Please note that only unacknowledged alarms and alarms from unmuted elements can fulfill the criteria for an alarm notification rule.</p>

Name	Icon	Explanation
Enabled, Active		This rule is currently sending notifications to its targets. An active rule is marked by a coloured grey node and suffixed by the text (Active) in the Alarm Notification Rules tree.
Disabled		This rule is prevented from sending notifications to its target. A disabled rule is marked by a light grey node with grey text, suffixed with the text (Disabled) in the Alarm Notification Rules tree.
Modified	 (Modified)	The rule is modified and changes are not yet saved. A modified rule is suffixed by the text (Modified) in the Alarm Notification Rules tree.

Definition area

In the Definition area you can view and modify the definition for the currently selected node in the [Alarm Notifications Rules tree](#).

Alarm Notification Criteria Definition

When an alarm notification criterion is selected in the Alarm Notifications Rules tree, the Alarm Notification Criteria definitions is shown in the Definition area.

Figure 41 Alarm notification criteria definition

Alarm Notification Criteria Definition
 Configure the alarm notification criteria.

Name:

Description:

Severity:

Alarm types:

☐ Communication
☐ Environmental
☒ Equipment
☐ Processing Error
☐ Quality of Service
☐ Security

☒ Include historical alarms

Maximum cleared time: hour(s) minute(s)

An alarm notification criterion defines when notifications should be triggered. An alarm notification criterion can trigger a notification when there exists at least one alarm that meets the criterion. In order to deactivate an alarm notification state, users are supposed to acknowledge the related alarms. Alarms for [muted elements](#) will not trigger a criteria. It is also possible to temporarily [disable](#) a notification rule.

An alarm notification criteria definition contains the following fields:

Table 10 Alarm notification criteria

Name	Explanation
Name	The name of the notification criterion / rule
Description	An optional detailed description for the notification criterion / rule.
Severity	The accepted alarm severity. Alarms with any other severity will always be filtered by this criterion.
Alarm types	The accepted alarm types. Alarms with an alarm type that is not selected here will always be filtered by this criterion.
Include historical alarms	If this option is deselected, all cleared alarms will be filtered by this criterion. If this option is selected, you must specify a maximum time. Alarms that have been cleared for a longer time than this will also be filtered.
Maximum cleared time	Can only be specified if "Include historical alarms" is selected. Defines how old a cleared alarm can be while still meeting the criterion.

Audible Notification Definition area

When an audible notification target is selected in the Alarm Notifications Rules tree, the Audible Notification Definition is shown in the Definition area.

Figure 42 Audible notification definition area

The screenshot shows a dialog box titled "Audible Notification Definition". Below the title bar, it says "Configure the audible notification properties." The dialog contains several fields: "Sound clip:" with a dropdown menu showing "dwuut_short_am" and buttons for "Upload..." and "Play"; "Recipients:" with a list of users and checkboxes; "Delay [seconds]:" with a numeric input field set to "0"; a checked "Loop" checkbox; and "Silence period [seconds]:" with a numeric input field set to "0".

Audible Notification Definition
Configure the audible notification properties.

Sound clip: dwuut_short_am [dropdown] [Upload...] [Play]

Recipients:

- ☒ heinz.sweinbecker
- ☐ silvia.corazon
- ☐ root
- ☒ olivier.ochoa
- ☒ anin.hernandez
- ☐ operator
- ☒ nathalia.ortiz

Delay [seconds]: 0

☒ Loop

Silence period [seconds]: 0

An audible notification is played back as audio within the PTP 820 NMS clients. Each time a new alarm that meets the alarm notification criteria is discovered, the sound will be scheduled to play after a preconfigured delay. If the state becomes inactive again during this time, no sound will be played. It is also possible to configure the sound to loop for as long as the state is active.

An audible notification definition contains the following fields:

Table 11 Audible notification definition

Name	Explanation
Sound clip	Defines which sound to play. Use the dropdown to select one of the sound files that are already uploaded to the PTP 820 NMS server, or press Upload... to browse for and upload a new sound file of type wav. Press Play to listen to the selected sound file.
Recipients	Declares which users the sound should be played for. It is recommended to only select users that are responsible for monitoring and solving alarm related incidents.
Delay	An optional delay, in seconds. No sound will be played if a new alarm is filtered (typically acknowledged) before this delay expires. Use 0 to disable the delay.
Loop	Select this option if audio playing should loop. You must then specify then also specify a silence period.
Silence period	Can only be specified if "Loop" is selected. A value of 0 indicates a normal, continuous loop. A higher value indicates the length of a silence period between play iterations.

The list of sounds that is available from the PTP 820 NMS server in the Sound clip dropdown menu can be maintained in the [Sound files preference page](#). Max file size for a sound is 2Mb. The server can maximum contain 35 sound files in total, including the default sound file PTP820NMSDefault.wav.

Email Notification Definition area

When an e-mail notification target is selected in the Alarm Notifications Rules tree, the E-mail Notification Definition area is shown in the Definitions area.

Figure 43 Email notification definition area

E-mail Notification Definition

Configure the e-mail notification properties.

Format:

Recipients:

[Configure e-mail server](#)

Delay [seconds]:

☒ Send deactivation notifications

☒ Send update notifications

Period [minutes]:

An e-mail notification sends its notifications as e-mails to specified e-mail addresses. For this to work, an outgoing SMTP server must be configured. When the alarm notification state becomes active, an e-mail is scheduled to be sent after a preconfigured delay. If the state becomes inactive again during this time, no e-mail will be sent. If an e-mail notification target is configured to send update notifications, relevant alarm changes that occur while the state is active will be merged into a single e-mail, that is sent periodically. If no changes have occurred during the latest period, no update e-mail will be sent.

An e-mail notification definition contains the following fields:










Table 12 Email notification definition

Name	Explanation
Format	<p>The textual format for sent e-mails. Three different formats can be chosen from the dropdown menu:</p> <p>HTML: a formatted notification, suitable for normal e-mails</p> <p>Plain text: an unformatted notification, suitable normal e-mails</p> <p>SMS compatible text: a short format text that is suited for SMS e-mail gateways. Be aware that this shorter format contains less information and might thus be less helpful.</p>
Recipients	<p>A list of e-mail addresses, to which e-mails shall be sent. You can enter multiple addresses by using "," or ";" as separator. Press Add Recipient... to browse for and add a previously used e-mail address.</p>
Configure e-mail server	<p>Click this link to configure the SMTP server. A valid SMTP configuration is required for e-mail notifications to function.</p>
Delay	<p>An optional delay, in seconds, for sending emails about activated notifications state. No e-mail will be sent if a new alarm is filtered (typically acknowledged) before this delay expires. Use 0 to disable the delay. This delay will not influence deactivation notifications and update notifications.</p>
Send deactivation notifications	<p>If this option is enabled, a deactivation e-mail will sent when the alarm notification state becomes inactive.</p>
Send update notifications	<p>If this option is enabled, update e-mails will be sent periodically, whenever relevant alarm changes have occurred within a period (as defined in the Period field). A relevant alarm change is the discovery of a new alarm that meets the criteria, and the filtering of an alarm that previously met the criteria.</p> <p>If this option is disabled, e-mails will only be sent when the alarm notification state becomes active (and optionally inactive).</p>

Name	Explanation
Period	Can only be specified if Send update notifications is enabled. The update notification period, in minutes. At the end of each period, an e-mail will be sent in case relevant alarm changes occurred during the period.

The e-mail server can also be configured in the [E-mail preference page](#).

Available operations

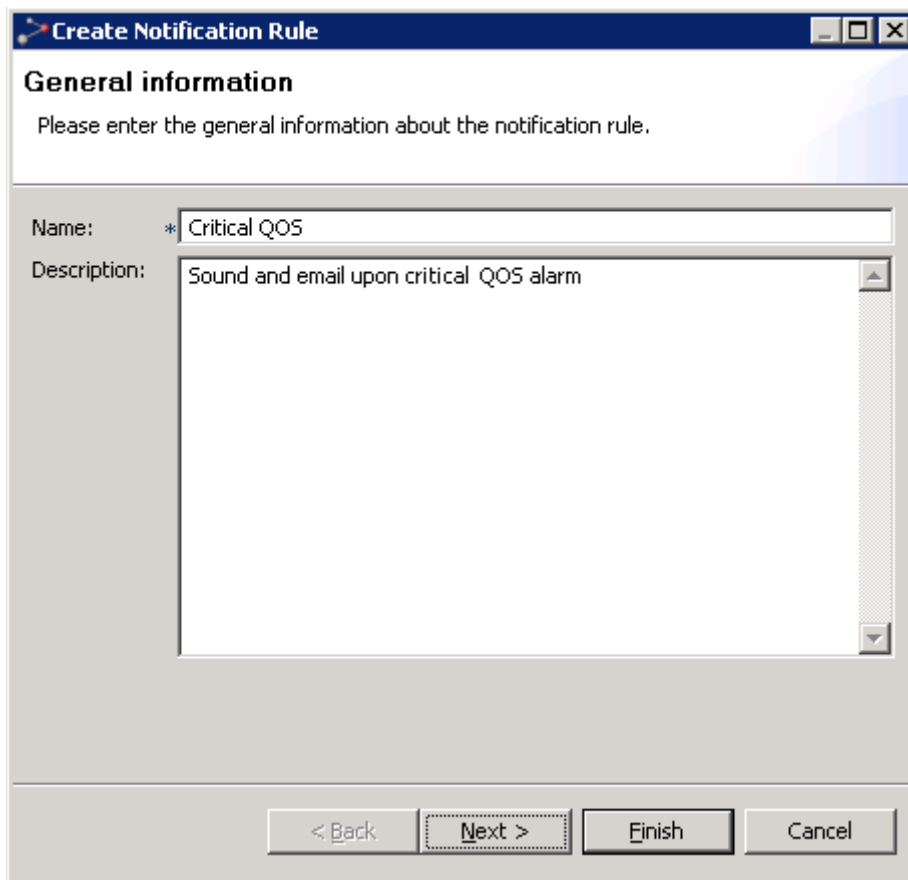
-  Save Modifications that you have made in the Alarm Notifications Rules tree or the Definitions area. If you try to close the view without saving data, the [Save Changes dialog](#) will appear.
-  Refresh the view with the latest configuration from the server. Any modifications that you have made will be lost.
-  Create criterion, by starting the [Create Criterion wizard](#). A notification criterion and associated notification targets can be created.
-  Add targets to the selected notification criterion, by starting the [Add Notification Targets wizard](#).
-  Clone the selected notification criteria and any attached notification targets.
-  Remove the selected notification criteria and notification targets.
-  Test the configuration of the selected notification target by sending a test notification. Only applicable for e-mail notifications.
-  Enable the selected notification criteria. Note that you must still save the view for this change to be applied.
-  Disable the selected notification criteria. Note that you must still save the view for this change to be applied

Create Notification Criterion wizard

When you perform the Create Criterion operation, a Create Notification Criterion wizard will be launched.

1 - General

Here you specify the general information about the criteria that you are about to create.

Figure 44 General information

The screenshot shows a Windows-style dialog box titled "Create Notification Rule". The "General information" tab is selected, and the instruction "Please enter the general information about the notification rule." is displayed. Below this, there are two input fields: "Name:" with a required field indicator (*) and "Description:". The "Name" field contains the text "Critical QOS", and the "Description" field contains the text "Sound and email upon critical QOS alarm". At the bottom of the dialog, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

Create Notification Rule

General information

Please enter the general information about the notification rule.

Name: * Critical QOS

Description: Sound and email upon critical QOS alarm

< Back Next > Finish Cancel

Add values for Name and Description as described under [Alarm Notification Criteria definition](#). Then press Next to continue, or Cancel to abort the wizard.

2 - Criteria configuration.

Here you configure the actual criteria.

Figure 45 Criteria information

Create Notification Rule

Notification criteria configuration

Please define the conditions for this notification criteria.

Severity: Critical

Alarm types:

- ☐ Communication
- ☐ Environmental
- ☐ Equipment
- ☐ Processing
- ☒ Quality of Service
- ☐ Security

☒ Include historical alarms

Maximum cleared time: 8 hour(s) 0 minute(s)

< Back Next > Finish Cancel

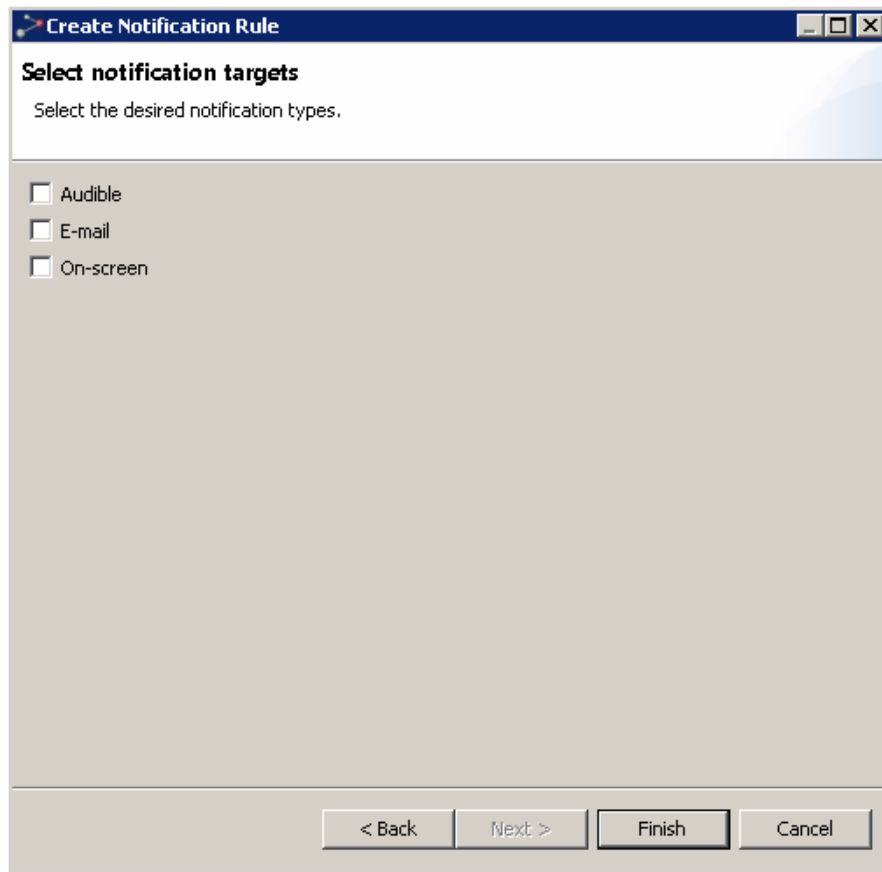
Add/update values for Severity, Alarm types, Include historical alarms and Maximum cleared time as described under [Alarm Notification Criteria definition](#).

Then press Next to save the notification criteria and continue, or Cancel to abort the wizard.

3 - Select notification targets.

Here you can select what notification targets you desire.

Figure 46 Select notification target



Select one or more target and press Next to continue, or Cancel to abort adding any targets.

4 - Audible notification configuration.

This step is only shown if you selected to add an audible notification target.

Figure 47 Audible notification configuration

Create Notification Rule

Audible notification configuration

Please configure how the audible notifications should be played.

Sound clip: *NMSDefault.wav Upload... Play

Recipients:

- ☒ root
- ☐ services_R
- ☐ services_RW

*

Delay [seconds]: 0

☒ Loop

Silence period [seconds]: 60

< Back Next > Finish Cancel

Add/update values for Sound clip, Recipients, Delay, Loop and Silence period as described under [Audible Notification Definition](#).

Then press Next to add e-mail notification target, or Cancel to abort.

5 - E-mail notification configuration.

This step is only shown if you selected to add an e-mail notification target.

Figure 48 Email notification configuration

Create Notification Rule

E-mail notification configuration

⚠ No e-mail server is defined.

Format: HTML

Recipients: *247callcenter@teletele.com

Add Recipient...

Configure e-mail server

Delay [seconds]: 0

☒ Send deactivation notifications

☒ Send update notifications

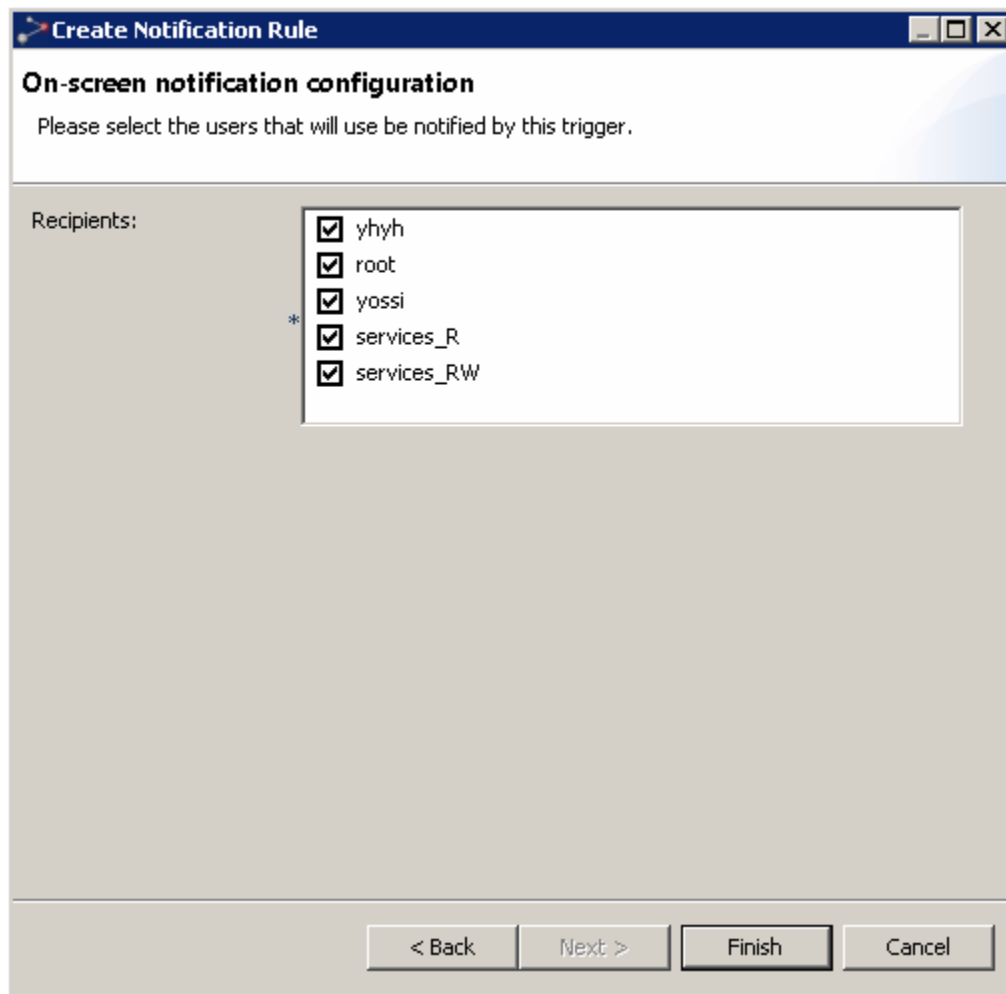
Period [minutes]: 15

< Back Next > Finish Cancel

Add/update values for Format, Recipients, Configure e-mail server, Delay, Send deactivation notifications, Send update notifications and Period as described under [Email Notification Definition](#).

6 On-screen notification configuration.

This step is only shown if you selected to add an on-screen notification target.




Add/update values for **Recipients** as described under [On-screen Notification Definition area](#). Then press **Finish** to complete wizard or **Cancel** to abort.

Add Notifications Targets wizard

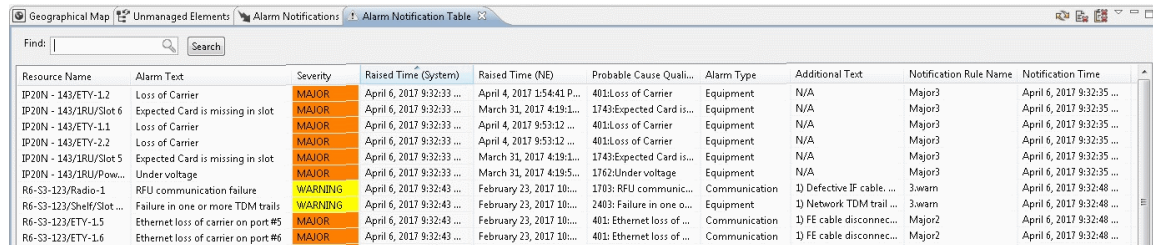
When you perform the Add Targets operation, an Add Notification Targets wizard will be launched. The steps in this wizard are the same as in the [Create Notification Criterion wizard](#), starting from the step [Select Notification Targets](#). If only one notification target is available for selection, then the step for selecting notification targets is skipped in this wizard.

Alarm Notification Table view

This view is opened from the main menu under **Views > Fault > Alarm Notifications**, or by clicking the on-screen notification icon  in the statusbar.

The table displays alarm notifications for alarms that meet the [On-screen Notifications](#) criteria of [Error! Reference source not found. Rules](#). That is, the alarms were not acknowledged within the number of minutes defined in the Alarm Notification Rule.

Note that the table displays up to 5000 of the most recent entries.



Resource Name	Alarm Text	Severity	Raised Time (System)	Raised Time (NE)	Probable Cause Qualifier	Alarm Type	Additional Text	Notification Rule Name	Notification Time
IP20N - 143/ETY-1.2	Loss of Carrier	MAJOR	April 6, 2017 9:32:33 ...	April 4, 2017 1:54:41 P...	401:Loss of Carrier	Equipment	N/A	Major3	April 6, 2017 9:32:35 ...
IP20N - 143/IRU/Slot 6	Expected Card is missing in slot	MAJOR	April 6, 2017 9:32:33 ...	March 31, 2017 4:19:1...	1743:Expected Card is...	Equipment	N/A	Major3	April 6, 2017 9:32:35 ...
IP20N - 143/ETY-1.1	Loss of Carrier	MAJOR	April 6, 2017 9:32:33 ...	April 4, 2017 9:53:12 ...	401:Loss of Carrier	Equipment	N/A	Major3	April 6, 2017 9:32:35 ...
IP20N - 143/ETY-2.2	Loss of Carrier	MAJOR	April 6, 2017 9:32:33 ...	April 4, 2017 9:53:12 ...	401:Loss of Carrier	Equipment	N/A	Major3	April 6, 2017 9:32:35 ...
IP20N - 143/IRU/Slot 5	Expected Card is missing in slot	MAJOR	April 6, 2017 9:32:33 ...	March 31, 2017 4:19:1...	1743:Expected Card is...	Equipment	N/A	Major3	April 6, 2017 9:32:35 ...
IP20N - 143/IRU/Power...	Under voltage	MAJOR	April 6, 2017 9:32:33 ...	March 31, 2017 4:19:5...	1762:Under voltage	Equipment	N/A	Major3	April 6, 2017 9:32:35 ...
R6-S3-123/Radio-1	RFU communication failure	WARNING	April 6, 2017 9:32:43 ...	February 23, 2017 10...	1703: RFU communic...	Communication	1) Defective IF cable. ...	3swam	April 6, 2017 9:32:48 ...
R6-S3-123/Shelf/Slot...	Failure in one or more TDM trails	WARNING	April 6, 2017 9:32:43 ...	February 23, 2017 10...	2403: Failure in one o...	Equipment	1) Network TDM trail ...	3swam	April 6, 2017 9:32:48 ...
R6-S3-123/ETY-1.5	Ethernet loss of carrier on port #5	MAJOR	April 6, 2017 9:32:43 ...	February 23, 2017 10...	401: Ethernet loss of ...	Communication	1) FE cable disconnec...	Major2	April 6, 2017 9:32:48 ...
R6-S3-123/ETY-1.6	Ethernet loss of carrier on port #6	MAJOR	April 6, 2017 9:32:43 ...	February 23, 2017 10...	401: Ethernet loss of ...	Communication	1) FE cable disconnec...	Major2	April 6, 2017 9:32:48 ...

Alarm Notification table




The table displays the following fields for each alarm notification:

Name	Explanation
Resource Name	Source of alarm - the network resource that generated the alarm.
Alarm Text	Gives the most likely reason for the alarm. Similar to "Native Probable Cause", as defined in TMF608. This is a textual description of the cause of the alarm, displayed exactly as sent from the NE or portrayed in the EMS user interface. The text can be customized using the Alarm Templates view.
Severity	One of the possible alarm severities: CRITICAL, MAJOR, MINOR, WARNING, INDETERMINATE or INFO. Severities can be customized using the Alarm Templates view.
Raised Time (System)	The time on the PTP 820 NMS system when the alarm was raised.
Raised Time (NE)	The time on the NE when the alarm was raised.
Probable Cause Qualifier	A code for identifying the alarm, e.g. used in the Alarm Templates view.
Alarm Type	One of the following types: Equipment, Communication, Environmental, Processing Error, Quality Of Service or Security.

Additional Text	Free form text description of the alarm.
Notification Rule Name	The name of the Alarm Notification Rule that met the criteria for sending the alarm notification.
Notification Time	The time when the alarm notification was sent.




Available operations

The following operations are available in the table, in addition to the standard toolbar icons.

-  **Refresh** Refresh the entire table and update it.
-  **Clear the selected alarm notifications** - Delete the selected alarm notifications from the table. This clears the selected alarm notifications for all users.
-  **Clear all alarm notifications in the view** - Delete all alarm notifications from the table. This clears all alarm notifications for all users.

Available statusbar operations

The following additional operations are available from the [Statusbar](#).

-  The **Notifications** area appears in red if there are un-viewed alarms in the [Alarm Notification Table view](#). The number of un-viewed alarms is also listed.
-  Clicking this Alarm Notification button opens the [Alarm Notification Table view](#). The icon appears yellow if there are un-viewed alarms in the table.
-  Clicking this icon opens the [Alarm Notifications view](#). The icon appears red if a Notification rule was disabled because over 1000 alarms a minute match the rule. In such a case, click the icon to open the [Alarm Notifications view](#) and modify the rule criteria.

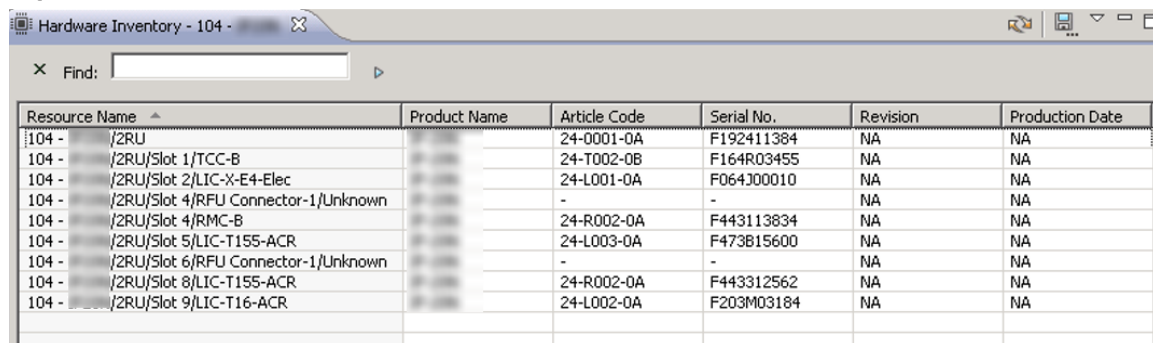
Configuration

Hardware Inventory view

This view is opened by selecting any node in one of the topology views and selecting Configuration | Hardware Inventory from the Context or View dropdown menu. The view will then open with the selection as a [scope](#) - presenting only hardware for the currently selected NE/nodes/subdomain, as shown below:

Alternatively, you can open the view unscoped by opening Views | Configuration | Hardware Inventory from the main menu. The view will then present hardware data from the entire network in the same table. Please note that the time consumed for this operation is a function of the number of nodes and resources per node in the network, and might cause a delay if your network is large. Opening the view without (or with a large) scope should only be done after careful consideration of the size and complexity of your network.

Figure 49 Hardware inventory view



Resource Name	Product Name	Article Code	Serial No.	Revision	Production Date
104 - /2RU		24-0001-0A	F192411384	NA	NA
104 - /2RU/Slot 1/TCC-B		24-T002-0B	F164R03455	NA	NA
104 - /2RU/Slot 2/LIC-X-E4-Elec		24-L001-0A	F064J00010	NA	NA
104 - /2RU/Slot 4/RFU Connector-1/Unknown		-	-	NA	NA
104 - /2RU/Slot 4/RMC-B		24-R002-0A	F443113834	NA	NA
104 - /2RU/Slot 5/LIC-T155-ACR		24-L003-0A	F473B15600	NA	NA
104 - /2RU/Slot 6/RFU Connector-1/Unknown		-	-	NA	NA
104 - /2RU/Slot 8/LIC-T155-ACR		24-R002-0A	F443312562	NA	NA
104 - /2RU/Slot 9/LIC-T16-ACR		24-L002-0A	F203M03184	NA	NA

This view is normally used together with the topology views (Geographical or Logical Map or Tree), and gives you an overview of the currently available hardware elements in the NE that was selected when opening the view.

"Hardware elements" refers to physical equipment in the NE, and varies a lot for the different types of NE, such as cards, interfaces, modules, boards and chips. The data in the table is gathered from the NE as the view is opened, and current status of the hardware can be updated by refreshing the table.

Hardware Inventory table

The table displays the following fields for each NE:





Table 13 Hardware inventory table

Name	Explanation
Resource Name	Name/location of this hardware element in the NE.
Product Name	Product name of the network element.
Article Code	Uniquely identifies the type of hardware element.

Name	Explanation
Serial no.	The serial number of the hardware element.
Revision	The hardware revision.
Production date	When the production process was completed for this hardware element.

Available operations

The following operations are available in the table, in addition to the standard toolbar icons.

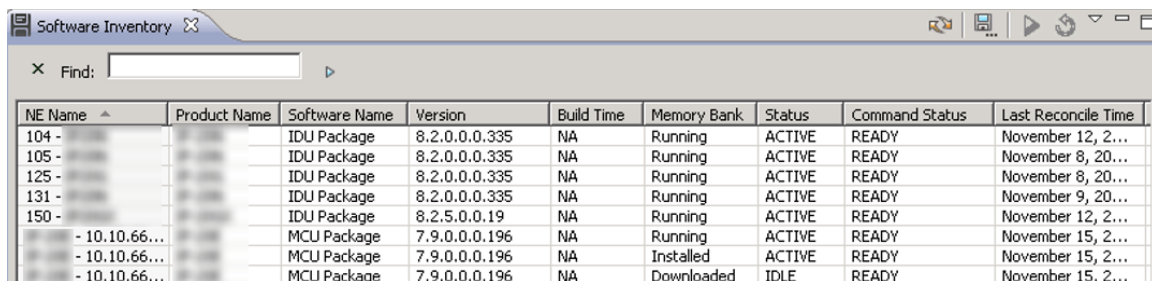
-  Refresh Refresh the entire table and update the status of the equipment.
-  Customize Columns Open the [Column Customize](#) dialog for the Hardware Inventory table, where you can select which column to display and the order of the columns.
-  Show Quick Search Enable the [Quick Search](#) field in the Hardware Inventory view. The quick search functionality makes it possible to search the contents of the view. All visible columns can be searched
-  Export to File... Export the current data to file. The table can be saved as an Excel spreadsheet (.xls), comma separated file (.csv) or extended markup language (.xml)

Software Inventory view

The view is opened by selecting an NE or domain node in one of the topological views and selecting **Configuration > Software Inventory** in the Context or View dropdown menus. The view will then open with the selection as a [scope](#) presenting only software for the currently selected NEs, as shown below:

Alternatively, you can open the view unscoped by selecting **Views > Configuration > Software Inventory** from the main menu. The view will then present software data from the entire network in the same table. Please note that the time consumed for this operation is a function of the number of nodes and resources per node in the network, and might cause a delay if your network is large. Opening the view without (or with a large) scope should only be done after careful consideration of the size and complexity of your network.

Figure 50 Software inventory view



NE Name	Product Name	Software Name	Version	Build Time	Memory Bank	Status	Command Status	Last Reconcile Time
104 -		IDU Package	8.2.0.0.0.335	NA	Running	ACTIVE	READY	November 12, 2...
105 -		IDU Package	8.2.0.0.0.335	NA	Running	ACTIVE	READY	November 8, 20...
125 -		IDU Package	8.2.0.0.0.335	NA	Running	ACTIVE	READY	November 8, 20...
131 -		IDU Package	8.2.0.0.0.335	NA	Running	ACTIVE	READY	November 9, 20...
150 -		IDU Package	8.2.5.0.0.19	NA	Running	ACTIVE	READY	November 12, 2...
- 10.10.66...		MCU Package	7.9.0.0.0.196	NA	Running	ACTIVE	READY	November 15, 2...
- 10.10.66...		MCU Package	7.9.0.0.0.196	NA	Installed	ACTIVE	READY	November 15, 2...
- 10.10.66...		MCU Package	7.9.0.0.0.196	NA	Downloaded	IDLE	READY	November 15, 2...

This view is normally used together with the topological views (Geographical or Logical Map, or Tree) and the [Software Download Jobs](#) view.

This view shows a table containing all available software memory banks for your NE. Each line displays the status of a memory bank and details about the software stored on this bank. Select a memory bank in the table to activate idle software or reset active software. The data in the table is gathered from the NE as the view is opened, and current status of the software can be updated by refreshing the table.

Rereading the Software Inventory is possible through Configuration | Reconcile SW Inventory. This is a scoped action, only available on the element node in the topology views.

The memory banks presented in the table are normally in one of the following categories:

- IDU flash banks: These memory banks normally appear in pairs, with one bank running while the other bank is idle. One bank will be labeled "active", containing the software currently running, and the other will normally be labeled "idle", containing software the user can switched to or overwrite during a software download.
- ODU flash banks: These memory banks contain software running on the ODU, but are located on the IDU. Similarly, to the IDU flash banks, software can be downloaded to an "idle" memory bank and then activated on the ODU.
- non-flash banks: These memory banks are not configurable and contain software that cannot be replaced.
- boot banks. These memory banks are not configurable by the software download process in PTP 820 NMS.

Jobs for downloading new software to memory banks on your NE are managed in the [Software Download Jobs](#) view, and created with the [Create Software Download Jobs](#) wizard.

Software Inventory Table

The table presents the following fields for each memory bank on the NE:







Table 14 Software inventory table

Name	Explanation
Software Name	The name of the software in this memory bank, as read from the NE.
NE Name	The name of the NE where this software is stored.
Product Name	Product name of the network element.
Version	Software revision. Normally a five character code, but the field will display NA if the system has this unit present but is unable to retrieve the information from it.
Build Time	When this software was created.
Memory Bank	Software location on the NE

Name	Explanation
Status	<p>Displays the status of the memory bank and can be one of the following values</p> <p>IDLE: Software is not being executed</p> <p>ACTIVE: Software is being executed</p> <p>ACTIVE_PENDING: Software is waiting to be executed (will be activated on next restart)</p> <p>DOWNLOADING: SW is being downloaded to this bank.</p> <p>ERASING FLASH: SW is being erased (during a download process)</p> <p>INVALID: corrupt software or wrong software version; SW Download has failed or SW bank has not been used.</p> <p>NOT_AVAILABLE: The IDU does not have contact with the unit using this software (only relevant for ODU banks) or corrupted memory bank</p>
Command Status	Displays the status of the software in the memory bank - whether the bank is currently busy running commands or not.
Last Reconcile Time	Displays when the software inventory was last reconciled (received from the element).

When downloading new software on an NE, one of the idle banks will be used for storing the new software. When downloading has completed successfully this bank can be activated and the other bank will become idle.

Available operations

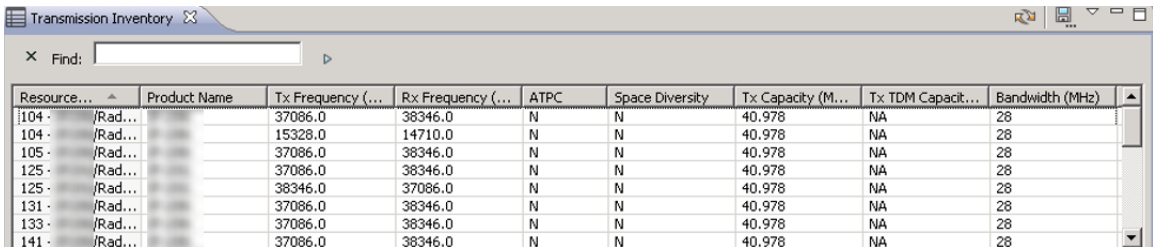
-  **Activate Software** Activate the currently selected software for the NE. This menu option will only be available for software that is ready on idle flash banks.
-  **Reset Software** Resets the currently selected software for the NE. This menu option will only be available for software that is ready on active flash banks.
-  **Refresh View** Refresh the list of software with the latest data from the NE.
-  **Customize Columns** Open the [Column Customize](#) dialog for the Software Inventory table, where you can select which column to display and the order of the columns.
-  **Show Quick Search** Enable the [Quick Search](#) field in the Software Inventory view. The quick search functionality makes it possible to search the contents of the view. All visible columns can be searched.
-  **Export to File...** Export the current data to file. The table can be saved as an Excel spreadsheet (.xls), comma separated file (.csv) or extended markup language (.xml)

Transmission Inventory View

The view is opened by selecting an NE or domain node in one of the topological views and then selecting **Configuration > Transmission** Inventory in the Context or View dropdown menus. A scoped view appears presenting only the transmission information for the currently selected NEs, as shown in the figure below.

Alternatively, you can open the view unscoped by selecting **Views > Configuration > Transmission Inventory** from the main menu. The view presents transmission data from the entire network of device nodes in the same table. Please note that the time consumed for this operation is a function of the number of device nodes and resources per node in the network, so opening an unscoped view may take some time if your network is large. Opening the view unscoped, or scoped to a large number of devices, should only be done after careful consideration of the size and complexity of your network.

Figure 51 Transmission inventory view



Resource...	Product Name	Tx Frequency (...)	Rx Frequency (...)	ATPC	Space Diversity	Tx Capacity (M...	Tx TDM Capacit...	Bandwidth (MHz)
104 -	/Rad...	37086.0	38346.0	N	N	40.978	NA	28
104 -	/Rad...	15328.0	14710.0	N	N	40.978	NA	28
105 -	/Rad...	37086.0	38346.0	N	N	40.978	NA	28
125 -	/Rad...	37086.0	38346.0	N	N	40.978	NA	28
125 -	/Rad...	38346.0	37086.0	N	N	40.978	NA	28
131 -	/Rad...	37086.0	38346.0	N	N	40.978	NA	28
133 -	/Rad...	37086.0	38346.0	N	N	40.978	NA	28
141 -	/Rad...	37086.0	38346.0	N	N	40.978	NA	28

The following table presents the transmission information available in this view.

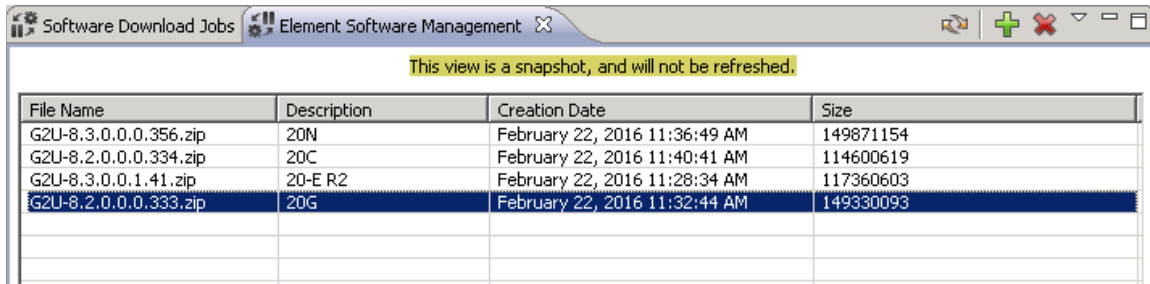
Table 15 Transmission inventory view information

Name	Explanation
Resource Name	The radio interface.
Product Name	The product name of the network element.
Tx Frequency (MHz)	The transmission radio frequency of the radio interface.
Rx Frequency (MHz)	The received radio frequency of the radio interface.
ATPC	Indicates whether ATPC is configured on the interface.
Space Diversity	Indicates whether Space Diversity is configured on the interface.
Tx Capacity (Mb/sec)	The available transmission capacity.
Tx TDM Capacity (Mb/sec)	The available received TDM capacity (not provided for PTP820 equipment)
Bandwidth (MHz)	The bandwidth of the radio interface

Element Software Management

This view can be opened from **Views > Configuration > Element Software Management** in the main menu.

Figure 52 Element Software Management



File Name	Description	Creation Date	Size
G2U-8.3.0.0.0.356.zip	20N	February 22, 2016 11:36:49 AM	149871154
G2U-8.2.0.0.0.334.zip	20C	February 22, 2016 11:40:41 AM	114600619
G2U-8.3.0.0.1.41.zip	20-E R2	February 22, 2016 11:28:34 AM	117360603
G2U-8.2.0.0.0.333.zip	20G	February 22, 2016 11:32:44 AM	149330093

In this view you can upload files from an external FTP server to the PTP 820 NMS server. For example, you may wish to upload an updated software version for the purpose of updating device software.

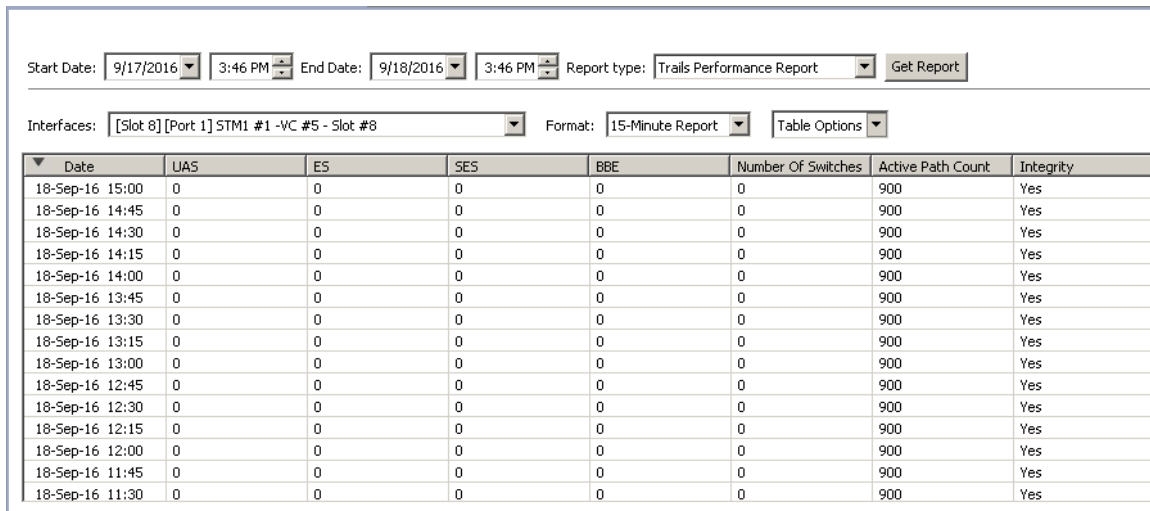
As prerequisites, you need to:

- Install an external FTP/SFTP server on the same machine as the PTP 820 NMS server. Refer to [Generating a TDM Trail report](#)
- [To generate the](#) report via CLI, refer to Generating Performance reports using a CLI command.

To generate the report using the GUI, refer to Generating Performance reports via the GUI.

Viewing a TDM Trail report

The following is an example of a 15-minute TDM Trails performance report:



Date	UAS	ES	SES	BBE	Number Of Switches	Active Path Count	Integrity
18-Sep-16 15:00	0	0	0	0	0	900	Yes
18-Sep-16 14:45	0	0	0	0	0	900	Yes
18-Sep-16 14:30	0	0	0	0	0	900	Yes
18-Sep-16 14:15	0	0	0	0	0	900	Yes
18-Sep-16 14:00	0	0	0	0	0	900	Yes
18-Sep-16 13:45	0	0	0	0	0	900	Yes
18-Sep-16 13:30	0	0	0	0	0	900	Yes
18-Sep-16 13:15	0	0	0	0	0	900	Yes
18-Sep-16 13:00	0	0	0	0	0	900	Yes
18-Sep-16 12:45	0	0	0	0	0	900	Yes
18-Sep-16 12:30	0	0	0	0	0	900	Yes
18-Sep-16 12:15	0	0	0	0	0	900	Yes
18-Sep-16 12:00	0	0	0	0	0	900	Yes
18-Sep-16 11:45	0	0	0	0	0	900	Yes
18-Sep-16 11:30	0	0	0	0	0	900	Yes

The TDM Trails report applies to TDM Trails on PTP820 devices.

The counters are collected only at the TDM Service Points, whether they are service endpoints or on the path of the service.

The following TDM service fragments are included in this report:

- TDM to Radio cross-connection points.
- TDM to TDM Cross-Connects.
- TDM to 2 Radio Cross-Connects, for Trails with protection.
- Radio to 2 Radios Cross-Connects , for Trails with protection, where the protection begins at a mid-point on the trail.
- TDM to 1 TDM and 1 Radio Cross-Connects, for Trails with protection where one network path is going over an STM-1 link (User link), while the other path is over the radio.

Reports are supported only for service configurations that can be created by PTP 820 NMS.

All discovered services on PTP820 equipment appear in the report. Note that the services need not be confirmed, discovery alone is sufficient. PTP 820 NMS generates a report for all trails that are in its database, regardless of the state of the trail (confirmed or unconfirmed).

If there is no PM data in the database for a trail, that trail does not appear in the report.

For each port on the path of the service, the following counters are displayed.

Table 2 Counters in TDM Trail report

Counter	Value in Summary Report
UAS	
ES	
SES	
BBE	Radio performance counters
Note: On the PTP820 , the BBE field is called FC but in the report the column is always labeled BBE whether for PTP820.	
Number of Switches	When there is no protection and/or for PTP820 devices, this value is zero.
Active Path Count	When there is no protection and/or for PTP820 devices, this value is set to either 0 (no service) or 900 (full service).

Note:

In the case of an STM-1 Group, the counters are gathered per each physical slot, separately.

The report will contain two tables and you must check which is the active card.



- Install and configure an FTP or SFTP server.
- Configure PTP 820 NMS with the FTP/SFTP server settings, using the [Preferences: External FTP/SFTP Server](#) page.

Software Download Jobs

Table 16 Software Download Jobs

Name	Explanation
File Name	The name of the file you uploaded from the FTP/SFTP server to the PTP 820 NMS server.
Description	The description you gave when uploading the file.
Creation Date	The date and time when file upload occurred.
Size	The size of the uploaded file.

Available Operations

-  Upload Software File - Upload a file from the FTP/SFTP server to the PTP 820 NMS server. Refer to [Uploading Software Files to the PTP 820 NMS Server](#).
-  Delete Selected Software File - delete the selected file from the PTP 820 NMS server.

Uploading Software Files to the PTP 820 NMS Server


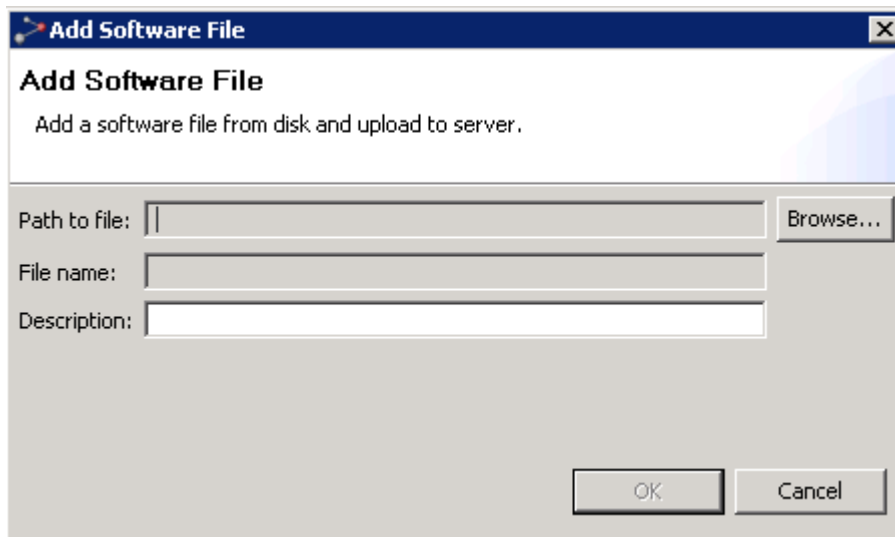
This option is opened by clicking the Upload Software File  button in the Element Software Management view.

Figure 53 Upload Software File to PTP 820 NMS Server



Add Software File

Add a software file from disk and upload to server.

Path to file:

File name:

Description:

Enter information about the file to upload, and a description in the Description field.

Press **OK**. A progress Information window appears, indicating the progress of the upload operation. When upload is completed, a message appears.

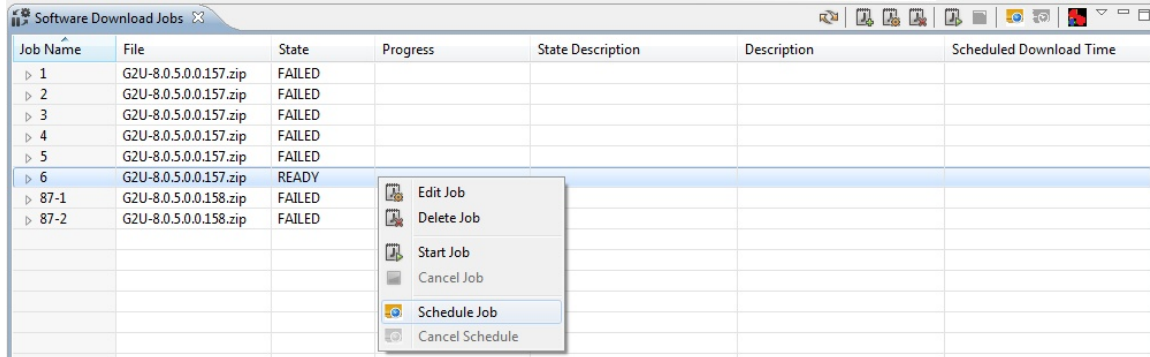
The uploaded file then appears in the Element Software Management view.

Software Download Jobs view

This view can be opened from Views | Configuration | Software Download Jobs in the main menu.

The view will also open whenever a job is created with the [Create Software Download Jobs](#) wizard, which is opened by selecting any domain or NE in one of the topological views and then selecting Configuration | Create Software Download Job in the context menu.

Figure 54 Software download jobs view



Job Name	File	State	Progress	State Description	Description	Scheduled Download Time
1	G2U-8.0.5.0.0.157.zip	FAILED				
2	G2U-8.0.5.0.0.157.zip	FAILED				
3	G2U-8.0.5.0.0.157.zip	FAILED				
4	G2U-8.0.5.0.0.157.zip	FAILED				
5	G2U-8.0.5.0.0.157.zip	FAILED				
6	G2U-8.0.5.0.0.157.zip	READY				
87-1	G2U-8.0.5.0.0.158.zip	FAILED				
87-2	G2U-8.0.5.0.0.158.zip	FAILED				

In this view you can manage and monitor software download jobs created with the Create Software Download Jobs wizard. The view contains a list of all software, including which NEs are included in each job. You are allowed to create new jobs, to modify unstarted jobs, and to start and stop jobs.

In the [Software Inventory](#) view you can see the current content of each memory bank on the NE: the software versions contained in the bank, the command status of the software and the idle/active status of the bank. When you have started downloading a software component to an NE, the download process will determine if one of the idle flash memory banks is suitable for this software version. If the software was transmitted OK, the idle software component will be replaced, and the new software can be activated using the Software Inventory view.








Please note that the term "download" is from the NE's point of view, not from the network manager. From the network manager's point of view, the download process handled by this view is considered an upload. Downloading from the NE to the network manager (e.g. downloading a backup of your NE's software from a memory bank) is not supported by this network management system.


Before running a Software Download job, please read [How to download software to an NE](#) for more information about the Software Download process.

Table 17 Software Download Jobs Table

Name	Explanation
Job Name	A name identifying each job and each of the NEs involved in this job. Click the plus sign to expand the list of NEs.
File	The name of the file you want to upload to the NE.
State	One of the following states: <ul style="list-style-type: none"> • INCOMPLETE The Create Software Download Jobs wizard is not finished and more data must be provided in order to run this job. • READY The job can be started • SCHEDULED FOR DOWNLOAD The job is scheduled for a future date and time. • RUNNING The job has been started • DONE The job has been completed successfully • FAILED job has failed
Progress	Displays a progress indicator for the job on each of the NEs downloading software.
State Description	Provides information about the current state of job.
Description	Details about the job.
Scheduled Download Time	The time when download is scheduled to occur. This is relevant when a job is scheduled for a future date and time.

Available operations

-  **Create Software Download Job** Create a new job by opening the [Create Software Download Jobs](#) wizard and selecting NEs from the entire network.
-  **Edit Job** Update the selected job by opening the Create Software Download Jobs wizard for this job. Now you can rename the job, add/remove NEs that are to receive software in this job or select another software file for downloading.
-  **Delete Job** Remove the selected job. Only possible if the job is not currently running.
-  **Start Job** Start the selected job. Only possible if the job is ready.
-  **Cancel Job** Abort the selected job. Only possible if the job is already running.
-  **Schedule Job** Schedule a future date and time for running the job.
-  **Cancel Schedule** Cancel the previously scheduled date and time.

-  **FTP/SFTP Server Status** Display the status of the FTP/SFTP server: whether the server is up, and whether server parameters are defined.

Create Software Download Jobs wizard

This wizard is opened by selecting **Create Software Download Job** in the menu in the [Software Download Jobs](#) view. The wizard will then allow you to create software download jobs for all available NEs in all domains in both geographical and logical models.

Alternatively the wizard can be opened "[scoped](#)", by selecting any domain or NE in one of the topological views (**Geographical, Logical Tree or Map**), and then selecting **Configuration > Create Software Download Job** from the menu. The wizard will then only allow you to create software download jobs for the available NEs within the selected scope.

This is a wizard for creating jobs for downloading software from the network management system to NEs.

When a job is created in this wizard, it must be started manually in the [Software Download Jobs](#) view. Here you can also monitor the progress of each job. The download process will locate an idle memory bank on the NE where the new software will be stored. If no idle memory bank suitable for your software is found on the NE where you try to download the software, the download process will fail. When the download has completed correctly, the new software can be activated in the [Software Inventory](#) view.

Please note that the wizard can be saved at any step by pressing the **Finish** button, even when the software download job is incomplete. The job will then appear in the job list in the **Software Download Jobs** view and its state will be INCOMPLETE. The wizard can be resumed at any time by selecting **Edit Job** in the **Software Download Jobs** view. This allows you to update job information, select/de-select NEs and/or change the software file to upload.

Create Software Download Jobs wizard - Basic information (Page 1)**Figure 55** Software download jobs - basic information

Create Software Download Job

Software Download Job - Basic information (Page 1/3)

Please enter common job parameters

Job name
PTP820E

Description
[Blurred text]

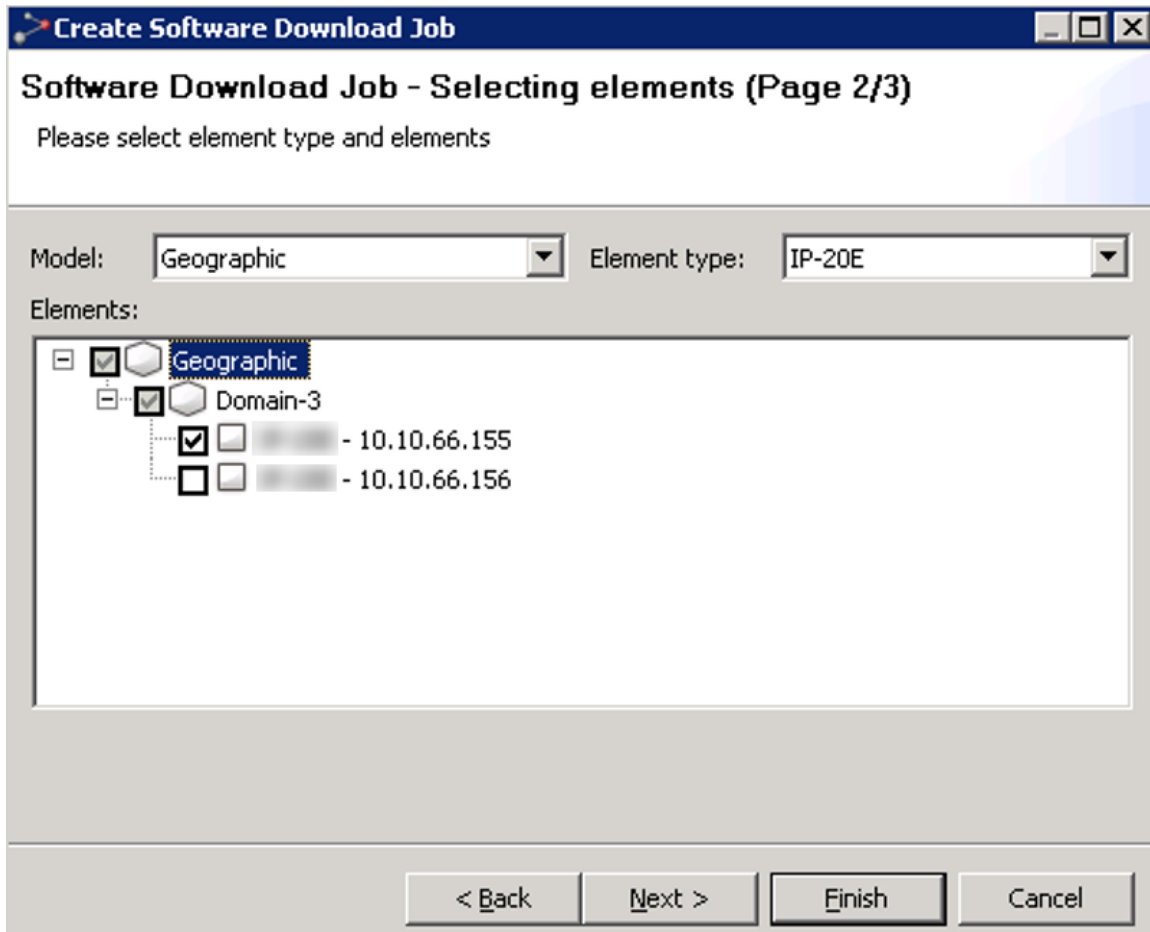
< Back Next > Finish Cancel

In this step you can enter information about the job.

Enter a name in the Job Name field which can identify this job, and more detailed information about this job in the optional Description field. Press Next when sufficient job information has been entered.

Create Software Download Jobs wizard - Selecting elements (Page 2)

Figure 56 Software download jobs – selecting elements



In this step you can select the NE to download new software to.

Use the Model dropdown menu to switch between the Geographical and Logical model. Use the Element type dropdown menu to display NEs of a different NE type in the tree. Click nodes in the Elements tree to select/de-select domains and NEs to download software to.

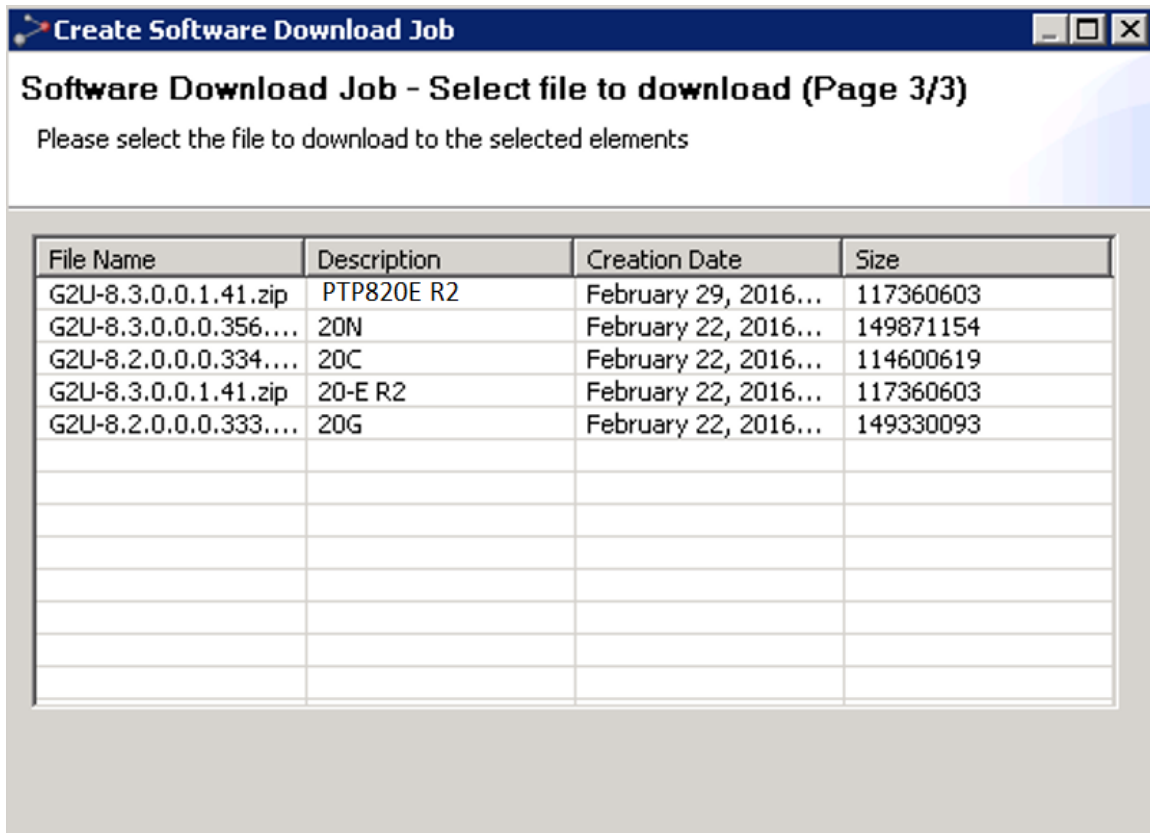
Please note that you can select NEs in more than one model, even though only one model type is displayed at a time in the Tree View. You cannot select NEs of different NE types in a single download job.


If the wizard is opened [scoped](#), this view will only present domains and NEs within the scope. The above snapshot displays an example where the wizard has been opened from the "Norway" domain in the Geographical model. If the wizard is opened scoped from a single NE, no selection is necessary and this page will be omitted from the wizard.

Press Next when the correct NE has been selected.

Create Software Download Jobs wizard - Select file to download (Page 3)

Figure 57 Software download jobs - selecting file to download



The window displays all the files uploaded to the PTP 820 NMS server using the Upload Software File  option in the [Element Software Management](#) view.

In this step you can select the software to download.

Press the Browse button to select a file containing your new software, and press Finish when done. The job will then appear in the Software Download Jobs view and its state will be READY.

Scheduling software download


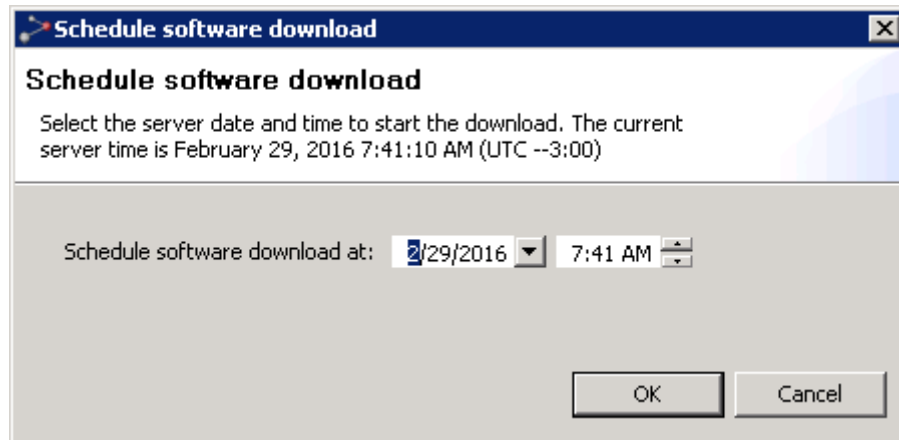

This option is enabled by selecting  Schedule Job in the menu of the [Software Download Jobs](#) view. It enables you to schedule a software download for a future date and time.

Figure 58 Schedule software download



Enter the desired date and time. The state of the job in the Software Download Jobs view changes to SCHEDULED FOR DOWNLOAD.

If you wish to cancel the scheduled software download job, select  Cancel Schedule in the menu in the [Software Download Jobs](#) view. The state of the job in the Software Download Jobs view changes back to READY.

Configuration File Management view

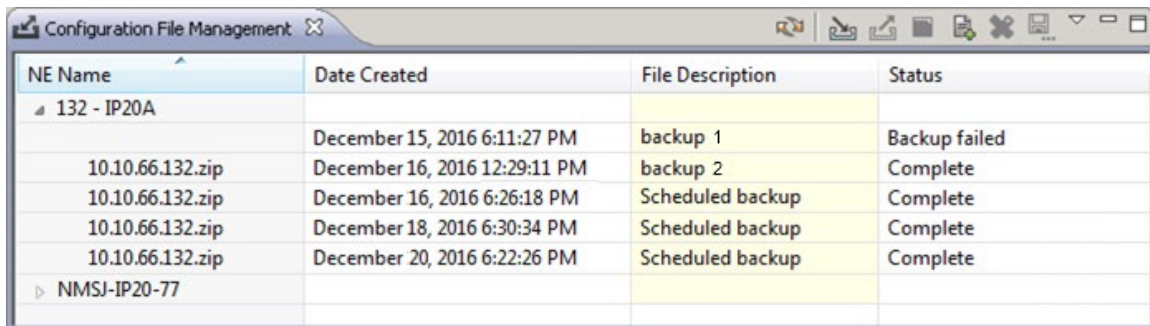
This view is opened by selecting an NE or domain node in one of the topological views and selecting Configuration | Configuration File Management in the Context or View dropdown menus. The view will then open with the selection as a scope presenting only elements that are enabled for configuration backup/restore in PTP 820 NMS.



Note

PTP 820 NMS supports backup/restore functionality for PTP 820C series and PTP 820S series.

Alternatively, you can open the view unscoped by selecting **Views > Configuration > Configuration File Management** from the main menu. The view will then present backup/restore capable elements from the entire network in the same table.

Figure 59 Configuration file management view


NE Name	Date Created	File Description	Status
132 - IP20A			
	December 15, 2016 6:11:27 PM	backup 1	Backup failed
10.10.66.132.zip	December 16, 2016 12:29:11 PM	backup 2	Complete
10.10.66.132.zip	December 16, 2016 6:26:18 PM	Scheduled backup	Complete
10.10.66.132.zip	December 18, 2016 6:30:34 PM	Scheduled backup	Complete
10.10.66.132.zip	December 20, 2016 6:22:26 PM	Scheduled backup	Complete
NMSJ-IP20-77			

This view shows a table containing a list of backup/restore capable elements including all their available configuration backup files and backup job status.

The backup files listed in the table include:

- Manually-created backups, created using the [Backup Configuration](#) option available on this page.
- Automatically-created backups, enabled using the [Scheduled Backup](#) option available in PTP 820 connection templates. The scheduled-backup files are indicated by the description “Scheduled backup” appearing in their File Description. Note that you can set the maximum number of scheduled backup configuration files to store in the PTP 820 NMS backup file repository for each NE (see [NE Configuration File Backup](#)).

Keep in mind:

- Running Backup and Restore operations cannot be cancelled.
- Any license files included in the backup file is ignored by the restore process.
- Configuration restore should not be run concurrently with software download on the same element.
- During restore, an Evolution element will automatically reset when the backup file is successfully transferred and processed. Before restoring two or more elements simultaneously, consider if the reset of one element can affect the restore process on others.

The backup and restore operations require the use of FTP or SFTP. As prerequisites, you need to:

- Install an external FTP/SFTP server on the same machine as the PTP 820 NMS server. Refer to [Install and configure an FTP or SFTP server](#).
- Configure PTP 820 NMS with the FTP/SFTP server settings, using the [Preferences: External FTP/SFTP Server](#) page.

Configuration File Management Table

The table displays the following fields:




Table 18 Configuration file management table






Name	Explanation
Resource	A backup/restore capable element. When expanded, this column shows the backup file's filename.
Date Created	Timestamp for backup creation
File Description	Backup file description. This entry can be edited directly in the table.
Status	Status of backup/restore operation

The Status field indicates job process as well as job status:

- DONE: A backup or restore operation has completed successfully.
- PENDING: A backup job waiting to be run.
- RUNNING: A running backup job. cannot be cancelled.
- RESTORING: A running restore job. cannot be cancelled.
- CANCELLED: A cancelled job.
- ADDED: A backup file added from local disk.
- BACKUP_FAILED: General backup job failure.
- BACKUP_TIMEOUT: Element access timed out - possible reason can be that element has lost contact. Used also when a backup job is running for more than 20 minutes, so that the user can delete the job.
- RESTORE_FAILED: General restore job failure.
- RESTORE_TIMEOUT: Element access timed out - possible reason can be that element has lost contact. Used also when a backup job is running for more than 20 minutes, so that the user can delete the job.

Available operations

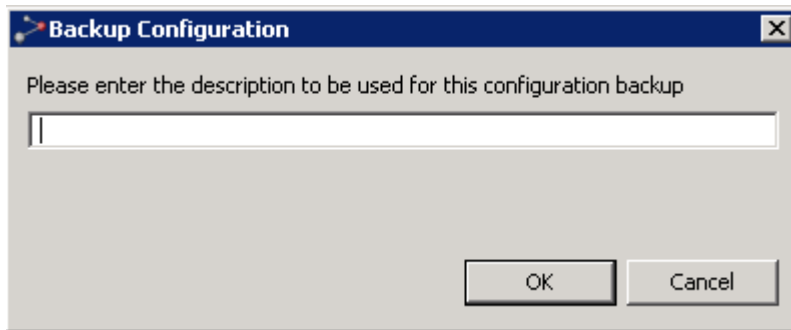
-  Refresh View Refresh the backup file list with the latest data from the server
-  Backup Configuration... Backup the configuration for a selected element. The configuration backup file will be restored in the PTP 820 NMS backup file repository at **C:\PTP820NMS\BackupConfigurations\<IP address-of-element>**
-  Restore Configuration Restore the configuration of the element using the selected configuration file.

-  **Delete file** Delete the selected configuration backups. Pending and currently running jobs will enter DELETING state before final removal
-  **Cancel Job** Cancel all PENDING backup jobs. Currently running jobs will be allowed to finish
-  **Save As...** Store a copy of the selected backup file in a desired location under a desired name.
-  **Add file...** Add a copy of selected backup file to the PTP 820 NMS backup file repository located at **C:\PTP820NMS\BackupConfigurations**
-  **FTP/SFTP Server Status** Display the status of the FTP/SFTP server: whether the server is up, and whether server parameters are defined.

Backup Configuration dialog

This dialog is opened when the [Backup Configuration](#) button is pressed.

Figure 60 Backup configuration dialog



In the dialog a suitable description can be entered. Press **OK** to backup the configuration of the element. The configuration backup file will actually be stored in the **BackupConfigurations\<IP-address-of-element>** folder, located under the [BackupConfigurations repository folder](#).

Note that you may not delete or rename a file in **BackupConfigurations\<IP-address-of-element>**; doing so will invalidate the file. However, you can copy a file and save it elsewhere, under any name, if you want an extra backup copy.



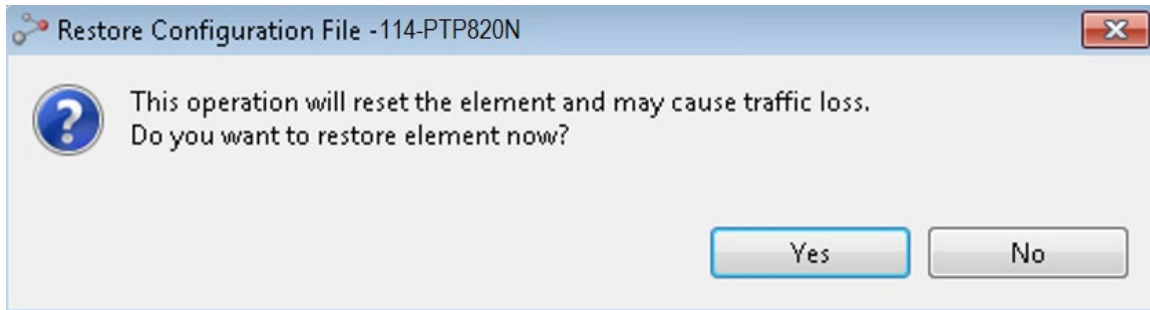
Note

That you may not delete or rename a file in **BackupConfigurations\<IP-address-of-element>**; doing so will invalidate the file. However, you can copy a file and save it elsewhere, under any name, if you want an extra backup copy.

Restore Configuration dialog

This dialog is opened when the [Restore Configuration](#) button is pressed.

Figure 61 Restore configuration dialog

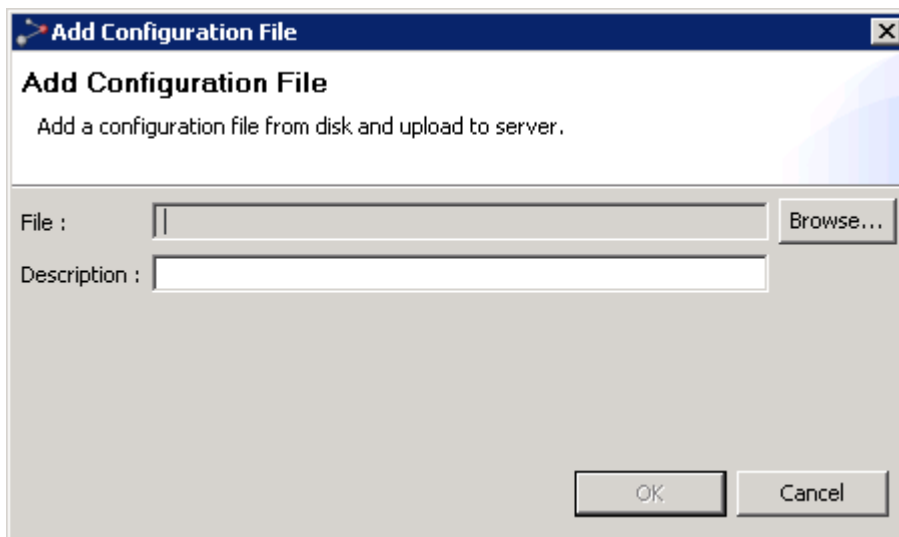


Click on the **Yes** button to continue with the restore process, or on the **No** button to abort.

Add Configuration File dialog

This dialog is opened when the Add File button is pressed.

Figure 62 Add configuration file



Click the **Browse** button and select the copy of a backup file you wish to add to the PTP 820 NMS backup repository.

Enter a suitable description and press **OK** to store it in the `BackupConfigurations\<IP-address-of-element>` folder, located under the [BackupConfigurations repository folder](#)

Name and location of BackupConfigurations and SoftwareImages repository folder

By default, the following two subfolders are located under `<system-user-dir>:\NgNMS` for Windows and `/NgNMS/` for Solaris:

- [SoftwareImages](#) – stores device software images, each in its own subfolder
- [BackupConfigurations](#) – stores device configuration backups, in `<IP-address-of-element>` subfolders

Keep in mind that the name and location of the folder containing the [BackupConfigurations](#) and [SoftwareImages](#) subfolders, can be set in the [backup.rootfolder](#) parameter of the [config_folder_location.properties](#) file, located in [<server installation folder>\server\wildfly-15.0.0.Final\standalone\configuration\](#) on the PTP 820 NMS server machine. You can change the folder name and path to a new path on a local drive only – you cannot specify a shared network storage or external drive. For more details refer to the *PTP 820 NMS NMS Installation Guide*.



Important: Do not change the structure of the repository folder. You can only copy files from the repository folder, not delete nor change the filenames of files located there.

Connection Templates view

This view is opened from the main menu under **Views > Configuration > Connection Templates**.

Figure 63 Connection templates view

Connection Type/T...	Description
> OpenSNMP	
> PTP 820C	
PTP-820C (Default: PTP-820C connection template)	
> PTP 820E	
> PTP 820F	
> PTP 820G	
> PTP 820GX	
> PTP 820S	
> PTP 850E	

Template Definition	
Modify details of selected template.	
<i>This template is currently not assigned</i>	
Connection Polling:	1200
Configuration Reconcile:	24
File transfer protocol:	FTP
Hypertext protocol:	HTTP
Hypertext User:	admin
Set Password...	
IP Address Family	
IP Address Family:	Disabled
SNMP Configuration Management	
SNMP Version:	v2c
SNMP User:	admin
Set Password...	
Authentication Algorithm:	MD5
Encryption Mode:	DES
Read Community:	public
Write Community:	private
Trap Receiver Management	
Trap Receiver Strategy:	Disabled
IP List:	

In this view you create and update the connection templates used in the [Discover Settings](#) view and the [Unmanaged Elements](#) view in the [Discover](#) perspective, and in the [Connection Template Assignment](#) view.

Some fields in a connection template may not be user editable, and are available only to provide additional information about the connection used.

A connection template contains a list of attributes used when setting up connections for this NE type. The available attributes are dependent on NE type, and may include parameters for authentication, like usernames, passwords and SNMP community names.

For some NE types, attributes for polling intervals are also available for configuration. For more details about polling, see the chapter about [How to configure polling and traps](#).



Note: Although Evolution Plus appears in the [Connection Templates table](#), this NE is not supported by PTP 820 NMS.



Note: PTP 820 NMS only supports networks that are completely IPv6 or completely IPv4, therefore the IP addresses in Connection Templates used in the [Discover](#) perspective and in the [Connection Templates Assignment view](#) must be aligned with the network IP family - either all in IPv4 or all in IPv6 format.

View area: Connection Templates table

The Connection Templates area consists of a table containing the following columns:

Table 19 Connection templates table view area

Name	Explanation
Connection Type / Templates	<p>There are different types of templates for different types of NEs. Each type may have different attributes.</p> <p>Any number of user defined templates can be created for a connection type. Click the Expand icon to the left of the connection type to expand a list. The factory-defined template for a connection template has the text "(Default)" appended to its template name in the table.</p>
Description	A user defined text describing the template. Edit directly in the table to change the description text.

View area: Template Definitions table

This area shows details of the connection template currently selected in the Connection Templates table. Editable values in the table are highlighted with pale yellow color.

The Template Definition area contains a link with initial text "This template is currently not assigned".

Clicking the link text will open the [Connection Template Assignment](#) view, filtered on the current Connection Template name.

As elements are assigned to the Connection Template, the link text will display the number of elements currently assigned to it.

Note that templates assigned to one or more elements cannot be deleted.

Examples of Template Definitions

Connection Template of type "OpenSNMP"

Connection template contains a new group, OpenSNMP, with one default template, Standard Open SNMP. The following attributes can be set or modified for OpenSNMP template:

Figure 64 Connection template of type "OpenSNMP"

Template Definition		
Modify details of selected template.		
This template is currently assigned to 9 network elements.		
Property	Value	Description
SNMP Version	v2c	The SNMP Version in the SNMP element
Read Community	public	The read community in the SNMP element
Connection Polling	1200	(seconds) Connection alive polling interval
Alarm Polling	300	(seconds) Active alarms polling interval

Attribute explanations:

Table 20 Attribute of "OpenSNMP"

Name	Explanation
SNMP Version	The SNMP version in the SNMP element.
Read Community	The community name required for reading data from the NE. Defaults to "public".
Connection Polling	Connection alive polling interval. Defaults to 20 minutes
Alarm Polling	Active alarms polling interval. Defaults to 300 seconds.

Connection Template; example and definitions

Figure 65 Connection template

Template Definition

Modify details of selected template

[This template is currently assigned to 7 network elements.](#)

Connection Polling:

1200

Configuration Reconcile:

24

Hypertext User:

admin

Set Password...

SNMP Configuration Management

Read Community:

public

Write Community:

private

Trap Receiver Management

Trap Receiver Strategy:

Disabled

IP Add List:

IP Remove List:

SNTP Configuration Management

SNTP Manager:

Element

SNTP Server:

SNTP Stratum Threshold:

7

SNTP Poll Interval:

16384

The Connection Template in the example above is currently not assigned to any anyelement as shown by the link text above.

Clicking the link text will open the [Connection Template Assignment](#) view.

Attribute Explanations:

Table 21 Connection template of type “PTP 820C” attributes

Name	Explanation
Connection Polling	Polling interval for determining if the element is reachable, but also checking for changes in alarm state or changes to configuration. Consider extending this interval to reduce system load if the PTP 820 NMS server has been listed as a Trap Receiver on the remote SNMP agent. If the amount of elements in the network is large, you can reduce network management traffic load by increasing this interval.
Configuration Reconcile	The configuration reconcile polling interval, in hours.

Name	Explanation
Hypertext user	<p>PTP 820 NMS uses the HTTP protocol and hence requires valid HTTP User and Password.</p> <p>Click on the Set Password button to set the corresponding HTTP Password.</p> <p>Whenever PTP 820 NMS fails to connect to an element due to wrong username/password, an HTTP Logon Failure alarm will be raised.</p>
Read Community	The SNMP community name required for reading data from the NE
Write Community	The SNMP community name required for writing data to the NE
Trap Receiver Strategy	<p>PTP 820 NMS can be configured to distribute Trap Receiver settings to elements assigned to a specific Connection Template.</p> <p>For each element in Managed state assigned to a Connection Template with Trap Receiver Strategy set to something else other than Disabled, PTP 820 NMS will:</p> <ul style="list-style-type: none"> Remove from the element's Trap Receiver list all entries with IP address given in the IP Remove List. Add new entries to the element's Trap Receiver list for each IP address given in the IP Add List. Entries added by PTP 820 NMS will be given Community String = "PTP 820 NMS" and a port number as defined in the Snmp Trap Port Number field in the System Server View. Clean up existing Trap Receiver settings with IP address also present in the IP Add List by: <ul style="list-style-type: none"> If necessary adjusting Port and Community String settings (if necessary) removing possible duplicates Poll every night and make sure that the elements' Trap Receiver lists are configured correctly. If element is unreachable, retry every half hour until element connection is established Remove PTP 820 NMS Server IPs from the element's Trap Receiver list when the element is set to Unmanaged state <p>can currently hold at most 3 Trap Receiver list entries. If PTP 820 NMS wants to add a new entry and the Trap Receiver list is full, there are three possibilities:</p> <ul style="list-style-type: none"> Do not add if the Trap Receiver Strategy PTP 820 NMS wants to add a new entry and the Trap Receiver list is full Remove one existing Trap Receiver list entry

Name	Explanation								
	<ul style="list-style-type: none"> Just throw away all existing Trap Receiver settings <p>These approaches are reflected in the available Trap Receiver Strategy settings:</p> <table> <tr> <td>Disabled</td><td>PTP 820 NMS will not make any changes to the elements' Trap Receiver lists. This is the default setting.</td></tr> <tr> <td>Add</td><td>PTP 820 NMS will attempt to update Trap Receiver lists. If list is full, will be raised.</td></tr> <tr> <td>Force Add</td><td>PTP 820 NMS will always update Trap Receiver lists. One existing entry will if needed be removed to make space for each IP address in the IP Add List.</td></tr> <tr> <td>Exclusive Add</td><td>PTP 820 NMS will always update Trap Receiver lists. The IP addresses in the IP Add List will be added, all other entries will be deleted.</td></tr> </table>	Disabled	PTP 820 NMS will not make any changes to the elements' Trap Receiver lists. This is the default setting.	Add	PTP 820 NMS will attempt to update Trap Receiver lists. If list is full, will be raised.	Force Add	PTP 820 NMS will always update Trap Receiver lists. One existing entry will if needed be removed to make space for each IP address in the IP Add List.	Exclusive Add	PTP 820 NMS will always update Trap Receiver lists. The IP addresses in the IP Add List will be added, all other entries will be deleted.
Disabled	PTP 820 NMS will not make any changes to the elements' Trap Receiver lists. This is the default setting.								
Add	PTP 820 NMS will attempt to update Trap Receiver lists. If list is full, will be raised.								
Force Add	PTP 820 NMS will always update Trap Receiver lists. One existing entry will if needed be removed to make space for each IP address in the IP Add List.								
Exclusive Add	PTP 820 NMS will always update Trap Receiver lists. The IP addresses in the IP Add List will be added, all other entries will be deleted.								
SNTP Manager	<p>PTP 820 NMS can be configured to distribute SNTP settings to all elements assigned to a specific Connection Template.</p> <p>For each element in Managed state assigned to a Connection Template with SNTP Manager set to " PTP 820 NMS", PTP 820 NMS will:</p> <ul style="list-style-type: none"> Enable SNTP on the element using values specified in the SNTP Server, SNTP Stratum Threshold and SNTP Poll Interval attributes. Poll every night that the element's NTP settings are correctly configured If element is unreachable, retry every half hour until element connection is established. <p>The possible values for SNTP Manager are:</p> <table> <tr> <td>Element</td><td>PTP 820 NMS will not make any changes to the elements' NTP configuration. This is the default setting.</td></tr> <tr> <td>PTP820NMS</td><td>PTP 820 NMS will attempt to update SNTP configuration.</td></tr> </table> <p>Note that if SNTP Manager is changed from "PTP 820 NMS" to "Element", PTP 820 NMS will NOT switch the elements' time settings to Manual time setting. PTP 820 NMS will simply stop monitoring the SNTP settings, allowing each element to be configured independently.</p> <p>Note that for PTP820 elements SNTP is referred to as NTP.</p>	Element	PTP 820 NMS will not make any changes to the elements' NTP configuration. This is the default setting.	PTP820NMS	PTP 820 NMS will attempt to update SNTP configuration.				
Element	PTP 820 NMS will not make any changes to the elements' NTP configuration. This is the default setting.								
PTP820NMS	PTP 820 NMS will attempt to update SNTP configuration.								

Connection Template of type PTP820C, PTP820E, PTP820S, PTP820G; example and definitions

Figure 66 Connection template

Template Definition

Modify details of selected template

[This template is currently assigned to 4 network elements.](#)

Connection Polling: 1200

Configuration Reconcile: 24

File transfer protocol: FTP

Hypertext protocol: HTTP

Hypertext User: admin

SNMP Configuration Management

SNMP Version: v3

Read Community: public

Write Community: private

SNMP User: admin

Authentication Algorithm: MD5

Encryption Mode: DES

Trap Receiver Management

Trap Receiver Strategy: Disabled

IP List:

NTP Configuration Management

NTP Configuration Strategy: Disabled

NTP Admin State: Disabled

NTP Version: NTPv4

NTP Server:

UTC Configuration Management

UTC Configuration Strategy: Disabled

UTC Offset Hours: 0

UTC Offset Minutes: 0

DST Start Month: 1

DST Start Day: 1

DST End Month: 1

DST End Day: 1

DST Offset (Hours): 1

The Connection Template in the example above is currently assigned to 4 elements as shown by the link text above.

Clicking the link text will open the [Connection Template Assignment](#) view.

Attribute Explanations:

Table 22 Connection template of type “PTP820C, PTP820E, PTP820S, PTP820G” attributes

Name	Explanation
Connection Polling	Polling interval for determining if the element is reachable, but also checking for changes in alarm state or changes to configuration. Consider extending this interval to reduce system load if the PTP 820 NMS server has been listed as a Trap Receiver on the remote SNMP agent. If the amount of elements in the network is large, you can reduce network management traffic load by increasing this interval.
Configuration Reconcile	The configuration reconcile polling interval, in hours.
File transfer protocol	Select one of the following: <ul style="list-style-type: none"> FTP SFTP
Hypertext protocol	Select one of the following: <ul style="list-style-type: none"> HTTP HTTPS <p>Note: PTP820 devices with version R7.9 or lower do not support HTTPS.</p>
Hypertext user	PTP 820 NMS uses the HTTP protocol, and hence requires a valid HTTP User and Password, for performing the following: <ul style="list-style-type: none"> Software Download / Reset / Activate Element Config Backup / Restore Reset of Performance Counters Trap Receiver Management NTP Management UTC Configuration End-to-End Service Provisioning <p>Click on the Set Password button to set the corresponding HTTP Password.</p> <p>Whenever PTP 820 NMS fails to connect to an element due to wrong username/password, a HTTP Logon Failure alarm will be raised.</p>
SNMP Configuration Management	PTP 820 NMS can be configured to use SNMP to secure the connection between PTP 820 NMS and PTP820 NEs.






Name	Explanation
SNMP Version	Select one of the following: <ul style="list-style-type: none">• v1• v2c• v3
Read Community	The community name required for reading data from the NE. This parameter is not relevant when SNMP v3 is selected.
Write Community	The community name required for writing data to the NE. This parameter is not relevant when SNMP v3 is selected.
SNMP User	The SNMP user name and password required when SNMP v3 is selected.
Authentication Algorithm	The authentication algorithm to use when SNMP v3 is selected. Select one of the following: <ul style="list-style-type: none">• None• MD5• SHA
Encryption Mode	The encryption mode to use when SNMP v3 is selected. Select one of the following: <ul style="list-style-type: none">• None• DES• AES





Name	Explanation				
Trap Receiver Management (PTP820 NEs only)	<p>PTP 820 NMS can be configured to distribute Trap Receiver settings to elements assigned to a specific Connection Template.</p> <p>For each element in Managed state assigned to a Connection Template with Trap Receiver Strategy set to enabled, PTP 820 NMS will:</p> <ul style="list-style-type: none"> • Overwrite the element's Trap Receiver list all entries with IP address given in the IP List. • Add new entries to the element's Trap Receiver list for each IP address given in the IP Add List. Entries added by PTP 820 NMS will be given Community String = " PTP 820 NMS " and a port number as defined in the Snmp Trap Port Number field in the System Manager Server View. • If less than 4 IP addresses are given in the Trap Receiver IP List, PTP 820 NMS will override the remaining entries with the null IP address "0.0.0.0" • Poll every night and make sure that the elements' Trap Receiver lists are configured correctly • If PTP 820 NMS does not succeed to write the information to a device, the information will be written at the next polling interval. <p>Elements can currently hold at most 3 Trap Receiver list entries.</p> <p>The following table summarizes PTP 820 NMS's action for the two Trap Receiver Strategy settings available for PTP820 NEs:</p> <table> <tr> <td>Disabled</td><td>PTP 820 NMS will not make any changes to the elements' Trap Receiver lists. This is the default setting.</td></tr> <tr> <td>Enabled</td><td>PTP 820 NMS will always update Trap Receiver lists. The IP addresses in the IP List will be added, all other entries will be deleted.</td></tr> </table>	Disabled	PTP 820 NMS will not make any changes to the elements' Trap Receiver lists. This is the default setting.	Enabled	PTP 820 NMS will always update Trap Receiver lists. The IP addresses in the IP List will be added, all other entries will be deleted.
Disabled	PTP 820 NMS will not make any changes to the elements' Trap Receiver lists. This is the default setting.				
Enabled	PTP 820 NMS will always update Trap Receiver lists. The IP addresses in the IP List will be added, all other entries will be deleted.				

Name	Explanation				
Scheduled Backup of Network Element Configuration	<p>Whether to enable automatic scheduled backup of the network elements to which this connection template is assigned. By default this option is disabled, but it is recommended to enable the option.</p> <p>If you select Enable, specify how often to back up the NEs and at what time of day to perform backup.</p> <p>The configuration backup files are stored in the PTP 820 NMS backup file repository at: <code><system-user-dir>\NgNMS\BackupConfigurations\<IP-address-of-element></code>. This is the same location where manual backups of NE configuration are stored. Both manual and scheduled configuration backups can be viewed in the, and restored from that view.</p> <p>For each NE, up to 4 scheduled backup files are saved, using the First-in, First-out (FIFO) method. You can set the number of scheduled backup files to store using the System Settings > Configuration > Error! Reference source not found. Preferences page. Note that there is no limit on the number of manual backup files the system stores.</p> <p>Backup will be performed only if the configuration file has changed since the last backup.</p> <p>The backup operation requires the use of FTP or SFTP. As prerequisites, you need to:</p> <ul style="list-style-type: none"> • Install an external FTP/SFTP server on the same machine as the PTP 820 NMS server. Refer to Install and configure an FTP or SFTP server. • Configure PTP 820 NMS with the FTP/SFTP server settings, using the Preferences: External FTP/SFTP Server page. 				
NTP Configuration Management (PTP820 NEs only)	<p>PTP 820 NMS can be configured to distribute NTP settings to all elements assigned to a specific Connection Template.</p> <p>For each element in Managed state assigned to a Connection Template with NTP Configuration Strategy set to "Enabled", PTP 820 NMS will:</p> <p>Write the "NTP Admin State", "NTP Version" and the "NTP Server (IP Address)" to the element.</p> <p>Poll every night that the element's NTP settings are correctly configured</p> <p>The possible values for NTP Configuration Strategy are:</p> <table border="1" data-bbox="493 1451 1492 1608"> <tr> <td data-bbox="493 1486 602 1512">Disabled</td><td data-bbox="623 1472 1365 1535">PTP 820 NMS will not make any changes to the elements' NTP configuration. This is the default setting.</td></tr> <tr> <td data-bbox="493 1570 594 1596">Enabled</td><td data-bbox="623 1570 1289 1596">PTP 820 NMS will attempt to update NTP configuration.</td></tr> </table> <p>Note that if NTP Configuration Strategy is changed from "Enabled" to "Disabled", PTP 820 NMS will simply stop monitoring the NTP settings, allowing each element to be configured independently.</p>	Disabled	PTP 820 NMS will not make any changes to the elements' NTP configuration. This is the default setting.	Enabled	PTP 820 NMS will attempt to update NTP configuration.
Disabled	PTP 820 NMS will not make any changes to the elements' NTP configuration. This is the default setting.				
Enabled	PTP 820 NMS will attempt to update NTP configuration.				

Name	Explanation				
UTC Configuration Management (PTP820 NEs only)	<p>PTP 820 NMS can be configured to distribute UTC Offset and DST settings to all elements assigned to a specific Connection Template.</p> <p>For each element in Managed state assigned to a Connection Template with UTC Configuration Strategy set to "Enabled", PTP 820 NMS will:</p> <p>Write the "UTC Offset (Hours and Minutes)", "DST Start Date", "DST End Date" and "DST Offset" to the element.</p> <p>Poll every night that the element's UTC Configuration settings are correctly configured</p> <p>If PTP 820 NMS does not succeed to write the information to a device, the information will be written at the next polling interval.</p> <p>The possible values for UTC Configuration Strategy are:</p> <table border="1"> <tr> <td>Disabled</td><td>PTP 820 NMS will not make any changes to the elements' UTC Offset or DST configuration. This is the default setting.</td></tr> <tr> <td>Enabled</td><td>PTP 820 NMS will attempt to update the elements' UTC Offset and DST configuration.</td></tr> </table> <p>Note that if UTC Configuration Strategy is changed from "Enabled" to "Disabled", PTP 820 NMS will simply stop monitoring the UTC and DST settings, allowing each element to be configured independently.</p>	Disabled	PTP 820 NMS will not make any changes to the elements' UTC Offset or DST configuration. This is the default setting.	Enabled	PTP 820 NMS will attempt to update the elements' UTC Offset and DST configuration.
Disabled	PTP 820 NMS will not make any changes to the elements' UTC Offset or DST configuration. This is the default setting.				
Enabled	PTP 820 NMS will attempt to update the elements' UTC Offset and DST configuration.				

Available operations

-  **Save** Save all changes made to the templates in this view. Note that these will immediately affect communication with all NEs for which changed templates are assigned. Further, new templates may be assigned in the Connection Template Assignment View, the Discover Settings View, and the Unmanaged Elements View. Depending on the changes in the templates, the [Confirm Save of Connection Templates](#) may appear.
-  **Refresh View** Refresh the view to receive the latest data from server
-  **Set As Default** Set the currently selected template as the "default template" in its connection type. The current default template is used as default when discovering new elements. Other templates may also be used for discovering new elements, but this must be manually selected in the Discover Settings View
-  **Create Template** Create a new template, by opening the [Create Template](#) dialog for the connection type currently selected in the Connection Templates table.
-  **Delete** Open the Confirm [delete](#) dialog and delete the template currently selected in the Connection Templates table

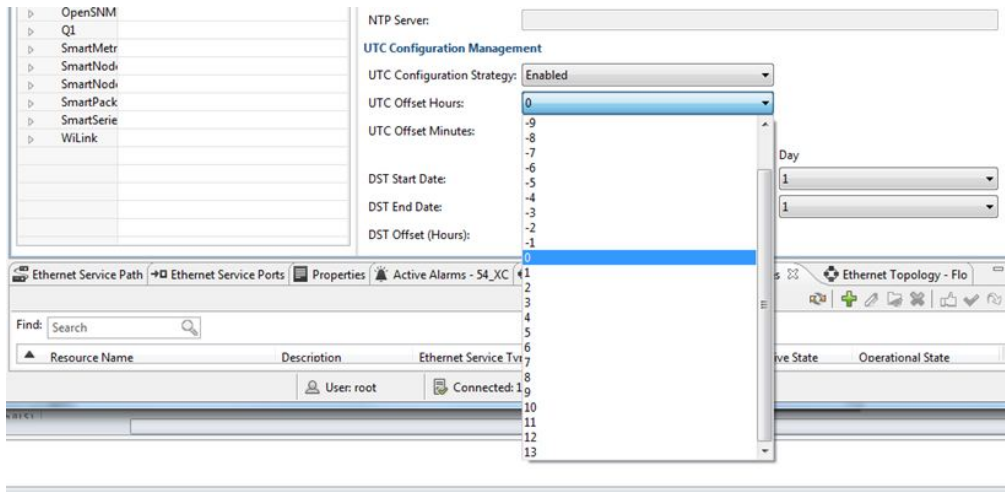
-  Clone Create a copy of the connection template currently selected in the Connection Templates table
-  Rename Rename the selected template
-  Horizontal Organize the [Connection Templates](#) area and the [Templates Definitions](#) area horizontally
-  Vertical Organize the [Connection Templates](#) area and the [Templates Definitions](#) area vertically

Setting UTC Offset (PTP 820 devices only)

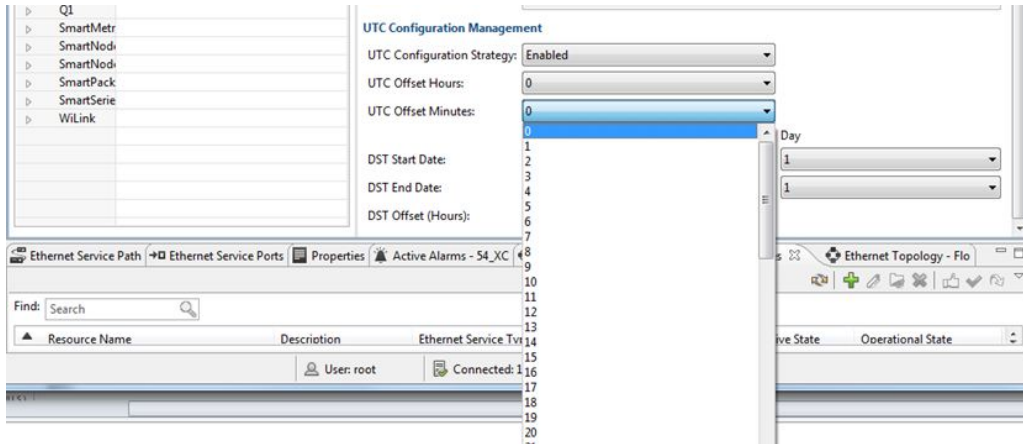
You can enable UTC Configuration Strategy to write down the Coordinated Universal Time (UTC) Offset and Daylight Savings Time (DST) information to the PTP 820 devices that are associated with this connection template.

Choose Enabled from the UTC Configuration Strategy dropdown box. Then choose the UTC Offset hours:

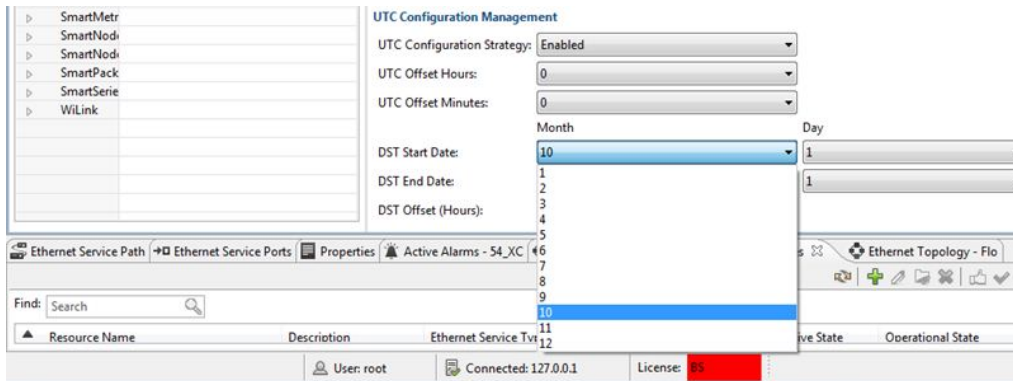
Figure 67 Setting UTC offset



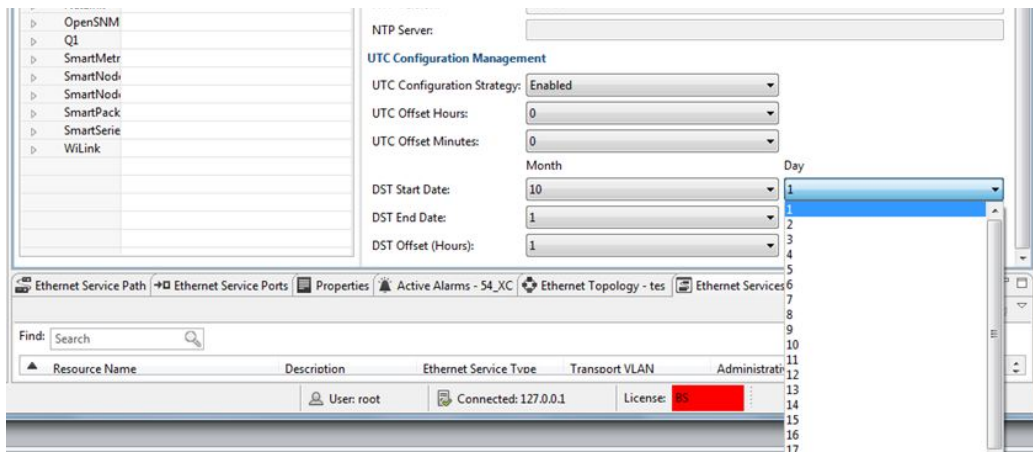
And also choose the UTC Offset minutes:



To set DST parameters, choose DST Start Date Month



Start Date Day



DST End Date Month and Day

And DST Offset (Hours)

Create Template dialog

The content in the Create Template dialog will depend on the connection type selected in the ConnectionTemplates table when creating a new connection template.

Create Template dialog for a connection type

This dialog is shown when using Create New Template with the connection type "" selected in the Connection Templates table.

Figure 68 Create template dialog for connection type

Create New Template

Please enter the details

Name: \Name

Description:

Read Community: public

Write Community: private

Connection Polling: 1200

Configuration Reconcile: 24

Hypertext User: admin

Password:

Confirm Password:

Trap Receiver Management

Trap Receiver Strategy: Disabled

IP Add List:

IP Remove List:

SNTP Configuration Management

SNTP Manager: Element

SNTP Server:

SNTP Stratum Threshold: 7

SNTP Poll Interval: 16384

OK Cancel

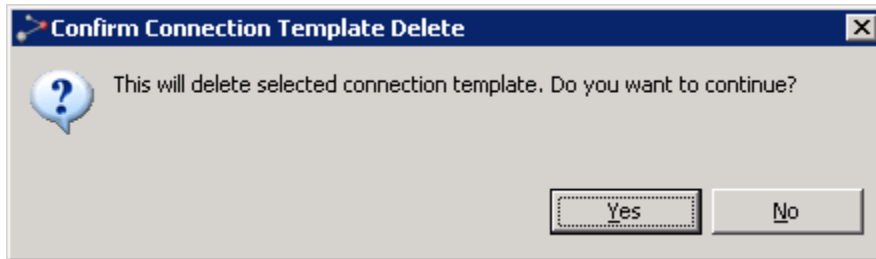
Enter a Template Name to identify the new template, and a more detailed Description of the new template. Enter a Read Community and Write Community which can provide the PTP 820 NMS server with a sufficient level of permissions on the SNMP elements where you want to assign this template.

Press OK to generate the template.

Delete Template dialog

This dialog is shown when using delete in the ConnectionTemplate table with a connection template selected.

Figure 69 Delete template dialog

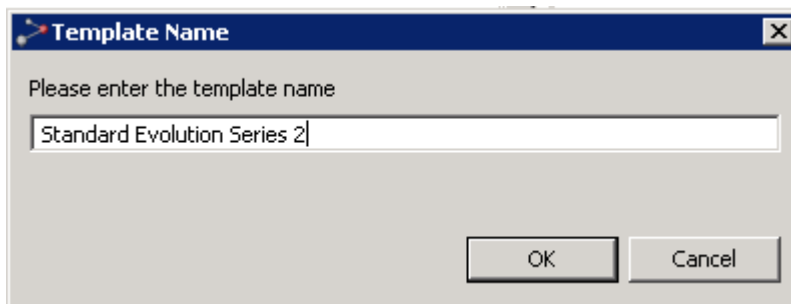


Press Yes to confirm the deletion, or press No to cancel.

Template Name dialog

This dialog is shown when using clone or rename in the Connection Template table with a connection template selected

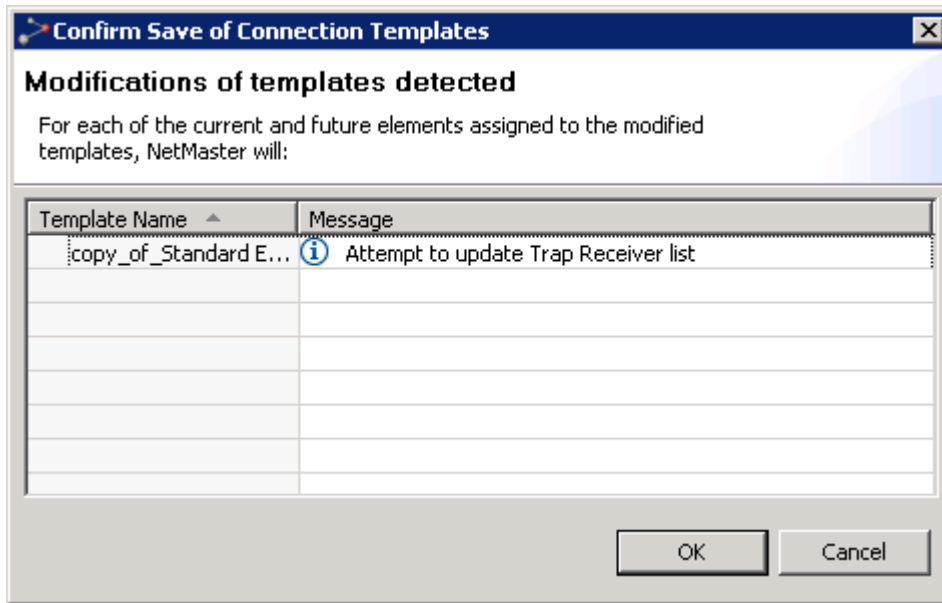
Figure 70 Template name dialog



Enter the new template name and press OK. The new/updated template will now appear in the Connection Template table.

Confirm Save of Connection Templates dialog

This dialog is shown when changes to at least one of the modified templates will cause PTP 820 NMS to update element configuration.

Figure 71 Confirm save of connection template dialog

Press OK to confirm save operation, or press Cancel to cancel.

Connection Templates Assignment view

This view is opened "[scoped](#)" by selecting any NE or domain in one of the topology views (**Geographical** or **Logical Map** or **Tree**) and selecting **Configuration > Connection Template Assignment** from the menu, or non-scoped by selecting **Views > Configuration > Connection Template Assignment** from the main menu.

Figure 72 Connection template assignment view

[illegible]

In this view, you can reassign connection templates for your managed NEs.

A connection template is a profile for [authenticating](#) the PTP 820 NMS server as an NE user. The templates identify PTP 820 NMS in the communication between the PTP 820 NMS server and the NE, containing user name/password for Q1 NE and read/write community names for SNMP NE. When you manage an NE, you will normally be provided with a certain level of permissions on the NE based on the values in the current connection template.

The templates used in the Connection Template Assignment view are created and updated in the [Connection Templates](#) view. The templates can be assigned to NEs at different stages of the discover process: in the [Discover Settings](#) view you can select connection templates used during a [search](#), in the [Unmanaged Elements](#) view you can reassign connection templates for discovered elements that are not yet managed, while connection templates for the managed elements are reassigned in the Connection Template Assignment view.

Connection Template Assignment table





The table contains the following columns:

Table 23 Connection template assignment table

Name	Explanation
Resource Name	Names of the NEs to which you want to assign a new template to.
Connection Type	Type of template used.
Connection Template	The short-name for the currently selected connection template. Click the dropdown list to select one of the connection templates available for this resource.
Template Description	A user-defined text describing the purpose of this template.

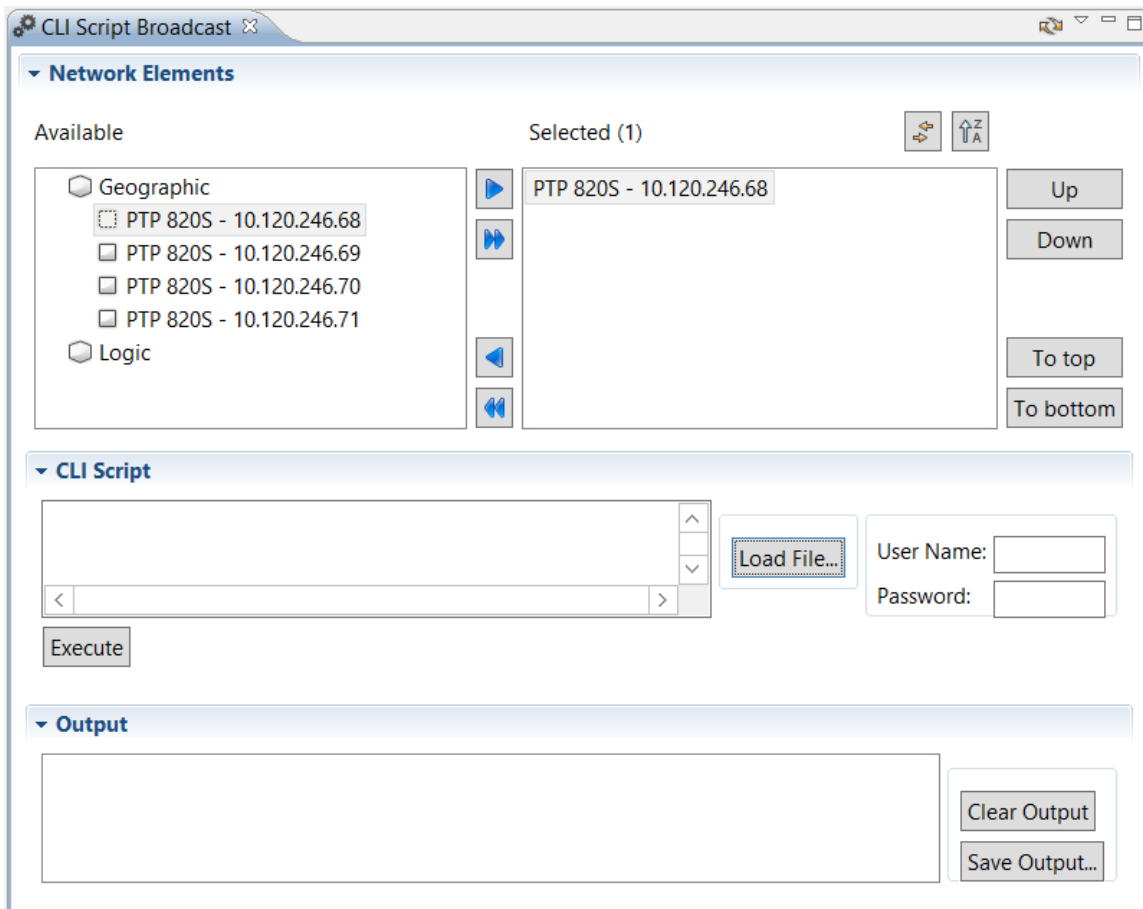
The table includes all NEs available for the node from which you opened the dialog.

Available operations

-  Click the dropdown menu in the Connection Template column to select a template for the NE on this line in the table.
- **Assign Template**  Use the context menu in the table to assign a connection template for one or more NEs currently selected in the table.
-  **Refresh** Refresh the view to receive the latest connection templates, and refresh the current template assignments from server.
-  **Save** Apply and save all changes made to template assignments in this view

CLI Script Broadcast view

This view is opened from the **main menu** under **Views > Configuration > CLI Script Broadcast**.



In this view you can run a CLI script on a batch of Cambium network elements (PTP 820s). The CLI script you specify will run on the group of devices you specify, in the order you specify, and the output will appear on screen. You can save this output to a file.

To run the CLI script on a batch of network elements:

- 1 Place the CLI script you wish to run, in a location that can be accessed from the machine running v the PTP 820 NMS client.

- 2 Specify the network elements on which to execute the CLI script, as follows: Select desired network elements in the **Available** window of the **Network Elements** area, and click the right arrow to display them in the **Selected** window. You can select elements from the geographical and/or logical tree. If you select an entire domain, the CLI script will be executed on each of the devices in the domain.
- 3 Optionally use the **Up**, **Down**, **To top** and **To bottom** buttons to re-order the list of elements. Note that the CLI script will first run on the first device in the list, then on the second device, etc.
- 4 Click **Load File** and specify the CLI script file. The file contents are displayed in the **CLI Script** window.
- 5 In the **User Name** and **Password fields**, enter the login credentials for accessing the network devices. The devices must all have the same login credentials if you wish to run the CLI script on them.
- 6 Click **Execute**.

The NMS executes the commands on the devices, one device at a time, in the order in which they appear in the window.

- If the NMS is unable to login to a device, it moves on to the next device in the list.
 - If the NMS is unable to execute a certain command, it halts command execution in that device and moves on to the next device in the list.
- 7 View the output in the **Output** window (refer to [Viewing the output of a CLI script execution](#)).
 - 8 Optionally click **Save Output** to save the output to a text file.
 - 9 Optionally click **Execute** to run the CLI script again. The results of the current execution are appended to the results of the previous execution. You might therefore first click **Clear Output** to delete the display in the Output window, before clicking **Execute** again.

CLI Script Considerations and Limitations

Please note the following CLI script limitations

- The CLI script cannot be executed by a root user.
- The CLI script does not support:
 - Running the help command
 - Retrieving the events log or the active alarms table
 - Running Unix commands
 - Changing a password on a device.

In other words, you cannot use a CLI script to change a password on a device.
- If the commands' output contains several instances of the character ">", this may cause the script to stop execution.
- The script file has a maximum size of 100KB.
- The script output has a maximum size of 10MB.

Please note the following CLI script considerations:

- If you want to run a script with output longer than a single screen, you need to add the command **cli_debug no-less** at the very beginning of the script.
- It is not recommended to run a script for the first time using PTP 820 NMS. Instead, first validate the commands manually.

- It is not recommended to run both configuration and monitoring commands in the same script, to avoid situations where the execution terminates in the middle as a result of exceeding the maximum output size.

Viewing the output of a CLI script execution

After execution is complete, the results appear in the **Output** window.

For each device, the following is displayed:

- A title line with the device name and IP address, followed by the execution status: Success or Failure
- Each script input line, followed by the console output.

A summary line appears at the end, listing the number of devices on which execution succeeded and the number of devices on which execution failed.

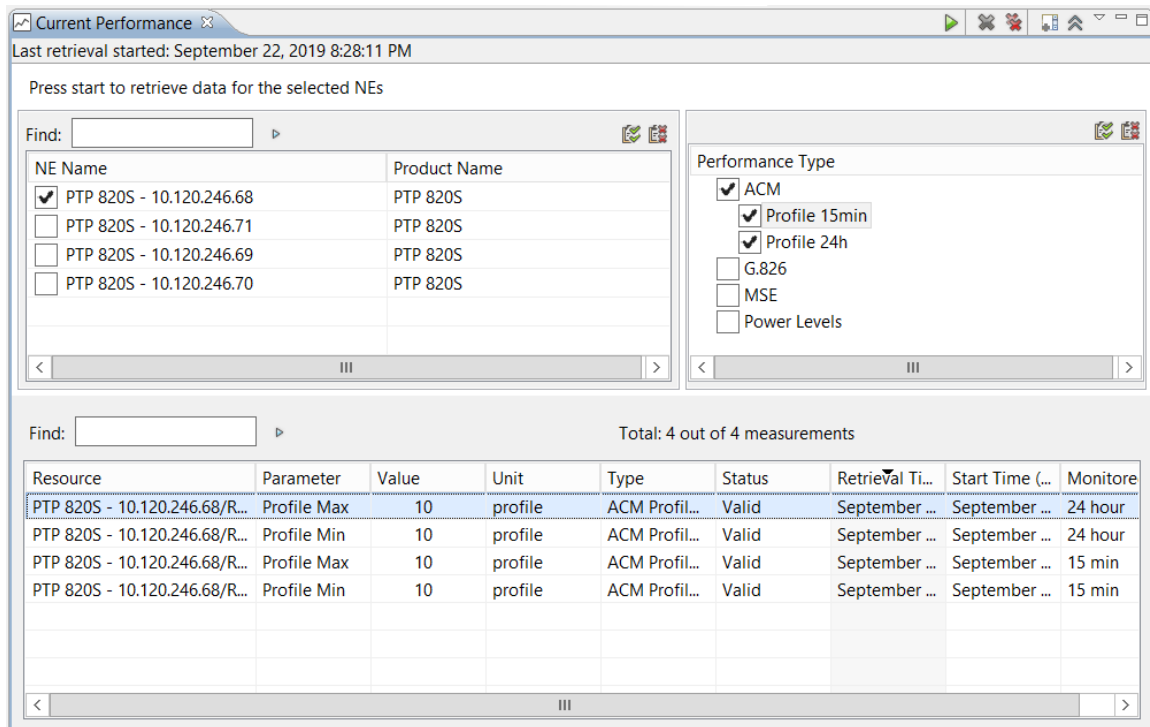
Note: A status of success indicates that the NMS was able to both access the device and run all the commands in the script.

Performance

Current Performance view

This view is opened "[scoped](#)" by selecting any NE or domain in one of the topology views (**Geographical** or **Logical Map** or **Tree**) and selecting **Performance >Current Performance** in the **Context** or **Dropdown** menu, or non-scoped by selecting **Views >Performance >Current Performance** from the main menu.

Figure 73 Current performance view



This is a view for reading the current performance measurement values directly from NE and present in a table. The view presents performance measurements as read from the NE each time the user selects the [Start Performance Reading](#) operation. Unlike the [Historical Performance](#) view, data read from elements this way are not stored in the PTP 820 NMS database. However, the data can be [exported to file](#) for further analysis.

Selector Control area

The Selector Control area is used for selecting data to present in the [Current Performance](#) table. The Selector Control area contains a NE Name table and a Performance Type table.

When both NE and Performance type are selected, current performance can be read from the NE by clicking Start Performance Reading icon on the view toolbar.

NE Name table

The table contains network elements that can be used for reading current performance. In the above [example](#), the table contains NEs from the [domain](#) "Analamanga", which is the [scope](#) in this example. Each NE in the table is identified by the following fields:

Table 24 NE name table

Name	Explanation
NE Name	The name of the equipment containing this parameter
Product Name	The type of NE

Click a checkbox with a NE in the table to select/unselect reading current performance from resources on this element. When the amount of NE in the table is large, the [Quick Search](#) field for the NE Name table can be used for filtering.

Performance Type table

This table contains all performance types/subtypes available from the NEs in the scope. The following performance types might be found in the table, depending on NE types and configurations in the scope:

Table 25 Performance type table

Performance Type	Explanation
G.821ACM	Measurements that can be read from the Q1 NE-types NL18xAdaptive Coding and NL24x. Can include subtypes of both 15min and 24hModulation measurements.
G.826	Measurements that can be found on the Q1 NE-types InterLink, CityLink and NL29x NE. Dependent of. Depending on the configuration of the elements, this can include performance subtypes B1 , B2 , PDH Parity and Link Errors . Can include subtypes of cumulative counters, 15min measurements, 24h measurements and monthly measurements
MSE	Mean Square Error measurements.
Power Levels	Analog measurements of received and transmitted power level from Radio. Can include subtypes for NE. Can include subtypes of current measurements (i.e. snapshots of current values), 1min registers, 15min registers and 24h registers.
Ethernet	A set of measurements for ethernet traffic that can be found on NEs.
Power Supply	Analog measurements from power supply

Click a checkbox in the table to select/unselect reading current performance of this performance type/subtype.

Current Performance table

This table presents the performance data last read from this NE.

Each performance measurement is identified by the following fields:

Table 26 Current performance table










Name	Explanation
Resource	The name of the equipment containing this parameter
Parameter	<p>The performance measurement types on the selected equipment, e.g.</p> <p>performance measurement types (as defined in G.826/G.821):</p> <p>SES - Severely Errored Seconds, a one-second period with one Errored Block Overstep (EBO) and/or one Severely Errored Overstep(SEBO)</p> <p>UAS - Unavailable Seconds.</p> <p>BBE - Background Block Error.</p> <p>ES - Errored Second, a one-second period with one or more Error Blocks (EB).</p> <p>DM- Degraded Minutes, error pulses</p> <p>power levels, such as:</p> <p>RPL - Received power level</p> <p>RPL_SDIV - Received power level on space diversity equipment</p> <p>ethernet statistics, such as:</p> <p>Drop Events In</p> <p>Packets In</p> <p>power supply, such as:</p> <p>Battery Voltage</p> <p>Battery Current</p>
Value	The measured performance value received from the NE
Unit	The measure unit for the Value
Type	The performance subtype, as selected in the Performance Type table.





Name	Explanation
Status	<p>The condition of the received data, eg:</p> <p>Valid – equals: performance measurement is valid</p> <p>Running – equals: a cumulative counter is running</p> <p>Invalid – equals: received performance data is not valid</p> <p>Unavailable – equals: performance data currently is not available for this NE, most likely due to time out</p>
Retrieval Time (System)	The server time when the measurement was received
Start Time (NE)	The timestamp when the measurement was started on the NE
Monitored Time	Lists the monitored time intervals

The data in the table can be exported to Excel spreadsheet, comma separated file or extensible markup language.

When the amount of data in the table is large, the [Quick Search](#) field for the Current Performance table can be used for filtering.

Available operations

-  **Start Performance Reading** Click to read new data from the elements.
-  **Clear Selected** Remove the currently selected row with measurements from the Current Performance table.
-  **Clear All** Remove all rows with measurements from the Current Performance table.
-  **Append Mode** Click to turn on/off Append Mode. When the Current Performance table is in Append Mode, data will be added to the end of the table each time you start performance reading from the elements. When the Current Performance Table not is in append mode, the content of the table will be cleared each time you read new data.
-  **Hide Selector** Click to hide the [Selector Control](#) area.
-  **Show Selector Control** Click to show the Selector Control area.
-  **Export to File...** Export your current data to file by open the [Export to File](#) dialog. You are allowed to save the table as an Excel spreadsheet (.xls), comma separated file (.csv) or extensible markup language (.xml)
-  **Customize Columns...** Open the [Customize Columns](#) dialog for the Current Performance view. In this dialog you can select which columns will be displayed in the table, and the order in which they appear.
-  Click a checkbox in the [NE Name](#) table to select/unselect reading performance from this element. Click a checkbox in the [Performance Type](#) table to select/unselect reading this performance type/subtype.

-  Select all checkboxes in the NE Name table or Performance Type table.
-  Unselect all checkboxes in the NE Name table or Performance Type table.
-  Click a Performance Type to expand a list of Performance Subtypes in the in the Performance Type table.
-  Double click inside the Current Performance table to [hide/show](#) the Selector Control area.

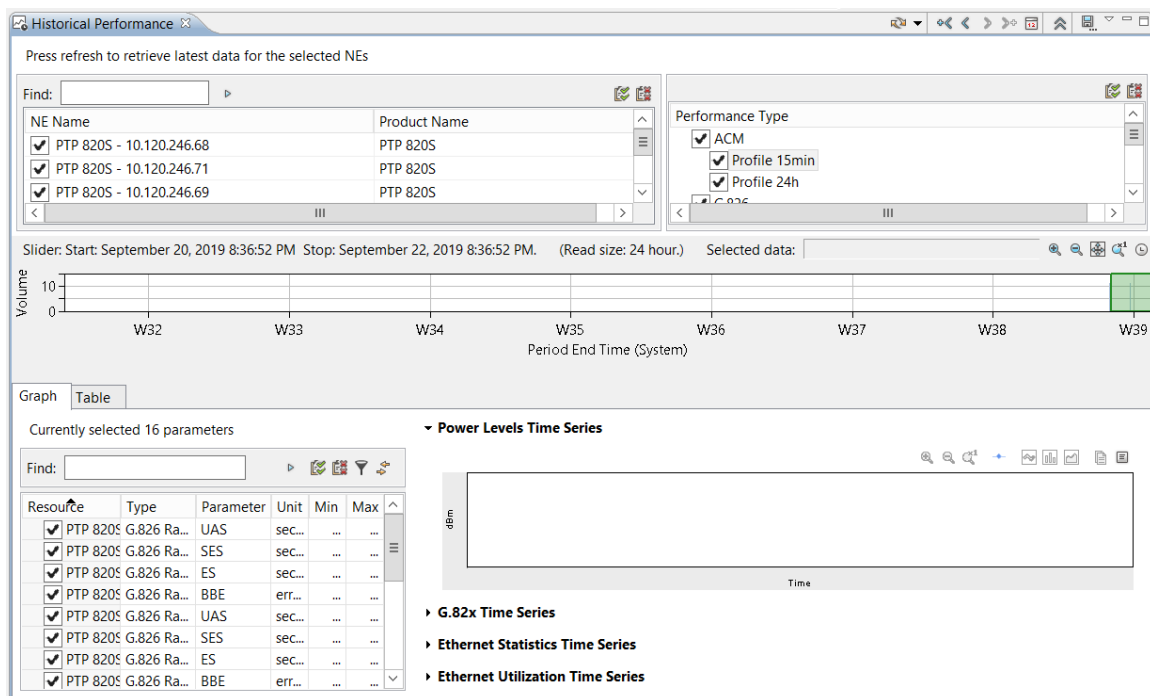
Historical Performance view

This view is opened "[scoped](#)" by selecting any NE or domain in one of the topology views (Geographical or Logical Map or Tree) and selecting Performance | Historical Performance in the Context or Dropdown menu, or non-scoped by selecting Views | Performance | Historical Performance from the main menu.

In this view you can study periods with historical performance data from NE

This is a view for analysing historical performance data that PTP 820 NMS already have been collected from NE. The performance collection is enabled by [assigning performance templates](#) to each NE in the [Performance Collection Control](#) view. Unlike the [Current Performance](#) view, the view presents periods with historical performance measurements that already are read from NE and stored in the ENS database. The data can be presented in a table or as a graph, and data can be [exported to file](#) for further analysis.

Figure 74 Historical performance view



The view contains a Selector Control area, to select NE and Performance Types to retrieve from database, and a Timeslider tool to navigate through the historical data found in the database. The data can be presented in the Historical Performance Graph pane or in the Historical Performance Table pane.

Selector Control area

The Selector Control area is used for selecting data to present in the Historical Performance table. The Selector Control area contains a NE Name table and a Performance Type table.

When both NE and Performance type are selected, historical performance can be read from the database by clicking Refresh Data icon on the view toolbar.

NE Name table

The table contains network elements that the PTP 820 NMS server might have read historical performance data from. In the above [example](#), the table contains NE from the [domain](#) "Oaxaca" (=the [scope](#) on the view tab in this example). Each NE in the table is identified by the following fields:

Table 27 NE name table

Name	Explanation
NE Name	The name of the equipment containing this parameter
Product Name	The type of NE

Click a checkbox with a NE in the table to select/unselect presenting historical performance from resources on this element. When the amount of NE in the table is large, the [Quick Search](#) field for the NE Name table is useful for filtering.

Performance Type table

This table contains all performance types/subtypes available from the NE in the scope. In the above [example](#), the NE contains parameters of all performance types, but if fewer performance types were available in the elements in the NE Name table, only these were presented.

The following performance types might be found in the table, depending on NE types and configurations in the scope:

Table 28 Performance type table

Name	Explanation
G.821ACM	Measurements that can be read from the Q1 NE-types NL18xAdaptive Coding and NL24x. Can include subtypes of both 15min and 24hModulation measurements.

Name	Explanation
G.826	Measurements that can be read from the Q1 NE-types InterLink, CityLink and NL29x. Dependent of. Depending on the configuration of the elements, this can include performance subtypes B1 , B2 , PDH Parity and Link Errors . Can include subtypes of 15min measurements, 24h measurements and monthly measurements.
MSE	Mean Square Error measurements.
Power Levels	Analog measurements of received and transmitted power level from Radio. Can include subtypes for 1min registers, 15min registers and 24h registers from NE.
Ethernet Statistics	A set of measurements for ethernet traffic that can be read from NEs..
Power Supply	Analog measurements from power supply

Click a checkbox in the table to select/unselect presenting historical performance of this performance type/subtype.

Timeslider tool for Historical Performance view

The Timeslider tool can be used for navigating in the historical performance data PTP 820 NMS already have read, as according to the selection in the Selector Control area. Please see [user manual description about the Timeslider](#) for how to operate this tool.

Historical Performance table

When the Table pane is selected in the Historical Performance view, the data will be presented in a table.

Figure 75 Historical performance view

Resource	Parameter	Value	Unit	Type	Status	Number of Periods	Period Start Time...	Period Start Time...	Period End...	Period End Time...
R5-S2-116/117/Radio-12	Profile Max	7	profile	ACM Profile 24h	Valid	1	November 30, ...	November 29, ...	November 30, ...	November 30, ...
R5-S2-116/117/Radio-12	Profile Min	7	profile	ACM Profile 24h	Valid	1	November 30, ...	November 29, ...	November 30, ...	November 30, ...
R5-S2-100/102/Radio+HSB.1	ES	0	seconds	G.826 Radio Ag...	Valid	1	November 30, ...	November 29, ...	November 30, ...	November 30, ...
R5-S2-100/102/Radio+HSB.1	SES	0	seconds	G.826 Radio Ag...	Valid	1	November 30, ...	November 29, ...	November 30, ...	November 30, ...
R5-S2-100/102/Radio+HSB.1	UAS	0	seconds	G.826 Radio Ag...	Valid	1	November 30, ...	November 29, ...	November 30, ...	November 30, ...
R5-S2-100/102/Radio+HSB.1	BBE	0	errors	G.826 Radio Ag...	Valid	1	November 30, ...	November 29, ...	November 30, ...	November 30, ...
R5-S2-100/102/Radio+HSB.2	ES	0	seconds	G.826 Radio Ag...	Valid	1	November 30, ...	November 29, ...	November 30, ...	November 30, ...
R5-S2-100/102/Radio+HSB.2	SES	0	seconds	G.826 Radio Ag...	Valid	1	November 30, ...	November 29, ...	November 30, ...	November 30, ...
R5-S2-100/102/Radio+HSB.2	UAS	0	seconds	G.826 Radio Ag...	Valid	1	November 30, ...	November 29, ...	November 30, ...	November 30, ...
R5-S2-100/102/Radio+HSB.2	BBE	0	errors	G.826 Radio Ag...	Valid	1	November 30, ...	November 29, ...	November 30, ...	November 30, ...
R5-S2-100/102/Radio+HSB.1	Profile Max	7	profile	ACM Profile 24h	Valid	1	November 30, ...	November 29, ...	November 30, ...	November 30, ...

The table presents the historical performance data last read from this NE. Each performance measurement is identified by the following fields:

Table 29 Historical performance table

Name	Explanation
Resource	The name of the equipment containing this parameter
Parameter	<p>The performance measurement types on the selected equipment, e.g.</p> <p>performance measurement types (as defined in G.826/G.821):</p> <p>SES - Severely Errored Seconds, a one-second period with one Errored Block Overstep (EBO) and/or one Severely Errored Overstep(SEBO)</p> <p>UAS - Unavailable Seconds.</p> <p>BBE - Background Block Error.</p> <p>ES - Errored Second, a one-second period with one or more Error Blocks (EB).</p> <p>DM- Degraded Minutes, error pulses</p> <p>power levels, such as:</p> <p>RPL - Received power level</p> <p>RPL_SDIV - Received power level on space diversity equipment</p> <p>ethernet statistics, such as:</p> <p>Drop Events In</p> <p>Packets In</p> <p>power supply, such as:</p> <p>Battery Voltage</p> <p>Battery Current</p>
Value	The measured performance value received from the NE
Unit	The measure unit for the Value
Type	The performance subtype, as selected in the Performance Type table.
Status	<p>The condition of the received data:</p> <p>Valid - equals: performance measurement is valid</p> <p>Invalid - equals: received performance data is not valid</p> <p>Unavailable - equals: performance data currently is not available for this NE, most likely due to time out</p>
Number of periods	Amount of measurements with same value. If several identical values are read, only Number of periods and period End Time are updated on this measurement.
Period Start Time (System)	The server time when the measurement was started on the NE

Name	Explanation
Period End Time (System)	The server time when the measurement was completed on the NE
Period Start Time (NE)	The timestamp from NE when the measurement was started on the NE
Period End Time (NE)	The timestamp from NE when the measurement was completed on the NE

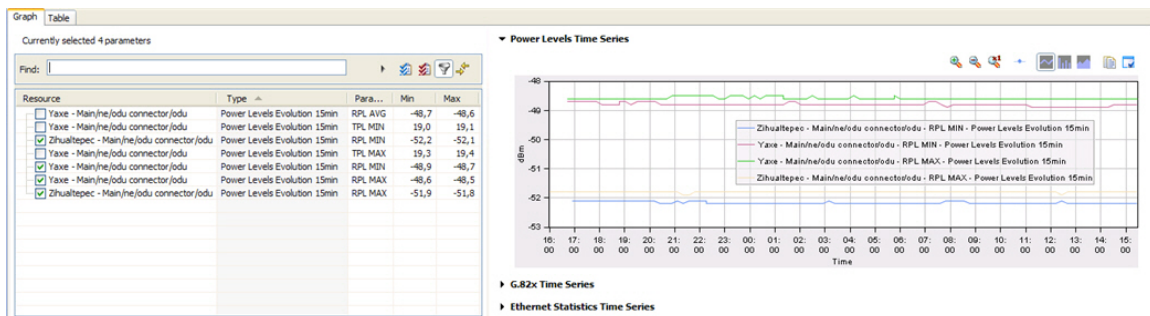
The data in the table can be exported to Excel spreadsheet, comma separated file or extensible markup language.

When the amount of data in the table is large, the [Quick Search](#) field for the Historical Performance table is useful for filtering.

Historical Performance graph

When the Graph pane is selected in the Historical Performance view, the data will be presented in a graph.

Figure 76 Historical performance graph



The Historical Performance pane consists of a Historical Data Selection table and a Historical Performance Graph area.

Historical Data Selection table

This table presents parameters on resources that PTP 820 NMS has read historical performance data from in the time interval specified by the Timeslider tool.

Each parameter/resource is identified by the following fields:

Table 30 Historical data selection table

Name	Explanation
Resource	The name of the equipment containing this parameter
Type	The performance subtype, as selected in the Performance Type table.

Name	Explanation
Parameter	<p>The performance measurement types on the selected equipment, e.g.</p> <p>performance measurement types (as defined in G.826/G.821):</p> <p>SES - Severely Errored Seconds, a one-second period with one Errored Block Overstep (EBO) and/or one Severely Errored Overstep(SEBO)</p> <p>UAS - Unavailable Seconds.</p> <p>BBE - Background Block Error.</p> <p>ES - Errored Second, a one-second period with one or more Error Blocks (EB).</p> <p>DM- Degraded Minutes, error pulses</p> <p>power levels, such as:</p> <p>RPL - Received power level</p> <p>RPL_SDIV - Received power level on space diversity equipment</p> <p>ethernet statistics, such as:</p> <p>Drop Events In</p> <p>Packets In</p> <p>power supply, such as:</p> <p>Battery Voltage</p> <p>Battery Current</p>
Min	The minimum value for this parameter within the time interval
Max	The maximum value for this parameter within the time interval

Click a checkbox in the table to select/unselect presenting historical performance of this performance type/subtype. Whenever a parameter/resource is selected in the table, a graph will immediately be displayed in the Historical Performance Graph area. When the amount of parameters/resources in the table is large, the [Quick Search](#) field for the NE Name table is useful for filtering.

The Hide constant data sets operation can be used to hide the resources/parameters that does not have any changes in values within the selected time interval.

The Synchronize all X-axis operation can be used to compare graphs of different performance types, and provides that the 3 graphs will have exactly the same x-axis.

Historical Performance Graph area

This area contains a graphical presentation of the performance data on the resources specified in the Historical Data Selection table. The Historical Performance Graph area contains different graphs for the 3 main different types of performance.

Table 31 Historical performance graph area

Name	Explanation
Power Levels Time Series	Analog measurements of received and transmitted power level from Radio.
G.82x Time Series	G.821 and G.826 measurements
Ethernet Statistics Time Series	Ethernet traffic measurements.
Ethernet Utilization Time Series	Ethernet utilization measurements.
Power Supply Time Series	Analog measurements from power supply.

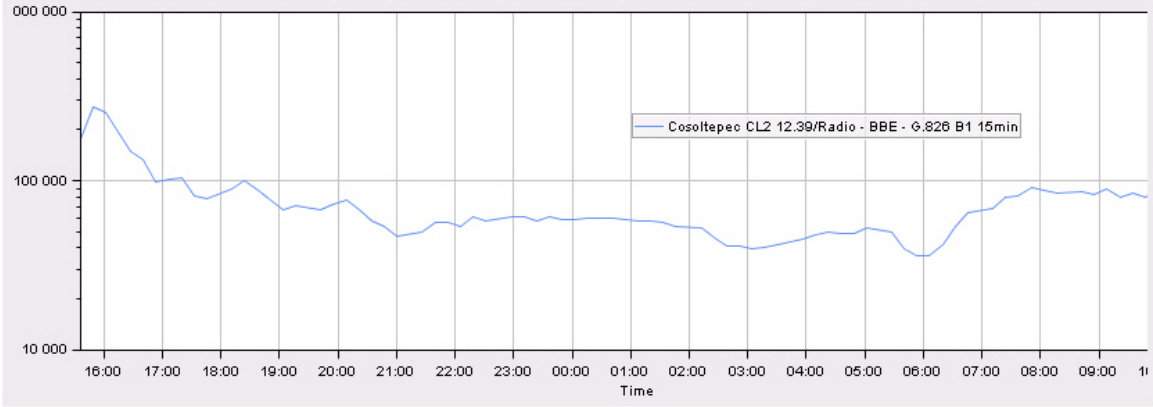
Each graph has a show/hide button to the left of the graph name.

When a graph not hidden, a graph toolbar can be found on each graph. The toolbar contains a set of operations for zooming, visual appearance, graph style and copy to clipboard. The graph styles Line graph, Bar graph and Area graph can be selected individually for the three graphs. Periods with invalid or missing performance data will be indicating with a "hole" in the graph.

Line graph

This is an example of a G.826 Time Series performance data in Line Graph mode:

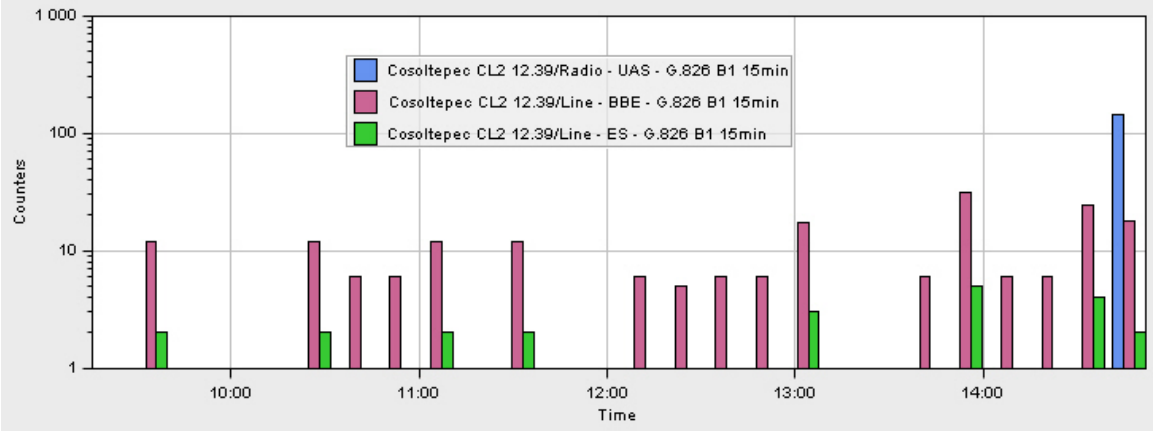
Figure 77 Line graph



Bar graph

This is an example of a G.82x graph in Bar Graph mode:

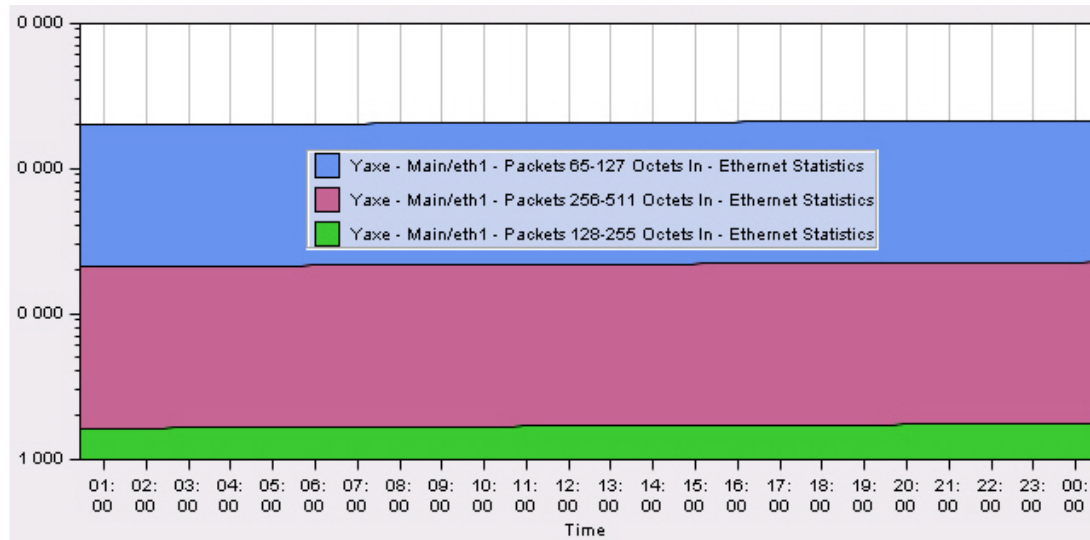
Figure 78 Bar graph



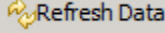







Area graph





















This is an example of an Ethernet Statistics graph in Area Graph mode:



Figure 79 Area graph



Available operations

-  **Refresh Data** Click to update graph/table with new/updated data from the database.
-  Extend previous read by adding 24 h of performance data prior to the currently oldest data. This corresponds to dragging the edge of the [Slider](#) to the left and adds a full read to the existing data already listed. The stop position is kept as before.
-  Get previous read by moving 24 h of performance data prior to the currently oldest data. This corresponds to positioning the Slider one 24 h period to the left of the current start position. The stop position is the previous start position.
-  Get next read by moving 24 h of performance data after the currently newest data. This corresponds to positioning the Slider to current stop position. The new stop position is 24 h after the previous stop position.
-  Extend next read by adding 24 h of performance data prior to the currently oldest data. This corresponds to dragging the edge of the Slider to the right and adds a full read to the existing data already listed. The start position is kept as before.
-  Go to selected time and date. This button opens the [Date and Time dialog](#). This corresponds to setting this date and time as a new starting point for the Slider. Data will be read from this starting point and new stop position is 24 h after the new starting point.
-  **Show Timeslider** - Show/hide the [Timeslider](#) tool.
-  **Show Timeslider scrollbar** Show/hide the Timeslider scrollbar at the bottom of the Timeslider tool. Whenever the Timeslider is [zoomed](#), the scrollbar can be used for navigating Timeslider bar along the time axis.

-  **Hide Selector** Click to hide the [Selector Control](#) area.
-  **Show Selector Control** Click to show the Selector Control area.
-  **Export to File...** Export your current data to file. You are allowed to save the table as an Excel spreadsheet (.xls), comma separated file (.csv) or extensible markup language (.xml)
-  **Customize Columns...** Open the [Customize Columns](#) dialog for the Active alarms view. In this dialog you can select which columns will be displayed in the table, and the order in which they appear.
-  Click a checkbox in the [NE Name](#) table to select/unselect reading performance from this element. Click a checkbox in the [Performance Type](#) table to select/unselect reading this performance type/subtype.
-  Select all checkboxes in the NE Name table or Performance Type table.
-  Unselect all checkboxes in the NE Name table or Performance Type table.
-  Click a Performance Type to expand a list of Performance Subtypes in the in the Performance Type table.
-  Double click inside the Historical Performance table or the Historical Data Selection table to [hide/show](#) the Selector Control area.
-  When this option is selected on the Historical Data Selection toolbar, only resources/parameters with changes in data values within the time interval, will be shown in the Historical Data Selection table.
-  When this option is selected on the Historical Data Selection toolbar, all graphs will have the identical X-axis, and all [zooming](#) within a graph will be synchronized with the other graphs.
-  Click to Show/Hide this graph.
-  Click to Zoom In along the X-axis on this graph
-  Click to Zoom Out along X-axis on this graph
-  Click to Reset Zoom on this graph
-  When Show Marker is selected on a Graph toolbar, each measurement will be indicated with a dot in the graph.
-  Click to display this graph as in Line Graph mode.
-  Click to display this graph as in Bar Graph mode
-  Click to display this graph as in Area Graph mode
-  Click to Copy to clipboard. This makes a copy of this graph available for pasting into other external applications.

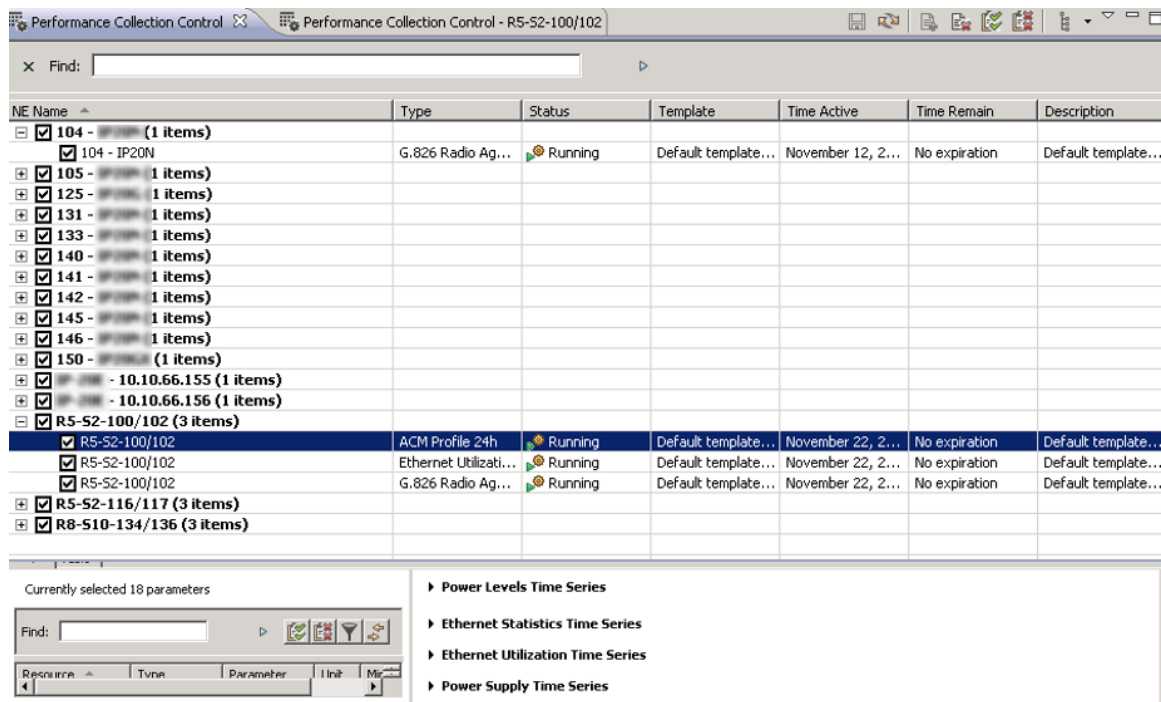
-  Click Change Visual Appearance to open the Chart Style of Performance Graph dialog. Here you can change colour settings and font for Plotting area, Gridlines, Axis, Legends and Chart Text.
-  click and drag inside a graph to [zoom in](#).

Performance Collection Control view

This view is opened by selecting **Views > Performance > Performance Collection Control** in the top menu. Alternatively, it can be opened scoped by selecting a NE in one of the topological views (**Geographical** or **Logical Map**, or **Tree**) and selecting **Performance > Performance Collection Control** from the context menu.

If there is no NE with performance parameters available in your selection, the view will open empty.

Figure 80 Performance collection control view



In this view, you can start and stop performance collection from NE, by assigning the templates created in the [Performance Templates](#) view. When performance collection from NE is enabled in this view, PTP 820 NMS will start storing performance data that can be presented in the [Historical Performance](#) view.

We use the term "assign a template to the NE", even though no change is actually made to the NE when assigning a performance template. The performance template is solely a definition of how PTP 820 NMS should collect a set of performance parameters type from a NE.





The Performance Collection Control view consists of a table containing the following columns:










Table 32 Performance collection control attributes

Name	Explanation
NE Name	The NE you can collect performance from. Each NE can have several associated alarm templates.
Type	Each performance type can have several associated performance templates.
Status	Displays the status about on performance collection using this template. Can be one of the following values Idle: performance data is not started Running: the server is currently polling this NE for performance data using this template Pending: the change on starting/stopping performance collection has not been saved to server yet.
Template	The name for the template, as defined in Performance Templates view.
Time Active	The time on the EMS server when collection was started using this template.
Time Remain	The time remaining until performance collecting stops, as according to in the Duration field for this template
Description	An optional text describing a template, as defined in Performance Templates view.

When the table is [grouped by NE Name](#) (default), each line in the table contains either an NE or a template. You can then click the [Expand](#) icon to see a list of all templates which currently is assigned to this NE. If no templates are assigned, the list will be empty. New templates can be assigned by selecting a NE in the NE Name column, and then use the [Assign Template](#) icon on the toolbar.

Available operations

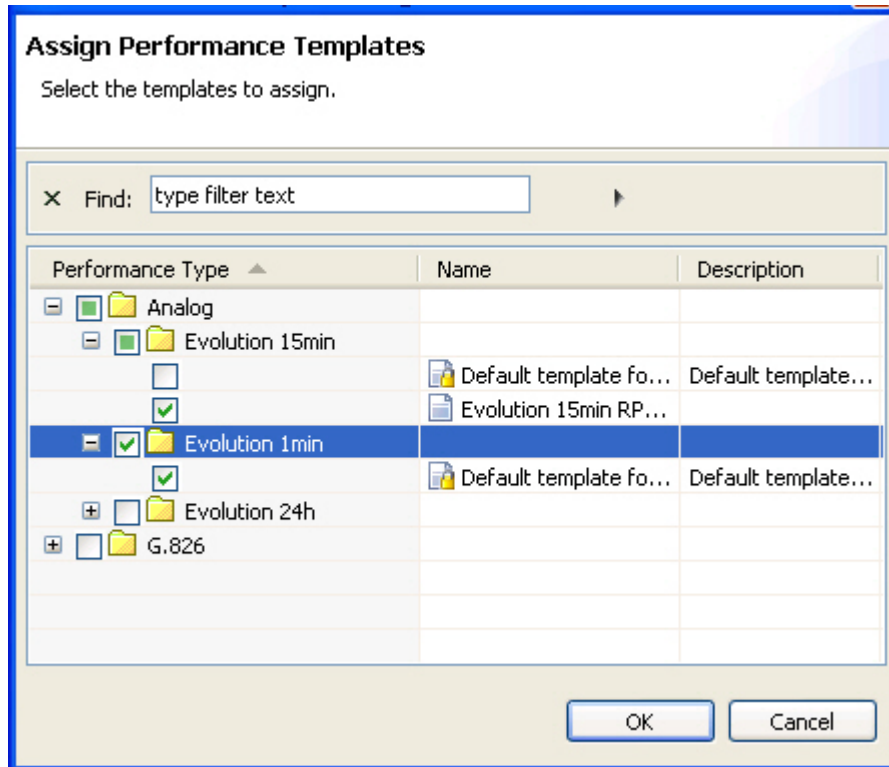
-  Click the checkbox to start/stop performance collection with one or more NE/templates in the table. The collection will start/stop when changes are saved and applied the view.
-  When the view is [grouped](#), you can click to [expand](#) the table to see all NE or templates within each group in the Performance Templates table.
-  Refresh Refresh the view, so that it is updated with the latest current template assignments and template definitions from the server.
-  Apply and save all changes made to template assignments in this view. If this view is closed without saving data, the [Save Changes](#) dialog will appear.

-  **Assign Templates...** Assign one or more new alarm template to one or more of the currently selected NE in the table, by using the [Performance Template Assignment](#) dialog
-  **Remove Assignment** Remove all currently selected templates from one or more NEs in the table.
-  **Enable All** Start performance collection on all templates for all NEs in the view.
-  **Disable All** Stop performance collection on all templates for all NEs in the view
-  **Group By** Select how to present the data, grouped by NE Name, Type, Template or None.
-  **Performance Templates** Open the [Performance Templates](#) view to create, view, update or delete templates.
-  **Show Quick Search** Enable the [Quick Search](#) field in the Performance Collection Control view. The quick search functionality makes it possible to search the contents of the view. All visible columns can be searched.
-  **Export to File...** Open the Save As dialog for the Performance Collection Control view, where you can export the content of the table to disk. Supported file format Supported file formats are Excel spreadsheet (.xls), comma separated file (.csv) or extensible markup language (.xml).
-  **Customize Columns...** Open the [Customize Columns](#) dialog for the Performance Collection Control view. In this dialog you can select which columns will be displayed in the table, and the order in which they appear.

Performance Template Assignment dialog

This dialog appears whenever you select [Assign Templates](#) with one or more NE selected in the Performance Collection Control table:

Figure 81 Assign performance templates



Expand the tree of performance types and click the checkboxes to assign a new template to the currently selected NE(s). After pressing OK, you will see the performance template assigned to the NE(s).

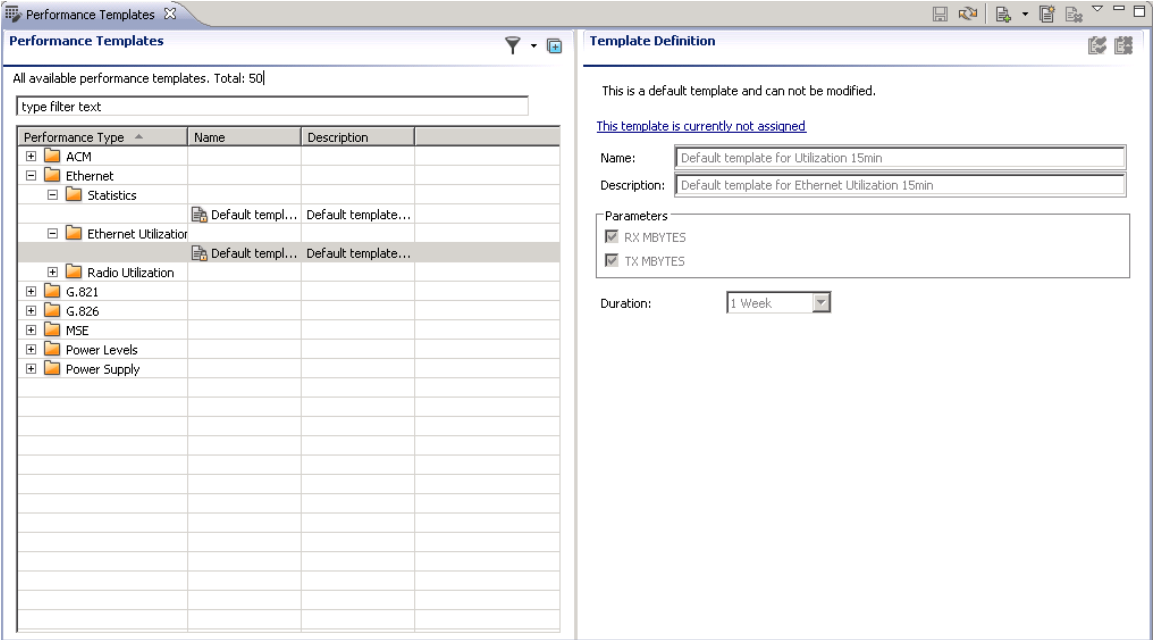
Each NE can only have one template of each Performance Type assigned. As a consequence, it is not possible to add a template of a type that is already assigned.

The dialog will only present templates of a performance type that valid for one or more of the currently selected NE(s). This means that the dialog might present some performance types that are only valid for a subset of the currently NE. If you try to add templates to more than one NE at the time, only templates that are supported for each NE will be assigned when pressing OK.

Performance Templates view

This dialog is opened by selecting **Views > Performance > Performance Templates** in the top menu.

Figure 82 Performance templates view



In this view you can create templates for collecting performance data from network elements.

The templates created in this view are used by the [Performance Collection Control](#) view, to select what performance data to collect from each element. If templates are already used for collecting performance data, changes in the Performance Templates view might affect the performance data presented in the [Historical Performance](#) view.

The Performance Template view consists of a Performance Templates area containing a table of alarm templates grouped by performance types, and a Template Definition area containing details about the currently selected performance template.

Performance Templates area

The Performance Templates area consists of a table containing the following columns:

Table 33 Performamnce template area attributes

Name	Explanation
Performance type	Each performance type can have several associated performance templates. Click the Expand icon to the left of the performance type to expand a list of all templates which have currently been created for that performance type.
Name	<p>A user defined name for each template.</p> <p>Click a template to view details about that template. Right click a template to clone or delete the currently selected template.</p> <p>For each performance type there is one default template with pre-defined settings, and cannot be changed by user. Note that default templates and templates assigned to one or more elements cannot be deleted.</p>
Description	An optional text describing a template.

Each line in the table contains either a performance type or a template. Select a type in the Performance Type column to create a new alarm template, or select a template to view its properties.

Template Definition area









This area appears when a template is selected in the table in the Performance Templates area.

