



# **NSP Network Services Platform**

Release 18.12

## **Applications Guide**

**3HE-14101-AAAE-TQZZA**

**Issue 1**

**December 2018**

---

**Legal notice**

Nokia is a registered trademark of Nokia Corporation. Other products and company names mentioned herein may be trademarks or tradenames of their respective owners.

The information presented is subject to change without notice. No responsibility is assumed for inaccuracies contained herein.

© 2018 Nokia.

# Contents

<b>1</b>	<b>NSP Launchpad</b> .....	<b>11</b>
1.1	To use the NSP Help .....	11
1.2	What is NSP? .....	12
1.3	User session administration .....	15
1.4	To configure NSP user settings .....	17
1.5	To configure NSP system settings .....	17
1.6	To configure NSP system colors .....	18
1.7	To configure NSP linked URLs .....	19
1.8	To configure NSP application access control .....	19
1.9	To configure event logging .....	20
1.10	To configure an e-mail server .....	21
1.11	Licensing .....	21
1.12	REST API .....	22
1.13	Accessibility .....	22
1.14	Troubleshooting .....	23
1.15	Documentation .....	24
<b>2</b>	<b>Fault Management</b> .....	<b>27</b>
2.1	Overview .....	27
2.2	Top Unhealthy NEs view .....	27
2.3	Alarm List views .....	28
2.4	Top Problems view .....	32
2.5	Inspector view .....	33
2.6	To configure current alarm list settings .....	33
2.7	To configure historical alarm list settings .....	34
2.8	To configure system alarm settings .....	35
2.9	To configure an e-mail policy .....	36
2.10	Fault Management general operations .....	37
<b>3</b>	<b>Network Supervision</b> .....	<b>39</b>
3.1	Overview .....	39
3.2	Network Supervision views .....	39
3.3	Network Supervision display formats .....	40
3.4	Routine NE maintenance with Network Supervision .....	45
3.5	To configure application preferences .....	50
3.6	To configure KPI threshold settings .....	50
3.7	To configure Event Timeline settings .....	51

---

3.8	To configure user preferences.....	51
3.9	Supervision Manager .....	52
3.10	Network Supervision general operations .....	53
<b>4</b>	<b>Service Supervision.....</b>	<b>57</b>
4.1	Overview .....	57
4.2	Routine service maintenance with Service Supervision.....	57
4.3	Service Supervision general operations.....	65
<b>5</b>	<b>Analytics .....</b>	<b>69</b>
5.1	Overview .....	69
5.2	Workflow to configure NFM-P analytics .....	70
5.3	To configure an NFM-P analytics rule .....	71
5.4	To configure analytics aggregation.....	71
5.5	To configure the Analytics application session time zone .....	72
5.6	To configure analytics server load balancing .....	73
5.7	To configure application preferences .....	74
5.8	To run a report.....	74
5.9	To manage saved reports.....	75
5.10	To schedule a report.....	76
5.11	To manage scheduled reports.....	77
5.12	To upload images for report branding .....	78
<b>6</b>	<b>Link Utilization.....</b>	<b>79</b>
6.1	Introduction to the Link Utilization application .....	79
6.2	Preparing for Link Utilization (initial setup).....	81
6.3	Viewing and managing utilization information .....	84
<b>7</b>	<b>Subscriber Manager.....</b>	<b>89</b>
7.1	Overview .....	89
7.2	KPI Monitor view .....	89
7.3	Troubleshoot view .....	93
7.4	Subscriber Manager general operations .....	95
<b>8</b>	<b>Telemetry .....</b>	<b>97</b>
8.1	About.....	97
8.2	To enable telemetry reporting for a managed NE .....	97
8.3	Telemetry troubleshooting .....	103

---

<b>9</b>	<b>Network Functions Manager - Packet</b> .....	<b>107</b>
9.1	About.....	107
<b>10</b>	<b>Inventory Management</b> .....	<b>109</b>
10.1	Overview .....	109
<b>11</b>	<b>Service Navigator</b> .....	<b>113</b>
11.1	Overview .....	113
11.2	Service Path Discovery .....	118
11.3	Service connectivity check .....	122
<b>12</b>	<b>Wireless NE Views</b> .....	<b>129</b>
12.1	The NFM-P Wireless NE Views application .....	129
<b>13</b>	<b>Wireless Supervision</b> .....	<b>133</b>
13.1	Overview .....	133
13.2	To launch the Wireless Supervision application .....	135
13.3	Configuring supervision objects .....	136
13.4	To configure a supervision group .....	137
13.5	To configure a summary view.....	139
<b>14</b>	<b>Policy Management</b> .....	<b>141</b>
14.1	About.....	141
14.2	Template and policy provisioning .....	141
<b>15</b>	<b>Service Fulfillment</b> .....	<b>161</b>
15.1	About.....	161
15.2	Getting started.....	161
15.3	Service provisioning .....	162
15.4	Service management .....	179
<b>16</b>	<b>Task Scheduler</b> .....	<b>183</b>
16.1	About.....	183
16.2	Bandwidth modification .....	183
<b>17</b>	<b>Autonomous System Optimizer</b> .....	<b>187</b>
17.1	About.....	187
17.2	Flow steering.....	187
<b>18</b>	<b>Ingress Peer Optimizer</b> .....	<b>191</b>
18.1	Overview .....	191
18.2	Ingress Peer Optimizer component description .....	191

---

18.3	Ingress Peer Optimizer pages.....	192
18.4	To set up the application .....	194
18.5	To configure the BGP peering topology .....	194
18.6	To configure color ID tags for links .....	197
18.7	To configure traffic optimization automation.....	198
18.8	To create internal LSP constraint services .....	200
18.9	To configure display preferences .....	201
<b>19</b>	<b>Latency Steering Optimizer.....</b>	<b>203</b>
19.1	About.....	203
19.2	Getting started.....	203
<b>20</b>	<b>Traffic Steering Controller.....</b>	<b>207</b>
20.1	About.....	207
20.2	Flow management.....	207
<b>21</b>	<b>IP/MPLS Optimization .....</b>	<b>211</b>
21.1	About.....	211
21.2	Getting started.....	211
<b>22</b>	<b>IP/MPLS Simulation .....</b>	<b>219</b>
22.1	About.....	219
22.2	Getting started.....	219
<b>23</b>	<b>Modeled Device Configurator .....</b>	<b>229</b>
23.1	Overview .....	229
23.2	To create an object.....	230
23.3	To modify an object .....	231
23.4	To delete an object.....	232
<b>24</b>	<b>Workflow Manager .....</b>	<b>233</b>
24.1	Workflows overview.....	233
24.2	Using the WFM .....	238
24.3	To use workflows.....	241
24.4	To use actions .....	242
<b>25</b>	<b>Cross Domain Coordinator .....</b>	<b>245</b>
25.1	About.....	245
25.2	Getting started.....	245

---

<b>26</b>	<b>Supervision Manager</b> .....	<b>255</b>
26.1	Overview .....	255
26.2	Supervision groups and views for Network Supervision .....	255
26.3	Supervision groups and views for Service Supervision .....	257
26.4	To associate a supervision group with a view .....	259
26.5	To search for a supervision object.....	260
26.6	To search for NEs or services with no supervision group .....	260
<b>27</b>	<b>VNF Manager</b> .....	<b>263</b>
27.1	Overview .....	263
<b>28</b>	<b>Device Administrator</b> .....	<b>269</b>
28.1	Overview .....	269
28.2	Workflow for using the Device Administrator application.....	269
28.3	To create an NE reachability policy .....	270
28.4	To create a mediation policy.....	271
28.5	To create an NE discovery rule .....	272
28.6	To view discovered NEs .....	274
28.7	To view or edit policies .....	274
28.8	To view or edit NE discovery rules .....	275

---

## List of tables

Table 1-1	Category: Analyze / Assure .....	<b>12</b>
Table 1-2	Category: Manage IP .....	<b>13</b>
Table 1-3	Category: Control / Fulfill / Optimize .....	<b>13</b>
Table 1-4	Category: Manage Data Centers / SD WAN .....	<b>14</b>
Table 1-5	Category: Manage Wireless .....	<b>14</b>
Table 1-6	Category: Administer NSP .....	<b>14</b>
Table 27-1	VNF lifecycle management tasks .....	<b>264</b>

---

## List of figures

Figure 10-1	BGP profile.....	110
Figure 10-2	Aging profile .....	111
Figure 11-1	IGP multi-layer map with overlay highlights .....	116
Figure 11-2	Peer group display .....	117
Figure 11-3	Service connectivity test results.....	124
Figure 11-4	VM Connectivity Results .....	125
Figure 24-1	Sample workflow .....	233



# 1 NSP Launchpad

## 1.1 To use the NSP Help

### 1.1.1

The NSP Help system includes information about all applications in the NSP product group (including applications that may not be licensed in your NSP deployment). The Help pages for individual applications are grouped according to application category, as laid out on the NSP Launchpad. The NSP Applications Guide provides the contents of the NSP Help system in PDF format, available on OLCS.

1

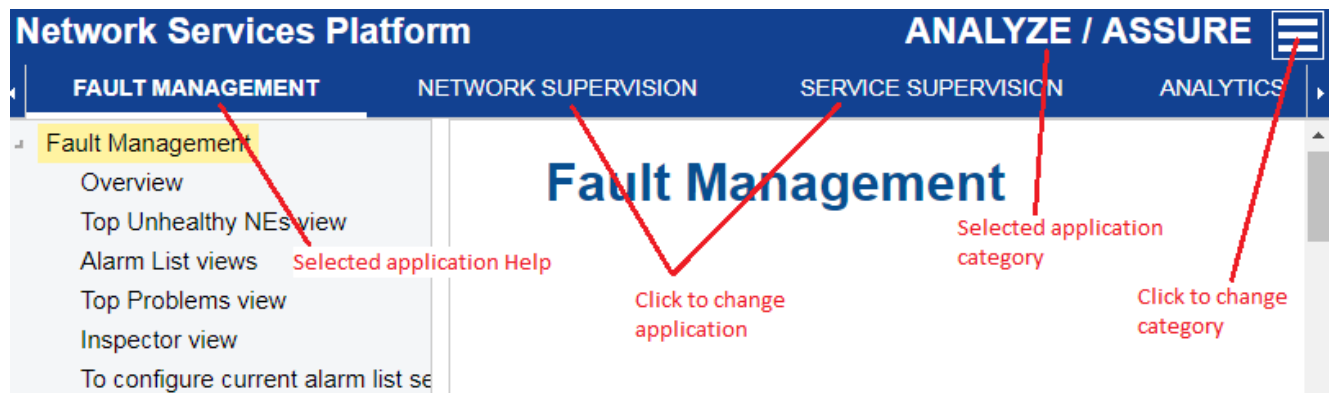
In the NSP Help page, click the menu button  in the upper right-hand corner and choose an application category from the drop-down list.

For example, the figure below shows the ANALYZE / ASSURE category, with the Fault Management Help displayed.

2

Click on an application name (displayed horizontally across the banner) to display the Help for another application in the same category.

END OF STEPS



## 1.2 What is NSP?

### 1.2.1

The Network Services Platform (NSP) allows operators to automate, optimize, and assure network services across multiple network layers and both physical and virtual infrastructure, including equipment from multiple vendors.

The NSP Launchpad is the central interface from which all NSP applications are opened, and from which system-wide user options and settings are configured.

### 1.2.2 Applications

The NSP includes the following applications:

Table 1-1 Category: Analyze / Assure

Application name	Description
Fault Management	Provides alarm monitoring, correlation, and troubleshooting for the most unhealthy NEs in the network, allowing you to filter, identify root causes, and determine the impact of alarms.
Network Supervision	Monitors the health of physical NEs and virtual NFs using pre-defined KPIs and alarms to provide a launchpad for monitoring the overall health of NEs in the network.
Service Supervision	Provides alarm and KPI monitoring on user-defined service views and groups.
Analytics	Provides graphical and tabular reports of network conditions and trends, based on the analysis of raw statistics data and big-data aggregation using business intelligence software. In NSP 18.6, the Analytics application requires an NFM-P license and NFM-P analytics server for data collection.
Link Utilization	Provides IP, MPLS, and aggregated utilization statistics for interfaces within a specific domain.
Subscriber Manager	Provides NE and subscriber KPI information and troubleshooting functions for subscriber hosts.
Telemetry	Provides a graphical dashboard of NE KPIs based on real-time telemetry statistics.

Table 1-2 Category: Manage IP

Application name	Description
Network Functions Manager - Packet	End-to-end network and service management across all domains of the converged IP network. Operational efficiency through fast provisioning and troubleshooting, service assurance, and enhanced network operations tools.

Table 1-3 Category: Control / Fulfill / Optimize

Application name	Description
Policy Management	Allows for the creation of customized global or domain rules, as well as highly abstract service definitions.
Service Fulfillment	Allows for multi-vendor service provisioning and activation across all network accessible to the NSD.
Task Scheduler	Enables users to do CRUD operations with respect to scheduling bandwidth modification requests/tasks on an existing E-Line service.
Autonomous System Optimizer	Allows traffic on monitored routers that is destined for autonomous systems to be steered to alternate next hops.
Latency Optimizer	Allows for traffic flows from an entry point router to a specific destination to be routed onto a path with the least possible latency.
Traffic Steering Controller	Allows all existing flows within a network to be viewed, and also allows additional flows to be created.
IP/MPLS Optimization	Provides a view of the IGP topology and PCE LSPs, displays the status of the network, and provides functionality to optimize the network resources.
IP/MPLS Simulation	Allows for modifications to IGP topology, PCE LSPs, links, and a variety of policies within a simulated environment
Ingress Peer Optimization	Optimizes connection utilization by moving traffic between peer routers to less used connections.

Table 1-3 Category: Control / Fulfill / Optimize (continued)

Application name	Description
Cross Domain Coordinator	Enables automatic discovery of cross domain links between IP and optical networks.
Modeled Device Configurator	Allows for viewing the state and configuration of model-based devices, and for editing the device configuration.
Workflow Manager	Allows for creation, execution, scheduling and event triggering of workflows using Mistral v2 DSL.

Table 1-4 Category: Manage Data Centers / SD WAN

Application name	Description
Inventory Management	Provides a dashboard inventory view of virtual network components and virtualized services in the network, allowing you to filter, search, and map data center network.
Service Navigator	Provides a dashboard of the operational health of the service objects in a specified administrative domain.

Table 1-5 Category: Manage Wireless

Application name	Description
Wireless NE View	Provides a visual representation of eNodeB hardware, links, states and fault status for a single NE.
Wireless Supervision	Provides alarm monitoring based on user-defined views and groups for an LTE RAN network.

Table 1-6 Category: Administer NSP

Application name	Description
Supervision Manager	Configure NE supervision groups and summary views of supervision groups for use with NSP applications.
VNF Manager	Provides VNF lifecycle management functionality for an NFV network.

Table 1-6 Category: Administer NSP (continued)

Application name	Description
Device Administrator	Allows for discovering model-based devices using mediation policies and network rules.

### 1.2.3 MDM-aware applications

MDM-aware applications include a framework to allow them to work with modeled devices (devices that are managed using MDM).

The following NSP applications are MDM-aware:

- Service Fulfillment
- Network Supervision
- Service Supervision
- Modeled Device Configurator
- Device Administrator
- Fault Management
- Telemetry
- Workflow Manager

Restrictions may apply; see the *NSP Release Notice*.

## 1.3 User session administration

### 1.3.1

The Session Administration GUI lists all active NSP user sessions and REST API sessions. Administrative users can manually terminate one or more sessions.

Administrative users can also send messages to one or more active NSP users. Messages would typically be sent to forewarn users of an upcoming session termination, or for other operational events in the NSP system. Sent messages are displayed in the NSP application views that the recipient user(s) have open. Messages are flagged as Information, Warning, or Urgent. The recipient user(s) must have NSP open on their desktop to receive messages.

**i** **Note:** Messages cannot be sent to REST API sessions because these sessions are automated and do not involve actual users. Administrative users should exercise caution in terminating REST API sessions, as they often involve critical network functions.

### 1.3.2 To manage user sessions

- 1 \_\_\_\_\_  
Sign in to NSP as an administrator.

---

2



From the NSP Launchpad, click More→Manage User Sessions.

The Session Administration application opens with a list of active NSP user sessions.

---

3

Do one of the following:

- **Terminate a single session:** select a user session in the list and click on the Terminate Session button  that appears at the end of the item.
- **Terminate multiple sessions:** press the CTRL key and click on the session items you want to terminate, or select all of the sessions by clicking on the Select All button . Then Click on the Terminate Sessions button on the Session Administration toolbar.

---

4

At the prompt, Click on the Terminate button to confirm the session termination.

---

END OF STEPS

### 1.3.3 To send a message to active users

---

1

Sign in to NSP as an administrator.

---

2



From the NSP Launchpad, click More→Manage User Sessions.

The Session Administration application opens with a list of active NSP user sessions.

---

3

Do one of the following:

- **Send a message to one user:** select a user session in the list and click on the Send Message button  that appears at the end of the item.
- **Send a message to all active users:** click on the Send Broadcast Message button  on the Session Administration toolbar.

---

4

In the message form that opens, select a message type and then type your message text in the box.

---

5

Click on the Send button.

---

END OF STEPS

---

## 1.4 To configure NSP user settings

### 1.4.1

Use this procedure to specify your personal GUI preferences for NSP applications.

1 \_\_\_\_\_  
Sign in to NSP.

2 \_\_\_\_\_  
Choose More→Settings from the NSP Launchpad.

3 \_\_\_\_\_  
Click User Preferences.


4 \_\_\_\_\_  
Set the application polling time.

5 \_\_\_\_\_  
Choose a Language from the drop-down menu.  
Nokia recommends that the NSP user preference for language matches the NSP system setting for language.

6 \_\_\_\_\_  
Enable the Color row with severity in IP and Wireless applications checkbox, if required.

7 \_\_\_\_\_  
Click Save.

END OF STEPS \_\_\_\_\_

 **Note:** If you click Restore to System Settings, the language is restored to the NSP system language.

## 1.5 To configure NSP system settings

### 1.5.1

Use this procedure to specify global settings for NSP applications.

1 \_\_\_\_\_  
Sign in to NSP as an administrator.

- 
- 2 \_\_\_\_\_  
From the NSP Launchpad, click More→Settings.
  - 3 \_\_\_\_\_  
Click System Settings.
  - 4 \_\_\_\_\_  
Set the application polling time.
  - 5 \_\_\_\_\_  
Choose a Language from the drop-down menu.
  - 6 \_\_\_\_\_  
Type a security statement in the text field and enable the checkbox to enable the security statement.
  - 7 \_\_\_\_\_  
Enable the Color row with severity in IP and Wireless applications checkbox, if required.
  - 8 \_\_\_\_\_  
Click Save.

END OF STEPS \_\_\_\_\_

## 1.6 To configure NSP system colors

### 1.6.1

Use this procedure to associate custom colors with alarm severities.

- 1 \_\_\_\_\_  
Sign in to NSP as an administrator.
- 2 \_\_\_\_\_  
Choose More→Settings from the NSP Launchpad.
- 3 \_\_\_\_\_  
Click System Colors.
- 4 \_\_\_\_\_  
Under Alarms, click on an alarm severity category and then click on the color you want to associate with the alarm severity category.  
Repeat this step to set custom colors for other alarm severity categories.

---

5 \_\_\_\_\_  
Select a text color.

6 \_\_\_\_\_  
Click Save.

END OF STEPS \_\_\_\_\_

## 1.7 To configure NSP linked URLs

### 1.7.1

Use this procedure to link up to 20 external URLs that application users can open in a new browser tab from the More menu on the NSP Launchpad.

1 \_\_\_\_\_  
Sign in to NSP as an administrator.

2 \_\_\_\_\_  
Choose More→Settings from the NSP Launchpad.

3 \_\_\_\_\_  
Click Linked URLs.

4 \_\_\_\_\_  
Configure the Display Name and URL parameters.

5 \_\_\_\_\_  
Click Add.

6 \_\_\_\_\_  
To remove a linked URL, hover over the URL item in the list and click the Delete button at the end of the row.

END OF STEPS \_\_\_\_\_

## 1.8 To configure NSP application access control

### 1.8.1

Use this procedure to specify which NSP applications are loaded on the NSP server, and available to users on the NSP Launchpad.

 **Note:**

---

Disabling unused NSP applications improves NSP start-up time.

1 \_\_\_\_\_

Sign in to NSP as an administrator.

2 \_\_\_\_\_

Choose More→Settings from the NSP Launchpad.

3 \_\_\_\_\_

Click App Access Control.

4 \_\_\_\_\_

Expand an application category and then enable or disable the check boxes to grant or restrict access to those applications.

5 \_\_\_\_\_

Enable the check box to indicate that you understand the implications your changes.

6 \_\_\_\_\_

Click Save.

If you are re-enabling access to an application, there may be a brief delay before the application icon appears on the Launchpad.

END OF STEPS \_\_\_\_\_

## 1.9 To configure event logging

### 1.9.1

Use this procedure to configure the recording of assurance events and/or to purge all existing event records from the database. Events can be retained for a time period of one to 30 days.

1 \_\_\_\_\_

Sign in to NSP as an administrator.

2 \_\_\_\_\_

Choose More→Settings from the NSP Launchpad.

3 \_\_\_\_\_

Click Event Logging Policy.

4 \_\_\_\_\_

Place a check mark in the Enable Event Logging check box.

---

5 \_\_\_\_\_

Configure the Retention Time parameter.

6 \_\_\_\_\_

Click Purge Event Records to delete all existing event records from the database.

7 \_\_\_\_\_

Click Save.

END OF STEPS \_\_\_\_\_

## 1.10 To configure an e-mail server

### 1.10.1

Use this procedure to configure connection information to an e-mail server for use with Fault Management alarm e-mail policies.

1 \_\_\_\_\_

Sign in to NSP as an administrator.

2 \_\_\_\_\_

Choose More→Settings from the NSP Launchpad.

3 \_\_\_\_\_

Click E-mail Server Settings.

4 \_\_\_\_\_

Specify the address of an e-mail server and the user name and credentials of an administrative user.

5 \_\_\_\_\_

Click Save.

END OF STEPS \_\_\_\_\_

## 1.11 Licensing

### 1.11.1

Two types of licenses exist for NSP: Standard and Premium. When a Premium NSP license is in use, all NSP applications can be accessed from the Launchpad. When a Standard NSP license is in use, applications that require a Premium NSP license are identified by a badge.

**NOTE:** To acquire an NSP license, please contact your local Nokia representative.

## 1.12 REST API

### 1.12.1

Applications that use REST APIs publish a set of URLs that point to resources, or web services, managed by them. Each domain application documents the URLs that are available to users. These URLs can be accessed through a browser by any authorized user, including OSSs that can use them to cross-launch from their own application.

See the [NSP Developer portal \(https://nsp.developer.nokia.com/\)](https://nsp.developer.nokia.com/) for more information.

## 1.13 Accessibility

### 1.13.1

You can use the keyboard to navigate and interact with most of the applications. Keyboard navigation allows you to highlight and select interactive components in the application using keystrokes instead of a mouse.

The following table lists the accessibility options:

Keystroke	Action
Tab	Move to next element
Shift + Tab	Go back to previous element
Alt + down arrow Option/ALT + down arrow in Apple/OSX	Open pop-up menus, such as drop-down menus
Shift + F10 Shift + Fn + F10 in Apple/OSX	Open contextual menus
Ctrl + c Command + c in Apple/OSX	Copy
Ctrl + v Command + v in Apple/OSX	Paste
Enter	Open a folder or expandable object, such as a tile Invoke an action on a button or menu item
F8 Fn + F8 in Apple/OSX	Move over larger components or to the next page of a perspective
F5 Shift + Fn + F5 in Apple/OSX	Refresh
Shift + F1 Shift + Fn + F1 in Apple/OSX	Open tooltip
Esc	Close tooltip or menu

Keystroke	Action
Arrow	When you select a tile using the Tab key, navigate across tiles in a matrix, such as the Fault Management Top Unhealthy NEs view, or matrix view in Service Supervision, using the arrow keys. Up and down arrows for navigation across menu items in an open contextual menu or pop-up menu Up and down arrows for navigation across table rows Left and right arrows for navigation across table column headers
Shift + right or left arrow	Re-order columns of a data table when applied to a selected header button

## 1.14 Troubleshooting

### 1.14.1

This section describes various issues that application users may encounter, and provides recommendations to assist in the resolution of these issues, where possible.

### 1.14.2 Browser connections

All NSP applications are supported on the latest version of Google Chrome. For information about additional supported browsers for NSP applications, see the NSP NFM-P Planning Guide.

**NOTE:** For the Safari web browser to open the Analytics application, you must ensure that the following Safari privacy settings are configured, if they appear in your browser version:

- Cookies And Website Data setting on the Safari Preferences page is set to **Always Allow**
- Prevent cross-site tracking is disabled

**NOTE:** If you are using Chrome or Firefox on Windows 8.1 or Windows Server 2012, it is recommended that you enable ClearType Text for optimal viewing of fonts. In the Windows Control Panel, open the Display settings, and enable the Turn on ClearType parameter under the Adjust ClearType text settings.

**NOTE:** You cannot switch browsers between clients or applications. You must always use the browser configured as the default. See the *NSP NFM-P System Administrator Guide* for more information.

**NOTE:** The NSP Launchpad should should always be used to access NSP applications, as user-created links to individual applications can be broken by activity switches and/or software upgrades.

---

### 1.14.3 Remove unused applications to improve performance

To improve NSP start-up time, an NSP administrator can prevent any unused NSP applications from appearing on the NSP Launchpad. See [1.8 “To configure NSP application access control” \(p. 19\)](#).

### 1.14.4 Browser- and session-related errors

Some HTTP errors and/or stalled user sessions can be avoided by adhering to the following suggested best practices for working with NSP:

- Although other browser types are supported, Chrome is the preferred browser.
- Sign in to the NSP Launchpad before opening additional NSP applications in other tabs.
- Before signing in as a different user, close all other NSP tabs and sign out of the last tab.
- If multiple NSP applications are open in one browser, close all other NSP tabs before signing out of the last NSP tab. Do not just close the browser.
- Avoid pausing a polling application for more than ten minutes.
- In the event of NSP server activity switch or shutdown, close all browser tabs. Following server recovery, sign in again.
- Enable cookies in your browser.

### 1.14.5 Application GUI behavior during server connection timeout

NSP application sessions that are terminated by loss of connection to an NSP server may require up to two minutes to reset after the server connection is restored. In the interim, the application GUI may appear to function but executing commands within the GUI will result in Server Not Found browser errors. This condition persists until an automated system function clears the old application session.

## 1.15 Documentation

### 1.15.1

This section provides information about accessing NSP product documentation.

### 1.15.2 NSP product-level documentation

Information about NSP in general is conveyed in product-level documentation.

The following documents apply to the entire NSP product and are available to registered users on the [Documentation Center \(http://documentation.nokia.com\)](http://documentation.nokia.com):

- NSP Deployment and Installation Guide
- NSP Lab Installer Reference
- NSP Release Notice
- NSP Analytics Report Catalog

In addition, the NSP has a [channel on YouTube \(https://www.youtube.com/channel/UCjnWSQv4u90rfrhoO3DSkeQ\)](https://www.youtube.com/channel/UCjnWSQv4u90rfrhoO3DSkeQ).

---

### 1.15.3 Application help

The NSP applications have documentation available from the product user interfaces.



---

## 2 Fault Management

### 2.1 Overview

#### 2.1.1

Fault Management provides alarm monitoring, correlation, and troubleshooting for the most unhealthy NEs in the network. Filter alarm lists, identify root causes, and determine alarm impacts.


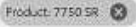



Fault Management components are also available in other applications in the NSP suite, such as Network Supervision and Service Supervision. Quickly investigate network problems and assess service impact with Fault Management and on-application alarm lists. Target specific alarms by filtering on set criteria.



### 2.2 Top Unhealthy NEs view

#### 2.2.1 Overview

The Top Unhealthy NEs view displays the NEs in your network with the highest number of alarms in a matrix format. NEs are represented as tiles, with alarm count information and links to alarm lists for the selected NE.

Manage the order and content of your Top Unhealthy NEs view using the following tasks:

- **Control what's visible in the matrix.** Click on the Filter button  and select one of these options:
  - Product - Select a product type from the list and you'll only see that NE product type in the matrix.
  - Topology Group - Select a topology group from the list and you'll only see NEs in that topology group in the matrix.
  - Unlocked Only - Select this option to see only unlocked NEs in the matrix.Add as many of these filters as you need. They appear as chip filters  at the top of the matrix. Click the Close button on a chip filter to remove it from the matrix.
- **Sort the matrix NE tiles.** Click the sort menu in the top right-hand corner of the matrix and select one of these options:
  - Total Active - NE tiles are sorted by the number of alarms against them.
  - Total Unacknowledged Active - NE tiles are sorted by the number of unacknowledged alarms against them.
  - Impact Counts - NE tiles are sorted by the number of network objects impacted by alarms on each NE.
- **View current alarms on an NE.** Hover over the More icon  and click the Current Alarms button .
- **View historical alarms on an NE.** Hover over the More icon and click the Historical Alarms button .

- **View current and historical alarms on an NE.** Hover over the More icon and click the Merged Alarms button .
- **Export a list of unhealthy NEs to a local CSV file.** Click More  > Export.

## 2.3 Alarm List views








### 2.3.1 Overview

The alarm list views present all alarms against NEs in your network. The lists can be filtered and sorted in a variety of ways to reduce the number of visible alarm messages to a manageable number. Open an alarm list from a specific NE to view alarms only for that NE. Open the general Alarm List view to see alarms for your entire network. Alarm messages are listed under three categories:



- The **current alarm list** displays all active alarms in the network, or for specific NEs.
- The **historical alarm list** displays all previously-active alarms in the network (or for specific NEs) over a specified time period.
- The **merged alarm list** displays all active and previously-active alarms in the network (or for specific NEs) over a specified time period.

### 2.3.2 To manage an alarm list

Manage the order and content of your alarm list using the following tasks:


- **Filter the Current Alarm List by severity.** Click on an alarm severity level icon in the Severity filter selector  to display only alarms of that particular severity level.
- **Filter the Current Alarm List to show root cause alarms only.** Click on the Filter button  and select Show Root Causes Only. A chip filter appears at the top of the list. Click on the Clear Filter button  to clear column filters.
- **Configure an advanced filter for the Current Alarm List.** Click on the Filter button  and select Advanced Filter.  
In the Advanced Filter form, specify a name and configure one or more filter criteria. Enable the Public option to make the filter available to other users, and accessible for alarm e-mail policies. Save the filter and click on the Apply button to apply it immediately. A chip filter appears at the top of the list. Click on the Clear Filter button  to remove the filter.
- **Filter the Historical or Merged Alarm List.** Click on the Source and Time Period chip filters to display alarm messages from a specific source system, and over a specific time period.
- **Filter the alarm list under a specific column.** Type a text string in the text field at the top of a column and press Enter, or use the date picker or drop-down menu (where available) and press Enter. Click on the Clear Filter button  to clear column filters.
- **Sort the alarm list under a specific column.** Click on a column header to sort the list under that column. Click the column header a second time to toggle the sort order (ascending/descending), as indicated by the Up/Down arrow.
- **Refresh the alarm list manually.** Click the Refresh button. 
- **Configure columns.** Right-click on a column header and choose Columns. A list of column names appears.

Click on the names of the columns that you want to display. Click above the column headers on the list to close the column selector and refresh the view.

- **Configure column sorting.** Right-click on a column header and choose Configure Sort. In the Configure Sort form, click Add Level  and choose the first column on which to sort, in ascending or descending order. You can continue to choose columns by which to sort the list. In the Configure Sort form, you can also copy, delete, and re-order selected entries.
- **Export alarms to a local CSV file.** Click More  > Export Visible Rows | All | Selected.





### 2.3.3 To manage alarm messages

Perform the following operations on selected alarm messages in the alarm list:


- **Acknowledge or unacknowledge an alarm.** On the right-hand side of an alarm item in the list, click More  > Acknowledge Alarm(s) | Unacknowledge Alarms.  
You can acknowledge or unacknowledge multiple alarms by pressing the Ctrl key and selecting the alarms, and clicking More > Acknowledge Alarm(s) | Unacknowledge Alarms in the top right-hand corner of the application window.  
If you select multiple NFM-P alarms, you can configure the Assigned Severity, and Acknowledgement Note. If you select multiple NFM-T alarms, you can configure the Acknowledgement Note. If you select both NFM-P and NFM-T alarms, you can configure the Acknowledgement Note.
- **Delete or clear an alarm.** Click More on the right side of a row and choose Delete Alarm(s) | Clear Alarm(s).  
You can delete or clear multiple alarms by pressing the Ctrl key and selecting the alarms, and clicking More > Delete Alarm(s) | Clear Alarms in the top right-hand corner of the application window.
- **Assign alarm severity.** On the right-hand side of an alarm item in the list, click More > Assign Severity.  
You can assign the same severity to multiple alarms by pressing the Ctrl key and selecting the alarms, and clicking More > Assign Severity in the top right-hand corner of the application window.
- **Assign alarm admin state.** On the right-hand side of an alarm item in the list, click More > Assign Admin State.  
You can assign the same admin state to multiple alarms by pressing the Ctrl key and selecting the alarms, and clicking More > Assign Admin State in the top right-hand corner of the application window.
- **Edit alarm custom text.** On the right-hand side of an alarm item in the list, click More > Edit Custom Text.  
You can add the same custom text to multiple alarms by pressing the Ctrl key and selecting the alarms, and clicking More > Edit Custom Text in the top right-hand corner of the application window.

### 2.3.4 To investigate alarms

Perform the following operations to further investigate selected alarm messages in the alarm list:


- **Show alarm details.** A selected alarm list item shows expanded information in the Details panel on the right-hand side of the GUI.
- **Show alarm impacts.** Click Show Impacts  on the right-hand side of an alarm item in the list to open the Impacts diagram for the selected alarm.  
**Note:** When NFM-T is deployed and an optical object is selected, viewing object impacts is not available
- **Show the root cause of an alarm.** Click Show Root Causes  on the right-hand side of an alarm item in the list to open the Root Cause diagram for the selected alarm.  
**Note:** This function is not available for NFM-T.
- **Show the object impacted by an alarm.** Click Show Object Impacts  on the right-hand side of an alarm item in the list to view the non-alarmed objects that are impacted by the alarm.  
**Note:** This function is not available for NFM-T.
- **Show alarms from the point of view of an affected object.** On the right-hand side of an alarm item in the list, click More  > Show Object Point Of View to open the Object Point of View diagram for the selected alarm.  
**Note:** This function is not available for NFM-T.


### 2.3.5 Alarm statistics

The Alarm Statistics chart displays network alarm counts by alarm severity. Click the Alarm Statistics button  to see the chart.

Click More  > Export Data to CSV to export the chart to a CSV file.


### 2.3.6 Alarm distribution


The Alarm Distribution diagram shows all root cause trees for the most impacting alarms for the network, with root cause alarms with no impacts hidden. Click the Alarm Distribution button  to see the diagram. The inner circle is each root cause alarm. The outer circles are objects impacted by the alarm, with the width of the blocks representing the impact magnitude. Click on an alarm to see its information in the panel on the right.

 **Note:** If the managed network yields only alarms with no impact, the Alarm Distribution diagram is blank.





In cases where the number of impacted objects is very high, the Alarm Distribution diagram data content is scaled down to maintain diagram readability. A message appears at the bottom of the diagram, indicating that scaling has occurred.

On the Info panel:


- Click Show Impacts  to open the Impacts diagram.


- Click Alarm List  to open the alarm list for the selected alarm, filtered by the alarm object full name.

Manage the order and content of your alarm distribution diagram using the following tasks:

- **Control what's visible in the alarm distribution diagram.** Click on the Filter button  and select one of the options (date range, name, system ID, product, topology group, or saved filter). Depending on what you select, additional filters options appear. Add as many of these filters as you need. They appear as chip filters  at the top of the diagram. Click the Close button on a chip filter to remove it from the diagram.
- **Hide specific alarm types.** Click More  and select the appropriate menu option to hide acknowledged alarms or maintenance (admin state) alarms.
- **Hide alarms of specific severity.** Click More  and de-select the appropriate severity options.



### 2.3.7 Alarm hierarchy

The Alarm Hierarchy diagram shows the most impactful problems in the network, allowing you to locate the biggest problems first, from the root cause alarm to the symptomatic alarms. Click the Alarm Hierarchy button  to see the diagram. Click on a ring or dot to zoom in, and click again to zoom out. Click on an alarm to see its information in the panel on the right.





 **Note:** Root cause alarms with no impact are hidden. If the managed network yields only alarms with no impact, the Alarm Hierarchy diagram is blank.

In cases where the number of impacted objects is very high, the Alarm Hierarchy diagram data content is scaled down to maintain diagram readability. A message appears at the bottom of the diagram, indicating that scaling has occurred.

On the Info panel:

- Click Show Impacts  to open the Impacts diagram.
- Click Alarm List  to open the alarm list for the selected alarm, filtered by the alarm object full name.

Manage the order and content of your Alarm Hierarchy diagram using the following tasks:

- **Control what's visible in the Alarm Hierarchy diagram.** Click on the Filter button  and select one of the options (date range, name, system ID, product, topology group, or saved filter). Depending on what you select, additional filters options appear. Add as many of these filters as you need. They appear as chip filters  at the top of the diagram. Click the Close button on a chip filter to remove it from the diagram.
- **Hide specific alarm types.** Click More  and select the appropriate menu option to hide acknowledged alarms or maintenance (admin state) alarms.
- **Hide alarms of specific severity.** Click More  and de-select the appropriate severity options.

## 2.4 Top Problems view

### 2.4.1

The Top Problems view displays the alarm types with the most occurrences in the network in the form of a bar chart. Each bar represents a specific alarm type, and its size represents the number of occurrences. The top 50 alarm types with the most occurrences are listed by default, from the highest to lowest number of occurrences. The top problems are polled according to the time interval your administrator set in the system preferences or that you set in your user preferences, from the Settings menu on the NSP Launchpad.

When you hover over a bar in the chart, the corresponding alarm type in the list is highlighted.

**Sort alarms.** Click the sort menu in the top right-hand corner of the chart and select a sort option (by total number of occurrences, total alarm count, or number of NEs on which the alarm is raised).

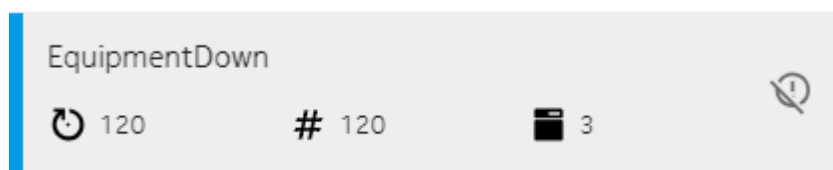
**Display preferences.** click More ⓘ and select a display preference for the chart. You can display the alarms by name, probable cause, or specific problem.

**Filter alarms by severity.** Click on the Filter button ⚙ (appears only when the alarms are displayed by alarm name) and select a severity level from the drop-down menu. Only alarms of the selected severity are displayed in the chart. Click the Close button on the chip filter to remove it from the chart.

**Export list of top problems to a CSV file.** Click More ⓘ > Export. Your display and sorting selections are preserved in the CSV file.

### 2.4.2 Alarm Type list






The Alarm Type list displays name and alarm count information for the top 50 alarm types displayed in the chart. The first icon in an alarm type list item shows the number of occurrences of the alarm type, the second icon shows the total alarm count, and the third icon shows the number of NEs affected by the alarm type. When you hover over an alarm type in the list, the corresponding bar in the chart is highlighted.



**Hide Alarm Types.** Hide an alarm type from the list and the chart by clicking the Hide button ⓘ that appears when you hover on the right-hand side of an alarm type item. If any alarms are hidden, the Hidden Alarm Type button is enabled on the main toolbar. Click this button to remove the alarm type from the list of hidden alarms (the alarm type is re-displayed).

## 2.4.3 Top Problems Matrix

The Top Problems Matrix view displays up to 50 NEs on which the selected alarm type occurs. Click on a bar in the Top Problems view to opens it in the Matrix view. Each affected NE is represented as a tile. The first icon in a tile shows the number of occurrences of the alarm type and the second shows the total alarm count.

- **View current alarms on an NE.** Hover over the More icon on a tile  and click the Current Alarms button .
- **View historical alarms on an NE.** Hover over the More icon on a tile and click the Historical Alarms button .
- **View current and historical alarms on an NE.** Hover over the More icon on a tile and click the Merged Alarms button .
- **Export a list of unhealthy NEs to a local CSV file.** Click More  > Export.

## 2.5 Inspector view

### 2.5.1

In the Inspector, search for specific NEs to be displayed in a matrix.

**Adding NEs** - Click on Add New NE and use the search menu to select your search criterion. You can enter text in the search field to limit the results or scroll through the list. Up to 256 results are listed. Click on an NE to add it to the beginning of the matrix, or drag an NE to the desired location in the matrix. You can add up to 50 NEs.

**Details** Click on an NE to view more information about the NE in the Details panel.

**Merged Alarms** Hover over the right side of the NE and click Merged Alarms to view the merged list of current and historical alarms.

**Removing NEs** Hover over the right side of the NE and click Remove to remove the NE from the Inspector. Click Remove All to remove all of the NEs from the Inspector.

## 2.6 To configure current alarm list settings

### 2.6.1

Configure aging and overflow settings for the current alarm list. These settings apply to NFM-T alarms and MDM alarms. NFM-P alarm settings are configured in the NFM-P GUI; see the *NFM-P System Administrator Guide*.

You must have administrator privileges to configure alarm settings.

1 \_\_\_\_\_

Click More→Settings. The Alarm Settings form opens.

2 \_\_\_\_\_

Click Current Alarms on the left-hand panel.

- 
- 3 \_\_\_\_\_  
Enable the Aging Settings option and specify the number of days after which alarms are deleted.
  - 4 \_\_\_\_\_  
Under Overflow Settings, specify the percentage of the maximum alarm count at which an alarm overflow warning is issued. (The maximum alarm count is hard coded at 150000 alarms if NFM-T and NFM-P are deployed in shared mode, or 300000 alarms if NFM-T is deployed alone.)
  - 5 \_\_\_\_\_  
Specify an overflow action. If you choose Halt, all new alarms are dropped. If you choose Wrap, alarms are purged from the database, based on the following settings:
    - Purge Amount - the percentage of the current alarm count to be deleted.
    - Purge Policy - either the lowest severity alarms are deleted first or the oldest alarms are deleted first.
  - 6 \_\_\_\_\_  
Save your changes.

END OF STEPS \_\_\_\_\_

## 2.7 To configure historical alarm list settings

### 2.7.1

Configure logging and overflow settings for the historical alarm list. These settings apply to NFM-T alarms and MDM alarms. NFM-P alarm settings are configured in the NFM-P GUI; see the *NFM-P System Administrator Guide*.

You must have administrator privileges to configure alarm settings.

- 1 \_\_\_\_\_  
Click More→Settings. The Alarm Settings form opens.
- 2 \_\_\_\_\_  
Click Historical Alarms on the left-hand panel.
- 3 \_\_\_\_\_  
Enable the Archive Settings option and enable either or both of the Log on Change and Log on Deletion options.

---

**4** \_\_\_\_\_  
Under Overflow Settings, specify the maximum alarm count at which an alarm overflow warning is issued.

**5** \_\_\_\_\_  
Specify a warning threshold as a percentage of the maximum alarm count, and specify the percentage of the alarm count to be purged at the time of the warning message.