The Template Definition area contains the following values:

Table 34 Template definition area attributes

Name	Explanation
Assignment link	<p>This is a link with a text describing how many elements this template is assigned to.</p> <p>Clicking the link text will open the Performance Collection Control view, filtered on the current Performance Template name.</p> <p>As performance are collected using the Performance Template, the link text will display the number of elements currently assigned to it. When no element is assigned, the initial text is "This template is currently not assigned".</p>
Name	A name for each template, can be edited in the Template Definition area.
Description	An optional text describing a template, can be edited in the Template Definition area.
Parameters	A list of available parameters within the currently selected performance template. Check/uncheck parameters to add/remove from the template.
Duration	A limit for how long data will be collected using this template. For some parameter types, the value No Expiration is available.
Polling Interval [sec]	<p>For some parameter types, (PTP820-related performance templates and Ethernet statistics templates), the user can specify how often the server should poll the elements for updates in parameter values.</p> <p>Note that collected measurements with a granularity of 24 hours or 1 month are never detected.</p> <p>The performance templates' polling interval must be a multiple of 15 minutes</p> <p>PTP820 performance templates:</p> <ul style="list-style-type: none"> • ACM - Profile 15min/24h • G.826 - Radio Aggregate 15min/24h • MSE - MSE 15min/24h • Power levels - PTP 20 15min/24h

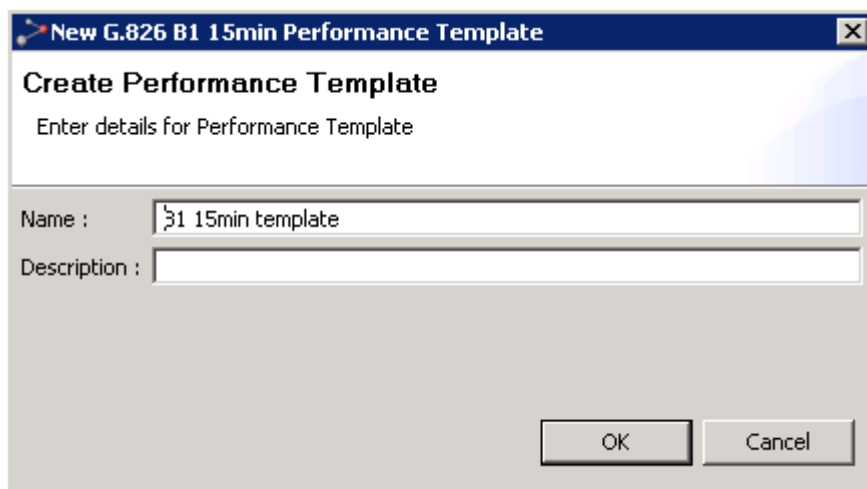
Available operations

-  **Save Modifications** Save all changes made to the templates in this view. When changes have been saved, the updates in the performance templates can influence the performance collection on the assigned elements.
-  **Refresh** Refresh the view to receive updated data from server.
-  **New Performance Template** Add a new template. The [New Performance Template](#) dialog will be opened.
-  **Clone** Clone the selected template. The [New Performance Template](#) dialog will be opened. This menu item will only be available if a template is selected in the Performance Template table.
-  **Delete** Delete the selected template. This menu item will only be available if a template is selected in the Performance Template table.
-  **Horizontal** Arrange the view horizontally.
-  **Vertical** Arrange the view vertically.
-  **Export to File...** Open the Save As dialog for the Performance Templates view, where you can export the content of the table to disk. Supported file formats are Excel spreadsheet (.xls), comma separated file (.csv) or extensible markup language (.xml).

New Performance Template dialog

This dialog is opened when using Create New Template with a performane or template type selected in the Performance Templates table.

Figure 83 New performance templates dialog



New G.826 B1 15min Performance Template

Create Performance Template
Enter details for Performance Template

Name : 31 15min template

Description :

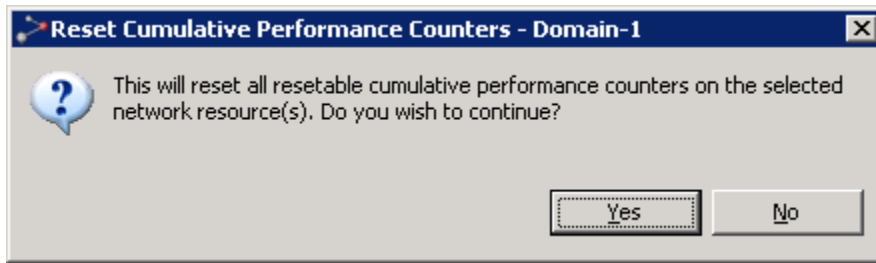
OK Cancel

Enter a name and description of the new template. After pressing OK, you will see the template in the Performance Templates table under your chosen performance type.

Reset Cumulative Performance Counters dialog

This dialog is opened by selecting an NE or domain in one of the topological views (Geographical or Logical Map, or Tree) and selecting Performance | Reset Cumulative Performance Counters from the menu.

Figure 84 Rest cumulative performance counters dialog



This is a dialog for confirming resetting of cumulative performance counters in the specified scope. "Resetting Performance Counters" means that the counter values are set to zero on the NE. This operation will not influence any performance data other than parameters of type "cumulative counters". Please note that not all performance data counters can be reset this way - which type of performance data where this operation is available will vary between NE-types and different equipment and configurations on each NE.

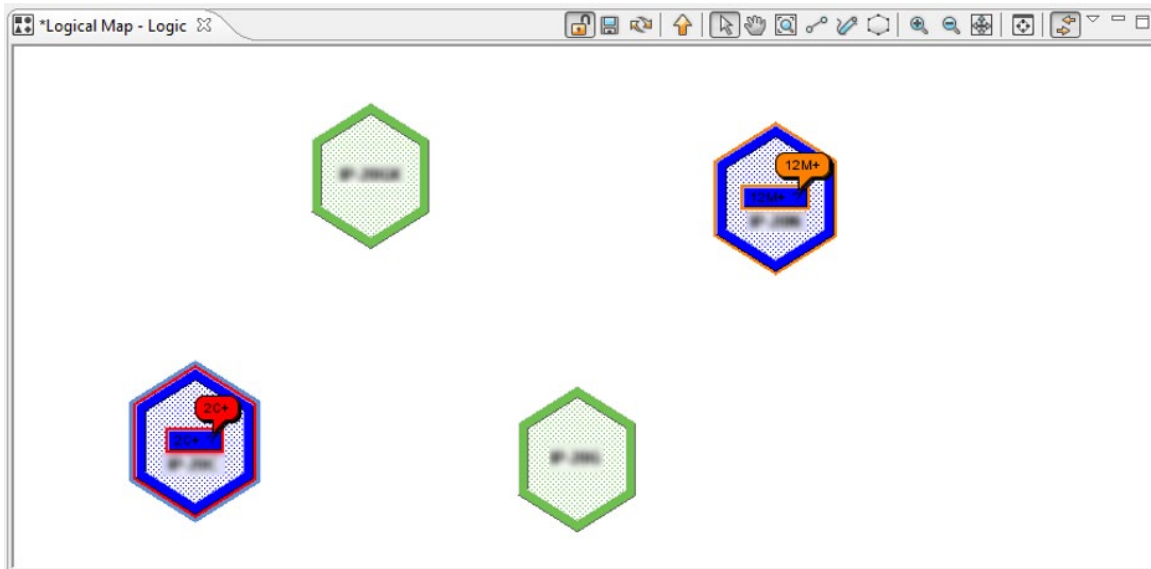
Press Yes to perform the resetting, or press No to abort.

Topology

Logical Map view

This view can be found in the [Logical Surveillance](#) perspective, and can be opened directly from the [Logical Tree](#) view by selecting a domain and then using the Logical Map menu. The view is also opened from **Views > Topology > Logical Map** in the main menu.

Figure 85 Logical map view



This is a view for monitoring and managing your network based on a logical model, and includes an editor for creating and editing a visual representation of your logical domains.

The model used in the Logical Map view is the same as is visualized with a tree structure in the [Logical Tree](#) view. You can browse, create, delete and move logical domains, and the view also allows you to include, move and delete NEs. The structure of your domains can be used for assigning resource permissions to different groups of users in the [Group Administration](#) view.

In the Logical Map view, you can create domains/sub-domains corresponding to a logical model of your NE. Examples of logical models are:

- Element type, element subtype, etc.
- Regional zones (with domains reflecting a geographical division of your network, but with boundaries which might overlap other geographical zones)
- Transmission capacity (e.g. 155/145Mb, 45/34Mb, 1.5/2Mb, etc.)
- Data communication network (with domains reflecting the physical connection of your network, which might overlap and differ from a geographical division)
- Company, contractor, party responsible
- Usage (e.g. main network, encrypted network, backup)
- Security profile (reflecting which security profile used for the NEs in each domain)

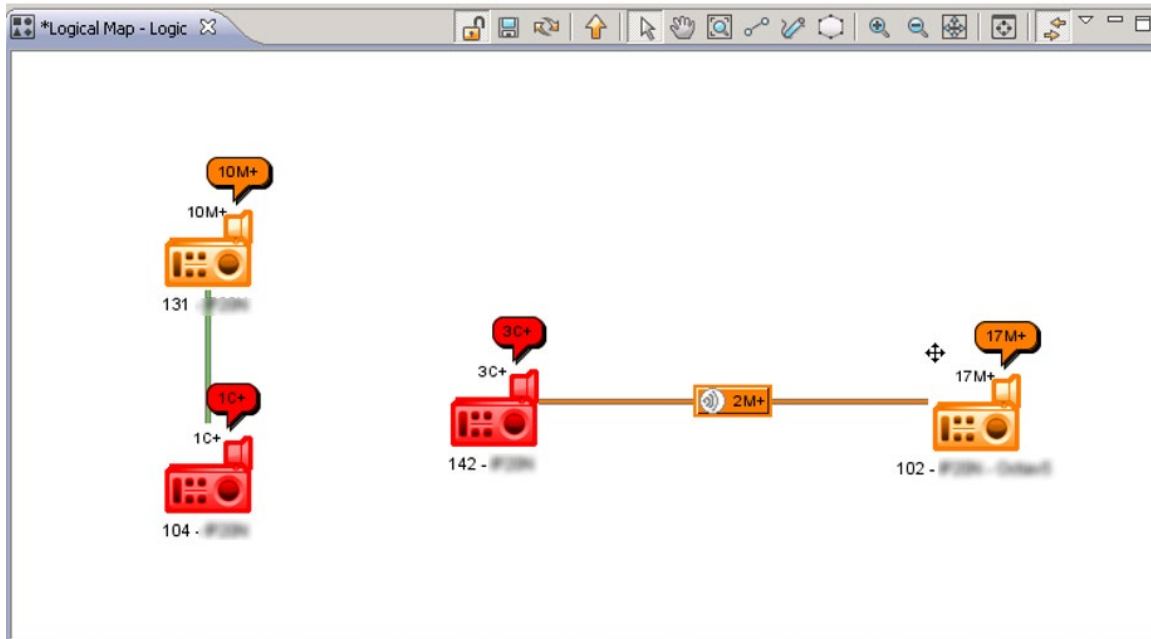
As this logical organization can be completely independent of the NE's geographical location, the same NE can exist in both models at the same time, or in only one. The Logical Model is completely separate from the Geographical Model used in the [Geographical Map](#) view. The two Map views operate on different models, but otherwise have exactly the same functionality.

The current alarm status for the different parts of your network are visualized in the map using colors, alarm counts and symbols. Details about alarms and how visualization is shown can be found in the chapter about [visualization of alarms](#).

In the above example, the Logical Model is organised by element types. We can, for example, see that the PTP820G and PTP820GX elements have a light green border, indicating no alarms. Both the PTP820C and the PTP820N elements have a blue border, indicating they are disconnected. The PTP820C element has an additional red border, and shows it has (at least) 2 new alarms with severity "Critical" (=red). The PTP820N element has an additional orange border, and shows it has (at least) 12 new alarms with severity "Major" (=orange).

The [scope](#) in the title of the view indicates the name of the domain currently displayed. In the above example, the title "Logic" indicates that the map currently displays the content of the domain "Logic" (which was the name of the top-level domain of this Logical Model)

In another example, NEs can be seen with topological links.

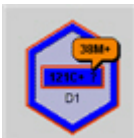
Figure 86 NEs topological links

In this example, the logical map shows some NE in the topological domain "Logic". We can, for example, see that the radio link "Ridge-Kotoka_Kotoka-Ridge" is solid orange, while the link "Dzorwulu long hop" colorless. This tells us:

- There are no new (unacked) alarms on the radio endpoints connecting the NE's 104 and 131.
- There are two new alarms with severity "Majorr" (=orange) on the radio endpoints connecting the NE's 142 and 102.

The objects in a map

Domains



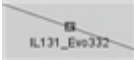
The colours of the [domain](#) represents the alarm state of all NE and subdomains contained in the domain, so that the color of the most severe alarm is presented. Details of alarms and how colours are used for presenting alarms in the tree can be found in the chapter about [visualization of alarms](#).

Network Elements (NE)




The colours of the [NE](#) represents the alarm state of the most severe alarms on the NE. Details of alarms and how colours are used for presenting alarms in the tree can be found in the chapter about [visualization of alarms](#).

Topological Links between NE


















A [topological link](#) between two NE in the map can represent termination points within same layer rate on each of the two NE, e.g. two ODU's connected with a radio link, or two or more E1 ports connected with an electrical cable. Alarm severity from [unacked](#) alarms on these connected termination points can be visualized on the link.

Radio links will be displayed in the map view with this icon: 



A topological link can only exist when both end-points of the link exist in the same domain. I.e. deleting one of the end NEs or moving one of the end NEs, will delete the link between them.



Available operations

-  Start editing the map.
-  Save Map Save the changes in the view. All changes to domain polygons, coordinates and background images are not saved on the server until the Save icon has been clicked. If moving to another domain level or trying to close a view without saving changes, the [Save Modified View](#) dialog will appear.
-  Refresh the view.
-  Up Go up one level, to the Parent Domain. The parent domain contains the current domain as a "child", and when going up one level the shape/outline of the previous domain and its "siblings" will be displayed (this operation is the opposite of [Doubleclick a Domain](#)).
-  Select Select. each domain and NE in the view with this tool. Hold down the shift key while selecting to select multiple objects. When the Select tool is enabled, you can:
 - -drag an object (domain or NE)
 - -open context menus for the currently selected object (domain or NE)
 - -Double-click a Domain to go down to this level in the Logical Map view (this operation is the opposite of [Go to Parent Domain](#))

-  **Pan** Pan the screen by dragging it in the direction you want.
-  **Zoom In** Zoom in on a specific area of the view by clicking and dragging a rectangle over the area you wish to see in more detail. When the mouse button is released the view will display only this selected area.
-  **Draw New Domain** Create a new logical domain by drawing a polygon outline in the view using this tool. Click once for each new polygon corner you want to create, and double-click to finish. When you have finished editing, the [New Administrative Domain](#) dialog will open, where you can enter a name for the domain. If relevant for your Logical Model, adding a [background image](#) to your map before drawing domains might help when drawing your map objects.
-  **Edit Domain Outline** Edit the shape of your logical domain outlines using this tool. You can:
 - click a corner and drag it in any direction
 - ctrl+click directly on a corner to delete it
 - ctrl+click on a line to create a new corner
-  **Create Link** Create a new [Topological Link](#) by drawing a line between two NEs in the view. When you have completed the link the [New Topological Link dialog](#) will open, where you can enter details for the link.
-  **Zoom In** Click to zoom in on a smaller area.
-  **Zoom Out** Click to zoom out to a larger area
-  **Zoom to Fit** Zoom and pan so that all objects on this level is displayed in the view.
-  **Map Overview** Open the [Map Overview](#) tool in a new view, where you can pan and zoom the area currently displayed
-  **Lock Map** Lock the map. This will disable
 - the movement of objects in the map
 - the changing of the shape of domain polygons
 - the creation of new domain polygons







If the map is locked, you can unlock it by pressing this icon again.

-  **New Domain** Create a new sub-domain under the currently selected domain. The [New Administrative Domain](#) dialog will open, where you can enter a name for the new domain.
-  **Include Managed Element** Select one or more managed NE from the Geographical Model and manage them in the Logical Model by placing them under the currently selected domain. The [Include Managed Elements](#) dialog will appear, where you can view the list of unmanaged elements and select which NE you want to manage.

-  **Move** Move the currently selected node (NE or sub-domain) to under another domain. If the node contains a sub-tree, this sub-tree with all its nodes will also be moved to the new domain. The [Move Resource](#) dialog will open where you will be able to select the domain you want to move the node to. The outline/shape of a domain will not remain when moving it.
-  **Delete** Delete the currently selected node (NE or sub-domain).

If the currently selected node is a domain, the entire sub-tree of domains and all its NEs will be deleted and the [Delete Domain from Model](#) dialog will be opened, where you can confirm or cancel the operation.

If the currently selected node is an NE, the [Delete Network Element from Model](#) dialog will appear. In this dialog you can also choose to remove the NE from the Geographical Model.

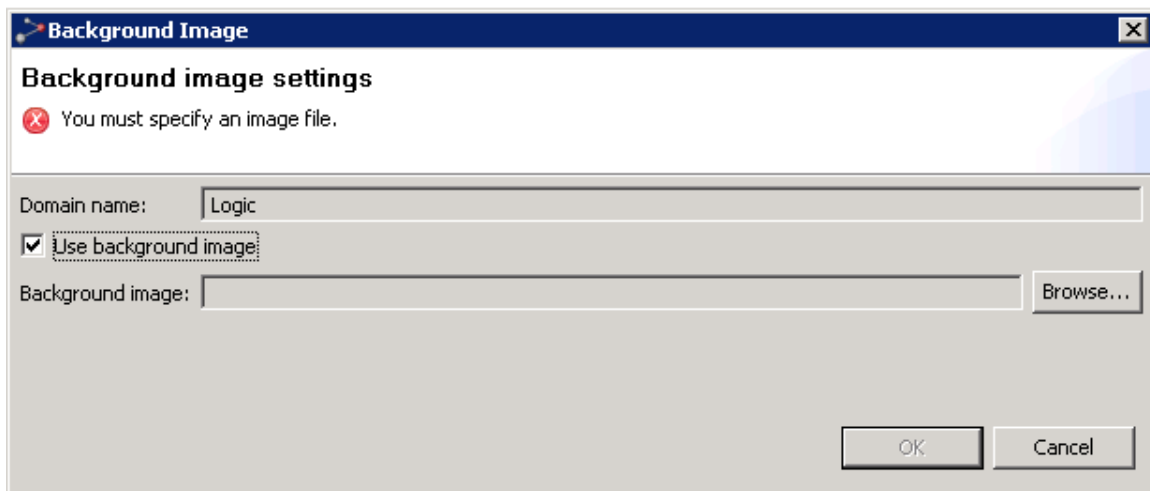
-  **Rename** Rename the currently selected node by opening the [Rename](#) dialog.
-  **Mute Notifications...** Mute an NE or a domain, to prevent alarms on the selected NE(s) from generating [alarm notifications](#). The [Mute Notifications dialog](#) will open, where you can choose to select a time for automatic unmuting the element. When being muted, NEs will have a [mute indicator](#) on NE level in the Map and Tree views.
-  **Unmute Notifications** Unmute a muted NE or a domain with muted element, to re-enable alarms on the selected NE(s) to generate [alarm notifications](#).
-  **Visible Layers** Select which layers are to be visible in the Logical Map view. Checking/unchecking menu items on this submenu allows you to hide/display:
 - Background images
 - Geographical Domains
 - Links
 - Managed Elements
 - Alarm Balloons
-  **Layout** Distribute your graphical elements within the current viewable area in the map. Selecting Random Layout will distribute your domains/NEs randomly, while selecting Grid Layout will distribute your domains/NEs in a regular grid pattern. This operation is useful when opening a domain with a lot of NEs for the first time, because all managed NEs by default are set with the same coordinates in the map.
-  **Background Image** Open the [Background Image](#) dialog, to enable/disable and select a background image to your Geographical Network view. The .gif, .jpg and .png file formats are allowed.
- In addition, the following views, dialogs and functions can be opened with data from a node in the view (using the currently selected node as [scope](#)):
 - Logical Map view
 - Logical Tree view
 - fault:
 - Active Alarms view
 - Historical Alarms view

- Alarm Templates Assignment view
- configuration:
 - Hardware Inventory view
 - Software Inventory view
 - Create Software Download Jobs wizard
 - Configuration File Management view
 - Connection Template Assignment view
 - External Tools
- performance:
 - Historical Performance view
 - Current Performance view
 - Performance Collection Control view
 - Reset Cumulative Performance Counters dialog
- reports:
 - Network Element Types Overview Report
 - Inventory Report
 - Performance Overview Report
 - Performance Details Report
- Properties view

Background Image dialog

This dialog appears when selecting the Background Image on the view dropdown.

Figure 87 Background image dialog



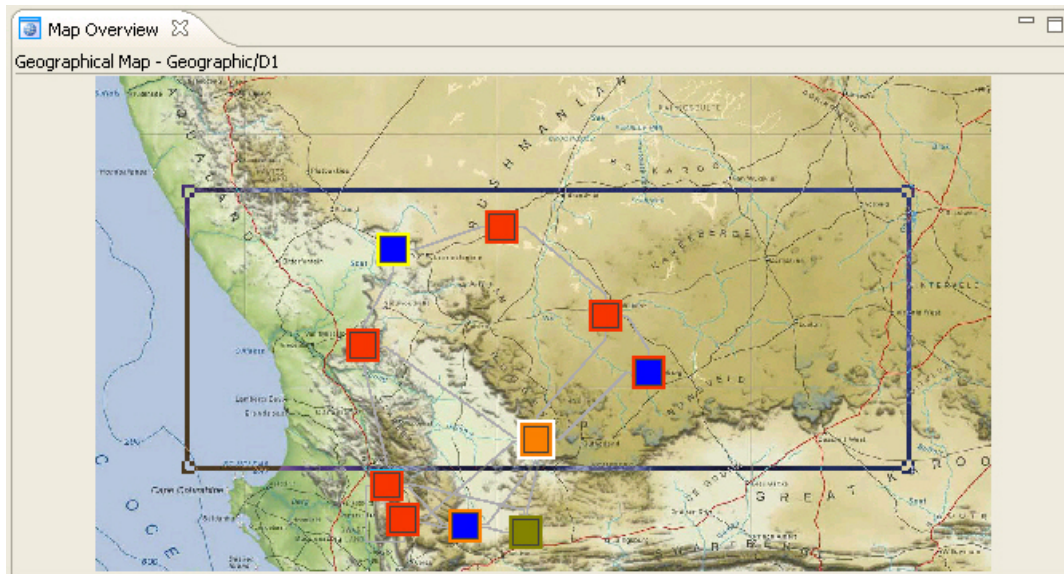
Check/ Uncheck the checkbox to enable/disable usage of background images on this level in the Logical Map. Browse your file system to find a background image and press OK, or press Cancel to abort changes.

Please note that you should avoid using images of different proportions as all background images will appear centred and in their original size.

Map Overview view

This tool appears when selecting [Map Overview](#) on the toolbar or view dropdown:

Figure 88 Map overview tool



The tool displays the entire map and a blue frame around the current viewable area in the Logical Map view. You can use the tool to do the following:

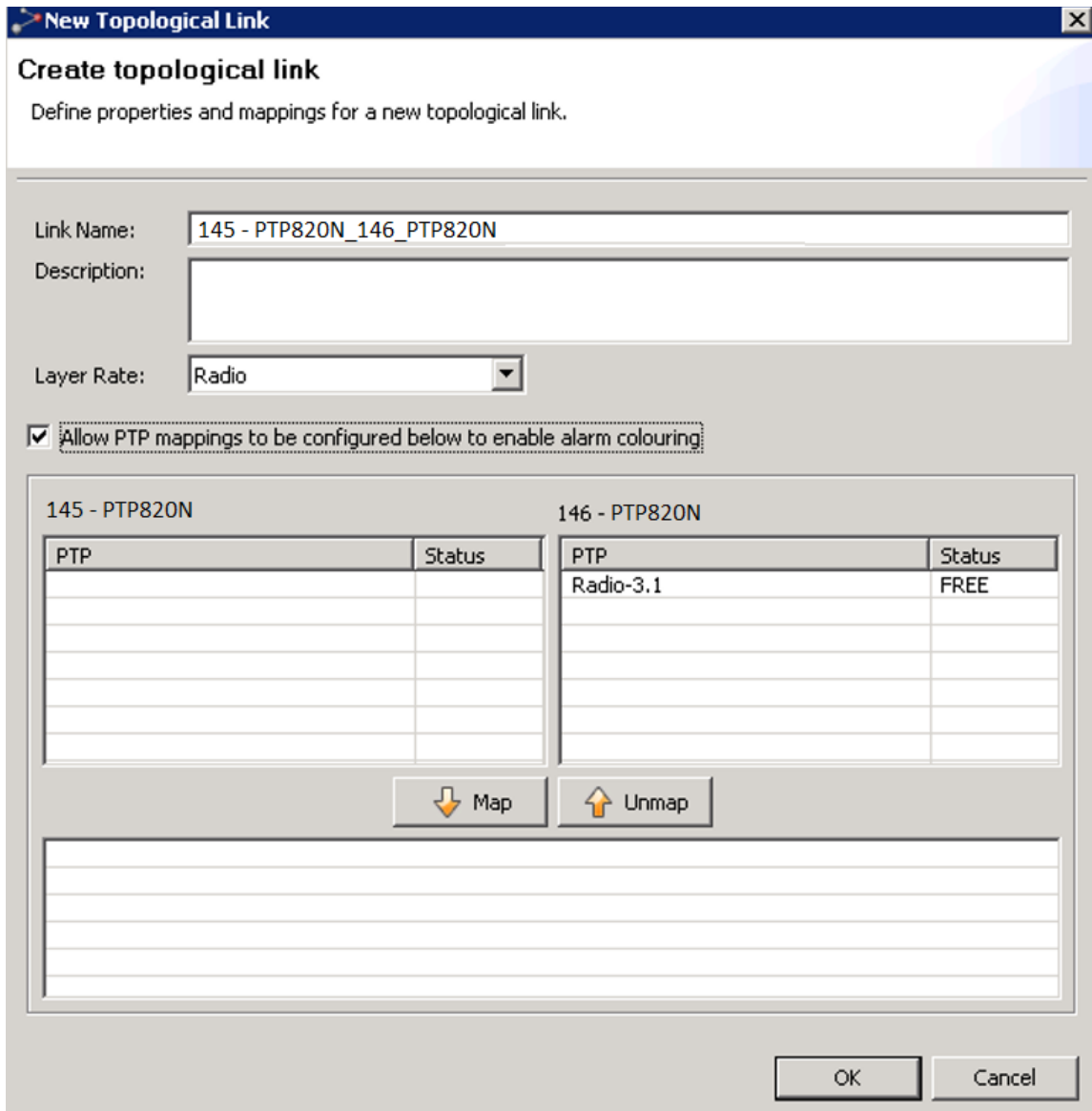
- Drag&draw the corners of the blue frame to zoom in/out the viewable area in the Logical Map view
- Drag inside the blue frame to pan the viewable area in the Logical Map view
- Click outside the blue frame to set a new centre for the viewable area in the Logical Map view

This tool can be useful when the viewable area in the Logical Map view is zoomed in to display only parts of the entire map. Please note that when the map is zoomed out to Zoom to fit (or less), the Map Overview tool cannot provide you with any useful navigation features.

New Topological Link dialog

This dialog appears whenever you are creating a topological link between two NEs:

Figure 89 New topological link dialog



The dialog box is titled "New Topological Link" and contains the following fields and controls:

- Link Name:** A text field containing "145 - PTP820N_146_PTP820N".
- Description:** An empty text field.
- Layer Rate:** A dropdown menu set to "Radio".
- Checkboxes:** A checked checkbox labeled "Allow PTP mappings to be configured below to enable alarm colouring".
- PTP Mappings:** Two side-by-side tables for configuring PTP mappings for "145 - PTP820N" and "146 - PTP820N".

PTP	Status

PTP	Status
Radio-3.1	FREE
- Buttons:** "Map" (with a downward arrow icon) and "Unmap" (with an upward arrow icon) buttons are located below the PTP mapping tables.
- Footer:** "OK" and "Cancel" buttons.

To complete the creation of the link, select a layer rate and alternatively enter a user label and a description and then press OK. Alternatively, also create terminal endpoint mapping, to enable alarms on the link.

Fields for a Topological link:**Table 35** Fields for a topological link

Name	Explanation
User Label	An optional name for the topological link. Default name is a combination of the NE names at the end points.
Description	Free text used for description of link
Layer Rate	<p>Signal type carried over this link. Depending on the termination points, the following layer rates can be available:</p> <ul style="list-style-type: none"> • radio : specifies physical media for technologies such as radio, corresponds to TMF layer rate LR_PHYSICAL_MEDIALESS • ds1 : 1.5 Mbit/s async/PDH signal, corresponds to TMF layer rate LR_T1_and_DS1_1_5M • ds3 : 45 Mbit/s async/PDH signal, corresponds to TMF layer rate LR_T3_and_DS3_45M • dsr_1 : STM-1 digital signal rate, corresponds to TMF layer rate LR_DSR_OC3_STM1 • dsr_4 : STM-4 digital signal rate, corresponds to TMF layer rate LR_DSR_OC12_STM4 • e1 : 2Mbit/s PDH signal, corresponds to TMF layer rate LR_E1_2M • e3 : 34 Mbit/s PDH signal, corresponds to TMF layer rate LR_E3_34M • ebus : proprietary EBUS signal • ethernet : all Ethernet rates, corresponds to TMF layer rate LR_Ethernet • Cascading ink • Electrical • Optical <p>If the NEs connected in the link do not share any TP endpoints of the same layer rate, the following layer rates can be selected in the dialog: radio, optical, electrical, ethernet.</p>
Allow PTP mappings to be configured below to TPs to enable alarm colouring	Select this option if you want to map termination points from each end of the topological link. When termination points are mapped, the alarmstate of these termination points will be visualized on the link in your map.

Name	Explanation
Terminal Endpoint mapping area	<p>In this area, you can define the mapping of endpoints from each end of the topological link.</p> <p>Use the Terminal Endpoint tables to select one endpoint from each side of the topological link, then press the Map button. Each time you add a pair of endpoints, they will appear in the Mapping table at the bottom of the Terminal Endpoint mapping area.</p> <p>An endpoint can have the following states in the Terminal Endpoint tables:</p> <p>FREE: this endpoint is available for mapping</p> <p>INCLUDED: this endpoint is already mapped on this topological link.</p> <p>OCCUPIED: this endpoint is mapped to another topological link</p> <p>When terminal endpoints are mapped, PTP 820 NMS will use these mappings to determine the alarmstate for the topological link. The Severity colour of unacked alarms will then be presented on the link.</p> <p>To unmap a pair of terminal endpoints, select a line with a mapping in the Mapping table and then press the Unmap button.</p>

Edit Topological Link dialog

This dialog appears whenever selecting the Edit context menu with a topological link selected in the map.

Figure 90 Edit topological link

Edit Topological Link

Edit topological link

Edit properties and mappings for an existing topological link.

Link Name: R6-S9-206_R6-S9-208

Description:

Layer Rate: Ethernet

☒ Allow PTP mappings to be configured below to enable alarm colouring

R6-S9-206		R6-S9-208	
PTP	Status	PTP	Status
ETH-1.Radio (port)	INCLUDE	ETH-1.Radio (port)	INCLUDE
ETY-1.1	FREE	ETY-1.1	FREE
ETY-1.2	FREE	ETY-1.2	FREE
ETY-1.3	FREE	ETY-1.3	FREE
ETY-1.4	FREE	ETY-1.4	FREE
ETY-1.5	FREE	ETY-1.5	FREE

Map Unmap

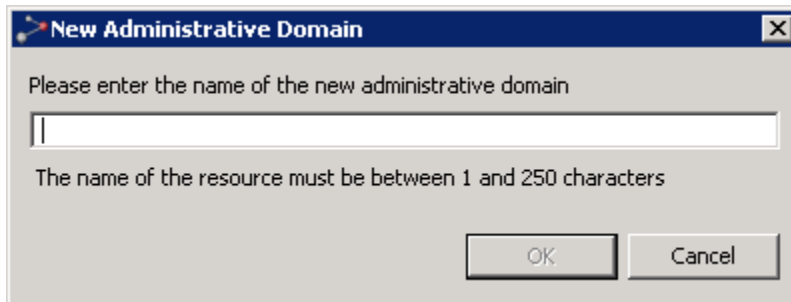
ETH-1.Radio (port) <--> ETH-1.Radio (port)

OK Cancel

Update the [fields for a topological link](#), then press OK.

New Administrative Domain dialog

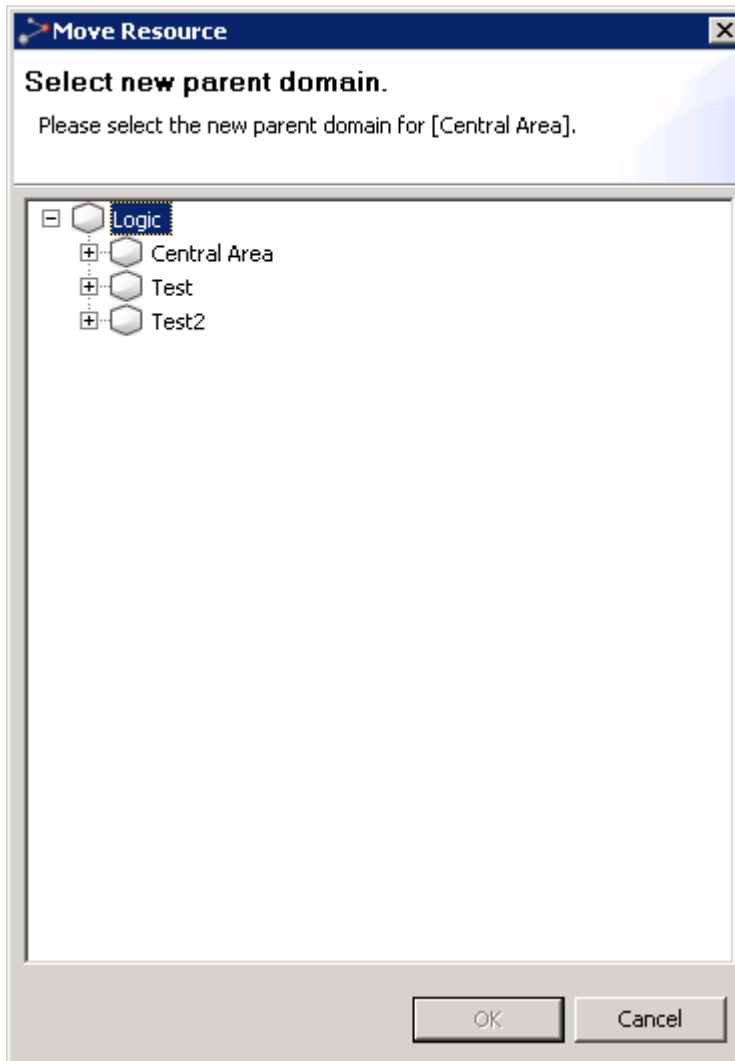
This dialog appears whenever selecting the New Domain context menu with a domain selected in the map:

Figure 91 New administrative domain dialog

Enter a name in the text field. When OK is pressed, the new subdomain is created and placed under the currently selected domain.

Move Resource dialog

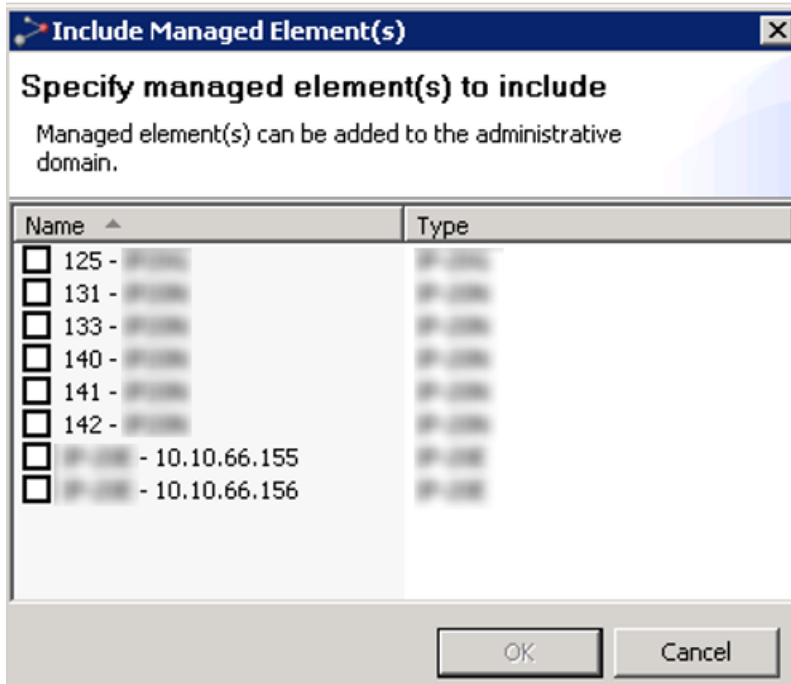
This dialog appears whenever selecting the Move context menu with a NE or subdomain in focus.

Figure 92 Move resource dialog

Browse the tree to find the parent domain where you want to move your node. The outline/shape of a domain will not remain when moving it to another level.

Include Managed Elements dialog

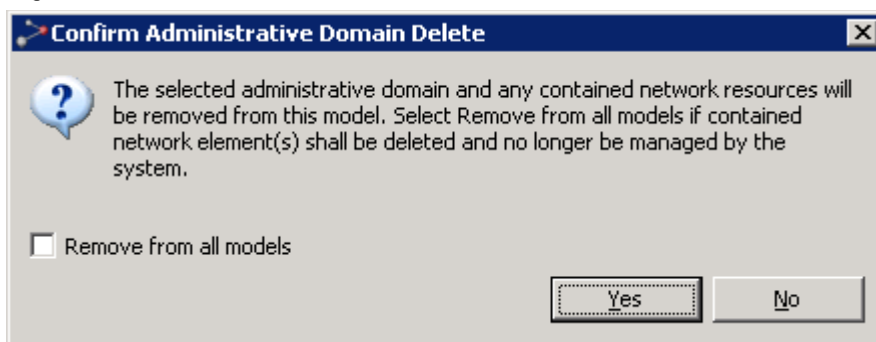
This dialog appears whenever selecting the Include Managed Elements context menu with a subdomain in focus in the map

Figure 93 Include managed elements dialog

This dialog presents a list of NEs that are managed in the Geographical Model (Geographical Tree and Map views), but not in the Logical Model. Select the NEs you want to manage, and they will be managed in the currently selected subdomain.

Delete Domain from Model dialog

This dialog appears whenever selecting the Delete context menu in the map with a domain in focus.

Figure 94 Delete domain from model dialog

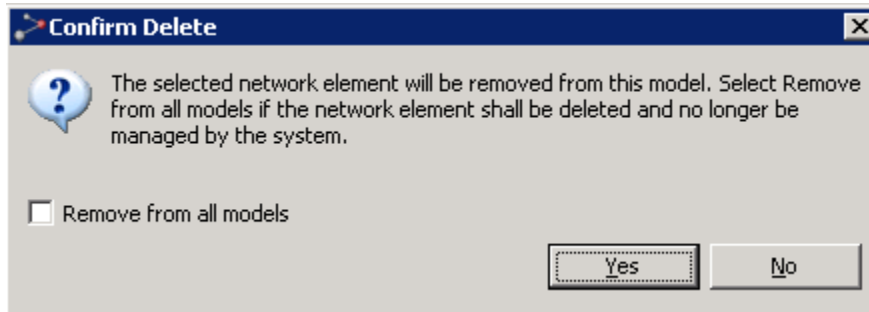
Press OK to confirm that you wish to delete the domain and all its NEs.

NEs deleted in this way will only be removed from the Logical Model (Logical Tree and Logical Map), and not from the Geographical Model (Geographical Tree and Geographical Map). The deleted NEs can be re-included in another domain in the Logical Model using the Include Managed Element function in this view. However, this is only possible if the NE also existed in the Geographical Model. If deleted NEs do not belong to any other model, they will become unmanaged once deleted. If so, they must be re-managed using the [Unmanaged Elements](#) view.

Delete Network Element from Model dialog

This dialog appears whenever selecting the Delete context menu in the map with an NE in focus.

Figure 95 Delete network element form model dialog

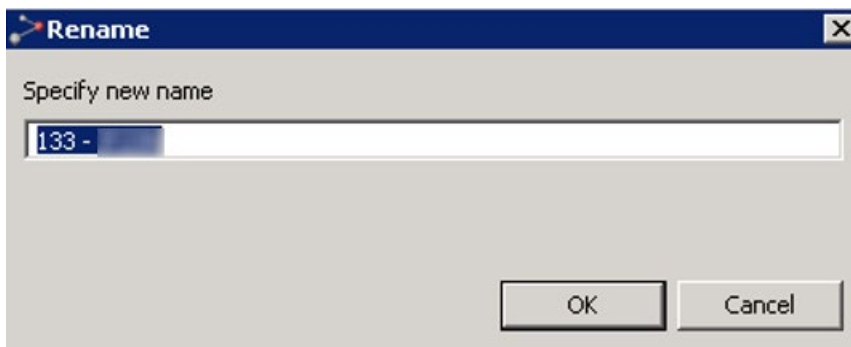


Press OK to confirm that you wish to delete the resource. If you check the Remove from all models checkbox, the NE will also be removed from the Geographical Model (Geographical Tree and Geographical Map). If so, they must be re-managed using the Unmanaged Elements view.

Rename dialog

This dialog appears whenever selecting the Rename context menu in the map with an NE or subdomain in focus.

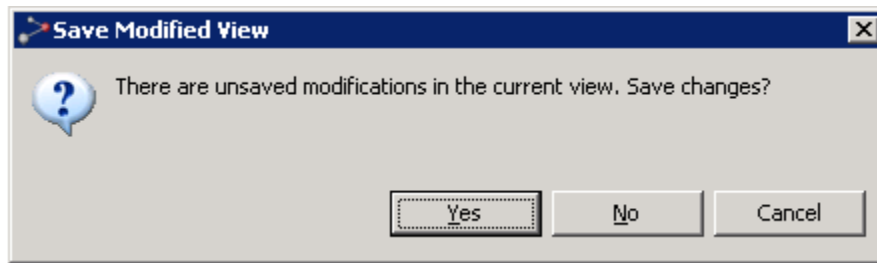
Figure 96 Rename dialog



Enter a new name and press OK to perform the rename or press Cancel to abort.

Save Modified View dialog

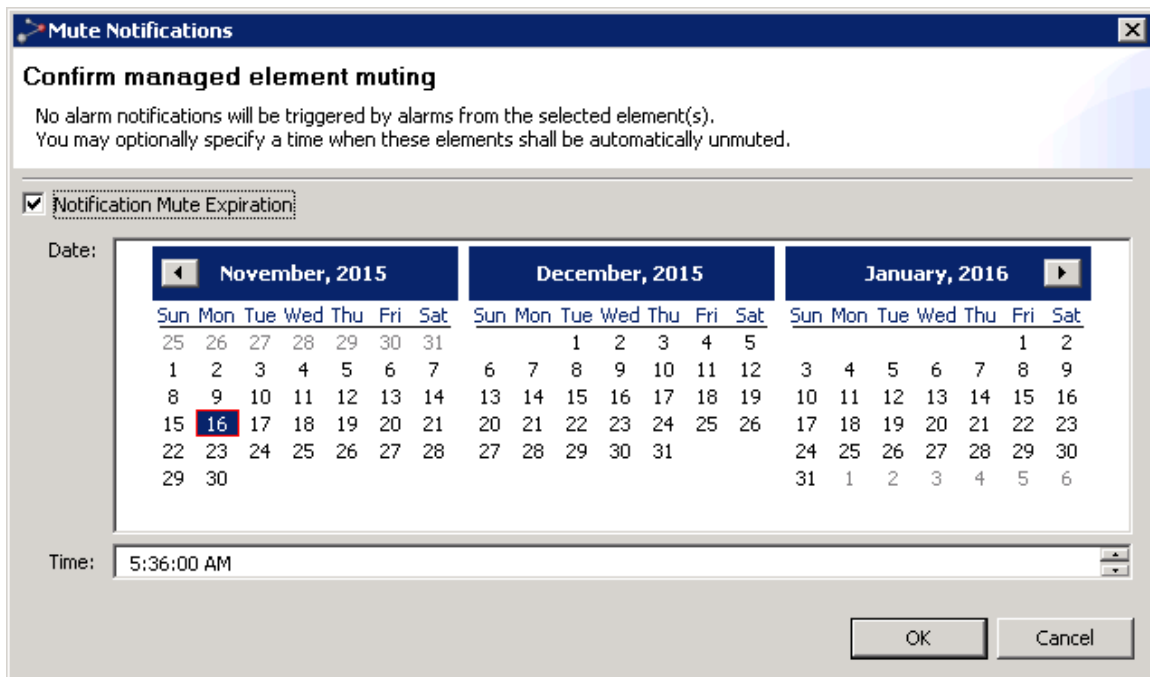
This dialog appears whenever you have made changes in the view, and then try to go [up](#) or [down](#) a domain level, or when you try to close the view without saving changes.

Figure 97 Save modified view dialog

Press OK to save changes to the map.

Mute Notifications dialog

This dialog appears whenever selecting the Mute Notifications context menu in the map with an NE or domain in focus.

Figure 98 Mute notifications dialog

This dialog requests confirmation to mute all selected elements, as well as any element beneath any selected administrative domain. Alarm notifications will not be sent for muted elements. In the tree and map views, muted elements can be identified by a [Mute indicator](#) on NE level. In the [Managed Elements view](#), [Active Alarms view](#) and [Historical Alarms view](#), you can identify muted elements by including and sorting by the Muted column.

When muting elements, you have the option to enable automatic unmuting. If Notifications Mute Expiration is not enabled, the selected elements will stay muted until they are manually unmuted. If you enable Notifications Mute Expiration, you must specify the Date and Time for the elements to be unmuted.

Press OK to enable muting or press Cancel to abort.

Geographical Map view

This view can be found in the Geographical [Surveillance](#) perspective, and is opened directly from the [Geographical Tree](#) view by using the Logical Map menu. The view can also be opened from **Views > Topology > Geographical Map** in the main menu.

Figure 99 Geographical map view



This is a view for monitoring and managing your network based on a geographical model and includes an editor for creating a geographical map. A map is built by creating a set of polygon objects reflecting the nature of your network.

The Geographical Model used in the Geographical Map view is the same as in the [Geographical Tree](#) view. You can browse, create, delete and move geographical domains, corresponding to the physical location (country, region, city, etc.) of your NE. This geographical organization of your network is separate from Logical Model used in the [Logical Map](#) view. The two Map views operate on different models, but otherwise have exactly the same functionality. An NE can exist in both models at the same time, or in only one.

The view also allows you to include, move and delete NEs. The structure of your domains can be used for assigning rights to different groups of users in the [Group Administration](#) view.

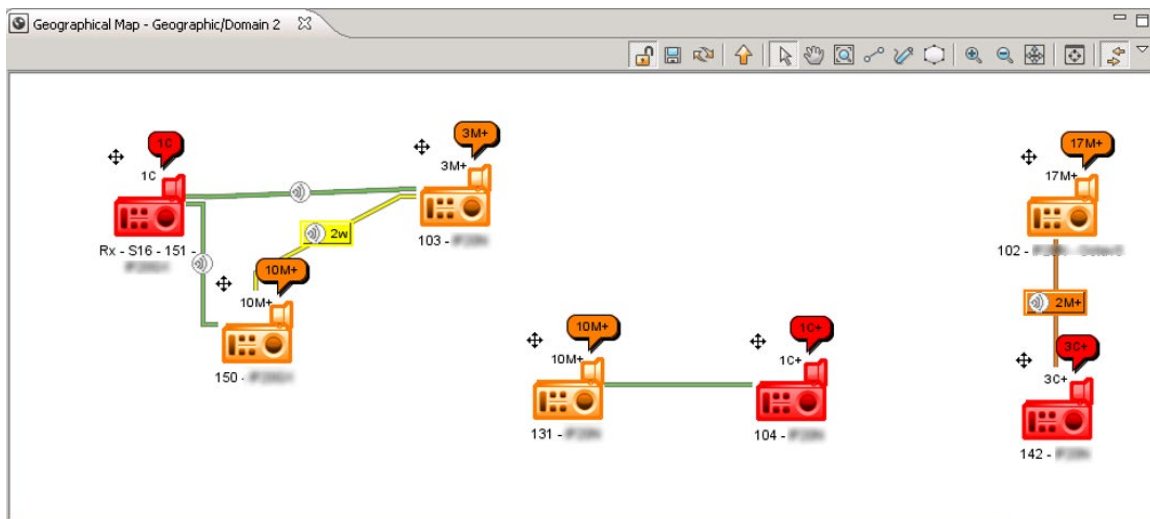
The current alarm status for the different parts of your network are visualized in the map using colors, alarm counts and symbols. Details about alarms and how visualization is shown can be found in the chapter about [visualization of alarms](#).

In the above example, the geographical map shows different domains equivalent to countries in Europe. We can, for example, see that the "Denmark" domain is solid orange, while the "Netherlands" domain is blue with a pink outline. This tells us:

- that there is (at least) one new alarm with severity "Major" (=orange) on (at least) one NE in Denmark. Studying alarm summaries on domains and balloons tells us that there are 89 active Major alarms, and of these 36 Major alarms are new (which indicates that 53 Major alarms are acknowledged (acked)). In addition there also is (at least one) new less severe alarm(s).
- that there is (at least) one NE in the Netherlands which has Loss of Connectivity, and that there is (at least) one active alarm with severity "Indeterminate". Studying alarm summaries tells us that there is exactly one new "Indeterminate" alarm. As the base element summary is hidden at the moment we would need to zoom the view a bit more to find out how many alarms have been acknowledged.

The [scope](#) in the title of the view indicates the name of the domain currently displayed. In the above example the title " Geographic\Europe" indicates that the map currently displays the content of the Europe domain.

In another example, NEs can be seen with topological links.

Figure 100 NEs topological links

In this example, the geographical map shows some NEs in the topological domain "Geographic/Domain2". We can, for example, see that:

- There are two new alarms with severity "Warning" (=yellow) on the radio endpoints connecting the NE's 150 and 103.
- There are two new alarms with severity Major (=orange) on the radio endpoints connecting the NE's 102 and 142.

The objects in a map

Domains



It is possible to [edit the shape of the domain](#), to make it look like the actual geographical domain represented by this domain. The colours of the [domain](#) represents the alarm state of all NE and subdomains contained in the domain, so that the color of the most severe alarm is presented. Details of alarms and how colours are used for presenting alarms in the tree can be found in the chapter about [visualization of alarms](#).

Network Elements (NE)



The colours of the [NE](#) represents the alarm state of the most severe alarms on the NE. Details of alarms and how colours are used for presenting alarms in the tree can be found in the chapter about [visualization of alarms](#).

Topological Links between NE










A [topological link](#) between two NE in the map can represent termination points within same layer rate on each of the two NE, e.g. two ODU's connected with a radio link, or two or more E1 ports connected with an electrical cable. Alarm severity from unacked alarms on these connected termination points can be visualized on the link.

Radio links will be displayed in the map view with this icon:






A topological link can only exist when both end-points of the link exist in the same domain. I.e. deleting one of the end NEs or moving one of the end NEs, will delete the link between them.

Available operations

- **Save Map** Save the changes in the view. All changes to domain polygons, coordinates and background images are not saved on the server until the Save icon has been clicked. If moving to another domain level or trying to close a view without saving changes, the [Save Modified View](#) dialog will appear.
- **Up** Go up one level to the Parent Domain. The parent domain contains the current domain as a "child", and when going up one level the shape/outline of the previous domain and its "siblings" will be displayed (this operation is the opposite of [Doubleclick a Domain](#)).
- **Select** Select each domain and NE in the view using this tool. Hold down the shift key while selecting to select multiple objects. When the Select tool is enabled, you can:
 - drag an object (domain or NE)
 - open context menus for the currently selected object (domain or NE)
 - Doubleclick a Domain to go down to this level in the Geographical Map view (this operation is the opposite of [Go to Parent Domain](#))
- **Pan** Pan can be used to scroll the view by dragging it in the direction you want.
- **Zoom Area** Zoom in on a specific area of the view by clicking and dragging a rectangle over the area you wish to see in more detail. When the mouse button is released the view will display only this selected area.
- **Draw New Domain** Use this tool to create a new Geographical Domain by drawing a polygon outline in the view. Click once for each new polygon corner you want to create, and double-click to finish. When you have finished editing, the [New Administrative Domain](#) dialog will open, where you can enter a name for the domain. It is recommended that you add the picture of a map as a [background image](#) to your map before drawing domains, because this will help you see the correct shape of your map objects.






-  **Edit Domain Outline** Edit the shape of your Geographical Domain outlines by selecting this tool. You can:
 - click a corner and drag it in any direction
 - ctrl+click directly on a corner to delete it
 - ctrl+click on a line to create a new corner
-  **Create Link** Create a new [Topological Link](#) by drawing a line between two NEs in the view. When you have completed the link the [New Topological Link dialog](#) will open, where you can enter details for the link.
-  **Zoom In** Click to zoom in on a smaller area.
-  **Zoom Out** Click to zoom out to a larger area
-  **Zoom to Fit** Click this icon to zoom and pan so that all objects on this level are displayed in the view.
-  **Map Overview** Open the [Map Overview](#) tool in a new view, where you can pan and zoom the area currently displayed
-  **Lock Map** Lock the map. This will disable
 - the movement of objects in the map
 - the changing of the shape of domain polygons
 - the creation of new domain polygons

If the map is locked, you can unlock the map by pressing this icon again.

-  **New Domain** Create a new sub-domain under the currently selected domain. The [New Administrative Domain](#) dialog will open, where you can enter a name for the new domain.
-  **Include Managed Element** Select one or more managed NEs from the Logical Model and place them under the currently selected domain in the Geographical Model. The [Include Managed Elements](#) dialog will appear, where you can view the list of unmanaged elements and select which NE you want to manage.
-  **Move** Move the currently selected node (NE or subdomain) to another domain. If the node contains a sub-tree, this sub-tree with all its nodes will also be moved to the new domain. The [Move Resource](#) dialog will open where you will be able to select the domain you want to move the node to. The outline/shape of a domain will not remain when moving it.
-  **Rename** Rename the currently selected node by opening the [Rename](#) dialog.
-  **Delete** Delete the currently selected node (NE or subdomain).

If the currently selected node is a domain, the entire sub-tree of domains and all its NEs will be deleted and the [Delete Domain From Model](#) dialog will be opened, where you can confirm or cancel the operation.

If the currently selected node is an NE, the [Delete Network Element from Model](#) dialog will appear. In this dialog you can also choose to remove the NE from the Logical Model.

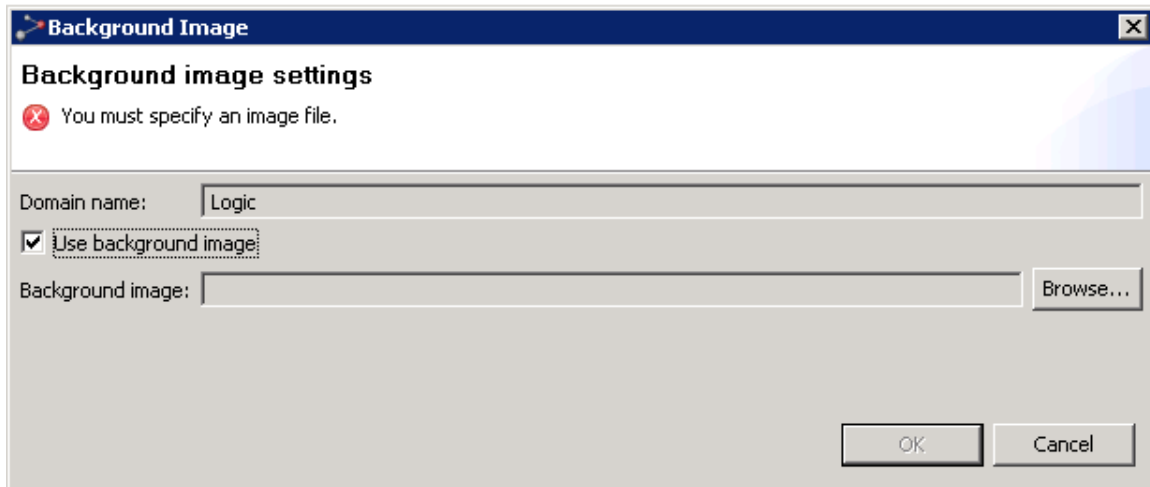
-  **Visible Layers** Select which layers are to be visible in the Geographical Map view. Checking/ unchecking menu items on this submenu allows you to hide/display:
 - Background image
 - Geographical Domains
 - Links
 - Managed Elements
 - Alarm Balloons
-  **Layout** Distribute your graphical elements within the current viewable area in the map. Selecting Random Layout will distribute your domains/NEs randomly, while selecting Grid Layout will distribute your domains/NEs in a regular grid pattern. This operation is useful when opening a domain with a lot of NEs for the first time, because all managed NEs by default are set with the same coordinates in the map.
-  **Background Image** Open the [Background Image](#) dialog, to enable/disable and select a background image to your Geographical Network view. The .gif, .jpg and .png file formats are allowed.
- In addition, the following views, dialogs and functions can be opened with data from a node in the view (using the currently selected node as [scope](#)):
- Geographical Map view
- Geographical Tree view
- fault:
 - Active Alarms view
 - Historical Alarms view
 - Alarm Templates Assignment view
-  **Mute Notifications...** Mute an NE or a domain, to prevent alarms on the selected NE(s) from generating [alarm notifications](#). The [Mute Notifications dialog](#) will open, where you can choose to select a time for automatic unmuting the element. When being muted, NEs will have a [mute indicator](#) on NE level in the Map and Tree views.
-  **Unmute Notifications** Unmute a muted NE or a domain with muted element, to re-enable alarms on the selected NE(s) to generate [alarm notifications](#).
- configuration:
 - Hardware Inventory view
 - Software Inventory view
 - Transmission Inventory view
 -
 - Create Software Download Jobs wizard
 - Configuration File Management view
 - Connection Templates Assignment view
 - External Tools
- performance:
 - Current Performance view
 - Historical Performance view
 - Performance Collection Control view
 - Reset Cumulative Performance Counters dialog

- reports:
 - Network Element Types Overview Report
 - Inventory Report
- Properties view

Background Image dialog

This dialog appears when selecting the Background Image on the view dropdown.

Figure 101 Background image dialog



Check/Uncheck the checkbox to enable/disable usage of background images on this level in the geographical map. Browse your file system to find a background image and press OK, or press Cancel to abort changes.

Please note that you should avoid using images of different proportions as all background images will appear centred and in their original size.

New Topological Link dialog

This dialog appears whenever you are creating a topological link between two NEs:

Figure 102 New topological link dialog

New Topological Link

Create topological link

Define properties and mappings for a new topological link.

Link Name:

145 - PTP820N_146_PTP820N

Description:

Layer Rate:

Radio

☒

Allow PTP mappings to be configured below to enable alarm colouring

145 - PTP820N

PTP	Status

146 - PTP820N

PTP	Status
Radio-3.1	FREE

Map

Unmap

OK

Cancel

To complete the creation of the link, select a layer rate and alternatively enter a user label and a description and then press OK. Alternatively, also create terminal endpoint mapping, to enable alarms on the link.

Fields for a Topological link:

Table 36 Fields for a topological link attributes

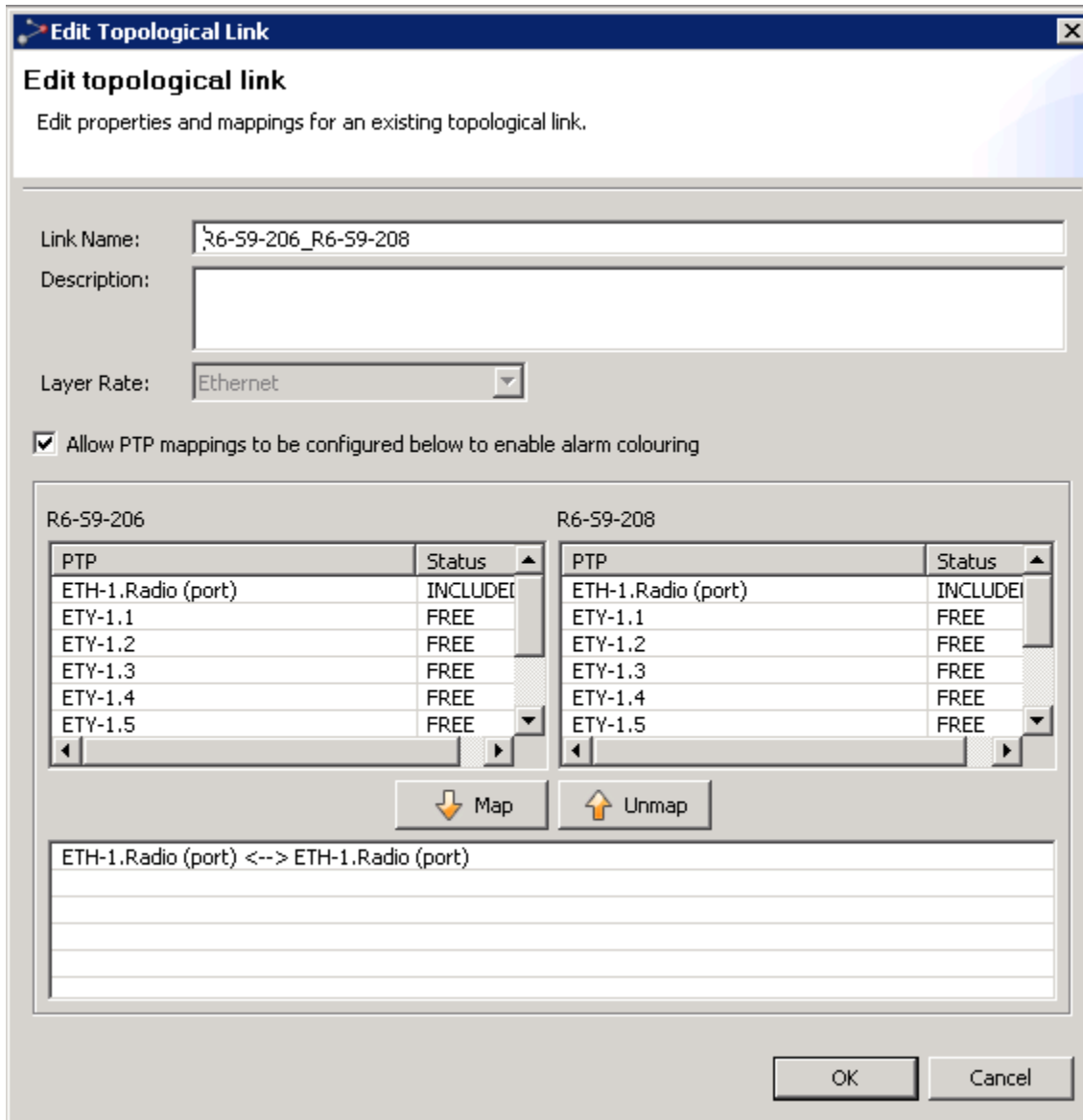
Name	Explanation
User Label	An optional name for the topological link. Default name is a combination of the NE names at the end points.
Description	Free text used for description of link

Name	Explanation
Layer Rate	<p>Signal type carried over this link. Depending of the termination points, the following layer rates can be available, :</p> <ul style="list-style-type: none"> • radio : specifies physical media for technologies such as radio, corresponds to TMF layer rate LR_PHYSICAL_MEDIALESS • ds1 : 1.5 Mbit/s async/PDH signal, corresponds to TMF layer rate LR_T1_and_DS1_1_5M • ds3 : 45 Mbit/s async/PDH signal, corresponds to TMF layer rate LR_T3_and_DS3_45M • dsr_1 : STM-1 digital signal rate, corresponds to TMF layer rate LR_DSR_OC3_STM1 • dsr_4 : STM-4 digital signal rate, corresponds to TMF layer rate LR_DSR_OC12_STM4 • e1 : 2 Mbit/s PDH signal, corresponds to TMF layer rate LR_E1_2M • e3 : 34 Mbit/s PDH signal, corresponds to TMF layer rate LR_E3_34M • ethernet : all Ethernet rates, corresponds to TMF layer rate LR_Ethernet • Cascading link • Electrical • Optical <p>If the NEs connected in the link do not share any TP endpoints of the same layer rate, the following layer rates can be selected in the dialog: radio, optical, electrical, ethernet.</p>
Enable mapping to TPs to enable alarm colouring	<p>Select this option if you want to map termination points from each end of the topological link. When termination points are mapped, alarmstate of these termination points will be visualized on the link in your map.</p>

Name	Explanation
PTP mappings area	<p>In this area you can define the mapping of physical termination points (PTPs) from each end of the topological link.</p> <p>Use the PTP tables to select one endpoint from each side of the topological link, then press the Map button. Each time you add a pair of endpoints, they will appear in the Mapping table at the bottom of the PTP mappings area.</p> <p>An endpoint can have the following states in the PTP tables:</p> <ul style="list-style-type: none">• FREE: this endpoint is available for mapping• INCLUDED: this endpoint is already mapped on this topological link.• OCCUPIED: this endpoint is mapped to another topological link• When termination points are mapped, PTP 820 NMS will use these mappings to determine alarmstate for the topological link. Severity colour of unacked alarms will then be presented on the link. <p>To unmap a pair of PTPs, select a line with a mapping in the Mapping table and then press the Unmap button.</p>

Edit Topological Link dialog

This dialog appears whenever selecting the Edit context menu with a topological link selected in the map.

Figure 103 Edit topological link dialog

The dialog box is titled "Edit Topological Link" and contains the following fields and controls:

- Link Name:** A text field containing "R6-S9-206_R6-S9-208".
- Description:** An empty text field.
- Layer Rate:** A dropdown menu set to "Ethernet".
- Checkboxes:** A checked checkbox labeled "Allow PTP mappings to be configured below to enable alarm colouring".
- PTP Mappings:** Two side-by-side tables for mapping PTPs between R6-S9-206 and R6-S9-208.

PTP	Status
ETH-1.Radio (port)	INCLUDE
ETY-1.1	FREE
ETY-1.2	FREE
ETY-1.3	FREE
ETY-1.4	FREE
ETY-1.5	FREE

PTP	Status
ETH-1.Radio (port)	INCLUDE
ETY-1.1	FREE
ETY-1.2	FREE
ETY-1.3	FREE
ETY-1.4	FREE
ETY-1.5	FREE

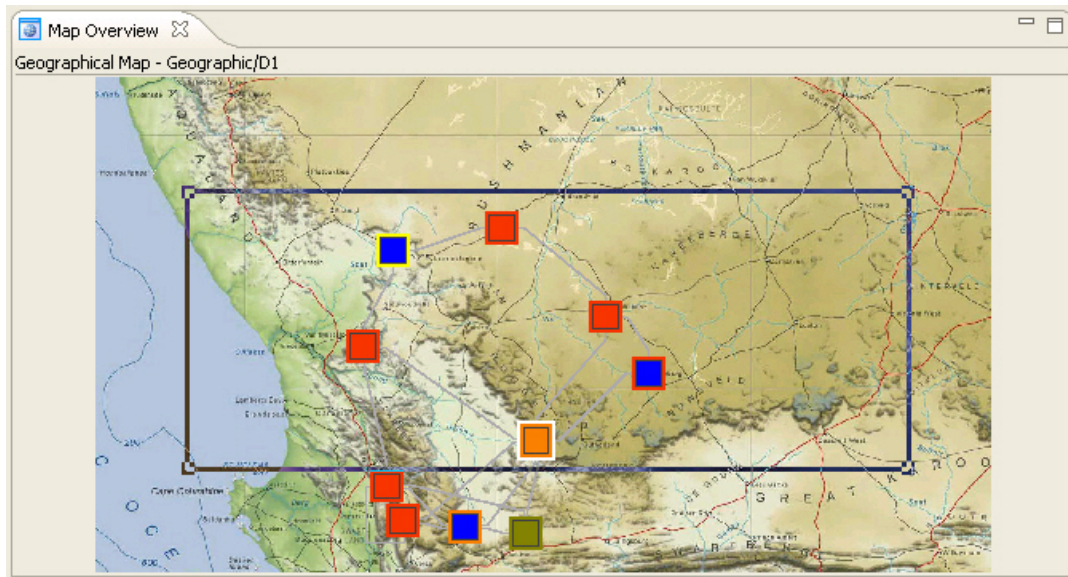
Below the tables are "Map" and "Unmap" buttons. At the bottom is a text area containing the mapping "ETH-1.Radio (port) <--> ETH-1.Radio (port)".

At the bottom right are "OK" and "Cancel" buttons.

Update the [fields for a topological link](#), then press OK.

Map Overview view

This tool appears when selecting [Map Overview](#) on the toolbar or view dropdown:

Figure 104 Map overview tool

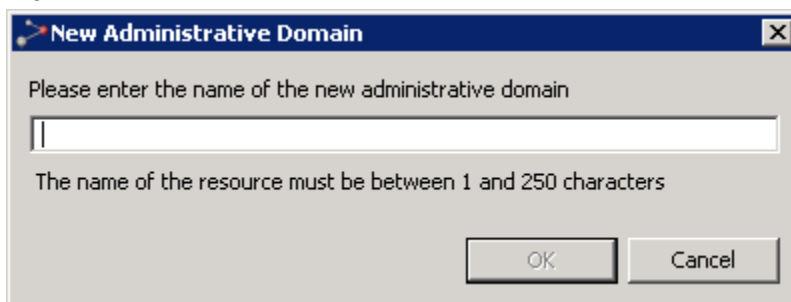
The tool displays the entire map and a blue frame around the current viewable area in the Geographical Map. You can use the tool to do the following:

- Drag&draw the corners of the blue frame to zoom in/out the viewable area in the Geographical Map
- Drag inside the blue frame to pan the viewable area in the Geographical Map
- Click outside the blue frame to set a new center for the viewable area in the Geographical Map

This tool can be useful when the viewable area in the Geographical Map view is zoomed in to display only parts of the entire map. Please note that when the map is zoomed out to Zoom to fit (or less), the Show Overview tool cannot provide you with any useful navigation features.

New Administrative Domain dialog

This dialog appears whenever selecting the New Domain context menu with a domain selected in the map:

Figure 105 New administrative domain dialog

Enter a name in the text field. When OK is pressed, the new subdomain is created and placed under the currently selected domain.

Move Resource dialog

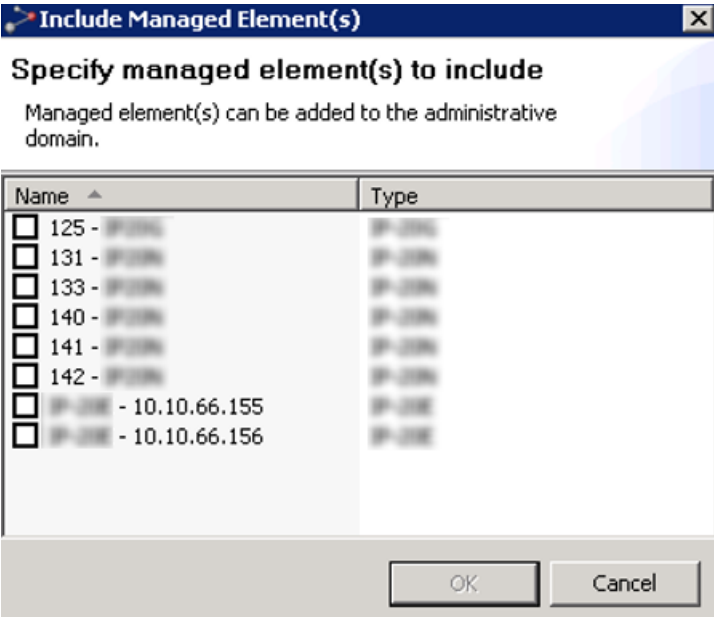
This dialog appears whenever selecting the Move context menu with a NE or subdomain in focus.

Browse the tree view to find the parent domain where you want to move your node. The outline/shape of a domain will not remain when moving it to another level.

Include Managed Elements dialog

This dialog appears whenever selecting the Include Managed Elements context menu with a domain in focus in the map

Figure 106 Include managed element

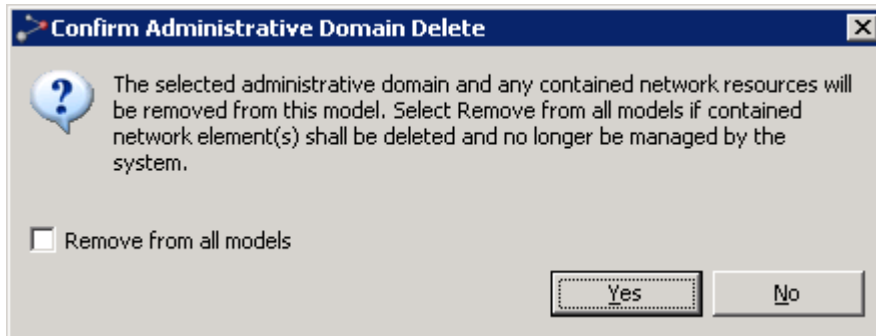


This dialog presents a list of NEs that are currently managed in the Logical Model (Logical Tree and Map views), but not in the Geographical Model. Select the NEs you want to manage, and they will be managed in the currently selected subdomain.

Delete Domain from Model dialog

This dialog appears whenever selecting the Delete context menu in the map with a domain in focus.

Figure 107 Delete domain from model dialog



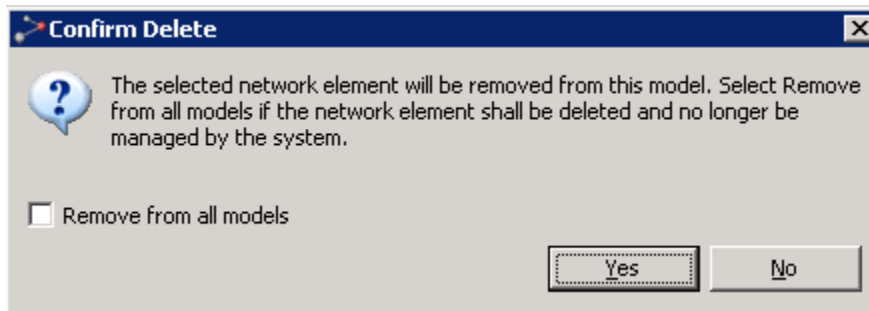
Press OK to confirm that you wish to delete the domain and all its NEs.

NEs deleted in this way will only be removed from the Geographical Model (Geographical Tree and Geographical Map), and not from the Logical Model (Logical Tree and Logical Map). The deleted NEs can be re-included in another domain in the Geographical Model using the Include Managed Element function in this view. However, this is only possible only if the NE also existed in the Logical Model. If deleted NEs do not belong to any other model, they will become unmanaged once deleted. If so, they must be re-managed using the [Unmanaged Elements](#) view.

Delete Network Element from Model dialog

This dialog appears whenever selecting the Delete context menu in the map with an NE in focus.

Figure 108 Delete network element from model dialog

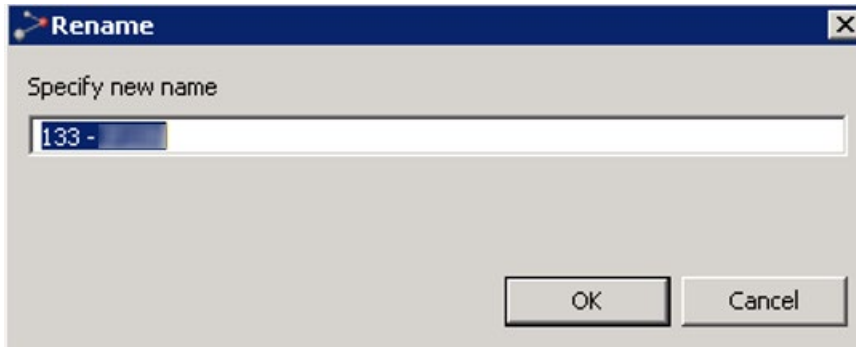


Press OK to confirm that you wish to delete the resource. If you check the Remove from all models checkbox, the NE will also be removed from the Logical Model (Logical Tree and Logical Map). If so, they must be re-managed using the Unmanaged Elements view.

Rename dialog

This dialog appears whenever selecting the Rename context menu in the map with an NE or subdomain in focus.

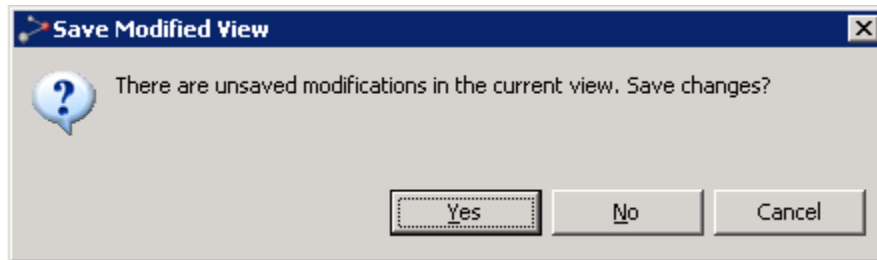
Figure 109 Rename dialog



Enter a new name and press OK to perform the rename or press Cancel to abort.

Save Modified View dialog

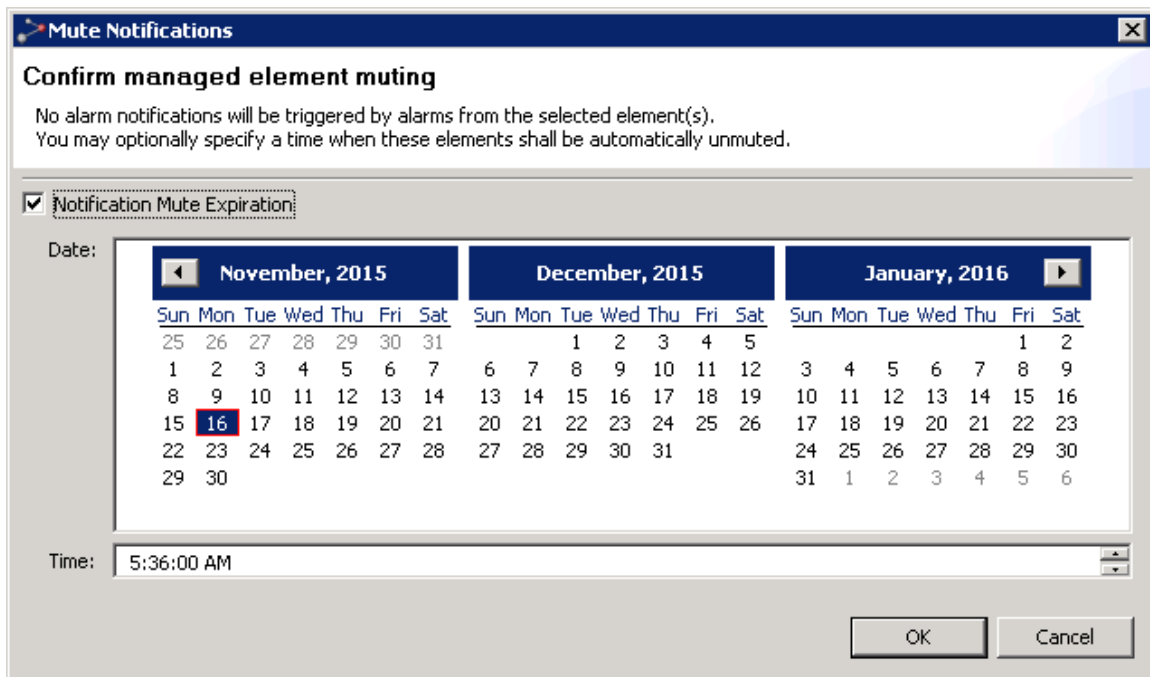
This dialog appears whenever you have made changes in the view, and then try to go [up](#) or [down](#) a domain level, or when you try to close the view without saving changes.

Figure 110 Save modified view dialog

Press OK to save changes to the map.

Mute Notifications dialog

This dialog appears whenever selecting the Mute Notifications context menu in the map with an NE or domain in focus.

Figure 111 Mute notifications dialog

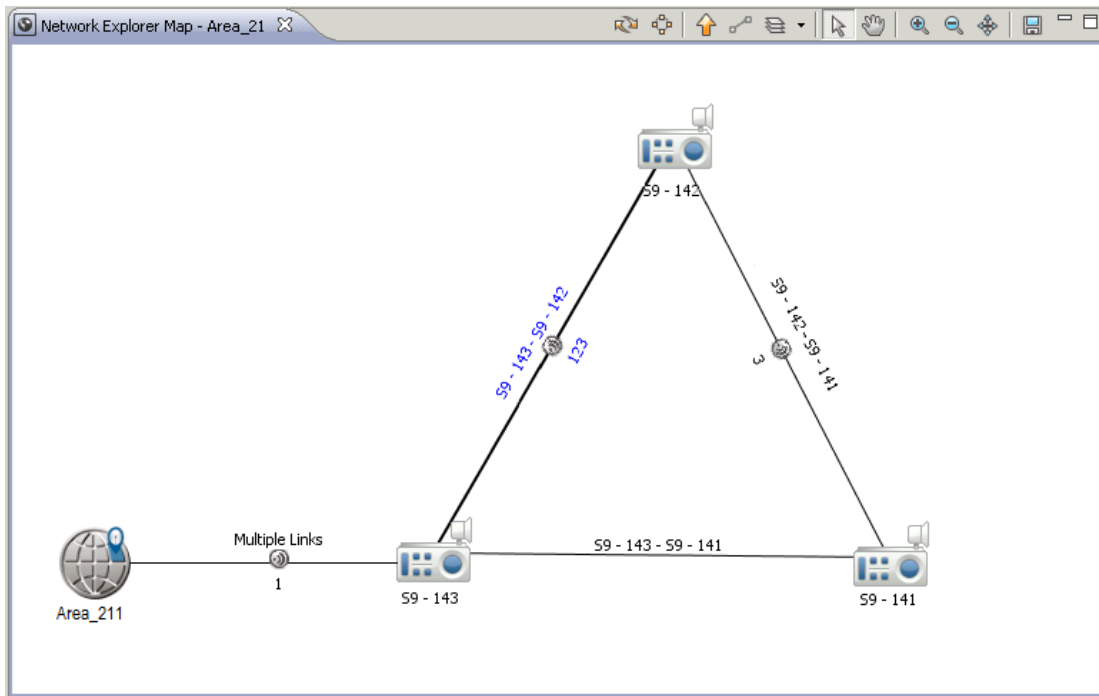
This dialog requests confirmation to mute all selected elements, as well as any element beneath any selected administrative domain. Alarm notifications will not be sent for muted elements. In the tree and map views, muted elements can be identified by a [Mute indicator](#) on NE level. In the [Managed Elements view](#), [Active Alarms view](#) and [Historical Alarms view](#), you can identify muted elements by including and sorting by the Muted column.

When muting elements, you have the option to enable automatic unmuting. If Notifications Mute Expiration is not enabled, the selected elements will stay muted until they are manually unmuted. If you enable Notifications Mute Expiration, you must specify the Date and Time for the elements to be unmuted.

Press OK to enable muting or press Cancel to abort.

Network Explorer Map view

This view can be found in the [Network Explorer](#) perspective, and is opened directly from the [Error! Reference source not found.](#) view by using the **Network Explorer Map** option. The view can also be opened from **Views > Topology > Network Explorer Map** in the main menu.



The hierarchical model used in the **Network Explorer Map** view is the same as in the [Error! Reference source not found.](#) view. You can move and delete NEs. You can also browse, create, delete and move geographical domains, corresponding to the physical location (country, region, city, etc.) of your NEs. The structure of your domains can be used for assigning rights to different groups of users in the [Group Administration](#) view.

In addition, the **Network Explorer Map** view displays the link name of each link, and the radio link ID of each radio link.

The objects in a map

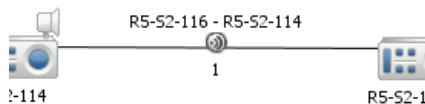
Domains



Network Elements (NE)

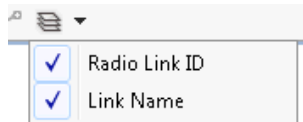


Relations between entities



A relation can exist between two domain, between a domain and an NE, or between NEs. A relation between two NEs on the map can represent termination points within the same layer rate on each of the two NEs, e.g. two ODU's connected with a radio link, or two or more E1 ports connected with an electrical cable.







You can display **Radio Link ID** and/or **Link Name**, for all link types, by activating those options in the task bar:
















Radio links are displayed in the map view with this icon:













Available operations

- Refresh – Refreshes the view. The color of the button indicates whether the information in the map is up-to-date:
 - Yellow – the information displayed in the map is up-to-date.
 - Red – the information in the map needs to be refreshed. Click the button to refresh.
- Reapply Layout – Refresh the layout from memory, without going to the server/database.
- Move Up – Moves up one level, to the **Parent Domain**. The parent domain contains the current domain as a "child", and when going up one level the shape/outline of the previous domain and its "siblings" is displayed (this operation is the opposite of [Doubleclick a Domain](#)).
- Link Nodes – Available only when two NEs are selected. Allows you to create a manual topological link in cases where automatic discovery of links is not supported for specific devices.
- Extra Layers – Enables selecting whether to hide or display on the map:
 - Link names
 - Radio Link IDs










-  **Select Tool** – Enables selecting each domain and NE in the view. Hold down the shift key while selecting, to allow selection of multiple objects. When the **Select** tool is enabled, you can:
 - Drag an object (domain or NE)
 - Open context menus for the currently selected object (domain or NE)
 - **Double-click a Domain** to go down to this level in the **Logical Map** view (this operation is the opposite of the **Go to Parent Domain** operation)
-  **Pan Tool** – **Pans** the screen by dragging it in the direction you want. Alternatively, hold down the mouse wheel, and move the mouse in the desired direction.
-  **Zoom In** – Click to **zoom in** on a smaller area. Alternatively, use the mouse wheel.
-  **Zoom Out** – Click to **zoom out** to a larger area. Alternatively, use the mouse wheel.
-  **Fit to View** – Centers the currently selected item in the middle of the view.
-  **Export as Image** – Enables saving the display as an image file.



















Operations available from the context menu of a domain in the map

- **Fault** – Opens the following Fault views and functions:
 -  **Active Alarms** – Opens an **Active Alarms** view for the selected domain.
 -  **Historical Alarms** – Opens a **Historical Alarms** view for the selected domain.
 -  **Alarm Templates Assignment** – Opens an **Alarm Templates Assignment** view for the selected domain.
 -  **Mute Notifications** – Mutes an NE or a domain, to prevent alarms on the selected NE(s) from generating [alarm notifications](#). The [Mute Notifications dialog](#) will open, where you can select a time for automatic unmuting of notifications. When notifications are muted, NEs will have a [mute indicator](#) on NE level in the **Map** and **Tree** views.
 -  **Unmute Notifications** – Unmutes a muted NE or a domain with muted element, to re-enable alarms on the selected NE(s) to generate [alarm notifications](#)
- **Configuration** – Opens the following Configuration views and functions:
 -  **Hardware Inventory** – Opens a **Hardware Inventory** view for the selected domain.
 -  **Software Inventory** – Opens a **Software Inventory** view for the selected domain.
 -  **Transmission Inventory** – Opens a **Transmission Inventory** view for the selected domain.
 -  **Create Software Download Job** – Opens the Create Software Download Jobs wizard, enabling you to create a software download job for the selected domain.
 -  **Configuration File Management** – Opens a **Configuration File Management** view for the selected domain.
 -  **Connection Template Assignment** – Opens a **Connection Template Assignment** view for the selected domain.
- **Performance** – Opens the following Performance views and functions:
 -  **Current Performance** – Opens a **Current Performance** view for the selected domain.
 -  **Historical Performance** – Opens a **Historical Performance** view for the selected domain.



-  Performance Collection Control – Opens a **Performance Collection Control** view for the selected domain.
-  Reset Cumulative Performance Counters – Opens a Reset Cumulative Performance Counters dialog for resetting counter values of cumulative counters to zero on the domain.
- Reports – Opens the following Report views and functions:
 -  Network Element Types Overview Report – Opens a **Network Element Types Overview Report** view for the selected domain.
 -  Inventory Report – Opens an **Inventory Report** view for the selected domain.
 -  Inventory Tables – Opens an **Inventory Tables** view for the selected domain.
-  Managed Elements – Opens a **Error! Reference source not found.** for the selected domain.
-  Topological Links – Opens a **Topological Links** view for the selected domain
-  New Domain – Opens a **New Administrative Domain** dialog for creating a **new sub-domain** under the currently selected domain.
-  Move – Moves the currently selected node (NE or subdomain) to another domain. If the node contains a sub-tree, this sub-tree with all its nodes will also be moved to the new domain. The **Move Resource** dialog will open where you will be able to select the domain you want to move the node to.
-  Rename – Enables renaming the managed domain.
-  Delete – Enables deleting the managed domain.
-  Properties – Displays the domain's properties in a **Properties** view.

Operations available from the context menu of an NE in the map

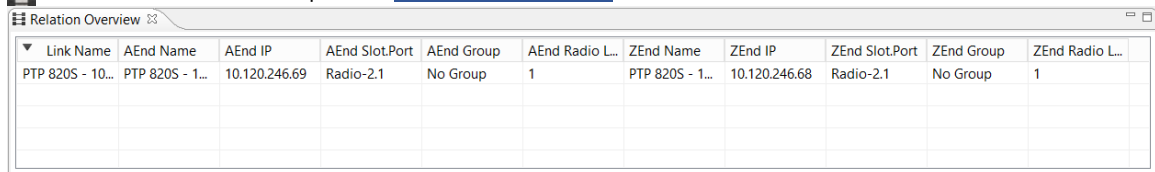
- Fault – Opens the following Fault views and functions:
 -  Active Alarms – Opens an **Active Alarms** view for the selected element.
 -  Historical Alarms – Opens a **Historical Alarms** view for the selected element.
 -  Alarm Templates Assignment – Opens an **Alarm Templates Assignment** view for the selected element.
 -  Mute Notifications – Mutes an NE or a domain, to prevent alarms on the selected NE(s) from generating [alarm notifications](#). The [Mute Notifications dialog](#) will open, where you can select a time for automatic unmuting of notifications. When notifications are muted, NEs will have a [mute indicator](#) on NE level in the **Map** and **Tree** views.
 -  Unmute Notifications – Unmutes a muted NE or a domain with muted element, to re-enable alarms on the selected NE(s) to generate [alarm notifications](#)
- Configuration – Opens the following Configuration views and functions:
 -  Hardware Inventory – Opens a **Hardware Inventory** view for the selected element.
 -  Software Inventory – Opens a **Software Inventory** view for the selected element.
 -  Transmission Inventory – Opens a **Transmission Inventory** view for the selected element.
 -  Create Software Download Job – Opens the Create Software Download Jobs wizard, enabling you to create a software download job for the selected element.

-  Configuration File Management – Opens a **Configuration File Management** view for the selected element.
-  Connection Template Assignment – Opens a Connection Template Assignment view for the selected element.
- Open SNMP Interface – Opens an “Open SNMP” Connection Template which can be used to manage the device. Basic SNMP management of the device will be triggered to read the inventory and faults from the device.
- External Tools – Enables opening a web EMS session with the selected device.
- Performance – Opens the following Performance views and functions:
 -  Current Performance – Opens a Current Performance view for the selected element.
 -  Historical Performance – Opens a Historical Performance view for the selected element.
 -  Performance Tables – Opens a Performance Tables view for the selected element.
 -  Performance Collection Control – Opens a Performance Collection Control view for the selected element.
- Reports – Opens the following Report views and functions:
 -  Network Element Types Overview Report – Opens a Network Element Types Overview Report view for the selected element.
 -  Inventory Report – Opens an Inventory Report view for the selected element.
 -  Inventory Tables – Opens an Inventory Tables view for the selected device.
-  Web EMS – Opens a web EMS session with the selected device.
-  Element Explorer – Opens an [Element Explorer](#) view for the selected element.
-  Topological Links – Opens a Topological Links view for the selected element
-  Reconcile – Instructs PTP 820 NMS to contact the network element, and update the PTP 820 NMS database with information about the element.
-  Ping/TraceRoute – Opens a Ping/TraceRoute view for the selected element.
-  Move – Moves the currently selected node (NE or subdomain) to another domain. If the node contains a sub-tree, this sub-tree with all its nodes will also be moved to the new domain. The **Move Resource** dialog will open where you will be able to select the domain you want to move the node to.
-  Rename – Enables renaming the managed element.
-  Delete – Enables deleting the managed element.
-  Properties – Displays the element’s properties in a **Properties** view.

Operations available from the context menu of an link in the map

- Fault – Opens the following Fault views and functions:
 -  Active Alarms – Opens an Active Alarms view for the selected link.
 -  Historical Alarms – Opens a Historical Alarms view for the selected link.

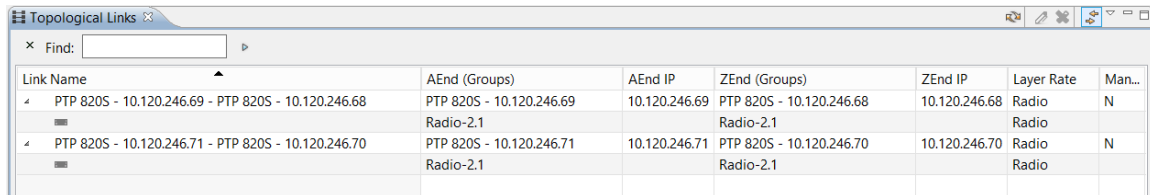
-  **Relation Overview** – Opens a [Relation Overview](#) view for the selected link.



Link Name	AEnd Name	AEnd IP	AEnd Slot.Port	AEnd Group	AEnd Radio L...	ZEnd Name	ZEnd IP	ZEnd Slot.Port	ZEnd Group	ZEnd Radio L...
PTP 820S - 10...	PTP 820S - 1...	10.120.246.69	Radio-2.1	No Group	1	PTP 820S - 1...	10.120.246.68	Radio-2.1	No Group	1

New Topological Link dialog

This dialog appears whenever you are creating a topological link between two NEs:



Link Name	AEnd (Groups)	AEnd IP	ZEnd (Groups)	ZEnd IP	Layer Rate	Man...
PTP 820S - 10.120.246.69 - PTP 820S - 10.120.246.68	PTP 820S - 10.120.246.69 Radio-2.1	10.120.246.69	PTP 820S - 10.120.246.68 Radio-2.1	10.120.246.68	Radio	N
PTP 820S - 10.120.246.71 - PTP 820S - 10.120.246.70	PTP 820S - 10.120.246.71 Radio-2.1	10.120.246.71	PTP 820S - 10.120.246.70 Radio-2.1	10.120.246.70	Radio	N

To complete the creation of the link, select a layer rate and alternatively enter a user label and a description and then press **OK**. Alternatively also create terminal endpoint mapping, to enable alarms on the link.

Fields for a Topological link:

Name	Explanation
User Label	An optional name for the topological link. Default name is a combination of the NE names at the end points.
Description	Free text used for description of link
Layer Rate	<p>Signal type carried over this link. Depending on the termination points, the following layer rates can be available :</p> <ul style="list-style-type: none"> radio : specifies physical media for technologies such as radio, corresponds to TMF layer rate LR_PHYSICAL_MEDIALESS ds1 : 1.5 Mbit/s async/PDH signal, corresponds to TMF layer rate LR_T1_and_DS1_1_5M ds3 : 45 Mbit/s async/PDH signal, corresponds to TMF layer rate LR_T3_and_DS3_45M dsr_1 : STM-1 digital signal rate, corresponds to TMF layer rate LR_DSR_OC3_STM1

	<ul style="list-style-type: none"> • dsr_4 : STM-4 digital signal rate, corresponds to TMF layer rate LR_DSR_OC12_STM4 • e1 : 2Mbit/s PDH signal, corresponds to TMF layer rate LR_E1_2M • e3 : 34 Mbit/s PDH signal, corresponds to TMF layer rate LR_E3_34M • ebus : Nera proprietary EBUS signal • ethernet : all Ethernet rates, corresponds to TMF layer rate LR_Ethernet • Cascading link • Electrical • Optical <p>If the NEs connected in the link do not share any TP endpoints of the same layer rate, the following layer rates can be selected in the dialog: radio, optical, electrical, ethernet.</p>
Enable PTP mappings to be configured below to enable alarm colouring	Select this option if you want to map termination points from each end of the topological link.
PTP mappings area	<p>In this area you can define the mapping of physical termination points (PTPs) from each end of the topological link.</p> <p>Use the PTP tables to select one endpoint from each side of the topological link, then press the Map button. Each time you add a pair of endpoints, they will appear in the Mapping table at the bottom of the PTP mappings area.</p> <p>An endpoint can have the following states in the PTP tables:</p> <ul style="list-style-type: none"> • FREE: this endpoint is available for mapping • INCLUDED: this endpoint is already mapped on this topological link. • OCCUPIED: this endpoint is mapped to another topological link <p>To unmap a pair of PTPs, select a line with a mapping in the Mapping table and then press the Unmap button.</p>

Edit Topological Link dialog

This dialog appears whenever selecting the **Edit** context menu with a topological link selected in the map.

Edit Topological Link

Edit topological link

Edit properties and mappings for an existing topological link.

Link Name: R6-S9-206_R6-S9-208

Description:

Layer Rate: Ethernet

☒ Allow PTP mappings to be configured below to enable alarm colouring

R6-S9-206		R6-S9-208	
PTP	Status	PTP	Status
ETH-1.Radio (port)	INCLUDE	ETH-1.Radio (port)	INCLUDE
ETY-1.1	FREE	ETY-1.1	FREE
ETY-1.2	FREE	ETY-1.2	FREE
ETY-1.3	FREE	ETY-1.3	FREE
ETY-1.4	FREE	ETY-1.4	FREE
ETY-1.5	FREE	ETY-1.5	FREE

Map Unmap

ETH-1.Radio (port) <--> ETH-1.Radio (port)

OK Cancel

Update the [fields for a topological link](#), then press **OK**.

New Administrative Domain dialog

This dialog appears whenever selecting the **New Domain** context menu with a domain selected in the map:

New Administrative Domain

Please enter the name of the new administrative domain

The name of the resource must be between 1 and 250 characters

OK Cancel

Enter a name in the text field. When **OK** is pressed, the new subdomain is created and placed under the currently selected domain.

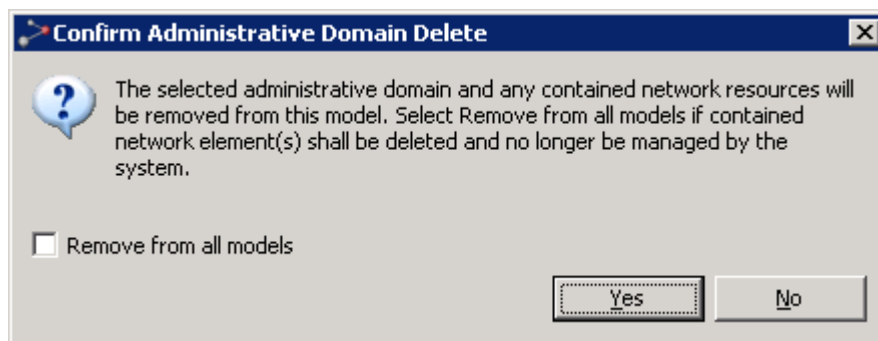
Move Resource dialog

This dialog appears whenever selecting the **Move** context menu with an NE or subdomain in focus.

Browse the tree view to find the parent domain where you want to move your node. The outline/shape of a domain will not remain when moving it to another level.

Delete Domain from Model dialog

This dialog appears whenever selecting the **Delete** context menu in the map with a domain in focus.



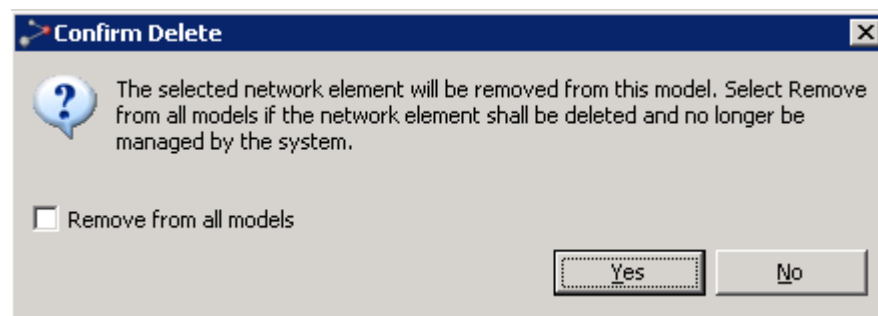
Press **Yes** to confirm that you wish to delete the domain and all its NEs.

NEs deleted in this way will be removed from the model (either Geographical or Logical) linked to the Network Explorer perspective. If deleted NEs do not belong to any other model, they will become unmanaged once deleted. If so, they can be re-managed using the [Unmanaged Elements](#) view.

If you check the **Remove from all models** checkbox, the domain and all its NEs will be removed from both the Logical model and Geographical model (**Tree** and **Map** views). In that case, you can re-manage them using the [Unmanaged Elements](#) view.

Delete Network Element from Model dialog

This dialog appears whenever selecting the **Delete** context menu in the map with an NE in focus.

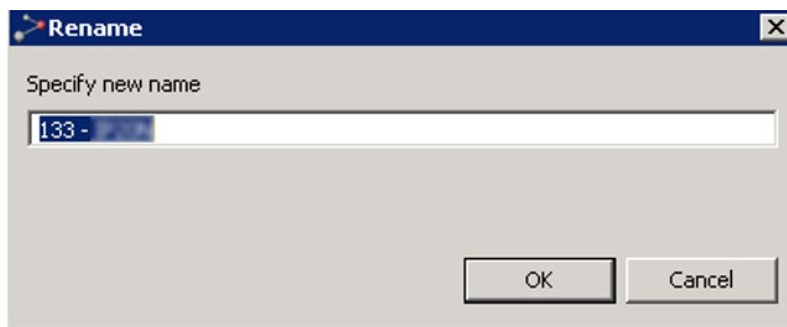


Press **Yes** to confirm that you wish to delete the resource. NEs deleted in this way will be removed from the model (either Geographical or Logical) linked to the Network Explorer perspective.

If you check the **Remove from all models** checkbox, the NE will be removed from both the Logical model and Geographical model (**Tree** and **Map** views). In that case, you can re-manage it using the [Unmanaged Elements](#) view.

Rename dialog

This dialog appears whenever selecting the **Rename** context menu in the map with an NE or subdomain in focus. PTP 820 device names are synchronized between PTP 820 NMS and the devices. That is, renaming a device on PTP 820 NMS sets the device name on the device itself; and changing the device name on the device itself changes the device name on PTP 820 NMS.

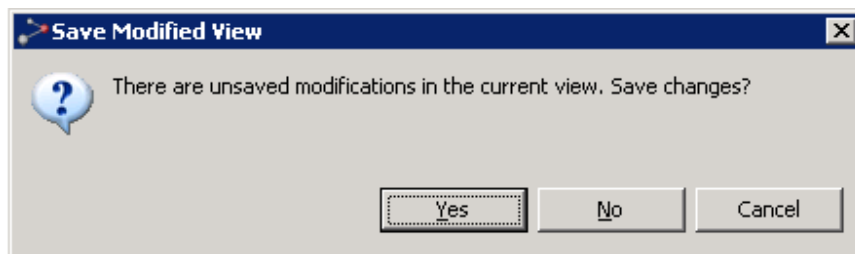


Enter a new name and press **OK** to perform the rename or press **Cancel** to abort.

Note: For PTP 820 devices, the device name can be up to 63 characters long.

Save Modified View dialog

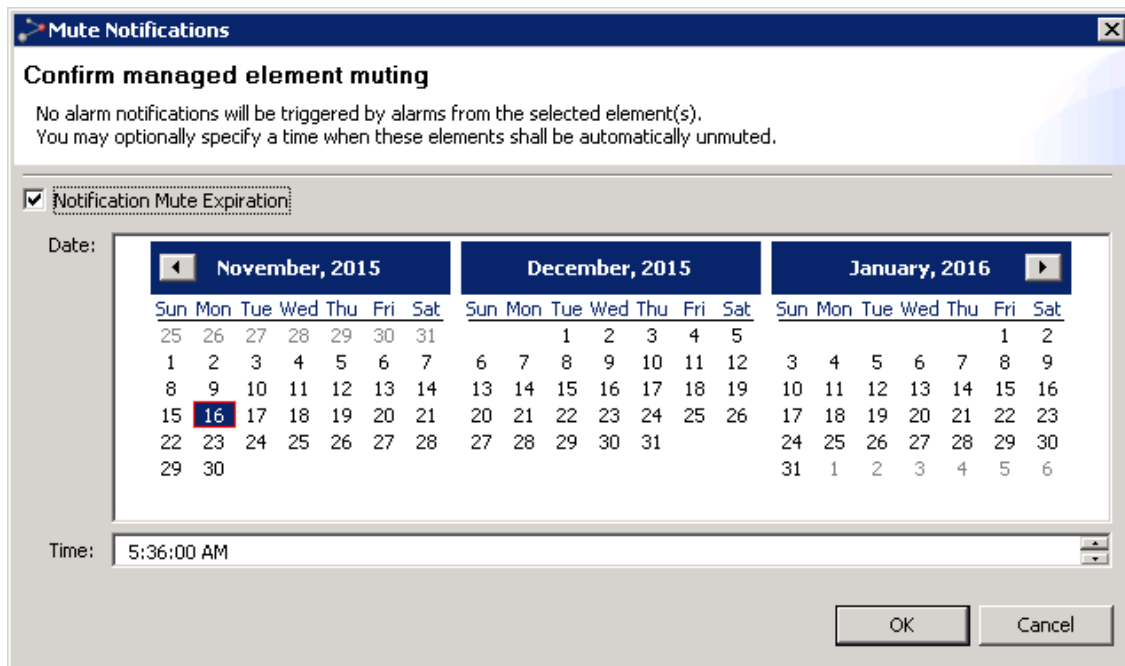
This dialog appears whenever you have made changes in the view, and then try to go up or down a domain level, or when you try to close the view without saving changes.



Press **OK** to save changes to the map.

Mute Notifications dialog

This dialog appears whenever selecting the **Fault > Mute Notifications** context menu in the map with an NE or domain in focus.



This dialog requests confirmation to mute all selected elements, as well as any element beneath any selected administrative domain. Alarm notifications will not be sent for muted elements. In the tree and map views, muted elements can be identified by a [Mute indicator](#) on the NE level. In the [Managed Elements view](#), [Active Alarms view](#) and [Historical Alarms view](#), you can identify muted elements by including and sorting by the **Muted** column.

When muting elements, you have the option to enable automatic unmuting. If **Notification Mute Expiration** is not enabled, the selected elements will stay muted until they are manually unmuted. If you enable **Notification Mute Expiration**, you must specify the **Date** and **Time** for the elements to be unmuted.

Press **OK** to enable muting or press **Cancel** to abort.

Managed Elements view

This view can be found in the Discover perspective as well as opened from **Views > Topology > Managed Elements** in the main menu or "[scoped](#)" by selecting a domain or NE in one of the topology views (Geographical or Logical Map or Tree) and then selecting Managed Elements in the Context or Dropdown menu.

Figure 112 Managed elements view

Geographical Domain	NE Name	Product Name	Configuration	IP Address	Comm. State
Domain-2	104 -		2RU; S-4: 1+0 / S-6: ...	10.10.66.104	Connected
Domain-2	105 -		2RU; S-3: 1+0	10.10.66.105	Connected
Domain-2	125 -		1RU; 1+0 / 1+0	10.10.66.125	Connected
Domain-2	131 -		1RU; S-5: 1+0	10.10.66.131	Connected
Domain-2	133 -		1RU; S-2: 1+0	10.10.66.133	Connected
Domain-3	140 -		2RU;	10.10.66.140	Connected
Domain-1	141 -		2RU; S-4: 1+0 / S-6: ...	10.10.66.141	Connected
Domain-1	142 -		2RU; S-: MC-ABC.1 0...	10.10.66.142	Connected
Domain-3	145 -		1RU;	10.10.66.145	Connected

This view shows elements currently managed by PTP 820 NMS.

Managed Elements table

The table displays the following fields for each NE in the table:

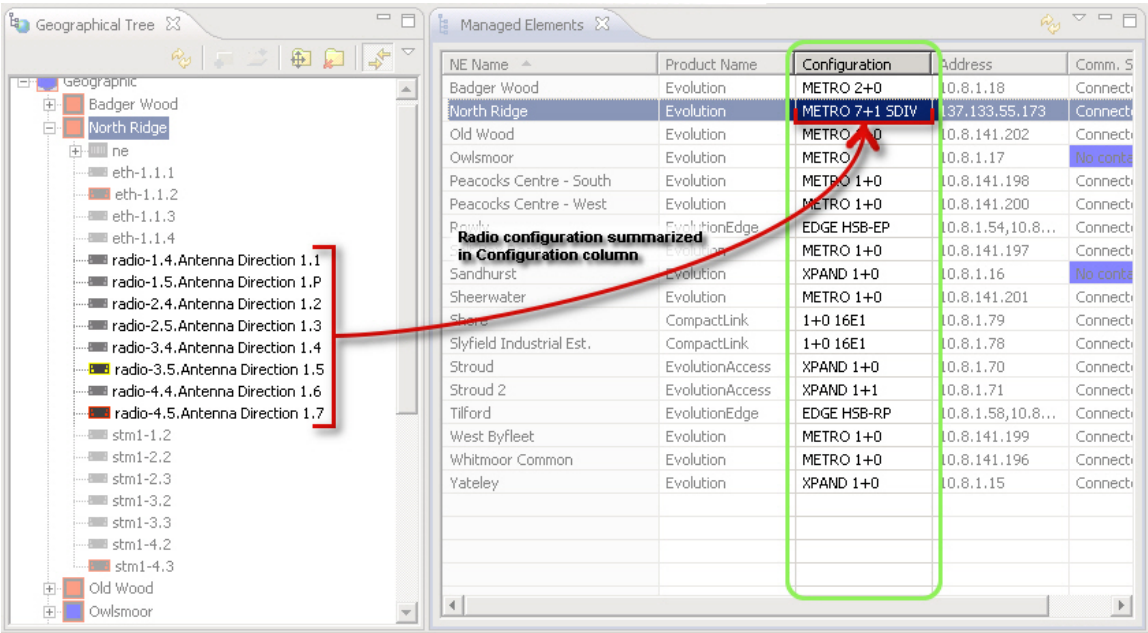
Table 37 Managed Elements table

Name	Explanation
Geographical Domain/Logical Domain	The domain to which the NE belongs.
NE Name	The PTP 820 NMS name of the NE. By default, set to the native name reported by the NE, but may be overridden by setting a new name in the properties view.
Product Name	The type of NE.
Configuration	A summary of the NE configuration, see further explanation below.
IP Address	The IP address for the management port of the NE
Comm. State	<p>The current communication state between the server and the NE:</p> <p>No contact: Indicates that there is Loss of Connectivity with the NE</p> <p>Connected: Indicates that communication currently is established with the NE</p>
System Level Version	<p>Identifies the version of the Managed Element as a whole, only available for some NE types.</p> <p>This column is by default not visible. In order to view it, select the Customize Columns button and change the columns settings.</p>
Notification Muted	Has the value "Y" if this NE currently is muted . Only alarms from unmuted elements can trigger alarm notifications .

Name	Explanation
Notification Mute Expiration	The time on the PTP 820 NMS server when muting on this element will automatically expire . Will have the value "Never" if element is muted without Notifications Mute Expiration enabled, and will be blank if element is not muted.
SysOID	The system object identifier as read during discovering of the element from sysObjectId variable defined in MIB2. By default, the column is hidden.

The configuration column which is populated for some NE types, summarizes the most important information about an element. For radio NEs, the summary is typically of the radio configuration. For example, in the figure below, **S-1.1,1.2:MC-ABC.1 2+0** in the second table row summarizes the information that Radio 1.1 and Radio 1.2 are under the MC-ABC.1 group, while **S-3.1: 1+0** and **S-2.1: 1+0** summarize the information that Radio-2.1 and Radio-3.1 are not under any group.



Figure 113 Managed elements configuration
























The above figure showing the relationship between the radio configuration and the Configuration column.







Available operations

The following operations are available in the table:

-  Refresh – Refreshes the display.
-  Link View – When activated, links this view with selected resources in other views.

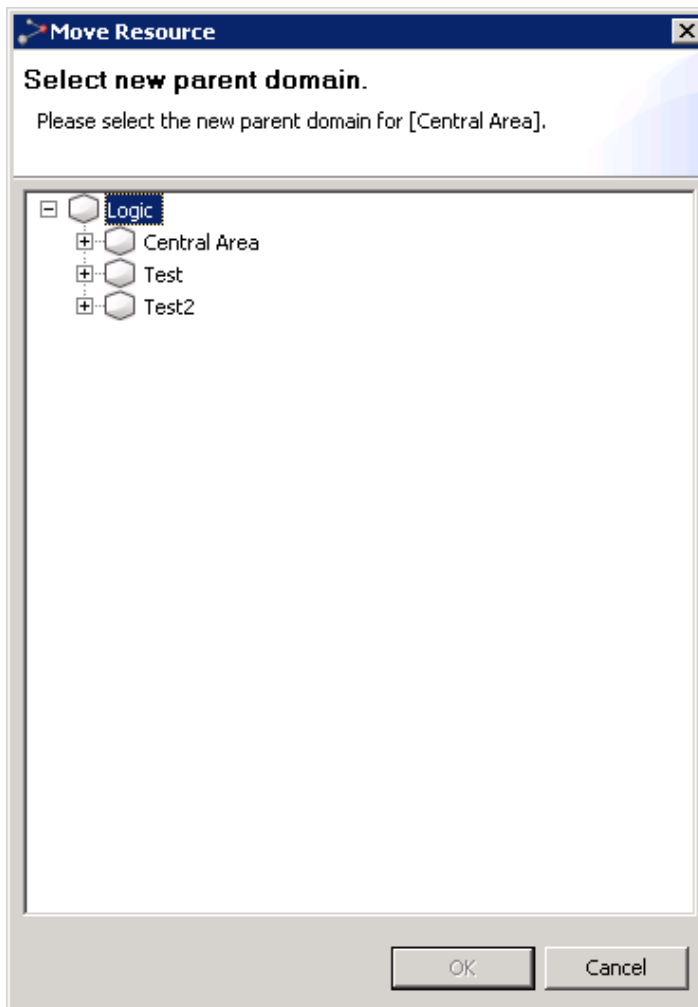
Operations available from the context menu of an element in the table

- Fault – Opens the following Fault views and functions:
 -  Active Alarms – Opens an Active Alarms view for the selected element.
 -  Historical Alarms – Opens a Historical Alarms view for the selected element.
 -  Alarm Templates Assignment – Opens an Alarm Templates Assignment view for the selected element.
-  Mute Notifications – Mutes an NE or a domain, to prevent alarms on the selected NE(s) from generating [alarm notifications](#). The [Mute Notifications dialog](#) will open, where you can select a time for automatic unmuting of notifications. When notifications are muted, NEs will have a [mute indicator](#) on NE level in the **Map** and **Tree** views.
-  Unmute Notifications – Unmutes a muted NE or a domain with muted element, to re-enable alarms on the selected NE(s) to generate [alarm notifications](#)
- Configuration – Opens the following Configuration views and functions:
 -  Hardware Inventory – Opens a Hardware Inventory view for the selected element.
 -  Software Inventory – Opens a Software Inventory view for the selected element.
 -  Transmission Inventory – Opens a Transmission Inventory view for the selected element.
 -  Create Software Download Job – Opens the Create Software Download Jobs wizard, enabling you to create a software download job for the selected element.
 -  Configuration File Management – Opens a Configuration File Management view for the selected element.
 -  Connection Template Assignment – Opens a Connection Template Assignment view for the selected element.
- Open SNMP Interface – Opens an “Open SNMP” Connection Template which can be used to manage the device. Basic SNMP management of the device will be triggered to read the inventory and faults from the device.
- External Tools – Enables opening a web EMS session with the selected device.
- Performance – Opens the following Performance views and functions:
 -  Current Performance – Opens a Current Performance view for the selected element.
 -  Historical Performance – Opens a Historical Performance view for the selected element.
 -  Performance Tables – Opens a Performance Tables view for the selected element.
 -  Performance Collection Control – Opens a Performance Collection Control view for the selected element.
- Reports – Opens the following Report views and functions:
 -  Network Element Types Overview Report – Opens a Network Element Types Overview Report view for the selected element.
 -  Inventory Report – Opens an Inventory Report view for the selected element.
 -  Inventory Tables – Opens an Inventory Tables view for the selected element.
 -  Web EMS – Opens a web EMS session with the selected device
 -  Show in Geographic Map – Opens a Geographical Map view of the domain.
 -  NE Outline – Opens the NE Outline view, displaying the equipment and port model for the selected device.

-  Topological Links – Opens a Topological Links view for the selected element
-  Reconcile – Instructs PTP 820 NMS to contact the network element, and update the PTP 820 NMS database with information about the element.
-  Ping/TraceRoute – Opens a Ping/TraceRoute view for the selected element.
-  Rename – Enables renaming the managed element.
-  Delete – Enables deleting the managed element.
- Select All – Selects all elements in the table.
-  Properties – Displays the element's properties in a Properties view.

Move Resource dialog

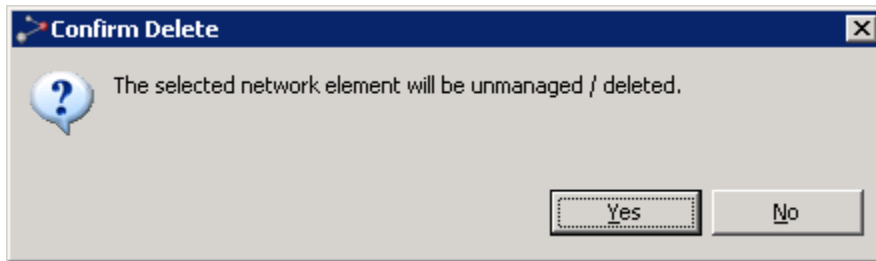
This dialog appears whenever selecting **Move** in the Managed Elements table.



Browse the tree in the dialog to find the parent domain to where you want to move your node. Please note that outlines/shapes of domains in the **Geographical Map** view will not remain when moving a domain like this. This is because the outline is stored at domain level.

Confirm Network Element Delete - NE exist in only one model

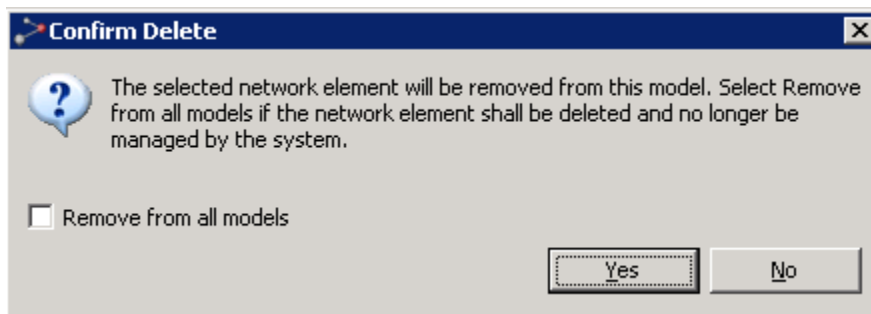
This dialog appears whenever selecting the **Delete** in the Managed Elements table, with an NE selected which only exists in one model.



Press **OK** to confirm you wish to delete the NE.

Confirm Network Element Delete - NE exists in both models

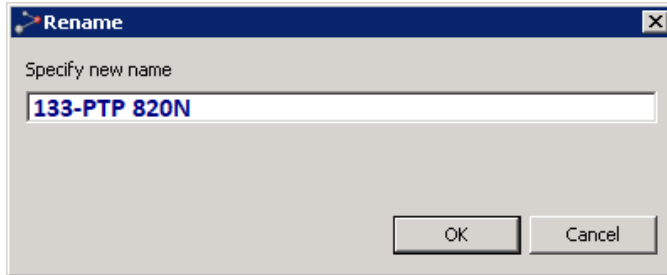
This dialog appears whenever selecting the **Delete** in the Managed Elements table, with an NE selected which exists in both Logical and Geographical model.



Press **OK** to confirm that you wish to delete the resource. If you check the **Remove from all models** checkbox, the NE will be removed from both the Logical Model (**Logical Tree** and **Map** views) and Geographical Model (**Geographical Tree** and **Map** views). If so, they can be re-managed using the [Unmanaged Elements](#) view.

Rename dialog

This dialog appears whenever selecting the **Rename** context menu. PTP 820 device names are synchronized between PTP 820 NMS and the devices. That is, renaming a device on PTP 820 NMS sets the device name on the device itself; and changing the device name on the device itself changes the device name on PTP 820 NMS.

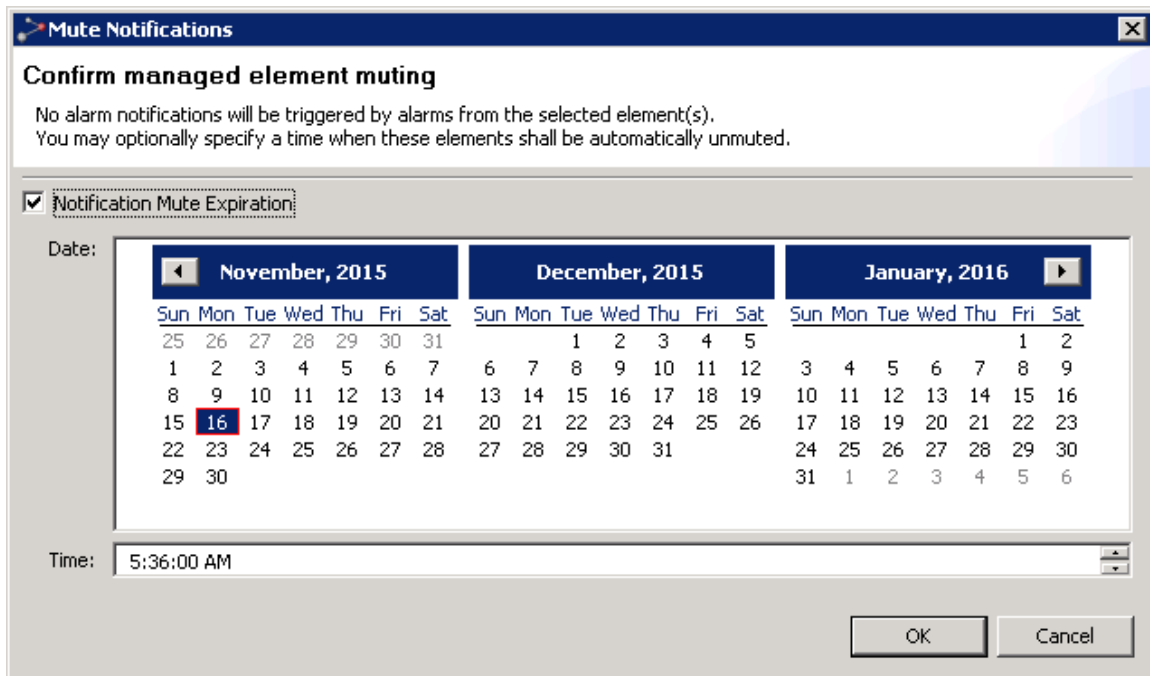


Enter a new name and press **OK** to perform the rename or press **Cancel** to abort.

Note: For PTP 820 devices, the device name can be up to 63 characters long.

Mute Notifications dialog

This dialog appears whenever selecting the **Mute Notifications** context menu in the tree with an NE or domain in focus.



This dialog requests confirmation to mute all selected elements, as well as any element beneath any selected administrative domain. Alarm notifications will not be sent for muted elements. In the tree and map views, muted elements can be identified by a [Mute indicator](#) on NE level. In the **Managed Elements** view, [Active Alarms view](#) and [Historical Alarms view](#), you can identify muted elements by including and sorting by the **Muted** column.

When muting elements, you have the option to enable automatic unmuting. If **Notifications Mute Expiration** is not enabled, the selected elements will stay muted until they are manually

unmuted. If you enable **Notifications Mute Expiration**, you must specify the **Date** and **Time** for the elements to be unmuted.

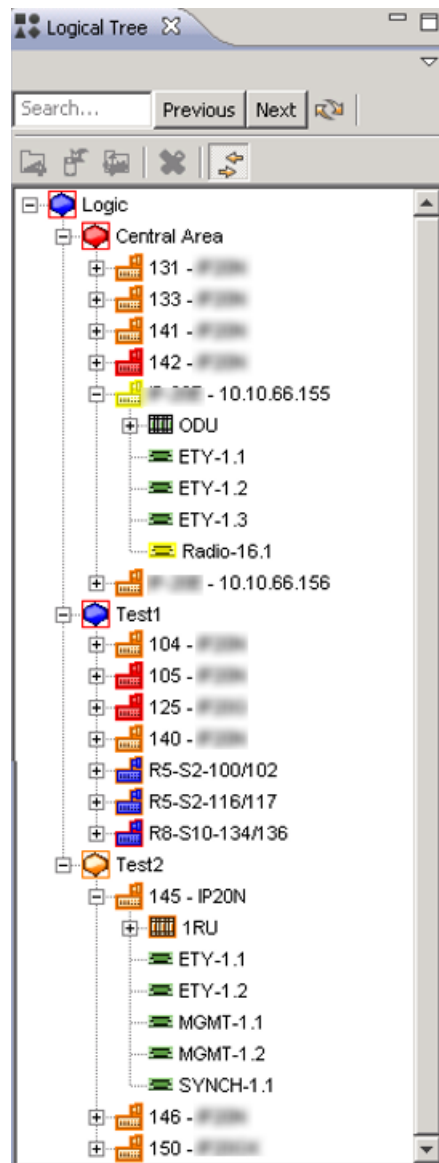
Press **OK** to enable muting or press **Cancel** to abort.

Logical Tree view

This view is found in the [Logical Surveillance](#) perspective

The view can also be opened by selecting **Views > Topology > Logical Tree** in the main menu.

The view can also be opened "[scoped](#)" by using the **Logical tree** menu with a domain selected in the **Logical Map** view or the **Logical Tree** view.



This is a view for organizing and monitoring your equipment based on a Logical Model of your network. The view allows you to browse the domains and browse each NE and its equipment (racks, ports, slots, ODU, etc.) reflecting the structure of each NE type.

The model used in the **Logical Tree** view is the same as in the **Logical Map** view. You can browse, create, delete and move logical domains, and the view also allows you to include, move and delete NEs. The structure of your domains can be used for assigning rights to different groups of users in the [Group Administration](#) view.






Examples of Logical Models of your network could be:

- Element type, element subtype, etc.
- Regional zones (with domains reflecting a geographical division of your network, but with boundaries which might overlap other geographical zones)
- Transmission capacity (e.g. 155/145Mb, 45/34Mb, 1.5/2Mb, etc.)
- Data communication network (with domains reflecting the physical connection of your network, which might overlap and differ from a geographical division)
- Company, contractor, party responsible
- Usage (e.g. main network, encrypted network, backup)
- Security profile (reflecting which security profile used for the NEs in each domain)

As this logical organization can be completely independent of the NE's geographical location, the same NE can exist in both models at the same time, or in only one. The Logical Model is separate from the Geographical Model used in the **Geographical Tree** view. The two **Tree** views operate on different models, but otherwise have exactly the same functionality.

The objects in a tree

The tree is a hierarchical representation of the domains and NEs, with each node in the tree containing one of the following objects:

-  A domain
-  A network element (NE)
-  An equipment holder
 - -an equipment holder represents resources on the NE that are capable of holding other physical components, such as racks (bays), shelves, slots or sub-slots.
-  A PTP or a CTP
 - a PTP (Physical Termination Point) is an end point of a topological link on an NE, typically a T1 port, T3 port or OC-N optical port.
 - a CTP (Connection Termination Point) is an end point of either a subnet connection or network interface at the network interface layer rate.
-  An equipment component
 - a manageable physical component of an NE, such as a circuit pack, a fan, a power supply or any other type of replaceable unit








Whenever an alarm is raised somewhere in the network, nodes will change color in the explorer view reflecting the current alarm status. The origin of each alarm can easily be found by inspecting this tree, as the colors are updated so that each node always contains the color of the most severe alarm in its subtree. Details of alarms and how colours are used for presenting alarms in the tree can be found in the chapter about [visualization of alarms](#).

Searching in the tree

You can search for elements in the tree. Enter a string in the **Search** field, and then use the **Next** (or **Previous**) button to go to the next (or previous):






- Element whose name includes the search string
- Element whose IP address includes the search string
- Domain whose name includes the search string

Available operations



-  **Refresh** Refresh the tree to present the latest NE status and the alarm state for the entire network.
-  **New Domain** Create a **new sub-domain** under the currently selected domain. The **New Administrative Domain** dialog will open, where you can enter a name for the new domain.
-  **Include Managed Element** Select one or more managed NE from the Geographical Model and manage them in the Logical Model by placing them under the currently selected domain. The **Include Managed Elements** dialog will appear, where you can view the list of unmanaged elements and select which NE you want to manage.
-  **Move** **Move** the currently selected node (NE or subdomain) to under another domain. If the node contains a subtree, this subtree with all its nodes will also be moved to the new domain. The **Move Resource** dialog will open where you will be able to select the domain you want to move the node to. Please note that outlines/shapes of domains in the **Logical Map** view will not remain when moving a domain like this. This is because the outline is stored at domain level.
-  **Ping/TraceRoute** - Opens a **Ping/TraceRoute** view for the selected NE.
-  Use **Drag & Drop** to move a selected resource directly into a domain in the tree. When clicking and dragging a node in the explorer view, a drag & drop indicator will appear in the mouse cursor. You can now drag the node into another domain, and when you release the mouse button the selected subtree will be moved into this node.
-  **Delete** **Delete** the selected node (NE or subdomain).

If the node is a domain, the entire subtree of domains and all its NEs will be deleted and the **Delete Domain from Model** dialog will open, where you can confirm or cancel the operation.

If the currently selected node is an NE, the **Delete Network Element from Model** dialog will appear. In this dialog you can also choose to remove the NE from the Geographical Model.

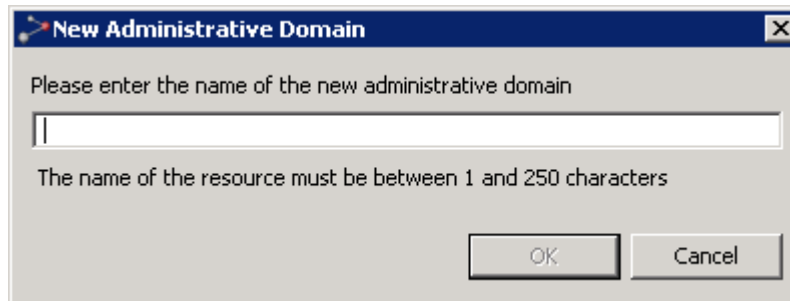
-  **Rename** **Rename** the currently selected node by opening the **Rename** dialog.
-  **Expand** the **selected node** in the tree by clicking the plus-sign. You can also expand a node by **double-clicking** an unexpanded node in the tree.
-  **Collapse** the **selected node** in the tree by clicking the minus-sign. You can also collapse a node by **double-clicking** an expanded node in the tree.
-  **Expand All** **Expand** the **entire subtree** below the currently selected node.
-  **Collapse All** **Collapse** the **entire subtree** below the currently selected node.

In addition, the following views, dialogs and functions can be opened with data from a node in the view (using the currently selected node as [scope](#)):

- **Logical Map** view (this view will also open when you **double-click** a domain in the tree)
- **Logical Tree** view
- fault:
 - **Active Alarms** view
 - **Historical Alarms** view
 - **Alarm Templates Assignment** view
 -  **Mute Notifications...** **Mute** an NE or a domain, to prevent alarms on the selected NE(s) from generating [alarm notifications](#). The [Mute Notifications dialog](#) will open, where you can choose to select a time for automatic unmuting of the element. When being muted, NEs will have a [mute indicator](#) on NE level in the **Map** and **Tree** views.
 -  **Unmute Notifications** **Unmute** a muted NE or a domain with muted element, to re-enable alarms on the selected NE(s) to generate [alarm notifications](#).
- configuration:
 - **Hardware Inventory** view
 - **Software Inventory** view
 - **Transmission Inventory** view
 - **Create Software Download Jobs** wizard
 - **Configuration File Management** view
 - **Connection Template Assignment** view
 - **External Tools**
- performance:
 - **Current Performance** view
 - **Historical Performance** view
 - **Performance Collection Control** view
 - **Reset Cumulative Performance Counters** dialog
- reports:
 - **Network Element Types Overview Report**
 - **Inventory Report**
- **Properties** view

New Administrative Domain dialog

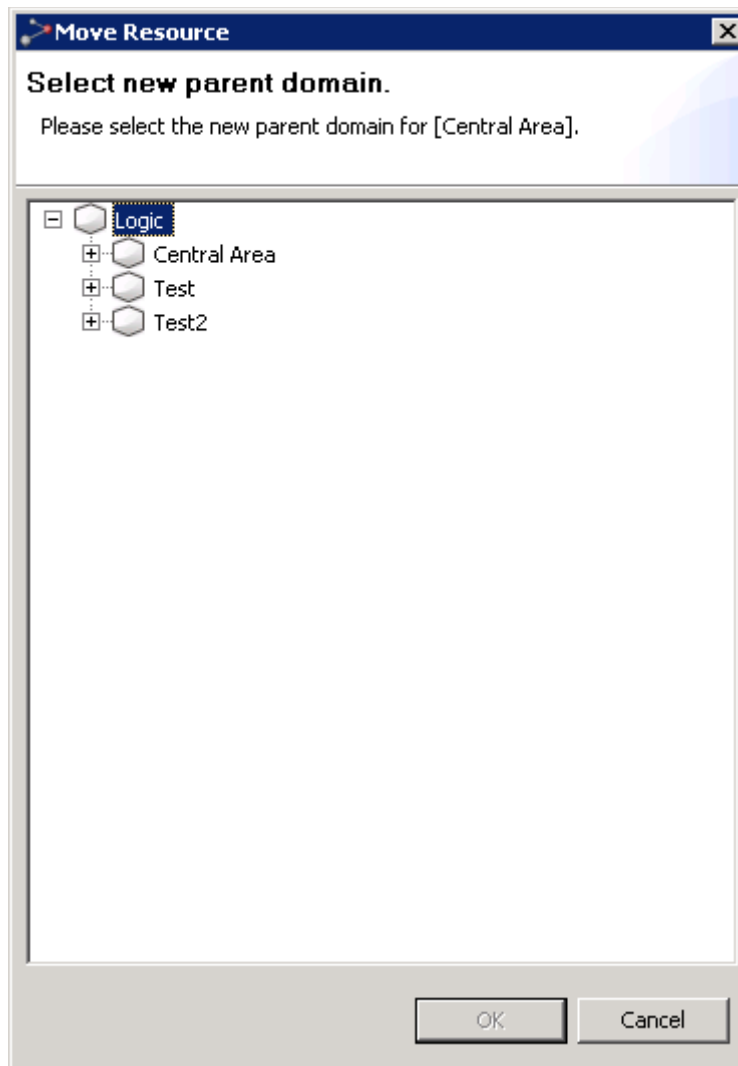
This dialog appears whenever selecting the **New Domain** context menu with a domain selected in the tree:



Enter a name in the text field. When **OK** is pressed, the new subdomain is created and placed under the currently selected domain.

Move Resource dialog

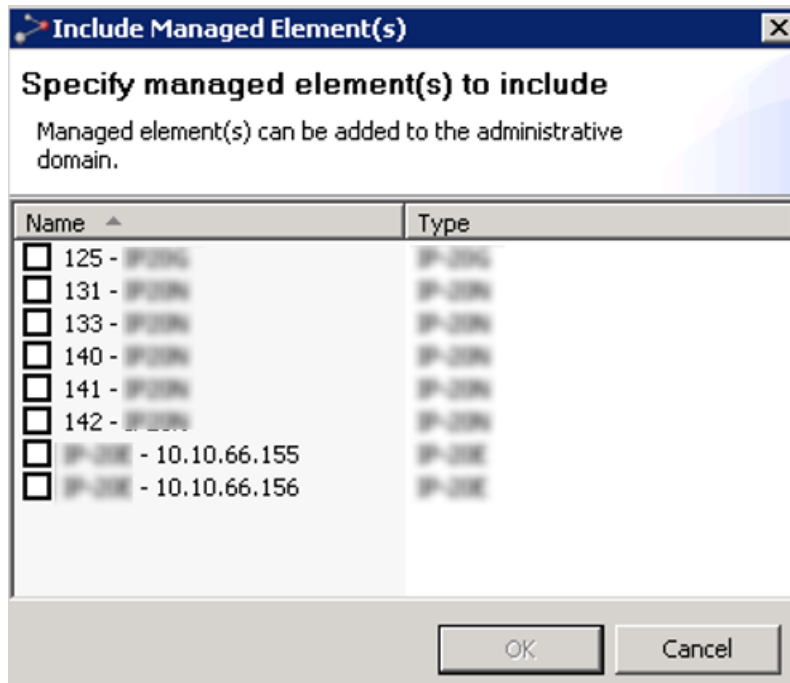
This dialog appears whenever selecting **Move** with an NE or subdomain in focus in the tree.



Browse the tree in the dialog to find the parent domain to where you want to move your node. Please note that outlines/shapes of domains in the **Logical Map** view will not remain when moving a domain like this. This is because the outline is stored at domain level.

Include Managed Elements dialog

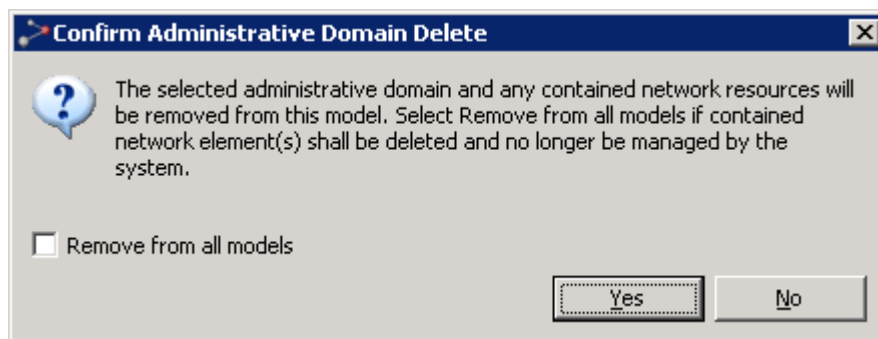
This dialog appears whenever selecting the **Include Managed Elements** context menu with a domain in focus in the tree.



This dialog presents a list of NEs that are managed in the Geographical Model (**Geographical Tree** and **Map** views), but not in the Logical Model. Select the NEs you want to manage, and they will be managed in the currently selected subdomain.

Delete Domain from Model dialog

This dialog appears whenever selecting the **Delete** context menu in the map with a domain in focus.



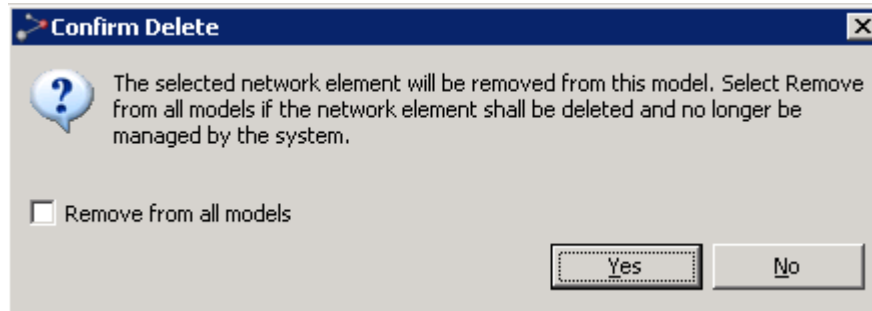
Press **OK** to confirm that you wish to delete the domain and all its NEs.

NEs deleted in this way will only be removed from the Logical Model (**Logical Tree** and **Logical Map**), and not from the Geographical Model (**Geographical Tree** and **Geographical Map**). The deleted NEs can be re-included in another domain in the Logical Model using the **Include Managed Element** function in this view. However, this is only possible if the NE also existed in the Geographical Model during the delete process. If a deleted NE does not belong to any other model, they will become unmanaged once deleted and must be re-managed using the [Unmanaged Elements](#) view.

In any case, if you check the **Remove from all models** checkbox, the domain and all its NEs will also be removed from the Geographical Model (**Geographical Tree** and **Geographical Map**). If so, they must be re-managed using the **Unmanaged Elements** view.

Delete Network Element from Model dialog

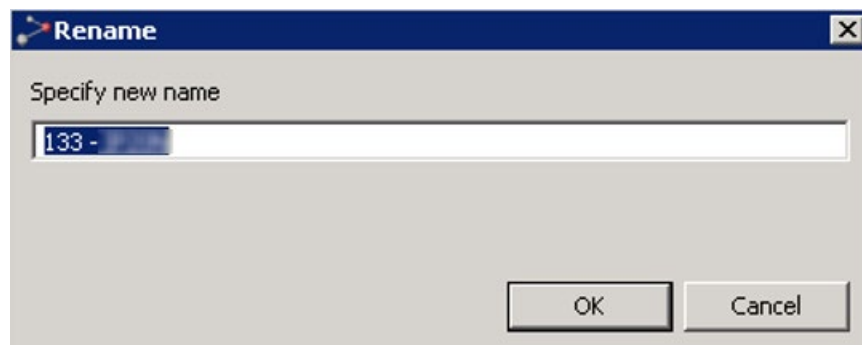
This dialog appears whenever selecting the **Delete** context menu in the tree with an NE in focus.



Press **OK** to confirm that you wish to delete the resource. If you check the **Remove from all models** checkbox, the NE will also be removed from the Geographical Model (**Geographical Tree** and **Geographical Map**). If so, they must be re-managed using the **Unmanaged Elements** view.

Rename dialog

This dialog appears whenever selecting the **Rename** context menu in the tree with an NE or subdomain in focus. PTP 820 device names are synchronized between PTP 820 NMS and the devices. That is, renaming a device on PTP 820 NMS sets the device name on the device itself; and changing the device name on the device itself changes the device name on PTP 820 NMS.

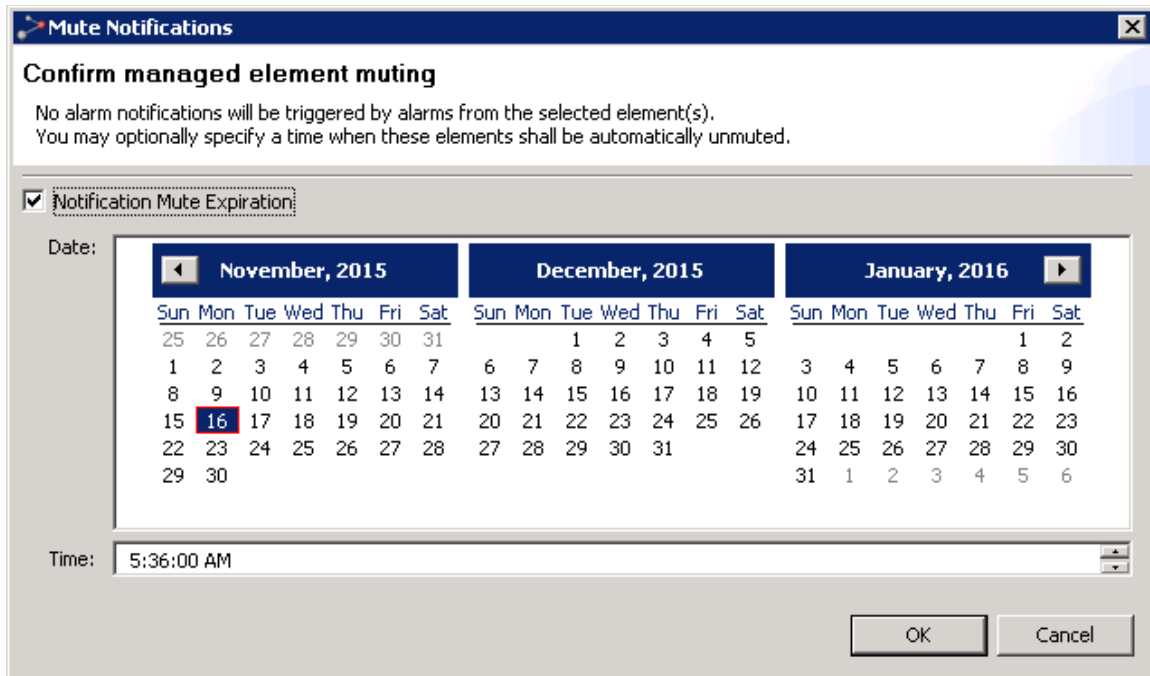


Enter a new name and press **OK** to perform the rename or press **Cancel** to abort.

Note: For PTP 820 devices, the device name can be up to 63 characters long.

Mute Notifications dialog

This dialog appears whenever selecting the **Mute Notifications** context menu in the tree with an NE or domain in focus.



This dialog requests confirmation to mute all selected elements, as well as any element beneath any selected administrative domain. Alarm notifications will not be sent for muted elements. In the tree and map views, muted elements can be identified by a [Mute indicator](#) on NE level. In the [Managed Elements view](#), [Active Alarms view](#) and [Historical Alarms view](#), you can identify muted elements by including and sorting by the **Muted** column.

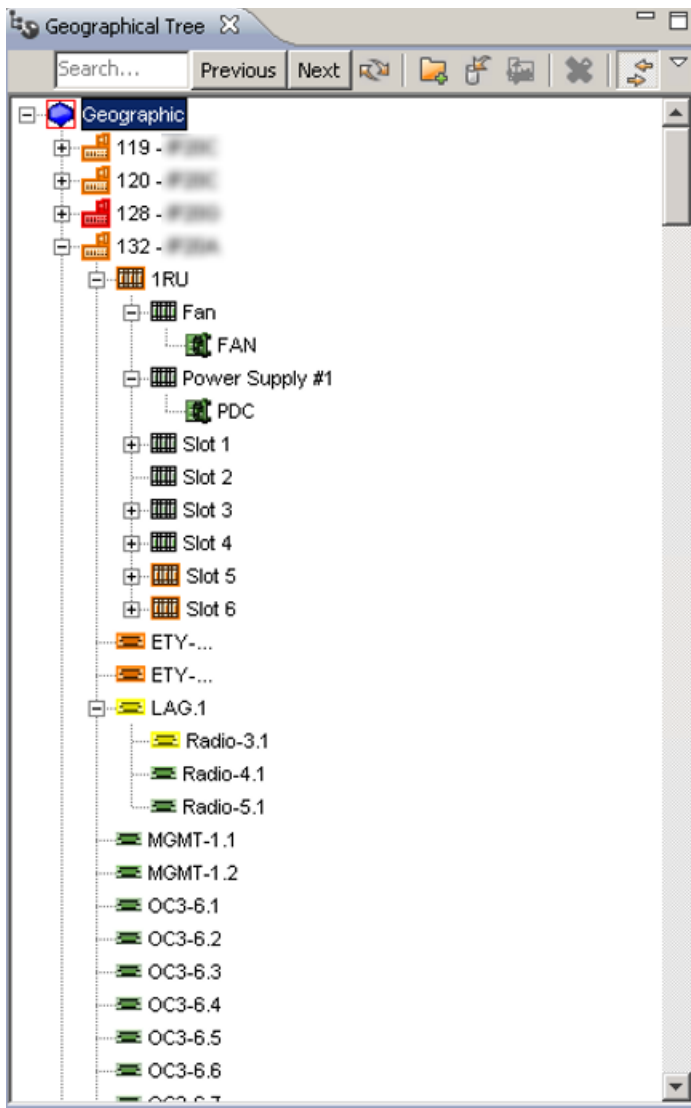
When muting elements, you have the option to enable automatic unmuting. If **Notifications Mute Expiration** is not enabled, the selected elements will stay muted until they are manually unmuted. If you enable **Notifications Mute Expiration**, you must specify the **Date** and **Time** for the elements to be unmuted.

Press **OK** to enable muting or press **Cancel** to abort.

Geographical Tree view

This view can be found in both the [Discover](#) perspective and the [Geographical Surveillance](#) perspective.

The view can also be opened by selecting Views | Topology | Geographical Tree in the main menu. The view can also be opened "[scoped](#)" by using the Geographical Tree menu with a domain selected in the [Geographical Map](#) view or the Geographical Tree view.

Figure 114 Topology: geographical tree view






This is a view for organizing and monitoring your equipment based on a geographical model of your network. The view allows you to browse the domains and browse each NE and its equipment (racks, ports, slots, ODUs, etc.) reflecting the structure of each NE type.

The Geographical Model used in the Geographical Tree view is the same as in the [Geographical Map](#) view. You can browse, create, delete and move geographical domains corresponding to the physical location (country, region, city, etc.) of your NE. This geographical organization of your network is separate from Logical Model used in the [Logical Tree](#) view. The two Tree views operate on different models, but otherwise have exactly the same functionality. An NE can exist in both models at the same time, or in only one.

The Geographical Tree view allows you to include, move and delete NEs. The structure of your domains can be used for assigning rights to different groups of users in the [Group Administration](#) view.

The objects in a tree

The tree is a hierarchical representation of the domains and NEs, with each node in the tree containing one of the following objects:

-  A domain
-  A network element (NE)
-  An equipment holder.
 - an equipment holder represents resources on the NE that are capable of holding other physical components, such as racks (bays), shelves, slots or sub-slots.
-  A PTP or a CTP.
 - a PTP (Physical Termination Point) is an end point of a topological link on an NE, typically a T1 port, T3 port or OC-N optical port.
 - a CTP (Connection Termination Point) is an end point of either a subnet connection or network interface at the network interface layer rate.
-  An equipment component
 - a manageable physical component of an NE, such as a circuit pack, a fan, a power supply or any other type of replaceable unit




Whenever an alarm is raised somewhere in the network, nodes will change color in the explorer view reflecting the current alarm status. The origin of each alarm can be found by browsing the tree, as the colors are updated so that each node always contains the color of the most severe alarm in its subtree. Details of alarms and how colours are used for presenting alarms in the tree can be found in the chapter about [visualization of alarms](#).




Searching in the tree

You can search for elements in the tree. Enter a string in the **Search** field, and then use the **Next** (or **Previous**) button to go to the next (or previous):






- Element whose name includes the search string
- Element whose IP address includes the search string
- Domain whose name includes the search string

Available operations



-  **Refresh** Refresh the tree to present the latest NE status and the alarm state for the entire network.
-  **New Domain** Create a new sub-domain under the currently selected domain. The [New Administrative Domain](#) dialog will open, where you can enter a name for the new domain.
-  **Include Managed Element** Select one or more managed NE from the Logical Model and manage them in the Geographical Model by placing them under the currently selected domain. The [Include Managed Elements](#) dialog will appear, where you can view the list of unmanaged elements and select which NE you want to manage.

-  **Move** Move the currently selected node (NE or subdomain) to another domain. If the node contains a subtree, this subtree with all its nodes will also be moved to the new domain. The [Move Resource](#) dialog will open where you will be able to select the domain you want to move the node to. Please note that outlines/shapes of domains in the Geographical Map view will not remain when moving a domain like this. This is because the outline is stored at domain level.
-  Use Drag & Drop to move a selected resource directly into a domain in the tree. When clicking and dragging a node in the explorer view, a drag & drop indicator will appear in the mouse cursor. You can now drag the node into another domain, and when you release the mouse button the selected subtree will be moved into this domain.
-  **Delete** Delete the selected node (NE or subdomain).
- If the node is a domain, the entire subtree of domains and all its NEs will be deleted and the [Delete Domain from Model](#) dialog will open, where you can confirm or cancel the operation.

If the currently selected node is an NE, the [Delete Network Element from Model](#) dialog will appear. In this dialog you can also choose to remove the NE from the logical model.

-  **Rename** Rename the currently selected node by opening the [Rename](#) dialog.
-  Expand the selected node in the tree by clicking the plus-sign. You can also expand a node by double-clicking an unexpanded node in the tree.
-  Collapse the selected node in the tree. You can also collapse a node by double-clicking an expanded node in the tree.
-  **Expand All** Expand the entire subtree below the currently selected node.
-  **Collapse All** Collapse the entire subtree below the currently selected node.

In addition, the following views, dialogs and functions can be opened with data from a node in the view (using the currently selected node as [scope](#)):

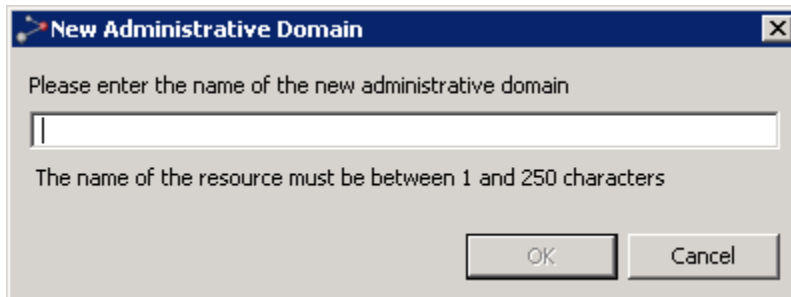
- Geographical Map view (this view will also open when you double-click a domain in the tree)
- Geographical Tree view
- Fault:
 - Active Alarms view
 - Historical Alarms view
 - Alarm Templates Assignment view
-  **Mute Notifications...** Mute an NE or a domain, to prevent alarms on the selected NE(s) from generating [alarm notifications](#). The [Mute Notifications dialog](#) will open, where you can choose to select a time for automatic unmuting the element. When being muted, NEs will have a [mute indicator](#) on NE level in the Map and Tree views.
-  **Unmute Notifications** Unmute a muted NE or a domain with muted element, to re-enable alarms on the selected NE(s) to generate [alarm notifications](#).
- Configuration:

- Hardware Inventory view
- Software Inventory view
- Transmission Inventory view
- Create Software Download Jobs wizard
- Configuration File Management view
- Connection Template Assignment view
- External Tools
- Performance:
 - Historical Performance view
 - Current Performance view
 - Performance Collection Control view
 - Reset Cumulative Performance Counters dialog
- Reports:
 - Network Element Types Overview Report
 - Inventory Report
- Properties view

New Administrative Domain dialog

This dialog appears whenever selecting the New Domain context menu with a domain selected in the tree:

Figure 115 Topology: new administrative domain dialog

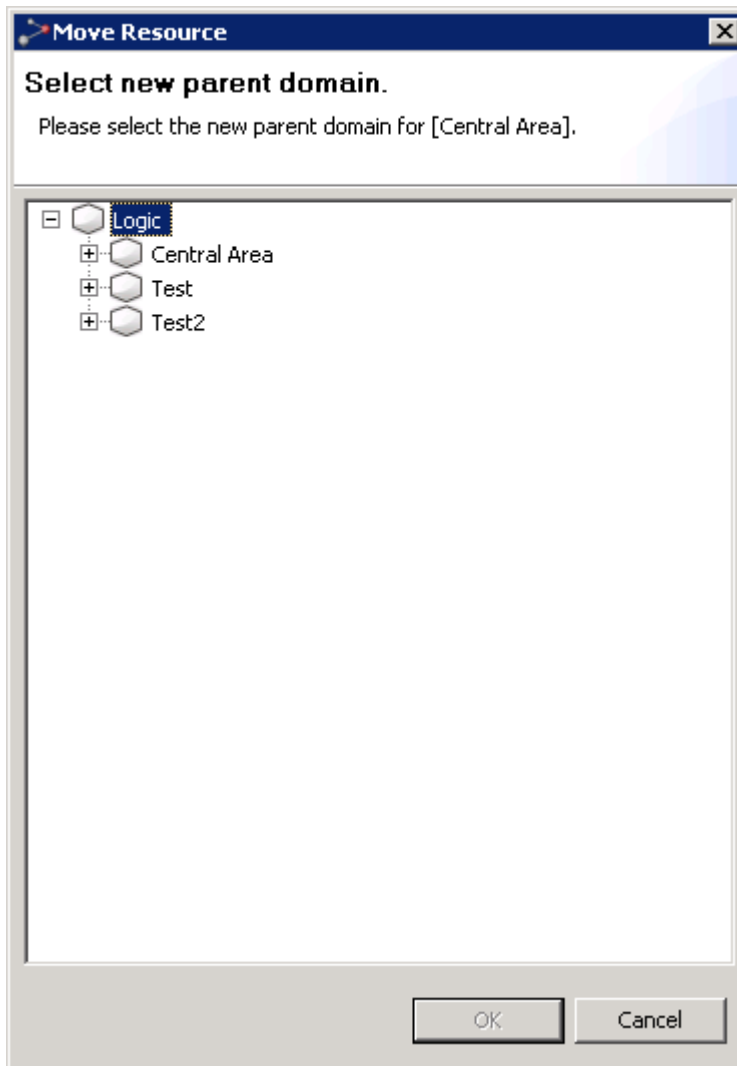


Enter a name in the text field. When OK is pressed, the new subdomain is created and placed under the currently selected domain.

Move Resource dialog

This dialog appears whenever selecting Move with an NE or subdomain in focus in the tree.

Figure 116 Topology: move resource dialog

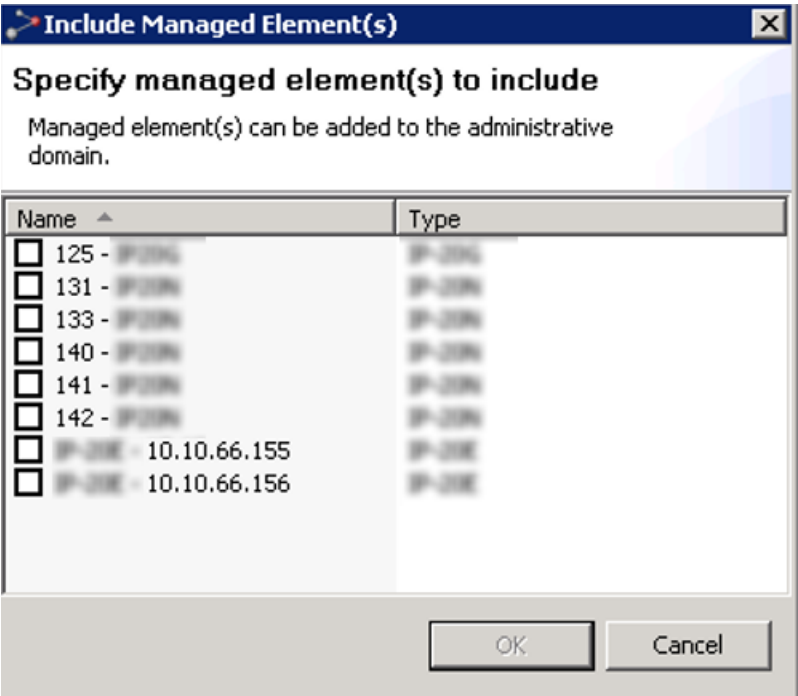


Browse the tree in the dialog to find the parent domain to where you want to move your node. Please note that outlines/shapes of domains in the Geographical Map view will not remain when moving a domain like this. This is because the outline is stored at domain level.

Include Managed Elements dialog

This dialog appears whenever selecting the Include Managed Elements context menu with a domain in focus in the tree.

Figure 117 Topology: Include manage elements dialog

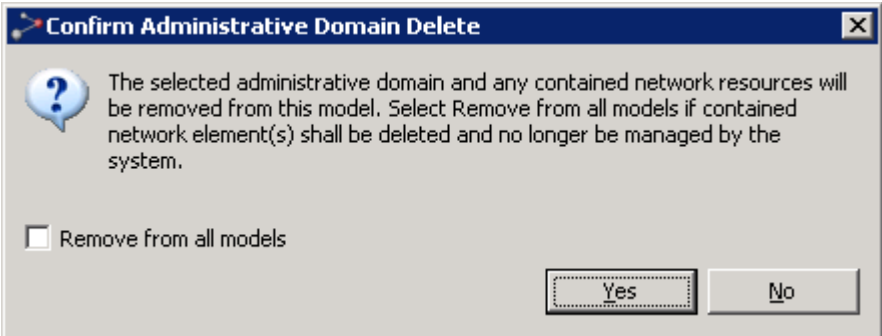


This dialog presents a list of NEs that are managed in the Logical Model (Logical Tree and Map views), but not in the Geographical Model. Select the NEs you want to manage, and they will be managed in the currently selected subdomain.

Delete Domain from Model dialog

This dialog appears whenever selecting the Delete context menu in the map with a domain in focus.

Figure 118 Topology: delete domain from model dialog



Press OK to confirm you wish to delete the domain and all its NEs.

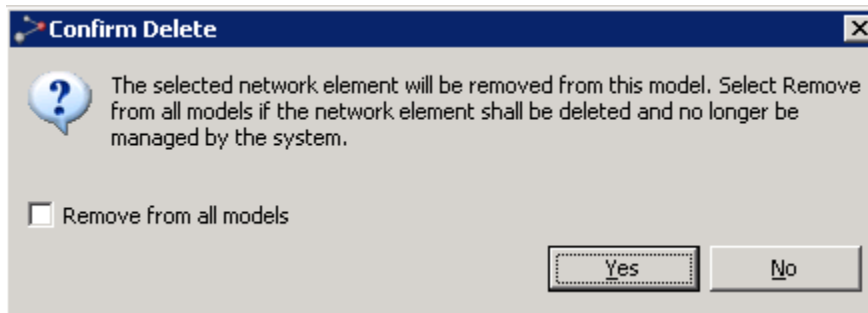
NEs deleted in this way will only be removed from the Geographical Model (Geographical Tree and Map views), and not from the Logical Model (Logical Tree and Map views). The deleted NEs can be re-included in another domain in the Geographical Model using the Include Managed Element function in this view. However, this is only possible if the NE also existed in the Logical Model during the delete process. If a deleted NE does not belong to any other model, they will become unmanaged once deleted and must be re-managed using the [Unmanaged Elements](#) view.

In any case, if you check the Remove from all models checkbox, the domain and all its NEs will also be removed from the Geographical Model (Geographical Tree and Geographical Map). If so, they must be re-managed using the Unmanaged Elements view.

Delete Network Element from Model dialog

This dialog appears whenever selecting the Delete context menu in the tree with an NE in focus.

Figure 119 Topology: delete network element from model dialog

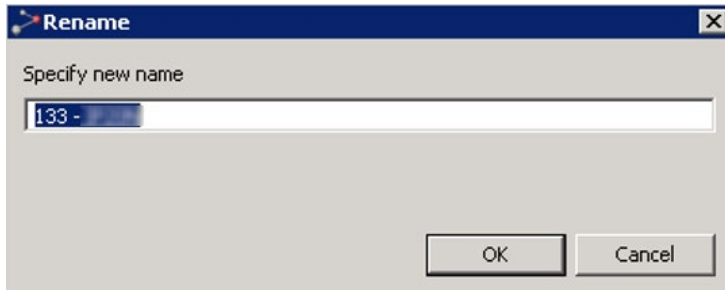


Press OK to confirm that you wish to delete the resource. If you check the Remove from all models checkbox, the NE will also be removed from the Logical Model (Logical Tree and Map views). If so, they must be re-managed using the Unmanaged Elements view.

Rename dialog

This dialog appears whenever selecting the Rename context menu in the tree with an NE or subdomain in focus.

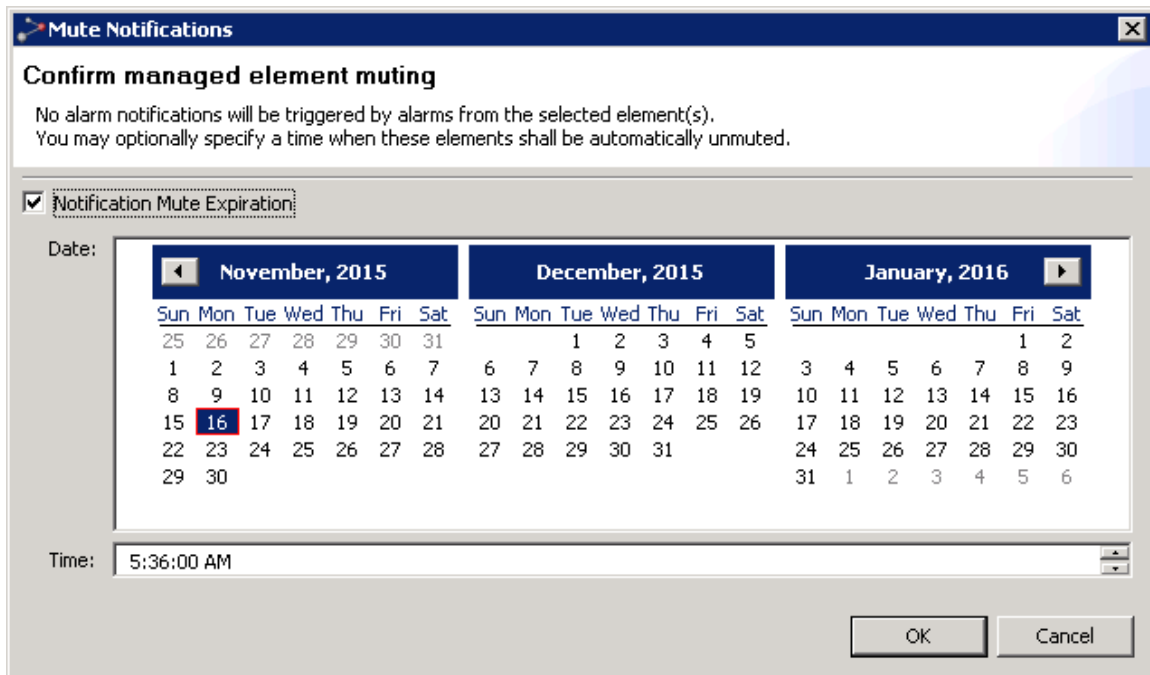
Figure 120 Topology: rename dialog



Mute Notifications dialog

This dialog appears whenever selecting the Mute Notifications context menu in the tree with an NE or domain in focus.

Figure 121 Topology: Mute notifications dialog



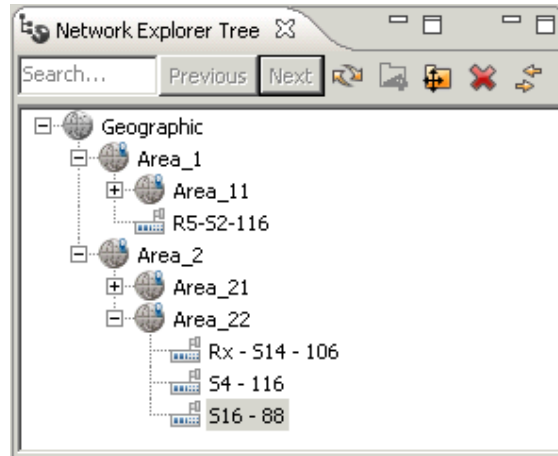
This dialog requests confirmation to mute all selected elements, as well as any element beneath any selected administrative domain. Alarm notifications will not be sent for muted elements. In the tree and map views, muted elements can be identified by a [Mute indicator](#) on NE level. In the [Managed Elements view](#), [Active Alarms view](#) and [Historical Alarms view](#), you can identify muted elements by including and sorting by the Muted column.

When muting elements, you have the option to enable automatic unmuting. If Notifications Mute Expiration is not enabled, the selected elements will stay muted until they are manually unmuted. If you enable Notifications Mute Expiration, you must specify the Date and Time for the elements to be unmuted.

Press OK to enable muting or press Cancel to abort.

Network Explorer Tree View

This view can be found in the [Network Explorer](#) perspective. The view can also be opened from **Views > Topology > Network Explorer Tree** in the main menu.





This is a view for organizing and monitoring your equipment based on a hierarchical model of your network. The view allows you to browse the domains and NEs.

The model used in the **Network Explorer Tree** view is the same as in the [Network Explorer Map](#) view. You can move and delete NEs. You can also browse, create, delete and move domains corresponding to the physical location (country, region, city, etc.) of your NE. The structure of your domains can be used for assigning rights to different groups of users in the [Group Administration](#) view.

The objects in a tree

The tree is a hierarchical representation of the domains and NEs, with each node in the tree containing one of the following objects:



-  A domain
-  A network element (NE)



Searching in the tree

You can search for elements in the tree. Enter a string in the **Search** field, and then press Enter or use the **Next** (or **Previous**) button to go to the next (or previous):















- Element whose name includes the search string
- Element whose IP address includes the search string
- Domain whose name includes the search string














Available operations

-  Refresh – Refreshes the tree to present the latest NE status for the entire network.
-  New Domain – Opens a **New Administrative Domain** dialog for creating a **new sub-domain** under the currently selected domain .







-  Move – Moves the currently selected node (NE or subdomain) to another domain. If the node contains a sub-tree, this sub-tree with all its nodes will also be moved to the new domain. The **Move Resource** dialog will open where you will be able to select the domain you want to move the node to.
-  Delete – Deletes the selected node (NE or subdomain).
 - If the node is a domain, the entire subtree of domains and all its NEs will be deleted and the **Confirm Administrative Domain Delete** dialog will open, where you can confirm or cancel the operation.
 - If the currently selected node is an NE, the **Confirm Delete** dialog will appear, where you can confirm or cancel the operation.






















Operations available from the context menu of a domain in the tree


- Fault – Opens the following Fault views and functions:
 -  Active Alarms – Opens an Active Alarms view for the selected domain.
 -  Historical Alarms – Opens a Historical Alarms view for the selected domain.
 -  Alarm Templates Assignment – Opens an Alarm Templates Assignment view for the selected domain.
 -  Mute Notifications – Mutes an NE or a domain, to prevent alarms on the selected NE(s) from generating [alarm notifications](#). The [Mute Notifications dialog](#) will open, where you can select a time for automatic unmuting of notifications. When notifications are muted, NEs will have a [mute indicator](#) on NE level in the **Map** and **Tree** views.
 -  Unmute Notifications – Unmutes a muted NE or a domain with muted element, to re-enable alarms on the selected NE(s) to generate [alarm notifications](#)
- Configuration – Opens the following Configuration views and functions:
 -  Hardware Inventory – Opens a Hardware Inventory view for the selected domain.
 -  Software Inventory – Opens a Software Inventory view for the selected domain.
 -  Transmission Inventory – Opens a Transmission Inventory view for the selected domain.
 -  Create Software Download Job – Opens the Create Software Download Jobs wizard, enabling you to create a software download job for the selected domain.
 -  Configuration File Management – Opens a Configuration File Management view for the selected domain.
 -  Connection Template Assignment – Opens a Connection Template Assignment view for the selected domain.
- Performance – Opens the following Performance views and functions:
 -  Current Performance – Opens a Current Performance view for the selected domain.
 -  Historical Performance – Opens a Historical Performance view for the selected domain.
 -  Performance Collection Control – Opens a Performance Collection Control view for the selected domain.

-  Reset Cumulative Performance Counters – Opens a Reset Cumulative Performance Counters dialog for resetting counter values of cumulative counters to zero on the domain.
- Reports – Opens the following Report views and functions:
 -  Network Element Types Overview Report – Opens a Network Element Types Overview Report view for the selected domain.
 -  Inventory Report – Opens an Inventory Report view for the selected domain.
 -  Inventory Tables – Opens an Inventory Tables view for the selected domain.
-  Show in Network Explorer Map – Displays the selected domain in the Network Explorer Map.
-  Network Explorer Map – Displays the contents of the selected domain in the Network Explorer Map.
-  Managed Elements – Opens a Managed Elements view for the selected domain.
-  Topological Links – Opens a Topological Links view for the selected domain.
-  New Domain – Open a **New Administrative Domain** dialog for creating a **new sub-domain** under the currently selected domain.
-  Move – Moves the currently selected node (NE or subdomain) to another domain. If the node contains a sub-tree, this sub-tree with all its nodes will also be moved to the new domain. The **Move Resource** dialog will open where you will be able to select the domain you want to move the node to.
-  Rename – Enables renaming the managed domain.
-  Delete – Enables deleting the managed domain.
- Select All – Selects all elements in the tree.
-  Properties – Displays the domain's properties in a Properties view.

Operations available from the context menu of an NE in the tree

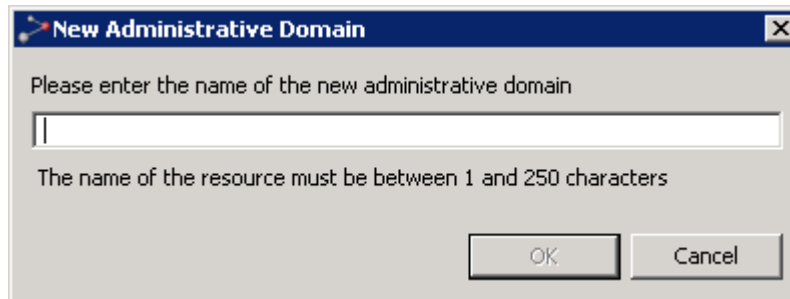
- Fault – Opens the following Fault views and functions:
 -  Active Alarms – Opens an Active Alarms view for the selected element.
 -  Historical Alarms – Opens a Historical Alarms view for the selected element.
 -  Alarm Templates Assignment – Opens an Alarm Templates Assignment view for the selected element.
 -  Mute Notifications – Mutes an NE or a domain, to prevent alarms on the selected NE(s) from generating [alarm notifications](#). The [Mute Notifications dialog](#) will open, where you can select a time for automatic unmuting of notifications. When notifications are muted, NEs will have a [mute indicator](#) on NE level in the **Map** and **Tree** views.
 -  Unmute Notifications – Unmutes a muted NE or a domain with muted element, to re-enable alarms on the selected NE(s) to generate [alarm notifications](#)
- Configuration – Opens the following Configuration views and functions:
 -  Hardware Inventory – Opens a Hardware Inventory view for the selected element.

-  Software Inventory - Opens a Software Inventory view for the selected element.
-  Transmission Inventory - Opens a Transmission Inventory view for the selected element.
-  Create Software Download Job - Opens the Create Software Download Jobs wizard, enabling you to create a software download job for the selected element.
-  Configuration File Management - Opens a Configuration File Management view for the selected element.
-  Connection Template Assignment - Opens a Connection Template Assignment view for the selected element.
- Open SNMP Interface- Opens an “Open SNMP” Connection Template which can be used to manage the device. Basic SNMP management of the device will be triggered to read the inventory and faults from the device.
- External Tools - Enables opening a web EMS session with the selected device.
- Performance - Opens the following Performance views and functions:
 -  Current Performance - Opens a Current Performance view for the selected element.
 -  Historical Performance - Opens a Historical Performance view for the selected element.
 -  Performance Tables - Opens a Performance Tables view for the selected element.
 -  Performance Collection Control - Opens a Performance Collection Control view for the selected element.
- Reports - Opens the following Report views and functions:
 -  Network Element Types Overview Report - Opens a Network Element Types Overview Report view for the selected element.
 -  Inventory Report - Opens an Inventory Report view for the selected element.
 -  Inventory Tables - Opens an Inventory Tables view for the selected element.
-  Web EMS - Opens a web EMS session with the selected element.
-  Show in Network Explorer Map - Displays the selected element in the Network Explorer Map
-  Element Explorer - Opens an [Element Explorer](#) view for the selected element.
-  Topological Links - Opens a Topological Links view for the selected element
-  Reconcile - Instructs PTP 820 NMS to contact the network element, and update the PTP 820 NMS database with information about the element.
-  Ping/TraceRoute - Opens a Ping/TraceRoute view for the selected element.
-  Move - Moves the currently selected node (NE or subdomain) to another domain. If the node contains a sub-tree, this sub-tree with all its nodes will also be moved to the new domain. The **Move Resource** dialog will open where you will be able to select the domain you want to move the node to.
-  Rename - Enables renaming the managed element.
-  Delete - Enables deleting the managed element.

- Select All – Selects all elements in the tree.
-  Properties – Displays the element's properties in a Properties view.

New Administrative Domain dialog

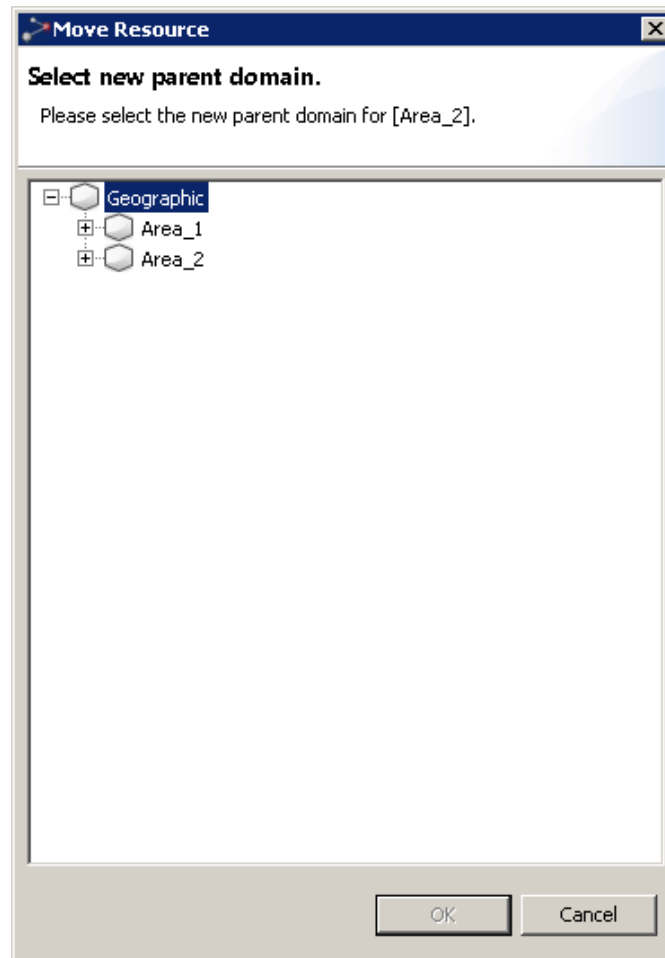
This dialog appears whenever selecting the **New Domain** context menu with a domain selected in the tree:



Enter a name in the text field. When **OK** is pressed, the new subdomain is created and placed under the currently selected domain.

Move Resource dialog

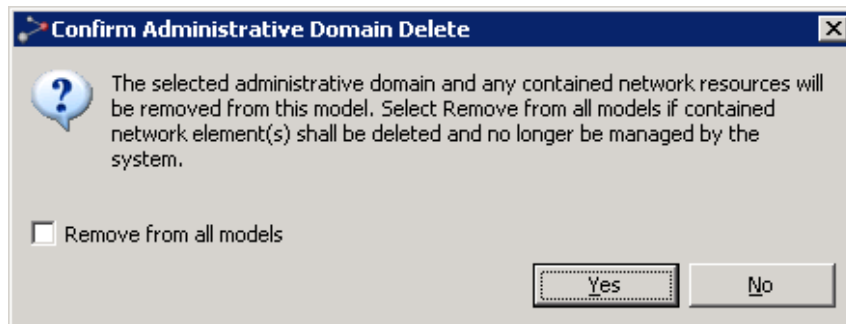
This dialog appears whenever selecting **Move** with an NE or subdomain in focus in the tree.



Browse the tree in the dialog to find the parent domain to where you want to move your node. The outlines/shape of a domain will not remain when moving it to another domain level.

Delete Domain from Model dialog

This dialog appears whenever selecting the **Delete** context menu in the tree with a domain in focus.



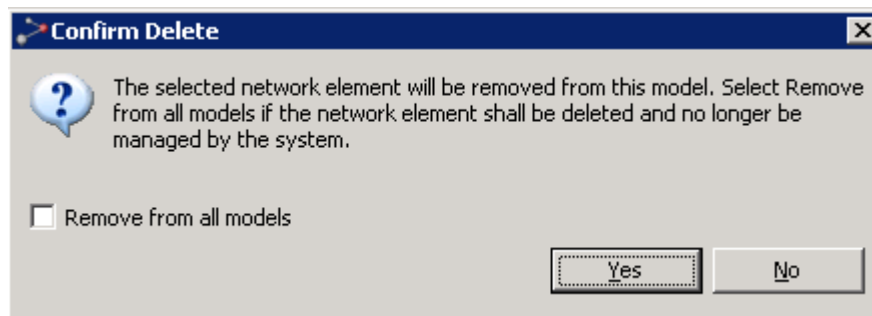
Press **Yes** to confirm that you wish to delete the domain and all its NEs.

NEs deleted in this way will be removed from the model (either Geographical or Logical) linked to the Network Explorer perspective. If deleted NEs do not belong to any other model, they will become unmanaged once deleted. If so, they can be re-managed using the [Unmanaged Elements](#) view.

If you check the **Remove from all models** checkbox, the NEs will be removed from both the Logical model and Geographical model (**Tree** and **Map** views). In that case, you can re-manage them using the [Unmanaged Elements](#) view.

Delete Network Element from Model dialog

This dialog appears whenever selecting the **Delete** context menu in the tree with an NE in focus.

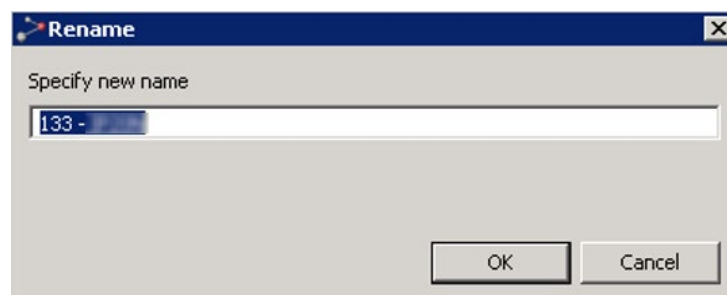


Press **Yes** to confirm that you wish to delete the resource. NEs deleted in this way will be removed from the model (either Geographical or Logical) linked to the Network Explorer perspective.

If you check the **Remove from all models** checkbox, the NE will also be removed from both the Logical model and Geographical model (**Tree** and **Map** views). In that case, you can re-manage it using the [Unmanaged Elements](#) view.

Rename dialog

This dialog appears whenever selecting the **Rename** context menu in the tree with an NE or subdomain in focus. ptp 820 device names are synchronized between PTP 820 NMS and the devices. That is, renaming a device on PTP 820 NMS sets the device name on the device itself; and changing the device name on the device itself changes the device name on PTP 820 NMS.



Enter a new name and press **OK** to perform the rename or press **Cancel** to abort.

Note:For PTP 820 devices, the device name can be up to 63 characters long.

Mute Notifications dialog

This dialog appears whenever selecting the **Mute Notifications** context menu in the tree with an NE or domain in focus.

Mute Notifications

Confirm managed element muting

No alarm notifications will be triggered by alarms from the selected element(s).
You may optionally specify a time when these elements shall be automatically unmuted.

☒ Notification Mute Expiration

Date:

November, 2015							December, 2015							January, 2016						
Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat
25	26	27	28	29	30	31			1	2	3	4	5							
1	2	3	4	5	6	7	6	7	8	9	10	11	12	3	4	5	6	7	8	9
8	9	10	11	12	13	14	13	14	15	16	17	18	19	10	11	12	13	14	15	16
15	16	17	18	19	20	21	20	21	22	23	24	25	26	17	18	19	20	21	22	23
22	23	24	25	26	27	28	27	28	29	30	31		24	25	26	27	28	29	30	
29	30												31	1	2	3	4	5	6	

Time: 5:36:00 AM

OK Cancel

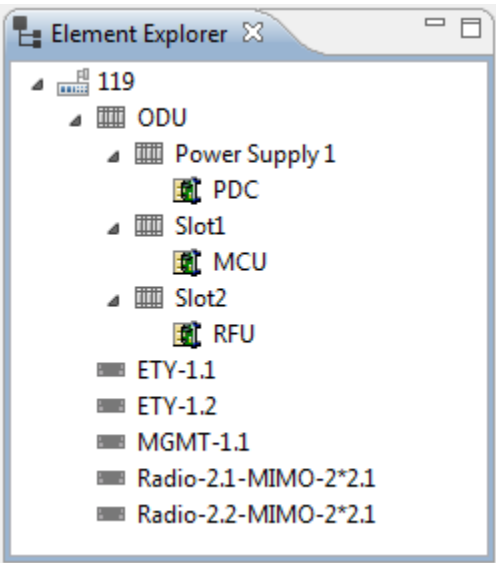
This dialog requests confirmation to mute all selected elements, as well as any element beneath any selected administrative domain. Alarm notifications will not be sent for muted elements. In the tree and map views, muted elements can be identified by a [Mute indicator](#) on NE level. In the [Managed Elements view](#), [Active Alarms view](#) and [Historical Alarms view](#), you can identify muted elements by including and sorting by the **Muted** column.

When muting elements, you have the option to enable automatic unmuting. If **Notification Mute Expiration** is not enabled, the selected elements will stay muted until they are manually unmuted. If you enable **Notification Mute Expiration**, you must specify the **Date** and **Time** for the elements to be unmuted.

Press **OK** to enable muting or press **Cancel** to abort.

Element Explorer view

This view can be found in the [Network Explorer](#) perspective. It can also be opened from **Views > Topology > Element Explorer** in the main menu or from the context menu of an NE selected in the Network Explorer Tree or Network Explorer Map view.



The view is always scoped to one NE, representing a snapshot of its hardware configuration at the moment the view was opened: racks, ports, slots, ODUs, etc.

Available operations from the context menu of an element in the tree

- Fault – Opens the following Fault views and functions:
 - Active Alarms – Opens an Active Alarms view for the selected element.
 - Historical Alarms – Opens a Historical Alarms view for the selected element.
- Select All– Selects all elements in the tree.
- Properties – Displays the properties of the selected element, in a Properties view.

Relation Overview view

This view can be found in the [Network Explorer](#) perspective. The view can also be opened from **Views > Topology > Relation Overview** in the main menu or from the context menu of a relation selected in the Network Explorer Map view. The view is always scoped to one relation, representing its status at the moment the view was opened.

Relation Overview										
Link Name	AEnd Name	AEnd IP	AEnd Slot/Port	AEnd Group	AEnd...	ZEnd Name	ZEnd IP	ZEnd Slot/P...	ZEnd Group	ZEnd Radio Link ID
S3 - 113 - IP20N1...	S3 - 113 - IP20N	10.10.66.113	Radio-4.1	MC-ABC.1	1	S3 - 112 - IP20N...	10.10.66.112	Radio-4.1	MC-ABC.1	1
S3 - 113 - IP20N1...	S3 - 113 - IP20N	10.10.66.113	Radio-3.1	MC-ABC.1	1	S3 - 112 - IP20N...	10.10.66.112	Radio-3.1	MC-ABC.1	1



The **Relation Overview** view displays additional details about a selected relation between elements in the [Network Explorer Map](#). If the relation encompasses multiple links (for example, you select a relation between two domains), each link is described in a separate row in the table.

Relation Overview table

The following table presents the link information provided in this view.

Name	Explanation
Link Name	The name of the link.
AEnd Name	The name of the device at the A-End of the link.
AEnd IP	The IP address of the device at the A-End of the link.
AEnd Slot.Port	The slot and port at the A-End of the link. The information also indicates the type of topological link that connects between devices: Radio – Radio link ETY – Ethernet link Cascading – Cascading link
AEnd Group	Displays the group name if the port at the A-End is a member of a group (relevant for IP20 device family).
AEnd Radio Link ID	Displays the radio link ID, if the link is a radio link.
ZEnd Name	The name of the device at the Z-End of the link.
ZEnd IP	The IP address of the device at the Z-End of the link.
ZEnd Slot.Port	The slot and port at the Z-End of the link. The information also indicates the type of topological link that connects between devices: Radio – Radio link ETY – Ethernet link Cascading – Cascading link
ZEnd Group	Displays the group name if the port at the Z-End is a member of a group (relevant for IP20 device family).
ZEnd Radio Link ID	Displays the radio link ID, if the link is a radio link.

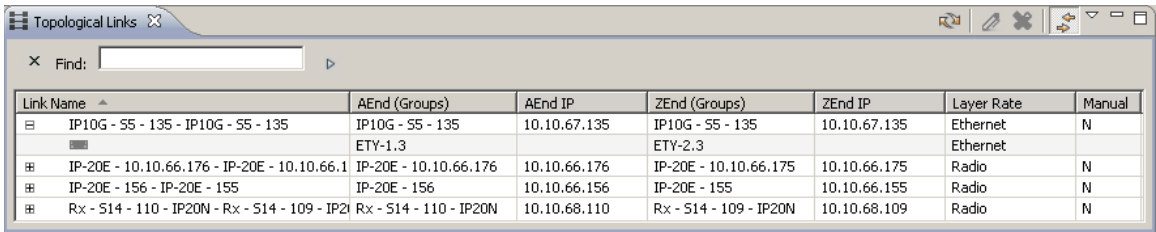
Available operations

-  Edit topological link - Enables editing the Link Name and Description in the [Error! Reference source not found.](#) dialog that appears.
-  Rename - Enables renaming the link.

Topological Links view

This view is opened from **Views > Topology > Topological Links** in the main menu. This view can be opened scoped to an element by:

- Selecting an element in the Geographical Tree view or Geographical Map view, and then selecting **Topological Links** from the Context menu.
- Selecting an element in the Ethernet Topology view or Ethernet Flow Domains view and then selecting **Topological Links** from the Context or Dropdown menu.
- Selecting an element in the TDM Topology view or TDM Domains view and then selecting **Topological Links** from the Context or Dropdown menu.



Link Name	AEnd (Groups)	AEnd IP	ZEnd (Groups)	ZEnd IP	Layer Rate	Manual
IP10G - S5 - 135 - IP10G - S5 - 135	IP10G - S5 - 135	10.10.67.135	IP10G - S5 - 135	10.10.67.135	Ethernet	N
	ETY-1.3		ETY-2.3		Ethernet	
IP-20E - 10.10.66.176 - IP-20E - 10.10.66.176	IP-20E - 10.10.66.176	10.10.66.176	IP-20E - 10.10.66.175	10.10.66.175	Radio	N
IP-20E - 156 - IP-20E - 155	IP-20E - 156	10.10.66.156	IP-20E - 155	10.10.66.155	Radio	N
Rx - S14 - 110 - IP20N - Rx - S14 - 109 - IP20N	Rx - S14 - 110 - IP20N	10.10.68.110	Rx - S14 - 109 - IP20N	10.10.68.109	Radio	N

This view shows the topological links (Radio, Ethernet or Cascading) that connect between devices. The devices and respective ports at each end of the links (the A-End and the Z-End) are described.



Topological Links table

The following table presents the link information available in this view.

Name	Explanation
Link Name	The name of the link.
AEnd (Groups)	The Device Name and the port at the A-End of the link. If the port at the A-End is a member of a group this is shown in brackets. Note that if you export the table to a file by selecting Export To File , the export report includes an additional column listing the AEnd port name.
AEnd IP	The IP of the device at the A-End of the link.

ZEnd (Groups)	The Device Name and the port at the Z-End of the link. If the port at the Z-End is a member of a group this is shown in brackets. Note that if you export the table to a file by selecting Export To File , the export report includes an additional column listing the ZEnd port name.
ZEnd IP	The IP of the device at the Z-End of the link
Layer Rate	The type of physical connection over the link.
Manual	Indicates whether the link information was manually configured in PTP 820 NMS ('Y') or whether PTP 820 NMS discovered the link itself by reading information from the element ('N').

Available operations

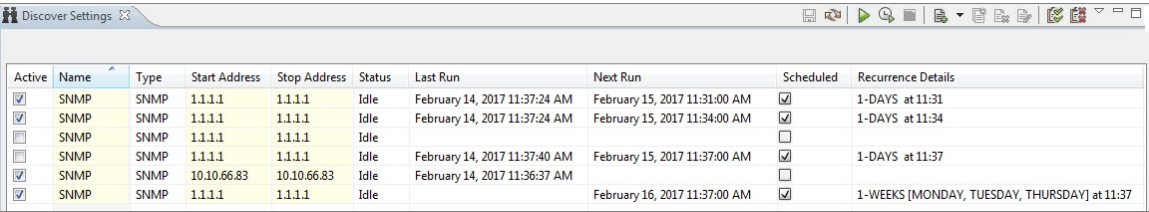
-  Edit topological link - Enables editing the Link Name and Description in the [Error! Reference source not found.](#) dialog that appears.
-  Export to file – Enables exporting the table to a file.

Discover

Discover Settings view

This view can be found in the [Discover](#) perspective and is normally used together with the [Unmanaged Elements](#) view.

Figure 122 Discover settings view



Active	Name	Type	Start Address	Stop Address	Status	Last Run	Next Run	Scheduled	Recurrence Details
<input checked="" type="checkbox"/>	SNMP	SNMP	1.1.1.1	1.1.1.1	Idle	February 14, 2017 11:37:24 AM	February 15, 2017 11:31:00 AM	<input checked="" type="checkbox"/>	1-DAYS at 11:31
<input checked="" type="checkbox"/>	SNMP	SNMP	1.1.1.1	1.1.1.1	Idle	February 14, 2017 11:37:24 AM	February 15, 2017 11:34:00 AM	<input checked="" type="checkbox"/>	1-DAYS at 11:34
<input type="checkbox"/>	SNMP	SNMP	1.1.1.1	1.1.1.1	Idle			<input type="checkbox"/>	
<input type="checkbox"/>	SNMP	SNMP	1.1.1.1	1.1.1.1	Idle	February 14, 2017 11:37:40 AM	February 15, 2017 11:37:00 AM	<input checked="" type="checkbox"/>	1-DAYS at 11:37
<input checked="" type="checkbox"/>	SNMP	SNMP	10.10.66.83	10.10.66.83	Idle	February 14, 2017 11:36:37 AM		<input type="checkbox"/>	
<input checked="" type="checkbox"/>	SNMP	SNMP	1.1.1.1	1.1.1.1	Idle		February 16, 2017 11:37:00 AM	<input checked="" type="checkbox"/>	1-WEEKS [MONDAY, TUESDAY, THURSDAY] at 11:37

In this view you can define settings for discovering new network elements to manage and to control the discover process. The newly discovered elements will be displayed in the [Unmanaged Elements](#) view.

Discover Settings table

This view shows a table of search ranges for discovering new NEs. Here, search ranges can be set up for discovering SNMP-based NEs (over UDP/IP). When a Search-row is selected in the table, the item can be edited, deleted, cloned, or renamed.

Each discover range is identified by the following fields:

Table 38 Discover settings table

Name	Explanation
Active	A "checked" checkbox indicates that the search range is enabled for the discover process. Click a checkbox to select/de-select a search
Name	A user-defined name for the search range
Type	The type of discover, possible values: SNMP
Start Address	The first IP address in the range the server will sequentially go through to search for manageable NEs. Only for discover type SNMP
Stop address	The last IP address in the range the server will sequentially go through to search for manageable NEs. Only for discover type SNMP

Name	Explanation
Status	<p>Current status for the search. Possible values:</p> <p>Idle - (No discover is running)</p> <p>Pending - (client is awaiting status from server)</p> <p>Running - (discover has started)</p> <p>Processed N of M addresses in XX seconds - (current status of the ongoing discover)</p> <p>Cancelled - (the discover process has been aborted)</p> <p>A Normal discover operation should result in the following state transition: Idle -> Pending -> Running -> Processed N of M address in XX seconds -> Idle</p>
Last Run	The time when the search range was last run
Timeout	<p>For SNMP range, the number of seconds a request for a given address in a range the server shall wait.</p> <p>The Timeout column is by default not visible. In order to view it, select the Customize Columns button and change the columns settings.</p>

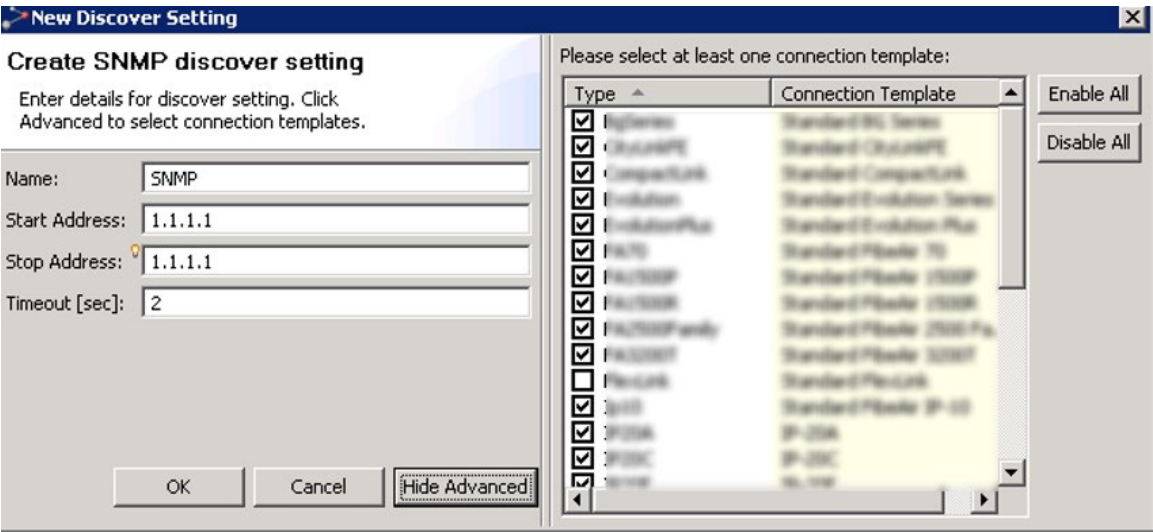
SNMP search

This search method can be used to discover all equipment communicating with the SNMP protocol within a range of IP-addresses, with the server communicating directly with each NE.

Settings for an SNMP Range search

Select a search range of type SNMP from the drop-down menu of the Create a New Discover Search in the toolbar to display this type of settings.

Figure 123 Setting for an SNMP range search



Fields for an SNMP Range search

Table 39 Fields for an SNMP range search

Name	Explanation
Name	A user-defined name for the search range
Start address	The first IP address in the range the server will sequentially go through to search for manageable NEs
Stop address	The last IP address in the range the server will sequentially go through to search for manageable NEs
Timeout	The number of seconds a request for a given address in a range the server shall wait
Connection templates	<p>A connection template contains the protocol specific attributes used during discover. There are several Connection types available; one for each NE family. If you just want to discover a certain NE type, unselect all other types listed. At least one connection template must be selected for a range to be valid. Please note that by default all Connection types will be included in a search.</p> <p>Connection templates can be updated and created in the Connection Templates view.</p>

The discover range should be defined with care and according to the nature of your local network.

Tip! For the Stop address, it is possible to make it equal to the Start address by pressing CTRL+Space on your keyboard and selecting the address in the displayed drop down.













Stop Address: 1.1.1.1




Timeout [sec]: 10.8.1.20

The maximum number of addresses allowed in an SNMP search is 5000.

Available operations

The following operations are available in the view:

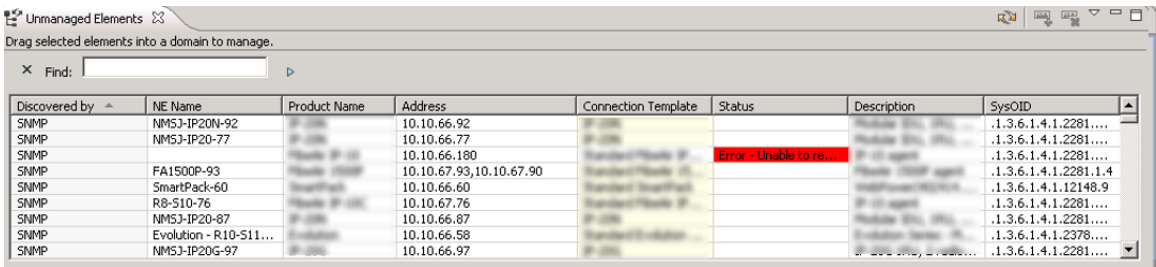
-  **Save modifications** Save the updates you have made in the Discover Settings table. If a search contains invalid settings, an explanation about the wrong settings will be displayed in the top of the Settings area, and Save Modifications will be disabled until these settings are fixed. If you try to close the view without saving data, the [Save Changes](#) dialog will appear
-  **Refresh settings** Refresh the view with the latest data from the discover setting on the server.
-  **Start Discover** Start searching for new NEs. The NE found in the discover process can be seen in the [Unmanaged Elements](#) view. All modifications in the Discover Settings table must be [saved](#) before Start discover can be used.
-  **Stop Discover** Abort the currently running discover process.
- **Create a New Search.**
-  **Clone** Clone the currently selected Search node in the Discover Settings table.
-  **Delete** Delete the currently selected Search node in the Discover Settings table.
-  **Edit...** Edit a selected row to change its parameters.
-  **Enable All Ranges** Enable All Ranges in the Discover Settings table.
-  **Disable All Ranges** Disable All Ranges in the Discover Settings table.
- ☒ **Click a checkbox in the Discover Settings table to enable/disable a search range**
-  **Export to File...** Open the Export to File dialog for the Discover Settings table, where you can select to export the content of the table to disk. Supported file format is CSV (Comma delimited).

-  **Import from File...** Open the Import from File dialog for the Discover Settings table, where you can select to import the content of a specified file into the table. Supported file format is CSV (Comma delimited).
-  **Customize Columns** Open the [Customize Columns dialog](#) for the Discover Settings view. In this dialog you can select which columns will be displayed in the table, and the order in which they appear.
-  **Unmanaged Elements** Open the Unmanaged Elements view
- In-cell edit is possible by either double-clicking a cell marked writeable or by pressing the F2 key. Navigating to the next writeable cell is possible using the Tab key, navigating back by using Shift+Tab.

Unmanaged Elements view

This view can be found in the Discover perspective, and is normally used together with the Discover Settings view.

Figure 124 Unmanaged elements view



In this view, you can "manage" the NEs you have discovered. "Manage an NE" means in this case placing the NE into a domain so that you can, for example, receive alarm status and performance data and update properties for the NE.

Unmanaged Elements table

This view shows a table with Network Elements that are discovered but not yet managed. Each NE is identified by the following fields:

Table 40 Unmanaaged elements table

Name	Explanation
Discovered by	The protocol used in the Discover Settings view when discovering this NE
NE Name	The name of the NE you have discovered
Product Name	The type of NE
Address	The IP address for the management port of the NE.
Connection Template	<p>The currently assigned connection template in PTP 820 NMS for managing this NE. The templates are defined in the Connection Template view, where you also can define which templates are to be used as default templates during the discover process.</p> <p>New templates can be assigned to each NE in the Connection template column</p>
Description	A textual description of the element as read from sysDescr variable defined in MIB2.

Name	Explanation
SysOID	The system object identifier as read during discovering of the element from sysObjectId variable defined in MIB2.
First Discovered	The time when the NE was first discovered This column is by default not visible. In order to view it, select the Customize Columns button and change the columns settings
Last Discovered	The time when the NE was last discovered. This column is by default not visible. In order to view it, select the Customize Columns button and change the columns settings









This table is used for selecting which NEs to manage. Use shift+click or ctrl+click to select more than one NE.


When selecting one or more lines of NEs in the table, these can be set to be managed directly in a domain by dragging them into this domain in any of the topology views (**Geographical** or **Logical Map** or **Tree**). The selected NEs can also be managed using [Manage Elements](#).

Elements which are successfully set to be managed will then be removed from the **Unmanaged Elements** table.

Available operations

The following operations are available in the table:

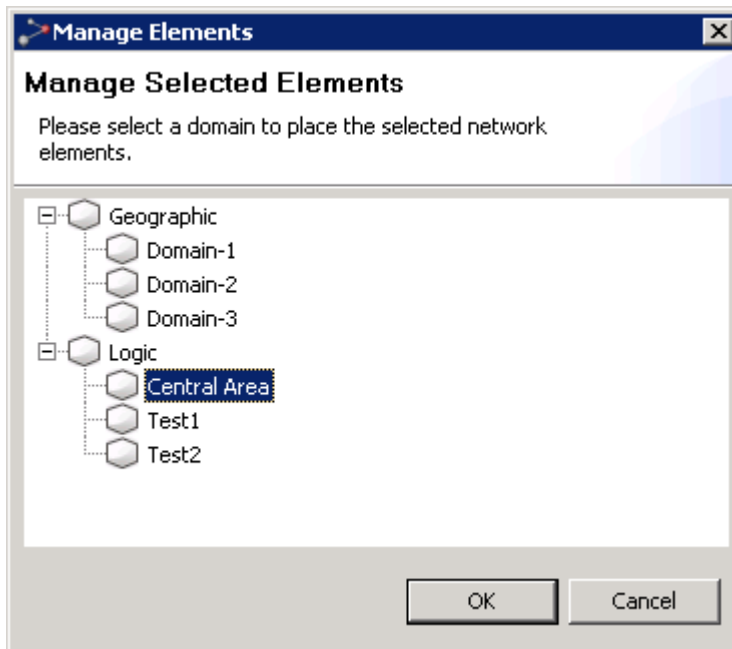
-  **Manage Element(s)** Open the [Manage Elements](#) dialog using the currently selected elements in the table as input.
-  **Delete Discovered Element(s)** Open the [Confirm Discovered Element Delete](#) dialog using the currently selected elements in the table as input.
-  **Refresh View** Refresh the list and display the new NEs that have been discovered since you last used Discover in the Discover Settings view.
-  **Open SNMP Interface** Open the [Open SNMP Interface view](#).  Drag one or more NE into a domain in one of the topology views (**Geographical** or **Logical Map** or **Tree**) to manage it.
-  Select a connection template from the dropdown menus in the **Connection Template** column to change the read/write community (SNMP) for managing the NE. Connection templates are defined in the [Connection Templates](#) view.
-  **Customize Columns** Open the [Customize Columns](#) dialog for the Unmanaged Elements view. In this dialog you can select which columns will be displayed in the table, and the order in which they appear.
-  **Show Quick Search** Enable the [Quick Search](#) field in the Unmanaged Elements view. The quick search functionality makes it possible to search the contents of the view. All visible columns can be searched.

-  **Export to File...** Export the current data to file. The table can be saved as an Excel spreadsheet (.xls), comma separated file (.csv) or extended markup language (.xml)

Manage Elements dialogue

This dialog is opened from the **Unmanaged Elements** table when using [Manage Elements](#) with an unmanaged element selected.

Figure 125 Manaaged elements dialogue



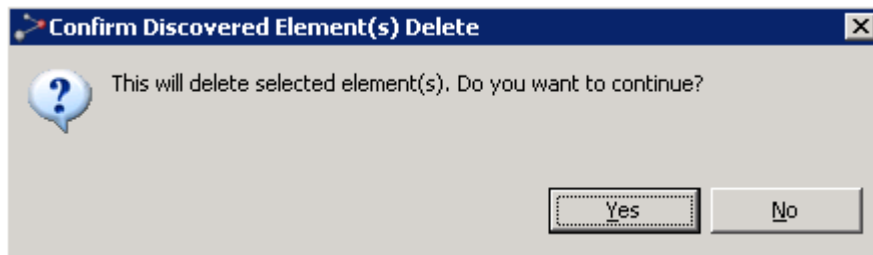
In this dialog you can select an administrative domain for all of the selected NEs. After pressing the **OK** button the NEs are added to the domain, and the elements will disappear from the table in the **Unmanaged Elements** view.

If no legal domain is selected, the OK button will be disabled.

Confirm Discovered Element Delete dialog

This dialog is opened when using **Delete** in the **Unmanaged Elements** table.

Figure 126 Confirm discovered element delete dialog



Pressing the Yes button will remove the currently selected element from the table of unmanaged elements. If the element is discovered again, it will re-appear in this table.

Services - Ethernet and TDM

Service Management

Service Management

PTP 820 NMS provides end-to-end provisions services for:

- Ethernet services (VLANs)
- 2 Mb TDM trails (E1/T1, VC12/VT15).

Provisioning and service inventory for services is managed through two service perspectives: The Ethernet Service Perspective and the TDM Service Perspective.

The perspectives are kept as similar as possible, even though they operate on different technologies.

Service List

The TDM Services view or Ethernet Services view is opened by selecting **Views > TDM > TDM Services**, or **Views > Ethernet > Ethernet Services**. The services list is initially empty. You can search for configured services by resource name, and by the minimum alarm severity existing on the service (where ALL in the alarm severity filter denotes all services, including unconfirmed services). Note that this view is a snapshot, and is not updated automatically..

To view further information about a specific service, you can right-click the service and select **Open Service Viewer**. This provides a view scoped to the domain in which the service is configured.

You can also view a scoped list of services configured on a domain by right-clicking an Ethernet or TDM domain in the navigator tree or map, and selecting **Ethernet Services** or **TDM Services**.

The scoped service list has three main columns: The service name or resource name, the administrative state and the operational state, in addition to some other minor columns. The service name is the name assigned to a particular service by the user, the administrative state is the desired state, and the operational state is the actual state of the service as seen on the elements.

Administrative State

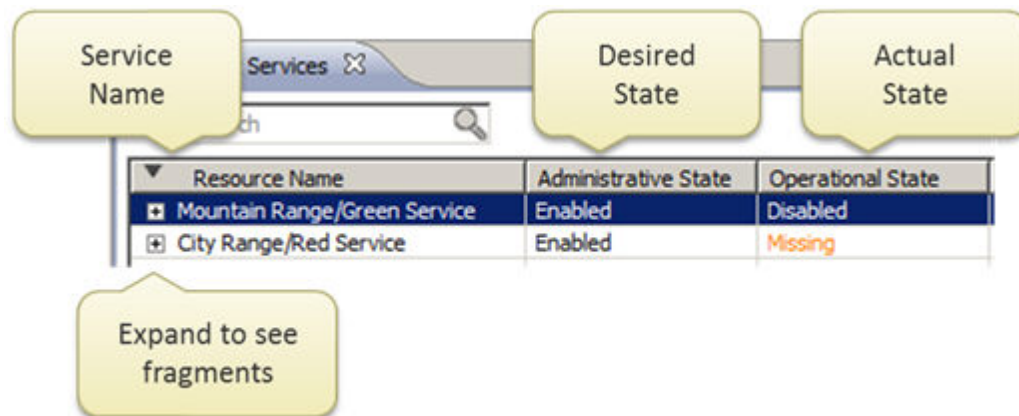
- **Enabled:** Service is created in NMS and the process of writing it to the element is initiated or completed. When completed on the element, the Operational State of the service on the element should also be Enabled.
- **Disabled:** Service is created in NMS and the process of writing it to the element is initiated or completed. When completed on the element, the Operational State of the service on the element should also be Disabled.
- **Unconfirmed:** Service is discovered on element, but not managed by NMS, its Operational State is always Unknown and no alarms are shown. The NMS operator may choose to leave it as Unconfirmed, accept it as managed, or delete it (which would trigger deletion on both element and NMS).

- **Deleting:** A command has been given to delete the end to end service but the command has not yet completed or has failed.
- **Pending:** Service or service fragment has a task in the NMS scheduler for configuring/reconciling/deleting a service on element(s).

Operational State

- **Enabled:** Service or service fragment is configured on the element(s) and available for traffic.
- **Disabled:** Service or service fragment is configured on the element(s) but not available for traffic.
- **Pending:** Service or service fragment has a task in the NMS scheduler for configuring/reconciling/deleting a service on element(s).
- **Misconfigured:** Service has one or more fragments with Administrative State Unconfirmed or Operational State Missing or Operational State Misconfigured. Additionally, service fragments can be misconfigured if an element specific configuration is invalid.
- **Missing:** Reported on a service fragment or entire service if it exists only in the NMS but is missing on the physical element(s)
- **Broken:** Reported on end to end service if service path detection finds that there is no connectivity between one or more endpoints or that an endpoint configuration is illegal.
- **Unknown:** The administrative state is Unconfirmed, or the state of the service on the element cannot be determined.
- **Down:** The operational state on the device is Down; the traffic cable may be disconnected.

The administrative and operational states are important as they describe the service workflow. Generally, services are created from the NMS, but since the current service status is also read back from the element, and new services can also be discovered from the network, the service states are used to model the different conditions.

Figure 127 Service list

Further, the service lists are organized as tree-views, in order that a service can be expanded to show how a service is built up from fragments down to the element level.

Last, but not least, more information about a particular service is available when it is selected in the service list. The service endpoints and also all the intermediate points that a service flows through between endpoints, are available in sub-views connected to the service list. There is also a connection from the service lists to two-dimensional graph views that visualizes the service through elements, ports and links in the network.

Service Actions

A set of actions are available on services from the service lists

- Create initiates a wizard to create new services, selecting endpoints and specifying all attributes
- Confirm allows any service discovered on the managed elements, probably created externally, to be managed as if created by the NMS.
- Edit allows changing any attribute of a service
- Rename allows changing the name and description of the end-to-end service
- Reapply allows rewriting of service configuration to one or more elements
- Reconcile for refreshing configuration from elements in order to recalculate operational state
- Delete allows deleting a service from the elements, from just the NMS or both.

These actions are general, and work for both Ethernet and TDM service views.

A note on Service Naming

Some element types do not allow storing the service name on the elements themselves, or may have restrictions with respect to length or allowed characters. For this reason, there is an extra column in the Service Lists, the NativeEmsName column that can be enabled by the user. This column reports the service name as seen on the physical element and may differ from the service name used in the NMS.

Ethernet Services

Ethernet Services overview

Ethernet services, the provisioning of end-to-end VLANs are managed by a set of views defined in the Ethernet Perspective:

- The Flow Domain Navigator view
- The Ethernet topology view
- The Ethernet services view

Additionally, central to the creating/editing of Ethernet services are:

- The Create Ethernet Service wizard
- The Edit Ethernet Service wizard

Ethernet flow domain navigator view

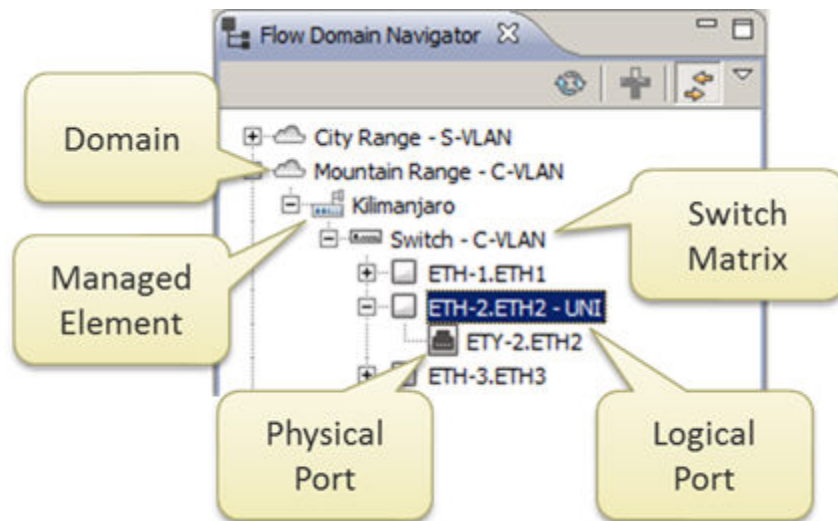
Before services can be created or discovered, the connectivity of the Ethernet network must be defined by Ethernet flow domains. Ethernet flow domains are created using the Create Flow Domain wizard. Because the divisioning into flow domains is semi-automatic, the user needs only to select a name for the flow-domain and a starting-point for the discovery. The starting point can be a port, or a switch. After a flow domain has been created, Ethernet services can be created or discovered between any port within the particular domain, but not between ports in different flow domains., unless nested under a common parent domain.

Presently, the allowed flow domain types are:

- SVLAN
- CVLAN

Management of flow domains is done from the flow domain navigator tree view. Elements or parts of elements that do not belong under any flow domain yet, can be found under the “Unattached” node. There are five level types in the flow domain hierarchy in the flow domain navigator:

1. **The flow domain level.** This level describes a hierarchy of flow domains. In future releases, the flow domains may themselves be nested.
2. **The managed element level.** This level lists the elements participating in this flow domain. Note that an element may participate in several flow domains.
3. **The switch matrix level** (Matrix Flow Domains). An element may consist of several switches, physical or logical. A switch is in itself a special case of a flow domain, but can in the NMS only be managed as part of a user-created flow domain.
4. **The logical Ethernet port level** (Flow Point Pools), which is probably the most significant level in the hierarchy. A logical port is in most cases 1:1 with physical ports, but in case of LAG or many radio channels, it serves as the single logical point through which a service is configured.
5. **The physical Ethernet port level** (Physical Termination Points). This level is just for additional information, showing what physical ports support the logical port.

Figure 128 Ethernet flow domain navigator

For flow domains, the flow domain navigator can be used to launch scoped services lists, and also launch the service creation wizard directly, by selecting two logical Ethernet ports and initiating the wizard from the context menu.

Finally, flow domains will automatically grow when new links are added to new elements, or split when links are deleted. However, if two islands, both containing more than two elements are connected, merging must be initiated manually by invoking the merge action.

Searching in the navigator tree

You can search for elements in the tree. Enter a string in the **Search** field, and then use the **Next** (or **Previous**) button to go to the next (or previous) element whose name includes the search string.


















Available operations








- Refresh - Refreshes the display.
- Link View - When activated, selecting a device in the tree selects the corresponding device in the Ethernet Topology map.
- Create Flow Domain - Opens the Create Flow Domain wizard, which guides you through the steps of creating a Flow Domain, beginning with the selected device and including devices that have connectivity with that device.

Operations available from the context menu of an element in the tree










Fault - Opens the following Fault views and functions:

- Active Alarms - Opens an Active Alarms view for the selected element.
- Historical Alarms - Opens a Historical Alarms view for the selected element.

-  Alarm Templates Assignment – Opens an Alarm Templates Assignment view for the selected element.
-  Mute Notifications – Mutes an NE or a domain, to prevent alarms on the selected NE(s) from generating [alarm notifications](#). The [Mute Notifications dialog](#) will open, where you can select a time for automatic unmuting of notifications. When notifications are muted, NEs will have a [mute indicator](#) on NE level in the Map and Tree views.
-  Unmute Notifications – Unmutes a muted NE or a domain with muted element, to re-enable alarms on the selected NE(s) to generate [alarm notifications](#)
- Configuration – Opens the following Configuration views and functions:
 -  Hardware Inventory – Opens a Hardware Inventory view for the selected element.
 -  Software Inventory – Opens a Software Inventory view for the selected element.
 -  Transmission Inventory – Opens a Transmission Inventory view for the selected element.
-  Create Software Download Job – Opens the Create Software Download Jobs wizard, enabling you to create a software download job for the selected element.
-  Configuration File Management – Opens a Configuration File Management view for the selected element.
-  Connection Template Assignment – Opens a Connection Template Assignment view for the selected element.
- Open SNMP Interface – Opens an “Open SNMP” Connection Template which can be used to manage the device. Basic SNMP management of the device will be triggered to read the inventory and faults from the device.
- External Tools – Enables opening a web EMS session with the selected device.
- Performance – Opens the following Performance views and functions:
 -  Current Performance - Opens a Current Performance view for the selected element.
 -  Historical Performance – Opens a Historical Performance view for the selected element.
-  Performance Collection Control – Opens a Performance Collection Control view for the selected element.
- Reports – Opens the following Report views and functions:
 -  Network Element Types Overview Report – Opens a Network Element Types Overview Report view for the selected element.
 -  Inventory Report – Opens an Inventory Report view for the selected element.
 -  Ethernet Services – Opens the Ethernet Services view. Relevant for an element that belongs in a flow domain.
-  Create Flow Domain – Opens the Create Flow Domain wizard, which guides you through the steps of creating a Flow Domain, beginning with the selected device and including devices that have connectivity with that device. Relevant for an unattached element (an element that does not belong to any flow domain).
-  Web EMS – Opens a web EMS session with the selected device

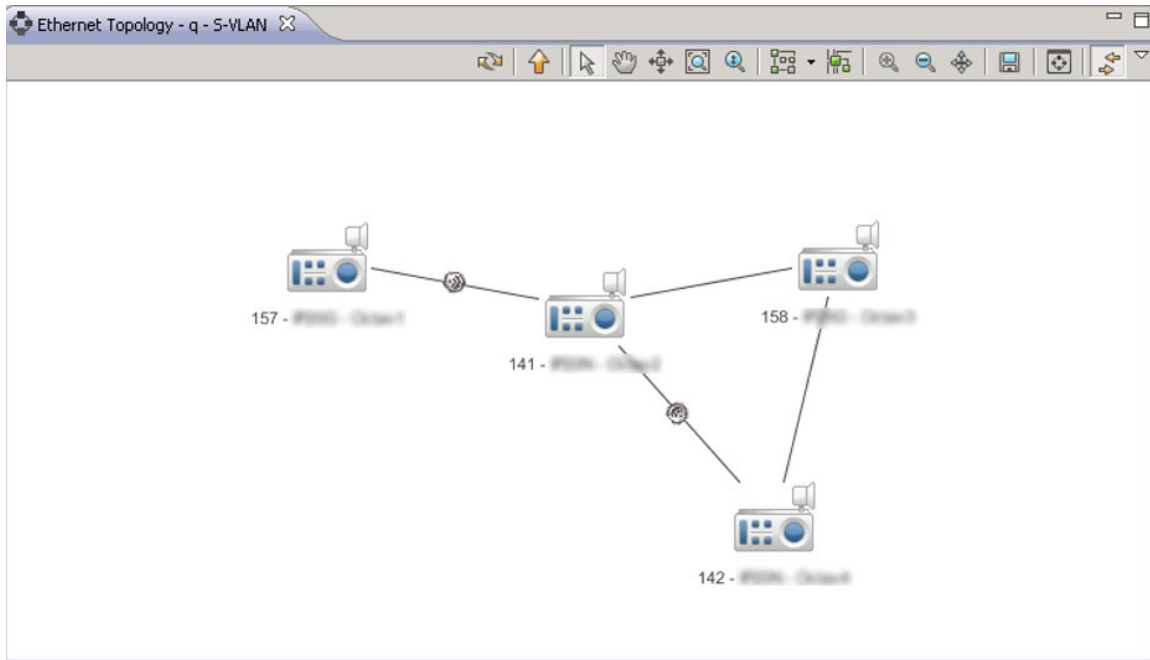
-  Show in Geographic Map – Opens a Geographical Map view of the domain.
-  NE Outline – Opens the NE Outline view, displaying the equipment and port model for the selected device.
-  Topological Links – Opens a Topological Links view for the selected element
-  Reconcile – Instructs PTP 820 NMS to contact the network element, and update the PTP 820 NMS database with information about the element.
-  Rename – Enables renaming the managed element.
-  Delete – Enables deleting the managed element.
- Select All – Selects all elements in the Flow Domain Navigator tree.
-  Properties – Displays the element's properties in a Properties view.

Operations available from the context menu of a defined flow domain

-  Create Ethernet Service – Opens the Create Ethernet Service wizard.
-  Ethernet Services – Opens an Ethernet Services view, showing the services defined in the selected flow domain.
-  Ethernet Topology – Opens an Ethernet Topology view, displaying the topology of the selected flow domain.
-  Merge – Takes two selected domains and merges them into one if there is connectivity between those domains.
-  Rename – Enables renaming the selected flow domain.
-  Perform Connectivity Mapping – Reviews the services in the domain and suggests connecting separate fragments into a single service based on VLAN Connectivity.
-  Update – Checks and updates, if necessary, the classification (UNI or NNI) of the network ports of all the devices in the flow domain. As a result, links may be removed from the flow domain if they are no longer NNI, and the flow domain may be split if there is no longer connectivity between devices.
-  Delete – Deletes the selected flow domain.
- Select All – Selects all elements in the Flow Domain Navigator tree.
-  Properties – Displays the domain's properties in a Properties View.







Ethernet topology view















The Ethernet topology view gives an overview of the connectivity in the Ethernet network. Managed Elements and Ethernet links between logical ports are visualized as well as flow domains. Like the Ethernet flow domain navigator, also the Ethernet topology view can be used for scoping the service list and service creation wizard.

Figure 129 Ethernet topology view










The domains in the graph can be “opened” or “closed” by double-clicking on the domain icons. To navigate down into a domain, double click inside an “opened” domain. To navigate back up, press the “up” button on the toolbar. It is also possible to eliminate the flow domains completely from this view by selecting the “Flat View” option from the view drop down menu.


















Available Operations

-  Refresh – Refreshes the view.
-  Move Up – Moves up one level, to the Parent Domain. The parent domain contains the current domain as a “child”, and when going up one level the shape/outline of the previous domain and its “siblings” is displayed (this operation is the opposite of [Doubleclick a Domain](#)).
-  Select Tool – Enables selecting each domain and NE in the view. Hold down the shift key while selecting, to allow selection of multiple objects. When the Select tool is enabled, you can:
 - Drag an object (domain or NE)
 - Open context menus for the currently selected object (domain or NE)
 - Double-click a Domain to go down to this level in the Logical Map view (this operation is the opposite of [Go to Parent Domain](#))
-  Pan Tool – Pans the screen by dragging it in the direction you want.
-  Link Navigation Tool – When clicking a link, alternates between focusing on one end point and focusing on the other end point.
-  Zoom Tool – Zooms in on a specific area of the view by clicking and dragging a rectangle over the area you wish to see in more detail. When the mouse button is released, the view displays only this selected area.

-  Interactive Zoom Tool – Zooms in and out of the entire map by rolling the mouse wheel forwards or backwards.
-  Orthogonal Layout – Displays the topology in an orthogonal layout
-  Hierarchical Layout – Displays the topology in a hierarchical layout.
-  Symmetric Layout – Displays the topology in a symmetrical layout.
-  Circular Layout – Displays the topology in a circular layout.
-  Link Routing – Displays links as curved lines.
-  Zoom In – Click to zoom in on a smaller area.
-  Zoom Out – Click to zoom out to a larger area
-  Best Fit – Centers the currently selected item in the middle of the view.
-  Export as Image – Enables saving the display as an image file.
-  Flat View – Enables eliminating the flow domains completely from this view
-  Show Managed Element Type – Displays each managed element's type, in addition to its displayed name
-  Topology Overview – Moves the focus to the Topology Overview view
-  Link View – When activated, selecting a device in the map selects the corresponding device in the Flow Domain Navigator tree.

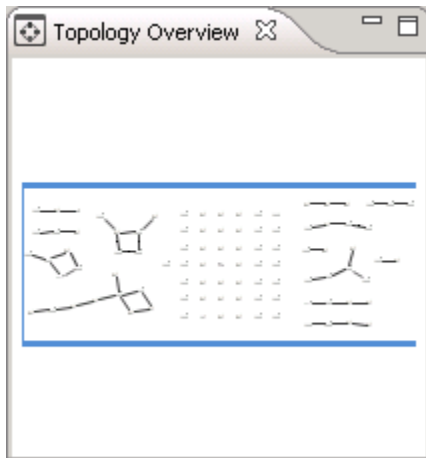
Operations available from the context menu of an element

- Fault – Opens the following Fault views and functions:
 -  Active Alarms – Opens an Active Alarms view for the selected element.
 -  Historical Alarms – Opens a Historical Alarms view for the selected element.
 -  Alarm Templates Assignment – Opens an Alarm Templates Assignment view for the selected element.
-  Mute Notifications – Mutes an NE or a domain, to prevent alarms on the selected NE(s) from generating [alarm notifications](#). The [Mute Notifications dialog](#) will open, where you can select a time for automatic unmuting of notifications. When notifications are muted, NEs will have a [mute indicator](#) on NE level in the Map and Tree views.
-  Unmute Notifications – Unmutes a muted NE or a domain with muted element, to re-enable alarms on the selected NE(s) to generate [alarm notifications](#)
- Configuration – Opens the following Configuration views and functions:
 -  Hardware Inventory – Opens a Hardware Inventory view for the selected element.
 -  Software Inventory – Opens a Software Inventory view for the selected element.
 -  Transmission Inventory – Opens a Transmission Inventory view for the selected element.
-  Create Software Download Job – Opens the Create Software Download Jobs wizard, enabling you to create a software download job for the selected element.

-  Configuration File Management – Opens a Configuration File Management view for the selected element.
-  Connection Template Assignment – Opens a Connection Template Assignment view for the selected element.
- Open SNMP Interface – Opens an “Open SNMP” Connection Template which can be used to manage the device. Basic SNMP management of the device will be triggered to read the inventory and faults from the device.
- External Tools – Enables opening a web EMS session with the selected device.
- Performance – Opens the following Performance views and functions:
 -  Current Performance - Opens a Current Performance view for the selected element.
 -  Historical Performance – Opens a Historical Performance view for the selected element.
 -  Performance Collection Control – Opens a Performance Collection Control view for the selected element.
- Reports – Opens the following Report views and functions:
 -  Network Element Types Overview Report – Opens a Network Element Types Overview Report view for the selected element.
 -  Inventory Report – Opens an Inventory Report view for the selected element.
 -  Ethernet Services – Opens the Ethernet Services view. Relevant for an element that belongs in a flow domain.
 -  Create Flow Domain – Opens the Create Flow Domain wizard, which guides you through the steps of creating a Flow Domain, beginning with the selected device and including devices that have connectivity with that device. Relevant for an unattached element (an element that is not currently associated with any flow domain).
 -  Web EMS – Opens a web EMS session with the selected device.
 -  Show in Geographic Map – Opens a Geographical Map view of the domain.
 -  NE Outline – Opens the NE Outline view, displaying the equipment and port model for the selected device.
 -  Topological Links – Opens a Topological Links view for the selected element
 -  Reconcile – Instructs PTP 820 NMS to contact the network element, and update the PTP 820 NMS database with information about the element.
 -  Rename – Enables renaming the managed element.
 -  Delete – Enables deleting the managed element.
 -  Properties – Displays the element's properties in a Properties view.

Topology Overview view

This view displays the entire Topology map with a blue frame around the current viewable area in the Topology map.

Figure 130 Topology overview

You can use this view to do the following:

- Drag&draw the corners of the blue frame to zoom in/out the viewable area in the Topology map.
- Drag inside the blue frame to pan the viewable area in the Topology map.
- Click outside the blue frame to set a new centre for the viewable area in the Topology map.

This tool can be useful when the viewable area in the Topology map view is zoomed in to display only parts of the entire map.

Ethernet Services View

This view is opened by selecting **Views > Ethernet> Ethernet Services**. It displays a list of Ethernet services. The list is initially empty. You can search for configured services by resource name, and by the minimum alarm severity existing on the service.

To view further information about a specific service, you can right-click a service in the list and select **Open Service Viewer**. This provides a view scoped to the domain in which the service is configured.

You can also view a scoped list of services configured on a domain by right-clicking an Ethernet domain in the navigator tree or map, and selecting **Ethernet Services**.

Figure 131 Ethernet Services view










Resource Name	Description	Alarm Severity	Ethernet Service Type	Transport VLAN	Administrative State	Operational State
test/EthService1			E-LAN	107	Unconfirmed	Unknown
141 - [redacted]				107	Unconfirmed	Unknown
142 - [redacted]				107	Unconfirmed	Unknown
test/EthService2		MAJOR	E-Line	108	Disabled	Missing
141 - [redacted]				108	Enabled	Missing
142 - [redacted]				108	Disabled	Missing

In addition to the service list columns common to both the Ethernet and the TDM services, the Ethernet services list has the following additional Ethernet-specific columns:







- Ethernet Service Type
- Transport VLAN

Two views are connected to the Ethernet Services view: The Ethernet Service Ports view, the Ethernet Service Path view, and the Properties view. The content of these are populated accordingly when a row in the Ethernet Services list is selected.


Available Operations




-  Refresh – Refreshes the display.
-  Create Ethernet Service – Opens the Create Ethernet Service wizard.
-  Customize columns – Enables setting the visible columns and their order.
-  Edit – Enables editing the selected service.
-  Rename Service – Renames the selected service.
-  Delete Selection – Deletes the selected service(s).
-  Confirm – Confirms that PTP 820 NMS should manage the Service.
-  Reapply – Reapplies the service configuration saved in the PTP 820 NMS Database, to the device.
-  Synchronize – Refreshes the Service Information in the PTP 820 NMS database, by reading back the service information from a particular device.

Operations available from the context menu of a defined Ethernet service

- Fault > Active Alarms – Open an Active Alarms view for the selected service
-  Reapply – Appears only if service configuration needs to be reapplied. For example, if the Administrative state is disabled, or the Operational State is **Missing** or **Disabled**, or a misconfiguration has occurred due to configuration changes on the devices of the service.
-  Edit – Opens the Edit Ethernet Service wizard, similar to the [Create Ethernet Service Wizard](#).
-  Rename Service – Enables renaming the selected service
-  Synchronize – Refreshes the service information in the PTP 820 NMS database, by reading back the service information from a particular device.
-  Delete – Deletes the selected service.
- Select All – Select all defined services.
-  Properties – Opens the Properties view for the service.

Operations available from the context menu of a defined Ethernet service fragment

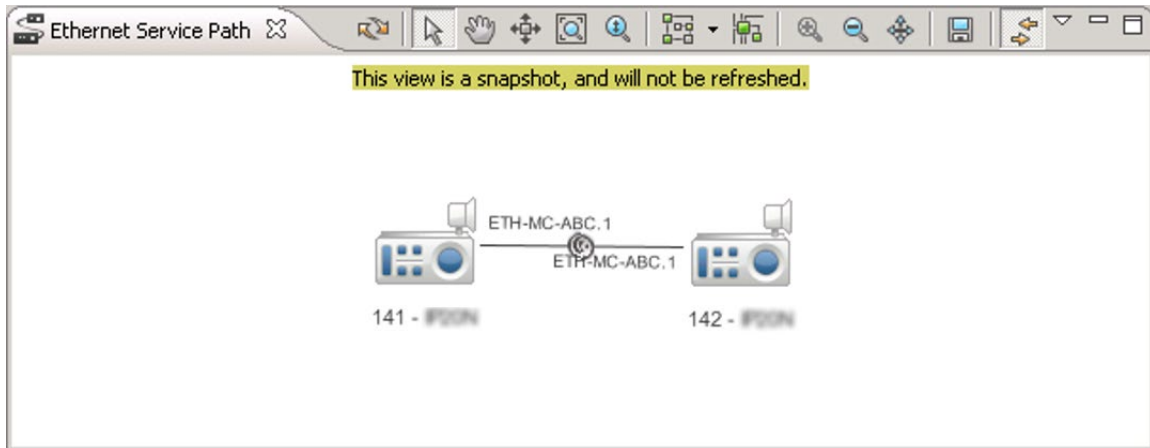
- Fault > Active Alarms – Open an Active Alarms view for the selected service fragment.
-  Reapply – Appears only if service configuration needs to be reapplied. For example, if the Administrative state is disabled, or the Operational State is **Missing** or **Disabled**, or a misconfiguration has occurred.

-  Rename Fragment - Enables renaming the selected service fragment
-  Synchronize - Refreshes the Service Information in the PTP 820 NMS database, by reading back the service information from a particular device.
- Select All - Selects all defined services.
-  Properties - Opens the Properties view for the service.

Ethernet Service Path View

The Ethernet Service Path view shows a visual two-dimensional graph of how the elements configured to carry the service are interconnected for a selected row in the [Ethernet Services View](#). Elements that have endpoints are highlighted. Also, tooltips give additional information about ports on link endpoints.

Figure 132 Ethernet Service Path view



Most of the operations available in [Ethernet Topology View](#) are available in this view also.

Ethernet Services Ports

The Ethernet Service Ports view shows information about the detailed service ports for a selected row in the [Ethernet Services View](#).

Figure 133 Ethernet Service Ports view

Resource Name	FPP ...	Classificat...	Encapsula...	Administr...	Operation...
142 - SP20NqETH-1.1/EthService2	UNI	dot1q	108	Disabled	Missing
141 - SP20NqETH-MC-ABC.1/EthService2	NNI	dot1q		Enabled	Missing
142 - SP20NqETH-MC-ABC.1/EthService2	NNI	dot1q		Enabled	Missing

The following table presents the service port information available in this view.

Table 41 Ethernet Services Ports view table

Name	Explanation
FPP Type	UNI for service end-points, NNI for intermediate points
Classification	VLAN header types or combinations of VLAN header types: <ul style="list-style-type: none"> For ports on S-VLAN based transport VLANs, the classification may be dot1q, AllToOne, Bundle-C or Bundle-S. For ports on C-VLAN based transport VLANs, the classification must be dot1q.
Encapsulation	VLAN Id(s) (tags), determining how packets arriving at a port are mapped to different services.
Administrative State	See Service List for details.
Operational State	See Service List for details.

Available operations

- Refresh - Refreshes the display.
- Customize Columns - Enables setting the visible columns and their order.
- Link View - When activated, selecting a device in the table selects the corresponding device in the Ethernet Topology map.
- Search - A search box enables filtering the display.

Create Ethernet Service Wizard

Creating an ethernet service through the NMS is by means of a simple wizard, guiding the user through 4 steps. To access the wizard, right click a domain in the Ethernet Domains tree or the Ethernet Topology map, and select **Create Ethernet Service**.

The wizard guides you through the following steps:

1. General staep requires the user to specify a flow domain, and enter a name (up to 255 characters) for identifying the service in the NMS. . If possible, this name is also written to the element. Optionally, a description can also be added.
2. Endpoints, select two or more endpoints, the logical ethernet ports on which the service is terminated. If service is successfully reserved in the system, the ports will be tagged as UNIs.
3. Other attributes, View and set the transport VLAN or classification on the endpoints. The lowest unused VLAN ID within the flow domain is preselected for the transport VLAN, but may be overridden by the user. The classification types allowed depends on the type of element and the type of flow domain.
4. Path Preview, to visualize the extent of the service in the network. Visualizes the elements and links which will be configured to carry the service once the wizard is completed.

When the finish button is pressed, two things happen: First, the resources are reserved in the NMS in order that other users cannot allocate the same resources. Secondly, if the resources are successfully reserved within the NMS, the wizard closes and NMS attempts to write the service to be written to all the elements shown previously in the path preview.

TDM Services

TDM Services overview

TDM (Time Division Multiplex) services, the provisioning of end-to-end end 2Mb TDM trails (E1/T1, VC12/VT15) is managed by a set of views defined in the TDM Perspective:

- The TDS Domains view
- The TDM Topology view
- The TDM Services view

Additionally, central to the creation/edition of TDM trail services are:

- The Create TDM Service wizard
- The Edit TDM Service wizard
- The Create STM-1/OC-3 User Link wizard

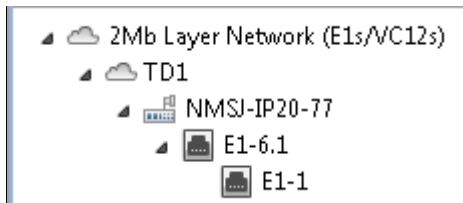
TDM Domains View

This is a view of all elements in the managed network able to transport 2Mb or 1.5Mb TDM trails and which have NMS support for this kind of functionality.

There are five level types in the multilayer subnetwork navigator:

1. The multilayer subnetwork level. This level lists the multilayer subnetworks.
2. The TDM domain level. This level lists the TDM domains, inherited from the Ethernet perspective.
3. The managed element level. This level lists the elements participating in a domain.
4. The physical port level (Physical Termination Point), representing the connectors visible on the outside of the real managed element, for instance an STM-1 electrical interface, or a radio transmitter/receiver.
5. The logical 2Mb/1.5Mb channel (Connection Termination Point), is probably the most significant level in the hierarchy. The CTPs are endpoints of TDM trail services. A simple E1 line interface has only one CTP, but a STM-1 electrical interface 63, and an OC-3 interface has 84 CTPs.

Figure 134 TDM Domains view





The TDM Domains view can be used to launch scoped services lists, and also launch the service creation wizard directly, by selecting two elements or CTPs and initiating the wizard from the context menu.

Searching in the navigator tree













You can search for elements in the tree. Enter a string in the **Search** field, and then use the **Next** (or **Previous**) button to go to the next (or previous) element whose name includes the search string.














Available operations

-  Refresh - Refreshes the display.
-  Link View - When activated, selecting a device in the tree selects the corresponding device in the Ethernet Topology map.






Operations available from the context menu of an element in the tree

Fault - Opens the following Fault views and functions:

-  Active Alarms - Opens an Active Alarms view for the selected element.
-  Historical Alarms - Opens a Historical Alarms view for the selected element.
-  Alarm Templates Assignment - Opens an Alarm Templates Assignment view for the selected element.
-  Mute Notifications - Mutes an NE or a domain, to prevent alarms on the selected NE(s) from generating [alarm notifications](#). The [Mute Notifications dialog](#) will open, where you can select a time for automatic unmuting of notifications. When notifications are muted, NEs will have a [mute indicator](#) on the NE level in the Map and Tree views.
-  Unmute Notifications - Unmutes a muted NE or a domain with a muted element, to re-enable alarms on the selected NE(s) to generate [alarm notifications](#)
- Configuration - Opens the following Configuration views and functions:
 -  Hardware Inventory - Opens a Hardware Inventory view for the selected element.
 -  Software Inventory - Opens a Software Inventory view for the selected element.
 -  Transmission Inventory - Opens a Transmission Inventory view for the selected element.
 -  Create Software Download Job - Opens the Create Software Download Jobs wizard, enabling you to create a software download job for the selected element.
 -  Configuration File Management - Opens a Configuration File Management view for the selected element.
 -  Connection Template Assignment - Opens a Connection Template Assignment view for the selected element.
 - Open SNMP Interface - Opens an "Open SNMP" Connection Template which can be used to manage the device. Basic SNMP management of the device will be triggered to read the inventory and faults from the device.
 - External Tools - Enables opening a web EMS session with the selected device.
 - Performance - Opens the following Performance views and functions:
 -  Current Performance - Opens a Current Performance view for the selected element.

-  Historical Performance – Opens a Historical Performance view for the selected element.
-  Performance Collection Control – Opens a Performance Collection Control view for the selected element.
- Reports – Opens the following Report views and functions:
-  Network Element Types Overview Report – Opens a Network Element Types Overview Report view for the selected element.
-  Inventory Report – Opens an Inventory Report view for the selected element.
-  TDM Services – Opens the TDM Services view.
-  Web EMS – Opens a web EMS session with the selected device
-  Show in Geographic Map – Opens a Geographical Map view of the domain.
-  NE Outline – Opens the NE Outline view, displaying the equipment and port model for the selected device.
-  Topological Links – Opens a Topological Links view for the selected element
-  Reconcile – Instructs PTP 820 NMS to contact the network element, and update the PTP 820 NMS database with information about the element.
-  Rename – Enables renaming the managed element.
-  Delete – Enables deleting the managed element.
- Select All – Selects all elements in the TDM Domains tree.
-  Properties – Displays the element's properties in a Properties view.

Operations available from the context menu of a defined domain

-  Create TDM Service – Opens the Create TDM Service wizard.
-  TDM Services – Opens a TDM Services view, showing the services defined in the selected domain.
-  TDM Topology – Opens a TDM Topology view, displaying the topology of the selected domain.
-  Rename – Enables renaming the selected domain.
- Select All – Selects all elements in the TDM Domains tree.
-  Properties – Displays the domain's properties in a Properties View.

TDM Topology view













The TDM topology view visualizes the connectivity in the TDM multilayer subnetworks.










The networks in the graph can be “opened” or “closed” by double-clicking on the network icons. To navigate down into a network, double click inside an “opened” network. To navigate back up, press the “up” button on the toolbar. It is also possible to eliminate the network structure completely from this view by selecting the “Flat View” option from the view toolbar drop down menu.

Additionally there are tools to pan, zoom and layout the graph for best visibility. There is an option for exporting the image to file, and finally an option to turn on visualization of element product names directly in the graph.

Tooltips on the links summarize the current allocation of the available 2Mb/1.5Mb channels.

Available operations












-  Create STM1/OC3 Link - Opens the Create STM-1/OC-3 User Link wizard.
-  Refresh - Refreshes the view.
-  Move Up - Moves up one level, to the Parent Domain. The parent domain contains the current domain as a “child”, and when going up one level the shape/outline of the previous domain and its “siblings” is displayed (this operation is the opposite of [Doubleclick a Domain](#)).
-  Select Tool - Enables selecting each domain and NE in the view. Hold down the shift key while selecting, to allow selection of multiple objects. When the Select tool is enabled, you can:
 - Drag an object (domain or NE)
 - Open context menus for the currently selected object (domain or NE)
 - Double-click a Domain to go down to this level in the Logical Map view (this operation is the opposite of [Go to Parent Domain](#))
-  Pan Tool - Pans the screen by dragging it in the direction you want.
-  Link Navigation Tool - When clicking a link, alternates between focusing on one end point and focusing on the other end point.
-  Zoom Tool - Zooms in on a specific area of the view by clicking and dragging a rectangle over the area you wish to see in more detail. When the mouse button is released, the view displays only this selected area.
-  Interactive Zoom Tool - Zooms in and out of the entire map by rolling the mouse wheel forwards or backwards.
-  Orthogonal Layout - Displays the topology in an orthogonal layout
-  Hierarchical Layout - Displays the topology in a hierarchical layout.
-  Symmetric Layout - Displays the topology in a symmetrical layout.
-  Circular Layout - Displays the topology in a circular layout.















-  Link Routing – Displays links as curved lines.
-  Zoom In – Click to zoom in on a smaller area.
-  Zoom Out – Click to zoom out to a larger area
-  Best Fit – Centers the currently selected item in the middle of the view.
-  Export as Image – Enables saving the display as an image file.
-  Flat View – Enables eliminating the domains completely from this view
-  Show Managed Element Type – Displays each managed element's type, in addition to its displayed name
-  Topology Overview – Moves the focus to the Topology Overview view
-  Link View – When activated, selecting a device in the map selects the corresponding device in the TDM Domains tree.

Operations available from the context menu of an element

The following operations are available from the context menu of an element:

Fault – Opens the following Fault views and functions:

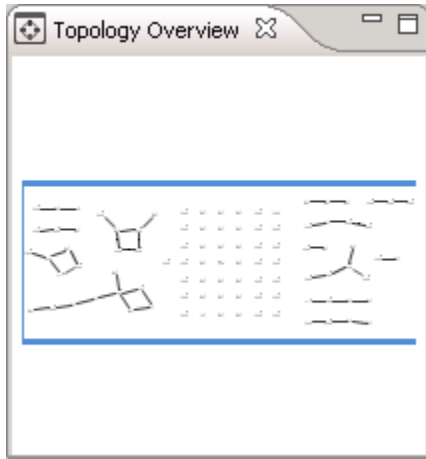
-  Active Alarms – Opens an Active Alarms view for the selected element.
-  Historical Alarms – Opens a Historical Alarms view for the selected element.
-  Alarm Templates Assignment – Opens an Alarm Templates Assignment view for the selected element.
-  Mute Notifications – Mutes an NE or a domain, to prevent alarms on the selected NE(s) from generating [alarm notifications](#). The [Mute Notifications dialog](#) will open, where you can select a time for automatic unmuting of notifications. When notifications are muted, NEs will have a [mute indicator](#) on the NE level in the Map and Tree views.
-  Unmute Notifications – Unmutes a muted NE or a domain with muted element, to re-enable alarms on the selected NE(s) to generate [alarm notifications](#)
- Configuration – Opens the following Configuration views and functions:
 -  Hardware Inventory – Opens a Hardware Inventory view for the selected element.
 -  Software Inventory – Opens a Software Inventory view for the selected element.
 -  Transmission Inventory – Opens a Transmission Inventory view for the selected element.
-  Create Software Download Job – Opens the Create Software Download Jobs wizard, enabling you to create a software download job for the selected element.
-  Configuration File Management – Opens a Configuration File Management view for the selected element.
-  Connection Template Assignment – Opens a Connection Template Assignment view for the selected element.
- Open SNMP Interface – Opens an “Open SNMP” Connection Template which can be used to manage the device. Basic SNMP management of the device will be triggered to read the inventory and faults from the device.

- External Tools – Enables opening a web EMS session with the selected device.
- Performance – Opens the following Performance views and functions:
 -  Current Performance - Opens a Current Performance view for the selected element.
 -  Historical Performance – Opens a Historical Performance view for the selected element.
 -  Performance Collection Control – Opens a Performance Collection Control view for the selected element.
- Reports – Opens the following Report views and functions:
 -  Network Element Types Overview Report – Opens a Network Element Types Overview Report view for the selected element.
 -  Inventory Report – Opens an Inventory Report view for the selected element.
 -  TDM Services – Opens a TDM Services view.
 -  Web EMS – Opens a web EMS session with the selected device
 -  Show in Geographic Map – Opens a Geographical Map view of the domain.
 -  NE Outline – Opens the NE Outline view, displaying the equipment and port model for the selected device
 -  Topological Links – Opens a Topological Links view for the selected element
 -  Reconcile – Instructs PTP 820 NMS to contact the network element, and update the PTP 820 NMS database with information about the element.
 -  Rename – Enables renaming the managed element.
 -  Delete – Enables deleting the managed element.
 -  Properties – Displays the element's properties in a Properties view.

Topology Overview view

This view displays the entire Topology map with a blue frame around the current viewable area in the Topology map.

Figure 135 Topology Overview



You can use this view to do the following:

- Drag&draw the corners of the blue frame to zoom in/out the viewable area in the Topology map.
- Drag inside the blue frame to pan the viewable area in the Topology map.
- Click outside the blue frame to set a new centre for the viewable area in the Topology map.

This tool can be useful when the viewable area in the Topology map view is zoomed in to display only parts of the entire map.

TDM Services View

This view is opened by selecting **Views > TDM> TDM Services**. It displays a list of TDM services. The list is initially empty. You can search for configured services by resource name, and by the minimum alarm severity existing on the service.

To view further information about a specific service, you can right-click a service in the list and select **Open Service Viewer**. This provides a view scoped to the domain in which the service is configured.

You can also view a scoped list of services configured on a domain by right-clicking a TDM domain in the navigator tree or map, and selecting **TDM Services**.

Figure 136 TDM Services view

[illegible]

In addition to the service list columns common to both the Ethernet and the TDM services, the TDM Services view has the following additional TDM-specific columns:

- **Protection**, which takes the values
 - Preemptive: May have resources taken to recover another SNC. Low Priority Channel
 - Unprotected (default): A trail that will fail if any fragment in its route fails.
 - Partially Protected: Protection exists but has at least one shared node, shared link or shared link and node.
 - Fully Protected: A trail that will not fail if any single managed resource along its route fails (excluding the originating and terminating nodes); for example, a trail that is diversely routed at any layer.
- **Priority**, holding the ACM (Adaptive Coding & Modulation) priority. Applicable to only certain element types, but denotes the priority of a certain trail compared to other trails going through links that may have varying capacity.
- **TDM Service Type**, describes the topology of the TDM trail or trail fragment.










Views are connected to the TDM Services list: The TDM Service Ports view and the TDM Service Path view. The content of these are populated accordingly when a row in the TDM Services list is selected.

The TDM Service Path shows a visual two-dimensional graph of how the elements configured to carry the service are interconnected. Elements that have endpoints are highlighted. Also, tooltips give additional information about ports on link endpoints.









More detailed information is available in the TDM Service Ports view. This is a list with the following columns:

- Resource Name, the fully qualified NMS name of a particular CTP (Connection Termination Point)
- Edge Point, Yes for service end-points, No for intermediate points.
- Administrative State should always be Enabled, Operational State likewise - unless the port is down.




Available Operations

-  Refresh – Refreshes the display.
-  Create TDM Service – Opens the Create TDM Service wizard.
-  Customize columns – Enables setting the visible columns and their order.
-  Edit – Enables editing the selected service.
-  Rename Service – Renames the selected service.
-  Delete Selection – Deletes the selected service(s).
-  Confirm – Confirms that PTP 820 NMS should manage the Service.
-  Reapply – Reapplies the service configuration saved in the PTP 820 NMS Database, to the device.
-  Synchronize – Refreshes the Service Information in the PTP 820 NMS database, by reading back the service information from a particular device.

Operations available from the context menu of a defined TDM service

- Performance – Opens the following Performance views and functions:
 -  Current Performance - Opens a Current Performance view for the selected service.
 -  Historical Performance – Opens a Historical Performance view for the selected service.
 -  Performance Collection Control – Opens a Performance Collection Control view for the selected service.
- Fault > Active Alarms – Open an Active Alarms view for the selected service
-  Edit – Opens the Edit Ethernet Service wizard, similar to [Create Ethernet Service Wizard](#).
-  Rename Service – Enables renaming the selected service
-  Synchronize – Refreshes the service information in the PTP 820 NMS database, by reading back the service information from a particular device.
-  Delete – Deletes the selected service.
- Select All – Select all defined services.
-  Properties – Opens the Properties view for the service.

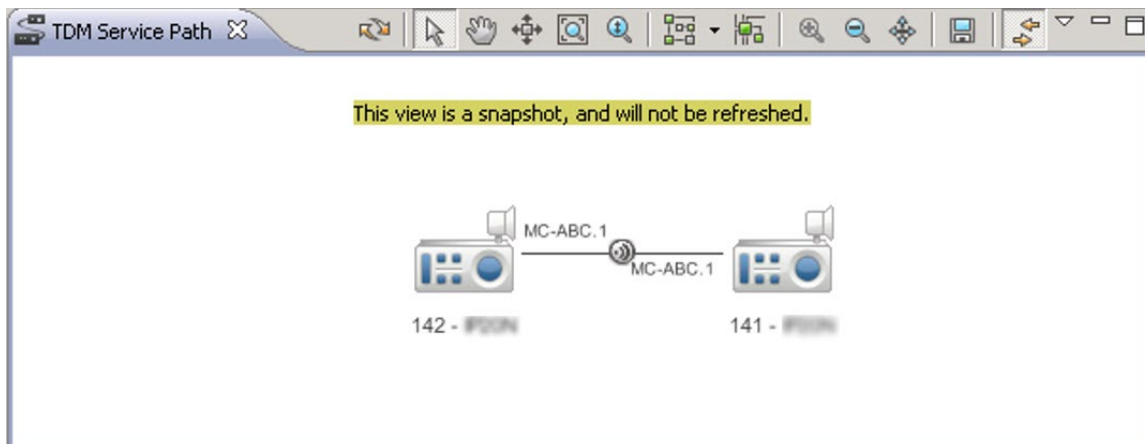
Operations available from the context menu of a defined TDM service fragment

- Fault > Active Alarms – Opens an Active Alarms view for the selected service fragment.
-  Reapply – Appears only if service configuration needs to be reapplied. For example, if the Administrative state is disabled, or the Operational State is **Missing** or **Disabled**, or a misconfiguration has occurred.
-  Synchronize – Refreshes the Service Information in the PTP 820 NMS database, by reading back the service information from a particular device.
- Select All – Selects all defined services.
-  Properties – Opens the Properties view for the service.

TDM Service Path View

The TDM Service Path view shows, for a selected row in the [TDM Services View](#), a visual two-dimensional snapshot of how the elements configured to carry the service, are interconnected. Tooltips give additional information about ports on link endpoints.

Figure 137 TDM Service Path view



Most of the operations available in the [TDM Topology view](#) are available in this view also.

TDM Service Ports View

The TDM Service Ports view shows, for a selected row in the [TDM Services View](#), detailed service ports information.

Figure 138 TDM Service Ports view




The following table presents the service port information available in this view.

Table 42 TDM Services Ports view table

Name	Explanation
Resource Name	The fully qualified NMS name of a particular CTP (Connection Termination Point)
Edge Point	'Y' for service end-points, 'N' for intermediate points.
Timing Mode	For PTP820 devices only: The timing mode configured on the Service Point: <ul style="list-style-type: none"> Recovered – The clock is recovered from the incoming stream. Loop Timing – The recovered clock from the incoming data stream is used for transmission of the outgoing data stream. System Reference – The clock is taken from an external network reference clock that is distributed throughout the network.
Trail ID	Displays the number of the trail

Name	Explanation
Administrative State	Displays the administrative state of the service port. See Service List for details
Operational State	<p>Displays the operational state of the port:</p> <ul style="list-style-type: none"> Unknown – No information is known; service may not be “managed” by PTP 820 NMS. Missing – The configuration of the port has been removed from the device. Misconfigured – There is conflicting information in the configuration of the port. Disabled – The port has been administratively disabled. Down – The Operational State of the port is down, the cable/link may be disconnected. Enabled – The port is configured and connected.

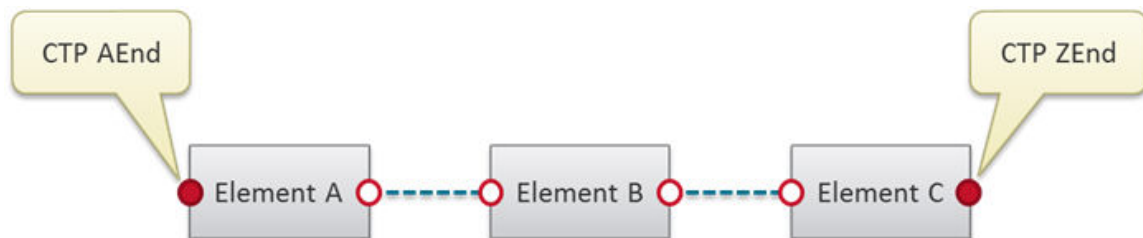
Available operations

-  Refresh – Refreshes the display.
-  Customize Columns – Enables setting the visible columns and their order.
-  Link View – When activated, selecting a device in the table selects the corresponding device in the TDM Topology map.
- Search – A search box enables filtering the display.

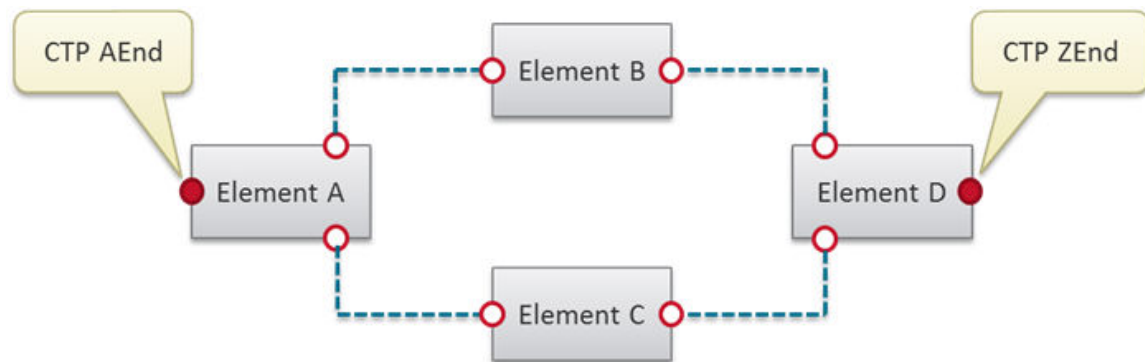
Example TDM service trails

Figure 139 TDM service trails

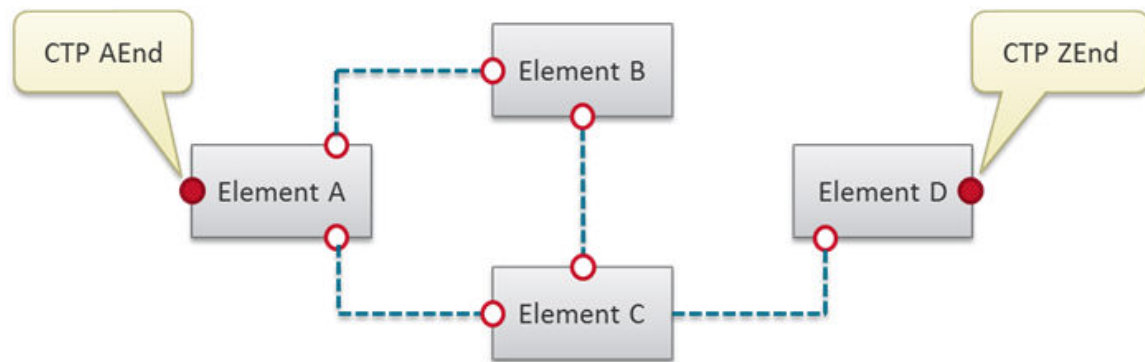
A simple, unprotected service trail



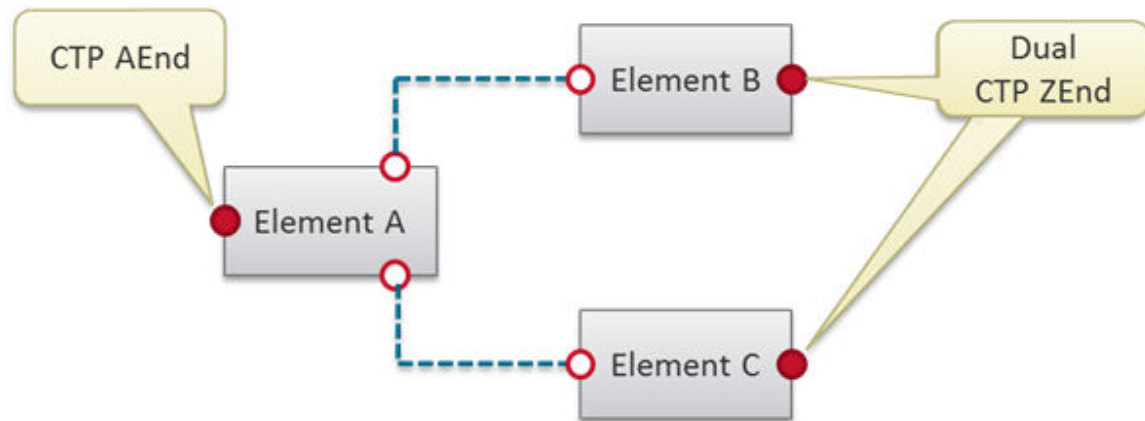
A fully protected service trail



A partially protected service trail




A dual ended service trail



Create STM-1/OC-3 User Link wizard - PTP820

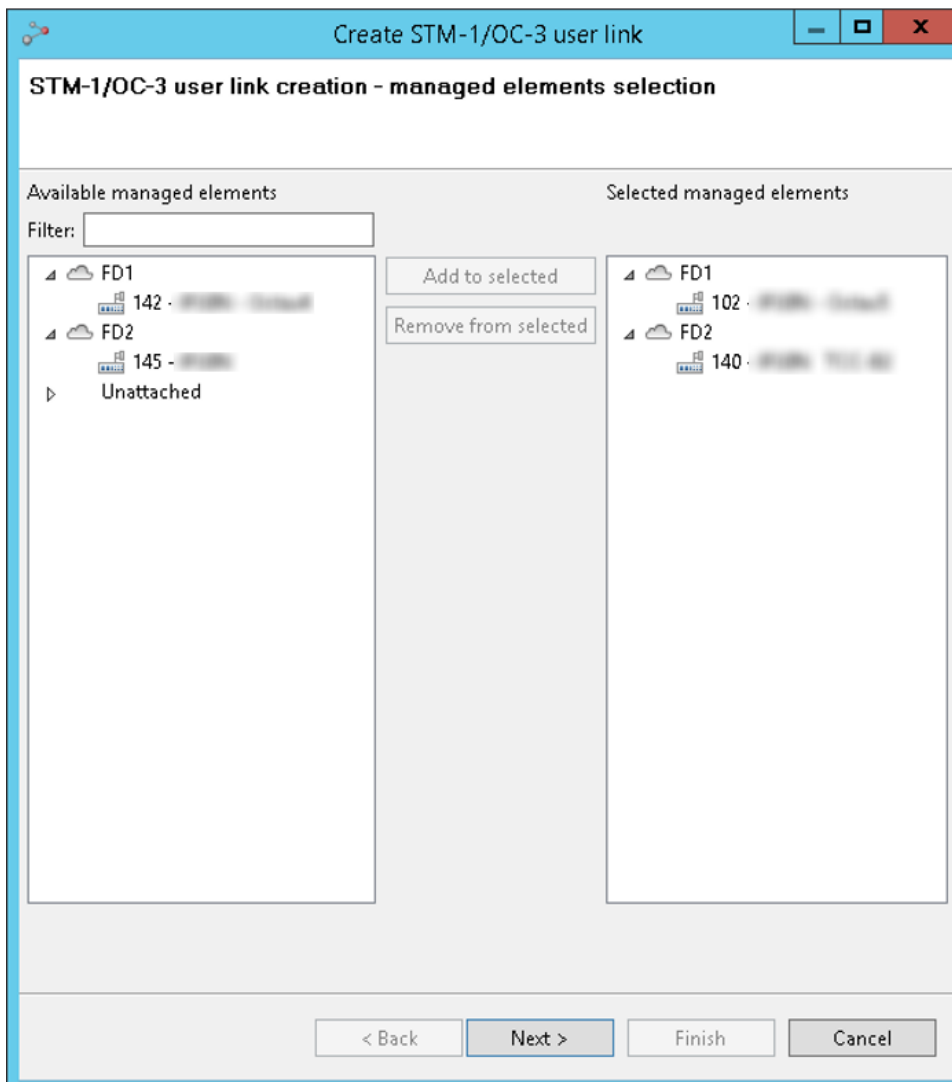
STM-1/OC-3 links between elements cannot be automatically discovered by PTP 820 NMS. If you connect two elements with a STM-1/OC-3 cable, you should enter this information into PTP 820 NMS so that the connection will be taken into account where relevant. For example, in the TDM Topology map, and in the Select Endpoints page of the Create TDM Service wizard.

You can enter information regarding a STM-1/OC-3 link between elements using the Create STM-1/OC-3 User Link wizard.

To access the wizard, select a domain or a device in the TDM Topology map, and click the blue plus sign  in the TDM Topology map toolbar.

The wizard guides you through the following steps:

1. In the first page of the wizard:



- a. Optionally, filter the list of **Available managed elements** by entering a string in the **Filter** field. Only elements whose name contains the search string will appear in the **Available managed elements** list.

- b. Select the first of the two connected elements in the **Available Managed Elements** list on the left, and click **Add to selected**.
 - c. Select the second of the two connected elements in the Available Managed Elements list on the left, and click **Add to selected**.
 - d. Click **Next**.
2. In the second page of the wizard:

Create STM-1/OC-3 user link

STM-1/OC-3 user link creation - link attributes and ports selection

Link name: NMSJ-IP20-77 - NMSJ-IP20N-88

Description:

Link type: STM-1/OC-3

NMSJ-IP20-77	NMSJ-IP20N-88
PTPs	PTPs
STM1-3	STM1-Group.1(2-5)

Map Unmap

< Back Next > Finish Cancel

- a. Optionally edit the **Link name**. By default, the name is a concatenation of the two selected element names.
- b. Optionally enter a **Description** for the link.

- c. On the left, under the name of the first element, select from the list of available STM-1/OC-3 ports or groups, the particular port/group participating in the link.
- d. On the right, under the name of the second element, select from the list of available STM-1/OC-3 ports or groups, the particular port/group participating in the link.
- e. Click **Map** to indicate that the two selected ports/groups are linked with an STM-1/OC-3 connection. The pair area refreshes to display the link graphically.
- f. Click **Finish**.

The STM-1/OC-3 link is written to the PTP 820 NMS database, and displayed in the TDM Topology map.

Create TDM Service wizard

Creating an TDM service through the NMS is by means of a simple wizard, guiding the user through following steps:

There are two prerequisites to creating a TDM service:

- Create Ethernet flow domains, as described in [Ethernet Flow Domain Navigator View](#). This is necessary because the TDM domains hierarchy is inherited from the Ethernet domains.
- If any STM-1/OC-3 links exist in the network, enter that information using the [Create STM-1/OC-3 User Link wizard](#). This is necessary because PTP 820 NMS cannot itself discover STM-1/OC-3 links between elements.

To access the wizard, right click a domain in the TDM Domains tree or the TDM Topology map, and select **Create TDM Service**.

The wizard guides you through the following steps:

1. The general step requires the user to
 - a. Select a Multilayer subnetwork.
 - b. Select a domain.
 - c. Enter a unique name (up to 255 characters) for identifying the service in the NMS. If possible, this name is also written to the element. Optionally add a description. Priority can be set as a wish, but can only be met if supported by network equipment.
 - d. Specify whether you wish to configure path protection. If protection is enabled, NMS attempts to set up multiple paths between endpoints with SNCP (Subnetwork Connection Protection). Select whether to setup 1:1 path protection, or 1+1 path protection.

Dual Ended can be checked if SNCP is used in a ring where part is implemented by equipment that cannot be configured by the NMS. [See example TDM service trails](#). ABR (Adaptive Bandwidth Recovery) can be enabled on a trail protected with SNCP - in order to free resources for ethernet running in parallel on the same links. Applicable only to certain element types.

If you select 1+1 path protection, you can optionally specify Dual ended.

For an explanation of TDM path protection, see [Example TDM service trails](#).

- e. Specify ACM priority.
2. Endpoints, specify the endpoints of the TDM service. These are the the CTPs (Connection Termination Points) or logical TDM channel in which the service is terminated. If dual ended has been selected in the previous step, the source endpoint is the single end and the selected endpoints are the dual endpoints.
3. Path constraints, allows the specification of elements, ports or logical ports that should be included into or excluded from path calculation.
4. Path Preview, to visualize the extent of the service in the network. Visualizes the elements and links which will be configured to carry the service once the wizard is completed.
5. If the path includes PTP820 user links (defined using the Create STM-1/OC-3 User Link wizard), an additional page appears for defining the channel for each of those links and the timing mode for each edge point.

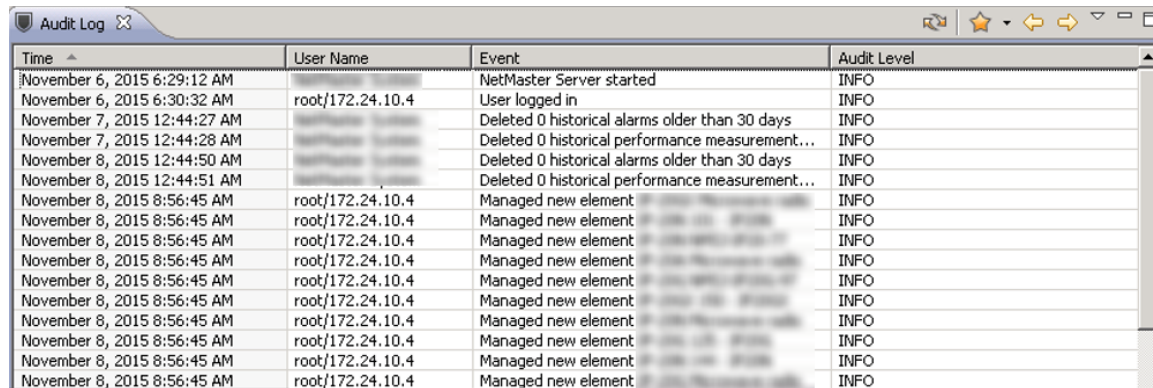
When the Finish button is pressed, two things happen: First, the resources are reserved in the NMS in order that other users cannot allocate the same resources. Secondly, if the resources are successfully reserved within the NMS, the wizard closes and NMS attempts to write the service to be written to all the elements shown previously in the path preview.

Administration

Audit Log view

This view can be found in the [Security Audit](#) perspective, and can be used together with the [User Administration](#) view. The view can be opened by selecting Views | Administration | Audit Log from the main menu.

Figure 140 Audit log view



Time	User Name	Event	Audit Level
November 6, 2015 6:29:12 AM		NetMaster Server started	INFO
November 6, 2015 6:30:32 AM	root/172.24.10.4	User logged in	INFO
November 7, 2015 12:44:27 AM		Deleted 0 historical alarms older than 30 days	INFO
November 7, 2015 12:44:28 AM		Deleted 0 historical performance measurement...	INFO
November 8, 2015 12:44:50 AM		Deleted 0 historical alarms older than 30 days	INFO
November 8, 2015 12:44:51 AM		Deleted 0 historical performance measurement...	INFO
November 8, 2015 8:56:45 AM	root/172.24.10.4	Managed new element	INFO
November 8, 2015 8:56:45 AM	root/172.24.10.4	Managed new element	INFO
November 8, 2015 8:56:45 AM	root/172.24.10.4	Managed new element	INFO
November 8, 2015 8:56:45 AM	root/172.24.10.4	Managed new element	INFO
November 8, 2015 8:56:45 AM	root/172.24.10.4	Managed new element	INFO
November 8, 2015 8:56:45 AM	root/172.24.10.4	Managed new element	INFO
November 8, 2015 8:56:45 AM	root/172.24.10.4	Managed new element	INFO
November 8, 2015 8:56:45 AM	root/172.24.10.4	Managed new element	INFO
November 8, 2015 8:56:45 AM	root/172.24.10.4	Managed new element	INFO
November 8, 2015 8:56:45 AM	root/172.24.10.4	Managed new element	INFO
November 8, 2015 8:56:45 AM	root/172.24.10.4	Managed new element	INFO

PTP 820 NMS collects a log of all administration activities performed by the users in the system so that you can monitor whether users act in a manner potentially damaging to the system. This view allows you to audit the event log, enabling you to identify users who should be blocked or removed.

As soon as you have identified a suspicious user, the user can be blocked and/or deleted in the User Administration view.

The log can also contain the following entries:

- [Deletion of historic alarms](#)
- [Deletion of historic performance measurements](#)
- Server start and stop

Audit Log table

The table displays the following data on each user event:

Table 43 Audit log table







Name	Explanation
Time	The time the event was generated.
Event	A description of what has happened
User Name	The login name of the user who has created the event. If the event is triggered by the PTP 820 NMS server itself, the User name will be "PTP 820 NMS System"
Audit Level	Severity of the event. One of the possible alarm severities: <ul style="list-style-type: none"> • INFO • ERROR • WARN

Please note that the table displays a query of data based on the current "Audit Log" filter (default is no filter, and page size=50). The filter defines what entries should be included/excluded in each query, and page size defines the maximum number of returns matching these filter criteria in each query. The Audit Log table can be filtered using the following parameters:

- Audit Level
- Event
- Time
- User Name

Filter criteria and a page size for the Audit Log table can be defined in the [Filter Manager](#) view

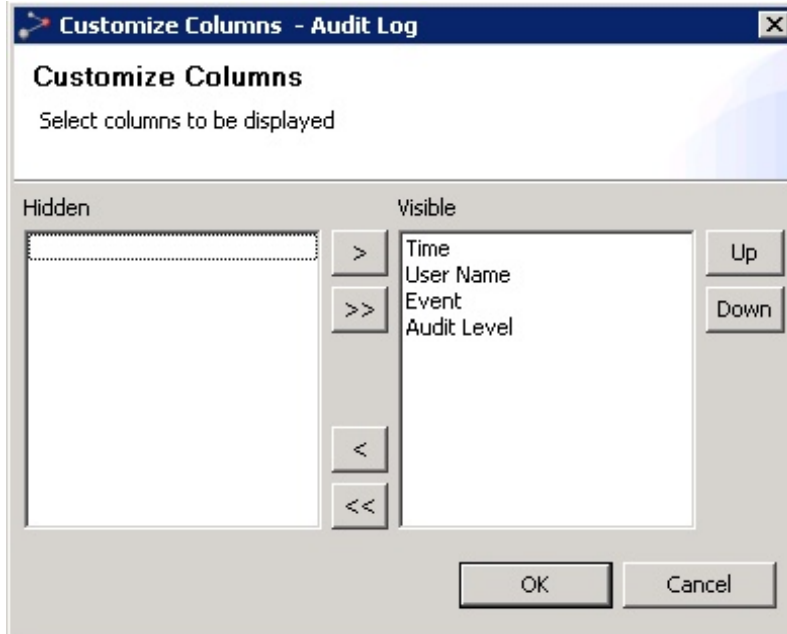
Available operations

-  Refresh Refresh the current query in the User Audit table.
-  Go to the previous page in the current query.
-  Go to the next page in the current query.
-  Filter Manager Open the [Filter Manager](#) view, where you can create filter conditions and set page sizes for filters that can be applied to the User Audit table.
-  Click the drop-down to select/apply one of the filters created and tagged as favorite in the Filter Manager view.
-  Customize Columns Open the [Customize Columns](#) dialog, where you can select which columns are to be displayed in the User Audit table.

Customize Columns dialog for Audit Log

This dialog is opened by selecting Customize Columns in the view drop-down, or in the context menu in the Audit Log table.

Figure 141 Customize columns dialog for audit log

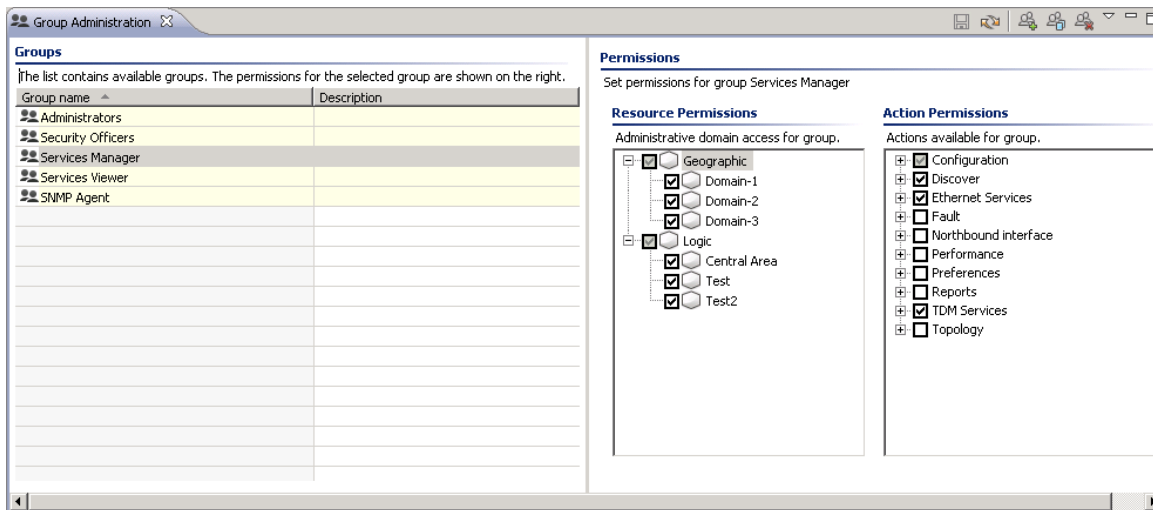


Details about how to use this dialog can be found in the chapter about the [Customize Columns](#) dialog.

Group Administration view

This view can be found in the [User Management](#) perspective, and is used together with the [User Administration](#) view.

The Group Administration view can be opened by selecting Views | Administration | Group Administration from the main menu.

Figure 142 Group administration view

In this view you can create and delete groups and assign permissions for the groups. The groups created here are used in the User Administration view to assign a set of permissions to each user.

The view contains a Groups table in the Groups area to the left, and a Resource Permissions tree and an Action Permissions Tree in the Permissions area to the right.

Groups table

This table presents the usergroups that are created on this server, and a short description of the group. You can change both the name and description of each group by clicking in the table. You are also allowed to delete, clone and create new groups to the table.

When selecting one of the groups in the table, the group's permissions will be displayed in the Resource Permissions tree and in the Action Permissions tree.

Resource Permissions tree

This tree displays domains where the currently selected usergroup has access. You can change permissions by checking/unchecking the checkboxes in the Resource Permissions tree. A usergroup can only see the domains where they have resourcepermissions all other domains will be hidden for users in this group.







As a user will see all NEs in a domain where it has permissions, you must place NEs in different domains to be able to give permissions to different users. Please note that the same NE can be managed in both Logical and Geographical Models, and restrictions on permissions for NEs must be applied in both models.

The domains in the Resource Permissions tree can be created, modified and deleted using the [Geographical Tree](#) view and the [Logical Tree](#) view.

Action Permissions area

This tree displays actions allowed for the currently selected usergroup. You can change permissions by checking/unchecking the checkboxes in the action tree. A usergroup can only see the menu items and icons where they have action permissions – all other domains will be hidden/disabled for users in this group.

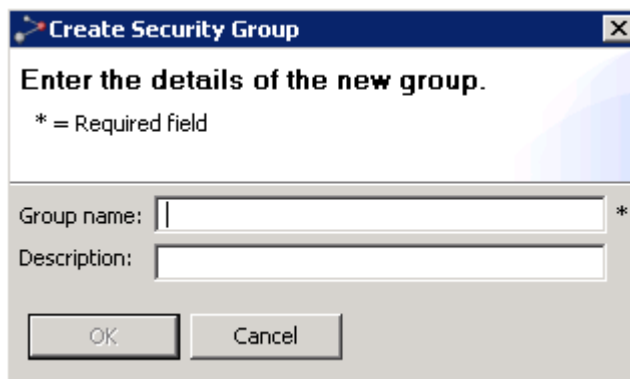
Available operations

-  Save the modifications you have made in the Group Administration view
-  Create Group Create a new usergroup starting with blank resource/action permissions. The [Create Security Group](#) dialog will be opened, where you can enter a name and description for the new group.
-  Clone selected Group Create a new usergroup, starting with the resource/action permissions of the group that is currently selected in the Groups table. The [Clone Security Group](#) dialog will be opened, where you can enter a name and description for the new group.
-  Delete Delete the currently selected usergroup and open the [Confirm Group Delete](#).
-  Refresh the data in all fields in the Group Administration view
-  Click a checkbox in the Resource Permissions tree or the Action Permissions tree to add/remove permissions for the currently selected usergroup in the Groups table.

Create Security Group dialog

This dialog can be opened by pressing the Create New Security Group icon in the Group Administration view

Figure 143 Create security group dialog



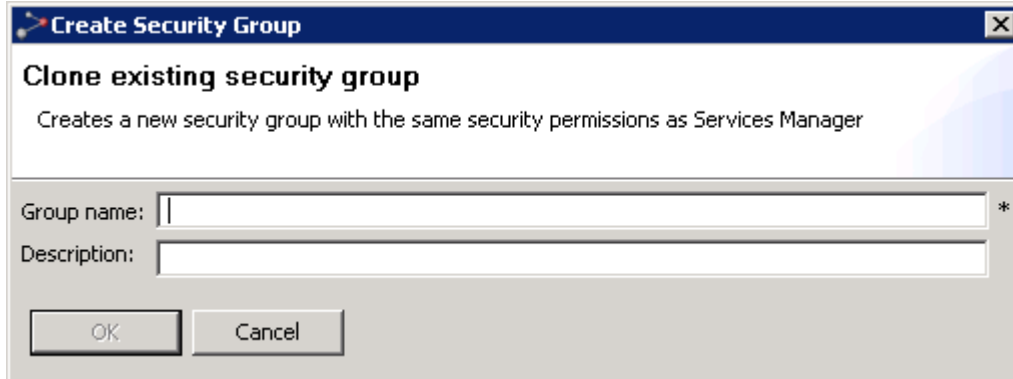
The dialog box is titled "Create Security Group" and contains the text "Enter the details of the new group." Below this, it states "* = Required field". There are two input fields: "Group name:" and "Description:". The "Group name:" field has an asterisk next to it, indicating it is a required field. At the bottom of the dialog are two buttons: "OK" and "Cancel".

Enter a name and a description of the group and press OK, or press Cancel to abort.

Clone Security Group dialog

This dialog can be opened by pressing the Clone Selected Group icon in the Group Administration view with a security group selected in the Groups table.

Figure 144 Clone security group dialog

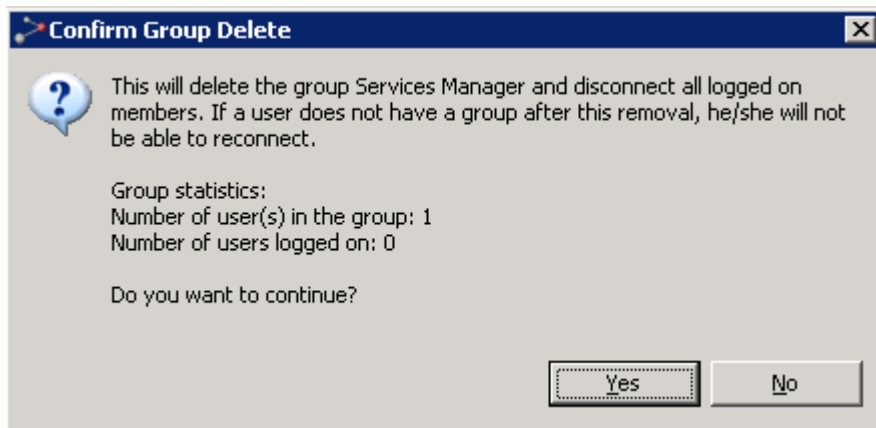


Enter a new name and a description of the group and press OK, or press Cancel to abort.

Confirm Group Delete dialog

This dialog opens after pressing Delete in the Group Administration view with a security group selected in the Groups table.

Figure 145 Confirm group delete dialog

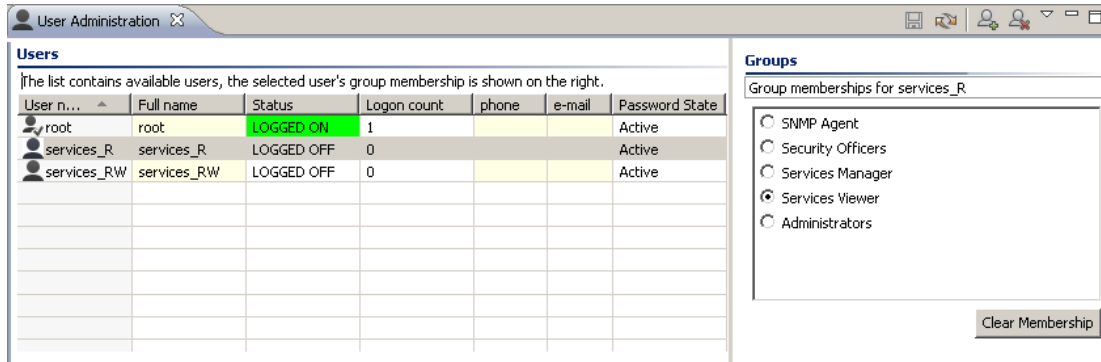


Press Yes to confirm the deletion, or press No to cancel.

User Administration view

This view can be found in the [User Management](#) perspective, and is used together with the Group Administration view. The view can be opened by selecting **Views > Administration > User Administration** from the main menu.

Figure 146 User administration view



In this view you can register new PTP 820 NMS users, update their properties, and modify their access permissions by assigning them to different user groups.

Users table

This table shows the users that are created on this server, with their properties. You can change the name, telephone number and e-mail address by clicking directly in the table.

Please note that the User name cannot be changed.

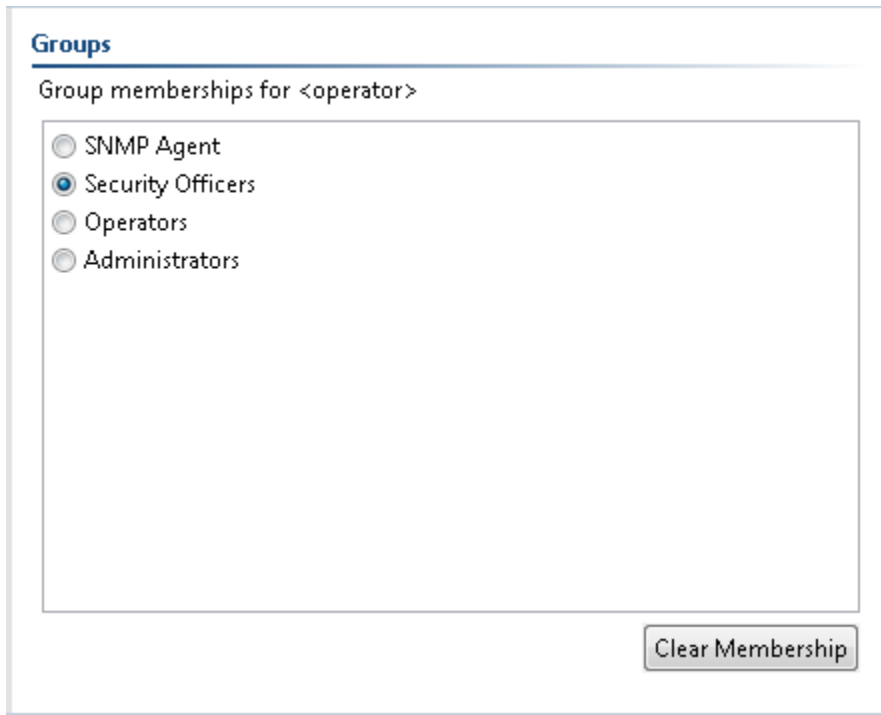
The **Password State** displays one of the following states:








- **New** – Indicates the user has a new password, either because the user is new, or because an admin changed the user's password.
- **Active** – The user has a usable password.
- **Expired** – Indicates the user's password has expired. In this case, the user must change his password in the window that appears upon a login attempt.
- **Locked-Out** – Indicates that the user exceeded the allowed maximum number of failed login attempts. In such a case, only a user with System Preferences rights can unlock the user by defining for the user a new password using the [Change Password](#) operation.

When selecting a line in the table, the group membership for the currently selected user will be presented in the Groups area.

Groups table

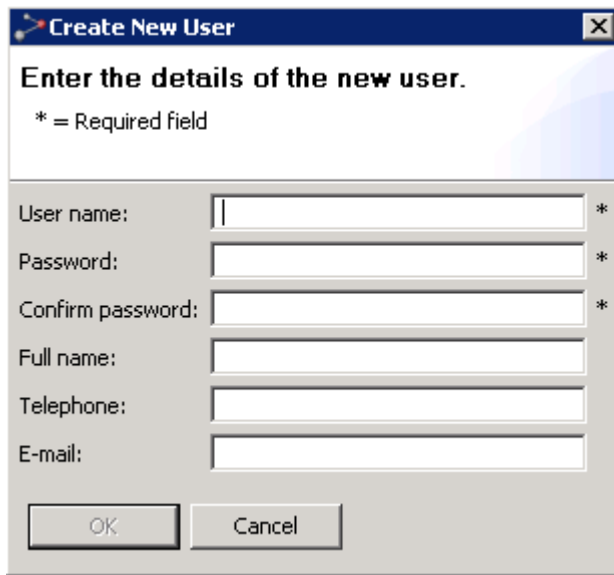
This table presents group membership information for the currently selected user in the [Users](#) table. New user-groups are created in the [Group Administration](#) view. You can change a user's group membership by selecting a different group, or remove the user from all groups by pressing Clear Membership.

Figure 147 User administration view**Available operations**

-  **Create User** Create a new user account and open the [Create New User](#) dialog.
-  **Block User Account** Temporarily remove all permissions for the currently selected user and open the [Block User](#) dialog. The user will then be denied access upon next login. This menu option will only be available when selecting a user that has not been blocked.
-  **Unlock User Account** Give back permissions for the currently selected, blocked user. The user can now log on again. This menu option will only be available when selecting a user that has been blocked.
-  **Change Password** Change password for the user and open the [Change Password](#) dialog. Please note that the process of changing password on a user that currently is logged in, will involve that the server automatically logs out this user.
-  **Delete User Account** Delete the selected user and open the [Confirm User Delete](#) dialog.
-  Refresh the data in all fields in the User Administration view
-  Save the modifications you have made in the User Administration view

Create New User dialog

This dialog can be opened by pressing Create New User in the User Administration view.

Figure 148 Create new user dialog

The 'Create New User' dialog box has a title bar with a blue gradient and a close button. The main area has a light blue gradient background. It contains the text 'Enter the details of the new user.' and a legend '* = Required field'. Below this are six input fields: 'User name:', 'Password:', 'Confirm password:', 'Full name:', 'Telephone:', and 'E-mail:'. The first three fields have an asterisk to their right, indicating they are required. At the bottom are 'OK' and 'Cancel' buttons.

Enter the data for the user and press OK, or press Cancel to abort. Please notice that User name cannot be changed after closing this dialog - all other fields in this dialog can be changed in the Users table.

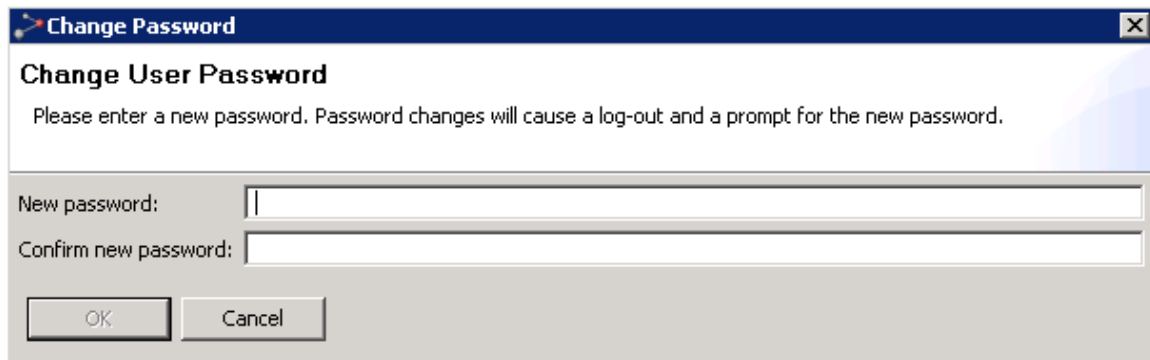
Block User dialog

This dialog can be opened when using [Block User](#) in the User Administration view with an unblocked user selected .

Press OK to confirm the user is to be blocked, or Cancel to abort the operation. The user will then be denied access upon next login, and cannot log in until the user has been [unblocked](#).

Change Password dialog

This dialog can be opened by pressing [Change Password](#) or [Create User](#) in the User Administration view.

Figure 149 Change password dialog

The 'Change Password' dialog box has a title bar with a blue gradient and a close button. The main area has a light blue gradient background. It contains the text 'Change User Password' and a message 'Please enter a new password. Password changes will cause a log-out and a prompt for the new password.' Below this are two input fields: 'New password:' and 'Confirm new password:'. At the bottom are 'OK' and 'Cancel' buttons.

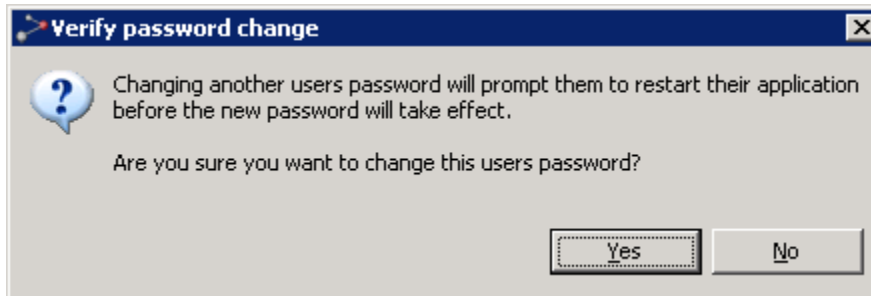
Enter the new password in both fields and press OK, or press Cancel to abort. Please note that the OK button will not be enabled before a legal password string is entered, as defined on server in the [Password Settings](#) preference page.

When pressing OK, the [Verify Password Change](#) dialog appears. If password change is confirmed, this user will be forced to log out as soon as you [Save](#) your changes in the User Administration view.

Verify Password Change dialog

This dialog is opened after pressing [Change Password](#) in the User Administration view and then OK in the [Change Password](#) dialog.

Figure 150 Verify password change dialog



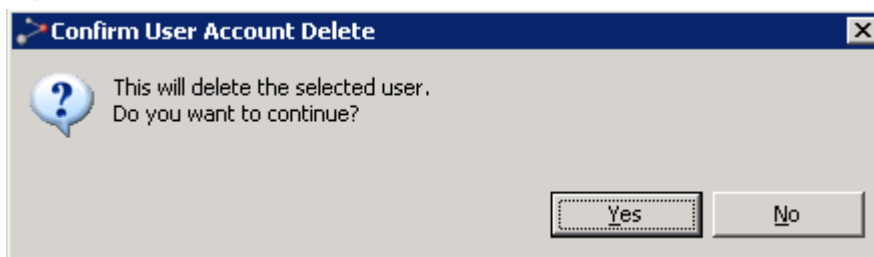
Press Yes to apply the password change. As soon as you [Save](#) the changes in the User Administration view, the affected user will be kicked out by the server, and the [PTP 820 NMS Login](#) dialog will appear for this user.

Alternatively press No to abort the password change.

Confirm User Delete dialog

This dialog can be opened by pressing Delete User with a user selected in the User Administration view.

Figure 151 Confirm user delete dialog



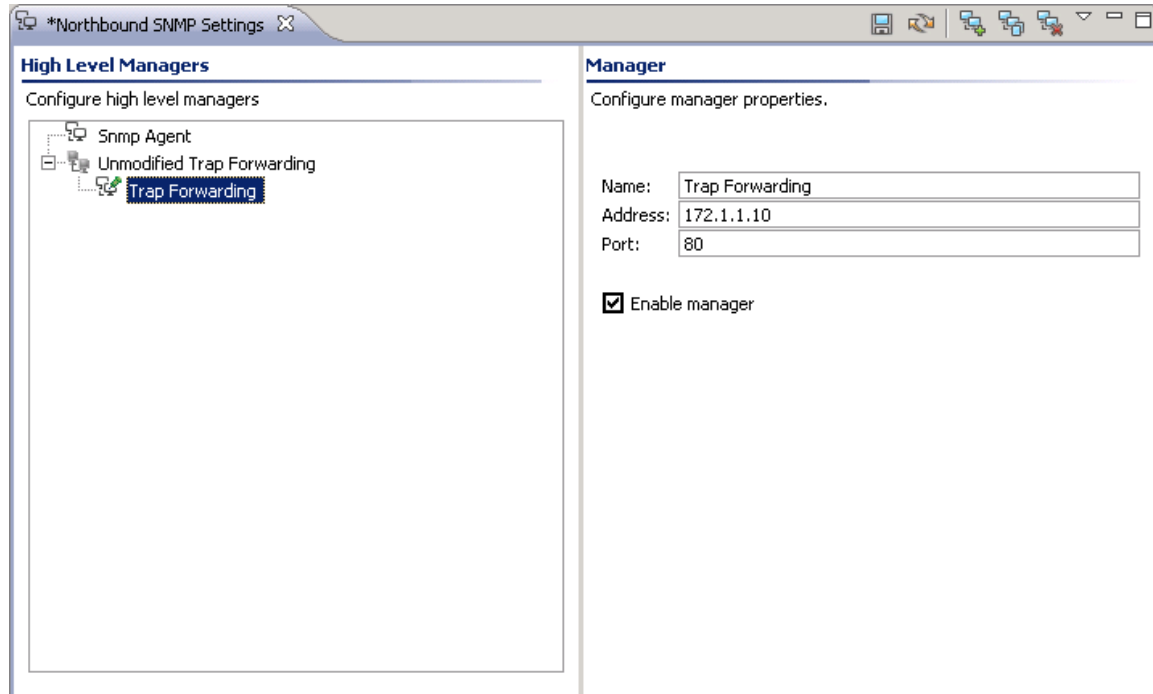
Press Yes to confirm the deletion, or press No to cancel.

Northbound Interface

Northbound SNMP Settings view

This view is opened from the main menu under **Views > Northbound Interface > Northbound SNMP Settings**.

Figure 152 Northbound SNMP settings view



In this view you can create and configure the High Level Managers (HLM):

- To communicate with PTP 820 NMS via the [PTP 820 NMS SNMP Agent](#).
- To enable unmodified trap forwarding.

You can create multiple HLMs that are SNMP Agents, and multiple HLMs that use unmodified trap forwarding.

All High Level Managers must be configured with access control and trap forwarding parameters prior to use. See [how to configure Northbound Interface SNMP](#), for a simple step-by-step description about settings in the PTP 820 NMS SNMP Agent and Northbound SNMP Settings view.

The PTP 820 NMS SNMP Agent provides a northbound interface for any SNMP based Network Management System to perform [Fault Management](#) of networks managed by PTP 820 NMS. The agent provides topological information according to ENTITY-MIB (RFC 2737), and alarm state of the various network elements through proprietary tables and variables. State changes are communicated to managers by means of SNMP traps. Detailed information about PTP 820 NMS's northbound interface can be found in the document PTP 820 NMS SNMP Agent Guide.pdf on installation CD.

The SNMP Agent is basically a specialized client that logs onto the PTP 820 NMS server with a user ID and exposes a set of information through a SNMP interface. The only requirement to the user ID is that it is a member of the predefined SNMP Agent user group, or a group with similar [Action Permissions](#). This gives a good control over the part of the network that is exposed to the HLMs, as the Resource Permissions for the SNMP Agent user group can be configured in detail in the exact same way as any other user group defined in PTP 820 NMS.

Unmodified Trap Forwarding

Unlike HLMs utilizing the SNMP agent, a HLM created for unmodified trap forwarding will forward the traps exactly as received, without imposing upon them any formatting or informational protocols. It forwards PTP 820 NMS management alarms in EMS format.



Note

If High Availability is implemented on the system, unmodified trap forwarding must be disabled on the standby server. See the High Availability Solution installation guide.

Unmodified trap forwarding functionality requires that the PTP 820 NMS user have SNMP northbound interface action permission. Also note that unmodified trap forwarding functions only with NEs which are licensed for Northbound SNMP capability.




PTP 820 NMS SNMP Agent and Unmodified Trap Forwarding are licensed features of PTP 820 NMS, and are available with the Northbound SNMP - No. of Network Elements license.

The Northbound SNMP settings view consists of a High Level Managers area containing a tree view with all HLMs and a Manager area containing details about the currently selected HLM.

High Level Managers area

This area contains a tree view with all configured High Level Managers.






The High Level Managers tree consists of the following objects:

-  The Manager node corresponds to a configured manager
-  The SNMP Configuration node contains community names and trap port for the manager.
-  The Alarm forwarding configuration node contains criteria for alarms forwarding over SNMP.

Manager area

This area presents the details of the currently selected manager node in the tree in the High Level Managers area. The contents of the Manager area depends on the actual settings of the manager selected.

Available operations

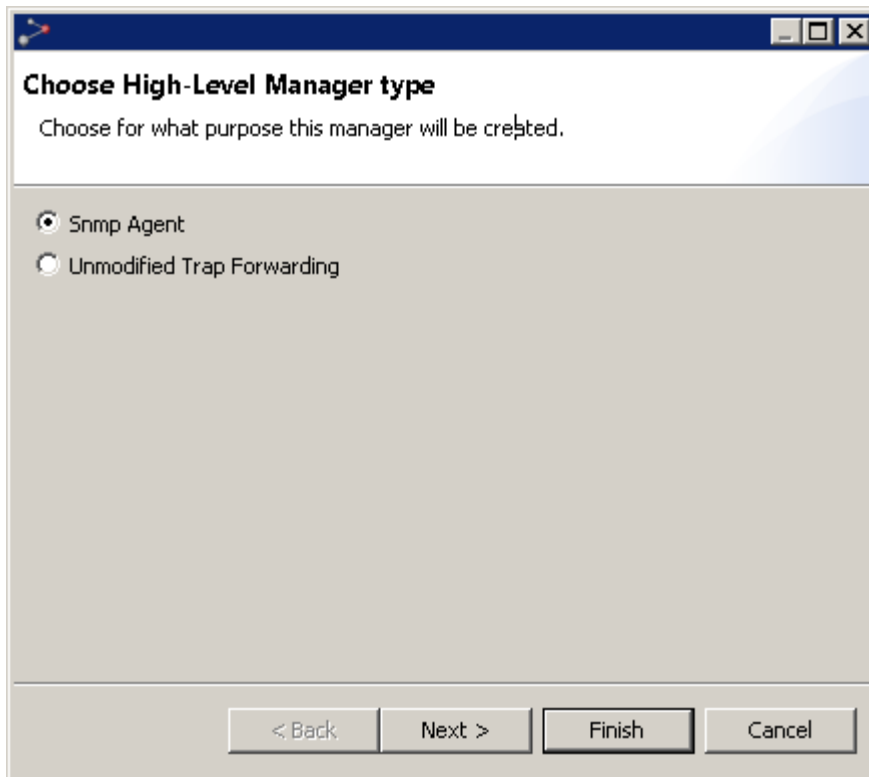
-  Save the updates you have made in the High Level Manager tree and Manager area. If the view contains invalid settings, an explanation about these settings will be displayed in the top of the Manager area as well as in the tree view. The Save Modifications operation will be disabled until these settings are corrected. If you try to close the view without saving data, the Save Changes dialog will appear.
-  Refresh the view with the latest data from the server.
-  Create a new High Level Manager. This operation will launch a [three step wizard](#) that will assist you in creating a new manager.
-  Clone the selected manager
-  Remove the selected manager. This operation is only available when a High Level Manager is selected in the HLM tree.

Create a new High Level Manager wizard

When you select the Create a new High Level Manager button, a wizard is launched.

The first screen of the wizard asks you to select which type of High Level Manager you want to create.

Figure 153 Create a new high level manager wizard



Select a purpose for the High Level Manager and click **Next**.

For SNMP Agent:

The wizard continues with the following three steps:

Step 1: Set manager properties - name and address

Figure 154 Set manager properties

The screenshot shows a Windows-style dialog box titled "Create a new high-level manager". Below the title bar, it says "Create High-Level Manager (1/3)" and "Set manager properties for name and address." There are three input fields: "Name:" with the text "High Level Manager 1", "Address:" with the text "137.133.21.45", and "SNMP Version:" with a dropdown menu showing "v2c". At the bottom, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

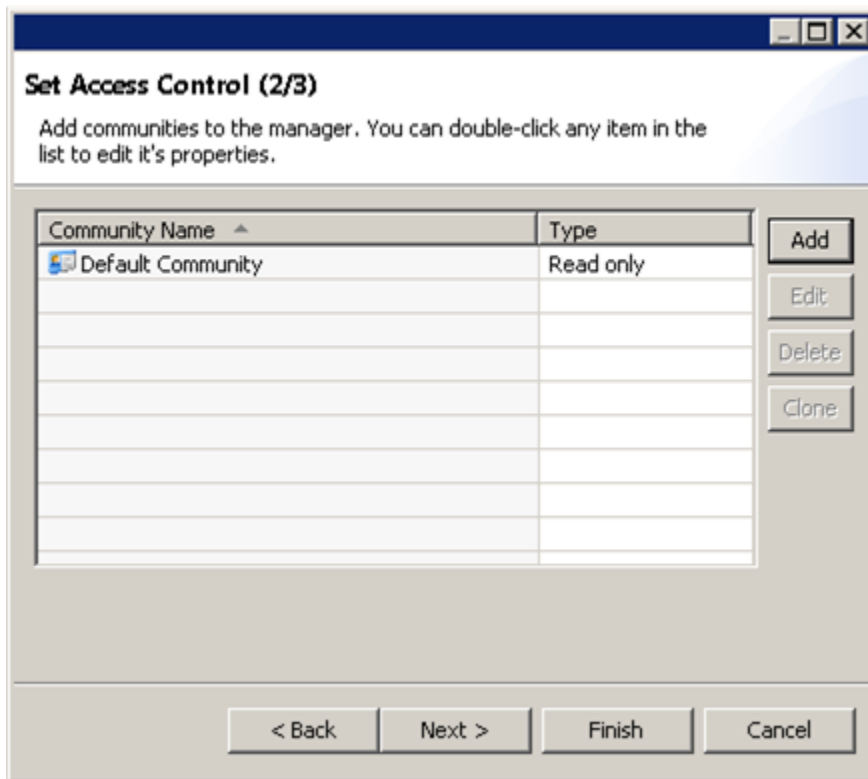
Complete the following fields described below:

- **Name:** A textual description of the manager. Each manager must have a unique name.
- **Address:** The IP address of the manager.
- **SNMP Version:** SNMP version used by the manager: **V2c** or **V3**.

Click **Next**. The following steps depend on the SNMP version you selected for the manager.

Step 2: For SNMP V2c manager: Add communities

Figure 155 Add communities



In this dialog, the SNMP community names associated with the manager are configured.

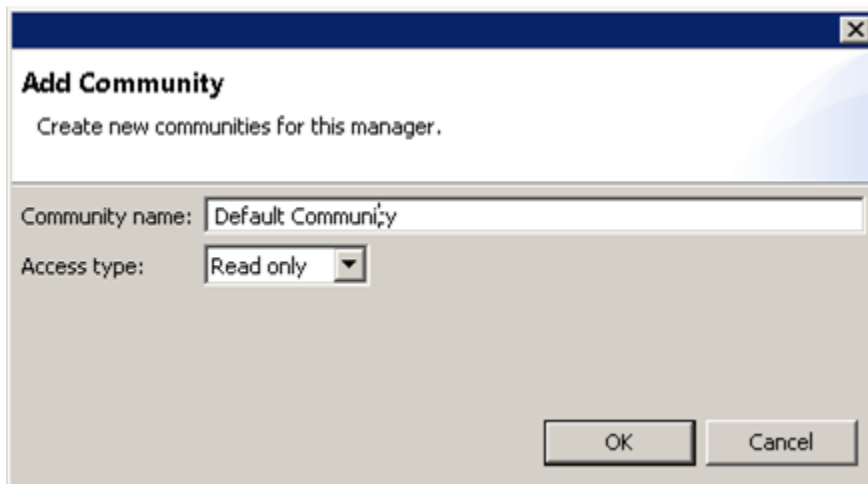
A manager can have several community names, but a community name can not be shared between managers.

A community name can be of the following types: Read only, Read/Write.

Double-click a community and use the controls on the right to add, edit, delete or clone a community.

To add a new community, click **Add**.

Figure 156 Add new community



Type a community name and select an access type. Options are:

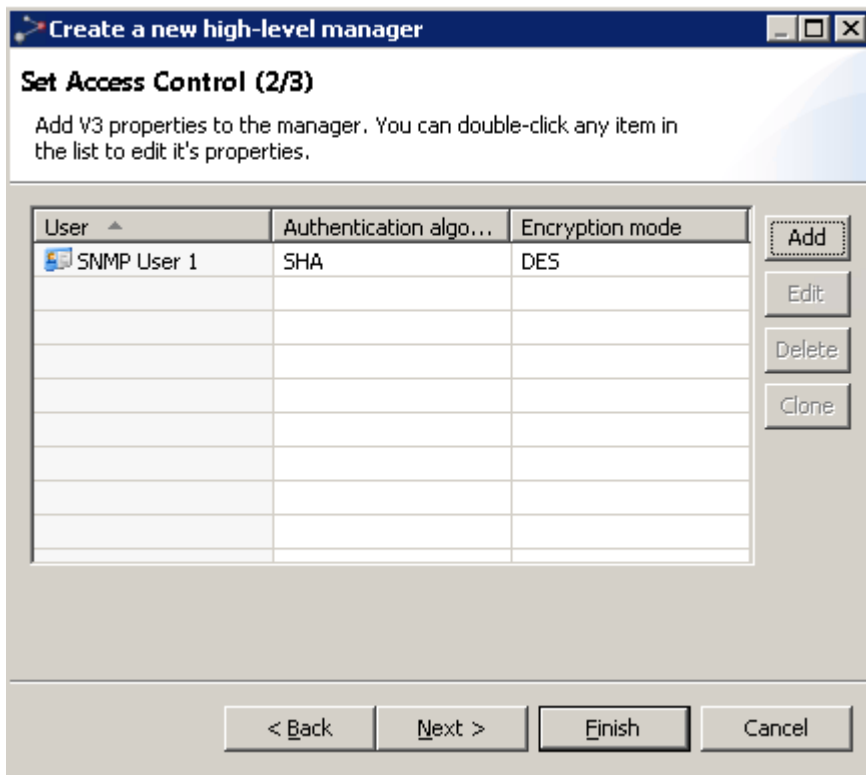
- Read only
- Read/write

Click **OK** to return to the Set Access Control window.

When are you are done adding communities, click **Next**.

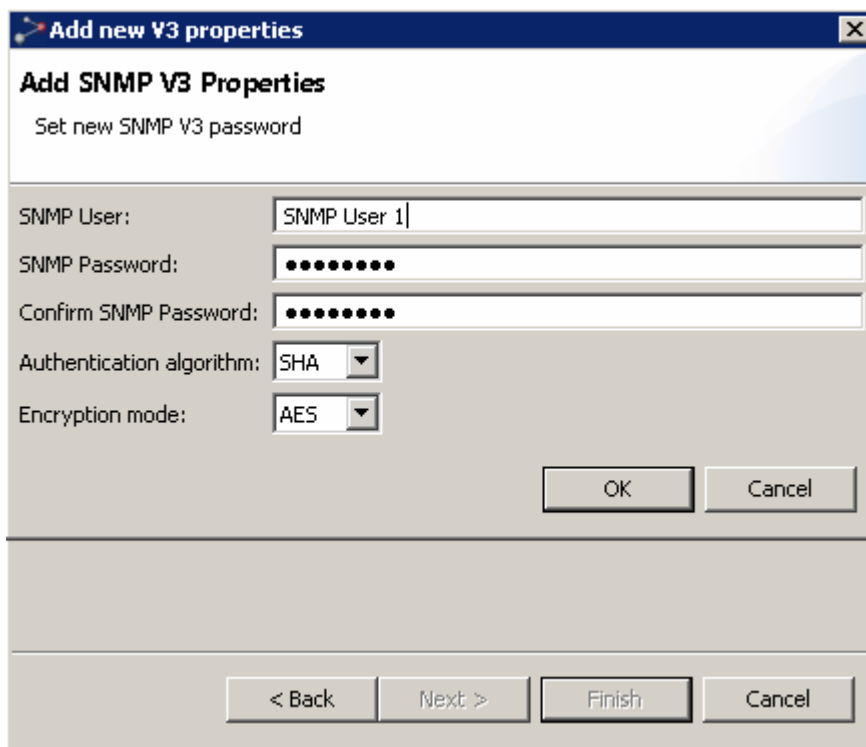
Step 2: For SNMP V3 manager: Add v3 users

Figure 157 Add V3 users



In this dialog, the SNMP V3 users associated with the manager are configured.

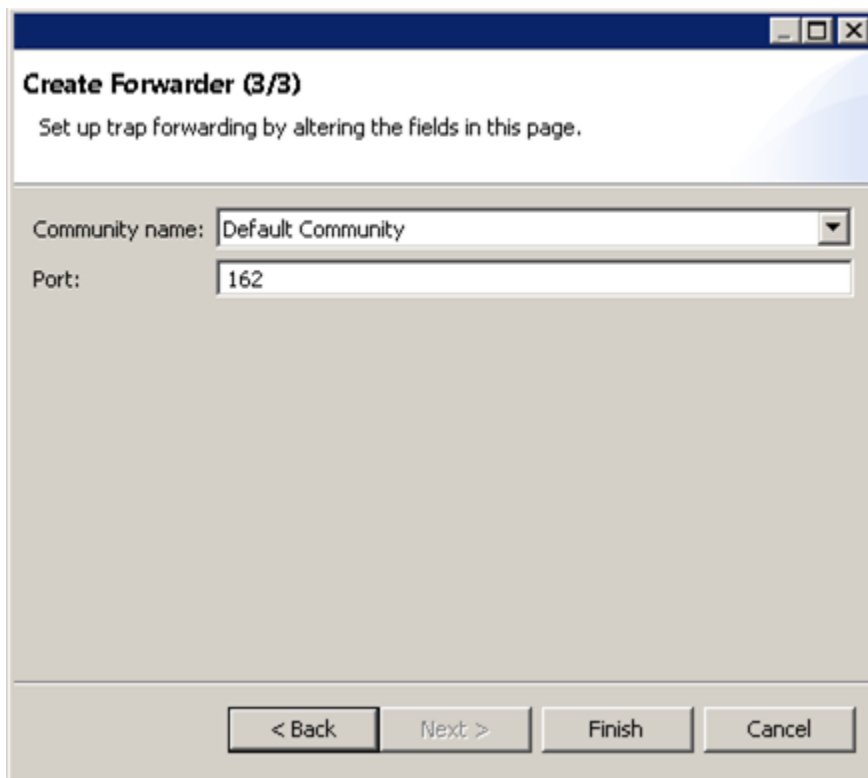
- Double-click an SNMP V3 user and use the controls on the right to edit, delete or clone an SNMP V3 user.
- To add an SNMP V3 user, click **Add**.

Figure 158 Add SNMP V3 Properties

The dialog box is titled "Add new V3 properties" with a close button (X) in the top right corner. Below the title bar, the main heading is "Add SNMP V3 Properties" followed by the instruction "Set new SNMP V3 password". The form contains five input fields: "SNMP User:" with the text "SNMP User 1", "SNMP Password:" with masked characters, "Confirm SNMP Password:" with masked characters, "Authentication algorithm:" with a dropdown menu showing "SHA", and "Encryption mode:" with a dropdown menu showing "AES". At the bottom right of the form area are "OK" and "Cancel" buttons. Below the form area, separated by a horizontal line, are four buttons: "< Back", "Next >", "Finish", and "Cancel".

- Enter a user name and password for the SNMP user.
- Specify an Authentication algorithm: None, SHA, or MD5.
- Specify an Encryption mode: None, AES, DES. Note that if you selected None for the Authentication algorithm, you must select None for the Encryption mode.
- Click **OK** to return to the Set Access Control window.
- When you are done adding SNMP V3 users, click **Next**.

Step 3: For SNMP v2c manager: Setting up a trap forwarder.

Figure 159 Setting up a trap forwarder

Create Forwarder (3/3)
Set up trap forwarding by altering the fields in this page.

Community name:

Port:

< Back Next > Finish Cancel

Configure the following fields:

- Community name: Community name sent with the trap. Select from the drop-down list.
- Port: Trap destination port number. Edit as required.

Step 3: For SNMP v2c manager: Setting up a trap forwarder.

Figure 160 Setting up a trap forwarder

Create a new high-level manager

Create Forwarder (3/3)

Set up trap forwarding by altering the fields in this page.

SNMPV3 User:

Port:

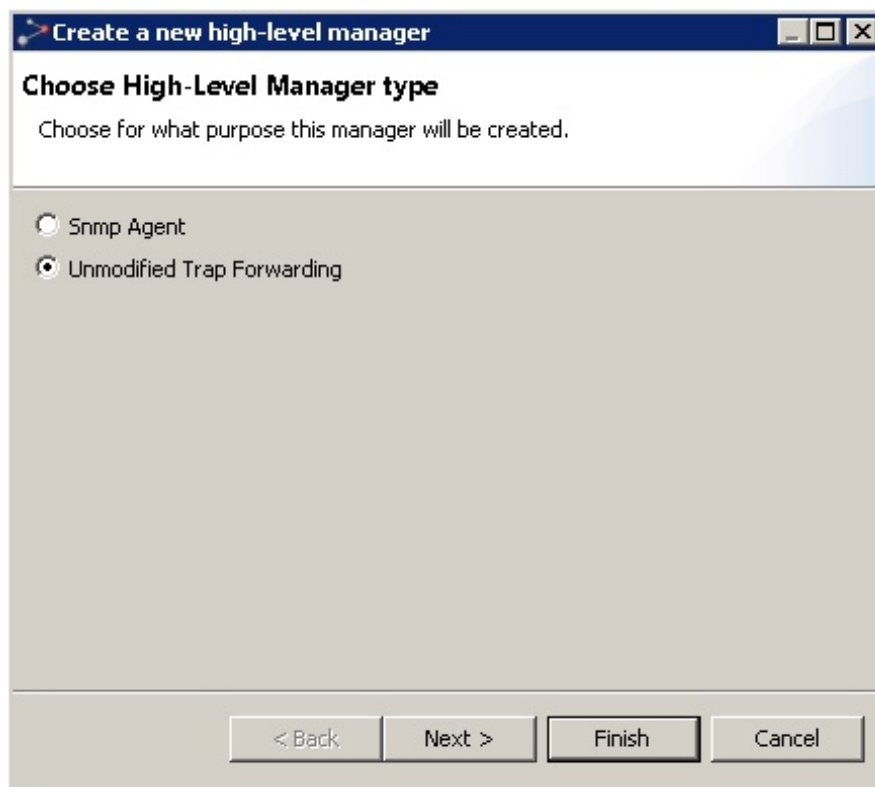
< Back Next > Finish Cancel

Configure the following fields:

- SNMPV3 user: The name of the SNMP v3 user sending the trap. Select from the drop-down list.
- Port: Trap destination port number. Edit as required.

For Unmodified Trap Forwarding:

Figure 161 Unmodified Trap Forwarding



Step 1:

The wizard continues with the following single step:

Figure 162 Create high-level manager

Complete the following fields described below:

- **Name:** A textual description of the manager. Each manager must have a unique name.
- **Address:** The IP address of the manager.
- **Port:** The port used by the manager.
- **Enable trap forwarding:** Check or leave unchecked this box as desired. If you don't enable trap forwarding here, the High Level Manager will be created as defined, and you can enable trap forwarding later.