**6** \_\_\_\_\_  
Specify a critical threshold as a percentage of the maximum alarm count, and specify the percentage of the alarm count to be purged at the time of the critical message.

**7** \_\_\_\_\_  
Save your changes.

END OF STEPS \_\_\_\_\_

## 2.8 To configure system alarm settings

### 2.8.1

Use this procedure to configure alarm handling options for alarm messages originating from the NSP system for the Fault Management application.

You must have administrator privileges to configure alarm settings.

**1** \_\_\_\_\_  
Click More→Settings. The Alarm Settings form opens.

**2** \_\_\_\_\_  
Click System Alarms on the left-hand panel to configure system-wide alarm settings.

**3** \_\_\_\_\_  
Enable the Alarm Severity Settings option and then configure manual and automatic options, as required.

**4** \_\_\_\_\_  
Enable the Alarm Deletion Settings option, as required, and then enable and configure any of the following options:

- Manual Alarm Deletion Settings
- Correlated Alarm Settings for Manually Deleted Alarms
- Automatic Alarm Deletion Settings

**5** \_\_\_\_\_

---

Enable the alarm acknowledgement policy, as required.

6

---

Save your changes.

END OF STEPS

---

## 2.9 To configure an e-mail policy

### 2.9.1

The Fault Management e-mail policy feature allows administrative users to configure e-mail notification policies for specific alarm messages in NFM-P, NFM-T, MDM, and NSP. An e-mail policy is configured with a filter. When an alarm message matches the filter criteria, the policy sends alarm notifications to a specified list of up to 20 user e-mail addresses. In order to manage bursts of alarm messages, e-mail notifications are pooled for up to one minute before sending. If there are more than ten alarms within one minute for a specific policy, a single e-mail notification is sent with a list of ten alarms. Each e-mail policy specifies the maximum number of e-mail notifications (up to 20) that can be sent over a one-hour period. The recipients are notified when the maximum has been reached.

**i** **Note:** LI and mirror service alarms are not sent in e-mail notifications.

In order for Fault Management to send e-mail notifications, you must configure connection information for an e-mail server through the NSP Launchpad; see the NSP Launchpad documentation.

You must have administrator privileges to configure alarm e-mail policies.

1

---

Click More→Settings. The Alarm Settings form opens.

2

---

Click E-mail Policies on the left-hand panel.

3

---

Click on the Create New Policy button  .

4

---

Type a name for the policy.

5

---

Select an alarm filter.

The Alarm Filter menu is populated with public advanced filters configured and saved in the Current Alarms list; see [2.3.2 “To manage an alarm list” \(p. 28\)](#).

---

**6** Click on the Add Recipient button and type the e-mail address of an intended recipient for the alarm notification. You can specify up to 20 recipients.

**7** Adjust the Max E-mails Per Hour slider to set the maximum number of alarm notifications that can be sent per hour.

**8** Check or un-check the Enabled option to enable/disable the policy.

**9** Click Apply to save the e-mail policy.

END OF STEPS

---

## 2.10 Fault Management general operations

### 2.10.1

This section describes specific application functions for which users may need additional information in order to maintain proper system operations. Where appropriate, recommendations are provided to assist in the resolution of functional issues.

### 2.10.2 Alarm reload behavior

When alarm messages from MDM and NFM-T sources are modified or deleted in the Fault Management application, the change is recorded in the NSP database, but not at the alarm source. If alarms are bulk-reloaded from an MDM or NFM-T source to the Fault Management application, previously modified or deleted alarms from that source are handled in the following manner:

- For alarms with modified fields, any data already in the NSP database is not overwritten by the reloaded alarm.
- Alarms in the NSP database that are tagged as Transient (i.e., not standing alarms) are not deleted by the reload, even if they are no longer present on the source system.



---

## 3 Network Supervision

### 3.1 Overview

#### 3.1.1

Network Supervision allows users to monitor the health of objects, such as NEs, cards, ports, or links, using KPIs, and monitor the fault status of a network. Network Supervision uses supervision groups, which can belong to one or more views.

A supervision group is a logical set of monitored objects, in this case NEs and VNFs, that is specified by user-defined filters.

NEs are both physical network functions and virtual network functions. Physical network functions are referred to as PNFs and virtual network functions are referred to as VNFs in the online help.

Supervision groups can be used to partition objects into distinct categories and are associated with views. There is no limit to the number of supervision groups to which an object can belong.

The criteria for monitored objects in a supervision group are based on inclusion filters. The inclusion filter is the rule on whether to include an object in a supervision group.

A view is a collection of one or more supervision groups that provides a summarized, high-level view of a group of network objects. There is no limit to the number of views to which a supervision group can belong, but each view can contain only up to 200 supervision groups.

### 3.2 Network Supervision views

#### 3.2.1

When you open Network Supervision for the first time, you must select a view. The view opens a summary of NE supervision groups, which are displayed as tile objects, with basic status information for the group. Once a view is selected, Network Supervision will always open to the view, unless you select a different view.

A view is made up of supervision groups, which are displayed as tile objects. Each group tile object provides a high-level view of the status of the NEs within the group:

- Tile banner color indicates the rough percentage of alarm-affected NEs in the group, in accordance with the application KPI threshold settings.
- Number of NEs in the group.
- Number of alarm-affected NEs in the group.
- Number of unacknowledged critical alarms in the group.

Views and supervision groups are created in the Supervision Manager; see [3.9.2 “To create a view”](#) (p. 52) and [3.9.3 “To create a supervision group”](#) (p. 53).

---



### 3.2.2 To select a view

- 1 \_\_\_\_\_  
In the Network Supervision application, click More→View.
- 2 \_\_\_\_\_  
Click on the view you want to display.

END OF STEPS \_\_\_\_\_

### 3.2.3 Working in a view

Navigate a view using the following tasks:

- **View the contents of a supervision group.** Double-click on the group tile object. The supervision group opens as a matrix, list, or other format.
- **View additional information for a supervision group.** Hover over the More button and click More Details  to expand the group tile. The expanded tile displays the number of alarm-affected cards, ports, and links in the group, as well as the number of acknowledged and unacknowledged alarms.
- **View all current alarms for a supervision group.** Hover over the More button and click Current Alarms  to open the Alarms list.

### 3.2.4 Supervision groups

A supervision group is a logical group of NEs. You can view a supervision group in a variety of formats.

**Change format.** Click the Format Changer in the upper right-hand corner of the GUI and select a format from the menu.



## 3.3 Network Supervision display formats







### 3.3.1 NE matrix

Displays NEs as tile objects, with basic information about hardware status for the NE. Tile banner color indicates the rough percentage of alarm-affected equipment on the NE, in accordance with the application KPI threshold settings.

---

### 3.3.2 NE list

Displays NEs as list items, with system information for the NE.


- **View current alarms for the supervision group.** Click on the Current Alarms button  on the toolbar. To return to the list, click on the Object View button.
- **Filter the NE list under a specific column.** Type a text string in the text field at the top of a column and press Enter. Click on the Clear Filter button  to clear column filters.
- **Sort the NE list under a specific column.** Click on a column header to sort the list under that column. Click the column header a second time to toggle the sort order (ascending/descending), as indicated by the Up/Down arrow.
- **View current alarms for an NE.** Select an NE list item and click on the Current Alarms button  on the right-hand side of the item.
- **View the event timeline diagram for an NE.** Select an NE list item and click on the Event Timeline button  on the right-hand side of the item.
- **View the troubleshooting map for an NE.** Select an NE list item and click on the Troubleshooting Map button  on the right-hand side of the item.
- **View the equipment Inventory for an NE.** Select an NE list item and select More  → Show Inventory from the menu on the right-hand side of the item.
- **View merged alarms for an NE.** Select an NE list item and select More→Merged Alarms from the menu on the right-hand side of the item.
- **View historical alarms for an NE.** Select an NE list item and select More→Historical Alarms from the menu on the right-hand side of the item.
- **Add an NE to the Watch view.** Select an NE list item and select More→Add To Watch View from the menu on the right-hand side of the item.
- **Open an NE in its management application.** Select an NE list item and select More→Show Object from the menu on the right-hand side of the item.
- **Run Analytics reports for an NE.** Select an NE list item and select More→Analytics Reports from the menu on the right-hand side of the item.
- **Copy NE information to the clipboard.** Select an NE list item and select More→Open In Copy Window from the menu on the right-hand side of the item. In the Copy window, press Ctrl+C or Command+C.




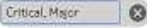







### 3.3.3 Topology map

Displays the NEs in a supervision group as a map of linked objects.

Physical topology maps can display either an Operational map view or a Utilization map view. The Operational map is displayed by default. Click on the View chip on the map to toggle between the Operational and Utilization map views. For information about the Utilization map, see [3.3.4 “Utilization map view” \(p. 43\)](#).

Topology maps allow you to perform the following:

- **Set number of hops from initial object.**  Set the hop count to show NEs and links a specified number of hops from the initial NE.

- **View quick NE information.** Hover over an NE or link object to display basic system and alarm information for the object.
- **View full NE details.** Click on the Info  button to open the Information panel, which displays detailed information about a selected map object.
- **Interpret map information.** Click on the Legend button  to open the map legend, which describes the meaning of different objects and status colors seen in the topology map.
- **Find alarm-affected NEs.** NE objects with alarms carry a badge. The badge color indicates alarm severity, as described in the Legend panel.
- **Filter the topology map content.** Click on the Add Filter button  and select one of the filter types: Alarm Severity, Chassis Type, Network Type, Product Type, or Status.  
A chip filter is added to the topology map . Click on the chip filter and select one or more criteria related to the filter type. You can add up to three filters. Click the Close button on a chip filter to remove it from the map.
- **Refresh map data.** Click on the Refresh Data button  to update the map contents.
- **View a map object in its management application.** Click on the NE or link object you want to view. In the Information panel, click More→Show Object. The object is opened for configuration in its management application.  
For NSP deployments that include NRC-X, click on a cross domain link and choose More... > Show in Cross Domain Coordinator. The Cross Domain Coordinator application opens with the cross domain link highlighted on the network map.
- **Map controls:** Vertex clustering is enabled by default. You can expand the cluster by clicking on a cluster, for example "6 Nodes", or by using the zoom controls.
  -  fit the map to available screen area
  -  adjust vertex size, show connectors, turn vertex clustering on or off, and specify the cluster distance. Show text labels for vertices and status charts for vertex clusters and link groups
  -  show or hide links, adjust link curvature, turn link grouping on or off, and specify the link grouping threshold
  -  show a bird's eye view of the map
  -  zoom in and out of the map
- **Restore default layout** Click More→Restore Default Layout, to return the map layout to the default layout, as specified by an Administrative user.  
Administrative users can click More→Set As Default Layout to set the current map layout as the default layout that loads when a user clicks on Restore Default Layout.
- **Search the map.** Click on the Search button  to search for PNFs, VNFs, or VNFCs based on different attributes, such as name, or location.

### To configure physical links


 **Note:** You must be logged in as an Administrative user to configure physical links.

1

Click More→Physical Links to open a list of manually-created physical links in the topology map view.

---

2

In the Manually Created Physical Links form, you can create a new link by clicking on the Create Physical Link button . In the Create Physical Link form, you specify the Name, Description, and Latency for the link, and then search endpoints for the link.

---

3

You can delete a physical link from the Manually Created Physical Links form by selecting it in the list and clicking on the Delete button at the end of the row.

---

END OF STEPS

### 3.3.4 Utilization map view

The Utilization map view displays colored arrows to show how much of the capacity on a port is being utilized. The Utilization map allows you to quickly assess how efficiently your network is managing traffic, and to identify ports that are over- or under-utilized. Click on the View chip on the Operational map to switch to the Utilization map.

Network utilization can be analyzed in physical topology maps for all NEs and links in a supervision group, and in troubleshooting maps on a focused set of NEs and links.

#### Requirements


Information in the Utilization map is based on statistics collected for IP links on Ethernet physical ports. Statistics must be supported and available for utilization to be displayed. The Operational State of NEs and ports must be Up.

Statistics are collected using SNMP or Telemetry.

For SNMP, NEs must be managed by the NFM-P and reachable using SNMP. The following NEs support SNMP statistics for the utilization map:

- 7450 ESS, Release 15.0 or later
- 7750 MG and MG VSR, Release 10.0 or later
- 7750 SR and VSR, Release 15.0 or later
- 7950 XRS, Release 15.0 or later

For Telemetry, NEs must be configured for Telemetry collection; see the Telemetry documentation in the Launchpad help for more information.

 **Note:** For the Utilization map, Telemetry collection must be enabled for NEs discovered by the NFM-P using SNMP. Telemetry collection for NEs discovered by the NSP using MDM is not supported.

The following NEs support Telemetry statistics for the utilization map:

- 7450 ESS, Release 15.0 or later, for chassis types that support Telemetry
- 7750 MG, Release 10.0 or later, for chassis types that support Telemetry
- 7750 SR, Release 15.0 or later, for chassis types that support Telemetry

- 7950 XRS, Release 15.0 or later, for chassis types that support Telemetry

The size of the supervision group may affect performance. Consider the following:

- If the number of links in the supervision group is large, there may be a delay before the Utilization option appears in the View chip.
- Statistics are collected by subscription from qualified ports. If there are too many qualified ports in the supervision group, no utilization information is displayed. For SNMP, the limit is 1000 ports; for Telemetry, the limit is 100 ports. A notification appears when the limit is exceeded.

### Initial setup

Perform the following to set preliminary preferences for the Utilization map view:

1. Choose the utilization statistics type (SNMP or Telemetry); see [3.5 “To configure application preferences” \(p. 50\)](#).
2. Set preferences for refresh rate, line thickness change threshold, and arrow color change threshold; see [“Utilization Map Preferences” \(p. 44\)](#).

### How it works

The Utilization map shows NEs connected by link lines that represent physical connections between endpoints. The lines have the following features:

- **Thickness.** The relative capacity on the link is indicated by a thin, medium, or thick line. Thinner lines indicate lower capacity, thicker lines indicate higher capacity. You can configure thresholds for the speed at which the line thickness changes; see [“Utilization Map Preferences” \(p. 44\)](#).
- **Color.** Physical links between endpoints are shown in grey. Utilization is shown as a green, orange, or red arrow along the grey line. Each color indicates a range of utilization: low, medium, or high. The colors change as utilization (in percent) crosses preset thresholds. To define custom threshold settings (color change points) for the utilization ranges, see [“Utilization Map Preferences” \(p. 44\)](#).
- **Arrow length.** The length of the colored arrow shows the relative utilization of the capacity on the link. Arrows grow from minimal utilization at an endpoint, to 100% utilization at the mid-point crossbar (for bidirectional links). The crossbar represents 100% utilization from either direction. Utilization rates near zero will show a disproportionately long arrow (it may look like 5% or so) to provide a visual cue that there is utilization on the link. A grey line with no colored arrow means either zero utilization, or there is no data available for that link. If SNMP or Telemetry statistics are not supported, traffic may be present, but no utilization arrow is displayed.

The Utilization map view is updated according to a user-defined refresh rate; see [“Utilization Map Preferences” \(p. 44\)](#).

### Utilization Map Preferences


Perform the following to configure Utilization Map Preferences:

1. In the Network Supervision application, click More → Utilization Map Preferences.

2. Configure the Refresh Rate, Port Speed Settings, and Color settings as required.  
Alternatively, restore the default settings.

The Port Speed settings define the thresholds at which the link lines change thickness. The Color settings define the thresholds at which the arrows change color.

3. Close the form.

 **Note:** Utilization preferences apply in the session in which they are configured, and in subsequent sessions.

### 3.3.5 Link list

The Link list shows a table of information about physical links in a supervision group. Each row of the table shows information for one physical link. The operational state of the link, and information about both endpoints (A and B), are displayed.

Filter and sort the Link list using the same filtering and sorting functions as other NSP list formats. Investigate alarms using the Current Alarms button; see [3.3.2 “NE list” \(p. 41\)](#).

Refresh the list using the Refresh button on the toolbar.

Open a Troubleshooting map for the link by hovering on an entry in the list and clicking on the Troubleshooting icon at the far right. The Troubleshooting map highlights the link and shows the two endpoint NEs, plus one hop from each endpoint. The Hop count and Explore functions are supported; see [3.3.6 “Troubleshooting map” \(p. 44\)](#).

### 3.3.6 Troubleshooting map

The Troubleshooting map displays an NE in a map, along with linked objects.

Troubleshooting maps provide an optional Utilization map view. Click on the View chip on the map to toggle between the Operational and Utilization map views. See [3.3.4 “Utilization map view” \(p. 43\)](#) for more information. In Troubleshooting maps, the Utilization view does not support the Hop count, Explore, or Refresh functions.


## 3.4 Routine NE maintenance with Network Supervision

### 3.4.1 Purpose

This topic provides you with a task flow to use the Network Supervision application to monitor the status of your network hardware (NEs and their installed equipment) and to locate and troubleshoot the root cause of problems.


### 3.4.2 Starting points for troubleshooting monitored NEs

Any of the following events could indicate that you need to troubleshoot your network:


- One or many KPI icons turn red or show upward trending arrows  on NEs in the Watch view.  
To add NEs to the Watch view, hover over an NE tile in the NE Matrix and click More > Add To Watch View.

- A summary group turns red or shows upward trending arrows in the Summary view.

Summary group with high KPIs	Number of affected NEs	Current critical unacknowledged alarm count	
Group Name			#
East Subnet	4	53	4

- NE tiles change color or show upward trending arrows  in the NE Matrix.

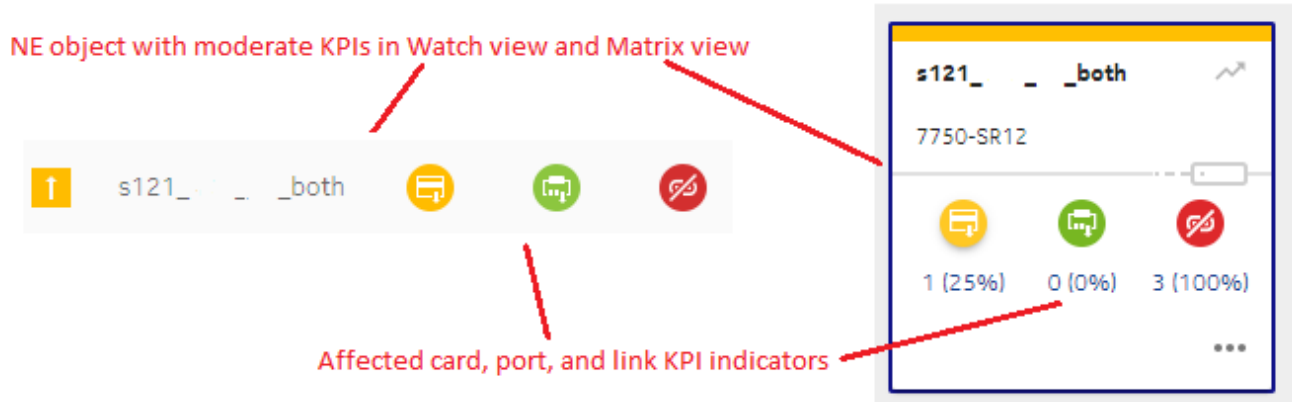
### 3.4.3 Triaging steps for a summary group

- 1 \_\_\_\_\_  
Select an affected summary group in the Summary view.
- 2 \_\_\_\_\_  
Determine the number of affected NEs and critical alarms for the group.
- 3 \_\_\_\_\_  
Click on the summary group to display its NEs in the NE Matrix.  
From the Matrix, you can open the Alarms list  to view alarms for the entire summary group.
- 4 \_\_\_\_\_  
Proceed to [3.4.4 “Triaging steps for an NE”](#) (p. 45).

END OF STEPS \_\_\_\_\_

### 3.4.4 Triaging steps for an NE

- 1 \_\_\_\_\_  
Select an affected NE in the Watch view or NE Matrix.
- 2 \_\_\_\_\_  
Determine which KPIs on the NE are affected (yellow or red color): the number of cards, ports, or links that are down.



Also look for upward trending arrows on NEs in the Watch view or NE Matrix. These indicate affected NEs that developed problems recently.

3

Select one or more of the following methods to troubleshoot the problem.

### Troubleshooting with the Alarms list and Event Timeline

4

Open the Alarms list to view all standing alarms for the selected NE; on the NE tile, click More > Current Alarms.

5

Click on an alarm message in the list to display complete details of the alarm, including descriptive and remedial information.

If you suspect that the affected object for the selected alarm is a cause of the current problem, you can open the affected object in its management application directly from the Alarms list. On the selected alarm item, click More > Show Affected Object. Make configuration changes to the affected object while monitoring the object in Network Supervision to determine if KPIs improve as a result of the change.

6

To further investigate a selected alarm, open its Impact Analysis diagram to view objects impacted by the alarm. On the selected alarm item, click Show Impacts .

The selected alarm object is circled in dark blue. Click on an alarm object to view details and remedial information.

The screenshot shows a comparison between two alarm types: 'EquipmentDown' (represented by a large orange and blue target icon) and 'LinkDown' (represented by a smaller blue target icon with a red center). A red arrow labeled 'Selected alarm details' points from the 'LinkDown' icon to the right-hand panel. This panel contains two sections: 'Description' and 'Remedial Action'. The 'Description' section states: 'The alarm is raised when the compositeEquipmentState attribute has equipmentOperationallyDown.' The 'Remedial Action' section states: 'This alarm indicates that a card in the The card must be replaced.'

If you suspect that the affected object for the selected alarm is a cause of the current problem, you can open the affected object in its management application from the Impact Analysis view. At the bottom of the Details panel, click Show Affected Object . Make configuration changes to the affected object while monitoring the object in Network Supervision to determine if KPIs improve as a result of the change.

7



Open the Event Timeline for the alarm to view events that occurred just prior to the alarm being raised, and determine the possible cause (for example, an object configuration change). Adjust the date range around the alarm event as required.

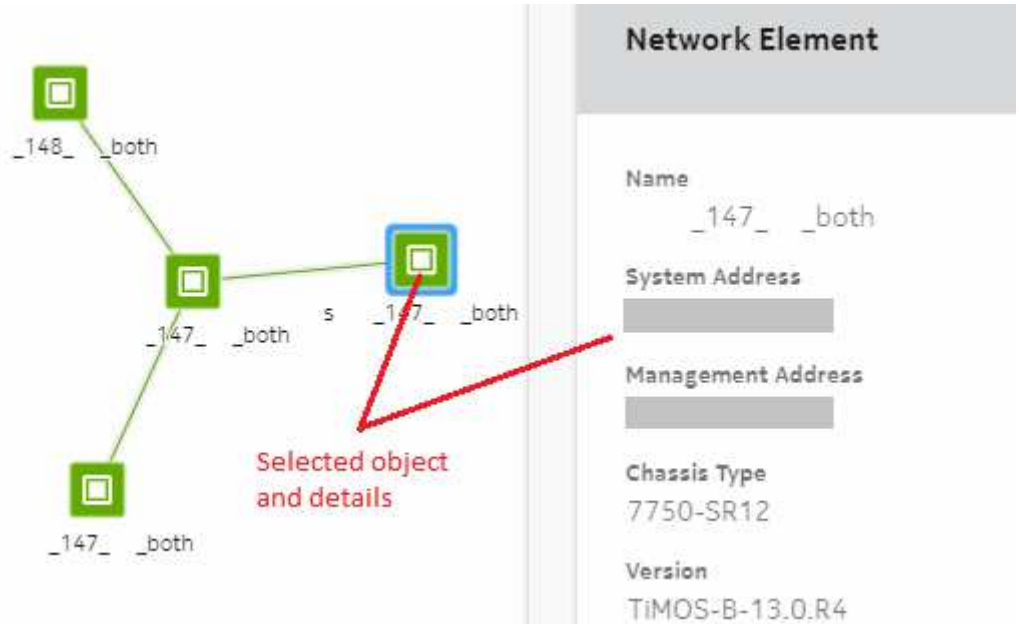
The screenshot displays an event timeline for the period '05 15:11:00 - 2018/06/06 15:16:00'. A red arrow labeled 'Event time range' points to the date range. Below the timeline, a red arrow labeled 'Details for selected event' points to a blue circular icon with a white double-headed arrow. To the right, a details panel for 'StateChangeEvent' is shown, with a red arrow pointing from the selected event icon to this panel. The details panel includes the following information: Name: network:10.10.10.117, Type: Network Element, and Class: netw.NetworkElement.

Select an event icon in the timeline to view information related to the event.

## Troubleshooting with the Troubleshooting Map

8

Return to the NE Matrix or Watch view and open the Troubleshooting Map  for the selected NE. Click on a red NE or link object and then click on the Info  button to view details about the object.



NE objects with alarms carry a badge. The badge color indicates alarm severity, as described in the Details panel. Hover over an NE or link object to view basic status or alarm information about the object.

To correct a problem on an affected object, you can open the object in its management application to change its configuration, or to undo a previous configuration change that caused the problem. On the Details panel, click More > Show Object. Make configuration changes to the affected object while monitoring the object in Network Supervision to determine if KPIs improve as a result of the change.

Click on the View chip on the Operational map to open the Utilization map. Inspect the map for links that are under- or over-utilized, based on the color and length of the utilization arrows. See [3.3.4 "Utilization map view" \(p. 43\)](#).

9

When troubleshooting is complete, verify that all alarms have cleared and KPI indicators are green.

END OF STEPS

---

## 3.5 To configure application preferences

### 3.5.1

You can specify whether an object's administrative state is used to calculate its KPI level in Network Supervision.

1 \_\_\_\_\_

Login to NSP as an administrator and launch Network Supervision.

2 \_\_\_\_\_

In the Network Supervision application, click More→Application Preferences.

3 \_\_\_\_\_

Enable or disable the checkbox to use object administrative state for KPI calculations.

4 \_\_\_\_\_

Select a statistics type for data collection for the Utilization map view.

5 \_\_\_\_\_

Save your changes.

END OF STEPS \_\_\_\_\_

## 3.6 To configure KPI threshold settings

### 3.6.1

Use the KPI Threshold Settings form to specify the affected NE/component counts at which Network Supervision GUI objects change color to indicate status change.

1 \_\_\_\_\_

In the Network Supervision application, click More→KPI Threshold Settings.

2 \_\_\_\_\_

In the KPI Threshold Settings form, drag the cursors on the threshold line to the levels at which you want object color changes to occur.

3 \_\_\_\_\_

Save your changes.

END OF STEPS \_\_\_\_\_

---

## 3.7 To configure Event Timeline settings

### 3.7.1

**i** **Note:** You must be logged into NSP as an administrative user to complete this procedure.

Use the Event Timeline settings form to enable/disable event logging and specify the object types that appear in the Event Timeline.

1 \_\_\_\_\_

In the Network Supervision application, click More→Timeline Settings.

2 \_\_\_\_\_

In the Timeline Settings form, enable or disable event recording in the Network Supervision application.

3 \_\_\_\_\_

Enable the checkbox for each network object type that you want to appear in the Event Timeline.

4 \_\_\_\_\_

Save your changes.

END OF STEPS \_\_\_\_\_

## 3.8 To configure user preferences

### 3.8.1

You can specify a variety of custom view settings in Network Supervision to suit your needs.

1 \_\_\_\_\_

In the Network Supervision application, click More→User Preferences.

2 \_\_\_\_\_

In the User Preferences form, configure view capacity, sorting, and refresh settings, as required.

3 \_\_\_\_\_

Save your changes.

END OF STEPS \_\_\_\_\_

---

## 3.9 Supervision Manager

### 3.9.1

The Supervision Manager is used to create network views and supervision groups for Network Supervision.

### 3.9.2 To create a view

**i** **Note:** You must be logged into NSP as an administrative user to complete this procedure.

- 1 \_\_\_\_\_  
In the Network Supervision application, click More→Supervision Manager. The Supervision Manager application opens on a new browser tab.
- 2 \_\_\_\_\_  
On the Views list on the left-hand side of the GUI, click the Add View (+) button. The Add a New View form appears.
- 3 \_\_\_\_\_  
Specify a name for the view.
- 4 \_\_\_\_\_  
Enable the Automatically Creates Supervision Groups option.  
If this option is disabled, the resulting view will contain no supervision groups. You can add groups later.
- 5 \_\_\_\_\_  
Choose an option to create supervision groups based on Product Type or VNF Type.
- 6 \_\_\_\_\_  
Click Ok. The Supervision Manager grid is populated with supervision groups, represented as tile objects.
- 7 \_\_\_\_\_  
Return to the Network Supervision application browser tab.
- 8 \_\_\_\_\_  
Click More→View and select the new view from the menu.

**END OF STEPS** \_\_\_\_\_

---

### 3.9.3 To create a supervision group

**i** **Note:** You must be logged into NSP as an administrative user to complete this procedure.

- 1 \_\_\_\_\_  
In the Network Supervision application, click More→Supervision Manager. The Supervision Manager application opens on a new browser tab.
- 2 \_\_\_\_\_  
On the Views list on the left-hand side of the GUI, click on the view to which you want to add a group.
- 3 \_\_\_\_\_  
On the right-hand side of the GUI, click on the Add Supervision Group (+) button. The Add Supervision Group form appears.
- 4 \_\_\_\_\_  
Specify a name for the supervision group and follow the instructions in the form, clicking Continue to navigate through the pages.  
  
In order to add NEs to the supervision group, you will need to specify inclusion filters to list the NEs. You can filter the NEs based on NE attributes, or you can create advanced filter expressions. Alternatively, you can manually add NEs to the group by specifying individual NE management IP addresses, or by importing a comma-separated list of NE management IP addresses.
- 5 \_\_\_\_\_  
When you have reviewed the list of NEs to include in the supervision group, click Finish to save the group.
- 6 \_\_\_\_\_  
Return to the Network Supervision application browser tab.

END OF STEPS \_\_\_\_\_

## 3.10 Network Supervision general operations

### 3.10.1

This section describes specific application functions for which users may need additional information in order to maintain proper system operations. Where appropriate, recommendations are provided to assist in the resolution of functional issues.

---

### 3.10.2 Mediation software capabilities

Actions performed on objects in the Network Supervision application depend on the capabilities of the object's source mediation software. In particular, certain application functions described in the Network Supervision Help may not be available when the NSP is deployed with the NFM-T, but in the absence of the NFM-P:

- The Event Timeline function is disabled for NFM-T objects in the Watch view, NE Matrix, and NE list.
- Event Timeline settings cannot be configured in an NFM-T-only deployment. Default settings are used.
- The Policy Agent function is not available in an NFM-T-only only deployment.
- The CBAM Access Point function is not available in an NFM-T-only deployment.

### 3.10.3 Map view performance

Users should consider the performance information in this section when working in Network Supervision map views.

Nokia recommends a maximum of 2000 NEs per supervision group. Multi-layer maps support a recommended maximum of 4000 objects.

Users should expect the following Multi-layer map loading times with different numbers of NEs:

- for 250 NEs (125 physical links); approximately six seconds for the initial page loading and four seconds to reload
- for 500 NEs (250 physical links); approximately nine seconds for the initial page loading and six seconds to reload
- for 2000 NEs (1000 physical links); approximately 50 seconds for the initial page loading and 28 seconds to reload

### 3.10.4 To purge assurance event records

The event timeline in applications is a log of events that is mapped over a specified period of time. You can filter the event types presented on the timeline, such as alarm events, OAM test failures, and configuration and state change events. You can use the event timeline to search for patterns in events over a period of time.

Perform this procedure to purge assurance event records when the AssuranceEventLoggingTurnedOff alarm is raised. This alarm is raised when the database disk space used to log assurance events grows above the predefined threshold.

Assurance Event logging is disabled to protect the database disk space.

**i** **Note:** You must be logged into the NFM-P as an administrator to perform this procedure.

1

---

From the NFM-P main menu, choose Tools→Events→Event Policies. The Manage Event Policies form opens.

---

**2** Choose the assurance.AssuranceEvent event type and click Properties. The Event Policy - assurance.AssuranceEvent (Edit) form opens.

**3** Click the More Actions button and choose Purge Event Records. The Event Policy - assurance.AssuranceEvent (Edit) Filter form opens.

**4** Click OK to purge all event records.

**5** If necessary, configure the Event Retention Time (hours) to a value lower than the default value.

**6** Save the changes and close the forms.

**END OF STEPS**

---



---

## 4 Service Supervision

### 4.1 Overview

#### 4.1.1

Service Supervision allows you to monitor the health of services using KPIs, and monitor the fault status of a network. Service Supervision uses supervision groups, which can belong to one or more views.

A supervision group is a logical set of monitored services that is specified by user-defined filters. Supervision groups can be used to partition services into distinct categories, and are associated with views. There is no limit to the number of supervision groups to which a service can belong.

Up to 50 000 services can be included in a supervision group. VLL, VPLS, MVPLS, IES, and VPRN services can be included.

The criteria for monitored objects in a supervision group are based on inclusion filters. The inclusion filter is the rule on whether to include an object in a supervision group. For example, for the Wireless Supervision application, the inclusion filters used to specify the eNodeBs in a supervision group must exclude pre-provisioned NEs and all other non-eNodeB NE types to avoid misleading alarms and KPI numbers.

A view is a collection of one or more supervision groups that provides a high-level view of a group of services. There is no limit to the number of views to which a supervision group can belong, but each view can contain only up to 5000 supervision groups.

#### 4.1.2 Service Supervision in shared deployments

When NSP is deployed with the NSD module and the Service Fulfillment application, the Service Supervision application provides supervision of services provisioned via the Service Fulfillment application and/or other means, such as the NFM-P service manager. The service terminology used in Service Supervision aligns with the terminology used in Service Fulfillment.

- From NSP version 18.12 onward with NSD deployments, the system administrator must use the Supervision Manager to manage supervision views and groups for the Service Supervision application; see the Supervision Manager documentation.
- For standalone NFM-P deployments with the Service Supervision application, the system administrator should continue to manage supervision views and groups within the NFM-P client, under Supervision settings; see [4.3.2 “To create a supervision group in NFM-P” \(p. 65\)](#) and [4.3.3 “To create a view in NFM-P” \(p. 66\)](#)

### 4.2 Routine service maintenance with Service Supervision


#### 4.2.1 Purpose

This topic provides you with task flows to use the Service Supervision application to monitor the status of the services running in your network and to locate and troubleshoot problems.

## 4.2.2 Starting points for troubleshooting monitored services

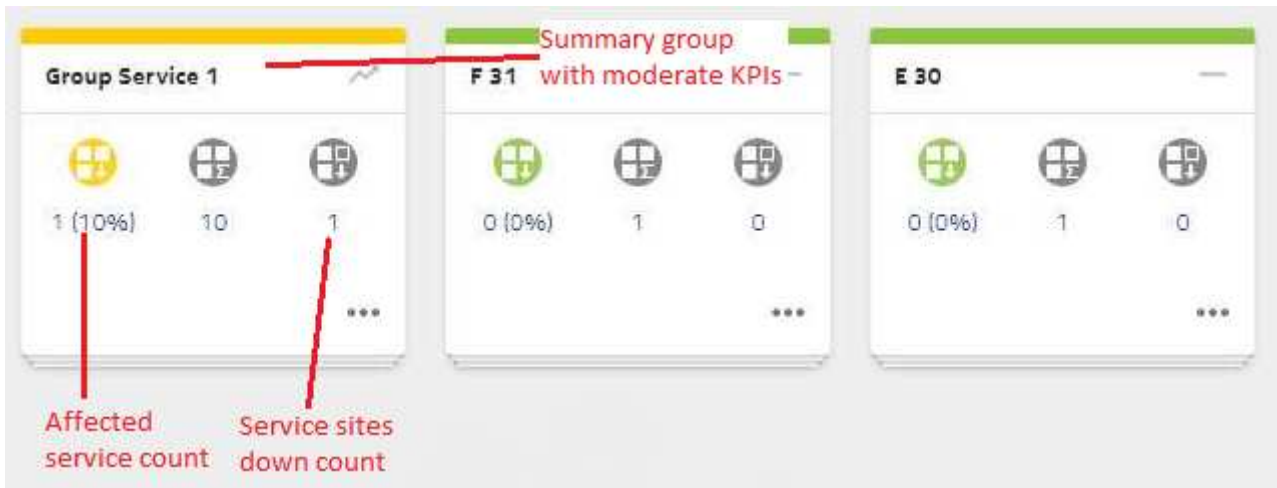
Changes to services manifest themselves through trending arrows on tiles and KPI icon color change on service objects.


Any of the following events could indicate that you need to troubleshoot your services:


- One or more KPI icons turn red on services in the Watch view.  
To add services to the Watch view, hover over a service item in the Service List and click More > Add To Watch Drawer.
- A trending arrow  appears on a tile or the tile changes color as services are impacted by new issues.
- A service item in the Service List shows problems with service objects: service site down, SAP down, SDP binding down, and/or OAM test validation failure.

## 4.2.3 Triaging steps for a group

- 1 \_\_\_\_\_  
Select an affected group tile in the view.
- 2 \_\_\_\_\_  
Determine the number of affected services and services with sites down for the group.



Click on the More Details button  to expand a group tile and view additional KPIs: services with SAPs down, SDP bindings down, or OAM test failures.

- 3 \_\_\_\_\_  
Double-click on the group to display its affected services in the Service List.  
From the Service List, you can open the Alarms list  to view alarms for the entire group.

4

Proceed to [4.2.4 “Triaging steps for services”](#) (p. 58).

END OF STEPS

## 4.2.4 Triaging steps for services

One or more KPI icons turn red on services in the Watch or the Service List.

1

Click on an affected service in the Watch view or double-click an affected service in the Service List.

The image shows two screenshots from a network management interface. The top screenshot is titled 'Watch View' and shows a table of services. The bottom screenshot is titled 'Service List' and shows a detailed view of the service 'VPLS 110'.

**Watch View Table:**

Service Name	KPI 1	KPI 2	KPI 3	KPI 4
EPIPE 4011	✓	✓	✓	✓
VPLS 110	✗	✓	✗	✓

**Service List View:**

Service Name	Service Manage...	State Ca...	KPI 1	KPI 2	KPI 3
VPLS 110	137	Site(s) D...	✗	✓	✗

Red annotations in the image point to the 'VPLS 110' row in both views. A red arrow points from the 'VPLS 110' row in the Watch View to the 'VPLS 110' row in the Service List. Another red arrow points from the 'VPLS 110' row in the Watch View to the 'Site, SAP, and SDP binding KPIs (Site and SDP bindings down)' text. A vertical red line is drawn between the two screenshots, indicating the transition from the Watch View to the Service List view.

Affected service in Watch view and Services List view

Site, SAP, and SDP binding KPIs (Site and SDP bindings down)

The affected service opens in the Service List as a list of service sites.

2


Determine which KPIs are affected (i.e. down ✗): service site down, SAP down, SDP binding down, and/or OAM test validation failure.

3

Open the Alarms list for the affected service; on the service item click More > Alarms. Use the Alarms List, Impacts diagram, and Event Timeline as described in [4.2.8 “Troubleshoot problems in the Alarms list”](#) (p. 62) and [4.2.9 “Troubleshoot problems in the Event Timeline”](#) (p. 62) to view events that might point to the problem.

- 
- 4 

---

 On the service item, click on the IGP Map icon  . On the IGP map, check the status of SDP bindings as described in [4.2.11 “Troubleshoot problems in the IGP Map”](#) (p. 64).
  - 5 

---

 To change the configuration of the service item in its management application, hover over a service item and click More > View Properties. Monitor the object in Service Supervision to determine if KPIs improve as a result of the change.
  - 6 

---

 After troubleshooting, verify that all alarms and KPIs have cleared and run OAM tests to prove that traffic can flow.

END OF STEPS 

---

#### 4.2.5 Triaging steps for a service site

For a selected service item in the Service List, the Service Site  KPI is Down.

- 1 

---

 Double-click on the service item to drill down to a list of all sites for the service.
- 2 


---

 Open the Alarms list for the affected service site; on the site item, click More > Alarms.
- 3 


---

 Use the Alarms List and Impacts diagram as described in [4.2.8 “Troubleshoot problems in the Alarms list”](#) (p. 62) to view events that might point to the problem.
- 4 

---

 On the service item, click on the Event Timeline icon  . Use the Event Timeline as described in [4.2.9 “Troubleshoot problems in the Event Timeline”](#) (p. 62) to view events that might point to the problem.
- 5 

---




 Select multiple affected service site item(s) and click on the OAM Test icon  . Perform OAM tests as described in [4.2.10 “Troubleshoot problems with OAM tests”](#) (p. 63) .

END OF STEPS 

---

#### 4.2.6 Triaging steps for a SAP




For a selected service item in the Service List, the SAP  KPI is Down.

- 
- 1 \_\_\_\_\_  
On the service item, click on the SAP icon to drill down to a list of SAPs on the service.
  - 2 \_\_\_\_\_  
On an affected SAP item, click on the Alarms icon  . Use the Alarms List and Impacts diagram as described in [4.2.8 “Troubleshoot problems in the Alarms list” \(p. 62\)](#) to view events that might point to the problem.
  - 3 \_\_\_\_\_  
On an affected SAP item, click on the Event Timeline icon  . Use the Event Timeline as described in [4.2.9 “Troubleshoot problems in the Event Timeline” \(p. 62\)](#) to view events that might point to the problem.
  - 4 \_\_\_\_\_  
Select multiple affected SAP item(s) and click on the OAM Test icon  . Perform OAM tests as described in [4.2.10 “Troubleshoot problems with OAM tests” \(p. 63\)](#) .

END OF STEPS \_\_\_\_\_

#### 4.2.7 Triaging steps for an SDP binding

For a selected service item in the Service List, the SDP Binding  KPI is Down.

- 
- 1 \_\_\_\_\_  
On the service item, click on the SDP Binding icon to drill down to a list of SDP bindings on the service.
  - 2 \_\_\_\_\_  
On an affected SDP binding item, click on the Alarms icon  . Use the Alarms List and Impacts diagram as described in [4.2.8 “Troubleshoot problems in the Alarms list” \(p. 62\)](#) to view events that might point to the problem.
  - 3 \_\_\_\_\_  
On an affected SDP binding item, click on the Event Timeline icon  . Use the Event Timeline as described in [4.2.9 “Troubleshoot problems in the Event Timeline” \(p. 62\)](#) to view events that might point to the problem.
  - 4 \_\_\_\_\_  
Select one or more affected SDP binding item(s) and click on the OAM Test icon  . Perform OAM tests as described in [4.2.10 “Troubleshoot problems with OAM tests” \(p. 63\)](#) .


END OF STEPS \_\_\_\_\_

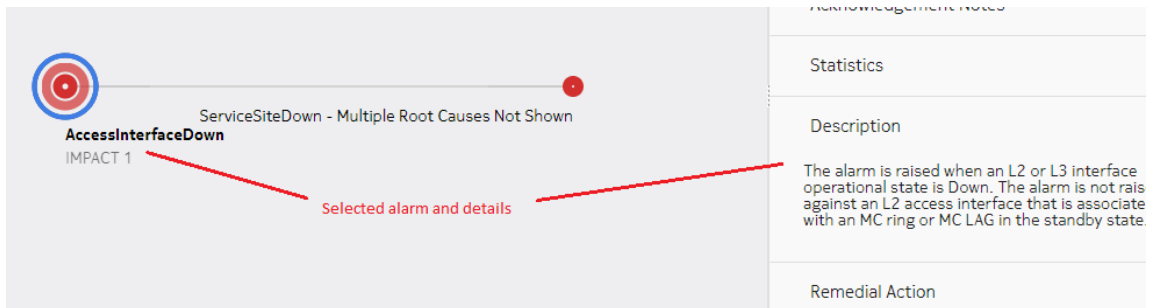
## 4.2.8 Troubleshoot problems in the Alarms list


Click on an alarm message in the list to display complete details of the alarm, including descriptive and remedial information.



If you suspect that the affected object for the selected alarm is a cause of the current problem, you can open the affected object in its management application directly from the Alarms list. On the selected alarm item, click More > Show Affected Object. Make configuration changes to the affected object while monitoring the object in Service Supervision to determine if KPIs improve as a result of the change.

From the Alarms list (in the context of the selected service) you can take the following actions:

- For an alarm item in the list, click Show Impacts  to determine the root cause of the alarm.
- The selected alarm object is circled in dark blue. Click on an alarm object to view details and remedial information.





If you suspect that the affected object for the selected alarm is a cause of the current problem, you can open the affected object in its management application from the Impact Analysis view. At the bottom of the Details panel, click Show Affected Object . Make configuration changes to the affected object while monitoring the object in Service Supervision to determine if KPIs improve as a result of the change.

- Open the Event Timeline  for the alarm.  
Set a date range  around the alarm event and view events that occurred prior to alarm being raised to determine a possible cause (for example, an object configuration change).

## 4.2.9 Troubleshoot problems in the Event Timeline

You can open the Event Timeline directly from a service object, or from individual alarm objects to view events that occurred prior to a hardware problem or an alarm being raised to determine a possible cause (for example, an object configuration change).

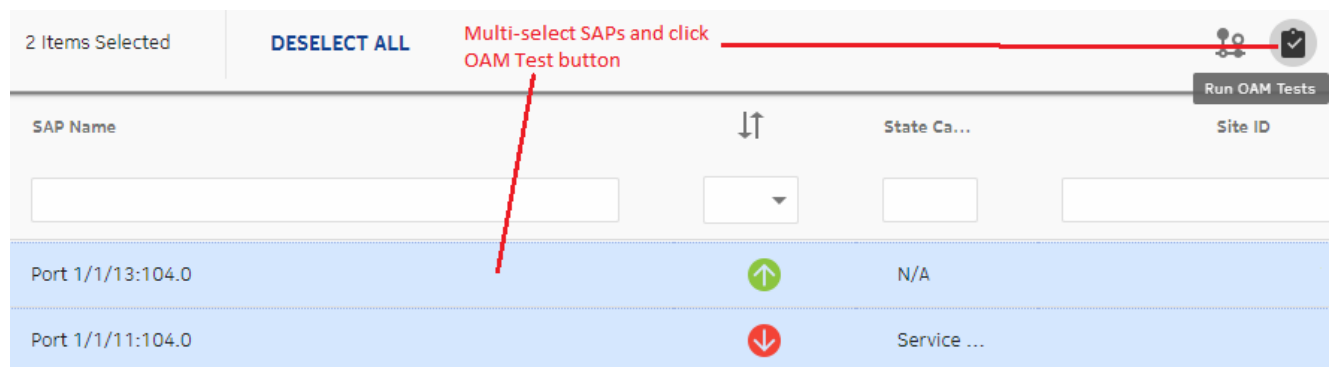
- Set an appropriate date range  around the hardware problem or alarm event.
- Select an event icon in the timeline and click Event Details  to view information related to the event. Use the Zoom function to expand clusters of events and search for causal events for a

failure.



#### 4.2.10 Troubleshoot problems with OAM tests

OAM diagnostic tests allow on-demand service performance monitoring and SLA verification to ensure that a service meets its performance settings in a controlled test time.



OAM tests can be run on a service by multi-selecting service sites, SAPs, or SDP bindings. A failed OAM test result generally indicates that the service or part of the service is not operational. Not all OAM test types apply to all service types.

Select a test type and click Run Test. The results are displayed in the Test Results Summary.

Status	Test Type	CFM Level	Executed	E:
Failed Result	CFM Loop Back	Level 7	2	

Test Type	CFM Level
CFM Loop Back	Level 7

**Test Execution Statistics**

0% (0) Succeeded

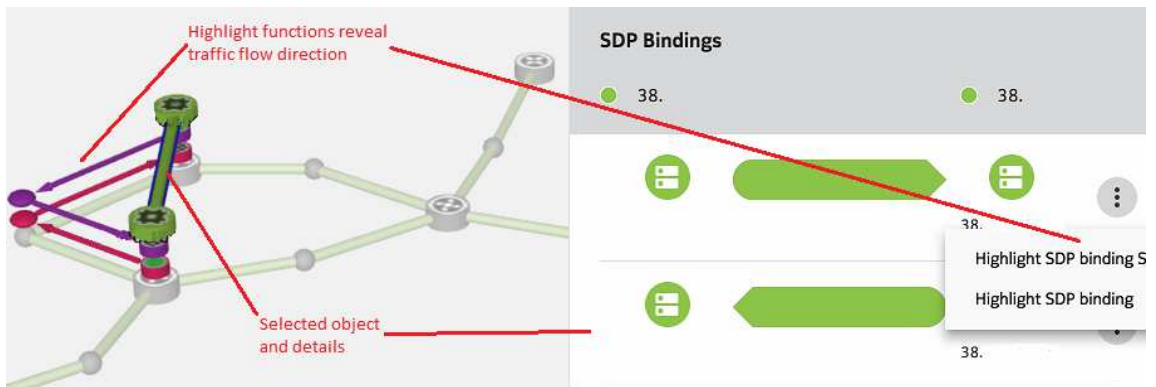
100% (2) Failed

### 4.2.11 Troubleshoot problems in the IGP Map

**Note:** CPAM configuration is required in the service management application in order for the IGP Map to display.

From the Service List, you can open a selected service in the IGP Map view. The IGP Map can be useful in identifying the service segment that is experiencing a failure.

- In the IGP Map, click on an SDP binding, IGP link, or Service site object and then click on the Info button to view details about the object.



- Set the Map Type parameter to Troubled SDPs to display only SDP bindings that are not working on the service.

---

## 4.3 Service Supervision general operations

### 4.3.1

This section describes specific application functions for which users may need additional information in order to maintain proper system operations. Where appropriate, recommendations are provided to assist in the resolution of functional issues.

### 4.3.2 To create a supervision group in NFM-P

Use this procedure to create a supervision group in deployments where NSP is running against NFM-P alone. To create a supervision group in mixed deployments where NSP is running against two or more management applications (such as NFM-P, NFM-T, MDM, or other), see the Supervision Manager documentation.

**i** **Note:** The Service Supervision application GUI includes a Create Automatically option for supervision group creation. In network deployments with a large number of services (more than 100,000), use of the Create Automatically option could take a long time to complete. Nokia recommends that automated supervision group creation operations are done during network maintenance periods, or immediately after an NSP upgrade. Nokia also recommends not to start a second automated supervision group creation operation until the current operation has completed.

- 1 \_\_\_\_\_  
Choose Administration→Supervision Settings from the NMF-P main menu. The Supervision Settings (Edit) form opens.
- 2 \_\_\_\_\_  
Configure the KPI History Interval (minutes) and KPI History Duration (hours) parameters.
- 3 \_\_\_\_\_  
Click on the Supervision Groups tab and click Create. The Supervision Group (Create) form opens.
- 4 \_\_\_\_\_  
Configure the parameters.  
The Category parameter distinguishes which monitored objects the Supervision Group manages, and to which application it applies in the view.  
For instance, when you set the Category parameter to service, you can create inclusion filters that apply only to service properties. You can add the supervision group to a view that has the Application parameter set to Service Supervision.
- 5 \_\_\_\_\_  
Configure the KPI History Interval (minutes) and KPI History Duration (hours) parameters.

---

**6** \_\_\_\_\_  
To apply an inclusion filter to the supervision group, click on the Inclusion Filters tab and click Add to select a filter.

**7** \_\_\_\_\_  
To create an inclusion filter, click on the Inclusion Filters tab and click Create, then Add. Configure the filter properties.

**8** \_\_\_\_\_  
To create an exclusion filter, click on the Exclusion Filters tab and click Create, then Add. Configure the filter properties.

**9** \_\_\_\_\_  
Search for the filter you created and add it to the supervision group.

**10** \_\_\_\_\_  
Save the changes and close the forms.

**END OF STEPS** \_\_\_\_\_

### **4.3.3 To create a view in NFM-P**

Use this procedure to create a view in deployments where NSP is running against NFM-P alone. To create a view in mixed deployments where NSP is running against two or more management applications (such as NFM-P, NFM-T, MDM, or other), see the Supervision Manager documentation.

**1** \_\_\_\_\_  
Choose Administration→Supervision Settings from the NMF-P main menu. The Supervision Settings (Edit) form opens.

**2** \_\_\_\_\_  
Configure the KPI History Interval (minutes) and KPI History Duration (hours) parameters, if required.

**3** \_\_\_\_\_  
Click the View tab and click Create or choose a view and click Properties. The View (Create|Edit) form opens.

**4** \_\_\_\_\_  
Configure the required general parameters.  
Configure the Application parameter to select the application to which to associate the view.

---

5 \_\_\_\_\_  
Click on the Supervision Groups tab.

6 \_\_\_\_\_  
Click Add to select the supervision group you created.

7 \_\_\_\_\_  
You can add user groups to restrict access to the view to only the users that belong to the selected user group or groups. Users with administrative privileges have access to all views. If no user group is assigned to a view, all users have access to the view. Click on the User Groups tab, and click Add to select one or more user groups.

8 \_\_\_\_\_  
Save the changes and close the forms.

END OF STEPS \_\_\_\_\_

#### 4.3.4 To enable the SAP Down state cause KPI

Because the monitoring of the operational state of all SAPs in NFM-P can affect performance, you must choose only the SAPs you want to monitor by performing this procedure in NFM-P.

1 \_\_\_\_\_  
Choose Manage→Service→Services from the NFM-P main menu. The Manage Services form opens.

2 \_\_\_\_\_  
Choose a service and click Properties. The *Service* (Edit) form opens.

3 \_\_\_\_\_  
Click on the Sites tab.

4 \_\_\_\_\_  
Choose the site on which you want to monitor the operational state of access interfaces and click Properties. The *Site* (Edit) form opens.

5 \_\_\_\_\_  
Enable the Monitor Access Interface Operational State parameter.

6 \_\_\_\_\_  
Save the changes and close the forms.

END OF STEPS \_\_\_\_\_

---

### 4.3.5 To purge assurance event records

Perform this procedure in NFM-P to purge assurance event records when the AssuranceEventLoggingTurnedOff alarm is raised. This alarm is raised when the database disk space used to log assurance events grows above the predefined threshold. Assurance Event logging is disabled to protect the database disk space.

- 1 \_\_\_\_\_  
Choose Tools→Event Policies from the NFM-P main menu. The Manage Event Policies form opens.
- 2 \_\_\_\_\_  
Choose the assurance.AssuranceEvent event type and click Properties. The Event Policy - assurance.AssuranceEvent (Edit) form opens.
- 3 \_\_\_\_\_  
Click the More Actions button and choose Purge Event Records. The Event Policy - assurance.AssuranceEvent (Edit) Filter form opens.
- 4 \_\_\_\_\_  
Click OK to purge all event records.
- 5 \_\_\_\_\_  
If necessary, configure the Event Retention Time (hours) to a value lower than the default value.
- 6 \_\_\_\_\_  
Save the changes and close the forms.

**END OF STEPS** \_\_\_\_\_

---

## 5 Analytics

### 5.1 Overview

#### 5.1.1 Introduction

The Analytics application provides insight into network infrastructure conditions, service utilization, subscriber traffic analysis, and quality of user experience using a variety of reports. Data is analyzed using business intelligence software and is presented in graphical or tabular reports.

#### 5.1.2 Analytics reports

Analytics reports enable a network operator to quickly determine the overall status of network functions and monitor trends. For example, you can identify the top subscribers in terms of overall network traffic, or based on application usage. The Analytics browser-based application allows a user to specify the reporting period, the objects on which to report, and the desired view. A report can be displayed in different formats such as a pie chart, trend diagram, or histogram.

You can [schedule](#) reports, or [save them](#) to be run again.

You can also export reports to files using the following formats:

- Excel (Paginated)
- Excel
- CSV
- DOCX
- RTF
- ODT
- ODS
- XLSX (Paginated)
- XLSX
- PPTX

#### 5.1.3 Server requirements

To accommodate the significant NFM-P Analytics data throughput, storage, and analysis requirements, an NFM-P system requires the following components:

- an NFM-P auxiliary database
- one or more NFM-P analytics servers that each host the business intelligence software and a web server
- one or more Flow Collectors, if IPFIX/Netflow based reports are required
- one or more NFM-P auxiliary servers, if required for additional statistics collection capacity

See the *NFM-P Planning Guide* for specific information about the NFM-P system requirements for Analytics, based on the managed network size, functional requirements, and deployment scope.

---

### 5.1.4 Browser requirements

If an adBlocker extension is in use, it may block some files in the Analytics application. To use the Analytics application with an adBlocker extension, add the NSP server and analytics server IP addresses to the whitelist.

### 5.1.5 Analytics configuration

An operator uses a GUI or OSS client to:

- enable or disable the collection of data
- specify the statistics classes for data aggregation
- specify how long to retain the raw and aggregated data

## 5.2 Workflow to configure NFM-P analytics

### 5.2.1

This workflow outlines the sequence of actions required to configure and manage NFM-P analytics.

- 1 \_\_\_\_\_  
Configure and enable the collection of the required statistics from NEs; see the *NFM-P Statistics Management Guide*.
- 2 \_\_\_\_\_  
Configure and enable the Flow Collector, if needed, and enable the required statistics; see the *NFM-P Statistics Management Guide*.
- 3 \_\_\_\_\_  
Configure one or more analytics rules to specify the statistics to collect; see [5.3 “To configure an NFM-P analytics rule” \(p. 71\)](#).
- 4 \_\_\_\_\_  
Configure one or more aggregation rules; see [5.4 “To configure analytics aggregation” \(p. 71\)](#).
- 5 \_\_\_\_\_  
Configure the time zone for the analytics session in the User Preferences menu. See [5.5 “To configure the Analytics application session time zone” \(p. 72\)](#).
- 6 \_\_\_\_\_  
Configure analytics server load balancing. See [5.6 “To configure analytics server load balancing” \(p. 73\)](#).

---

7 \_\_\_\_\_  
Configure report purging in the Application Preferences menu. See [5.7 “To configure application preferences”](#) (p. 74).

8 \_\_\_\_\_  
Configure scheduled reports as needed; see [5.10 “To schedule a report”](#) (p. 76).

END OF STEPS \_\_\_\_\_

## 5.3 To configure an NFM-P analytics rule

### 5.3.1

Perform this procedure to enable or disable raw data collection, and to specify data retention, for a statistics class to be processed using NFM-P analytics. Raw data collection is enabled by default for each statistics class.

1 \_\_\_\_\_  
Choose Tools→Analytics→AA Collection Manager from the NFM-P main menu. The AA Collection Manager form opens with a list of analytics rules displayed.

2 \_\_\_\_\_  
Select the required analytics rule and click Properties. The Analytics Rule (Edit) form opens.

3 \_\_\_\_\_  
Select the Collection Enabled parameter.

4 \_\_\_\_\_  
Configure the Raw Data Retention Time (days) parameter.

5 \_\_\_\_\_  
Close the AA Collection Manager form.

END OF STEPS \_\_\_\_\_

## 5.4 To configure analytics aggregation

### 5.4.1

Perform this procedure to configure the following for a statistics class to be processed using the Analytics application:

- level of data aggregation
- retention of the aggregation data

---

**i** **Note:** You can also configure the aggregation rule for a statistics class from the properties form of the analytics rule associated with the statistics class.

1 \_\_\_\_\_  
Choose Tools→Analytics→Aggregation Manager from the NFM-P main menu. The Aggregation Manager form opens.

2 \_\_\_\_\_  
Select an aggregation time zone if needed. The aggregation time zone is the time zone used to define daily, weekly, or monthly aggregations, that is, the definition of midnight.

3 \_\_\_\_\_  
On the Aggregation Rule tab, select the required aggregation rule and click Properties. The Aggregation Rule (Edit) form opens.

4 \_\_\_\_\_  
Select the Enable Aggregation parameter.

5 \_\_\_\_\_  
Configure the Aggregation Sync Time parameter.

6 \_\_\_\_\_  
Configure the Aggregation Levels parameter. As you select or deselect an option, other options may be automatically selected or deselected, as the aggregation logic requires.

7 \_\_\_\_\_  
Configure the parameters in the Aggregation Retention Configuration panel to specify how long the aggregation data is stored.

8 \_\_\_\_\_  
Click OK to save your changes and close the form.

9 \_\_\_\_\_  
Close the Aggregation Manager form.

END OF STEPS \_\_\_\_\_

## 5.5 To configure the Analytics application session time zone

### 5.5.1

Perform this procedure to configure the time zone for the analytics session. If no time zone is selected, the browser time zone will be used for report generation.

---

The session time zone defines the current time displayed in the Analytics application. The time zone used for aggregation, that is, the definition of when a day ends, is the aggregation time zone. The session time zone and the aggregation time zone should be the same. See [5.4 "To configure analytics aggregation" \(p. 71\)](#).

- 1 \_\_\_\_\_  
Open the help menu at the top right of the Analytics application main page.
- 2 \_\_\_\_\_  
Choose User Preferences. The default browser time zone is displayed.
- 3 \_\_\_\_\_  
Choose a time zone from the Select Time Zone of Current Analytics Browser Session menu.
- 4 \_\_\_\_\_  
Click Apply to save your changes and close the form.

END OF STEPS \_\_\_\_\_

## 5.6 To configure analytics server load balancing

### 5.6.1

Perform this procedure to manage load balancing if more than one analytics server is in use.

If load balancing is disabled, analytics server sessions are managed according to the order the analytics servers connected to the NSP server. Every user session in the Analytics application will connect to the first analytics server to connect to the NSP server. If the first server is down, application sessions will connect to the next server.

Load balancing can be configured with the following policies:

- round-robin: every user session request to the Analytics application is sent to the next analytics server in the list
- round-robin-with-stickiness: the round-robin system is used the first time a browser connects to the Analytics application. Browser cookies are used to bind the browser to the same analytics server for future sessions.

- 1 \_\_\_\_\_  
Open the help menu at the top right of the Analytics application main page.
- 2 \_\_\_\_\_  
Choose Analytics Server Load Balancing. The Analytics Server Load Balancing form opens.
- 3 \_\_\_\_\_  
Configure the Enable Load Balancing check box.

---

4 \_\_\_\_\_  
Select a load balancing policy.

5 \_\_\_\_\_  
Click Apply to save your changes and close the form.

END OF STEPS \_\_\_\_\_

## 5.7 To configure application preferences

### 5.7.1

Perform this procedure to configure analytics report purging. When the number of reports in the Results folder exceeds the configured number of reports to keep, the oldest reports exceeding the maximum number are permanently deleted. If you need to keep more than 5000 reports, Nokia recommends configuring your scheduled jobs to output to an FTP server; see [5.10 “To schedule a report” \(p. 76\)](#).

The purge is performed automatically every 24 hours or manually from the Application Preferences menu.

1 \_\_\_\_\_  
Open the help menu at the top right of the Analytics application main page.

2 \_\_\_\_\_  
Choose Application Preferences. The default number of reports to keep is displayed.

3 \_\_\_\_\_  
Enter the number of reports to keep.

4 \_\_\_\_\_  
To purge reports manually if needed, click Purge Results Now and click OK in the confirmation message.

5 \_\_\_\_\_  
Click Apply to save your changes and close the form.

END OF STEPS \_\_\_\_\_

## 5.8 To run a report

### 5.8.1

Before you can run a report, statistics collection and aggregation must be configured in the NFM-P. Report-specific prerequisites may apply; see the *NSP Analytics Report Catalog* for details.

---

If you want to save a report to a subfolder in the Results folder, the subfolder must be created before the report can be saved to it; see [5.9 “To manage saved reports” \(p. 75\)](#).

1 \_\_\_\_\_  
Click Repository from the Analytics application main page.

2 \_\_\_\_\_  
Select Reports and Dashboards→Application Assurance or Network and Service→*Report name*, where *Report name* is the report you need to run.

3 \_\_\_\_\_  
Configure the input parameters and click Apply.  
The report appears in the report pane.

4 \_\_\_\_\_  
To save the report:  
1. Select Save As at the top left of the report pane.  
2. In the Save As dialog, enter a name for the report version, and a description if required.  
3. In the list view at the bottom of the Save As dialog, navigate to the subfolder.  
4. Click Save.

5 \_\_\_\_\_  
To export the report, point to Export at the top left of the report pane and select a file type. A file is created.  
Depending on your browser settings, the file may download automatically.

END OF STEPS \_\_\_\_\_

## 5.9 To manage saved reports

### 5.9.1

You can save reports to the Results folder to make them available to run again with the same inputs. You can save different versions of the same report with different inputs, and organize them in subfolders as needed. Save reports directly to subfolders, or copy and paste them from the main Results folder into subfolders as needed.

Each report version is assigned a resource ID at the time of saving. The resource ID is based on the name that is entered in the Save As dialog when the report is saved. After the report is saved, the name field can be updated. This means that you can have two report versions with the same displayed name, because their resource IDs are unique in the folder.

**Example** If you want to save both a Port Throughput Summary and a SAP Throughput report for a set of inputs representing the Eastern region, you can save the reports as PTEast and STEast. This gives each report a unique resource ID. From the Results folder, edit the name of both report

---

versions to Eastern. This will make it easy to identify that both report versions have the same inputs.

1

---

From the Analytics application main page, select Repository→Results.

The list of reports with saved versions is displayed. Click the arrow beside a report to expand the list of versions.

2

To run a saved report version, you can either:

- Click on the report name to open the report inputs. At the top of the inputs panel, choose the report version to run.
- Click on the report version name.

3

To create a subfolder in the Results folder:

1. Right click on Results in the folder pane and choose Add Folder.
2. In the Add Folder dialog, enter a name for the folder and a description if needed.
3. Click Add.

END OF STEPS

---

## 5.10 To schedule a report

### 5.10.1

Perform this procedure to configure a schedule. You can schedule reports to run once or to repeat.

1

---

From the Repository pane or the Results folder, right-click on a report or report version and choose Schedule. The Scheduled Jobs page opens.

2

---

In the Scheduled Jobs page, click Create Schedule. The New Schedule page opens.

3

---

In the Schedule panel, configure the scheduled start of the job, and the recurrence.

4

---

Click Parameters to set the input parameters for the scheduled report.

If you are scheduling a saved report version, the input parameters will already be set.

---

**5** Click Output Options to set the report format, for example, PDF, and where it will be saved.

**6** Click Notifications to configure notification of job status, success, or failure, or for email copies of the report to be sent.

**7** Click Save to add your scheduled job to the Schedules page.

END OF STEPS

---

## 5.11 To manage scheduled reports

### 5.11.1

You can edit or delete scheduled report jobs that you created, that is, jobs for which your username appears in the owner column on the Schedules page.

To edit or delete tasks for which you are not the owner, you must log in to the Launchpad as the admin user.

If a scheduled job is deleted, it is immediately removed from the list and no further reports will be run according to the schedule. If you want a scheduled job to stop running but remain in the list for future use, you can disable it.

Deleting the scheduled job does not delete results of previously run reports from the Results folder.

Scheduled jobs that were upgraded from a release prior to 18.6 are owned by samuser. These tasks can only be managed by the admin user.

**1** Select Schedules from the Analytics application main page. The scheduled jobs are displayed, with the Edit and Delete icons at the right of the page.

**2** To disable a scheduled job, remove the check mark from the Enabled check box. The job will stop running but remain in the list.

**3** To delete a scheduled job, click the Delete icon. The scheduled job is removed from the list.

**4** To edit the scheduled job:

1. Click the Edit icon. The Scheduled Jobs page opens.
2. Configure the parameters you need to change.

---

3. Click Save.

END OF STEPS

---

## 5.12 To upload images for report branding

### 5.12.1

You can add logos to certain reports. Images can be saved to the analytics server or uploaded from the Analytics application. For the server procedure, see the NFM-P System Administrator guide.

Image files can be in any of the following formats:

- JPEG
- PNG
- JPG
- SVG
- GIF
- BMP

The images will be scaled to fit an 80 pixel square when they are shown in the report.

1

---

Log in to the Launchpad as the admin user.

2

---

From the Analytics application main page, right-click on the Images folder.

3

---

Select Add Resource→File→Image. The Add File page opens.

4

---

Click Choose File and navigate to the image file.

5

---

Configure the Name and Resource ID parameters.



**Note:** The user will be asked to specify the Resource ID when adding the image to a report.

6

---

Click Submit. The file is saved to the Images folder.

END OF STEPS

---

---

## 6 Link Utilization

### 6.1 Introduction to the Link Utilization application

#### 6.1.1 In this section:

[6.1.2 "Overview" \(p. 79\)](#)

[6.1.3 "Current and historical utilization" \(p. 79\)](#)

[6.1.4 "Statistics view" \(p. 80\)](#)

[6.1.5 "Weather Map view" \(p. 80\)](#)

[6.1.6 "Reference Speed" \(p. 80\)](#)

[6.1.7 "Sign out and links to other NSP applications" \(p. 81\)](#)

#### 6.1.2 Overview

The Link Utilization application provides graphical views of utilization for IP and MPLS interfaces within a specific administrative domain. The views allow you to assess how efficiently your network is managing traffic, and to identify interfaces (links) that are over- or under-utilized.

You can toggle between a Statistics view and a Weather Map view. The Statistics view shows utilization data in comparison charts and in a list of interfaces. The Weather Map view mimics CPAM L3 IGP topology to show utilization on IP and MPLS interfaces. You can click on items in the map to show detailed information.

In the Statistics view and the Weather Map view, you can switch among different administrative domains and configure the data retrieval time. For IP utilization in the Statistics view, you can also select a reference speed.

Statistics and other data are provided for the application using functions in the NFM-P. You must enable collection of the required performance statistics for the NEs or objects that participate in the application.

The NFM-P uses the performance statistics to derive a traffic rate for a given time period. That rate is then shown as a percentage of the capacity on the corresponding interface. The result is shown graphically and in the list of interfaces table.

#### 6.1.3 Current and historical utilization

The Link Utilization application allows you to view current or historical utilization. Current utilization is displayed by default, and shows the latest statistics for which a calculated percentage is available. The time period is based on the polling interval configured in the MIB Entry policy used for statistics collection.

Historical utilization is available when you select a date and time that is in the past, in the Set Data Retrieval Time dialog. The utilization shown in the application is an average for the hour that ends at the selected time.

---

The NFM-P delays historical utilization calculations by half an hour, to ensure that all statistics have been flushed to the database.

**Note:** For historical utilization, Nokia recommends that you select a time that is at least one hour in the past. If the selected time is too recent, statistics collection and calculations may not be complete. In such cases, NFM-P systems that deploy an auxiliary database may show no results, and systems with no auxiliary database may show current rather than historical utilization.

#### 6.1.4 Statistics view

The Statistics view shows utilization data in charts and in a list of interfaces.

The upper part of the display contains pie charts that show IP, MPLS, and Aggregated utilization statistics. Each colored segment of a pie chart corresponds to a utilization percentage range. A legend of Utilization Ranges identifies the percentage range associated with each color; for instance, red is for links operating at 81 to 100% of capacity. The relative sizes of the pie chart segments indicate the proportion of interfaces operating in each percentage range. That is, if a red segment makes up half of a chart, half of the interfaces in that admin domain are operating at 81 to 100% of their capacity.

The charts allow you to quickly assess how many interfaces in the admin domain are lightly utilized, moderately utilized, or heavily utilized. You can click on a utilization range within any chart to view a list of interfaces operating at that range. You can also click on the icon on the top-right corner of each pie chart to visualize the utilization data in the Weather map view.

The lower part of the display shows the list of interfaces that are participating in the utilization calculations, and is populated or refreshed when you click on a segment in a pie chart. You can expand an MPLS interface to view any LSPs that are contributing to the utilization. You can manage the display of information in the list by sorting and filtering, to view fine-grained results. You can also export interface information to a CSV file.

See [6.3.4 “To view and manage data in the Statistics view” \(p. 85\)](#).

#### 6.1.5 Weather Map view

The Weather Map view mimics CPAM L3 IGP topology to show utilization on IP or MPLS interfaces. Links are displayed between objects on the map. Colored arrows show the utilization in each direction, pointing toward a midline in the link that indicates full utilization. The color of the arrows, and how closely they approach the midline, indicate the level of utilization.

Panning and view controls allow you to move the map, change your viewing angle, or zoom in and out. You can click on an interface with utilization to view data for that interface, or click on a router icon to view data for that router.

See [6.3.5 “To view and manage data in the Weather Map view” \(p. 86\)](#).

#### 6.1.6 Reference Speed

Utilization is shown (in percent) as the statistical traffic rate over the reference speed. The reference speed is either the port speed or the interface speed. The reference speed is correlated with the capacity on the link.

For MPLS and Aggregated utilization, the reference speed is always Port Speed. Port Speed is the actual operational port speed.

---

For IP utilization in the Statistics view, you can choose either Port Speed or Interface Speed in the Reference Speed drop down. The interface speed may vary from the actual port speed, depending on configuration.

When Interface Speed is selected, the Statistics view shows only IP utilization. When Port Speed is selected, the Statistics view shows IP, MPLS, and Aggregated utilization.

Depending on the Reference Speed selected, either the Port Speed or the Interface Speed is displayed in the list of interfaces.

Interface Speed is not supported in the Weather Map view. The Weather Map uses only Port Speed.

### 6.1.7 Sign out and links to other NSP applications

You can sign out of the Link Utilization application, or quickly navigate to other NSP applications or the launchpad, by clicking on the navigation icon next to the User field in the top right of the display.

## 6.2 Preparing for Link Utilization (initial setup)

### 6.2.1 In this section:

[6.2.2 "Workflow to configure Link Utilization" \(p. 80\)](#)

[6.2.3 "To overwrite the default database partitioning size" \(p. 82\)](#)

[6.2.4 "To enable statistics collection for LDP-only links" \(p. 83\)](#)

### 6.2.2 Workflow to configure Link Utilization

For the Link Utilization application to function, preliminary steps are required to ensure that data is collected, stored, processed, and made available to the application. The following workflow describes these preliminary configurations.

1

---

If required, change the default partitioning in the NFM-P database. See [6.2.3 "To overwrite the default database partitioning size" \(p. 82\)](#).

2

---

Enable performance statistics collection for IP interfaces, MPLS interfaces, and LSPs by setting the Administrative State parameter of the MIB Entry policy to Up and setting the Polling Interval parameter to less than one hour:

- IP interfaces - for a MIB statistics policy, or for the IP Interface Stats (Routing Management: General) monitored statistics class on the Statistics tab of the Network Interface properties form, configure the policy for the MIB entry vRtrIfStatsEntry.
- MPLS interfaces - for a MIB statistics policy, or for the MPLS Interface Stats (Path/Routing Management: MPLS) monitored statistics class on the Statistics tab of the MPLS Interface properties form, configure the policy for the MIB entry vRtrMplsIfStatEntry.
- LSPs - for a MIB statistics policy, or for the MPLS LSP Egress Stats (Path/Routing

---

Management: MPLS) monitored statistics class on the Statistics tab of the Dynamic LSP properties form, configure the policy for the MIB entry vRtrMplsLspStatisticsEntry.

See “Performance statistics collection” in the *NFM-P Statistics Management Guide* for more information about how to configure performance statistics collection.

If your network contains links that use only LDP interfaces, not MPLS interfaces, see [6.2.4 “To enable statistics collection for LDP-only links”](#) (p. 83).

3

---

For LSP utilization, on the Accounting tab of the Dynamic LSP properties form for each LSP, assign an accounting policy and set the Administrative State to Up.

See “To configure a Dynamic LSP” in the *NFM-P User Guide* for more information.

4

---

For LSP utilization, create an LSP path monitor for each dynamic LSP.

See “To monitor a dynamic LSP” in the *CPAM User Guide* for more information.

5

---

Configure retention times for historical LSP utilization statistics.

A statistics event occurs each time an object is polled and statistics are collected. For LSP utilization statistics, an event policy defines the retention times for statistics in the NFM-P database. For longer retention times, ensure that the system has sufficient physical disk space.

See “To monitor a dynamic LSP” in the *CPAM User Guide* for more information.

END OF STEPS

---

### 6.2.3 To overwrite the default database partitioning size

The Link Utilization application provides database partitioning with the following default values:

CPAM\_STATS\_DEFAULT\_DB\_SIZE\_IN\_MBYTE = 20480

CPAM\_STATS\_MIN\_DB\_SIZE\_IN\_MBYTE = 500

CPAM\_STATS\_MAX\_DB\_SIZE\_IN\_MBYTE = 61440

Perform the following to overwrite the database partitioning size:

1

---

Log in to the main server station as the nsp user.

2

---

Navigate to the /opt/nsp/nfmp/server/nms/config directory.

3

---

Create a backup copy of the nms-server.xml file.

---

4



## NOTICE

### Service-disruption hazard

Contact your Nokia technical support representative before you attempt to modify the `nms-server.xml` file. Modifying the `nms-server.xml` file can have serious consequences that can include service disruption.

Open the `nms-server.xml` file using a plain-text editor.

---

5

To overwrite the default size, add the following lines to the `nms-sever.xml` file.

```
<cpamUtilizationStats  
cpamStatisticDbSizeInMBytes = "<size_in_bytes>"/>
```

For example:

```
<cpamUtilizationStats  
cpamStatisticDbSizeInMBytes = "1024"/>
```

---

6

Save and close the `nms-server.xml` file.

---

7

Open a console window.

---

8

Navigate to the `/opt/nsp/nfmp/server/nms/bin` directory.

---

9

Enter the following at the prompt:

```
bash$ ./nmserver.bash read_config
```

The main server reads the `nms-server.xml` file.

---

10

Log out of the main server and close the open console windows.

---

END OF STEPS

## 6.2.4 To enable statistics collection for LDP-only links

In Nokia MPLS networks, you can create LDP interfaces or MPLS interfaces on routing instances. LDP interfaces use only LDP signaling. MPLS interfaces use RSVP signaling.

---

Statistics for MPLS link utilization are collected only from MPLS interfaces. LDP interfaces do not provide statistics for link utilization. To collect statistics for links that use only LDP interfaces, you must create a corresponding MPLS interface for each LDP interface, using the same interface ID.

If you do not want to enable RSVP signaling on the corresponding MPLS interfaces, leave them administratively down. The MPLS statistics will still be collected and used in link utilization calculations for the LDP-only links.

## 6.3 Viewing and managing utilization information

### 6.3.1 In this section:

[6.3.2 “Before you begin” \(p. 83\)](#)

[6.3.3 “To configure the Admin Domain, Data Retrieval Time, and Reference Speed” \(p. 83\)](#)

[6.3.4 “To view and manage data in the Statistics view” \(p. 85\).](#)

[6.3.5 “To view and manage data in the Weather Map view” \(p. 86\).](#)

[6.3.6 “Troubleshooting to confirm statistics collection” \(p. 87\).](#)

### 6.3.2 Before you begin

For the Link Utilization application to provide information, preliminary configurations and settings must be completed. See [6.2 “Preparing for Link Utilization \(initial setup\)” \(p. 81\)](#).

If the display shows no utilization, see [6.3.6 “Troubleshooting to confirm statistics collection” \(p. 87\)](#).

### 6.3.3 To configure the Admin Domain, Data Retrieval Time, and Reference Speed

For the Statistics view and the Weather Map view, you can specify the admin domain and the data retrieval time for utilization statistics. For IP utilization in the Statistics view, you can also choose the reference speed.

Perform the following procedure to select the admin domain, data retrieval time, and reference speed parameters for the utilization display.

1

---

To select the administrative domain, click on the Admin Domain drop-down in the menu bar. The available options correspond to the IGP administrative domains configured in the network.

2

---

To select the data retrieval time, perform the following:

1. Click on the Data Retrieval Time in the menu bar. The Set Data Retrieval Time dialog opens.
2. Click on the calendar icon to show the date chooser, then select a date. Click Today to display data for the current day.
3. Enter a time, or use the arrows to scroll and select a time.
4. To display the current utilization, select Latest.

---

5. Click Update.

See [6.1.3 “Current and historical utilization” \(p. 79\)](#) for more information.

3

---

To select the reference speed, click on the Reference Speed drop-down in the menu bar, and select a reference speed.

See [6.1.6 “Reference Speed” \(p. 80\)](#) for more information.

END OF STEPS

---

### 6.3.4 To view and manage data in the Statistics view

The Statistics view shows utilization data in charts and in a list of interfaces. For an overview of the Statistics view functionality, see [6.1.4 “Statistics view” \(p. 80\)](#).

1

---

Click on Statistics in the view selector bar. The Statistics view is displayed, showing utilization pie charts for IP, MPLS, and Aggregated utilization.

The charts allow you to quickly assess how many interfaces of each type are lightly utilized, moderately utilized, or heavily utilized. The Utilization Ranges legend identifies the percentage of utilization associated with each color.

2

---

Click on a colored segment within any chart to view a list of interfaces operating at the utilization percentage range for that color. A list of interfaces with utilization rates in the selected range is displayed in the list of interfaces.

Alternatively, you can display the data in the Weather Map view by clicking on the icon in the top-right corner of the chart.

3

---

To maximize the size of the list of interfaces, click on the maximize icon in the upper right of the list.

4

---

For MPLS utilization, you can expand an interface to view the LSPs that are contributing to the utilization.

5

---

To remove or restore columns, right-click on a column header and choose Columns.

6

---

To filter the list, perform the following:

1. To filter any column, enter text into the field below the column header. The filter shows results that contain the entered text.

2. To filter by timestamp, click on the calendar icon in the Time of Computation column, then configure a range for the date and time. The filter shows results from within the configured range.
3. Click on the filter icon to clear any filters that have been applied.

---

7

To sort columns, perform the following:

1. To rearrange the order of columns, click and drag on the column headers.
2. To configure the sorting priority for columns, right-click on a column header and choose Configure Sort. The Sort dialog opens.

In the Sort dialog, you can create a list of priority levels for sorting columns, or edit the priority levels at any time. When multiple levels are configured, the priority levels are displayed numerically in the column headers. For columns assigned with a priority level, you can configure ascending or descending order.

3. To quickly sort by ascending or descending order for any column, click on the column header. Alternatively, you can right-click on a column header and choose Sort Ascending or Sort Descending.

**Note:** Changing the ascending or descending order in a column using these methods establishes the column as the first-level priority for sorting, and removes any priority levels configured in the Sort dialog.

---

8

To adjust the width of columns, click and drag the lines between columns.

Alternatively, right-click on a column header and choose Auto Fit to make the column wide enough to display all text in the longest entry in that column. Choose Auto Fit All Columns to make all columns wide enough to display all text.

---

9

To export interface information in the list to a CSV file, click on the Export icon.

You can choose to export visible rows, selected rows, or all rows. Click on the drop-down arrow beside the Export icon and select an option.

---

10

To change the type of statistics shown in the list of interfaces, click on the drop-down at the top-left of the list, then select a Utilization Range from the colored buttons.

Alternatively, you can click on another segment in the pie charts.

---

END OF STEPS

### 6.3.5 To view and manage data in the Weather Map view

The Weather Map view mimics CPAM L3 IGP topology to show utilization on IP and MPLS interfaces. For an overview of the Weather Map view functionality, see [6.1.5 “Weather Map view” \(p. 80\)](#).

- 
- 1 

---

Click on Weather Map in the view selector bar. The Weather Map view is displayed.

The NE icons and the colored links between them allow you to quickly assess NEs and interfaces that are lightly utilized, moderately utilized, or heavily utilized. Colors correspond to the percent utilization ranges shown in the Statistics view.
  - 2 

---

Choose the type of Weather Map to display. On the left side of the menu bar, click on the drop-down arrow for the Weather Map type and choose a statistics type from the menu.
  - 3 

---

Use the zoom, view, and panning controls in the upper left to move the map, change your viewing angle, or zoom in and out.

Click on the View Options drop-down to show or hide the panning controls.

You can click and drag icons to change the shape of the map, or click and drag empty space to pan on the map.
  - 4 

---

Click on a colored arrow to view detailed information about that interface. Use CTRL-click to view details for multiple interfaces at one time.
  - 5 

---

Click on a router icon to view detailed information about that router. Use CTRL-click to view details for multiple routers at one time.
  - 6 

---

Double-click on a group to view its components. Double-click on a blank area of the map to back out.

END OF STEPS

---

### 6.3.6 Troubleshooting to confirm statistics collection

For IP and MPLS utilization, a very low utilization rate may show as 0%. In such a case, to confirm that the application is functioning properly, you can view the list of interfaces table in the lower part of the Statistics view. If the table contains results and shows a Time of Computation, interfaces are appropriately managed for statistics collection.

To confirm values for very low utilization rates, open the properties form for the IP or MPLS interface in the NFM-P GUI, and view the Statistics tab.



---

## 7 Subscriber Manager

### 7.1 Overview




#### 7.1.1






The Subscriber Manager KPI Monitor view displays KPI and statistics information for NEs within a specified supervision group. Each NE object in the view can be expanded to display detailed KPI and alarm information for individual NEs. The Troubleshoot view displays session-related information for subscriber hosts and user equipment (UE) devices connected to an access point (AP).

In order for the Subscriber Manager to display information, statistics collection must be configured in the NFM-P; see [7.4.2 “Statistics polling” \(p. 95\)](#). The Subscriber Manager supports automatic statistics configuration on the 7750 SR release 10.0 and later, and the 7750 MG release 5.0 and later.

### 7.2 KPI Monitor view

#### 7.2.1

The default KPI monitor view format is the Top NE Matrix, which displays the top NEs in a supervision group as tile objects in a matrix, sorted by KPI level. The NE tiles display system ID information and KPI values for Critical Alarm Count , CPU Usage , and Memory Usage . The banner color of each NE tile indicates the NE's KPI value range, as specified by the KPI type specified in the Sort menu.

- **Sort the view:** Click on the Sort menu  CPU Usage  and select the KPI by which you want to sort the view. The view is re-ordered according to the selected KPI.
- **Change the view format:** Click on the List button  to change the view to a list format, with all NEs in the supervision group.
- **Search for an NE or supervision group:** Click on the Search button . In the Search menu, select a search parameter from the drop-down list and then begin typing a search string in the text field. The result list updates as you type.
- **Change application settings:** Click More  > Settings. Configure the Red/Yellow/Green colour change thresholds for KPI indicators, the KPI refresh interval, and the maximum number of NEs to appear in the application window.  
**Note:** Changing the refresh interval may impact server performance. A higher refresh interval results in more frequent server calls.
- **Sort the list under a heading:** When viewing NEs as a list, click on one of the column headings to sort the list under that heading. Click the heading again to reverse the sort order, as indicated by Up/Down arrows.
- **Filter the list contents:** When viewing NEs as a list, type a text string in the field under a column heading to reduce the list to include only entries that contain the filter string, under that heading. The filter results update as you type.