To enable trap forwarding using SNMP V3:

- Check the Use SNMP V3 (Ensure SNMP V3 settings are completed) checkbox in the PTP 820 NMS Heartbeat Preferences page
- Configure the SNMP V3 settings in the [SNMP V3](#) Preferences pages.

Click **Finish**.

Create an Alarm Forward Configuration

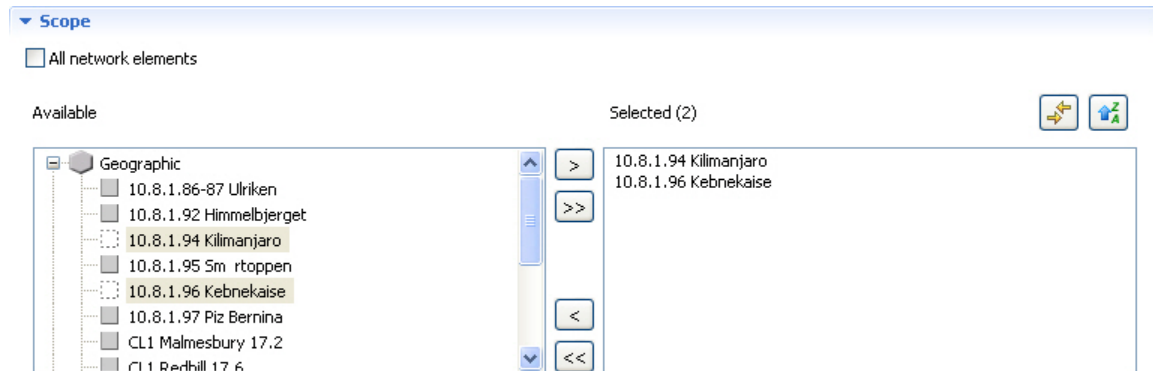
By default, the Alarm Forwarding Configuration is disabled, this means that all alarms from PTP 820 NMS will be sent northbound without any filtering.

In order to enable Alarm Forwarding right-click on the Alarm forwarding configuration node and select Enable,

There are several criteria that can be defined for alarms:

Scope

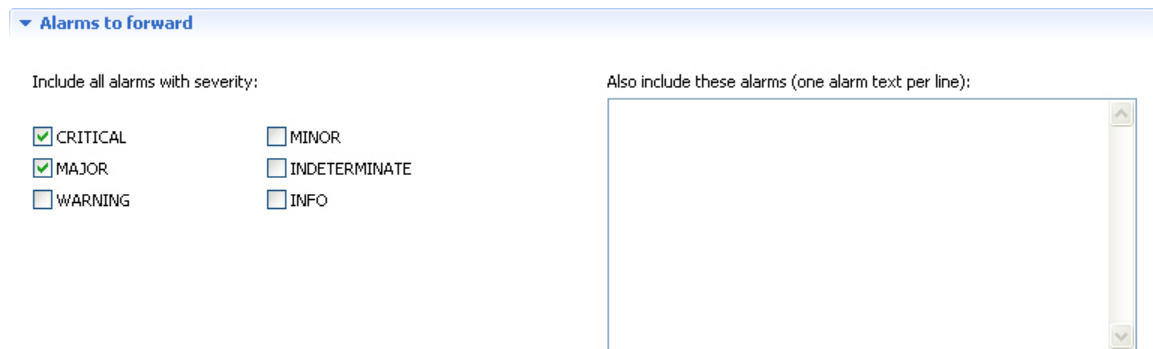
Figure 163 Create an alarm forward view



In this section the network elements that are of interest can be defined, either All network elements or Selected network elements

Alarms to forward

Figure 164 Create an alarm forward configuration



In this section it is possible to limit alarms to be forwarded according to severity. I.e. northbound manager is only interested in Critical and Major alarms.

It is also possible to add specific alarms in addition to the selected severity. When adding alarms specify the whole alarm text for the alarm (alarm name) or use wild cards.

Wild card * can be used to substitute any character.

Alarms to block

Figure 165 Alarms to block

Exclude alarms (one alarm text per line):

Note! These alarms will be blocked regardless of the alarm forwarding settings.

RPS CH2 ACTIVE TX

In this section it is possible to exclude specific alarms from being forwarded. The alarms specified will be block regardless of the other alarm forwarding criteria specified.

When adding alarms specify the whole alarm text for the alarm (alarm name) or use wild cards. Wild card * can be used to substitute any character.

Other options

Figure 166 Other options

☐ Discard toggling alarms

☐ Attach additional information to the alarm to be forwarded

In this section it is possible to specify rules for discarding toggling alarms and to attach additional information to the alarm that is forwarded.

Discard Toggling alarm

Toggling alarms may cause "noise" in the higher level management system and it is possible to discard such alarms by enabling Discard toggling alarms.

When Discard toggling alarms is enabled the delay can be set between 1 and 60 seconds.

Attach additional information

It is possible to add additional information to alarms being forwarded: either free text, or values that maps to the NEs' resource names

This information is added ptp820nms OID of the trap sent to HLM.

Reports

Note: If you are using Internet Explorer 11, some generated reports may appear completely empty. The solution is to add the following lines to the **ngnms.ini** file (located in C:\Program Files (x86)\PTP820NMS\GUI Client):

-Dorg.eclipse.swt.browser.DefaultType=ie

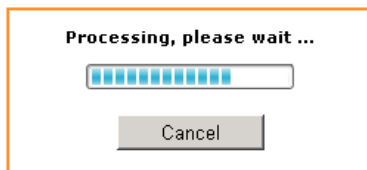
-Dorg.eclipse.swt.browser.IEVersion=7000

Note: The time it takes to generate a report is a function of the number of nodes and resources per node in the network, and might cause a delay if your network is large. The first time a report is requested after the PTP 820 NMS server is started, the report framework is loaded. This initial loading consumes extra resources, but subsequent reports consume less resources and are generated faster.

When generating the reports available from **Views > Reports**, a progress bar is displayed during report generation.

Reports generally contain a header with the report title, the time it was generated and the report scope.

Figure 167 Report view

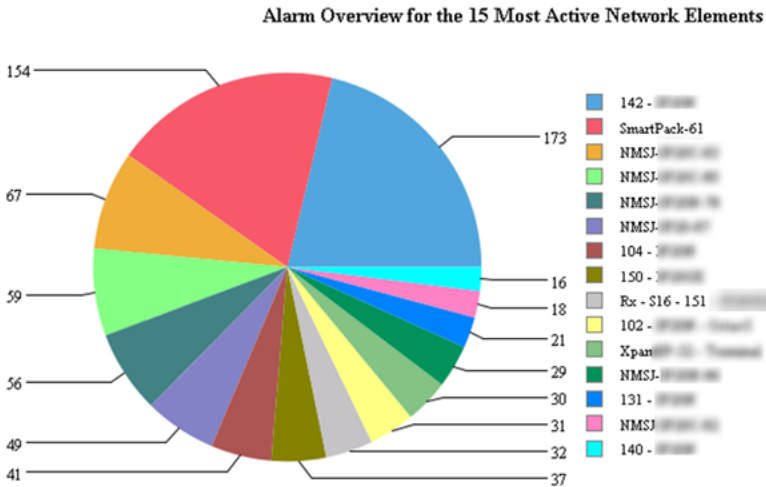


Report Header

The header contains the title of the report and the time that the report was generated.

Alarm Overview chart

Figure 168 Alarm overview chart



The Alarm Overview for Network Elements chart displays the 100 most frequent alarms grouped by Network Element where the total number of occurrences is given as a number associated with each piece of pie. The chart will only display the 15 most active Network Elements; i.e. the elements with most occurrences of alarms.

Example: Network Element A has 3 top 100 most frequent alarms where there are 8 occurrences of each alarm, the element will be displayed as a pie with the value 24.

Network Element B has 1 alarm type among top 100 most frequent alarms, but 20 occurrences. This will be displayed as a pie piece with value 20.

Frequent Alarms list

Figure 169 Frequent alarms list

Listing of Top-100 Most Frequent Alarms Last 7 days sorted by Most Active Network Element

Element: 142 - (Sum alarms: 173)

Resource Name	Alarm Text	Severity	No Of Alarms
142 - (F2000-001) (Bus 1)	Main Board was reset	WARNING	1
142 - (F2000-001) (Bus 1)	Configuration file backup created	WARNING	45
142 - (F2000-001) (Bus 1)	Radio interface is down	WARNING	2
142 - (F2000-001) (Bus 1)	Cable open	MAJOR	2
142 - (F2000-001) (Bus 1)	Card was inserted to slot	WARNING	6
142 - (F2000-001) (Bus 1)	Remote communication failure	CRITICAL	2
142 - (F2000-001) (Bus 1)	Ethernet interface is up	WARNING	3
142 - (F2000-001) (Bus 1)	RFU communication failure	WARNING	4
142 - (F2000-001) (Bus 1)	Configuration file transfer failure	WARNING	36
142 - (F2000-001) (Bus 1)	User issued command for transfer of configuration file	WARNING	46
142 - (F2000-001) (Bus 1)	Loss-of-frames alarm on TDM	MAJOR	2

Table 44 Alarm attributes










Name	Explanation
Resource Name	Source of alarm - the network resource that generated the alarm
Alarm Text	Gives the most likely reason for the alarm
Severity	The alarm severity
No Of Alarms	The number of occurrences of this alarm (i.e. how many times this alarm has been turned on and off)

Table Of Contents pane

The Table Of Contents pane can be opened by pressing the [TOC button](#) on the Alarm Frequency Report grouped by Network Element toolbar.

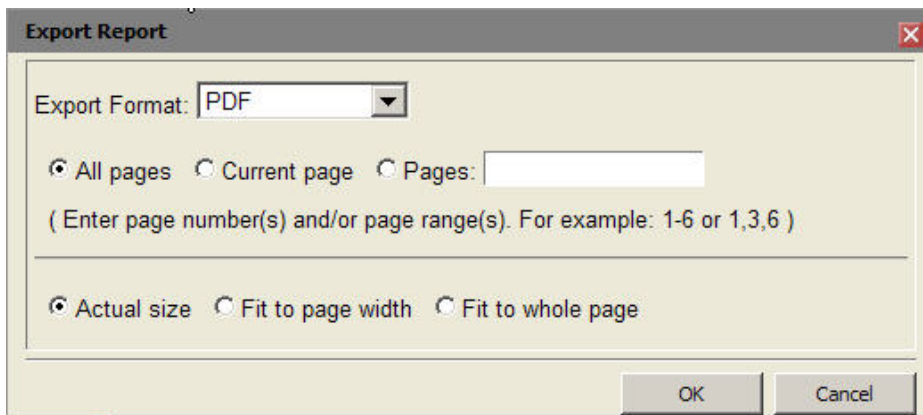
When the Table Of Contents pane is opened, the left hand side of the report contains a section displaying all NEs in the report grouped by NE type. It is possible to expand each NE type and access each specific NE directly by clicking on it.

Available operations

-  TOC button: toggles table of contents
-  Export button: export report to another format, e.g. in order to print it..
-  Navigate to first page
-  Navigate to previous page
-  Navigate to next page
-  Navigate to last page
-  Refresh the entire report
-  **Go to page:**  Navigate to a specific page by specifying a number and then press the green arrow

Export Report dialog

The Export Report dialog is opened by pressing the [Export button](#).

Figure 170 Export report dialog

It is possible to export the reports to external formats in order to store the report or print it. The format of the report will change to the better when displayed in an external format viewer as for example Adobe Reader for PDF-format.

It is recommended to use the external PDF-format before printing the report.

Select Export format from the list and then press the OK button. The report may then be opened by an installed viewer for the chosen format or stored on disk for later processing. If opening the report by an installed viewer on the PTP 820 NMS client, it will be automatically started in a separate window dispatched from the PTP 820 NMS client.

The PTP 820 NMS installation does not include any viewer for the external formats.

NG Performance Reports Generation

Overview

You can instruct PTP 820 NMS to collect network-wide Performance Monitoring (PM) counters information for PTP 820 devices, and then generate various performance reports either through the GUI or using the `pmreport` command line interface (CLI) command. The performance reports can be generated whether the PTP 820 NMS server is running on a Windows or Solaris machine, and are available whether the database is Postgres or Oracle.

The reports display PM counters for all the enabled ports of the specified devices. For 2500SC, the reports display PM counters also for disabled interfaces.

You can generate any of the following types of performance reports:

Performance Report Type	Available for device types
Ethernet Radio Interface Performance report	PTP 820
E1 / DS1 Interface Performance report	PTP 820
STM1 / OC3 Interface Performance report	PTP 820
Radio Performance report	PTP 820

RMON report	PTP 820
Trails Performance report	PTP 820

Reports can be generated for any of the following time periods:

- A 15 minute interval counters report
- A summarized daily report – The cutoff time is 24:00, and the entry with time 24:00 is included
- A summarized weekly report – The cutoff is Saturday at 24:00, and the entry for Saturday at 24:00 is included
- A summarized monthly report – The cutoff is the last day of the month at 24:00, and the entry for the last day of the month at 24:00 is included
 - **Note:** In the generated reports, the time format for midnight is represented by the date of the previous day and the time 24:00. For example: "25-Feb-16 24:00" rather than "26-Feb-16 00:00".
 - Report sizes are limited. If the limit is exceeded, a message is displayed requesting to limit the number of devices or the report time period.
 - For RMON reports, only multiples of 15-minute interval counters are available.

Enabling collection of network-wide PM and RMON counters

A prerequisite to generating performance reports is to enable collection of network-wide counters, as follows:

- To enable collection of PM counters, check the **Enable Network-wide PM Collection** option in the [Network-wide PM Collection](#) Preferences page (you can also optionally change the polling interval).
- To enable collection of RMON counters, check the **Enable RMON Collection** option in the [Network-wide Statistic Counters](#) Preferences page (you can also optionally change the polling interval).
- Restart the PTP 820 NMS server for the **Enabling Collection** instructions to take effect. In a [Server High Availability](#) setup, stop the Secondary server while you enable polling or change the polling interval on the Primary server. After saving the settings on the Primary server, restart the Primary server and then start the Secondary server.
- Set server and devices time: To ensure correct PM counters collection, both the PTP 820 NMS server and the devices being polled must be set to the correct time. You can set the NTP and UTC configuration for PTP 820 devices through the device's connection template. For other device types, set the correct time on the device itself.
- If the PTP 820 NMS client is running on a remote machine, synchronize the UTC time on the remote machine with the UTC time on the PTP 820 NMS server machine.

Generating Performance reports using a CLI command

Once PTP 820 NMS is collecting network-wide performance counters from devices, you can generate various performance reports using the [pmreport](#) CLI command.

The report is generated as soon as the CLI command is given, and saved to the specified location.

Note that report generation using the CLI command can be scheduled by using the operating system (Windows Task Scheduler or Unix Crontab).

Note: Following a PTP 820 NMS server or client installation on a Windows or Solaris machine, you must log off the operating system and log on again for the [pmreport](#) command to work.

pmreport command syntax

The **pmreport** command can be called from any directory on the PTP 820 NMS client or server machine. Its syntax is as follows:

```
pmreport [-IP <IP list>] [-NEType <PTP 820>]-OFN <file name> -RT <report type> [-
PM_TYPE <interface-type>] [-radio_type <radio-interface>] [-SDAY | -WEEK | -
SMONTH] [-SD <date>] [-ED <date>] [-DURATION <n>h|<n>d] [-LAST <n>h|<n>d] [-
SERVERIP <IP>] -USER <user-name> -PASSWORD <password> [-FILTER <minimum
threshold> | -FFILTER <logical expression>] [-Delta] [-Group <domain-name>][-
noheaders] [-timestamp|timestamp D|timestamp M]
```

where:

Parameter	Format	Mandatory/Optional	Description
IP	-IP <IP> <IP> Or -IP ALL	O, if omitted the default parameter is "ALL"	<p>The IP addresses, separated by spaces, of the target devices. For example: -IP 172.24.30.100 172.24.30.101</p> <p>For PTP 820 devices, you can specify the IP address in either IPv4 or IPv6 format. Use the same format used to <u>Discover</u> the device..</p> <p>When specifying an IPv6 address, you can use any of the following representations:</p> <ul style="list-style-type: none"> • The full representation of 8 groups of 4 hexadecimal digits, separated by colons. For example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334 • Omitting leading zeros in groups. In this case, the above example address would be entered as: 2001:db8:85a3:0:0:8a2e:370:7334 • If the address contains chains of consecutive zero groups (a zero-group is a groups whose 4 digits are zero) – Replacing a chain of zero-groups with a double colon, with the following stipulations: <ul style="list-style-type: none"> • Only one double colon per address. • The longest zero-groups chain is replaced with a double colon. • If there is more than one longest zero-groups chain, the leftmost one is replaced with a double colon. <p>Use -IP ALL to generate a report for all devices in the database.</p>

			<p>Note: When using ALL, it is recommended to specify a limited time interval using -SD and -ED. The data for the entire network can reach a considerable size if not limited to a specific time period.</p>
NEType	-NEType <PTP 820>	O	<p>Enables you to limit the report to PTP 820 elements only. For example:</p> <p>-NEType PTP820</p> <p>Note : You can still provide a list of IPs. The report will be generated for all the specified IPs that match the device type.</p>
OFN	-OFN <filepath\name.ext>	M	<p>The output file name and path. If the extension is .txt, the file will be saved in text format. If the extension is .csv, the file will be saved in CSV format.</p> <p>If the filepath is not specified, the report will be placed in the folder from which the command pmreport was executed.</p> <p>Note: Make sure you have full permissions to the specified folder. Otherwise, no report is created or saved.</p>
RT	-RT <report-type>	M	<p>The report type. This can be set to any of the following (including the quote marks):</p> <p>"Interface Performance Report"</p> <p>"Radio Performance Report"</p> <p>"RMON Report"</p> <p>"Trails Performance Report"</p> <p>"Enhanced Radio Performance Report"</p> <p>"Enhanced Radio Ethernet Performance Report"</p>
PM_TYPE	-PM_TYPE <interface-type>	O	<p>For which type of interface to generate an Interface Performance report. The options are:</p> <ul style="list-style-type: none"> • E1 • T1 • STM1 • OC3 • ETHERNET_RADIO <p>Note that the interface type must be entered in capital letters.</p> <p>This parameter is relevant only for Interface Performance reports.</p> <p>If this parameter is not included in the CLI command when the report type (RT) is</p>

			set to "Interface Performance Report", a report is generated for all interfaces (E1, DS1, STM1, OC3, Radio Ethernet) that are present on the devices included in the report.
radio_type	-radio_type <radio-interface>	O	<p>Generate a separate Radio Performance Report for different radio interfaces. The options are:</p> <p>RADIO - Radio port</p> <p>RUAS - Radio channels</p> <p>This parameter is relevant only for Radio Performance reports.</p>
SDAY	-SDAY	O	<p>Generate a summarized daily report.</p> <p>If neither SDAY nor SWEET nor SMONTH is specified, a 15-minute-interval counters report is produced.</p> <p>This option is not relevant for RMON counter reports.</p>
SWEEK	-SWEET	O	<p>Generate a summarized weekly report.</p> <p>If neither SDAY nor SWEET nor SMONTH is specified, a 15-minute-interval counters report is produced.</p> <p>This option is not relevant for RMON counter reports.</p>
SMONTH	-SMONTH	O	<p>Generate a summarized monthly report.</p> <p>If neither SDAY nor SWEET nor SMONTH is specified, a 15-minute-interval counters report is produced.</p> <p>This option is not relevant for RMON counter reports.</p>
SD	-SD "dd/MM/yy HH:mm"	O	<p>Start date and time for the report.</p> <p>For example:</p> <p>-SD "17/05/15 12:00"</p>
ED	-ED "dd/MM/yy HH:mm"	O	<p>End date and time for the report.</p> <p>For example:</p> <p>-ED "18/05/15 23:59"</p>
DURATION	-DURATION <n>h <n>d	O	<p>As an alternative to setting the start date and end date of the report, you can define to include in the report only the PMs from a specific numbers of hours or days prior to</p>

			<p>the time of command execution. For example:</p> <p>-DURATION 12h</p> <p>In this case, the report will include the PMs from the 12 hours prior to command execution.</p>
LAST	-LAST [<n>h <n>d]	O	<p>As an alternative to setting the start date and end date of the report, you can define to include in the report only the PMs from a specific number of FULL hours or days prior to the time of command execution. For example:</p> <p>-LAST 1d</p> <p>The report will include the PMs from the last 1 day - from 00:01 to 24:00.</p> <p>-LAST 3h The report will include the PMs from the last 3 hours. If the command is executed at 10:59 the report will include PMs from 07:15 to 10:00.</p>
SERVERIP	-SERVERIP <IP>	O, if omitted the default value is "localhost"	<p>The PTP 820 NMS server IP address, which must be provided if you are generating a report from the PTP 820 NMS client rather than the PTP 820 NMS server machine.</p> <p>If not provided, -SERVERIP LOCALHOST is the default setting.</p>
USER	-USER	M	<p>The name of the user with read access to the target devices. Make sure to specify an active user with a valid password.</p>
PASSWORD	-PASSWORD	M	<p>The password of the user with read access to the target devices.</p>
FILTER	-FILTER <minimum threshold>	O	<p>Filter the report by a minimum threshold. Only fields that exceed the specified value are presented.</p> <p>For example: -FILTER 0 specifies not to show zero value fields.</p> <p>Note:</p> <ul style="list-style-type: none"> You cannot use both FILTER and FFILTER in the same command. FILTER can be used only once in a command.

			if you employ filtering and no counter values match the filter, the report will display empty tables.
FFILTER	-FFILTER "<field-name><operator><value> <boolean-op> <field-name><operator><value> <boolean op> <field-name><operator><value> --- "	O	<p>Filter the report by a logical expression. Each part of the expression is composed of:</p> <ul style="list-style-type: none"> < field name> - a field name as it appears in the column header: For example, "Frame Error Rate". Note that field names which include spaces must be enclosed in quotes. <operator> - any of the following: > >= < <= = <> <value> - a number <p>While: <Boolean op> - one of the following boolean operators between two parts of the expression.</p> <ul style="list-style-type: none"> Use: for OR, Use: & for AND <p>Syntax considerations:</p> <ul style="list-style-type: none"> Replace any spaces in column names with underscores. <p>Note:</p> <ul style="list-style-type: none"> You cannot use both FILTER and FFILTER in the same command. FFILTER can be used only once in a command. The filtering instructions are performed in the order in which they are listed, from left to right. Percentage fields cannot be filtered. If the same field name appears in PTP 820 reports but the units differ, then filtering cannot work for both. <p>if you employ filtering and no counter values match the filter, the report will display empty tables.</p>
Delta	-DELTA	O	<p>Display the difference between counter readings in the report, rather than the actual counter value.</p> <p>This option is available for RMON counter reports only.</p>

Group	-Group <domain-name>	O	Generate a report only for the devices in the specified domain and its subdomains.
noheaders	-noheaders	O	<p>Generate Interface Performance reports in a single table, without titles. This facilitates parsing of the Interface Performance report. The titles are replaced by the following columns which are added to the table:</p> <ul style="list-style-type: none"> • IP • System Name • Slot Number • Interface <p>This option is available only for Interface Performance reports, and only if you use the -pm_type parameter to specify a single interface.</p>
timestamp	-timestamp or -timestamp D or -timestamp M	O	<p>Add a timestamp to the report filename.</p> <ul style="list-style-type: none"> • If you specify -timestamp or -timestamp D, then the filename will have the following format: <filename>_DDMMYYYY_HH_MM_SS.<extension> <p>If you specify -timestamp M, then the filename will have the following format: <filename>_MMDDYYYY_HH_MM_SS.<extension></p>

Note: The parameters are not case sensitive, except where noted otherwise.

pmreport CLI command - examples

The following are examples of commands for generating Ethernet Radio Interface Performance reports:

```
pmreport -IP 172.24.30.100 172.24.30.101 -OFN C:\Temp\report\test1 -RT "Interface Performance Report" -pm_type ETHERNET_RADIO -SD "17/05/15 12:00" -ED "18/05/15 23:59" -USER admin -PASSWORD NmsSystem1 -FILTER 0

pmreport -IP 2001:db8:85a3:0:0:8a2e:370:7334 -OFN C:\Temp\report\test1 -RT "Interface Performance Report" -pm_type ETHERNET_RADIO -SD "17/05/15 12:00" -ED "18/05/15 23:59" -USER admin -PASSWORD NmsSystem1 -FILTER 0

pmreport -IP ALL -OFN C:\Temp\report\test2 -RT "Interface Performance Report" -pm_type ETHERNET_RADIO -SMONTH -SD "17/05/15 12:00" -ED "18/05/15 23:59" -SERVERIP 172.24.30.1 -USER admin -PASSWORD NmsSystem1 -FFILTER "Peak_Capacity>10&Average_Throughput>30|Average_Capacity>25"
```

The following is an example of a command for generating an Interface Performance report with no headers:

```
pmreport -CLI -IP all -OFN "C:\noheadersPMReport.csv" -RT "Interface Performance Report" -USER admin -PASSWORD NmsSystem1 -pm_type ETHERNET_RADIO -noheaders
```

The following is an example of a command for generating an OC3 Interface Performance report:

```
pmreport -IP 10.10.68.107 -OFN output.csv -RT "Interface Performance Report" -pm_type OC3 -USER admin -PASSWORD NmsSystem1
```

The following is an example of a command for generating a RMON Performance report that will display the difference between counter readings in the report, rather than the actual counter value:

```
pmreport -IP 10.10.68.107 -OFN output.csv -RT "RMON Report" -user admin -password NmsSystem1 -DELTA
```

The following is an example of a command for generating a Trails Performance report:

```
pmreport -IP 10.10.68.107 -OFN output.csv -RT "Trails Performance Report" -user admin -password NmsSystem1
```

The following are examples of commands for generating a Radio Performance report:

```
pmreport -IP 172.24.30.100 172.24.30.101 -OFN C:\Temp\report\test1 -RT "Radio Performance Report" -SD "17/05/15 12:00" -ED "18/05/15 23:59" -USER admin -PASSWORD NmsSystem1 -FILTER 0
```

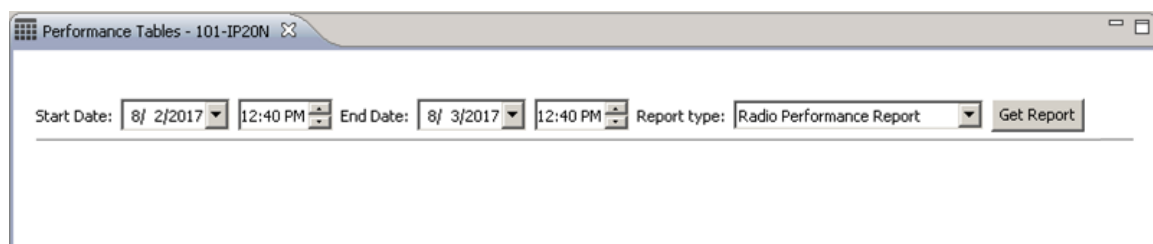
```
pmreport -IP ALL -OFN C:\Temp\report\test2 -RT "Radio Performance Report" -SMONTH -SD "17/05/15 12:00" -ED "18/05/15 23:59" -SERVERIP 172.24.30.1 -USER admin -PASSWORD NmsSystem1 -FFILTER "Min_RSL>10&Max_RSL>30"
```

```
pmreport -OFN output.csv -IP 10.10.68.107 -user admin -password NmsSystem1 -RT "Radio Performance Report" -radio_type RUAS
```

Generating Performance reports via the GUI

Once PTP 820 NMS is collecting network-wide PM counters for devices, you can generate various performance reports through the GUI.

- 1 Right click an PTP 820 device in the GUI display (for example in a navigation tree or a topology view).
- 2 Select **Performance > Performance Tables**.
The **Performance Tables** view appears.



- 3 In the **Start Date** and **End Date** fields, enter desired dates. The default dates are for the past 24 hours.
- 4 In the **Report Type** field, select the report type.
- 5 Click **Get Report**. The report appears on screen.

The screenshot shows a web-based report generation interface. At the top, there are input fields for 'Start Date' (8/ 2/2017), 'End Date' (8/ 3/2017), and 'Report type' (Radio Performance Report). A 'Get Report' button is to the right. Below these are dropdowns for 'Interfaces' (Slot 3 Radio), 'Format' (15-Minute Report), and 'Table Options'. The main area displays a table with the following data:

Date	IP	UAS	ES	SES	BBE	Min RSL	Max RSL
03-Aug-17 11:30	10.10.68.109	0	0	0	0	-49	-49
03-Aug-17 11:15	10.10.68.109	0	0	0	0	-49	-49
03-Aug-17 11:00	10.10.68.109	0	0	0	0	-49	-49
03-Aug-17 10:45	10.10.68.109	0	0	0	0	-49	-49
03-Aug-17 10:30	10.10.68.109	0	0	0	0	-49	-49
03-Aug-17 10:15	10.10.68.109	0	0	0	0	-49	-49
03-Aug-17 10:00	10.10.68.109	0	0	0	0	-49	-49
03-Aug-17 09:45	10.10.68.109	0	0	0	0	-49	-49
03-Aug-17 09:30	10.10.68.109	0	0	0	0	-49	-49
03-Aug-17 09:15	10.10.68.109	0	0	0	0	-49	-49
03-Aug-17 09:00	10.10.68.109	0	0	0	0	-49	-49
03-Aug-17 08:45	10.10.68.109	0	0	0	0	-49	-49
03-Aug-17 08:30	10.10.68.109	0	0	0	0	-49	-49
03-Aug-17 08:15	10.10.68.109	0	0	0	0	-49	-49

- 6 In the **Format** field, select one of the following:
 - 15-minute Report
 - Daily Report
 - Weekly Report
 - Monthly Report

Note that this field does not exist for RMON reports.
- 7 In the **Interfaces** dropdown, select for which interface to show the report.
- 8 Click **Table Options** > **Customize Columns** to select which columns to display.
- 9 Click **Table Options** > **Export to File** to export the report to a file.

You can sort the report by clicking any of the columns.

Generating an Interface Performance Report

You can generate the following types of Interface Performance reports:

- [Ethernet Radio](#)
- [E1](#)
- [DS1](#)
- [STM1](#)
- [OC3](#)
- [XC Carrier](#)

Generating an Ethernet Radio Interface Performance report

- To generate the report via CLI, refer to [Generating Performance reports using a CLI command](#).

- To generate the report using the GUI, refer to [Generating Performance reports via the GUI](#).

Viewing an Ethernet Radio Interface Performance report

The following is an example of a 15 minute Ethernet Radio interface performance report:

Start Date: End Date: Report type:

Interfaces: Format:

Date	IP	Frame Error Rate ...	Peak Throughput	Average Through...	Throughput Exce...	Peak Capacity	Average Capacity
03-Aug-17 11:30	10.10.68.109	0	0 Mbps	0 Mbps	0	0 Mbps	0 Mbps
03-Aug-17 11:15	10.10.68.109	0	0 Mbps	0 Mbps	0	0 Mbps	0 Mbps
03-Aug-17 11:00	10.10.68.109	0	0 Mbps	0 Mbps	0	0 Mbps	0 Mbps
03-Aug-17 10:45	10.10.68.109	0	0 Mbps	0 Mbps	0	0 Mbps	0 Mbps
03-Aug-17 10:30	10.10.68.109	0	0 Mbps	0 Mbps	0	0 Mbps	0 Mbps
03-Aug-17 10:15	10.10.68.109	0	0 Mbps	0 Mbps	0	0 Mbps	0 Mbps
03-Aug-17 10:00	10.10.68.109	0	0 Mbps	0 Mbps	0	0 Mbps	0 Mbps
03-Aug-17 09:45	10.10.68.109	0	0 Mbps	0 Mbps	0	0 Mbps	0 Mbps
03-Aug-17 09:30	10.10.68.109	0	0 Mbps	0 Mbps	0	0 Mbps	0 Mbps
03-Aug-17 09:15	10.10.68.109	0	0 Mbps	0 Mbps	0	0 Mbps	0 Mbps
03-Aug-17 09:00	10.10.68.109	0	0 Mbps	0 Mbps	0	0 Mbps	0 Mbps
03-Aug-17 08:45	10.10.68.109	0	0 Mbps	0 Mbps	0	0 Mbps	0 Mbps
03-Aug-17 08:30	10.10.68.109	0	0 Mbps	0 Mbps	0	0 Mbps	0 Mbps
03-Aug-17 08:15	10.10.68.109	0	0 Mbps	0 Mbps	0	0 Mbps	0 Mbps

All Ethernet Radio interface performance reports contain the same PM counters. However, the 15-minute report displays the actual values obtained at each 15-minute reading, while the summarized reports display a summary of the daily, weekly, or monthly values, calculated as follows:

Counter	Value in Summary Report
Frame Error Rate (%)	Maximum of the entries
Peak Throughput	Maximum of the entries
Average Throughput	Average of the entries
Throughput Exceeded (seconds)	Sum of the entries
Peak Capacity	Maximum of the entries
Average Capacity	Average of the entries
Capacity Exceeded (seconds)	Sum of the entries
Peak Utilization	Maximum of the entries
Average Utilization	Average of the entries
Seconds Exceeding Threshold	Sum of the entries

Generating an E1 / DS1 Interface Performance report

- To generate the report via CLI, refer to [Generating Performance reports using a CLI command](#).
- To generate the report using the GUI, refer to [Generating Performance reports via the GUI](#).

Viewing an E1 / DS1 Interface Performance report

The following is an example of a 15 minute E1 interface performance report:

Start Date: 8/ 2/2017 12:49 PM End Date: 8/ 3/2017 12:49 PM Report type: Interface Performance Report Get Report

Interfaces: [Slot 1] E1 #1 Format: 15-Minute Report Table Options

Date	IP	UAS	ES	SES	BBE	Integrity
03-Aug-17 03:15	10.10.68.98	900	0	0	0	Yes
02-Aug-17 21:00	10.10.68.98	900	0	0	0	Yes
02-Aug-17 20:45	10.10.68.98	900	0	0	0	Yes
02-Aug-17 20:30	10.10.68.98	900	0	0	0	Yes
02-Aug-17 20:15	10.10.68.98	900	0	0	0	Yes
02-Aug-17 20:00	10.10.68.98	900	0	0	0	Yes
02-Aug-17 19:45	10.10.68.98	900	0	0	0	Yes
02-Aug-17 19:30	10.10.68.98	900	0	0	0	Yes
02-Aug-17 19:15	10.10.68.98	900	0	0	0	Yes
02-Aug-17 19:00	10.10.68.98	900	0	0	0	Yes
02-Aug-17 18:45	10.10.68.98	900	0	0	0	Yes
02-Aug-17 18:30	10.10.68.98	900	0	0	0	Yes
02-Aug-17 18:15	10.10.68.98	900	0	0	0	Yes
02-Aug-17 18:00	10.10.68.98	900	0	0	0	Yes
02-Aug-17 17:45	10.10.68.98	900	0	0	0	Yes

All E1/DS1 interface performance reports contain the same PM counters. However, the 15-minute report displays the actual values obtained at each 15-minute reading, while the summarized reports display a summary of the daily, weekly, or monthly values, calculated as follows:

Counter	Value in Summary
UAS	Sum of the entries
ES	Sum of the entries
SES	Sum of the entries
BBE - (set to zero for PTP 820 interfaces)	Sum of the entries

Generating an STM1 / OC3 Interface Performance report

- To generate the report via CLI, refer to [Generating Performance reports using a CLI command](#).
- To generate the report using the GUI, refer to [Generating Performance reports via the GUI](#).

Viewing an STM1 / OC3 Interface Performance report

The following is an example of a 15 minute OC3 interface performance report:

Start Date: 8/ 2/2017 12:51 PM End Date: 8/ 3/2017 12:51 PM Report type: Interface Performance Report

Interfaces: [Slot 1] STM-1 #1 Format: 15-Minute Report Table Options

Date	IP	ES	SES	EB	BBE	Integrity
03-Aug-17 12:45	10.10.67.135	0	0	0	0	Yes
03-Aug-17 12:30	10.10.67.135	0	0	0	0	Yes
03-Aug-17 12:15	10.10.67.135	0	0	0	0	Yes
03-Aug-17 12:00	10.10.67.135	0	0	0	0	Yes
03-Aug-17 11:45	10.10.67.135	0	0	0	0	Yes
03-Aug-17 11:30	10.10.67.135	0	0	0	0	Yes
03-Aug-17 11:15	10.10.67.135	0	0	0	0	Yes
03-Aug-17 11:00	10.10.67.135	0	0	0	0	Yes
03-Aug-17 10:45	10.10.67.135	0	0	0	0	Yes
03-Aug-17 10:30	10.10.67.135	0	0	0	0	Yes
03-Aug-17 10:15	10.10.67.135	0	0	0	0	Yes
03-Aug-17 10:00	10.10.67.135	0	0	0	0	Yes
03-Aug-17 09:45	10.10.67.135	0	0	0	0	Yes
03-Aug-17 09:30	10.10.67.135	0	0	0	0	Yes
03-Aug-17 09:15	10.10.67.135	0	0	0	0	Yes

The 15-minute STM1/OC3 report displays the actual values obtained at each 15-minute reading, while the summarized reports display a summary of the daily, weekly, or monthly values, calculated as follows:

Counter	Value in Summary
UAS	Sum of the entries
ES	Sum of the entries
SES	Sum of the entries
EB	Sum of the entries
BBE	Sum of the entries
CV	Sum of the entries

Generating an XC Carrier Interface Performance report

- To generate the report via CLI, refer to [Generating Performance reports using a CLI command](#).
- To generate the report using the GUI, refer to [Generating Performance reports via the GUI](#).

Generating a Radio Performance report

- To generate the report via CLI, refer to [Generating Performance reports using a CLI command](#).
- To generate the report using the GUI, refer to [Generating Performance reports via the GUI](#).
- The following is an example of a 15 minute Radio Performance report:

Start Date: 8/ 2/2017 12:51 PM End Date: 8/ 3/2017 12:51 PM Report type: Radio Performance Report

Interfaces: [Slot 1] Radio #1 Format: 15-Minute Report Table Options

Date	IP	UAS	ES	SES	BBE	Min RSL	Max RSL
03-Aug-17 12:45	10.10.67.135	0	0	0	0	-15	-99
03-Aug-17 12:30	10.10.67.135	0	0	0	0	-15	-99
03-Aug-17 12:15	10.10.67.135	0	0	0	0	-15	-99
03-Aug-17 12:00	10.10.67.135	0	0	0	0	-15	-99
03-Aug-17 11:45	10.10.67.135	0	0	0	0	-15	-99
03-Aug-17 11:30	10.10.67.135	0	0	0	0	-15	-99
03-Aug-17 11:15	10.10.67.135	0	0	0	0	-15	-99
03-Aug-17 11:00	10.10.67.135	0	0	0	0	-15	-99
03-Aug-17 10:45	10.10.67.135	0	0	0	0	-15	-99
03-Aug-17 10:30	10.10.67.135	0	0	0	0	-15	-99
03-Aug-17 10:15	10.10.67.135	0	0	0	0	-15	-99
03-Aug-17 10:00	10.10.67.135	0	0	0	0	-15	-99
03-Aug-17 09:45	10.10.67.135	0	0	0	0	-15	-99
03-Aug-17 09:30	10.10.67.135	0	0	0	0	-15	-99

- The 15-minute report displays the actual values obtained at each 15-minute reading, while the summarized reports display a summary of the daily, weekly, or monthly values, calculated as follows:

Counter	Value in Summary Report
UAS	Sum of the entries
ES	Sum of the entries
SES	Sum of the entries
BBE	Sum of the entries
Min RSL	Minimum of the entries
Max RSL	Maximum of the entries
RSL Thresh 1	Sum of the entries
RSL Thresh 2	Sum of the entries
Min TSL	Minimum of the entries
Max TSL	Maximum of the entries
TSL Thresh	Sum of the entries
Green %	Minimum of the entries
Lowest ACM Profile	Lowest of the entries
Highest ACM Profile	Highest of the entries
Lowest Bitrate (Kbps)	Lowest of the entries
Highest Bitrate (Kbps)	Highest of the entries
Lowest Number of TDM interfaces	Lowest of the entries
Highest Number of TDM Interfaces	Highest of the entries
Min MSE (dB)	Minimum of the entries

Max MSE (dB)	Maximum of the entries
MSE Threshold Exceeded (seconds)	Sum of the entries
Min XPI (dB)	Minimum of the entries
Max XPI (dB)	Maximum of the entries
Excessive XPI (seconds)	Sum of the entries

Generating a RMON report

- To generate the report via CLI, refer to [Generating Performance reports using a CLI command](#).
- To generate the report using the GUI, refer to [Generating Performance reports via the GUI](#).

Viewing a RMON report

The following is an example of a 60 minute RMON performance report:

Start Date:	9/13/2017	5:16 PM	End Date:	9/14/2017	5:16 PM	Report type:	RMON Report	Get Report
Interfaces:	[Slot 2] Radio Ethernet #1	Table Options						
Date	IP	TX BytCnt (octets)	TX Unicst (packe...	TX Mlticst (pack...	TX Brdcst (packe...	TX Pause (packe...	TX FcsErr (packe...	
14-Sep-17 17:01	10.10.67.176	78088704	152517	0	0	0	0	
14-Sep-17 16:46	10.10.67.176	78088704	152517	0	0	0	0	
14-Sep-17 16:31	10.10.67.176	78088704	152517	0	0	0	0	
14-Sep-17 16:16	10.10.67.176	78088704	152517	0	0	0	0	
14-Sep-17 16:01	10.10.67.176	78088704	152517	0	0	0	0	
14-Sep-17 15:46	10.10.67.176	78088704	152517	0	0	0	0	
14-Sep-17 15:31	10.10.67.176	78088704	152517	0	0	0	0	
14-Sep-17 15:16	10.10.67.176	78088704	152517	0	0	0	0	
14-Sep-17 15:01	10.10.67.176	78088704	152517	0	0	0	0	
14-Sep-17 14:46	10.10.67.176	78088704	152517	0	0	0	0	
14-Sep-17 14:31	10.10.67.176	78088704	152517	0	0	0	0	
14-Sep-17 14:16	10.10.67.176	78088704	152517	0	0	0	0	
14-Sep-17 14:01	10.10.67.176	78088704	152517	0	0	0	0	
14-Sep-17 13:46	10.10.67.176	78088704	152517	0	0	0	0	

Note that summarized reports are not available for RMON counters.

The RMON counters displayed for PTP 820 devices include:

Name of Column	Description	Units
TX BytCnt	TX byte count	Octets
TX FrCnt	TX frame count	packets
TX Mlticst	TX multicast frame count	packets
TX Brdcst	TX broadcast frame count	packets
TX Cntrl	TX control frame count	packets
TX Pause	TX pause frame count	packets

TX FcsErr	TX fcs error frame count	packets
TX LngErr	TX length error frame count	packets
TX OverSz	TX oversize frame count	packets
TX UnderSz	TX undersize frame count	packets
TX Frag	TX fragment frame count	packets
TX Jabber	TX jabber frame count	packets
TX 64	TX 64 frame count	packets
TX 65-127	TX 65-127 frame count	packets
TX 128-255	TX 128-255 frame count	packets
TX 256-511	TX 256-511 frame count	packets
TX 512-1023	TX 512-1023 frame count	packets
TX 1024-1518	TX 1024-1518 frame count	packets
TX 1519-1522	TX 1519-1522 frame count	packets
RX BytCnt	RX byte count	Octets
RX FrCnt	RX frame count	packets
RX Mltcst	RX multicast frame count	packets
RX Brdcst	RX broadcast frame count	packets
RX Cntrl	RX control frame count	packets
RX Pause	RX pause frame count	packets
RX FcsErr	RX fcs error frame count	packets
RX LngErr	RX length error frame count	packets
RX CodeErr	RX code error count	errors
RX OverSz	RX oversize frame count	packets
RX UnderSz	RX undersize frame count	packets
RX Frag	RX fragment frame count	packets
RX Jabber	RX jabber frame count	packets
RX 64	RX 64 frame count	packets
RX 65-127	TX 65-127 frame count	packets
RX 128-255	TX 128-255 frame count	packets
RX 256-511	TX 256-511 frame count	packets
RX 512-1023	TX 512-1023 frame count	packets

RX 1024-1518	TX 1024-1518 frame count	packets
RX 1519-1522	TX 1519-1522 frame count	packets
RX ExcMax	RX exceed max frame count	packets
RX ExcMaxwErr	RX exceed max with error frame count	packets

Generating an Enhanced Radio Performance report

The Enhanced Radio Performance report can only be generated using the CLI,

- To generate the report via CLI, refer to [Generating Performance reports using a CLI command](#).

Viewing an Enhanced Radio Performance report

The following is an example of a 15 minute enhanced radio performance report:

Enhanced Radio Performance Report - R5-S2-114 (10.10.67.114) [Slot 1]								
15-Minute Report								
Radio #1								
Report Save Time: 2017-09-05 15:14:28								
Date	IP	UAS	ES	SES	BBE	Min RSL	Max RSL	Integrity
05-Sep-17 15:00	10.10.67.114	0	0	0	0	-55	-54	Yes
05-Sep-17 14:45	10.10.67.114	0	0	0	0	-55	-54	Yes
05-Sep-17 14:30	10.10.67.114	0	0	0	0	-55	-54	Yes
05-Sep-17 14:15	10.10.67.114	0	0	0	0	-56	-54	Yes
05-Sep-17 14:00	10.10.67.114	0	0	0	0	-55	-54	Yes
05-Sep-17 13:45	10.10.67.114	0	0	0	0	-56	-54	Yes
05-Sep-17 13:30	10.10.67.114	0	0	0	0	-56	-54	Yes
05-Sep-17 13:15	10.10.67.114	0	0	0	0	-56	-54	Yes
05-Sep-17 13:00	10.10.67.114	0	0	0	0	-55	-54	Yes
05-Sep-17 12:45	10.10.67.114	0	0	0	0	-56	-54	Yes

The 15-minute report displays the actual values obtained at each 15-minute reading, while the summarized reports display a summary of the daily, weekly, or monthly values, calculated as follows:

Counter	Value in Summary Report
UAS	Sum of the entries
ES	Sum of the entries
SES	Sum of the entries
BBE	Sum of the entries
Min RSL	Minimum of the entries

Max RSL	Maximum of the entries
---------	------------------------

Generating a TDM Trails Performance report

- To generate the report via CLI, refer to [Generating Performance reports using a CLI command](#).
- To generate the report using the GUI, refer to [Generating Performance reports via the GUI](#).

Viewing a TDM Trail report

The following is an example of a 15 minute TDM Trails performance report:

Start Date: End Date: Report type:

Interfaces: Format:

Date	IP	UAS	ES	SES	BBE	Number Of Switches	Active Path Count
03-Aug-17 12:45	10.10.67.135	0	0	0	0	0	900
03-Aug-17 12:30	10.10.67.135	0	0	0	0	0	900
03-Aug-17 12:15	10.10.67.135	0	0	0	0	0	900
03-Aug-17 12:00	10.10.67.135	0	0	0	0	0	900
03-Aug-17 11:45	10.10.67.135	0	0	0	0	0	900
03-Aug-17 11:30	10.10.67.135	0	0	0	0	0	900
03-Aug-17 11:15	10.10.67.135	0	0	0	0	0	900
03-Aug-17 11:00	10.10.67.135	0	0	0	0	0	900
03-Aug-17 10:45	10.10.67.135	0	0	0	0	0	900
03-Aug-17 10:30	10.10.67.135	0	0	0	0	0	900
03-Aug-17 10:15	10.10.67.135	0	0	0	0	0	900
03-Aug-17 10:00	10.10.67.135	0	0	0	0	0	900
03-Aug-17 09:45	10.10.67.135	0	0	0	0	0	900
03-Aug-17 09:30	10.10.67.135	0	0	0	0	0	900

The TDM Trails report applies to TDM Trails on PTP 820 devices.

The counters are collected only at the TDM Service Points, whether they are service endpoints or on the path of the service.

The following TDM service fragments are included in this report:

- TDM to Radio cross-connection points.
- TDM to TDM Cross-Connects.
- TDM to 2 Radio Cross-Connects, for Trails with protection.
- Radio to 2 Radios Cross-Connects, for Trails with protection, where the protection begins at a mid-point on the trail.
- TDM to 1 TDM and 1 Radio Cross-Connects, for Trails with protection where one network path is going over an STM-1 link (User link), while the other path is over the radio.

Reports are supported only for service configurations that can be created by PTP 820 NMS.

All discovered services on PTP 820 equipment appear in the report. Note that the services need not be confirmed, discovery alone is sufficient. PTP 820 NMS generates a report for all trails that are in its database, regardless of the state of the trail (confirmed or unconfirmed).

If there is no PM data in the database for a trail, that trail does not appear in the report.

For each port on the path of the service, the following counters are displayed.

Counter	Explanation
UAS	Radio performance counters
ES	
SES	
BBE Note: On the PTP 820, the BBE field is called FC but in the report the column is always labeled BBE	
Number of Switches	When there is no protection and/or for PTP 820 devices, this value is zero.
Active Path Count	When there is no protection and/or for PTP 820 devices, this value is set to either 0 (no service) or 900 (full service).

Note: In the case of an STM-1 Group, the counters are gathered per each physical slot, separately.

The report will contain two tables and you must check which is the active card.

NG Inventory Reports Generation

You can instruct PTP 820 NMS to generate various inventory reports either through the GUI or using the [inreport](#) command line interface (CLI) command. The inventory reports can be generated whether the PTP 820 NMS server is running on a Windows or Solaris machine, and are available whether the database is Postgres or Oracle.

Note that report generation using the CLI command can be scheduled by using the operating system (Windows Task Scheduler or Unix Crontab).

You can generate any of the following types of inventory reports:

Inventory Report Type	Available for device types
Frequency Change Report	PTP 820
Full Link Report	PTP 820
Network Element Report	All managed devices
Radio Report	PTP 820
Link report	PTP 820
Licensing Report	PTP 820
Versions Report	PTP 820
Serial Numbers Report	PTP 820

Note that in all inventory reports, if a field is not relevant for a particular device, the report displays **N/A** (Not Applicable) for that field.

Generating Inventory reports using a CLI command

The report is generated as soon as the CLI command is given, and saved to the specified location.

inreport command syntax

The **inreport** command can be called from any directory on the PTP 820 NMS client or server machine. Its syntax is as follows:

```
inreport -IP <IP list> -OFN <file name> -RT <report type> [-SD <date>] [-ED <date>]
[-DURATION <n>h<n>d] [-LAST <n>h<n>d] -USER <user-name> -PASSWORD
<password> [-NEType <PTP 820>] [-Group <domain_name>] [-Master]
[-timestamp|-timestamp D|-timestamp M]
```

where:

Parameter	Format	Mandator y/ Optional	Description
IP	-IP <IP> <IP> Or -IP ALL	O, if omitted the default parameter is "ALL"	<p>The IP addresses, separated by spaces, of the target devices. For example: -IP 172.24.30.100 172.24.30.101</p> <p>For PTP 820 devices, you can specify the IP address in either IPv4 or IPv6 format. Use the same format used to Discover the device.</p> <p>When specifying an IPv6 address, you can use any of the following representations:</p> <ul style="list-style-type: none"> • The full representation of 8 groups of 4 hexadecimal digits, separated by colons. For example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334 • Omitting leading zeros in groups. In this case, the above example address would be entered as: 2001:db8:85a3:0:0:8a2e:370:7334 • If the address contains chains of consecutive zero groups (a zero-group is a groups whose 4 digits are zero) – Replacing a chain of zero-groups with a double colon, with the following stipulations: <ul style="list-style-type: none"> • Only one double colon per address. • The longest zero-groups chain is replaced with a double colon.

			<ul style="list-style-type: none"> If there is more than one longest zero-groups chain, the leftmost one is replaced with a double colon. <p>Use -IP ALL to generate a report for all devices in the database.</p>
OFN	-OFN <filepath\name.ext>	M	<p>The output file name and path. If the extension is .txt, the file will be saved in text format. If the extension is .csv, the file will be saved in CSV format.</p> <p>The pathname may be a full pathname or a relative pathname. If a relative pathname is specified, the output folder will be placed under <the installation folder of PTP 820 NMS>/CLI_Reports.</p> <p>For example: C:\PTP 820 NMS\CLI_Reports\...</p> <p>Note: When run in a machine that is not the PTP 820 NMS server machine, the absolute path must be used.</p> <p>Note: Make sure you have full permissions to the specified folder. Otherwise, no report is created or saved.</p>
RT	-RT <report-type>	M	<p>The report type. This can be set to any of the following (including the quote marks):</p> <p>"Frequency Change Report"</p> <p>"Full Link Report"</p> <p>"Network Element Report"</p> <p>"Radio Report"</p> <p>"Link Report"</p> <p>"Licensing Report"</p> <p>"Versions"</p> <p>"Serial Numbers Report"</p>
SD	-SD "dd/MM/yy HH:mm"	O	<p>Start date and time for the report.</p> <p>For example:</p> <p>-SD "17/05/15 10:00"</p> <p>Note: This parameter is relevant only for the "Frequency Change Report".</p> <p>If the SD is omitted, the default value is the oldest entry stored in the database (to view or set the storage period, refer to Error! Reference source not found.).</p>
ED	-ED "dd/MM/yy HH:mm"	O	<p>End date and time for the report.</p> <p>For example:</p> <p>-ED "18/05/15 10:00"</p>

			<p>Note: This parameter is relevant only for the 'Full Link Report' and "Frequency Change Report".</p> <p>If the ED is omitted from a Full Link Report, the default value is 00:00 of today (thus the report spans all 24 hours of yesterday).</p> <p>If the ED is omitted from a Frequency Change Report, the default value is the current time.</p>
DURATION	-DURATION <n>h <n>d	O	<p>As an alternative to setting the start date and end date of the report, you can define to include in the report only the alarms from a specific numbers of hours or days prior to the time of command execution. For example:</p> <p>-DURATION 12h</p> <p>In this case, the report will include the alarms from the 12 hours prior to command execution.</p> <p>Note: The time refers to the device time.</p> <p>Note: This parameter is relevant only for the "Frequency Change Report".</p>
LAST	-LAST [<n>h <n>d]	O	<p>As an alternative to setting the start date and end date of the report, you can define to include in the report only the alarms from a specific number of FULL hours or days prior to the time of command execution. For example:</p> <p>-LAST 1d</p> <p>The report will include the alarms from the last 1 day - from 00:01 to 24:00.</p> <p>-LAST 3h</p> <p>The report will include the alarms from the last 3 hours. If the command is executed at 10:12, the report will include alarms from 07:01 to 10:00.</p> <p>Note: The time refers to the device time.</p> <p>Note: This parameter is relevant only for the "Frequency Change Report".</p>
USER	-USER	M	<p>The name of the user with read access to the target devices. Make sure to specify an active user with a valid password.</p>
PASSWORD	-PASSWORD	M	<p>The password of the user with read access to the target devices.</p>

NEType	-NEType <PTP 820>	O	<p>Enables you to limit the report to PTP 820 elements only.</p> <p>Note : You can still provide a list of IPs. The report will be generated for all the specified IPs that match the device type.</p>
GROUP	-GROUP <domain_name>	O	<p>When the Group option is provided, the report will be generated only for the devices in the specified domain and its sub-domains.</p>
MASTER	-MASTER	O	<p>Relevant only for a Versions report.</p> <p>Instructs PTP 820 NMS to list in the Versions report only master packages (software packages for an entire device).</p>
timestamp	-timestamp or -timestamp D or -timestamp M	O	<p>Add a timestamp to the report filename.</p> <ul style="list-style-type: none"> If you specify -timestamp or -timestamp D, then the filename will have the following format: <filename>_DDMMYYYY_HH_MM_SS.<extension> <p>If you specify -timestamp M, then the filename will have the following format: <filename>_MMDDYYYY_HH_MM_SS.<extension></p>

Generating Inventory reports via the GUI

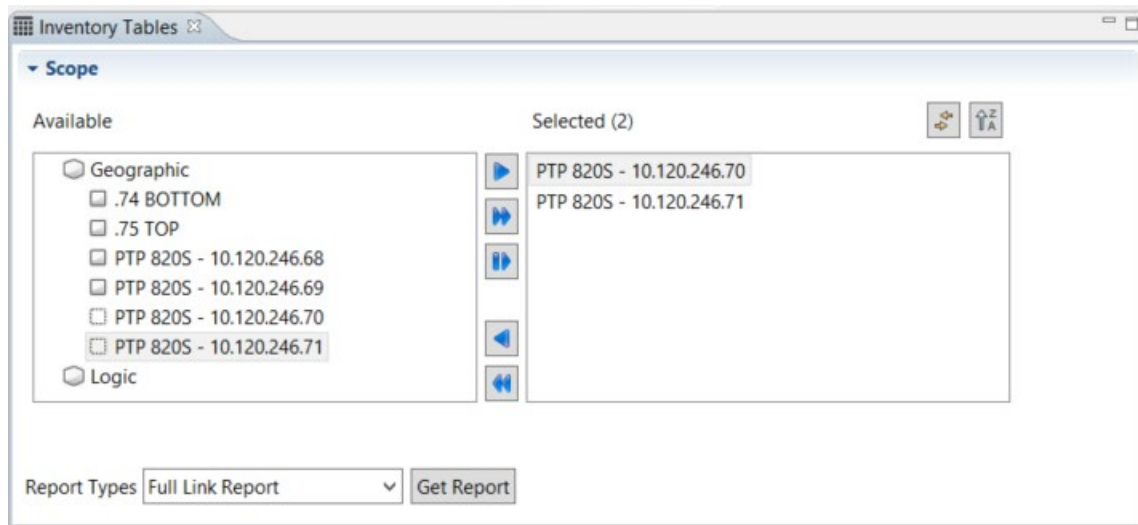
You can generate various inventory reports through the GUI.

1 Perform one of the following:


- Right-click a device or domain in the GUI display (for example in a navigation tree or topology view), and select **Reports > Inventory Tables**.
- Select **View > Reports > Inventory tables**.

The **Inventory Tables** view appears.

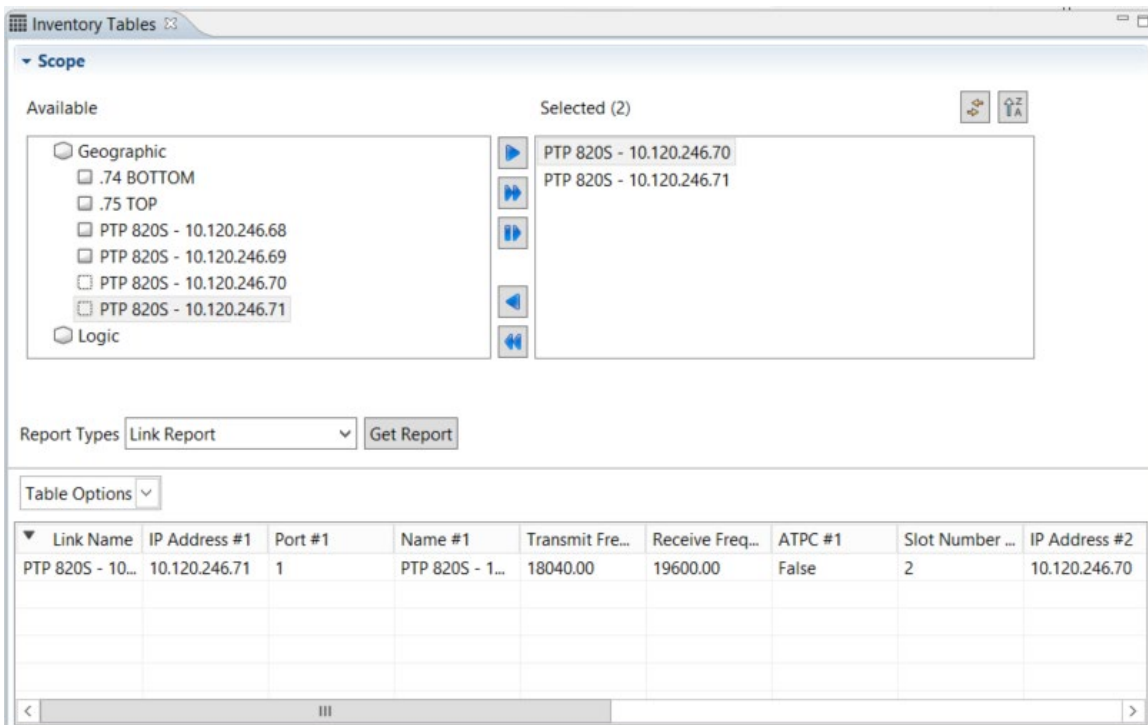
If you had right-clicked a device or domain, it appears already selected in the **Scope** section.



- 2 In the **Scope** section, move to the **Selected** pane all the NEs for which you wish to generate a report.

Optionally rearrange the order of the NEs using the  icon. This determines the order in which the NEs are listed in the **Selected** pane.



- 3 In the **Report Types** field, select the report type.
- 4 Click **Get Report**. The report appears on screen.



- 5 Click **Table Options** > **Customize Columns** to select which columns to display.
- 6 Click **Table Options** > **Export to File** to export the report to a file.

You can sort the report by clicking any of the columns.

Available operations

-  Link View – When activated, selecting a device in the **Selected** pane, selects the device in the tree appearing in the **Available** pane, and vice versa.
-  Order ascending/descending – orders the devices appearing in the **Selected** pane in ascending/descending order. This determines the order in which the NEs are listed in the right pane.

Generating a Frequency Change Report

The Frequency Change report provides information about changes in Tx and Rx frequency of radio ports in network elements. This report can be generated for any PTP 820 NEs.

The report by default displays the data in descending order (most recent change first). Each line displays a change that occurred in Tx and/or Rx frequency of a radio port on the specified PTP 820 devices between the specified start time and end time. If no start time or end time are specified, all stored frequency-change entries are displayed. Keep in mind that you can specify how long to keep the collected frequency-change data in the database. To do so, refer to [Error! Reference source not found.](#)

- To generate the report via CLI, refer to [Generating Inventory reports using a CLI command.](#)
- To generate the report using the GUI, refer to [Generating Inventory reports via the GUI.](#)

Viewing a Frequency Change report

The following is an example of a Frequency Change Report.

Report Types

Frequency Change Report

Get Report

Table Options

▼ Date and...	Name	IP Address	Slot	Port	Previous Freq...	New Freq. Tx ...	Previous Freq...	New Freq. ...
23-Sep-19 0...	PTP 820S - 1...	10.120.246.71	2	1	18040.000	18000.000	19600.000	19600.000
23-Sep-19 0...	PTP 820S - 1...	10.120.246.70	2	1	19600.000	19600.000	18040.000	18000.000

The Frequency Change report provides the following frequency-change information for the selected devices.

Field Name	Description
Date and Time	The date and time when PTP 820 NMS noted the change in frequency.
Name	The name of the network element.
IP Address	The IP address of the network element.
Slot	The slot number of the radio port.

Port	The port number of the radio port.
Previous Freq. Tx (MHz)	The Radio Frequency in the Tx direction before the change.
New Freq. Tx (MHz)	The Radio Frequency in the Tx direction after the change.
Previous Freq. Rx (MHz)	The Radio Frequency in the Rx direction before the change.
New Freq. Rx (MHz)	The Radio Frequency in the Rx direction after the change.

Generating a Full Link Report

The Full Link report displays:

- Up-to-date information regarding the link
- 24 hours of link PM counters.
 - **Note:** The Full Link report differentiates between E1/DS1 traffic and Ethernet traffic. In this way, it is different from Interface performance reports. The Full Link report provides capacity and throughput PMs for E1/DS1 traffic and Ethernet traffic separately, whereas the Interface performance report provides capacity and throughput PMs for the entire radio link.
 - **Important:** If you perform changes in your system, for some parameters the full link report may show the current values instead of the actual values that existed during the timeframe of the report, because PTP 820 NMS does not save parameters' history. To avoid this situation, generate a full link report at the beginning of the workday.
- To generate the report via CLI, refer to [Generating Inventory reports using a CLI command](#).
- To generate the report using the GUI, refer to [Generating Inventory reports via the GUI](#).

Prerequisites

A prerequisite to generating full link reports is to enable collection of network-wide PM counters at least one day prior to generating a full link report. To enable collection of PM counters, check the **Enable Network-wide PM Collection** option in the [Network-wide PM Collection](#) Preferences page (you can also optionally change the polling interval).

Supported link configurations

The full link reports can provide information for the following types of links:

- Links between PTP 820 devices

Viewing a Full Link Report

The following is an example Full LinkReport:

	A	B	C	D	E	F	G	H
1								
2	Full Link Report							
3								
4	Report Save Time: 2019-09-23 09:54:53							
5								
6	Link Name	Site A Name	Site A Loc	Site A IP	Site A Phy	Site B Name	Site B Loc	Site B IP
7	PTP 820S - 10.120.246.71 - PTP 820S - 10.120.246.70	PTP 820S - 10.120.246.71	N/A	10.120.246.71	Slot 2 / Po	PTP 820S - 10.120.246.70	N/A	10.120
8	PTP 820S - 10.120.246.69 - PTP 820S - 10.120.246.68	PTP 820S - 10.120.246.69	N/A	10.120.246.69	Slot 2 / Po	PTP 820S - 10.120.246.68	N/A	10.120
9	.75 TOP - .74 BOTTOM	.75 TOP	N/A	10.120.200.75	Slot 1 / Po	.74 BOTTOM	N/A	10.120
10								
11								
12								
13								
14								

The Full Link report displays the following link information.

Field Name	Description	Report Units
Link Name	The name of the link between the port of one device (Site A) and the port of the second device (Site B.)	
Site A Name	Site A Device Name.	
Site A Location	Site A System Location.	
Site A Id	Site A Main IP address, in IPv4 format.	
Site A Physical Port	Slot x / Port x at Site A.	
Site B Name	Site B Device Name.	
Site B Location	Site B System Location.	
Site B Id	Site B Main IP address, in IPv4 format.	
Site B Physical Port	Slot x / Port x at Site B.	
Link Configuration	The type of link.	
Site A Radio	The RFU type of the site A radio.	
Site B Radio	The RFU type of the site B radio.	
Site A Tx Freq Min	Site A minimum Tx frequency.	MHz
Site A Tx Freq Max	Site A maximum Tx frequency.	MHz

Site B Tx Freq Min	Site B minimum Tx frequency.	MHz
Site B Tx Freq Max	Site B maximum Tx frequency.	MHz
Site A Tx Freq	Site A's configured Tx frequency.	MHz
Site B Tx Freq	Site B's configured Tx frequency.	MHz
Site A Radio Script	The radio script used by Site A.	
Site B Radio Script	The radio script used by Site B.	
MRMC Script Operational Mode	"Fixed" or "Adaptive".	
MRMC Script Profile	Relevant only if "MRMC Script Operational Mode" = Fixed.	
MRMC Script Maximum Profile	Relevant only if "MRMC Script Operational Mode" = Adaptive.	
MRMC Script Minimum Profile	Relevant only if "MRMC Script Operational Mode" = Adaptive.	
ATPC	Indicates whether ATPC is configured on both devices.	
Site A Max Power (Preset)	Site A pre-set maximum power value.	dBm
Site B Max Power (Preset)	Site B pre-set maximum power value.	dBm
Site A Tx Power (Current)	The value is updated every time it is read from the NE.	dBm
Site B Tx Power (Current)	The value is updated every time it is read from the NE.	dBm
Site A Rx Level (Current)	The value is updated every time it is read i from the NE.	dBm
Site B Rx Level (Current)	The value is updated every time it is read from the NE.	dBm

Site A Max Tx Power [Last 24 hours]	The highest 15-minute Tx power counter for Site A in the 24 hours preceding report initiation.	dBm
Site B Max Tx Power [Last 24 hours]	The highest 15-minute Tx power counter for Site B in the 24 hours preceding report initiation	dBm
Site A Min Tx Power [Last 24 hours]	The lowest 15-minute Tx power counter for Site A in the 24 hours preceding report initiation.	dBm
Site B Min Tx Power [Last 24 hours]	The lowest 15-minute Tx power counter for Site B in the 24 hours preceding report initiation.	dBm
Site A Max Rx Level [Last 24 hours]	The highest 15-minute Rx power counter for Site A in the 24 hours preceding report initiation.	dBm
Site B Max Rx Level [Last 24 hours]	The highest 15-minute Rx power counter for Site B in the 24 hours preceding report initiation.	dBm
Site A Min Rx Level [Last 24 hours]	The lowest 15-minute Rx power counter for Site A in the 24 hours preceding report initiation.	dBm
Site B Min Rx Level [Last 24 hours]	The lowest 15-minute Rx power counter for Site B in the 24 hours preceding report initiation.	dBm
Site A Max E1/T1	Site A maximum E1/T1 counter value.	no unit
Site B Max E1/T1	Site B maximum E1/T1 counter value.	no unit
Site A Active E1/T1	The value is updated every time it is read from the NE.	no unit
Site B Active E1/T1	The value is updated every time it is read from the NE.	no unit

Site A E1/T1 Utilization	Percentage of site A's E1/T1 utilization.	percentage
Site B E1/T1 Utilization	Percentage of site B's E1/T1 utilization.	percentage
Site A Max Ethernet Capacity	Site A's capacity of the radio reserved for Ethernet packets of the link presented by this row in the report.	Mb/s
Site B Max Ethernet Capacity	Site B's capacity of the radio reserved for Ethernet packets of the link presented by this row in the report.	Mb/s
Site A Max Ethernet Throughput [Last 24 hours]	<p>Site A's peak (last 24 hours) Ethernet throughput which was sent over the radio in the last 24 hours. Note this may also exceed the capacity, if the packets are small or header compression is used.</p> <p>In the case of ABC groups, the Max Ethernet Throughput is the peak Ethernet throughput the entire ABC group, which may include several radios, and therefore may exceed the Max Ethernet Capacity which is only of the specific link in the group. To determine the capacity of the group it is necessary to sum all the capacity values of all the members of the group.</p>	Mb/s
Site B Max Ethernet Throughput [Last 24 hours]	<p>Site B's peak (last 24 hours) Ethernet throughput which was sent over the radio in the last 24 hours. Note this may also exceed the capacity, if the packets are small or header compression is used.</p> <p>In the case of ABC groups, the Max Ethernet Throughput is the peak Ethernet throughput of the</p>	Mb/s

	entire ABC group, which may include several radios, and therefore may exceed the Max Ethernet Capacity which is only of the specific link in the group. To determine the capacity of the group it is necessary to sum all the capacity values of all members of the group.	
Site A Min Ethernet Throughput [Last 24 hours]	The minimum Ethernet throughput for Site A over the period in the report. This refers only to the Ethernet portion of the radio traffic.	Mb/s
Site B Min Ethernet Throughput [Last 24 hours]	The minimum Ethernet throughput for Site B over the period in the report. This refers only to the Ethernet portion of the radio traffic.	Mb/s
Site A AVG Ethernet Throughput [Last 24 hours]	The average Ethernet throughput for Site A over the period in the report. This refers only to the Ethernet portion of the radio traffic.	Mb/s
Site B AVG Ethernet Throughput [Last 24 hours]	The average Ethernet throughput for Site B over the period in the report. This refers only to the Ethernet portion of the radio traffic.	Mb/s
Site A Radio Link ID	The Site A radio link ID.	
Site B Radio Link ID	The Site B radio link ID.	

Generating a Network Element Report

The Network element report provides status information and data about network elements. This report can be generated for any NEs supported by PTP 820 NMS.

- To generate the report via CLI, refer to [Generating Inventory reports using a CLI command](#).

- To generate the report using the GUI, refer to [Generating Inventory reports via the GUI](#).

Viewing a Network Element report

The following is an example of a Network Element Report.

Report Types

Network Element Report

Get Report

Table Options

▼ IP Address	Status	Name	System Locat...	System Cont...	Product Type	Last Reachable
10.120.246.71	Reachable	PTP 820S - 1...	N/A	N/A	PTP 820S	2019-09-23 09:54:21.458
10.120.246.70	Reachable	PTP 820S - 1...	N/A	N/A	PTP 820S	2019-09-23 09:51:53.064
10.120.246.69	Reachable	PTP 820S - 1...	N/A	N/A	PTP 820S	2019-09-23 09:52:41.028
10.120.246.68	Reachable	PTP 820S - 1...	N/A	N/A	PTP 820S	2019-09-23 09:58:07.521
10.120.200.75	Reachable	.75 TOP	N/A	N/A	PTP 820G	2019-09-23 10:01:19.7
10.120.200.74	Reachable	.74 BOTTOM	N/A	N/A	PTP 820G	2019-09-23 10:01:46.152

The Network element report provides the following status information and data for the selected devices.

Field Name	Description
IP address	All the IP addresses of the network element.
Status	The availability of the network element: reachable, unreachable, or uninvestigated.
Name	The network element's User defined name.
System location	The physical location of the network element.
System contact	The network user responsible for the network element.
Last reachable	The last reachable date and time of the network element. Applicable only for network elements with a status state of Reachable or Unreachable.
Product type	The type of network element.
System name	The system name of the network element.

Generating a Link report

The link report provides data about links, such as transmit and receive frequencies and slot number locations.

- To generate the report via CLI, refer to [Generating Inventory reports using a CLI command](#).

- To generate the report using the GUI, refer to [Generating Inventory reports via the GUI](#).

Viewing a Link report

The following is an example of a Link Report.

Report Types

Link Report

Get Report

Table Options

▼ Link Name	IP Address #1	Port #1	Name #1	Transmit Fre...	Receive Freq...	ATPC #1	Slot Number ...	IP Address #2
PTP 820S - 10...	10.120.246.71	1	PTP 820S - 1...	18000.00	19600.00	False	2	10.120.246.70
PTP 820S - 10...	10.120.246.69	1	PTP 820S - 1...	17800.00	19500.00	False	2	10.120.246.68
.75 TOP - .74 ...	10.120.200.75	1	.75 TOP	17900.00	19500.00	False	1	10.120.200.74

<

III

>

The Link Report provides the following information about links.

Field Name	Description
Link Name	The name of the link between the port of one device and the port of the second device.
IP Address #1	The IP address of the network element at one end of the link.
Port #1	The number of the port at one end of the link.
Name #1	The system name of the slot at one end of the link.
Transmit Frequency (MHz) #1	The transmit frequency at one end of the link.
Receive Frequency (MHz) #1	The receive frequency at one end of the link.
ATPC #1	Indicates whether one end of the link is using Ad hoc TCP.
Slot Number #1	The slot number of the interface at one end of the link. IDUs in an shelf get each a “slot ID” indicating their position: slot 1 is the lowest IDU and 6 is the highest.
IP Address #2	The IP address of the network element at the other end of the link.
Port #2	The number of the port at the other end of the link.
Name #2	The system name of the slot at the other end of the link.
Transmit Frequency (MHz) #2	The transmit frequency at one end of the link.
Receive Frequency (MHz) #2	The receive frequency at the other end of the link.
ATPC #2	Indicates whether the second end of the link is using Ad hoc TCP.
Slot Number #2	The slot number of the interface at the other end of the link. IDUs in an PTP shelf get each a “slot ID” indicating their position: slot 1 is the lowest IDU and 6 is the highest.
Radio Link ID #1	The radio link ID at one end of the link.

Radio Link ID #2	The radio link ID at the other end of the link.
------------------	---

Generating a Radio Report

The radio report display information about radio interfaces. This report can be generated for any PTP 820 devices.

- To generate the report via CLI, refer to [Generating Inventory reports using a CLI command](#).
- To generate the report using the GUI, refer to [Generating Inventory reports via the GUI](#).

Viewing a Radio report

The following is an example of a radio report.

	A	B	C	D	E	F	G	H	I
1									
2	Radio Report								
3									
4	Report Save Time: 2019-09-23 10:06:19								
5									
6	IP Address	Slot Num	Name	Slot	RFU Type	Modem T	Transmit Frequency (MHz)	Receive Frequency (MHz)	Min Transmit Frequency (MHz)
7	10.120.246.71	2	PTP 820S - 10.120.246.71	Carrier 1	RFU-S	N/A	18000	19600	17699
8	10.120.246.70	2	PTP 820S - 10.120.246.70	Carrier 1	RFU-S	N/A	19600	18000	19259
9	10.120.246.69	2	PTP 820S - 10.120.246.69	Carrier 1	RFU-S	N/A	17800	19500	17699
10	10.120.246.68	2	PTP 820S - 10.120.246.68	Carrier 1	RFU-S	N/A	19500	17800	19259
11	10.120.200.75	1	.75 TOP	Carrier 2	Unknown	N/A	37086	38346	13.25
12	10.120.200.75	1	.75 TOP	Carrier 1	RFU-C	N/A	17900	19500	17726.85
13	10.120.200.74	1	.74 BOTTOM	Carrier 2	Unknown	N/A	37086	38346	13.25
14	10.120.200.74	1	.74 BOTTOM	Carrier 1	RFU-C	N/A	19500	17900	19286.85
15									

The radio report provides the following information for the radio interfaces of the specified network elements.

Field Name	Description
IP address	The IP address of the network element.
Slot number	The slot number of the interface. IDUs in a shelf get each a "slot ID" indicating their position: slot 1 is the lowest IDU and 6 is the highest.
Name	The slot's system name.
Slot	The port's identification.
RFU type	The product type of the RFU.
Modem type	The type of modem in use.
Transmit frequency (MHz)	The configured transmit frequency.
Receive frequency (MHz)	The measured receive frequency.
Min transmit frequency (MHz)	The minimum transmit frequency, given the specific device and selected radio script.
Max transmit frequency (MHz)	The maximum transmit frequency, given the specific device and selected radio script.

Channel spacing (MHz)	The allocated bandwidth for the RF channel.
Transmit level	The average transmit level for the measured interval.
ATPC	The Automatic Transmit Power Control status (enabled or disabled).
ATPC reference level	The Received Signal Level value.
Link ID	The link ID.
XPIC	Indicates whether XPIC is enabled or disabled on the radio interface.
Admin state	Reports whether the radio interface is Enabled or Disabled.
Operational status	Indicates whether the radio is operational.
Multi Radio admin	The status of the multi-radio unit (enabled or disabled).

Generating a Licensing Report

The licensing report provides data about the licenses enabled for each network element. This report can be generated for any PTP 820 devices.

- To generate the report via CLI, refer to [Generating Inventory reports using a CLI command](#).
- To generate the report using the GUI, refer to [Generating Inventory reports via the GUI](#).

Viewing a Licensing report

The following is an example of a licensing report.

Report Types Serial Numbers Report Get Report

Table Options ▼

IP Address	Slot Number	Name	Slot	Type	Serial Number	Part Number
10.120.246.71	0	PTP 820S - 1...	N/A	PTP 820-S	F515J03158	C180082B012A
10.120.246.71	0	PTP 820S - 1...	N/A	PTP 820-S	F515J03158	C180082B012A
10.120.246.70	0	PTP 820S - 1...	N/A	PTP 820-S	F115203879	C180082B011A
10.120.246.70	0	PTP 820S - 1...	N/A	PTP 820-S	F115203879	C180082B011A
10.120.246.69	0	PTP 820S - 1...	N/A	PTP 820-S	F235908980	C180082B012A
10.120.246.69	0	PTP 820S - 1...	N/A	PTP 820-S	F235908980	C180082B012A
10.120.246.68	0	PTP 820S - 1...	N/A	PTP 820-S	F525S01636	C180082B011A
10.120.246.68	0	PTP 820S - 1...	N/A	PTP 820-S	F525S01636	C180082B011A

The licensing report provides the following information about the licenses enabled for the network element.

Field Name	Description
IP address	The IP address of the network element.

Slot number	The slot number of the interface. IDUs in a shelf get each a “slot ID” indicating their position: slot 1 is the lowest IDU and 6 is the highest.
License type	The license type.
License code	The license validity code.
Demo admin	Indicates whether the demo license is enabled or disabled.
Demo timer	The remaining validity period of the license for trial or demo licenses.
Feature	Indicates which feature set is enabled by the license.
License	The license status.
License per usage	The capacity of the license feature.
Usage configuration	Indicates whether the feature is allowed or not allowed for the given license.
License model	The license model for allowed features.

Generating a Versions Report

The versions report provides data about the software and firmware versions installed on network elements. This report can be generated for any PTP 820 devices.

You can optionally select to display in the Versions report only master packages (software packages for an entire device).

- To generate the report via CLI, refer to [Generating Inventory reports using a CLI command](#).
- To generate the report using the GUI, refer to [Generating Inventory reports via the GUI](#).

Viewing a Versions report

The following is an example of a versions report. Each device can contain several software/firmware packages, and the report displays each package in a separate row.

Report Types Versions Get Report ☐ Show only master packages

Table Options

IP Address	Slot Number	Name	Slot	Type	Version	Downloaded Version
10.10.66.138	0	138-G-Setup8	N/A	gnss	9.5.0.0.0.192	9.5.0.0.0.192
10.10.66.138	0	138-G-Setup8	N/A	gnss-fpga-fw-elic	N/A	1.8.3
10.10.66.138	0	138-G-Setup8	N/A	gnss-fpga-fw-rmc	N/A	2.3
10.10.66.138	0	138-G-Setup8	N/A	gnss-rmc-b	N/A	3.10.23
10.10.66.138	0	138-G-Setup8	N/A	gnss-fpga-fw-tcc	625b	N/A
10.10.66.138	0	138-G-Setup8	N/A	gnss-atp	9.5.0.0.0.192	N/A
10.10.66.138	0	138-G-Setup8	N/A	gnss-management	1.9.5.11	1.9.5.11

You can optionally select **Show only master packages** to display, for each device, the version information of its master package only (a master package is a software package for an entire device).

Report Types Versions Get Report ☒ Show only master packages

Table Options

IP Address	Slot Number	Name	Slot	Type	Version	Downloaded Version
10.10.66.138	0	138-G-Setup8	N/A	gnss	9.5.0.0.0.192	9.5.0.0.0.192

The versions report provides the following information about the software and firmware versions installed on the specified network elements.

Field Name	Description
IP address	The IP address of the network element.
Slot number	The slot number of the interface. IDUs in a shelf get each a “slot ID” indicating their position: slot 1 is the lowest IDU and 6 is the highest.
Name	The slot’s system name.
Slot	The port’s identification.
Type	The type of software or firmware package.
Version	The version number of the currently-installed software/firmware.
Downloaded version	The version number of the downloaded (but not yet installed) software/firmware

Generating a Serial Numbers Report

The serial numbers report displays the serial number for each network element. This report can be generated for any PTP 820 family device.

- To generate the report via CLI, refer to [Generating Inventory reports using a CLI command](#).
- To generate the report using the GUI, refer to [Generating Inventory reports via the GUI](#).

Viewing a Serial Numbers report

The following is an example of a serial numbers report.

Report Types Serial Numbers Report Get Report

Table Options

IP Address	Slot Number	Name	Slot	Type	Serial #	Part #
10.10.66.168	8	168 - IP20N	N/A	RFU-C	I008212927	1C15004L0D
10.10.66.168	8	168 - IP20N	N/A	RMC-A	F422U08414	24-R001-0A
10.10.66.168	127	168 - IP20N	N/A	1U/2U Chassis	F473M07837	24-0001-0A
10.10.66.156	0	IP-20E - 156	N/A	IP-20	F055509267	25-0002-0D
10.10.66.155	0	IP-20E - 155	N/A	IP-20	F204F02959	25-0001-0A
10.10.66.102	1	102-IP20Setup1-I...	N/A	RFU-C	F22002443	1C15004L0D
10.10.66.102	1	102-IP20Setup1-I...	N/A	Unknown	-	-
10.10.66.102	127	102-IP20Setup1-I...	N/A	IP-20G	F144F02408	24-G001-0B

The serial numbers report provides the following serial number information for each specified network element.

Field Name	Description
IP address	The IP address of the network element.
Slot number	The slot number of the interface. IDUs in a shelf get each a “slot ID” indicating their position: slot 1 is the lowest IDU and 6 is the highest.
Name	The slot’s system name.
Slot	The port’s identification.
Type	The unit type: IDU or RFU.
Serial #	The device ID.
Part #	The part number of the interface.

NG Alarm Reports Generation

You can instruct PTP 820 NMS to generate alarm reports using the [alarmreport](#) command line interface (CLI) command. The alarm reports can be generated whether the PTP 820 NMS server is running on a Windows or Solaris machine, and are available whether the database is Postgres or Oracle.

Note that report generation using the CLI command can be scheduled by using the operating system (Windows Task Scheduler or Unix Crontab).

Generating Alarms reports using a CLI command

You can generate various types of alarm reports using the [alarmreport](#) CLI command:

The report is generated as soon as the CLI command is given, and saved to the specified location.

Note: Following a PTP 820 NMS server or client installation on a Windows or Solaris machine, you must log off the operating system and log on again for the [alarmreport](#) command to work.

alarmreport command syntax

The [alarmreport](#) command can be called from any directory on the PTP 820 NMS client or server machine. Its syntax is as follows:

```
alarmreport [-IP <IP list>] [-NEType <PTP 820>]-OFN <file name> -RT <report type> [-SD <date>] [-ED <date>] [-DURATION <n>h<n>d] [-LAST <n>h<n>d] [-TOP <number>|no] [-LIMIT <number>] [-SERVERIP <IP>] -USER <user-name> -PASSWORD <password> [-GROUP <domain-name>] [-timestamp|timestamp D|timestamp M]
```

where:

Parameter	Format	Mandatory/Optional	Description
-----------	--------	--------------------	-------------

IP	-IP <IP> <IP> Or -IP ALL	O, if omitted the default parameter is "ALL"	<p>The IP addresses, separated by spaces, of the target devices. For example: -IP 172.24.30.100 172.24.30.101</p> <p>For PTP 820 devices, you can specify the IP address in either IPv4 or IPv6 format. Use the same format used to <u>Discover</u> the device.</p> <p>When specifying an IPv6 address, you can use any of the following representations:</p> <ul style="list-style-type: none"> • The full representation of 8 groups of 4 hexadecimal digits, separated by colons. For example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334 • Omitting leading zeros in groups. In this case, the above example address would be entered as: 2001:db8:85a3:0:0:8a2e:370:7334 • If the address contains chains of consecutive zero groups (a zero-group is a groups whose 4 digits are zero) – Replacing a chain of zero-groups with a double colon, with the following stipulations: <ul style="list-style-type: none"> • Only one double colon per address. • The longest zero-groups chain is replaced with a double colon. • If there is more than one longest zero-groups chain, the leftmost one is replaced with a double colon. <p>Use -IP ALL to generate a report for all devices in the database.</p> <p>Note: When using ALL, it is recommended to specify a limited time interval using -SD and -ED. The data for the entire network can reach a considerable size if not limited to a specific time period.</p>
NEType	-NEType <PTP 820 NMS>	O	<p>Enables you to limit the report to PTP 820 elements only, or PTP 820 NMS only (PTP 820 NMS alarms that are not associated with a specified device). For example: -NEType NMS</p> <p>Note : You can still provide a list of IPs. The report will be generated for all the specified IPs that match the device type.</p>

			Note: The NMS option is relevant only for 'Alarm log' and 'Current Alarms' reports.
OFN	-OFN <filepath\name. ext>	M	<p>The output file name and path. If the extension is .txt, the file will be saved in text format. If the extension is .csv, the file will be saved in CSV format.</p> <p>If the filepath is not specified, the report will be placed in the folder from which the command alarmreport was executed.</p> <p>Note: Make sure you have full permissions to the specified folder. Otherwise, no report is created or saved.</p>
RT	-RT <report-type>	M	<p>The report type. This can be set to any of the following (including the quote marks):</p> <p>"Alarm log" – current and historical alarms</p> <p>"Current Alarms" – current alarms</p> <p>"Alarmed NEs" – NEs ordered by number of alarms</p> <p>"Alarm Frequency" – the most frequent logged alarms in the specified period</p> <p>"Alarm Frequency by NE" – the most frequent logged alarms in the specified period, by NE</p> <p>Note: When specifying the "Current Alarms" option, all the time-related options (SD, ED, DURATION and LAST) are irrelevant</p>
SD	-SD "dd/MM/yy HH:mm"	O	<p>Start date and time for the report.</p> <p>For example:</p> <p>-SD "17/05/15 12:00" – any alarm from 12:01 and later will be included in the report.</p> <p>Note: The time refers to the device time.</p>
ED	-ED "dd/MM/yy HH:mm"	O	<p>End date and time for the report.</p> <p>For example:</p> <p>-ED "18/05/15 23:59" – any alarm from 23:58 and earlier will be included in the report.</p> <p>Note: The time refers to the device time.</p>
DURATION	-DURATION <n>h <n>d	O	<p>As an alternative to setting the start date and end date of the report, you can define to include in the report only the alarms from a specific numbers of hours or days</p>

			<p>prior to the time of command execution. For example: -DURATION 12h</p> <p>In this case, the report will include the alarms from the 12 hours prior to command execution.</p> <p>Note: The time refers to the device time.</p>
LAST	-LAST [<n>h <n>d]	O	<p>As an alternative to setting the start date and end date of the report, you can define to include in the report only the alarms from a specific number of FULL hours or days prior to the time of command execution. For example:</p> <p>-LAST 1d The report will include the alarms from the last 1 day - from 00:01 to 24:00.</p> <p>-LAST 3h The report will include the alarms from the last 3 hours. If the command is executed at 10:12, the report will include alarms from 07:01 to 10:00.</p> <p>Note: The time refers to the device time.</p>
TOP	-TOP <number> no	O	<p>Limits the number of results to include in the report. You can specify a number from 1-1000, or for an 'Alarmed NEs' report you can specify no, which means there is no limitation; that is, all NEs in the database will be included in the report.</p> <p>The default settings are as follows:</p> <ul style="list-style-type: none"> • For an 'Alarmed NEs' report - 30 • For an 'Alarm Frequency' report - 20 • For an 'Alarm Frequency by NE' report - 15 <p>Note: This parameter is relevant only for 'Alarmed NEs', 'Alarm Frequency' and 'Alarm Frequency by NE' reports.</p>
LIMIT	-LIMIT <number>	O	<p>Limits the number of alarms that the report should consider. You can specify a number from 1-1000.</p> <p>The default setting is 100.</p>

			Note: This parameter is relevant only for 'Alarm Frequency' and 'Alarm Frequency by NE' reports.
SERVERIP	-SERVERIP <IP>	O, if omitted the default value is "localhost"	The PTP 820 NMS server IP address, which must be provided if you are generating a report from the PTP 820 NMS client rather than the PTP 820 NMS server machine. If not provided, -SERVERIP LOCALHOST is the default setting.
USER	-USER	M	The name of the user with read access to the target devices. Make sure to specify an active user with a valid password.
PASSWORD	-PASSWORD	M	The password of the user with read access to the target devices.
Group	-Group <domain-name>	O	Generate a report only for the devices in the specified domain and its subdomains.
timestamp	-timestamp or -timestamp D or -timestamp M	O	Add a timestamp to the report filename. <ul style="list-style-type: none"> If you specify -timestamp or -timestamp D, then the filename will have the following format: <filename>_DDMMYYYY_HH_MM_SS.<extension> If you specify -timestamp M, then the filename will have the following format: <filename>_MMDDYYYY_HH_MM_SS.<extension>

Note: The parameters are not case sensitive, except where noted otherwise.

alarmreport CLI command – example command

The following is an example of a command for generating a "Current Alarms" alarm report:

```
alarmreport -IP 172.24.30.100 172.24.30.101 -OFN C:\Temp\report\CurrentAlarms1 -
RT "Current Alarms" -SD "17/05/15 12:00" -ED "18/05/15 23:59" -USER admin -
PASSWORD cer1
```

Generating an Alarm Log report

The Alarm log lists current and historical alarms. You can generate reports listing all alarms, or PTP 820 NMS alarms only, or alarms associated with specific devices only.

- To generate the report via CLI, refer to [Generating Alarms reports using a CLI command](#).

The following is an example Alarm Log Report listing historical alarms:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1															
2	Alarm Log Report														
3															
4	Report Save Time: 2018-04-16 10:50:44														
5															
6	Ack	Raised Time (System)	Cleared Time (System)	Raised Time (NE)	Cleared Time (NE)	IP	Slot Number	Name	Severity	Module	Description				
7	FALSE	12/04/2018 17:30		12/04/2018 17:28		10.10.66.148	4	S10 - 148 - IP20N	MINOR		Unequipped label received on TDM-LIC VC12/VC11				
8	FALSE	12/04/2018 17:30		12/04/2018 17:28		10.10.66.148	4	S10 - 148 - IP20N	MAJOR		Alarm Indication Signal (AIS) on TDM-LIC TDM port				
9	FALSE	12/04/2018 17:30	12/04/2018 17:30	12/04/2018 17:28	12/04/2018 17:28	10.10.66.148	4	S10 - 148 - IP20N	MINOR		Unequipped label received on TDM-LIC VC12/VC11				
10	FALSE	12/04/2018 17:30	12/04/2018 17:30	12/04/2018 17:28	12/04/2018 17:28	10.10.66.148	4	S10 - 148 - IP20N	MINOR		Unequipped label received on TDM-LIC VC12/VC11				
11	FALSE	12/04/2018 17:30	12/04/2018 17:30	12/04/2018 17:28	12/04/2018 17:28	10.10.66.148	4	S10 - 148 - IP20N	MAJOR		Loss Of Frame (LOF) on TDM-LIC STM1/OC3 port				
12	FALSE	12/04/2018 17:30	12/04/2018 17:30	12/04/2018 17:28	12/04/2018 17:28	10.10.66.148	4	S10 - 148 - IP20N	MAJOR		Excessive BER on TDM-LIC STM1/OC3 port				
13	FALSE	12/04/2018 17:30	12/04/2018 17:30	12/04/2018 17:28	12/04/2018 17:28	10.10.66.148	4	S10 - 148 - IP20N	CRITICAL		Loss Of Signal (LOS) on TDM-LIC STM1/OC3 port				
14	FALSE	12/04/2018 17:30	12/04/2018 17:30	12/04/2018 17:27	12/04/2018 17:27	10.10.66.148	3	S10 - 148 - IP20N	WARNING		Radio interface is up				
15	FALSE	12/04/2018 17:30	12/04/2018 17:30	12/04/2018 17:27	12/04/2018 17:27	10.10.66.148	3	S10 - 148 - IP20N	MINOR		Radio signal degrade				
16	FALSE	12/04/2018 17:30	12/04/2018 17:30	12/04/2018 17:26	12/04/2018 17:27	10.10.66.148	3	S10 - 148 - IP20N	WARNING		RFU RX level out of range				
17	FALSE	12/04/2018 17:30	12/04/2018 17:30	12/04/2018 17:24	12/04/2018 17:27	10.10.66.148	3	S10 - 148 - IP20N	CRITICAL		Remote communication failure				
18	FALSE	12/04/2018 17:30	12/04/2018 17:30	12/04/2018 17:23	12/04/2018 17:27	10.10.66.148	3	S10 - 148 - IP20N	CRITICAL		Radio loss of frame				
19	FALSE	12/04/2018 17:30	12/04/2018 17:30	12/04/2018 17:23	12/04/2018 17:28	10.10.66.148	4	S10 - 148 - IP20N	MINOR		Alarm Indication Signal (AIS) on TDM-LIC VC12/VC11				
20	FALSE	12/04/2018 17:30	12/04/2018 17:30	12/04/2018 17:23	12/04/2018 17:28	10.10.66.148	4	S10 - 148 - IP20N	MAJOR		Loss Of Frame (LOF) on TDM-LIC STM1/OC3 port				
21	FALSE	12/04/2018 17:30	12/04/2018 17:30	12/04/2018 17:23	12/04/2018 17:28	10.10.66.148	4	S10 - 148 - IP20N	CRITICAL		Loss Of Signal (LOS) on TDM-LIC STM1/OC3 port				
22	FALSE	12/04/2018 17:30	12/04/2018 17:30	12/04/2018 17:23	12/04/2018 17:28	10.10.66.148	4	S10 - 148 - IP20N	MAJOR		Excessive BER on TDM-LIC STM1/OC3 port				
23	FALSE	12/04/2018 17:30	12/04/2018 17:30	12/04/2018 17:23	12/04/2018 17:23	10.10.66.148	3	S10 - 148 - IP20N	MINOR		Radio signal degrade				
24	FALSE	12/04/2018 17:30	12/04/2018 17:30	12/04/2018 17:23	12/04/2018 17:23	10.10.66.148	3	S10 - 148 - IP20N	WARNING		Radio interface is down				
25	FALSE	12/04/2018 17:30		12/04/2018 17:22		10.10.66.148	4	S10 - 148 - IP20N	MAJOR		Loss-of-frames alarm on TDM service				
26	FALSE	12/04/2018 17:30	12/04/2018 17:30	12/04/2018 17:22	12/04/2018 17:22	10.10.66.148	4	S10 - 148 - IP20N	INDETERMINATE		Card operational state is Up				
27	FALSE	12/04/2018 17:30	12/04/2018 17:30	12/04/2018 17:22	12/04/2018 17:23	10.10.66.148	4	S10 - 148 - IP20N	MINOR		Unequipped label received on TDM-LIC VC12/VC11				

Viewing an Alarm Log Report

The Alarm Log Report displays the following information.

Field Name	Description
Ack	TRUE if the alarm has been acknowledged, FALSE if not.
Raised Time (System)	The time on the PTP 820 NMS server when the alarm was raised.
Cleared Time (System)	The time on the PTP 820 NMS server when the alarm was cleared.
Raised Time (NE)	The time on the NE when the alarm was raised.
Cleared Time (NE)	The time on the NE when the alarm was cleared.
IP	The IP address of the network resource that generated the alarm.

Slot Number	The slot of the entity that generated the alarm.
Name	The name of the NE that generated the alarm.
Severity	One of the possible alarm severities: CRITICAL, MAJOR, MINOR, WARNING, INDETERMINATE or INFO. Note that severities can be customized using the Error! Reference source not found.
Module	
Description	Lists the most likely reason for the alarm. This is a textual description of the cause of the alarm, displayed exactly as sent from the NE or portrayed in the EMS user interface. The text can be customized using the Error! Reference source not found.

Generating a Current Alarms report

The Current Alarms Report lists current alarms. You can generate reports listing all alarms, or PTP 820 NMS alarms only, or alarms associated with specific devices only.

- To generate the report via CLI, refer to [Generating Alarms reports using a CLI command.](#)

The following is an example Current Alarms Report:

	A	B	C	D	E	F	G	H	I	J	K	L
1												
2	Current Alarms Report											
3												
4	Report Save Time: 2019-09-23 10:25:30											
5												
6	Ack	Raised Time (System)	Raised Time (NE)	IP	Slot Num	Name	Severity	Module	Description			
7	FALSE	9/23/2019 9:41	9/23/2019 9:24	10.120.200.75	1	.75 TOP	MAJOR		Loss-of-frames alarm on TDM service			
8	FALSE	9/23/2019 9:41	9/23/2019 9:24	10.120.200.75	1	.75 TOP	MAJOR		Loss Of Signal (LOS) on TDM-LIC TDM port			
9	FALSE	9/23/2019 8:21	9/23/2019 8:17	10.120.200.75	1	.75 TOP	MAJOR		Loss of Carrier			
10	FALSE	9/23/2019 9:41	9/23/2019 9:24	10.120.200.75	1	.75 TOP	MAJOR		Protection configuration mismatch!			
11	FALSE	9/23/2019 9:41	9/23/2019 9:24	10.120.200.74	1	.74 BOTTC	MAJOR		Protection configuration mismatch!			
12	FALSE	9/23/2019 9:41	9/23/2019 9:24	10.120.200.74	1	.74 BOTTC	MAJOR		Loss-of-frames alarm on TDM service			
13	FALSE	9/23/2019 9:41	9/23/2019 9:24	10.120.200.74	1	.74 BOTTC	MAJOR		Loss Of Signal (LOS) on TDM-LIC TDM port			
14	FALSE	9/23/2019 8:21	9/23/2019 8:17	10.120.200.74	1	.74 BOTTC	MAJOR		Loss of Carrier			

Viewing a Current Alarms Report

The Current Alarms Report displays the following information.

Field Name	Description
Ack	TRUE if the alarm has been acknowledged, FALSE if not.
Raised Time (System)	The time on the PTP 820 NMS server when the alarm was raised.
Raised Time (NE)	The time on the NE when the alarm was raised.
IP	The IP address of the network resource that generated the alarm.
Slot Number	The slot of the entity that generated the alarm.
Name	The name of the NE that generated the alarm.
Severity	One of the possible alarm severities: CRITICAL, MAJOR, MINOR, WARNING, INDETERMINATE or INFO. Note that severities can be customized using the Error! Reference source not found.
Module	
Description	Lists the most likely reason for the alarm. This is a textual description of the cause of the alarm, displayed exactly as sent from the NE or portrayed in the EMS user interface. The text can be customized using the Error! Reference source not found.

Generating an Alarmed NEs report

The Alarmed NEs report lists the NEs, ordered by number of alarms on the NE.

The date and time values appearing in the report are based on the System Raised Time, that is, the time when PTP 820 NMS received the alarm. Note that both Active and Historical alarms are taken into account when generating this report.

- To generate the report via CLI, refer to [Generating Alarms reports using a CLI command](#).

The following is an example Alarm Log report listing historical alarms:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1														
2	Alarm Log Report													
3														
4	Report Save Time: 2019-09-23 10:30:57													
5														
6	Ack	Raised Time (System)	Cleared Time (System)	Raised Time (NE)	Cleared Time	Slot Num	Name	Severity	Module	Description				
7	FALSE	9/23/2019 9:41		9/23/2019 9:24	10.120.200	1	.74 BOTTIC MAJOR			Protection configuration mismatch!				
8	FALSE	9/23/2019 9:41		9/23/2019 9:24	10.120.200	1	.74 BOTTIC MAJOR			Loss-of-frames alarm on TDM service				
9	FALSE	9/23/2019 9:41		9/23/2019 9:24	10.120.200	1	.74 BOTTIC MAJOR			Loss Of Signal (LOS) on TDM-LIC TDM port				
10	FALSE	9/23/2019 9:41		9/23/2019 9:24	10.120.200	1	.75 TOP MAJOR			Protection configuration mismatch!				
11	FALSE	9/23/2019 9:41		9/23/2019 9:24	10.120.200	1	.75 TOP MAJOR			Loss-of-frames alarm on TDM service				
12	FALSE	9/23/2019 9:41		9/23/2019 9:24	10.120.200	1	.75 TOP MAJOR			Loss Of Signal (LOS) on TDM-LIC TDM port				
13	FALSE	9/23/2019 8:21	9/23/2019 9:41	9/23/2019 8:17	10.120.200	1	.74 BOTTIC MAJOR			Loss-of-frames alarm on TDM service				
14	FALSE	9/23/2019 8:21	9/23/2019 9:41	9/23/2019 8:17	10.120.200	1	.74 BOTTIC MAJOR			Loss Of Signal (LOS) on TDM-LIC TDM port				
15	FALSE	9/23/2019 8:21		9/23/2019 8:17	10.120.200	1	.74 BOTTIC MAJOR			Loss of Carrier				
16	FALSE	9/23/2019 8:21	9/23/2019 9:41	9/23/2019 8:17	10.120.200	1	.75 TOP MAJOR			Loss-of-frames alarm on TDM service				
17	FALSE	9/23/2019 8:21	9/23/2019 9:41	9/23/2019 8:17	10.120.200	1	.75 TOP MAJOR			Loss Of Signal (LOS) on TDM-LIC TDM port				
18	FALSE	9/23/2019 8:21		9/23/2019 8:17	10.120.200	1	.75 TOP MAJOR			Loss of Carrier				

Viewing an Alarmed NEs Report

The Alarmed NES Report displays the following information.

Field Name	Description
Resource Name	The name of the network resource that generated the alarm.
IP	The IP address of the network resource that generated the alarm.
Number of Alarms	The total number of alarms for the network resource in the specified time interval.

Generating an Alarm Frequency report

The Alarm Frequency report lists the most frequent logged alarms in the specified period.

The date and time values appearing in the report are based on the System Raised Time, that is, the time when PTP 820 NMS received the alarm. Note that both Active and Historical alarms are taken into account when generating this report.

- To generate the report via CLI, refer to [Generating Alarms reports using a CLI command](#).

The following is an example Alarm Frequency Report:

	A	B	C	D
1				
2	Alarm Frequency Report			
3				
4	Report Save Time: 2019-09-23 10:35:38			
5				
6	Top-20 Most Frequent Alarms between 2019-09-01 12:00:00 and 2019-09-23 23:59:00			
7				
8	Alarm Text	Number of Alarms		
9	Loss Of Signal (LOS) on TDM-LIC TDM port		4	
10	Loss-of-frames alarm on TDM service		4	
11	Loss of Carrier		2	
12	Protection configuration mismatch!		2	
13				
14	Top-100 Most Frequent Alarms between 2019-09-01 12:00:00 and 2019-09-23 23:59:00			
15				
16	Resource Name	Alarm Text	Severity	Number of Alarms
17	.75 TOP/ETY-1.1	Loss of Carrier	MAJOR	1
18	.75 TOP/E1-1.2	Loss-of-frames alarm on TDM service	MAJOR	1
19	.74 BOTTOM	Protection configuration mismatch!	MAJOR	1
20	.75 TOP/E1-1.1	Loss Of Signal (LOS) on TDM-LIC TDM port	MAJOR	1
21	.74 BOTTOM/E1-1.2	Loss Of Signal (LOS) on TDM-LIC TDM port	MAJOR	1
22	.75 TOP/E1-1.1	Loss-of-frames alarm on TDM service	MAJOR	1
23	.74 BOTTOM/E1-1.2	Loss-of-frames alarm on TDM service	MAJOR	1
24	.75 TOP/E1-1.2	Loss Of Signal (LOS) on TDM-LIC TDM port	MAJOR	1
25	.75 TOP	Protection configuration mismatch!	MAJOR	1
26	.74 BOTTOM/E1-1.1	Loss Of Signal (LOS) on TDM-LIC TDM port	MAJOR	1
27	.74 BOTTOM/ETY-1.1	Loss of Carrier	MAJOR	1
28	.74 BOTTOM/E1-1.1	Loss-of-frames alarm on TDM service	MAJOR	1

Viewing an Alarm Frequency Report

The Alarm Frequency Report displays the following information.

Field Name	Description
Alarm Text	Lists the most likely reason for the alarm. This is a textual description of the cause of the alarm, displayed exactly as sent from the NE or portrayed in the EMS user interface. The text can be customized using the Error! Reference source not found.
Number of Alarms	The total number of alarms for the alarm type/network resource in the specified time interval.
Resource Name	The name of the network resource that generated the alarm.
Severity	One of the possible alarm severities: CRITICAL, MAJOR, MINOR, WARNING, INDETERMINATE or INFO. Note that severities can be customized using the Error! Reference source not found.

Generating an Alarm Frequency by NE report

The Alarm Frequency by NE Report lists the most frequent logged alarms in the specified period, by NE.

The date and time values appearing in the report are based on the System Raised Time, that is, the time when PTP 820 NMS received the alarm. Note that both Active and Historical alarms are taken into account when generating this report.

- To generate the report via CLI, refer to [Generating Alarms reports using a CLI command](#).

The following is an example Alarm Frequency by NE Report:

	A	B	C	D	E	F
1						
2	Alarm Frequency by NE Report					
3						
4	Report Save Time: 2019-09-23 10:52:27					
5						
6	Alarm Overview for the 15 Most Active Network Elements between 2019-09-01 12:00:00 and 2019-09-23 23:59:00					
7						
8	Resource Name	Number of Alarms				
9	.75 TOP	6				
10	.74 BOTTOM	6				
11						
12	Listing of Top-100 Most Frequent Alarms between 2019-09-01 12:00:00 and 2019-09-23 23:59:00 sorted by Most Active Network Element					
13						
14	Element: .75 TOP (Sum alarms: 6)					
15						
16	Resource Name	Alarm Text	Severity	Number of Alarms		
17	.75 TOP/ETY-1.1	Loss of Carrier	MAJOR	1		
18	.75 TOP/E1-1.2	Loss-of-frames alarm on TDM service	MAJOR	1		
19	.75 TOP/E1-1.2	Loss Of Signal (LOS) on TDM-LIC TDM port	MAJOR	1		
20	.75 TOP/E1-1.1	Loss-of-frames alarm on TDM service	MAJOR	1		
21	.75 TOP/E1-1.1	Loss Of Signal (LOS) on TDM-LIC TDM port	MAJOR	1		
22	.75 TOP	Protection configuration mismatch!	MAJOR	1		
23						
24	Element: .74 BOTTOM (Sum alarms: 6)					
25						
26	Resource Name	Alarm Text	Severity	Number of Alarms		
27	.74 BOTTOM/ETY-1.1	Loss of Carrier	MAJOR	1		
28	.74 BOTTOM/E1-1.2	Loss-of-frames alarm on TDM service	MAJOR	1		
29	.74 BOTTOM/E1-1.2	Loss Of Signal (LOS) on TDM-LIC TDM port	MAJOR	1		
30	.74 BOTTOM/E1-1.1	Loss-of-frames alarm on TDM service	MAJOR	1		
31	.74 BOTTOM/E1-1.1	Loss Of Signal (LOS) on TDM-LIC TDM port	MAJOR	1		
32	.74 BOTTOM	Protection configuration mismatch!	MAJOR	1		

Viewing an Alarm Frequency by NE Report

The Alarm Frequency by NE Report displays the following information.

Field Name	Description
Alarm Text	Lists the most likely reason for the alarm. This is a textual description of the cause of the alarm, displayed exactly as sent from the NE or portrayed in the EMS user interface. The text can be customized using the Error! Reference source not found.
Number of Alarms	The total number of alarms for the alarm type/network resource in the specified time interval.
Resource Name	The name of the network resource that generated the alarm.
Severity	One of the possible alarm severities: CRITICAL, MAJOR, MINOR, WARNING, INDETERMINATE or INFO. Note that severities can be customized using the Error! Reference source not found.

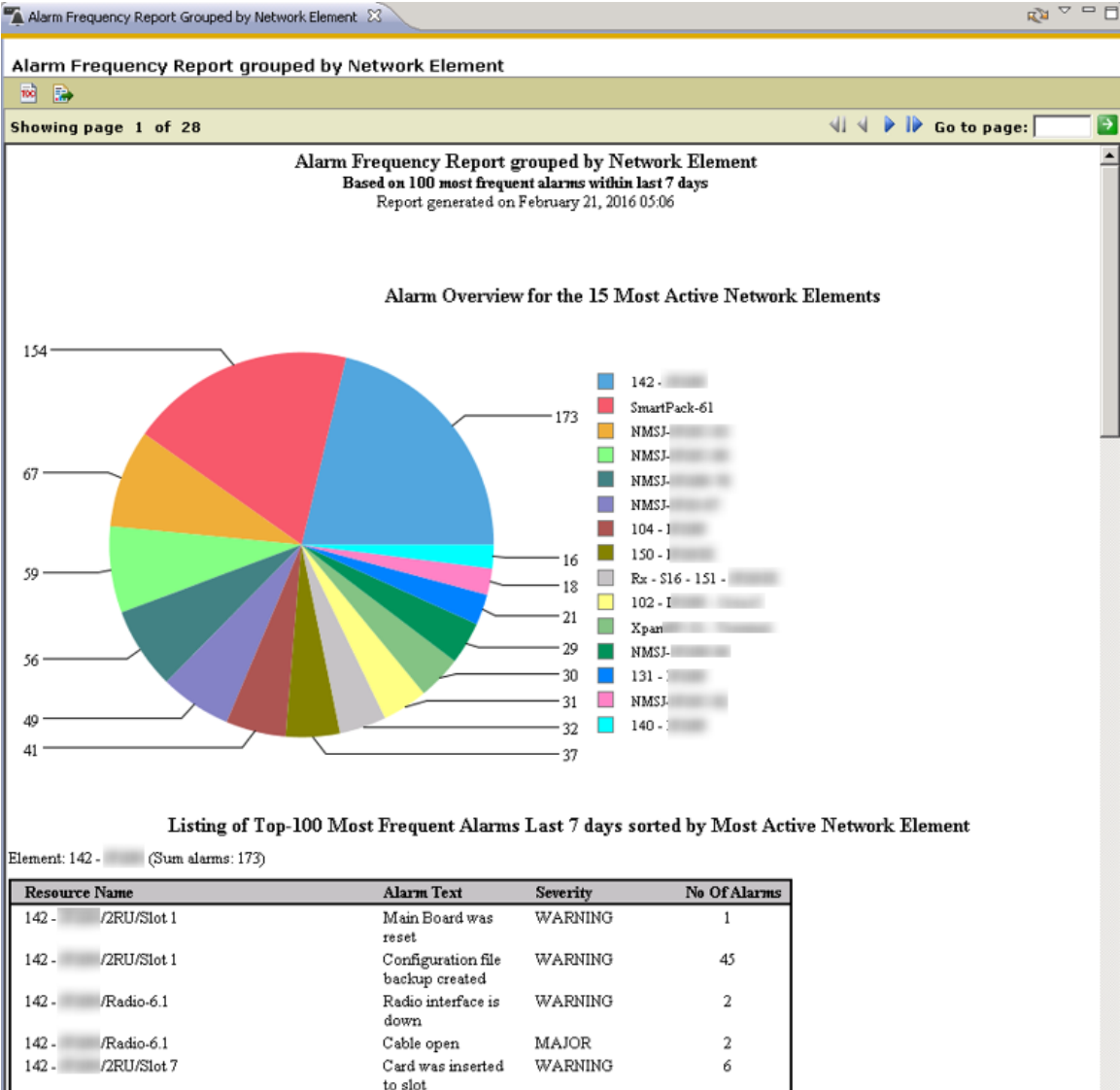
Legacy Alarm Frequency Report grouped by Network Element

The view is opened by selecting **Views > Reports > Alarm Frequency Report grouped by Network Element** from the **main** menu.

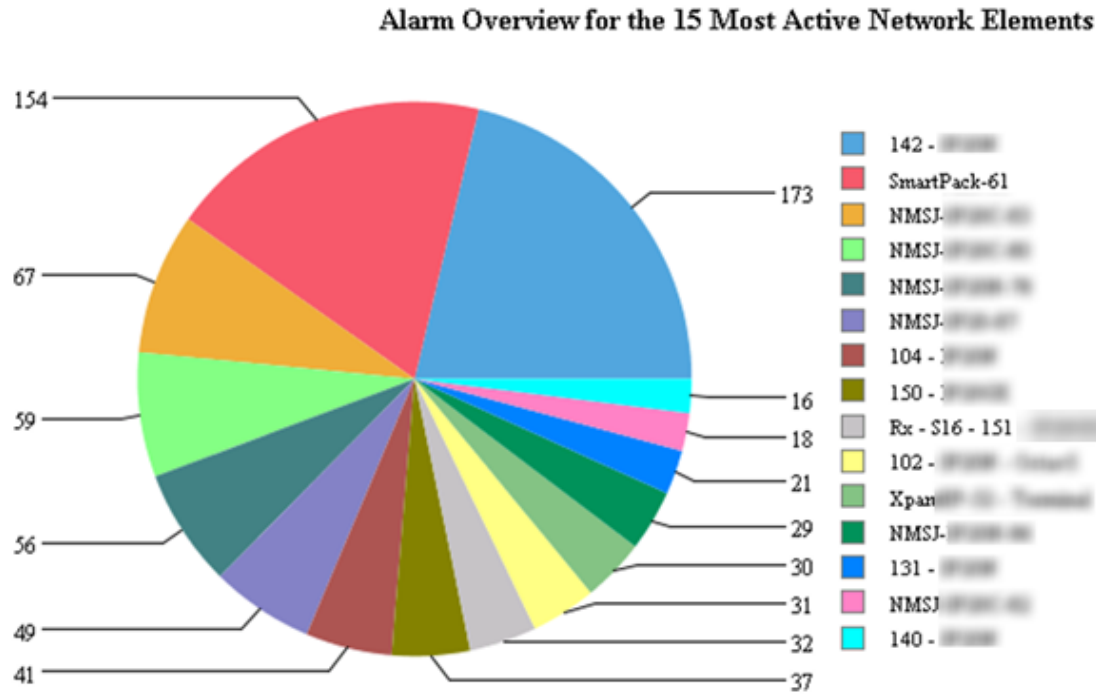
The report displays the 100 most frequent logged alarms in the entire network during the last 7 days. For the purpose of the report, the same alarm on 2 different elements is considered to be 2 different alarms. In addition, the report does not distinguish between alarms on managed and unmanaged network elements. Note also that alarms on network elements that have been removed from a managed state may be displayed in the report.

Viewing an Alarm Frequency Report grouped by Network Element

The following is an example of an Alarm Frequency Report grouped by Network Element:



Alarm Overview for the 15 Most Active Network Elements



The **Alarm Overview for the 15 Most Active Network Elements** chart displays the 100 most frequent alarms grouped by Network Element where the total number of occurrences is given as a number associated with each slice. The chart displays the 15 most active Network Elements; i.e. the elements with the most occurrences of alarms.

For example:

- If Network Element A has 3 top 100 most frequent alarms where there are 8 occurrences of each alarm, then the element will be displayed as a slice with a value of 24.
- If Network Element B has 1 alarm type among the top 100 most frequent alarms, but 20 occurrences, then the element is displayed as a slice with a value of 20.

Listing of Top-100 Most Frequent Alarms Sorted by Most Active Network Element

Listing of Top-100 Most Frequent Alarms Last 7 days sorted by Most Active Network Element

Element: 142 - **PHN** (Sum alarms: 173)

Resource Name	Alarm Text	Severity	No Of Alarms
142 - PHN	Main Board was reset	WARNING	1
142 - PHN	Configuration file backup created	WARNING	45
142 - PHN	Radio interface is down	WARNING	2
142 - PHN	Cable open	MAJOR	2
142 - PHN	Card was inserted to slot	WARNING	6
142 - PHN	Remote communication failure	CRITICAL	2
142 - PHN	Ethernet interface is up	WARNING	3
142 - PHN	RFU communication failure	WARNING	4
142 - PHN	Configuration file transfer failure	WARNING	36
142 - PHN	User issued command for transfer of configuration file	WARNING	46
142 - PHN	Loss-of-frames alarm on TDM	MAJOR	2










The tables in the **Listing of Top-100 Most Frequent Alarms Sorted by Most Active Network Element** section are sorted by number of alarms within the top 100 most frequent ones.

The alarms are grouped by the name of the element. The ordering of the elements is given by the NI with the highest occurrences of alarms.

For each alarm the following information is displayed:

Name	Explanation
Resource Name	Source of alarm - the network resource that generated the alarm
Alarm Text	Gives the most likely reason for the alarm
Severity	The alarm severity
No Of Alarms	The number of occurrences of this alarm (i.e. how many times this alarm has been turned on and off)

Available operations

-  TOC button: toggle the display of the table of contents pane. The TOC pane displays all NEs in the report grouped by NE type
-  Export button: export the report to another format, e.g. in order to print it.
-  Navigate to first page
-  Navigate to previous page
-  Navigate to next page
-  Navigate to last page
-  Refresh the entire report
-  **Go to page:**  Navigate to a specific page by specifying a number and then press the green arrow

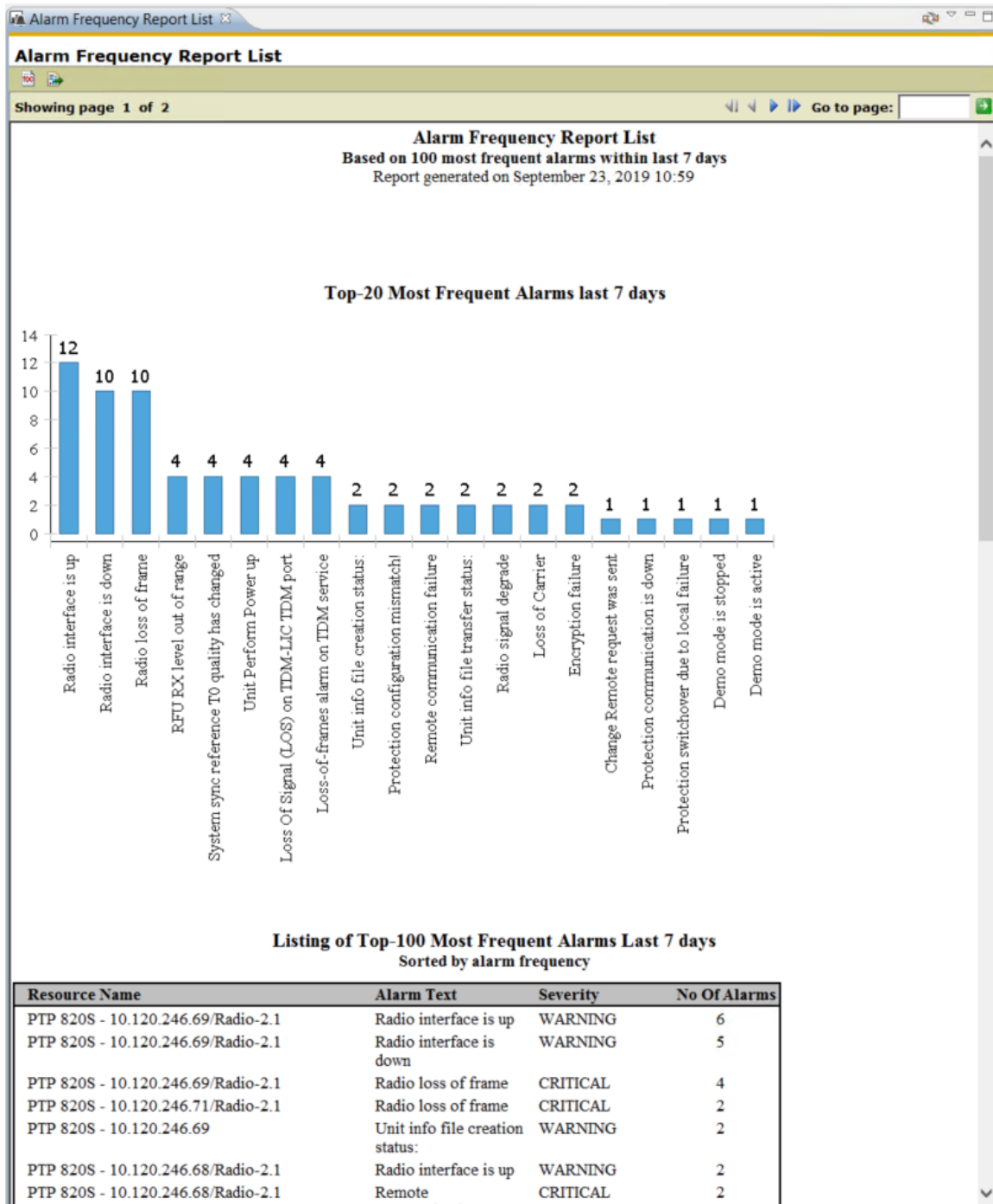
Legacy Alarm Frequency Report List

The view is opened by selecting **Views > Reports > Alarm Frequency Report List** from the **main** menu.

The Alarm Frequency Report List report displays the 100 most frequent logged alarms in the entire network during the last 7 days. For the purpose of the report, the same alarm on 2 different elements is considered to be 2 different alarms. In addition, the report does not distinguish between alarms on managed and unmanaged network elements. Note also that alarms on network elements that has been removed from a managed state may be displayed in the report.

Viewing an Alarm Frequency Report List

The following is an example of an Alarm Frequency Report List:



Top-20 Most Frequent Alarms

Listing of Top-100 Most Frequent Alarms Last 7 days Sorted by alarm frequency			
Resource Name	Alarm Text	Severity	No Of Alarms
PTP 820S - 10.120.246.69/Radio-2.1	Radio interface is up	WARNING	6
PTP 820S - 10.120.246.69/Radio-2.1	Radio interface is down	WARNING	5
PTP 820S - 10.120.246.69/Radio-2.1	Radio loss of frame	CRITICAL	4
PTP 820S - 10.120.246.71/Radio-2.1	Radio loss of frame	CRITICAL	2
PTP 820S - 10.120.246.69	Unit info file creation status:	WARNING	2
PTP 820S - 10.120.246.68/Radio-2.1	Radio interface is up	WARNING	2
PTP 820S - 10.120.246.68/Radio-2.1	Remote communication failure	CRITICAL	2
PTP 820S - 10.120.246.68/Radio-2.1	Radio loss of frame	CRITICAL	2
PTP 820S - 10.120.246.69	Unit info file transfer status:	WARNING	2
PTP 820S - 10.120.246.71/Radio-2.1	Radio interface is up	WARNING	2
PTP 820S - 10.120.246.68/Radio-2.1	Radio interface is down	WARNING	2
PTP 820S - 10.120.246.70/Radio-2.1	Radio interface is down	WARNING	2
PTP 820S - 10.120.246.70/Radio-2.1	Radio loss of frame	CRITICAL	2
PTP 820S - 10.120.246.70/Radio-2.1	Radio interface is up	WARNING	2
PTP 820S - 10.120.246.71/Radio-2.1	Radio signal degrade	MINOR	1
PTP 820S - 10.120.246.71/Radio-2.1	Encryption failure	CRITICAL	1
PTP 820S - 10.120.246.68	Demo mode is stopped	WARNING	1
PTP 820S - 10.120.246.71	Unit Perform Power up	WARNING	1
PTP 820S - 10.120.246.68	Change Remote	MAJOR	1

The **Top-20 Most Frequent Alarms** bar graph is sorted by Alarm Text. Only the top 20 most frequent alarms are shown in this bar. This bar graph gives a clear indication when alarms of a specific Alarm Text occur very often in the system.

Listing of Top-100 Most Frequent Alarms Sorted by Alarm Frequency










Listing of Top-100 Most Frequent Alarms Last 7 days Sorted by alarm frequency			
Resource Name	Alarm Text	Severity	No Of Alarms
IP-20E - 10.10.66.156/Radio-16.1	Radio interface is up	WARNING	2530
IP-20E - 10.10.66.156/Radio-16.1	Radio loss of frame	CRITICAL	2514
IP-20E - 10.10.66.156/Radio-16.1	Radio interface is down	WARNING	2511
150 - IP20GX/IDU/Fan	Extreme Temperature	MAJOR	31
IP-20E - 10.10.66.156	User issued command for transfer of configuration file	WARNING	8
IP-20E - 10.10.66.156	Configuration file transfer in progress	WARNING	8
IP-20E - 10.10.66.156	Software download status:	WARNING	8
IP-20E - 10.10.66.155	Software download status:	WARNING	8
IP-20E - 10.10.66.155	Software installation status:	WARNING	7
IP-20E - 10.10.66.156	Software installation status:	WARNING	6
IP-20E - 10.10.66.156	Configuration file transfer successful	WARNING	6
142 - IP20N/2RU/Slot 1	User issued command for transfer of configuration file	WARNING	5
146 - IP20N/1RU/Slot 1	User issued command for transfer of configuration file	WARNING	5

The table in the **Listing of Top-100 Most Frequent Alarms Sorted by Alarm Frequency** is sorted by No of Alarms in descending order.

For each alarm the following information is displayed:

Name	Explanation
Resource Name	Source of alarm - the network resource that generated the alarm
Alarm Text	Gives the most likely reason for the alarm
Severity	The alarm severity
No Of Alarms	The number of occurrences of this alarm (i.e. how many times this alarm has been turned on and off)

Available operations

-  TOC button: toggle the display of the table of contents pane. The TOC pane displays all NEs in the report grouped by NE type
-  Export button: export the report to another format, e.g. in order to print it.
-  Navigate to first page
-  Navigate to previous page
-  Navigate to next page
-  Navigate to last page
-  Refresh the entire report
-  **Go to page:**  Navigate to a specific page by specifying a number and then press the green arrow

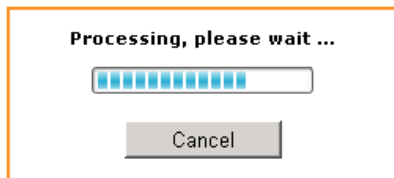
Legacy Network Element Types Overview Report

The view is opened by selecting an NE or domain node in one of the topological views and **selecting Reports > Network Element Types Overview Report** in the [Context](#) menu. The view will then open with the selection as a [scope](#) presenting only report data for the currently selected NEs.

Alternatively you can open the view unscoped by selecting Views | Reports | NE Types Overview Report from the main menu. The view will then present report data from the entire network in the same table. Please note that the time consumed for this operation is a function of the number of nodes and resources per node in the network, and might cause a delay if your network is large.

When generating a report the system displays the progress bar shown below.

Figure 171 NE type report

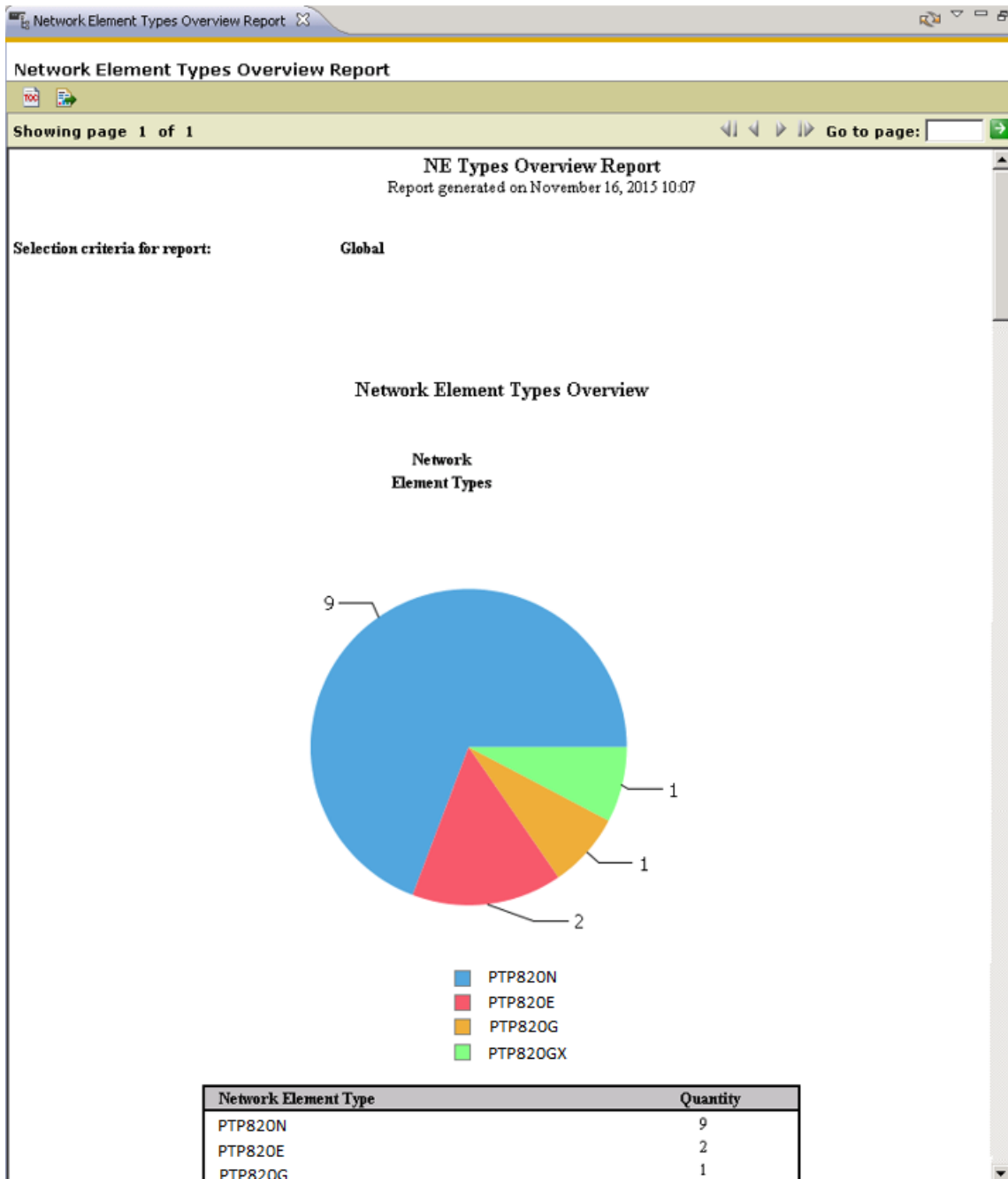


The only operation available to the user is to cancel the report.

The first time a report is opened after the PTP 820 NMS server is started, the report framework is loaded. This initial loading consumes extra resources. The subsequent reports will consume less resource and run faster.

When processing completes, the report is displayed.

Figure 172 NE type report view












The NE Types Overview report displays a chart and a table indicating how many elements of each NE type are managed by PTP 820 NMS within the scope of the report.

- A chart and table indicating the breakdown of different element configurations among the NEs managed by PTP 820 NMS within the scope of the report.
- A summary that displays:
- Actual number of Elements and Radio Licenses in license.
 - Use by the selected managed elements / Available Licenses / Total number of Licenses

- Actual number of OpenSNMP Licenses in use by the selected managed elements / Available Licenses / Total number of Licenses
- Total number of managed elements in the scope of the report or in the system
- Total number of different network element types in the scope of the report
- Total number of different element configurations in the scope of the report

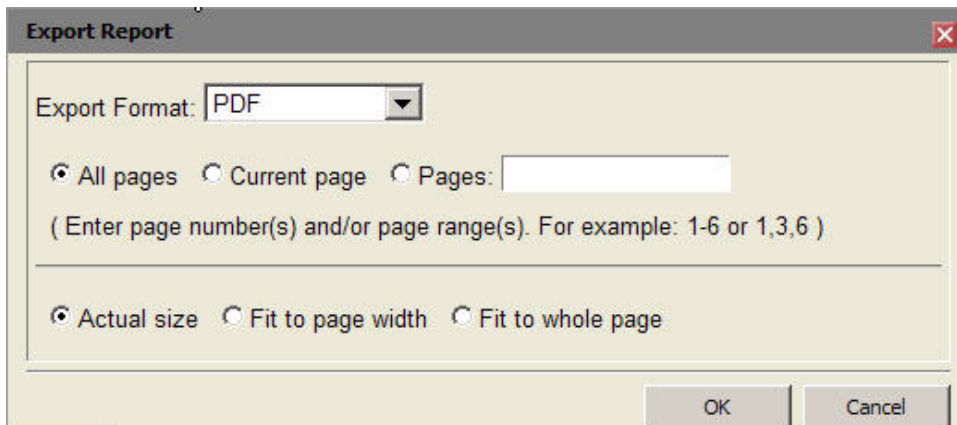
Available operations

-  TOC button: toggles table of contents
-  Export button: export report to another format, e.g. in order to print it.
-  Navigate to first page
-  Navigate to previous page
-  Navigate to next page
-  Navigate to last page
-  Refresh the entire report
-  **Go to page:**  Navigate to a specific page by specifying a number and then press the green arrow

Export Report dialog

The Export Report dialog is opened by pressing the [Export button](#).

Figure 173 Export report dialog



It is possible to export the reports to external formats in order to store the report or print it. The format of the report will change to the better when displayed in an external format viewer as for example Adobe Reader for PDF-format.

It is recommended to use the external PDF-format before printing the report.

Select Export format from the list and then press the OK button. The report may then be opened by an installed viewer for the chosen format or stored on disk for later processing. If opening the report by an installed viewer on the PTP 820 NMS client, it will be automatically started in a separate window dispatched from the PTP 820 NMS client.

The PTP 820 NMS installation does not include any viewer for the external formats.

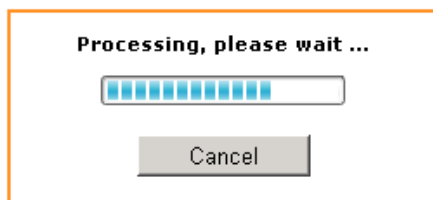
Legacy Inventory Report

The view is opened by selecting an NE or domain node in one of the topological views and selecting **Reports > Inventory Report** in the [Context](#) menu. The view will then open with the selection as a [scope](#) presenting only report data for the currently selected NEs.

Alternatively you can open the view unscoped by selecting **Views > Reports > Inventory Report** from the main menu. The view will then present report data from the entire network in the same table. Please note that the time consumed for this operation is a function of the number of nodes and resources per node in the network, and might cause a delay if your network is large.

When generating a report, the system displays the progress bar shown below.

Figure 174 Generating a inventory report



The only operation available to the user is to cancel the report.

The first time a report is opened after the PTP 820 NMS server is started, the report framework is loaded. This initial loading consumes extra resources. The subsequent reports will consume less resource and run faster.

When processing completes, the report is displayed.

Figure 175 Hardware and software inventory report

Inventory Report

Showing page 1 of 4

Inventory Report
Report generated on November 16, 2015 10:47

Selection criteria for report: Global

Elements of type: IP-20E

Element: - 10.10.66.155
Configuration: 140

HW Inventory

Resource Name	Article Code	Serial No.	Revision	Production Date
- 10.10.66.155/ODU	25-0001-0A	F204F02959	NA	

SW Inventory

Software Name	Version	Build Time	Memory Bank	Status
MCU Package	7.9.0.0.0.196		Running	ACTIVE

Transmission Inventory

Resource name	Tx Freq. (MHz)	Rx Freq. (MHz)	ATPC Space Diversity	Tx Capacity (Mb/s)	Tx TDM Capacity (Mb/s)	Bandwidth (MHz)
- 10.10.66.155/Radio-16.1	85,999	72,000	N N	262.188		250

Element: IP-20E - 10.10.66.156
Configuration: 140

HW Inventory

Resource Name	Article Code	Serial No.	Revision	Production Date
- 10.10.66.156/ODU	25-0001-0J	UM13421860	NA	

SW Inventory

Software Name	Version	Build Time	Memory Bank	Status
MCU Package	7.9.0.0.0.196		Installed	ACTIVE
MCU Package	7.9.0.0.0.196		Downloaded	IDLE

Transmission Inventory

Resource name	Tx Freq. (MHz)	Rx Freq. (MHz)	ATPC Space Diversity	Tx Capacity (Mb/s)	Tx TDM Capacity (Mb/s)	Bandwidth (MHz)
- 10.10.66.156/Radio-16.1	72,000	81,124	N N	262.188		250

Company Confidential

Page 1 of 4

The Inventory report displays hardware, software, and transmission inventories for all the managed elements within the scope of the report.

The fields displayed in the inventory report can be grouped into three main categories; hardware, software, and transmission inventory.

Report Header

The header contains the title of the report and the time that the report was generated.

In addition, the header may contain information about the scope of the report.

HW Inventory table

The hardware inventory part of the report displays the following fields for each NE:

Table 45 HW inventory table

Name	Explanation
Resource Name	Name/location of this hardware element in the NE.
Article Code	Uniquely identifies the type of hardware element.
Serial no.	The serial number of the hardware element.
Revision	The hardware revision.
Production date	When the production process was completed for this hardware element.

SW Inventory table

The software inventory part of the report presents the following fields for each memory bank on the NE:

Table 46 SW inventory table

Name	Explanation
Software Name	The name of the software in this memory bank, as read from the NE.
Version	The software revision. Normally a five character code, but the field will display NA if the system has this unit present but is unable to retrieve the information from it.
Build Time	When this software was created.
Memory Bank	The software location on the NE

Name	Explanation
Status	<p>Displays the status of the memory bank and can be one of the following values:</p> <p>IDLE: Software is not being executed</p> <p>ACTIVE: Software is being executed</p> <p>ACTIVE_PENDING: Software is waiting to be executed (will be activated on next restart)</p> <p>DOWNLOADING: SW is being downloaded to this bank.</p> <p>ERASING FLASH: SW is being erased (during a download process)</p> <p>INVALID: corrupt software or wrong software version; SW Download has failed or SW bank has not been used.</p> <p>NOT_AVAILABLE: The IDU does not have contact with the unit using this software (only relevant for ODU banks) or corrupted memory bank</p>

Transmission Inventory table

The transmission inventory part of the report displays the following fields for each NE:

Table 47 SW inventory table










Name	Explanation
Resource Name	The radio interface.
Tx Freq. (MHz)	The transmission radio frequency of the radio interface.
Rx Freq. (MHz)	The received radio frequency of the radio interface.
ATPC	Indicates whether ATPC is configured on the interface.
Space Diversity	Indicates whether Space Diversity is configured on the interface.
Tx Capacity (Mb/s)	The available transmission capacity.
Tx TDM Capacity (Mb/s)	The available received TDM capacity (not provided for PTP820 equipment)
Bandwidth (MHz)	The bandwidth of the radio interface

Table Of Contents pane

The Table Of Contents pane can be opened by pressing the [TOC button](#) on the Inventory Report toolbar.

When the Table Of Contents pane is opened, the left hand side of the report contains a section displaying all NEs in the report grouped by NE type. It is possible to expand each NE type and access each specific NE directly by clicking on it.

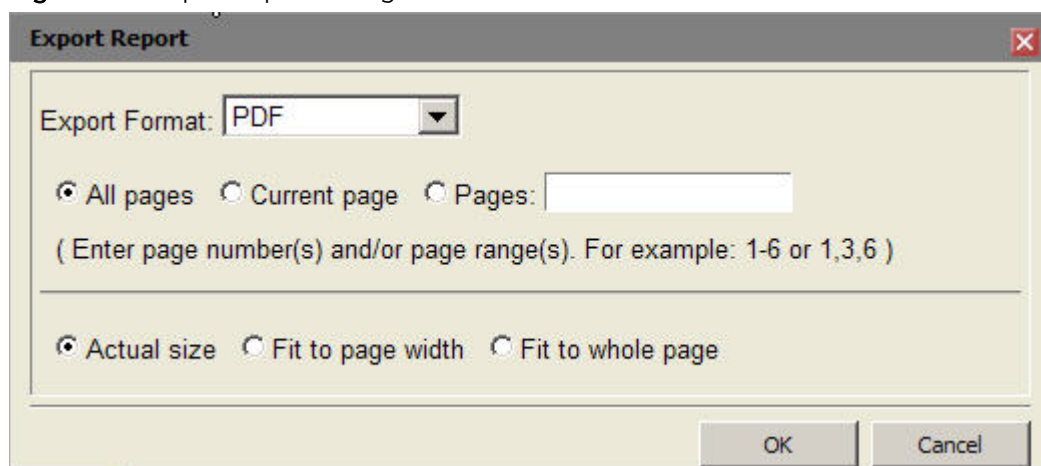
Available operations

-  TOC button: toggles table of contents
-  Export button: export report to another format, e.g. in order to print it.
-  Navigate to first page
-  Navigate to previous page
-  Navigate to next page
-  Navigate to last page
-  Refresh the entire report
-  **Go to page:**  Navigate to a specific page by specifying a number and then press the green arrow

Export Report dialog

The Export Report dialog is opened by pressing the [Export button](#).

Figure 176 Export report dialog



It is possible to export the reports to external formats in order to store the report or print it. The format of the report will change to the better when displayed in an external format viewer as for example Adobe Reader for PDF-format.

It is recommended to use the external PDF-format before printing the report.

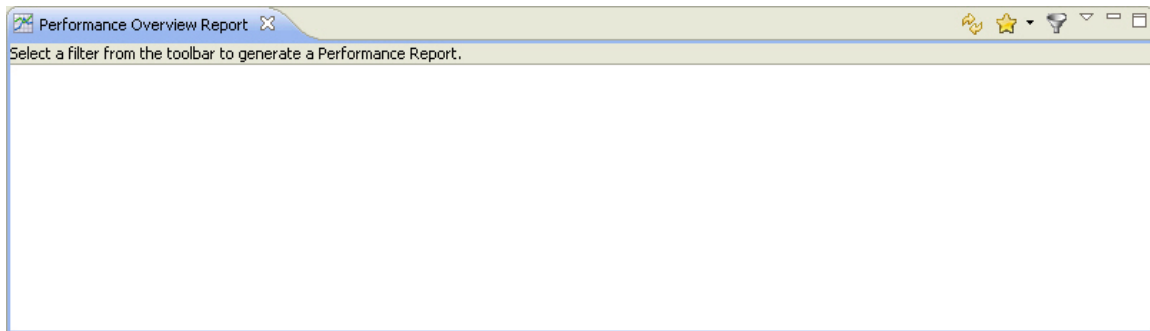
Select Export format from the list and then press the OK button. The report may then be opened by an installed viewer for the chosen format or stored on disk for later processing. If opening the report by an installed viewer on the PTP 820 NMS client, it will be automatically started in a separate window dispatched from the PTP 820 NMS client.

The PTP 820 NMS installation does not include any viewer for the external formats.

Legacy Performance Overview Report

The view is opened by selecting **Views > Reports > Performance Overview** Report from the main menu. The view will come up empty with a message saying you have to select a filter.

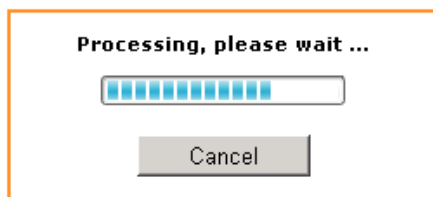
Figure 177 Performance report



If you already have defined a performance filter, select it from the [Filters](#) dropdown menu. Otherwise press the Filter Manager icon in the toolbar to create a filter in the [Filter Manager](#) view.

From the Filter dropdown menu, select the filter and report generation starts as shown below.

Figure 178 Generating performance report

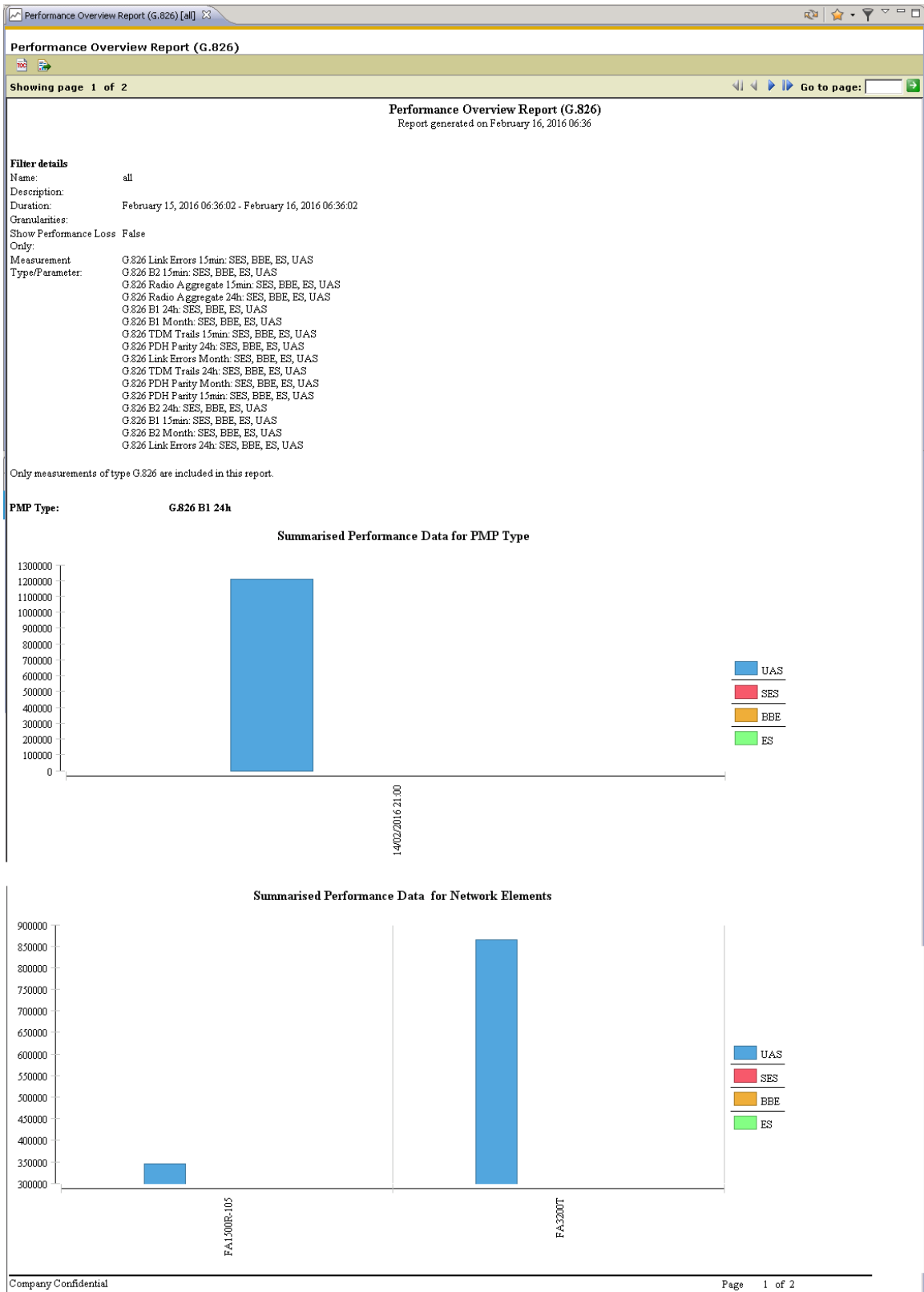


The only operation available during report generation, is to cancel the report.

The first time a report is opened after the PTP 820 NMS server is started, the report framework is loaded. This initial loading consumes extra resources. The subsequent reports will consume less resource and run faster.

When processing completes, the report is displayed.

Figure 179 Performance report view



The Performance Overview report can be used to localize NE and time periods with performance problems. For more details about analyzing the results, see the chapter about [how to use the performance reports](#).

The report displays a summary of the performance measurement points matching the filter you specified. Two graphical representations are made; one graph showing errors over time and one graph showing errors for each network element.

Only periodic measurements of type G.826 [B1](#), G.826 [B2](#) or G.826 [PDH parity](#) is included in the report.

Report Header

The header contains the title of the report and the time that the report was generated.

Filter details

The filter details contain a summary of the applied filter settings.

Filter details	
Name:	all
Description:	
Duration:	February 15, 2016 06:36:02 - February 16, 2016 06:36:02
Granularities:	
Show Performance Loss	False
Only:	
Measurement	G.826 Link Errors 15min: SES, BBE, ES, UAS
Type/Parameter:	G.826 B2 15min: SES, BBE, ES, UAS
	G.826 Radio Aggregate 15min: SES, BBE, ES, UAS
	G.826 Radio Aggregate 24h: SES, BBE, ES, UAS
	G.826 B1 24h: SES, BBE, ES, UAS
	G.826 B1 Month: SES, BBE, ES, UAS
	G.826 TDM Trails 15min: SES, BBE, ES, UAS
	G.826 PDH Parity 24h: SES, BBE, ES, UAS
	G.826 Link Errors Month: SES, BBE, ES, UAS
	G.826 TDM Trails 24h: SES, BBE, ES, UAS
	G.826 PDH Parity Month: SES, BBE, ES, UAS
	G.826 PDH Parity 15min: SES, BBE, ES, UAS
	G.826 B2 24h: SES, BBE, ES, UAS
	G.826 B1 15min: SES, BBE, ES, UAS
	G.826 B2 Month: SES, BBE, ES, UAS
	G.826 Link Errors 24h: SES, BBE, ES, UAS

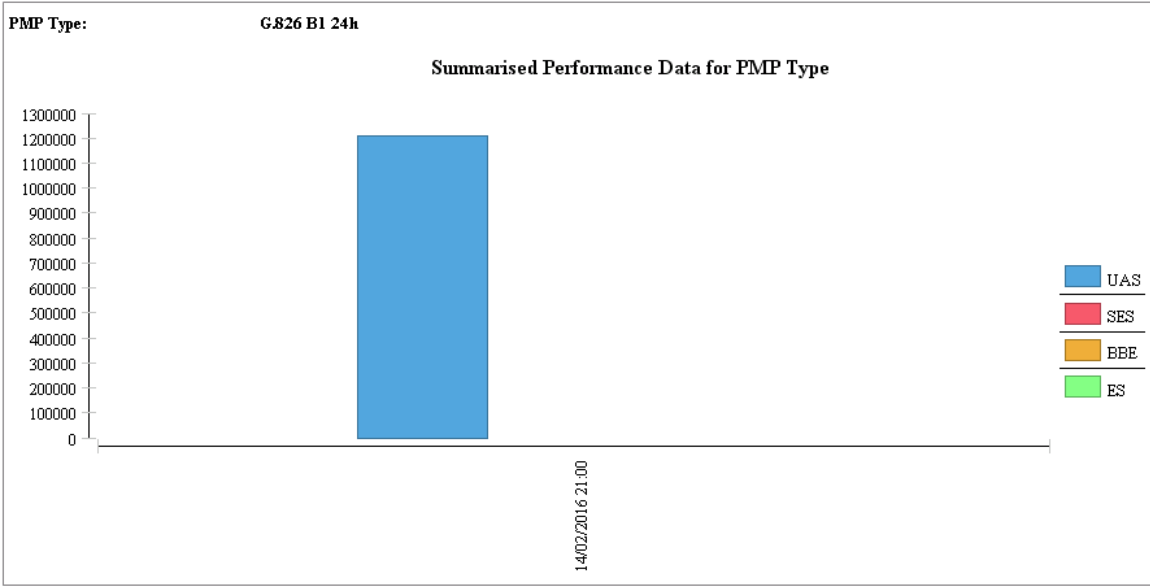
Time View

The performance graph section displays a sum of performance measurements grouped by granularity (15 Min, 24 hour) and measurement type (G.826 [B1](#), G.826 [B2](#), G.826 [PDH parity](#)).

Time Graph

The time graph shows a sum of errors for each sampled time period.

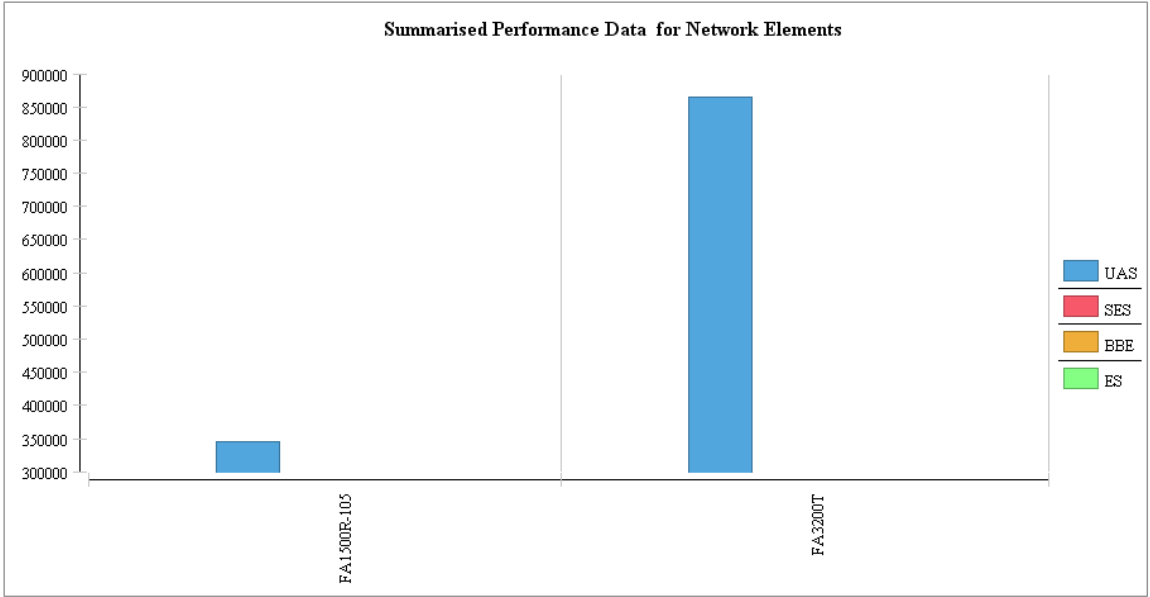
Figure 180 Performance time graph



Element View

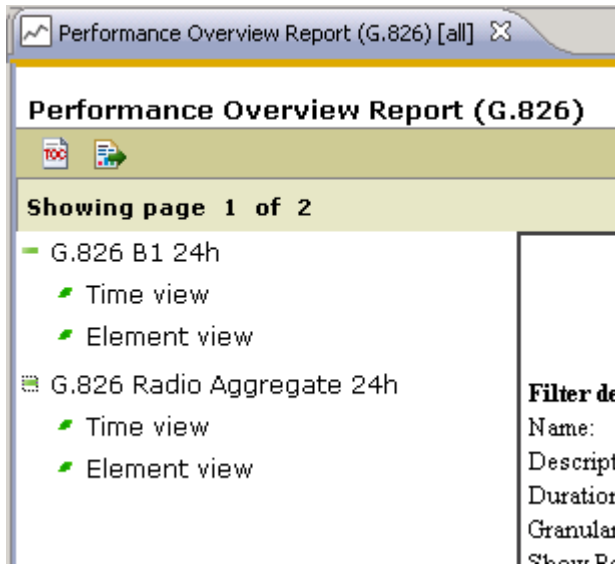
The summarised graph shows a summation of parameters for each managed element. The order of the elements is according to the order in the specified filter.

Figure 181 Performance summarized graph



TOC Browser area

The TOC Browser area of the report contains a table of content, which can be used for navigation within the report. Click the [TOC](#) button to show/hide the TOC Browser. Click the tree structure in the TOC to navigate to different graphs in the Performance Overview Report.



Figure 182 Performance report TOC

Measurement Types

- G.826 [B1](#): One byte of the SOH frame is allocated for regenerator section error monitoring. This B1 byte contains a Bit Interleaved Parity 8 (BIP-8) code using even parity. The BIP-8 is computed over all bits of the previous STM-1 frame after scrambling and is placed in byte B1 of the current frame before scrambling.
- G.826 [B2](#): Three bytes of the SOH frame is allocated for multiplex section error monitoring. The B2 bytes contain a Bit Interleaved Parity 24 (BIP-24) code using even parity. The BIP-24 is computed over all bits of the previous STM-1 frame except for the first three rows of SOH and is placed in the B2 bytes of the current frame before scrambling.
- G.826 [PDH parity](#): Bits in the proprietary PDH frame is allocated for error monitoring.

Available operations

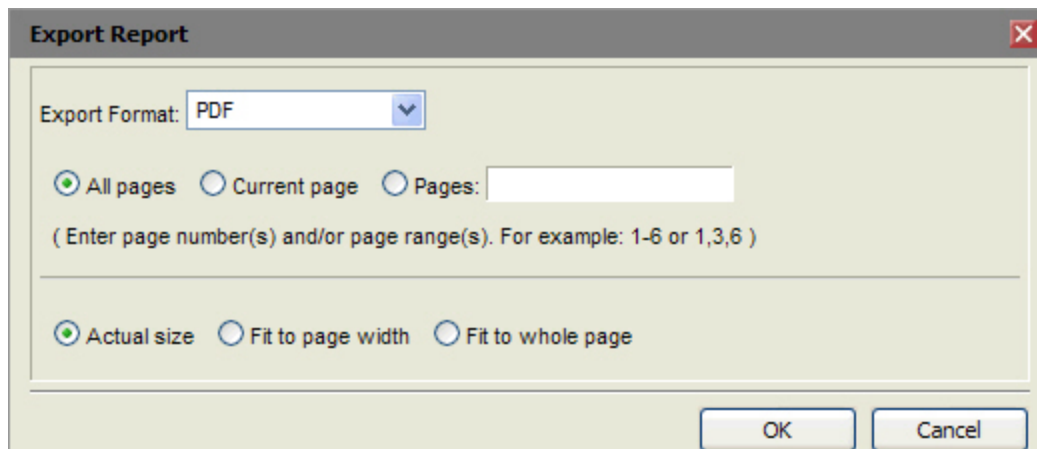
- TOC button: toggles table of contents
- Export button: export report to another format, e.g. in order to print it.
- Navigate to first page
- Navigate to previous page
- Navigate to next page
- Navigate to last page
- Refresh the entire report
- Go to page: Navigate to a specific page by specifying a number and then press the green arrow

-  Click the Filters dropdown menu to pick a filter from a list of user-defined Performance filters, as defined in the Filter Manager view. The selected filter will be used for generating a Performance Overview report. When a filter is applied, it will be displayed as an additional scope (presented in brackets) on the View tab.
-  Open the Filter Manager View

Export Report dialog

- The Export Report dialog is opened by pressing the [Export](#) button.