### Expanded NE/site information

View additional NE/site information through the following actions:

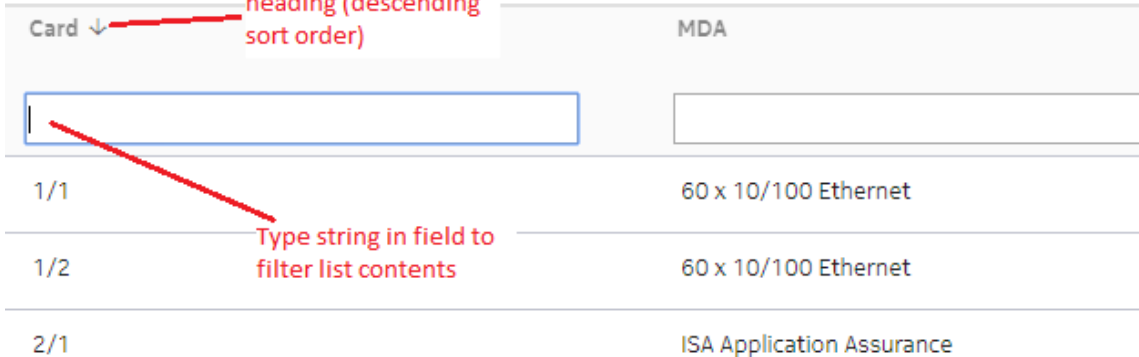
- View equipment installed on the NE: in the matrix, hover over an NE object and click More > Site Details; see 7.2.2 “Equipment list” (p. 89).
- View DHCP servers configured on the site: in the matrix, hover over an NE object and click More > Local DHCP Servers; see 7.2.3 “Local DHCP Server list” (p. 91).
- View KPI plots for the site: in the matrix, hover over an NE object and click More > Site Plotter; see 7.2.4 “Statistics” (p. 91).
- View expanded site information: in the matrix, hover over an NE object and click More > Site Info; see 7.2.5 “Site Info” (p. 93).

## 7.2.2 Equipment list






The equipment list displays all cards and MDAs configured on the selected NE, along with relevant subscriber statistics for each item.

- **Sort the list under a heading:** Click on one of the column headings to sort the list under that heading. Click the heading again to reverse the sort order, as indicated by Up/Down arrows.
- **Filter the list contents:** Type a text string in the field under a column heading to reduce the list to include only entries that contain the filter string, under that heading. The filter results update as you type.

(sim212)







Card ↓	MDA
1/1	60 x 10/100 Ethernet
1/2	60 x 10/100 Ethernet
2/1	ISA Application Assurance

- **Search for an NE or supervision group:** Click on the Search button . In the Search menu, select a search parameter from the drop-down list and then begin typing a search string in the text field. The result list updates as you type.
- **View other NE information:** Click on the buttons in the upper right-hand corner of the GUI     to change to the Local DHCP Server list, Statistics, or Site Info view.

---

### 7.2.3 Local DHCP Server list

The Local DHCP Server list displays all DHCP servers and routing instances configured on the selected NE, along with relevant statistics for each server.

- **Sort the list under a heading:** Click on one of the column headings to sort the list under that heading. Click the heading again to reverse the sort order, as indicated by Up/Down arrows.
- **Filter the list contents:** Type a text string in the field under a column heading to reduce the list to include only entries that contain the filter string, under that heading. The filter results update as you type.
- **Search for an NE or supervision group:** Click on the Search button . In the Search menu, select a search parameter from the drop-down list and then begin typing a search string in the text field. The result list updates as you type.
- **View other NE information:** Click on the buttons in the upper right-hand corner of the GUI    to change to the Equipment list, Statistics, or Site Info view.





### 7.2.4 Statistics

The Statistics view displays a series of graphical plots of individual KPIs, covering a pre-configured time period. The plots are minimized in a matrix format by default, but you can enlarge them individually for closer inspection.

- **Enlarge a statistic plot:** Click on a statistic plot in the matrix. The plot is maximized for closer examination.  
In cases where there are multiple plots for a single KPI, the plots are displayed in different colors. You can display or hide individual plots by clicking them at the bottom of the enlarged plot view. Hover the mouse pointer over the plot to display KPI values at a specific point on the plot. You can zoom in and out on a plot by turning the mouse wheel while hovering over a specific

location. Click the Close button  outside the enlarged plot view to return to the tile view.



- **Change plotter time period:** Click on the Calendar button  to select the date before which statistics are displayed. After selecting a date, click the Refresh button. The resulting plots display KPIs over the two days prior to the selected date.
- **View other NE information:** Click on the buttons in the upper right-hand corner of the GUI    to change to the Local DHCP Server list, Equipment list, or Site Info view.

### Configuring statistics collection






In order for the statistics plots to display adequate amounts of information, you may need to configure the retention period for the following NE MIB entries in the NFM-P:

- **Shelf Level:** Equipment Temperature (Physical Equipment), Memory Statistics (Physical Equipment), CPU Statistics (Physical Equipment), Subscriber Host Equipment System Statistics (Physical Equipment), Memory Utilization Statistics (Physical Equipment)
- **Card Level:** CPU Utilization Statistics (Physical Equipment), Subscriber Host Equipment Slot Statistics (Physical Equipment)
- **MDA Level:** Subscriber Host Equipment MDA Statistics (Physical Equipment)  
See the NSP NFM-P Statistics Management Guide for more information.

---

## 7.2.5 Site Info

The Site Info page provides an expanded layout of subscriber statistics, KPI readings, alarm counts, and NE system information.

- **Search for an NE or supervision group:** Click on the Search button . In the Search menu, select a search parameter from the drop-down list and then begin typing a search string in the text field. The result list updates as you type.
- **View other NE information:** Click on the buttons in the upper right-hand corner of the GUI     to change to the Local DHCP Server list, Equipment list, or Statistics view.

## 7.3 Troubleshoot view


### 7.3.1

The Troubleshoot view displays subscriber and host information for a selected subscriber or AP. You can view statistics and other information for hosts, and run ICMP Ping and Trace tests.

Upon opening the Troubleshoot view, you must search for a subscriber or AP to display its information:

- [7.3.2 “To search for a subscriber” \(p. 92\)](#)
- [7.3.3 “To search for an AP” \(p. 94\)](#)
- [7.3.4 “To perform an advanced object search” \(p. 94\)](#)

### 7.3.2 To search for a subscriber

1 \_\_\_\_\_  
In the Troubleshoot view, select Subscribers from the Search menu   .

2 \_\_\_\_\_  
Click on the link next to the Search menu. A list of all subscribers in the supervision group is returned.


3 \_\_\_\_\_  
To filter the search results, select Subscriber ID or Site ID in the menu and type a filter string in the field. The results list is reduced to include only objects with the specified string.

4 \_\_\_\_\_  
Click on an item in the search results to open it in the Troubleshoot view.

**END OF STEPS** \_\_\_\_\_

---

### 7.3.3 To search for an AP

- 1 \_\_\_\_\_  
In the Troubleshoot view, select AP IP Address from the Search menu  .
- 2 \_\_\_\_\_  
Click on the link next to the Search menu. A list of all APs in the supervision group is returned.
- 3 \_\_\_\_\_  
To filter the search results, select one of the options in the menu and type a filter string in the field. The results list is reduced to include only objects with the specified string.
- 4 \_\_\_\_\_  
Click on an item in the search results to open it in the Troubleshoot view.

END OF STEPS \_\_\_\_\_

### 7.3.4 To perform an advanced object search

The Advanced Search function allows you to search for objects using a wider variety of search criteria.




- 1 \_\_\_\_\_  
In the Troubleshoot view, click on the Subscriber Search, AP IP Search, or WLAN GW Tunnel Search button. An advanced search form opens.
- 2 \_\_\_\_\_  
Depending on the type of object you are searching, the advanced search form presents you with a variety of possible search criteria associated with the object type. Type a search string in one or more of the fields.
- 3 \_\_\_\_\_  
Click on the Search button. A list of search results is returned.
- 4 \_\_\_\_\_  
Click on an item in the search results to open it in the Troubleshoot view.

END OF STEPS \_\_\_\_\_

### 7.3.5 Hosts list




The Hosts list displays all subscriber hosts with a selected subscriber, or the subscribers associated with a selected AP.

- **Sort the list under a heading:** Click on one of the column headings to sort the list under that heading. Click the heading again to reverse the sort order, as indicated by Up/Down arrows.

- **Filter the list contents:** Type a text string in the field under a column heading to reduce the list to include only entries that contain the filter string, under that heading. The filter results update as you type.
- **View other host information:** Click on the buttons in the upper right-hand corner of the GUI    to change to the Statistics list or ICMP Ping/Trace tests.



### 7.3.6 Statistics list

The Statistics list displays operational statistics for a selected subscriber host.

- **Sort the list under a heading:** Click on one of the column headings to sort the list under that heading. Click the heading again to reverse the sort order, as indicated by Up/Down arrows.
- **Filter the list contents:** Type a text string in the field under a column heading to reduce the list to include only entries that contain the filter string, under that heading. The filter results update as you type.
- **View other host information:** Click on the buttons in the upper right-hand corner of the GUI    to change to the Hosts list or ICMP Ping/Trace tests.

### 7.3.7 To run an ICMP Ping or Trace test on a host

1


In the Hosts list, hover over the host item you want to test and click on the ICMP Ping button  or ICMP Trace button  at the end of the row.

2

Configure the test parameters on the Parameters panel  as required.

3

Click on the Run button.

The test result appears in the left-hand side of the GUI. Click on an element to view its information on the Details panel .

END OF STEPS

## 7.4 Subscriber Manager general operations

### 7.4.1

This section describes specific application functions for which users may need additional information in order to maintain proper system operations. Where appropriate, recommendations are provided to assist in the resolution of functional issues.

### 7.4.2 Statistics polling

Statistics polling is only enabled for MIB entry policies applicable to NE types and versions, managed for default and non-default NE MIB statistics policies. The Subscriber Management application scans for newly-managed NEs, and enables applicable MIB entry policies every 30

seconds. Statistics polling is not disabled when an NE is un-managed.

NFM-P users may change the administrative state and polling interval of MIB entry policies through the Java GUI or OSSI. This means that polling may be disabled for a policy, or its polling interval changed after it is enabled by the Subscriber Management application. If an NE is un-managed and re-managed, polling is enabled on all applicable policies and the polling interval set to 15 minutes.

If you are working with NE versions that are older than the versions listed above, you must configure statistics collection manually in the NFM-P, as described in "Statistics collection configuration" in the NFM-P Statistics Management Guide.

Enable collection for the following MIB entries:

<b>KPI Monitor perspective</b>	<b>Troubleshoot perspective</b>
sgiCpuUsage	SLAProfInstStatsEntry
sgiMemoryUsed	SLAProfInstEgrPStatsEntry
tmnxSubMgmtMdaStatsEntry	SLAProfInstEgrQStatsEntry
tmnxSubMgmtSystStatsEntry	SLAProfInstIngPStatsEntry
tmnxWlanGwlsaMemberEntry	SLAProfInstIngQStatsEntry
wlanGwStatsGroup	SubIngPStatsEntry
tmnxDhcpServerStatsEntry	SubscriberIngQStatsEntry
tmnxDhcpSvrPoolStatsEntry	SubscriberEgrQStatsEntry
tmnxDhcpServerStats6Entry	SubEgrOverrideCounterEntry
tmnxDhcpsPoolStats6Entry	

---

## 8 Telemetry

### 8.1 About

#### 8.1.1 Description

The NSP Telemetry application uses gRPC telemetry data from NEs to provide a near-real-time graphical dashboard of NE KPIs.

The application supports the monitoring of NEs discovered using the following:

- SNMP
- MDM

**i** **Note:** Telemetry reporting is sensitive to NE and NSP clock synchronization. To ensure that the Telemetry data from multiple NEs is assigned to the correct reporting period, it is strongly recommended that you engage NTP or a similar mechanism to maintain synchrony between the NE and NSP system clocks.

#### 8.1.2 Getting started

To enable Telemetry reporting for one or more NEs, you must do the following:

- Enable TLS between each NE and the NSP.
- Enable gRPC access on a designated NE user account.
- Add each NE to the NSP configuration.

See [8.2 “To enable telemetry reporting for a managed NE” \(p. 97\)](#) for configuration information.

#### Troubleshooting

In the event that an NE fails to forward Telemetry data to the NSP, see [8.3 “Telemetry troubleshooting” \(p. 103\)](#) for information about determining the cause.

## 8.2 To enable telemetry reporting for a managed NE

### 8.2.1 Description

The following steps describe how to enable the collection of gRPC telemetry data from one or more NEs by the NSP. The data is used as statistical input for reporting by the NSP Telemetry application.

The telemetry data from an NE is forwarded over a channel secured using TLS. Establishing the channel requires the distribution of security artifacts to the NE, as described in the procedure steps. For information about configuring and managing TLS on an NE, see the *NE System Management Guide*.

---

## Prepare security artifacts

1

Obtain the required TLS artifacts. You can use a publicly available utility such as OpenSSL to generate and manage the artifacts, which are the following:

- public certificate
- private server certificate

**i** **Note:** As a certificate renewal reminder, it is important to record the expiry date of each certificate.

1. Generate an RSA encryption key for the public certificate.
2. Create a Certificate Signing Request, or CSR, for the public certificate.
3. Have the CSR signed by a CA.
4. Generate an RSA encryption key for the private server certificate.
5. Create a Certificate Signing Request, or CSR, for the private server certificate.
6. Have the CSR signed by a CA.

**i** **Note:** The Subject Alternative Name, or SAN, of the private server certificate, must include the management IP address of each NE that is to establish a gRPC session using the certificate.

## Add certificate to each NSP truststore

2

Log in to the appropriate station as the nsp user.

- if the NSP system includes the NSD and NRC—standalone or primary NSP server
- if the NSP system includes only the NFM-P—standalone or primary NFM-P main server

3

Open a console window.

4

Copy the `/opt/nsp/os/ssl/nsp.truststore` file to a secure location, and record the location for use later in the procedure.

5

Enter the following:

```
bash$ keytool -import -alias alias -keystore truststore_location -file certificate_file ↵
```

where

*alias* is the certificate alias

*truststore\_location* is the absolute path of the secure truststore location recorded in [Step 4](#)

---

*certificate\_file* is the absolute path of the file that contains the certificate to import



**Note:** The certificate must be used to sign the server certificates.

You are prompted to trust the certificate that you are importing.

6

---

Enter **yes** ↵.

The certificate is imported to the truststore.

7

---

If you are configuring an NFM-P main server, perform the following steps.

1. Enter the following:

```
bash$ cp /opt/nsp/os/ssl/nsp.truststore /opt/nsp/os/tls ↵
```

2. Enter the following:

```
bash$ cd /opt/nsp/nfmp/server/nms/bin ↵
```

3. Enter the following to stop the main server:

```
bash$ ./nmserver.bash stop ↵
```

4. Enter the following to switch to the root user:

```
bash$ su ↵
```

5. Enter the following to open the samconfig utility:

```
# samconfig -m main ↵
```

The following is displayed:

```
Start processing command line inputs...
```

```
<main>
```

6. Enter the following:

```
<main> configure tls truststore-file truststore_location ↵
```

where *truststore\_location* is the absolute path of the secure truststore location recorded in [Step 4](#)

The prompt changes to `<main configure>`.

7. Enter the following:

```
<main configure> back ↵
```

The prompt changes to `<main>`.

8. Enter the following:

```
<main> apply ↵
```

The configuration is applied.

9. Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

---

10. Enter the following to switch back to the nsp user:

```
# exit ↵
```

11. Enter the following to start the main server:

```
bash$ ./nmserver.bash start ↵
```

8

---

Close the console window.

9

---

If the NSP system is redundant, perform [Step 2](#) to [Step 8](#) on the standby NSP server or NFM-P main server station.

## Enable security on NE

10

---

Log in to the NE as the admin user.

11

---

Transfer the certificate files from the NSP server or NFM-P main server station to a compact flash drive on the NE, for example, cf3:.

12

---

Enter the following to import the public certificate to a file:

```
/admin certificate import type cert input drive/CA_cert_file output  
public_cert_file format pem ↵
```

where

*drive* is a compact flash drive, for example, cf3:

*CA\_cert\_file* is the name of the transferred public certificate file

*public\_cert\_file* is the public certificate file to create on the NE

13

---

Enter the following to import the private server certificate to a file:

```
/admin certificate import type key input drive/server_cert_file output  
private_cert_file format pem ↵
```

where

*drive* is a compact flash drive, for example, cf3:

*server\_cert\_file* is the name of the transferred private server certificate file

*private\_cert\_file* is the private server certificate file to create on the NE

14

---

Create a TLS cipher list.

1. Enter the following:

```
/configure system security tls server-cipher-list gRPC_cipher_list  
create ↵
```

where *gRPC\_cipher\_list* is a name to assign to the TLS cipher list for gRPC

2. Enter the following for each cipher:

```
cipher n name cipher_name ↵
```

where

*n* is the cipher priority

*cipher\_name* is the name of a cipher; see the latest device documentation for the currently available ciphers

For example:

```
cipher 1 name tls-rsa-with-null-md5  
cipher 2 name tls-rsa-with-null-sha  
cipher 3 name tls-rsa-with-null-sha256  
cipher 4 name tls-rsa-with3des-edc-cbc-sha  
cipher 5 name tls-rsa-with-aes128-cbc-sha  
cipher 6 name tls-rsa-with-aes256-cbc-sha  
cipher 7 name tls-rsa-with-aes128-cbc-sha256  
cipher 8 name tls-rsa-with-aes256-cbc-sha256
```

---

## 15

Create a TLS certificate profile.

1. Enter the following:

```
/configure system security tls cert-profile gRPC_cert_profile  
create ↵
```

where *gRPC\_cert\_profile* is a name to assign to the TLS certificate profile for gRPC

2. Enter the following, in sequence:

```
entry 1 create ↵  
cert "public_cert_file" ↵  
key "private_cert_file" ↵  
exit ↵
```

```
no shutdown ↵
```

where

*public\_cert\_file* is the file created in [Step 12](#)

*private\_cert\_file* is the file created in [Step 13](#)

---

## 16

Create a TLS server profile.

1. Enter the following:  

```
/configure system security tls server-tls-profile gRPC_server_profile create ↵
```

where *gRPC\_server\_profile* is a name to assign to the TLS server profile for gRPC
2. Enter the following, in sequence:  

```
cert-profile grpc_cert_profile ↵  
cipher-list grpc_cipher_list ↵  
no shutdown ↵
```

## Configure and enable gRPC on NE

### 17

1. Enter the following:  

```
/configure system grpc tls-server-profile gRPC_server_profile ↵
```

where *gRPC\_server\_profile* is the name of the server profile created in [Step 16](#)
2. Enter the following:  

```
/configure system security user username access console grpc ↵
```

where *username* is the name of the user to be granted gRPC access
3. Enter the following:  

```
/configure system security user admin console member administrative
```
4. Enter the following:  

```
/configure system grpc no shutdown ↵
```

### 18

Log out of the NE.

## Add NE to NSP telemetry collector configuration

### 19

- Perform one of the following.
- a. Enable telemetry collection for an NE discovered by the NFM-P using SNMP.
    1. Open an NFM-P GUI client.
    2. Choose Administration→Mediation from the NFM-P main menu. The Mediation (Edit) form opens.
    3. Select the mediation policy associated with the NE and click Properties. The Mediation Policy (Edit) form opens.
    4. In the gRPC panel, configure the Password and Confirm Password parameters using the gRPC NE user password.
    5. Select the Use Secure Transport parameter in the gRPC panel.

6. Save your changes and close the form.
- b. Enable telemetry collection for an NE discovered by the NSP using MDM; see “Workflow for using the Device Administrator application” in the Device Administrator Help for information about using the application to configure device mediation and discovery.

20

---

Open the NSP Telemetry application.

21

---

Specify the system IP address of each NE to monitor.

22

---

View the Telemetry dashboard to monitor NE performance, as required.

END OF STEPS

---

## 8.3 Telemetry troubleshooting

### 8.3.1 Description

Telemetry reporting by an NE occurs only when the TLS, gRPC, and NE user configurations are correct.

**i** **Note:** Telemetry reporting is sensitive to NE and NSP clock synchronization. To ensure that the Telemetry data from multiple NEs is assigned to the correct reporting period, it is strongly recommended that you engage NTP or a similar mechanism to maintain synchrony between the NE and NSP system clocks.

### 8.3.2 To troubleshoot NSP Telemetry reporting

The following steps describe a series of basic checks that can help you identify a Telemetry reporting issue.

See the NE documentation for specific information about using CLI commands and interpreting NE log messages.

Contact technical support for further assistance.

1

---

View the Telemetry application logs on the NSP server.

1. Log in as the root user on the primary or standalone NSP server or NFM-P main server, as required.
2. Open a console window.
3. View real-time log updates to the following Telemetry application logs using the “tail -f” command, or scan the log files to identify error messages:
  - /opt/nsp/os/tomcat/logs/telemetry.log

- 
- /opt/nsp/os/tomcat/logs/telemetry-collector.log
  - /opt/nsp/os/tomcat/logs/telemetry-collector-Notif.log
- For example, in /opt/nsp/os/tomcat/logs/telemetry-collector.log:
- The following error message indicates that the NE is not recognized by the NSP, perhaps because the NE is not discovered:  
No connection found for system id [n.n.n.n] for subscription.  
Please verify your connection configuration.
  - The following error message typically indicates a TLS certificate issue; for example, the certificate is not imported to the NSP truststore, the NE certificate import has failed, or the Secure Transport parameter in the gRPC mediation policy is incorrectly set:  
Network element [n.n.n.n] unavailable: UNAVAILABLE: Channel closed while performing protocol negotiation

---

## 2

To see whether gRPC is active on an NE, enter the following at the NE CLI:

```
show system grpc <^
```

Ensure that the Administrative State is Enabled, and the Operational State is Up.

```
show system security user # admin certificate display type cert cf3:/cert.pem format pem #  
show log log-id 98 subject TLS # show log log-id 98 subject Cert
```

---

## 3

To view the status of the gRPC TLS server profile on an NE, enter the following at the NE CLI:

```
show system security tls server-tls-profile <^
```

Ensure that the AdminState and OperState indicators of the gRPC server profile each read Up.

---

## 4

To view the status of the gRPC TLS certificate profile on an NE, enter the following at the NE CLI:

```
show system security tls cert-profile <^
```

Ensure that the AdminState and OperState indicators of the gRPC certificate profile each read Up, and that OperFlags does not indicate a problem, such as an invalid or expired certificate.

---

## 5

To view statistics about the gRPC NE user login and logout operations, including failed login attempts, enter the following at the NE CLI:

```
show log event-control "security" | match grpc <^
```

---

## 6

To display the SNMP security log for the purpose of identifying the NE user login and logout operations, perform the following steps at the NE CLI.

1. Enter the following:

```
configure log log-id 98 <^
```

- 
2. Enter the following:  
`from security ↵`
  3. Enter the following:  
`to memory ↵`
  4. Enter the following:  
`no shutdown ↵`
  5. Enter the following:  
`show log log-id 98 ↵`  
The security log entries are displayed in chronologically descending order.
  6. View the log entries to identify failed login and logout operations by the gRPC NE user.

## 7

---

If you require assistance from technical support, provide the following:

- the Telemetry application logs listed in [Step 1](#)
- the output of the NE status and log display commands in this procedure
- the `/opt/nsp/os/tomcat/logs/telemetry-collector-Metrics.log` file

**END OF STEPS**

---



---

## 9 Network Functions Manager - Packet

### 9.1 About

#### 9.1.1

The Network Functions Manager - Packet (NFM-P) application provides end-to-end network and service management across all domains of the converged IP network. Operational efficiency through fast provisioning and troubleshooting, service assurance, and enhanced network operations tools.

To access the NFM-P customer documentation, go to the NFM-P GUI and click Help→User Documentation.



---

# 10 Inventory Management

## 10.1 Overview

### 10.1.1

The Inventory Management application provides a dashboard inventory view of virtual network components and virtualized services in the network. It lists the total count of an object type, along with the number of operational and not operational objects. The dashboard view panel provides an at-a-glance summary of the virtual network components and virtualized services associated with the specified data center. It lists the total count of an object type, along with the number of operational and not operational objects.

#### Integrated help

The Inventory Management application has integrated help to guide you through the features and explain use case workflows. This integrated help includes product tours and use case videos. Click on the Help (?) button for a list of tours available in the application.

### 10.1.2 Inventory Search panel

The inventory search panel provides a list of VMs in the specified data center. The panel allows you to quickly find the status of a specific VM and view its associated underlay components. It includes a persisted administrative state for the last known status of VMs.

You can click on the Services tab to view the service-to-underlay mapping. You can select a virtualized service and see associated network components in a hierarchical view. The inventory represents of drill-down view of the component hierarchy. When you select a virtualized service from the Services tab, the Associated Components tab updates with a list of the associated V-Switches, V-Switch controllers, and upstream routers. When you select a Virtual Switch Controller, the Upstream Routers list updates to show routers for the selected controller. When you select a V-Switch, the panel shows a list of V-Ports for that service.

### 10.1.3 Inventory Topology panel

The inventory topology panel displays a conceptual map of the specified data center. It shows the association of virtual services controllers, virtual switch groups, virtual switches, virtual machines, and virtual ports. The topology also displays software gateways as both VRS-G and VSG virtual switches.

### 10.1.4 Profiles panel

The Profiles view allows you to configure local and global DC policies. The following profiles can be configured from the Profile View:

- BGP profiles
- aging profiles
- historical event profile

- historical event partition profile

### BGP Profiles

BGP Profiles are local profiles that monitor BGP prefix updates according to user-defined rules. The profiles then either log or reject the prefix—whichever action is specified.

There is one default BGP profiles that is created automatically when the data center is created. The default profile logs prefixes for internal BGP events for L2 and L3 GRE domains and for L3 domains with VXLAN tunnels.

You can create up to eight additional BGP profiles. You can specify a priority order to determine which profiles should attempt to match a prefix first. When a profile matches a prefix, the specific action is performed and no other profile matches are attempted.

See the *Configure BGP profiles* tour on the Profile View for more information about the parameters that can be configured for a BGP profile. The tour describes the required input format for each parameter.

Figure 10-1 BGP profile

General	
ID :	1
Name :	DC:1 BGPProfile:1
Priority :	10
Description :	Log Internal BGP Events for DC L2 and L3 GRE domains
Route Type :	Internal DC
RT Type :	Unspecified
RD Type :	Unspecified
RT RD Relation :	RT matches RD
Community List :	0:0
Next Hops :	0.0.0.0
Action :	Log Prefix

### Ageout constraint profiles

Ageout constraint policies (or aging profiles) define the period of time that a persisted object is retained in the VSAP database. When the age of an object reaches the ageout value, VSAP deletes the object from the database.

Figure 10-2 Aging profile

<b>General</b>	
Class Name :	dctr.VirtualMachine
Description :	Ageout Constraint Policy
Administrative State :	Up
Qualified Ageout Time :	168
<b>Deletion Interval</b>	
Synchronization Time :	2015/05/11 00:00:00 000 -04:00 GMT
Interval :	1
Next Deletion Start Time :	2015/05/12 11:00 EDT
<b>Status</b>	
In Progress :	
Last Started :	2015/05/12 10:00:00 293 -04:00 GMT
Last Skipped Interval :	N/A
Last Completed :	2015/05/12 10:00:00 373 -04:00 GMT

### Historical event and historical event partition profiles

You can configure these profiles to specify the window of time in which events can be correlated. You can also modify the profiles to specify the following:

- configure historical retention behavior
- configure the maximum database size and length of a historical interval



---

# 11 Service Navigator

## 11.1 Overview

### 11.1.1

The Service Navigator application shows a dashboard of the operational health of the service objects in a specified administrative domain. Virtualized services within VSAP are grouped by their customer, domain, and zone ID, allowing for easy searchability and navigation by enterprise from the application.

You can use the Service Navigator application to perform in-depth forensic analysis such as root cause and impact analysis. You can also perform an underlay ping test to assess network health or a data path audit to receive information on the NSG V-Switch.

#### Integrated help

The Service Navigator application has integrated help to guide you through the features and explain use case workflows. This integrated help includes product tours and use case videos. Click on the Help (?) button for a list of tours available in the application.

### 11.1.2 Reachability monitoring

You can specify an enterprise and domain to view a list of the V-Ports within that domain. The list includes V-Port functional state and BGP reachability state. In cases where the functional or reachability state is down, you can hover over the BGP state flag to view correlated alarms causing the administrative down state.

If there are software gateway bridge ports in the network, VSAP creates a bare metal device child object for associated BGP events and reachability monitoring. You can view bare metal objects from the Bare Metal Device tab.

If there are NSG access routes in the network, they are displayed in the NSG Access Routes tab. The icon on the tab displays as green if all listed routes are reachable, red if some routes are unreachable, and grey if there are no routes listed.

#### V-Port reachability audit

You can perform an on-demand audit of V-Port prefix reachability using VSAP EVPN prefix lists. After a significant network event, such as VSC failure or BGP event loss, you may wish to confirm V-Port reachability state by querying the EVPN prefix list

The V-Port audit retrieves EVPN routes to update V-Port reachability state after a network change. When the audit is complete, you can refresh the V-Port list to see any state changes.

### 11.1.3 Fault management

The fault management window allows you to perform alarm management and forensic event tracking on the selected domain or V-Port. It consists of an Alarms and Historical Events tab.

The Alarms tab allows you to view all alarms on the selected domain or V-Port. It provides alarm monitoring, correlation, and troubleshooting for virtual network objects and virtualized services in the network. It allows you to filter, identify root causes, and determine the impact of alarms. It includes the data center correlation framework to correlate faults unique to virtual network objects. You can perform alarm management functionality, such as alarm acknowledgment or severity configuration. You can also view alarm statistics and correlation trees from the fault management window.

The Historical Events tab allows you to perform root cause and historical impact analysis on events in the past. You can query the event log for a list of DC network events that occurred in a specified time window and then determine the causes or impacts of an event.

### 11.1.4 Underlay ping

You can use the Service Navigator application to perform an underlay test. You can use this test to troubleshoot a service-attached VM to assess the underlay health of the data center network. This functionality is useful if, for example, VSAP statistics show a decline in performance statistics for a V-Port.


You must create the Nuage OAM System script bundle before you can execute it in the VSAP Java GUI or Service Navigator web application. The Nuage OAM System script bundle includes the control script and CLI script use to execute the OAM ping test between two endpoints. The script is included as an example script from which you can create an underlay test script bundle.






### 11.1.5 Topology maps

You can open the map window by selecting a domain in the Domain panel and clicking the View Map button. You can use the map to highlight services within a domain or to show advertising and underlay routers for a selected V-Port. You can also select an endpoint on the map to view virtual component information and interface statistics. You must enable IP interface statistics in the VSAP Java GUI before you can view interface statistics in the Service Navigator application, and create a VSD client before you can view BGP peer information for NSG nodes.

#### Icons

The topology map uses the following icons to distinguish data center network elements.

Icon	Network element
	Router

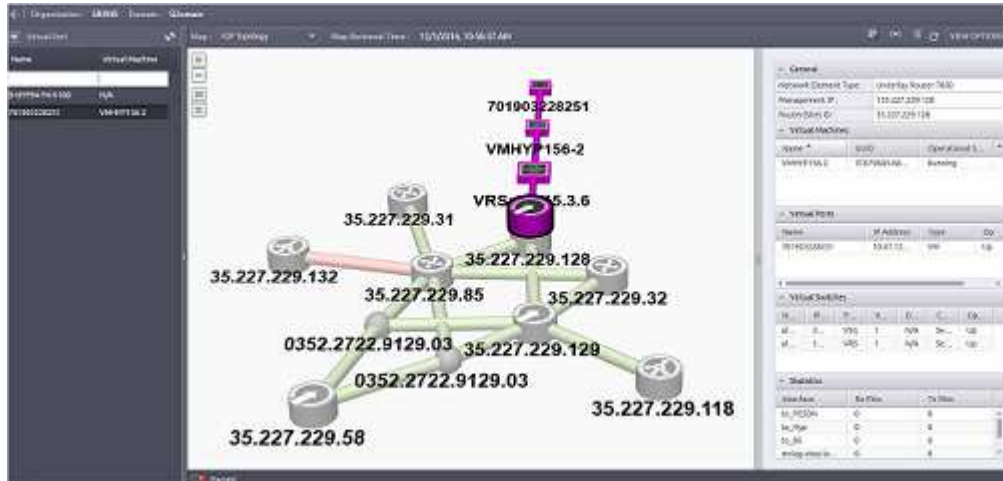
Icon	Network element
	7850 VSG
	VSC
	MC LAG
	NSG-BR
	NSG-UBR

## Overlay highlights

The multi-layer map allows you to view more than one overlay highlight at once. Select the V-Ports from the Virtual Port panel and click one or more of the highlight buttons to display the highlight overlay.

- Service topology—magenta
- Advertising router—blue

Figure 11-1 IGP multi-layer map with overlay highlights



## Peer/link group panel

You can click on a link in the BGP map to open the peer group panel, or a link in the IGP map to open the link group panel. The BGP peer group is displayed as green (up) or red (not up) based on the connection state of the peer group. The IGP peer group displays the same colors based on the operational state. Depending on whether you selected an IGP or BGP peer/link group, the group panel displays different information.

Figure 11-2 Peer group display

Site ID :	35.227.229.132
Site Name :	VSC132
Group Name :	test
Peer Address :	35.227.229.85
Local AS :	65123
Peer AS :	65123
Family :	ipv4, vpnipv4, evpn, mcastVpn ...
Admin State :	Up
Operational State :	Up
Connection State :	Established

**Expand in place**

You can click a network element to expand its associated components on the map. On a data center topology map, you can view the associated V-Switch, VM, Container, or V-Port. On a WAN topology map, you can view the WAN cloud and associated NSG V-Switches. You can click any

---

expanded component to open the information panel and view more details.

This functionality allows you to view specific endpoints on the map when viewing a highlighted service. Rather than a service highlight showing upstream routers as an endpoint, the map automatically expands the network element and highlights the service to the associated VM.

### Layout persistence

The Service Navigator retains the NE layout from the previous user session. You can manually refresh the map to ensure you have the latest layout. You can enable Auto Refresh to allow the map to periodically update the layout automatically. The automatic refresh setting applies to the topology map only. The V-Port panel is not automatically refreshed. If service highlighting is enabled, the highlight is redrawn according to the updated NE layout.

### Linked domains and underlays

When the selected domain is linked to one or more domains using an NSG-BR, you can use the domain linking map to view the link topology and the status of the cross-domain links. You can also view BGP links into other domains through an NSG-BR using the BGP topology map.

When the selected domain contains underlays that are linked using an NSG-UBR, you can use the BGP topology map to view the links. Selecting multiple V-Ports will display underlay elements that the V-Ports have in common, and the links between them.

## 11.2 Service Path Discovery

### 11.2.1 Overview

You can use the Service Navigator application to highlight the most likely data path between two vports, or display current data flows between the vports. You can display the data path for a protocol or a known application, and specify the source and destination ports. This section describes how to enable service path discovery on the VSAP, how to display service paths and data flows, and how to resolve errors.

### 11.2.2 Prerequisites

Before you can discover service paths, you must ensure that the node hypervisors have the correct software installed, that the VSAP can communicate with the nodes using Telnet, and the nodes can communicate properly with each other.

The following workflow describes the high-level steps required to enable service path discovery.

1. During discovery, configure a mediation security policy that uses Telnet for communication. See the *VSAP User Guide*.
2. Install the VSAP service discovery software packages. See the *VSAP User Guide*.
3. Ensure that flow logging is enabled on the VSD. See the VSD user documentation for information about enabling flow logging.

### 11.2.3 Displaying a service path

You can discover service paths using the topology map on the Service Navigator application by selecting a source and destination vPort from the list, and clicking on the Discover Service Path button. From the window, you can select a protocol or application, and specify source and destination ports. See [11.2.4 “To discover a service path” \(p. 120\)](#).

#### Service path operations

When you discover service paths, you can specify the operation used to discover the path. The following table describes the operations available after you click on the Discover Service Path button.

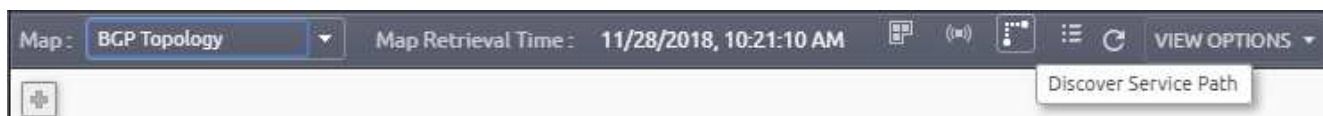
Operation	Description	Options	See
Default	Discover a service path using ICMP, TCP, or UDP with the saved default values	You can specify source and destination ports for TCP and UDP.	<a href="#">11.2.4 “To discover a service path” (p. 120)</a> <a href="#">“Setting defaults” (p. 119)</a>
Known Applications	Discover a service path using one of the following applications: <ul style="list-style-type: none"> <li>• SCP/SSH</li> <li>• FTP</li> <li>• HTTP</li> <li>• DHCP</li> </ul>	You can specify source and destination ports. Default destination ports are provided, depending on the application.	<a href="#">11.2.4 “To discover a service path” (p. 120)</a>
Manual	Discover a service path using ICMP, TCP, or UDP with manually-entered source and destination ports	You can specify source and destination ports for TCP and UDP.	<a href="#">11.2.4 “To discover a service path” (p. 120)</a>
Active Flows	Display a list of active flows between the two selected vPorts. You can select a flow from the list and display the service path for that flow.	You can specify how many flows to display, and which types of flows (TCP, UDP or both) are displayed	<a href="#">11.2.5 “To display active flows” (p. 120)</a>

#### Setting defaults

When you configure source and destination ports for a service path discovery action, you can enable the Set As Default option to save the configured values as the default values for that operation. Default values are saved individually for each source vPort.

## 11.2.4 To discover a service path

- 1 \_\_\_\_\_  
From the Service Navigator application, select a VSD Organization from the search field. Entering a % symbol in the search field displays a list of all discovered organizations. A list of domains in the selected organization appears in the Domain panel.
- 2 \_\_\_\_\_  
Select a domain in the Domain panel, and click on the Map button. The topology map window opens.
- 3 \_\_\_\_\_  
Select the BGP or IGP topology map from the Map drop-down menu. The selected topology map for the chosen domain appears, with a list of vPorts displayed in the Virtual Ports panel.
- 4 \_\_\_\_\_  
Click on a vPort in the Virtual Ports panel to select it as the source port for the service path, then hold the CTRL key and click on a second port to select it as the destination port.
- 5 \_\_\_\_\_  
Click on the Discover Service Path button. The Customer Packet Application Type form opens.



- 6 \_\_\_\_\_  
Select an operation from the Operation drop-down menu.
- 7 \_\_\_\_\_  
Configure the parameters as required. See [“Service path operations”](#) (p. 119) for information about service path discovery operations.
- 8 \_\_\_\_\_  
Click on the Show Path button. The discovered service path is highlighted on the topology map.

## 11.2.5 To display active flows

- 1 \_\_\_\_\_  
From the Service Navigator application, select a VSD Organization from the search field. Entering a % symbol in the search field displays a list of all discovered organizations. A list of domains in the selected organization appears in the Domain panel.

- 2 \_\_\_\_\_  
Select a domain in the Domain panel, and click on the Map button. The topology map window opens.
- 3 \_\_\_\_\_  
Select the BGP or IGP topology map from the Map drop-down menu. The selected topology map for the chosen domain appears, with a list of vPorts displayed in the Virtual Ports panel.
- 4 \_\_\_\_\_  
Click on a vPort in the Virtual Ports panel to select it as the source port for the service path, then hold the CTRL key and click on a second port to select it as the destination port.
- 5 \_\_\_\_\_  
Click on the Discover Service Path button. The Customer Packet Application Type form opens.



- 6 \_\_\_\_\_  
In the Operation drop-down menu, select Active Flows.
- 7 \_\_\_\_\_  
Configure the Protocol and Most Active Flows parameters. The Most Active Flows parameter specifies the number of flows to display, starting with the most active flows based on total transmitted packets.
- 8 \_\_\_\_\_  
Click on the Show active flows button. A list of flows appears in the Active Flows panel below the Virtual Ports list. You can mouseover a flow to view details about that flow.

Src Port	Dst Port	Protocol	Total Tx Pkts
N/A	N/A	ICMP	9577
39246	1000	Tcp	9577

Src VPort	100.100.100.55
Dst VPort	200.200.200.183
Protocol	ICMP
Src Port	N/A
Dst Port	N/A
Total Tx Pkts	9577

9

To view the service path for a flow, right-click on the flow and choose Show Path. The path is highlighted on the topology map.

## 11.3 Service connectivity check

### 11.3.1 Overview

You can use the topology map on the Service Navigator to perform underlay and overlay connectivity checks on the vPorts in a domain. After a connectivity check is performed, the service connectivity status icon on the topology map and beside each vPort is updated to show the connectivity state.

To perform a service connectivity check on all connections in a domain, see [11.3.4 “To perform a service connectivity check on a domain” \(p. 125\)](#). To perform a service connectivity check on the connection between two vPorts, see [11.3.5 “To perform a service connectivity check on a vPort pair” \(p. 126\)](#).

### 11.3.2 Prerequisites

Before you can perform a service connectivity check, you must ensure that the node hypervisors have the correct software installed, that the VSAP can communicate with the nodes using Telnet, and the nodes can communicate properly with each other.

The following workflow describes the high-level steps required to enable service connectivity checking.

1. During discovery, configure a mediation security policy that uses Telnet for communication. See the *VSAP User Guide*.
2. Install the VSAP service discovery software packages. See the *VSAP User Guide*.

#### Supported ACL check criteria

During a service connectivity check, the VSAP queries OVS configurations to discover any customer-configured ingress or egress ACLs that may affect overlay service connectivity between two vPorts. The following table lists the supported security policy ACL configurations. See the VSD user documentation for more information about configuring security policies.

**i** **Note:** Depending on flow output, some configurations may not be considered in the service connectivity testing.

ACL match criteria	Supported options
Action	Drop, Allow
Protocol	ICMP, Any
ACL Type	Local
Destination Network	Any
Origin Location	Any, Zone, Subnet
Ether Type	IPv4-0x0800
DSCP Marker	Any
Service Type	None
Dest IP Match	–
Source IP Match	–

### 11.3.3 Service connectivity test results

When a service connectivity check is complete, a summary of the test results is displayed in the Service Connectivity Test Results window, and the Service Connectivity Status icons for the domain and for each tested vPort are updated to reflect the results of the test. When a test fails, the status icon for the vPort and domain changes to the Failed state. You can right-click on a vPort and select Show Service Connectivity Results to see detailed information about the tests performed on that vPort.

#### Service Connectivity Test Results window

The Service Connectivity Test Results window appears when a service connectivity check is complete. The following figure shows an example test result window.

Figure 11-3 Service connectivity test results

Service Connectivity Test Results	
VTEPs Tested:	3
Average Network Delay(ms):	8.046166
Maximum Network Delay(ms):	10.816
Minimum Network Delay(ms):	3.295
Number of Successful Tests:	728
Number of Failed Tests:	38
Failure Reason(s):	Datapath flow dropped

The window summarizes the tests performed on the domain or selected vPorts. The following table describes the parameters that appear in the test result window.

Parameter	Description
VTEPs tested	The number of VTEPs included in the test
Average Network Delay(ms)	The average network delay recorded in all applicable tests
Maximum Network Delay(ms)	The highest network delay recorded out of all tests
Minimum Network Delay(ms)	The lowest network delay recorded out of all tests
Number of Successful Tests	The number of successful tests performed
Number of Failed Tests	The number of tests that resulted in failure
Failure Reason(s)	All failure reasons returned for any failed tests

### VM Connectivity Results window

When you right-click on a vPort and select Show Service Connectivity Results, the VM Connectivity Results window appears. The following figure shows an example test results window.

Figure 11-4 VM Connectivity Results

Src VPort	Dst VPort	Status	Test Failed VTEP(s)	Network Delay	Failure Reason(s)	Src VTEP	Dst VTEP
100.100.100.55	100.100.100.102	Up	N/A	N/A	N/A	10.10.20.2	10.10.20.2
100.100.100.55	100.100.100.147	Up	N/A	N/A	N/A	10.10.20.2	10.10.20.2
100.100.100.55	100.100.100.158	Up	N/A	N/A	N/A	10.10.20.2	10.10.20.2
100.100.100.55	100.100.100.202	Up	N/A	N/A	N/A	10.10.20.2	10.10.20.2
100.100.100.55	100.100.100.58	Up	N/A	N/A	N/A	10.10.20.2	10.10.20.2
100.100.100.55	100.100.100.123	Up	N/A	N/A	N/A	10.10.20.2	10.10.20.2
100.100.100.55	100.100.100.10	Up	N/A	N/A	N/A	10.10.20.2	10.10.20.2
100.100.100.55	100.100.100.93	Up	N/A	N/A	N/A	10.10.20.2	10.10.20.2
100.100.100.55	100.100.100.209	Up	N/A	N/A	N/A	10.10.20.2	10.10.20.2
100.100.100.55	200.200.200.24	Up	N/A	7.723	N/A	10.10.20.2	10.10.10.2
100.100.100.55	200.200.200.91	Up	N/A	7.723	N/A	10.10.20.2	10.10.10.2
100.100.100.55	200.200.200.183	Up	N/A	7.723	N/A	10.10.20.2	10.10.10.2
100.100.100.55	200.200.200.123	Up	N/A	7.723	N/A	10.10.20.2	10.10.10.2
100.100.100.55	200.200.200.113	Up	N/A	7.723	N/A	10.10.20.2	10.10.10.2
100.100.100.55	200.200.200.166	Up	N/A	7.723	N/A	10.10.20.2	10.10.10.2
100.100.100.55	100.100.100.224	Up	N/A	9.471	N/A	10.10.20.2	20.20.20.1
100.100.100.55	100.100.100.47	Up	N/A	9.471	N/A	10.10.20.2	20.20.20.1
100.100.100.55	100.100.100.81	Up	N/A	9.471	N/A	10.10.20.2	20.20.20.1
100.100.100.55	100.100.100.205	Up	N/A	9.471	N/A	10.10.20.2	20.20.20.1

The table in the window displays information about each test that was performed on the vPort during the most recent service connectivity check. Each row represents a separate test summary for results between two vPorts. The following table describes the columns in the VM Connectivity Results window.

Column	Description
Src VPort	The address of the source vPort involved in the test
Dst VPort	The address of the destination vPort involved in the test
Status	The status of the connection between the two vPorts involved in the test, displayed as Up or Down
Test Failed VTEP(s)	Any VTEPs which failed during the test
Network Delay	The network delay recorded during a test
Failure Reason(s)	The failure reasons returned for a failed test
Src VTEP	The VTEP for the source vPort
Dst VTEP	The VTEP for the destination vPort

### 11.3.4 To perform a service connectivity check on a domain

Perform this procedure to check the service connectivity of all connections in a domain.

- 1 

---

From the Service Navigator application, select a VSD Organization from the search field. Entering a % symbol in the search field displays a list of all discovered organizations. A list of domains in the selected organization appears in the Domain panel.
- 2 

---

Select a domain in the Domain panel, and click on the Map button. The topology map window opens.
- 3 


---

Select a topology map from the Map drop-down menu. The selected topology map appears.
- 4 

---

Click on the Check Service Connectivity button. The Service Connectivity Status icon changes to indicate that a check is in progress, and the progress of the check is displayed as a percentage beside the icon.

Depending on the size of your network, the check can take several hours. When the check is complete, the Service Connectivity Test Results window opens and displays a summary of the test results.

 **Note:** Only one connectivity check can be in progress at a time.
- 5 

---

To view detailed information about test results, right-click on a vPort and select Show Service Connectivity Results. The VM Connectivity Results window appears.

### 11.3.5 To perform a service connectivity check on a vPort pair

Perform this procedure to check the service connectivity between two vPorts in a domain.

- 1 

---

From the Service Navigator application, select a VSD Organization from the search field. Entering a % symbol in the search field displays a list of all discovered organizations. A list of domains in the selected organization appears in the Domain panel.
- 2 

---

Select a domain in the Domain panel, and click on the Map button. The topology map window opens.
- 3 

---

Select a topology map from the Map drop-down menu. The selected topology map appears.
- 4 

---

Click on a vPort in the Virtual Port panel, then control-click on a second vPort to select both ports.

---

5

Right-click on one of the selected ports and select Start Service Connectivity Test. The Service Connectivity Status icon changes to indicate that a check is in progress, and the progress of the check is displayed as a percentage beside the icon.

When the check is complete, the Service Connectivity Test Results window opens and displays a summary of the test results.



**Note:** Only one connectivity check can be in progress at a time.

---

6

To view detailed information about test results, right-click on a vPort and select Show Service Connectivity Results. The VM Connectivity Results window appears.



---

## 12 Wireless NE Views

### 12.1 The NFM-P Wireless NE Views application

#### 12.1.1 Overview

The NFM-P Wireless NE Views application provides a graphical representation of wireless equipment and logical entities. The application displays the following:

- Cards—control board, modem board
- Radio modules—RRH, TRDU, RFME
- Ports—SFP, antenna ports, cell antenna ports
- Links
- LteCells
- Sectors

Alongside the graphical representation of the eNodeB hardware is a contextual alarm list that allows operators to perform alarm management and drill-down.

#### 12.1.2 Views and functions

The display of the Wireless NE Views application is divided into two areas:

- **Graphical View**

The Graphical View is a circular display of the eNodeB NE, connected hardware, and logical objects. The Graphical View displays NE components as a wedge shape when the eNodeB has fewer than 3 cells. The view features the following:

- named sections for modems, boards, radio modules, and LteCells
- contextual tooltips that display identifying and state information for each section
- directional port-to-port link information
- color-coded health and state information for components and links
- selection of specific components to display specific fault management information
- right-click contextual options to navigate to the logical view (for LteCell) or components view (for all others)

- **Alarm List**

The Alarm List displays a filterable list of alarms currently raised against the selected hardware or object. You can expand alarms to view specific alarm fields, and perform right-click actions including:

- view impact, root cause, and object point of view diagrams
- assign OLC state
- acknowledge, delete, clear, and assign severity/urgency
- navigate to the affected object in the NFM-P GUI
- view alarm and object alarm histories

- view current and historical alarm snapshots
- You can add/remove, sort, and autofit columns in the Alarm List by right-clicking on a column and selecting the options in the Columns list. You can reposition columns by clicking and dragging.

### 12.1.3 Object and link health indicators

Objects in Wireless NE Views are colored according to their health status. The application uses the following rules:

- Objects are light gray by default.
- If the Administrative State of an object is “locked” or in shutdown, the object is dark gray.
- If the Administrative State of an object is “unlocked”, the following logic applies:  
IF there is a critical alarm OR the operational state is disabled OR the availability status is “off duty”, THEN the object border is red.  
ELSE  
IF there is a major alarm OR the availability status is “degraded” THEN the object border is orange.  
ELSE  
The border is green.

Links in Wireless NE Views are colored according to the health status of the connected objects. The application uses the following rules:

- CPRI links: the health of the link is equal to the lowest health of the connected radio equipment.
- Antenna links: the health of the link is equal to the antennaPort health

### 12.1.4 General features and behavior

The following statements describe general Wireless NE Views features and behavior:

- You can select an eNodeB to display using the search bar in the top-right of the application.
- The search bar also features a drop-down list to select an eNodeB directly.
- There is a refresh button next to the search bar.
- When the central eNodeB object is selected, or no object is selected, all alarms are displayed by the Alarm List. Selecting an object displays the alarms for that object only.
- You can rotate sections of the NE view by clicking and dragging components, which is useful for aligning links in the display.
- You can zoom in and out using the mouse scroll wheel.
- Tooltips display the following information:
  - identifiers (name, alias, ID, hardware number, management IP)
  - state and status indicators
  - the number of major and critical alarms
  - the Site Name of RFMs
- Tooltips are refreshed every 8 seconds.
- Antenna ports and cell antenna ports are displayed with their rdnlId.

- 
- SFPs are displayed with (and in order of) their position number.
  - Pre-provisioned NEs are not available for display by the Wireless NE Views.

### **12.1.5 User preferences**

The Wireless NE Views application features a preferences menu with the following options:

- Show all links—enable or disable the display of all links by default.
- Show unhealthy links—enable or disable health indicators for links.
- Show highlighted links—enable or disable highlighting for links on selected components.
- Show tooltips—enable or disable tooltips.



---

## 13 Wireless Supervision

### 13.1 Overview

#### 13.1.1 Features

The NFM-P Wireless Supervision application provides an at-a-glance view of LTE RAN network fault status in a dynamic web-based GUI. You can perform the following tasks using the Wireless Supervision application:

- view full and regional network status quickly and efficiently
- view network KPIs and prioritize network problems accordingly
- investigate network alarms and view fault correlation
- perform alarm management tasks such as alarm acknowledgement and clearing
- launch the NFM-P GUI to perform more detailed troubleshooting tasks such as eNodeB and cell reset
- drill down to eNodeB objects for more detailed status information
- view trace status information for all supported trace types

#### 13.1.2 Wireless Supervision views and functions

The Wireless Supervision application GUI features the following views:

- **Summary View**

The Summary View panel displays the following set of supervision group KPIs for the all managed eNodeBs in the selected summary view:

- number of unacknowledged critical alarms
- percentage of non-operational eNodeBs—percentage of eNodeBs with an Administrative State of “unlocked” and an Operational State of “disabled”
- percentage of non-operational cells—percentage of cells with an Administrative State of “unlocked” and an Operational State of “disabled”

Clicking on a KPI number opens the relevant details view for the KPI type (Alarm List, eNodeBs view, or LteCells view). Clicking on the All Groups icon returns to the Matrix view.

KPIs are colored as follows:

- alarms—red when at least one unacknowledged critical alarm is raised on an eNodeB in the group, otherwise green.
- eNodeB—red for 10% or more non-operational, orange for 5%-9%, green for below 5%.
- LteCell—same criteria as eNodeB.

New supervision group are automatically added to the Matrix View of the selected Summary View at the end of each polling period.

- **Matrix View**

The Matrix View displays at-a-glance KPIs of all supervision groups in the current summary view. Each group displays three colored bars that display the status of the critical alarm, non-operational eNodeB, and non-operational cell KPIs.

The group icons in the Matrix View and Summary View are colored to reflect the combined overall KPI status as follows:

- red—more than 75% of KPIs are not green
- orange—all but one KPI are not green, or one KPI is red
- yellow—one KPI is not green
- green—all KPIs are green

The Matrix View displays groups from worst to best KPI status, which is the same order listed above. You can mouse-over a group to view a status tooltip, and click to expand the group for details on KPIs and eNodeB/LteCell counts. The Matrix View features a group navigation menu that can be accessed by clicking on the top right corner of a group and provides access to all group views.

- **Alarm List**

The Alarm List displays a filterable list of alarms currently raised against the selected supervision group, eNodeB, or cell. Selecting the Group Alarms View or clicking on the alarm KPI for a supervision group displays the full group view. The Alarm List is also displayed (collapsed by default) at the bottom of the eNodeBs, LteCells, and Sites Views and displays the alarms raised against the selected object. You can expand alarms to view specific alarm fields, and perform right-click actions including:

- view impact, root cause, and object point of view diagrams
- update OLC state
- acknowledge, delete, clear, and assign severity/urgency of alarms
- navigate to the affected object in the NFM-P GUI
- view alarm and object alarm histories
- view current and historical alarm snapshots

The Alarm List features a pause button in the bottom-left corner of the panel. This button enables or disables alarm polling, which is 30 seconds by default and can be changed in the global User Preferences menu at the application selection screen. All alarm list views feature an export to CSV option.

- **eNodeBs View**

The eNodeB View displays a filterable list of eNodeBs with columns for state, status, and SW version information. You can perform an in-context launch of the Wireless NE Views application by right-clicking on an eNodeB and choosing Show in Wireless NE Views.

- **LteCells View**

The LteCell View displays a filterable list of LteCells with columns for state and status information. You can perform an in-context launch of the Wireless NE Views application by right-clicking on an LteCell and choosing Show in Wireless NE Views. The LteCells view features an advanced filter that can be used to filter out LteCells in the shutdown state, for example: *Availability Status equal "offline offDuty" OR Availability Status equal "offDuty offLine"*

- **Sites View**

The Sites View displays a filterable list of eNodeBs, RFMs, and SMMs with columns for state, status, and SW version information. Elements are displayed in the Sites View when they share a

---

site name with another component. Components with unique site names are not displayed. The Sites View features right-click contextual menus to the NFM-P client or SMM management interface.

- **Traces Dashboard View**

The Traces Dashboard View displays filterable status information for all trace types in the supervision group. Right-click contextual menus provide navigation to relevant properties forms in the NFM-P client.

You can add/remove, sort, and autofit columns in the eNodeB/LteCell View and Alarm List by right-clicking on a column and selecting the options in the Columns list. You can reposition columns by clicking and dragging.

The Wireless Supervision features a global pause button in the bottom-left corner of the window.

## 13.2 To launch the Wireless Supervision application

### 13.2.1 Before you begin

You can launch the Wireless Supervision application:

- by specifying a browser path and launching from the NFM-P client GUI
- by navigating to the NFM-P launch panel URL with a compatible web browser

### 13.2.2 Steps

1

---

To specify the browser path for launching the Wireless Supervision application from the NFM-P client GUI, perform the following. This step only needs to be performed once.

Specifying a browser path is not required when navigating to the NFM-P launch panel URL.

1. Choose Application→User Preferences from the NFM-P main menu. The User Preferences form opens.
2. Scroll to the bottom of the form and specify the Browser Path by performing one of the following:
  - Click Browse, navigate to the web browser executable file on the local workstation, and click Open. The Browser Path is updated.
  - Click Reset and manually specify the path to the web browser executable file.
3. Save the changes and close the form.

2

---

To launch from the NFM-P client GUI, choose Application→Wireless Supervision from the NFM-P main menu. The NFM-P opens the specified web browser and launches the Wireless Supervision application.

3

---

To navigate to the NFM-P launch panel using a compatible web browser, open the web browser on the local workstation and perform the following:

1. Navigate to the following URL:  
`server/login`  
where  
`server` is the NFM-P server IP address
2. Enter login credentials and click Login.

4

Click the Launch Wireless Supervision application icon. The Wireless Supervision application launches.

END OF STEPS

## 13.3 Configuring supervision objects

### 13.3.1 Object types

The NFM-P Wireless Supervision application organizes eNodeBs using the following configurable network objects:

- **Supervision groups**

A supervision group is a logical set of NEs that is specified by user-defined filters. Supervision groups can be used to partition NEs into distinct categories and are associated with summary views. There is no limit to the number of supervision groups that an eNodeB can belong to.

**Note:** For performance reasons, do not exceed 500 eNodeBs per supervision group.

- **Summary views**

A summary view is a collection of one or more supervision groups that provides a summarized, high-level view of a group of network objects. There is no limit to the number of summary views that a supervision group can belong to.

### 13.3.2 Monitoring eNodeBs with the Wireless Supervision application

The view of eNodeBs in the Wireless Supervision application GUI is based on the currently selected summary view. You can populate summary views with managed eNodeBs using the following methods:

- **Automatically** using the “Create Automatically by Using Topology Group” option in the Supervision Group Settings menu of the Wireless Supervision application. Applying this option creates a supervision group for each equipment group in the NFM-P and adds them to the Default Wireless Summary View. This method provides a view of all eNodeBs in the managed network organized by equipment group. After applying, automatic creation does not take subsequent equipment group changes into account and must be re-applied.
- **Manually** using the NFM-P client GUI. You can configure supervision groups that include eNodeB-specific inclusion filters and associate the groups with a summary view. This method allows the creation of a targeted view of a specific subset of managed eNodeBs.

---


## 13.4 To configure a supervision group

### 13.4.1 Before you begin

Supervision groups include NEs based on inclusion filters. The inclusion filters used to specify the eNodeBs in the supervision group must exclude pre-provisioned NEs and all other non-eNodeB NE types to avoid misleading alarms and KPI numbers.

### 13.4.2 Steps

- 1 \_\_\_\_\_  
Choose Administration→Supervision Settings from the NFM-P main menu. The Supervision Settings (Edit) form opens.
- 2 \_\_\_\_\_  
Click on the Supervision Groups tab.
- 3 \_\_\_\_\_  
Click Create. The Supervision Group (Create) form opens.
- 4 \_\_\_\_\_  
Configure the parameters:
  - Displayed Name
  - Description
  - Category—must be set to “NE Access” for eNodeB supervision

 **Note:** The Supervised Alarms Severities parameter does not apply to eNodeB supervision. All eNodeB alarms are displayed in the Wireless Supervision application regardless of severity.
- 5 \_\_\_\_\_  
Click on the Inclusion Filters tab.
- 6 \_\_\_\_\_  
Click Add. The Select Form opens.
- 7 \_\_\_\_\_  
Perform one of the following:
  - a. To create an inclusion filter, go to [Step 8](#).
  - b. To apply an existing inclusion filter, go to [Step 16](#).
- 8 \_\_\_\_\_  
Click Inclusion Filter. The Inclusion Filter Creation form opens.

---

9

Configure the filter properties.

1. Choose an item from the Attribute drop-down menu.
2. Choose an item from the Function drop-down menu.
3. Configure the Value parameter.
4. Choose a Boolean Operator from the Operators drop-down menu, if applicable.
5. Click Add.

---

10

To add a filter that excludes pre-provisioned NEs:

1. Select “General: Network Element (Network)→State” as the Attribute.
2. Set the Function to “NOT EQUAL” and the Value to “Pre-provisioned”.
3. Click Add.

---

11

Perform one of the following:

- a. To filter additional properties, repeat [Step 9](#).
- b. If you are finished filtering properties, go to [Step 12](#).

---

12

Click Save. The Save Filter form opens.

---

13

Configure the parameters:

- Filter Name
- Description
- Public

---

14

Click Save. The filter is saved.

---

15

Close the Inclusion Filter Creation form.

---

16

Click Search in the Supervision Group form. A list of inclusion filters is displayed.

---

17

Choose an inclusion filter in the list and click OK. The filter is added to the supervision group.

---

18 \_\_\_\_\_  
Add additional filters, as required.

19 \_\_\_\_\_  
Save the changes and close the forms.

END OF STEPS \_\_\_\_\_

## 13.5 To configure a summary view

### 13.5.1 Steps

1 \_\_\_\_\_  
Choose Administration→Supervision Settings from the NFM-P main menu. The Supervision Settings (Edit) form opens.


2 \_\_\_\_\_  
Click on the Summary Views tab.

3 \_\_\_\_\_  
Click Create. The Supervision View (Create) form opens.

4 \_\_\_\_\_  
Configure the parameters:

- Displayed Name
- Description

5 \_\_\_\_\_  
For the Application parameter, select “Wireless Supervision”.

 **Note:** If “Wireless Supervision” is not specified as the Application, the summary view is not available for in the Wireless Supervision application.

6 \_\_\_\_\_  
Click on the Supervision Groups tab.

7 \_\_\_\_\_  
Click Add. The Select form opens.

8 \_\_\_\_\_  
Configure the filter criteria, if required, and click Search. A list of supervision groups is displayed.

---

**9** \_\_\_\_\_  
Select one or more supervision groups from the list and click OK. The Select form closes and the Supervision View (Create) form reappears with the selected supervision group(s) in the list.

**10** \_\_\_\_\_  
Add more supervision groups to the summary view, as required.

**11** \_\_\_\_\_  
Save the changes and close the form.

**END OF STEPS** \_\_\_\_\_

---

## 14 Policy Management

### 14.1 About

#### 14.1.1

The Policy Management application enables customized, policy-driven behavior. It also maintains rules that allow the NSD and NRC modules to customize network policies such as global or domain rules for routing algorithms selection and execution. The Policy Management application provides service definitions that describe services in highly abstract, customizable ways while supporting mapping (mediation) of these definitions to the low-level network concepts.

### 14.2 Template and policy provisioning

#### 14.2.1

This section describes the provisioning of templates and policies using the Policy Management application.

- [14.2.2 "To create an E-Line service template" \(p. 142\)](#)
- [14.2.3 "To create an E-LAN service template" \(p. 143\)](#)
- [14.2.4 "To create a C-Line service template" \(p. 145\)](#)
- [14.2.5 "To create an L3 VPN service template" \(p. 146\)](#)
- [14.2.6 "To create an IES service template" \(p. 147\)](#)
- [14.2.7 "To create an Endpoint QoS template" \(p. 148\)](#)
- [14.2.8 "To create a Generic QoS policy" \(p. 149\)](#)
- [14.2.9 "To modify the RD/RT Range policy" \(p. 150\)](#)
- [14.2.10 "To create a Tunnel Profile policy" \(p. 152\)](#)
- [14.2.11 "To create a Steering Parameter" \(p. 155\)](#)
- [14.2.12 "To modify the IP/MPLS Configuration policy" \(p. 155\)](#)
- [14.2.13 "To create a Router ID Mapping policy" \(p. 156\)](#)
- [14.2.14 "To create a Path Profile policy" \(p. 157\)](#)
- [14.2.15 "To create a Mediation Profile" \(p. 158\)](#)
- [14.2.16 "To create a Workflow Profile" \(p. 159\)](#)

## 14.2.2 To create an E-Line service template

1 \_\_\_\_\_  
 In the Policy Management application, click on Service Templates to expand the template type list and then click E-Line. The system displays the list of existing E-Line service templates.

2 \_\_\_\_\_  
 Click CREATE TEMPLATE. The Create E-Line Service Template form opens.

3 \_\_\_\_\_  
 Configure the required parameters in the PROPERTIES panel.

**i** **Note:** During the service template configuration, you can click CANCEL at any time to close the form without saving the template.

Parameter	Description
Name	The name of the E-Line Service template
Admin State	Specifies the administrative state required for the service
Mediation Profile	Specifies a Mediation Profile to apply
Workflow Profile	Specifies a Workflow Profile to apply
Tunnel Profile	Specifies a Tunnel Profile to apply
Endpoint QoS Template	Specifies an Endpoint QoS template to apply
Bidirectional	Specifies whether or not a return path is required, and if so, what type of return path should be determined
Optimize on (Objective)	Specifies the primary goal when identifying resources and/or paths for service creation
Max Hops (Span)	Specifies the maximum number of hops to consider
Max Latency (microseconds)	Specifies the maximum latency to consider
Max Cost	Specifies the maximum cost to consider
Monitor Bandwidth	Specifies whether or not to monitor bandwidth
MTU	Specifies the MTU for the service. The range is 0 to 9194
Description	Describes the E-Line service template

Parameter	Description
VC Type	Specifies the type of pseudowire for the E-Line service template.
Tunnel Type	Specifies the type of tunnel to be used by the E-Line service to which the template is applied. <ul style="list-style-type: none"> <li>• For pseudowire-based E-Line services, select NONE.</li> <li>• For EVPN-based E-Line services, select a specific tunnel type or ANY.</li> </ul>

4

Configure the Port Filter field to limit the number of ports that will be available to serve as endpoints for the service based on desired criteria.

5

To assign tenants to the service template, click TENANT PERMISSIONS. Add and remove tenants with the permission to use the service template when creating a service, as required.

6

Click CREATE. The system creates the E-Line service template and closes the form.

END OF STEPS

### 14.2.3 To create an E-LAN service template

1

In the Policy Management application, click on Service Templates to expand the template type list and then click E-LAN. The system displays the list of existing E-LAN service templates.

2

Click CREATE TEMPLATE. The Create E-LAN Service Template form opens.

3

Configure the required parameters in the PROPERTIES panel.



**Note:** During the service template configuration, you can click CANCEL at any time to close the form without saving the template.

Parameter	Description
Name	The name of the E-LAN Service template

Parameter	Description
Admin State	Specifies the administrative state required for the service
Mediation Profile	Specifies a Mediation Profile to apply
Tunnel Profile	Specifies a Tunnel Profile to apply
Endpoint QoS Template	Specifies an Endpoint QoS template to apply
Bidirectional	Specifies whether or not a return path is required, and if so, what type of return path should be determined
Optimize on (Objective)	Specifies the primary goal when identifying resources and/or paths for service creation
Max Hop (Span)	Specifies the maximum number of hops to consider
Max Latency (microseconds)	Specifies the maximum latency to consider
Max Cost	Specifies the maximum cost to consider
Monitor Bandwidth	Specifies whether or not to monitor bandwidth
MTU	Specifies the MTU for the service. The range is 0 to 9194
Description	Describes the E-LAN service template
VC Type	Specifies the type of pseudowire for the E-LAN service template
Tunnel Type	Specifies the type of tunnel to be used by the E-LAN service to which the template is applied. <ul style="list-style-type: none"> <li>• For pseudowire-based E-LAN services, select NONE.</li> <li>• For EVPN-based E-LAN services, select a specific tunnel type or ANY.</li> </ul>

4

Configure the Port Filter field to limit the number of ports that will be available to serve as endpoints for the service based on desired criteria.

5

To assign tenants to the service template, click TENANT PERMISSIONS. Add and remove tenants with the permission to use the service template when creating a service, as required.

- 6 \_\_\_\_\_  
 Click CREATE. The system creates the E-LAN service template and closes the form.


END OF STEPS \_\_\_\_\_

### 14.2.4 To create a C-Line service template

- 1 \_\_\_\_\_  
 In the Policy Management application, click on Service Templates to expand the template type list and then click C-Line. The system displays the list of existing C-Line service templates.

- 2 \_\_\_\_\_  
 Click CREATE TEMPLATE. The Create C-Line Service Template form opens.

- 3 \_\_\_\_\_  
 Configure the required parameters in the PROPERTIES panel.

 **Note:** During the service template configuration, you can click CANCEL at any time to close the form without saving the template.

Parameter	Description
Name	The name of the C-Line Service template
Admin State	Specifies the administrative state required for the service
Tunnel Profile	Specifies a Tunnel Profile to apply
Bidirectional	Specifies whether or not a return path is required, and if so, what type of return path should be determined
Optimize on (Objective)	Specifies the primary goal when identifying resources and/or paths for service creation
Max Hop (Span)	Specifies the maximum number of hops to consider
Max Latency (microseconds)	Specifies the maximum latency to consider
Max Cost	Specifies the maximum cost to consider
MTU	Specifies the MTU for the service. The range is 0 to 9194
Description	Describes the C-Line Service template
VC Type	Specifies the type of pseudowire for the C-Line service.

4 \_\_\_\_\_  
 Configure the Port Filter field to limit the number of ports that will be available to serve as endpoints for the service based on desired criteria.

5 \_\_\_\_\_  
 To assign tenants to the service template, click TENANT PERMISSIONS. Add and remove tenants with the permission to use the service template when creating a service, as required.

6 \_\_\_\_\_  
 Click CREATE. The system creates the C-Line service template and closes the form.

END OF STEPS \_\_\_\_\_

### 14.2.5 To create an L3 VPN service template

1 \_\_\_\_\_  
 In the Policy Management application, click on Service Templates to expand the template type list and then click L3 VPN. The system displays the list of existing L3 VPN service templates.

2 \_\_\_\_\_  
 Click CREATE TEMPLATE. The Create L3 VPN Service Template form opens.

3 \_\_\_\_\_  
 Configure the required parameters in the PROPERTIES panel.

**i** **Note:** During the service template configuration, you can click CANCEL at any time to close the form without saving the template.

Parameter	Description
Name	The name of the L3 VPN Service template
Admin State	Specifies the administrative state required for the service
Mediation Profile	Specifies a Mediation Profile to apply
Tunnel Profile	Specifies a Tunnel Profile to apply
Endpoint QoS Template	Specifies an Endpoint QoS template to apply
Tunnel Type	Specifies the tunnel to be used by the service
Bidirectional	Specifies whether or not a return path is required, and if so, what type of return path should be determined

Parameter	Description
Optimize on (Objective)	Specifies the primary goal when identifying resources and/or paths for service creation
Max Hop (Span)	Specifies the maximum number of hops to consider
Max Latency (microseconds)	Specifies the maximum latency to consider
Max Cost	Specifies the maximum cost to consider
MTU	Specifies the MTU for the service. The range is 0 to 9194
Description	Describes the L3 VPN Service template

4

Configure the Port Filter field to limit the number of ports that will be available to serve as endpoints for the service based on desired criteria.

5

To assign tenants to the service template, click TENANT PERMISSIONS. Add and remove tenants with the permission to use the service template when creating a service, as required.

6

Click CREATE. The system creates the L3 VPN service template and closes the form.

END OF STEPS

### 14.2.6 To create an IES service template

1

In the Policy Management application, click on Service Templates to expand the template type list and then click IES. The system displays the list of existing IES service templates.

2

Click CREATE TEMPLATE. The Create IES Template form opens.

3

Configure the required parameters in the PROPERTIES panel.



**Note:** During the service template configuration, you can click CANCEL at any time to close the form without saving the template.

---

Parameter	Description
Name	The name of the IES Service template
Admin State	Specifies the administrative state required for the service
Mediation Profile	Specifies a Mediation Profile to apply
Endpoint QoS Template	Specifies an Endpoint QoS template to apply
MTU	Specifies the MTU for the service. The range is 0 to 9194
Description	Describes the IES Service template

4

---

Configure the Port Filter field to limit the number of ports that will be available to serve as endpoints for the service based on desired criteria.

5

---

To assign tenants to the service template, click TENANT PERMISSIONS. Add and remove tenants with the permission to use the service template when creating a service, as required.

6

---

Click CREATE. The system creates the IES service template and closes the form.

END OF STEPS

---

## 14.2.7 To create an Endpoint QoS template

1

---

In the Policy Management application, click on Service Templates to expand the template type list and then click Endpoint QoS. The system displays the list of existing Endpoint QoS service templates.

2

---

Click CREATE TEMPLATE. The Create Endpoint QoS Template form opens.

3

---

Configure the required parameters:



**Note:** During the service template configuration, you can click CANCEL at any time to close the form without saving the template.

Parameter	Description
Name	The name of the Endpoint QoS template
Description	Describes the Endpoint QoS template
Import QoS Profile	
QoS Profile	Specifies the Generic QoS Profile to be used
QoS Profile Description	Describes the Generic QoS Profile that is in use
QoS Settings	
Ingress QoS	These parameter groups are filled automatically when a QoS profile is imported. Each group includes CoS, CIR, PIR, CBS and MBS values.  The system also displays the Ingress Scheduler and Egress Scheduler details associated with the QoS profile.
Egress QoS	

- 4 \_\_\_\_\_  
 Click CREATE. The system creates the Endpoint QoS service template and closes the form.

END OF STEPS \_\_\_\_\_

### 14.2.8 To create a Generic QoS policy

- 1 \_\_\_\_\_  
 In the Policy Management application, click on Service Templates to expand the template type list and then click Generic QoS Policies. The system displays the list of existing Generic QoS Policies.

- 2 \_\_\_\_\_  
 Click CREATE POLICY. The Create Generic QoS Policy form opens.

- 3 \_\_\_\_\_  
 Configure the required parameters:

**i** **Note:** During the service template configuration, you can click CANCEL at any time to close the form without saving the template.

Parameter	Description
Name	The name of the Generic QoS policy
Description	Describes the Generic QoS policy

Parameter	Description
GQP Id	Specifies the Generic QoS policy identifier
<b>INGRESS</b> panel	
Queue Configurations	Add and configure one or multiple queue configurations, as required.
Ingress Scheduler	Configure an ingress scheduler. Select a scheduler type and configure the CIR and PIR parameters.
Ingress Policies	Select an ingress policy.
<b>EGRESS</b> panel	
Queue Configurations	Add and configure one or multiple queue configurations, as required.
Egress Scheduler	Configure an egress scheduler. Select a scheduler type and configure the CIR and PIR parameters.
Egress Policies	Select an egress policy.

4 \_\_\_\_\_  
 Click CREATE. The system creates the Generic QoS Policy and closes the form.


END OF STEPS \_\_\_\_\_

### 14.2.9 To modify the RD/RT Range policy

1 \_\_\_\_\_  
 In the Policy Management application, click on Service Policies to expand the policy type list and then click RD/RT Range. The system displays a list that contains the RD/RT Range default policy.

2 \_\_\_\_\_  
 Point to the RD/RT Range default policy and then click the EDIT button. The Edit RD/RT Range Policy form opens.

3 \_\_\_\_\_  
 Edit the RD/RT Range default policy, as required:

 **Note:** During the policy editing, you can click CANCEL at any time to close the form without saving the changes.

Parameter	Description
Name	The name of the policy cannot be edited.
Description	Describes the RD/RT Range policy.
<b>Route Distinguisher (RD)</b>	
Type	Specifies the RD type.
Use Provider AS	Specifies whether or not the NSP uses the AS number from the provider network configuration. If confederation is used, then confederation AS will be used.
Administrative Number	Specifies the RD administrative number. Is you enabled the Use Provider AS parameter, the administrative number cannot be edited.
Assigned Number (Min)	Specifies the minimum assigned number. For Type-0, the value must be between 0 and 4294967295, inclusive. For Type-2, the value must be between 0 and 65535, inclusive
Assigned Number (Max)	Specifies the maximum assigned number. For Type-0, the value must be between 0 and 4294967295, inclusive. For Type-2, the value must be between 0 and 65535, inclusive.
<b>Route Target (RT)</b>	
Type	Specifies the RT type.
Use Provider AS	Specifies whether or not the NSP uses the AS number from the provider network configuration. If confederation is used, then confederation AS will be used.
Administrative Number	Specifies the RT administrative number. Is you enabled the Use Provider AS parameter, the administrative number cannot be edited.
Assigned Number (Min)	Specifies the minimum assigned number. For Type-0, the value must be between 0 and 4294967295, inclusive. For Type-2, the value must be between 0 and 65535, inclusive

Parameter	Description
Assigned Number (Max)	Specifies the maximum assigned number. For Type-0, the value must be between 0 and 4294967295, inclusive. For Type-2, the value must be between 0 and 65535, inclusive.

- 4 \_\_\_\_\_  
 Click SAVE. The system saves the RD/RT Range default policy and closes the form.

END OF STEPS \_\_\_\_\_

### 14.2.10 To create a Tunnel Profile policy

- 1 \_\_\_\_\_  
 In the Policy Management application, click on Service Policies to expand the policy type list and then click Tunnel Profile. The system displays a list that contains existing Tunnel Selection policies.

- 2 \_\_\_\_\_  
 Click CREATE POLICY. The Create Tunnel Profile form opens.

- 3 \_\_\_\_\_  
 Configure the required parameters:

**i** **Note:** During the policy creation, you can click CANCEL at any time to close the form without saving the policy.

Parameter	Description
Name	The name of the Tunnel Selection policy
Description	Describes the Tunnel Selection policy
<b>Tunnel Selection Rules</b>	
Use existing tunnels	Specifies whether or not services can ride on top of previously-created NSP tunnels
Expand existing tunnels	Specifies whether or not services can grow previously-created NSP tunnels and get more bandwidth without forcing a re-route (works only if the Use existing tunnels parameter is enabled)

Parameter	Description
Redirect existing tunnels	Specifies whether or not services can force a re-route of previously-created NSP tunnels (works only if the Use existing tunnels parameter is enabled)
Create new tunnels	Specifies whether or not services can create new tunnels
Avoid operational state down	Specifies whether or not the tunnel avoids routers that are operationally down
Book bandwidth in core for ELINE	Specifies whether or not the service can reserve bandwidth in the core (applies only to E-Line services)
<b>Tunnel Creation Rules</b>	
Consumable	Specifies whether or not new services can ride this tunnel
Auto Deletable	Specifies whether or not the tunnel is deleted automatically when the last service is removed from it
Auto Modifiable	Specifies whether or not the tunnel parameters are modifiable due to changes in the services that are riding it
Protected	Specifies whether or not the tunnel has a protection path. The protection path is signaled only after the primary path fails.
Protection Type	You can set the value of this parameter if the Protected parameter was enabled. Specifies the path protection type. The protection path is pre-signaled and available for immediate recovery after a primary path failure.
<b>Tunnel Type Prioritization</b> The Tunnel Type Prioritization panel lists the available tunnel types in the order of their priority level, starting with the highest priority (0). You can modify the tunnel type priority for tunnel profiles. Click and drag a tunnel type to a new position in the list and then release it, as required. To remove a tunnel type from the priority list, drag it under the Not applicable line.	
Strict RSVP	Specifies the priority level for Strict RSVP LSPs
Strict RSVP (PCC)	Specifies the priority level for Strict RSVP PCC LSPs
SR-ISIS	Specifies the priority level for SR-ISIS LSPs

Parameter	Description
SR-OSPF	Specifies the priority level for SR-OSPF LSPs
LDP	Specifies the priority level for LDP tunnels
BGP	Specifies the priority level of BGP tunnels
GRE	Specifies the priority level of GRE tunnels
Strict SR-TE	Specifies the priority level of Strict SR-TE tunnels
Strict SR-TE (PCC)	Specifies the priority level for Strict SR-TE PCC LSPs
Loose RSVP	Specifies the priority level for Loose RSVP LSPs
Loose SR-TE	Specifies the priority level for Loose SR-TE LSPs
FRR Enabled	Enables and disables the FRR protection
<b>Tunnel Endpoint Conditions</b> The Tunnel Endpoint Conditions parameters are only configurable when the “Create New Tunnels” tunnel selection rule is enabled. The Tunnel Endpoint Conditions override the default NSD behavior to use system-ip as the tunnel termination point. Only applicable for SR-SR.	
Target IP address	Specifies the intended tunnel termination IP address
Select Tunnel Type	Specifies the protocol to be used during tunnel deployment; LDP or SR-ISIS
<b>Steering Parameters for Tunnel Selection</b>	
Included	Select steering parameter values to include or to exclude, or both, as required.
Excluded	


4

Click SAVE. The system saves the Tunnel Selection policy and closes the form.

END OF STEPS

---

### 14.2.11 To create a Steering Parameter

- 1 \_\_\_\_\_  
In the Policy Management application, click on Service Policies to expand the policy type list and then click Steering Parameters. The system displays a list that contains existing Steering Parameter policies.
- 2 \_\_\_\_\_  
Click CREATE POLICY. The Create Steering Parameter form opens.
- 3 \_\_\_\_\_  
Configure the name of the Steering Parameter.  
 **Note:** You can click CANCEL at any time to close the form without saving the Steering Parameter.
- 4 \_\_\_\_\_  
Click SAVE. The system saves the Steering Parameter and closes the form.

END OF STEPS \_\_\_\_\_

### 14.2.12 To modify the IP/MPLS Configuration policy

- 1 \_\_\_\_\_  
In the Policy Management application, click on IP/MPLS Policies to expand the policy type list and then click Configuration. The system displays a list that contains a single entry: the System IP MPLS Configuration default policy.
- 2 \_\_\_\_\_  
Point to the the System IP MPLS Configuration default policy and then click the EDIT button. The Edit the System IP MPLS Configuration form opens.
- 3 \_\_\_\_\_  
Edit the System IP MPLS Configuration default policy, as required.

Parameter	Description
Description	Specifies the description of the System IP MPLS Configuration default policy
Maintenance Mode	Specifies the IP/MPLS maintenance mode: Manual or Automatic

END OF STEPS \_\_\_\_\_

### 14.2.13 To create a Router ID Mapping policy

1 \_\_\_\_\_  
 In the Policy Management application, click on IP/MPLS Policies to expand the policy type list and then click Router ID Mapping. The system displays a list that contains existing Router ID Mapping policies.

2 \_\_\_\_\_  
 Click CREATE POLICY. The Create Router ID Mapping Policy form opens.

3 \_\_\_\_\_  
 Configure the required parameters:

**i** **Note:** During the policy creation, you can click CANCEL at any time to close the form without saving the policy.

Parameter	Description
Name	Specifies the name of the Router ID Mapping template
System IP Address	Specifies the system IP address of the router
System Name	Specifies the router system name
PCC Address	Specifies the address of the PCC associated with the router
Description	Specifies the router description
Router Info	Click ADD to add as many Router Info entries, as required. For each Router Info entry, you must specify the following information: <ul style="list-style-type: none"> <li>• Network Identifier</li> <li>• AS Number</li> <li>• BGP-LS ID (topology identifier)</li> <li>• Router ID</li> <li>• Protocol (the protocol that the IGP router is using)</li> </ul>

4 \_\_\_\_\_  
 Click SAVE. The system saves the Router ID Mapping policy and closes the form.

END OF STEPS \_\_\_\_\_

### 14.2.14 To create a Path Profile policy

1 \_\_\_\_\_

In the Policy Management application, click on IP/MPLS Policies to expand the policy type list and then click Path Profile. The system displays a list that contains existing Path Profile policies.

2 \_\_\_\_\_

Click CREATE POLICY. The Create Path Profile Policy form opens.

3 \_\_\_\_\_

Configure the required parameters:



**Note:** During the policy creation, you can click CANCEL at any time to close the form without saving the policy.

Parameter	Description
Reserved Profile ID	When this parameter is enabled, the Path Profile template assumes the Name and role of the default Path Profile template
Name	The name of the Path Profile template
Profile ID	The Profile ID of the paths to be included in path computation
Bidirectional	The bidirectional mode to be used in path computation
Disjoint	The Disjoint mode to be used in path computation
Optimize on (Objective)	Specifies the primary goal when identifying paths for path computation
Explicit Route Strategy	Specifies the explicit route strategy for the service
Control Reroute Strategy	Specifies the control reroute strategy to apply to the service
Max Hop (Span)	Specifies the Max Hops constraint to be used in path computation
Max Cost	Specifies the Max Cost constraint to be used in path computation
Max TE Metric	Specifies the Max TE Metric constraint to be used in path computation
Max Latency	Specifies the maximum latency to consider

Parameter	Description
Latency Threshold	Specifies when to re-signal an LSP that is optimized on latency. If no change in latency (0), re-signal is automatically triggered. If the change is less than 0, the LSP is not re-signalled. If the change is greater than 0, the LSP is re-signalled. The default value is -1.
Description	Describes the Path Profile template
Exclude Route Objects	Click ADD to add as many route objects to exclude as you need. You must specify the IP address and the hop type for each route object.
Include Route Objects	Click ADD to add as many route objects to include as you need. You must specify the IP address for each route object.

4

Click SAVE. The system saves the Path Profile policy and closes the form.

END OF STEPS

### 14.2.15 To create a Mediation Profile

The creation of mediation profiles is possible only if the appropriate augmentation files are predefined and available on the NSD. Before you start creating a mediation profile, complete the following steps:

1. Create the json augmentation files that describe the additional properties required for the mediation profile.
2. Store the json augmentation files in the NSD database by using the REST endpoint defined for this purpose.
3. Create a custom script to implement the desired service configuration. The script uses the augmented properties defined in the json files to apply the service configuration.
4. Copy the custom script to the appropriate location and install it.

**i** **Note:** The prerequisite steps can be different for your deployment, depending on the system that manages your NEs: MDM or NFM-P.

1

In the Policy Management application, click on Mediation Profiles to expand the policy type list, and then click on Mediation Profile. The system displays a list that contains existing mediation profiles.

**2** \_\_\_\_\_  
 Click CREATE PROFILE. The Create Mediation Profile form opens.

**3** \_\_\_\_\_  
 Configure the required parameters.

Parameter	Description
Name	Specifies the name of the Router ID Mapping template
Description	Specifies the router description
Service Type	Select a service type: <ul style="list-style-type: none"> <li>• E-LAN</li> <li>• E-Line</li> <li>• L3 VPN</li> </ul>
Mediation Info	Click ADD to add as many Mediation Info items as you need. You must specify the following details for each Mediation Info item: <ul style="list-style-type: none"> <li>• Mediation Profile</li> <li>• Mediation Version</li> <li>• Global Template Name</li> </ul>

**4** \_\_\_\_\_  
 Click SAVE. The system saves the Mediation Profile and closes the form. The NSD adds the new mediation profile to the list of profiles that you can select when creating a service template for the selected service.