Figure 183 Export report dialog

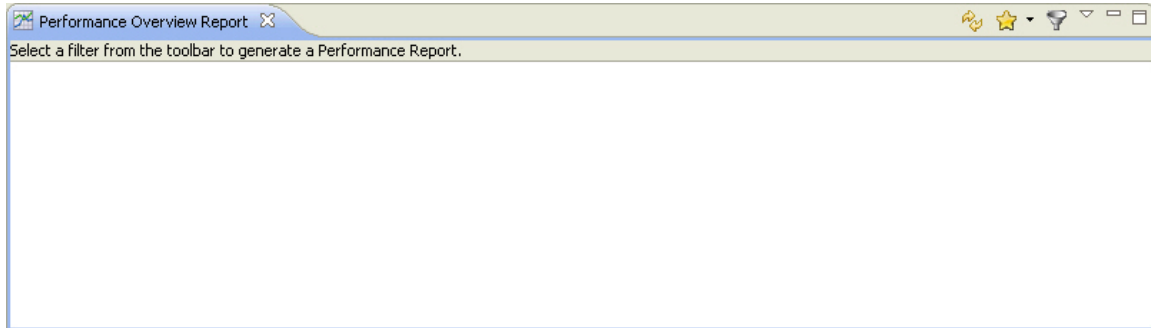


- It is possible to export the reports to PDF and Microsoft Excel formats in order to store the report or print it. The format of the report will change to the better when displayed in an external format viewer as for example Adobe Reader for PDF-format.
- It is recommended to use the external PDF-format before printing the report.
- Select Export Format from the list and then press the **OK** button. The report may then be opened by an installed viewer for the chosen format or stored on disk for later processing. Reports opened by an installed viewer will appear in a separate window dispatched from the PTP 820 NMS client.
- The PTP 820 NMS installation does not include any viewer for the external formats.

Legacy Performance Details Report

The view is opened by selecting **View > Reports > Performance Details** Report from the main menu. The view will come up empty with a message saying you have to select a filter.

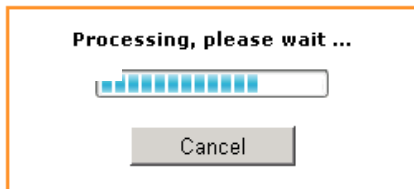
Figure 184 Performance detailed report



If you already have defined a performance filter, select it from the [Filters](#) dropdown menu. Otherwise press the [Filter Manager](#) icon in the view-toolbar, to create a filter in the [Filter Manager](#) view.

From the Filter dropdown menu, select the filter and report generation starts as shown below.

Figure 185 Generating performance detailed report

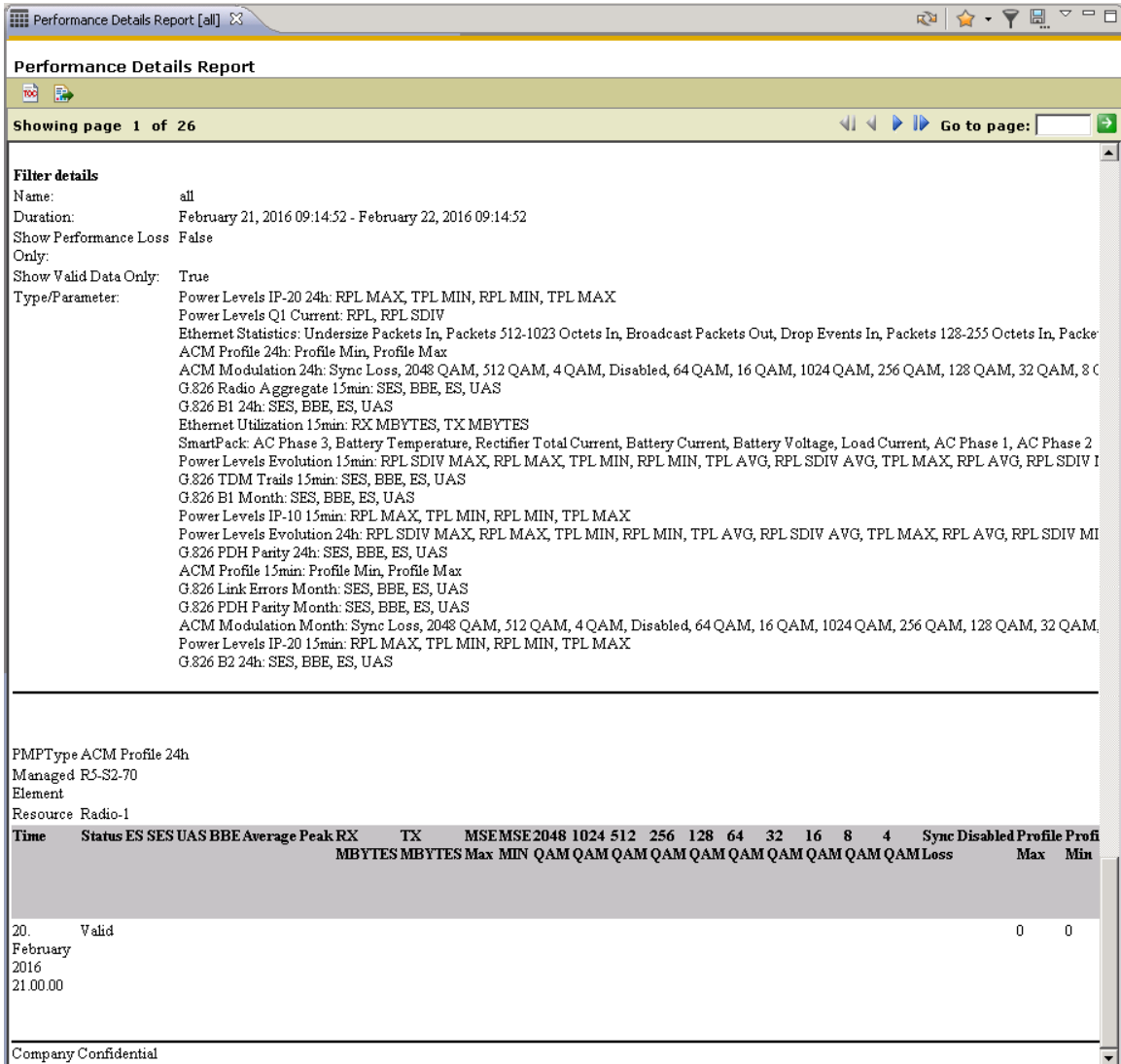


The only operation available during report generation, is to cancel the report.

Please note that the first time a report is opened after the PTP 820 NMS server is started, the report framework is loaded. This initial loading consumes extra resources. The subsequent reports will consume less resource and run faster.

When processing completes, the report is displayed.

Figure 186 Performance detailed report view



The Performance Details is used for analyzing NE and time periods with performance problems. For more details about how to pinpoint NE and periods, see the chapter about [how to use the performance reports](#).

The report displays the performance measurement points matching the filter you specified. Currently there are two types of measurement points available: Periodic measurements and analogue measurements. Periodic measurement are measurements cumulated over a predefined period of time (15 minutes or 24 hours) while analog values are instant.

Report Header

The header contains the title of the report and the time that the report was generated.

Filter details

The filter details contain a summary of the applied filter settings.

Filter details	
Name:	all
Duration:	February 21, 2016 09:14:52 - February 22, 2016 09:14:52
Show Performance Loss Only:	False
Show Valid Data Only:	True
Type/Parameter:	Power Levels IP-20 24h: RPL MAX, TPL MIN, RPL MIN, TPL MAX

Performance Details

The performance details section contains performance details for a managed element and contained resources.

Figure 187 Performance details

Time	Status	ES	SES	UAS	BBE	Average	Peak	RX	TX	MSE	MSE	2048	1024	512	256	128	64	32	16	8	4	Sync Disabled	Profile	Profi
								MBYTES	MBYTES	Max	MIN	QAM	QAM	QAM	QAM	QAM	QAM	QAM	QAM	QAM	QAM	Loss	Max	Min
20. February 2016 21.00.00	Valid																						0	0

For each resource the following information is displayed:

Table 48 Performance table attributes

Name	Explanation
Time	Time of the measurement period.
Type	Type of measurement, see Measurement Types below.
Status	The status of the measurement: Data OK: The measurement has been conducted over a complete period. Data not OK: Measurement period is incomplete (due to SW restart), or the NE clock has been adjusted more than 10 seconds during the measurement period.
ES	Errored Seconds. The number of one second periods with one or more errored blocks.
SES	Severely Errored Seconds. The number of one-second periods which contains > 30% errored blocks or at least one Severely Disturbed Period (SDP). A SDP is a period where Loss Of Signal (LOS) or Loss Of Frame (LOF) has been detected. SES is a subset of ES.

Name	Explanation
UAS	The number of UnAvailable Seconds. A period of unavailable time begins at the onset of 10 consecutive SES events. These ten seconds are considered to be a part of the unavailable time. A new period of available time begins at the onset of ten consecutive non-SES events. These 10 seconds are considered to be part of available time.
BBE	The number of Background Block Errors. An errored block not occurring as part of an SES.
Tx	Transmitter Power Level (dBm)
Rx	Receiver Power Level (dBm)

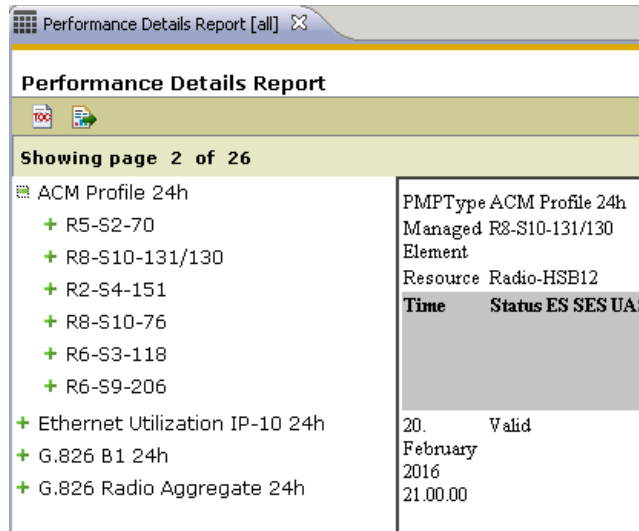
Measurement Types

- G.826 [B1](#): One byte of the SOH frame is allocated for regenerator section error monitoring. This B1 byte contains a Bit Interleaved Parity 8 (BIP-8) code using even parity. The BIP-8 is computed over all bits of the previous STM-1 frame after scrambling and is placed in byte B1 of the current frame before scrambling.
- G.826 [B2](#): Three bytes of the SOH frame is allocated for multiplex section error monitoring. The B2 bytes contain a Bit Interleaved Parity 24 (BIP-24) code using even parity. The BIP-24 is computed over all bits of the previous STM-1 frame except for the first three rows of SOH and is placed in the B2 bytes of the current frame before scrambling.
- G.826 [PDH parity](#): Bits in the proprietary PDH frame is allocated for error monitoring.

TOC Browser area

The TOC Browser area of the report contains a table of content, which can be used for navigation within the report. Click the [TOC](#) button to show/hide the TOC Browser. Click the tree structure in the TOC to navigate to pages containing different data in the Performance Details Report.

Figure 188 Performance report TOC



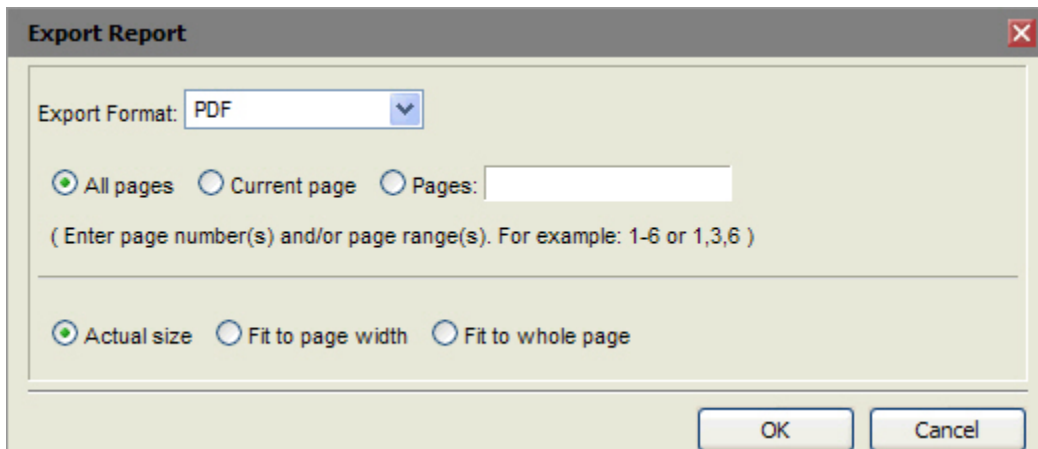
Available operations

- TOC button: toggles table of contents
- Export button: export report to another format, e.g. in order to print it.
- Navigate to first page
- Navigate to previous page
- Navigate to next page
- Navigate to last page
- Refresh the entire report
- **Go to page:** Navigate to a specific page by specifying a number and then press the green arrow
- Click the Filters dropdown menu to pick a filter from a list of user-defined Performance filters, as defined in the Filter Manager view. The selected filter will be used for generating a Performance Details report. When a filter is applied, it will be displayed as an additional scope (presented in brackets) on the View tab.
- Open the Filter Manager View
- Exports the content of the report as is without any formatting.

Export Report dialog

The Export Report dialog is opened by pressing the [Export](#) button.

Figure 189 Export report dialog



It is possible to export the reports to PDF and Microsoft Excel formats in order to store the report or print it. The format of the report will change to the better when displayed in an external format viewer as for example Adobe Reader for PDF-format. It is recommended to use the external PDF-format before printing the report.

Select Export Format from the list and then press the OK button. The report may then be opened by an installed viewer for the chosen format or stored on disk for later processing. Reports opened by an installed viewer will appear in a separate window dispatched from the PTP 820 NMS client.

The PTP 820 NMS installation does not include any viewer for the external formats.

Exporting the Performance Details report to Excel format

If further manipulation of the data is needed in Microsoft Excel it is recommended to use the Export Performance Details Tool in the toolbar instead of the Export Report window. This tool will generate a report without any formatting.

When the export is completed, an icon appears in the [Progress](#) area in the [Statusbar](#) in the lower right corner.


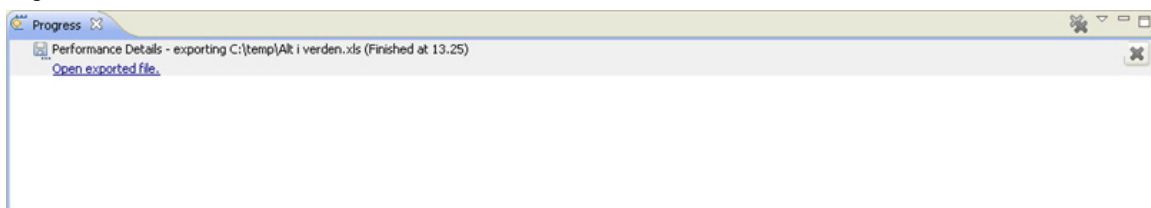
-  Click this icon to open the generated file. The file opens in Microsoft Excel if the xls extension is correctly associated, otherwise Explorer.exe will be opened. Alternatively the exported file can be opened from the [Progress](#) view.

Figure 190 Exporting the performance details report to Excel



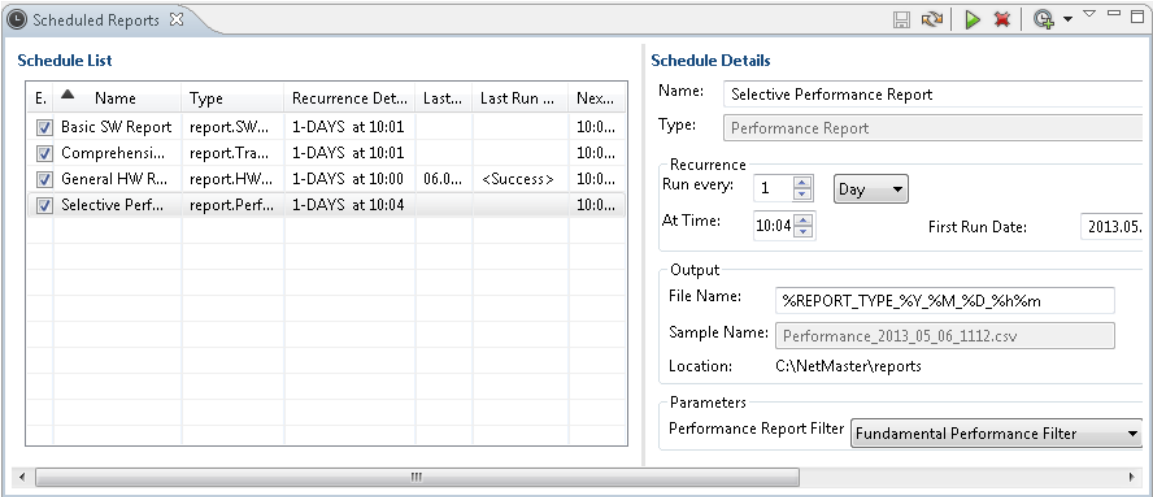
Example of unformatted Excel export is shown below. For more details and examples of how to use the exported data, see the chapter about [how to use Excel to analyze Performance Details Reports](#).

Filter name	Filter A												
Filter description	This filter contains all available elements.												
Time periode	10. august 2008 14:25:41 - 10. september 2008 14:25:41												
Number of measurements	34249												
<i>Granularity</i>	<i>Managed Element</i>	<i>Resource</i>	<i>Time</i>	<i>Type</i>	<i>Status</i>	<i>ES</i>	<i>SES</i>	<i>UAS</i>	<i>BBE</i>				
15min	NMS Lab - InterLink Lower	Radio Port Channel 1	8. september 2008 11 G.826-B2	Data OK		0	0	900	0				
15min	NMS Lab - InterLink Lower	Radio Port Channel 1	8. september 2008 11 G.826-B2	Data OK		0	0	900	0				
15min	NMS Lab - InterLink Lower	Line Port Channel 1	8. september 2008 11 G.826-B2	Data OK		0	0	900	0				
15min	NMS Lab - InterLink Lower	Line Port Channel 1	8. september 2008 11 G.826-B2	Data OK		0	0	900	0				
15min	NMS Lab - InterLink Lower	Line Port Channel 1	8. september 2008 11 G.826-B1	Data OK		0	0	900	0				
15min	NMS Lab - InterLink Lower	Line Port Channel 1	8. september 2008 11 G.826-B1	Data OK		0	0	900	0				
15min	NMS Lab - InterLink Lower	Line Port Channel 1	8. september 2008 11 G.826-B1	Data OK		0	0	900	0				
15min	NMS Lab - InterLink Lower	Line Port Channel 1	8. september 2008 11 G.826-B1	Data OK		0	0	900	0				
15min	NMS Lab - InterLink Lower	Line Port Channel 1	8. september 2008 2 G.826-B1	Data OK		0	0	900	0				
15min	NMS Lab - InterLink Lower	Line Port Channel 1	8. september 2008 2 G.826-B1	Data OK		0	0	900	0				
15min	NMS Lab - InterLink Lower	Line Port Channel 1	8. september 2008 2 G.826-B1	Data OK		0	0	900	0				
15min	NMS Lab - InterLink Lower	Line Port Channel 1	8. september 2008 2 G.826-B1	Data OK		0	0	900	0				
15min	NMS Lab - InterLink Lower	Line Port Channel 1	8. september 2008 2 G.826-B1	Data OK		0	0	900	0				
15min	NMS Lab - InterLink Lower	Line Port Channel 1	8. september 2008 2 G.826-B1	Data OK		0	0	900	0				
15min	NMS Lab - InterLink Lower	Line Port Channel 1	8. september 2008 2 G.826-B1	Data OK		0	0	900	0				
15min	NMS Lab - InterLink Lower	Line Port Channel 1	8. september 2008 2 G.826-B1	Data OK		0	0	900	0				
15min	NMS Lab - InterLink Lower	Line Port Channel 1	8. september 2008 2 G.826-B1	Data OK		0	0	900	0				
15min	NMS Lab - InterLink Lower	Radio Port Channel 1	9. september 2008 1 G.826-B1	Data OK		0	0	900	0				

Scheduled Reports view

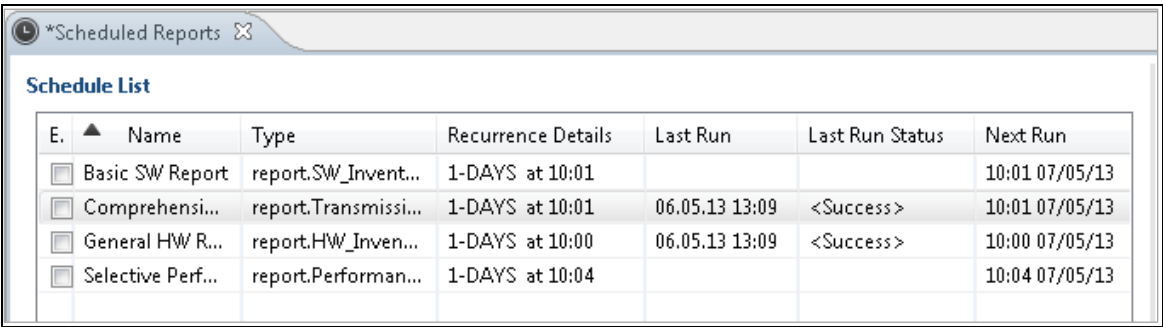
The view is opened by selecting **Views > Reports > Scheduled Reports** from the **main** menu. Scheduled Reports enables you to schedule reports for legacy [software inventory](#), legacy [hardware inventory](#), and legacy transmission inventory views, as well as legacy [performance reports](#), at pre-determined times and recurring intervals. The reports are exported in CSV format and stored at a configurable location.

Figure 191 Schedule reports



Schedule list

The **Schedule List** pane lists the various scheduled reports.



Schedule Details

The **Schedule Details** pane displays the details of the report selected in the Schedule List pane.

Schedule Details

Name:

Type:

Recurrence

Run every:

At Time: First Run Date:

Output

File Name: Report Format:

Sample Name: ☐ Zipped






Location:





Administrative Domains

☒ Geographic

☒ Logic

Available operations

-  Save the modifications you have made in the Scheduled Reports view.
-  Refresh the data in all fields in the Scheduled Reports view.
-  Delete the selected scheduled report.
-  Run immediately the selected scheduled report.
-  Create scheduled report. Pressing the dropdown arrow displays the following options:

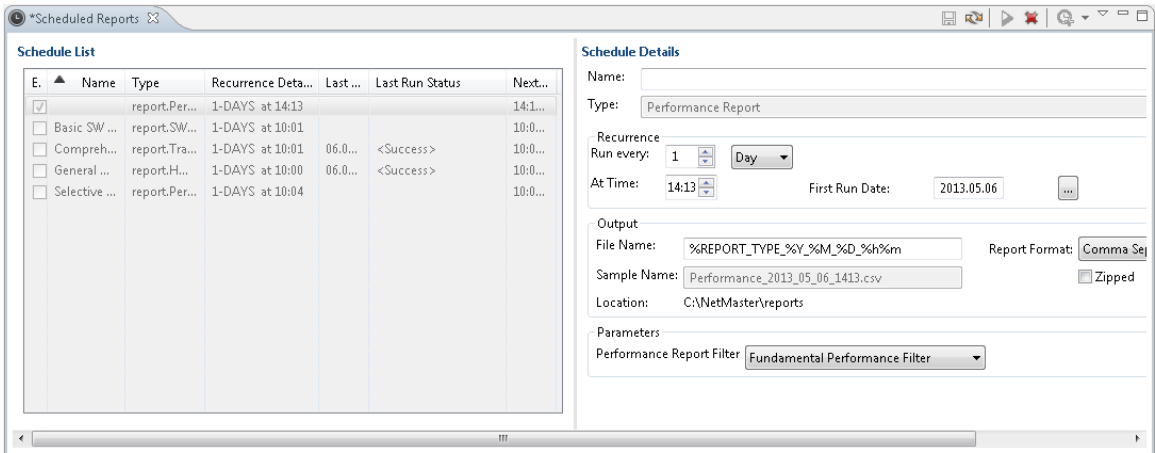
-  Create HW Inventory Report Task
-  Create SW Inventory Report Task
-  Create Transmission Inventory Report Task
-  Create Performance Report Task

Pressing the icon creates a new scheduled report of the type selected the previous time a scheduled report was created.

Creating a new scheduled report

To create a new scheduled report :

1. Select the desired option from the [Create Scheduled Report](#) dropdown button. An unnamed scheduled report appears in the Schedule Lists, with its details available in the Schedule Details pane.



- 2. Type a name for the report in the Name field.
- 3. Configure the recurrence and Output details as necessary.
- 4. Configure the type-specific variables:
 - For Inventory reports, select the domains.
 - For Performance reports, select a Performance Report Filter.



Note At least one Performance Report Filter must exist in order to create a Performance scheduled report. To create a Performance Report Filter, see the [Filter Manager view](#).

- 5. Save the created scheduled report.

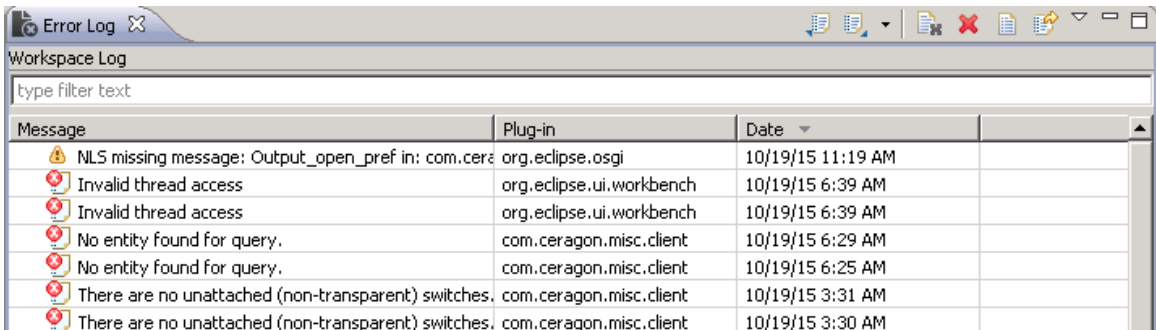
When the report runs, the output will be saved at the specified location in .CSV format.

Other

Error Log view

The view can be opened by selecting **Views > Other > Error Log** from the main menu.

Figure 192 Error log view



The Error Log keeps a log of errors that have been encountered by the software. The **Message** field describes the error that occurred, and the **Plug-in** is the software module in which the error occurred. The date and time of the error is listed in the **Date** field.

Web Browser view

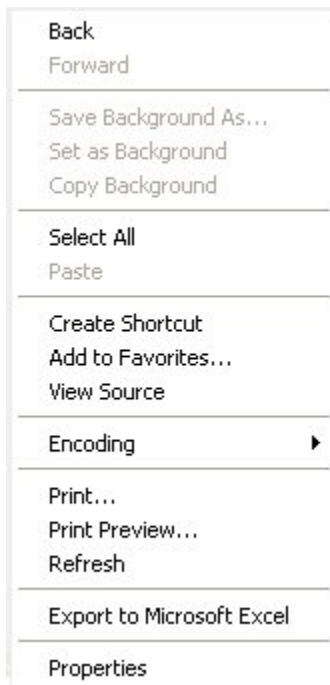
The view can be opened by selecting **Views > Other > Web Browser** from the main menu.

The purpose of this view is to enable an embedded web browser within the PTP 820 NMS client. This view can typically be used for a simple integration to other systems having a web interface. The default URL used by the browser is defined in the main menu **Window >Preferences > Web Browser**.

Available operations

- Refresh View Refresh the contents of the view.
- Preferences Opens the Preferences Web Browser dialog where you can set the URL to be used by the Web Viewer.

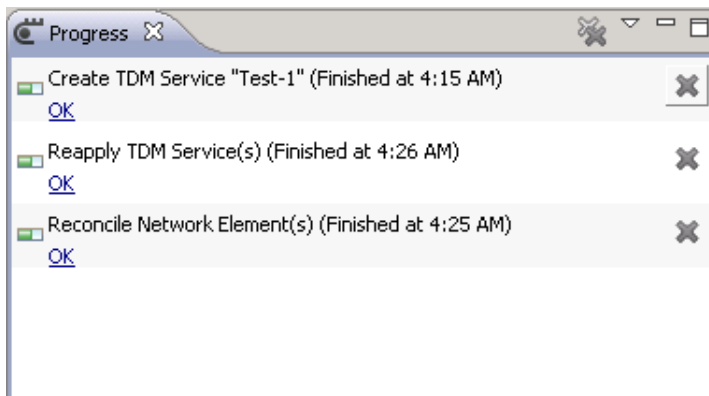
By right-clicking inside the view browser, specific commands are displayed. The commands available are dependent on the browser available, below is an example of [context menu](#) operations available in Microsoft Internet Explorer.



Progress view

The view can be opened by double-clicking the [Progress statusbar](#) or by selecting **Views > Other > Progress** from the main menu

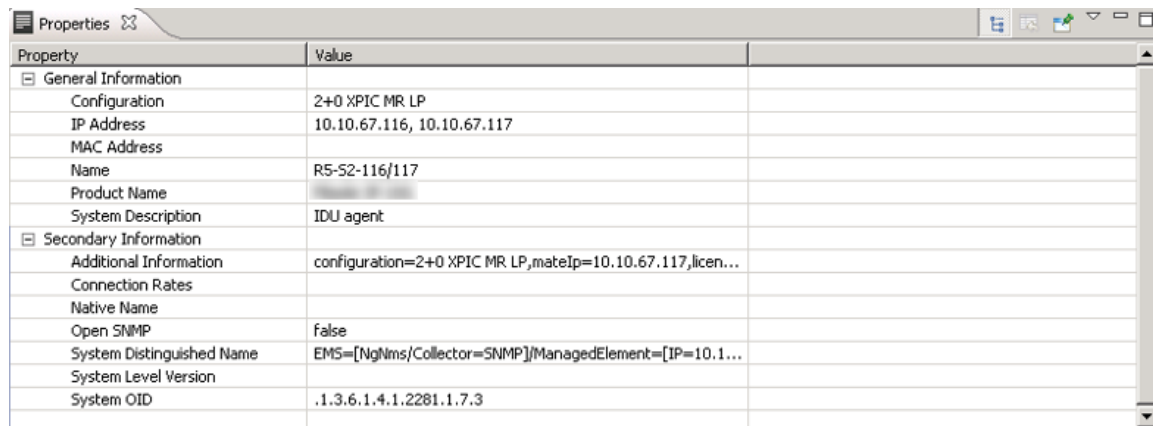
Figure 193 Progress view



This view displays any process that causes the client to wait for the server to read or write data in the database. Whenever process like this is active, it is presented in the Progress view with a progress-bar. When the process is finished, it will disappear from the view.

Properties view

The view can be opened by selecting **Views > Other > Properties** from the main menu, or on the context menu of any of the topological views (**Geographical** or **Logical Map** or **Tree**).

Figure 194 Properties view


Property	Value
General Information	
Configuration	2+0 XPIC MR LP
IP Address	10.10.67.116, 10.10.67.117
MAC Address	
Name	RS-S2-116/117
Product Name	
System Description	IDU agent
Secondary Information	
Additional Information	configuration=2+0 XPIC MR LP, mateIp=10.10.67.117, licen...
Connection Rates	
Native Name	
Open SNMP	false
System Distinguished Name	EMS=[NgNms/Collector=SNMP]/ManagedElement=[IP=10.1...
System Level Version	
System OID	.1.3.6.1.4.1.2281.1.7.3





This view is used together with any view containing NE (only managed NE) or domains.


Property table

This table contains values for the last selected object in the perspective. When selecting a new object in any view, the Properties table will be updated and then present values for this object.

Each line in the table contains a property and a current value for the currently selected object. Some of the values in the Value column is editable, indicated by the cursor when the field is clicked. A new value can be typed directly in the table and then saved to PTP 820 NMS. No values in the Property column can be edited, but all pairs of properties/values can be copied to clipboard.

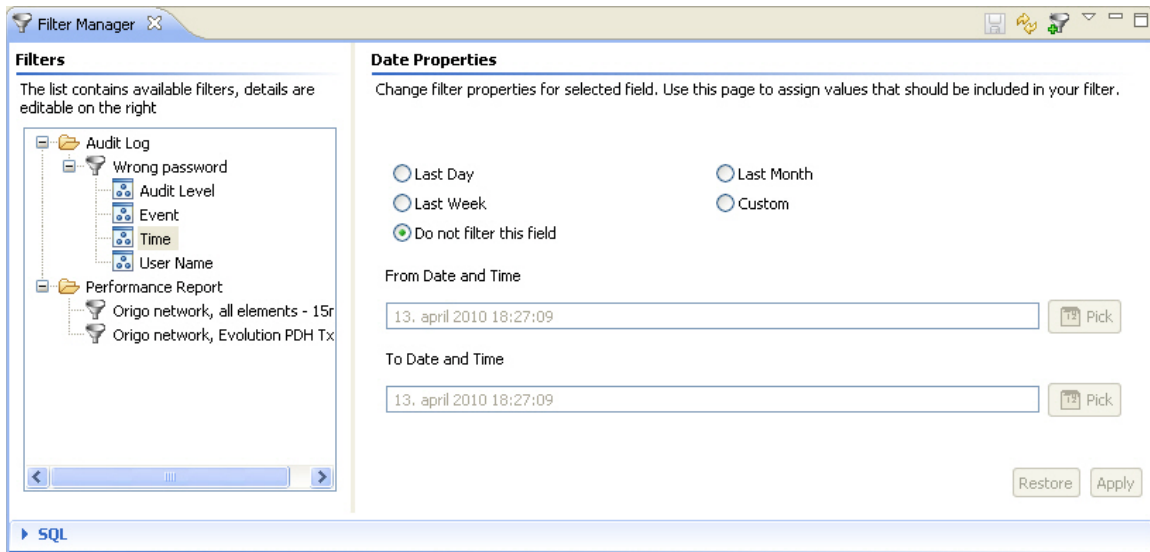
Available operations

-  **Copy** Copy the Property and Value of the currently selected line in the table to clipboard. The content is copied as plain text, separated by a TAB-character (tabulator). Only one pair of Property/Value can be copied this way.
-  Type a new value into a field in the Value column. The values that is editable this way is indicated by a cursor-change when the field is clicked.
-  **Restore Default Value** Undo a recent change in a field the Value column.
-  **Show Categories** Displays the properties by categories.

 **Pin to Selection** If this option is selected, the Properties view will continue to display the properties of the currently selected NE, even if you select another component in the Geographical or Logical map or tree.

Filter Manager view

This view can be opened by selecting **Filter Manager** on the [view dropdown](#) in the [Audit Log](#), [Performance Overview Report](#) or the [Performance Details Report](#) view. Alternatively the view can be opened by selecting **Views > Other > Filter Manager** from the **main** menu.



The purpose of this view is to create and maintain filters for the **Audit Log** view, the **Performance Overview Report** view and the **Performance Details Report** view. The filters define what is to be included, and the number of lines to be displayed in the tables and reports. The view contains a **Filters** area to the left, and a **Filter Properties** area to the right.

Filters area

This area contains the **Filters tree** which consists of the following objects:

- **User Audit** The **Filter Category node** corresponds to the views you want to filter. Expand a category to see all filters which are available to this view.
- **root events** The **Filter node** corresponds to a definition of filter and paging. Select a filter to update filter name, paging, page size or description of the filter. Only filters which are "included in favorites" are available in the favorites list in the corresponding view. A dimmed node icon indicates that this filter is not included in favorites.
- **Audit Time** The **Parameters node** corresponds to each of the fields in the corresponding table that can be used for filtering. Select a filter to update this filter parameter: enable/disable filtering of the field and add boundaries for filtering. A tiny green arrow on the node-icon indicates that filtering is enabled on this parameter node.

Filter Properties area

The content of this area depends on what node is selected in the **Filters tree** in the **Filters area**. When a property is updated, the changes in the area can be discarded by pressing the **Restore** button. Pressing the **Apply** button will save the changes made to this property. If you have changed values and leave a **Filter Properties** area without pressing **Restore** or **Apply**, the [Continue? dialog](#) appears, where you can discard or save the changes.

Filter Properties area - Filter Properties

This **Filter Properties** area is displayed when selecting a **Filter node** in the **Filters tree**

Filter Properties

Change filter name, paging properties and description.

Filter name:

☒ Use result paging

Page size:

Description:

Update the name and description for a filter. You can also disable/enable paging and change the page size used for filtering. If paging is disabled, all data is searched for each query. The page size defines the maximum number of items matching these filter criteria to search for in each query.

Please note that running a filter without paging can result in poor performance on the server as this can result in a large amount of data.

Filter Properties area - Text Properties

This **Filter Properties** area is displayed when selecting a **Parameter node** containing text values in the **Filters tree**

Text properties

On this page you can make string-searches a part of your custom filter. You can search for the existence of a substring by using the wildchar '%' in front or behind the searchstring.

%Test Will give you all matches ending with 'Test'
Test% Will give you all matches starting with 'Test'

☐ Include pattern

☒ Do not filter this field

Search value:

Define a filter using a string (or sub-string) that should be matched.

Filter Properties area - Date Properties

This **Filter Properties** area is displayed when selecting a **Parameter node** containing date values in the **Filters tree**

Date properties

Change filter properties for selected field. Use this page to assign values that should be included in your filter

☐ Last Day ☐ Last Month
☐ Last Week ☒ Custom
☐ Do not filter this field

From Date and Time

June 26, 2005 12:00 AM

To Date and Time

September 17, 2005 12:00 AM

Define a filter based on a period (time-interval) that should be matched. The boundaries for the period are defined in the **Date and Time** dialog.

Filter Properties area - Performance Filter

This Filter Properties area is displayed when selecting a **Performance Filter** node in the **Filters** tree.

Performance Report Filter Properties

Change filter name, description and properties.

Filter name and description

Filter name:

Description:

Scope

Available

- ☒ Geographic
- ☒ Logic

Selected (16)

- ☒ ...
- ☒ ...
- ☒ ...
- ☒ ...
- ☒ ...
- ☒ ...
- ☒ ...
- ☒ ...
- ☒ ...
- ☒ ...
- ☒ ...
- ☒ ...
- ☒ ...
- ☒ ...
- ☒ ...

> >> < <<

Up Down To top To bottom

Duration

☐ Last Day
 ☒ Last Month
 ☐ Last Week
 ☐ Custom

From Date and Time

November 22, 2015 10:10:10 AM

To Date and Time

November 22, 2015 10:10:10 AM

Measurement Type/Parameter

- ☒ ACM
- ☒ Ethernet
- ☒ G.826
- ☒ Power Levels
- ☒ Power Supply
- ☒ MSE

Other options

☒ Show performance loss only
 ☒ Show valid data only

Filter Properties area - Performance Filter - Filter name and description section

Filter name and description

Filter name:

Description:

Update the name and description for a filter.

Filter Properties area - Performance Filter - Scope section

Scope

Available

- Geographic
 - Domain-1
 - 141 -
 - 142 -
 - 150 -
 - Domain-2
 - 104 -
 - 105 -
 - 125 -
 - 131 -
 - 133 -
 - Domain-3
 - R5-S2-100/102
 - R5-S2-116/117

Selected (3)

- 141 -
- 104 -
- 105 -


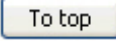
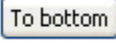
Buttons: Up, Down, To top, To bottom, >, >>, <, <<

Select the managed elements to be included in the report. When an element is moved to the selected list it is marked in the **Available** list with this dotted icon:

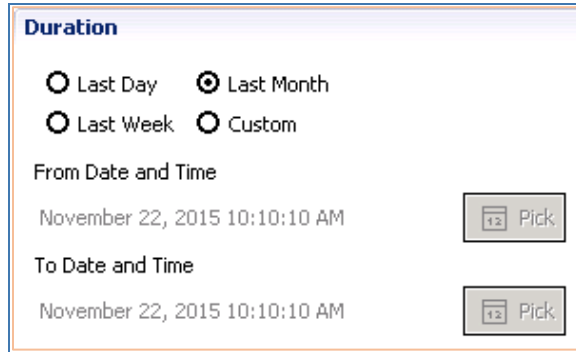
The order of managed elements in the **Selected** list will be used when report is generated. To change order use the **Up**, **Down**, **To top** or **To bottom** buttons.

Available operations in the Scope area:

- Selected resource(s) in the **Available** list is added to the **Selected** list. If selected resource is a domain all elements below are added.
- Add all available resources to the **Selected** list.
- Remove selected resource(s) from **Selected** list.
- Remove all managed elements from the **Selected** list.
- Move selected resource(s) up in the **Selected** list.

-  Move selected resource(s) down in the **Selected** list.
-  Move selected resource(s) to the top of the **Selected** list.
-  Move selected resource(s) to the end of the **Selected** list.


Filter Properties area - Performance Filter - Duration section




Duration

☐ Last Day ☒ Last Month
☐ Last Week ☐ Custom

From Date and Time

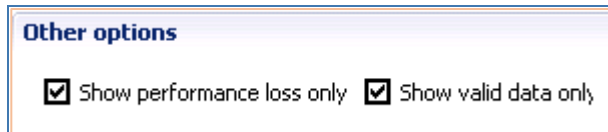
November 22, 2015 10:10:10 AM 

To Date and Time

November 22, 2015 10:10:10 AM 

Select the period (time-interval) that should be matched.

Filter Properties area - Performance Filter - Show performance loss only

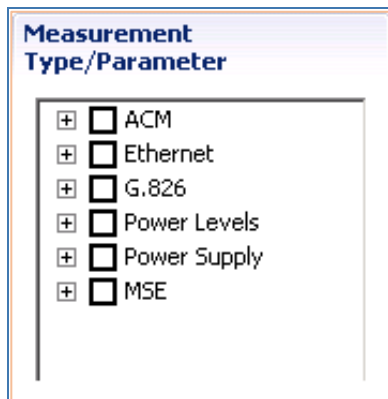


Other options

☒ Show performance loss only ☒ Show valid data only

- Check **Show performance loss only** to only show performance measurements with performance loss. This setting is only valid for G.826 measurement types.
- Check **Show valid data only** to hide all invalid data.

Filter Properties area - Performance Filter - Measurement Type/Parameter section



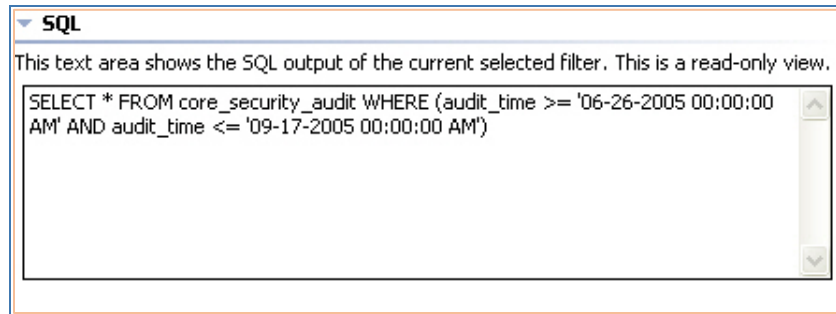
Measurement Type/Parameter

- ☐ ACM
- ☐ Ethernet
- ☐ G.826
- ☐ Power Levels
- ☐ Power Supply
- ☐ MSE

Select the measurements to be matched.

SQL area

This area can be displayed by pressing the **SQL header** in the bottom left corner of the **Filter Manager** view whenever an **Audit Log** filter is selected in the [Filters](#) list.



This area displays the SQL code of the currently selected filter in the **Filters tree**. The **SQL field** is read-only, and is merely a help for users who are familiar with reading SQL code to verify that the filter definitions are correct.

Available operations

- **Create new filter** Open the **Create New Filter** dialog, where you can create Audit and Performance Report filters.
- **Rename filter** Change the name of the currently selected filter by opening the **Rename Filter** dialog.
- **Remove filter** Remove the currently selected filter
- **Include in favorites** Add/remove the currently selected filter (or filter category) to the list of favorite filters in its corresponding view. Only filters that are "included in favorites" are available in the favorites list in the corresponding view
- **SQL** Click to show/hide the **SQL** area
- **Expand the selected node** in the tree by clicking the plus-sign. You can also expand a node by **double-clicking** an unexpanded node in the tree.

How to create a Performance Report filter

Performance Report filters are used for selecting performance data to be presented in the [Performance Overview Report](#) and [Performance Details Report](#).

To create a Performance Report filter:

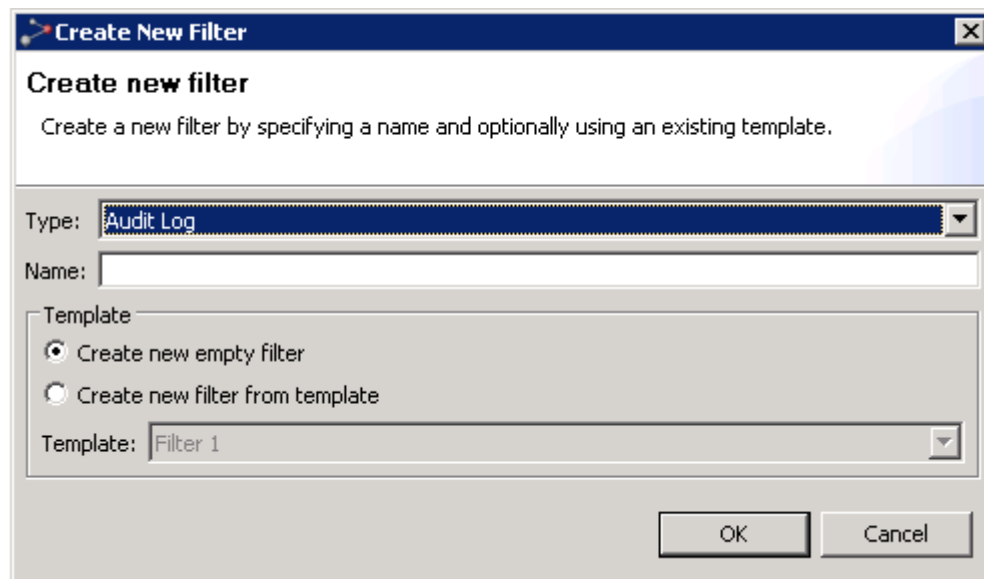
- 1 Open the [Filter Manager](#) view from the [main](#) menu, by selecting **Views > Other > Filter Manager**.
- 2 In the [Filters area](#); select **Performance Report**, and use the operation [Create New Filter](#).
- 3 In the [Create New Filter dialog](#); enter a **Filter Name**. If you already have a performance filter you want to use as a template, select **Create new filter from template**, and pick a template from the **Template** list. Then close the dialog by pressing **OK**.
- 4 The new performance report filter can now be found in the **Filters area Filter Manager** view. You might need to [expand](#) the **Performance Report Filters** in the table to see the new template.
- 5 Select the new filter in the **Filters** area. Details about the template can now be seen in the [Performance Report Filter Properties](#) area, which initially is empty.

- 6 In the [Scope](#) section, select the NE to be included in the report by moving them from the **Available** to the **Selected** list.
- 7 Use the **Up**, **Down**, **To top** and **To bottom** buttons to define order of the NE in the report.
- 8 In the **Duration** area, select the period you want to include in the report. Use **Custom** to select an interval which includes future measurements.
- 9 Use the **Show performance loss only** checkbox to hide data without performance loss.
- 10 Select parameters of the measurement type you want in the **Measurement Type/Parameter** section.
- 11 When you have finished updating the filter, store the changes by pressing **Apply** button on the bottom of the **Performance Report Filter Properties** area, and then pressing **Save** on the [view toolbar](#).

The new filter is now available in the **Filters** dropdown menu in the [Performance Overview Report](#) and [Performance Details Report](#).

Create New Filter dialog

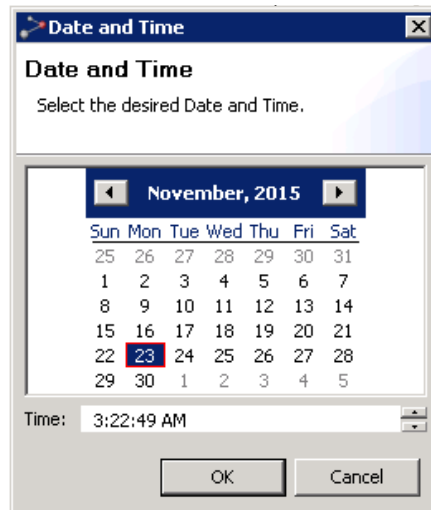
This dialog can be opened by selecting **Create New Filter** in the context menu, view dropdown or on the view toolbar.



Select filter type (Audit Log or Performance Report) from the dropdown and enter a name. Create a blank filter, or pick one of your existing filters as a template. The filter will be created when you press **OK**.

Date and Time dialog

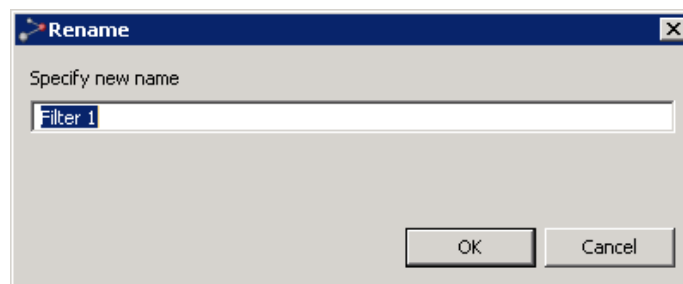
This dialog can be opened by pressing the **Pick** button in a **Date Properties** area in the **Filter Manager** view. The **Date Properties** area is available when selecting a **Parameter node** contains a date in the **Filters tree**.



Select a date and press **OK** to apply

Rename Filter dialog

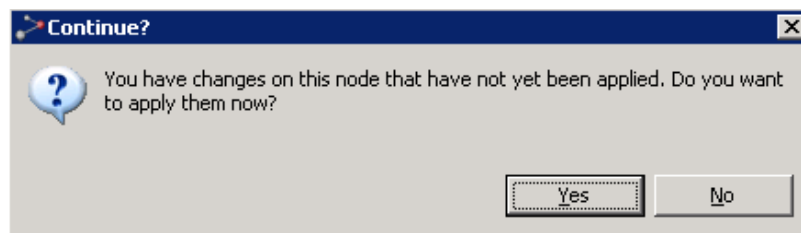
This dialog can be opened by selecting **Rename Filter** in the context menu in the **Filters tree** with a filter node selected.



Enter the new name and press **OK**, or press **Cancel** to discard changes.

Continue? dialog

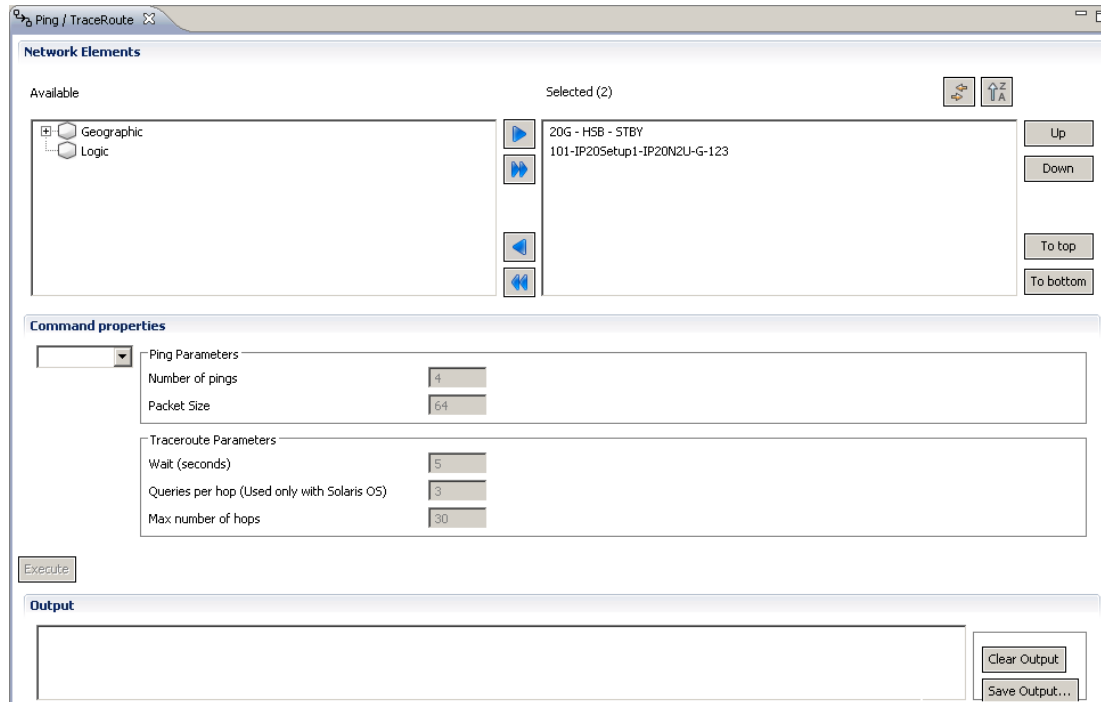
This dialog appears whenever you leave a node in the **Filters tree** without saving changed values in the **Filter Properties** area.



Press **Yes** to save changes or press **No** to discard.

Ping/TraceRoute view

The view can be opened by selecting **Views > Other > Ping/TraceRoute** from the main menu. It can also be opened scoped from the context menu of up to 30 devices selected in the Geographical/Logical/Ethernet/TDM/Network Explorer Tree or in the Geographical/Logical/Ethernet/TDM/network Explorer Map.



In this view you can run a ping or Traceroute command on the selected network elements. The ping or Traceroute command you specify will run on the group of devices you specify, in the order you specify, and the output will appear on screen. You can save this output to a file.

To run ping or Traceroute on a batch of network elements:

- 1 Specify the network elements on which to execute ping or Traceroute, as follows: Select desired network elements in the **Available** window of the **Network Elements** area, and click the right arrow to display them in the **Selected** window. If the view is opened scoped, the selected devices appear in the **Selected** pane. You can select elements from the geographical and/or logical tree. If you select an entire domain, the ping or Traceroute command will be executed on each of the devices in the domain.
- 2 Optionally use the **Up**, **Down**, **To top** and **To bottom** buttons to re-order the list of elements. Note that ping or Traceroute will first run on the first device in the list, then on the second device, etc.
- 3 In Command Properties, select from the dropdown list either **Ping** or **TraceRoute**.
- 4 If you selected **Ping**, specify the ping parameters:
 - Number of Pings. The range is 1 – 100, default is 4.
 - Packet Size. The range is 64 – 1472, default is 64.
- 5 If you selected **TraceRoute**, specify the Traceroute parameters:
 - Wait (seconds). The range is 1 – 10, default is 5.
 - Queries per hop (used only with Solaris OS). The range is 1 – 10, default is 3.



- Max number of hops. The range is 1 – 30, default is 30.
- 6 Click **Execute**.
PTP 820 NMS executes ping or Traceroute on the devices, one device at a time, in the order in which they appear in the window.
 - 7 View the output in the **Output** area.
 - 8 Optionally click **Save Output** to save the output to a text file.
 - 9 Optionally click **Execute** to run ping or Traceroute again. The results of the current execution are appended to the results of the previous execution. You might therefore first click **Clear Output** to delete the display in the **Output** window, before clicking **Execute** again.

Note: If the Server restarts while a Ping or Traceroute session is in progress, then following Server Restart the view will need to be re-opened and the Ping or Traceroute command will need to be given again.

Note: For devices with multiple IPs, ping or Traceroute will be executed on the first IP address listed in the device's [Error! Reference source not found.](#) (accessible from **Views > Other > Properties**).

Available operations

The following operations are available in the view:

-  Link View – When activated, selecting a device in the **Selected** pane, selects the device in the tree appearing in the **Available** pane, and vice versa.
-  Order ascending/descending – orders the devices appearing in the **Selected** pane in ascending/descending order. This determines the order in which the NEs are listed in the **Selected** pane.

Open SNMP Interface

Open SNMP Interface

The purpose of the Open SNMP functionality is to be able to discover and manage SNMP elements that are not fully integrated in PTP 820 NMS. These types of elements will be called open SNMP network elements (open SNMP NEs).

The following main points covered in the first release of open SNMP are:

1. Discover any MIB2 compliant SNMP equipment (SNMP version v1 and v2c)
2. Set any discovered SNMP equipment to managed state
3. Only ME node is shown in tree views
4. Connection polling
5. Allow configuration of launching of external tools
6. Allow configuration of alarm handling through Open SNMP Interface view:
 - o Reconcile current alarm table
 - o Reconcile current alarms given as single OIDs
 - o Reconcile current alarms given as single OIDs using a mask
7. Configuration import/export

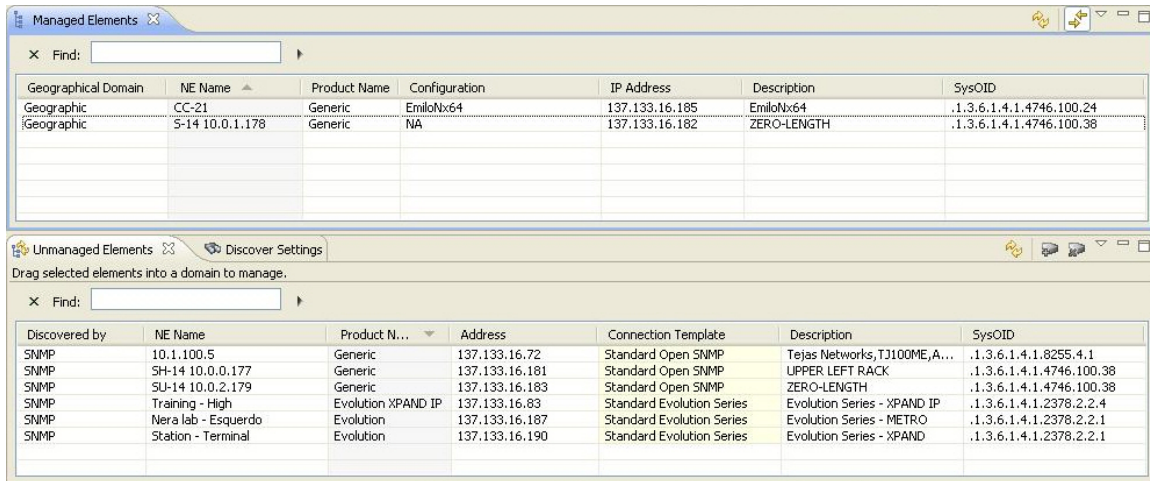
License and permissions

The functionality is a licensed PTP 820 NMS feature with license counting (as for full integrated elements) for open SNMP elements. If the No. of Open SNMP Elements license is disabled, it is still possible to discover open SNMP elements, but it will not be possible to put them in managed state.

The Open SNMP configuration functionality is available if the logged in user has the following action permissions to access it: Configuration -> Open SNMP Interface. Without this permission a user can still discover and manage Open SNMP elements, but not create or change Open SNMP configuration in the Open SNMP Interface view.

Discover and manage

Discovering and managing open SNMP elements is done the same way as for full integrated elements. One has to make sure that the OpenSNMP template is selected in Discover Settings dialog and the correct Open SNMP template is defined. If an unknown discovered Open SNMP element type is discovered, the product name is set to Generic:

Figure 195 Discover and manage


The screenshot shows the 'Managed Elements' window with a search bar and a table of discovered elements. The table has columns: Geographical Domain, NE Name, Product Name, Configuration, IP Address, Description, and SysOID.

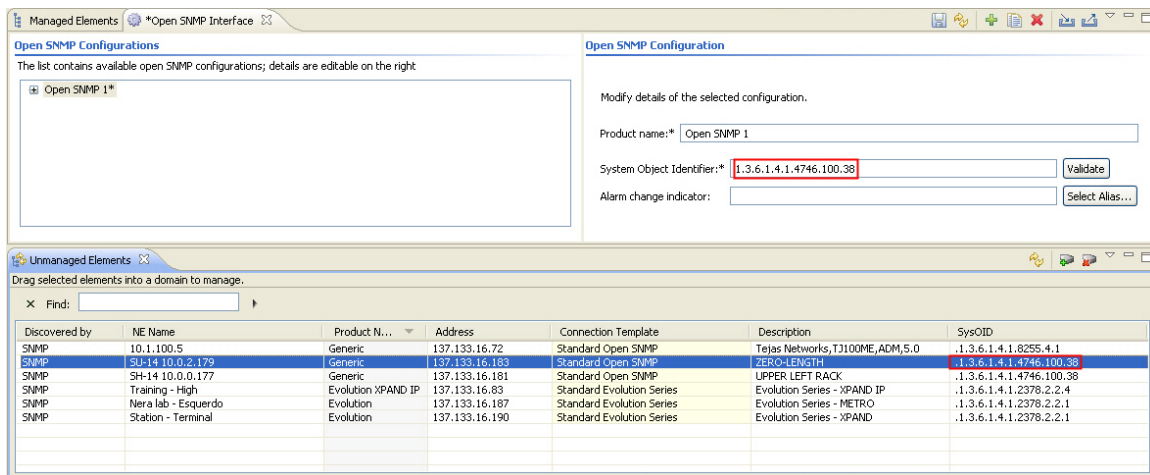
Geographical Domain	NE Name	Product Name	Configuration	IP Address	Description	SysOID
Geographic	CC-21	Generic	EmiloNx64	137.133.16.185	EmiloNx64	.1.3.6.1.4.1.4746.100.24
Geographic	5-14 10.0.1.178	Generic	NA	137.133.16.182	ZERO-LENGTH	.1.3.6.1.4.1.4746.100.38

Below the table is a section for 'Unmanaged Elements' with a search bar and a table of discovered elements. The table has columns: Discovered by, NE Name, Product N..., Address, Connection Template, Description, and SysOID.

Discovered by	NE Name	Product N...	Address	Connection Template	Description	SysOID
SNMP	10.1.100.5	Generic	137.133.16.72	Standard Open SNMP	Tejas Networks,TJ100ME,A...	.1.3.6.1.4.1.8255.4.1
SNMP	SH-14 10.0.0.177	Generic	137.133.16.181	Standard Open SNMP	UPPER LEFT RACK	.1.3.6.1.4.1.4746.100.38
SNMP	SU-14 10.0.2.179	Generic	137.133.16.183	Standard Open SNMP	ZERO-LENGTH	.1.3.6.1.4.1.4746.100.38
SNMP	Training - High	Evolution XPAND IP	137.133.16.83	Standard Evolution Series	Evolution Series - XPAND IP	.1.3.6.1.4.1.2378.2.2.4
SNMP	Nera lab - Esquerdo	Evolution	137.133.16.187	Standard Evolution Series	Evolution Series - METRO	.1.3.6.1.4.1.2378.2.2.1
SNMP	Station - Terminal	Evolution	137.133.16.190	Standard Evolution Series	Evolution Series - XPAND	.1.3.6.1.4.1.2378.2.2.1

It is possible to manage unknown Open SNMP element types, but no alarms are presented (except the LOST CONTACT alarm if PTP 820 NMS detects lack of connectivity with the element). For alarm handling, configuration needs to be created in the Open SNMP Interface view. The element's sysOID is used to identify the Open SNMP element type.

Opening configuration view by selecting an open SNMP NE with no configuration assigned:

Figure 196 Configuration view


The screenshot shows the 'Open SNMP Interface' window. On the left, there is a list of 'Open SNMP 1*' configurations. On the right, the configuration details are shown, including fields for Product name, System Object Identifier, and Alarm change indicator.

Open SNMP Configurations

The list contains available open SNMP configurations; details are editable on the right

- Open SNMP 1*

Open SNMP Configuration

Modify details of the selected configuration.

Product name:* Open SNMP 1

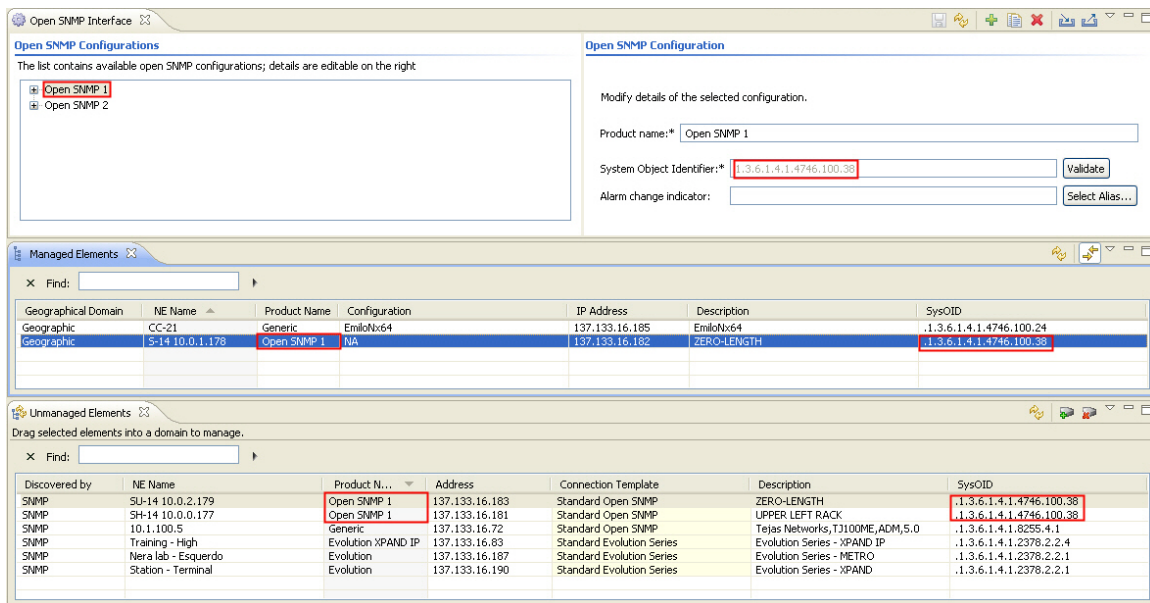
System Object Identifier:* 1.3.6.1.4.1.4746.100.38

Alarm change indicator:

Below the configuration view is a section for 'Unmanaged Elements' with a search bar and a table of discovered elements. The table has columns: Discovered by, NE Name, Product N..., Address, Connection Template, Description, and SysOID.

Discovered by	NE Name	Product N...	Address	Connection Template	Description	SysOID
SNMP	10.1.100.5	Generic	137.133.16.72	Standard Open SNMP	Tejas Networks,TJ100ME,ADM,5.0	.1.3.6.1.4.1.8255.4.1
SNMP	SU-14 10.0.2.179	Generic	137.133.16.183	Standard Open SNMP	ZERO-LENGTH	.1.3.6.1.4.1.4746.100.38
SNMP	SH-14 10.0.0.177	Generic	137.133.16.181	Standard Open SNMP	UPPER LEFT RACK	.1.3.6.1.4.1.4746.100.38
SNMP	Training - High	Evolution XPAND IP	137.133.16.83	Standard Evolution Series	Evolution Series - XPAND IP	.1.3.6.1.4.1.2378.2.2.4
SNMP	Nera lab - Esquerdo	Evolution	137.133.16.187	Standard Evolution Series	Evolution Series - METRO	.1.3.6.1.4.1.2378.2.2.1
SNMP	Station - Terminal	Evolution	137.133.16.190	Standard Evolution Series	Evolution Series - XPAND	.1.3.6.1.4.1.2378.2.2.1

If the selected open SNMP NE already has a configuration assigned, the view will be opened with the assigned configuration selected:

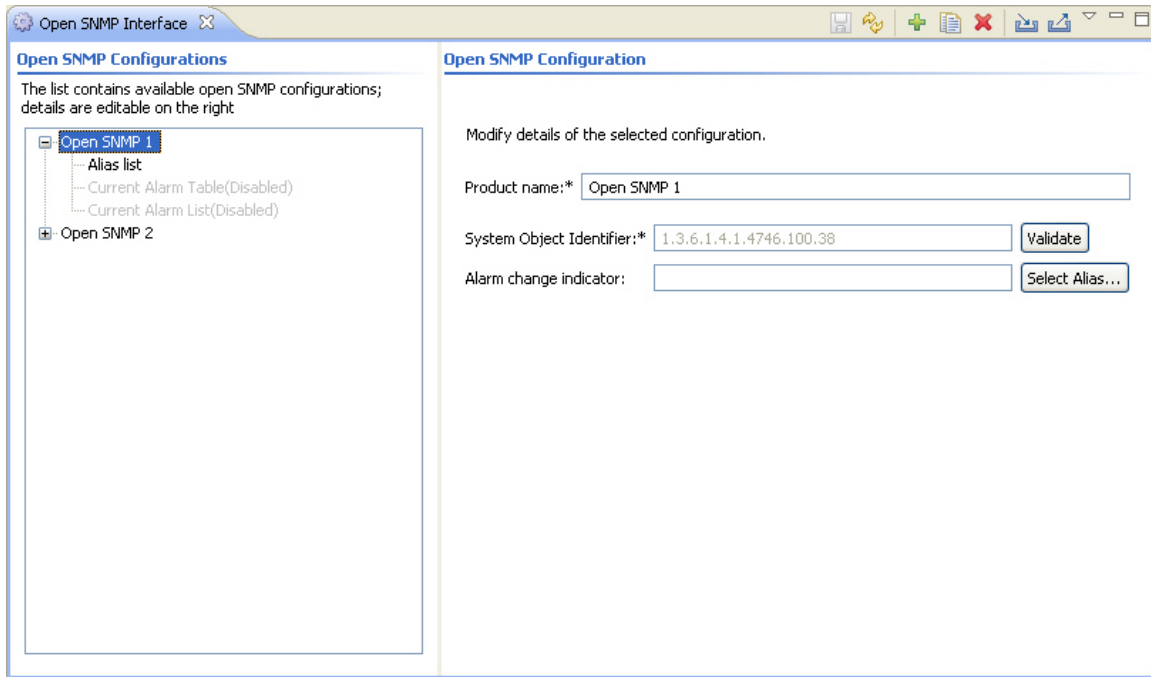
Figure 197 SNMP NE configuration assign

Open SNMP Interface view

This view contains configuration functionality for the Open SNMP type elements and can be opened from the following locations:

- **Views > Configuration > Open SNMP** Interface from the main menu.
- By selecting an open SNMP NE in Unmanaged Elements view and then selecting Open SNMP Interface action from the Context or View dropdown menu.
- By selecting a node representing an open SNMP NE in one of the topology views and then selecting **Configuration > Open SNMP Interface** from the Context or View dropdown menu.

In the last two cases, if the selected open SNMP NE has no configuration assigned, a new configuration will be created and the element's sysOID will be filled in. All other attributes will be empty.

Figure 198 SNMP interface view

The purpose of Open SNMP functionality is to be able to discover and manage SNMP elements that are not fully integrated in PTP 820 NMS.

More information is found here:

- [Open SNMP Interface](#)
- [Alias list configuration](#)
- [Current alarm table configuration](#)
- [Open SNMP Current alarm list](#)

The Open SNMP Interface view consists of an SNMP tree area containing existing configurations, and an area containing details about the currently selected configuration.

Open SNMP tree area

This tree area holds the different Open SNMP configurations:

Table 49 Open SNMP tree area attributes

Name	Explanation
<Product name>	Product name as configured in the individual configurations
Alias list	Aliases are user defined labels mapped to the object identifiers (OIDs) defined in the NE's MIB file. They will be used when the user needs to specify an OID in the open SNMP configuration. See Open SNMP Alias List for more information.
Current Alarm Table	Alarm configuration for elements supporting an SNMP based current alarms table. See Open SNMP Current alarm table for more information.
Current Alarm List	Alarm configuration for elements that give current alarms as dedicated SNMP OIDs, optionally available for multiple alarms for a single OID based on the bit position of the OID value. See Open SNMP Current alarm list for more information.

Open SNMP configuration area

This is where general Open SNMP settings can be edited:








Table 50 Open SNMP configuration area attributes

Name	Explanation
Product name	The type of NE that will be shown in Unmanaged Elements view, Managed Elements view, External Tools Assignments preference page, Properties view scoped to an element, and various reports. This is also the name of the open SNMP configuration and has to be unique within the configuration set defined in the Open SNMP Interface view. By default, this name is automatically generated and set to Open SNMP x, where x=1,2,... . It is not allowed to use Generic (ignoring case considerations) as product name because this is reserved for unknown Open SNMP elements. The asterisk (*) indicates that this value is mandatory.

Name	Explanation
System Object Identifier	<p>Defined in MIB2, this is a unique object identifier assigned by the manufacturers to their SNMP elements. Once an Open SNMP configuration is saved, the sysOID cannot be modified. The configuration will be assigned automatically to all the discovered and managed elements that match this sysOID.</p> <p>SysOIDs for existing fully integrated elements are not allowed to be used.</p> <p>The asterisk (*) indicates that this value is mandatory.</p>
Alarm change indicator	<p>Some MIBs define a sequence number or time stamp for the latest entry in the event log. By polling this number, PTP 820 NMS can detect that new entries or rows are available in the current alarm table.</p> <p>If the element's MIB file defines an alarm change indicator, this field can be configured by creating an alias in the Alias List that maps to the alarm change indicator OID.</p> <p>If not configured, alarm reconcile will be run every alarm polling interval.</p>

Available operations

The following operations are available in the view:

-  Save modifications that you have made in the Open SNMP Configuration view. If you try to close the view without saving the data, the Save Changes dialog will appear.
-  Refresh the view with the latest configuration from the server. Any modifications that you have made will be lost.
-  Create a configuration by opening Create open SNMP configuration dialog. In the dialog the user must specify the product name and the sysOID.
-  Clone the selected configuration by opening Clone open SNMP configuration dialog where the user is asked to modify the product name and the sysOID.
-  Delete the selected open SNMP configuration(s). It will not be possible to delete the configurations that are in use by discovered or managed elements.
-  Import an open SNMP configuration from a file. The file must correspond to the format required by PTP 820 NMS. If a configuration with same sysOID exists, a dialog will ask you to overwrite the existing configuration, or to create a new one.
-  Export the selected configuration(s) to file(s) named <Product name>-Configuration-<current system date>.xml.

Open SNMP Alias List

Aliases are user defined labels mapped to the SNMP object identifiers (OIDs). They will be used when the user needs to specify OIDs in the open SNMP configuration fields. When an alias is used, it will be inserted like this: <Alias name>.

Figure 199 Open SNMP alias list

Alias List

Create unique aliases to be used for this Open SNMP configuration. An alias is a descriptive name that maps to an OID.

[illegible]

More information about the Alias List table:

Table 51 Alias list table

Name	Explanation
Alias name	A descriptive name mapped to an OID to be used in an Open SNMP configuration when defining various fields like Alarm Text, Alarm Severity etc.
OID	An object identifier as defined in the NE's MIB file used to read useful information from the element. An OID may be mapped to more than one alias.

Name	Explanation
Translation	<p>The translation is intended for elements that use an alarm identifier instead of the actual alarm text,. Then it is possible to define a mapping (translation) between the read OID value and the text to be displayed in the Alarm Text column in the Active Alarms and Historical Alarms view.</p> <p>It is also possible to use translations to provide more readable values for fields like Severity or Alarm Type,</p> <p>When a translation is defined it will be shown like this in the Translation column: {oid_value1=mapped_value1, oid_value2=mapped_value2...}, where oid_value is the value read from an OID, and mapped_value is a user defined value.</p>
Validation	<p>The OIDs in the Alias List can be validated against a real element. Make sure to supply correct IP address, SNMP version and read community when validating OIDs.</p>

Alias List validation

The Alias List should be verified against a real element of target type. Add the IP address of the element, the SNMP version and the read community, and press the Validate All button.

If the OID can be verified, the value read from the OID will be displayed in the Validation column. If during the validation, it was detected that the OID represents a scalar object, the suffix '.0' will be added to the OID. If the OID represents a table, the value displayed in the Validation column will be the < OID of the first accessible column for the first instance in the table>=<the value read for this instance>. If the OID represents a column in the table the value displayed in the Validation column will be the < OID of this column for the first instance in the table>=<the value read for this instance>.

If the OID cannot be verified, the OID will be colored in red and nothing will be shown in the Validation column.

Validation of OIDs representing tables with more than one index is not supported. These OIDs will be marked as invalid.

The figure below shows an example list of aliases with validations against an element with IP address 10.8.1.15. First eight aliases maps to OIDs defined in standards MIBs like SNMPv2-MIB and RFC1213-MIB.

Figure 200 Alias list validation

Alias name	OID	Translation	Validation
alias1_system	1.3.6.1.2.1.1		
alias2_sysDescr	1.3.6.1.2.1.1.1.0		Evolution Series - METRO
alias3_interfaces	1.3.6.1.2.1.2		
alias4_ifTable	1.3.6.1.2.1.2.2		.1.3.6.1.2.1.2.2.1.1==1
alias5_ifEntry	1.3.6.1.2.1.2.2.1		.1.3.6.1.2.1.2.2.1.1==1
alias6_ifDescr	1.3.6.1.2.1.2.2.1.2		.1.3.6.1.2.1.2.2.1.2.1==p0
alias7_ifDescrInstance1	1.3.6.1.2.1.2.2.1.2.1		.1.3.6.1.2.1.2.2.1.2.1==p0
alias8_ifDescrInstance110	1.3.6.1.2.1.2.2.1.2.110		.1.3.6.1.2.1.2.2.1.2.110==su11-eth1
dummyalias1	1.2.3.4.5		
dummyalias2	1.3		
faultCurrentAlarmEntryEventType	1.3.6.1.4.1.2378.1.1.2.2.1.3.1.1.8		.1.3.6.1.4.1.2378.1.1.2.2.1.3.1.1.8.11==3
faultCurrentAlarmEntryName	1.3.6.1.4.1.2378.1.1.2.2.1.3.1.1.2		.1.3.6.1.4.1.2378.1.1.2.2.1.3.1.1.2.11==NO RESPONSE FROM SNTP SERVER
faultCurrentAlarmEntrySeverity	1.3.6.1.4.1.2378.1.1.2.2.1.3.1.1.3	{3=critical, 2=alert, 1=em...	.1.3.6.1.4.1.2378.1.1.2.2.1.3.1.1.3.11==2
faultCurrentAlarmEntrySource	1.3.6.1.4.1.2378.1.1.2.2.1.3.1.1.4		.1.3.6.1.4.1.2378.1.1.2.2.1.3.1.1.4.11==/ne
faultLogCurrentSequenceNumber	1.3.6.1.4.1.2378.1.1.2.2.1.2.7.0		33

Specify the information needed to validate the OIDs:

IP Address:

SNMP version:

Community name:

alias1_system maps to the OID corresponding to system node in SNMPv2-MIB. The OID is invalid as no value can be read from it.

alias2_sysDescr maps to the OID corresponding to sysDescr scalar object under system node in SNMPv2-MIB. The value read is displayed in the Validation column.

alias3_interfaces maps to the OID corresponding to interfaces node in MBR2200M-SMI. The OID is invalid as no value can be read from it.

alias4_ifTable maps to the OID corresponding to ifTable node in RFC1213-MIB. This is a table so the value displayed in the Validation column is the value of the first column and the first instance.

alias5_ifEntry maps to the OID corresponding to ifEntry node in RFC1213-MIB. The value displayed in the Validation column is the value of the first column and the first instance as displayed for alias4_ifTable.

alias6_ifDescr maps to the OID corresponding to ifDescr column defined in ifTable in RFC1213-MIB. The value displayed in the Validation column is the value of the first instance.

alias7_ifDescrInstance1 maps to the OID corresponding to the first instance for ifDescr column defined in ifTable in RFC1213-MIB. The value displayed in the Validation column is as displayed for alias6_ifDescr.

alias8_ifDescrInstance110 maps to the OID corresponding to instance 110 for ifDescr column defined in ifTable in RFC1213-MIB.







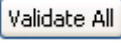
The next two aliases, dummyalias1 and dummyalias2 map to some invalid OIDs.

The last aliases in the table give other example of mappings.

Notice also that for alias2_sysDescr and faultLogCurrentSequenceNumber a suffix “.0” was added to the OIDs as these are scalars.

Available operations

The following operations are available in the Alias List page:

-  Create an entry in the Alias List table.
-  Modify a selected entry in the Alias List table. This can be done also by double-clicking on the selected row.
-  Delete one or more entries from the Alias List table. Aliases that are in use cannot be deleted.
-  Validate the selected alias(es) in the Alias List table.
-  Import a list of aliases from a file and replace the content of the Alias List table. The file must correspond to the format required by PTP 820 NMS.
-  Export to a file the content of Alias List table. The default file name will be <product_name>-AliasList.properties.
-  Validate All Validate all the aliases in the Alias List table against the specified element IP address.

Current alarm table configuration

Current alarm table configuration page is used to configure handling of alarms for open SNMP elements for which the alarms are presented in a table format in the MIB file. The strategy is disabled by default when an open SNMP configuration is created. You can enable it from the pop-up menu by clicking right on the Current Alarm Table in the tree.

Figure 201 Current alarm table configuration**Current Alarm Table**

Configure handling of alarms for open SNMP elements for which the alarms are presented in a table format in the MIB file.

Alarm Text Mapping

Alarm text:

Severity Mapping

Severity:

Critical:	<input type="text" value="High Critical"/>	Warning:	<input type="text" value="Warning"/>
Major:	<input type="text" value="Major"/>	Indeterminate:	<input type="text" value="Indeterminate"/>
Minor:	<input type="text" value="Minor"/>	Info:	<input type="text" value="Info"/>

Probable Cause Qualifier Mapping

Specify the OID mapping for probable cause qualifier. Make sure the mapping gives unique values. For example, alarm source can be used in the mapping together with other OID mappings:

Probable cause qualifier:

Alarm Type Mapping

Alarm type:

Equipment:	<input type="text" value="3"/>	Processing Error:	<input type="text" value="4"/>
Communication:	<input type="text" value="1"/>	Quality of Service:	<input type="text" value="5"/>
Environmental:	<input type="text" value="2"/>	Security:	<input type="text" value="6 7"/>

Additional Text Mapping

Additional Text:

If the following aliases are created in the Alias List in the figure above:

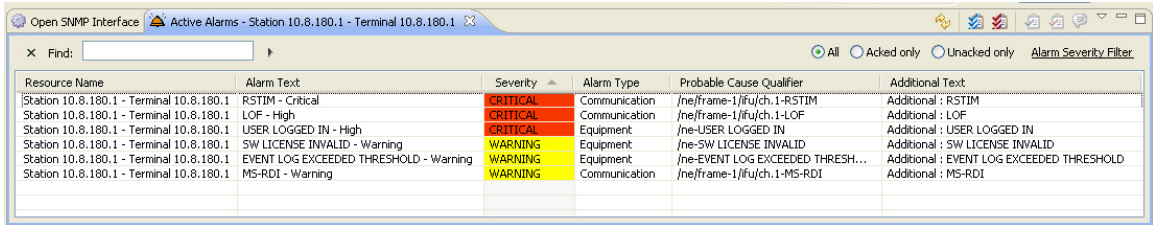
- faultCurrentAlarmEntryName maps to an OID which value gives the alarm text
- faultCurrentAlarmEntrySource maps to an OID which value gives the source of the alarm
- faultCurrentAlarmEntryEventType maps to an OID which value gives the alarm type
- faultCurrentAlarmEntrySeverity maps to an OID which value gives the alarm severity with the following translation: {1=Indeterminate, 2=Warning, 3=Info, 4=Major, 5=Minor, 6=Critical, 8=High}

Then a possible configuration in the Current Alarm Table can be done as shown above.

Notice that the faultCurrentAlarmEntrySeverity alias is added to the configuration of the Alarm Text. This causes the translated alarm severity to be appended to the Alarm Text.

The Active Alarms view for the Open SNMP configuration defined above may look something like this:

Figure 202 Active alarms view



Resource Name	Alarm Text	Severity	Alarm Type	Probable Cause Qualifier	Additional Text
Station 10.8.180.1 - Terminal 10.8.180.1	RSTIM - Critical	CRITICAL	Communication	/ne/frame-1/fu/ch.1-RSTIM	Additional : RSTIM
Station 10.8.180.1 - Terminal 10.8.180.1	LOF - High	CRITICAL	Communication	/ne/frame-1/fu/ch.1-LOF	Additional : LOF
Station 10.8.180.1 - Terminal 10.8.180.1	USER LOGGED IN - High	CRITICAL	Equipment	/ne-USER LOGGED IN	Additional : USER LOGGED IN
Station 10.8.180.1 - Terminal 10.8.180.1	SW LICENSE INVALID - Warning	WARNING	Equipment	/ne-SW LICENSE INVALID	Additional : SW LICENSE INVALID
Station 10.8.180.1 - Terminal 10.8.180.1	EVENT LOG EXCEEDED THRESHOLD - Warning	WARNING	Equipment	/ne-EVENT LOG EXCEEDED THRESH...	Additional : EVENT LOG EXCEEDED THRESHOLD
Station 10.8.180.1 - Terminal 10.8.180.1	MS-RDI - Warning	WARNING	Communication	/ne/frame-1/fu/ch.1-MS-RDI	Additional : MS-RDI

The following fields can be configured on the Current Alarm Table page:

Table 52 Current alarm table

Name	Explanation
Alarm text	Holds a combination of fixed text and aliases added in the field by typing or by inserting using Select Alias button. The mapping configured here will determine the value that will be displayed in the Alarm Text column in Active Alarms and Historical Alarms views.

Name	Explanation
Severity	<p>Holds a combination of fixed text and aliases added in the field by typing or by inserting using Select Alias button. The mapping configured here will determine the value that will be displayed in column Severity from Active Alarms and Historical Alarms views.</p> <p>In addition, the alarm severity must be mapped into one of the following PTP 820 NMS notations: Critical, Major, Minor, Warning, Info and Indeterminate. If no mapping is configured, Indeterminate will be used by default. The mapping consists in one or more OID values or translation values written using regular expressions.</p> <p><u>Example:</u> If the values read using the mapping defined for Severity field are 1, 2, 3, 4, 5, 6, 7, and 8, the following mapping can be configured for the severities in PTP 820 NMS notation:</p> <p>Critical: 1 3 Warning: 5</p> <p>Major: 2 Info: 6 7</p> <p>Minor: 4 Indeterminate: 8</p> <p>If the following translation is defined for the alias used in Severity field, then the translated values can be used instead of OID values:</p> <p>1=emergency 5=warning</p> <p>2=alert 6=notice</p> <p>3=critical 7=info</p> <p>4=error 8= unknown</p> <p>Critical: emergency critical Warning: warning</p> <p>Major: alert Info: info notice</p> <p>Minor: error Indeterminate: unknown</p>

Name	Explanation
Probable Cause Qualifier	<p>Holds a combination of fixed text and aliases added in the field by typing or by inserting using Select Alias... button. The mapping configured here will determine the value that will be displayed in column Probable Cause Qualifier from Active Alarms and Historical Alarms views.</p> <p><u>Note1:</u> The mapping defined for the probable cause qualifier must result in unique values, otherwise some alarms will overlap each other in the Active Alarms and Historical Alarms views. For example, alarm source can be used in the mapping together with other OID mappings.</p> <p><u>Example:</u> If the following aliases are created in the Alias List:</p> <p>faultCurrentAlarmEntryName = maps to an OID which value gives the alarm text</p> <p>faultCurrentAlarmEntrySource = maps to an OID which value gives the source of the alarm</p> <p>Then the probable cause qualifier can be mapped to the following:</p> <p>< faultCurrentAlarmEntrySource> - < faultCurrentAlarmEntryName></p>

Name	Explanation
Alarm Type	<p>Holds a combination of fixed text and aliases added in the field by typing or by inserting using Select Alias... button. The mapping configured here will determine the value that will be displayed in column Alarm Type from Active Alarms and Historical Alarms views.</p> <p>In addition, the alarm type must be mapped into one of the following PTP 820 NMS notations: Equipment, Communication, Environmental, Processing Error, Quality of Service and Security. If no mapping is configured, Equipment will be used by default. The mapping consists in one or more OID values or translation values written using regular expressions.</p> <p><u>Example:</u> If the values read using the mapping defined for Alarm Type field are 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, and 11, the following mapping can be configured for the alarm types in PTP 820 NMS notation:</p> <p>Equipment: 1 5 Processing Error: 4</p> <p>Communication: 2 Quality of Service: 3</p> <p>Environmental: 10 Security: 6 7 8 9 11</p> <p>If the following translation is defined for the alias used in the Alarm Type field, then the translated values can be used instead of OID values:</p> <p>1=other 7=integrityViolation</p> <p>2=communications Alarm 8=operationalViolation</p> <p>3=qualityOfService Alarm 9=physicalViolation</p> <p>4=processingError Alarm 10=environmental Alarm</p> <p>5=equipment Alarm 11=timeDomainViolation</p> <p>6=securityServiceOrMechanismViolation</p>
Additional Text	<p>Holds a combination of fixed text and aliases added in the field by typing or by inserting using Select Alias... button. The mapping configured here will determine the value that will be displayed in column Additional Text from Active Alarms and Historical Alarms views.</p>

Current alarm list configuration

Current alarm list configuration page is used to configure handling of alarms for open SNMP elements for which the alarms are defined as scalars in the MIB file. Each list entry defines one alarm. If the same OID is configured for more than one alarm, the Bit position field must be different.


The strategy is disabled by default when an open SNMP configuration is created. You can enable it from the pop-up menu by clicking right on the Current Alarm List in the tree.

The Mapping for raised field specifies the OID value associated with a raised alarm condition. It is also possibility to define a Mapping for raised using [regular expressions](#).

Figure 203 Current alarm list

Current Alarm List

Configure handling of alarms for open SNMP elements for which the alarms are defined as scalars in the MIB file.



Alias ▲	Mask	Alarm Text	Severity	Alarm Type	Additional Text
framerCardAlarmFlag	8	TPLL Tx PLL error	Critical	Environmental	
framerCardAlarmFlag	6	RPLL Rx PLL error	Critical	Environmental	
framerCardAlarmFlag	2	BER6	Major	Equipment	
framerCardAlarmFlag	14	Loss of Clock(LCK2)	Warning	Equipment	
framerCardAlarmFlag	4	BER3	Major	Equipment	
framerCardAlarmFlag	16	Loss of Frame Alignment...	Minor	Equipment	
framerCardAlarmFlag	10	FLID error	Major	Equipment	
framerCardAlarmFlag	17	Framer digital loop state	Info	Environmental	
radioAlarmFlag	9	TxMute State	Info	Communication	
radioAlarmFlag	6	MWaveLockDetectAlrm(1...	Critical	Processing Error	
radioAlarmFlag	2	ALCArm	Minor	Equipment	
radioAlarmFlag	7	LoopbackLockDetAlrm	Critical	Equipment	
radioAlarmFlag	4	TxLockDetectAlrm	Major	Communication	
radioAlarmFlag	1	RSSIAlrm	Minor	Equipment	
radioAlarmFlag	8	RF LoopBack State	Warning	Equipment	
radioAlarmFlag	3	RxLockDetectAlrm	Major	Communication	
radioAlarmFlag	5	DDSLockDetectAlrm(Inva...	Critical	Processing Error	

Mapping for raised:




The following fields can be configured on the Current Alarm List page:

Table 53 Current alarm list

Name	Explanation
Alias name	Must be an alias defined in the Alias List.
Bit position	<p>Contains the bit position from the right. Allowed values are numbers from 1 to 64. The same mask cannot be specified twice for the same OID. If no mask is used, the OID cannot be used twice.</p> <p><u>Example:</u> If the MIB defines the following alarm mask for a single OID:</p> <p>bit0 : RSSIAlarm, bit1 : ALCArm, bit2 : RxLockDetectAlarm, bit3 : TxLockDetectAlarm, bit4 : DDSLockDetectAlarm(Invalid), bit5 : MWaveLockDetectAlarm(Invalid), bit6 : LoopbackLockDetAlarm, bit7 : Rf LoopBack State, bit8 : TxMute State</p> <p>Then possible values in the Bit position field are 1-9.</p>
Alarm text	Gives the most likely reason for the alarm
Severity	One of the possible alarm severities: Critical, Major, Minor, Warning, Indeterminate, or Info. By default, Indeterminate is used.
Alarm type	One of the following types: Equipment, Communication, Environmental, Processing Error, or Quality Of Service. By default, Equipment is used.
Additional Text	Free form text description of the alarm.

Available operations

The following operations are available in the Current Alias List page:

-  Create an entry in the Current Alarm List table by opening Create alarm OID dialog where the user has to specify the alias name, the mask, the alarm text, the severity, the alarm type and the additional text.
-  Modify a selected entry in the Current Alarm List table. This can be done also by double-clicking a selected entry in the table.
-  Delete one or more selected entries from Current Alarm List table. The aliases that are in use cannot be deleted unless all the references are removed.

Preferences

Preferences: Fault Colors and Sounds

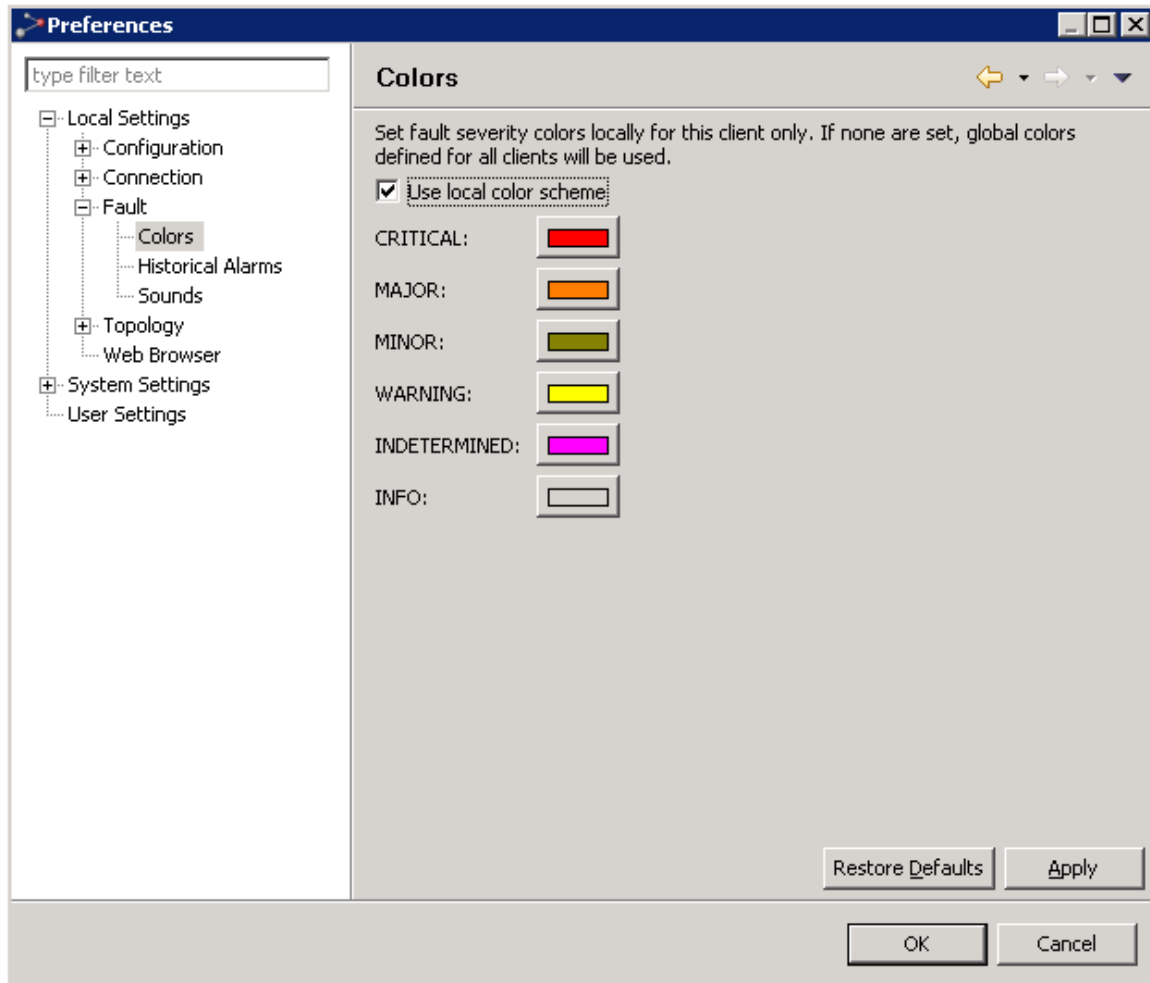
In these preferences pages you can set several general definitions for color and sound notifications for changes to alarms and connection states on NEs in your network. These settings might influence [all GUI where alarms are visualized](#).

Definitions for fault colors and sounds are done on several preference pages:

- Local color scheme is defined on the client in the [Local Colors](#) preference page
- Local colors for displaying of "Loss of Connectivity" state and for displaying connectivity is defined on the client in the [Local Connectivity colors](#) preference page
- Sounds and notification-dialogs is defined on the client in the [Sounds](#) preference page
- Global color scheme is defined on the server in the [System Colors](#) preference page
- Global colors for displaying of "Loss of Connectivity" state and for displaying connectivity is in the [System connectivity colors](#) preference page

Local Colors

This page can be found under Local Settings | Fault | Colors in the [Preferences](#) pages.

Figure 204 Preferences local colors

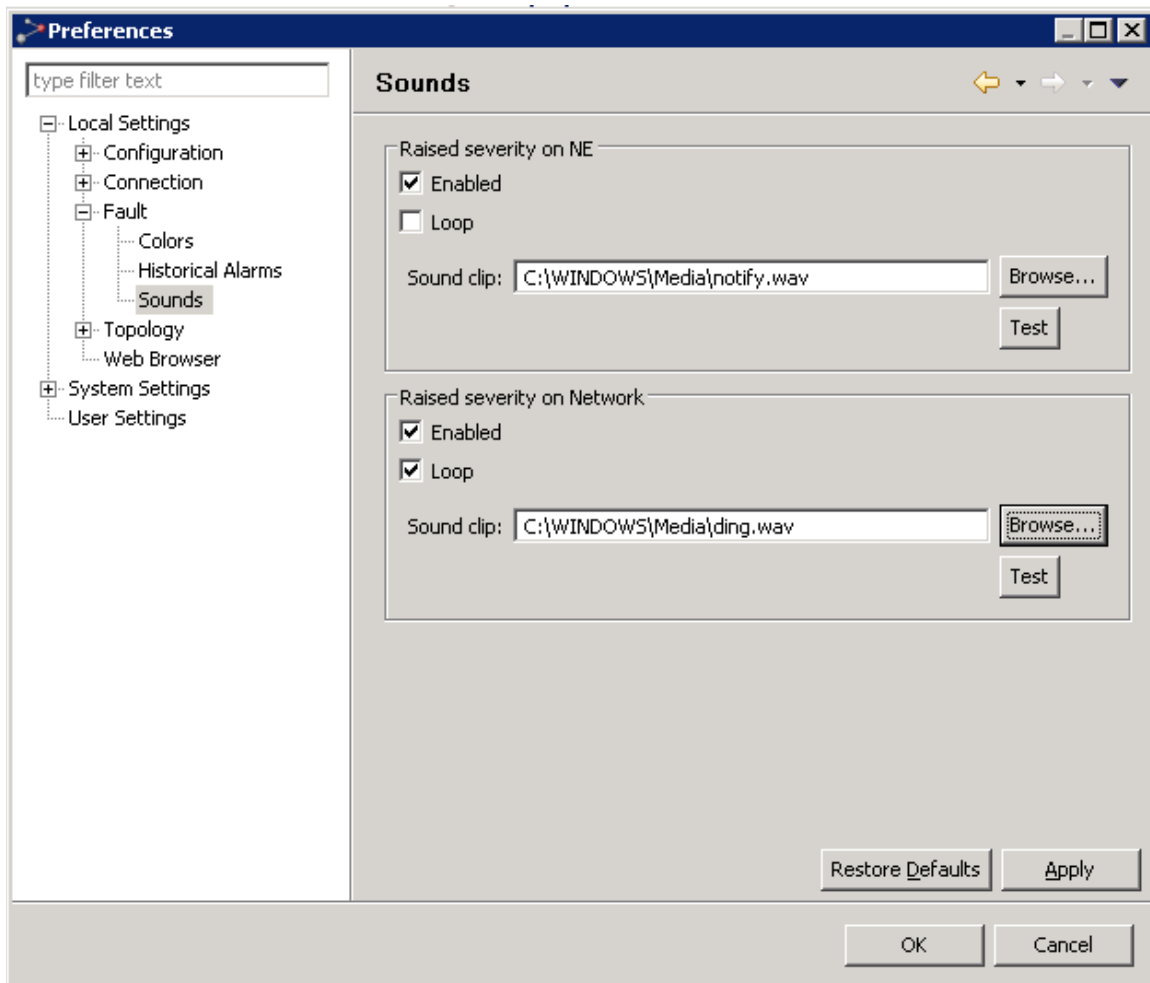
On the Local Colors preferences page you can define your own [severity colors](#) on your local client. These settings will affect colors for faults and states for NEs in all topology views (Geographical or Logical Map or Tree), in the [Active Alarms](#) view and in the [Alarm Summary](#) view.

Click the Use local color scheme checkbox to enable/disable use of local color settings.

If local color settings are enabled, you can click each of the color buttons to select a new color for its corresponding severity/state. These color definitions on the Local Colors preference page will override the server definitions in the [System Colors](#) preferences page.

Sounds

This page can be found under Local Settings > Fault > Sounds in the [Preferences](#) pages.

Figure 205 Preferences sounds

In the Sounds preferences page you can enable sound notification whenever an alarm [severity](#) is increased in certain nodes in your network.

The Sounds page consists of two areas with similar input fields:

- In the Raised severity on NE area you can define notifications given when receiving alarms that increase the severity of an NE node.
- In the Raised severity on Network area you can define notifications given when receiving alarms that increase the severity of the top-node in a network model - including both the [Geographical model](#) and the [Logical model](#).

The controllers available in the two areas are as follows:

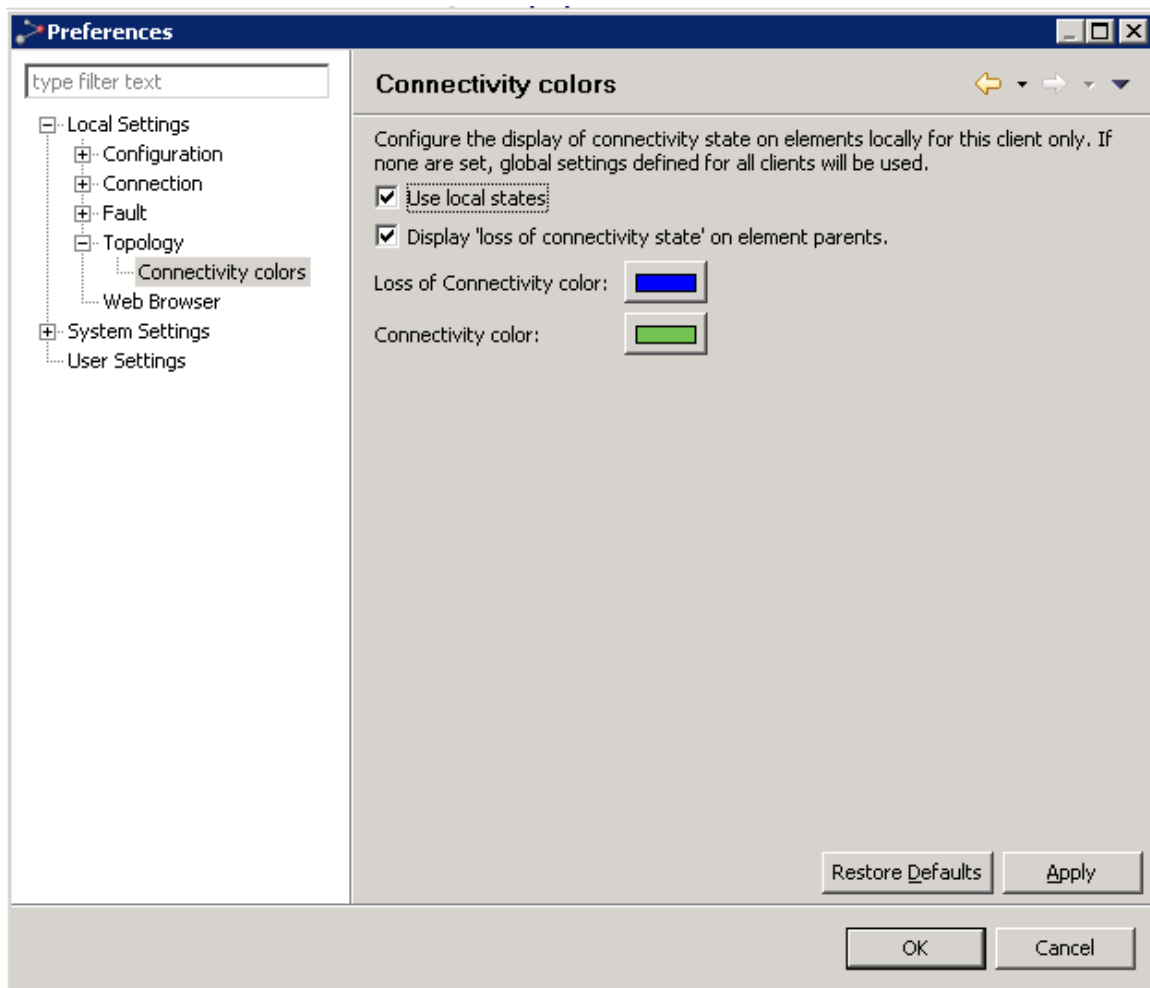
- Click the Enabled checkbox to enable/disable sound notifications for the category in this area

- Click the Loop checkbox to enable/disable "looping" of this sound notification. "Looping" means that whenever a severity is increased, an [Alarm](#) dialog will appear with a warning indicating that an increased alarm severity has been detected, and the notification sound will be repeated until this dialog is closed. The Alarm dialog will appear irrespective of what [dialog](#), [view](#) or [perspective](#) is currently open in PTP 820 NMS.
- Click the Browse button to select a notification sound. The file must be of the type .wav (uncompressed Windows audio waveform files).
- The path for the notification sound is displayed in the Sound clip field. Alternatively write the path and filename for the .wav file here.
- Use the Test button to listen to your selected notification sound.

Local connectivity colors

This page can be found under Local Settings | Topology | Connectivity colors in the [Preferences](#) pages.

Figure 206 Preferences local connectivity colors



In the Connectivity colors preferences page you can define your own colors to be used to display [loss of connectivity](#) (i.e. when contact is lost with the NE) and connectivity (i.e. when "normal" connection is established with the NE). These settings will be used to display connectivity for NEs in all topology views (Geographical or Logical Map or Tree).

Click the Use local states checkbox to enable/disable use of local color settings.

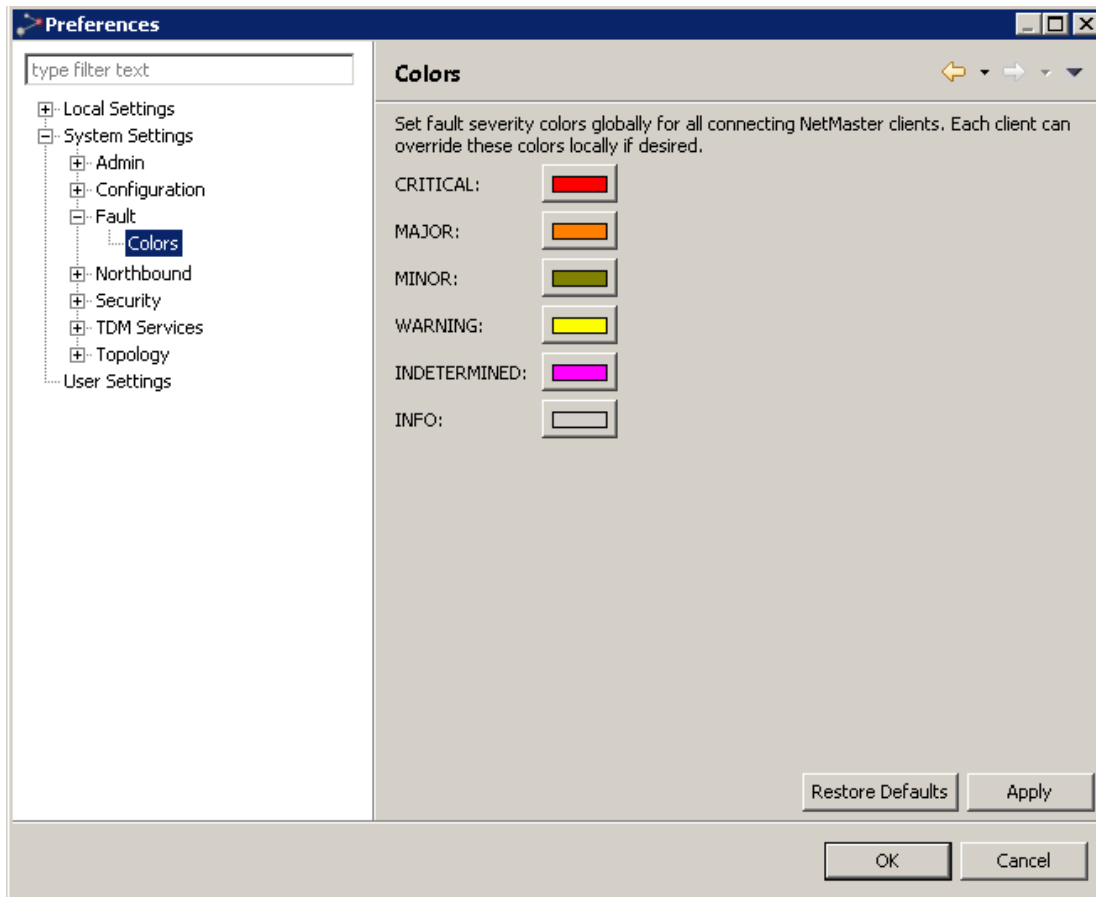
Click the Display 'loss of connectivity state' on element parents checkbox to choose whether color for "loss of connectivity" should be displayed only on NE level in the topology views, or if "loss of connectivity" should be propagated to higher levels in the tree/map.

If local color states are enabled, you can click each of the color buttons to select new colors for its corresponding connectivity state. These color definitions on the Local Colors preference page will override the server definitions in the [System Connectivity colors](#) preferences page.

System Colors

This page can be found under **System Settings > Fault > Colors** in the [Preferences](#) pages.

Figure 207 Preferences system colors



On the System Colors preferences page you can define colors for visualizing faults and states on all clients connected to this server. This setting will affect the [severity colors](#) for the topology views (Geographical or Logical Map or Tree), in the [Active Alarms](#) view and in the [Alarm Summary](#) view.

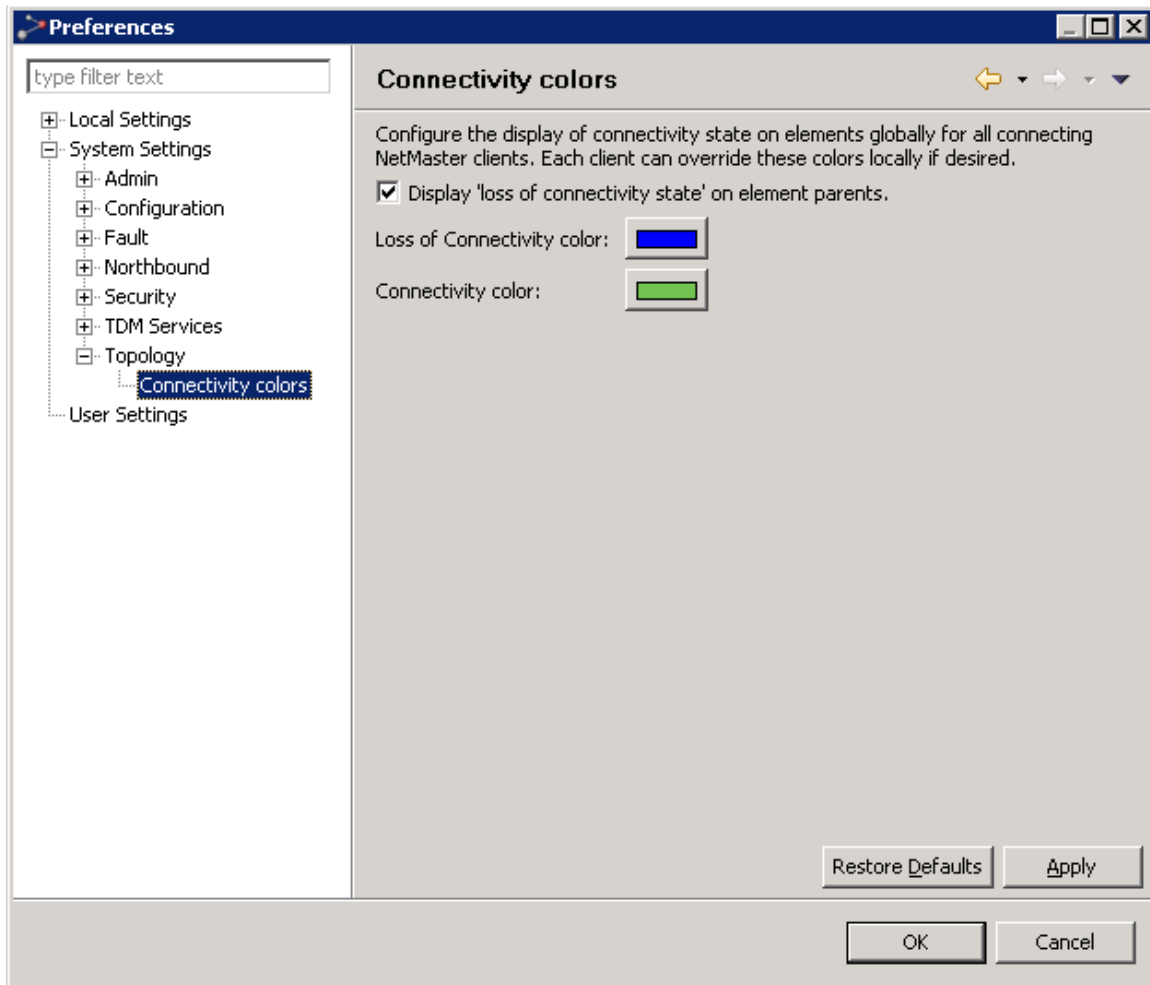
Click each of the color buttons to select a new color for its corresponding severity/state.

Please note that these color settings can be overridden on the client, if the user enables use of a Local Color Scheme in the [Local Colors](#) preferences page.

System connectivity colors

This page can be found under System Settings > Topology > Connectivity colors in the [Preferences](#) pages.

Figure 208 Preferences system connectivity colors



In the System Connectivity colors preferences page you can define what colors that should be used to display connectivity state on all clients connected to this server. These settings affect display of connectivity in all topology views (Geographical or Logical Map or Tree).

Click the Display 'loss of connectivity state' on element parents checkbox to choose if color for "loss of connectivity" should be displayed only on NE level, or if "loss of connectivity" should be propagated to higher levels in the tree/map.

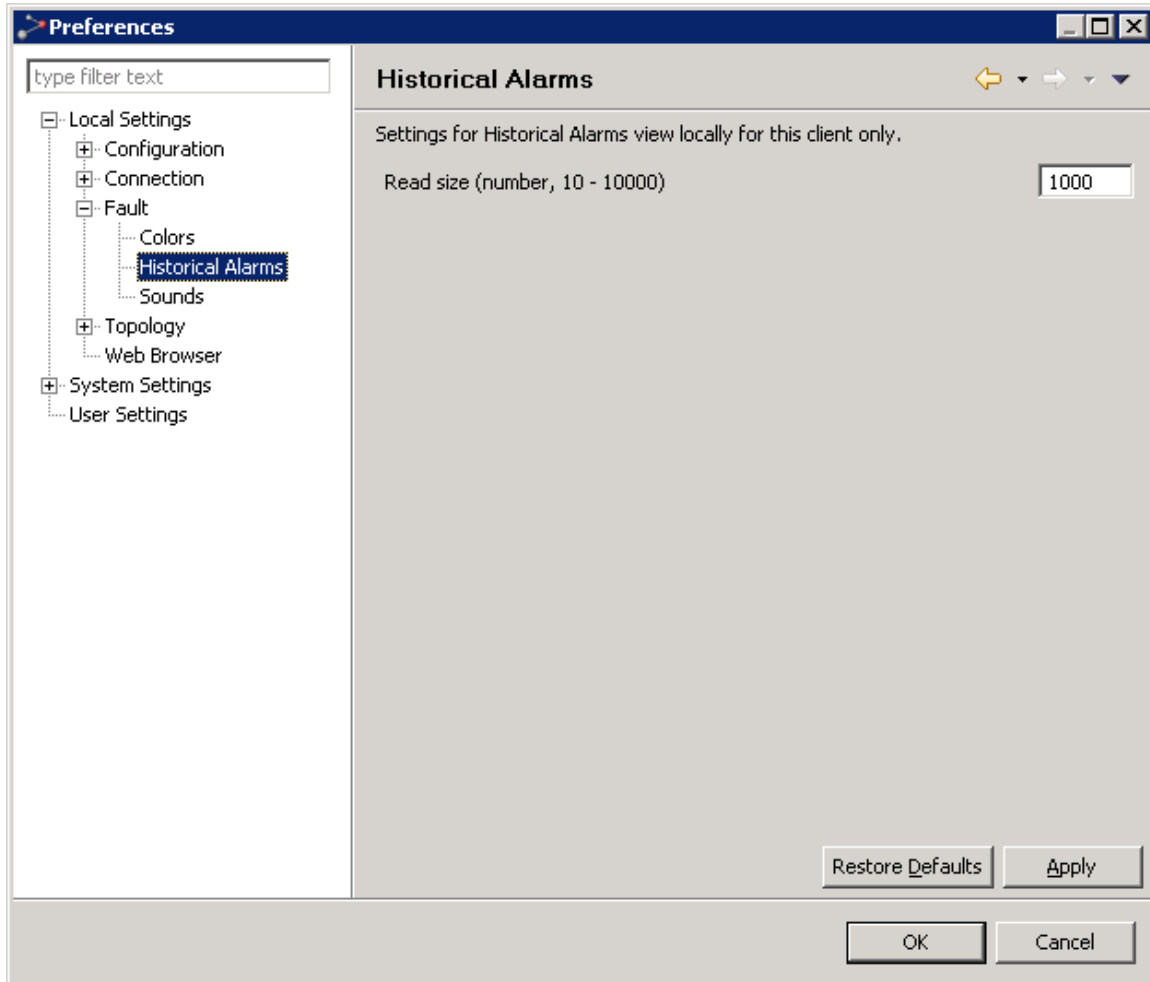
Click each of the color buttons to select a new color for its corresponding severity/state.

Please note that these color settings can be overridden on the client, if the user enables use of a Local State color in the [Local Connectivity colors](#) preferences page.

Preferences: Historical Alarms

This page can be found under **Local Settings > Fault > Historical Alarms** in the [Preferences](#) pages.

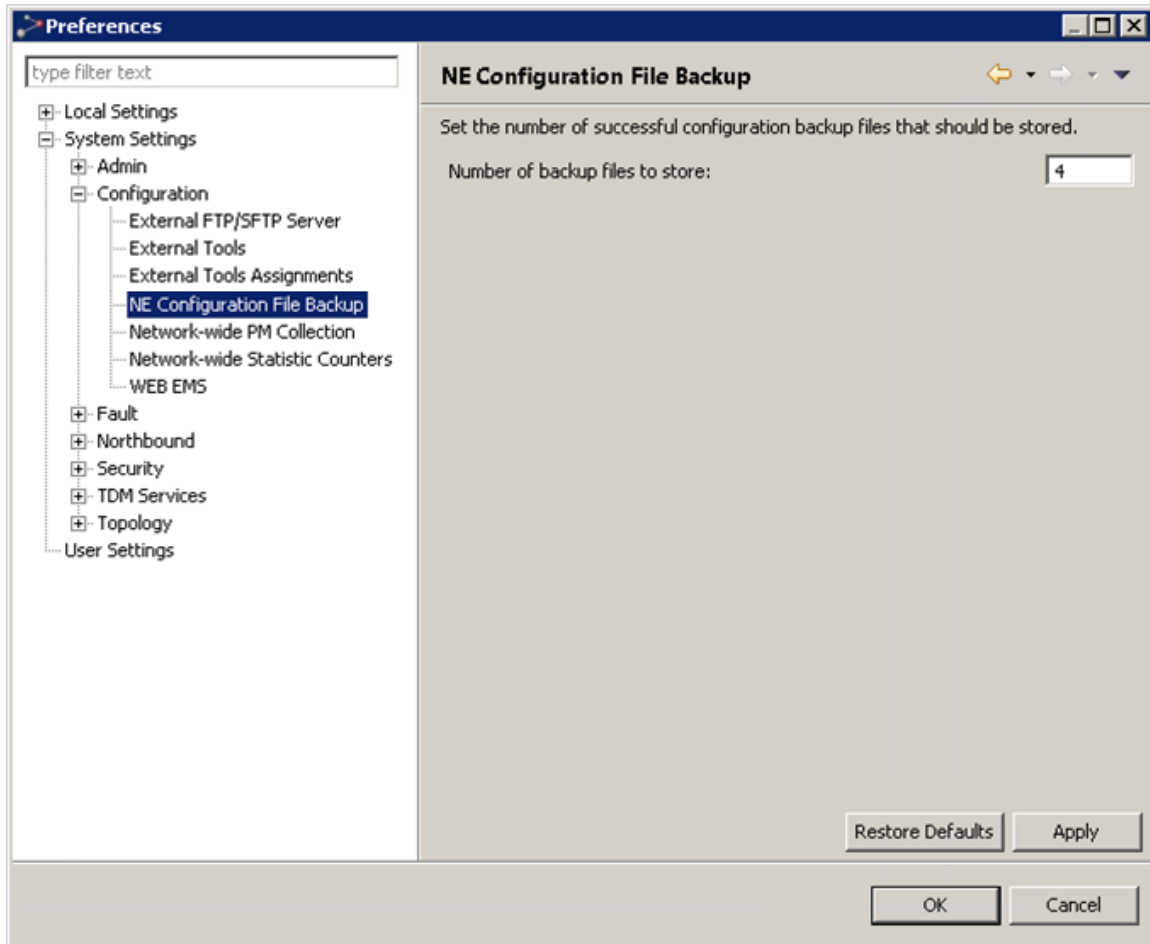
Figure 209 Preferences - Historical Alarms



On the Historical Alarms preferences page, you can define the maximum number of alarms you can view per read size in the Historical Alarms view.

Preferences: NE Configuration File Backup

This page can be found under **System Settings > Configuration > NE Configuration File Backup** in the [Preferences](#) pages.



In this page you can set the maximum number of scheduled backup configuration files saved in the PTP 820 NMS backup file repository for each NE.

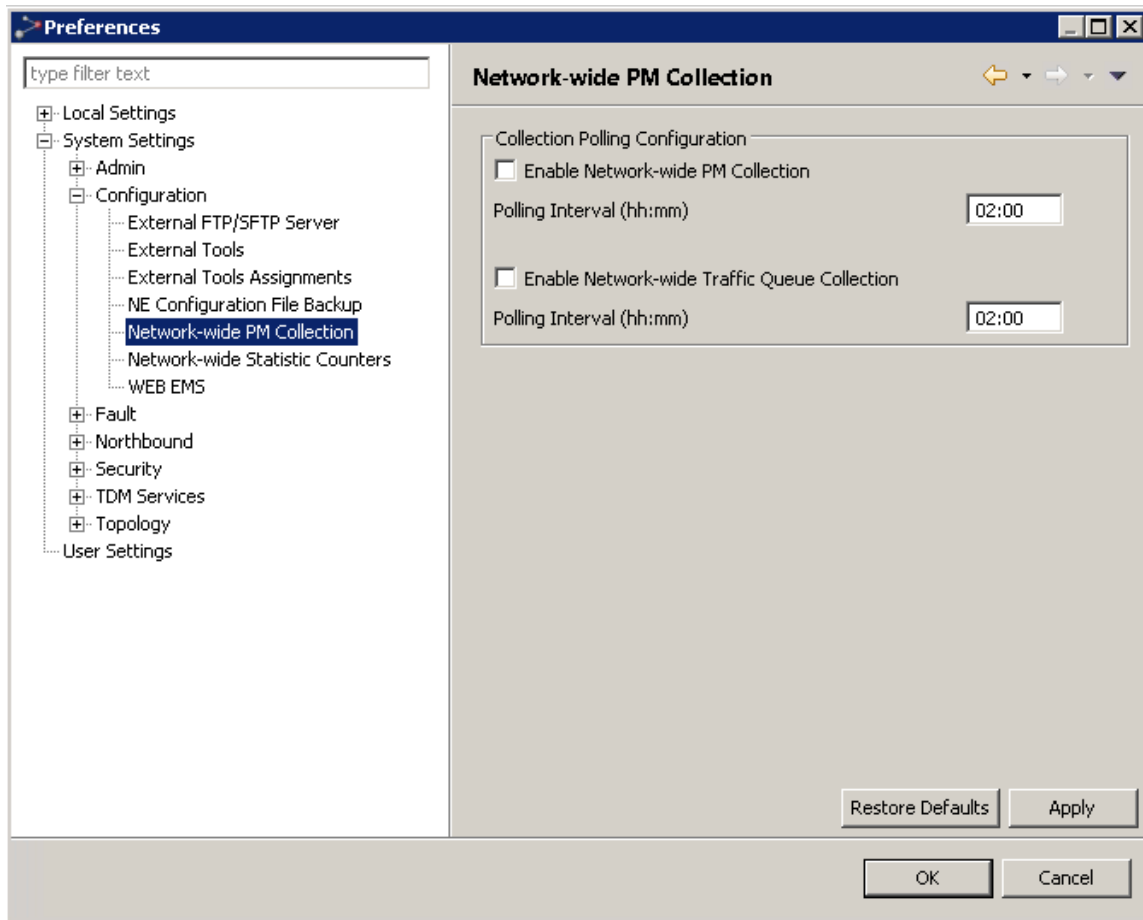
Enter the maximum number in *Number of backup files to store*. You can enter a number between 1 – 4. PTP 820 NMS employs a FIFO (First-in First-out) policy, with the newest backup file overwriting the oldest one.

To enable scheduled backup of configuration files, use the [Scheduled Backup](#) option available in PTP 820 connection templates.

Backup will be performed only if the configuration file has changed since the last backup.

Preferences: Network-wide PM Collection

This page can be found under **System Settings > Configuration > Network-wide PM Collection** in the Preferences pages.

Figure 210 Preferences - Network wide PM Collection

Each PTP 820 device stores its own Performance Monitoring (PM) values, and each PTP 820 stores its own Traffic Queue values, for each fifteen-minute interval in the past 24 hours. As each new 15-minute interval ends, the device saves the newest values by overwriting the oldest values.

PTP 820 NMS collects these values by polling the devices. In this page you can disable, enable or set the time interval for PTP 820 NMS collection of these values in the Preferences window.

Keep in mind that you can specify how long to keep the collected information in the database. To do so, refer to [Preferences: Days to keep historic data](#).

Once PTP 820 NMS is collecting network-wide PM counters and traffic queue counters, you can generate various PM reports either through the GUI or using the `pmreport` CLI command. For information see [NG Performance Reports](#).

Network-wide PM collection

- Check the **Enable Network-wide PM Collection** checkbox to enable PM collection. PTP 820 NMS will collect all the 15-minute port performance counters for all enabled ports of all PTP 820 devices managed by PTP 820 NMS.



Note: Collection of the PM counters for Performance reports is separate from the collection mechanism used in the Performance Collection Control View which is assigned per device and per counter (using templates), so if PM collection is activated in the Performance Collection Control as well, devices may be polled twice for the same information.

A restart is required for the network-wide PM collection to take effect.

Performance counters are not collected for Multi-Carrier ABC groups on PTP 820G/GX devices.

- If you enable PM collection, then in its **Polling Interval** field you can enter an interval in the format <hours>:<minutes>, where the hours range from 00 to 23 and the minutes are either 00, 15, 30 or 45. That is, the polling interval must be a multiple of a 15-minute interval, with a range from 00:15 to 23:45.

For example, if you want PTP 820 NMS to poll the devices and collect their PM counter values every five and a half hours, specify a polling interval of 05:30.



Note: A reset is required for the polling interval change to take effect.

In a [Server High Availability](#) setup, stop the Secondary server while you enable polling or change the polling interval on the Primary server. After saving the settings on the Primary server, restart the Primary server and then start the Secondary server.

Network-wide Traffic Queue collection

- Check the **Enable Network-wide Traffic Queue Collection** checkbox to enable collection of traffic queue data. PTP 820 NMS will collect all the 15-minute port traffic queue counters for all enabled ports of all PTP 820 devices managed by PTP 820 NMS.



Note: A restart is required for any change in the network-wide traffic queue collection to take effect.

- If you enable traffic queue collection, then in its **Polling Interval** field you can enter an interval in the format <hours>:<minutes>, where the hours range from 00 to 23 and the minutes are either 00, 15, 30 or 45. That is, the polling interval must be a multiple of a 15-minute interval, with a range from 00:15 to 23:45.

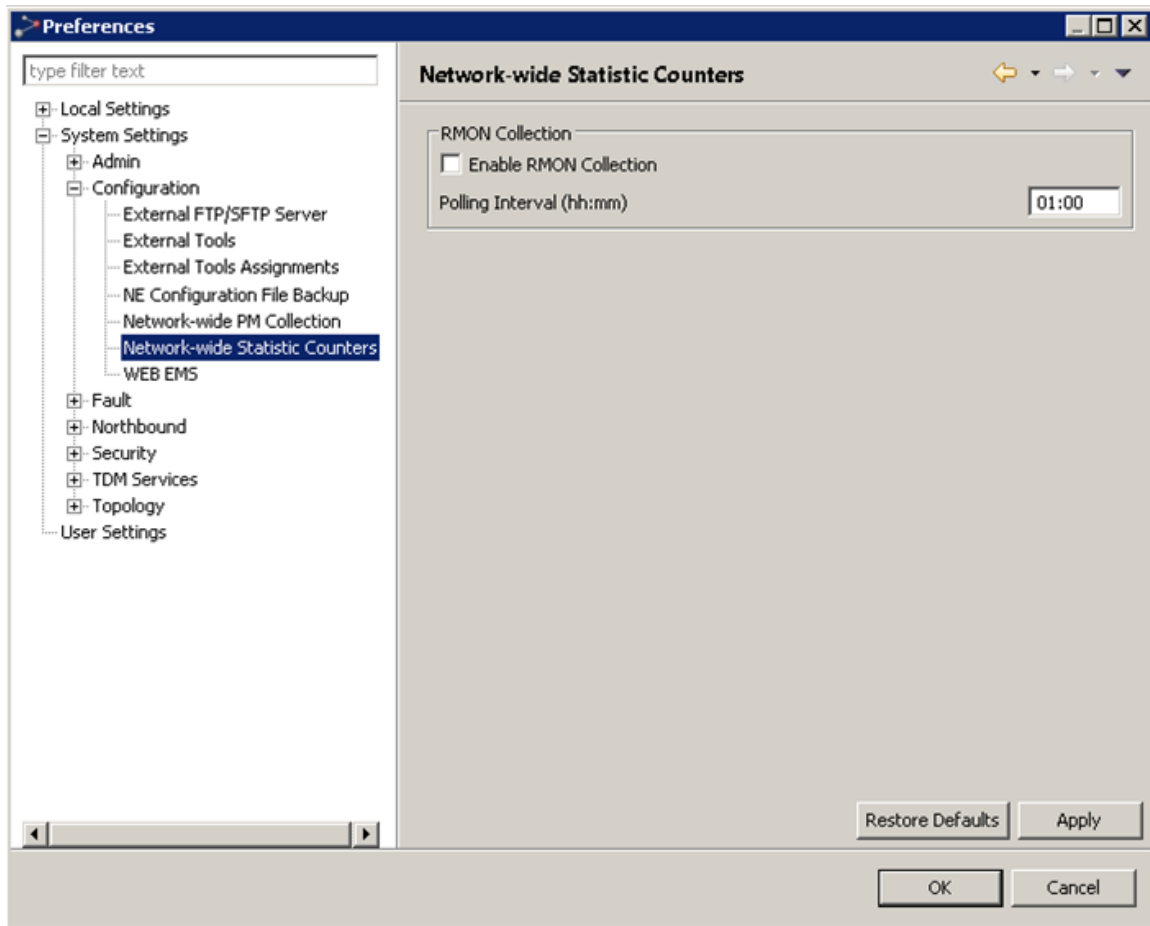


Note: A reset is required for the polling interval change to take effect.

In a [Server High Availability](#) setup, stop the Secondary server while you enable polling or change the polling interval on the Primary server. After saving the settings on the Primary server, restart the Primary server and then start the Secondary server.

Preferences: Network-wide Statistic Counters - RMON Collection

This page can be found under **System Settings > Configuration > Network-wide Statistic Counters** in the Preferences pages.



At any given time, each PTP820 device keeps the RMON value of the current 15-minute interval. PTP 820 NMS can collect these RMON values by polling the PTP820 devices. In this page you can disable, enable or set the time interval for PTP 820 NMS collection of RMON counters.

- Check the Enable RMON Collection checkbox to enable collection of RMON counters. PTP 820 NMS will collect the current 15-minute RMON counter for each enabled port of all PTP820 devices managed by PTP 820 NMS.



Note: Collection of the RMON counters for Performance reports is separate from the collection mechanism used in the Performance Collection Control View which is assigned per device and per counter (using templates), so if PM collection is activated in the Performance Collection Control as well, devices may be polled twice for the same information.

A restart is required for the network-wide RMON counters collection to take effect.

RMON counters are not collected for Multi-Carrier ABC groups on PTP820G/GX devices.

- If you enable PM collection, then in the Polling Interval field you can enter an interval in the format <hours>:<minutes>, where the hours range from 00 to 23 and the minutes are either 00, 15, 30 or 45. That is, the polling interval must be a multiple of a 15-minute interval, with a range from 00:15 to 23:45.

For example, if you want PTP 820 NMS to poll the devices and collect their RMON counter values every five and a half hours, specify a polling interval of 05:30.



Note: A reset is required for the polling interval change to take effect.

In a [Server High Availability](#) setup, stop the Secondary server while you enable polling or change the polling interval on the Primary server. After saving the settings on the Primary server, restart the Primary server and then start the Secondary server

Note: A reset is required for the polling interval change to take effect.

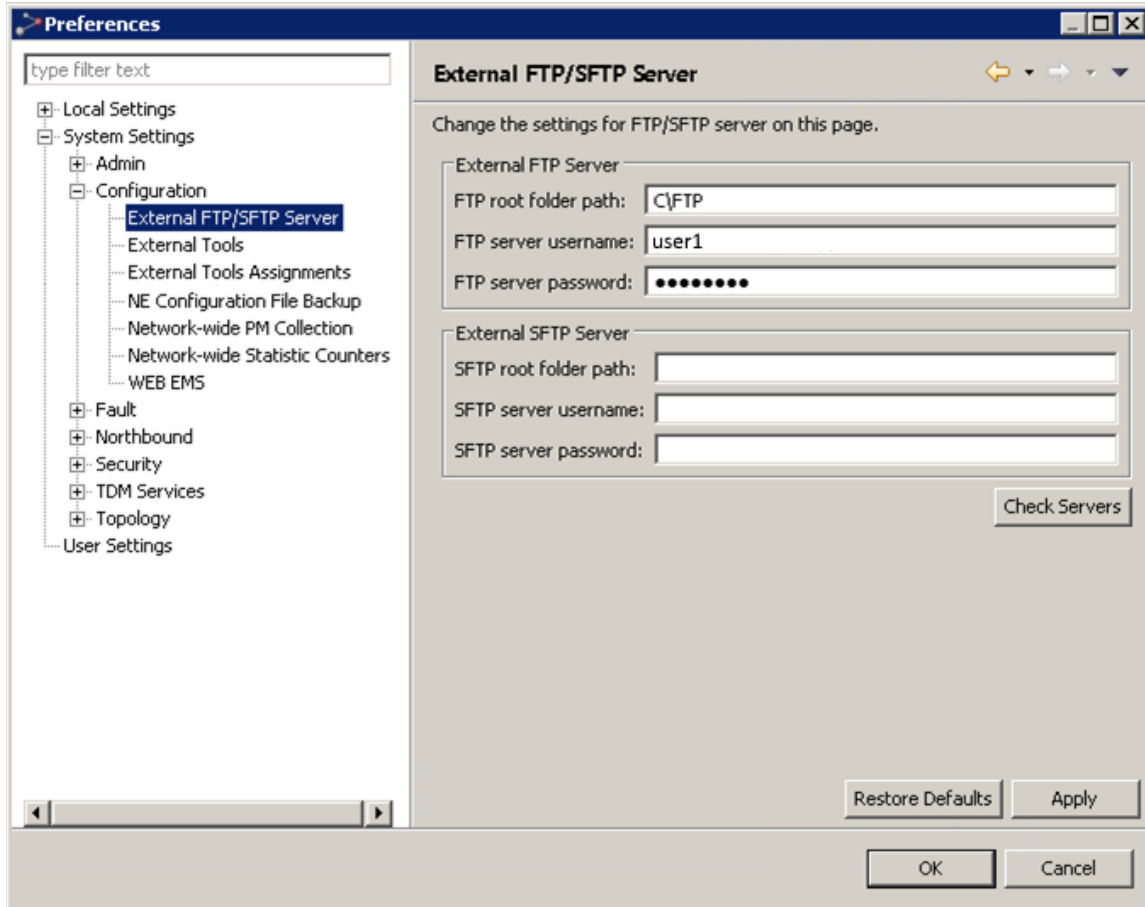
Keep in mind that you can specify how long to keep the collected PM information in the database. To do so, refer to [Preferences: Days to keep historic data](#).

Once PTP 820 NMS is collecting network-wide RMON counters for PTP820 devices, you can generate an RMON report either through the GUI or through using the pmreport CLI command. For information, [NG Performance Reports Generation](#).

Note: In a [High Availability](#) server setup, stop the Secondary server while you enable polling or change the polling interval on the Primary server. After saving the settings on the Primary server, restart the Primary server and then start the Secondary server.

Preferences: External FTP/SFTP Server

This page can be found under **System Settings > Configuration > External FTP/SFTP Server** in the [Preferences](#) pages.



In this page you can configure the settings of the external FTP and/or SFTP server used for downloading and uploading files to the PTP 820 NMS server. The FTP/SFTP server must be installed on the same machine as the PTP 820 NMS server. For installation instruction, refer to [Install and configure an FTP or SFTP server](#).

Preferences: External Configuration Tools

In the preferences pages you can define how to open external tools for configuring NEs in your network. External tools are opened by selecting a NE in the topology views (Geographical or Logical Map or Tree) and using the menu Configuration | External Tools.

Definitions for external configuration tools are done on several preference pages:

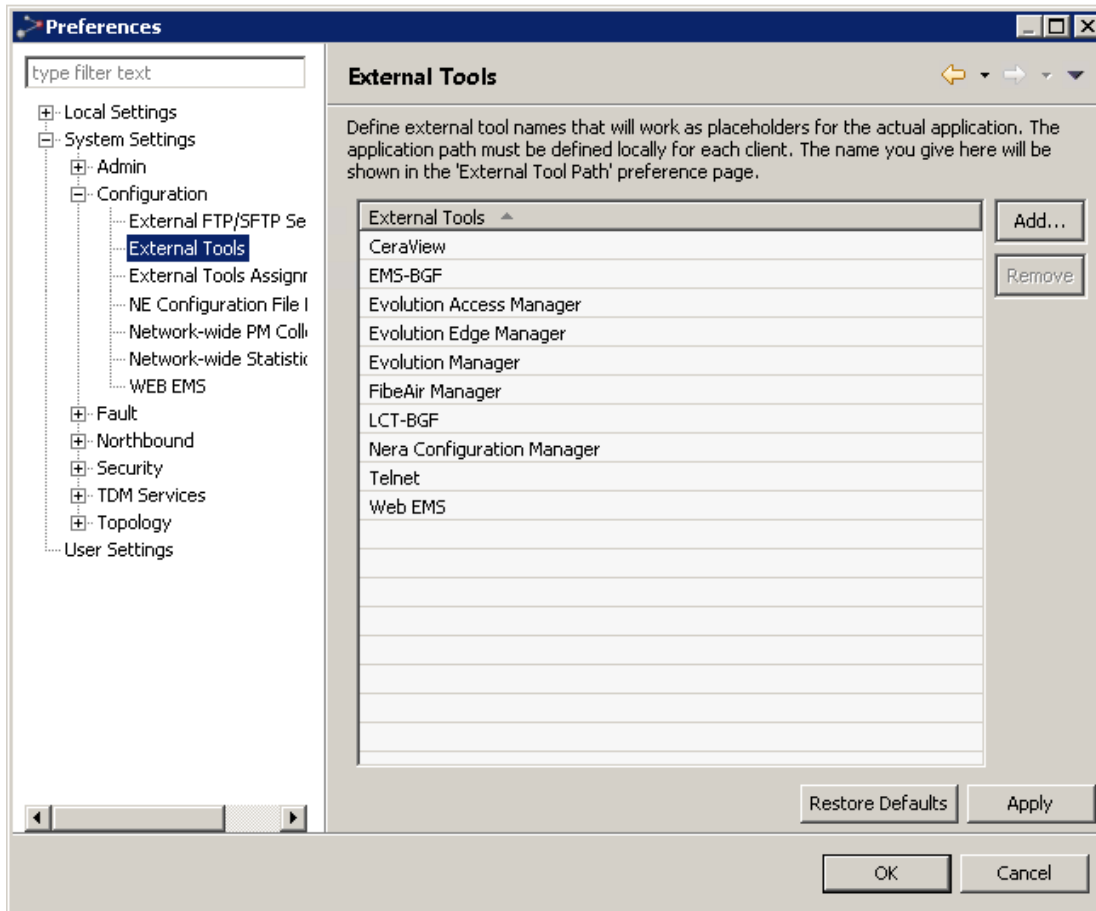
- Group-names for external tools are defined on the server in the [External Tools](#) preference page
- Local paths for external tool applications are defined on the client in the [External Tools Path](#) preference page

- Mapping between a tool and a NE-type are defined on the server in the [External Tools Assignment](#) preference page.

External Tools

This page can be found under **System Settings > Configuration > External Tools** in the [Preferences](#) pages.

Figure 211 Preferences external tools



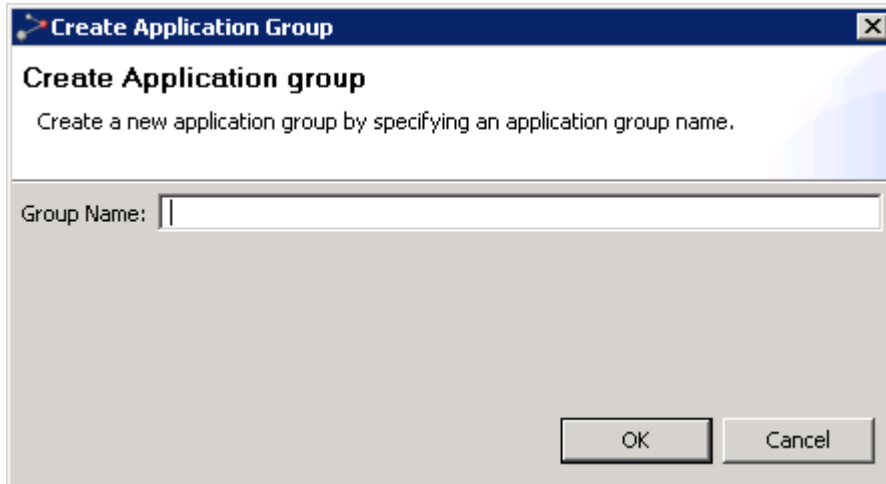
In this page you can create and remove application groups for configuring NEs in your network. Use the Add button to [create a new entry](#) in the External Tools column, or use the Remove button to [delete a selected entry](#) from the column.

The entries in the External Tools column can be found under the context menu **Configuration > External Tools** in the topology views (Geographical or Logical Map or Tree) whenever clicking an NE with this application group enabled. The entries are enabled for each NE type in the [External Tools Assignment](#) system preferences page. The local application path for launching each of the application groups is defined for each client using the [External Tool Paths](#) preferences page.

Create Application group dialog

This dialog is opened whenever the Add button in the [External Tools](#) preferences page is clicked.

Figure 212 Create application group dialog

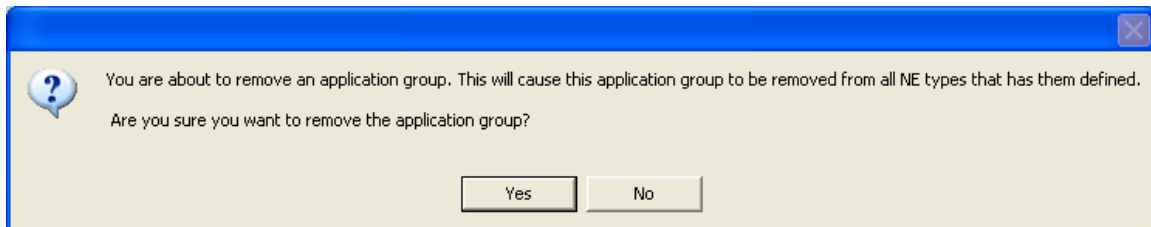


Enter a name for this application group, and then press OK.

Confirm Delete Application group dialog

This dialog is opened whenever the Remove button with an External Tool selected in the [External Tools](#) preferences page is clicked.

Figure 213 Confirm delete application group dialog

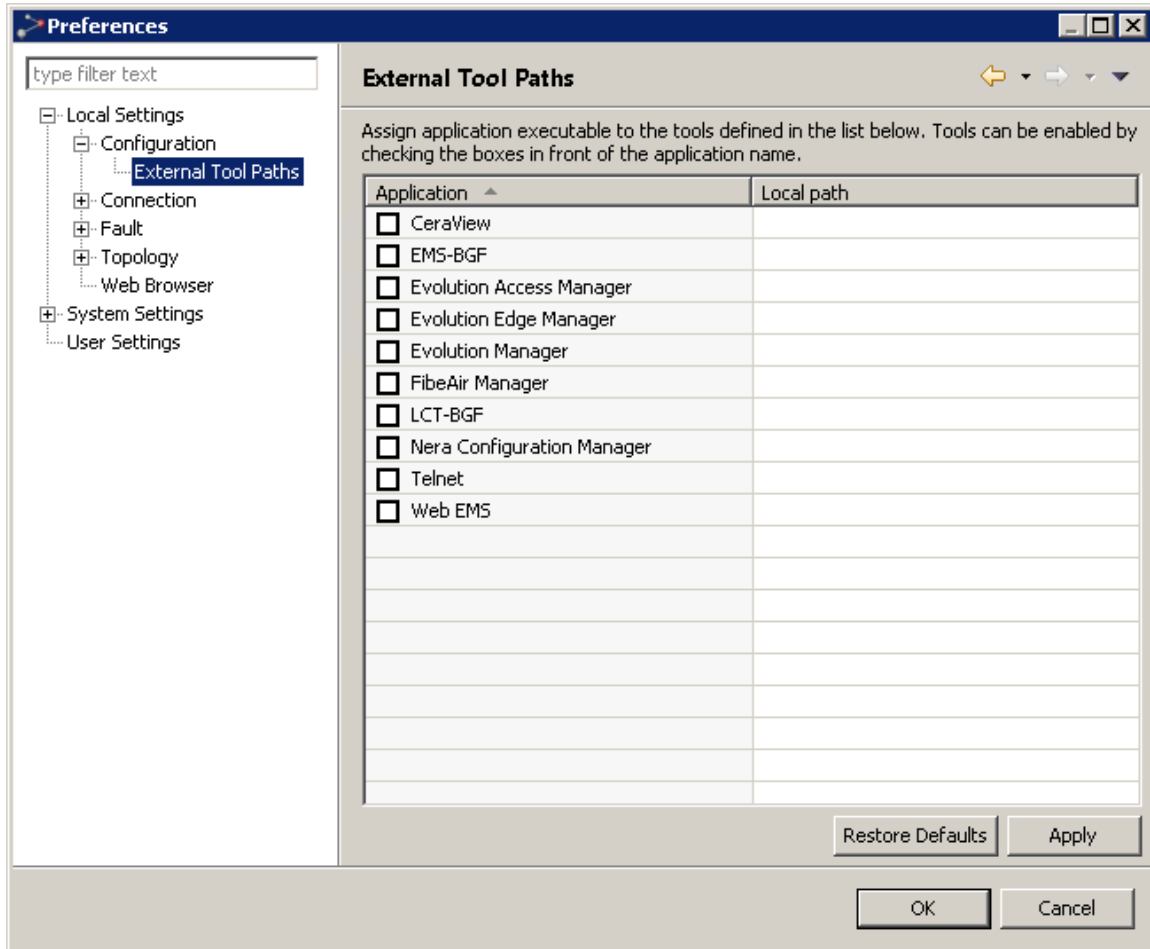


Press Yes to remove the application group, or No to abort the deletion.

External Tool Paths

This page can be found under Local Settings > Configuration > External Tool Paths in the [Preferences](#) pages.

Figure 214 External tool paths



In this preferences page you can enable/disable external applications for configuring different types of NEs from your client, and define local paths for launching these applications.

Select an application group in the Application column to enter a new path for this application. When an application is selected, you can change the path in the Local Path column, either by writing a new path in this cell, or by clicking the Browse button.

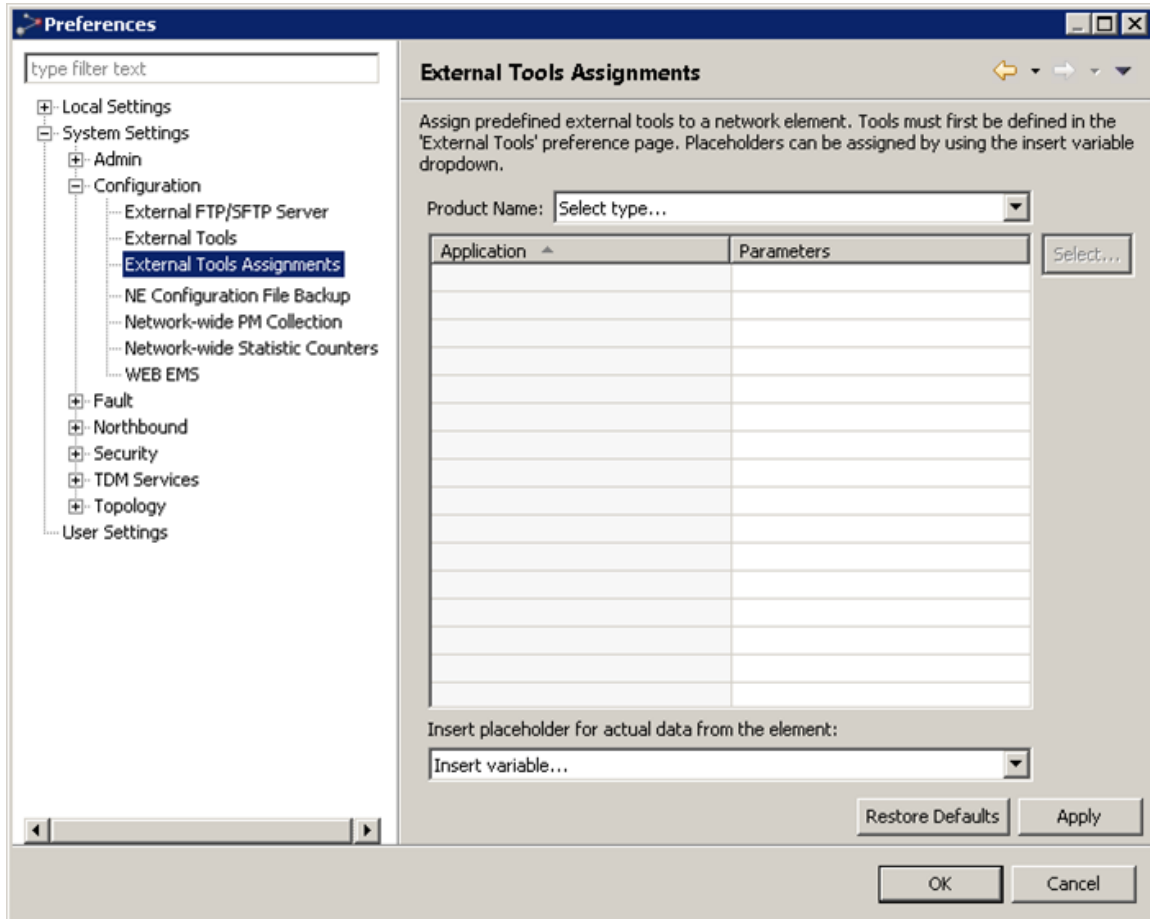
Check/uncheck a checkbox in the Application column to enable/disable the use of this application to configure NEs on your local client.

Only applications that is enabled, can be found in the list of applications in the context menu Configuration | External Tools when selecting NE in the topology views (Geographical or Logical Map or Tree). To appear in the list of external tools for a certain NE, the application also needs to be assigned to this NE's type in the [External Tools Assignment](#) preferences page. The list of applications in the Application column is created and updated in the [External Tools](#) preferences page.

External Tools Assignments

This page can be found under **System Settings > Configuration > External Tools Assignment** in the [Preferences](#) pages.

Figure 215 External tool assignments



In this page you can map application groups to NE types, and define parameters for opening these applications.

Use the NE Type dropdown to select an NE type you want to assign an external tool to. Then click the Select button to add/remove external tools for this NE type.

Insert parameters for opening the application by writing directly in a cell in the Parameters column, or by selecting an application in the table and then using the dropdown Insert placeholder for actual data from the element one or more times.

Application Parameters (place holders)

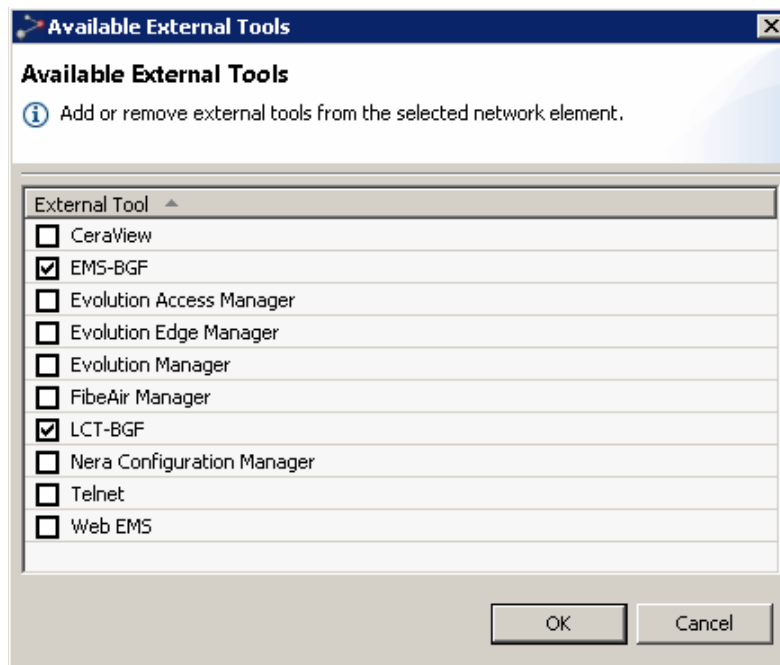
- %IP - The IP address of the NE
- %RC - The SNMP read community string of the NE
- %WC - The SNMP write community string of the NE
- %NN - The name of the NE. Used by FlexMan
- %LOGIN - User name

- %USER_PWD - User Password
- %HTTPS - HTTP or HTTPS

Available External Tools dialog

This dialog is opened whenever clicking the Select button in the [External Tools Assignment](#) preferences page.

Figure 216 Available external tools dialog



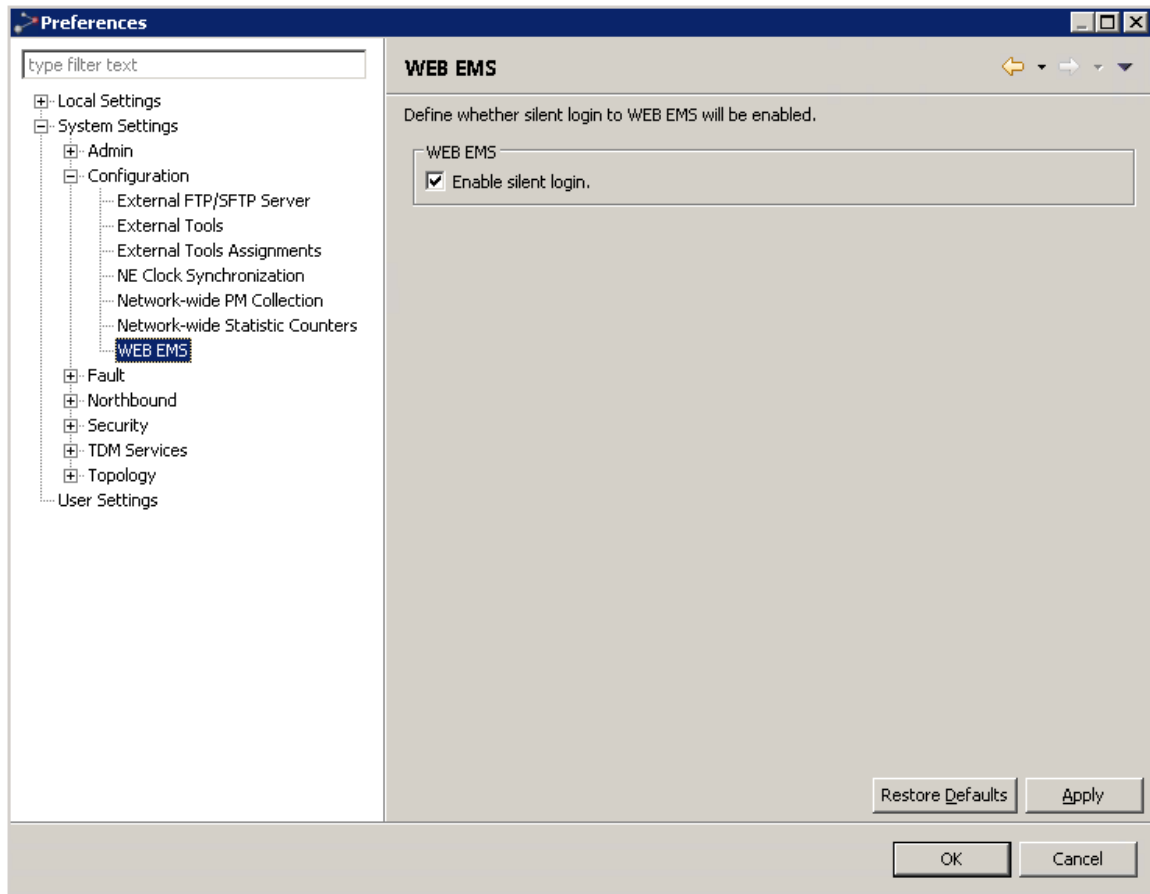
The checked checkboxes in the External Tool column refers to application groups that are enabled for this NE type. Click checkboxes in the table to add/remove external tools.

Description of the available external tools

WEB PTP 820 NMS

This page can be found under **System Settings > Configuration > WEB PTP 820 NMS** in the [Preferences](#) pages.

Figure 217 Web EMS



This page allows you to choose whether to enable silent login to Web EMS. By default, the login is set to silent login.

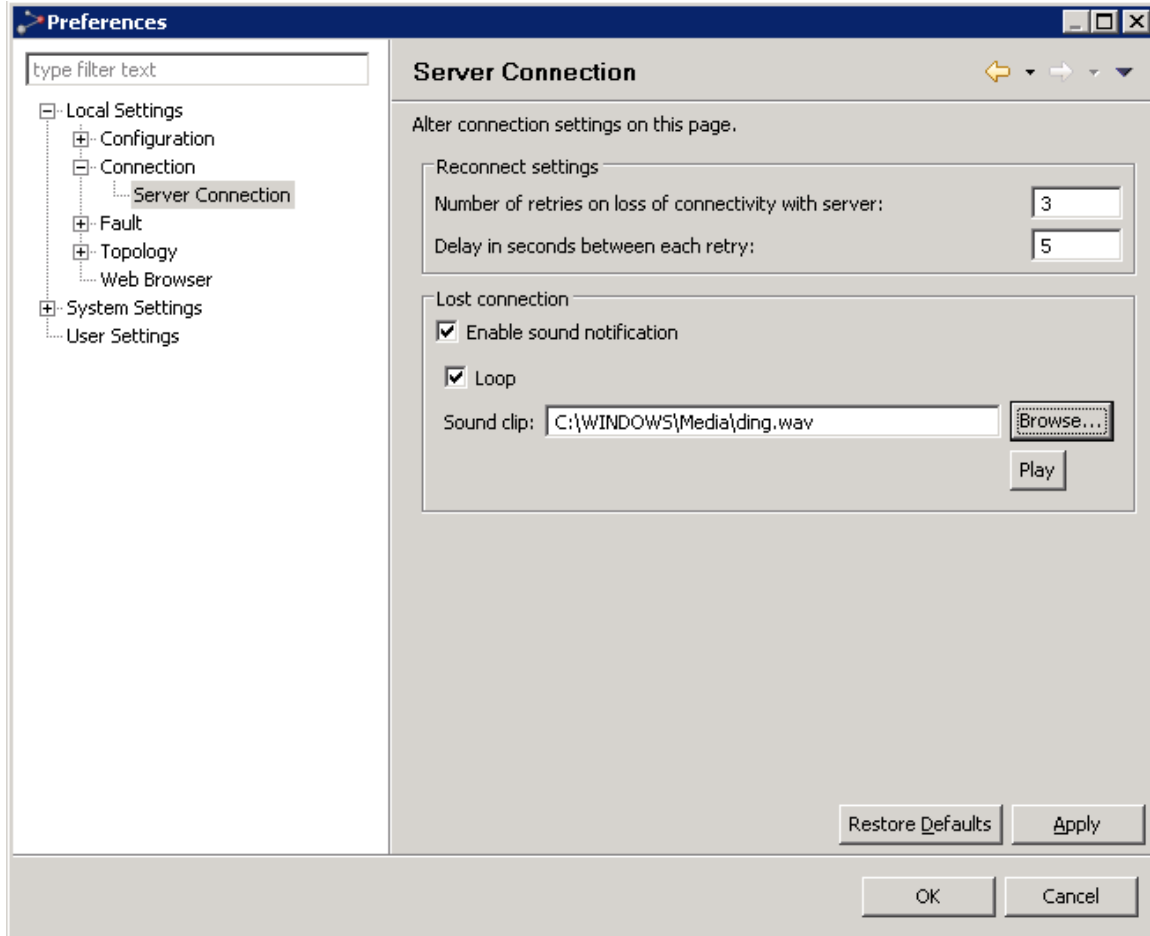
If the checkbox is enabled the web browser opens and the user is not prompted for username and password. If this feature is not enabled the browser will open a page that has two text fields, one for username and one for password.

Note that this feature is only available for devices that already permit silent login (PTP 820 Family).

Preferences: Server Connection

This page can be found under **Local Settings > Connection > Server Connection** on the [Preferences](#) pages.

Figure 218 Preferecnes server connection



In the Server Connection preferences page you can define how your local PTP 820 NMS client should behave when the connection with the PTP 820 NMS server is lost.







In the Reconnect settings area you can define how many times the client should try to reconnect when the connection to server is lost, and how many seconds the server should wait between each try.

In the Lost connection area, select Enable sound notification if you want an audible alert when the connection to the PTP 820 NMS server goes down. The audio will play once all automatic attempts to re-establish the connection have failed. Click Browse... to select a sound from your file system, and Play to listen to the selected sound. Deselect Loop if you do not want the audio playing to loop.

Whenever the connection status changes, this can be seen in the [Connection Status](#) field. If the client has finished retrying as defined in the Reconnect settings area, the [PTP 820 NMS Login](#) dialog will appear with a warning that connection has been lost. An audible notification will be played in case it has been configured on this page.

Connection Status field

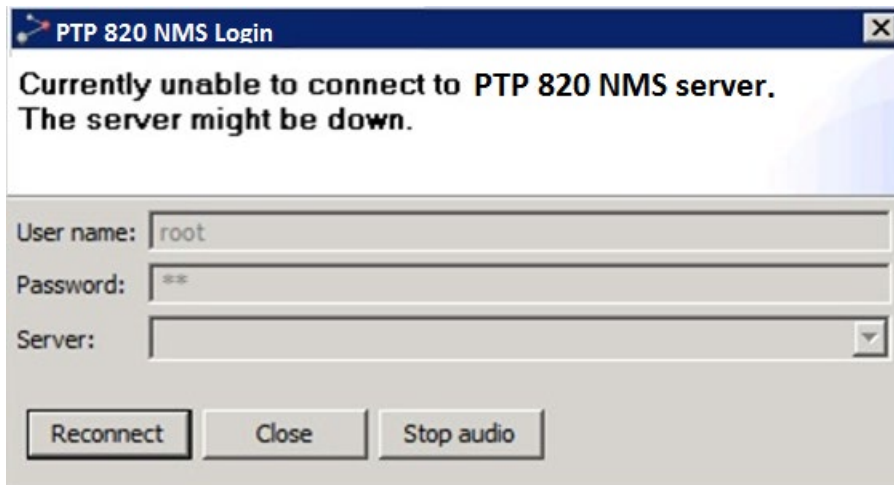
The status of the server connection is displayed in the Connection Status field on the [Status bar](#). The connection status is visualized with graphics and text, and can be one of the following:

-  **Connected: localhost** - the client is currently connected, and the name of the server is displayed.
-  **Connection problems** - the client has detected problems communicating with the server.
-  **Negotiating** - the client is trying to connect to the server, using the current User name and Password.
-  **Waiting for retry 2/3** - the client is unable to connect to the server, and is waiting to retry. The number of failed logins and a number of total tries available is displayed. The total number of tries, and the number of seconds between each negotiation is defined in the Reconnect settings area in the Server Connection preferences page.
-  **Unable to connect** - the client has been unable to reconnect after losing the connection, and the PTP 820 NMS Login dialog has appeared.
-  **Not Connected** - the user has been unable to connect with the PTP 820 NMS Login dialog.

PTP 820 NMS Login dialog - server connection lost

This dialog appears whenever the client has lost the connection, and has finished trying to reconnect as defined in the Server Connection preferences page.

Figure 219 PTP 820 NMS login dialog



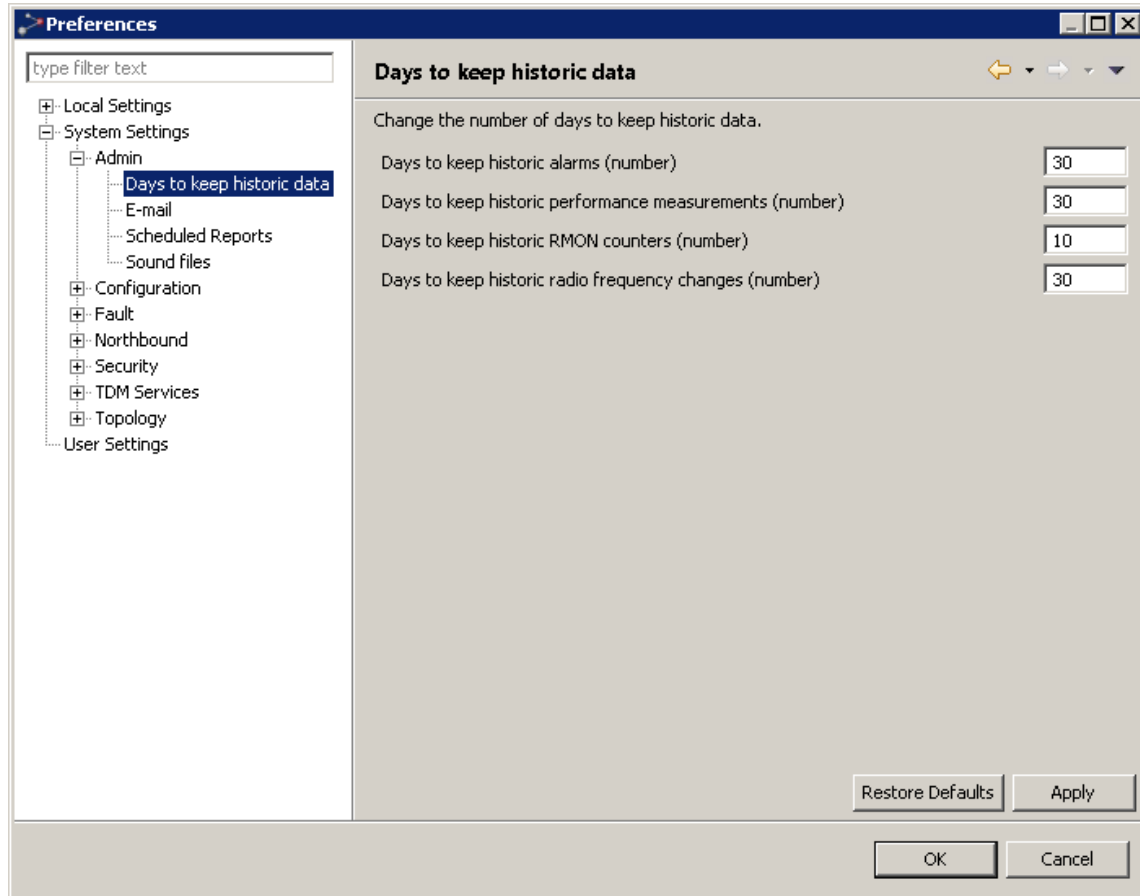
Press Stop audio to stop the [sound that notifies that server connection is lost](#). Press Reconnect to try a new login, or press Close to abort the login process.

The values for User name, Password and Server are the same as for the [PTP 820 NMS Login](#) dialog. Alternatively, update these values, and then try Reconnect.

Preferences: Days to keep historic data

This page can be found under **System Settings > Admin > Days to keep historic data** in the [Preferences](#) pages.

Figure 220 Preferences day to keep historic data



In the Days to keep historic data preferences page it is possible to change the number of days to keep:

- Historic alarms
- Historic performance measurements
- Historic RMON counters
- Historic radio frequency changes

In the Days to keep historic alarms (number) field it is possible to define how many days to keep historic alarms in the database. Valid values are 1 day or more and there are no upper limit.

The default setting after installing or upgrading PTP 820 NMS will be 30 days.

In the Days to keep historic performance measurements (number) field it is possible to define how many days to keep historic performance measurements in the database. Valid values are 1 day or more and there is no upper limit.

The default setting after installing or upgrading PTP 820 NMS will be 30 days.

In the Days to keep historic RMON counters (number) field it is possible to define how many days to keep historic RMON counters data in the database. Valid values are between 1 - 100 days.

The default setting after installing or upgrading PTP 820 NMS will be 10 days.

Deletion criteria for historic data

When PTP 820 NMS server starts it will schedule a task that will execute at 00:44 every night to delete historic data.

All cleared alarms that have raised time older than the value in the number of days to keep historic alarms (number) field will be deleted.

All performance measurements older than the value in the number of days to keep historic performance measurements (number) field will be deleted.

Audit Log

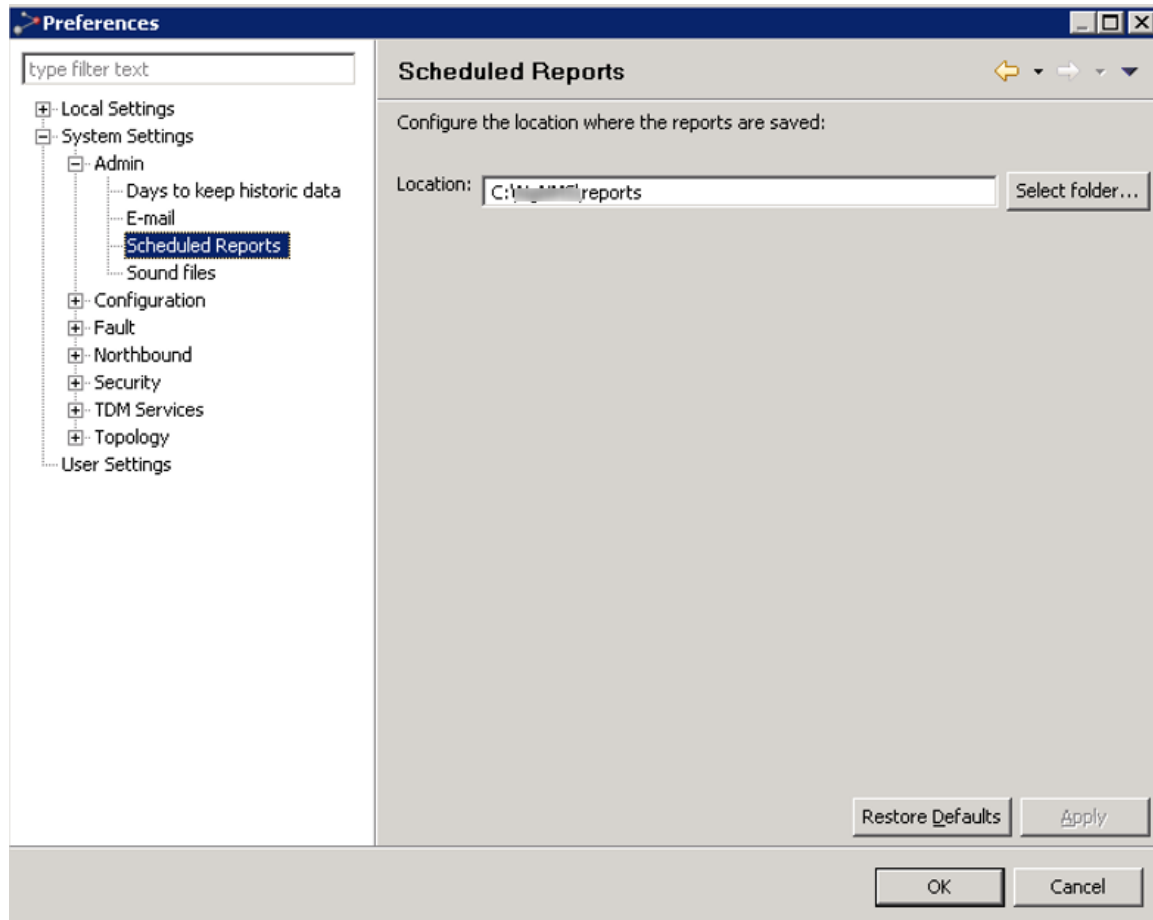
When historic data has been deleted, an [audit log](#) entry will be created which states the number of entries deleted for:

- Historic alarms
- Historic performance measurements

Audit log entries will be made also when no historic data has been deleted.

Preferences: Scheduled Reports

This page can be found under **System Settings > Admin > Scheduled Reports** in the [Preferences](#) pages.



In the Scheduled Reports preferences page, it is possible to configure the location where reports are saved.

Preferences: Alarm Notifications - E-mail and Sound files

In these preferences pages you can view and update some general definitions for [alarm notifications](#). Changes in these definitions can update the collection of sound files used for [audible notifications](#), and can configure mail server used for [e-mail notifications](#).

Configurations for alarm notifications are done on several preference pages:

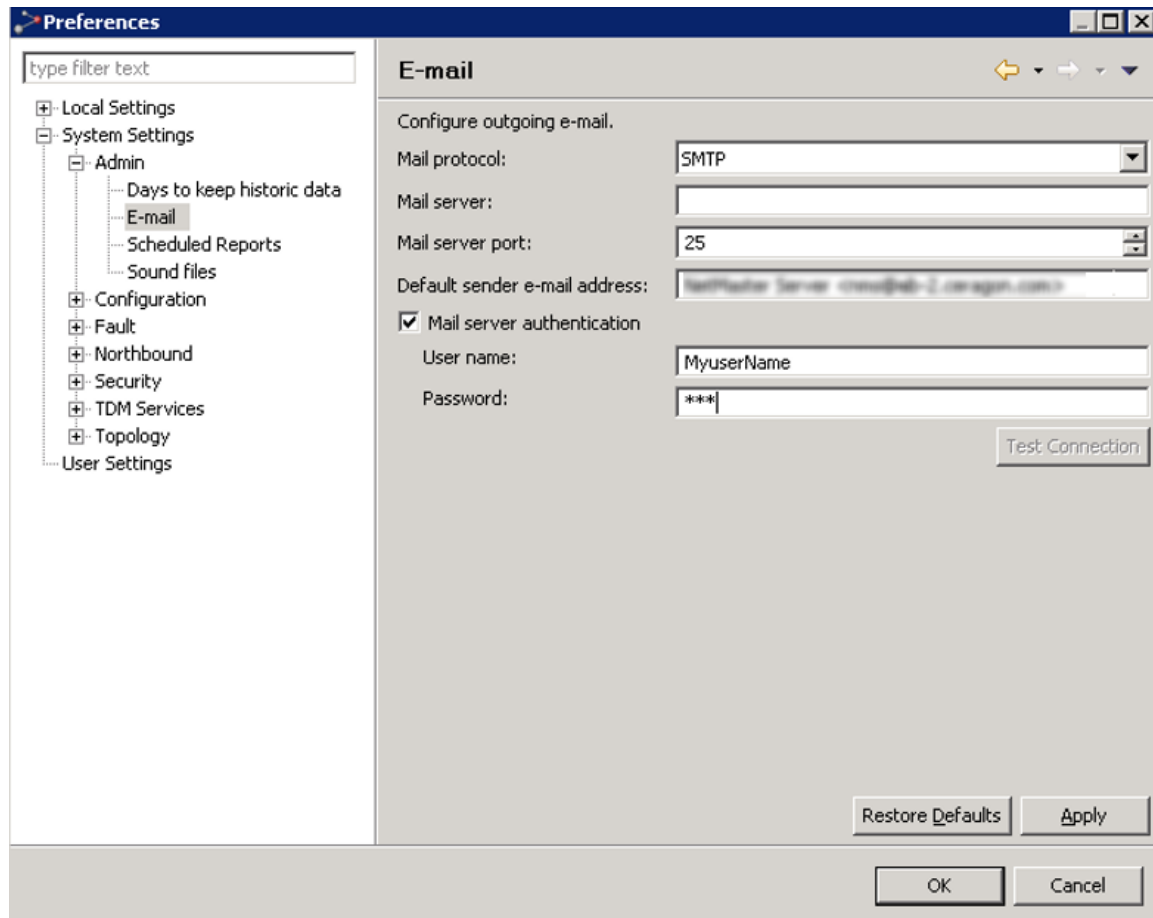
- The mail server can be configured on the [E-mail preference page](#)
- The collection of sound files on the PTP 820 NMS server can be updated in the [Sound files preference page](#)

Please note that e-mail and sounds also can be configured directly in the Alarm Notifications view.

E-mail

This page can be found under **System Settings > Admin > E-mail** in the [Preferences](#) pages.

Figure 221 Preferences – email notification



On this page, you can configure an SMTP server to use for outgoing e-mails. These settings are important for the e-mail notification feature to function.

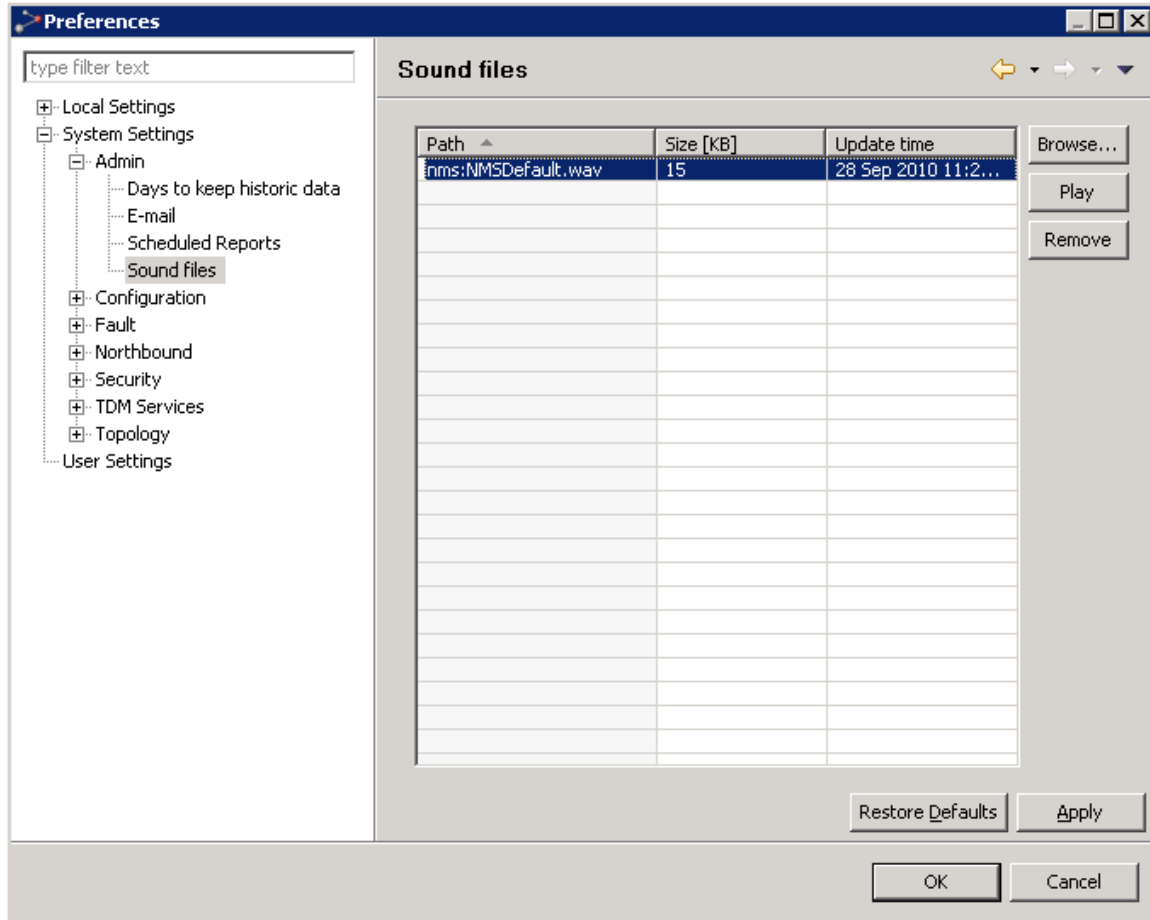
Enter the hostname or IP address of the SMTP server in the Mail server field. Enter the SMTP server port in the field Mail server port. In the Default sender e-mail address field, you can specify the e-mail address to be used for the sender field of outgoing e-mails. If the SMTP server requires authentication, you must enable Mail server authentication and enter the credential data in fields User name and Password.

To test the server connectivity, press Test Connection and wait for a dialog to pop up and declare whether the test was successful or not.

Sound files

This page can be found under **System Settings > Admin > Sound** files in the [Preferences](#) pages.

Figure 222 Preferences – sound files



This page lists all sound files that are uploaded to the PTP 820 NMS server.

To upload a new file, you first press **Browse...** and select the local file to upload. You can then press **Play** to listen to this audio file, or **Remove** to remove it. Added files will not be physically uploaded until you apply your changes.

To listen to an already uploaded file, select the file in the table and press Play.

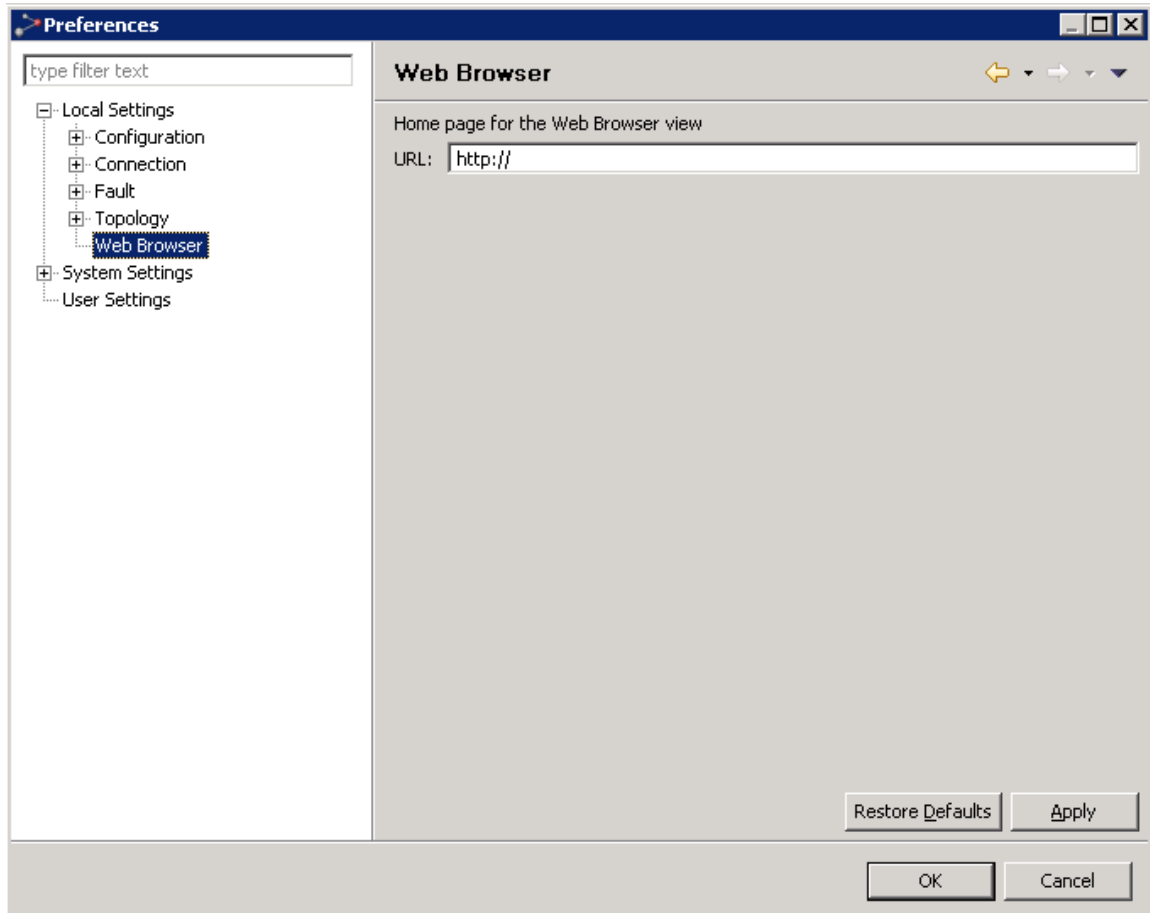
To remove an already uploaded file from the server, select the files that you want to remove and press Remove. The files will not be physically removed until you apply your changes. Please note that neither the default PTP 820 NMS file PTP 820 NMSDefault.wav nor files that are in use can be deleted.

Max file size for a sound is 2Mb. The server can maximum contain 35 sound files in total, including the default PTP 820 NMS file.

Preferences: Web Browser

This page can be found under **Local Settings > Web Browser** in the Preference pages.

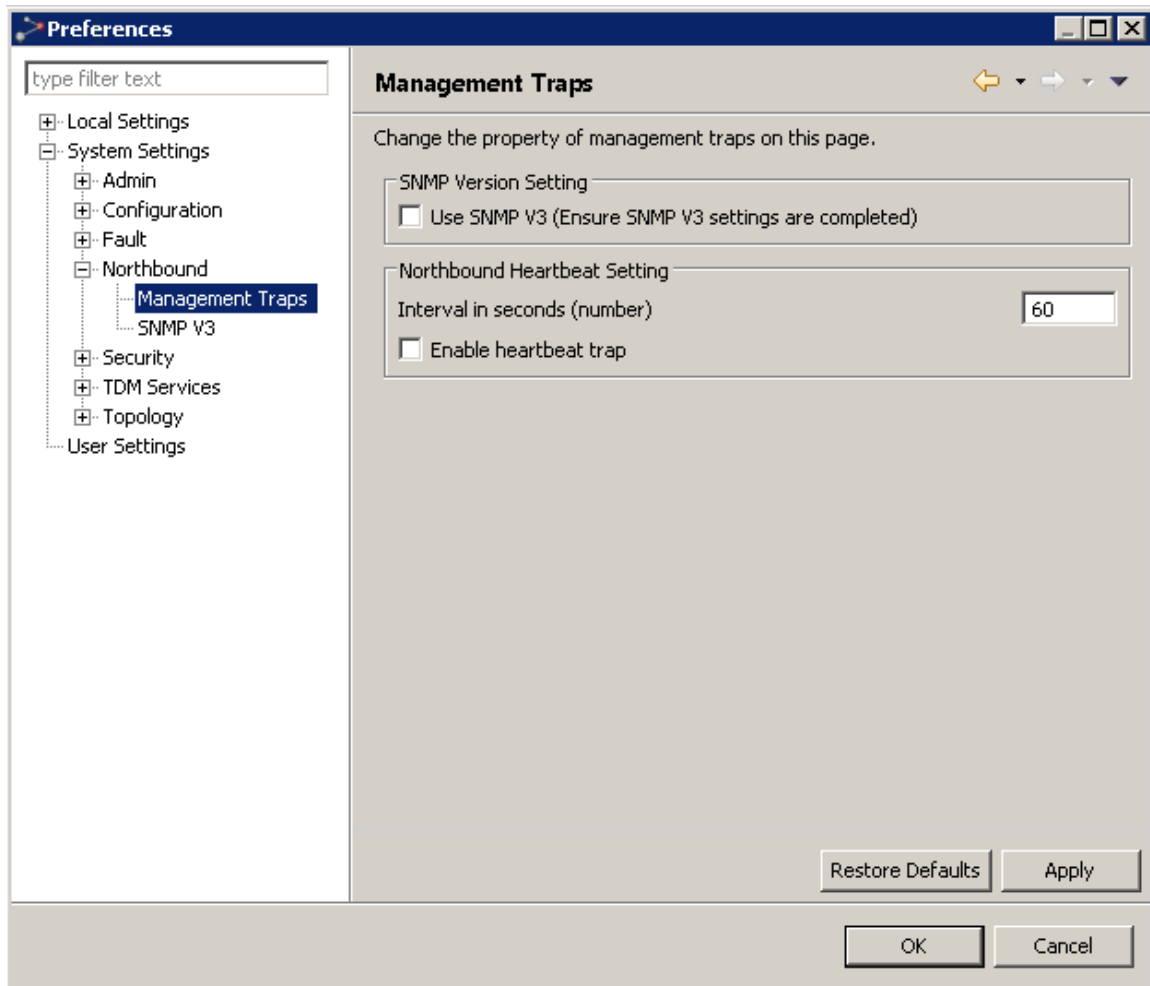
Figure 223 Preferences web browser



In the Web Browser preferences page you can define the default URL that will be used by the [Web Browser view](#).

Preferences: PTP 820 NMS Management Traps

This page can be found under **System Settings > Northbound > Management Traps** in the **Preferences** pages.



SNMP Version Setting

You can specify to enable trap forwarding using SNMP V3 by checking the Use SNMP V3 (Ensure SNMP V3 settings are completed) checkbox. If you enable this option, enter the SNMP V3 settings in the [SNMP V3](#) Preferences page.

The trap sent from the PTP 820 NMS SNMP agent consists of the following fields:

- sysUpTime
- snmpTrapOID (PTP 820 NMS HeartBeatTrap)

PTP 820 NMS is also capable of sending a trap in case of connection loss between PTP 820 NMS and the HLMS.

This trap is sent only once, and is not affected by the **PTP 820 NMS Heartbeat** feature.

This trap consists of the following fields:

- sysUpTime
- snmpTrapOID (PTP 820 NMS ShutdownTrap)

Northbound Heartbeat Setting

Northbound Heartbeat is a feature that enables PTP 820 NMS to send traps to all configured [High Level Managers](#) stating that everything is OK.

In the **Interval in seconds (number)** field you can define how often this trap is sent from PTP 820 NMS to the HLMs.

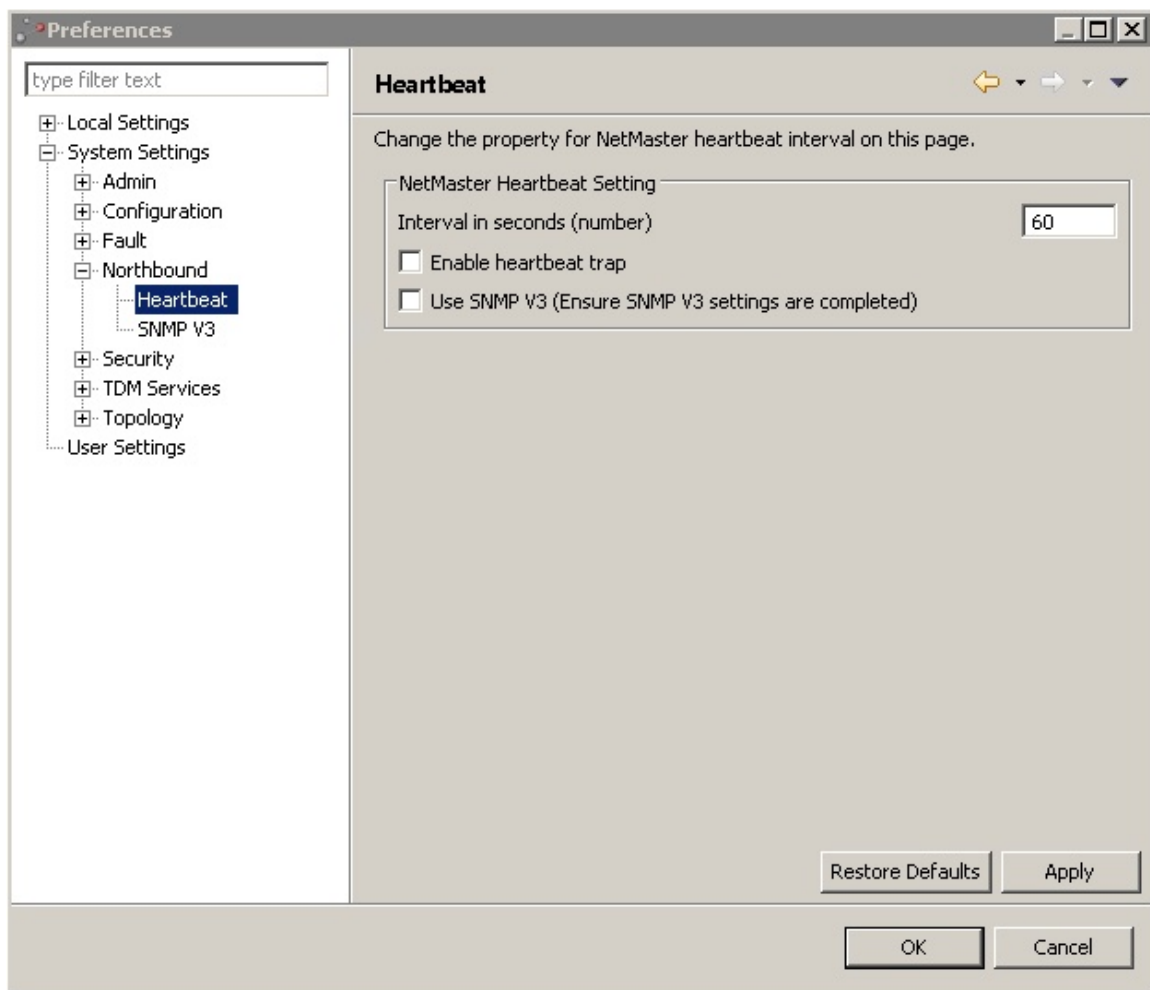
The default value is set to 60 seconds.

The trap can be enabled by checking the **Enable heartbeat trap** checkbox.

For more detailed information on the Northbound SNMP features in PTP 820 NMS, consult the SNMP Agent Guide supplied on the PTP 820 NMS installation media.

This page can be found under **System Settings > Northbound > EMS Heartbeat** in the [Preferences](#) pages.

Figure 224 Preferences EMS heartbeat



EMS Heartbeat is a feature that enables EMS to send traps to all configured [High Level Managers](#) stating that everything is OK.

In the Interval in seconds (number) field you can define how often this trap is sent from EMS to the HLMs.

The default value is set to 60 seconds.

You can specify to enable trap forwarding using SNMP V3 by checking the Use SNMP V3 (Ensure SNMP V3 settings are completed) checkbox. If you enable this option, enter the SNMP V3 settings in the [SNMP V3](#) Preferences page.

The trap can be enabled by checking the Enable heartbeat trap checkbox.

The trap sent from EMS SNMP agent consists of the following fields:

- sysUpTime
- snmpTrapOID (PTP820NMSHeartBeatTrap)

EMS is also capable of sending a trap in case of connection loss between EMS the HLMS.

This trap is sent only once, and is not affected by the EMS Heartbeat feature.

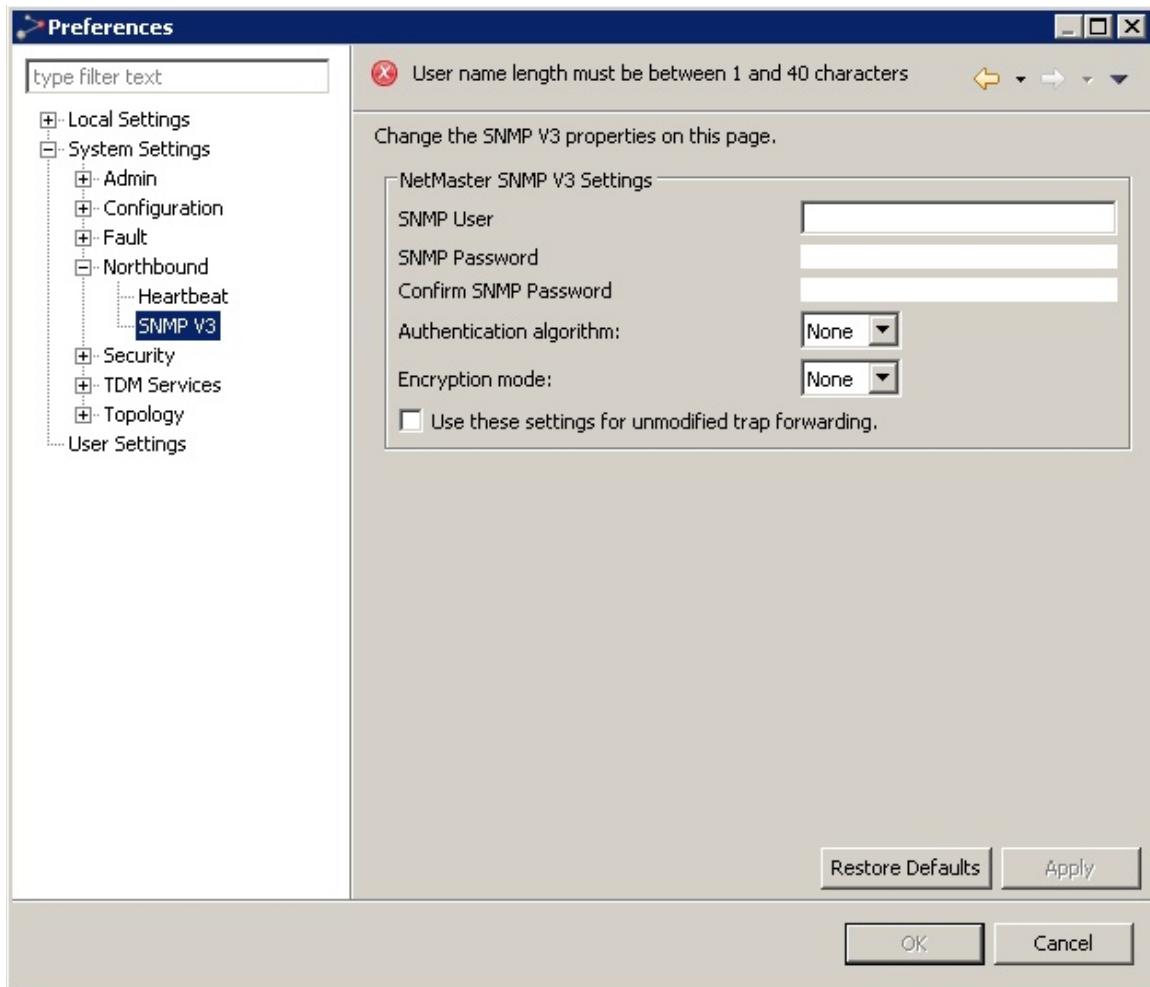
This trap consists of the following fields:

- sysUpTime
- snmpTrapOID (PTP820NMSShutdownTrap)

For more detailed information on the Northbound SNMP features in EMS, consult the SNMP Agent Guide supplied on the EMS installation media.

Preferences: SNMP V3

This page can be found under **System Settings > Northbound > SNMP V3** in the [Preferences](#) pages.

Figure 225 Preferences SNMP V3

You must set the following PTP 820 NMS SNMP V3 properties if you enabled trap forwarding using SNMP V3 by checking the Use SNMP V3 (Ensure SNMP V3 settings are completed) checkbox in the [Error! Reference source not found.](#) page.

- Enter a user name and password for the SNMP user.
- Specify an Authentication algorithm: None, SHA, or MD5.
- Specify an Encryption mode: None, AES, DES.
- Check the Use these settings for unmodified trap forwarding checkbox to use these settings for unmodified trap forwarding to a High Level Manager (see [Northbound SNMP Settings View](#) for details).

Preferences: Password Settings

This page can be found under System Settings | Security | Password in the [Preferences](#) pages.

Figure 226 Preferences password settings

The screenshot shows the 'Preferences' dialog box with the 'Password' settings page selected. The left pane shows a tree view with 'Password' selected under 'Security'. The right pane contains the following settings:

- Password Settings**
 - Minimum number of uppercase characters in passwords: 1
 - Minimum number of numeric characters in passwords: 1
 - Minimum number of special characters in passwords: 1
 - ☐ Allow white spaces in passwords
 - Minimum password length (number): 3
 - Maximum password length (number): 9
 - Maximum failed login attempts (number) (0 - Unlimited attempts): 5
 - ☒ Enforce a password change upon first login
- Password Expiration**
 - Maximum number of days the password shall be valid (0 - Never expires): 90
 - Number of days to display expiration warnings (0 - No warnings): 12
- Password History**
 - Disallow previously used passwords (0 - No restriction): 12

Buttons at the bottom: Restore Defaults, Apply, OK, Cancel.

In the Password preferences page you can define rules for password definition for all [users](#) on this server:



Note: The password rules in this page do not apply when [RADIUS authentication](#) is enabled. Password policy in such a case is handled by the RADIUS server.

The only password rules that apply to a root user's password are password length, and the characters that the password can or must include.

Password Settings:

- **Minimum number of upper case characters in passwords** – The number must be between 1 and 30. The default is 1.
- **Minimum number of numeric characters in passwords** – The number must be between 1 and 30. The default is 1.
- **Minimum number of special characters in passwords** – The number must be between 1 and 30. The default is 1.
- **Allow white spaces in passwords** – The default is to deny the use of white spaces (option unchecked)
- **Minimum password length (number)** – The number must be between 1 and 50. The default is 8.
- **Maximum password length (number)** – The number must be between 1 and 100. The default is 12.

- **Maximum failed login attempts (number)** – The number must be between 0 and 20. The default is 5. Zero means that unlimited wrong attempts may be used without locking out the user. If the number is non-zero, then exceeding the specified number causes the user to be locked out and prevented from logging in until the user is unlocked in the [User Administration](#) view.
- **Enforce a password change upon first login** – The default is to enforce (option checked), requiring the user to change the password upon first login. Note that this does not apply to a root user.

Password Expiration:

- **Maximum number of days the password shall be valid** – The number must be between 0 and 1000. The default is 90. Zero means that the password will never expire.
- **Number of days to display expiration warnings** – The number must be between 0 and 30. The default is 12. Zero means no warnings are displayed.

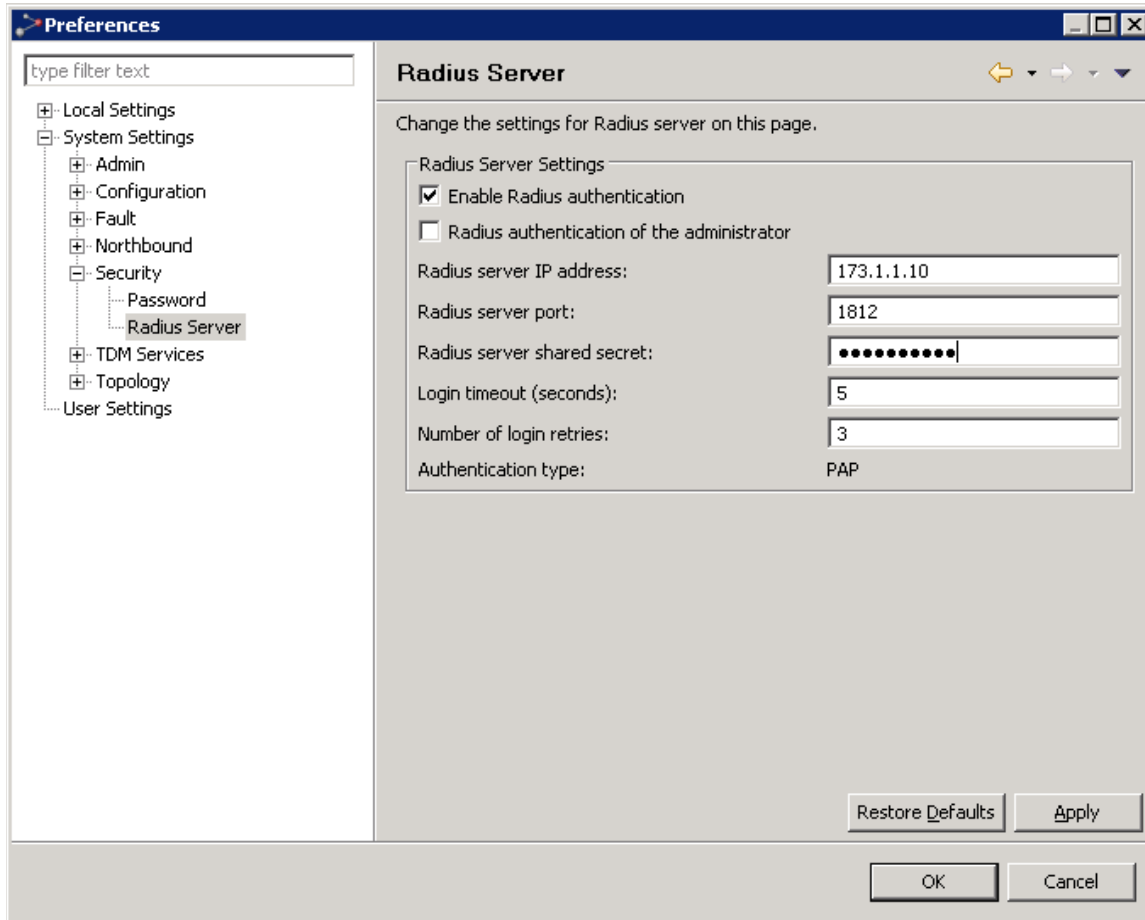
Password History:

- **Disallow previously used passwords** – The number must be between 0 and 20. The default is 12. Zero means that any previous password can be re-used.

Whenever a user tries to enter a new password, only passwords that follow the above rules will be accepted.

Preferences: RADIUS Server

This page can be found under **System Settings > Security > RADIUS Server** in the [Preferences](#) pages.

Figure 227 Preferences Radius server

In the RADIUS Server preferences page you can create and modify RADIUS server settings for all [users](#) on this server:

Modify the following fields:

- **Enable RADIUS authentication** - Check to enable RADIUS authentication. If left unchecked no other fields will be available.
- **RADIUS Authentication of the administrator** - When checked, EMS will also enable RADIUS authentication for the administrator.
- **RADIUS server IP address** - Enter the valid IP address for the RADIUS server. An error message informs you if the address you are entering is invalid.
- **RADIUS server port** - Enter the port number being used for the RADIUS server. The default port is UDP 1812. An error message informs you if the port number you are entering is outside the valid range.
- **RADIUS server shared secret** - Enter the pre-determined shared secret, a string of between 1 and 128 characters.
- **Login timeout (seconds)** - Enter the number of seconds the server will wait for a user to login before timing out. The timeout must be between 3 and 30 seconds.

- **Number of Login retries** - Enter the number of times you want to allow a user to try to enter his/her login information before barring the user. The number of retries must be between 1 and 10.

Click one or more of the following, as applicable:

- **Apply** - applies modifications, leaves window open.
- **Restore Defaults** - reverts to application preset defaults.
- **OK** - applies changes and closes window.
- **Cancel** - closes window without applying changes.

Working with a RADIUS Server

When PTP 820 NMS works with RADIUS, the usernames and passwords should be configured only on the RADIUS server, and not configured in PTP 820 NMS. However, the groups to which these users are assigned on the RADIUS server should exist with certain privileges in PTP 820 NMS as well.

For example:

On the RADIUS Server: User1 (with password “user1”) is assigned to Group1. The Radius Client policy should allow this group to have access.

In PTP 820 NMS: In the User Management Perspective, only Group1 should be created and privileges should be assigned to it.

When User1 tries to log into PTP 820 NMS, PTP 820 NMS contacts the RADIUS Server and checks whether the group existing in its User Management Perspective exists also on the RADIUS Server.

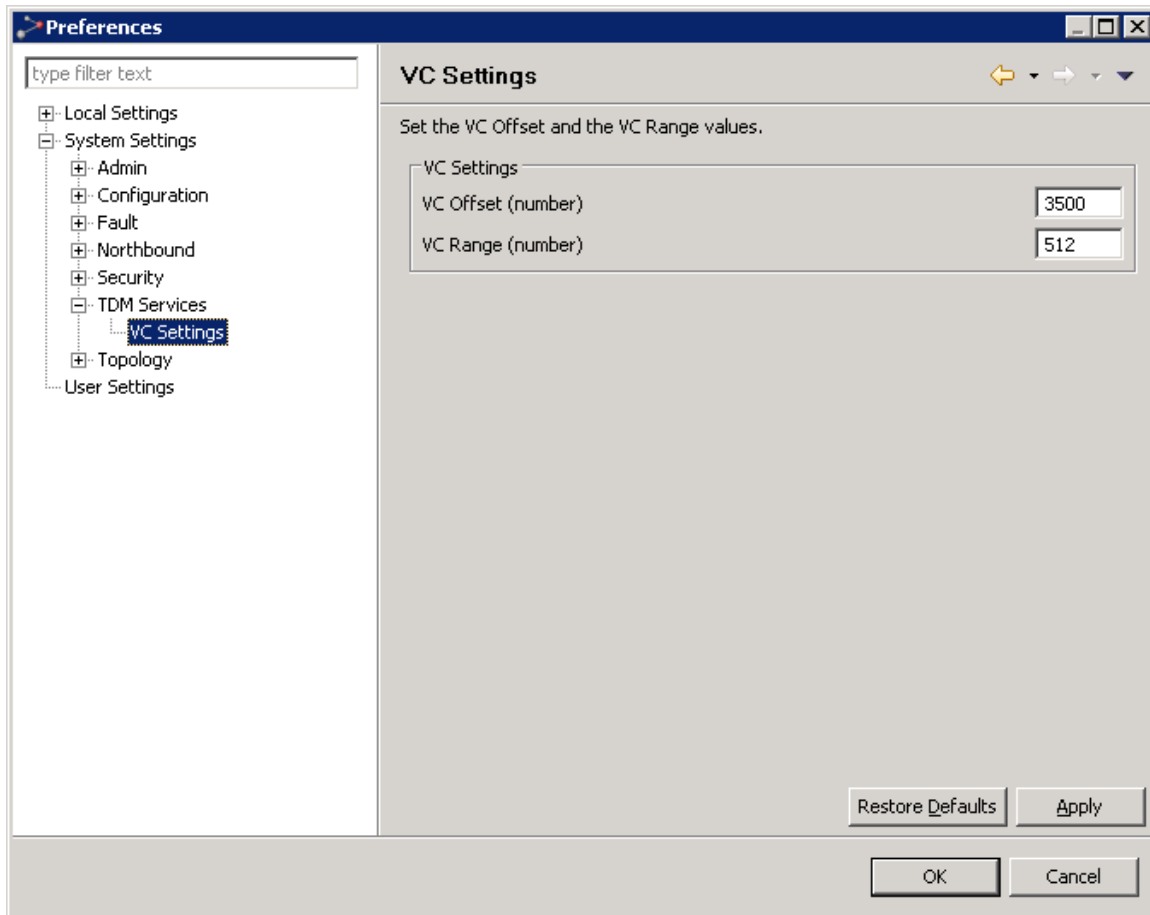
Because the group exists and the policy allows group members to connect, and because User1 is in the group, User1 is allowed to log into PTP 820 NMS with the privileges that were assigned to Group1. After the first log in, the user User1 will also be automatically added in PTP 820 NMS, and assigned to Group1. (Note that PTP 820 NMS will continue contacting the RADIUS server and checking whether the user and the group are allowed, every time the user logs in.)

RADIUS and Northbound Interface

Please note that when RADIUS authentication is Enabled, the Northbound Interface user will also be authenticated via the RADIUS server, therefore a Northbound Interface user group must be defined in the RADIUS server.

Preferences: TDM Services VC Settings

This page can be found under **System Settings > TDM Services > VC** in the [Preferences](#) pages.

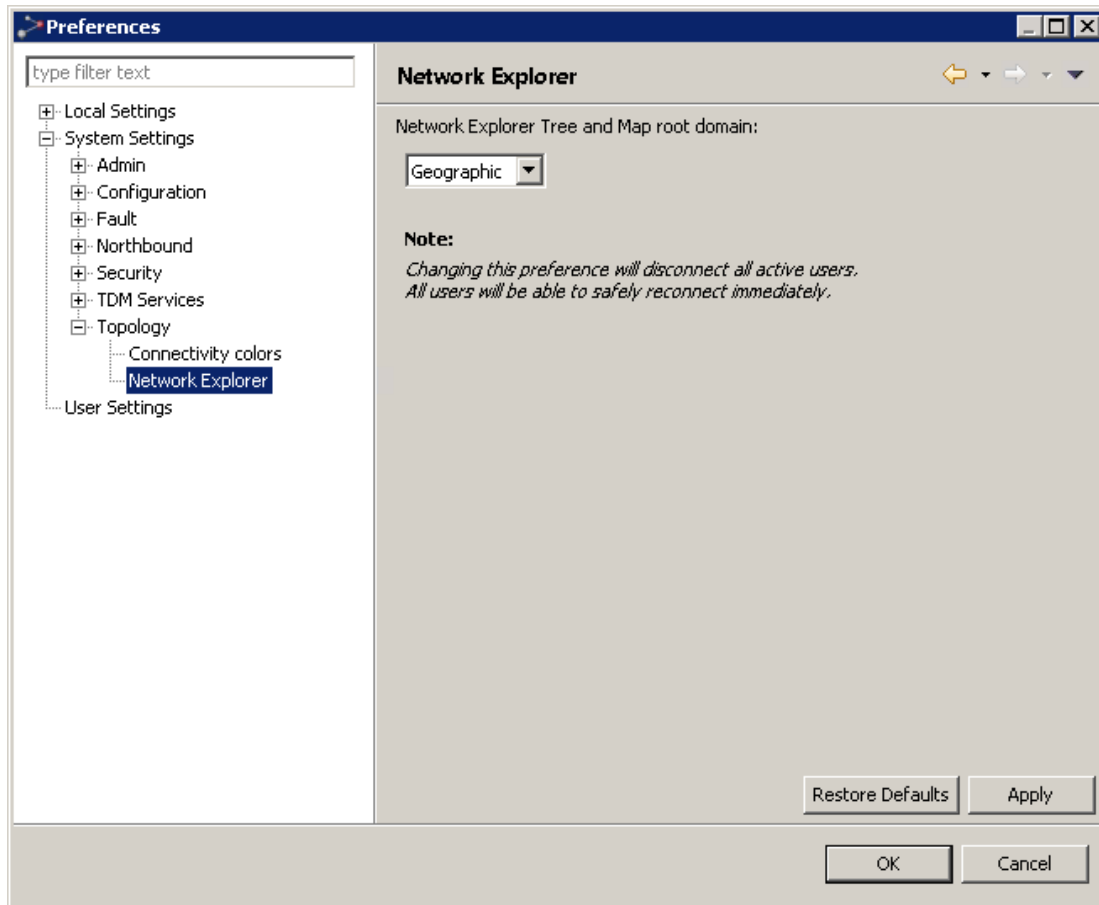
Figure 228 Preferences user settings

In the VC Settings preferences page, users can set the Virtual Channel offset and range values for TDM services.

- VC Offset can range from 0 to 4093. The default value is 3500.
- VC Range can range from 1 to x; where x is the minimum of the following two values:
 - 512
 - $4094 - \text{"VC Offset"}$

Preferences: Network Explorer

This page can be found under **System Settings > Topology** in the **Preferences** pages.



In this page, specify which resource model to link to the [Network Explorer](#) perspective: the [Geographical Surveillance](#) perspective or the [Logical Surveillance](#) perspective. This determines which resource model the Network Explorer perspective displays and with which resource model it is synchronized. Any change in the Network Explorer perspective is automatically reflected in the perspective to which it is linked, and vice versa.

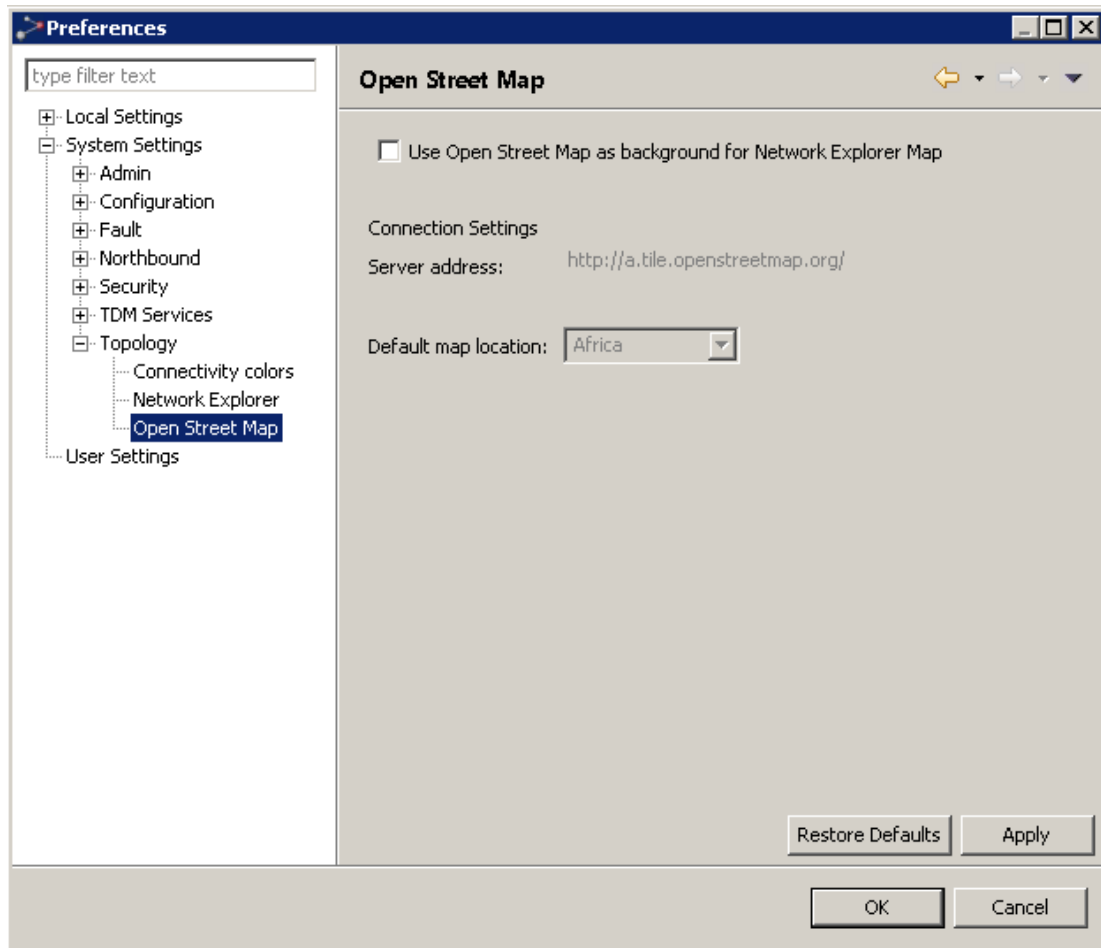


Note: Changing this preference disconnects all users. They will be able to reconnect immediately.

This preference determines which resource model appears in the [Network Explorer](#) perspective for all users from now on. We therefore recommend choosing the resource model once, and abiding by that choice.

Preferences: Open Street Map

This page can be found under **System Settings > Topology > Open Street Map** in the **Preferences** pages.



In the **Open Street Map** preferences page you can enable setting an Open Street Map as the background for a domain in [Network Explorer Map](#).

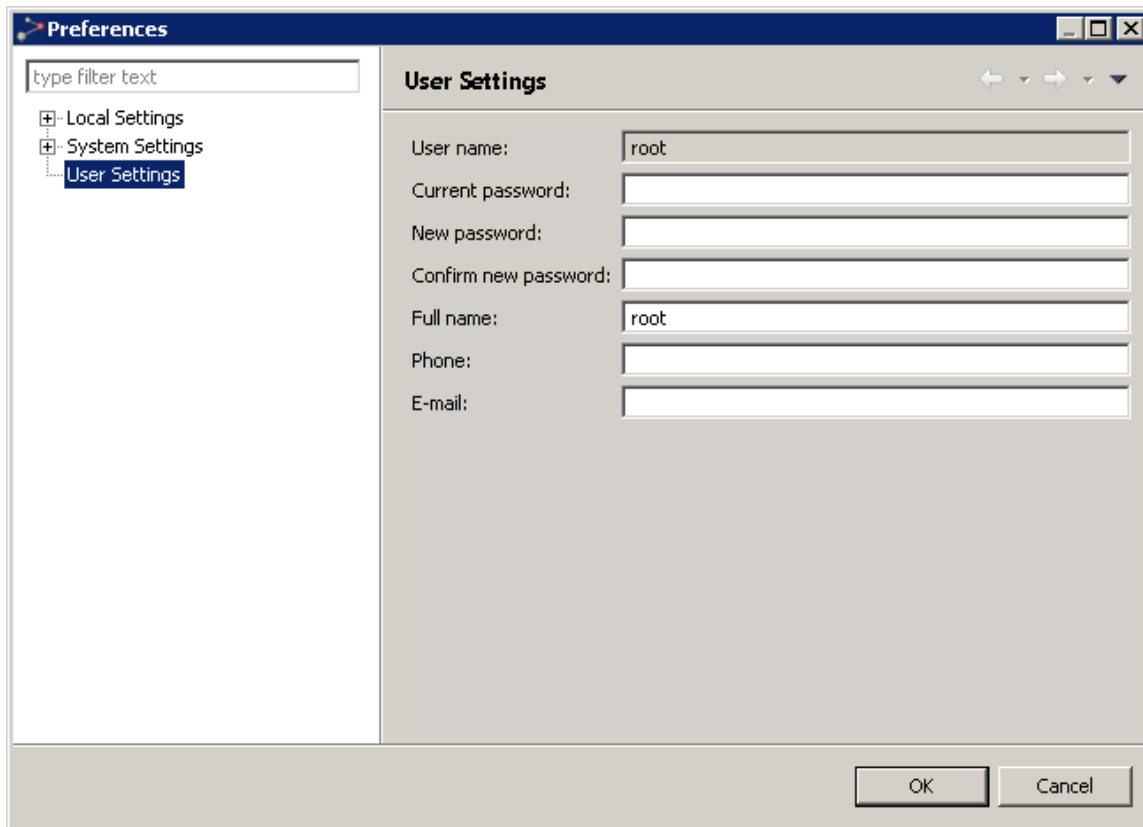
If you check the **Use Open Street Map as background for Network Explorer Map** checkbox, you can set the following two options:

- In **Server address**, you can specify an Open Street Map server. You can enter any of the following:
 - <http://a.tile.openstreetmap.org/>
 - <http://b.tile.openstreetmap.org/>
 - <http://c.tile.openstreetmap.org/>
 - <http://a.tile.stamen.com/toner/>
 - <http://tiles.wmflabs.org/bw-mapnik/>
 - <http://tiles.wmflabs.org/osm-no-labels/>
- In **Default map location**, you can select which region to display by default when Open Street Map view is selected.

To save changes, click **Apply** and then click **OK**.

Preferences: User Settings

This page can be found under **System Settings > User Settings** in the **Preferences** pages.



The screenshot shows the 'User Settings' window within the 'Preferences' application. The window has a title bar with standard OS controls. On the left is a sidebar with a search box labeled 'type filter text' and a tree view containing 'Local Settings', 'System Settings', and 'User Settings' (which is selected and highlighted). The main area is titled 'User Settings' and contains several form fields: 'User name:' with the value 'root', 'Current password:', 'New password:', 'Confirm new password:', 'Full name:' with the value 'root', 'Phone:', and 'E-mail:'. At the bottom right are 'OK' and 'Cancel' buttons.

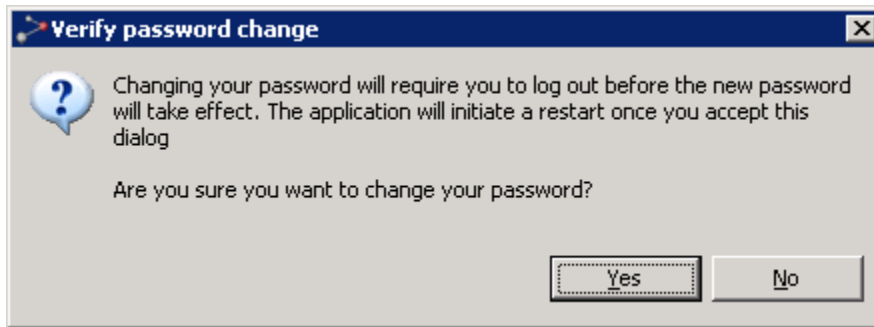
In the **User Settings** preferences page all users can update their own user details. The following values can be updated:

- Password
- Full name
- Phone
- E-mail

Users with [permissions](#) for **User account management** enabled can also update user details for other users with the [User Administration](#) view.

Verify Password Change dialog

This dialog is opened whenever entering a new password in the User Settings preference page.

Figure 229 Verify password change dialog

Press Yes to apply the password change. You will now log off the EMS client application, and the [PTP 820 NMS Login](#) dialog appears.

Alternatively press No to abort the password change. All changes in the User Settings preference page except the new password is now saved.




System Tray Monitors

EMS Server monitor

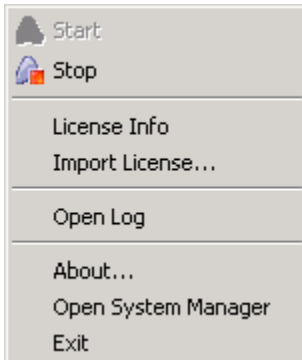
Please note that this GUI only is available in the Windows version. On Solaris platform the similar functions can be handled in [EMS System Manager](#).

The EMS Server monitor is located in the Windows taskbar system tray.

The server monitor has three different states:

-  Server is running
-  Server is stopped.
-  Info: Server is starting or stopping.

Right-clicking the server monitor icon displays the following menu:

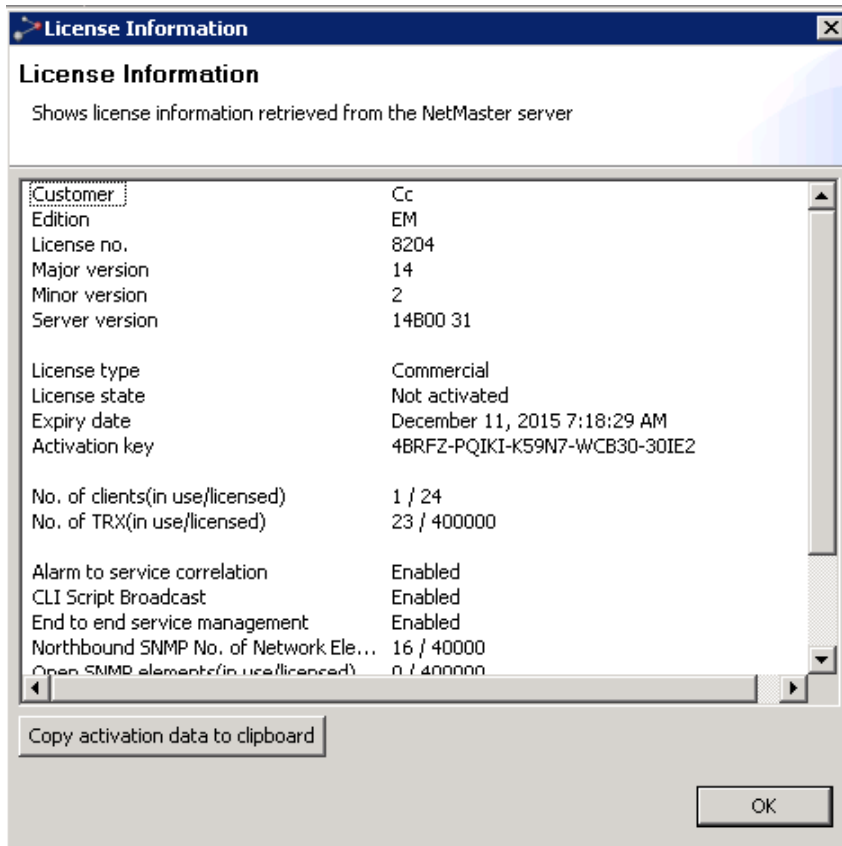


The menu options Start and Stop are used to start or stop the EMS Server.

Only a user defined as an Administrator can start or stop the PTP 820 NMS Server through the server monitor.

License Info dialog

This dialog is opened when selecting the License Info menu option.

Figure 230 License information

Press the Copy activation key to clipboard in order to paste the Activation key to another application (e-mail etc.).

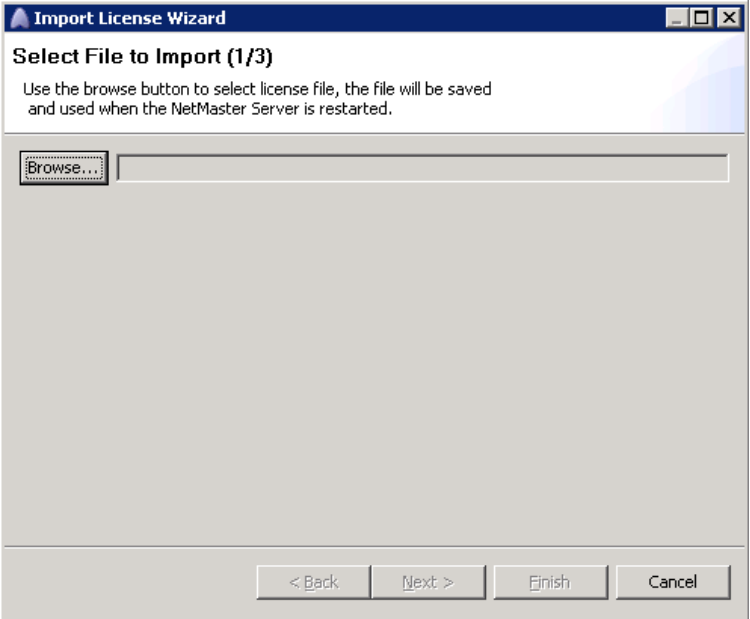
The Activation key in the License Info dialogue is generated from the MAC-address of one of the enabled network cards on the EMS server. In order to be absolutely certain of which network card the license is bound to it is recommended to disable all network cards except one. When the License is activated with this Activation key, the license will be locked to this network card. If the network card later is disabled the EMS server will stop with a "violation lock" error message.

Import License Wizard

The Import License Wizard is started when selecting the Import License menu option.

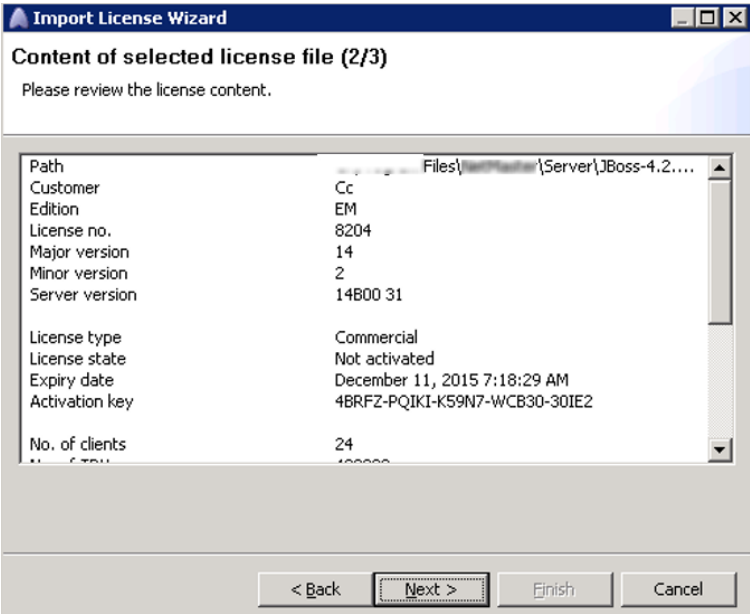
Step 1:

Figure 231 Import license wizard - 1/3



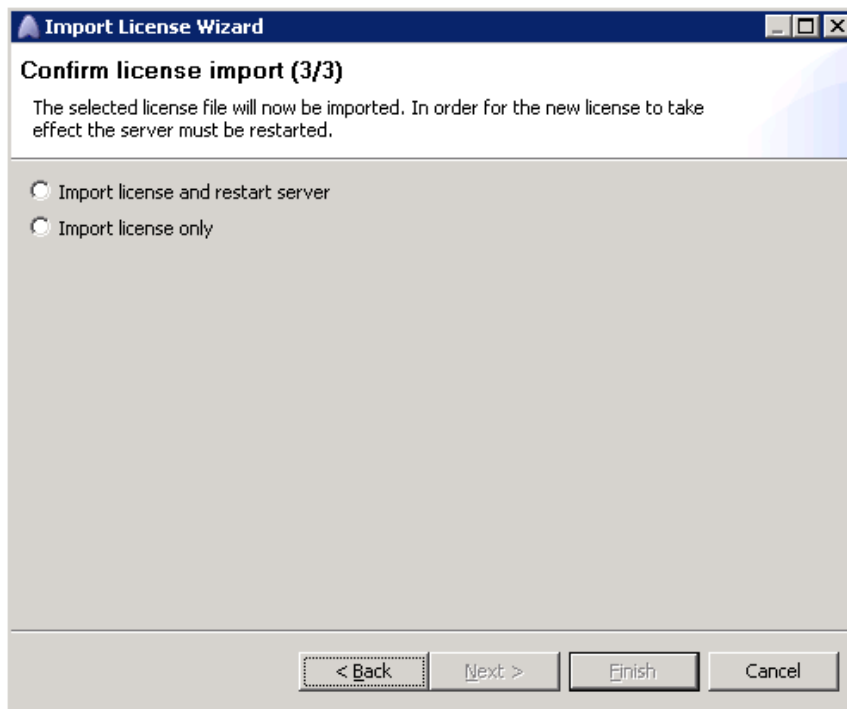
Step 2:

Figure 232 Import license wizard - 2/3



Step 3:

Figure 233 Import license wizard - 3/3



Importing license on a PC without network connection

Please note that importing a license will fail if the server does not have any network connection available. The import license dialog does not complete.

However, if you would like to install EMS for demonstration purposes on a laptop without network connections, it is possible to use the loopback adapter.

Installation of loopback adapter:

1. Open Control Panel.
2. Start the wizard for Add Hardware, and then click Next.
3. Select Yes, I have already connected the hardware, and then click Next.
4. At the bottom of the list, select Add a new hardware device, and then click Next.
5. Select Install the hardware that I manually select from a list, and then click Next.
6. Select Network adapters, and then click Next.
7. In the Manufacturer list, select Microsoft.
8. In the Network Adapter list, select Microsoft Loopback Adapter, and then click Next.
9. Complete installing loopback adapter by finishing the wizard.

Enable/Disable loopback adapter:

1. Open Network Connections.
2. Right-click the loopback adapter (Device Name = "Loopback Adapter") connection and select Enable/Disable.

The evaluation license will then be associated with the loopback adapter.

Please note: Do not use the activation key for the loopback adapter. Make sure that you have a network connection if you want to activate the license.

About dialog

This dialog is opened when selecting the About menu option. The dialog contains EMS version and database details.

PTP 820 NMS SNMP Agent monitor



Note

Please note that this GUI only is available in the Windows version. On Solaris platform the similar functions must be handled by editing logininfo.properties and by starting, stopping and reading service status for nifservice, as described in [how to configure Northbound Interface SNMP](#).

The PTP 820 NMS SNMP Agent Service monitor is located in the Windows taskbar system tray.

The EMS SNMP Agent Service is installed as a Windows service. The SNMP Agent Service monitor application monitors and configures the SNMP Agent.

The monitor application displays an icon on the taskbar indicating the current service state:

- Service is running.
- Service is stopped.
- Info: Service is starting or stopping.
- Service error.

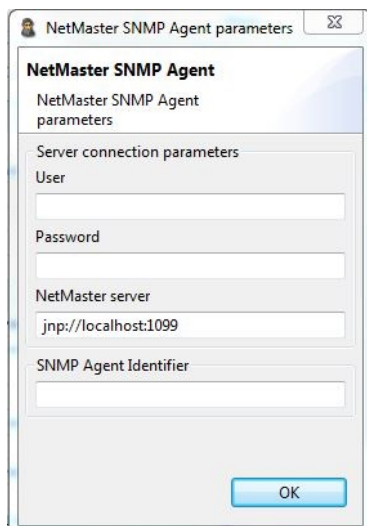
Note that in a High Availability server setup (Refer [Error! Reference source not found.](#)), the SNMP agent service icon of the Standby server is red to indicate it is in Standby mode.

By right-clicking the taskbar icon, it is possible to start, stop or configure the service.

Only a user defined as an Administrator can start or stop the SNMP agent service using the SNMP Agent Service monitor.

Configure displays the following dialogue:

Figure 234 SNMP agent parameters



Field description:

- User: Name of the user that shall be used to log on to the NMS server.
- Password: The password of the NMS SNMP Agent user.

- EMS server: URL for the NMS server to monitor.

Important note: The service must be restarted for configuration changes to take effect.

In the NMS Client use the [Northbound SNMP Settings](#) view to configure the High Level Managers (HLM) that shall be allowed to communicate with NMS via the SNMP Agent.

See also:

- [how to configure Northbound Interface SNMP](#), for a simple step-by-step description about what settings is needed in NMS SNMP Agent and Northbound SNMP Settings view.
- the document PTP 820 NMS SNMP Agent Guide.pdf on installation CD, for detailed information about Northbound Interface.

Chapter 6: SNMP Agent

The PTP 820 NMS SNMP agent is available as a licensed feature. The Northbound Hardware and Software Inventory reporting capabilities are available as licensed features for SNMP agent.

The Simple Network Management Protocol (SNMP) architecture is based on a query/response model. The client, which sends out queries, is generally described as the manager. The SNMP Server (the device that answers the queries) is referred to as the agent. The SNMP protocol enables a network management station to read and change (or write) an agent's parameters according to the rules of SNMP. SNMP also allows the agents to send an unsolicited message to the management station under certain circumstances (a trap).

This chapter includes:

- [PTP 820 NMS SNMP Agent](#)
- [MIB Overview](#)
- [Installation](#)
- [Configuration](#)
- [Verification](#)
- [Troubleshooting](#)

PTP 820 NMS SNMP Agent

The EMS SNMP agent makes it possible for any SNMP based management system to perform fault management of any EMS managed network. The agent provides the current state of the network through an active alarm table, while alarm state changes are communicated efficiently to the manager/client through use of SNMP traps.

SNMP Agent

The SNMP agent runs as a standalone application, either on the same PC as the EMS server or on a remote PC. It is basically a specialized client that logs onto the EMS server with a user ID and provides access to a set of information through an SNMP interface

Please note that the SNMP agent will be counted as a logged in user and will decrease the number of clients available on your EMS license.

Protocols Supported

The SNMP agent supports SNMP version 2c. The default port used by the agent is UDP port 161. This port is configurable as described in [Potential port conflict](#).

MIBs Supported

The SNMP agent supports the following MIBs:

- MIB-II (RFC3418)
- Entity-MIB (RFC2737)

MIB Overview

MIB Overview

All the information that is available from the Agent is presented in an information module — Management Information Base (MIB). MIB modules are built as trees and information is presented at the tree's leafs. The MIBs are written according to the Structure of Management Information version 2(SMIv2) as defined in [RFC 2578](#). Each leaf node will have a unique identifier: Object Identifier (OID).

Supported Standard MIBs

The EMS SNMP agent supports two standard MIBs: MIB-II and Entity-MIB.

MIB-II

The MIB-II information is defined in [RFC3418](#) and describes common information to be provided by all SNMP compatible agents. The EMS agent support parts of the information defined.

System Group

The system node OID is 1.3.6.1.2.1.1.

Table 54 System group description

OID	Description	Default value	Access
sysDescr	A textual description of the entity	PTP 820 NMS NIF Adapter	Read-Only
sysObjectID	The ID of the SNMP agent.	1.3.6.1.4.1.2378.2.3.1	Read-Only
sysUpTime	The time (in hundredths of a second) since the network management portion of the system was last re-initialized	N/A	Read-Only
sysContact	The textual identification of the contact person for this managed node, together with information on how to contact this person. If no contact information is known, the value is the zero-length string.	<blank>	Read-Write
sysName	An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string.	<blank>	Read-Write

OID	Description	Default value	Access
sysLocation	The physical location of this node (e.g., telephone closet, 3rd floor). If the location is unknown, the value is the zero-length string	<blank>	Read-Write
sysServices	A value which indicates the set of services that this entity may potentially offers	72	Read-Only

SNMP group

Collection of objects providing basic statistics on requests being delivered to the agent. For a description of the listed objects see [RFC3418](#). The SNMP node OID is 1.3.6.1.2.1.11.

Table 55 SNMP group example

OID	Description
snmpInPkts.0	9745
snmpOutPkts.0	9745
snmpInBadVersions.0	0
snmpInBadCommunityNames.0	0
snmpInBadCommunityUses.0	0
snmpInASNParseErrs.0	0
snmpInTooBigs.0	0
snmpInNoSuchNames.0	0
snmpInBadValues.0	0
snmpInReadOnlys.0	0
snmpInGenErrs.0	0
snmpInTotalReqVars.0	124453
snmpInTotalSetVars.0	1
snmpInGetRequests.0	0
snmpInGetNexts.0	9126
snmpInSetRequests.0	1
snmpInGetResponses.0	0
snmpInTraps.0	0

OID	Description
snmpOutTooBigs.0	0
snmpOutNoSuchNames.0	1
snmpOutBadValues.0	0
snmpOutGenErrs.0	0
snmpOutGetRequests.0	0
snmpOutGetNexts.0	0
snmpOutSetRequests.0	0
snmpOutGetResponses.0	9769
snmpOutTraps.0	865
snmpEnableAuthenTraps.0	1
snmpSilentDrops.0	0
snmpProxyDrops.0	0

Entity-MIB

The Entity-MIB information is defined in [RFC2737](#) and is used by EMS to present network elements currently managed. The only table supported is the entPhysicalTable (OID 1.3.6.1.2.1.47.1.1.1) which contains one row for each managed element.

Table 56 entPhysicalTable description

Name	Description	Example
entPhysicalIndex	The index of this entry	1
entPhysicalDescr	A textual description of physical entity. This is the unique identifier for the element in EMS (system distinguished name).	EMS=ManagedElement=[IP=10.8.1.15].
entPhysicalVendorType	An indication of the vendor-specific hardware type of the physical entity.	null (not applicable)
entPhysicalContainedIn	The value of entPhysicalIndex for the physical entity which contains this physical entity. A value of zero indicates this physical entity is not contained in any other physical entity.	0
entPhysicalClass	An indication of the general hardware type of the physical entity.	chassis(3)
entPhysicalParentRelPos	An indication of the relative position of this child component among all its sibling components.	-1 (not applicable)
entPhysicalName	The textual name of the physical entity.	NMS-LAB (User label in EMS)
entPhysicalHardwareRev	The vendor-specific hardware revision string for the physical entity.	zero-length (not applicable)
entPhysicalFirmwareRev	The vendor-specific firmware revision string for the physical entity.	zero-length (not applicable)
entPhysicalSoftwareRev	The vendor-specific software revision string for the physical entity.	zero-length (not applicable)
entPhysicalSerialNum	The vendor-specific serial number string for the physical entity.	zero-length (not applicable)

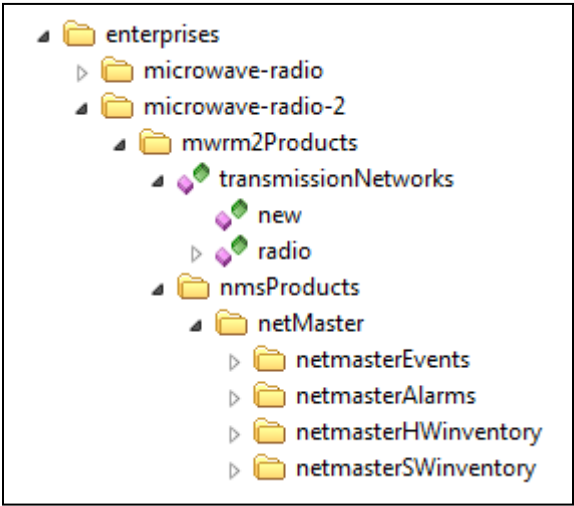
Name	Description	Example
entPhysicalMfgName	The name of the manufacturer of this physical component. In EMS, this field contains the product name of the NE.	
entPhysicalModelName	The vendor-specific model name identifier string associated with this physical component. In EMS, this field contains the configuration data for the NE.	Metro 1+0
entPhysicalAlias	This object is an alias name for the physical entity as specified by a network manager, and provides a non-volatile handle for the physical entity.	NMS-LAB (User label in EMS)
entPhysicalAssetID	This object is a user-assigned asset tracking identifier for the physical entity as specified by a network manager, and provides non-volatile storage of this information.	zero-length (not applicable)
entPhysicalIsFRU	This object indicates whether or not this physical entity is considered a field replaceable unit by the vendor.	true(1)

Microwave-specific MIBs

Several MIBs have been created to provide microwave-specific information. All PTP 820 NMS specific MIBs can be found on the PTP 820 NMS installation CD, under the folder PTP 820 NMS MIBs.

microwave-radio-2

The microwave-radio-2 branch is shown in the following diagram.



MWRM2-NMS-MIB

This MIB module describes the interface between PTP 820 NMS and High Level Managers (HLMs).

netmasterAlarmTable

The netmasterAlarmTable (OID 1.3.6.1.4.1.2378.1.2.1.1.1) describes the active alarms in PTP 820 NMS. There is one row in the table for each active alarm. When an alarm is raised, one row is added to the table. When an alarm is cleared, the corresponding row is removed.

netmasterAlarmTable description

OID	Description
netmasterAlarmId	Unique identifier for each alarm that is generated from the NMS. Two similar alarms from the same NE should have different alarmIds. The alarmIds are guaranteed to be unique but not necessarily in sequence.
netmasterAlarmObjectName	The System Distinguished Name (SDN) used for identifying the managed element that is the source of the Alarm. This identifier is the same as used in the entPhysicalTable. The type of this field is a DisplayString with a maximum length of 255 characters.
netmasterAlarmObjectType	Indicates the object class (type) to which the source of the alarm belongs to, see section 3.3.2.2 TmfObjectType.

netmasterAlarmTimeNe	The time of generation of the event, see section 3.3.1.1 <i>DateAndTime</i> . This is an optional field and may be reported empty.
netmasterAlarmTimeEms	The time of realization of the event by the EMS, see section 3.3.1.1 <i>DateAndTime</i> .
netmasterAlarmIsClearable	True if the alarm/event represents a condition that can be cleared at a later time (or is itself a clear); false otherwise.
netmasterAlarmProbableCause	Defines further qualification as to the probable cause of the alarm. The type of this field is DisplayString limited to 255 characters. The values for this field are based on the probableCause definitions found in TMF608.
netmasterAlarmNativeProbableCause	Defines further native qualifications as to the probable cause of the alarm. The type of this field is DisplayString limited to 255 characters
netmasterAlarmProbableCauseQualifier	This parameter, when present, may further qualify the source of the alarm. The qualifier consists of two parts: <netmasterAlarmNativeProbableCause>:<Originating node below managed element>. If originating node is the managed element node itself, it will only be <netmasterAlarmNativeProbableCause>
netmasterAlarmLayer	The layer to which this alarm is relevant. This parameter, when present, may further qualify the source of the alarm. The field is an integer with the following legal values: 1 (N/A), 2 (ds1), 4 (ds3), 5 (e1), 6 (e2), 7 (e3), 8 (e4), 15 (sts3c au4), 20 (section3 rs1), 25 (line3 ms1), 46 (electrical), 47 (optical), 48 (radio), 73 (dsr 1), 74 (dsr 4), 93 (dsr 2x1), 96 (ethernet), 10000 (ebus)
netmasterAlarmAdditionalText	Free form text description to be reported. NMS is not required to understand the semantics of this field for interpretation of the notification.
netmasterAlarmPerceivedSeverity	Indication of how it is perceived that the capability of the object has been affected. See section 3.3.2.3 <i>TmfPerceivedSeverity</i> .
netmasterAlarmType	The AlarmType classifies the alarm into one of the five basic categories as specified in ITU-T X.733. See section 3.3.2.1 <i>TmfAlarmType</i> .
netmasterAlarmAcknowledgeIndication	Indication as to whether the alarm has been acknowledged.
netmasterAlarmResourceDisplayname	Source of the alarm in a user friendly pattern.
netmasterAlarmDeviceType	The type of NE involved

netmasterAlarmLocation	Location of originating device
netmasterAlarmCLLI	Common Language Location Identifier (CLLI) of originating device.
netmasterAlarmNelpv4Address	The IPv4 address of the NE involved. The NE's IPv4 address will appear only if the NE is managed with IPv4.
netmasterAlarmNelpv6Address	The IPv6 address of the NE involved. The NE's IPv6 address will appear only if the NE is managed with IPv6.
netmasterAlarmOriginalAlarmId	The Alarm Identity Number provided by the device that represents the alarm reason.
netmasterAlarmIfIndex	The device IfIndex that identifies the interface which is the source of the alarm.
netmasterAlarmAlarmState	Indication of whether the trap is an alarm which is raised (1) or cleared (0), or whether an event (2) has occurred.
netmasterAlarmNMSServerId	A user-defined Identity string of the PTP 820 NMS server to be sent by the SNMP Agent in all traps to the HLM.

An example on how an alarm will appear in the netmasterAlarmTable is shown below.

Example of row in netmasterAlarmTable

Variable binding included	Example
netmasterAlarmId	200001009
netmasterAlarmObjectName	EMS=[NgNms/Collector=SNMP]/ManagedElement=[IP=10.8.1.16]
netmasterAlarmObjectType	equipment(9)
netmasterAlarmTimeNe	2008-10-29,22:55:1.0,+1:0
netmasterAlarmTimeEms	2008-10-30,9:7:30.103,+1:0
netmasterAlarmIsClearable	true(1)
netmasterAlarmProbableCause	EQPT
netmasterAlarmNativeProbableCause	ADC OVERRANGE
netmasterAlarmProbableCauseQualifier	ADC OVERRANGE:EquipmentHolder=[rack=ne/shelf=frame-1/slot=slot-4]/Equipment=riu
netmasterAlarmLayer	1 (not applicable)
netmasterAlarmAdditionalText	riu14
netmasterAlarmPerceivedSeverity	major(3)
netmasterAlarmType	equipmentAlarm(3)
netmasterAlarmAcknowledgeIndication	notApplicable(0)

Variable binding included	Example
netmasterAlarmResourceDisplayname	nmslab/ne/frame-1/slot-4/riu
netmasterAlarmDeviceType	PTP 820N
netmasterAlarmLocation	Central Bucharest
netmasterAlarmCLLI	Bucharest
netmasterAlarmNelpv4Address	10.10.66.101
netmasterAlarmNelpv6Address	2001:db8:85a3:0:0:8a2e:370:7334
netmasterAlarmNMSServerId	NMS_server_west
netmasterAlarmOriginalAlarmId	101
netmasterAlarmIfIndex	268477057
netmasterAlarmAlarmState	raised
netmasterAlarmNMSServerId	NMS_123

netmasterSyncAlarms (OID 1.3.6.1.4.1.2378.1.2.1.1.2) starts the synchronization of alarms from a particular HLM on the port specified by this object. This command sends all active alarms as traps.

netMasterAlarmTrap

A netmasterAlarmTrap (OID 1.3.6.1.4.1.2378.1.2.1.0.1) signifies that an alarm event has occurred. The alarm event can be either due to an alarm condition in one of the network elements being monitored by PTP 820 NMS or by the PTP 820 NMS system itself. The trap will contain variable bindings referencing a row in the netMasterActiveAlarmsTable as illustrated in the example below which shows the variable bindings included in a trap when the unique alarm 200001009 is raised.

To determine if an alarm is raised or cleared, the variable binding netMasterPerceivedSeverity must be used. If this field is set to cleared(6) the alarm is cleared, otherwise the alarm is raised and the severity of this alarm is according to the value: indeterminate(1), critical(2), major(3), minor(4), warning(5).

To match an existing raised alarm with an incoming cleared alarm, the netMasterAlarmId should be used. This ID is the same when an alarm goes from raised to cleared.

netmasterAlarmTrap example

Variable bindings included in trap	Example
sysUpTime.0	00h:57m:57s.92th
snmpTrapOID.0	netmasterAlarmTrap (1.3.6.1.4.1.2378.1.2.1.0.1)
netmasterAlarmId.200001009	200001009
netmasterAlarmObjectName.200001009	EMS=[NgNms/Collector=SNMP]/ManagedElement=[IP=10.8.1.16]

Variable bindings included in trap	Example
netmasterAlarmObjectType.200001009	equipment(9)
netmasterAlarmTimeNe.200001009	2008-10-29,22:55:1.0,+1:0
netmasterAlarmTimeEms.200001009	2008-10-30,9:7:30.103,+1:0
netmasterAlarmIsClearable.200001009	true(1)
netmasterAlarmProbableCause.200001009	EQPT
netmasterAlarmNativeProbableCause.200001009	ADC OVERRANGE
netmasterAlarmProbableCauseQualifier.200001009	ADC OVERRANGE:EquipmentHolder=[rack=ne/s helf=frame-1/slot=slot-4]/Equipment=riu
netmasterAlarmLayer.200001009	1
netmasterAlarmAdditionalText.200001009	riu14
netmasterAlarmPerceivedSeverity.200001009	major(3)
netmasterAlarmType.200001009	equipmentAlarm(3)
netmasterAlarmAcknowledgeIndication.200001009	notApplicable(0)
netmasterAlarmResourceDisplayname.200001009	nmslab/ne/frame-1/slot-4/riu
netmasterAlarmDeviceType.200001009	PTP 820N
netmasterAlarmLocation.200001009	Central Bucharest
netmasterAlarmCLLI.200001009	Bucharest
netmasterAlarmNelpv4Address.200001009	10.10.66.101
netmasterAlarmNelpv6Address.200001009	2001:db8:85a3:0:0:8a2e:370:7334
netmasterAlarmNMSServerId.200001009	NMS_server_west
netmasterAlarmOriginalAlarmId.200001009	101
netmasterAlarmIfIndex.200001009	268477057
netmasterAlarmAlarmState.200001009	Raised(1)
NetmasterAlarmNMSServerId.200001009	NMS_123

netMasterHeartBeatTrap

A netmasterHeartBeatTrap (OID 1.3.6.1.4.1.2378.1.2.1.0.2) signifies that PTP 820 NMS server is up and running. PTP 820 NMS Heartbeat is a feature that enables PTP 820 NMS to send traps to all configured High Level Managers stating that everything is OK. The interval of the heartbeat trap is configurable.

By default this trap is not enabled. To setup the generation of heartbeat traps see section 5.5 *Enabling heartbeat traps*.

netmasterHeartBeatTrap example

Variable bindings included in trap	Example
sysUpTime.0	01h:12m:51s.22th
snmpTrapOID.0	netmasterHeartBeatTrap (1.3.6.1.4.1.2378.1.2.1.0.2)

netMasterShutdownTrap

A netmasterShutdownTrap (OID 1.3.6.1.4.1.2378.1.2.1.0.3) signifies that the PTP 820 NMS SNMP agent no longer has contact with the PTP 820 NMS server.

netmasterShutdownTrap example

Variable bindings included in trap	Example
sysUpTime.0	02h:33m:17s.342th
snmpTrapOID.0	netmasterShutdownTrap (1.3.6.1.4.1.2378.1.2.1.0.3)

netmasterHWInventoryTable

The netmasterHWInventoryTable (OID 1.3.6.1.4.1.2378.1.2.1.2.1) contains all hardware inventory data for the network elements managed by PTP 820 NMS. The table is indexed using the entPhysicalIndex from the Entity-MIB physical table and the netmasterHWInventoryIndex. This makes it possible to request information for a specific managed element. The Entity-MIB presented by the PTP 820 NMS SNMP agent contains all the network elements currently managed.

netmasterHWInventoryTable description

OID	Description
netmasterHWInventoryPhysicalIndex	The entPhysicalIndex from the Entity-MIB physical table.
netmasterHWInventoryIndex	Unique identifier for each hardware inventory.
netmasterHWInventoryResource	Name/location of this hardware entry in the Network Element.
netmasterHWInventoryArticleCode	Uniquely identifies the type of hardware element.
netmasterHWInventorySerialNo	The serial number of the hardware element.
netmasterHWInventoryRevision	The hardware revision.

netmasterHWInventoryLastChangeTime

The netmasterHWInventoryLastChangeTime (OID 1.3.6.1.4.1.2378.1.2.1.2.2) describes the time of the last update to the hardware inventory table.

netmasterSWInventoryTable

The netmasterSWInventoryTable (OID 1.3.6.1.4.1.2378.1.2.1.3.1) contains all software inventory data for the network elements managed by PTP 820 NMS. The table is indexed using the entPhysicalIndex from the Entity-MIB physical table and the netmasterSWInventoryIndex. This makes it possible to request information for a specific managed element. The Entity-MIB presented by the PTP 820 NMS SNMP agent contains all the network elements currently managed.

netmasterSWInventoryTable description

OID	Description
netmasterSWInventoryPhysicalIndex	The entPhysicalIndex from Entity-MIB physical table.
netmasterSWInventoryIndex	Unique identifier for each software inventory.
netmasterSWInventoryResource	The name of the NE where this software is stored.
netmasterSWInventoryName	The name of the software in this memory bank, as read from the NE.
netmasterSWInventoryVersion	Software revision. Normally a five character code, but the field will display NA if the system has this unit present but is unable to retrieve the information from it.
netmasterSWInventoryBuildTime	The time when this software was created.
netmasterSWInventoryMemoryBank	Software location on the NE
netmasterSWInventoryStatus	<p>Displays the status of the memory bank and can be one of the following values</p> <ul style="list-style-type: none"> • IDLE: Software is not being executed. • ACTIVE: Software is being executed. • ACTIVE_PENDING: Software is waiting to be executed (will be activated on next restart). • DOWNLOADING: Software is being downloaded to this bank. • ERASING_FLASH: Software is being erased (during a download process). • INVALID: Corrupt software or wrong software version; software download failed or software bank has not been used. • NOT_AVAILABLE: The IDU does not have contact with the unit using this software (only relevant for ODU banks) or corrupted memory bank.

netmasterSWInventoryLastChangeTime

The netmasterSWInventoryLastChangeTime (OID 1.3.6.1.4.1.2378.1.2.1.3.2) describes the time of the last update to the software inventory table.

netmasterHWinventoryLastChangeTrap

A netmasterHWinventoryLastChangeTrap (OID 1.3.6.1.4.1.2378.1.2.1.0.4) signifies that a change in hardware inventory has occurred. The trap will contain variable bindings referencing a row in netmasterHWInventoryTable. A netmasterHWinventoryLastChangeTrap may occur, for example, when an NE has been added into managed state, removed from managed state or a hardware component has been added or removed from an NE.

netmasterHWinventoryLastChangeTrap example

Variable bindings included in trap	Example
sysUpTime.0	0 days 00h:03m:26s.32th
snmpTrapOID.0	netmasterHWinventoryChangeTrap
netmasterHWinventoryPhysicalIndex.3	1
netmasterHWinventoryResource.3	EMS=[NgNms/Collector=SNMP]/ManagedElement=[IP=10.8.1.19]/EquipmentHolder=[rack=ne/shelf=pdhFrame/slot=slot-4]/Equipment=riu
netmasterHWinventoryArticleCode.3	FDM5559A
netmasterHWinventorySerialNo.3	91100827
netmasterHWinventoryRevision.3	52 34 42 09 52 32 41 30

netmasterSWinventoryLastChangeTrap

A netmasterSWinventoryLastChangeTrap (OID 1.3.6.1.4.1.2378.1.2.1.0.5) signifies that a change in the software inventory has occurred. The trap will contain variable bindings referencing a row in netmasterSWInventoryTable. A netmasterSWinventoryLastChangeTrap may occur, for example, when an NE has been added into managed state, removed from managed state, after a software switch or after the installation of new software.

netmasterSWinventoryLastChangeTrap example

Variable bindings included in trap	Example
sysUpTime.0	0 days 00h:03m:26s.34th
snmpTrapOID.0	netmasterSWinventoryChangeTrap
netmasterSWinventoryPhysicalIndex.1	1
netmasterSWinventoryResource.1	NMSLab - 10.8.1.19 - 10.8.1.19
netmasterSWinventoryName.1	SW-EVOLUTION-ACCESS-APP
netmasterSWinventoryVersion.1	3A1
netmasterSWinventoryBuildTime.1	2009-6-9,0:0:0.0,+2:0
netmasterSWinventoryMemoryBank.1	1
netmasterSWinventoryStatus.1	ACTIVE

Textual Conventions used

SNMPv2-TC

DateAndTime

The DateAndTime type is a common way of displaying time information in SNMP. The base type is an Octet String that is formatted according to the rules described below. Most SNMP Managers/Browser have built in support for decoding this type correctly.

"2d-1d-1d,1d:1d:1d.1d,1a1d:1d"

"A date-time specification."

field	octets	contents	range
-----	-----	-----	-----
1	1-2	year	0..65536
2	3	month	1..12
3	4	day	1..31
4	5	hour	0..23
5	6	minutes	0..59
6	7	seconds	0..60
		(use 60 for leap-second)	
7	8	deci-seconds	0..9
8	9	direction from UTC	'+' / '-'
9	10	hours from UTC	0..11
10	11	minutes from UTC	0..59

For example, Tuesday May 26, 1992 at 1:30:15 PM EDT would be displayed as:

1992-5-26,13:30:15.0,-4:0

MWRM2-TMF-TC

This MIB module defines TMF based Textual Conventions used in network management systems.

TmfAlarmType

The TmfAlarmType classifies the alarm into one of the five basic categories as specified in ITU-T X.733:

- communicationAlarm(1)
- environmentalAlarm(2)
- equipmentAlarm(3)
- processingErrorAlarm(4)
- qualityOfServiceAlarm(5)

TmfObjectType

Used to indicate the object class (type) to which the object instance belong:

- ems(1)
- managedElement(2)
- multilayerSubnetwork(3)
- topologicalLink(4)
- subnetworkConnection(5)
- physicalTerminationPoint(6)
- connectionTerminationPoint(7)
- terminationPointPool(8)
- equipment(9)
- equipmentHolder(10)
- protectionGroup(11)
- trafficDescriptor(12)
- aid(13)

TmfPerceivedSeverity

Indication of how it is perceived that the capability of the object has been affected:

- indeterminate(1)
- critical(2)
- major(3)
- minor(4)
- warning(5)
- cleared(6)

Configuration

License check

Before continuing, it is important that you check your EMS license. It must contain the Northbound SNMP feature; otherwise the SNMP agent will not start. Also, the license must contain the Northbound SNMP Inventory feature in order to read the hardware and software inventory data. To check your license, you can utilize the EMS Server monitor application located in the system tray. Right-click the EMS Server monitor application icon and select **License Info**.

Creating a EMS SNMP agent user

Create a new user and add this user to the predefined user group SNMP Agent. See How to create a new user in the PTP 820 NMS User Manual for details. The user group for the SNMP Agent must have the following action permissions:

- Configuration/Inventory Views
- Fault/Alarm Management
- Fault/Historical Alarms
- Northbound Interface/SNMP Northbound Interface

Creating an NIF setting

If you do not create an NIF setting, no SNMP manager will be able to communicate with the EMS SNMP agent. Every SNMP manager must have a corresponding NIF setting to communicate with the agent:

1. In the EMS client open the Northbound Interface SNMP Settings view by clicking **View > Northbound Interface > SNMP Settings**.
2. Click **Create a new High Level Manager** to start the Create High-Level Manager wizard.

See [Northbound SNMP Settings View](#) for details.

Alarm Forwarding

By default, all alarms are forwarded to High Level Managers without any filtering. By enabling and configuring the alarm forwarding rule it is possible to customize the information sent.

There are several criteria that can be defined:

- Scope
 - “ All network elements or selected network elements
- Alarms to forward
 - “ According to severity (Critical, Major, Minor, Warning, Indeterminate, Info)
- Specific alarms (possible with wild cards)
 - “ Alarms to block
 - “ Exclude specific alarms from being forwarded (possible with wild cards)
- Other
 - “ Discard toggling alarms, possible to delay from 1 second to 60 seconds.
 - “ Attach additional information to the alarm being forwarded.

Enabling heartbeat traps

To enable heartbeat traps, you need to set a system preference using the EMS GUI client:

- 1 In the EMS client, open Northbound Heartbeat Preferences by clicking **System Settings > Northbound > PTP820NMS heartbeat**.
- 2 In the PTP 820 NMS Heartbeat Preference page, check the Enable Heartbeat checkbox and set the Notification Interval. The default interval is 60 seconds.
- 3 You can specify to enable trap forwarding using SNMP V3 by checking the Use SNMP V3 (Ensure SNMP V3 settings are completed) checkbox. If you enable this option, enter the SNMP V3 settings in the [SNMP V3](#) Preferences page.
- 4 Click **OK** to save changes.



Note

In order to receive heartbeat traps from the EMS SNMP agent, you must first have created an NIF setting with traps defined (see [Creating an NIF setting](#)).

In a [High Availability](#) server setup, even if heartbeat traps are enabled on both servers, only the Active server will send heartbeat traps.

Configuring the EMS SNMP agent

- 1 Configuring the EMS SNMP agent is described in EMS SNMP agent in the PTP 820 user manual:
- 2 Right-click the EMS SNMP Agent Service icon in the Windows taskbar system tray and select Configuration.
- 3 Enter the user name and password for the SNMP Agent user with which to log on to the EMS server as defined in Creating a EMS SNMP agent user.

- 4 Enter the URL for the EMS Server to be monitored. The URL must be of the format 'jnp://<EMS sever address>:1099'. In most cases the EMS server and EMS SNMP agent is located on the same PC and the URL will be: jnp://localhost:1099. The port 1099 is the Java RMI Registry Port on the EMS server and should not be changed.

Potential port conflict

By default, the EMS SNMP agent will try to bind to UDP port 161. If other SNMP agents, like Microsoft SNMP Agent, shall run in parallel, the default port for the EMS agent must be changed in order to avoid port conflict. To change the default port for EMS SNMP agent:

- 1 Locate the file wrapper.conf (<EMS installation dir>\Northbound SNMP\bin\conf\wrapper.conf).
- 2 Open the file in a text editor.
- 3 Find the line wrapper.app.parameter.2=-p 161.
- 4 Change the port number from 161 to the required port number, ex. 9000.
- 5 Save the changes.

**Note**



Changing the SNMP port for EMS requires the HLM to use this port when requesting information from EMS.

Verification

After completing the installation and configuration, it is recommended that you verify that the EMS SNMP agent is operating correctly.

Make sure that EMS server is running with some elements in a managed state. At this time you should have:

- A EMS user that is a member of the SNMP Group.
 - An NIF setting matching your SNMP manager.
 - The configuration of the SNMP agent contains the user name and password of PTP 820 NMS user.
1. Start the SNMP Agent service by right-clicking the EMS SNMP Agent monitor icon and selecting **Start**.

The icon should change from stopped () to running ()

2. Open the log. It should look similar to the following:

```
2008-11-03 14:18:47,687 INFO  Number of Higher Level Manager(s) defined : 1
2008-11-03 14:18:48,109 INFO  PTP 820 NMS SNMP Agent started. Waiting for
requests from HLMs
```

Now the EMS SNMP agent should be configured correctly. However if you have access to a MIB browser, there are additional tests that can be performed. These tests are described in sections

- 6.1 Test of MIB-2 attributes
- 6.2 Test of the entPhysicalTable
- 6.3 Test of EMS specific attributes

Note also that if the permissions to read the hardware and software inventory data are changed, the SNMP Agent must be restarted in order for the change to take effect.

Test of MIB-2 attributes

Start the MIB browser and make sure you have loaded the EMS MIBs:

- entity-mib (RFC-2737)

Enter the IP address of the EMS server and provide the read and write community names configured for this manager in EMS (NIF settings).

Using the MIB browser, query all the OIDs below the mib-2.system node. Your result should look similar to this:

```
***** SNMP QUERY STARTED *****
```

```
1: sysDescr.O (octet string) PTP 820 NMS NIF Adapter
[4E.65.74.4D.61.73.74.65.72.20.4E.49.46.20.41.64.61.70.74.65.72 (hex)]
```

```
2: sysObjectID.0 (object identifier) 1.3.6.1.4.1.2378.2.3.1
3: sysUpTime.0 (timeticks) 6548200
4: sysContact.0 (octet string) (zero-length)
5: sysName.0 (octet string) Super SNMP
server[53.75.70.65.72.20.53.4E.4D.50.20.73.65.72.76.65.72 (hex)]
6: sysLocation.0 (octet string) (zero-length)
7: sysServices.0 (integer) 72
8: sysORLastChange.0 (timeticks) 0
9: sysORID.1 (object identifier) 1.3.6.1.6.3.1
10: sysORDescr.1 (octet string) The Mib Module for SnmpV2
entities.[54.68.65.20.4D.69.62.20.4D.6F.64.75.6C.65.20.66.6F.72.20.53.6E.6D.70.56.32.20.65.6E.
74.69.74.69.65.73.2E (hex)]
11: sysORUpTime.1 (timeticks) 6548356
**** SNMP QUERY FINISHED ****
```

Test of the entPhysicalTable

The entPhysicalTable contains all network elements managed by EMS. Read the table by using an SNMP tool of your choice. You should see something similar to what is displayed below.

Figure 235 License is not valid

Name	PID	Session Name	Session ID	Private Bytes	Working Set	User Name	Description
System	4	System	0	1,024	1,024	System	System
smss.exe	16	System	0	1,024	1,024	System	System
csrss.exe	20	System	0	1,024	1,024	System	System
explorer.exe	288	explorer	1	1,024	1,024	System	System
notepad.exe	312	notepad	1	1,024	1,024	System	System
chrome.exe	320	chrome	1	1,024	1,024	System	System

Test of PTP820 NMS specific attributes

ptp820nmsAlarmTable

The `ptp820nmsAlarmTable` (1.3.6.1.4.1.2378.1.2.1.1.1) contains all active alarms. In the example below, there are 43 active alarms and the table read results in 43 rows. Please note that the table contains all the columns described in `ptp820nmsAlarmTable`, even though not all columns are visible in the picture.

Figure 236 ptp820nmsAlarmTable

ptp820nmsSynchAlarms

The attribute **ptp820nmsSynchAlarms** (1.3.6.1.4.1.2378.1.2.1.1.2) can be used for synchronizing the active alarms and also to verify trap reception. Setting this attribute to a port value sends all active alarms as traps. In this case, both the EMS server and MIB browser are running on the same PC. EMS will, by default, bind to the SNMP trap port, and therefore, the MIB browser has to be configured to bind trap listening to a different port (ex. 8001). Setting the attribute **ptp820nmsSynchAlarms** to 8001, results in 43 Ptp820nmsAlarmTrap traps received, the same number as active alarms in the **ptp820nmsAlarmTable**.

Test of the ptp820nmsHWInventoryTable

The **ptp820nmsHWInventoryTable** (OID 1.3.6.1.4.1.2378.1.2.1.2.1) contains all hardware inventory data for the network elements managed by EMS. In the example below, there are 3 hardware inventory entries for managed element 10.8.1.19 and the table read results in 3 rows.

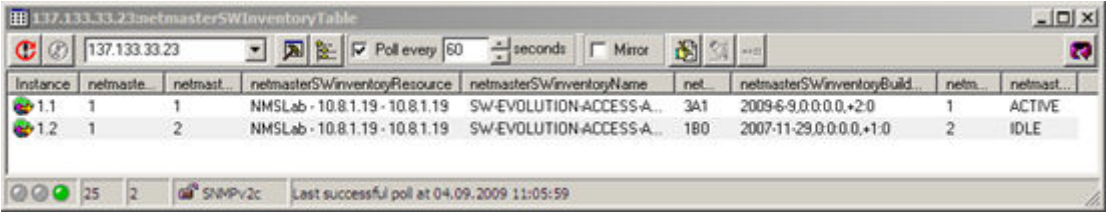
Figure 237 ptp820nmsHWInventoryTable

Instance	netma...	netmas...	netmasterHWInventoryResource	netmasterHWInventoryAut...	netmasterHWInventorySer...	netmasterHWInventoryRevision
1.1	1	1	EMS=[NERA Networks AS/Col...	FSPX57098	93000012	M2A
1.2	1	2	EMS=[NERA Networks AS/Col...	NA	NA	NA
1.3	1	3	EMS=[NERA Networks AS/Col...	FDM5559A	91100827	52 34 42 09 52 32 41 30

Test of the ptp820nmsSWInventoryTable

The **ptp820nmsSWInventoryTable** (OID 1.3.6.1.4.1.2378.1.2.1.3.1) contains all software inventory data for the network elements managed by EMS. In the example below, there are 2 software inventory entries for managed element 10.8.1.19 and the table read results in 2 rows.

Figure 238 ptp820nmsSWInventoryTable



The screenshot shows a window titled "137.133.33.23netmasterSWInventoryTable". It contains a table with 8 columns: Instance, netmaste..., netmast..., netmasterSWinventoryResource, netmasterSWinventoryName, net..., netmasterSWinventoryBuild..., netm..., and netmast... The table has two rows of data. Row 1.1 shows a device with IP 10.8.1.19, name SW-EVOLUTION-ACCESS-A..., net ID 3A1, build 2009-6-9.0.0.0.0.+2-0, netm ID 1, and status ACTIVE. Row 1.2 shows a device with IP 10.8.1.19, name SW-EVOLUTION-ACCESS-A..., net ID 180, build 2007-11-29.0.0.0.0.+1-0, netm ID 2, and status IDLE. The window also includes a toolbar with icons for refresh, help, and settings, and a status bar at the bottom indicating the last successful poll at 04.09.2009 11:05:59.

Instance	netmaste...	netmast...	netmasterSWinventoryResource	netmasterSWinventoryName	net...	netmasterSWinventoryBuild...	netm...	netmast...
1.1	1	1	NMSLab - 10.8.1.19 - 10.8.1.19	SW-EVOLUTION-ACCESS-A...	3A1	2009-6-9.0.0.0.0.+2-0	1	ACTIVE
1.2	1	2	NMSLab - 10.8.1.19 - 10.8.1.19	SW-EVOLUTION-ACCESS-A...	180	2007-11-29.0.0.0.0.+1-0	2	IDLE

Troubleshooting

Troubleshooting

SNMP agent fails to start

There might be several reasons for the SNMP agent service failure to start. To find further qualifications, open the agent log by right-clicking the SNMP agent icon and selecting **Open log**.

EMS server is not running

If you try to start the EMS SNMP agent, and the EMS server is not running, you will see that the status of the agent service goes from **Starting > Running -> Stopped**. The log will look like the following:

```
2008-11-06 14:05:16,828 ERROR Logon failed (Cannot connect to server)
2008-11-06 14:05:16,828 ERROR PTP 820 NMS SNMP Agent failed to start.
2008-11-06 14:05:18,937 INFO PTP 820 NMS SNMP agent stopped
```

Start the EMS server and try again.

Invalid user or password

If the provided user or password is not configured correctly, you will get the same behavior and message in the log as described in [EMS server is not running](#). Check that the configured user and password is correct.

License is not valid

If you try to start the EMS SNMP agent and the EMS license does not contain the Northbound SNMP feature, you will see that the status of the agent service goes from Starting > Running > Stopped. See [License check](#) regarding how to verify your license.

```
2008-11-06 14:05:16,828 NorthBound SNMP Service not started: License does not
allow NorthBound SNMP
2008-11-06 14:05:18,937 INFO PTP 820 NMS SNMP agent stopped
```

Cannot bind to UDP port 161

If another process is using UDP port 161, the EMS SNMP agent will fail to start. In the log you will see a message similar to the following:

```
2008-11-06 14:05:16,828 Bind Exception : Port 161 is in use. See PTP 820 NMS
installation guide on how to change SNMP agent port.
2008-11-06 14:05:18,937 INFO PTP 820 NMS SNMP agent stopped
```

See [Potential port conflict](#) for instructions on how to change the port used by the SNMP agent.

No traps are received

In order to receive traps, it is important that any firewall on the computer running the SNMP manager must be configured so UDP port 162 is open.

No hardware and software inventory data reported

Check that the license contains the Northbound SNMP Inventory feature and that the provided user has permissions to read the hardware and software inventory data.

No. of TRX count

For devices with built-in fixed radios, each of the radios requires a license, even if some of the radios are not used. Thus, the number of TRX licenses for each PTP 820G, PTP 820GX and PTP 820C is always 2, even if the device is configured as a 1+0 system.

Non-radio devices integrated into PTP 820 NMS are counted as using 1 TRX license.

Chapter 7: PTP 820 NMS Alarms

The following table lists the PTP 820 NMS alarm traps, as well as their descriptions and probable causes. These traps generated by PTP 820 NMS will be sent also through [NorthBound SNMP](#) if it is configured

Note that an [Alarm Template](#) exists for PTP 820 NMS alarms (under the <NMS> node), in which you can customize PTP 820 NMS alarms by changing the alarm text, etc.

Note also that in addition to the PTP 820 NMS alarms, a Heartbeat trap may also be sent if you enabled this in the [PTP 820 NMS Management Trap](#) Preferences window.

Alarm Text	Probable Cause	Severity	Description	Probable Cause/ Corrective Actions
Lost contact	EMS	Indeterminate	PTP 820 NMS lost connection with a device.	<p>Network problem, or the device has been restarted or powered down.</p> <ul style="list-style-type: none"> Check that the device is powered up and that there is connectivity through the network between PTP 820 NMS and the device. <p>Check that the Management Vlan on the device is enabled.</p>
HTTP logon failure	EMS	Warning	PTP 820 NMS has failed to open an HTTP connection with the device.	Check the HTTP credentials configured in the connection template.
Network elements number exceeds the license limit	NMS	Major	The number of managed network elements exceeds the license limit.	The installed license limits the number of radios that PTP 820

				NMS may manage. Install a new license with allowance for a larger number of Trx radios.
NE Type Mismatch	EMS	Indeterminate	Sent by PTP 820 NMS when it discovers that the NE type of a device has changed.	The NE type at the given IP address has changed. Delete the NE from PTP 820 NMS and rediscover.
Mate server not connected	NMS	Major	Relevant in a Server High Availability setup: Sent by either the Primary Server or Secondary server when two PTP 820 NMS servers are working in High Availability mode (one active and one standby), and communication with the mate server has failed.	Network problem, or the server has stopped or been shutdown. The server may have lost communication with the database.
Mate server is down	NMS	Major	Relevant in a Server High Availability setup: Sent by either the Primary Server or Secondary server when two PTP 820 NMS servers are working in High Availability mode (one active and one standby), and the server lost	Network problem, or the server has stopped or been shutdown. The server may have lost communication with the database.

			connection to its mate server.	
High Availability not licensed on Primary	NMS	Critical	Relevant in a Server High Availability setup: The license installed on the Primary server does not include Server High Availability.	Install a license with Server High Availability enabled.
File synchronization failure	NMS	Major	Relevant in a Server High Availability setup: Sent by the Primary server when two PTP 820 NMS servers are working in High Availability mode (one active and one standby), and file synchronization failed following a previously successful synchronization, or upon the first synchronization after High Availability was configured and both servers are active.	Network problem, server machine problem, or file system problem.
Server is Active	NMS	Indeterminate	Relevant in a Server High Availability setup. Note that this trap is an event notification, not an alarm notification.	

Chapter 8: System Manager

The purpose of the System Manager tool is to provide the PTP 820 NMS operators an easier and more flexible way to deal with some PTP 820 NMS administrative tasks:

- Set up EMS database connection
- Upgrade old EMS database to a new version
- Backup/restore database (requires System Manager on database server)
- Schedule database backup and database maintenance tasks
- Configure email notification
- Start and stop of EMS Server

This chapter includes:

- [PTP 820 NMS System Manager](#)
- [General menu](#)
- [Administration menu](#)
- [License menu](#)
- [Settings menu](#)
- [Other menu](#)
- [System Manager maintenance](#)

PTP 820 NMS System Manager

The purpose of the System Manager tool is to provide the PTP 820 NMS operators an easier and more flexible way to deal with some PTP 820 NMS administrative tasks:

- Set up EMS database connection
- Upgrade old EMS database to a new version
- Backup/restore database (requires System Manager on database server)
- Schedule database backup and database maintenance tasks
- Configure email notification
- Start and stop of EMS Server

PTP 820 NMS System Manager is a web application, i.e. it needs to run in a browser.

Internet Explorer is the only supported browser for System Manager. Mozilla FireFox and Google Chrome seems also to work fine, but be aware that questions related to unsupported browsers will not be answered by Customer Support.

System Manager uses wizards to guide the user through different setup and configuration tasks, and views that hold settings or other information, and from which the user can start the wizards.

[At the end of this chapter](#) is a list of the 11 views and 11 wizards available in System Manager.

System Manager Logon

The System Manager logon window looks like this:

Figure 239 System manager logon



Default user/password for System Manager is root/pw.

Given the fact that System Manager is a web application potentially available to many people, it is important to change the root password as soon as possible to reduce the risk of unauthorised access.

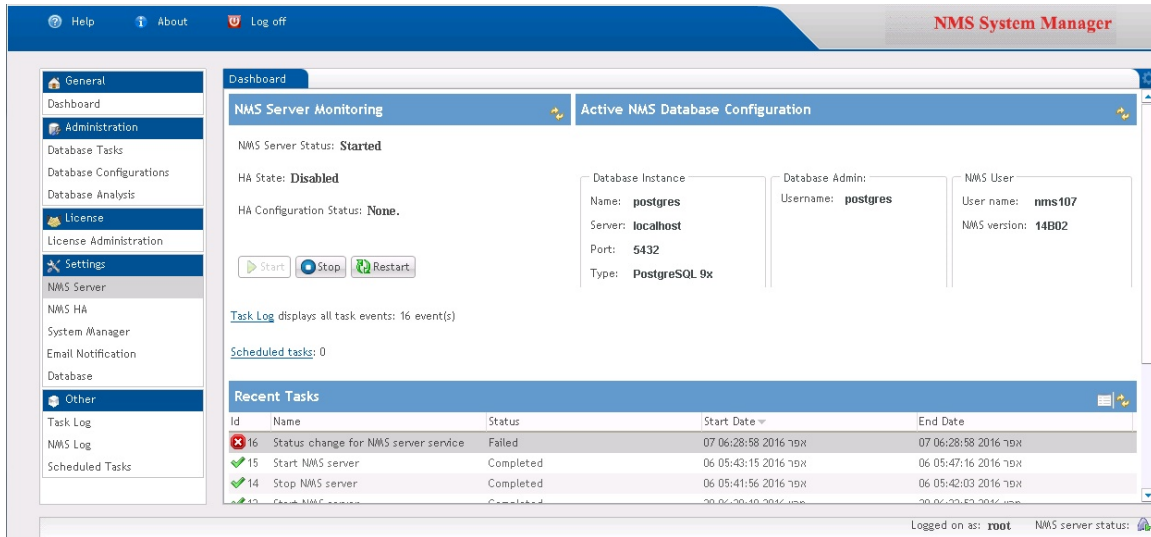
If the logon window doesn't appear properly, please press F5 in your browser to refresh the web page.

System Manager GUI Components Overview

System Manager GUI consists of an expandable menu on the left hand side and a main area on the right hand side. In addition, there is an About, Log off and Help button available on the top left corner. At the bottom right corner there is an area displaying logged in user and EMS server status.

After a successful logon System Manager may look like this:

Figure 240 System manager view

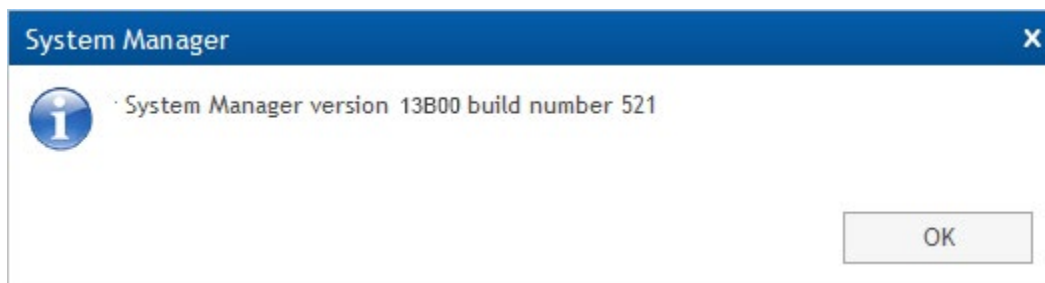


There are four distinct GUI areas as described below.

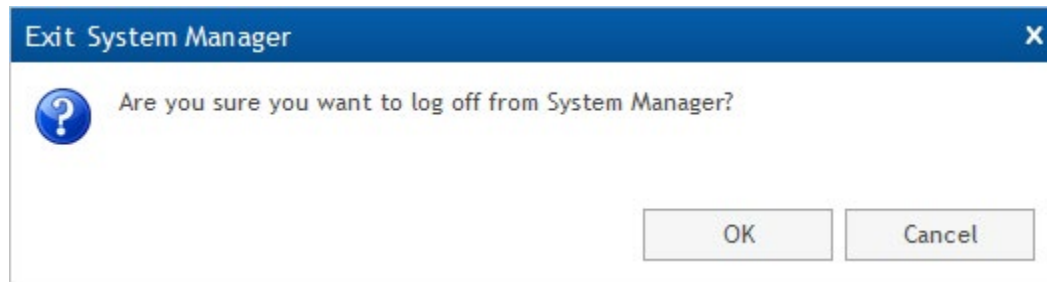
Toolbar area


There are 3 buttons available in the toolbar area at the top left hand corner:

-  **About** Opens System Manager version information:



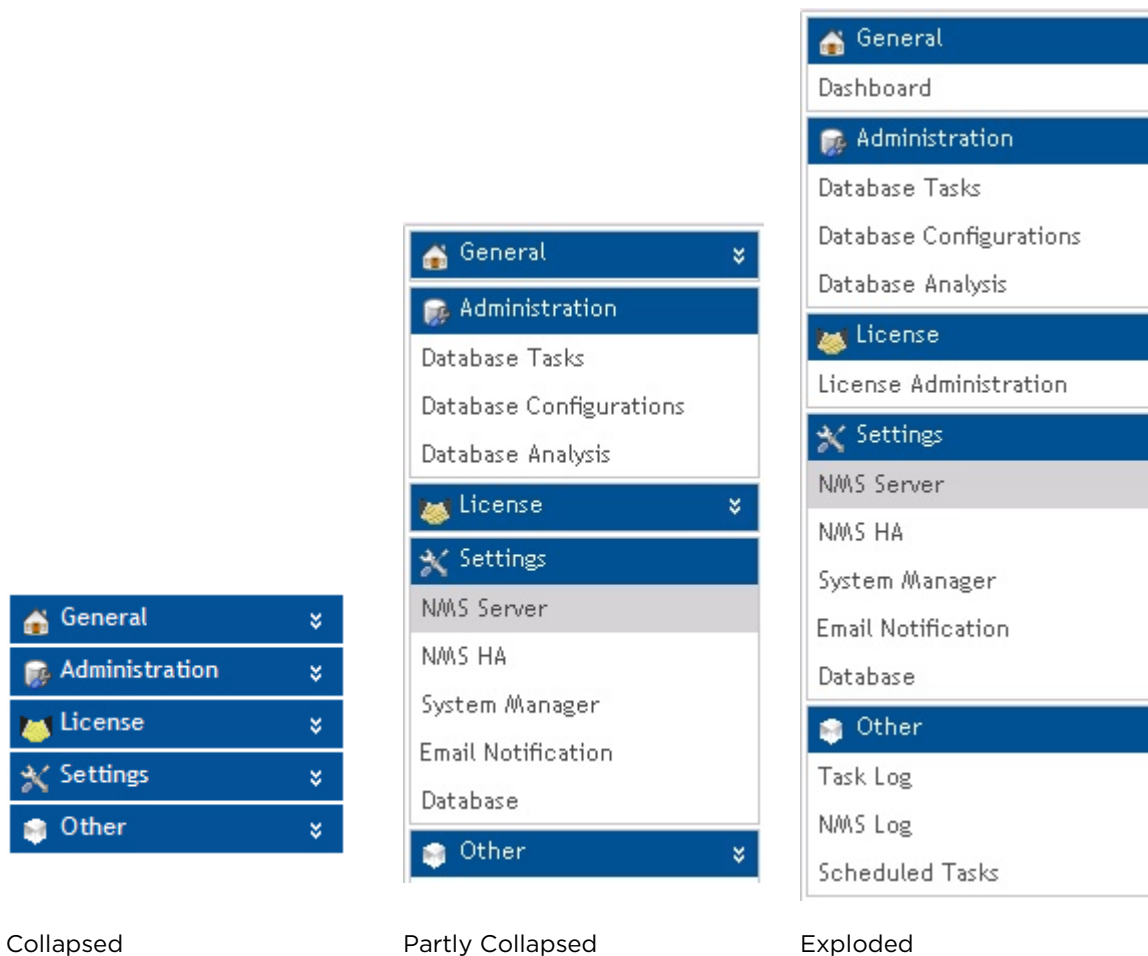
-  **Log off** Confirm System Manager log off by pressing OK here:



-  **Help** Opens System Manager Help in a separate browser window.

Menu area

The System Manager menu can be exploded and collapsed. Default is collapsed.



Collapsed

Partly Collapsed

Exploded

Click on any menu item to open the corresponding view in the main area.

The views are listed in the Available System Manager views section below.



Main area

The System Manager main area is where the different views are displayed. The default view (which cannot be closed) is the Dashboard. The individual views are explained in separate pages.

Several views may be open at the same time, but only one view will be visible in the main area at the time. Click a view tab to make this view visible in the main area.

Example below shows the [Scheduled Tasks view](#). Five open but hidden views are represented as tabs. Click on any of these tabs to show the associated view.

Figure 241 Scheduled tasks view

Dashboard	Database Tasks	Server	System Manager	Scheduled Tasks *	Database Configurations	 
Scheduled Tasks						
Description	Period in d	Next Start Date ▼	Delay until run (or sinc	User	Database Connection	
Backup active	29	17 Apr 2010 00:58:00	708:20:07		nmsora:1521:nmsora	
Optimize	15	02 Apr 2010 04:58:50	352:20:57		nmsora:1521:nmsora	

If you click on a menu item that already is open (but not shown) in the main area, the existing view will be shown. It is not possible to open several occurrences of the same view.




Status bar area

The System Manager status bar is always visible in the bottom right hand corner:

Logged on as: **root** NetMaster server status: 

This shows logged on user and EMS server status.

The server status has 3 states:

EMS Server Status	Explanation
	EMS server is started.
	EMS server is starting or stopping.
	EMS server is stopped.

Available System Manager views and wizards

Here is a list of the 11 views and 11 wizards available in System Manager.

Click on the links below to open more detailed information on each.

Table 57 System manager menus

General Views	Explanation
Dashboard	Default view in System Manager. This view cannot be closed. It is designed to give a quick overview of: EMS server status EMS database configuration Latest task logs
Administration Views	Explanation
Database Tasks	A collection of database related wizards to help you set up and maintain your EMS database: PTP 820 EMS Initial Setup wizard Set Active User/Schema wizard Create User/Schema wizard Reinitialize User/Schema wizard Delete User/Schema wizard Upgrade User/Schema wizard Backup Active User/Schema wizard Backup User/Schema wizard Restore User/Schema wizard
Database Configurations	Shows list of all stored database configurations, with option to create, clone, edit, delete and test database configurations.
Database Analysis	Shows list of database inconsistency reports, with option to run the Analyze User/Schema wizard to create new reports. This feature is primarily intended to aid problem solving in connection with customer cases reported to Customer Support.
License Views	Explanation
License Administration	Shows overview of current imported EMS license, with option to run the Import License wizard to import a new license into PTP 820 NMS.

Settings Views	Explanation
EMS Server	<p>EMS server related settings. Allows you to:</p> <p>Enable email notification if EMS server stops unexpectedly</p> <p>Reset the EMS root password on active EMS database</p>
PTP 820 NMS HA	PTP 820 NMS server High-Availability (HA) settings. Allows you to define a PTP 820 NMS server High-Availability setup.
System Manager	<p>System Manager related settings. Allows you to:</p> <p>Change System Manager root password</p> <p>Default root password is "pw" and should be changed as soon as possible.</p>
Email Notification	<p>Fill in the SMTP settings required to enable System Manager to send notification email to configured recipients if:</p> <p>EMS server stops unexpectedly</p> <p>Scheduled database optimization fails</p> <p>Scheduled database backup fails</p>
Database	<p>Database related settings. Allows you to:</p> <p>Change backup files storage location</p> <p>Enable/disable old backup files deletion job</p> <p>Enable/disable database optimization job</p> <p>Enable/disable email notification in case a scheduled job fails</p> <p>Enable/disable email notification in case a database optimization job fails</p>
Others Views	Explanation
Task Log	Shows the list of all Task Logs, with options to refresh list and inspect Task Log details.
EMS Log	Shows the list of all EMS server log entries, with options to refresh list, archive and delete logs.
Scheduled Tasks	Shows the list of all scheduled tasks, with options to refresh list and to delete unwanted scheduled tasks from the list.

General menu

Dashboard View

The Dashboard view is designed to give a quick overview of:

- EMS server status
- EMS database configuration
- The 10 latest task logs

It also gives one-click access to:

- Start, stop or restart EMS server (depending on current status)
- Open [Task Log view](#) to see the full list of task logs
- Open [Scheduled Tasks view](#) to see the full list of scheduled tasks

[Task Log](#) displays all task events: 118 event(s)

[Scheduled tasks](#): 2

This view is always opened when you log into System Manager. The view cannot be closed from the main area. If it gets hidden by other views and you want to show it again, you can either:

- Open General menu and click Dashboard
- Locate and click the main area Dashboard tab

Dashboard view content

Dashboard view consists of several parts, making important information visible on a single page:

Figure 242 Dashboard view content

NMS Server Monitoring

NMS Server Status: **Started**

HA State: **Disabled**

HA Configuration Status: **None**.

Start Stop Restart

[Task Log](#) displays all task events:
16 event(s)

[Scheduled tasks](#): 0

Active NMS Database Configuration

Database Instance		Database Admin:	NMS User
Name:	postgres	Username: postgres	User name: nms107
Server:	localhost		NMS version: 14B02
Port:	5432		
Type:	PostgreSQL 9x		

Recent Tasks

Id	Name	Status	Start Date	End Date
16	Status change for NMS server service	Failed	07 06:28:58 2016 אפר	07 06:28:58 2016 אפר
15	Start NMS server	Completed	06 05:43:15 2016 אפר	06 05:47:16 2016 אפר
14	Stop NMS server	Completed	06 05:41:56 2016 אפר	06 05:42:03 2016 אפר

The following is an example of Dashboard view when PTP 820 NMS is not participating in a [High Availability](#) server setup.

Figure 243 Dashboard view

NMS Server Monitoring

NMS Server Status: **Started**

HA State: **Active**

HA Configuration Status: **Configuration saved.**

Start Stop Restart

[Task Log](#) displays all task events: 6 event(s)

[Scheduled tasks](#): 0

Active NMS Database Configuration

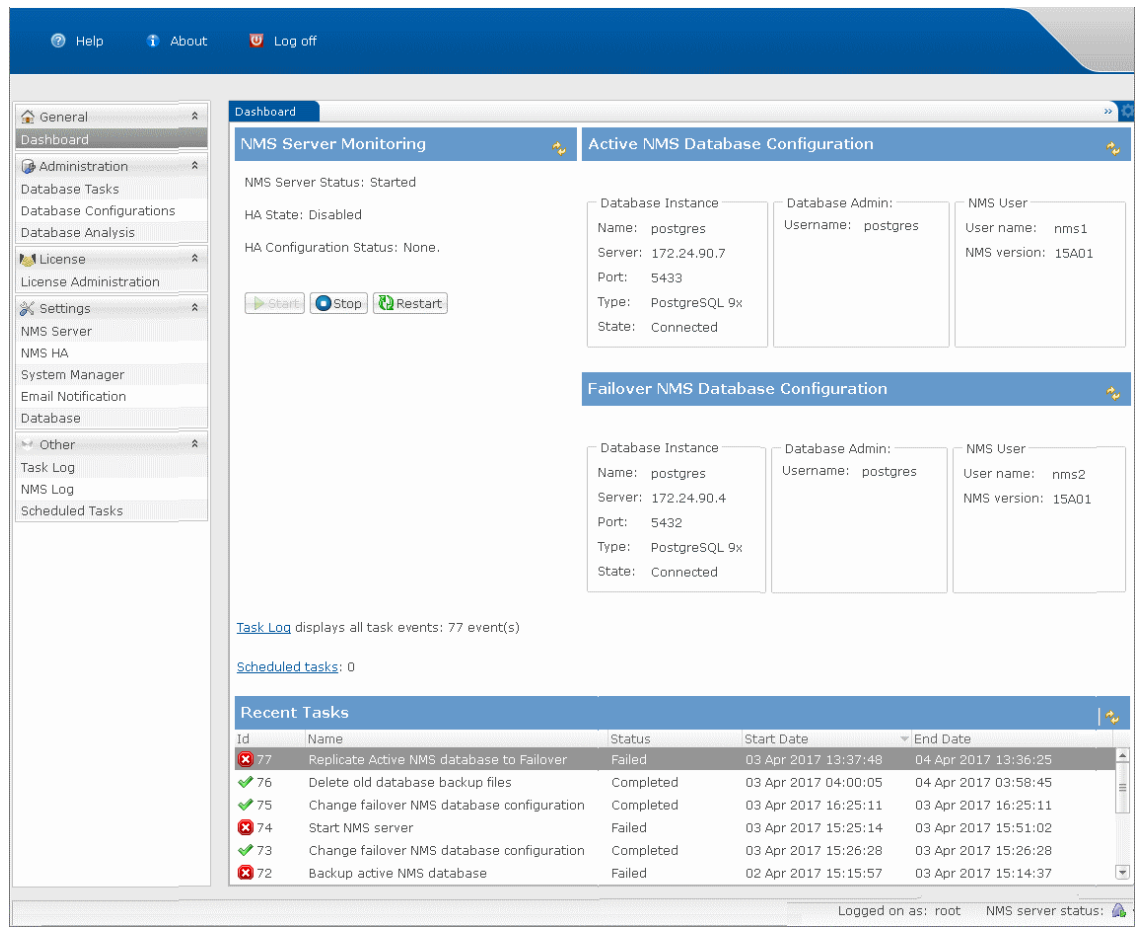
Database Instance		Database Admin:	NMS User
Name:	nmsorcl	Username: system	User name: hapm178
Server:	10.10.67.23		NMS version: 14B02
Port:	1521		
Type:	Oracle 11x		

Recent Tasks

Id	Name	Status	Start Date	End Date
6	Restart NMS server Mar 2016	Completed	19 08:45:01 Mar 2016	19 08:48:46 Mar 2016
5	Restart NMS server Mar 2016	Completed	18 17:42:05 Mar 2016	18 17:44:53 Mar 2016
4	Start NMS server Mar 2016	Completed	18 17:37:36 Mar 2016	18 17:40:19 Mar 2016
3	Change active NMS database configuration Mar 2016	Completed	18 17:30:26 Mar 2016	18 17:30:26 Mar 2016
2	Upgrade NMS database Mar 2016	Completed	18 17:30:04 Mar 2016	18 17:30:09 Mar 2016
1	Active license was changed Mar 2016	Completed	18 17:29:17 Mar 2016	18 17:29:17 Mar 2016

The following is an example of Dashboard view when PTP 820 NMS is participating in a [High Availability](#) server setup.

Figure 244 Dashboard view

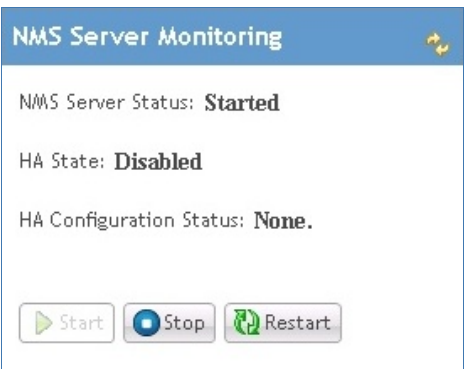


There are three distinct GUI areas and two links as described below.

PTP 820 NMS Server Monitoring area

This area is used to display and change EMS server status:




Figure 245 EMS server monitoring area




PTP 820 NMS Server Status

To ensure that correct status is shown, the current server status is checked every 10th second. Depending on this status the Start, Stop and Restart EMS server buttons may be disabled.

Table 58 EMS status buttons

Change EMS Status	Explanation
	Start EMS server. Disabled if server is running.
	Stop EMS server. Disabled if server is stopped.
	Restart EMS server. Disabled if server is stopped.

Press  to refresh the EMS Server Status.

PTP 820 NMS HA State

Every 10 seconds, the Standby server (whether Primary or Secondary), queries the Active server to determine whether it is up. If the Active server is not up, the Standby server becomes the Active server.

The HA state field in the [Error! Reference source not found.](#) of each server's System Manager shows the [Server High Availability](#) status of the two servers . The possible values are:

- Initializing
- Active
- Stand-by
- Disabled
- Switching to Active
- Switching to Stand-by

During a switchover:

- The HA state of the server switching over to Active mode changes from **Stand-by** to **Switching to Active** and then to **Active**.
- The HA state of the server switching over to Standby mode changes from **Active** to **Switching to Stand-by** and then to **Stand-by**.

If you are working in the PTP 820 NMS Client when the active server goes down, an error message appears:

[Currently unable to connect to the Active server. Press Reconnect to attempt a new connection.](#)

Wait approximately 10 minutes until switchover is complete, and then press Reconnect to connect the PTP 820 NMS client to the currently-active server.

Following a switchover between the two servers, the newly active server takes over control of the network.

- PM collection is continued from where the previous server left off.
- Any missing traps are read from the device during the next polling time interval.
- Any Software Download jobs that were interrupted will be re-run after a period of 25 minutes.
- Any configuration backup, configuration restore or discovery jobs, fail and need to be re-run by the user.
- Any service related operations that were in the process of being written to the devices will need to be re-applied by the user.
- Any user clients are disconnected from the server and will need to login again.
- Any wizards that a user client was working on will need to be activated again and the information re-entered.

PTP 820 NMS HA Configuration Status

Displays the [High Availability configuration status of the](#) PTP 820 NMS server. The possible values are:

Table 59 HA Configuration Status

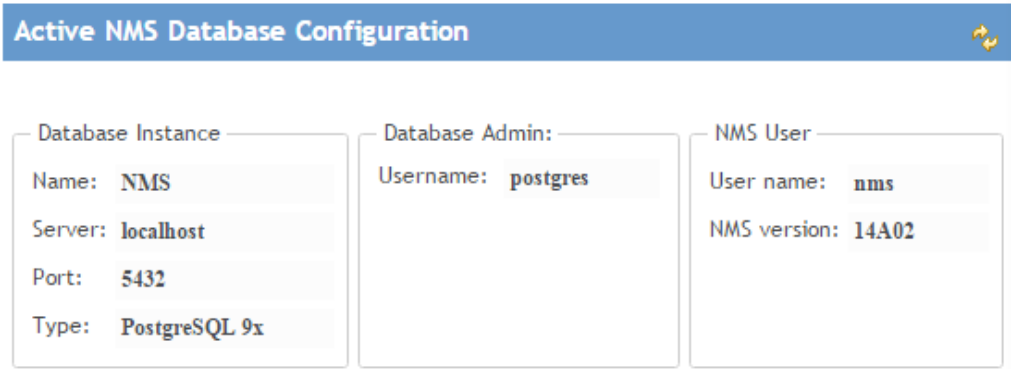
Change EMS Status	Explanation
None	PTP 820 NMS server is in a standalone configuration (High Availability not configured).
Configuration Saved	High Availability is successfully configured.
Mate PTP 820 NMS Software Version mismatch	The two mates participating in the High Availability configuration have different PTP 820 NMS software versions.
Key is missing or invalid	A problem related to the security keys (private key and public key) used for encrypting communications in a High Availability configuration between the Primary server's system manager and the Secondary server's system manager. The key files may be missing, or the keys are not in the files, or the keys could not be used to encrypt.
The mate is not set as Secondary	The PTP 820 NMS server is configured to be the Primary server in a High Availability configuration, but the mate server is not the Secondary server.

Could not communicate with mate	No response is received from the mate server in a High Availability configuration. This may occur because the mate is not reachable or because the mate was unable to understand the encrypted message.
The mate is not set as Primary	The PTP 820 NMS server is configured to be the Secondary server during the High Availability verification process.

Active PTP 820 NMS Database Configuration area

This area is used to present database configuration information:

Figure 246 Active EMS database configuration area



Press  to refresh the Active EMS Database Configuration area.

Server High Availability - Manual Intervention

In certain situations, for example due to communication failure between the servers and databases machines, each server may remain connected to a different one of the databases, causing both servers to act as the Active Server and to operate on a different one of the databases. When communication is restored between the machines, an alarm is raised and replication backup between the two database machines is not allowed.

In such situations, manual intervention is required to decide which should be the Active Server and which should be the Active Database and to manually restore the server and database High Availability configuration. Until such manual intervention, the two servers will continue to run independently on the two different databases.

Manual Intervention Steps

The manual intervention steps depend on whether the PTP 820 NMS server you wish to designate as the Primary server (which we will call Server1) is already connected to the database you wish to designate as the Active database, or if it is instead connected to the database you wish to designate as the Failover database.

We will call the database that Server1 is using, DatabaseA; and we will call the database that Server2 is using, DatabaseB.

If you wish to keep DatabaseA as the Active database, you need to:

- 1 Stop Server2.
- 2 Using the [Set Active/Failover User/Schema wizard](#), configure on Server2 that DatabaseA is the Active database, and DatabaseB is the Failover database.
- 3 Start Server2; it will become the Standby server.

If instead you wish to set DatabaseB as the Active database, you need to:

- 1 Stop both Server1 and Server2.
- 2 Using the [Set Active/Failover User/Schema wizard](#), configure on Server1 that DatabaseB is the Active database, and DatabaseA is the Failover database.
- 3 Start Server1; it will become the Active server.
- 4 Start Server2; it will become the Standby server.

Recent Task area


This area is used to display the 10 newest Task Log entries.


The list by default shows the newest entry first. You can sort otherwise by clicking on a column header. You can also drag and drop columns to change column order.

See [Task Log view](#) for more information about tasks and subtasks.

Figure 247 Recent task area

Recent Tasks				
Id	Name	Status	Start Date	End Date
✓ 36	Delete old database backup files	Completed	25 Jul 2015 07:14:25	25 Jul 2015 07:14:30
✗ 35	Read license information	Failed	05 Jul 2015 10:09:03	05 Jul 2015 10:09:03
✗ 34	Read license information	Failed	24 Jun 2015 22:36:45	24 Jun 2015 22:36:45
✓ 33	Delete old database backup files	Completed	20 Jun 2015 06:20:41	20 Jun 2015 06:20:45
✓ 32	Delete old database backup files	Completed	17 Jun 2015 09:02:30	17 Jun 2015 09:02:35
✓ 31	Delete old database backup files	Completed	09 Jun 2015 04:17:51	09 Jun 2015 04:17:53
✓ 30	Delete old database backup files	Completed	08 Jun 2015 07:24:12	08 Jun 2015 07:24:13
✓ 29	Delete old database backup files	Completed	05 Jun 2015 04:11:01	05 Jun 2015 04:11:05
✓ 28	Delete old database backup files	Completed	04 Jun 2015 05:45:25	04 Jun 2015 05:45:28
✗ 27	Read license information	Failed	29 May 2015 21:09:55	29 May 2015 21:09:55

Press  to refresh the Recent Task list.

Press  to open task details for selected task. You can also double click on a row to open task details.

Task Log link

There is a direct link open [Task Log view](#) to see the full list of task logs:

[Task Log](#) displays all task events: 118 event(s)

Schedule Task link

There is a direct link to open [Scheduled Tasks view](#) to see the full list of scheduled tasks:

[Scheduled tasks](#): 2

Administration menu

Database Task View

Database Task view consists of a collection of database related wizards to help you set up and maintain your EMS database.

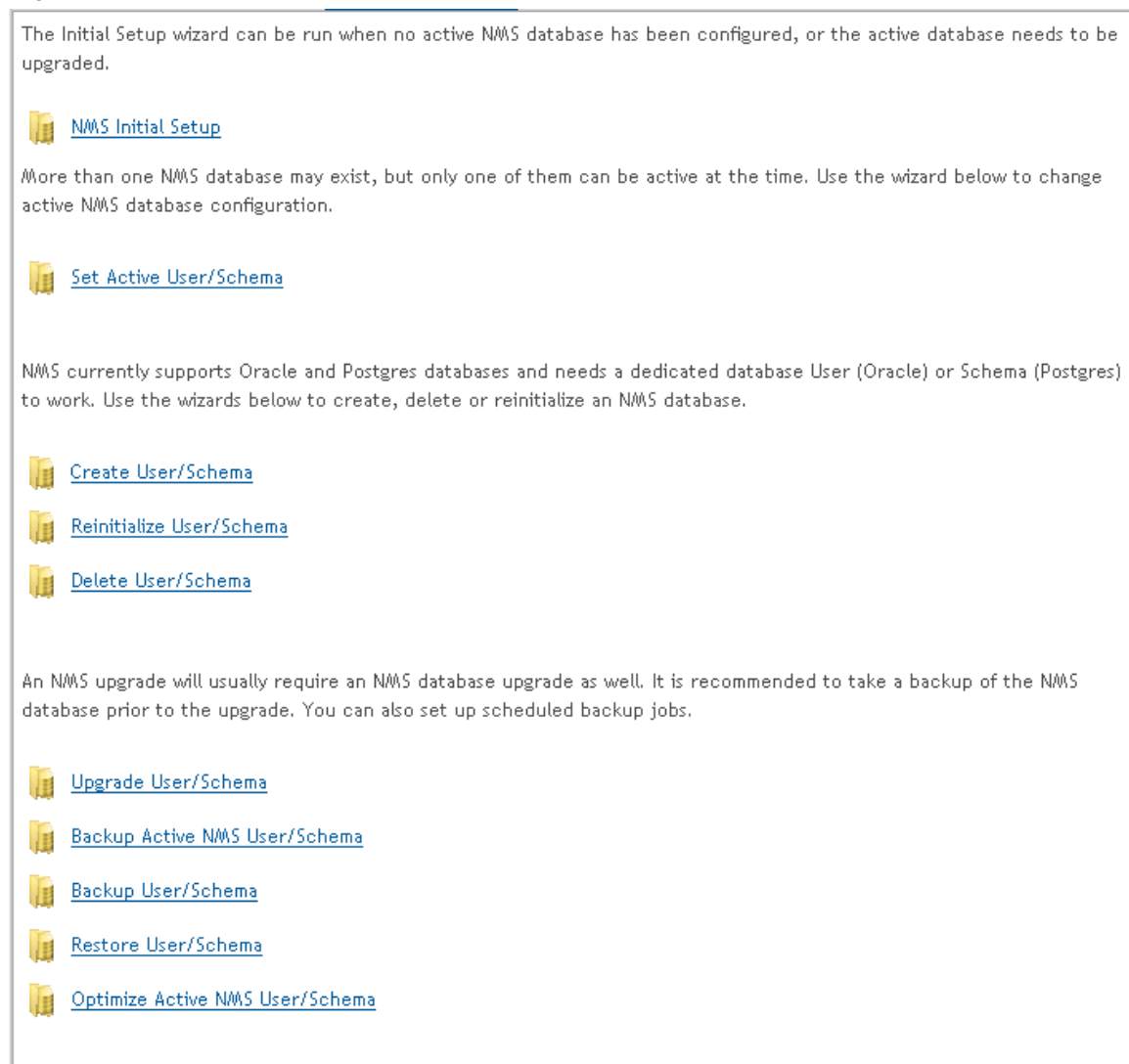
To open this view you can either:

- Open Administration menu and click Database Task
- Locate and click the main area Database Task tab, if present

Database Task view content

Database Task view consists of a list of various database related wizards:

Figure 248 Database task view content



Database Task wizards

Click on any of the links below to open the corresponding wizard help page.

- [PTP 820 EMS Initial Setup wizard](#)
- [Set Active User/Schema wizard](#)
- [Create User/Schema wizard](#)
- [Reinitialize User/Schema wizard](#)
- [Delete User/Schema wizard](#)
- [Upgrade User/Schema wizard](#)
- [Backup Active User/Schema wizard](#)
- [Backup User/Schema wizard](#)
- [Restore User/Schema wizard](#)
- [Optimize Active NMS User/Schema](#)

Database Configurations View

Database Configurations shows a list of all stored database configurations, with option to create, clone, edit, delete and test configurations.

To open this view, you can either:

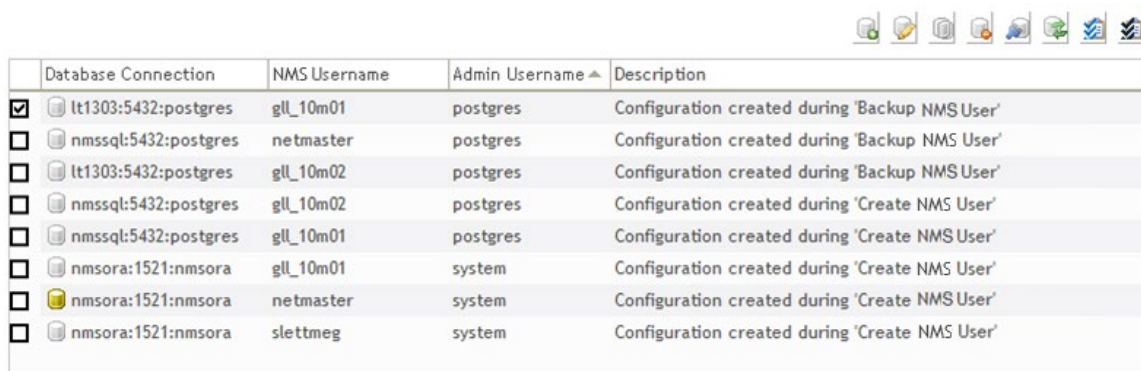
- Open Administration menu and click Database Configurations
- Locate and click the main area Database Configurations tab, if present

Database Configurations view content


Database Configurations view contains a list and a toolbar.

You can sort the list by clicking on a column header. You can also drag and drop columns to change column order.

Figure 249 Database configurations view content











	Database Connection	NMS Username	Admin Username ▲	Description
<input checked="" type="checkbox"/>	lt1303:5432:postgres	gll_10m01	postgres	Configuration created during 'Backup NMS User'
<input type="checkbox"/>	nmssql:5432:postgres	netmaster	postgres	Configuration created during 'Backup NMS User'
<input type="checkbox"/>	lt1303:5432:postgres	gll_10m02	postgres	Configuration created during 'Backup NMS User'
<input type="checkbox"/>	nmssql:5432:postgres	gll_10m02	postgres	Configuration created during 'Create NMS User'
<input type="checkbox"/>	nmssql:5432:postgres	gll_10m01	postgres	Configuration created during 'Create NMS User'
<input type="checkbox"/>	nmsora:1521:nmsora	gll_10m01	system	Configuration created during 'Create NMS User'
<input type="checkbox"/>	nmsora:1521:nmsora	netmaster	system	Configuration created during 'Create NMS User'
<input type="checkbox"/>	nmsora:1521:nmsora	slettmeg	system	Configuration created during 'Create NMS User'

Current active database configuration is prefixed with a .

All non-active configurations are prefixed with a .

Use the check box column to select the configurations to be target for operations.

Table 60 Database configuration buttons

Operation	Explanation
	Add a new configuration. Always enabled.
	Edit selected configuration. Enabled when exactly one configuration is selected. Only the configuration description can be edited for the active configuration.
	Clone selected configuration. Enabled when exactly one configuration is selected.
	Delete selected configuration. Enabled when one or more configurations are selected.
	Test selected configuration. Enabled when exactly one configuration is selected.
	Refresh list. Always enabled.
	Selects all configurations in the list. Always enabled.
	Deselects all configurations in the list. Always enabled.

Add, Edit or Clone a configuration

You can make an existing database configuration and optionally an existing user/schema name known to System Manager using the Add new configuration button. You can edit an existing database configuration or clone it to create a new configuration.

In all cases (Add, Edit & Clone) the following dialog will appear:

Figure 250 Add database configurations

The fields marked with * are required.

Description: Test configuration

Database connection parameters:

Database instance name: * nmstest

Database type: * Oracle

Database server address: * nmsora

Database server port: * 1521

Database administrator user:

Name: system

Password:

NMS user/schema:

Name: elb_test_2

Password: ...

Test Connection OK Cancel

Field explanations:

Table 61 Database configuration attributes

Name	Explanation
Description	Descriptive text for the database configuration
Database instance name	Name of an existing database instance
Database type	Either Oracle or Postgres
Database server address	IP address or hostname for the database server (use localhost for a 1+0 configuration)
Database server port	Tcp port for the database. Default 1521 for Oracle, 5432 for Postgres.

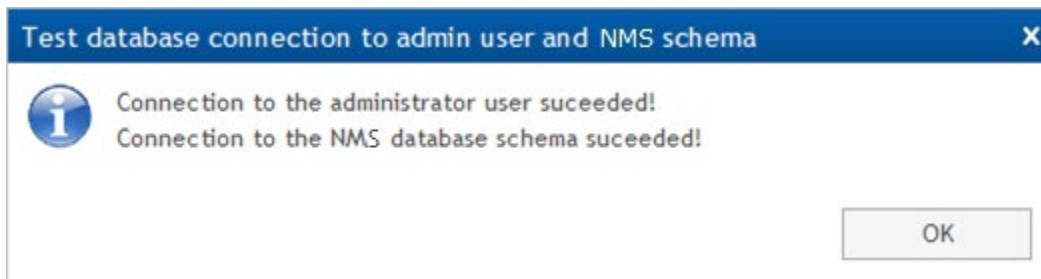
Database administrator user: Name	The database system user
Database administrator user: Password	Password for the database system user
EMS user/schema: Name	Name of a EMS user/schema
EMS user/schema: Password	Password of a EMS user/schema

Press OK to save the configuration, or Cancel to discard changes.