END OF STEPS \_\_\_\_\_

### 14.2.16 To create a Workflow Profile

**1** \_\_\_\_\_  
 In the Policy Management application, click on Mediation Profiles to expand the policy type list, and then click on Workflow Profiles. The system displays a list of existing workflow profiles.

**2** \_\_\_\_\_  
 Click CREATE PROFILE. The Create Workflow Profile form opens.

---

**3**

Configure the required parameters.

Parameter	Description
Name	Specifies the name of the workflow profile
Description	Specifies the workflow profile description

---

**4**

In the Workflow Profile Information section, use the drop-down menus to specify the actions to be taken in the following scenarios:

Workflow profile is created

- Pre-deployment
- Post-deployment success
- Post-deployment failure

Workflow profile is updated

- Pre-deployment
- Post-deployment success
- Post-deployment failure

Workflow profile is deleted

- Pre-deployment
- Post-deployment success
- Post-deployment failure

---

**5**

Click CREATE. The Create Workflow Profile form closes and the new workflow profile can be selected when creating or updating an E-Line service template.

**END OF STEPS**

---

---

## 15 Service Fulfillment

### 15.1 About

#### 15.1.1

The Service Fulfillment application allows for multi-vendor service provisioning and activation across all networks accessible to the NSD. It authorizes northbound interface (NBI) service requests, executes routing algorithms that allocate network resources for these services, and then deploys the services to the network. Network deployment is performed through the mediation framework. The Service Fulfillment application can use existing tunnels or create new tunnels to satisfy service demands. The services that can be provisioned from the Service Fulfillment application include L3 VPN, C-Line, E-LAN and E-Line services.

The Service Fulfillment application also provides an abstract, real-time view of the network resources that can be consumed by services, allowing service providers and end users to interact with the network through simple APIs, and to programmatically control the network. Network abstraction is used to simplify how the network appears to the IT/OSS layer. This allows services to be defined and enhanced more quickly by presenting only the subset of network services and endpoints that are relevant to a specific application, thereby greatly reducing the complexity the application is exposed to.

After a service request has been communicated through simple RESTful APIs, or through the Service Fulfillment application, the NSD uses operator-defined policies to guide dynamic network resource selection and automated provisioning. These policies use a real-time view of the network (including link and tunnel utilization) to map service connection requests to the best available tunnels/paths (Layer 0 to Layer 3) that meet the customer's Service Level Agreement (SLA) requirements and the operator's network efficiency goals. For example, the NSD can track booking and use real-time network KPIs to assess whether existing tunnels/paths are congested. If so, the NSD uses operator-defined policies to bind incoming service requests to less utilized paths that provide approximately the same connection attributes. It can revert the services to the optimal paths when demand subsides. If no path that meets the requested attributes is available, the NSD asks the relevant NRC module to compute a new path.

**i** **Note:** For IP-only deployments, the NSD must integrate with the NFM-P, CPAM, vCPAA, and VSR-NRC. For optical-only deployments, the NSD must integrate with NFM-T.

### 15.2 Getting started

#### 15.2.1 To create physical links between ports

You can use the Service Fulfillment application to create a physical link between ports. You can also use the REST APIs of the NSD and NRC modules for the same purpose. For more information, see the *NSP Developer portal*.

Physical links exist only in the NSD database; nothing is provisioned to the NFM-P or NFM-T. The operational state of one or both the linked ports determines the operational state of the physical link. Updates to the link may be required when the port operational state changes. The NSD can

---

also be used to delete physical links that have been created using the NSD.

- 1 \_\_\_\_\_  
On the Inventory page of the Service Fulfillment application, click Physical Links. The application displays a list of existing physical links.
- 2 \_\_\_\_\_  
Click CREATE LINK. The Create Physical Link form opens.
- 3 \_\_\_\_\_  
Click on SELECT PORTS, and search for available ports. You can search for a specific port by NE Name or Port Name.
- 4 \_\_\_\_\_  
Select the desired ports one at a time and click DONE after you added all the required ports..
- 5 \_\_\_\_\_  
Click CREATE. The system creates the physical link.

END OF STEPS \_\_\_\_\_

## 15.3 Service provisioning

### 15.3.1

This section describes the provisioning of services using the Service Fulfillment application.

- [15.3.2 "To enable service CAC" \(p. 162\)](#)
- [15.3.3 "To provision E-LAN services" \(p. 163\)](#)
- [15.3.4 "To provision E-Line services" \(p. 166\)](#)
- [15.3.5 "To provision C-Line services" \(p. 170\)](#)
- [15.3.6 "To provision L3 VPN services" \(p. 173\)](#)
- [15.3.7 "To provision IES services" \(p. 176\)](#)

### 15.3.2 To enable service CAC

- 1 \_\_\_\_\_  
On your NSD and NRC server, navigate to the following directory: `/opt/nsp/server/tomcat/webapps/sdn/WEB-INF/config/`
- 2 \_\_\_\_\_  
Modify the system.config file as follows:

---

```
algo
{
  serviceCAC="on"

  multiVendorServiceCAC = "on"
}
```

- 3 

---

 Save your changes and close the system.config file.

END OF STEPS 


---

### 15.3.3 To provision E-LAN services

- 1 

---

 In the Service Fulfillment application, click on the SERVICES tab and then click on START SERVICE CREATION.

 **Note:** You can also enter the general configuration information for the service, such as the service name and type, before clicking START SERVICE CREATION. If you do that, then skip the next step.

#### General configuration

- 2 

---

 Enter the general configuration information for the new service.
1. Type a name for the service.
  2. Select E-LAN as the Service Type.
  3. Select a tenant for the service, as required.
  4. If required, select a template to apply to the service.

#### Service parameters

- 3 

---

 Click ADDITIONAL PROPERTIES to configure the service parameters. The Additional Properties form opens. Configure the parameters, as required.

Parameter	Description
Description	Describes the service.

Parameter	Description
Tunnel Profile	Specifies the Tunnel Profile (also known as a policy) to apply to the service.
Path Profile	Specifies the path profile to be used by the service.
Admin State	Specifies the current administrative state of the service.
Bidirectional	Specifies whether or not a return path is required, and if so, what type of return path should be determined. Select one of the following options: Symmetric Reverse Route Preferred or Any Reverse Route.
Objective	Specifies the primary goal when identifying resources and/or paths for service creation. Select one of the following options: Latency, Hops (Span) or Cost.
MTU	Specifies the MTU for the service. The range is 0 to 9194.
Maximum Hops	Specifies the maximum number of hops to consider.
Maximum Latency	Specifies the maximum latency to consider.
Maximum Cost	Specifies the maximum cost to consider.
Enable EVPN Tunnel Selection	Enables the configuration of an EVPN-based E-LAN service, so that you can select a tunnel type from the following options: LDP, RSVP-TE, SR-ISIS, SR-OSPF, SR-TE, and BGP. The ANY option indicates to the NSD that any supported tunnel type in the EVPN context can be selected in the order of preference.

4 \_\_\_\_\_  
Click OK. The Additional Properties form closes.

5 \_\_\_\_\_  
Click CONTINUE. The service configuration focus moves to the endpoint configuration area.

## Endpoints

6 \_\_\_\_\_  
Select a topology type. Your topology type selection (Full Mesh or Hub and Spoke) determines the endpoint selection.

7 \_\_\_\_\_  
Select the service endpoints.

1. Click SELECT PORTS to display the list of available endpoints.

2. If required, use the drop-down menu and the text box at the top of the list to filter the available endpoints by NE name or port.
3. Select a service endpoint: move the mouse pointer to the right of the endpoint entry and click the required selection icon.  
Perform this step to select additional endpoints, as required.
4. Click DONE after selecting the endpoints.
5. If required, click VIEW ENDPOINT LIST to display the list of selected endpoints. To return to the map view, click VIEW SERVICE MAP.

**8**

Click CONTINUE. The system checks the selected endpoints and informs you that the endpoint is missing required values. You need to perform additional configuration on each endpoint.

**9**

Click the endpoint entry and click the Edit icon. The port configuration form opens.

**10**

Configure the required endpoint parameters.

Parameter	Description
Admin State	Specifies the current administrative state of the endpoint
Outer Tag	Specifies the outer tag. Applicable to Dot1Q or QinQ ports.
Inner Tag	Specifies the inner tag. Applicable to Dot1Q or QinQ ports.
QoS Profile Name	Specifies the QoS Profile to be used

**11**

If a QoS Profile was specified in the previous step, click SHOW QOS SETTINGS to view the QoS settings applied by the profile.

**12**

Click OK. The endpoint configuration form closes.

Perform the additional configuration steps for each service endpoint. When all the service endpoints are correctly configured, continue to the next step.

**13**

Click CONTINUE. The system displays the service configuration summary so that you can review it.

---

## Configuration review

14

Review the service configuration summary. You can click the Map icon to view the service representation in the map.

15

Perform one of the following tasks:

- a. If the service configuration is correct, click **DEPLOY**. The system attempts to deploy the service, and displays a message to inform you that the service was successfully created or that there are service configuration errors. Investigate the errors, correct the service configuration and deploy the service again.
- b. If you want to save the service without deploying it, click **SAVE**. A saved service does not reserve any bandwidth and network resources, and the system checks the availability of resources for a saved service only at deployment time.
- c. If you need to modify the service configuration, click **BACK** to go to previous service configuration steps, as required.

END OF STEPS

---

### 15.3.4 To provision E-Line services

1

In the Service Fulfillment application, click on the **SERVICES** tab and then click on **START SERVICE CREATION**.



**Note:** You can also enter the general configuration information for the service, such as the service name and type, before clicking **START SERVICE CREATION**. If you do that, then skip the next step.

## General configuration

2

Enter the general configuration information for the new service.

1. Type a name for the service.
2. Select E-Line as the Service Type.
3. Select a tenant for the service, as required.
4. If required, select a template to apply to the service.

## Service parameters

### 3

Click **ADDITIONAL PROPERTIES** to configure the service parameters. The Additional Properties form opens. Configure the parameters, as required.

Parameter	Description
Description	Describes the service.
Tunnel Profile	Specifies the Tunnel Profile (also known as a policy) to apply to the service
Path Profile	Specifies the path profile to be used by the service.
Diverse From	Specifies an existing NSD-managed E-Line service for the new E-Line service to be diverse from. As a result, the new E-Line creates LSPs with the same path profile and group ID as the LSPs used in the specified E-Line.
Admin State	Specifies the current administrative state of the service
Bidirectional	Specifies whether or not a return path is required, and if so, what type of return path should be determined. Select one of the following options: Symmetric Reverse Route Preferred or Any Reverse Route.
Objective	Specifies the primary goal when identifying resources and/or paths for service creation. Select one of the following options: Latency, Hops (Span) or Cost.
MTU	Specifies the MTU for the service. The range is 0 to 9194.
Maximum Hops	Specifies the maximum number of hops to consider
Maximum Latency	Specifies the maximum latency to consider
Maximum Cost	Specifies the maximum cost to consider

Parameter	Description
Enable EVPN Tunnel Selection	Enables the configuration of an EVPN-based E-Line service, so that you can select a tunnel type from the following options: LDP, RSVP-TE, SR-ISIS, SR-OSPF, SR-TE, and BGP. The ANY option indicates to the NSD that any supported tunnel type in the EVPN context can be selected in the order of preference.

4 \_\_\_\_\_  
Click OK. The Additional Properties form closes.

5 \_\_\_\_\_  
Click CONTINUE. The service configuration focus moves to the endpoint configuration area.

## Endpoints

6 \_\_\_\_\_

Select the service endpoints.

1. Click SELECT PORTS to display the list of available endpoints.
2. If required, use the drop-down menu and the text box at the top of the list to filter the available endpoints by NE name or port.
3. Select a service endpoint: move the mouse pointer to the right of the endpoint entry and click the required selection icon.  
Perform this step to select additional endpoints, as required.
4. Click DONE after selecting the endpoints.
5. If required, click VIEW ENDPOINT LIST to display the list of selected endpoints. To return to the map view, click VIEW SERVICE MAP.

7 \_\_\_\_\_  
Click CONTINUE. The system checks the selected endpoints and informs you that the endpoint is missing required values. You need to perform additional endpoint configuration.

8 \_\_\_\_\_  
Move the mouse pointer to the right of the endpoint entry and click the Edit icon. The port configuration form opens.

9

Configure the required endpoint parameters.

Parameter	Description
Admin State	Specifies the current administrative state of the endpoint
Outer Tag	Specifies the outer tag. Applicable to Dot1Q or QinQ ports.
Inner Tag	Specifies the inner tag. Applicable to Dot1Q or QinQ ports.
QoS Profile Name	Specifies the QoS Profile to be used

10

If a QoS Profile was specified in the previous step, click SHOW QOS SETTINGS to view the QoS settings applied by the profile.

11

Click SAVE. The endpoint configuration form closes.

Perform the additional configuration steps for each service endpoint. When all the service endpoints are correctly configured, continue to the next step.

12

Click CONTINUE. The system displays the service configuration summary so that you can review it.

## Configuration review

13

Review the service configuration summary. You can click the Map icon to view the service representation in the map.

14

Perform one of the following tasks:

- a. If the service configuration is correct, click DEPLOY. The system attempts to deploy the service, and displays a message to inform you that the service was successfully created or that there are service configuration errors. Investigate the errors, correct the service configuration and deploy the service again.
- b. If you want to save the service without deploying it, click SAVE. A saved service does not reserve any bandwidth and network resources, and the system checks the availability of resources for a saved service only at deployment time.
- c. If you need to modify the service configuration, click BACK to go to previous service

configuration steps, as required.

END OF STEPS

### 15.3.5 To provision C-Line services

1

In the Service Fulfillment application, click on the SERVICES tab and then click on START SERVICE CREATION.

**i** **Note:** You can also enter the general configuration information for the service, such as the service name and type, before clicking START SERVICE CREATION. If you do that, then skip the next step.

#### General configuration

2

Enter the general configuration information for the new service.

1. Type a name for the service.
2. Select C-Line as the Service Type.
3. Select a tenant for the service, as required.
4. If required, select a template to apply to the service.

#### Service parameters

3

Click ADDITIONAL PROPERTIES to configure the service parameters. The Additional Properties form opens. Configure the parameters, as required.

Parameter	Description
Description	Describes the service.
Tunnel Profile	Specifies the Tunnel Profile to apply to the service
Include RTP Header	Enables the inclusion of CEM RTP across the IP/MPLS core network
Admin State	Specifies the current administrative state of the service
Bidirectional	Specifies whether or not a return path is required, and if so, what type of return path should be determined

Parameter	Description
Maximum Hops	Specifies the maximum number of hops to consider
Maximum Latency	Specifies the maximum latency to consider
Maximum Cost	Specifies the maximum cost to consider
Objective	Specifies the primary goal when identifying resources and/or paths for service creation. Select one of the following options: Latency, Hops (Span) or Cost.
MTU	Specifies the MTU for the service. The range is 0 to 9194.

4

Click OK. The Additional Properties form closes.

5

Click CONTINUE. The service configuration focus moves to the endpoint configuration area.

## Endpoints

6

Select a VC Type option. This specifies the type of pseudowire for the C-Line service.

7

Select the service endpoints.

1. Click SELECT PORTS to display the list of available endpoints.
2. If required, use the drop-down menu and the text box at the top of the list to filter the available endpoints by NE name or port.
3. Select a service endpoint: move the mouse pointer to the right of the endpoint entry and click the required selection icon.  
Perform this step to select additional endpoints, as required.
4. Click DONE after selecting the endpoints.
5. If required, click VIEW ENDPOINT LIST to display the list of selected endpoints. To return to the map view, click VIEW SERVICE MAP.

8

Click CONTINUE. The system checks the selected endpoints and informs you that the endpoint is missing required values. You need to perform additional endpoint configuration.

**9** \_\_\_\_\_  
Click on the endpoint. The port configuration form opens.

**10** \_\_\_\_\_  
Configure the required endpoint parameters.

Parameter	Description
Admin State	Specifies the current administrative state of the endpoint
Time Slots	Specifies the time slot to be used by the service.
QoS Profile Name	Specifies the QoS Profile to be used

**11** \_\_\_\_\_  
If a QoS Profile was specified in the previous step, click SHOW QOS SETTINGS to view the QoS settings applied by the profile.

**12** \_\_\_\_\_  
Click SAVE. The endpoint configuration form closes.  
Perform the additional configuration steps for each service endpoint. When all the service endpoints are correctly configured, continue to the next step.

**13** \_\_\_\_\_  
Click CONTINUE. The system displays the service configuration summary so that you can review it.

### Configuration review

**14** \_\_\_\_\_  
Review the service configuration summary. You can click the Map icon to view the service representation in the map.

**15** \_\_\_\_\_  
Perform one of the following tasks:

- a. If the service configuration is correct, click DEPLOY. The system attempts to deploy the service, and displays a message to inform you that the service was successfully created or that there are service configuration errors. Investigate the errors, correct the service configuration and deploy the service again.
- b. If you want to save the service without deploying it, click SAVE. A saved service does not reserve any bandwidth and network resources, and the system checks the availability of resources for a saved service only at deployment time.
- c. If you need to modify the service configuration, click BACK to go to previous service

configuration steps, as required.

END OF STEPS

### 15.3.6 To provision L3 VPN services

1

In the Service Fulfillment application, click on the SERVICES tab and then click on START SERVICE CREATION.



**Note:** You can also enter the general configuration information for the service, such as the service name and type, before clicking START SERVICE CREATION. If you do that, then skip the next step.

#### General configuration

2

Enter the general configuration information for the new service.

1. Type a name for the service.
2. Select L3 VPN as the Service Type.
3. Select a tenant for the service, as required.
4. If required, select a template to apply to the service.

#### Service parameters

3

Click ADDITIONAL PROPERTIES to configure the service parameters. The Additional Properties form opens. Configure the following parameters, as required.

Parameter	Description
Description	Describes the service.
Tunnel Profile	Specifies the Tunnel Profile to apply to the service.
Path Profile	Specifies a path profile for the service.
Admin State	Specifies the current administrative state of the service
Bidirectional	Specifies whether or not a return path is required, and if so, what type of return path should be determined

Parameter	Description
Objective	Specifies the primary goal when identifying resources and/or paths for service creation. Select one of the following options: Latency, Hops (Span) or Cost.
Encryption	Specifies whether or not IP VPN encryption is enabled.
Tunnel Type	Specifies the type of tunnel to be used by the E-Line service.
MTU	Specifies the MTU for the service. The range is 0 to 9194
Maximum Hops	Specifies the maximum number of hops to consider
Maximum Latency	Specifies the maximum latency to consider
Maximum Cost	Specifies the maximum cost to consider

4

Click OK. The Additional Properties form closes.

5

Click CONTINUE. The service configuration focus moves to the endpoint configuration area.

## Endpoints

6

Select the Topology Type for the service. Your topology type selection (Full Mesh or Hub and Spoke) determines the endpoint selection.

7


Select the service endpoints.

1. Click SELECT PORTS to display the list of available endpoints.
2. If required, use the drop-down menu and the text box at the top of the list to filter the available endpoints by NE name or port.
3. Select a service endpoint: move the mouse pointer to the right of the endpoint entry and click the required selection icon.  
Perform this step to select additional endpoints, as required.
4. Click DONE after selecting the endpoints.
5. If required, click VIEW ENDPOINT LIST to display the list of selected endpoints. To return to the map view, click VIEW SERVICE MAP.

8 \_\_\_\_\_  
Click CONTINUE. The system checks the selected endpoints and informs you that the endpoint is missing required values. You need to perform additional endpoint configuration.

9 \_\_\_\_\_  
Click on the endpoint entry. The port configuration form opens.

10 \_\_\_\_\_  
Configure the required endpoint parameters.

 **Note:** The endpoint configuration supports both IPv4 and IPv6 addresses.

Parameter	Description
Interface Name	The name of the service interface. Maximum of 32 characters. Must begin with a letter.
Admin State	Specifies the current administrative state of the endpoint
Outer Tag	Specifies the outer tag. Applicable to Dot1Q or QinQ ports.
Inner Tag	Specifies the inner tag. Applicable to Dot1Q or QinQ ports.
Primary IP Address	Specifies the primary IP address assigned to the service endpoint.
Secondary Addresses	Add as many valid IP addresses as required using the Add (+) icon.
Static Routes	Add as many static routes as required using the Add (+) icon. Specify the destination network IP address and subnet mask of the static route assigned to the service endpoint
eBGP Peers	Add as many eBGP peers as required using the Add (+) icon, and specify the IP address and the AS for each eBGP peer.
QoS Profile Name	Specifies the QoS Profile to be used

11 \_\_\_\_\_  
If a QoS Profile was specified in the previous step, click SHOW QOS SETTINGS to view the QoS settings applied by the profile.

12 \_\_\_\_\_  
Click SAVE. The endpoint configuration form closes.  
Perform the additional configuration steps for each service endpoint. When all the service endpoints are correctly configured, continue to the next step.

---

13

Click CONTINUE. The system displays the service configuration summary so that you can review it.

## Configuration review

---

14

Review the service configuration summary. You can click the Map icon to view the service representation in the map.

---

15

Perform one of the following tasks:

- a. If the service configuration is correct, click DEPLOY. The system attempts to deploy the service, and displays a message to inform you that the service was successfully created or that there are service configuration errors. Investigate the errors, correct the service configuration and deploy the service again.
- b. If you want to save the service without deploying it, click SAVE. A saved service does not reserve any bandwidth and network resources, and the system checks the availability of resources for a saved service only at deployment time.
- c. If you need to modify the service configuration, click BACK to go to previous service configuration steps, as required.

---


END OF STEPS

### 15.3.7 To provision IES services

---

1

In the Service Fulfillment application, click on the SERVICES tab and then click on START SERVICE CREATION.

 **Note:** You can also enter the general configuration information for the service, such as the service name and type, before clicking START SERVICE CREATION. If you do that, then skip the next step.

## General configuration

---

2

Enter the general configuration information for the new service.

1. Type a name for the service.
2. Select IES as the Service Type.
3. Select a tenant for the service, as required.
4. If required, select a template to apply to the service.

## Service parameters

3

Click **ADDITIONAL PROPERTIES** to configure the service parameters. The Additional Properties form opens. Configure the following parameters, as required.

Parameter	Description
Description	Describes the service.
Admin State	Specifies the current administrative state of the service
MTU	Specifies the MTU for the service. The range is 0 to 9194

4

Click **OK**. The Additional Properties form closes.

5

Click **CONTINUE**. The service configuration focus moves to the endpoint configuration area.

## Endpoints

6

Select the service endpoints.

1. Click **SELECT PORTS** to display the list of available endpoints.
2. If required, use the drop-down menu and the text box at the top of the list to filter the available endpoints by NE name or port.
3. Select a service endpoint: move the mouse pointer to the right of the endpoint entry and click the required selection icon.  
Perform this step to select additional endpoints, as required.
4. Click **DONE** after selecting the endpoints.
5. If required, click **VIEW ENDPOINT LIST** to display the list of selected endpoints. To return to the map view, click **VIEW SERVICE MAP**.

7

Click **CONTINUE**. The system checks the selected endpoints and informs you that the endpoint is missing required values. You need to perform additional endpoint configuration.

8

Click on the endpoint entry. The port configuration form opens.

9

Configure the required endpoint parameters.

**i** **Note:** The endpoint configuration supports both IPv4 and IPv6 addresses.

Parameter	Description
Interface Name	The name of the service interface. Maximum of 32 characters. Must begin with a letter.
Admin State	Specifies the current administrative state of the endpoint
Primary IP Address	Specifies the primary IP address assigned to the service endpoint.
Secondary Addresses	Add as many valid IP addresses as required using the Add (+) icon.
Static Routes	Add as many static routes as required using the Add (+) icon. Specify the destination network IP address and subnet mask of the static route assigned to the service endpoint
QoS Profile Name	Specifies the QoS Profile to be used

10

If a QoS Profile was specified in the previous step, click SHOW QOS SETTINGS to view the QoS settings applied by the profile.

11

Click SAVE. The endpoint configuration form closes.

Perform the additional configuration steps for each service endpoint. When all the service endpoints are correctly configured, continue to the next step.

12

Click CONTINUE. The system displays the service configuration summary so that you can review it.

### Configuration review

13

Review the service configuration summary. You can click the Map icon to view the service representation in the map.

14

Perform one of the following tasks:

- a. If the service configuration is correct, click DEPLOY. The system attempts to deploy the

---

service, and displays a message to inform you that the service was successfully created or that there are service configuration errors. Investigate the errors, correct the service configuration and deploy the service again.

- b. If you want to save the service without deploying it, click **SAVE**. A saved service does not reserve any bandwidth and network resources, and the system checks the availability of resources for a saved service only at deployment time.
- c. If you need to modify the service configuration, click **BACK** to go to previous service configuration steps, as required.

**END OF STEPS**

---

## 15.4 Service management

### 15.4.1

This section describes the management of existing services and service components using the Service Fulfillment application.

[15.4.2 "To view and edit a service" \(p. 178\)](#)

[15.4.3 "To view all services and edit a service" \(p. 180\)](#)

[15.4.4 "To manage service tunnel bandwidth" \(p. 181\)](#)

### 15.4.2 To view and edit a service

**1**

---

On the **SERVICES** tab, click in the Search for a service box. The system displays a drop-down list of the existing services.

If you know the service name or part of it, start typing it in the Search for a service box. The system filters the list of services and shows only the service names that contain the characters that you typed.

**2**

---

Click on a service. The system displays general information about the service in the Service Info panel and highlights the service on the map.

**3**

---

You can now view and modify service details. Click one of the following buttons:

a. **EDIT**

The Edit Service page opens. You can modify the service properties and endpoints.

b. **SERVICE MAP**

The Service Map page opens. You can click on the map elements to view information about the service and its components.


c. **SERVICE ENDPOINTS**

---

The Service Endpoints page opens. The endpoints defined are listed in a table. Click on an endpoint to view details about it.

d. OPEN IN NFM-T

The service is displayed in the NFM-T application.

 **Note:** Some of the listed options might not be available on your system.

END OF STEPS

---

### 15.4.3 To view all services and edit a service

1

On the SERVICES tab, click on the All Services icon. The system displays the list of all created services.

2

Click on a service. The system displays general information about the service in the Info panel.

3

Point to a service and then click one of the following buttons:

a. Edit

The Edit Service page opens. You can modify the service properties and endpoints.

b. View Service Map

The Service Map page opens. You can click on the map elements to view information about the service and its components.

c. View Endpoints

The Service Endpoints page opens. The endpoints associated with the service are listed in a table. Click on an endpoint to view details about it.

d. More...→Manage Tenants

The system opens the Manage Tenants form, in which you can add tenants to the service.

e. More...→Delete

The system prompts you to confirm your choice and then deletes the service.

f. More...→Open in Service Supervision

The service is displayed in the Service Supervision application. For details about the tasks that you can perform on the service, see the documentation for the Service Supervision application.

END OF STEPS

---

---

## 15.4.4 To manage service tunnel bandwidth

You can modify the parameters of a discovered brownfield service tunnel in the Service Fulfillment application. This enables you to support services with bandwidth booking in the core and to restrict or to allow for consumption, modification and deletion in a different way from how the service tunnels were discovered.

**i** **Note:** The brownfield service tunnel are tunnels created previously in the NFM-P that you can discover and then use with services created in the NSD and NRC.

You can manage the service tunnel bandwidth by modifying the values of the following parameters:

- Consumable

This parameter controls whether the tunnel can be used or not for creating services in the NSD and NRC. By default, all greenfield and brownfield service tunnels have the Consumable parameter enabled. Disable the Consumable parameter to prevent the services created in the NSD and NRC from using the service tunnel.

- Auto Modifiable

This parameter allows you to give the NSD and NRC full control of the available bandwidth on the service tunnel. When you enable the Auto Modifiable parameter, the NSD and NRC calculates the available bandwidth automatically and, as a result, the Available Bandwidth parameter is not modifiable anymore. Now the NSD and NRC treat the brownfield service tunnel as a green field tunnel, except the tunnel cannot be deleted in the NSD and NRC.

- Available Bandwidth

This parameter allows you to set how much bandwidth is available to the NSD and NRC to use on a brownfield service tunnel. Then you must use the same bandwidth values when creating a service that uses the service tunnel. When the service is deleted, the available bandwidth on the service tunnel reverts to the previous value.

**i** **Note:** You must perform the bandwidth management tasks on the service tunnel for both tunnel directions.

1 \_\_\_\_\_  
In the Service Fulfillment application, click on the INVENTORY tab, and then click Service Tunnels. The system displays a table with the available service tunnels.

2 \_\_\_\_\_  
Search for the service tunnel that you need to manage.  
You can filter the service tunnels displayed in the list by Tunnel Name, Source Node, Destination Node and Transport type. Just type numbers or characters, or both, in the search boxes and the system filters dynamically the services that meet your criteria.

3 \_\_\_\_\_  
Click on a service tunnel. The system displays information about the service tunnel in the Info panel.

---

**4** \_\_\_\_\_  
Click Edit. The Manage Service Tunnel form opens.

**5** \_\_\_\_\_  
Modify the bandwidth management parameters of the service tunnel, as required.

**6** \_\_\_\_\_  
Click SAVE. The service tunnel modifications are saved.

**END OF STEPS** \_\_\_\_\_

## 16 Task Scheduler

### 16.1 About

#### 16.1.1

The Task Scheduler application enables users to do CRUD operations with respect to scheduling bandwidth modification requests/tasks on an existing E-Line service. The user is able to schedule a one time, or repeatable service modification request (such as bandwidth modification) for their E-Line service. After accepting a scheduled task, the application allows the end user to view, modify, or delete existing tasks. In the case of modification, the user can change both the start date and the task execution intervals. The user can view all of their current requests and the state of those requests (Scheduled / Running / Disabled). The user can see a historical log of all executed tasks and their Success/Fail status and results.

### 16.2 Bandwidth modification

#### 16.2.1

This section describes the scheduling of bandwidth modification tasks using the Task Scheduler application.

[16.2.2 "To schedule bandwidth modification tasks" \(p. 183\)](#)

#### 16.2.2 To schedule bandwidth modification tasks

1 \_\_\_\_\_

In the Task Scheduler application, click CREATE TASK. The Create Bandwidth Modifications Task form opens.

2 \_\_\_\_\_

Configure the required parameters:

Parameter	Description
Task Name	The name of the task
Start Time	The execution time of the task
End Time	The termination time of the task
Repeat	Specifies at what interval the task repeats, if at all

3

If the Repeat parameter was set to *Never* in [Step 2](#), configure the following parameters:

Parameter	Description
Starts At	The execution date of the task
Ends At	The termination date of the task

4

If the Repeat parameter was set to *Daily* or *Weekly* in [Step 2](#), configure the following parameters:

Parameter	Description
Expiry Type	The termination policy of the task
Recur Every	The interval between every recurrence
Recurrence Start Date	The start date of the recurrence

5

If the Repeat parameter was set to *Monthly* in [Step 2](#), configure the following parameters:

Parameter	Description
Expiry Type	The termination policy of the task
Recur Every [month(s)]	The interval between every recurrence
Recur Every (day of month)	The day of the month on which the task is executed
Recurrence Start Date	The start date of the recurrence

6

Select a service for which to schedule a bandwidth modification task.

7

Configure the required parameters for both Endpoint 1 and Endpoint 2:

Parameter	Description
Generic QoS Profile	Specifies the Generic QoS Profile to be used
CIR	Specifies the Committed Information Rate in Kbps.
PIR	Specifies the Peak Information Rate in Kbps.
CBS	Specifies the Committed Burst Size in KB.

---

Parameter	Description
MBS	Specifies the Maximum Burst Size in KB.

8

Click Submit. The bandwidth modification task is scheduled.

**END OF STEPS**



---

# 17 Autonomous System Optimizer

## 17.1 About

### 17.1.1

The Autonomous System Optimizer application is used to steer traffic on monitored routers, on a per-destination-AS-basis, to alternate next hops. Steering per destination AS implies that steering will be performed for all prefixes associated with a given destination AS. The NRC-P will automatically correlate the destination AS number to the set of prefixes associated with it. Steering is accomplished using the NRC-P OpenFlow controller, by automatically adding an OpenFlow flow rule per destination subnet. This allows the user to offload high traffic usage from the uplinks onto alternate paths on a per-AS-basis.

Users can monitor traffic distribution on a set of uplinks so that link congestion and/or high bandwidth utilization can be identified per AS. The traffic monitoring is accomplished by collecting flow statistics, per AS, on Nokia 7750, 7450, and 7950 routers. These flow statistics are then communicated to the collector with IPFIX record encoding.

The application allows users to identify the set of top bandwidth consumption per destination AS, while the set of destination subnets associated with a given AS are automatically identified. Threshold Crossing Alarms (TCAs) on the monitored links can be tracked and a user can plot both real-time and historical port utilization.

## 17.2 Flow steering

### 17.2.1

This section describes the steering of flows using the Autonomous System Optimizer application.

[17.2.2 "To steer flows to next hops for autonomous systems" \(p. 187\)](#)

[17.2.3 "To steer flows to next hops for VIP customers" \(p. 188\)](#)

[17.2.4 "To configure next hop trackers" \(p. 189\)](#)

[17.2.5 "To create next hop trackers" \(p. 190\)](#)

### 17.2.2 To steer flows to next hops for autonomous systems

1

---

From the AS page of the Autonomous System Optimizer application, click on the Steer AS button. The Steer Flows form opens.

2

---

Choose one or more destination ASes from the drop-down menu and click CONTINUE.

- 
- 3
- Perform one of the following:
- a. Choose a next hop from the Select Next Hop drop-down menu and click CONTINUE.
  - b. Enter a valid IPv4 IP address in the Custom Next Hop field and click CONTINUE.
- 4
- Verify your changes and click FINISH. The new flow is added.

END OF STEPS

---

### 17.2.3 To steer flows to next hops for VIP customers

- 1
- Perform one of the following:
- a. From the VIP customers page of the Autonomous System Optimizer application, click on the Subnets button. The Subnets page opens. Continue to [Step 2](#).
  - b. From the Steering Diagram page of the Autonomous System Optimizer application, select a VIP customer from the list of Top Traffic Contributors and click on the CUSTOM STEERING button. The Steer Flows form opens. Go to step [Step 3](#).
  - c. From the VIP customers page of the Autonomous System Optimizer application, click on the Steer VIP customer button. The Steer Flows form opens. Go to [Step 4](#).
- 2
- Click on the Steer VIP Subnets button. The Steer Flows form opens. Go to step [Step 4](#).
- 3
- Click on the BACK button.
- 4
- Perform one of the following:
- a. Click CONTINUE.
  - b. Enable the *Steer all subnets not already steered* checkbox and click CONTINUE.
  - c. With the *Steer all subnets not already steered* checkbox enabled, delete subnets from the Selected Subnets drop-down menu to achieve partial steering of the VIP customer. Click CONTINUE.
  - d. With the *Steer all subnets not already steered* checkbox disabled, choose one or more subnets from the Subnet(s) to steer drop-down menu and click CONTINUE.
- 5
- Perform one of the following:

- a. Choose a next hop from the Select VIP Next Hop drop-down menu and click CONTINUE.
- b. Choose a next hop from the Select Next Hop drop-down menu and click CONTINUE.
- c. Enter a valid IPv4 IP address in the Custom Next Hop field and click CONTINUE.

6

Verify your changes and click FINISH. The new flow is added.

END OF STEPS

## 17.2.4 To configure next hop trackers

1

From the Settings page of the application, click on Tracker Settings.

2

As required, configure the following parameters:

Parameter	Description
AS Tracker Measurement Period (sec)	The frequency (in seconds) of reachability tests destined for non-VIP next hops
VIP Tracker Measurement Period (sec)	The frequency (in seconds) of reachability tests destined for VIP next hops
AS Tracker Measurement Threshold	Within a test destined for a non-VIP next hop, specifies the number of failed packets that will constitute reachability failure and trigger automatic unsteering (if configured)
VIP Tracker Measurement Threshold	Within a test destined for a VIP next hop, specifies the number of failed packets that will constitute reachability failure and trigger automatic unsteering (if configured)

3

Toggle AS Automatic Steering ON or OFF. When set to ON, AS traffic is automatically unsteered when the next hop is determined to be unreachable, as per the AS Tracker Measurement Period (sec) and AS Tracker Measurement Threshold parameter values.



**Note:** If traffic is automatically unsteered, manual re-steering will be available once the next hop is again determined to be reachable. Prior to this, the next hop will be unavailable for steering.

---

4

Toggle VIP Automatic Steering ON or OFF. When set to ON, VIP traffic is automatically unsteered when the next hop is determined to be unreachable, as per the VIP Tracker Measurement Period (sec) and VIP Tracker Measurement Threshold parameter values.

**i** **Note:** If traffic is automatically unsteered, manual re-steering will be available once the next hop is again determined to be reachable. Prior to this, the next hop will be unavailable for steering.

END OF STEPS

---

### 17.2.5 To create next hop trackers

---

1

From the Settings page of the application, click on Next Hop Trackers, then click on Add Next Hop Trackers. The Add Next Hop Trackers form opens.

---

2

Configure the following parameters:

Parameter	Description
Monitored Router	The unique identifier for the monitored router
Next Hop IP Address/Next Hop Router IP Address	The unique identifier for the next hop bundle

---

3

Click SAVE. The Next Hop Tracker is created.

END OF STEPS

---

---

## 18 Ingress Peer Optimizer

### 18.1 Overview

#### 18.1.1

The Ingress Peer Optimizer application controls and optimizes incoming traffic by monitoring statistics provided through the Deepfield system. The application monitors the traffic utilization on EBGP peering links and routers. If a link becomes congested, the Ingress Peer Optimizer moves the traffic between peer routers to a less used link. The traffic move is based on the selection of corresponding routes with the selected statistical information, such as prefix and community, according to predefined policies.

### 18.2 Ingress Peer Optimizer component description

#### 18.2.1 Ingress Links page

The Ingress Links page is the main page of the Ingress Peer Optimizer application, and shows a graphical representation of your network topology. You can view your defined slices, border routers, external routers, and the links between the routers. On this page, you can perform the following tasks:

- Filter the displayed information.  
The default graphic shows all the existing peers links in your topology. You can select the High utilization links filtering option to show only the most utilized links.
- View detailed information about each topology component.  
Click an object, and the application displays all the applicable details in the Info panel.
- Navigate to other pages of the Ingress Peer Optimizer application.  
Choose a page entry from the More... menu, or click on a page icon on the title bar to navigate to that page.

#### 18.2.2 More... menu options

The More... menu provides links to the following application pages:

- BGP Peering Topology
- BGP Communities
- Automation
- Application Setup
- Display Preferences
- Help

---

### 18.2.3 Title bar icons

The icons on the application title bar allow you to navigate to the following pages:

- Ingress Links
- Community Status
- Event History

## 18.3 Ingress Peer Optimizer pages

### 18.3.1 BGP Peering Topology

On the BGP Peering Topology page, you can build your network topology. See [18.5 “To configure the BGP peering topology” \(p. 194\)](#).

### 18.3.2 BGP Communities

The BGP Communities page shows a table that lists all the BGP communities defined in your network. On the BGP Communities page, you can perform the following tasks:

- Add a new community  
Click ADD COMMUNITY, configure the parameters on the Add BGP Community form, and save your changes.
- Edit an existing community  
In the BGP Communities table, point to the community that you need to edit, and click Edit BGP Community. Modify the parameters in the Edit BGP Community form, as required, and save your changes.
- Delete a community  
In the BGP Communities table, point to the community that you need to delete, and click Delete BGP Community.

### 18.3.3 Automation

On the Automation page, you configure the Ingress Peer Optimizer application to steer the traffic when a link utilization reaches a threshold. See [18.7 “To configure traffic optimization automation” \(p. 198\)](#).

### 18.3.4 Application Setup

On the Application Setup page, you select the Inbound Peering Model that fits your traffic steering needs and the Steering Template that the application uses to control the congestion in your network. See [18.4 “To set up the application” \(p. 194\)](#).

### 18.3.5 Display Preferences

The Display Preferences page allows for the visual customization of the Ingress Peer Optimizer application. See [18.9 “To configure display preferences” \(p. 201\)](#).

---

### 18.3.6 Help

When you choose Help from the More... menu, the Ingress Peer Optimizer application opens a dialog box that provides instructions about accessing the online help for the application.

### 18.3.7 Ingress Links

The Ingress Links page shows a diagram of the slices, border routers, external routers and links configured in your network topology. On the Ingress Links page, you can perform the following tasks:

- View details about your network topology components.  
Point to any component (border router, external router or peer link) to display general information about the component.  
Click on a link, and the application displays details about the selected peer link in the Info panel, including the link capacity and current utilization, and the community traffic breakdown
- Filter the links shown in the diagram. The filtering options are All peer links and High utilization links.

### 18.3.8 Community Status

The Community Status page shows a table that lists all the BGP communities defined in your network. On the Community Status page, you can perform the following tasks on each link:

- View details about a community.  
Click on a community entry, and the Ingress Peer Optimizer application displays details about the community in the Info panel.
- Steer the community to a preferred link.  
Point to a community and click Steer. The Steer to Preferred Link form opens. Review the information on the form and, if required, select the Ignore utilization constraints check box. Click STEER.

### 18.3.9 Event History

The Event History page shows a table that lists steering events that occurred in your network. On the Community Status page, you can perform the following tasks:

- View details about an event. Click on an event in the table, and the Ingress Peer Optimizer application displays details about the event in the Info panel.
- Filter the events by the period they occurred. The filtering options are: Last hour, Last 4 hours, Last 8 hours, Last 24 hours and Last week.

You can use the Event History details to review and analyze the steering events that happened in your network during the selected interval.

---

## 18.4 To set up the application

### 18.4.1

The first time you start the Ingress Peer Optimizer, the application opens the Application Setup page. At the setup stage you need to select the Inbound Peering Model that fits your traffic steering needs and the Steering Template that the application uses to control the congestion in your network.

1

Select one of the following inbound peering models:

- Peering Only
- Extended Peering

2

Select a steering template option:

- Automated Ingress Peer Optimizer
- Manual Ingress Peer Optimizer



**Note:** After you selected a steering template, you can view more information about the selected option by clicking DETAILS in each template panel.

3

Click BUILD APPLICATION. The application opens the Ingress Links page.

END OF STEPS

---

### 18.4.2

You can return to the Application Setup page at any time if you need to review the configured inbound peering model and the steering template. Then click RETURN TO APPLICATION to leave the Application Setup.

You can also change the inbound peering model and the steering template, but you must first reset the application.

## 18.5 To configure the BGP peering topology

### 18.5.1

After performing the initial setup, the application opens the Ingress Links page. This is the main page of the Ingress Peer Optimizer application.

The Ingress Links page shows the topology of the peer routers whose traffic the Ingress Peer Optimizer monitors and optimizes, but is empty after the application setup. You need to configure your BGP peering topology.

---

1

Click SET BGP PEERING TOPOLOGY. The BGP Peer Topology page opens, displaying a diagram of the network topology. Hover over any customer, optimization slice, border router, or neighbour to view a of preview of their contents.



**Note:** When this page is first opened, only a default slice is displayed.

## Adding an optimization slice

---

2

Click ADD OPTIMIZATION SLICE. The Add Optimization Slice form opens.

---

3

Configure the required slice parameters.

Parameter	Description
Slice Name	Type the name of the slice.
Site	Click ADD SITE, and type a site name. You can add one or multiple sites to a slice.

---

4

Click CREATE. The application creates the optimization slice and returns to the BGP Peer Topology page.

## Adding a border router

---

5

Click ADD above the Border Routers graphic. The Add Border Router to: *SliceName* form opens.

---

6

Configure the required border router parameters.

Parameter	Description
Router	Select a border router.
Site	Select the router site.
AS Number	Type the number of the AS that includes the border router.
Policy Name	Specifies a policy name, which allows for redirect to LSP

---

**i** **Note:** If a border router is added to multiple optimization slices, the parameter values provided most recently will be propagated to all optimization slices to which the border router had previously been added.

7 \_\_\_\_\_  
Click ADD. The application adds the border router to the slice.

### Adding a neighbor

8 \_\_\_\_\_  
Click ADD above the Neighbors graphic. The Add Neighbor form opens.

9 \_\_\_\_\_  
Configure the required neighbor parameters.

Parameter	Description
Name	Type the name of the neighbor.
AS Number	Type the number of the AS that includes the neighbor.

10 \_\_\_\_\_  
Click ADD. The application adds the neighbor to the topology.

### Adding a link

11 \_\_\_\_\_  
Click ADD above the Links graphic. The Add Link to: *SliceName* form opens.

12 \_\_\_\_\_  
Configure the required link parameters.

Parameter	Description
Border Router	Select a border router.
Local Export Policy Name	Type the name of the local export policy that you need to use. The name must match that of the BGP policy that you defined on the router.
Local Interface IP Address	Type the IP address of the interface configured on the router.
Local Interface Id (optional)	Type the index of the interface configured on the router.

---

Parameter	Description
Neighbor	Select a neighbor to peer with the border router.
Remote Interface IP Address	Type the IP address of the interface configured on the neighbor router.
Remote Interface Id (optional)	Type the index of the interface configured on the neighbor router.
Color Id (optional)	Select a pre-configured color ID from the drop-down menu. See <a href="#">18.6 "To configure color ID tags for links" (p. 197)</a> for more information.
ECMP Group Id (optional)	Type the ID of the ECMP (Equal Cost Multipath) configured on the router.

13

---

Click ADD. The application adds the link to the slice.

14

---

Click the left arrow in the top left corner of the BGP Peer Topology page to return to the Ingress Links page.

END OF STEPS

---

## 18.6 To configure color ID tags for links

### 18.6.1

1

---

Configure the BGP peering topology as described in [18.5 "To configure the BGP peering topology" \(p. 194\)](#).

2

---

On the BGP Peer Topology page's diagram, click on a set of links. A list of the links contained within that set appears.

3

---

Click on the button next to the ADD LINK button and choose Manage Color ID tags from the contextual menu. The Manage Color ID Tags form opens.

4

---

Click on the ADD TAG button to add a color ID tag. A new color ID appears on the form, numbered sequentially.

- 
- 5 \_\_\_\_\_  
Supply a Tag value for the new color ID.
- 6 \_\_\_\_\_  
As required, click on the Delete icon inline with any color ID tag to delete that color ID tag.
- 7 \_\_\_\_\_  
Click SAVE. The Manage Color ID Tags form closes.
- END OF STEPS \_\_\_\_\_

## 18.7 To configure traffic optimization automation

### 18.7.1

The automation of traffic optimization enables the Ingress Peer Optimizer application to steer the traffic automatically when a link utilization reaches a threshold.

- 1 \_\_\_\_\_  
On the Ingress Links page, click the More... menu and choose Automation. The Automation page of the Ingress Peer Optimizer application opens.
- 2 \_\_\_\_\_  
Turn the Automation ON or OFF, as required.

#### Automation parameters

- 3 \_\_\_\_\_  
Configure the required automation parameters.

Parameter	Description
BGP policy deployment time (sec)	The time between BGP policy deployment and traffic steering.
Alternate route selection rules	Choose an option to set what links the automation considers.
Enable hierarchy for alternative route selection	Select this check box to enable automation to prefer alternative links hierarchically: first links on the same router, next on the same site, and then on the same slice. If no preferred alternative links are found on a slice, the preference mechanism moves to the next slice.

---

Parameter	Description
Path redundancy limit	Configure the number of redundant paths allowed for a steering entity, in addition to the primary path. The default is 0, which means that the path redundancy is disabled.
Use same-color alternate link	Select this check box to restrict the selection of an alternate link only to the same color group when a link is congested.

## Global Thresholds

4

---

Configure the required Global Thresholds parameters.

Parameter	Description
Trigger utilization (%)	When utilization exceeds the specified utilization level on a link, the application triggers automation to move traffic from that link.
Target utilization (%)	The automation attempts to reduce the utilization to just above the specified level. If this is not possible, then automation attempts to reduce the utilization to just below the specified level.
Max utilization on alternate (%)	When traffic is offloaded onto any link, the link utilization does not exceed the defined level.
Use simplified threshold colors	Select this check box to use only the red and green colors for the links.

## Custom Thresholds

5

---

Click ADD. The Add Custom Thresholds form opens.

6

---

Configure the required custom threshold parameters, and save your changes.

---

## Save Automation changes

7

Review your Automation parameter configuration and save your changes. The application also allows you to discard the changes and revert to the initial Automation parameter configuration.

END OF STEPS

---

## 18.8 To create internal LSP constraint services

### 18.8.1

Internal LSP constrain services are deployed on border routers and are used to redirect traffic matching prefixes in the prefix-list onto an LSP. By specifying a prefix list, one internal LSP constraint service can be created for a group of prefixes.

**i** **Note:** This functionality is only supported on Juniper routers.

1

Ensure that the "Policy Name" parameter was populated during the creation of any border router to be used in this procedure. See ["Adding a border router" \(p. 195\)](#) for more information.

2

From the Ingress Links page of the application, click on a link. The Info panel is populated.

3

Click STEER. The Steer BGP Communities form opens.

4

Choose an AS to steer, then choose an alternate route to which to steer that system's traffic. The Internal LSP Constraints option appears.

**i** **Note:** If additional internal LSP constraint services exist, they can be viewed and/or deleted from this page.

5

Click ADD. The Add Internal LSP Constraint form opens.

---

6

Configure the required parameters:

Parameter	Description
Border Router	Specifies the border router to which the service will apply
LSP to use	Specifies the LSP to which the service will apply (must be pre-configured on the node)
Customer subnets	Specifies the subnet(s) to which the service will apply (CPAA must be configured in NFM-P to discover subnets)

---

7

Click SAVE. A POST request is sent to configure the service on the border router. This request creates a prefix list and an entry on the policy that is defined on the border router. This entry will contain a match for the prefix list, as well as an action to redirect the traffic over a specific LSP.

END OF STEPS

---

## 18.9 To configure display preferences

### 18.9.1

---

1

From the External Peers or Internal Peers page of the Ingress Peer Optimizer application, click on the More... button and choose Display Preferences from the contextual menu.

---

2

Configure the Identify Router By parameter. Choose one of the following from the drop-down menu:

- IP Address
- Name

---

3

Click SAVE. Your selected preferences are applied.

END OF STEPS

---



---

## 19 Latency Steering Optimizer

### 19.1 About

#### 19.1.1

The Latency Steering Optimizer application allows for traffic from an entry point router to a specific destination to be routed onto a path with the least possible latency.

### 19.2 Getting started

#### 19.2.1

This section describes the configuration of various objects using the Latency Steering Optimizer application.

[19.2.2 "To add an NE point" \(p. 203\)](#)

[19.2.3 "To add or modify a destination site" \(p. 204\)](#)

[19.2.4 "To modify an internal connection" \(p. 205\)](#)

[19.2.5 "To add or modify an external connection" \(p. 205\)](#)

[19.2.6 "To configure Latency optimization settings" \(p. 206\)](#)

#### 19.2.2 To add an NE point

1 \_\_\_\_\_

From the Settings page of the Latency Steering Optimizer application, click on NE points.

2 \_\_\_\_\_

Perform one of the following:

- a. To delete an NE point, click on the Delete button inline with the desired NE point. No further action is required.
- b. To add an NE point, click on ADD NE POINT. The Add NE point form opens. Continue to [Step 3](#).

3 \_\_\_\_\_

Select a router from the list to monitor.

4 \_\_\_\_\_

If required, select the datapath ID of the OF switch to be used from the drop-down menu.

---

**5** \_\_\_\_\_  
If required, enable the Border Router checkbox to identify the NE point as a border router.

**6** \_\_\_\_\_  
Click SAVE. The NE point is added.

**END OF STEPS** \_\_\_\_\_

### 19.2.3 To add or modify a destination site

**1** \_\_\_\_\_  
From the Settings page of the Latency Steering Optimizer application, click on Destination sites.

**2** \_\_\_\_\_  
Perform one of the following:

- a. To delete a destination site, click on the Delete button inline with the desired site. No further action is required.
- b. To add a destination site, click ADD DESTINATION SITE. The Add Destination Site form opens. Continue to [Step 3](#).
- c. To modify a destination site, click on the Edit button inline with the desired site. The Edit Destination Site form opens. Continue to [Step 3](#).

**3** \_\_\_\_\_  
Configure the Site Name parameter.

**4** \_\_\_\_\_  
If required, click ADD POINT to add a destination point, then configure the Name and Probe IP Address parameters.  
Alternatively, click on the Delete Point button inline with any point to delete that point.

**5** \_\_\_\_\_  
Click on the Add Subnet(s) button.

**6** \_\_\_\_\_  
Click ADD SUBNET, then enter a subnet prefix in the provided field.  
Alternatively, click on the Delete Subnet button inline with any subnet to delete that subnet.

**7** \_\_\_\_\_  
Click DONE. Subnet configurations are saved.

- 
- 8 \_\_\_\_\_  
Click SAVE. The Destination site is added/modified.

END OF STEPS \_\_\_\_\_

## 19.2.4 To modify an internal connection

- 1 \_\_\_\_\_  
From the Settings page of the Latency Steering Optimizer application, click on Internal connections.

- 2 \_\_\_\_\_  
To modify an internal connection, click on the Edit button inline with the desired connection. The Edit connection form opens.

- 3 \_\_\_\_\_  
Choose whether or not to set latency for the connection by enabling the appropriate option.

- 4 \_\_\_\_\_  
If you chose to set latency for the connection in [Step 3](#), enter a latency value (in milliseconds) in the provided field.

- 5 \_\_\_\_\_  
Click UPDATE. The internal connection is modified.

END OF STEPS \_\_\_\_\_

## 19.2.5 To add or modify an external connection

- 1 \_\_\_\_\_  
From the Settings page of the Latency Steering Optimizer application, click on External connections.

- 2 \_\_\_\_\_  
Perform one of the following:
- a. To delete an external connection, click on the Delete button inline with the desired connection. No further action is required.
  - b. To add an external connection, click ADD CONNECTION. The Add connection form opens. Continue to [Step 3](#).
  - c. To modify an external connection, click on the Edit button inline with the desired connection. The Edit connection form opens. Continue to [Step 6](#).

- 
- 3 \_\_\_\_\_  
Select a Border Router from the drop-down menu.
  - 4 \_\_\_\_\_  
Populate the ASBR Interface IP Address field.  
**i** **Note:** The ASBR Interface IP Address field can be left blank when creating an initial external connection for a given border router, however, the field must be populated with a valid address when adding additional external connections for that border router.
  - 5 \_\_\_\_\_  
Select a Destination site from the drop-down menu, then select a Destination point.
  - 6 \_\_\_\_\_  
Choose whether or not to set latency for the connection by enabling the appropriate option.
  - 7 \_\_\_\_\_  
If you chose to set latency for the connection in [Step 6](#), enter a latency value (in milliseconds) in the provided field.
  - 8 \_\_\_\_\_  
Click SAVE or UPDATE. The external connection is added/modified.

END OF STEPS \_\_\_\_\_

## 19.2.6 To configure Latency optimization settings

- 1 \_\_\_\_\_  
From the Settings page of the Latency Steering Optimizer application, click on Latency optimization settings.
- 2 \_\_\_\_\_  
Perform one of the following:
  - a. Toggle Automatic Steering ON or OFF.
  - b. Toggle Automatic Latency Measurement ON or OFF. If ON, enter an Automatic latency measurement interval (in seconds) in the provided field.
  - c. Specify (in percentage) the Latency Steering Optimization Threshold.
- 3 \_\_\_\_\_  
Click SAVE. Your configurations are saved.

END OF STEPS \_\_\_\_\_

---

## 20 Traffic Steering Controller

### 20.1 About

#### 20.1.1

The Traffic Steering Controller application allows for the manipulation of flow rules, such as the addition or deletion of flow rules using the NRC-P OpenFlow controller. The application also allows flow tables from the OpenFlow switches of any 7x50 router within a network to be displayed. Nokia SROS OpenFlow Experimenters are supported, and can redirect traffic to alternate next hops, using plugins.

### 20.2 Flow management

#### 20.2.1

This section describes the management of flows using the Traffic Steering Controller application.

[20.2.2 "To add a flow entry" \(p. 207\)](#)

#### 20.2.2 To add a flow entry

1

---

Perform one of the following:

- a. To add a flow from the Switches page of the application, perform the following:
  1. Select a switch from the list. The Switch Details form opens.
  2. Click on the Actions button and choose Add Flow Entry from the contextual menu. The Add Flow Entry form opens.
- b. From the Flows page of the application, click on the Add Flow Entry button. The Add Flow Entry form opens.

2

---

Configure the following parameters:

Parameter	Description
Application ID	The ID of the application that deployed the flow. Negative numbers are reserved and should not be used.
Cookie	The hexadecimal, controller-issued ID for the flow
Priority	The priority of the flow

- 
- 3** \_\_\_\_\_  
As required, click on the Add Match Criteria button and choose one or more of the following match criteria to add.
- 4** \_\_\_\_\_  
Populate the corresponding field for any added match criteria, then click CONTINUE.
- 5** \_\_\_\_\_  
Choose an instruction type from the drop-down list.
- 6** \_\_\_\_\_  
As required, click Add Action to add additional actions, then click Finish. The flow entry is created.
- END OF STEPS** \_\_\_\_\_

### 20.2.3 To view flow entries

- 1** \_\_\_\_\_  
Perform one of the following:
- a. To search for a flow from the Switches page of the application, perform the following:
    - 1. Select a switch from the list. The Switch Details form opens.
    - 2. Click on the Actions button and choose View Flow Entries from the contextual menu. The View Flow Entries form opens.
  - b. From the Flows page of the application, click on the View Flow Entries button. The View Flow Entries form opens.
- 2** \_\_\_\_\_  
Click Add Filter to add one or more attributes for which to filter.
- 3** \_\_\_\_\_  
From the drop-down menu, select one or more table columns to display on the results screen.
- 4** \_\_\_\_\_  
To undo any previous selections, click RESTORE DEFAULT.
- 5** \_\_\_\_\_  
Click APPLY. The results are displayed on the Flows page of the application.

---

**6**

If required, click Add Filter to apply attributes for which to filter.

**END OF STEPS**

---



## 21 IP/MPLS Optimization

### 21.1 About

#### 21.1.1

The IP/MPLS Optimization application provides a view of the IGP topology and PCE LSPs. It also displays the status of the IGP network and provides functionality to optimize the network resources.

### 21.2 Getting started

#### 21.2.1

This section describes the tasks you must perform in order to use the IP/MPLS Optimization application.

[21.2.2 “To find a path” \(p. 211\)](#)

[21.2.3 “To create PCE-initiated LSPs” \(p. 212\)](#)

[21.2.4 “To place a link set into maintenance mode” \(p. 214\)](#)

[21.2.5 “To create a path profile policy” \(p. 215\)](#)

[21.2.6 “To create a router ID mapping policy” \(p. 216\)](#)

[21.2.7 “To modify the system IP MPLS configuration policy” \(p. 217\)](#)

#### 21.2.2 To find a path

1

From the Network Map page of the application, click on the Path Finder icon.

2

Configure the following parameters:

Parameter	Description
Source	The network element that will serve as the source for the path
Destination	The network element that will serve as the destination for the path
Secondary Source	The network element that will serve as the secondary source for the path
Secondary Destination	The network element that will serve as the secondary destination for the path

Parameter	Description
Objective	The primary goal when identifying paths for path computation
Path Type	The signalling type to be used for the path
Disjoint	The Disjoint mode to be used in path computation
Bidirectional	The bidirectional mode to be used in path computation
Max Hops (span)	The Max Hops constraint to be used in path computation
Max Cost	The Max Cost constraint to be used in path computation
Max Latency	The Max Latency constraint to be used in path computation
Max TE Metric	The Max TE Metric constraint to be used in path computation
Bandwidth (Mbps)	Specifies the bandwidth required for the path

3

Click SHOW. The optimal path is highlighted on the topology map.

END OF STEPS

### 21.2.3 To create PCE-initiated LSPs



**Note:** Before a PCE-initiated LSP can be successfully created, certain commands must be executed on the source node. See the *NSD and NRC User Guide* for more information.

1

From the LSPs page of the application, click on the Create PCE LSP icon.

2

Configure the required parameters:

Parameter	Description
Path Name	The name of the PCE-initiated LSP
PCC Address	The address of the PCC
Source	Specifies the source node for the path
Destination	Specifies the destination node for the path

Parameter	Description
Administration	Specifies the desired administrative state
Template ID	Specifies the ID of the template to be applied
Path Type	Specifies the type of path (must be Segment Routing)
Objective	Specifies the primary goal when identifying path resources
Bandwidth (Mbps)	Specifies the bandwidth required for the LSP

**3**

As required, click **ADVANCED OPTIONS**. Configure the parameters:

Parameter	Description
Max Hops (Span)	Specifies the maximum number of hops to consider
Max Cost	Specifies the maximum cost to consider
Max TE Metric	Specifies the maximum TE metric to consider
Max Latency	Specifies the maximum latency to consider
Include Any Bit Pos	Specifies any bit between 0 and 31 to include
Exclude Any Bit Pos	Specifies any bit between 0 and 31 to exclude
Include All Bit Pos	Specifies all bits between 0 and 31 to include
Profile ID	Specifies the identifier of the path profile to apply
Group ID	Specifies the identifier of the group to which this LSP belongs

**4**

Click **SAVE**. The PCE-initiated LSP is created.

**5**

From the LSP List page, PCE-initiated LSPs can be shutdown, turned up, or deleted by clicking on the inline **More...** button and choosing the desired action from the contextual menu.

**END OF STEPS**

---

## 21.2.4 To place a link set into maintenance mode

When a link set is placed into maintenance mode, the LSPs riding the link set must be rerouted. This can be done manually or automatically.

In order for the NRC-P to reroute these LSPs automatically, the `nrcp` block of the `/opt/nsp/configure/config/arm-system.conf` file must be modified as follows:

```
nrcp {  
  
nrcp_link_maintenance_policy="swift"  
  
bgpLs  
  
{  
  
    isTopoSourceBgpLS=true  
  
}  
  
}
```

When maintenance mode is deactivated for a link set, and the above modification has been made, the LSPs will automatically return to their original link set.

1 \_\_\_\_\_

Perform one of the following:

- a. From the Network Map page of the application, select an IGP link on the map and click on the Info button.
- b. From the Link List page of the application, select an IGP link from the list.

2 \_\_\_\_\_

Click on the More... button and choose Activate Maintenance Mode for Link Set. A confirmation window opens.

3 \_\_\_\_\_

Click OK. The confirmation window closes and the link set is placed into maintenance mode.

**i** **Note:** If the NRC-P has not been configured to automatically reroute LSPs whose link set has been placed into maintenance mode, these LSPs will need to be manually rerouted.

4 \_\_\_\_\_

To deactivate maintenance mode for a link set, click on the More... button and choose Deactivate Maintenance Mode for Link Set. A confirmation window opens.

5

Click OK. The confirmation window closes and maintenance mode is deactivated for the link set.



**Note:** If the NRC-P has not been configured to automatically reroute LSPs whose link set has been placed into maintenance mode, these LSPs will need to be manually returned to their original link set.

END OF STEPS

## 21.2.5 To create a path profile policy

1

From the Policy List page of the application, choose Path Profiles from the drop-down menu and click CREATE POLICY. The Create Path Profile policy form opens.

2

Configure the required parameters:

Parameter	Description
Reserved Profile ID	When this parameter is enabled, the Path Profile template assumes the Name and role of the default Path Profile template
Name	The name of the Path Profile template
Profile ID	The Profile ID of the paths to be included in path computation
Bidirectional	The bidirectional mode to be used in path computation
Disjoint	The Disjoint mode to be used in path computation
Optimize on (Objective)	Specifies the primary goal when identifying paths for path computation
Bandwidth Strategy	Specifies the strategy to use for LSP bandwidth in the path computation
Explicit Route Strategy	Specifies the explicit route strategy for the service
Control Route Strategy	Specifies the strategy to use when recomputing the path
Max Hops (span)	Specifies the Max Hops constraint to be used in path computation

Parameter	Description
Max Cost	Specifies the Max Cost constraint to be used in path computation
Max TE Metric	Specifies the Max TE Metric constraint to be used in path computation
Max Latency	Specifies the maximum latency to consider
Latency Threshold	Specifies when to re-signal an LSP that is optimized on latency. If no change in latency (0), re-signal is automatically triggered. If the change is less than 0, the LSP is not re-signalled. If the change is greater than 0, the LSP is re-signalled. The default value is -1.
Description	Describes the Path Profile template

3

As required, Exclude Route Objects by adding the IP address(es) of the object(s) to be excluded.

4

As required, Include Route Objects by adding the IP address(es) of the object(s) to be included. You must also specify Hop Type.

5

Click CREATE. The Path Profile policy is created.

END OF STEPS

## 21.2.6 To create a router ID mapping policy

1

From the Policy List page of the application, choose Router ID Mapping from the drop-down menu and click CREATE POLICY. The Create Router ID Mapping Policy form opens.

2

Configure the required parameters:

Parameter	Description
Name	Specifies the name of the Router ID Mapping template

Parameter	Description
System IP Address	Specifies the system IP address of the router
System Name	Specifies the router system name
PCC Address	Specifies the address of the PCC associated with the router
Description	Specifies the router description
Router Info	<p>Click ADD to add as many Router Info entries, as required. For each Router Info entry, you must specify the following information:</p> <ul style="list-style-type: none"> <li>• Network Identifier</li> <li>• AS Number</li> <li>• BGP-LS ID (topology identifier)</li> <li>• Router ID</li> <li>• Protocol (the protocol that the IGP router is using)</li> </ul>

3

Click CREATE. The Router ID Mapping policy is created.

END OF STEPS

## 21.2.7 To modify the system IP MPLS configuration policy

1

Perform one of the following:

- a. From the Policy List page of the application, choose System IP MPLS Configuration from the drop-down menu and click CREATE POLICY. The Edit System IP MPLS Configuration form opens.
- b. From the Policy List page of the application, click on the Edit button inline with the System IP MPLS Configuration policy. The Edit System IP MPLS Configuration form opens.

2

Configure the required parameters:

Parameter	Description
Description	Describes the System IP MPLS Configuration policy

---

Parameter	Description
Maintenance Mode	Specifies whether or not links are placed into maintenance mode automatically or manually

**3**

---

Click SAVE. The System IP MPLS Configuration policy is modified.

**END OF STEPS**

---

---

## 22 IP/MPLS Simulation

### 22.1 About

#### 22.1.1

The IP/MPLS Simulation application allows for modifications to IGP topology, PCE LSPs, links, and a variety of policies within a simulated environment.

### 22.2 Getting started

#### 22.2.1

This section describes the tasks you must perform in order to use the IP/MPLS Simulation application.

[22.2.2 “To import a network from NRC-P” \(p. 219\)](#)

[22.2.3 “To add an admin domain” \(p. 220\)](#)

[22.2.4 “To add a node” \(p. 220\)](#)

[22.2.5 “To add a link” \(p. 221\)](#)

[22.2.6 “To find a path” \(p. 223\)](#)

[22.2.7 “To create PCE-initiated LSPs” \(p. 224\)](#)

[22.2.8 “To turn down a link set” \(p. 225\)](#)

[22.2.9 “To create a path profile policy” \(p. 226\)](#)

[22.2.10 “To create a router ID mapping policy” \(p. 227\)](#)

#### 22.2.2 To import a network from NRC-P

1

---

Perform one of the following:

- a. If opening the IP/MPLS Simulation application for the first time, the Import Network from NRC-P form will appear. Continue to step [Step 2](#).
- b. If a network topology has been deleted, click on the More... button on the Network Map page of the application and choose Import Network from NRC-P. The Import Network from NRC-P form opens. Continue to step [Step 2](#).

2

---

Enable the Network radio button or the Network and LSPs radio button to specify which elements of the network to import, then configure the parameters:

Parameter	Description
CAS server IP	The IP address of the CAS server from which to retrieve a security token
Username	The username with which to log in to the CAS server
Password	The password to be used with the specified username

3

Click IMPORT. The Network topology is imported from NRC-P.

END OF STEPS

### 22.2.3 To add an admin domain

1

From the Network Map page of the application, click on the (+) button and choose Add Domain from the contextual menu. The Create Admin Domain form appears.

2

Configure the parameters:

Parameter	Description
Network ID	Specifies the network identifier
AS number	Specifies the AS number
BGPLS ID	Specifies the BGP-LS identifier

3

Click CREATE. The admin domain is added to the network topology.



**Note:** An admin domain is automatically deleted if not populated with network elements.

END OF STEPS

### 22.2.4 To add a node



**Note:** An admin domain must have been imported or added to the application before a node can be successfully added. See [22.2.2 “To import a network from NRC-P” \(p. 219\)](#) or [22.2.3 “To add an admin domain” \(p. 220\)](#) for more information.


**1** \_\_\_\_\_  
From the Network Map page of the application, or the Node List page of the application, click on the (+) button and choose Add Node from the contextual menu. The Create Node form appears.

**2** \_\_\_\_\_  
Configure the parameters:

Parameter	Description
Router ID	Specifies the router identifier
Topology	Specifies the domain to which the router belongs
Protocol	Specifies the protocol to be used by the router; OSPF or ISIS


**3** \_\_\_\_\_  
Perform one of the following:

- a. Click on the CREATE button that features a refresh icon. The node is added to the network topology and the form remains open for further additions.
- b. Click CREATE. The node is added to the network topology.

 **Note:** Nodes can be deleted from the network entirely or removed on a per-instance basis.

**END OF STEPS** \_\_\_\_\_

## 22.2.5 To add a link

 **Note:** Nodes must have been imported or added to the application before a link can be successfully added. See [22.2.2 “To import a network from NRC-P” \(p. 219\)](#) or [22.2.4 “To add a node” \(p. 220\)](#) for more information.

**1** \_\_\_\_\_  
From the Network Map page of the application, or the Link List page of the application, click on the (+) button and choose Add PointToPoint Link or Add Broadcast Link from the contextual menu. A creation form appears.

2

Configure the parameters:


Parameter	Description
Admin Domain	Specifies the administrative domain in which to create the link
Protocol	Specifies the protocol to apply to the link
Source	Specifies the link source
New Subnet	Specifies whether or not a new subnet will be created; only for broadcast links.
Destination	Specifies the link destination

3

Click on the Forward Direction tab and configure the parameters:

Parameter	Description
<b>Source to destination parameters</b>	
IP Address	Specifies the IP address of the destination node (forward direction) or source node (reverse direction)
Latency	Specifies the maximum latency to consider
Cost	Specifies the maximum cost to consider
<b>Traffic engineering parameters</b> These parameters are only configurable when the Enable Traffic Engineering slider is enabled	
Bandwidth (Mbps)	Specifies the maximum bandwidth to consider
Admin Group	Specifies the admin group to which the link will belong
SRLG	Specifies the SRLG to which the link will belong
TE Metric	Specifies the maximum TE metric to consider
RSVP	Specifies whether or not the link will be RSVP
SR	Specifies whether or not the link will be SR

- 4 \_\_\_\_\_  
Click on the Reverse Direction tab and configure the parameters as described in step [Step 3](#).

 **Note:** The Reverse Direction tab is available only for Point-To-Point links.

- 5 \_\_\_\_\_  
Perform one of the following:
- a. Click on the CREATE button that features a refresh icon. The link is added to the network topology and the form remains open for further additions.
  - b. Click CREATE. The link is added to the network topology.

END OF STEPS \_\_\_\_\_

### 22.2.6 To find a path

- 1 \_\_\_\_\_  
From the Network Map page of the application, click on the Path Finder icon.

- 2 \_\_\_\_\_  
Configure the following parameters:

Parameter	Description
Source	The network element that will serve as the source for the path
Destination	The network element that will serve as the destination for the path
Secondary Source	The network element that will serve as the secondary source for the path
Secondary Destination	The network element that will serve as the secondary destination for the path
Objective	The primary goal when identifying paths for path computation
Path Type	The signalling type to be used for the path
Disjoint	The Disjoint mode to be used in path computation
Bidirectional	The bidirectional mode to be used in path computation
Max Hops (span)	The Max Hops constraint to be used in path computation

Parameter	Description
Max Cost	The Max Cost constraint to be used in path computation
Max Latency	The Max Latency constraint to be used in path computation
Max TE Metric	The Max TE Metric constraint to be used in path computation
Bandwidth (Mbps)	Specifies the bandwidth required for the path

3

Click SHOW. The optimal path is highlighted on the topology map.

END OF STEPS

## 22.2.7 To create PCE-initiated LSPs

1

From the LSP List page of the application, click on the Create PCE LSP icon.

2

Configure the required parameters:

Parameter	Description
Path Name	The name of the PCE-initiated LSP
PCC Address	The address of the PCC
Objective (Optimize on)	Specifies the primary goal when identifying path resources
Max Hops (Span)	Specifies the maximum number of hops to consider
Bandwidth (Mbps)	Specifies the bandwidth required for the LSP
Include Any Bit Pos	Specifies any bit between 0 and 31 to exclude
Exclude Any Bit Pos	Specifies any bit between 0 and 31 to exclude
Path Type	Specifies the type of path (must be Segment Routing)
Source	Specifies the source node for the path
Destination	Specified the destination node for the path

Parameter	Description
Profile ID	Specifies the identifier of the path profile to apply
Group ID	Specifies the identifier of the group to which this LSP belongs

3

Click SAVE. The PCE-initiated LSP is created.

END OF STEPS

## 22.2.8 To turn down a link set

1

Perform one of the following:

- a. To turn down a link set from the Network Map page of the application, perform the following:
  1. Select an IGP link on the map and click on the Info button.
  2. Click on the More... button and choose Turn Link Set Down. The link set is turned down.
- b. To turn down a link set from the Link List page of the application, perform the following:
  1. From the Link List page of the application, select an IGP link from the list.
  2. Click on the Turn Link Down button inline with the desired link. The link, and the other member of its set, is turned down.

2

Click SIMULATE. The Simulation Results form opens.



**Note:** The SIMULATE button is only available when a traffic-affecting network enhancement or degradation has occurred. Some actions, such as Create LSP or Re-signal, are disabled when the SIMULATE button is available.



**Note:** Simulation results are only available for the most recent simulated activity and will be overwritten when the SIMULATE button is next clicked.

3

Click DETAILS to view a list of LSPs affected by the configuration.



**Note:** This list can be revisited by clicking on the Simulation Results tab. Only the results of the most recent configuration are displayed.

4

As required, perform one of the following:

- a. To return a link set to an operational state from the Network Map page of the application, perform the following:
  1. On the map, select an IGP link that is operationally down and click on the Info button.
  2. Click on the More... button and choose Turn Link Set Up. The link set is turned down.
- b. To return a link set to an operational state from the Link List page of the application, perform the following:
  1. From the Link List page of the application and select an operationally down IGP link from the list.
  2. Click on the Turn Link Up button inline with the desired link. The link, and the other member of its set, is turned up.

END OF STEPS

## 22.2.9 To create a path profile policy

1

From the Policy List page of the application, choose Path Profiles from the drop-down menu and click CREATE POLICY. The Create Path Profile policy form opens.

2

Configure the required parameters:

Parameter	Description
Reserved Profile ID	When this parameter is enabled, the Path Profile template assumes the Name and role of the default Path Profile template
Name	The name of the Path Profile template
Profile ID	The Profile ID of the paths to be included in path computation
Bidirectional	The bidirectional mode to be used in path computation
Disjoint	The Disjoint mode to be used in path computation
Optimize on (Objective)	Specifies the primary goal when identifying paths for path computation
Bandwidth Strategy	Specifies the strategy to use for LSP bandwidth in the path computation
Explicit Route Strategy	Specifies the explicit route strategy for the service

Parameter	Description
Control Route Strategy	Specifies the strategy to use when recomputing the path
Max Hops (span)	Specifies the Max Hops constraint to be used in path computation
Max Cost	Specifies the Max Cost constraint to be used in path computation
Max TE Metric	Specifies the Max TE Metric constraint to be used in path computation
Max Latency	Specifies the maximum latency to consider
Latency Threshold	Specifies when to re-signal an LSP that is optimized on latency. If no change in latency (0), re-signal is automatically triggered. If the change is less than 0, the LSP is not re-signalled. If the change is greater than 0, the LSP is re-signalled. The default value is -1.
Description	Describes the Path Profile template

3

As required, Exclude Route Objects by adding the IP address(es) of the object(s) to be excluded.

4

As required, Include Route Objects by adding the IP address(es) of the object(s) to be included. You must also specify Hop Type.

5

Click CREATE. The Path Profile policy is created.

END OF STEPS

## 22.2.10 To create a router ID mapping policy

1

From the Policy List page of the application, choose Router ID Mapping from the drop-down menu and click CREATE POLICY. The Create Router ID Mapping Policy form opens.

**2**

Configure the required parameters:

Parameter	Description
Name	Specifies the name of the Router ID Mapping template
System IP Address	Specifies the system IP address of the router
System Name	Specifies the router system name
PCC Address	Specifies the address of the PCC associated with the router
Description	Specifies the router description
Router Info	<p>Click ADD to add as many Router Info entries, as required. For each Router Info entry, you must specify the following information:</p> <ul style="list-style-type: none"> <li>• Network Identifier</li> <li>• AS Number</li> <li>• BGP-LS ID (topology identifier)</li> <li>• Router ID</li> <li>• Protocol (the protocol that the IGP router is using)</li> </ul>

**3**

Click CREATE. The Router ID Mapping policy is created.

**END OF STEPS**

---

## 23 Modeled Device Configurator

### 23.1 Overview

#### 23.1.1

The MDC allows the user to configure parameters and view state information defined in the NE adaptation schema.

The schemas displayed by MDC may vary based on the adaptors that are installed. For example, an SR device will have a config schema and a state schema. The state schema is read-only.

The MDC displays the NE parameters. Choose Configured Attributes View from the drop-down menu at the top of the page to view only the configured parameters on the NE. Choose All Attributes View to view all of the available parameters, including parameters with default values.

#### 23.1.2 Performing configuration

You can configure multiple parameters on the displayed branch of the NE schema. When changing levels within the schema, you will be prompted if there are un-submitted changes. When a configuration change is submitted, a progress bar appears and then a success or failure message is returned by the NE.

The MDC reads and writes NE data through the MDM adaptation. The MDC performs syntax checks according to what is defined in the device adaptation YANG model, e.g. string length, max value, etc. Further validation may be handled by the device at commit time.

If configuration is committed successfully, it is applied to the running configuration on the NE through the device adaptation. Persistence may require device specific configuration on the NE; see the NE documentation.

If the commit operation fails, the failure message will provide the reason for the failure. The application will continue to display your configured values, allowing you to edit and commit again.

#### 23.1.3 Config basket

The configuration basket lets you create a list of configuration changes and submit multiple changes at the same time.

The config basket displays the list of changes, with links to the schema where the changes will be made. You can preview, cancel, or submit the changes, or click the link to return to the schema and edit the change. From the config basket, click CONTINUE EDITING to return to the schema.

The following restrictions apply:

- The config basket can only be used for one NE at a time. Changes cannot be pushed from the config basket to multiple NEs.
- Changes in the config basket can only be committed to the NE or removed from the basket. There is no validation function.

- 
- The config basket does not support committing changes for more than one schema at a time. Configuration changes for each schema must be submitted in separate submit operations.
  - The config basket contents are only populated for the duration of the session: they cannot be saved for later use.
  - Leaf list items cannot be modified using the MDC. The parent object must be deleted and recreated.

## 23.2 To create an object

### 23.2.1

- 1 \_\_\_\_\_  
In the MDC application, click in the Search field. A list of NEs that were discovered using the Device Administrator application and have deployed MDC adaptors appears.  
You can use the filter to find a specific NE using NE ID, NE Name, Node Type, or Version.
  - 2 \_\_\_\_\_  
Double-click on an NE. A list of available schemas for the NE appears.
  - 3 \_\_\_\_\_  
Click on a schema in the list to view the specific attributes of the schema.
  - 4 \_\_\_\_\_  
Navigate through the different branches of the schema to the object you want to create.  
To navigate to a previous configuration window, click on the desired object in the Root > path.
  - 5 \_\_\_\_\_  
Click CREATE *n* and configure the applicable parameters.
  - 6 \_\_\_\_\_  
Once the desired object instance parameters are configured, click ADD TO CONFIG BASKET.  
The newly created object is added to the config basket. It appears in the list, however, it is not yet committed.
  - 7 \_\_\_\_\_  
Click CONFIG BASKET to review your list of changes.
  - 8 \_\_\_\_\_  
Click SUBMIT to commit the changes in the config basket.
- END OF STEPS** \_\_\_\_\_

---

## 23.3 To modify an object

### 23.3.1

1 \_\_\_\_\_

In the MDC application, click in the Search field. A list of NEs that were discovered using the Device Administrator application and have deployed MDC adaptors appears.

You can use the filter to find a specific NE using NE ID, NE Name, Node Type, or Version.

2 \_\_\_\_\_

Double-click on an NE. A list of available schemas for the NE appears.

3 \_\_\_\_\_

Click on a schema in the list to view the specific attributes of the schema.

4 \_\_\_\_\_

Navigate through the different branches of the schema to the object you want to modify.

To navigate to a previous configuration window, click on the desired object in the Root > path.

5 \_\_\_\_\_

Perform the following as needed:

1. Configure the required parameters in the branch you navigated to.

The change is marked by a white bullet.

2. Click ADD TO CONFIG BASKET.

Your configured changes are added to a list in the config basket. The bullet marking the change becomes a solid bullet.

3. If required, navigate to another branch and add additional changes to the config basket.

6 \_\_\_\_\_

Click CONFIG BASKET to review your list of changes.

7 \_\_\_\_\_

Click SUBMIT to commit the changes in the config basket.

END OF STEPS \_\_\_\_\_

---

## 23.4 To delete an object

### 23.4.1

- 1 

---

In the MDC application, click in the Search field. A list of NEs that were discovered using the Device Administrator application and have deployed MDC adaptors appears.  
You can use the filter to find a specific NE using NE ID, NE Name, Node Type, or Version.
- 2 

---

Double-click on an NE. A list of available schemas for the NE appears.
- 3 

---

Click on a schema in the list to view the specific attributes of the schema.
- 4 

---

Navigate through the different branches of each schema to the object you want to delete.  
To navigate to a previous configuration window, click on the desired object in the Root > path.
- 5 

---

Click the Delete icon. The deletion is added to the config basket.
- 6 

---

Click CONFIG BASKET to review your list of changes.
- 7 

---

Click SUBMIT to commit the changes in the config basket.

**END OF STEPS** 

---

---

## 24 Workflow Manager

### 24.1 Workflows overview

#### 24.1.1

The WFM allows you to create and execute workflows using Mistral's v2 DSL YAML. You can create automated procedures and closed loop automation using Nokia NSP or 3rd party APIs.

Some example use cases for the WFM:

- Node software upgrades
- Service activation tests
- Service fulfillment invoking pre and post deployment workflows
- Customizable policy logic for other applications
- Mass migration of services from one tunnel type to another
- One place scheduling for all NSP REST APIs and node CLI
- Centralized orchestration for Nokia NSP and 3rd party vendor APIs

The WFM uses Mistral DSL v2 which is based on YAML. YAML defines expressions in workflow and action definitions. The formatting of the YAML must comply with Mistral DSL v2 specifications. For more information about Mistral DSL v2, the workflow hierarchy and associated attributes, refer to the Mistral DSL v2 specification online.

As part of workflow creation and execution, you will interact with these objects:

- [Workflows](#)
- [Input](#)
- [Output](#)
- [Tasks](#)
- [Actions](#)

#### 24.1.2 Workflows

A workflow represents the process to do a job, for example, configure a service. Workflow attributes are described in detail in the Mistral DSL v2 specification. The following is a sample of a workflow:

*Figure 24-1* Sample workflow

```
version: '2.0'

validateWFMAPI:
  description: 'Validate WFM APIs'
  type: direct
```

```
input:
  - token_auth: 'Token_info'
  - rest_gateway_host: '198.51.100.0'
  - wfm_port: '8543'
  - apis:
    - '/v1/workflow'
    - '/v1/workflow?limit=1'

output:
  status: <% $.status %>

tasks:
  validateAllApis:
    wait-before: 30
    with-items: api in <% $.apis%>
    action: std.http
    input:
      url: 'https://<% $.rest_gateway_host %>:<% $.wfm_port%>/wfm/api<%
$.api %>'
      method: GET
      verify: False
      headers:
        Content-Type: 'application/json'
        Authorization: <% $.token_auth%>
    publish:
      data: <% task(validateAllApis).result.content.response %>
    on-complete:
      - validateWFAllAPI
      - validateWFLimitAPI
    on-error:
      - FailedApiCall

  validateWFAllAPI:
    publish:
      length1: <% $.data[0].totalRows %>
    on-complete:
      - successDone: <% $.length1 > 2 %>
      - FailedValidation: <% $.length1 < 2 %>
      - branchSuccess

  validateWFLimitAPI:
    publish:
      length2: <% $.data[1].totalRows %>
    on-complete:
      - successDone: <% $.length2 = 1 %>
      - FailedValidation: <% $.length2 != 1 %>
      - pause
```

---

```
- branchSuccess

branchSuccess:
  join: all
  publish:
    status: "branched after pause"

successDone:
  publish:
    status: "DONE"

FailedValidation:
  publish:
    status: "Validation Failed"

FailedApiCall:
  publish:
    status: "Error on Api <% $.api %>"
```

### 24.1.3 Input

Input is the input parameters of a workflow or task, if required. The value of each parameter is a JSON-compliant type (number, string, etc), a dictionary, or a list. It can also be an expression to retrieve a value from a task context, or any of the mentioned types containing inline expressions (for example, string “<% \$.movie\_name %> is a cool movie!”).

**Example** In the [sample workflow](#), the token authorization credentials, REST gateway host, WFM port, and APIs are inputs for the workflow. The `validateAllApis` task uses the host, port, and API information to create a URL as an inline expression.

### 24.1.4 Output

Output is a data structure containing expressions that define workflow output. The output attribute is optional.

**Example** The output of the [sample workflow](#) is the status of the validation performed by the workflow. The expression that defines the output is created by the `publish` statements in the last four tasks of the workflow. Depending on the path performed, one of these tasks will be executed and the status will be defined.

### 24.1.5 Tasks

A task defines a specific logical step in a workflow. The actions performed by the task can take input data as needed, and produce output data, as defined by the action.

A single task is a logical step that can perform an action, for example, performing a REST request using `std.http` or CLI request using `std.ssh`. A task can call other workflows. A task can also be iterated over a list of items performing bulk operations.

**Example** The `validateAllApis` task in the [sample workflow](#) uses the `std.http` action to perform a REST request.

---

Tasks can also be chained together based on the following criteria. Tasks that are not chained are executed at the same time.