If the user and password information for either the database system user or a EMS user/schema is present, you can press Test Connection to verify your database configuration.

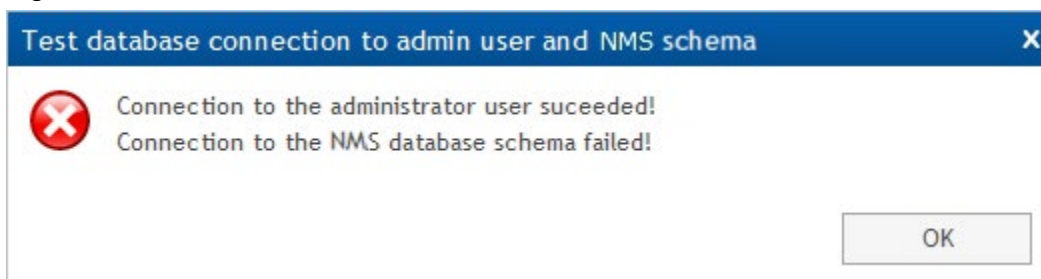
If both user/password pairs are correctly filled in, the following dialog should be displayed:

Figure 251 Database connection to admin user successful



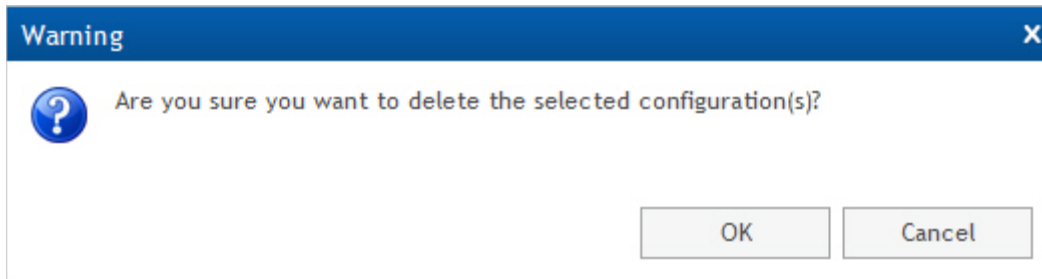
If for instance the EMS user/schema password is wrong, you may get the following dialog:

Figure 252 Database connection to admin user failure



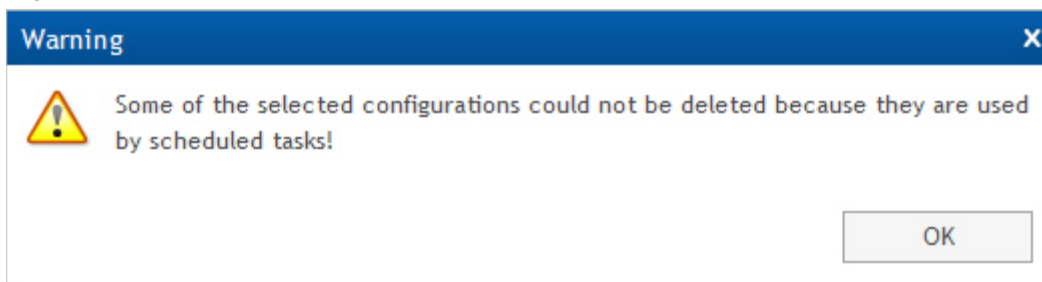
Delete a configuration

If one or more non-active database configurations are selected, you can attempt to delete them:

Figure 253 Delete a configuration warning

Press OK to delete the selected configurations.

You are not allowed to delete a database configuration that is used in any periodic database backup or database optimization jobs:

Figure 254 Delete a configuration not allowed warning

Database Analysis View

Shows list of database inconsistency reports, with an option to run the [Analyze User/Schema wizard](#) to create new reports.

This feature is primarily intended to aid problem solving in connection with customer cases reported to Customer Support.

To open this view, you can either:




- Open Administration menu and click Database Analysis
- Locate and click the main area Database Analysis tab, if present

Database Analysis view content

Database Analysis view contains a toolbar, a file list, a link to launch the [Analyze User/Schema wizard](#) and a file content display area.

Database Analysis toolbar

The Database Analysis toolbar consists of three parts:

Operation	Explanation
	Display selected analysis report file content in the display area
	Delete the selected analysis report file
	Refresh the analysis report file list

Database Analysis file list

The Database Analysis file list shows all analysis report files:

Report analysis file location is decided on last page of the Analyze User/Schema wizard.

Launch the Analyze User/Schema wizard

Click on the Database Analysis link to open the [Analyze User/Schema wizard](#):

Use [Database Analysis](#) wizard to perform database inconsistency checks on a NetMaster database.

File content display area

The area below the analysis report file list is used to display the selected analysis report content.

A successful Database Consistency Tests after Upgrade report:

```
====> Database Tests of category:'upgrade' Started at 2010-03-08 18.05 (version:R11A00).
--> Running test: Check content of state_alarms.managed_element_fk
--> Running test: Check that no RX-FAIL or TX-FAIL exists
--> Running test: Check that old sequences are removed
--> Running test: Check that unused actions from the core_security_action table are removed
--> Running test: Check that display path is populated
--> Running test: Check that pmps are removed
--> Running test: Check that core_ejb3_sequence is populated
--> Running test: Check that wmlink is removed from preferences
====> Database Tests Finished. 8 tests executed, 0 tests failed.
```

A successful Generic Database Consistency Tests report:

```
====> Database Tests of category:'consistency' Started at 2010-03-17 10:37 (version:R11A00).  
---> Running test: Check that no elements have managed_state=0 but no unmanaged_time  
---> Running test: Check that no elements have managed_state=1 but set unmanaged_time  
---> Running test: Ensure that no security templates has no active assignments, but some assignments to unmanaged elements  
====> Database Tests Finished. 3 tests executed, 0 tests failed.
```

PTP 820 NMS Initial Setup Wizard

The EMS Initial Setup Wizard contains the necessary steps needed to complete the EMS installation.

EMS System Manager opens automatically as the last step of the EMS Installer.

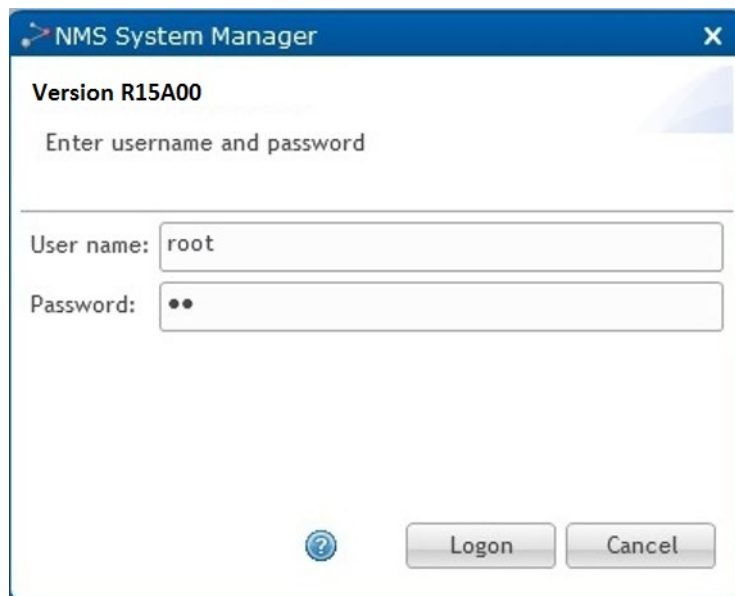
You can also start EMS Initial Setup wizard from the Administration->Database Tasks view in System Manager.

In a [High Availability](#) server setup, Initial Setup should be performed on both the Primary and the Secondary servers.

System Manager Logon

The System Manager logon window looks like this:

Figure 255 System manager logon



Default user/password for System Manager is root/pw.

Given the fact that System Manager is a web application potentially available to many people, it is important to change the root password as soon as possible to reduce the risk of unauthorised access.

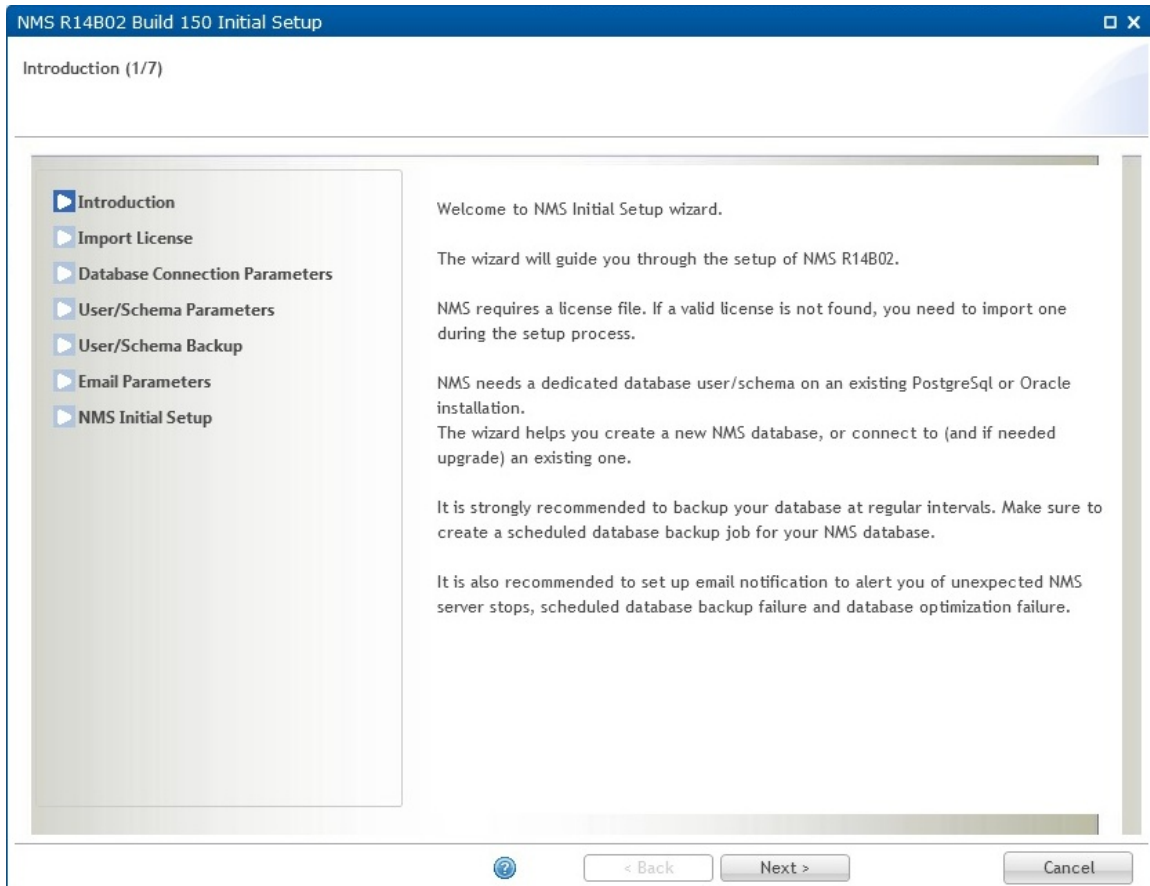
If the logon window doesn't appear properly, please press F5 in your browser to refresh the web page.

Initial Setup Wizard page 1 : Introduction

If System Manager detects that no active EMS database has been set, or that the detected database is of an older version and needs to be updated, the EMS Initial Setup Wizard will start automatically.

The first page shown is the introduction giving an overview of the wizard steps:

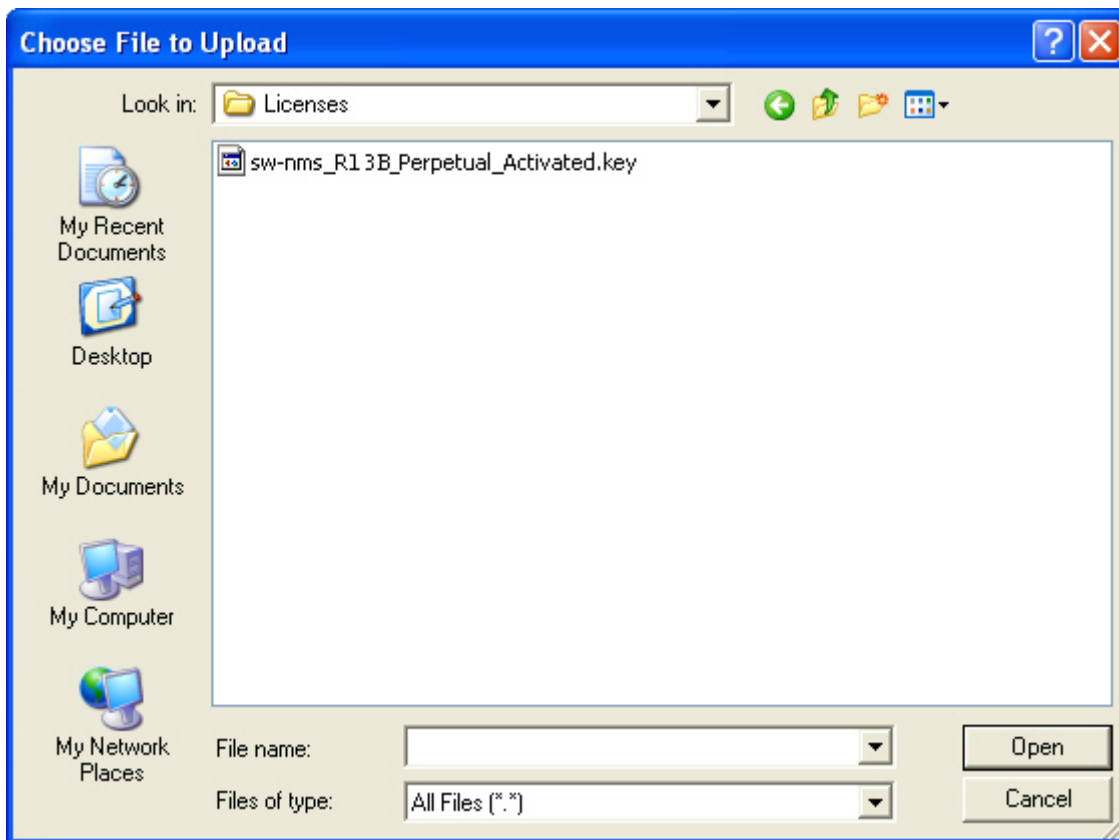
Figure 256 Initial setup wizard -1/7



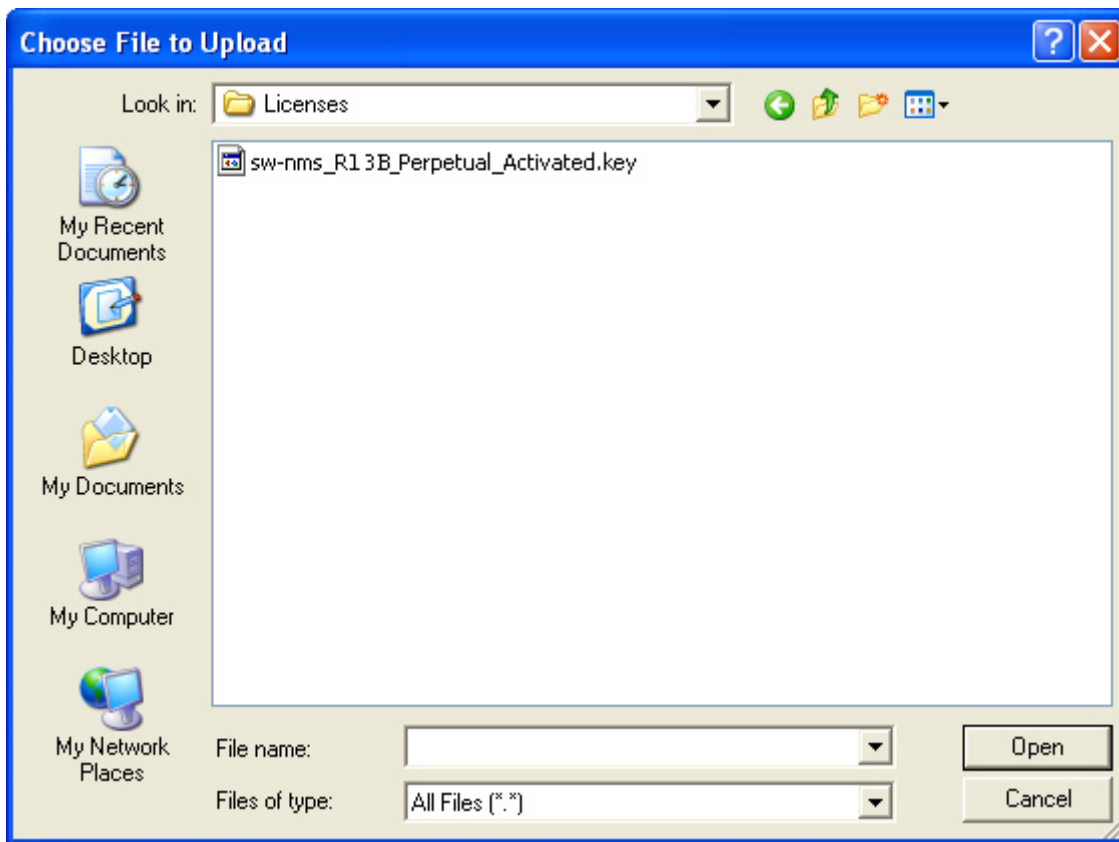
Press Next to continue the EMS Initial Setup wizard.

Initial Setup Wizard page 2: Import License

EMS requires a valid license. A new license file is required for all major EMS releases.

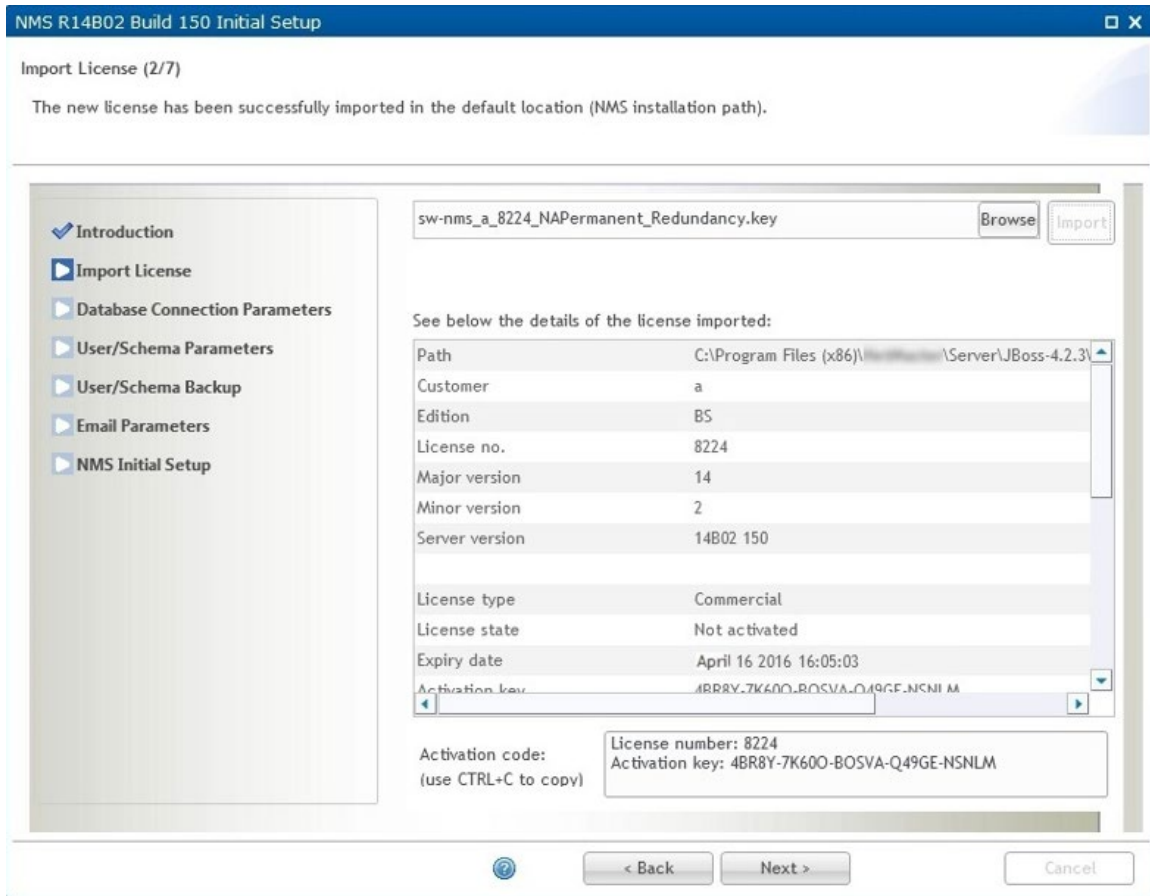
Figure 257 Initial setup wizard - 2/7

Type in the path and license file name or press Browse to locate your license file:

Figure 258 Selecting license file

Select the license file and press Open, then press the Import button to import the license into EMS:

You may have to copy the license file to a local disk for the import action to work.

Figure 259 Copying license file

Press Next to continue the EMS Initial Setup wizard.

Initial Setup Wizard page 3: Database Connection Parameters

EMS requires a dedicated database user/schema. Supported database systems are Oracle and Postgres. The database server must already be installed and properly configured, either on the same machine as the EMS server (a 1+0 configuration), or on a separate database server (a 2+0 configuration).

If you perform an upgrade from an older EMS version, the database connection parameters are filled in and disabled from editing.

Figure 260 Initial setup wizard - 3/7

NMS R14B02 Build 150 Initial Setup

Database Connection Parameters (3/7)

The fields marked with * are required.

Navigation:

- Introduction
- Import License
- Database Connection Parameters**
- User/Schema Parameters
- User/Schema Backup
- Email Parameters
- NMS Initial Setup

Database connection parameters:

Database instance name: *

Database type: * Oracle

Database server address: *

Database server port: * 1521

Database administrator user:

Username:* system

Password:*

Buttons: < Back, Next >, Cancel

If you are setting up the Primary and Secondary servers in a [High Availability](#) server setup:

- For a single Relational Database Management System (RDBMS) and single database (Postgres or Oracle) setup, enter the address of the database used by the Primary server.
- For a multiple RDBMS and single database (using Oracle RAC) setup, do the following both in the Primary and in the Secondary servers:
 - a) Set the Database instance name to the Service Name configured for RAC.
 - b) Set the Database type to Oracle.
 - c) In the Database server address field, instead of entering an address, enter the DNS address of the RAC instances (all the nodes on which RAC is installed are configured in the DNS)

The rest of settings are the same as for regular databases.

Figure 261 Initial setup wizard - 3/7

NMS R14802 Build 217 Initial Setup

Database Connection Parameters (3/7)

The fields marked with * are required.

Database connection parameters:

Database instance name: * racorcl.ceragon.com

Database type: * Oracle

Database server address: * vnvrac-scan.ceragon.com

Database server port: * 1521

Database administrator user:

Username: * system

Password: *

< Back Next > Cancel

All parameters are mandatory:

Name	Explanation
Database instance name	Name of a database instance.
Database type	Either Oracle or Postgres.
Database server address	IP address or hostname for the database server. Use localhost for a 1+0 configuration.
Database server port	Tcp port for the database. Default 1521 for Oracle, 5432 for Postgres.

Please notice that in order to do the initial setup, you need to have a Database administrator user with sufficient privileges.

Press Next to continue the EMS Initial Setup wizard.

Initial Setup Wizard page 4: User/Schema Parameters

The Initial Setup wizard can create a new Oracle user or Postgres schema for EMS. It is also possible to connect to an existing EMS database. If the existing database is not of current version, the wizard will upgrade it to the latest version.

If you perform an upgrade from an older EMS version, the old EMS database settings are filled in and disabled from editing.

When setting up the Secondary server in a [High Availability](#) server setup, select to use an Existing database user/schema, and enter the user/schema username and password you specified during Primary server setup.

Figure 262 Initial setup wizard - 4/7

All shown parameters are mandatory:

Name	Explanation
Username	Name of your EMS user/schema.
Password	Password for your EMS user/schema.

Name	Explanation
Confirm password	Confirm the password. This field is hidden when connecting to an existing EMS database.

Press Next to continue the EMS Initial Setup wizard.

Initial Setup Wizard page 5 : User/Schema Backup

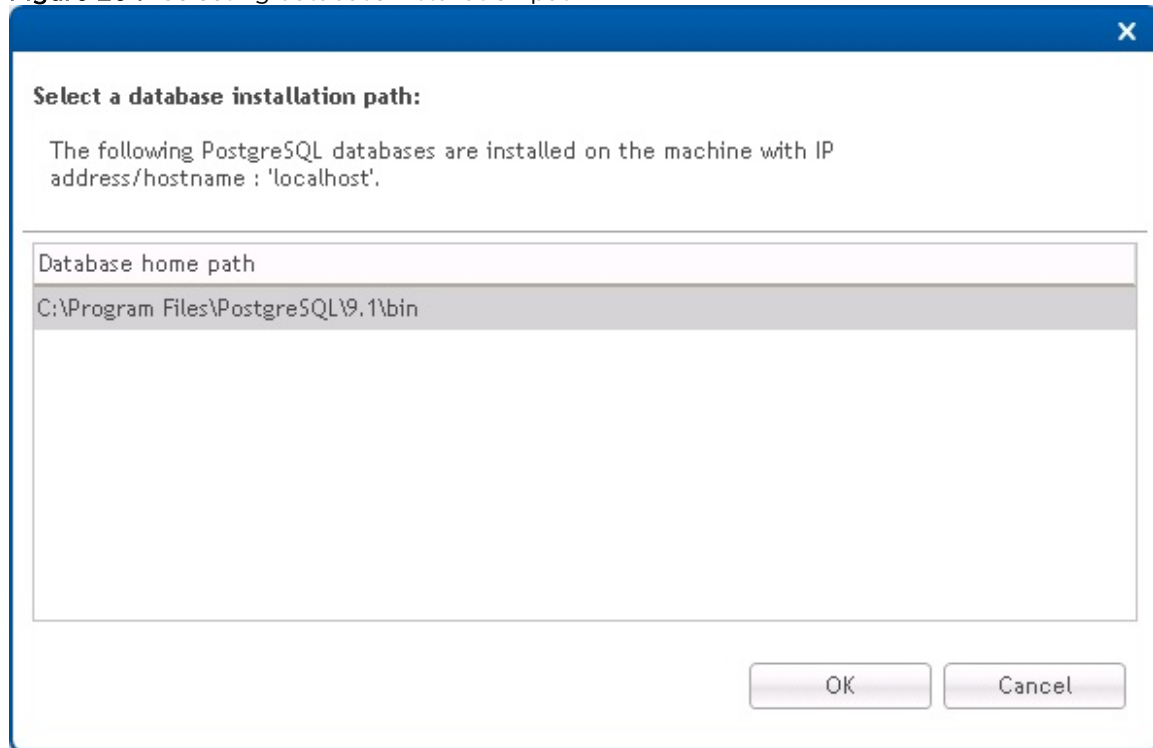
It is recommended to back up the EMS database at regular intervals. You can set up periodic backup using System Manager.

The Backup before upgrade section is shown only when the selected EMS database requires upgrade from an older version. The backup is placed in the location specified in the [Database view](#) available from the Settings menu. The default location is C:\PTP820NMS\Backup\Database.

Figure 263 Initial setup wizard - 5/7

The Database Install Path is the database server path to the tools System Manager needs to run backup and restore operations. The tools in question are exp.exe and imp.exe for Oracle and pg_dump and pg_restore for Postgres.

Press the Select Database Path to allow System Manager to try to find the Database Install Path automatically:

Figure 264 Selecting database installation path

If System Manager fails to locate the correct path for you, you have to supply the correct path yourself.

You can check the Skip schedule backup check box if you don't want to set up periodic backup. You can schedule periodic backup later if desired by using the Backup Active User/Schema or Backup User/Schema wizards.

To initiate periodic backup, leave the Skip schedule backup check box unchecked and adjust the start time and backup interval as desired. Be aware that in a 2+0 configuration (EMS server and EMS database on separate machines) the backup files will be stored on both servers. The backup files are zipped to reduce disk space consumption, but you should make sure to select a file system with enough free disk space to hold the backup files.

It is possible to change the backup file storage location on the EMS server. It is also possible to configure number of days to keep the scheduled database backups. Both settings are found in the Database settings in System Manager.

If periodic backup is enabled, it is recommended to also enable deletion of old backup files to prevent the file system from filling up. Note that the deletion of old backup files in a 2+0 configuration is performed on the database server as well as on the EMS server.

When the settings are configured as desired, press Next to continue the EMS Initial Setup wizard.

If System Manager on the database server is not compatible with the System Manager on the EMS server, the backup will be aborted with an error message. If so, you should upgrade the outdated System Manager, and then rerun the EMS Initial Setup wizard.

Initial Setup Wizard page 6: Email Parameters

It is possible to set up System Manager to send email notification in case of:

- Periodic backup failure
- EMS server unexpected shutdown
- Database optimization failure

In order to make use of the email notification feature, you need an SMTP server in your network.

Figure 265 Initial setup wizard - 6/7

If you don't want to make use of the email notification feature, you can check the Skip email notification setup check box.

If you want email notification, you need to fill in the following settings:

Name	Explanation
Mail Server Address	IP address or hostname to your SMTP server.

Mail Server Port	SMTP port on your mail server. Default is 25.
From Address	The email address that will appear as the email sender. Be aware that no validation is performed whether this is a real email address or not.
To Address	Email recipient. May be a list of email addresses, separated by comma or semicolon.
Username	Username for Mail Server Authentication.
Password	Password for Mail Server Authentication.

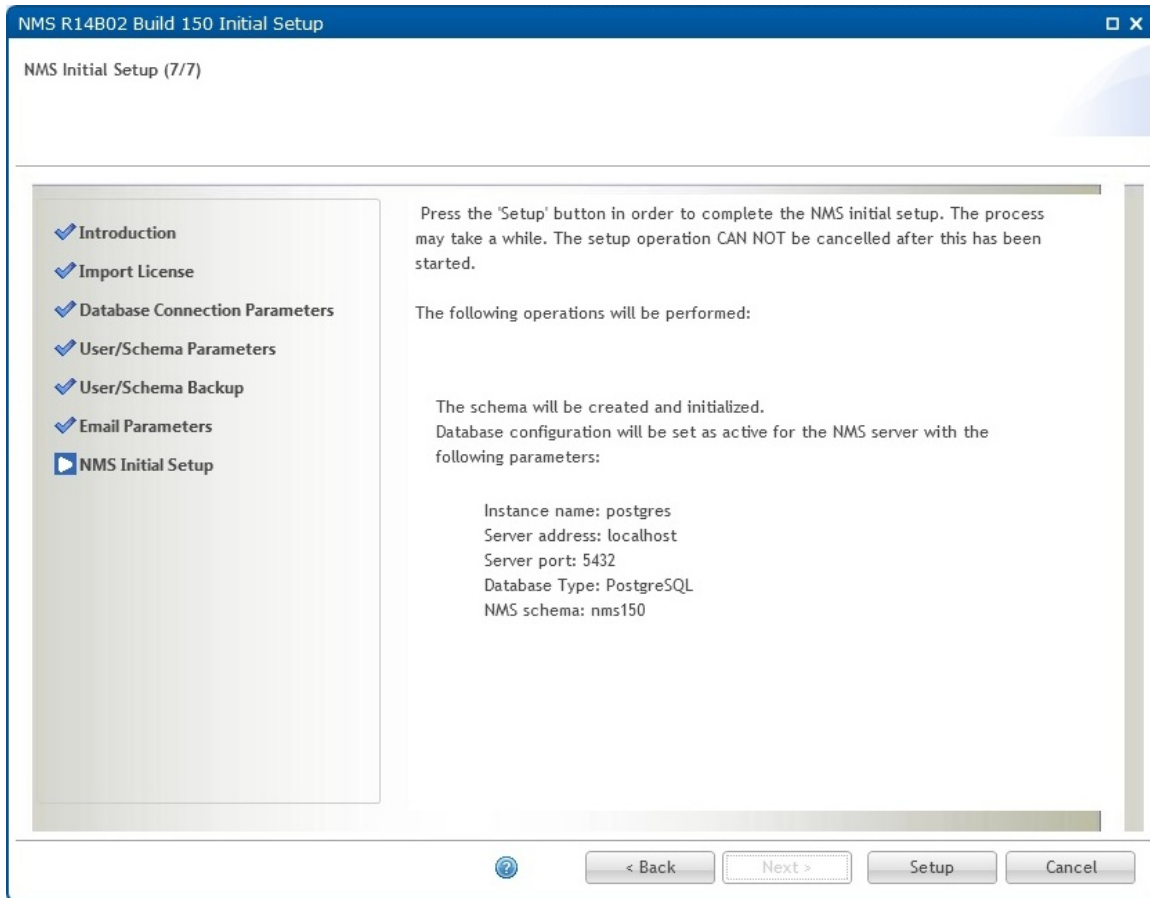
Press the Send Test Email button to send a test email to verify that the email notification settings are correct.

Press Next to continue the EMS Initial Setup wizard.

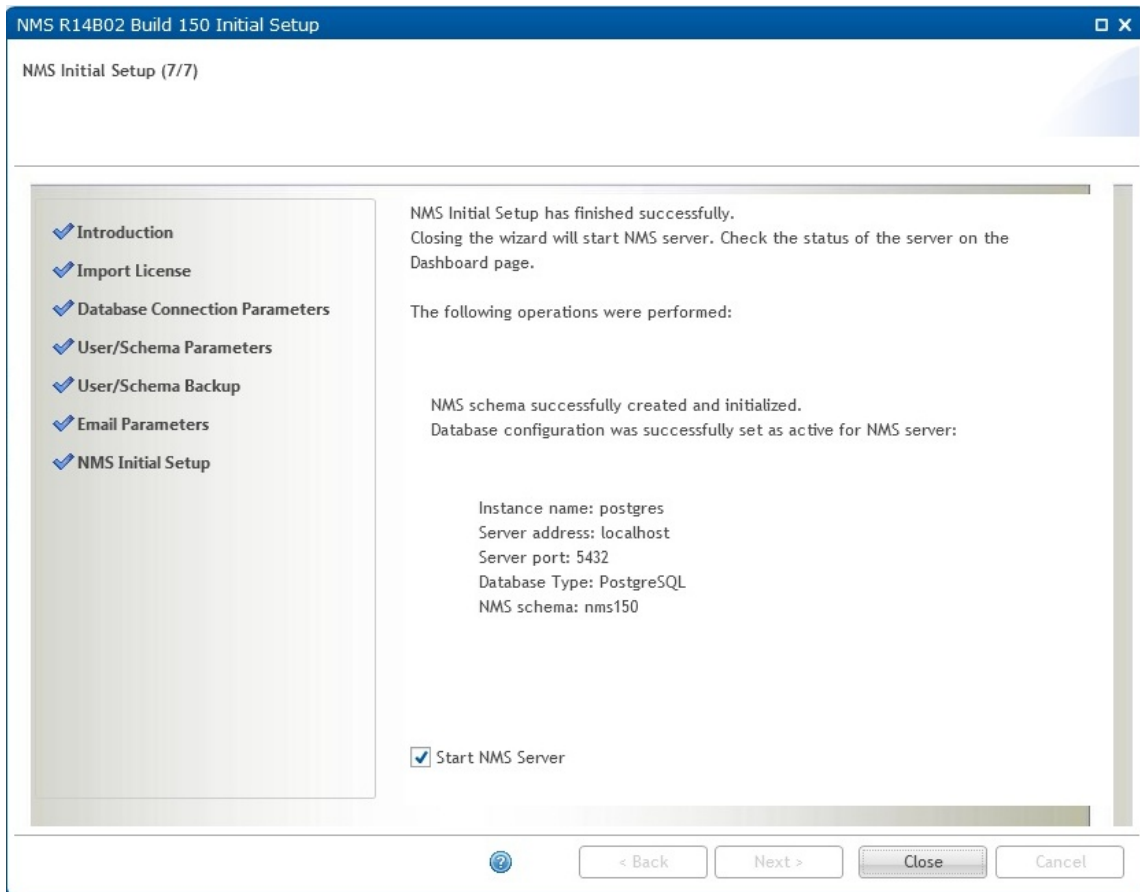
Initial Setup Wizard page 7: EMS Initial Setup

This is the final page in the Initial Setup Wizard.

Verify the operation list summary and press Setup to initiate the setup process.

Figure 266 Initial setup wizard - 7/7

When the setup process is complete, the following page is displayed:

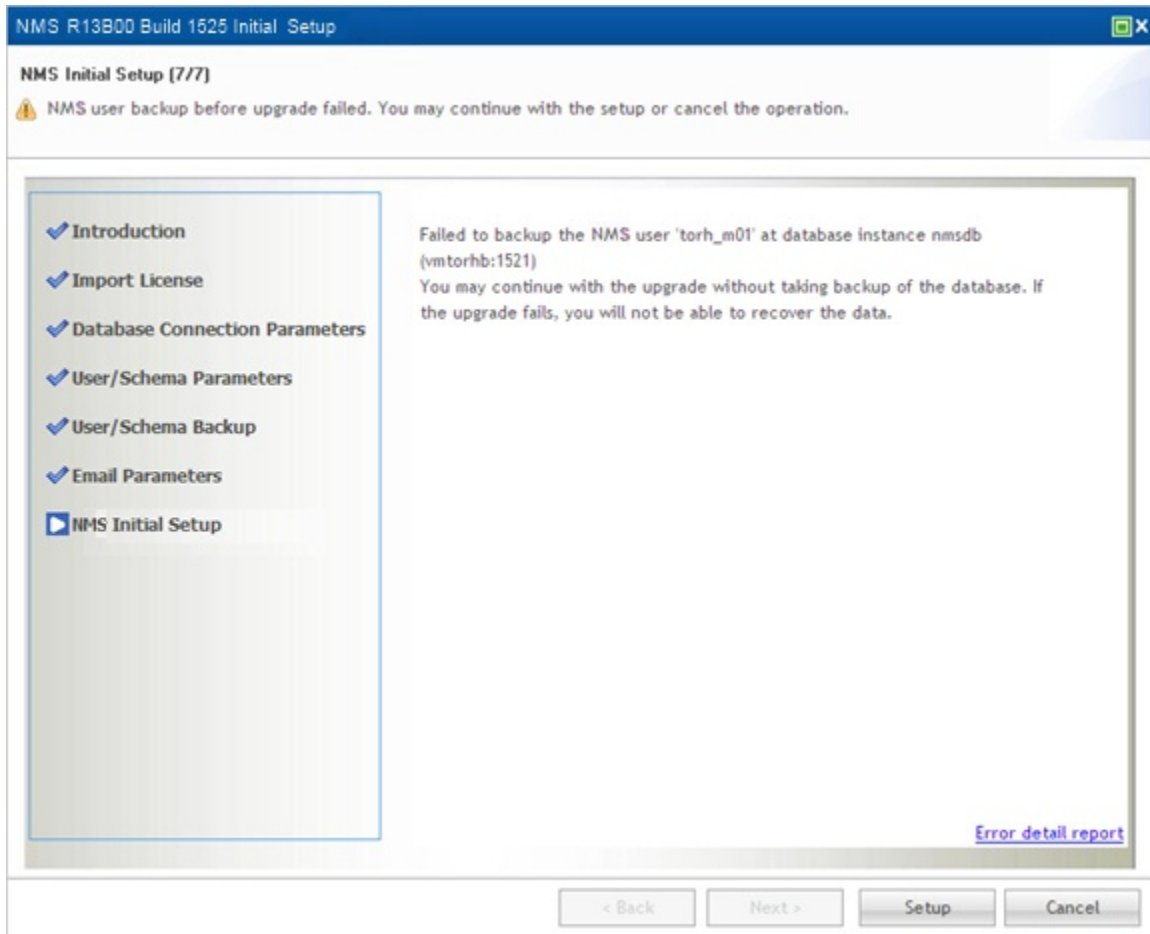
Figure 267 Initial setup wizard - 7/7 : start EMS server

Uncheck the Start PTP 820NMS Server check box if you don't want to start the NMS server. For example, if you are configuring a [High Availability](#) server setup, first complete [High Availability](#) configuration before starting the Primary and Secondary servers.

Press Close to complete the EMS Initial Setup wizard.

Error situations and recovery - Backup before upgrade fails

If backup before upgrade fails, it is still possible to continue database upgrade process:

Figure 268 Initial setup wizard - 7/7 : backup before upgrade fails

Press Error detail report link to see error details:

Figure 269 Error details reports

The dialog box, titled "Error Details Report" with a close button (X), displays the following information:

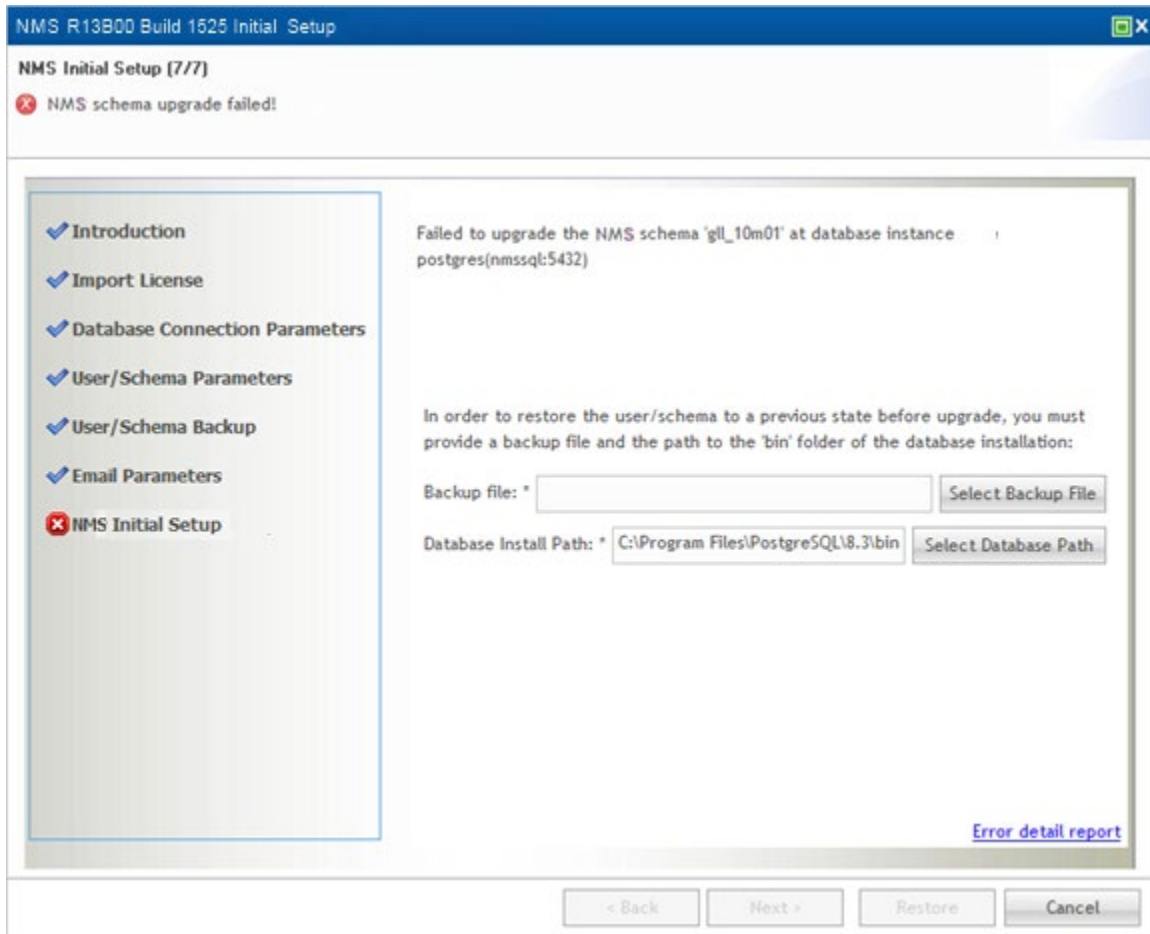
- Start Date:** 12 Mar 2010 10:40:42
- End Date:** 12 Mar 2010 10:40:44
- Task Type:** Backup NMS database
- Status:** Failed
- Subtask:** Backup database (selected from a dropdown menu)
- Subtask status:** Failed
- Description:** Backup NMS database
- Details:**
 - Backing up NMS database 'torh_m01' at nmsdb (vmtorhb)
 - Task failed because an exception occurred.
 - java.net.ConnectException: Connection refused: connect
 - If the database server is located on a separate machine than NMS server, check if System Manager on the database server is up and running.

An "OK" button is located at the bottom right of the dialog box.

Make sure to take a backup of your database manually, then press Setup to continue upgrade.

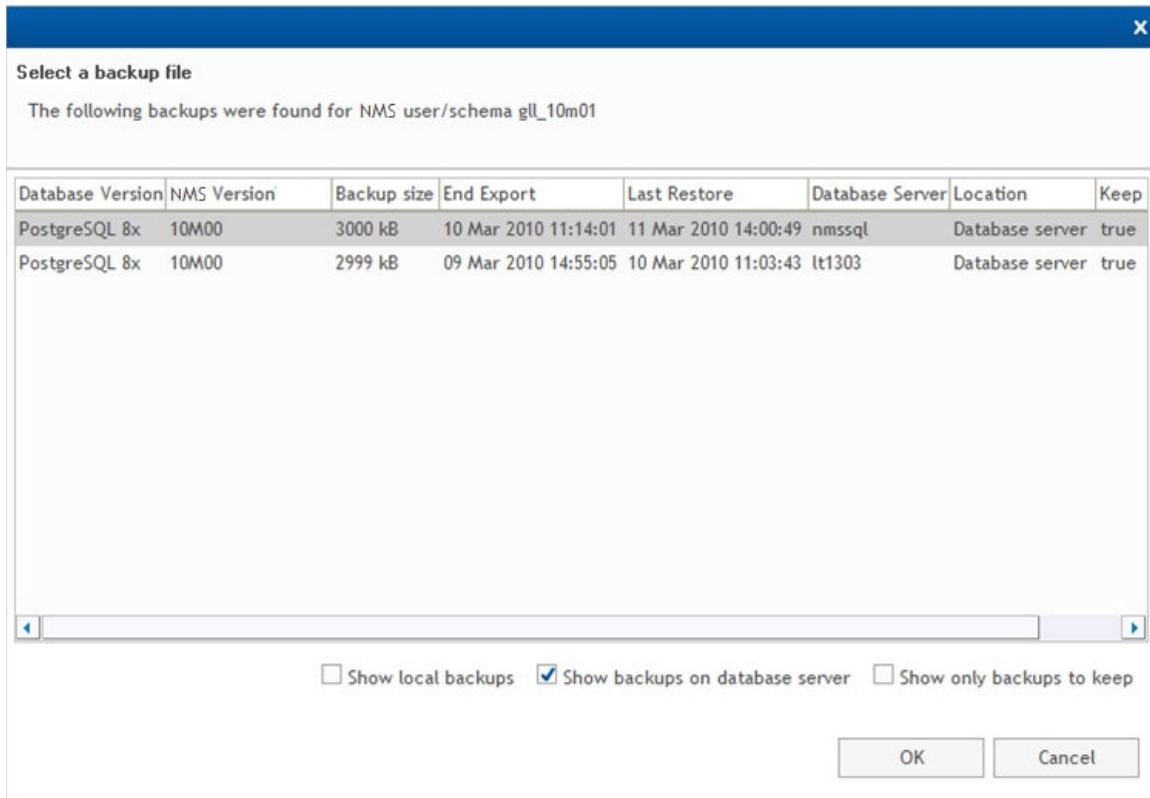
Error situations and recovery - Upgrade of database failed

If upgrade process completes with failure, the following page is displayed, giving the option to restore the possible corrupt database:

Figure 270 Initial setup wizard - 7/7: upgrade of database failed

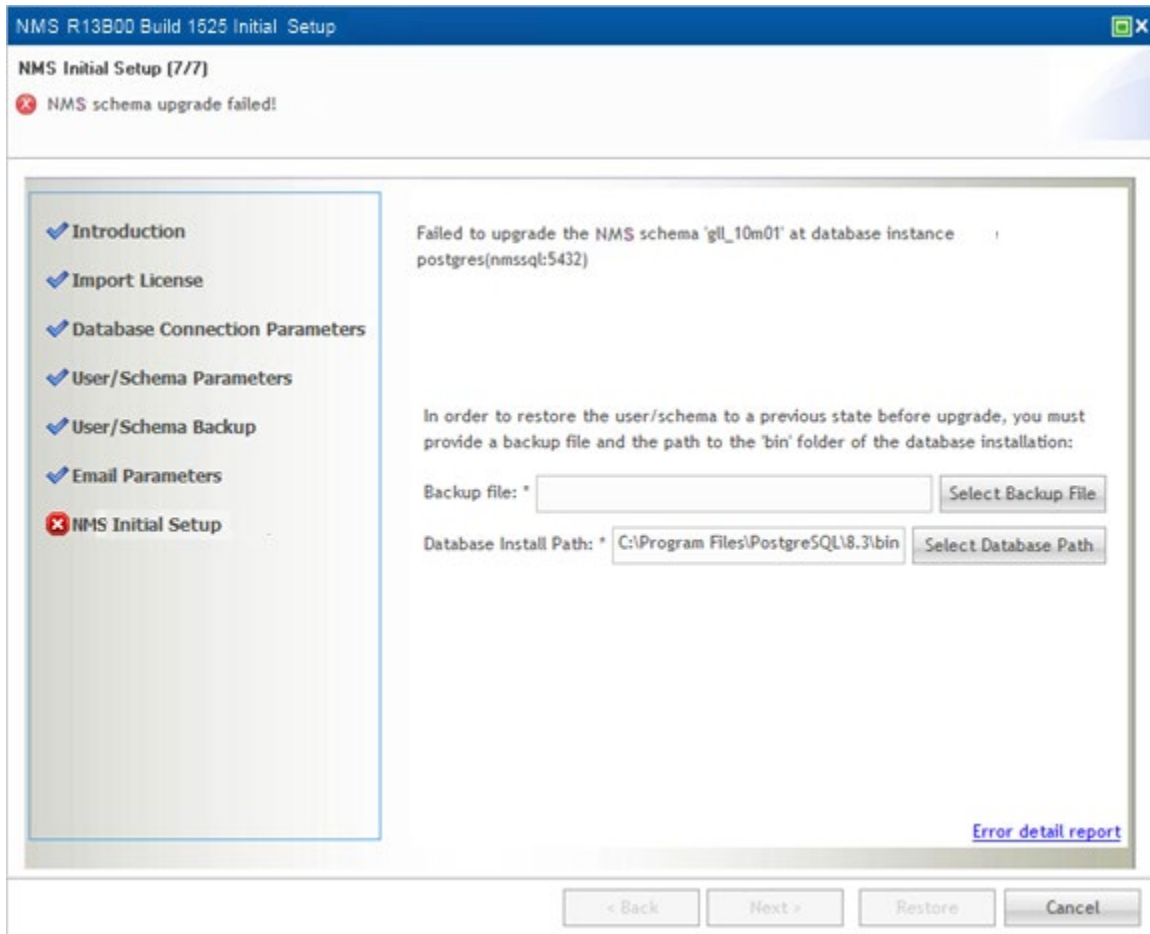
Check the Error detail report to see what caused the upgrade to fail.

An upgrade failure may leave your database in a corrupt state. It is recommended to restore it to a consistent state. Press the Select Backup File button to select an existing database backup. If a backup before upgrade was requested and was successfully performed, it should appear as the newest entry in the backup list:

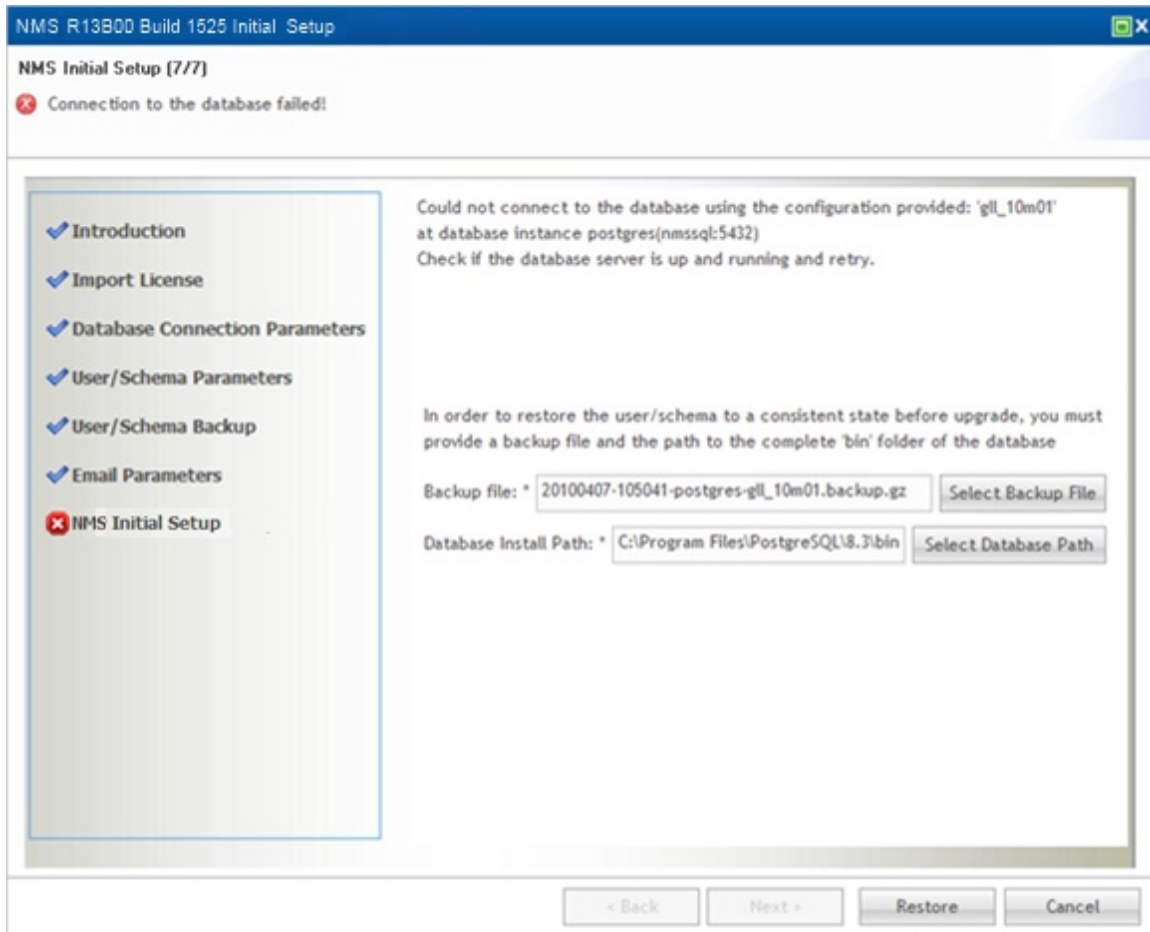
Figure 271 Selecting backup file

Select a backup file and press OK to return to the EMS Initial Setup wizard page.

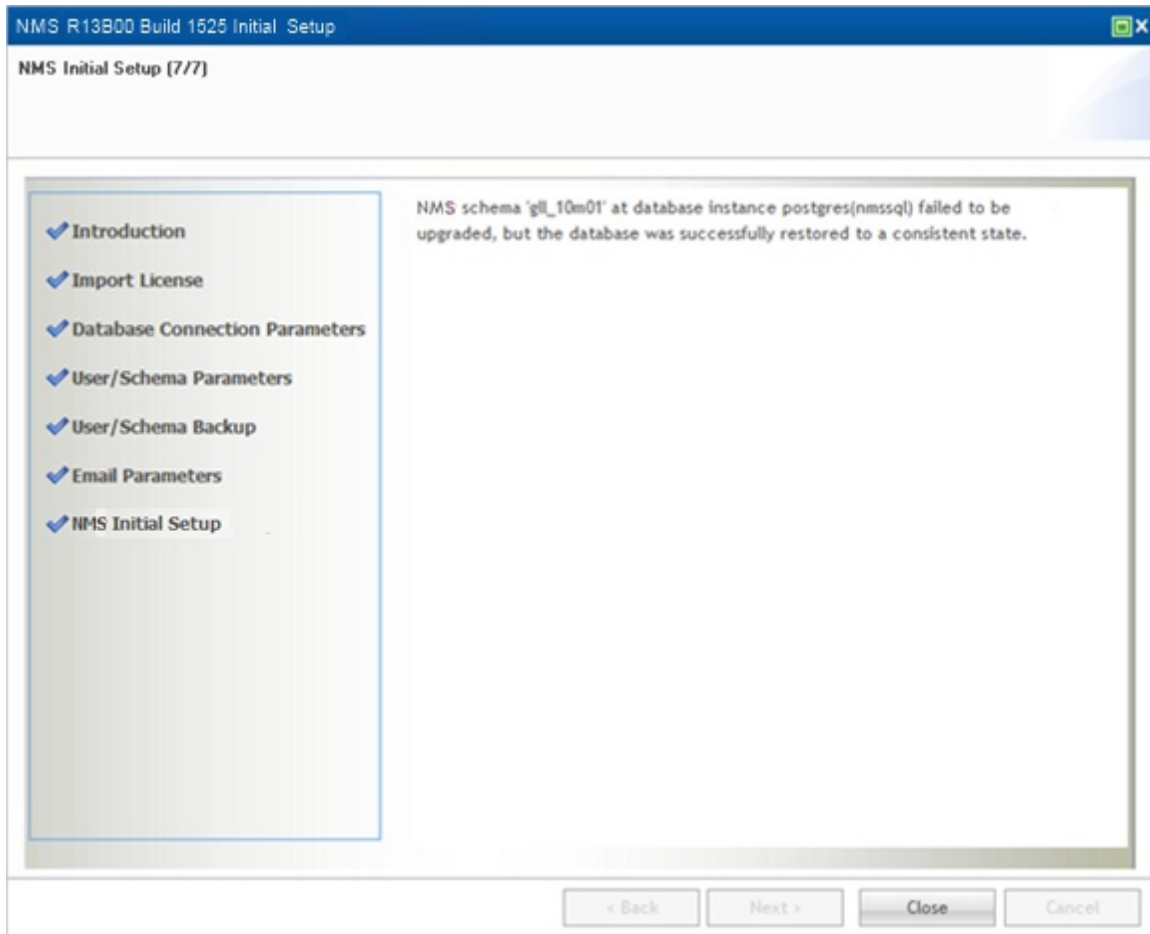
Press Restore button to restore the selected database backup:

Figure 272 Initial setup wizard - 7/7 : Schema upgrade failed

If the restore fails as well, you may cancel the wizard or retry the restore operation:

Figure 273 Initial setup wizard - 7/7 : Connection to the database failed

If restore completes successfully, the following page appears:

Figure 274 Initial setup wizard - 7/7

Press Close to close the Upgrade User/Schema wizard.

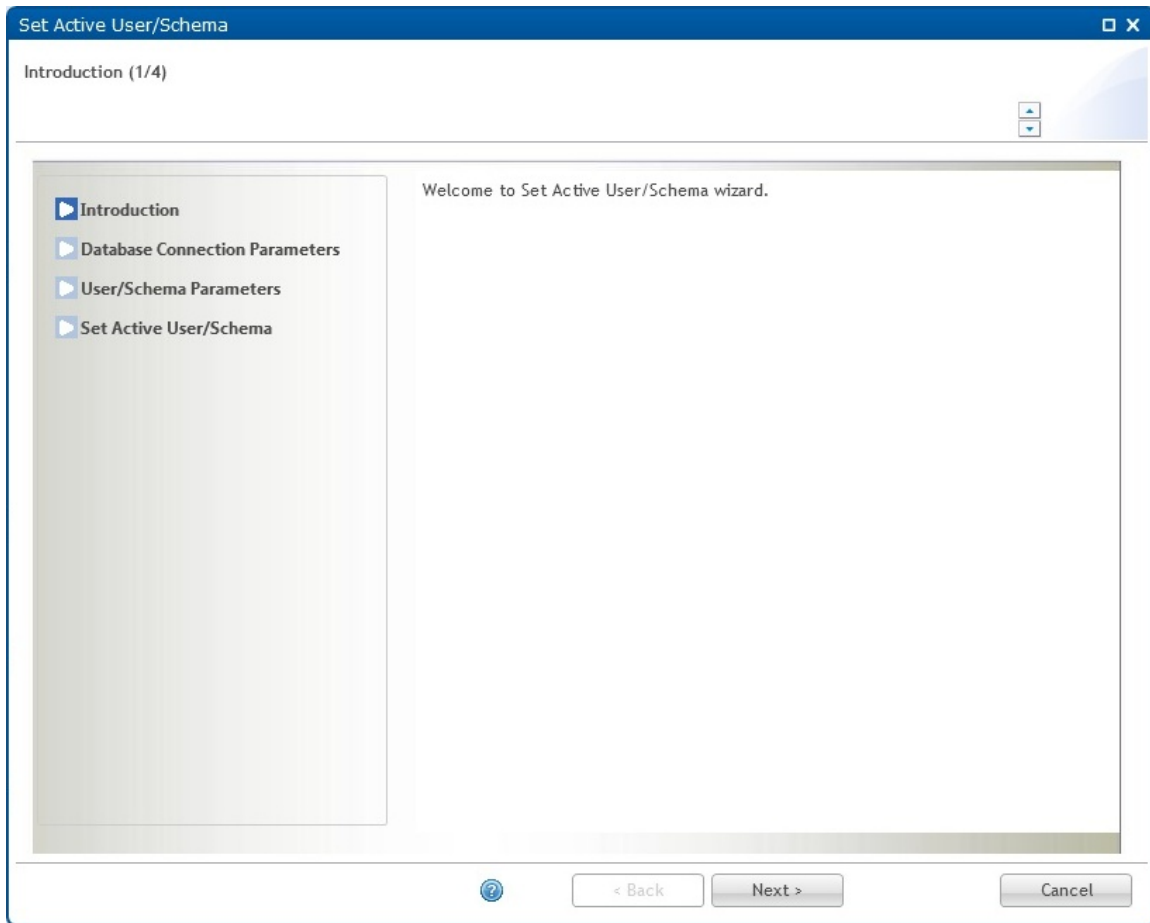
Set Active User/Schema Wizard

This wizard allows you to connect your EMS server to another EMS database.

Open the Set Active User/Schema wizard from the **Administration->Database Tasks** view in System Manager.

If the new user or schema is of an old version, you must first upgrade it to current version using the Upgrade User/Schema wizard.

Note that in a [High Availability](#) server setup, both the Primary and Secondary servers must point to the same database. Therefore, if you want to connect to another PTP 820 NMS database, you must run this wizard for both the Primary and the Secondary servers.

Set Active Wizard page 1: Introduction**Figure 275** Set Active Wizard page 1 : Introduction

Press Next to continue the Set Active User/Schema wizard.

Set Active Wizard page 2 : Database Connection Parameters

Specify the database connection parameters for the EMS database you want to set active.

Figure 276 Set Active Wizard page 2 : Database Connection Parameters

Set Active User/Schema

Database Connection Parameters (2/4)

Please review or change the default configuration below.
The fields marked with * are required.

☒ Introduction
☐ Database Connection Parameters
☐ User/Schema Parameters
☐ Set Active User/Schema

Database connection parameters:

Database instance name: * postgres

Database type: * PostgreSQL

Database server address: * localhost

Database server port: * 5432

Database administrator user:

Username: * postgres

Password: *

Select Existing Parameters

? < Back Next > Cancel

Press Select Existing Parameters button to select database connection parameters already defined in System Manager:

Figure 277 Selecting exiting database connection

Instance Name	Server Name/Address	Server Port	Database Type	Administrator User
postgres	nmssql	5432	PostgreSQL	postgres
nmsora	nmsora	1521	Oracle	system

OK Cancel

If the desired parameters are not present in the list, you need to fill in the parameters manually.

All parameters are mandatory:

Name	Explanation
Database instance name	Name of a database instance.
Database type	Either Oracle or Postgres.
Database server address	IP address or hostname for the database server. Use localhost for a 1+0 configuration.
Database server port	Tcp port for the database. Default 1521 for Oracle, 5432 for Postgres.
Username	The database system user. Saved for later use.
Password	Password for the database system user.

Please notice that in order to set active, you need to have a Database administrator user with sufficient privileges.

Press Next to continue the Set Active User/Schema wizard.

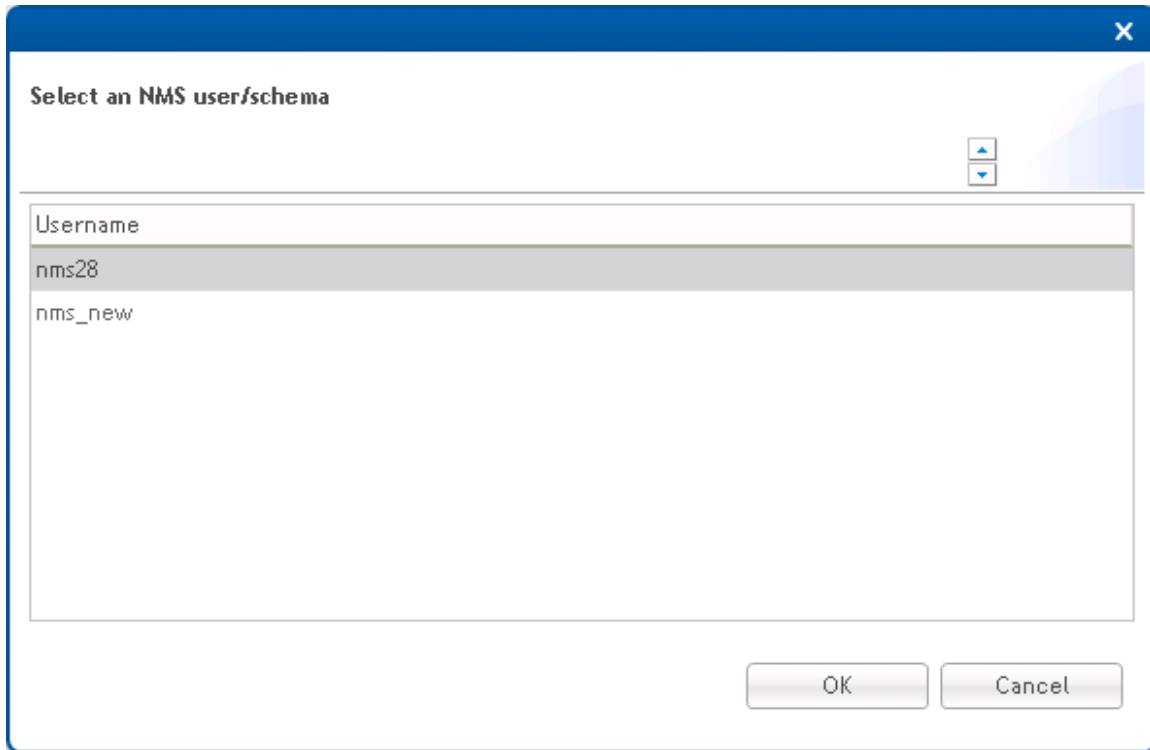
Set Active Wizard page 3: User/Schema Parameters

Specify the Oracle user or Postgres schema you want to set as active EMS database configuration.

Figure 278 Set Active Wizard page 3 : User/Schema Parameters

The screenshot shows a window titled "Set Active User/Schema" with a close button in the top right corner. The window has a blue header bar. Below the header, the title "User/Schema Parameters (3/4)" is displayed. A message states: "Please review or change the default configuration below. The fields marked with * are required." On the left side, there is a vertical list of steps: "Introduction" (checked), "Database Connection Parameters" (checked), "User/Schema Parameters" (selected with a blue square icon), and "Set Active User/Schema" (indicated by a right-pointing triangle). The main area contains the text: "Enter the NMS database schema name and password or use the button below to select existing parameters from System Manager configuration files." Below this text are two input fields: "Username:*" with the value "nms150" and "Password:*" with masked characters "••". A button labeled "Select Existing Parameters" is located at the bottom right of the main area. At the bottom of the window, there is a navigation bar with a help icon (question mark in a circle), "< Back", "Next >", and "Cancel" buttons.

Press Select Existing Parameters button to select existing parameters already defined in System Manager:

Figure 279 Selecting user/schema

If the desired parameters are not present in the list, you have to fill in the parameters manually.

Both parameters are mandatory:

Name	Explanation
Username	Name of desired EMS user/schema
Password	Password for the desired EMS user/schema

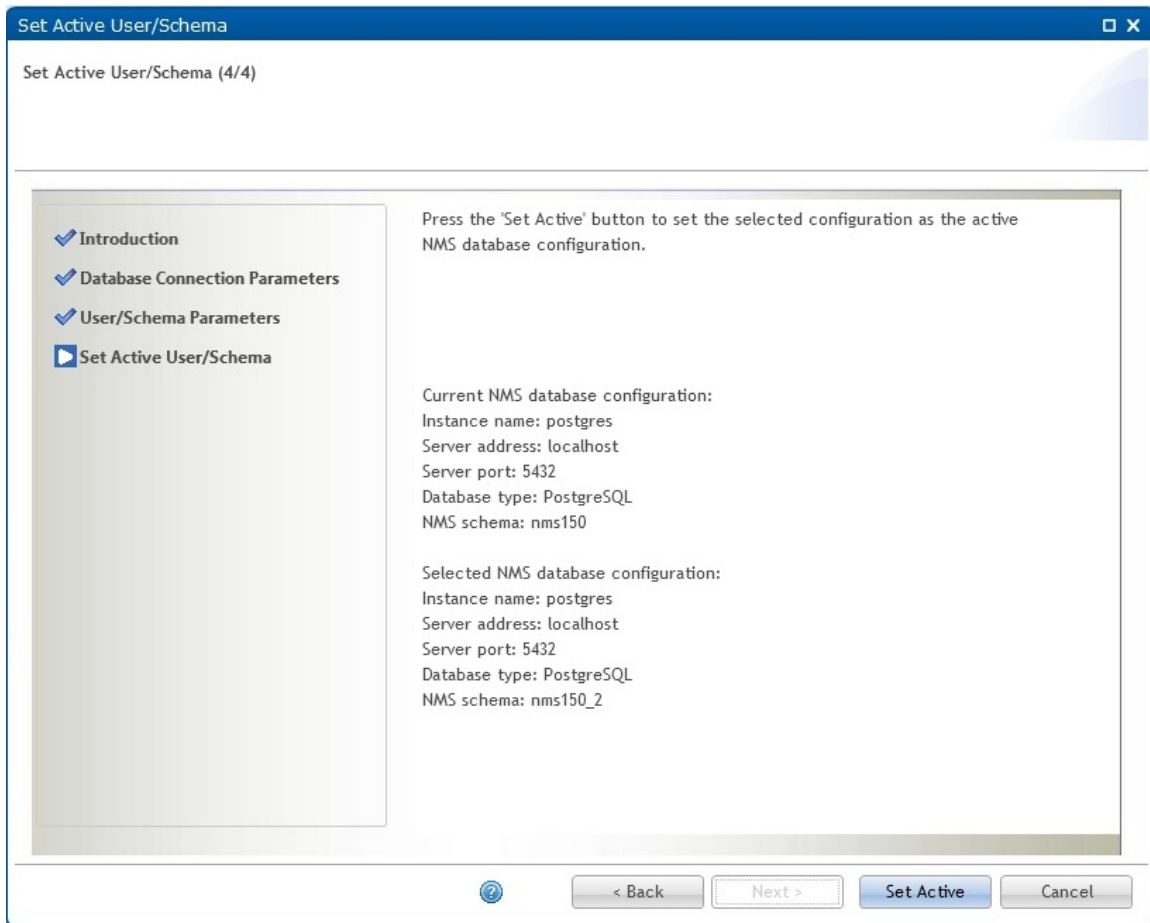
Press Next to continue the Set Active User/Schema wizard.

Set Active Wizard page 4: Set Active

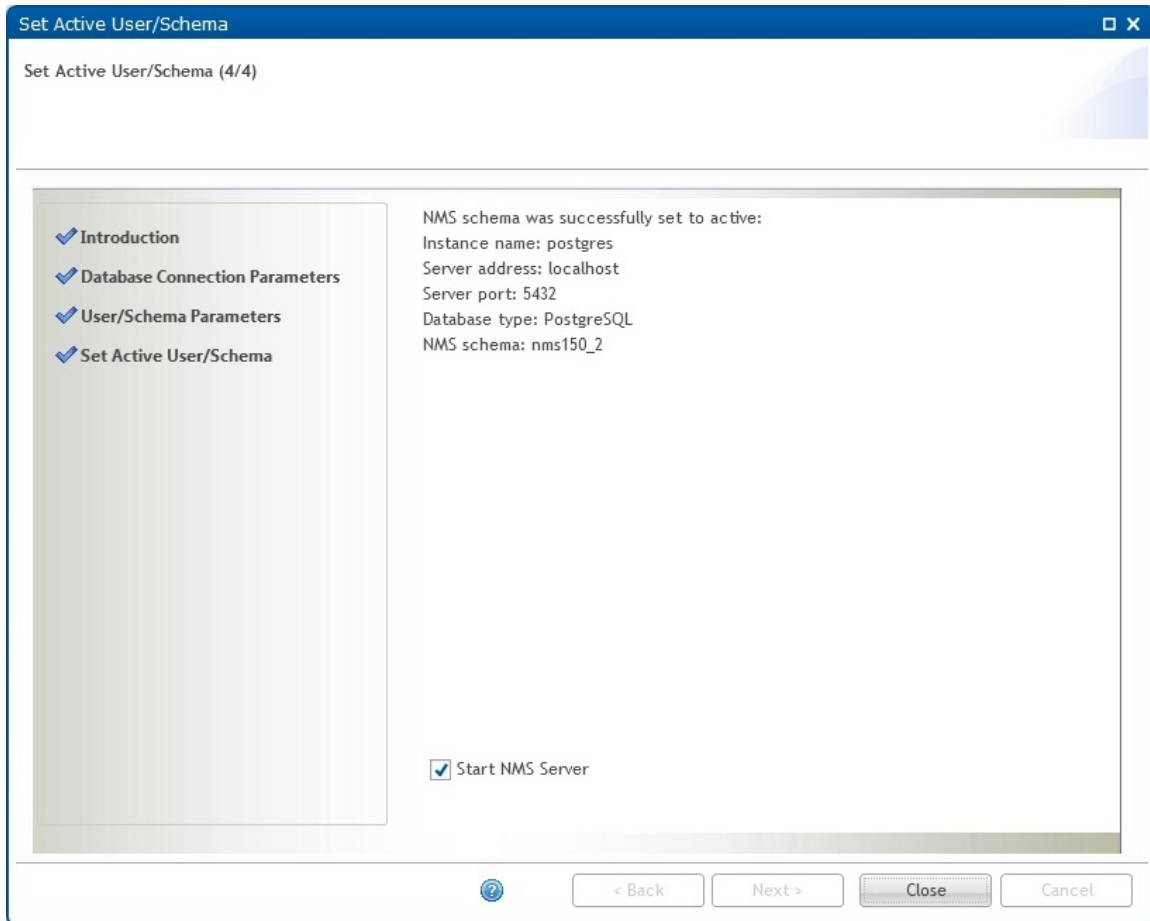
This is the final page in the Set Active User/Schema Wizard.

Verify the operation list summary and press Set to initiate the set active process.

If the EMS server runs it will be stopped. It is also recommended to close all EMS clients.

Figure 280 Set Active Wizard page 4 : Set Active

When the set active process is complete, the following page is displayed:

Figure 281 Set active user/schema

Uncheck the Start PTP 820 NMS Server check box if you don't want to start the PTP820NMS server.

In a [High Availability](#) server setup, uncheck the Start EMS Server check box both for the Primary server and the Secondary server. After you finish setting the active user/schema in both servers, you can start the servers from the System Manager.

Press Close to complete the Set Active User/Schema wizard.

Create User/Schema Wizard

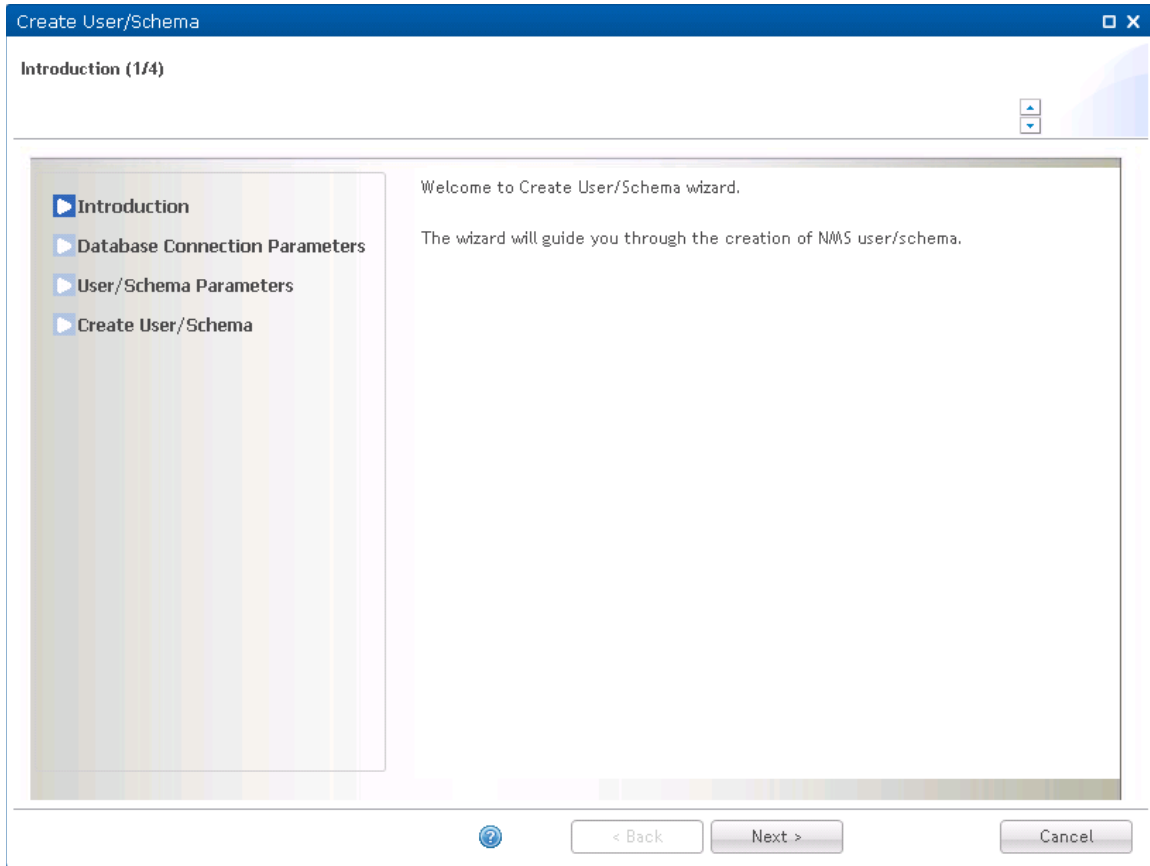
This wizard allows you to create a new Oracle user or Postgres schema and prepare it for EMS use.

Open the Create User/Schema wizard from the **Administration->Database Tasks** view in System Manager.

Create Wizard page 1: Introduction

Start page for Create User/Schema wizard.

Figure 282 Create Wizard page 1 : Introduction



Press Next to continue the Create User/Schema wizard.

Create Wizard page 2: Database Connection Parameters

EMS requires a dedicated database user/schema. Supported database systems are Oracle and Postgres. The database server must already be installed and properly configured, either on the same machine as the EMS server (a 1+0 configuration), or on a separate database server (a 2+0 configuration).

Figure 283 Create Wizard page 2 : Database Connection Parameters

Create User/Schema

Database Connection Parameters (2/4)

Please review or change the default configuration below.
The fields marked with * are required.

Database connection parameters:

Database instance name: * postgres

Database type: * PostgreSQL

Database server address: * localhost

Database server port: * 5432

Database administrator user:

Username: * postgres

Password: *

Select Existing Parameters

< Back Next > Cancel

Press Select Existing Parameters button to select database connection parameters already defined in System Manager:

Figure 284 Selecting a database connection

Instance Name	Server Name/Address	Server Port	Database Type	Administrator User
postgres	nmssql	5432	PostgreSQL	postgres
nmsora	nmsora	1521	Oracle	system

OK Cancel

If the desired parameters are not present in the list, you have to fill in the parameters manually.

All parameters are mandatory:

Name	Explanation
Database instance name	Name of a database instance.
Database type	Either Oracle or Postgres.
Database server address	IP address or hostname for the database server. Use localhost for a 1+0 configuration.
Database server port	Tcp port for the database. Default 1521 for Oracle, 5432 for Postgres.
Username	The database system user needed to create the EMS user/schema.
Password	Password for the database system user.

Please notice that in order to create, you need to have a Database administrator user with sufficient privileges.

Press Next to continue the Create User/Schema wizard.

Create Wizard page 3: User/Schema Parameters

Specify the new Oracle user or Postgres schema name to be created and prepared for EMS use:

Figure 285 Create Wizard page 3 : User/Schema Parameters

All parameters are mandatory:

Name	Explanation
Username	Name of new EMS user/schema
Password	Password for the new EMS user/schema
Confirm password	Confirm the password

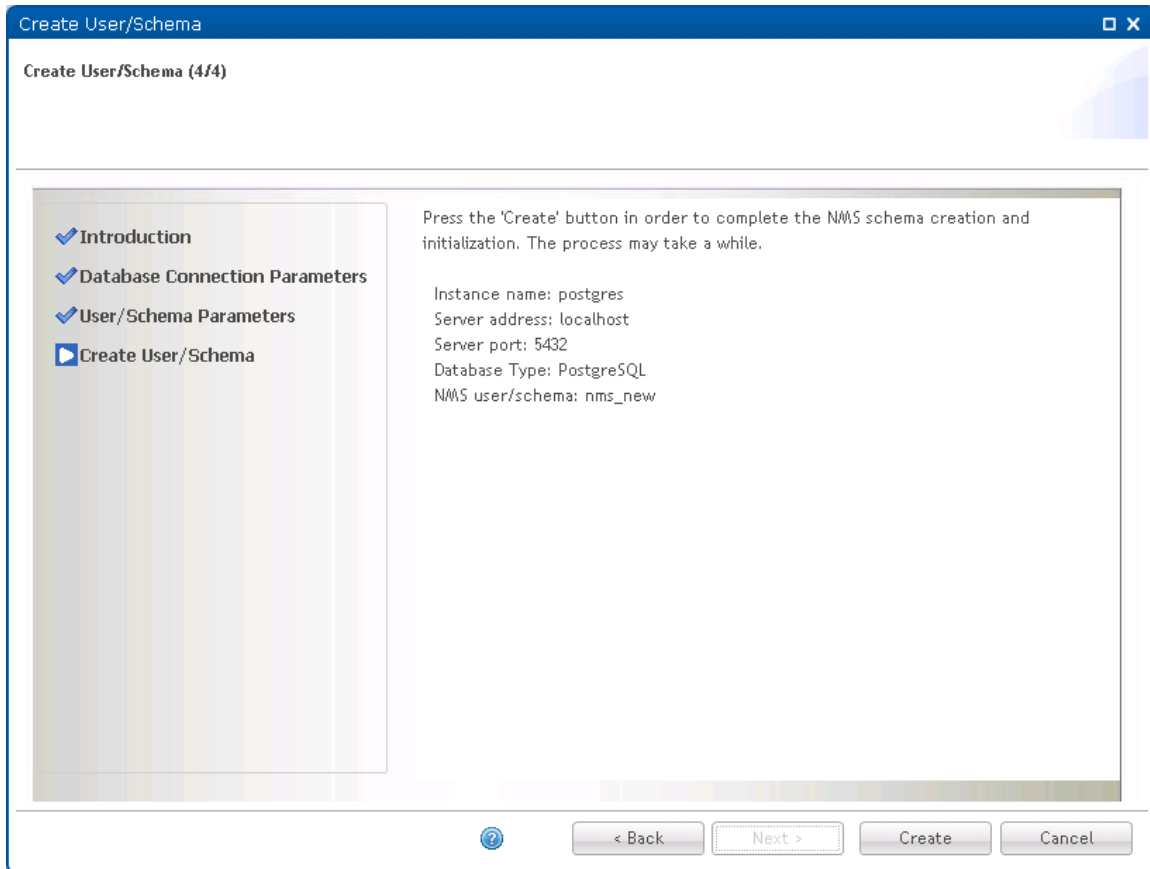
Press Next to continue the Create User/Schema wizard.

Create Wizard page 4: Create User/Schema

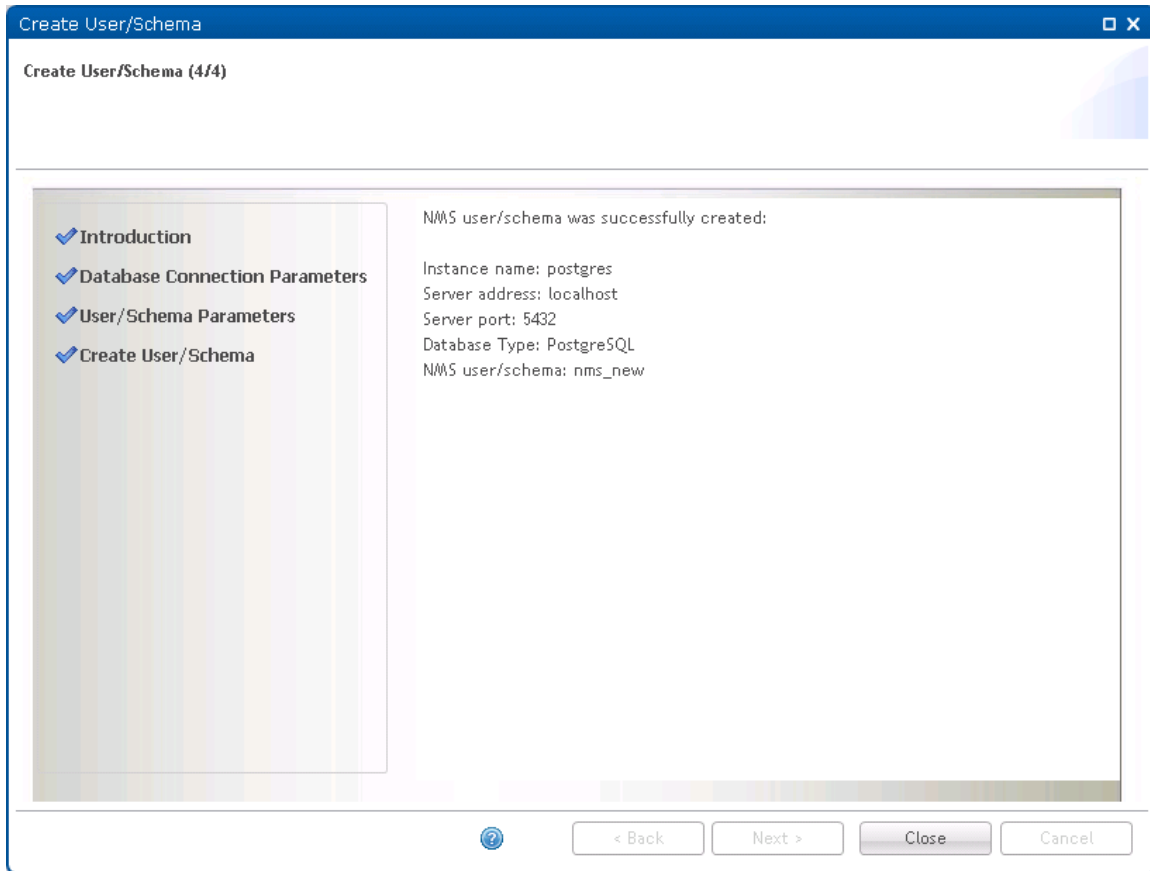
This is the final page in the Create User/Schema Wizard.

Verify the operation list summary and press Create to initiate the create process.

Figure 286 Create Wizard page 4 : Create User/Schema



When the create process is complete, the following page is displayed:

Figure 287 Create Wizard page 4 : creation process complete

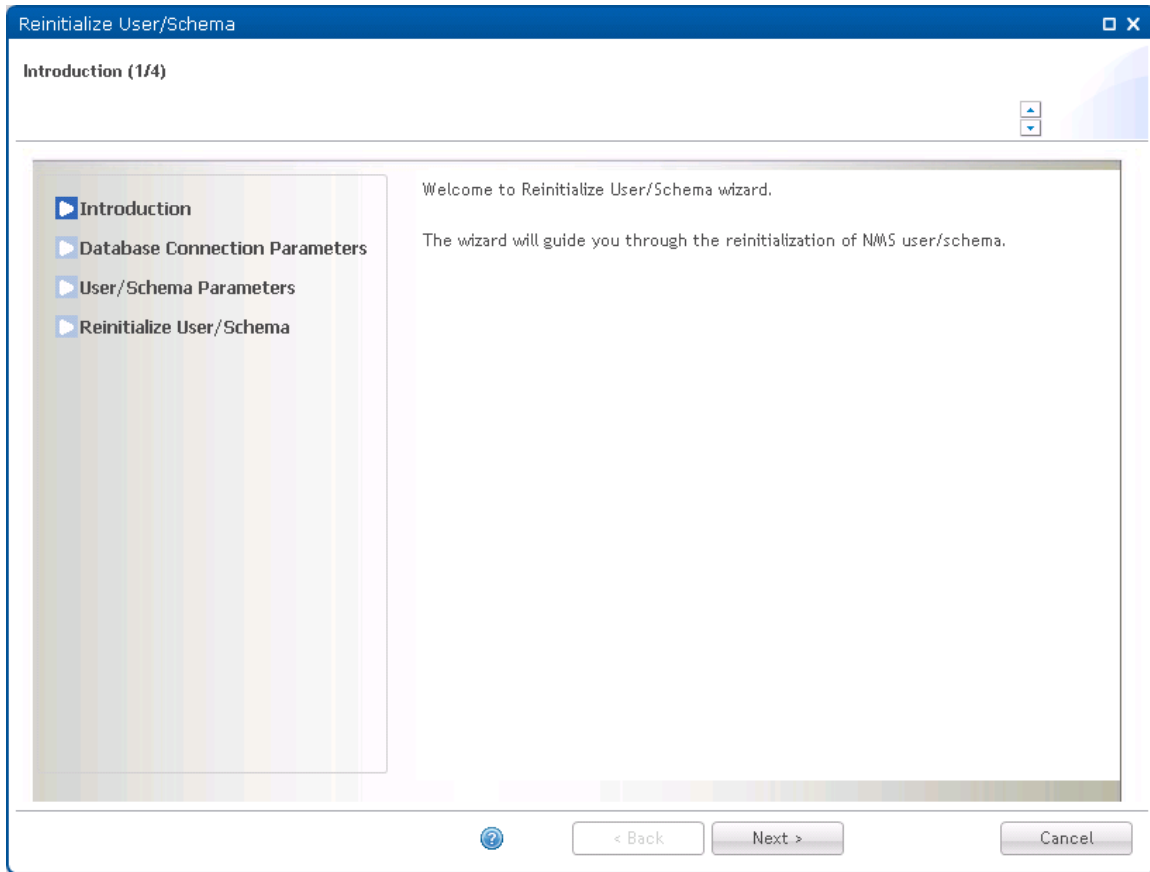
Press Close to complete the Create User/Schema wizard.

Reinitialize User/Schema Wizard

This wizard allows you to reinitialize an existing Oracle user or Postgres schema. All existing data is lost and the database is prepared as for a fresh EMS installation.

Open the Reinitialize User/Schema wizard from the **Administration->Database Tasks** view in System Manager.

If the selected user or schema is of an old version, you must first upgrade it to current version using the Upgrade User/Schema wizard.

Reinitialize Wizard page 1: Introduction**Figure 288** Reinitialize Wizard page 1 : Introduction

Press Next to continue the Reinitialize User/Schema wizard.

Reinitialize Wizard page 2: Database Connection Parameters

Specify the database connection parameters for the EMS database you want to reinitialize.

Figure 289 Reinitialize Wizard page 2 : Database Connection Parameters

The screenshot shows the 'Reinitialize User/Schema' wizard, specifically the 'Database Connection Parameters (2/4)' page. The window title is 'Reinitialize User/Schema'. Below the title bar, the page is titled 'Database Connection Parameters (2/4)' and includes a note: 'Please review or change the default configuration below. The fields marked with * are required.' On the left, a sidebar contains four steps: 'Introduction' (checked), 'Database Connection Parameters' (selected), 'User/Schema Parameters', and 'Reinitialize User/Schema'. The main area is titled 'Database connection parameters:' and contains the following fields: 'Database instance name: *' with the value 'postgres', 'Database type: *' with a dropdown menu showing 'PostgreSQL', 'Database server address: *' with the value 'localhost', and 'Database server port: *' with the value '5432'. Below these is the 'Database administrator user:' section, which includes 'Username: *' with the value 'postgres' and 'Password: *' with a masked password field. A 'Select Existing Parameters' button is located at the bottom right of the main area. At the bottom of the window, there is a question mark icon, '< Back' and 'Next >' buttons, and a 'Cancel' button.

Reinitialize User/Schema

Database Connection Parameters (2/4)

Please review or change the default configuration below.
The fields marked with * are required.

Database connection parameters:

Database instance name: * postgres

Database type: * PostgreSQL

Database server address: * localhost

Database server port: * 5432

Database administrator user:

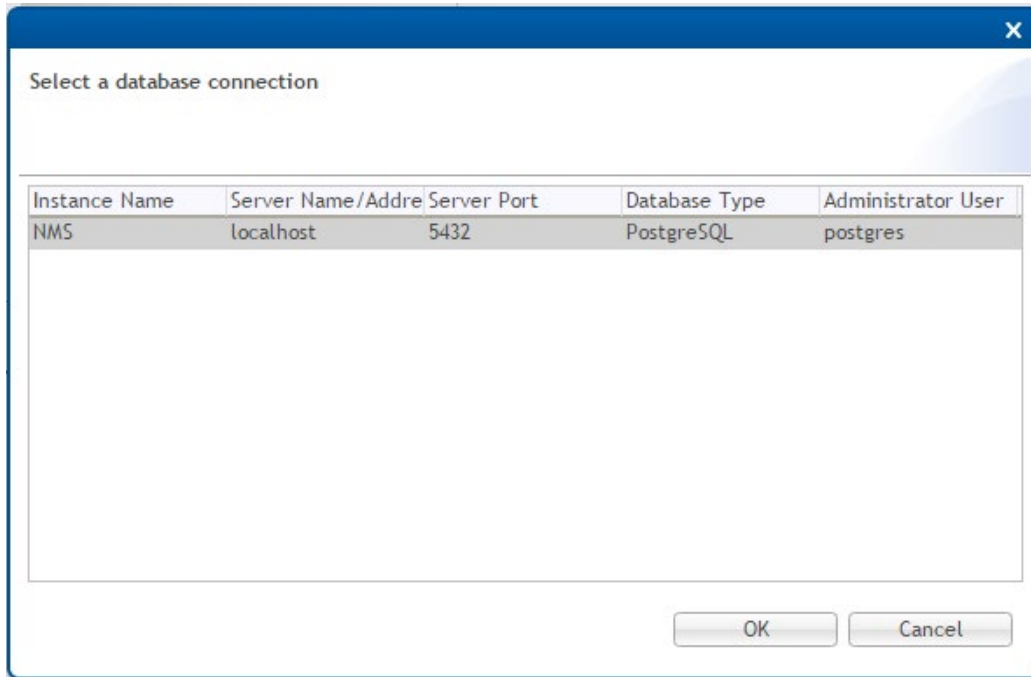
Username: * postgres

Password: *

Select Existing Parameters

< Back Next > Cancel

Press Select Existing Parameters button to select database connection parameters already defined in System Manager:

Figure 290 Selecting a database connection

If the desired parameters are not present in the list, you need to fill in the parameters manually.

All parameters are mandatory:

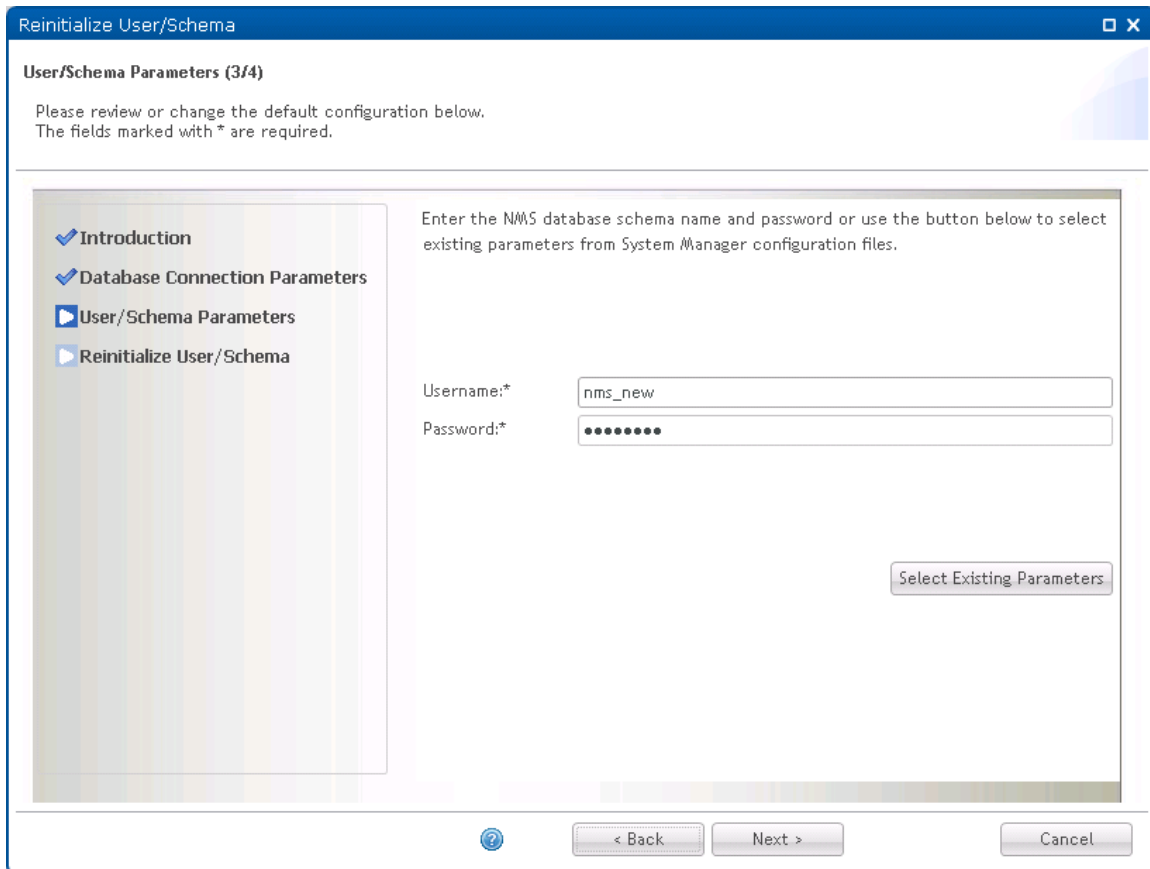
Name	Explanation
Database instance name	Name of a database instance.
Database type	Either Oracle or Postgres.
Database server address	IP address or hostname for the database server. Use localhost for a 1+0 configuration.
Database server port	Tcp port for the database. Default 1521 for Oracle, 5432 for Postgres.
Username	The database system user needed to reinitialize the EMS user/schema.
Password	Password for the database system user.

Press Next to continue the Reinitialize User/Schema wizard.

Reinitialize Wizard page 3: User/Schema Parameters

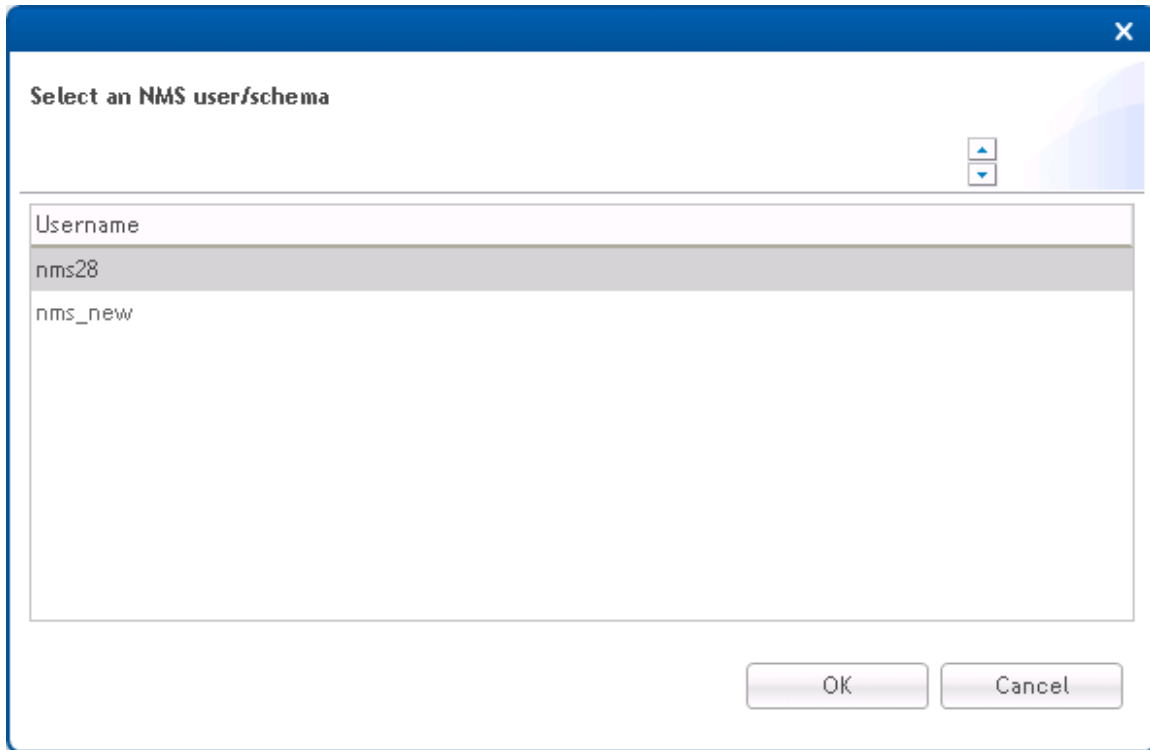
Specify the Oracle user or Postgres schema you want to reinitialize.

Figure 291 Reinitialize Wizard page 3 : User/Schema Parameters



The image shows a screenshot of the 'Reinitialize User/Schema' wizard, page 3 of 4. The window title is 'Reinitialize User/Schema'. The page is titled 'User/Schema Parameters (3/4)'. Below the title, it says 'Please review or change the default configuration below. The fields marked with * are required.' On the left, there is a navigation pane with four items: 'Introduction' (checked), 'Database Connection Parameters' (checked), 'User/Schema Parameters' (selected), and 'Reinitialize User/Schema'. The main area contains the text 'Enter the NMS database schema name and password or use the button below to select existing parameters from System Manager configuration files.' Below this text are two input fields: 'Username:*' with the value 'nms_new' and 'Password:*' with masked characters. At the bottom right of the main area is a button labeled 'Select Existing Parameters'. At the bottom of the window are three buttons: a help button (question mark icon), '< Back', and 'Next >', and a 'Cancel' button on the far right.

Press Select Existing Parameters button to select existing parameters already defined in System Manager:

Figure 292 Selecting user/schema

If the desired parameters are not present in the list, you have to fill in the parameters manually.

Both parameters are mandatory:

Name	Explanation
Username	Name of desired EMS user/schema
Password	Password for the desired EMS user/schema

Press Next to continue the Reinitialize User/Schema wizard.

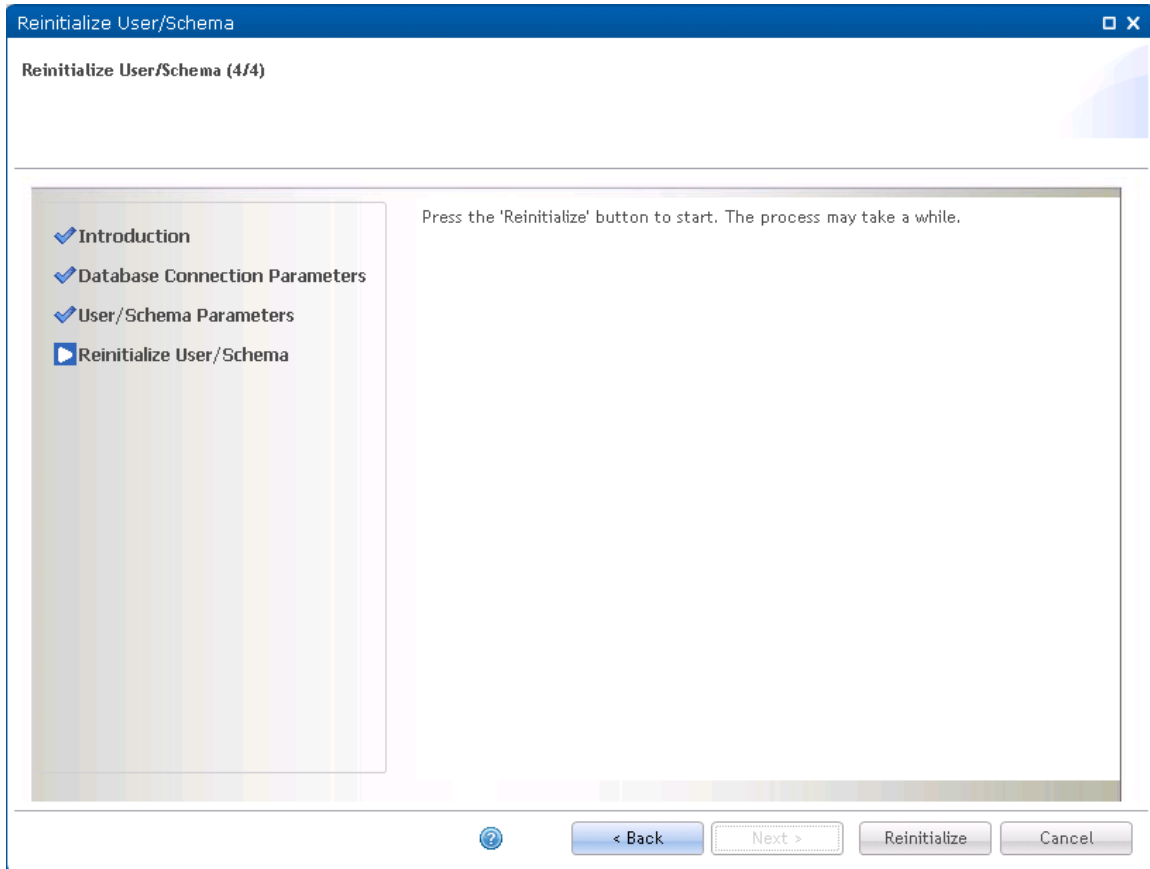
Reinitialize Wizard page 4: Reinitialize User/Schema

This is the final page in the Reinitialize User/Schema Wizard.

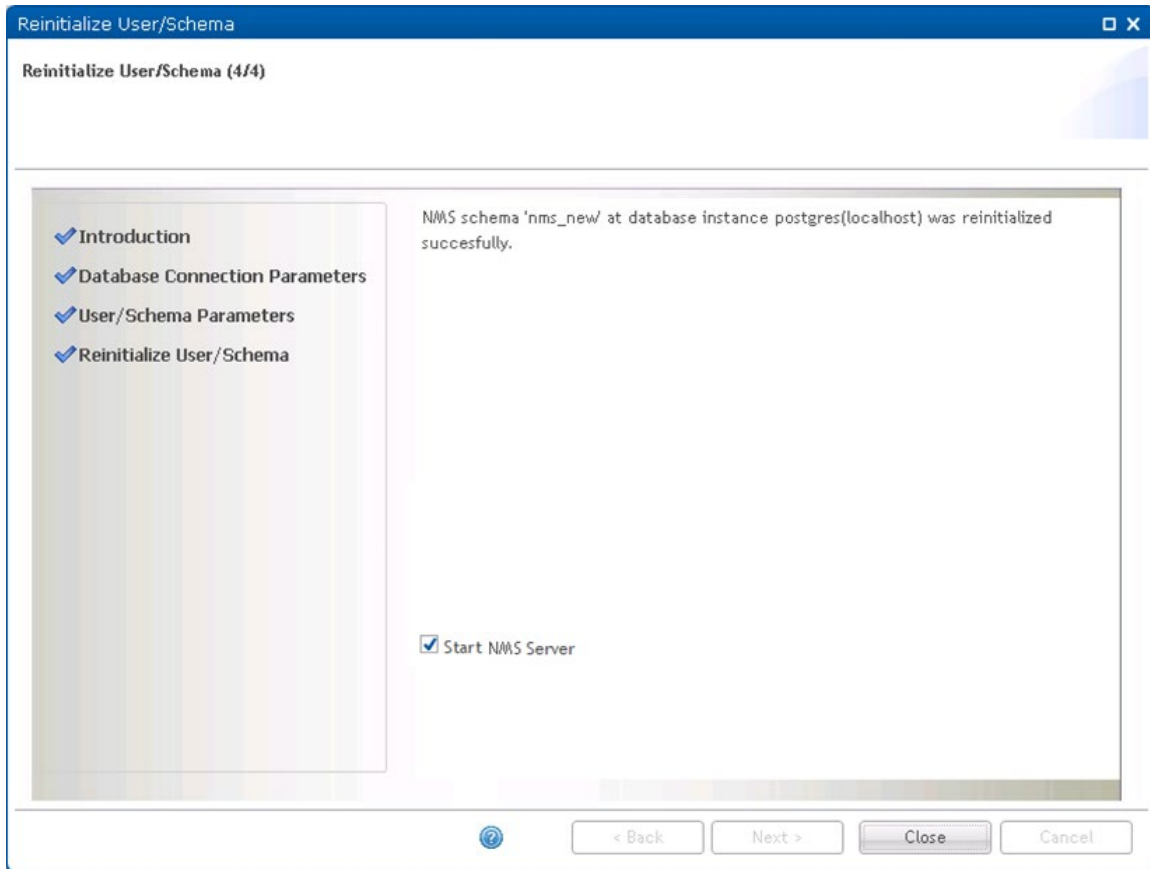
Confirm by checking the checkbox and press Reinitialize to initiate the reinitialize process.

If you are reinitializing the active schema, the EMS server will be stopped if running. It is also recommended to close all EMS clients.

Figure 293 Reinitialize Wizard page 4 : Reinitialize User/Schema

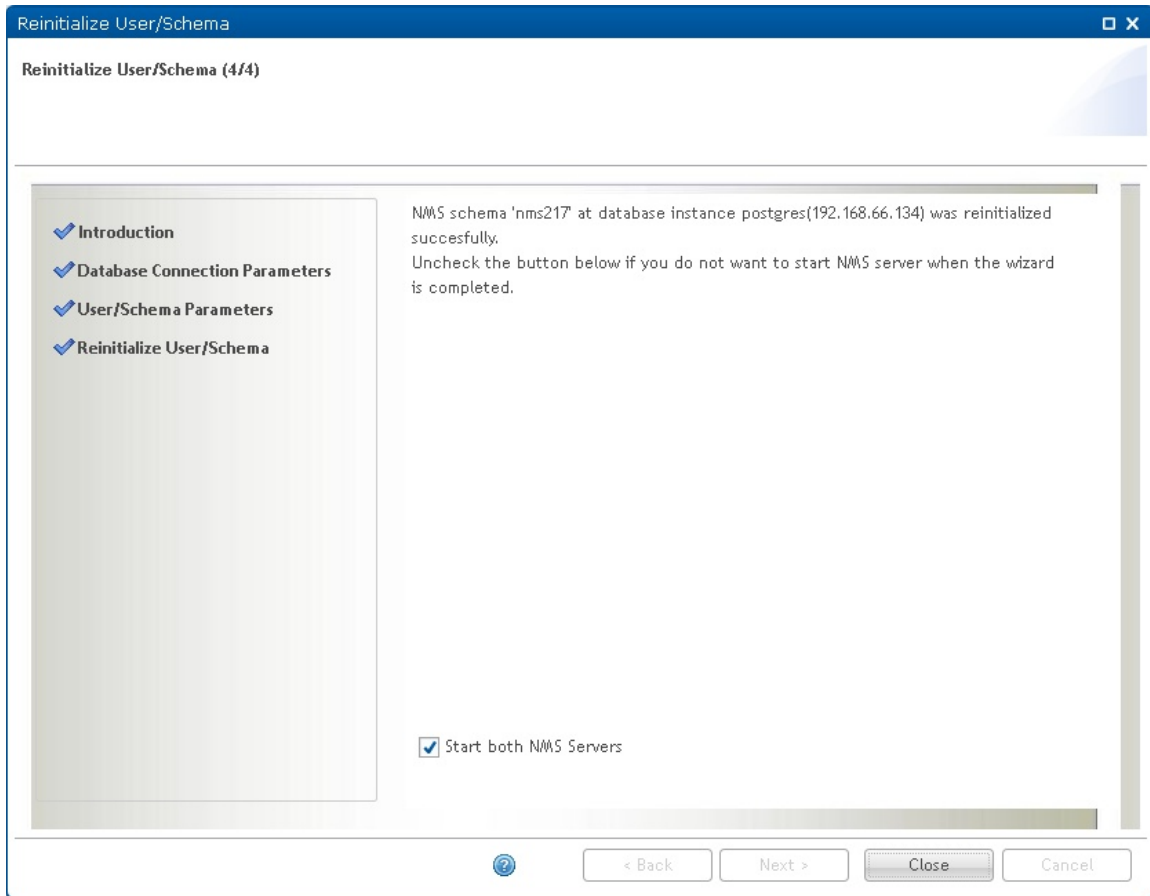


When the reinitialize process is complete, the following page is displayed:

Figure 294 Reinitialize Wizard page 4 : Reinitialized

Uncheck the Start PTP 820 NMS Server check box if you don't want to start the PTP 820 NMS server.

If you are working in a [High Availability](#) server setup, a page similar to the following page is displayed:

Figure 295 Reinitialize Wizard page 4 : Reinitialized

Uncheck the Start both NMS Servers check box if you do not want to start the Primary and Secondary servers.

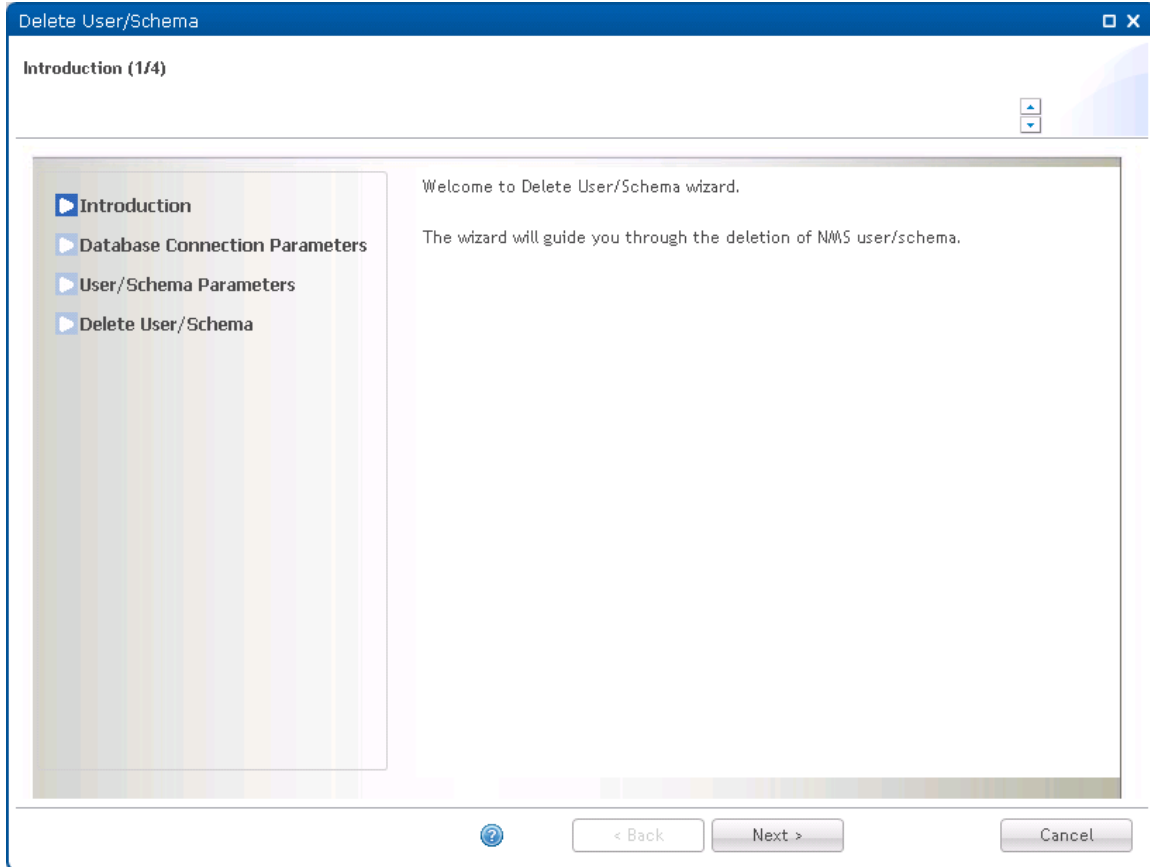
Press Close to complete the Reinitialize User/Schema wizard.

Delete User/Schema Wizard

This wizard allows you to delete an existing Oracle user or Postgres schema.

Open the Delete User/Schema wizard from the **Administration->Database Tasks** view in System Manager.

The active EMS database cannot be deleted.

Delete Wizard page 1: Introduction**Figure 296** Delete Wizard page 1 : Introduction

Press Next to continue the Delete User/Schema wizard.

Delete Wizard page 2: Database Connection Parameters

Specify the database connection parameters for the EMS database you want to delete.

Figure 297 Delete Wizard page 2 : Database Connection Parameters

Delete User/Schema

Database Connection Parameters (2/4)

Please review or change the default configuration below.
The fields marked with * are required.

Database connection parameters:

Database instance name: * postgres

Database type: * PostgreSQL

Database server address: * localhost

Database server port: * 5432

Database administrator user:

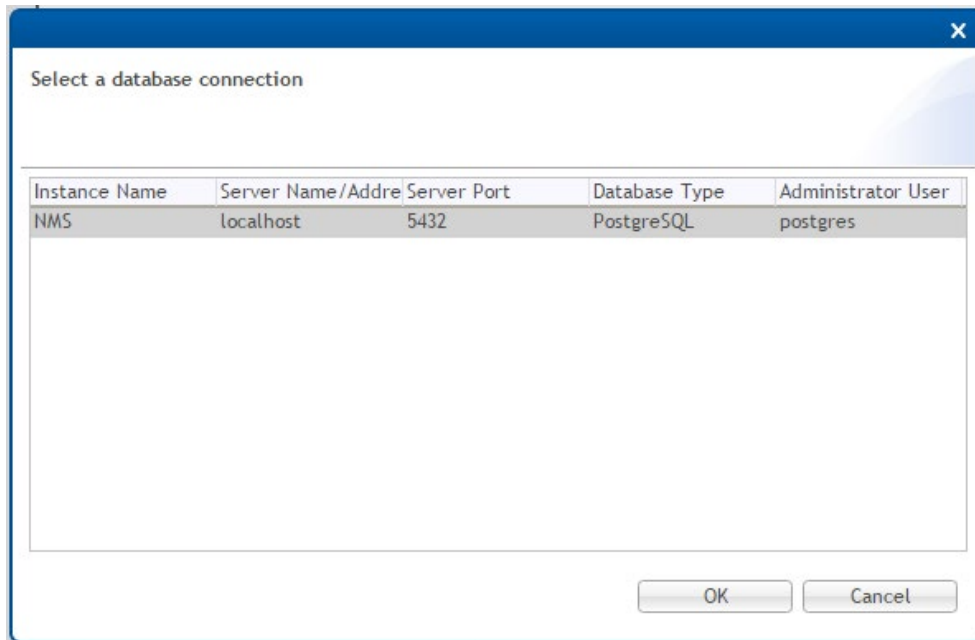
Username: * postgres

Password: *

Select Existing Parameters

< Back Next > Cancel

Press Select Existing Parameters button to select database connection parameters already defined in System Manager:

Figure 298 Selecting a database connection

If the desired parameters are not present in the list, you need to fill in the parameters manually.

All parameters are mandatory:

Name	Explanation
Database instance name	Name of a database instance.
Database type	Either Oracle or Postgres.
Database server address	IP address or hostname for the database server. Use localhost for a 1+0 configuration.
Database server port	Tcp port for the database. Default 1521 for Oracle, 5432 for Postgres.
Username	The database system user needed to delete the EMS user/schema.
Password	Password for the database system user.

Press Next to continue the Delete User/Schema wizard.

Delete Wizard page 3: User/Schema Parameters

Specify the Oracle user or Postgres schema you want to delete.

Figure 299 Delete Wizard page 3 : User/Schema Parameters

Delete User/Schema

User/Schema Parameters (3/4)

The fields marked with * are required.

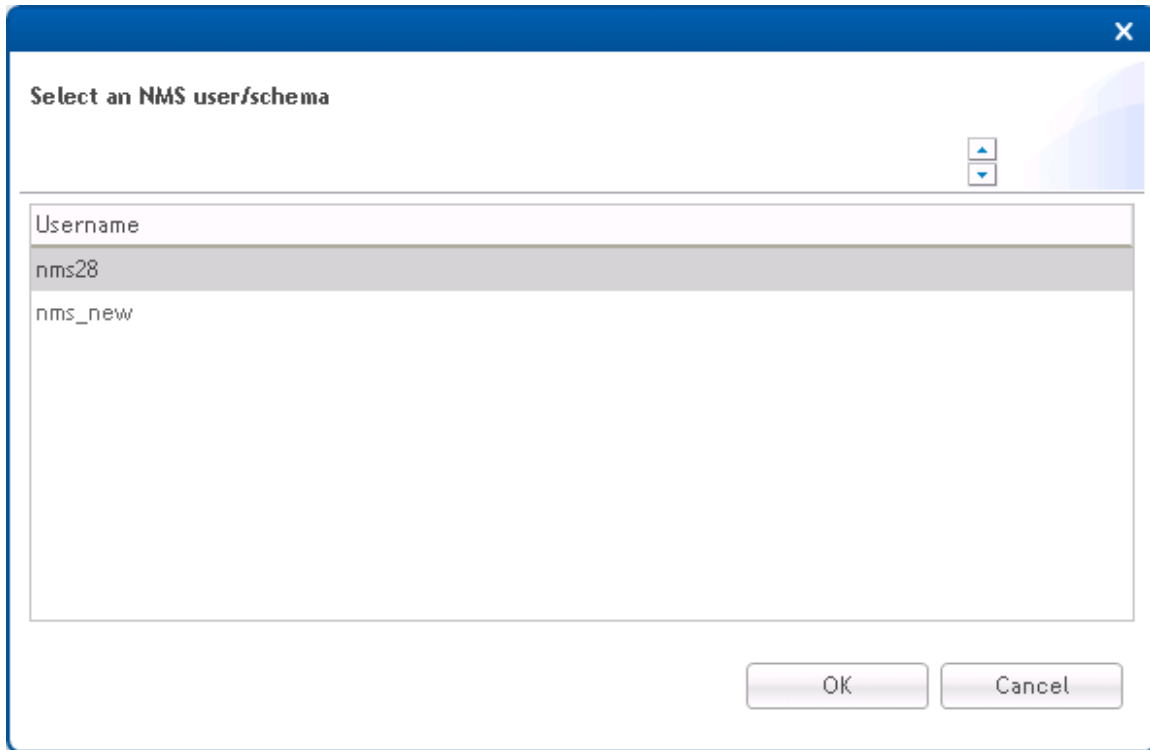
☒ Introduction
☒ Database Connection Parameters
☐ **User/Schema Parameters**
☐ Delete User/Schema

Enter the NMS database schema name and password or use the button below to select existing parameters from System Manager configuration files. The active NMS database configuration CAN NOT be deleted.

Username:*

Password:*

Press Select Existing Parameters button to select existing parameters already defined in System Manager:

Figure 300 Selecting user/schema

If the desired parameters are not present in the list, you have to fill in the parameters manually.

Both parameters are mandatory:

Name	Explanation
Username	Name of desired EMS user/schema
Password	Password for the desired EMS user/schema

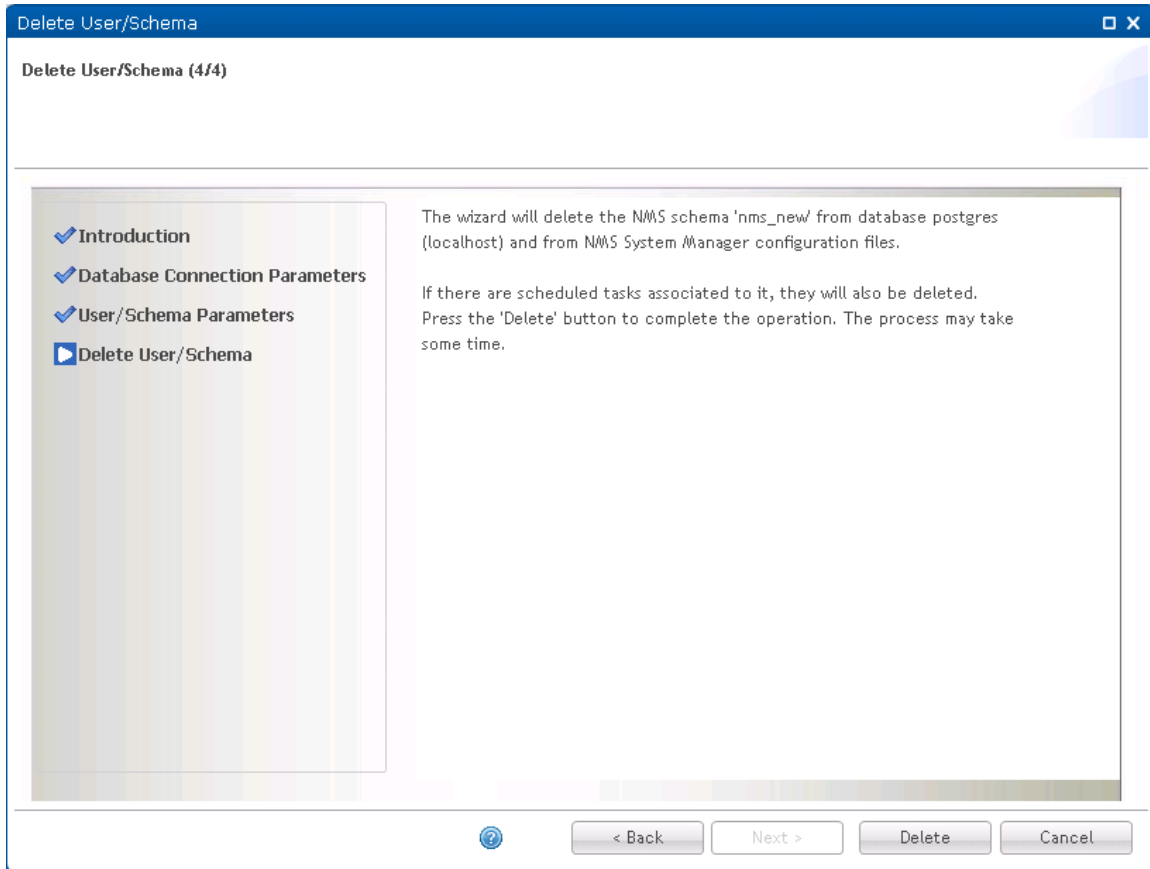
Press Next to continue the Delete User/Schema wizard.

Delete Wizard page 4: Delete User/Schema

This is the final page in the Delete User/Schema Wizard.

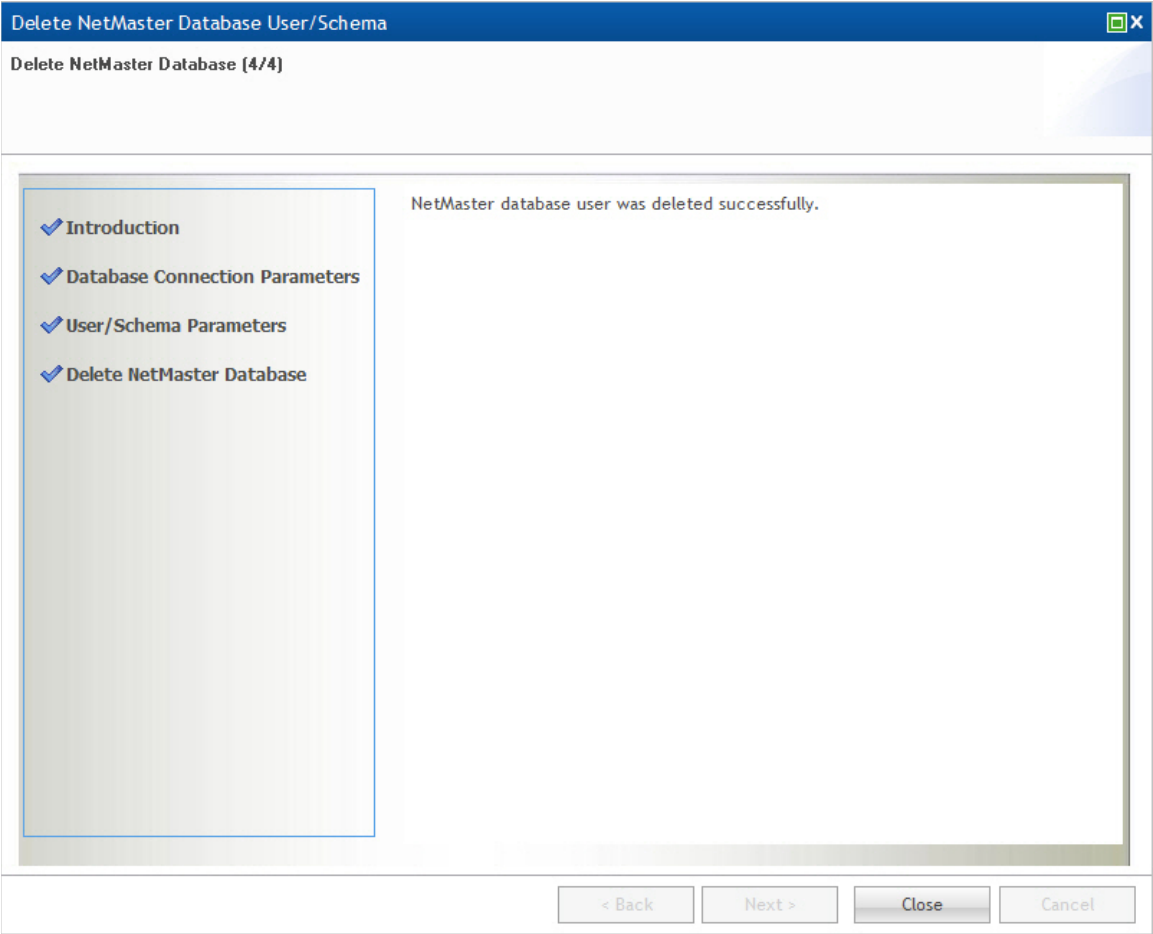
Press Delete to initiate the delete process.

Figure 301 Delete Wizard page 4 : Delete User/Schema



When the delete process is complete, the following page is displayed:

Figure 302 Deleting database



Press Close to complete the Delete User/Schema wizard.

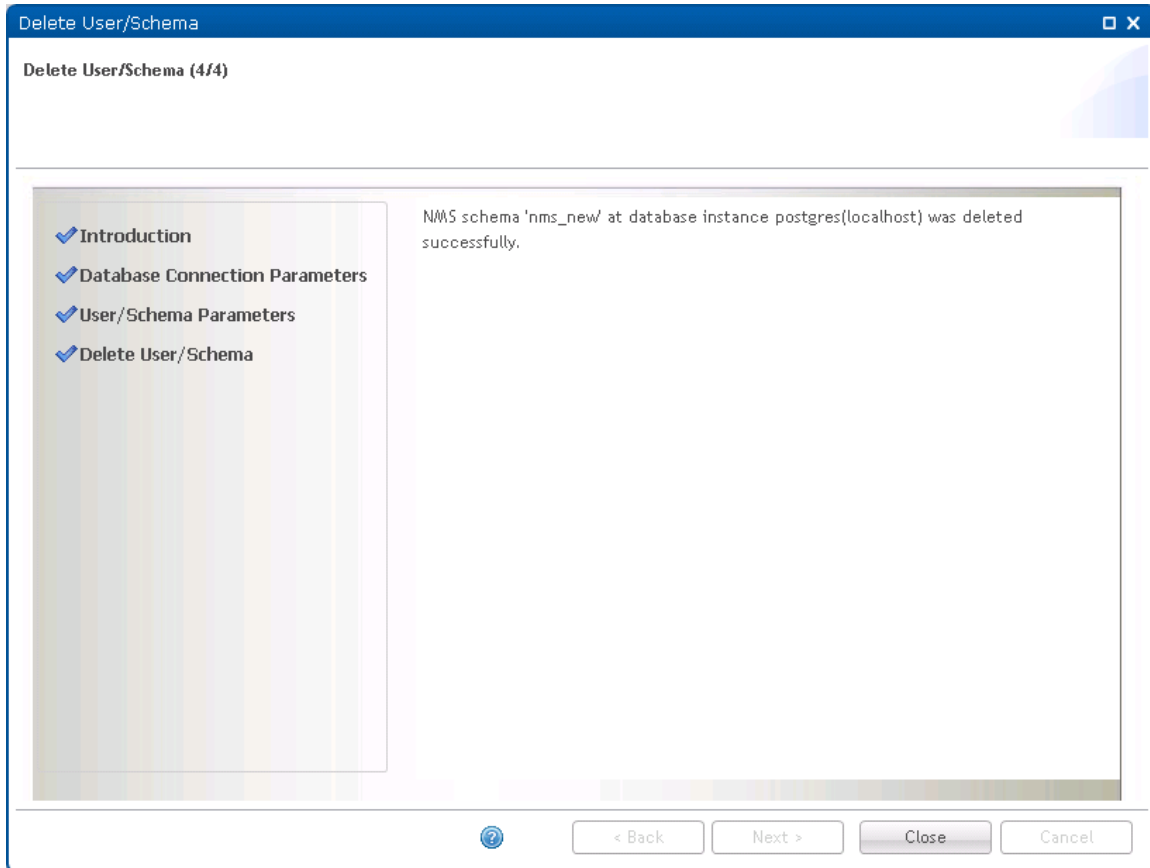
Upgrade User/Schema Wizard

This wizard allows you to upgrade an old EMS database to current version.

Open the Upgrade User/Schema wizard from the **Administration->Database Tasks** view in System Manager.

Upgrade Wizard page 1: Introduction

Figure 303 Upgrade Wizard page 1 : Introduction



Press Next to continue the Upgrade User/Schema wizard.

Upgrade Wizard page 2: Database Connection Parameters

Specify the database connection parameters for the EMS database you want to upgrade.

Figure 304 Upgrade Wizard page 2 : Database Connection Parameters

Upgrade User/Schema

Database Connection Parameters (2/5)

Please review or change the default configuration below.
The fields marked with * are required.

Database connection parameters:

Database instance name: * postgres

Database type: * PostgreSQL

Database server address: * localhost

Database server port: * 5432

Database administrator user:

Username: * postgres

Password: *

Select Existing Parameters

< Back Next > Cancel

Press Select Existing Parameters button to select database connection parameters already defined in System Manager:

Figure 305 Selecting a database connection

Instance Name	Server Name/Address	Server Port	Database Type	Administrator User
postgres	nmssql	5432	PostgreSQL	postgres
nmsora	nmsora	1521	Oracle	system

If the desired parameters are not present in the list, you have to fill in the parameters manually.

All parameters are mandatory:

Name	Explanation
Database instance name	Name of a database instance.
Database type	Either Oracle or Postgres.
Database server address	IP address or hostname for the database server. Use localhost for a 1+0 configuration.
Database server port	Tcp port for the database. Default 1521 for Oracle, 5432 for Postgres.
Username	The database system user needed to upgrade the EMS user/schema.

Please notice that in order to upgrade, you need to have a Database administrator user with sufficient privileges.

Press Next to continue the Upgrade User/Schema wizard.

Upgrade Wizard page 3: User/Schema Parameters

Specify the Oracle user or Postgres schema you want to upgrade.

Figure 306 Upgrade Wizard page 3 : User/Schema Parameters

Upgrade User/Schema

User/Schema Parameters (3/5)

Please review or change the default configuration below.
The fields marked with * are required.

Introduction
Database Connection Parameters
User/Schema Parameters
User/Schema Backup
Upgrade User/Schema

Enter the NMS database schema name and password or use the button below to select existing parameters from System Manager configuration files.

Username:* nms150_2

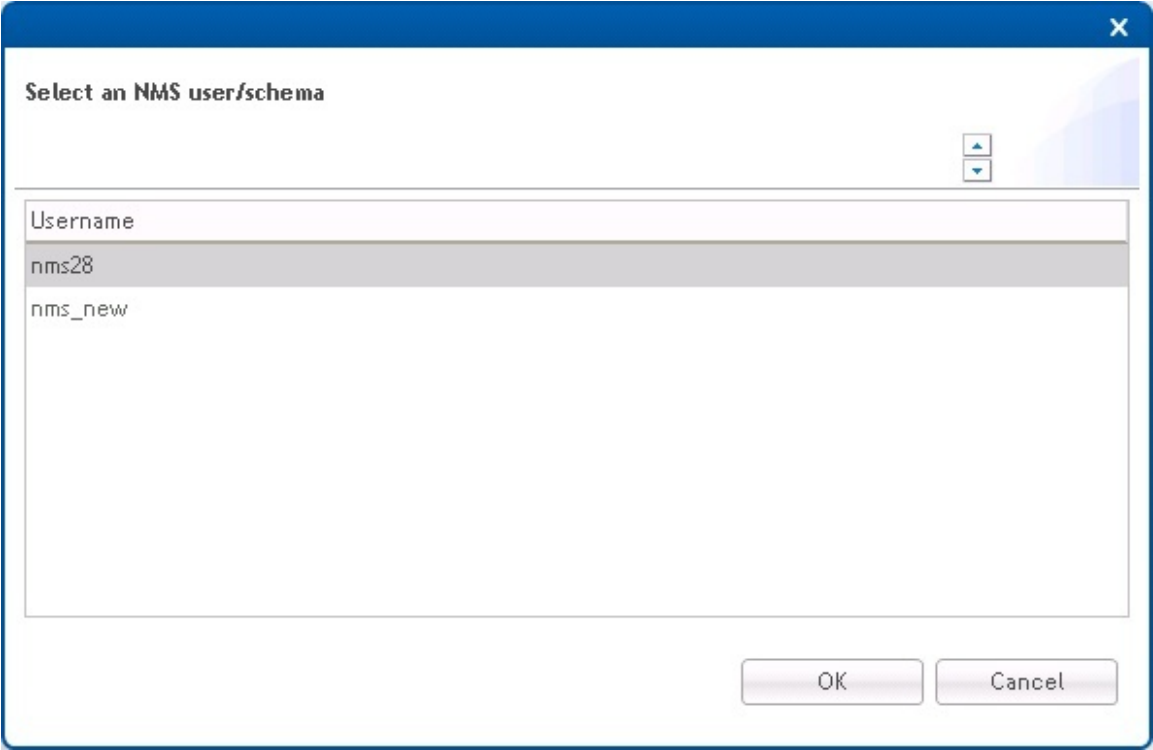
Password:* ..

Select Existing Parameters

< Back Next > Cancel

Press Select Existing Parameters button to select existing parameters already defined in System Manager:

Figure 307 Select a user/schema



If the desired parameters are not present in the list, you have to fill in the parameters manually.

Both parameters are mandatory:

Name	Explanation
Username	Name of desired EMS user/schema
Password	Password for the desired EMS user/schema

Press Next to continue the Upgrade User/Schema wizard.

Upgrade Wizard page 4: User/Schema Backup

It is recommended to take a backup of the database prior to upgrade, making it possible to restore the database to a recent and consistent state in case of upgrade failure.

It is also recommended to allow System Manager to perform backups of your database at regular intervals.

Figure 308 Upgrade Wizard page 4 : User/Schema backup

Upgrade User/Schema

User/Schema Backup (4/5)

The fields marked with * are required.

Introduction
Database Connection Parameters
User/Schema Parameters
User/Schema Backup
Upgrade User/Schema

Backup Settings

Database Install Path:*

Backup before upgrade

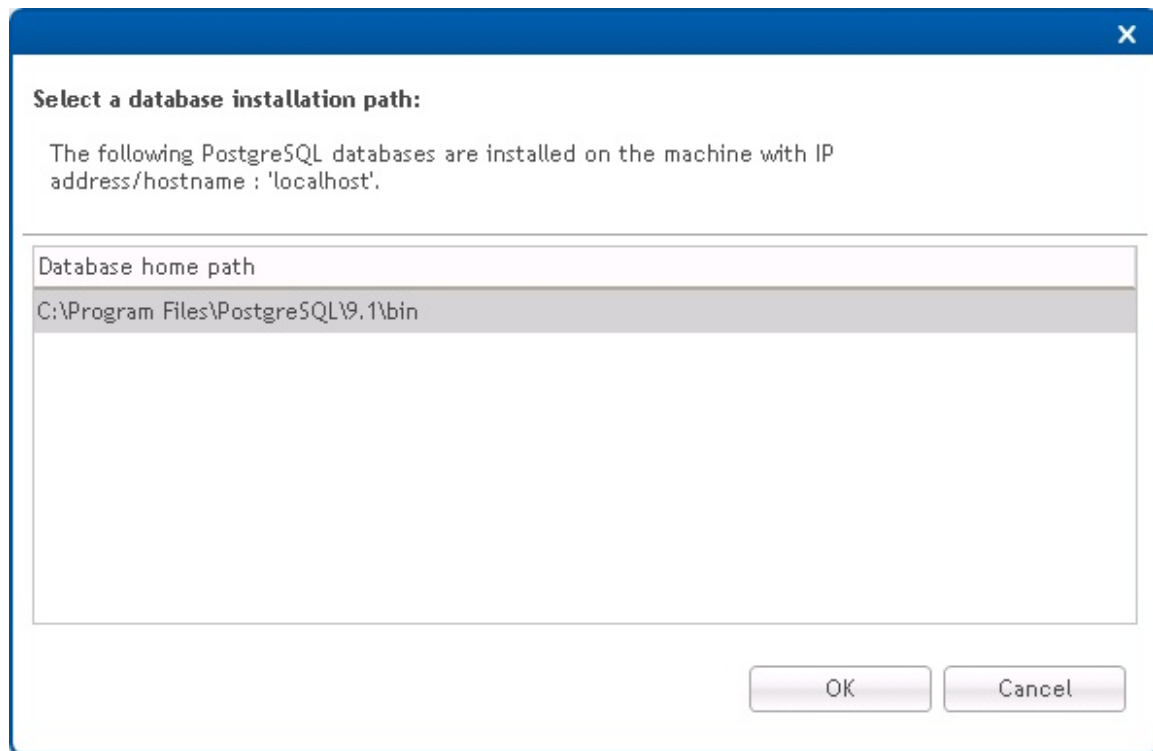
It is important to make a backup of your database before upgrading it. If the upgrade operation fails, the backup can help you to restore the database to a consistent state before upgrade.

☐ Skip backup before upgrade

< Back Next > Cancel

The Database Install Path is the database server path to the tools System Manager needs to run to perform backup and restore operations. The tools in question are exp.exe and imp.exe for Oracle and pg_dump and pg_restore for Postgres.

Press the Select Database Path to allow System Manager to try to find the Database Install Path automatically:

Figure 309 Selecting a database installation path

If System Manager fails to locate the correct path for you, you have to supply the correct path yourself.

It is possible to change the backup file storage location on the EMS server. It is also possible to configure number of days to keep the scheduled database backups. Both settings are found in the Database settings in System Manager.

If periodic backup is enabled, it is recommended to also enable deletion of old backup files to prevent the file system from filling up. Note that the deletion of old backup files in a 2+0 configuration is performed on the database server as well as on the EMS server.

A database backup will be performed prior to database upgrade unless the Skip backup before upgrade check box is checked. The backup is placed in the location specified in the [Database view](#) available from the Settings menu. The default location is C:\PTP820NMS\Backup\Database.

When the settings are configured as desired, press Next to continue the Upgrade User/Schema wizard.

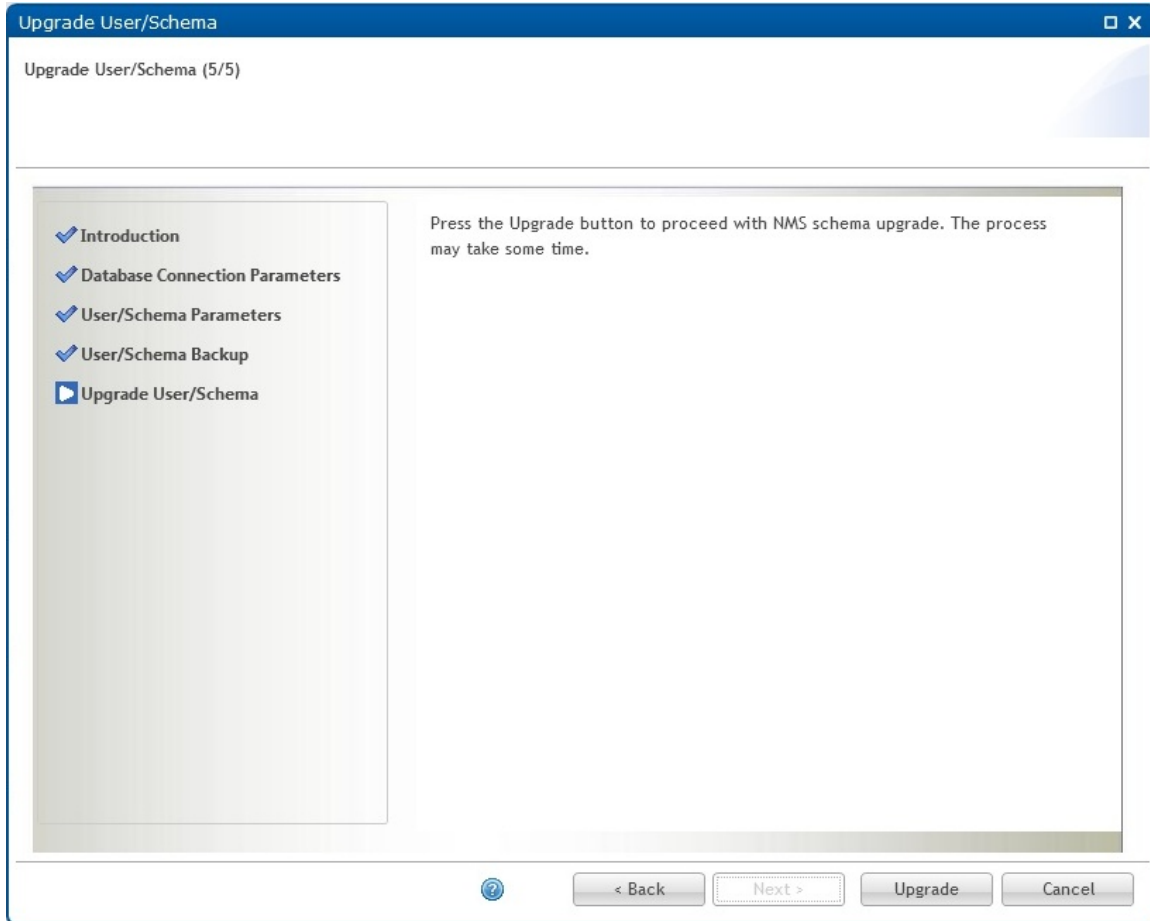
If System Manager on the database server is not compatible with the System Manager on the EMS server, the backup will be aborted with an error message. If so, you should upgrade the outdated System Manager, and then rerun the Upgrade User/Schema wizard.

Upgrade Wizard page 5: Upgrade User/Schema

This is the final page in the Upgrade User/Schema Wizard.

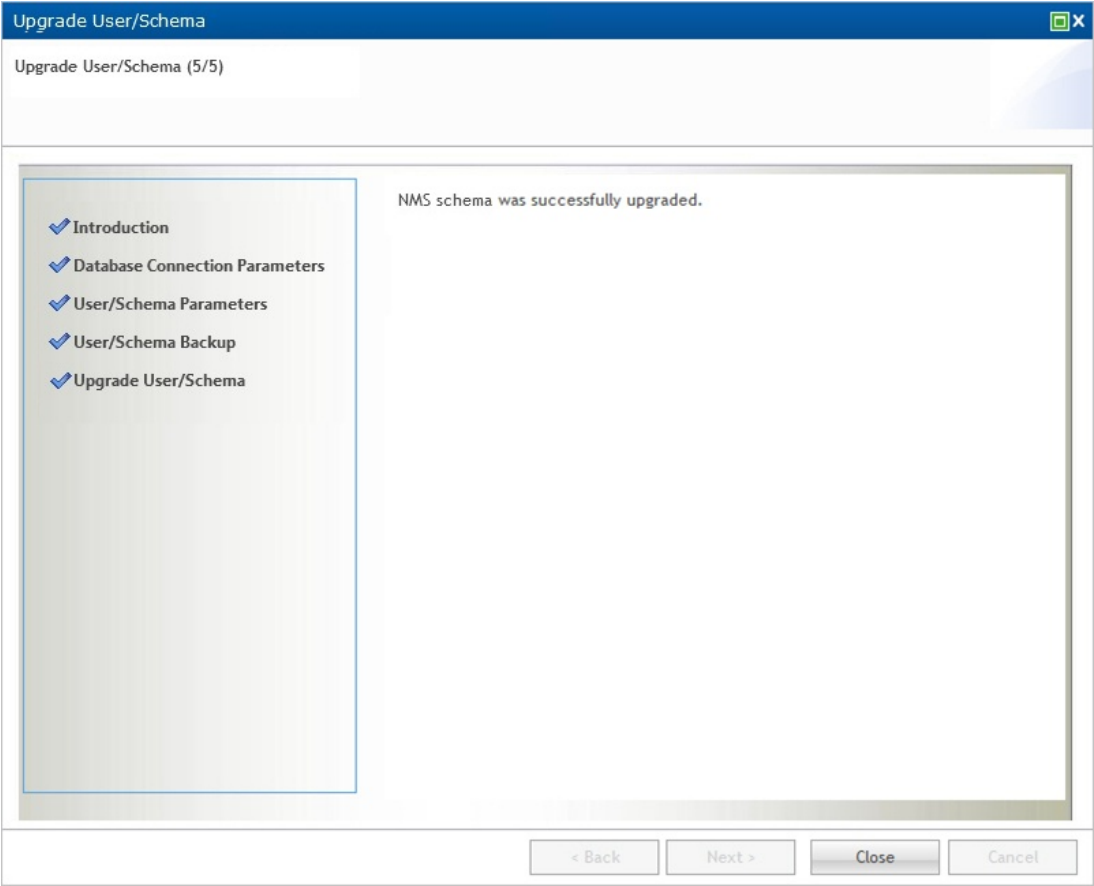
Verify the operation list summary and press Upgrade to initiate the upgrade process.

Figure 310 Upgrade Wizard page 5 : Upgrade User/Schema



If the upgrade process completes with success, the following page is displayed:

Figure 311 Upgrade Wizard page 5 : Upgrade complete

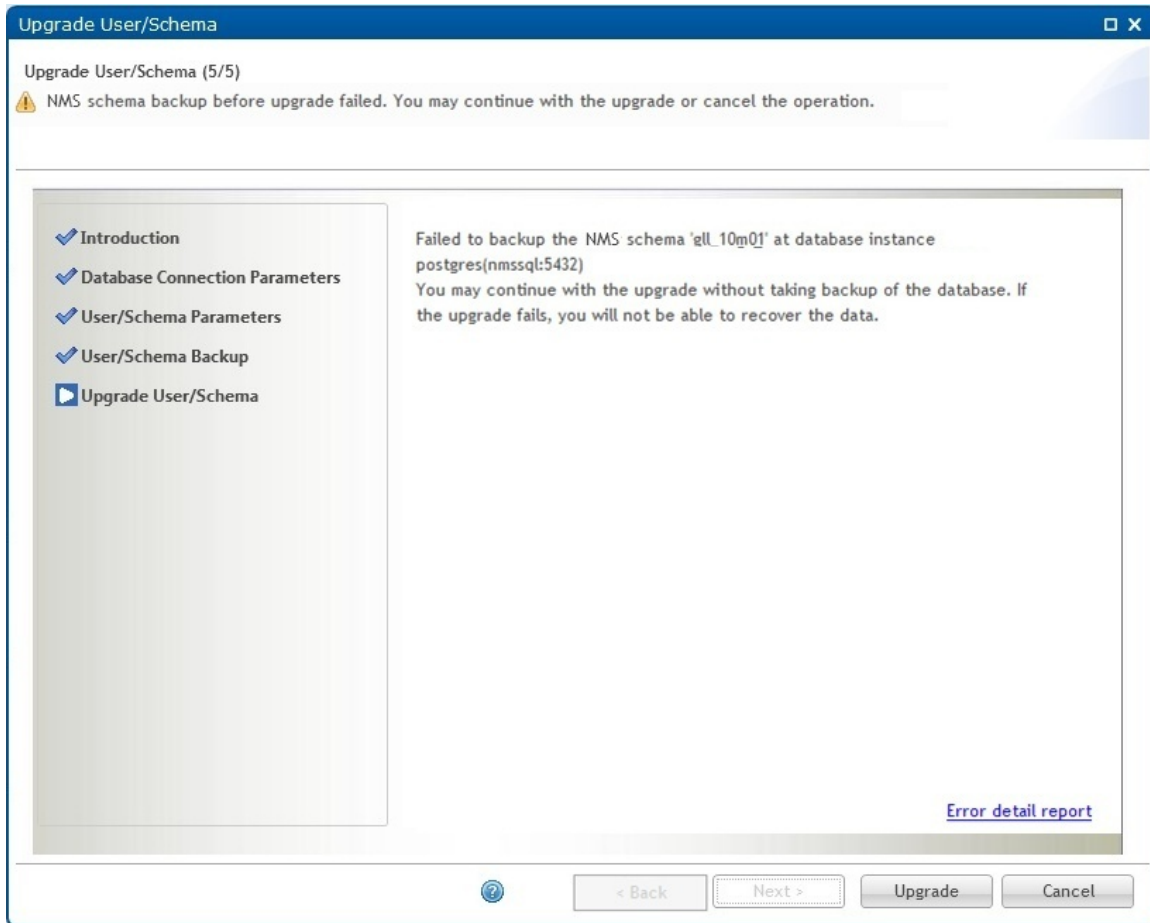


Press Close to complete the Upgrade User/Schema wizard.

Error situations and recovery - Backup before upgrade fails

If backup before upgrade fails, it is still possible to continue database upgrade process:

Figure 312 Backup before upgrade fails



Press Error detail report link to see error details:

Figure 313 Error details report

Error Details Report

Start Date: 12 Mar 2010 10:40:42

End Date: 12 Mar 2010 10:40:44

Task Type: Backup NMS database

Status: Failed

Subtask: Backup database

Subtask status: Failed

Description: Backup NMS database

Details:

Backing NMS database 'torh_m01' at nmsdb (vmtorhb)

Task failed because an exception occurred.

java.net.ConnectException: Connection refused: connect

If the database server is located on a separate machine than NMS server,
check if System Manager on the database server is up and running.

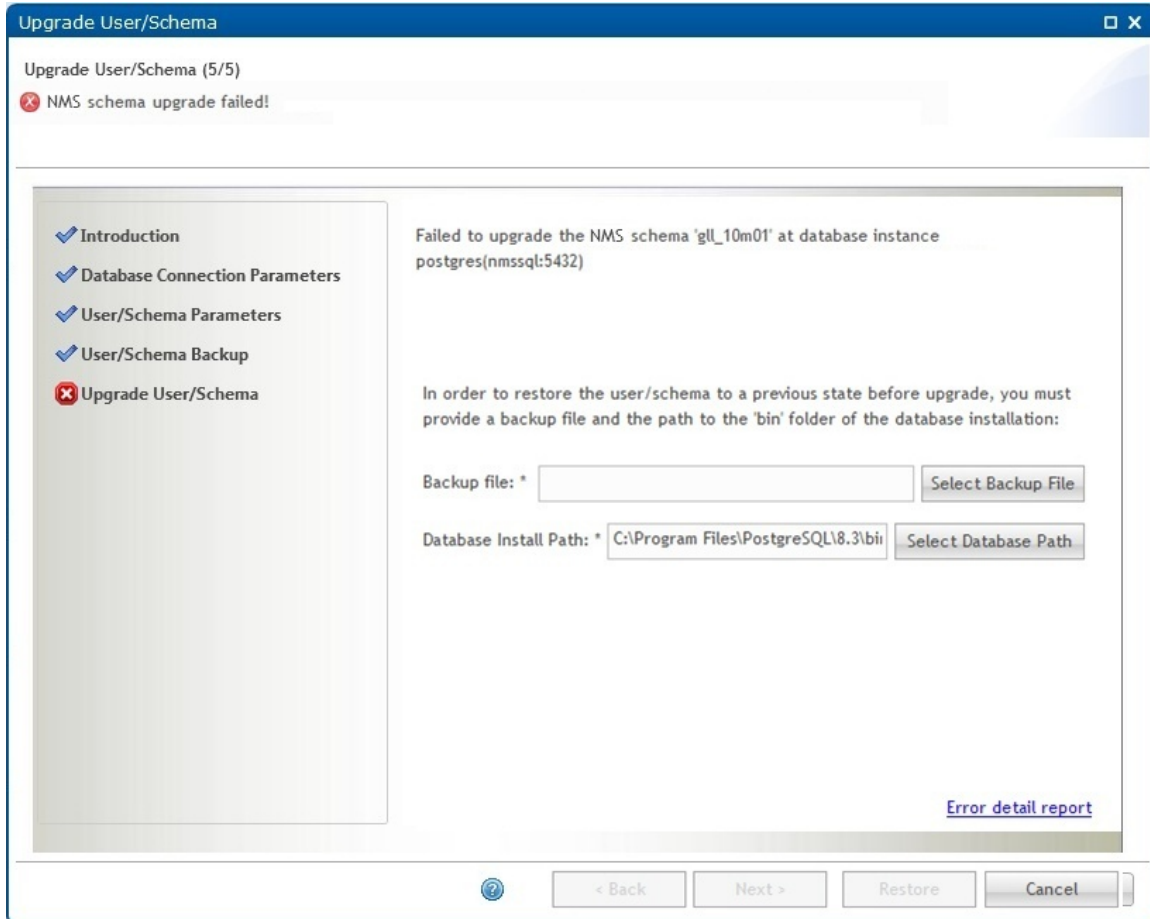
OK

Make sure to take a backup of your database manually, then press Upgrade to continue upgrade.

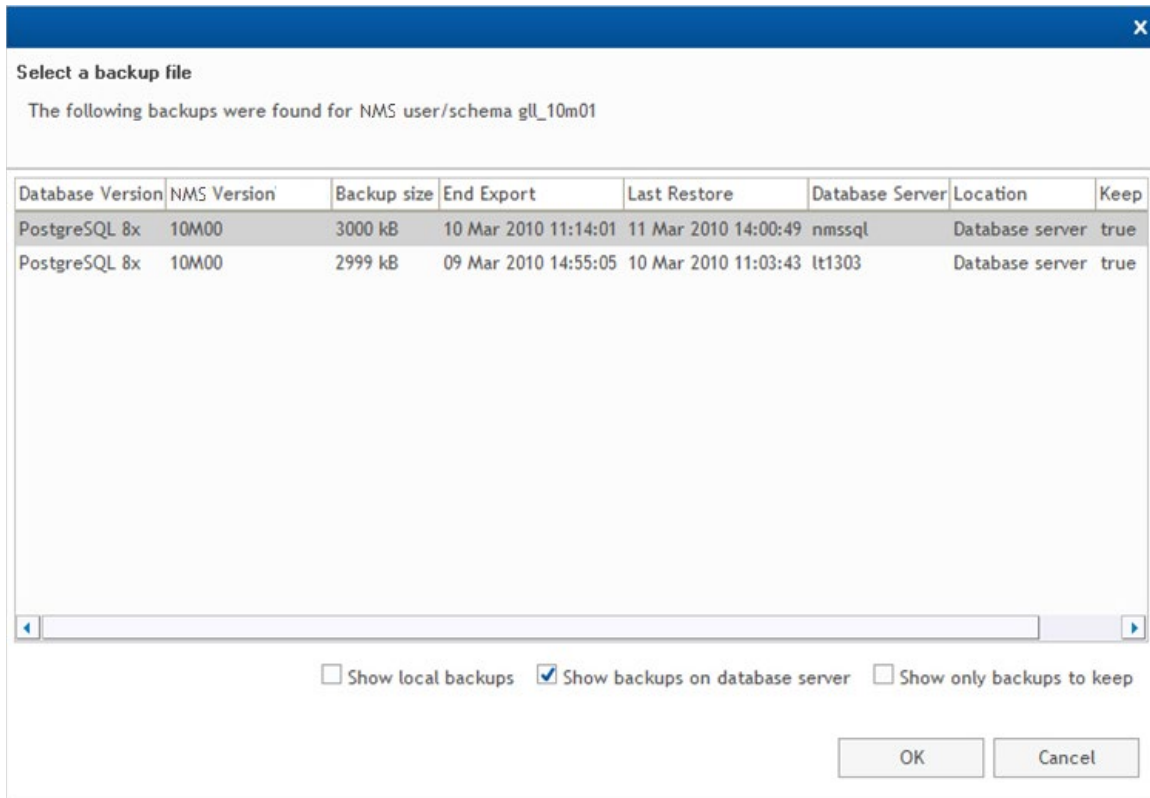
Error situations and recovery - Upgrade of database failed

If upgrade process completes with failure, the following page is displayed, giving the option to restore the possible corrupt database:

Figure 314 Upgrade of database failed



Check the Error detail report to see what caused the upgrade to fail. An upgrade failure may leave your database in a corrupt state. It is recommended to restore it to a consistent state. Press the Select Backup File button to select an existing database backup. If a backup before upgrade was requested and was successfully performed, it should appear as the newest entry in the backup list:

Figure 315 Selecting a backup file

Select a backup file and press OK to return to the Upgrade User/Schema wizard page.

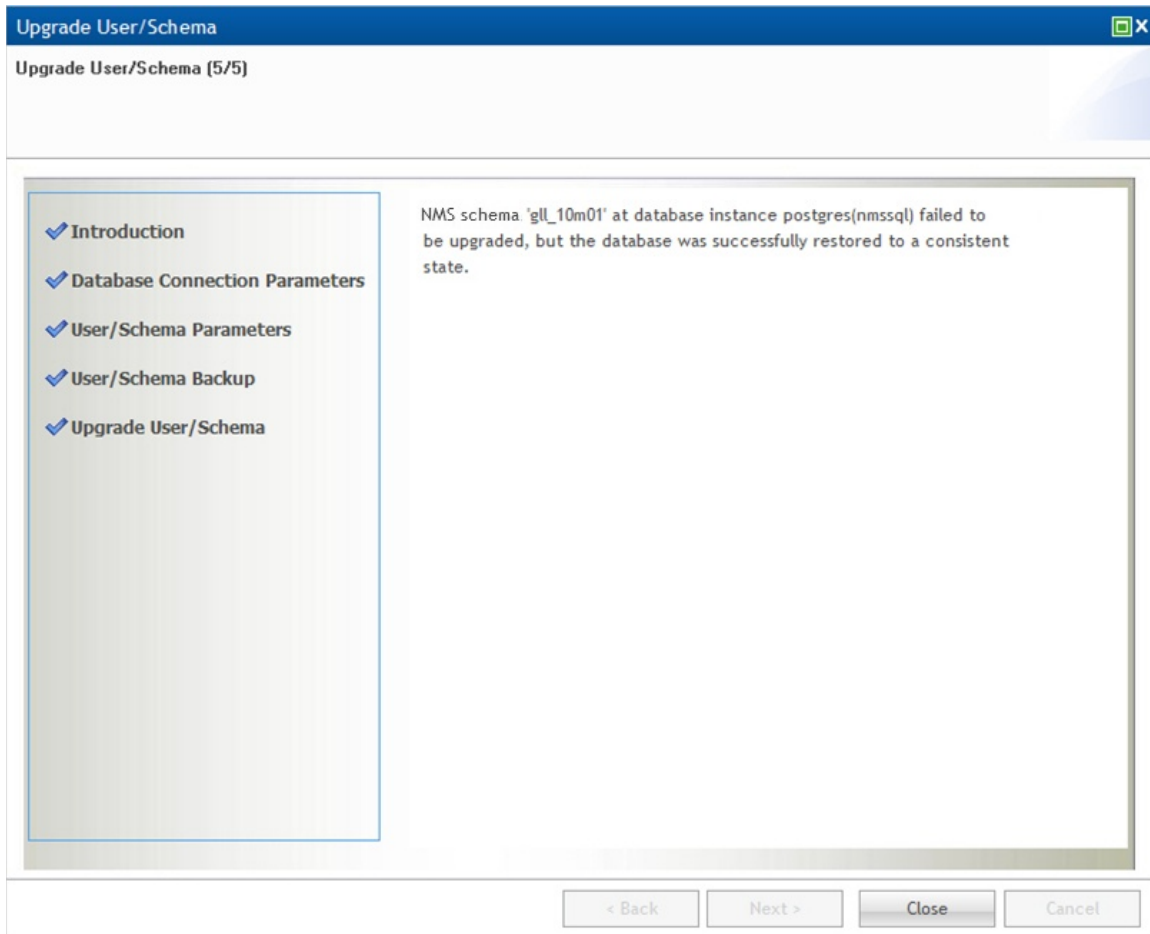
Press Restore button to restore the selected database backup:

If the restore fails as well, you may cancel the wizard or retry a restore operation:

Figure 316 Database backup restore - retry

The screenshot shows a window titled "Upgrade User/Schema" with a close button in the top right corner. Below the title bar, it says "Upgrade User/Schema (5/5)" and "Fields marked with * are required!". On the left is a sidebar with a list of steps: "Introduction", "Database Connection Parameters", "User/Schema Parameters", "User/Schema Backup", and "Upgrade User/Schema" (which is selected with a blue square icon). The main area contains the following text: "Failed to upgrade the NMS schema 'gll_10m01' at database instance postgres(nmssql:5432)". Below this, it says: "In order to restore the user/schema to a previous state before upgrade, you must provide a backup file and the path to the 'bin' folder of the database installation:". There are two input fields: "Backup file: *" with the value "20100310-111349-postgres-gll_10m01.backup.gz" and a "Select Backup File" button; and "Database Install Path: *" with the value "C:\Program Files\PostgreSQL\8.3\bin" and a "Select Database Path" button. At the bottom, there is a question mark icon, a "< Back" button, a "Next >" button, a "Restore" button, and a "Cancel" button.

If restore completes successfully, the following page appears:

Figure 317 Restore database complete

Press Close to complete the Upgrade User/Schema wizard.

Backup Active User/Schema Wizard

This wizard allows you to back up the Oracle user or Postgres schema set as active EMS database.

It is also possible to set up periodic backup at configurable intervals on the active database.

Open the Backup Active User/Schema wizard from the Administration->Database Tasks view in System Manager.

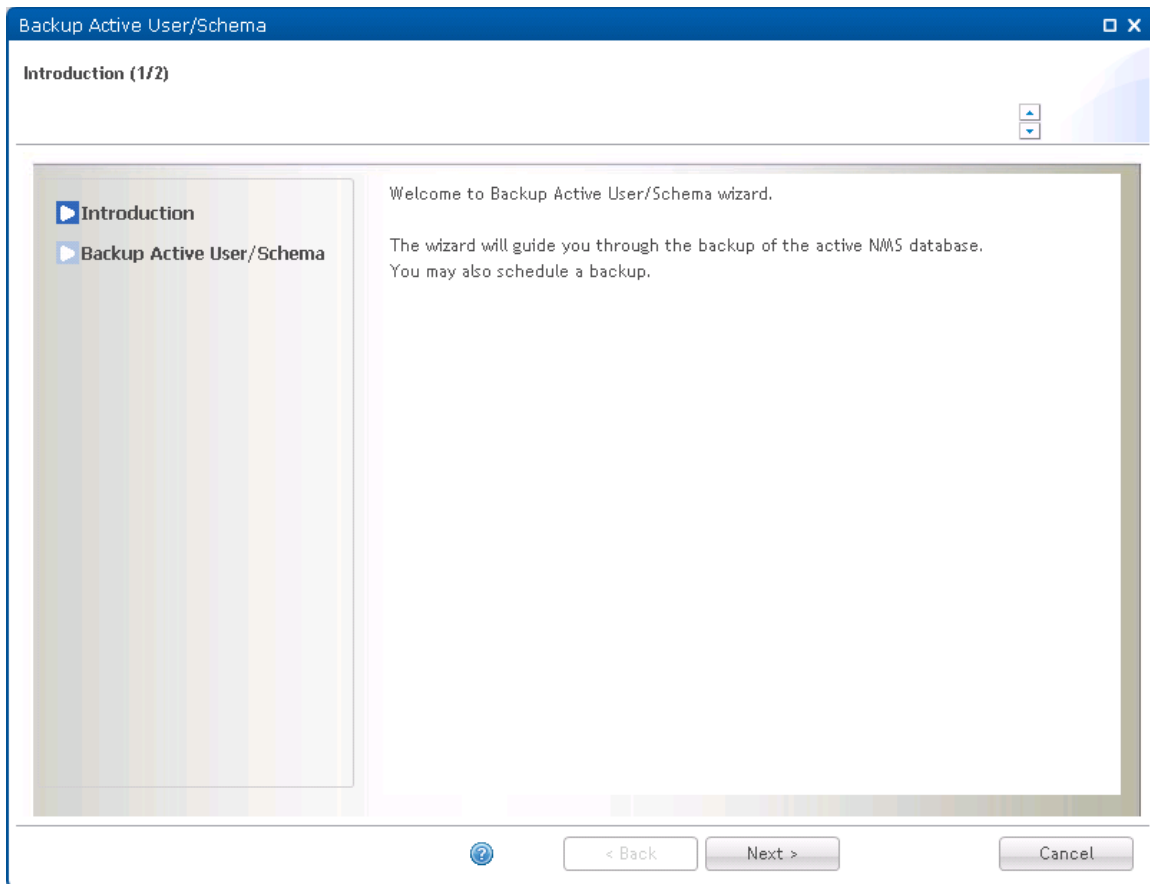
If you want to backup any other EMS database, you must use the Backup User/Schema wizard.

Be aware that this operation will always take backup of the current active EMS database. This means that if you change active database, the next scheduled backup will be taken of the new active EMS database.

If System Manager does not know the database server install path for the new active database, the Set Active User/Schema wizard will remove any scheduled backup jobs on active database and encourage the user to reschedule the job using the Backup Active User/Schema wizard.

Backup Active Wizard page 1: Introduction

Figure 318 Backup Active Wizard page 1 : Introduction

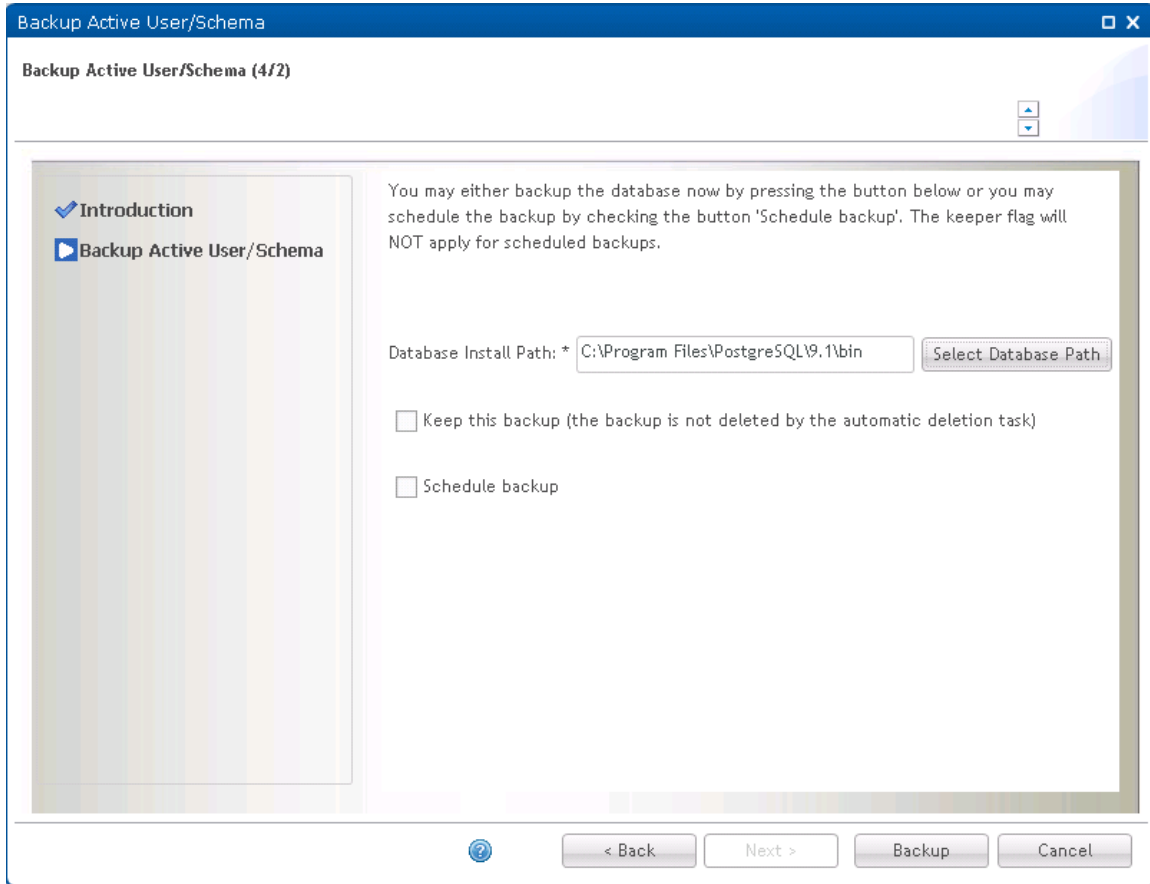


Press Next to continue the Backup Active User/Schema wizard.

Backup Active Wizard page 2: Backup Active User/Schema

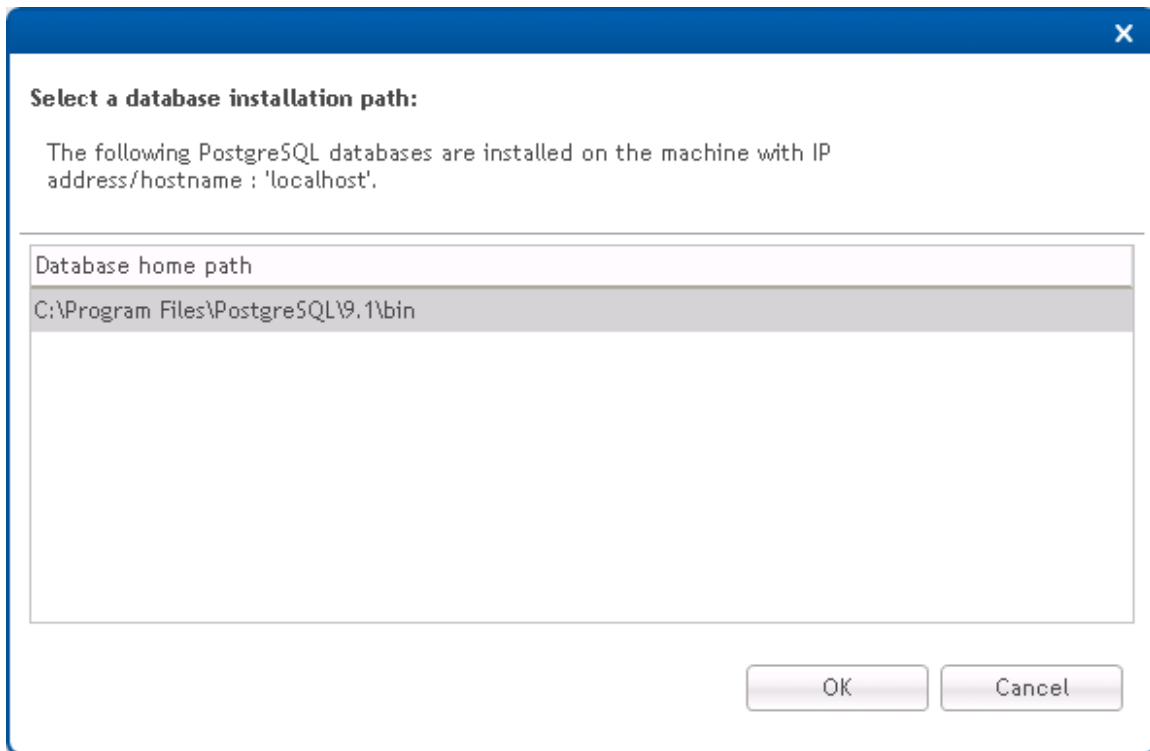
This is the final page in the Backup Active User/Schema Wizard.

Figure 319 Backup Active Wizard page 2 : Backup Active User/Schema



The Database Install Path is the database server path to the tools System Manager needs to run backup and restore operations. The tools in question are exp.exe and imp.exe for Oracle and pg_dump and pg_restore for Postgres.

If the Database Install Path is empty, press the Select Database Path to allow System Manager to try to find the Database Install Path automatically:

Figure 320 Selecting a database path

If System Manager fails to locate the correct path for you, you have to supply the correct path yourself.

Be aware that in a 2+0 configuration (EMS server and EMS database on separate machines), backup files are stored on both servers. The backup files are zipped to reduce disk space consumption, but you should make sure to select a file system with enough free disk space to hold the backup files.

It is possible to change the backup file storage location on the EMS server. It is also possible to configure System Manager to delete backups older than a given number of days. If enabled, all backup files created by periodic backup jobs will be targeted for deletion. In a 2+0 configuration old backup files are deleted on the database server as well as on the EMS server. The storage location and old backup files deletion settings are found in the Database settings in System Manager.

You can select either to take a backup right now, or to initiate periodic backup on the active EMS database.

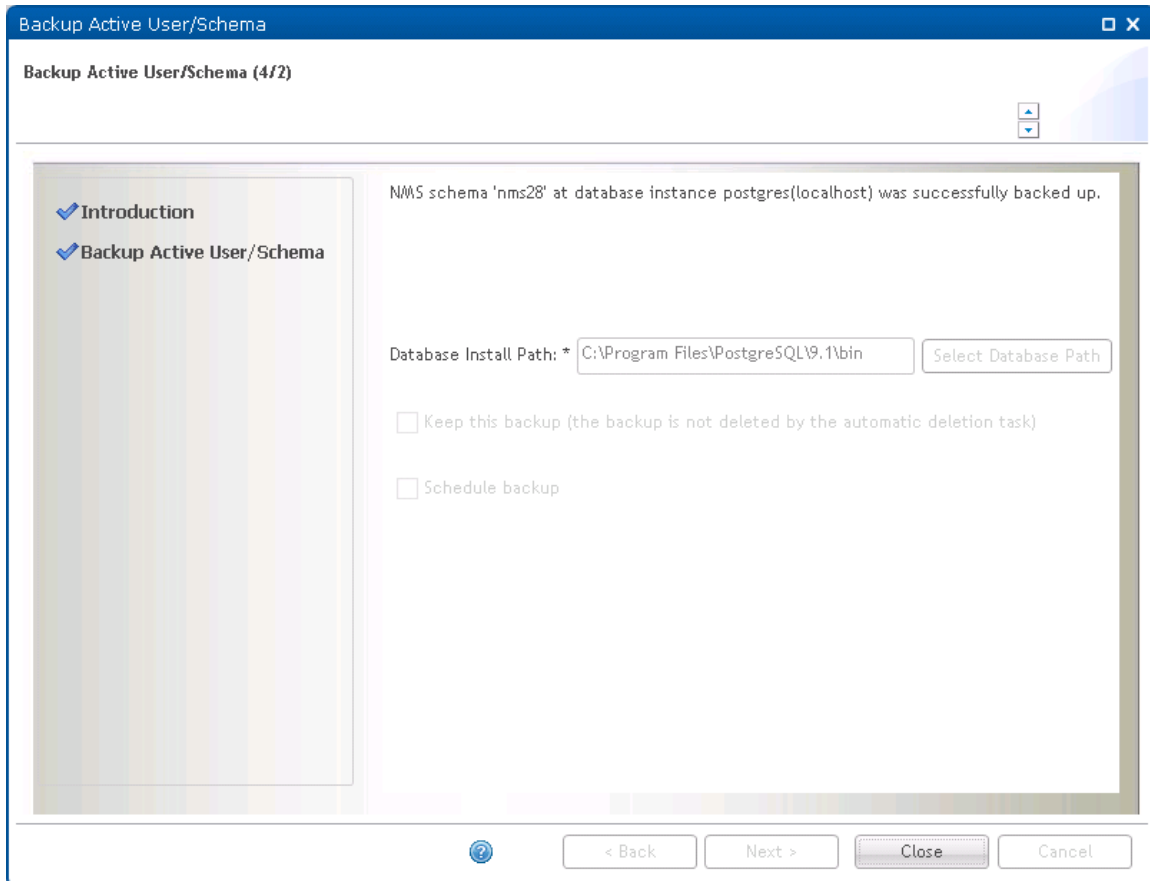
Take a backup now

Leave the Scheduled backup check box unchecked. If this is checked, System Manager will initiate periodic backup.

Check the Keep this backup check box if you want this backup to be ignored by the old backup files deletion job.

Press Backup Active to initiate the backup process causing the following page to appear:

Figure 321 Database backup



Press Close to complete the Backup Active User/Schema wizard.

If System Manager on the database server is not compatible with the System Manager on the EMS server, the backup will be aborted with an error message. If so, you should upgrade the outdated System Manager, and then rerun the Backup Active User/Schema wizard.

Initiate periodic backup

To initiate periodic backup, check the Schedule backup check box and adjust the start time and backup interval as desired. If you specify a start time in the past, the periodic backup is scheduled and the first periodic backup is taken immediately.

If you enable periodic backup, it is recommended to also enable deletion of old backup files to prevent the file system from filling up.

Press Schedule to schedule the periodic backup on selected EMS database:

Figure 322 Schedule database backup

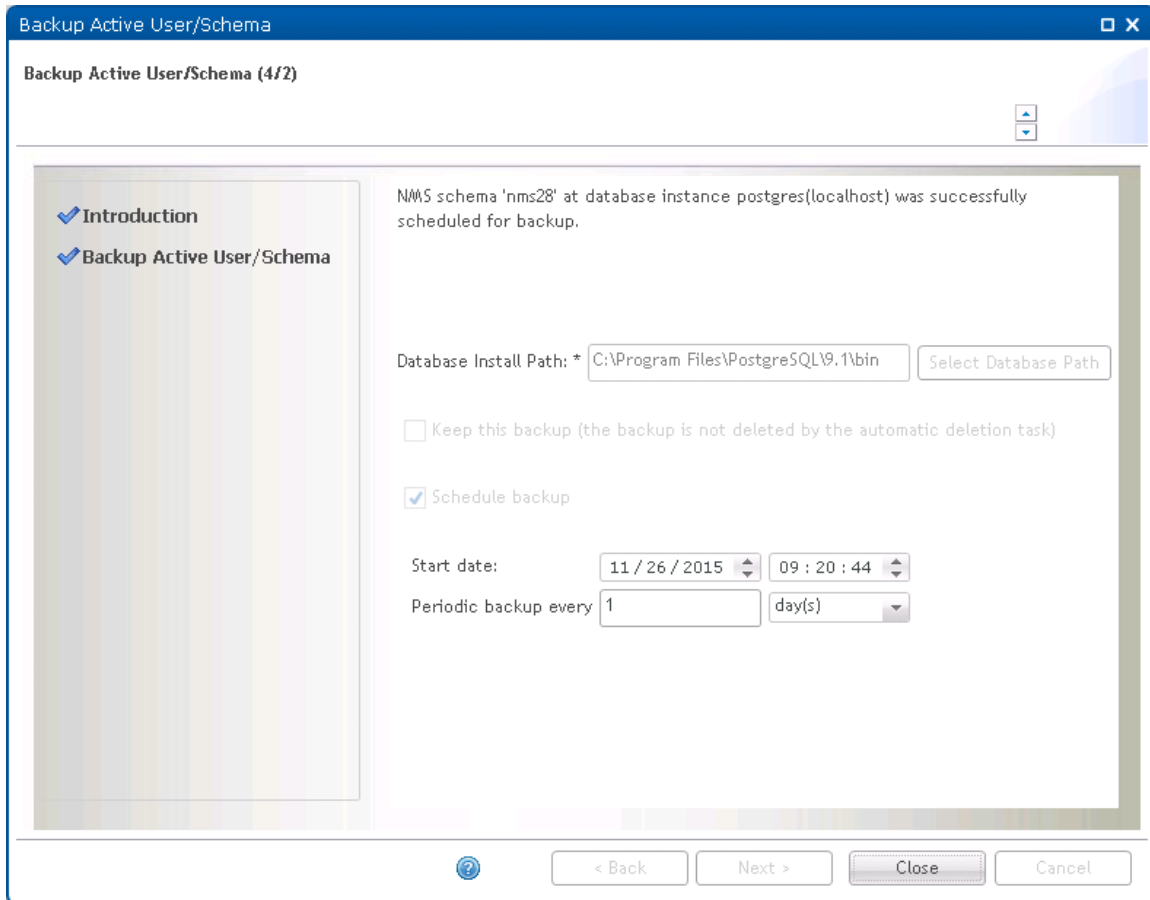
The screenshot shows a window titled "Backup Active User/Schema" with a subtitle "Backup Active User/Schema (4/2)". On the left is a sidebar with "Introduction" (checked) and "Backup Active User/Schema" (selected). The main area contains the following text: "You may either backup the database now by pressing the button below or you may schedule the backup by checking the button 'Schedule backup'. The keeper flag will NOT apply for scheduled backups."

Below the text are the following fields and controls:

- Database Install Path: * C:\Program Files\PostgreSQL\9.1\bin (with a "Select Database Path" button)
- ☐ Keep this backup (the backup is not deleted by the automatic deletion task)
- ☒ Schedule backup
- Start date: 11 / 26 / 2015 (calendar icon) 09 : 22 : 13 (time icon)
- Periodic backup every 1 day(s) (dropdown menu)

At the bottom are buttons: "< Back", "Next >", "Schedule", and "Cancel".

This page is shown if schedule operation was successful:

Figure 323 Schedule database backup complete

Press Close to complete the Backup Active User/Schema wizard.

Backup User/Schema Wizard

This wizard allows you to backup an existing Oracle user or Postgres schema.

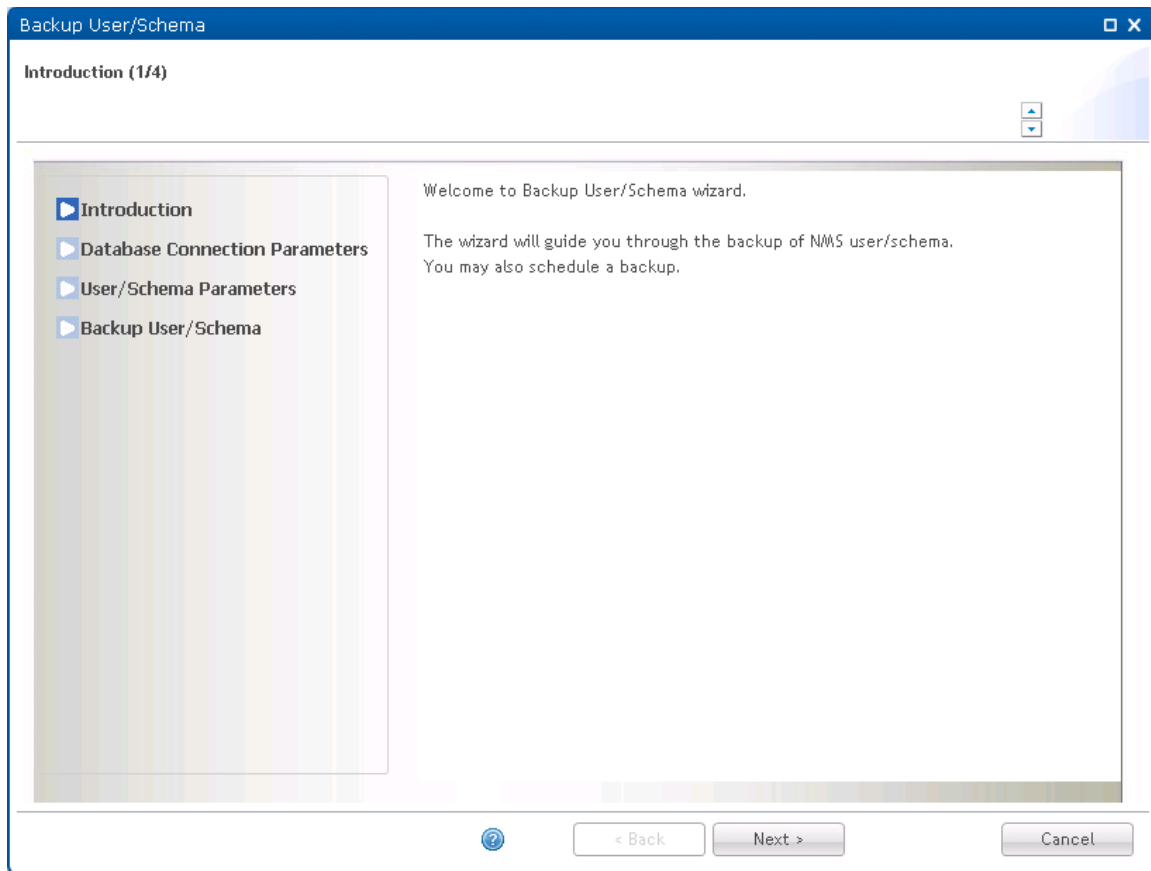
It is also possible to set up periodic backup at configurable intervals.

Open the Backup User/Schema wizard from the Administration->Database Tasks view in System Manager.

If you want to back up the active EMS database, you can also use the Backup Active User/Schema wizard.

Backup Wizard page 1: Introduction

Figure 324 Backup Wizard page 1 : Introduction



Press Next to continue the Backup User/Schema wizard.

Backup Wizard page 2: Database Connection Parameters

Specify the database connection parameters for the EMS database you want to backup.

Figure 325 Backup Wizard page 2 : Database Connection Parameters

Backup User/Schema

Database Connection Parameters (2/4)

Please review or change the default configuration below.
The fields marked with * are required.

Database connection parameters:

Database instance name: * postgres

Database type: * PostgreSQL

Database server address: * localhost

Database server port: * 5432

Database administrator user:

Username: * postgres

Password: *

Select Existing Parameters

< Back Next > Cancel

Press Select Existing Parameters button to select database connection parameters already defined in System Manager:

Figure 326 Selecting a database connection

Instance Name	Server Name/Address	Server Port	Database Type	Administrator User
postgres	nmssql	5432	PostgreSQL	postgres
nmsora	nmsora	1521	Oracle	system

If the desired parameters are not present in the list, you need to fill in the parameters manually.

All parameters are mandatory:

Name	Explanation
Database instance name	Name of a database instance.
Database type	Either Oracle or Postgres.
Database server address	IP address or hostname for the database server. Use localhost for a 1+0 configuration.
Database server port	Tcp port for the database. Default 1521 for Oracle, 5432 for Postgres.
Username	The database system user needed to back up the EMS user/schema.
Password	Password for the database system user.

Please notice that in order to do backup, you need to have a Database administrator user with sufficient privileges.

Press Next to continue the Backup User/Schema wizard.

Backup Wizard page 3: User/Schema Parameters

Specify the Oracle user or Postgres schema you want to backup.

Figure 327 Backup Wizard page 3 : User/Schema Parameters

Backup User/Schema

User/Schema Parameters (3/4)

Please review or change the default configuration below.
The fields marked with * are required.

Introduction
Database Connection Parameters
User/Schema Parameters
Backup User/Schema

Enter the NMS database schema name and password or use the button below to select existing parameters from System Manager configuration files.

Username:* nms28

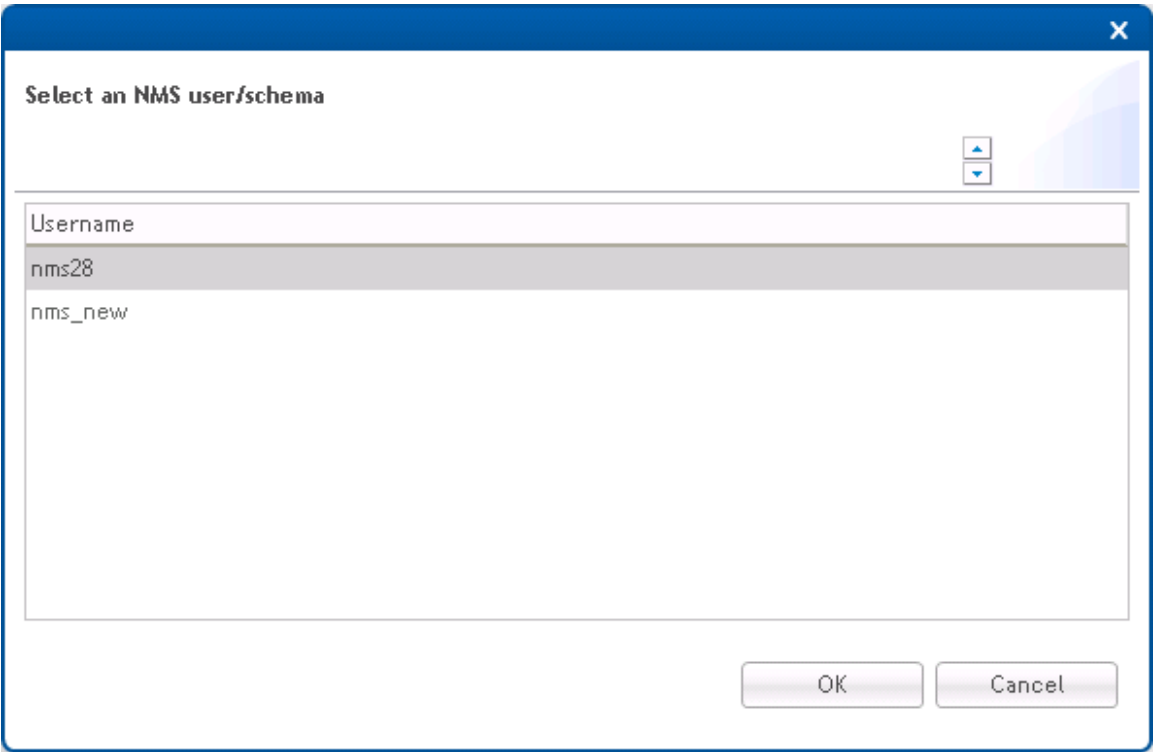
Password:*

Select Existing Parameters

< Back Next > Cancel

Press Select Existing Parameters button to select existing parameters already defined in System Manager:

Figure 328 Select a user/schema



If the desired parameters are not present in the list, you have to fill in the parameters manually.

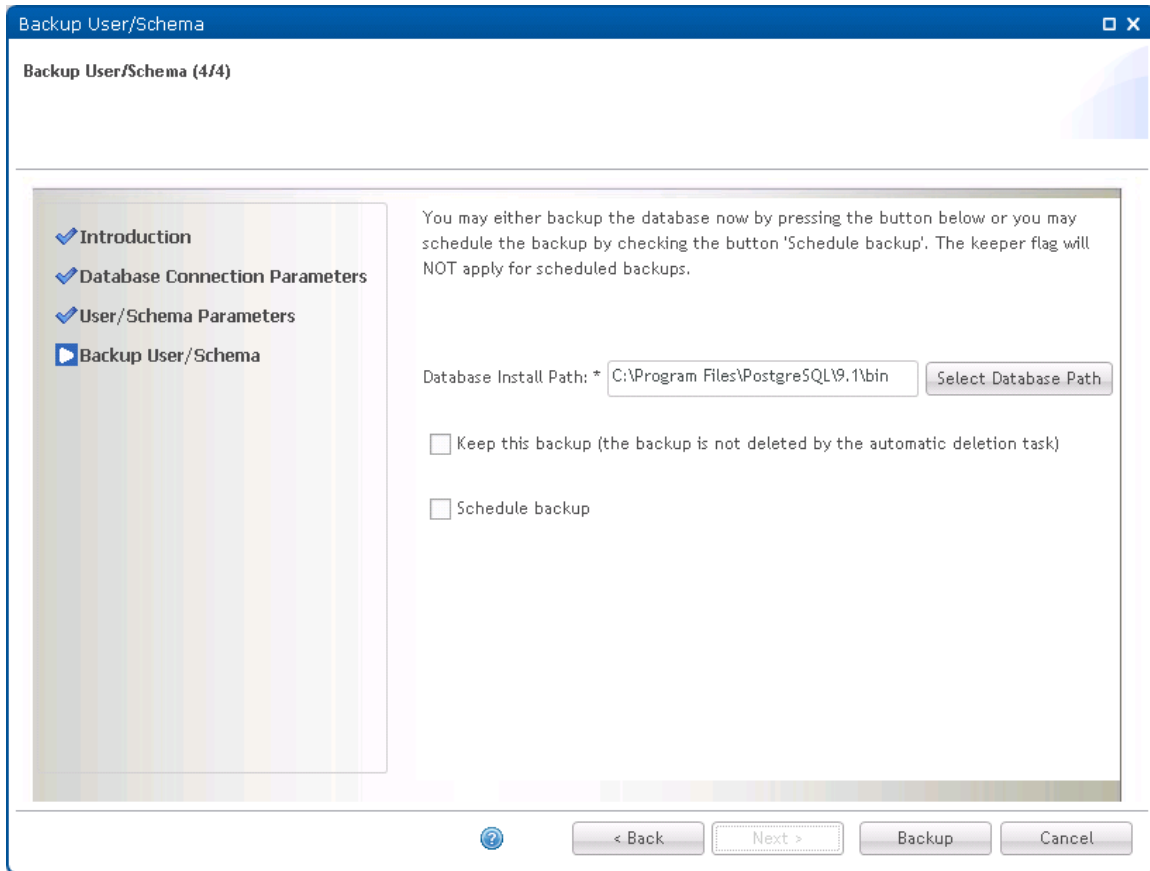
Both parameters are mandatory:

Name	Explanation
Username	Name of desired EMS user/schema
Password	Password for the desired EMS user/schema

Press Next to continue the Backup User/Schema wizard.

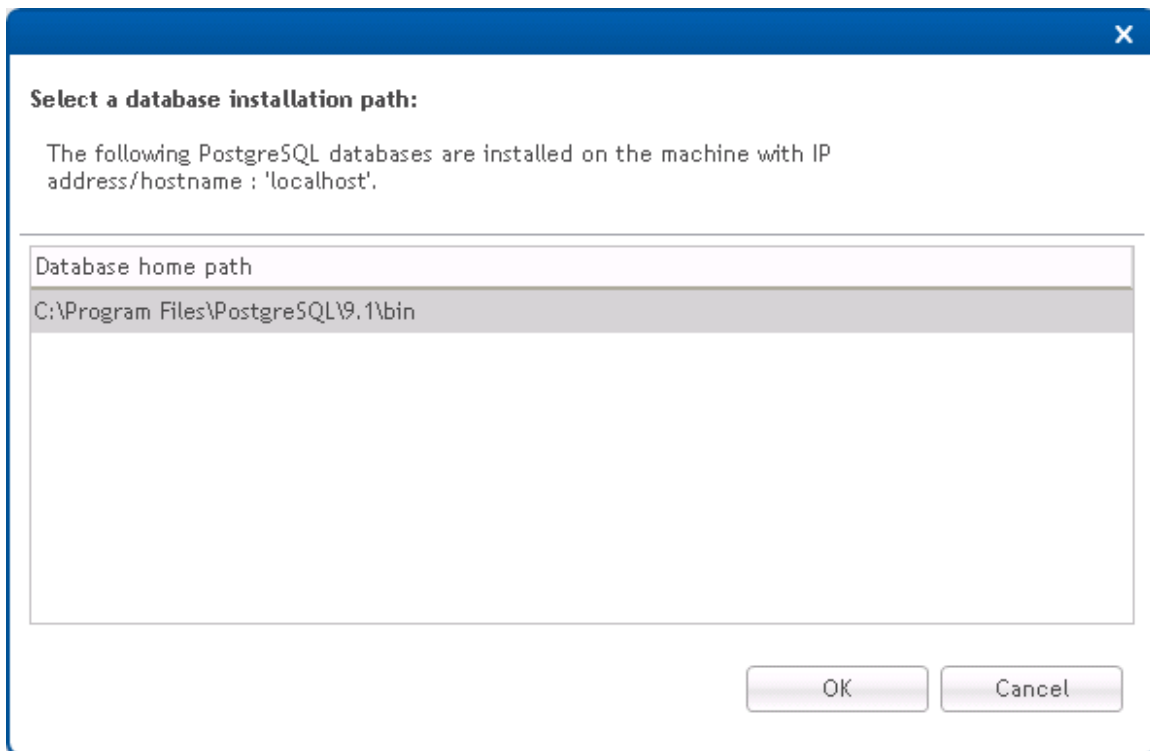
Backup Wizard page 4: Backup User/Schema

This is the final page in the Backup User/Schema Wizard.

Figure 329 Backup Wizard page 4 : Backup User/Schema

The Database Install Path is the database server path to the tools System Manager needs to run backup and restore operations. The tools in question are exp.exe and imp.exe for Oracle and pg_dump and pg_restore for Postgres.

If the Database Install Path is empty, press the Select Database Path to allow System Manager to try to find the Database Install Path automatically:

Figure 330 Selecting a database installation path

If System Manager fails to locate the correct path for you, you have to supply the correct path yourself.

Be aware that in a 2+0 configuration (EMS server and EMS database on separate machines), backup files are stored on both servers. The backup files are zipped to reduce disk space consumption, but you should make sure to select a file system with enough free disk space to hold the backup files.

It is possible to change the backup file storage location on the EMS server. It is also possible to configure System Manager to delete backups older than a given number of days. If enabled, all backup files created by periodic backup jobs will be targeted for deletion. In a 2+0 configuration old backup files are deleted on the database server as well as on the EMS server. The storage location and old backup files deletion settings are found in the Database settings in System Manager.

You can select either to take a backup right now, or to initiate periodic backup on the selected user/schema.

If System Manager on the database server is not compatible with the System Manager on the EMS server, the backup will be aborted with an error message. If so, you should upgrade the outdated System Manager, and then rerun the Backup User/Schema wizard.

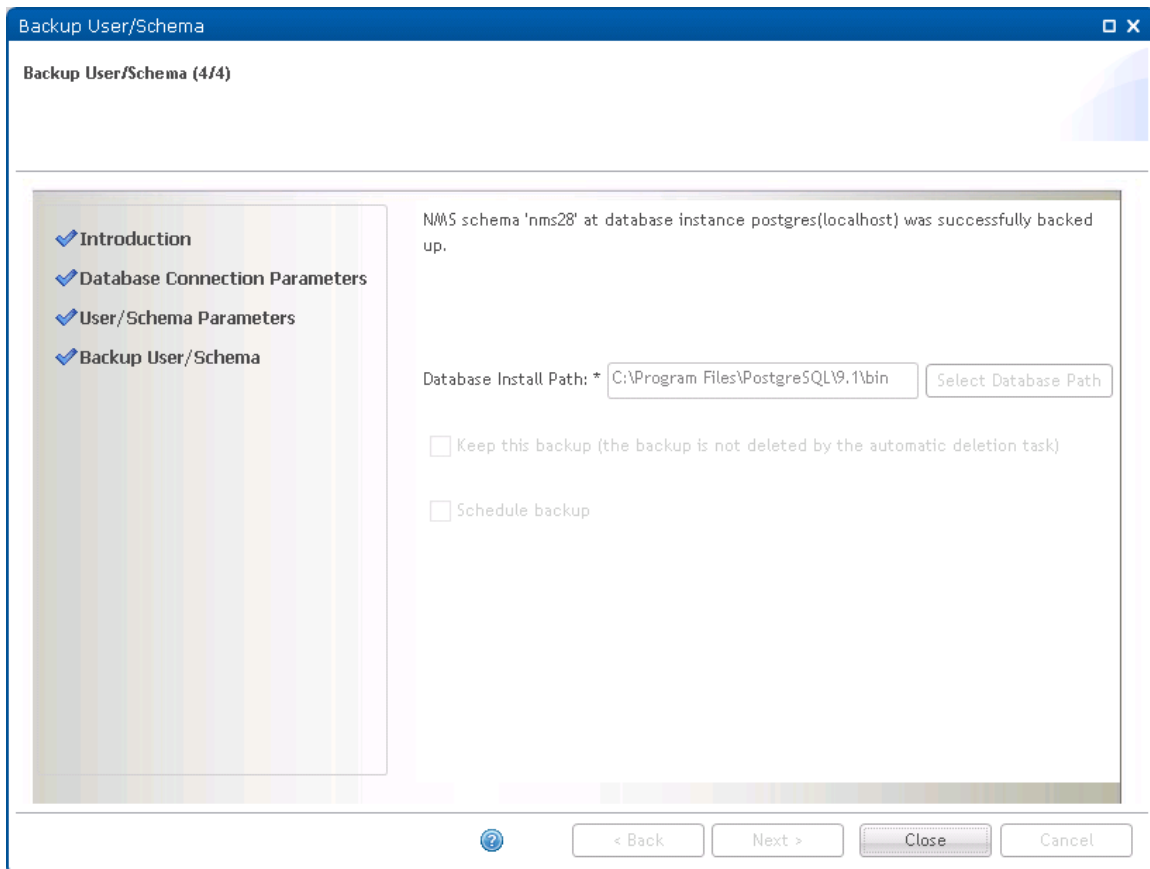
Take a backup now

Leave the Scheduled backup check box unchecked. If this is checked, System Manager will initiate periodic backup.

Check the Keep this backup check box if you want this backup to be ignored by the old backup files deletion job.

Press Backup to initiate the backup process causing the following page to appear:

Figure 331 Initiating backup process



Press Close to complete the Backup User/Schema wizard.

Initiate periodic backup

To initiate periodic backup, check the Schedule backup check box and adjust the start time and backup interval as desired. If you specify a start time in the past, the periodic backup is scheduled and the first periodic backup is taken immediately.

If you enable periodic backup, it is recommended to also enable deletion of old backup files to prevent the file system from filling up.

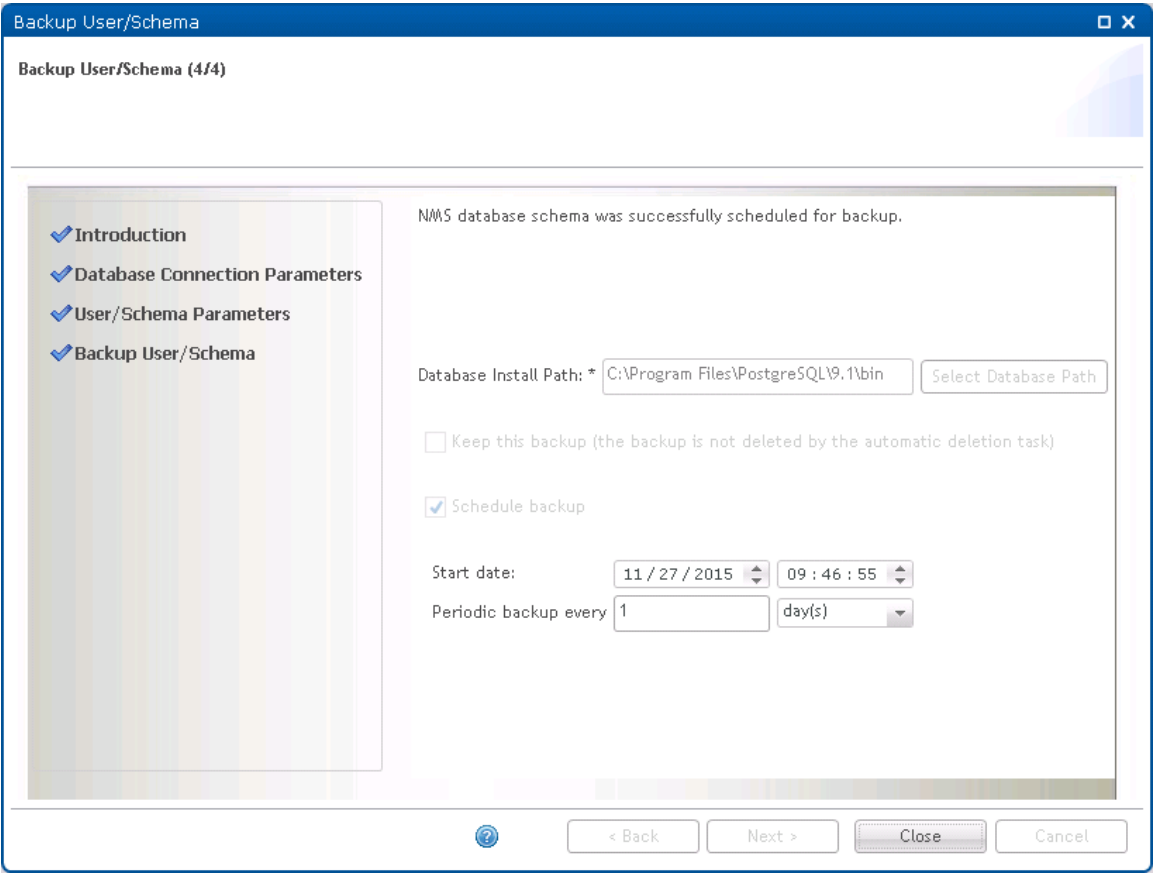
Press Schedule to schedule the periodic backup on selected EMS database:

Figure 332 Schedule of periodfic backup database

The screenshot shows a window titled "Backup User/Schema" with a subtitle "Backup User/Schema (4/4)". On the left is a sidebar with four items: "Introduction", "Database Connection Parameters", "User/Schema Parameters", and "Backup User/Schema" (which is selected and highlighted with a blue arrow). The main area contains the following text: "You may either backup the database now by pressing the button below or you may schedule the backup by checking the button 'Schedule backup'. The keeper flag will NOT apply for scheduled backups." Below this text are several fields: "Database Install Path: * C:\Program Files\PostgreSQL\9.1\bin" with a "Select Database Path" button; an unchecked checkbox "Keep this backup (the backup is not deleted by the automatic deletion task)"; a checked checkbox "Schedule backup"; "Start date:" with a date picker set to "11 / 26 / 2015" and a time picker set to "09 : 44 : 49"; and "Periodic backup every" with a text input set to "1" and a dropdown menu set to "day(s)". At the bottom are four buttons: a help icon (?), "< Back", "Next >", and "Schedule" (which is highlighted), and a "Cancel" button.

This page is shown if schedule operation was successful:

Figure 333 Schedule of periodfcic backup database complete



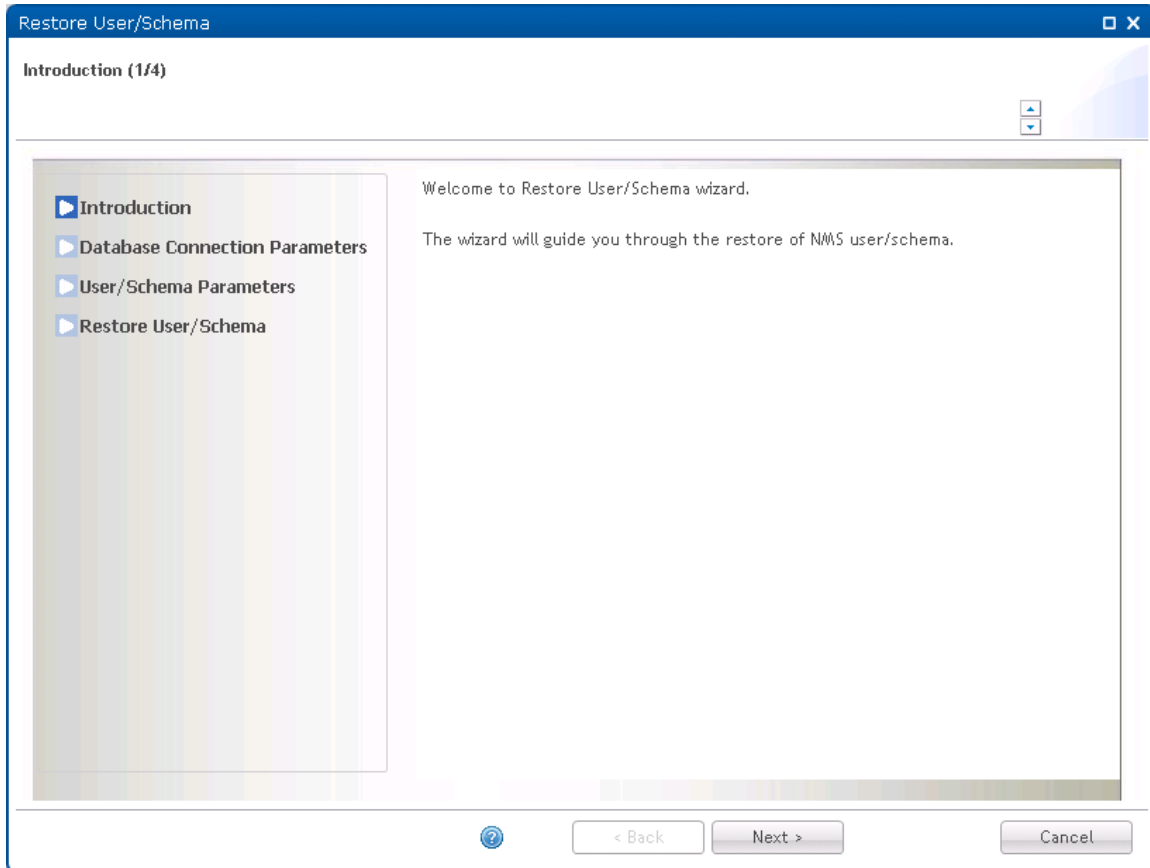
Press Close to complete the Backup User/Schema wizard.

Restore User/Schema Wizard

This wizard allows you to restore a backup file for an existing Oracle user or Postgres schema. Open the Restore User/Schema wizard from the **Administration->Database Tasks** view in System Manager.

Restore Wizard page 1: Introduction

Figure 334 Restore Wizard page 1 : Introduction



Press Next to continue the Restore User/Schema wizard.

Restore Wizard page 2: Database Connection Parameters

Specify the database connection parameters for the EMS database you want to restore.

Figure 335 Restore Wizard page 2 : Database Connection Parameters

Restore User/Schema

Database Connection Parameters (2/4)

Please review or change the default configuration below.
The fields marked with * are required.

Database connection parameters:

Database instance name: * postgres

Database type: * PostgreSQL

Database server address: * localhost

Database server port: * 5432

Database administrator user:

Username: * postgres

Password: *

Select Existing Parameters

< Back Next > Cancel

Press Select Existing Parameters button to select database connection parameters already defined in System Manager:

Figure 336 Selecting a database connection

Instance Name	Server Name/Address	Server Port	Database Type	Administrator User
postgres	nmssql	5432	PostgreSQL	postgres
nmsora	nmsora	1521	Oracle	system

OK Cancel

If the desired parameters are not present in the list, you need to fill in the parameters manually.

All parameters are mandatory:

Name	Explanation
Database instance name	Name of a database instance.
Database type	Either Oracle or Postgres.
Database server address	IP address or hostname for the database server. Use localhost for a 1+0 configuration.
Database server port	Tcp port for the database. Default 1521 for Oracle, 5432 for Postgres.
Username	The database system user needed to restore the EMS user/schema.
Password	Password for the database system user.

Please notice that in order to do restore, you need to have a Database administrator user with sufficient privileges.

Press Next to continue the Restore User/Schema wizard.

Restore Wizard page 3: User/Schema Parameters

Specify the Oracle user or Postgres schema you want to restore.

Figure 337 Restore Wizard page 3 : User/Schema Parameters

Restore User/Schema

User/Schema Parameters (3/4)

Please review or change the default configuration below.
The fields marked with * are required.

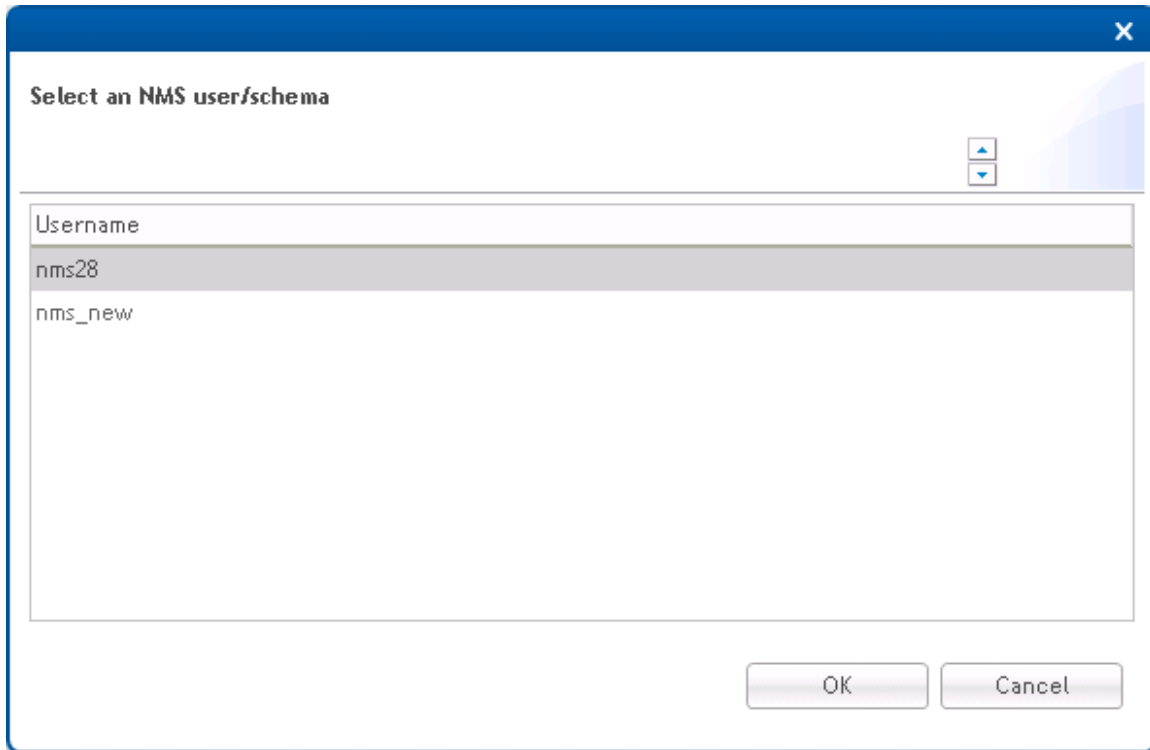
☒ Introduction
☒ Database Connection Parameters
☒ **User/Schema Parameters**
☐ Restore User/Schema

Enter the NMS database schema name and password or use the button below to select existing parameters from System Manager configuration files.

Username:*

Password:*

Press Select Existing Parameters button to select existing parameters already defined in System Manager:

Figure 338 Selecting user/schema

If the desired parameters are not present in the list, you have to fill in the parameters manually.
Both parameters are mandatory:

Name	Explanation
Username	Name of desired EMS user/schema
Password	Password for the desired EMS user/schema

Press Next to continue the Restore User/Schema wizard.

Restore Wizard page 4: Restore User/Schema

This is the final page in the Restore User/Schema Wizard.

Figure 339 Restore Wizard page 4 : Restore User/Schema

Restore User/Schema

Restore User/Schema (4/4)

The fields marked with * are required.

☒ Introduction
☒ Database Connection Parameters
☒ User/Schema Parameters
☒ Restore User/Schema

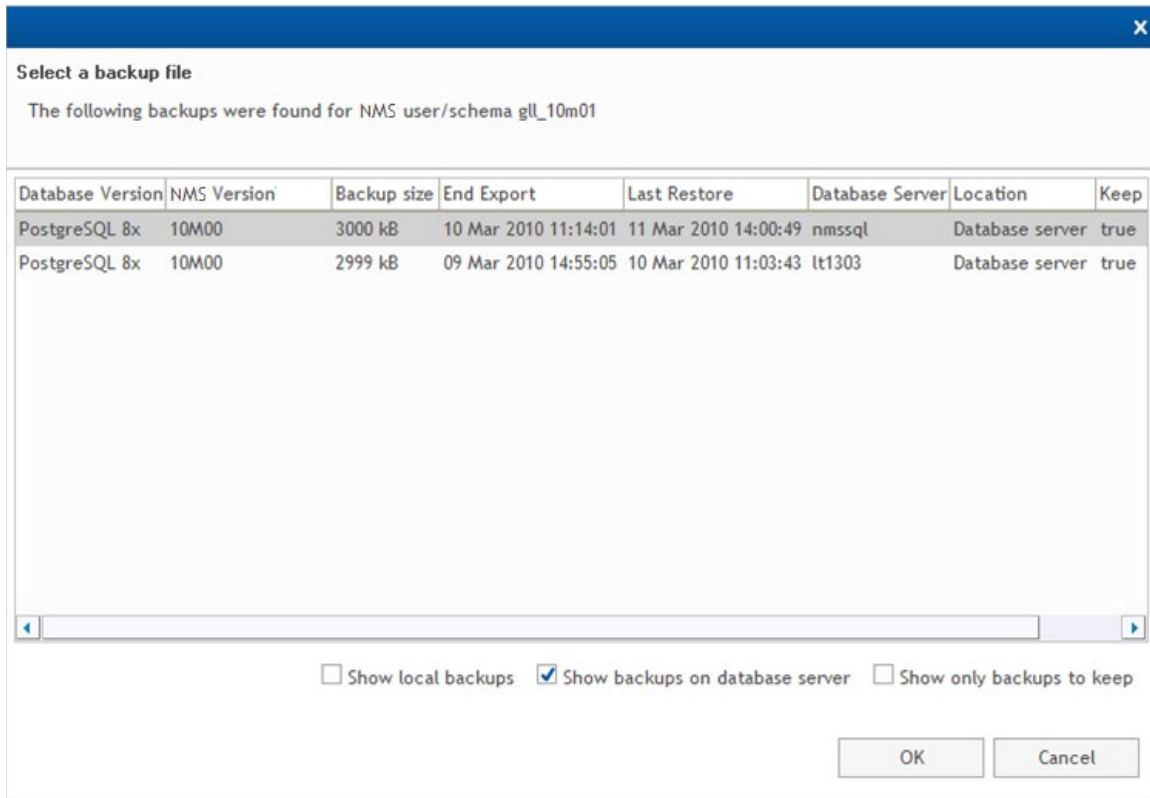
You chose to restore the active NMS schema. Confirm by checking the button below if this is really that you want to do. If NMS server is running, it will be stopped. Select the backup file to be restored and the database installation path before continuing the operation.

☒ Confirm to restore the active NMS database schema

Backup File: * 20151128-094739-postgres-nms28.backup.gz

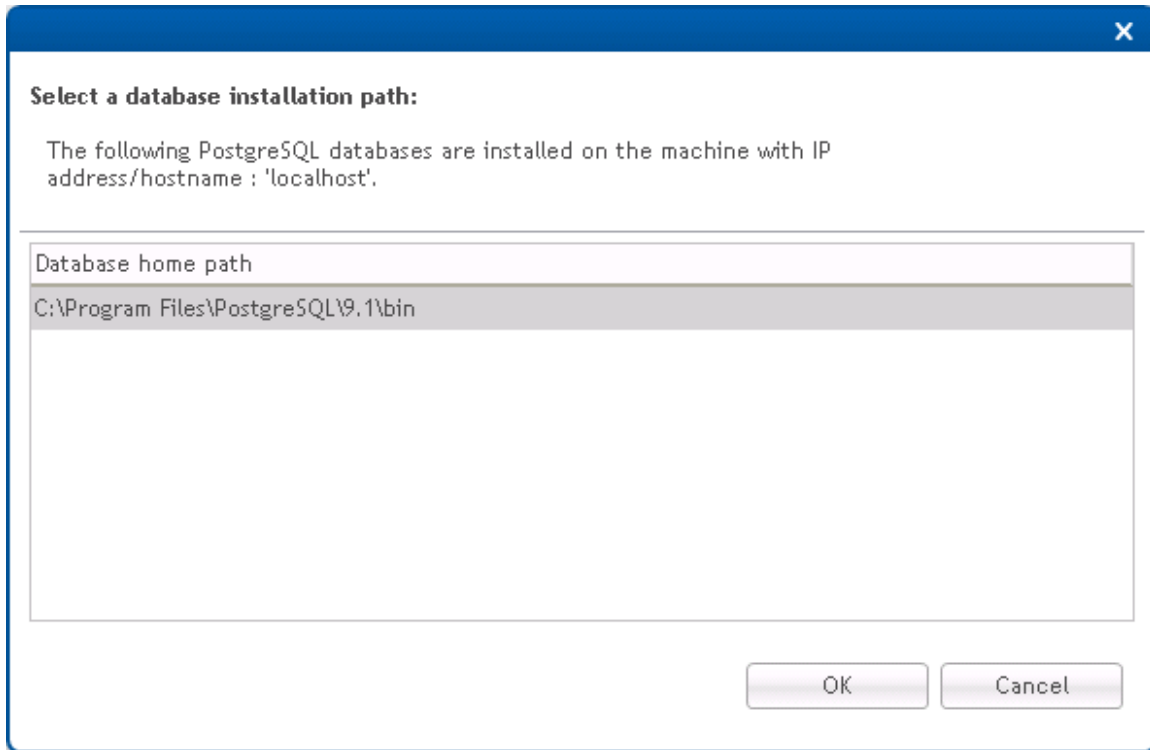
Database Install Path: * C:\Program Files\PostgreSQL\9.1\bin

Press the Select Backup File button to select an existing database backup.

Figure 340 Selecting a backup file

The Database Install Path is the database server path to the tools System Manager needs to run backup and restore operations. The tools in question are exp.exe and imp.exe for Oracle and pg_dump and pg_restore for Postgres.

If the Database Install Path is empty, press the Select Database Path to allow System Manager to try to find the Database Install Path automatically:

Figure 341 Selecting a database installation path

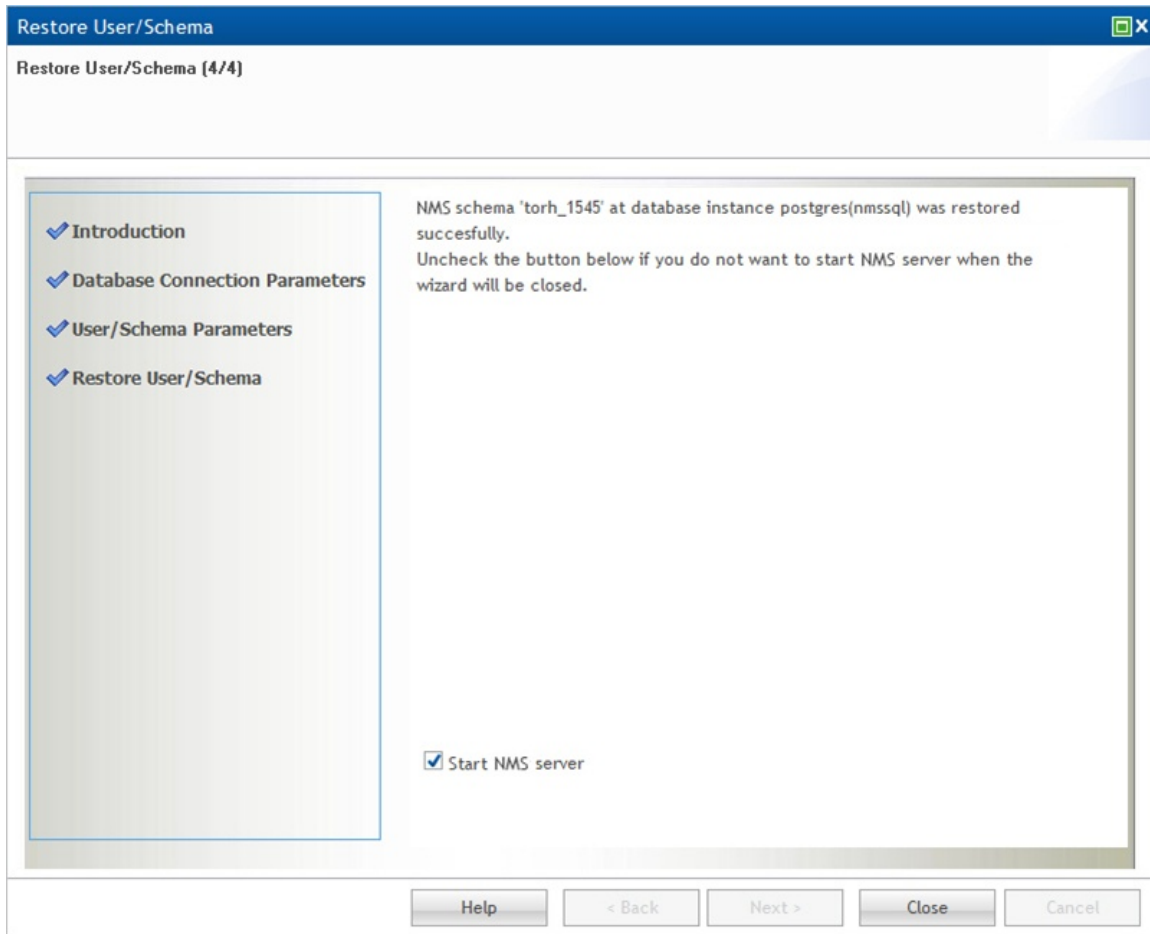
If System Manager fails to locate the correct path for you, you have to supply the correct path yourself.

Check the Confirm to restore the active EMS user/schema check box to confirm that you want to proceed with the operation.

Press Restore to initiate the restore operation. If EMS server is started, it will be stopped.

If System Manager on the database server is not compatible with the System Manager on the EMS server, the backup will be aborted with an error message. If so, you should upgrade the outdated System Manager, and then rerun the Restore User/Schema wizard.

The following page appears after a successful restore operation:

Figure 342 Restore of database file

Uncheck the Start EMS Server check box if you don't want to start the EMS server.

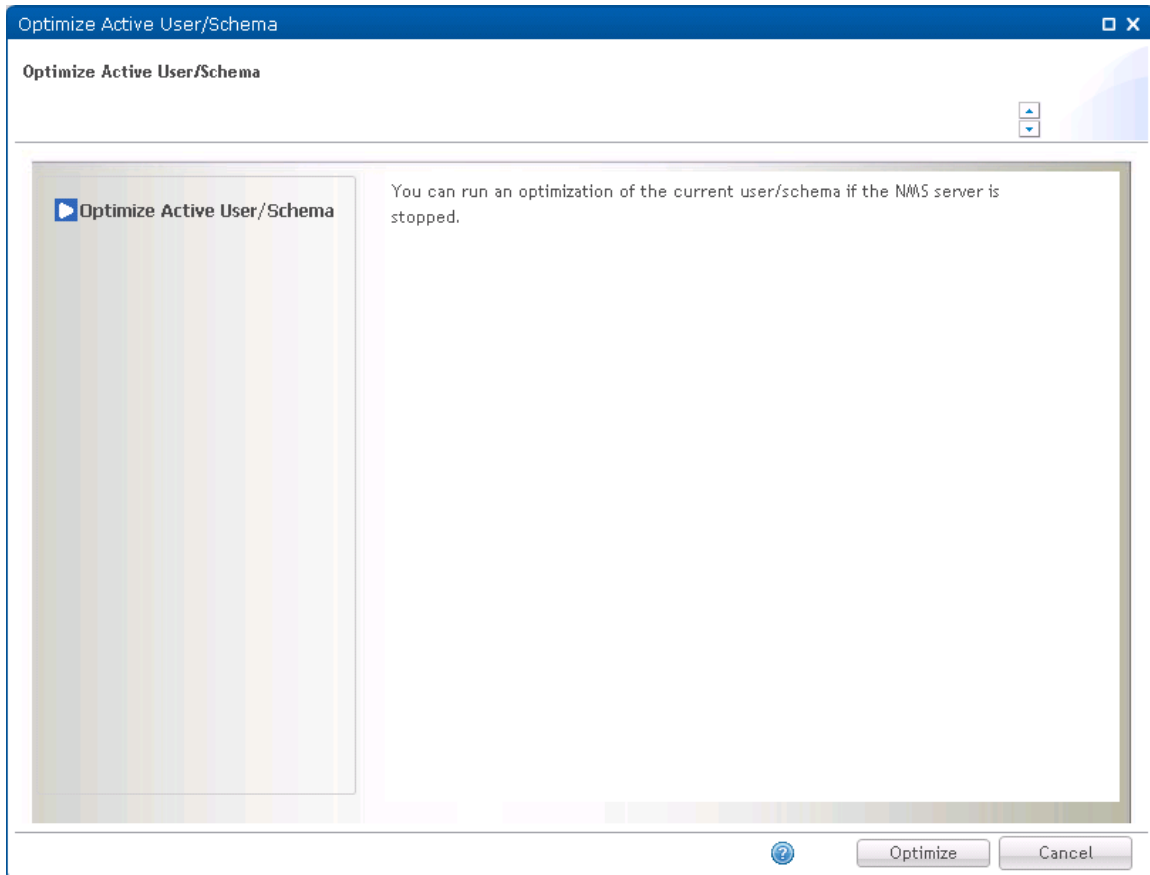
Press Close to complete the Restore User/Schema wizard.

Optimize Active NMS User/Schema

This wizard allows you to optimize the space consumption of the active user/schema.

Open the Optimize Active User/Schema wizard from the **Administration > Database Tasks** view in System Manager.

Figure 343 Optimize Active User/Schema wizard



Press Optimize to optimize the space consumption of the active user/schema.

Analyze User/Schema Wizard

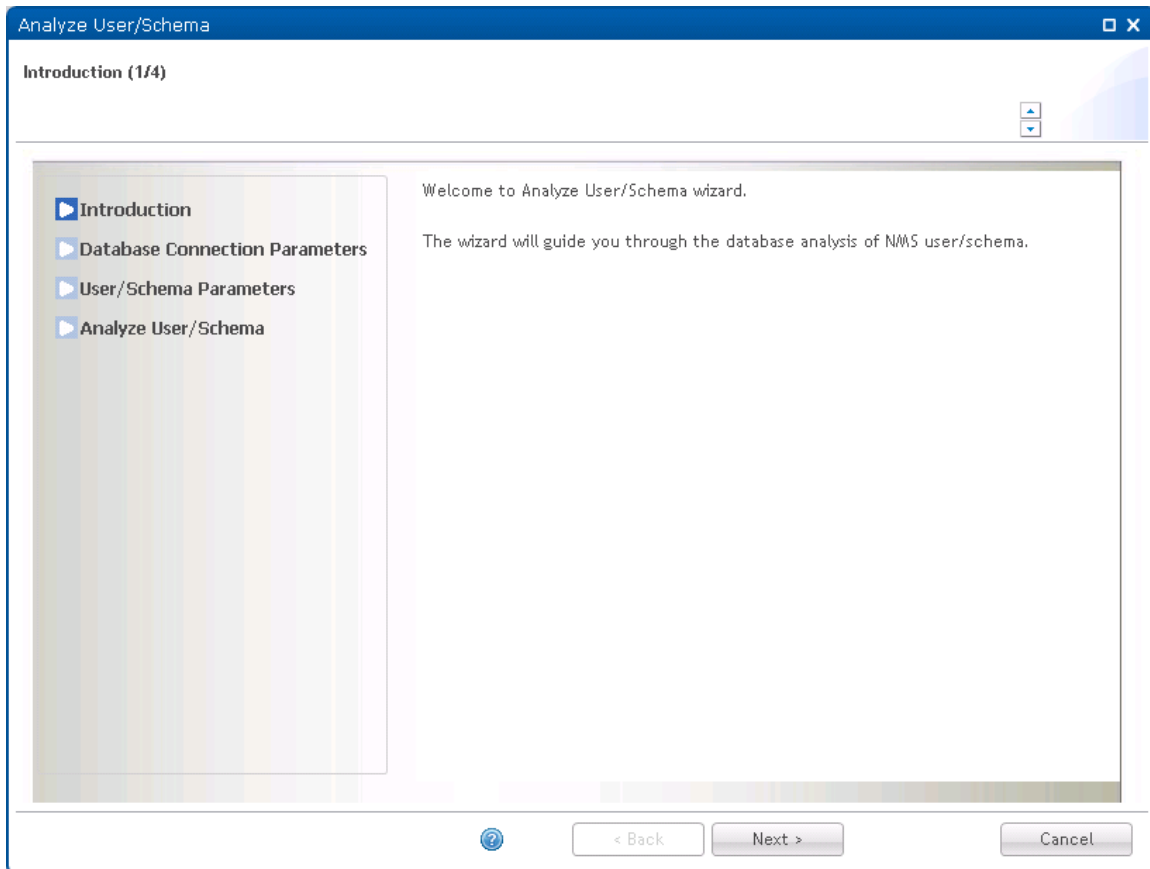
This wizard allows you to analyze an existing EMS database for possible problems.

Open the Analyze User/Schema wizard from the **Administration->Database Analysis** view in System Manager.

The reports generated by the Analyze User/Schema wizard are intended to aid problem solving in connection with customer cases reported to Customer Support.

Analyze Wizard page 1: Introduction

Figure 344 Analyze Wizard page 1 : Introduction



Press Next to continue the Analyze User/Schema wizard.

Analyze Wizard page 2: Database Connection Parameters

Specify the database connection parameters for the EMS database you want to analyze.

Figure 345 Analyze Wizard page 2 : Database Connection Parameters

Analyze User/Schema

Database Connection Parameters (2/4)

Please review or change the default configuration below.
The fields marked with * are required.

Database connection parameters:

Database instance name: * postgres

Database type: * PostgreSQL

Database server address: * localhost

Database server port: * 5432

Database administrator user:

Username: * postgres

Password: *

Select Existing Parameters

< Back Next > Cancel

Press Select Existing Parameters button to select database connection parameters already defined in System Manager:

Figure 346 Selecting a database connection

Instance Name	Server Name/Address	Server Port	Database Type	Administrator User
postgres	nmssql	5432	PostgreSQL	postgres
nmsora	nmsora	1521	Oracle	system

OK Cancel

If the desired parameters are not present in the list, you need to fill in the parameters manually.

All parameters are mandatory:

Name	Explanation
Database instance name	Name of a database instance.
Database type	Either Oracle or Postgres.
Database server address	IP address or hostname for the database server. Use localhost for a 1+0 configuration.
Database server port	Tcp port for the database. Default 1521 for Oracle, 5432 for Postgres.
Username	The database system user needed to analyze the EMS user/schema.
Password	Password for the database system user.

Please notice that in order to analyze, you need to have a Database administrator user with sufficient privileges.

Press Next to continue the Analyze User/Schema wizard.

Analyze Wizard page 3: User/Schema Parameters

Specify the Oracle user or Postgres schema you want to analyze.

Figure 347 Analyze Wizard page 3 : User/Schema Parameters

Analyze User/Schema

User/Schema Parameters (3/4)

Please review or change the default configuration below.
The fields marked with * are required.

✓ Introduction
✓ Database Connection Parameters
▶ **User/Schema Parameters**
▶ Analyze User/Schema

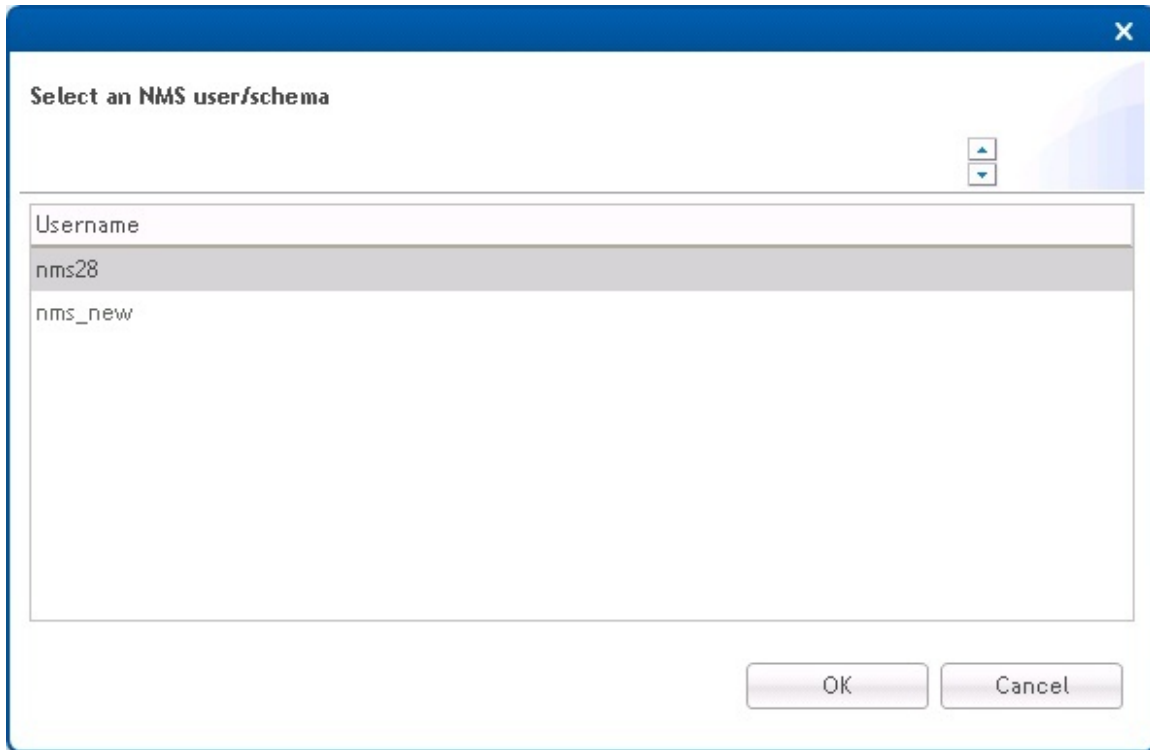
Enter the NMS database schema name and password or use the button below to select existing parameters from System Manager configuration files.

Username:* nms28
Password:* •••••

Select Existing Parameters

< Back Next > Cancel

Press Select Existing Parameters button to select existing parameters already defined in System Manager:

Figure 348 Selecting a user/schema

If the desired parameters are not present in the list, you have to fill in the parameters manually.

Both parameters are mandatory:

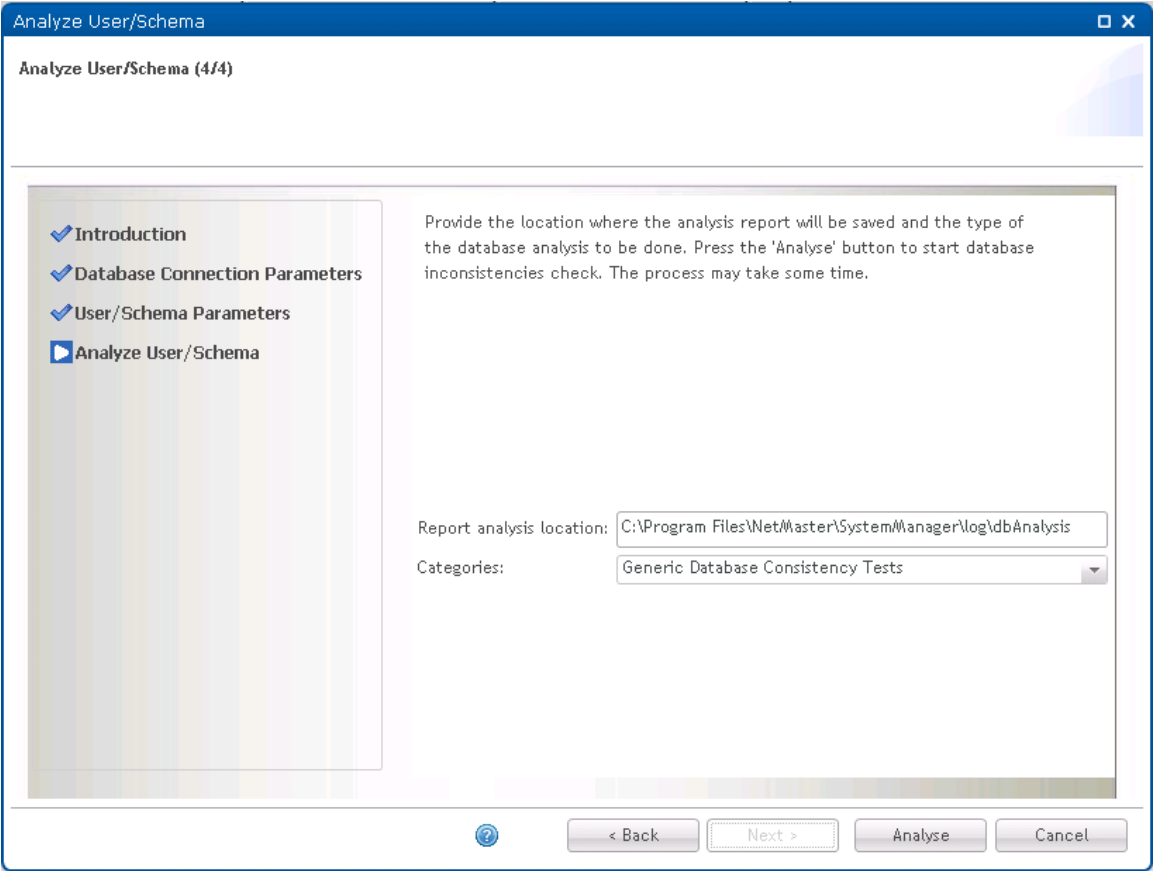
Name	Explanation
Username	Name of desired EMS user/schema
Password	Password for the desired EMS user/schema

Press Next to continue the Analyze User/Schema wizard.

Analyze Wizard page 4: Analyze User/Schema

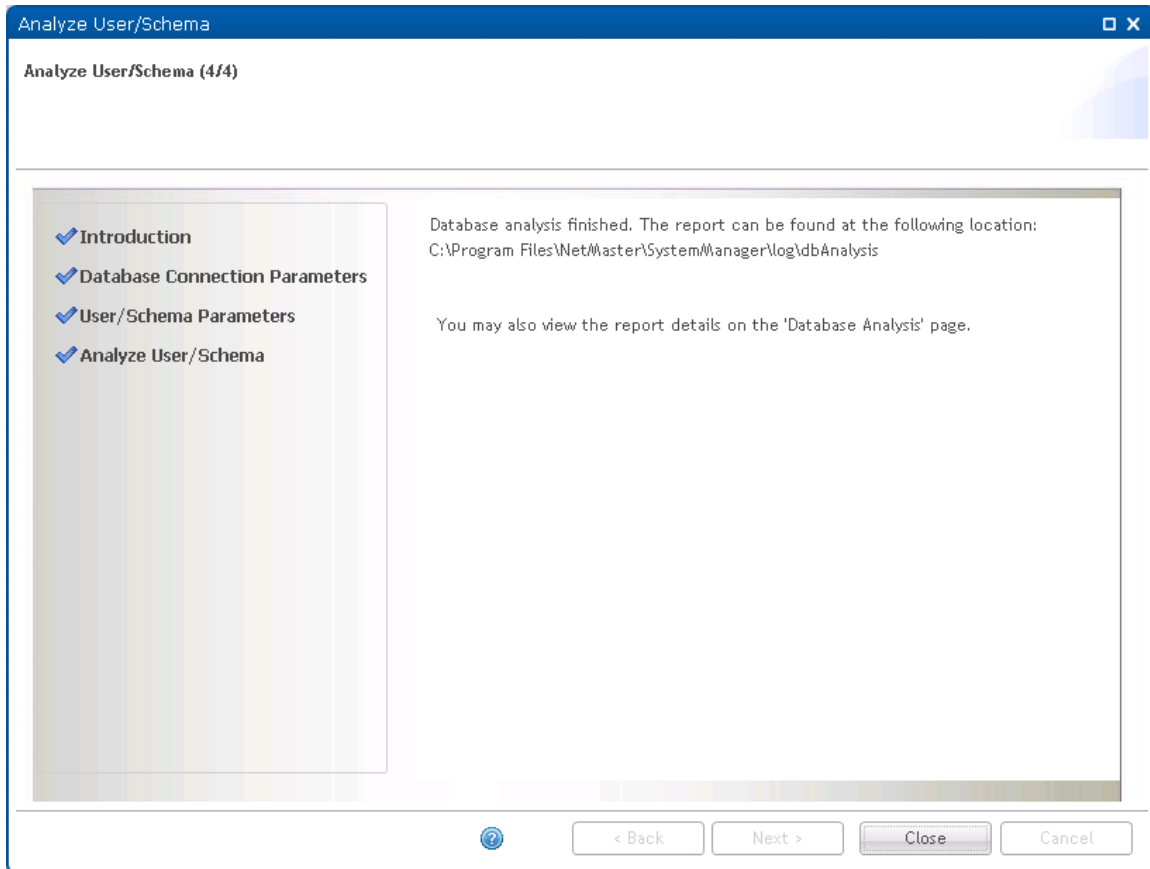
This is the final page in the Analyze User/Schema Wizard.

Figure 349 Analyze Wizard page 4 : Analyze User/Schema



Name	Explanation
Report analysis location	Where to put the analysis reports. Default location: C:\PTP820NMS\SystemManager\log\dbAnalysis
Categories	Drop down list box containing two possible values: <ul style="list-style-type: none">Database Consistency Tests after Upgrade A set of database tests related to upgrade (for the full list of tests, refer to File content display area).Generic Database Consistency Tests A set of general database related tests (for the full list of tests, refer to File content display area).

Press Analyze to initiate the analyze process causing the following page to appear:

Figure 350 Analyze Wizard page 4 : Initiate analyze process

See the Administration->Database Analysis view help for more information.

Press Close to complete the Analyze User/Schema wizard.

Note that if a test or several tests fail, the output will list the database operation that failed, and the actual versus the expected result.

License menu

License Administration View

Shows overview of current imported EMS license, with option to run

- [Import License wizard](#) to import a new license into EMS.
- [Update Capabilities wizard](#) to invoke the additional capabilities provided by a new imported license.

To open this view, you can either:

- Open License menu and click License Administration
- Locate and click the main area License Administration tab, if present

License Administration view content

License Administration view contains a link to launch the Import License wizard and a license content display area.

Figure 351 License administration

Dashboard **License Administration** »

Use [Import License](#) wizard to import a new license.

Use [Update capabilities](#) wizard to update the NBI and Scheduled Reports capabilities.

A license was found in the default location (NMS installation path):

Path	C:\Program Files\Juniper Networks\Server\JBoss-4.2.3\server\license\sw-nms.key
Customer	En
Edition	EM
License no.	8222
Major version	14
Minor version	2
Server version	14B00 31
License type	Commercial
License state	Not activated
Expiry date	07:18:29 Mar 11 2015
Activation key	8222-14B00-31-14B00-31-14B00-31-14B00-31
No. of clients	24
No. of TRX	400000
Alarm to service correlation	Enabled
CLI Script Broadcast	Enabled
End to end service management	Enabled
Northbound SNMP No. of Network	40000
Open SNMP elements	400000
Radius authentication	Enabled
Redundancy	Enabled
Redundancy No. of TRX	400000
Scheduled Reports No. of Network	40000

License number: 8222

Activation code (select and press Ctrl+C to copy):

Activation key: 8222-14B00-31-14B00-31-14B00-31-14B00-31

- Click on the Import License link to open the [Import License wizard](#).

To be able to generate valid license files, Customer Support needs the activation key. This information is therefore available in a copy and paste friendly area at the bottom of the License Administration view.

The Activation key in the License Info dialogue is generated from the MAC-address of one of the enabled network cards on the EMS server. In order to be absolutely certain of which network card the license is bound to it is recommended to disable all network cards except one. When the License is activated with this Activation key, the license will be locked to this network card. If the network card later is disabled, the EMS server will stop with a “violation lock” error message.

- Click on the Update capabilities link to open the [Update Capabilities wizard](#).

Import License Wizard

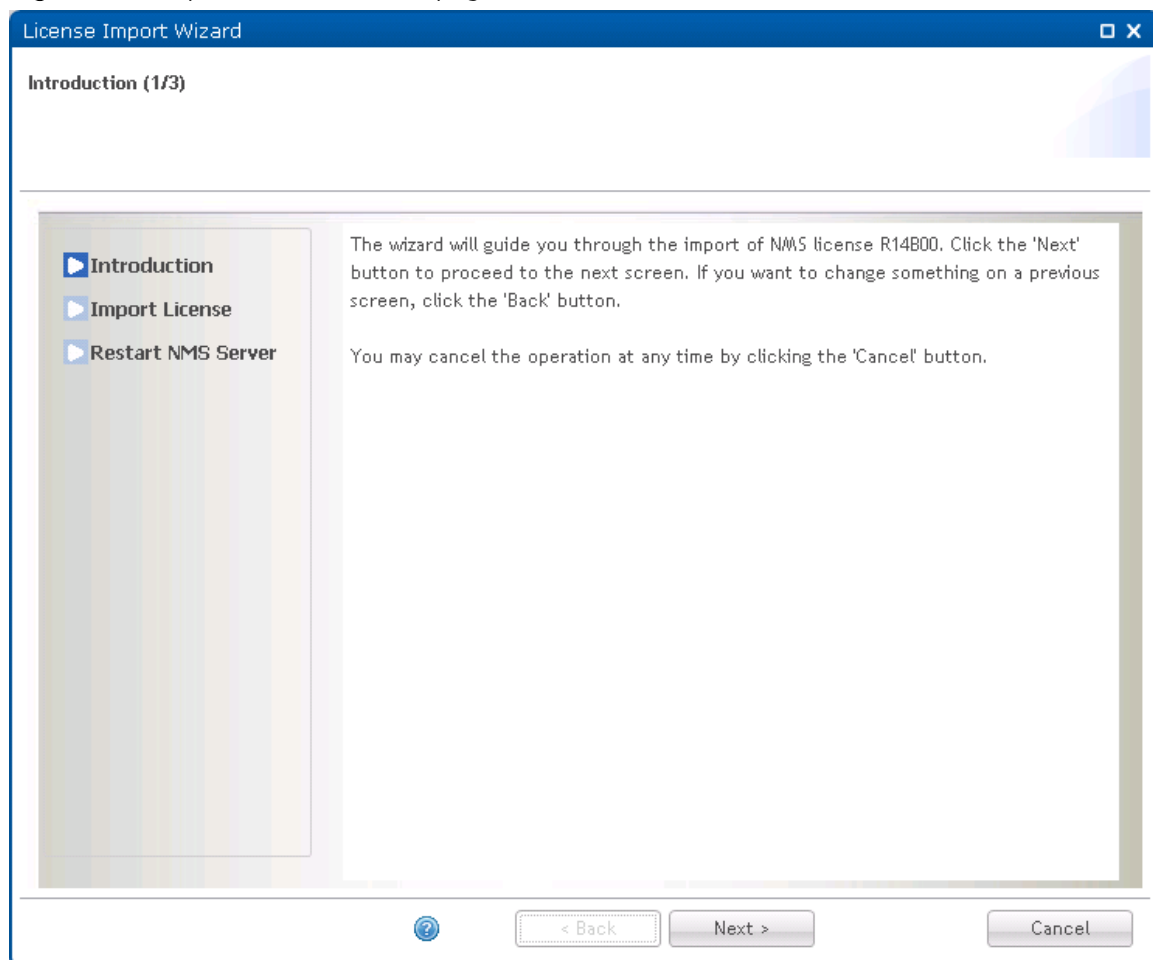
This wizard allows you to import a new license into EMS.

Open the Import License wizard from the License->License Administration view in System Manager.

Import License Wizard page 1: Introduction

The first page shown is the introduction giving an overview of the wizard steps:

Figure 352 Import License Wizard page 1 : Introduction

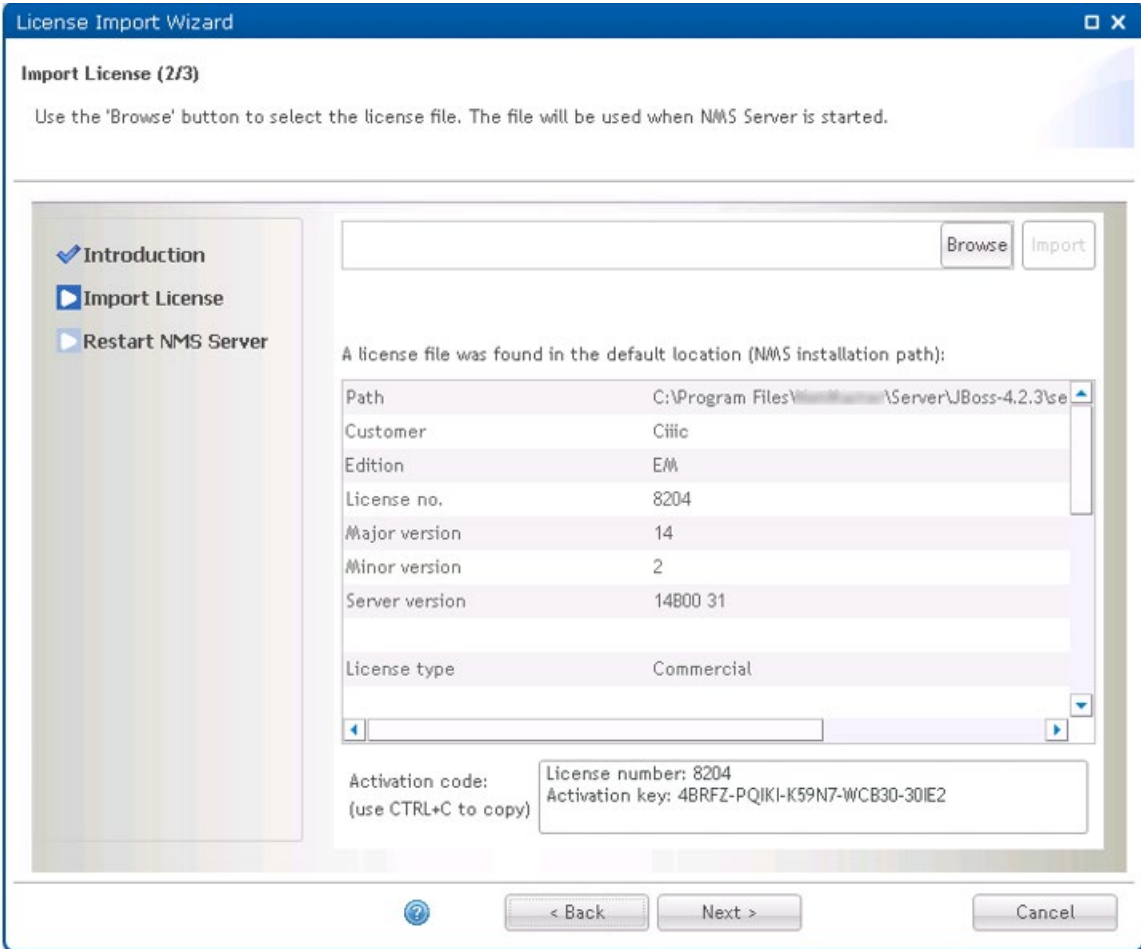


Press Next to continue the Import License wizard.

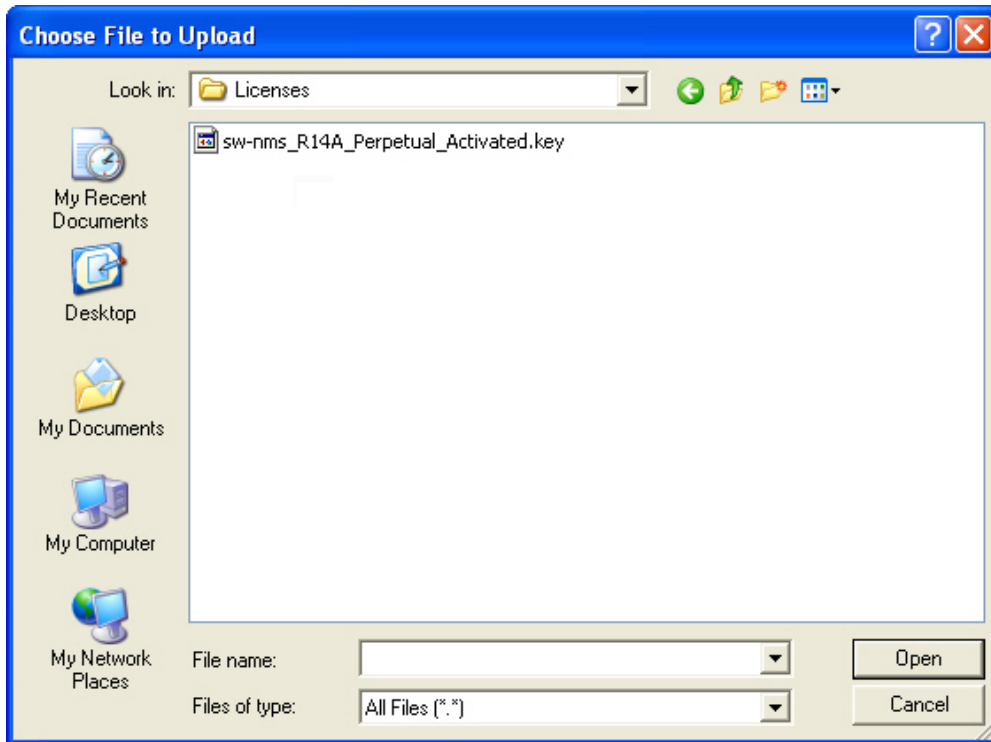
Import License Wizard page 2: Import License

EMS requires a valid license. A new license file is required for all major EMS releases.

Figure 353 Import License Wizard page 2 : Import License

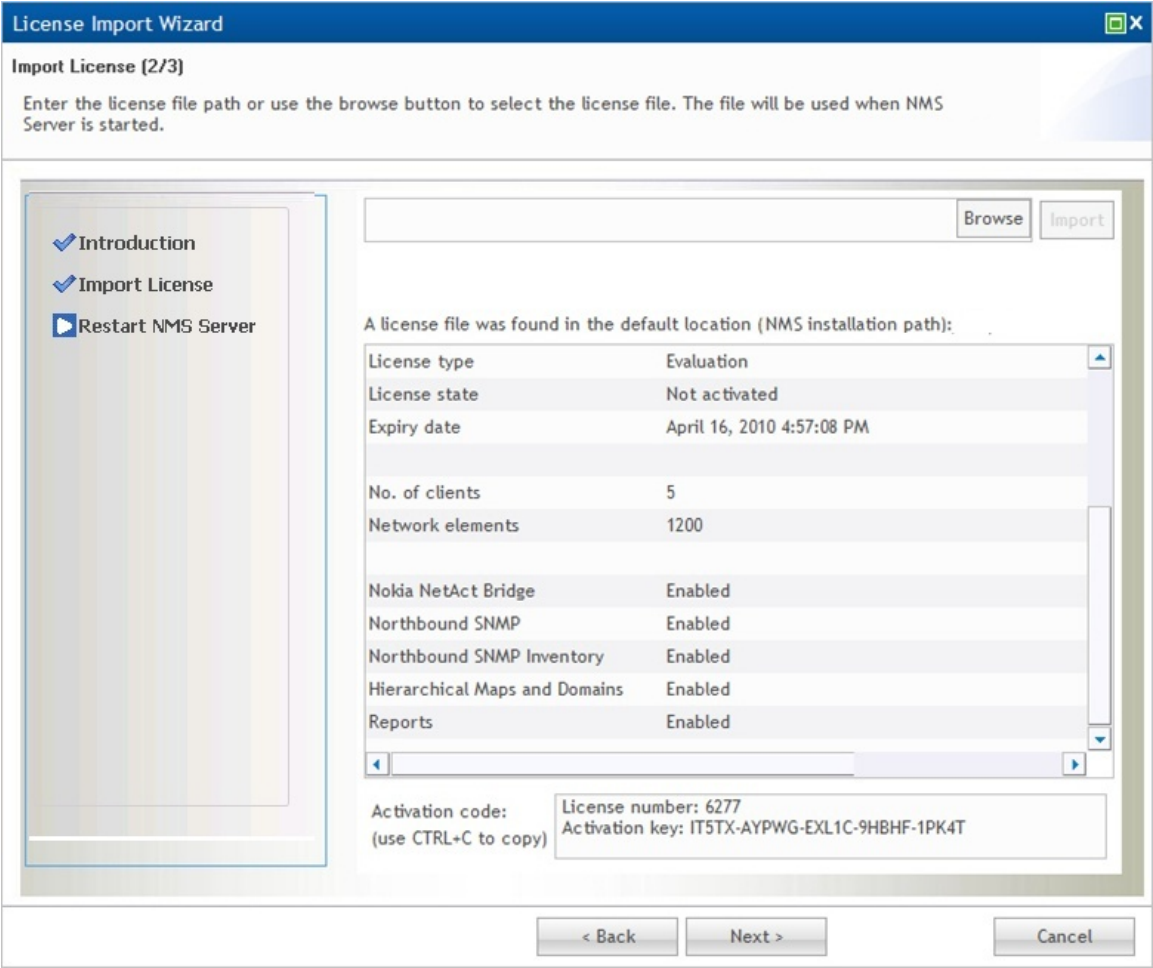


Press Browse to locate your license file:

Figure 354 Import License Wizard page 2 : selecting file

Select the license file and press Open, then press the Import button to import the license into EMS:

Figure 355 Import License Wizard page 2 : Import License



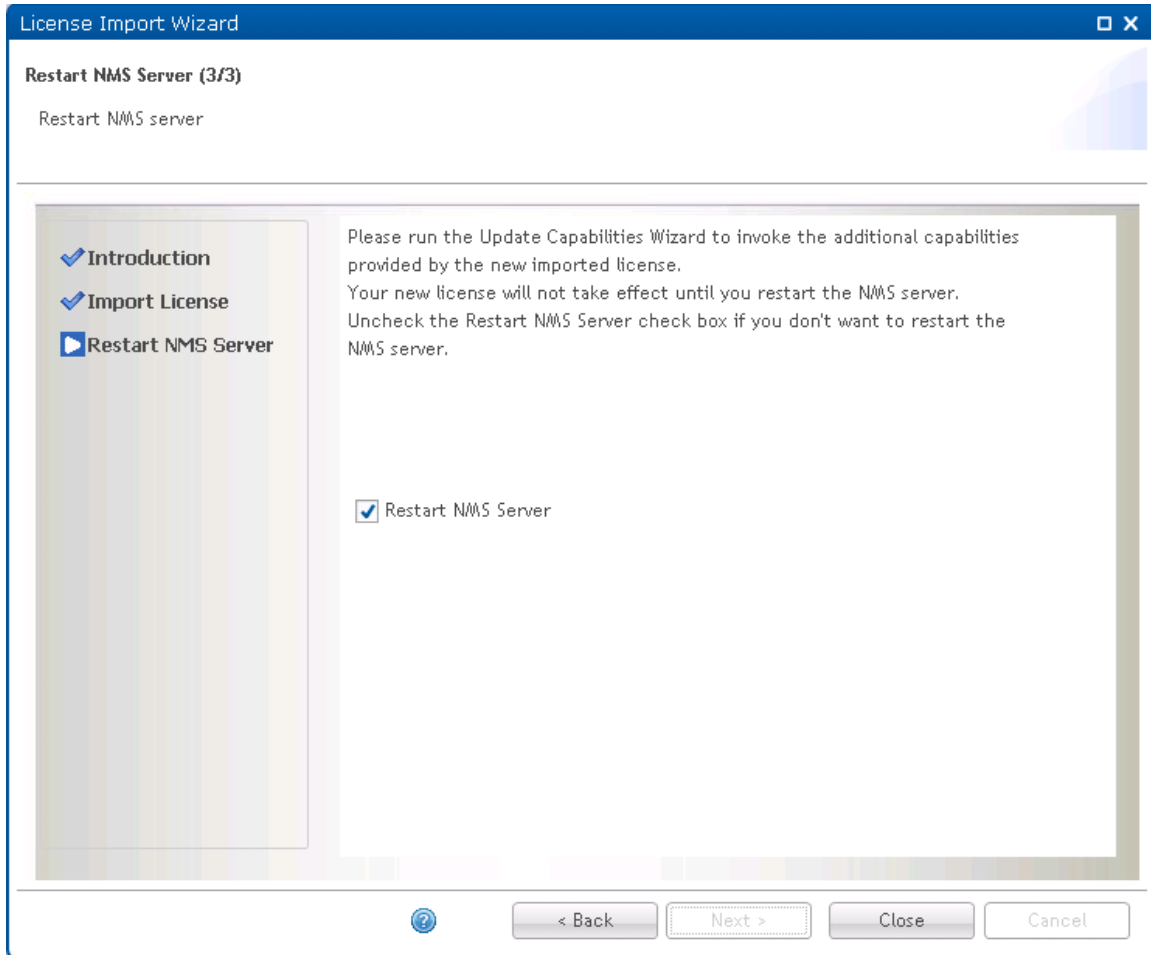
You may have to copy the license file to a local disk for the import action to work.

Press Next to continue the Import License wizard.

Import License Wizard page 3: Restart server

This is the final page in the Import License wizard.

Figure 356 Import License Wizard page 3 : Restart server



Uncheck the Restart EMS Server check box if you don't want to restart the EMS server.

Press Close to complete the Import License wizard.

Update Capabilities wizard

Use this wizard following the import of a new license to invoke the additional capabilities provided by the new imported license.

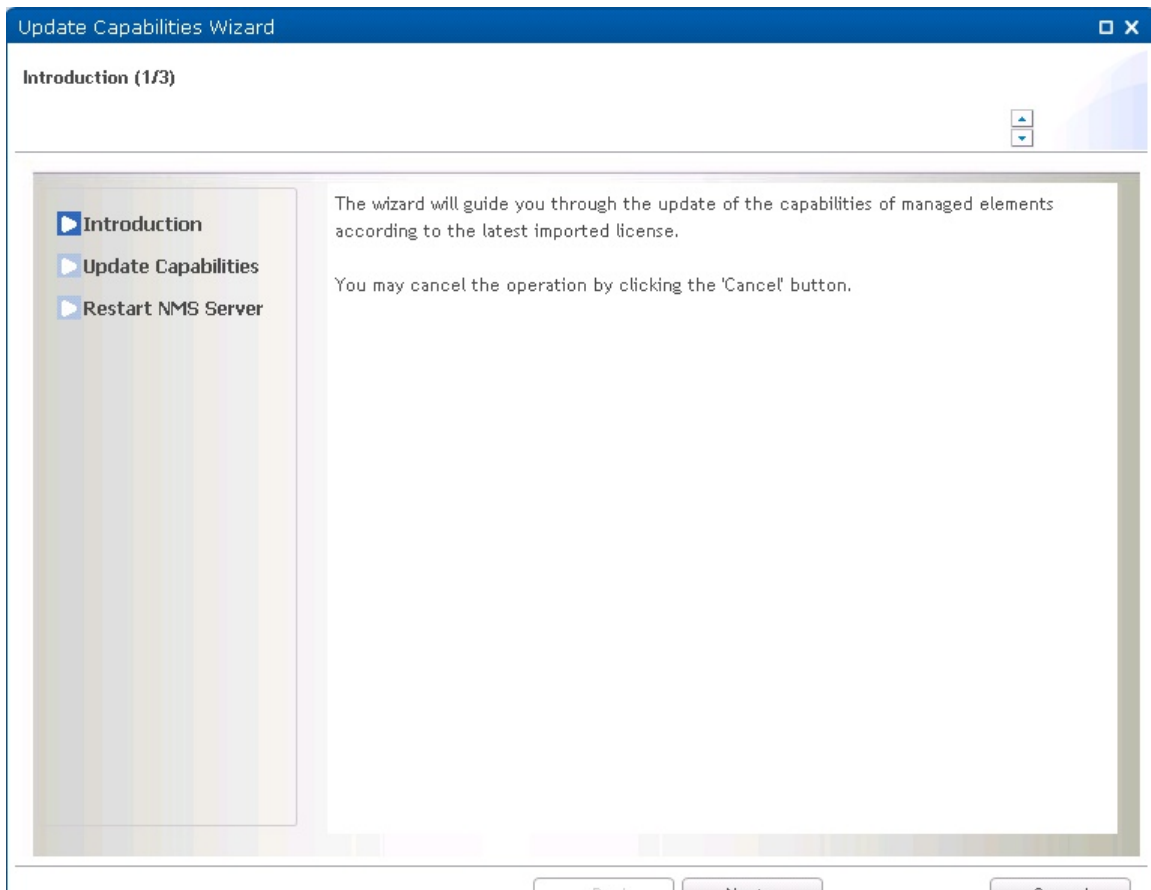
This is necessary in the following case: If you start managing an element after the capabilities of the current license were consumed, then even after you import a license with a higher number of capabilities, elements that previously did not receive any capabilities will still not receive any, unless you run the Update Capabilities wizard.

Open the Update Capabilities wizard from the License->License Administration view in System Manager.

Update Capabilities Wizard page 1: Introduction

The first page shown is the introduction giving an overview of the wizard steps:

Figure 357 Update Capabilities Wizard page 1 : Introduction

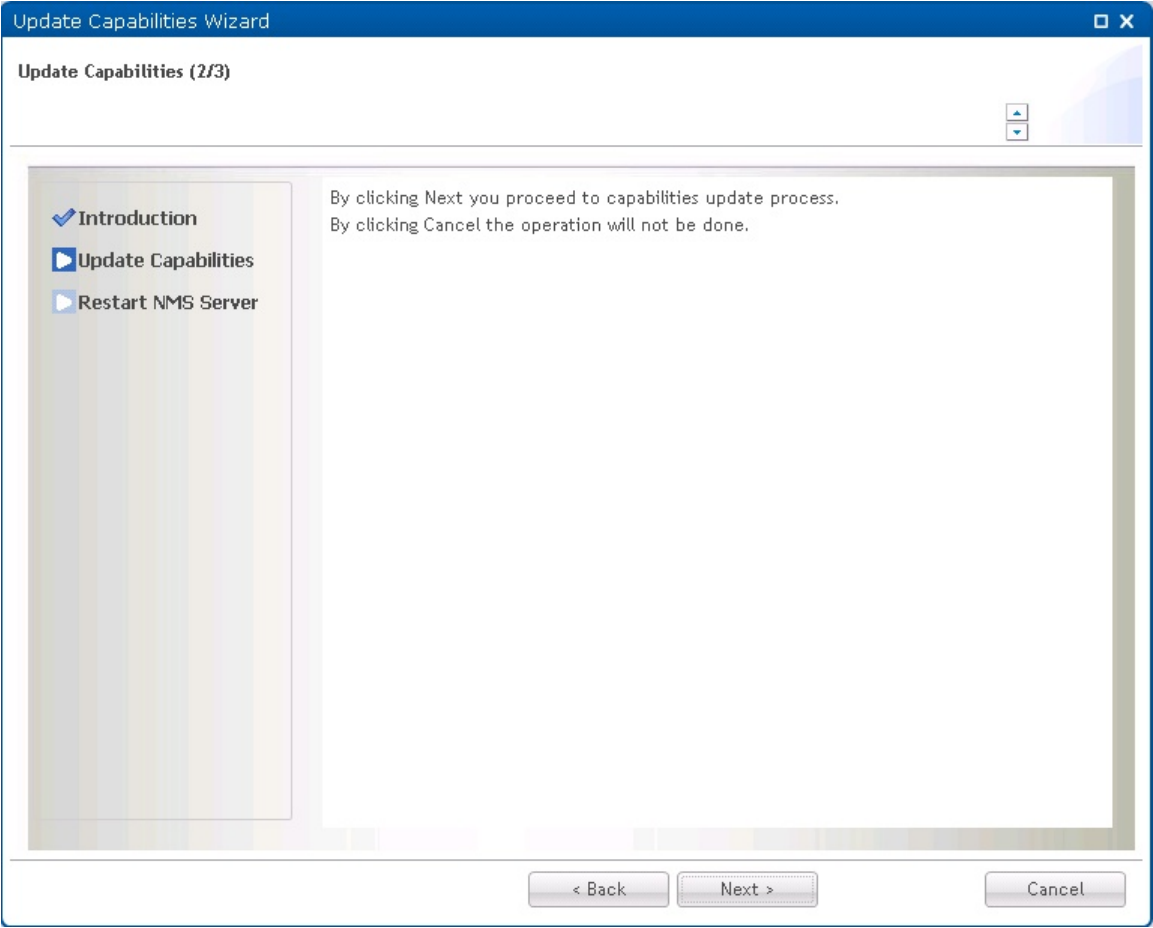


Press Next to continue the Update Capabilities wizard.

Update Capabilities Wizard page 2: Update Capabilities

You can proceed to the next page and update the capabilities, or cancel the operation.

Figure 358 Update Capabilities Wizard page 2 : Update Capabilities



Update Capabilities Wizard page 3: Update Capabilities

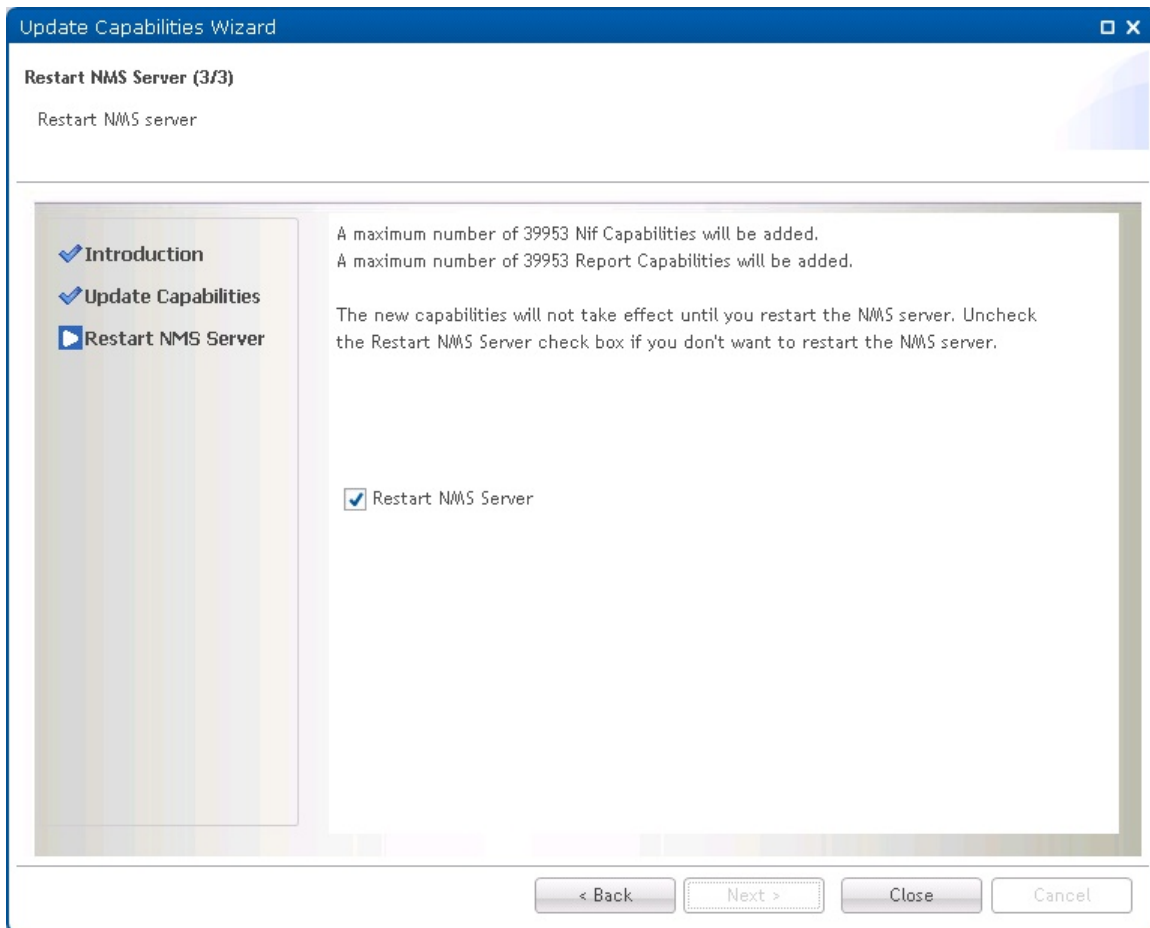
This page lists the number of NIF capabilities and Report capabilities that will be added. For example, if:

- The current license capabilities include 10 Scheduled Reports and
- The Imported new license capabilities include 1000 Scheduled Reports

Then after invoking the Update Capabilities wizard, this page informs you that 990 Report Capabilities will be added.

Note that if the new license has a smaller number of capabilities than the previous one, capabilities will not be erased.

Figure 359 Update Capabilities Wizard page 3 : Update Capabilities



Uncheck the Restart EMS Server check box if you don't want to restart the EMS server.

Press Close to complete the Update Capabilities wizard and update the capabilities of managed elements.

Settings menu

PTP 820 NMS Server View

This view contains EMS server related settings that allows you to:

Enable email notification if EMS server stops unexpectedly

- Reset the EMS root password on active EMS database
- Update scalability parameters for the EMS server

To open this view you can either:

- Open Settings menu and click EMS Server
- Locate and click the main area EMS Server tab, if present

PTP 820 NMS Server view content

EMS Server view contains scalability parameters, Snmp Trap Port Number, a check box for email notification configuration and a button for resetting the EMS server root password:

Figure 360 EMS server view content

Use the following settings for adjusting the scalability parameters to improve NMS server performance when managing large networks. One must be aware that changing the parameters may cause NMS to stop working. NMS server must be restarted for any changes of the parameters to take effect. Whenever NMS server stops unexpectedly because of an error situation, an email notification can be sent by selecting the checkbox below.

The license allows for up to 400000 elements. Maximum Connection Pool Size should be between 9-10% of the elements in managed state plus 100 but no more than 600

NMS Server Settings

Maximum Connection Pool Size:

Maximum Thread Pool Size:

Maximum Heap Size (MB):

Snmp Trap Port Number:

☐ Send notification when NMS server stops unexpectedly

The NMS root user may be reset if an active database configuration is set.

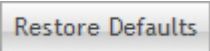


The following fields can be updated:

Table 62 EMS server page attributes

Name	Explanation
Maximum Connection Pool Size	<p>Specifies the maximum number of physical connections that can be created in the pool. Increase this parameter to allow for greater concurrency.</p> <p>Maximum Connection Pool Size cannot be larger than available connections configured in database. For Oracle database, consider increasing the PROCESSES parameter. For PostgreSQL database, consider increasing the max_connections and max_prepared_transactions parameters. Maximum Connection Pool Size cannot be less than 150. The default value is set to 150</p>
Maximum Thread Pool Size	<p>The application uses thread pools to manage concurrent tasks.</p> <p>Maximum Thread Pool Size must be at least 100 and cannot be larger than 90% of Maximum Connection Pool Size. The default value is set to 100. For Windows machines, the value cannot be larger than 250, and for Solaris machines, the value cannot be greater than 5000. It is also recommended that Maximum Thread Pool Size to be at least 10% of the number of elements in managed state.</p>
Maximum Heap Size	<p>Increase this parameter when the application needs a lot of memory.</p> <p>Maximum Heap Size must be at least 512 MB. For Windows machines, the value cannot be greater than 1300 MB. The default value is set to 512MB. It is also recommended that Maximum Heap Size to be at least 300 MB + 0,5 MB x the number of elements in managed state and not more than 50% of available physical memory.</p>
Snmp Trap Port Number	<p>The port that EMS listens to for incoming element traps. The trap port must be available for EMS on the system where EMS is running.</p> <p>Default trap port is 162. One reason to change the port number can be to avoid port conflicts caused by other SNMP monitoring tools that are running in parallel with EMS on the same server.</p> <p>If you need to change the port number, you will have to configure your elements to send traps on the new trap port.</p> <p>Before changing this value, please make sure that all your different element types managed by EMS can be configured to use the new trap port number.</p>

	EMS supports SNMP v3 for PTP820 elements. In order to handle SNMPv3 traps while continuing to handle SNMPv1 and SNMPv2 traps, two additional ports are used internally: 1621 (for V1 and V2) and 1622 (for V3). However, because there is a single trap receiver for traps from all device types, these internal port are used for all elements that send traps to EMS.
Send notification when EMS server stops unexpectedly	Check the check box to enable email notification when EMS stops unexpectedly. See Settings->Email Notification for email notification setup.

When managing large networks of elements (> 1000 NEs) it is recommended to adjust the scalability parameters for better performance. Changing the values of the scalability parameters requires EMS server restart for the changes to take effect.

Operation	Explanation
	Revert to default (check box not checked)
	Make current check box state active
	Cancel check box change

Press the Reset EMS root user password button to reset the root password for the active EMS database.

This dialogue should then appear:



NMS HA View - Configuring High Availability

This view contains NMS High-Availability (HA) settings that allow you to define an NMS High Availability setup. For a full description of HA and how to configure it, refer to the PTP 820 NMS Server High Availability chapter in the PTP 820 NMS Installation Guide.

Figure 361 NMS HA view

Use the following settings to set the High Availability (HA) mode of the NMS server. When saving these settings the NMS Server on this machine must be stopped.

Setting the Server Mode to Primary requires that:

- The same NetMaster software version is installed on both machines, the local and the mate.
- The Mate Server System Manager is running on the Mate machine.
- Connectivity exists between the two System Managers.
- The NMS Server on the mate machine is stopped.

HA Settings

Server Mode: Standalone

Automatic Switch Time(mins): 120

Time for sync file system(mins): 60

Mate Server IP:

Mate Username

☒ File Synchronization Pause

Restore Defaults Save Cancel Generate Keys

If HA is already configured, the configurable settings depend on whether the server is the Primary server or the Secondary server.

- If this server is the Primary server, all fields can be edited.
- If this server is the Secondary server, only the Server Mode field can be edited. All other settings are view-only. This means that you can change the Secondary server's mode, to either:
 - Primary – If you set a Secondary server to be the Primary server, you must reconfigure HA anew, as described in [Configure PTP 820 NMS Server for High Availability](#). The only step you do not need to perform is that of generating and copying encryption keys.
 - Standalone – In this case, the Primary server become unable to communicate with its mate, and its HA Configuration Status in the System Manager's dashboard is "Could not communicate with mate".

To configure or edit HA, set the following:

Table 63 EMS server page attributes

Input Fields	Explanation
Server Mode	<p>Specify the HA mode of the EMS server to which this client is connected:</p> <ul style="list-style-type: none"> Primary – this server is the Primary server in the HA setup, and the Secondary server is the server specified in the Mate server IP. Standalone – this server is not participating in an HA setup.
Automatic Switch Time (mins)	<p>The amount of time that the Secondary server should remain as the Active server following a switchover, regardless of the Primary server's status. If the Primary server remains in the up state continuously throughout the Automatic Switch Time period, a switchover is performed to switch the Primary server back to Active mode. However, if the Primary server goes down during the Automatic Switch Time period, countdown is reset, and is started new as soon as the Primary server restarts.</p> <p>The switchover is smooth; if any tasks are in progress, switchover is delayed until the tasks are completed. All scheduled tasks are switched over from the Secondary to the Primary, to be run as scheduled.</p> <p>During this time period, if the Secondary server stops, the Primary server automatically becomes the Active server if it is running.</p> <p>The default setting is 120 minutes.</p>
Time for sync file system (mins)	<p>Specify the frequency of mate-to-mate synchronization. During synchronization, any files on one mate that are more up to date than the other mate's files, or are missing in the other mate, are copied from one mate to the other.</p> <p>The default setting is 60 minutes.</p>
Mate server IP	The IP of the mate server.
Mate Username	The domain username of the mate server. This is necessary to enable access for file synchronization purposes.
File Synchronization Pause	<p>When this checkbox is checked, file synchronization between the two mates is not performed.</p> <p>This is useful for example in cases where you wish to remove old files from the file system. In this case, check the checkbox, and then delete the old files from both servers, to prevent the files from being copied back at the next File Synchronization. When you finish deleting the files, uncheck the checkbox.</p>

System Manager View

System Manager related settings. Allows you to:

- Change System Manager root password

Default root password is "pw" and should be changed as soon as possible.

To open this view you can either:

- Open Settings menu and click System Manager
- Locate and click the main area System Manager tab, if present

System Manager contents

This is where you can change the System Manager root user password:

Figure 362 System manager contents

Dashboard

System Manager

Use the following settings to change the System Manager user password. The current password is required in order to do this change. The fields marked with * are required.

Change System Manager user password

Old password: *

New password: *

Confirm password: *

Save

Cancel

Input Fields	Explanation
Old password	Old password. Default is "pw".
New password	New password. Must be at least 2 characters and can only consist of: a-z, A-Z, 0-9, @, -, _, #, ., and \$.
Confirm password	Type new password once more to prevent accidental typos.

Press Save button to change password or press Cancel button to cancel the changes.

Email Notification View

This view contains the necessary settings System Manager needs to be able to send email notifications.

It is possible to configure System Manager to send email notifications if:

- EMS server stops unexpectedly (see [EMS Server settings](#))
- Scheduled database optimization fails (see [Database settings](#))
- Scheduled database backup fail (see [Database settings](#))

To open this view you can either:

- Open Settings menu and click Email Notification
- Locate and click the main area Email Notification tab, if present

Email Notification view content

Email Notification view contains input fields for email notification configuration:

Figure 363 Email notification view content

The Email parameters are used when sending email to one or more recipients (the email addresses must be separated by ',' or ';'). Email notification may be sent when scheduled database backups have finished with errors, or when NetMaster server has stopped because of an error situation.
The fields marked with * are required.

Email Notification Settings

Mail protocol: SMTP

Mail Server Address:* mymailserver.com

Mail Server Port:* 25

From Address: santa@northpole.com

To Address:* me@myself.com

☒ Mail Server Authentication

Username:* myuser

Password:* ••••••••

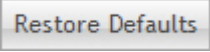

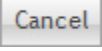
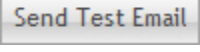
Restore Defaults Save Cancel Send Test Email

If you want email notification, you need to fill in the following settings:

Name	Explanation
Mail Server Address	IP address or hostname to your SMTP server.
Mail Server Port	SMTP port on your mail server. Default is 25.

From Address	The email address that will appear as the email sender. Be aware that no validation is performed whether this is a real email address or not.
To Address	Email recipient. May be a list of email addresses, separated by comma or semicolon.
Username	Username for Mail Server Authentication.
Password	Password for Mail Server Authentication.

The following operations are available:

Operation	Explanation
	Revert to default (set port to 25, clear all other fields).
	Save Email Notification settings.
	Cancel changes.
	Send a test email to verify current Email Notification settings.

Database View

This view contains database related settings that allows you to:

- Change backup files storage location
- Enable/disable old backup files deletion job
- Enable/disable database optimization job
- Enable/disable email notification in case a scheduled job fails
- Enable/disable email notification in case a database optimization job fail

To open this view, you can either:

- Open Settings menu and click Database
- Locate and click the main area Database tab, if present

Database view content

EMS Server view contains database related settings:

Figure 364 Database view content

Dashboard

Database

Use the following settings to automatically delete old backups. The number of days to keep old backups is by default set to 15. If the database server is not on the same machine as the NMS server, backup files will be copied also on the database server. Whenever the backup failed because of an error situation, an email notification can be sent by selecting the checkbox below.

Database Backup Settings

Backup location: C:\NgnMS\backup\database\

☒ Automatic deletion of historical backups

Days to keep database backups: 15

☐ Send notification when backup task fails

Restore Defaults

Save

Cancel

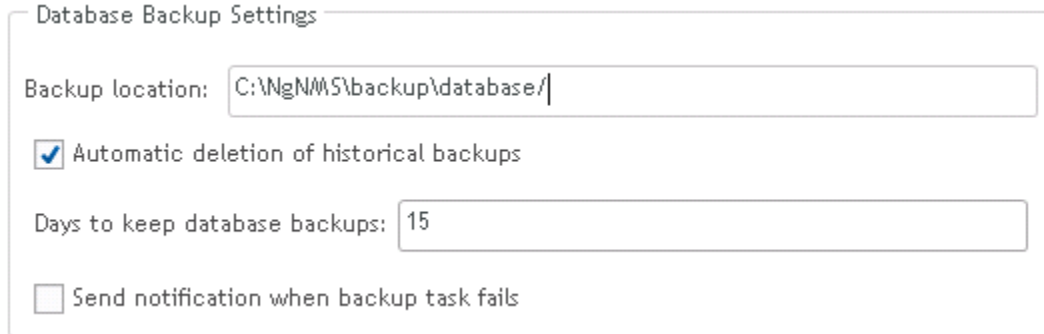
The following operations are available:

Operation	Explanation
Restore Defaults	Revert to default values.
Save	Save current state.
Cancel	Cancel changes.

Database Backup Settings

Available database backup related settings:

Figure 365 Database backup settings



Database Backup Settings

Backup location:

☒ Automatic deletion of historical backups

Days to keep database backups:

☐ Send notification when backup task fails

Database backup and restore must take place on the database server, so the backup files are stored there. If EMS Server is installed on a separate machine, the backup files are also copied to the location given in the Backup location setting on the EMS machine.

You can enable automatic deletion of old backup files. By default days to keep is set to 15.

The job is scheduled to run at 04:00 nightly.

If the database server is on a separate machine, the old backup files deletion job will delete old backup files from both the EMS Server and the database server.

Check the Send notification when backup task fails check box to enable email notification if a periodic backup job fails. See [Email Notification settings](#) for email notification setup.

Other menu

Task Log View

This view shows the list of all Task Log entries, with options to refresh list and inspect Task Log details.

To open this view, you can either:

- Open Other menu and click Task Log view
- Locate and click the main area Task Log tab, if present
- Locate and click the Task Log link on [Dashboard view](#)

The Task Log view updates itself automatically.

Task Log view content



Task Log view contains a list of all available tasks:

Figure 366 Task log view content

Task Log x Dashboard					
Id	Name	Status	Start Date	End Date	
✓11	Backup active NMS database	Completed	26 09:19:51 Mar 2015	26 09:20:00 Mar 2015	
✓10	Create NMS database	Completed	26 08:51:22 Mar 2015	26 08:51:22 Mar 2015	
✓9	Delete NMS database	Completed	26 08:29:51 Mar 2015	26 08:29:51 Mar 2015	
✓8	Reinitialize NMS database	Completed	26 08:03:21 Mar 2015	26 08:03:21 Mar 2015	
✓7	Create NMS database	Completed	26 07:38:11 Mar 2015	26 07:38:11 Mar 2015	
✗6	Status change for NMS server service	Failed	14 04:40:09 Mar 2015	14 04:40:09 Mar 2015	
✓5	Start NMS server	Completed	11 07:15:21 Mar 2015	11 07:18:48 Mar 2015	
✓4	Start NMS server	Completed	06 06:26:06 Mar 2015	06 06:29:21 Mar 2015	
✓3	Change active NMS database configuratio	Completed	06 06:23:51 Mar 2015	06 06:23:51 Mar 2015	

Double click a task entry to view its task details.

You can also click:

Button	Explanation
	Open task details
	Refresh task list

Task Details dialog

A Task Details dialog may look like this:

Figure 367 Task details dialog

Task Details

Start Date: 27 09:40:52 2015 Mar **End Date:** 27 09:41:01 2015 Mar

Task Type: Backup active NMS database **Status:** Completed

Subtask: Backup database **Subtask status:** Completed

Description: Backup NMS database

Details:

Database 'nms28' backed up at server 'localhost'.
Backup file name and location: C:\NgNMS\backup\database\20151127-094052-postgres-nms28.backup.gz

OK

Some tasks like the one shown above contain subtasks.

The first subtask in the task shown above is to initiate a backup job on a remote database server. The second subtask is to copy the backup file from the remote database server to the local EMS Server. The file is put in the folder specified in the [Database settings view](#).

The second subtask is shown below.

Figure 368 Second subtask details dialog

Task Details

Start Date:

27 09:40:52 2015 Mar

End Date:

27 09:41:01 2015 Mar

Task Type:

Backup active NMS database

Status:

Completed

Subtask:

Backup database

Subtask status:

Completed

Description:

Backup database
Copy database backup to server



Details:

Database 'nms28' backed up at server 'localhost'.

Backup file name and location: C:\NgNMS\backup\database\20151127-094052-postgres-nms28.backup.gz

OK

Arrow buttons:

Button	Explanation
	Show task details for task above. If top task is shown, wrap to bottom task.
	Show task details for task below. If bottom task is shown, wrap to top task.

PTP 820 NMS Log View

This view shows the list of all EMS server log entries, with options to refresh list, archive and delete logs.

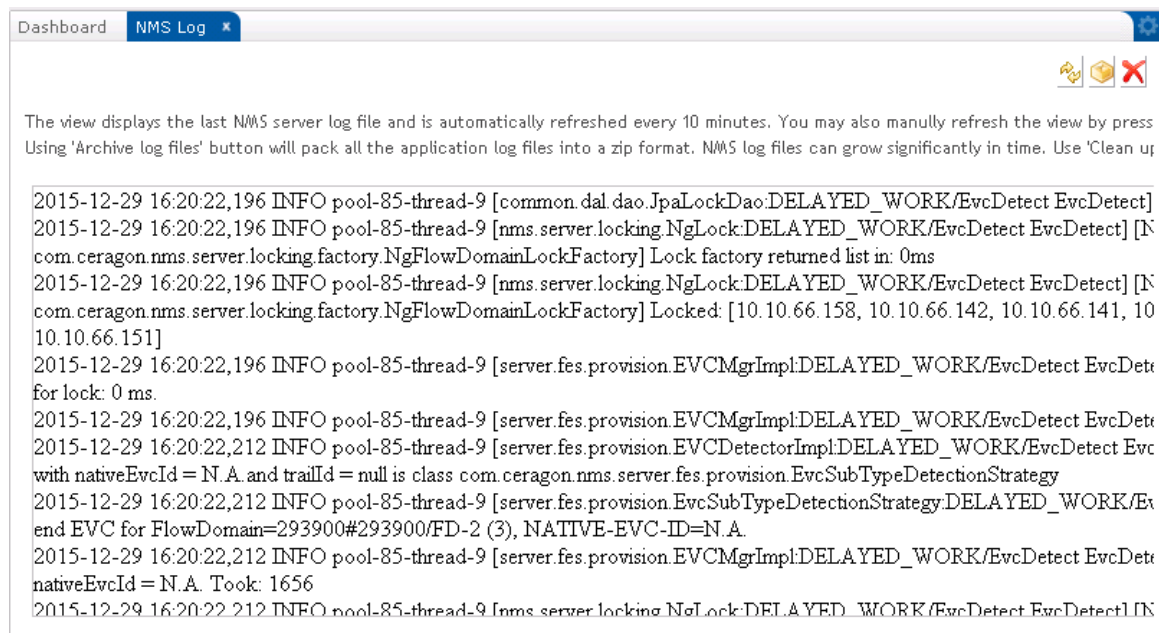
To open this view, you can either:

- Open Other menu and click EMS Log view
- Locate and click the main area EMS Log tab, if present

PTP 820 NMS Log view content

The PTP 820 NMS Log view shows the last EMS server log, i.e. <EMS installation>/JBoss-4.2.3/server/ptp820nms/log/server.log.




Figure 369 EMS log view content



Use the scrollbar to inspect the content of the EMS log.

The log is automatically refreshed every 10 minutes, and can be refreshed manually by pressing the Refresh button in the toolbar.

The following operations are available:

Button	Explanation
	Refresh log field manually
	Use 'Archive log files' button to pack all the application log files in a zip format. The archive is named by default "PTP820NMSLogFiles.zip" and it will be saved under PTP 820 NMS installation folder. You may change the name and the location of the archive in the popup dialog that opens when pressing the 'Archive log files' button.
	Use 'Clean up old log files' button to delete old EMS log files located under <PTP 820 NMS installation>/JBoss-4.2.3/server/ptp820nms/log/

EMS log files can grow significantly in time, and the log file folder should be monitored regularly. Please note that only the historical log files will be deleted this way, not the log file currently being written to by EMS.

Scheduled Tasks View

This view shows the list of all scheduled tasks, with options to refresh and to delete unwanted scheduled tasks from the list.

To open this view, you can either:

- Open Other menu and click Scheduled Tasks
- Locate and click the main area Scheduled Tasks tab, if present
- Locate and click the Scheduled Tasks link on [Dashboard view](#)

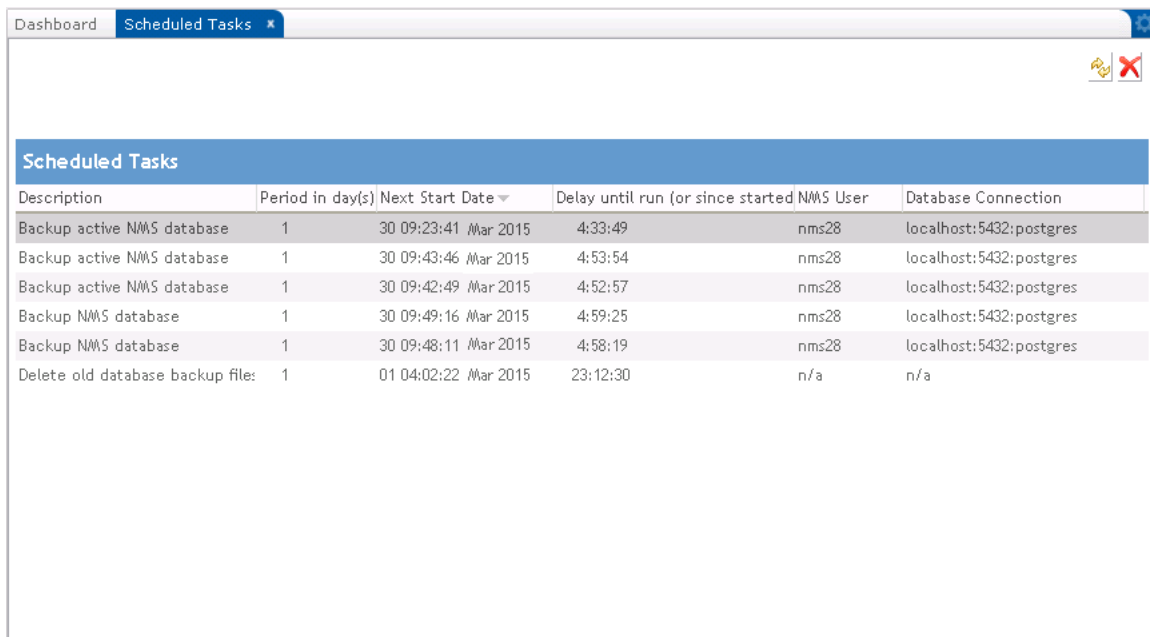
The Scheduled Tasks view does not update itself automatically.

Use the Refresh button or reopen the view.

Scheduled Tasks view content

Scheduled Tasks view contains a list of the configured scheduled System Manager tasks:

Figure 370 Scheduled tasks view content





Scheduled Tasks					
Description	Period in day(s)	Next Start Date	Delay until run (or since started)	NMS User	Database Connection
Backup active NMS database	1	30 09:23:41 Mar 2015	4:33:49	nms28	localhost:5432:postgres
Backup active NMS database	1	30 09:43:46 Mar 2015	4:53:54	nms28	localhost:5432:postgres
Backup active NMS database	1	30 09:42:49 Mar 2015	4:52:57	nms28	localhost:5432:postgres
Backup NMS database	1	30 09:49:16 Mar 2015	4:59:25	nms28	localhost:5432:postgres
Backup NMS database	1	30 09:48:11 Mar 2015	4:58:19	nms28	localhost:5432:postgres
Delete old database backup file:	1	01 04:02:22 Mar 2015	23:12:30	n/a	n/a

Table 64 Field description:

Field	Explanation
Description	Task description
Period	Number of days between job runs
Next Start Date	Time for next job run
Delay until run	If a job is running, this field shows time since job start, shown like this: (hh:mm:ss). If a job is waiting to run, this field shows count down time till job start, shown like this: hh:mm:ss.
EMS User	User/Schema to be used by periodic database jobs
Database Connection	Database parameters to be used by periodic database jobs

The following operations are available:

Operation	Explanation
	Delete the selected scheduled task
	Refresh scheduled task list

System Manager maintenance

System Manager maintenance

System Manager must be installed on your EMS Server machine. If you run a separate database server on Windows, you must also install the System Manager standalone in order to get the backup and restore functionality to work. System Manager is installed as a service on both the EMS server and the database server.

The System Manager service is intended to run together with the EMS Server, running periodic database backup and optimization jobs and keeping track of the scheduled tasks and EMS Server availability, with the ability to send email notifications in case of failures.

Database Analysis view contains a toolbar, a file list, a link to launch the [Analyze User/Schema wizard](#) and a file content display area.

Periodic backup cleanup

Periodic backup of your EMS database is recommended, but can produce large files on your file systems. If a periodic backup is scheduled, it is also vital to configure a backup file deletion job to prevent file system to fill up with backup files.

See the [Backup Active User/Schema wizard](#) or the [Backup User/Schema wizard](#) for information on how to set up periodic backup jobs.

See the [Database settings view](#) for information on how to set up periodic backup file deletion jobs.

Internal cleanup job

To prevent file system to fill up, System Manager runs a hidden task that does the following:

- Delete log files from: `<EMS_Install_Dir>\SystemManager\log\RemoteMessages`
The 500 newest log files are kept.
- Delete old Task Log entries. The 1000 newest entries are kept.

The internal cleanup job is run nightly at 05:00 am.

Log files

System Manager log files are found here: `<EMS_Install_Dir>\SystemManager\Tomcat-6.0.18-win\logs\wrapper.log*`.

System Manager keeps the 20 newest wrapper log files of 5 MB each.

In case you need to report System Manager problems to Customer Support, please append the relevant wrapper.log file to the case. This will make it easier for us to investigate the problem.

System Manager troubleshooting

This chapter contains tips that may help you solve System Manager related problems.

Logon window does not appear

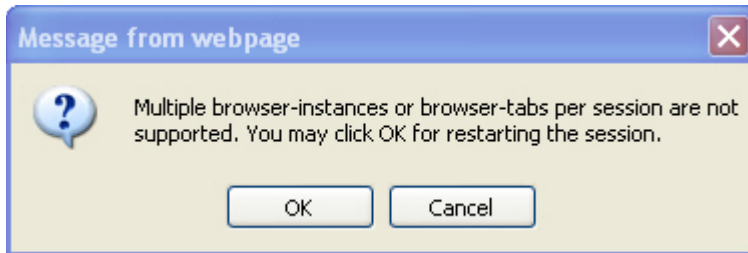
Sometimes the System Manager logon window does not appear.

To fix this, press F5 to refresh the browser window.

Multiple browser sessions

If System Manager detects more than one browser session (using the same browser tool) on the same machine, the following message will appear:

Figure 371 Multiple browser sessions



You can run multiple System Manager sessions using:

- browsers on separate machines
- using different browser tools on same machine

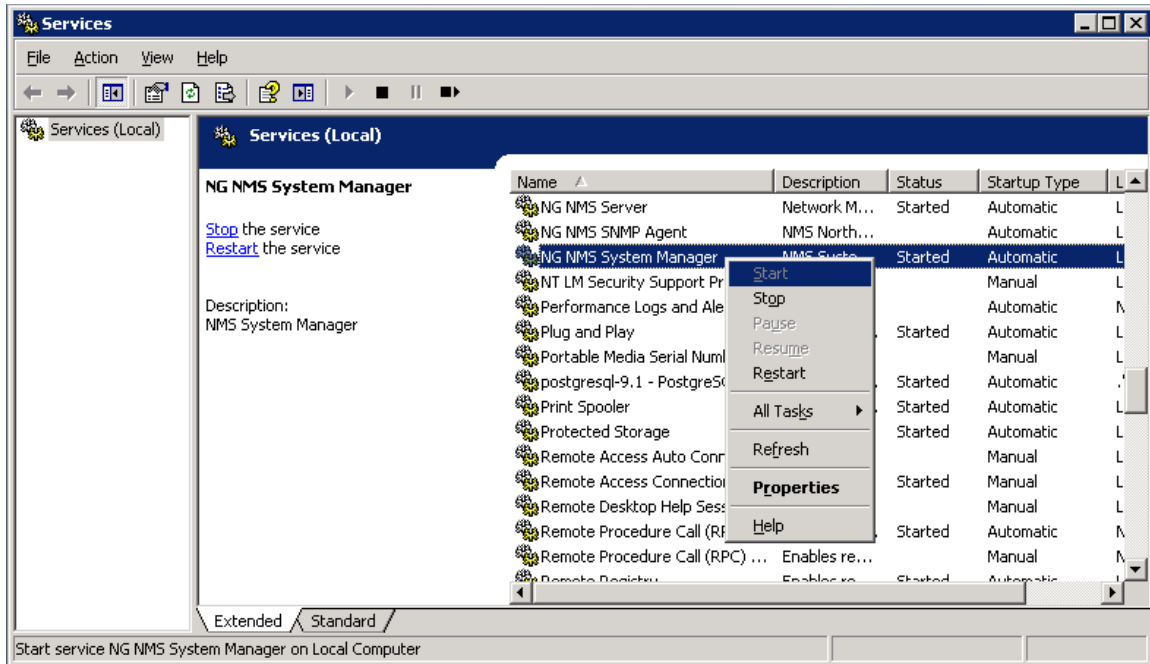
System Manager not available

If your browser can't find the System Manager pages, make sure that the System Manager service is up and running.

Windows version

Open Windows Services and restart the PTP 820 NMS System Manager service:

Figure 372 Windows services



Solaris version

If you want to check the status of the EMS services:

```
svcs sysman PTP 820 NMS nifservice
```

If you need to restart the EMS System Manager service:

1. First disable the System Manager service

```
svcadm disable -s sysman
```

2. Then start the service by running:

```
svcadm enable -s sysman
```

Memory problem

System Manager browser session may time out after 15 or more minutes of inactivity. If this doesn't happen, there is a danger that a System Manager browser window will start to consume memory.

If this happens in your system, close down the browser.

License import problem

If you want to import a license on a remote disk, you may have to copy the license file to a local disk for the import action to work.

System Manager troubleshooting

This chapter contains tips that may help you solve System Manager related problems.

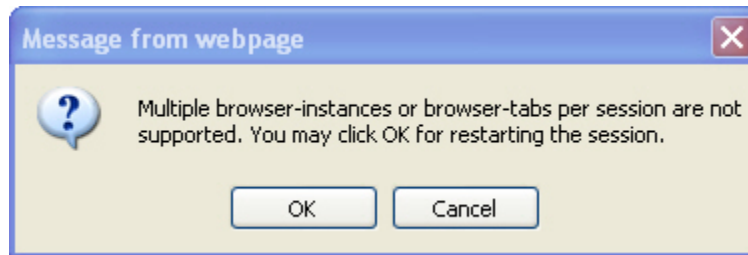
Logon window does not appear

Sometimes the System Manager logon window doesn't appear.

To fix this, press F5 to refresh the browser window.

Multiple browser sessions

If System Manager detects more than one browser session (using the same browser tool) on the same machine, the following message will appear:



You can run multiple System Manager sessions using:

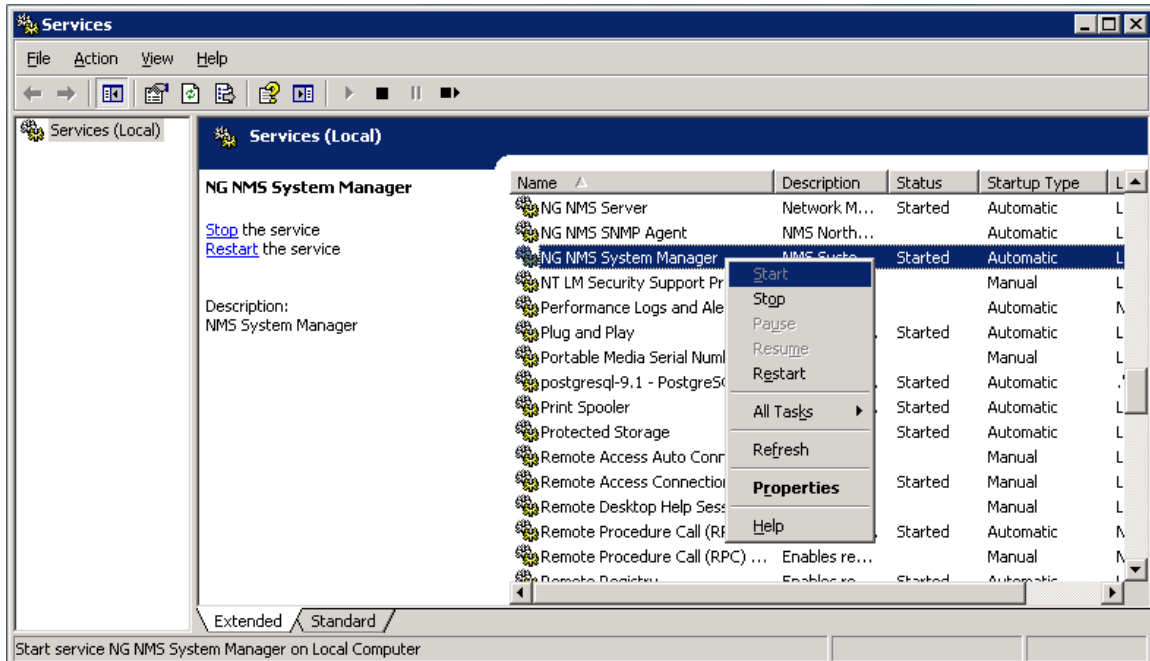
- browsers on separate machines
- using different browser tools on same machine

System Manager not available

If your browser can't find the System Manager pages, make sure that the System Manager service is up and running.

Windows version

Open Windows Services and restart the **PTP 820 NMS System Manager** service:



Solaris version

If you want to check the status of the PTP 820 NMS services:

```
svcs ngSysMgr ngNMSService ngNIFService
```

If you need to restart the PTP 820 NMS System Manager service:

- 1 First disable the System Manager service

```
svcadm disable -s ngSysMgr
```

- 2 Then start the service by running:

```
svcadm enable -s ngSysMgr
```

Memory problem

System Manager browser session may time out after 15 or more minutes of inactivity. If this doesn't happen, there is a danger that a System Manager browser window will start to consume memory.

If this happens in your system, close down the browser.

License import problem

If you want to import a license on a remote disk, you may have to copy the license file to a local disk for the import action to work.

Chapter 9: Abbreviations

A

ABC	Adaptive Bandwidth Control
ABR	Adaptive Bandwidth Recovery
Ack	Acknowledged
ACM	Adaptive Coded Modulation
ADC	Analog to Digital Converter
AES	Advanced Encryption Standard
ATPC	Automatic Transmit Power Control

B

BBE	Background Block Error
BBER	Background Block Error Ratio
BIP	Bit Interleaved Parity

C

C/N	Carrier to Noise ratio
CLI	Command Line Interface
CMON	Cluster Monitoring
CPU	Central Processing Unit
CSV	Comma-Separated Values file format
CTP	Connection Termination Point
C-VLAN	Classified Virtual LAN

D

dB	Decibel
dBm	Decibel per Milliwatt
DCN	Dynamic Circuit Network
DES	Data Encryption Standard

D

DM	Degraded Minutes
DST	Daylight Savings Time

E

EB	Errored Blocks
EBO	Errored Block Overstep
EBUS	Serial Bus (Energy Bus)
EDT	Eastern Daylight Time
E-LAN	Ethernet Local Area Network
EMS	Element Management System
ES	Errored Second

F

FC	Fiber-optic Connector
FCPS	Fault, Configuration, Performance and Security
FIFO	First-in First-out
FTP	File Transfer Protocol

G

GUI	Graphical User Interface
-----	--------------------------

H

HA	High-Availability
HBS	Base System Unit
HLM	High Level Manager
HSB	Hot-Standby
HSU	Subscriber Unit
HTML	Hypertext Markup Language file format
HTTP	Hypertext Transfer Protocol
HTTPS	Secured Hypertext Transfer Protocol
HW	Hardware

I

IANA	Internet Assigned Numbers Authority
ID	Identifier
IDU	Indoor Unit
IP	Internet Protocol
ITU	International Telecommunication Union

K

Kbps	Kilobits per second
------	---------------------

L

LAG	Link Aggregation Group
LOF	Loss of Frame
LOS	Loss of Signal

M

Mb	Megabyte
Mbps	Megabits per second
MD5	Message Digest cryptographic hash algorithm
MHz	Mega Hertz
MIB	Management Information Base
MRMC	Multi-Rate Multi-Constellation
MSE	Mean Square Error
MSTP	Multiple Spanning Tree Protocol

N

N/A	Not Applicable
NE	Network Element
NI	Network Interface
NMS	Network Management System
NNI	Network-to-Network Interface

N

NTP	Network Time Protocol
-----	-----------------------

O

OC3	Optical Carrier 3
ODU	Optical Channel Data Unit
OFN	Output file name
OFS	Operational Fixed Service
OID	Object Identifier
OSS	Operations Support System

P

PDF	Portable Document Format file format
PDH	Plesiochronous Digital Hierarchy
PM	Performance Monitoring
PMP	Point to Multi-Point
PTP	Physical Termination Point
PWD	Password

Q

QoS	Quality of Service
-----	--------------------

R

RBAC	Role Based Access Control
RDI	Reverse Defect Indication
RF	Radio Frequency
RFC	Request for Comments (publication)
RFU	Radio Frequency Unit
RMON	Remote Monitoring
RPL	Received Power Level
RPL_SDIV	Received Power Level on Space Diversity equipment
RSL	Received Signal Level

R

RT	Report Type
RUAS	Radio channels
RX	Receive

S

SCP	Secure Copy
SDH	Synchronous Digital Hierarchy
SDN	System Distinguished Name
SDP	Severely Disturbed Period
SEBO	Severely Errored Blocked Overstep
SES	Severely Errored Seconds
SFTP	SSH File Transfer Protocol
SHA	Secure Hash Algorithm
SMIv	Structure of Management Information version
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SOAM	Service Operations, Administration, and Maintenance
SOH	Section Overhead
SQL	Structured Query Language
STM	Synchronous Transport Module
S-VLAN	Service Virtual Local Area Network
SW	Software
SysOID	System Object Identifier

T

TAR	Tape Archive file format
TC	Textual Convention
TCP	Transmission Control Protocol

T

TDM	Time Division Multiplexing
TMF	TeleManagement Forum
TOC	Table of Contents
TRX	Transceiver
Tx	Transmitter Power Level
TX	Transmit

U

UAS	Unavailable Seconds
UDP/IP	User Datagram Protocol/Interface Protocol
UNI	User Network Interface
UTC	Coordinated Universal Time

V

VC	Virtual Channel
VLAN	Virtual Local Area Network

W

Web EMS	Web-Based Element Management System
---------	-------------------------------------

X

XC	Cross connect
XML	Extensible Markup Language file format
XPI	Cross-Polarization Interference
XPIC	Cross Polarization Interference Cancellation