1. on-success (runs only if the task ran successfully)

- task 1
- task 2

2. on-error (runs only if the task failed)

- task 3
- task 4

**Example** In the [sample workflow](#), the `FailedApiCall` task only runs if `validateAllApis` fails.

3. on-complete (always runs)

- task 5
- task 6
- task 7

**Example** In the [sample workflow](#), the `validateWFAllAPI` task runs a set of tasks on completion.

On-success and on-error chaining run subsequent tasks at the same time. On-complete chaining runs subsequent tasks in sequence.

**Example** In the [sample workflow](#), the `validateWFAllAPI` task runs the `branchSuccess` task after the conditional `successDone` and `FailedValidation` tasks have completed.

Based on the type of action used in a task, a task requires mandatory inputs as defined by the action. For example, the `std.http` action requires the following inputs:

```
someTask:
  action: std.http
  input:
    url: 'https://<% $.rest_gateway_host %>:<% $.nsd_port%>/ports/'

  method: GET
  verify: False
  headers:
    Content-Type: 'application/json'
    Authorization: 'Bearer <% $.token %>'
  publish:
    portResult: <% task().result.content.response.data %>
```

A list of common attributes is available in the Mistral DSL v2 specification. Mistral allows task policies, conditional branching, and evaluating expression using Jinja2 or YAQL.

**Example** In the `validateWFAllAPI` task in the [sample workflow](#), the `successDone` and `FailedValidation` tasks are conditional: only one of these tasks will run depending on the value of the `length` variable.

## 24.1.6 Actions

An action has a name and input parameters, and outputs a result. A task can execute an action. It can also use the result output by an action. WFM is packaged with a set of system actions such as `std.http` and `std.ssh`. System actions cannot be deleted or modified.

You can create ad-hoc actions from system actions. An ad-hoc action is created as a wrapper around a system action, allowing you to set default values and modify the desired output of the action. Ad-hoc actions cannot be used as base actions for another ad-hoc action.

### Example of a system action

The system action `std.email` sends an email message via SMTP. Required parameters are the addresses of recipients and sender, and the SMTP server credentials. Optional parameters are the subject and body text of the email.

When this action is included in a task, the parameters must be provided as part of the task.

**Example** In the [sample workflow](#), the `validateAllApis` task executes the system action `std.http` to access an IP address using HTTP.

### Example of an ad-hoc action

The YAML for an ad-hoc action includes the base system action, the parameters for performing the action, and any input and output you need for the ad-hoc action.

For example, the standard email action requires multiple parameters. Its use can be simplified by creating an ad-hoc action. The following ad-hoc action, `error_email`, is wrapped around `std.email` action to provide the `std.email` input parameters. The only input required by the ad-hoc action is an execution id.

```
version: '2.0'

error_email:
  input:
    - execution_id
  base:std.email
  base-input:
    to_addrs: [admin@mywebsite.org]
    subject: 'Something went wrong with your workflow :('
    body: |
      Please take a look at Dashboard to find out what's wrong with your
      workflow execution
      <% $.execution_id %>.
      -- Sincerely, NSP Team
    from_addr: 'nsp@nokia.com'
    smtp_server: 'smtp.nokia.com'
    smtp_password: 'SECRET'
```

The ad-hoc action can be incorporated into a workflow:

```
nsp_workflow:
```

```
tasks:
  ...
  send_error_email:
    action: error_email execution id=<% execution().id %>
```

## 24.2 Using the WFM

### 24.2.1 Dashboard

The main dashboard shows an overview of all workflow executions. You can view the status of all running workflow executions, waiting on input action executions, failed workflow executions, and paused workflow executions, and drill down to the respective filtered lists based on the execution status. You can also view the upcoming scheduled workflows, most recently failed executions, and recent workflows.

From the main menu, you can navigate to the workflows view or drill down to other components in the workflow hierarchy.

Each view provides a list of the selected objects. From a view, you can search for, create, edit, or delete an object. Point to a list item to see a menu of object-specific options at the right of the page.

From the Dashboard menu, you can navigate to the following views:

- [Workflows](#)  
The Workflows view shows the global list of workflows created or imported to the WFM.
- [Workflow Executions](#)  
A workflow execution is an instance of an executed workflow. The Workflow Executions view shows the global list of workflow executions in the WFM.
- [Schedules](#)  
The Schedules view shows the global list of active schedules in the WFM.
- [Action Executions](#)  
The Action Executions view shows the global list of executions of actions performed by workflows. Only executions in a running or failed state are shown.
- [Actions](#)  
The Actions view lists both system and ad-hoc actions.

### 24.2.2 Workflows view

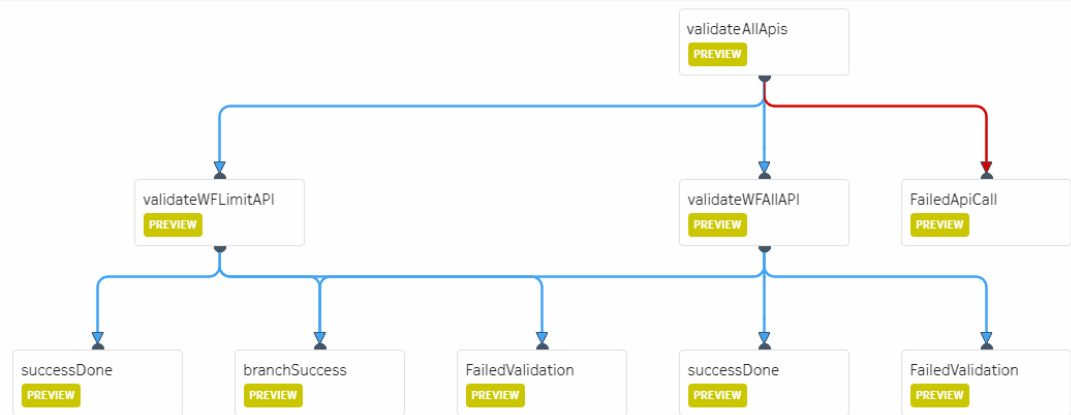
The Workflows view displays a list of the workflows that have been created or imported to the WFM. Double-click on a workflow to display the Info page for the workflow. In the left Status panel, you can view the status of running, failed, paused or success workflow executions.

You can use the Info menu to navigate to views for the selected workflow: Executions, Definition, Schedules, and Flow.

- Executions - the filtered list of executions for the workflow. You can create an execution of the workflow from this view.
- Definition - show the YAML definition

- Schedules - the filtered list of configured schedules for the workflow. You can create a schedule for the workflow from this view.
- Flow - view a graphical representation of the workflow

**Example** The following is a flow view of the [sample workflow](#).



### 24.2.3 Workflow Executions view

When a workflow is executed, an execution is created with a unique execution ID. The execution is added to the list on the Workflow Executions view. The Workflow Executions view provides a global list of workflows that have been executed using the WFM, including their inputs, outputs and state. You can create an execution of any workflow from this view.

The following operations are supported for a workflow execution:

- Modify State - you can modify the state of a running execution to paused, error, or cancelled  
**Note:** The workflow task that is currently running is not cancelled and runs to completion. No new tasks for the workflow are scheduled.
- Resume - you can resume a paused execution
- Re-run - you can start a new workflow execution with the same inputs. The execution you selected re-run from is not affected. For example, if you re-run a paused execution, the execution will remain paused and a new execution with the same inputs will be created and started.
- Delete
- Update

Double-click on an execution to display the Info page for the execution. In the left Status panel, you can view the status of running, waiting, failed, paused, or success tasks.

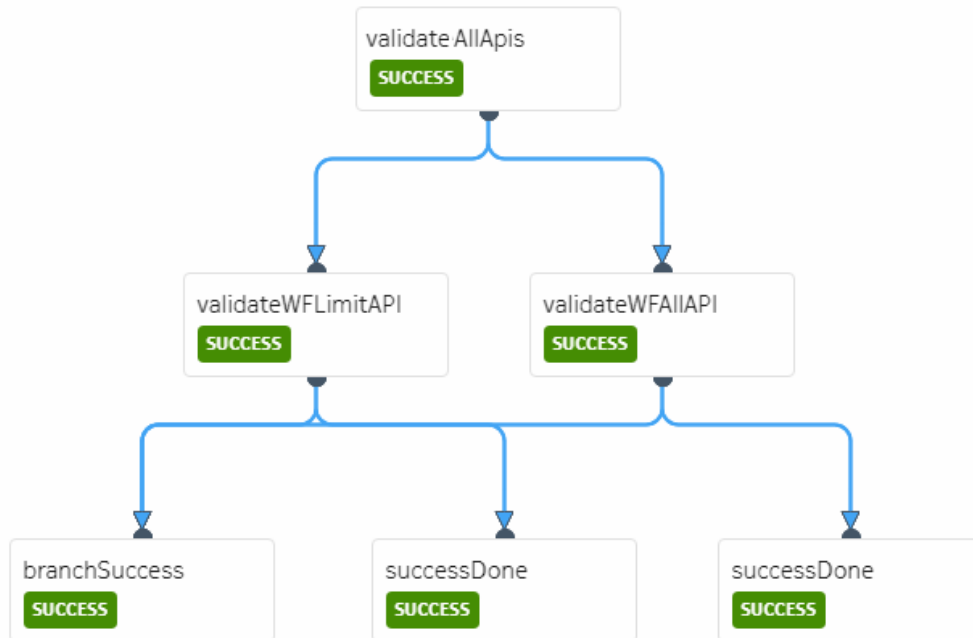
You can use the Info menu to navigate to views for the execution: Tasks, Definition, Input/Output, and Flow.

- Tasks- the filtered list of tasks performed when the execution ran.

**Example** The `FailedApiCall` task in the [sample workflow](#) only executes if `validateAllApis` fails, therefore if the `validateAllApis` task succeeded, `FailedApiCall` will not appear in the Tasks view.

- Definition - show the YAML code that was executed, including input parameters entered.
- Input/Output - show the input provided when the execution was created, and the output generated.
- Flow - view a graphical representation of the execution, including success or failure of workflow tasks. The flow view shows the path that was performed, not the full workflow.

**Example** The following is a flow view of an execution of the [sample workflow](#).



#### 24.2.4 Schedules view

Select Details for a schedule to view the input and parameters for the scheduled executions. You can create a schedule for any workflow from this view.

#### 24.2.5 Action Executions view

As a workflow proceeds, actions are executed to perform the workflow tasks. The Action Executions view shows the action executions that are currently in a running or failed state.

You can create or modify an action execution. You can perform an invoke callback operation to push the status of the action execution to running or failed.

The action executions view only shows action executions that are initiated by workflows. If you create an action execution, a dialog box will pop up with the results. Creating an action execution can be useful for testing ad-hoc actions.

---

## 24.2.6 Actions view

The Actions view shows the actions saved to the WFM application. Both system actions and ad-hoc actions are listed. You can create, edit, or delete an ad-hoc action.

## 24.3 To use workflows

### 24.3.1

The deployment of a workflow is successful only if the validation is successful. If the validation fails, the validation failure message provides information to facilitate a correct workflow.

A workflow can be imported or exported. You can import and export workflows as text files. An imported workflow must be validated before it can be saved to the WFM.

### Create or modify a workflow

1 \_\_\_\_\_

From the WFM application, choose Workflows from the main menu. A list of existing workflows appears.

2 \_\_\_\_\_

Click CREATE WORKFLOW or choose an existing workflow and click Update. The Create|Update Workflow window and YAML editor open.

3 \_\_\_\_\_

Specify a name and description for the workflow.

4 \_\_\_\_\_

Define the workflow tasks and click VALIDATE & UPDATE FLOW to check your workflow.

5 \_\_\_\_\_

Click Flow to view a graphical representation of the workflow.

6 \_\_\_\_\_

Click CREATE|UPDATE to save your workflow.  
The workflow appears in the list.

### Create or modify a workflow execution

7 \_\_\_\_\_

Choose one of the following options:

- a. To create a workflow execution, select an existing workflow and click Execute. The CREATE EXECUTION window opens.

- 
- b. To modify a workflow execution, open an existing workflow and choose Info→Executions. A list of executions appears. Select an execution and from the More menu, choose Update. The Update Execution window opens.

8

---

Provide the required information and inputs.

You can select Kafka Notification to receive events for the workflow execution states and action execution states. An event is triggered when there is a state change on execution or actions.

9

---

Click CREATE|UPDATE to start|update your workflow execution.

## Create a schedule

10

---

From the WFM application, select an existing workflow and click the Schedule icon at the right of the page. The Create Schedule window opens.

11

---

In the CONFIGURATION panel, provide a schedule name and input.

12

---

Click SCHEDULE and choose the schedule details for the workflow.

13

---

Click SCHEDULE to save your schedule.

END OF STEPS

---

## 24.4 To use actions

### 24.4.1

An action can only be deployed if it validates.

### Create or modify an action

1

---

From the WFM application, choose Actions from the main menu. A list of existing actions appears.

2

---

Click CREATE ACTION or select an existing action and click Update. The Create|Update Action window and YAML editor open.

---

**3** Define the action and click Validate to check your work.

**4** Click CREATE|UPDATE to save your work.

### **Create or modify an action execution**

**5** From the WFM application, choose Action Executions from the main menu. A list of existing action executions appears.

**6** Click CREATE ACTION EXECUTION or select an existing action execution and click Update. The Create|Update Action Execution window and YAML editor open.

**7** Provide the required information and inputs.

**8** Click CREATE|UPDATE to save your work.

An action execution list item is only created if an action is executed by a workflow. When you create an action execution, the results appear in a pop-up message but the action execution is not added to the list. You can create an action execution to test if an action will validate.

**END OF STEPS**

---



---

## 25 Cross Domain Coordinator

### 25.1 About

#### 25.1.1

The Cross Domain Coordinator application enables the automatic discovery of cross domain links between IP and optical networks. In addition, it realizes a fine-grained, multi-layer correlation of topology properties such as Shared Risk Groups (SRG) and latency to improve the IP service performance and resiliency. The application can be manually synchronized with other NSP applications, thereby achieving full integration.

### 25.2 Getting started

#### 25.2.1

This section describes procedures that are required to use the Cross Domain Coordinator application.

[25.2.2 “To configure the Network Map” \(p. 245\)](#)

[25.2.4 “To import existing cross domain links” \(p. 248\)](#)

[25.2.5 “To automatically discover cross domain links” \(p. 248\)](#)

[25.2.6 “To manually create cross domain links” \(p. 249\)](#)

[25.2.7 “To delete cross domain links” \(p. 249\)](#)

[25.2.8 “To upload or withdraw optical SLRG and/or latency” \(p. 250\)](#)

[25.2.9 “To place link sets into maintenance mode” \(p. 251\)](#)

[25.2.10 “To import existing Link Layer Interconnect links” \(p. 251\)](#)

[25.2.11 “To manually create Link Layer Interconnect links” \(p. 252\)](#)

[25.2.12 “To view Link Layer Interconnect links on a multi-layer map” \(p. 252\)](#)

[25.2.13 “To view existing optical services” \(p. 253\)](#)

[25.2.14 “To view transport controllers” \(p. 253\)](#)

[25.2.15 “To perform a diversity analysis” \(p. 253\)](#)

[25.2.16 “To export lists to CSV” \(p. 254\)](#)

#### 25.2.2 To configure the Network Map

1

---

Choose Network Map from the drop-down menu, then choose a domain from the Domains drop-down menu. The chosen domain is visualized on the map.

---

## 2

As required, click on any of the following map control buttons/sliders to customize your view:


- Fit To Screen - Automatically lay out the network map to fit within the confines of your screen
- Adjust Vertexes - Open the Vertex Controls panel
- Vertex labels - Toggles vertex labels on or off
- Vertex size - Increases or decreases the size of on-screen vertexes
- Clustering - Toggles clustering on or off
- Dynamic cluster size - Specifies whether or not the size of on-screen clusters should scale dynamically
- Cluster distance - Increases or decreases the amount of vertexes that can be contained within a single cluster
- Cluster threshold for network - Increases or decreases the number of network elements the network will support before clustering is implemented
- Cluster threshold for screen - Increases or decreases the number of network elements the application will allow to appear on screen before clustering is implemented
- Adjust Links - Opens the Link Controls panel
- Show Links - Toggles the appearance of links on the map on or off
- Link curvature - Increases or decreases the curvature of links on the map
- Link grouping threshold - Specifies the number of links that can exist between the same two vertexes before grouping is implemented
- Link increment factor - Increases or decreases the distance between links that exist between the same two vertexes
- Show link count - Toggles link counts on or off
- Zoom in - Zooms in on the map as centered
- Zoom out - Zooms out from the map as centered

---

## 3

Select an object on the map to view more information about the selected object. If a cross domain link was selected, click any of the following buttons to view a list of the specified objects:

- Navigate to IGP Links riding over this link
- Navigate to IP Services riding over this link
- Navigate to Link Layer Interconnects riding over this link

 **Note:** Navigation to IP Services is only supported for services that are marked as “NSD managed” within NFM-P and are riding over the following types of LSPs:

- With pcep-report enabled, RSVP or Segment-Routed
- With pcep-report disabled, only strict-hop RSVP LSPs for primary-path

---

4

Click on the Legend button to learn more about the icons and colors used on the map.

---

5

Click on the View Options button and perform any of the following:

1. Enable highlighting for one or more of the following:
  - Cross Domain Links
  - IP Domain
  - Optical Domain
2. If Link Layer Interconnects are present, click on the ADD LINK LAYER INTERCONNECT(S) button. A form opens:
  - Enable the Identify individual links radio button to search for individual LLI links by name, or enable the Identify all links in a group radio button to search for groups of LLI links by name.
  - Select up to five LLI links, then click DONE. The LLI links are highlighted on the map.
3. If optical services are present, click on the ADD OPTICAL SERVICES button. A form opens:
  - Select up to five optical services, then click DONE. The optical services are highlighted on the map.

---

6

Click on the Refresh Map button to reload the page.



**Note:** The UI, including the map, is automatically updated.

---

END OF STEPS

### 25.2.3 To manage clustered objects

This procedure can be used to perform a variety of actions on clustered objects. For more information about enabling clustering, see [25.2.2 “To configure the Network Map” \(p. 245\)](#).

---

1

To hide a cluster, perform the following:

1. Select a cluster, then right-click and choose Hide from the contextual menu. The cluster is hidden from the network map.
2. Click on the icon that appears at the bottom of the screen to toggle cluster visibility on or off.

---

2

To expand a cluster, perform the following:

1. Select a cluster, then right-click and choose Expand from the contextual menu. The cluster is expanded on the network map.
2. Close the popup that appears at the bottom of the screen to return the objects to a clustered state.

---

3

To filter on a cluster, perform the following:

1. Select a cluster, then right-click and choose Filter from the contextual menu. The cluster is isolated on the network map.
2. Close the popup that appears at the bottom of the screen to stop filtering on the cluster.

END OF STEPS

---

## 25.2.4 To import existing cross domain links

1

Choose Cross Domain Links from the drop-down menu, then click on the Sync with Network icon. All existing cross domain links are imported into the Cross Domain Coordinator application and appear in the list.

2

As required, perform [25.2.7 "To delete cross domain links" \(p. 249\)](#) to delete a cross domain link.

END OF STEPS

---

## 25.2.5 To automatically discover cross domain links

1

Choose Cross Domain Links from the drop-down menu, then click on the Discover Cross Domain Links icon. The Discover Cross Domain Links form opens.

2

Specify one of more LLDP discovery methods and click CONTINUE.

3

Choose a Context Type and, if required, select one or more Discovery Targets from the displayed list. Click CONTINUE.

4

Click START and monitor the Discovery Progress until completion. Close the Discover Cross Domain Links form.

5

As required, perform [25.2.7 "To delete cross domain links" \(p. 249\)](#) to delete a cross domain link.

---

6

As required, click on the Commit button inline with any discovered cross domain link to commit that link.

END OF STEPS

---

### 25.2.6 To manually create cross domain links

1

Choose Cross Domain Links from the drop-down menu, then click on the Create Physical Links icon. The Create Physical Links form opens.

2

Configure the parameters:

Parameter	Description
Description	A custom description of the cross domain link
Latency	The amount of latency for the cross domain link

3

Choose an NE and Port to serve as the First Endpoint.

4

Choose an NE and Port to serve as the Second Endpoint.

5

Click CREATE. The manually-created cross domain link appears in the list.

6

As required, perform [25.2.7 "To delete cross domain links" \(p. 249\)](#) to delete a cross domain link.

END OF STEPS

---

### 25.2.7 To delete cross domain links

1

Choose Cross Domain Link from the drop-down menu. A list of existing Cross Domain Links is displayed.

- 
- 2
- Click on the Delete button inline with any Cross Domain Link to delete that link. A dialog box opens. Perform one of the following:
- If a Link Layer Interconnect link is riding on the link, perform [Step 3](#).
  - If no Link Layer Interconnect link is riding on the link, perform [Step 4](#).

- 
- 3
- As required, enable the Delete Optical Infrastructure checkbox. When this checkbox is enabled, the underlying infrastructure of the LLI link (such as the optical services) is also deleted. If this button is not enabled, the underlying infrastructure is preserved for future use. Continue to [Step 4](#).

- 
- 4
- Click DELETE. The specified action is taken.

END OF STEPS

---

## 25.2.8 To upload or withdraw optical SLRG and/or latency

- 
- 1
- Perform one of the following:
- To upload or withdraw optical SLRG and/or latency on an IGP running over the optical network, choose Network Map from the drop-down menu. Proceed to [Step 2](#).
  - To upload or withdraw optical SLRG and/or latency on an IGP link running over the optical network, choose IP-Optical Correlation from the drop-down menu. Go to [Step 4](#).

- 
- 2
- Select a link on the map and click on the Info button. Information for that link is displayed.

- 
- 3
- Click on the Navigate to IGP Links button. A list of IGP links riding over the selected link is displayed.

- 
- 4
- Perform one of the following:
- Click on the IP-Optical Upload/Withdraw icon at the top of the screen to perform a bulk modification of IGP links.
  - Click on the IP-Optical Upload/Withdraw icon inline with an IGP link to modify that link.

- 
- 5
- Choose one of the following from the contextual menu:

- 
- **Upload SRLG** - optical Shared Risk Link Groups (SRLGs) are retrieved from transport controllers, correlated with the corresponding IP links, and exported into the NRC-P in order to ensure optical diversity
  - **Upload Latency** - optical latency information is retrieved from the NRC-T, correlated with the corresponding IP links, and propagated into the NRC-P in order to circumvent delay measurements within the IP layer
  - **Upload SRLG and Latency** - both SRLGs and Latency information are retrieved and uploaded
  - **Withdraw SRLG** - previously-uploaded SRLGs are withdrawn
  - **Withdraw Latency** - previously-uploaded Latency is withdrawn
  - **Withdraw SRLG and Latency** - previously-uploaded SRLGs and Latency are withdrawn

END OF STEPS

---

### 25.2.9 To place link sets into maintenance mode

1

---

Perform one of the following:

- a. Choose Network Map from the drop-down menu, then select a link on the map. Proceed to step [Step 2](#).
- b. Choose IP-Optical Correlation from the drop-down menu. Go to [Step 3](#).

2

---

Click on the Navigate to IGP Links button. A list of IGP links riding over the selected link is displayed.

3

---

Click on the Activate Maintenance Mode for Link Set button inline with an IGP link to place the link set into maintenance mode. A dialog box opens.

4

---

Click OK. The link set is placed into maintenance mode.

END OF STEPS

---

### 25.2.10 To import existing Link Layer Interconnect links

1

---

Choose Link Layer Interconnect from the drop-down menu, then click on the Sync with Network icon. All existing LLI links are imported into the Cross Domain Coordinator application and appear in the list.

- 
- 2 \_\_\_\_\_  
As required, click on the Delete button inline with any imported LLI link to delete that link.

END OF STEPS \_\_\_\_\_

### 25.2.11 To manually create Link Layer Interconnect links

- 1 \_\_\_\_\_  
Choose Link Layer Interconnect from the drop-down menu, then click on the Create Link Layer Interconnect icon. The Create Link Layer Interconnect form opens.

- 2 \_\_\_\_\_  
Configure the parameters:

Parameter	Description
Description	A custom description of the LLI link
Group	The name of the group to which the LLI link will belong

- 3 \_\_\_\_\_  
Choose an NE and Port to serve as the First Endpoint.

- 4 \_\_\_\_\_  
Choose an NE and Port to serve as the Second Endpoint.

- 5 \_\_\_\_\_  
Click CREATE. The manually-created Link Layer Interconnect appears in the list.

- 6 \_\_\_\_\_  
As required, click on the Delete button inline with any created LLI link to delete that link.

END OF STEPS \_\_\_\_\_

### 25.2.12 To view Link Layer Interconnect links on a multi-layer map

- 1 \_\_\_\_\_  
Choose Link Layer Interconnect from the drop-down menu. A list of existing Link Layer Interconnect links is displayed.

- 2 \_\_\_\_\_  
Click on the Multi-Layer View button inline with any LLI link to view that link on a multi-layer map, which can include the following layers (depending on the selected link):

- LLI

- 
- Switched Ethernet
  - DSR
  - Physical

3

---

Click on an LLI link in the multi-layer map to open a linear diagram. Click on any icon within the linear diagram to highlight that portion on the multi-layer map.

4

---

See [25.2.2 “To configure the Network Map” \(p. 245\)](#) for more information about the on-screen controls that can be used to configure the multi-layer map.

END OF STEPS

---

### 25.2.13 To view existing optical services

1

---

Choose Optical Service from the drop-down menu. A list of existing optical services is displayed.

2

---

As required, click on the View on Map button inline with any optical service to highlight that service on the network map.

3

---

As required, click on the Delete button inline with any optical service to delete that service.

END OF STEPS

---

### 25.2.14 To view transport controllers

1

---

Choose Controllers from the drop-down menu. The controllers with which NRC-X is interfacing are displayed.

2

---

Click on any controller to view additional details for that controller.

END OF STEPS

---

### 25.2.15 To perform a diversity analysis

1

---

Perform one of the following:

- 
- a. Choose Network Map from the drop-down menu, then click on the Diversity Analysis button. A form opens.
  - b. Choose Link Layer Interconnect from the drop-down menu, then click on the Diversity Analysis button. A form opens.

2

---

Specify the scope of the analysis, then click CONTINUE.



**Note:** In order for a diversity analysis to be performed on IP Services, the services must be marked as “NSD managed” within NFM-P and must be riding over the following types of LSPs:

- With pcep-report enabled, RSVP or Segment-Routed
- With pcep-report disabled, only strict-hop RSVP LSPs for primary-path

3

---

Click START and monitor the Diversity Progress until completion, then select a diversity group from the list to view Group Details.

4

---

Click Download Previous Diversity Report to export the results as a .csv file.

END OF STEPS

---

## 25.2.16 To export lists to CSV

1

---

Choose Cross Domain Link, IP-Optical Correlation, or Link Layer Interconnect from the drop-down menu.

2

---

Click on the More... button and choose Export. The displayed list is saved as a .csv file.

END OF STEPS

---

---

## 26 Supervision Manager

### 26.1 Overview

#### 26.1.1 Supervision Manager for Network Supervision

The Supervision Manager allows administrators to create and manage supervision groups and views for use in the Network Supervision application. The Supervision Manager can be accessed only by users with administrative access rights.

A supervision group is a logical set of monitored objects, in this case NEs and VNFs, that is specified by user-defined filters. Supervision groups can be used to partition objects into distinct categories and are associated with views. There is no limit to the number of supervision groups to which an object can belong. The criteria for monitored objects in a supervision group are based on inclusion filters. The inclusion filter is the rule on whether to include an object in a supervision group.

A view is a collection of one or more supervision groups that provides a summarized, high-level view of network objects. There is no limit to the number of views to which a supervision group can belong, but each view can contain only up to 250 supervision groups.

#### 26.1.2 Supervision Manager for Service Supervision

**i** **Note:** Supervision manager is used to create supervision groups and views for use in the Service Supervision application in shared NSP deployments, where the NSD module is installed and multiple network management applications (such as NFM-P, NFM-T, MDM, or other) are in use.

The Supervision Manager can be accessed only by users with administrative access rights.

A supervision group is a logical set of monitored objects, in this case services, that is specified by user-defined filters. Supervision groups can be used to partition objects into distinct categories and are associated with views. There is no limit to the number of supervision groups to which an object can belong. The criteria for monitored objects in a supervision group are based on inclusion filters. The inclusion filter is the rule on whether to include an object in a supervision group.

A view is a collection of one or more supervision groups that provides a summarized, high-level view of network objects. There is no limit to the number of views to which a supervision group can belong, but each view can contain only up to 5000 supervision groups.



### 26.2 Supervision groups and views for Network Supervision

#### 26.2.1

This section describes how to configure views and supervision groups for use with the Network Supervision application.



---

## 26.2.2 To create a view for Network Supervision

- 1 \_\_\_\_\_  
Ensure that Network Supervision is selected in the upper left-hand corner of the Supervision Manager GUI  . If you launched Supervision Manager from Network Supervision, it will already be selected.
- 2 \_\_\_\_\_  
On the Views list on the left-hand side of the GUI, click the Add View button  . The Add a New View form appears.
- 3 \_\_\_\_\_  
Specify a name for the view.
- 4 \_\_\_\_\_  
Enable the Automatically Creates Supervision Groups option. If the Automatically Creates Supervision Groups option is disabled, the resulting view will contain no supervision groups. You can add groups later.  
  
If the number of automatically-created groups exceeds 250, multiple views are created. In this case, all of the created views are listed.
- 5 \_\_\_\_\_  
Choose an option to create supervision groups based on Product Type or VNF Type.
- 6 \_\_\_\_\_  
Click Ok. The Supervision Manager grid is populated with supervision groups, represented as tile objects.

END OF STEPS \_\_\_\_\_

## 26.2.3 To create a supervision group for Network Supervision

- 1 \_\_\_\_\_  
Ensure that Network Supervision is selected in the upper left-hand corner of the Supervision Manager GUI  . If you launched Supervision Manager from Network Supervision, it will already be selected.
- 2 \_\_\_\_\_  
On the Views list on the left-hand side of the GUI, click on the view to which you want to add a supervision group.
- 3 \_\_\_\_\_  
On the right-hand side of the GUI, click on the Add Group button  . The Add Supervision Group form appears.

---






4

Specify a name, description, and alarm severity assignment for the group and follow the instructions in the form, clicking Continue to navigate through the pages.

---

5


In the Add NEs step, specify NEs for the group, either through inclusion filters or manually:

- **Filter NEs based on NE attributes.** Select Attribute Filter from the menu, click the Add Filter button  **FILTER**, and select an NE attribute. When the new filter appears in the list, click Add Filter  and type an attribute value. You can specify multiple attributes.
- **Filter NEs based on advanced filter expressions.** Select Advanced Filter from the menu and click on the Operator or Criteria button  **OPERATOR** to create a filter expression. Select a filter criterion and condition and then specify a value. Depending on the combination of criterion and condition, you can use additional filter functions to add to the filter expression.
- **Add NEs to the group manually.** Select Manual Entry from the menu. You can then click on the Import button  **IMPORT** to import a comma-separated list of NE management IP addresses, or click on the Add Management IP Address button  **MANAGEMENT IP** and specify an individual NE management IP address.

When you have finished configuring your filters, click Continue. The filter results are listed in the Review and Adjustments form.

---

6

Review the list of NEs to include in the supervision group. If you want to exclude any of the listed NEs, click on the Exclude button  on the item. Click Finish to save the group.

If the number of NE objects in the list exceeds 2000, multiple groups are created. In this case, all of the created groups are added to the view.

---

END OF STEPS

## 26.3 Supervision groups and views for Service Supervision


### 26.3.1

This section describes how to configure views and supervision groups for use with the Service Supervision application in shared NSP deployments, where the NSD module is installed and multiple network management applications (such as NFM-P, NFM-T, MDM, or other) are in use.

### 26.3.2 To create a view for Service Supervision


---

1

Ensure that Service Supervision is selected in the upper left-hand corner of the Supervision Manager GUI  **Service Supervision** . If you launched Supervision Manager from Service Supervision, it will already be selected.

- 
- 2 

---

On the Views list on the left-hand side of the GUI, click the Add View button  . The Add a New View form appears.
  - 3 

---

Specify a name for the view.
  - 4 

---

Enable the Automatically Creates Supervision Groups option. If the Automatically Creates Supervision Groups option is disabled, the resulting view will contain no supervision groups. You can add groups later.

If the number of automatically-created groups exceeds 5000, multiple views are created. In this case, all of the created views are listed.
  - 5 

---

Choose an option to create supervision groups based on customer ID or site ID.
  - 6 

---

Click Ok. The Supervision Manager grid is populated with supervision groups, represented as tile objects.


END OF STEPS 

---

### 26.3.3 To create a supervision group for Service Supervision

- 1 


---

Ensure that Service Supervision is selected in the upper left-hand corner of the Supervision Manager GUI  . If you launched Supervision Manager from Service Supervision, it will already be selected.
- 2 

---

On the Views list on the left-hand side of the GUI, click on the view to which you want to add a supervision group.
- 3 

---

On the right-hand side of the GUI, click on the Add Supervision Group button  . The Add Supervision Group form appears.
- 4 






---

Specify a name, description, and alarm severity assignment for the group and follow the instructions in the form, clicking Continue to navigate through the pages.

---

5


In the Add Services step, specify services for the group, either through inclusion filters or manually:

- **Filter services based on service attributes.** Select Attribute Filter from the menu, click the Add Filter button  **FILTER** , and select a service attribute. When the new filter appears in the list, click Add Filter  and type an attribute value. You can specify multiple attributes.
- **Filter services based on advanced filter expressions.** Select Advanced Filter from the menu and click on the Operator or Criteria button  to create a filter expression. Select a filter criterion and condition and then specify a value. Depending on the combination of criterion and condition, you can use additional filter functions to add to the filter expression.
- **Add services to the group manually.** Select Manual Entry from the menu. You can then click on the Import button  **IMPORT** to import a comma-separated list of service IDs, or click on the Add ID button  and specify an individual service ID.

When you have finished configuring your filters, click Continue. The filter results are listed in the Review and Adjustments form.

---

6

Review the list of services to include in the supervision group. If you want to exclude any of the listed services, click on the Exclude button  on the item. Click Finish to save the group.

If the number of services in the list exceeds 50000, multiple groups are created. In this case, all of the created groups are added to the view.

---

END OF STEPS

## 26.4 To associate a supervision group with a view

### 26.4.1

---

1

On the Views list on the left-hand side of the GUI, click on the view with which you want to associate a supervision group.


---

2

Click on the Associate button  .

---

3

In the Associate Group(s) form, click on the Add button  and type the name of a supervision group in the Name field. The list populates with near matches as you type.

---

4

Select the group name you want to associate in the list and click Done. You can repeat these steps to select more groups for association with the view.

---

5 \_\_\_\_\_  
In the Associate Group(s) form, click Associate. The group is added to the view.

END OF STEPS \_\_\_\_\_

## 26.5 To search for a supervision object

### 26.5.1

Use this procedure to search for a supervision group, view, NE, or service. The availability of search objects depends on the application from which you launched Supervision Manager.

1 \_\_\_\_\_  
Click on the Search button  .

2 \_\_\_\_\_

Select any of the available object types from the menu:

- Group
- View
- (from Network Supervision) NE - Name, Management IP, System ID
- (from Service Supervision) Service - Name, ID, Type

3 \_\_\_\_\_  
Type a search string in the text field. The list populates with near matches as you type.

4 \_\_\_\_\_  
Click Done.

END OF STEPS \_\_\_\_\_

## 26.6 To search for NEs or services with no supervision group


### 26.6.1

Use this procedure to search for NEs or services that do not belong to a supervision group. The availability of search objects depends on the application from which you launched Subscriber Manager.

1 \_\_\_\_\_  
Click on the Ungrouped NEs|Services button  .

---

**2** \_\_\_\_\_  
The Ungrouped NEs|Services form opens with a list of objects. You can filter the list contents or sort the list under a column by typing a string under the column name.

**3** \_\_\_\_\_  
Select a list item and click on the Associate button  to associate it with a supervision group.

**4** \_\_\_\_\_  
Click Close.

**END OF STEPS** \_\_\_\_\_



---

## 27 VNF Manager

### 27.1 Overview


#### 27.1.1

The VNF Manager application is the interface used for the NFM-P as VNF manager solution. The application allows you to instantiate, maintain, and terminate VNFs managed by the NFM-P. The NFM-P provides an interface with the cloud management entity that provisions cloud resources. The NFM-P validates these resources and provides assurance and monitoring through the VNF Manager application and other features in the NFV solution.

#### 27.1.2 VNF lifecycle management

The NFM-P provides an interface with OpenStack Heat to allow you to perform VNF lifecycle tasks from the VNF Manager application. You can perform the following lifecycle tasks directly from within the VNF Manager application:

- Instantiation—create a VNF instance from a specified cloud access point and a VNF catalog
- Deletion—delete a VNF instance
- Deployment—deploy a VNF instance to the cloud network
- Scaling—reduce or expand processing capacity by adding VMs to a VNF
- Healing—reboot a failing VNF component
- Sync—synchronize a VNF with the OpenStack tenant

 **Note:** Automatic scale-in is not supported.

#### 27.1.3 Product help tours

You can click on the menu in the application toolbar or on some panel toolbars to view a list of help tours. These tours are designed to explain the application features and provide workflows for completing management and monitoring tasks.

#### 27.1.4 VNF catalogs

You can use the VNF Manager application to create and manage VNF catalogs. A VNF catalog is a collection of VNFs with a template that determines the type of VNF managed. The catalog includes deployment specifications, KPIs, and recipes for VNF management functions that are applicable to the VNF type. These become the default VNF settings that are defined when you instantiate a VNF using the catalog. You are able to configure these settings for specific VNFs during VNF instantiation.

You can create the following types of VNF catalogs:

- Generic
- VMG

- VMM
- VSR
- VSR-I

In addition to specifying the catalog type, you must also define a directory name. The directory name specifies the VNFD directory where the HOT files are located. The VNF Manager automatically determines the catalog type and version based on the HOT files in the specified directory. You must configure a VNF catalog before you create a VNF object.

**Generic VNF catalogs**

While the VMG, VMM, and VSR catalog types include deployment settings and recipes specific to each NE type, the generic VNF catalog can be used for other NE types without node-specific settings. The onboarding, instantiation, and lifecycle management functions of generic VNF catalogs are the same as for the NE-specific catalogs. You must specify a VNFD directory and configure HOT template files for a generic VNF catalog.

**27.1.5 Cloud access point**

The VNF Manager application provides an interface with OpenStack for VNF management. You must define a cloud access point before you create a VNF object. You can use multiple cloud access points for VNFs under different tenants. For each cloud access point, you must provide login credentials for the tenant group and specify a Keystone URL. Specify an access URL, port number, and Keystone version in the format *http://127.227.135.61:5000/v2.0*.

The cloud access point defines parameters such as VNFC image/flavor and network/subnet ID, which are configurable during VNF instantiation.

**27.1.6 VNF management**

The VNF Manager application provides an at-a-glance view of VNFs and VNFCs in the network. VNF onboarding allows the application to archive, upload, and validate VNF software images with OpenStack Heat.

The following table describes the lifecycle management tasks that can be executed from the VNF Manager application.

*Table 27-1 VNF lifecycle management tasks*

Task	Description
Add	Instantiates a new VNF. You must choose a catalog and cloud access point when you create a new VNF.
Delete	Deletes a VNF.
Deploy	Deploys the VNF to OpenStack Heat. Newly instantiated VNFs are not automatically deployed. The Deployment State parameter shows whether the VNF has been deployed.

Table 27-1 VNF lifecycle management tasks (continued)

Task	Description
Scale-out	Increases processing capacity by adding a VM. You must specify the scaling template from the drop-down menu. The scale-out template defines the type and number of VNFCs to be added.
Scale-in	Decreases processing capacity by removing a VM. You must specify the scaling template from the drop-down menu. The scale-in template defines the type and number of VNFCs to be removed.
Sync	Synchronizes the VNF with OpenStack Heat.
Rescan Discovery Rule	Manually scan VNF discovery rules for new rule elements.
Reboot	Reboots the VNF component. The Reboot button is available from the VNF component list that opens when you select an VNF.

### Manual scaling



#### CAUTION

#### Service Disruption

*The manual scale-in function removes a VM without checking the node for subscribers. Nokia recommends you check the VM for subscribers and move them to another VM before using the scale-in function.*

You can use the VNF Manager application to manually scale-in or scale-out to adjust the processing capacity of a VNF. When you use a scaling operation, you must select a scaling template to use. Each scaling template specifies a type and number of VNFCs to be scaled in or out. The scale-in and scale-out operations use the same scaling templates.

These scaling templates are defined by the `VNF_Type.userdef_chars.grow.hot.yaml` files in the `grow` sub-directory of the VNF catalog directory. The name of the scaling templates must specify the applicable VNF. A VMG scaling template must lead with `VMG` in the template name and a VMM scaling template must lead with `VMM`. For example, a scaling template designed to scale one load balancing VNF on a CMG might be named `CMG.1LB.grow.hot.yaml`. Nokia recommends that the template name specify the number and type of VNFCs to be scaled.

**i** **Note:** The `userdef_chars` part of the template filename cannot contain a period.

For automatic scaling, the NFM-P looks for a file with the name `VNF_Type.default.grow.hot.yaml`.


You can include a `grow_meta_data` entry in the meta file to specify which parameters are user-configurable during a VNF scaling operation in the VNF Manager application. For example, you can include `gw_subnet` in the `grow_meta_data` entry to allow the user to specify a subnet during VNF scale-out.


### 27.1.7 VNF instantiation

The VNF Manager application uses VNF catalogs to instantiate VNFs on a cloud management system such as OpenStack. When you use the application to instantiate a VNF, you must specify a cloud access point which includes a cloud management system URL to which the NFM-P deploys the VNF. The VNF catalog selected during VNF instantiation defines the default settings that are required by the VNFD for lifecycle management operations. These settings are read from the catalog `.env.yaml` file. You can customize these settings for a specific VNF during instantiation, as required.

The cloud access point provides the list of available VNFC images and flavors. You can select the required images and flavors from drop-down menus during VNF instantiation.

You can also configure the System Address during VNF instantiation. These parameters uniquely identify the VNF. Alarms affecting the VNF or associated VNFCs list these parameters as System Name and Site ID.

 **Note:** The instantiated VNF is not deployed until you click Deploy.

 **Note:** The system address provided for the VNF should match the system address configured in the NE.

#### Initial configuration for CMG and VSR

During VNF instantiation, you can specify an initial configuration file for the CMG and VSR. Specify an FTP server address with the configuration file using the `primary_config` parameter. You must also specify the login credentials, system name, and SNMPv2 or SNMPv3 community string. The configuration file is uploaded to the file storage specified for the VNF instance. When the VNF is instantiated, it is automatically configured with the specifications in the initial configuration file.

#### Topology discovery rules

During VNF instantiation, you can specify a topology discovery rule for VSR, CMG, or VMM. If no discovery rules are defined, you can cross-launch the NFM-P Java GUI to create one. The NFM-P automatically creates a discovery rule element for the VNF once the VNF is successfully deployed. You can also manually trigger a discovery rule scan by clicking the Rescan Discovery Rule button. The ready-only Managed State identifies whether the VNF is managed by a discovery rule.

When the VNF is deleted, the NFM-P automatically removes the discovery rule element.

### 27.1.8 VNF component reboot

You can use the Reboot function to manually reboot a VNF component from the application GUI. To view a list of VNF components associated with a VNF, double-click the VNF. When you click the Reboot button, you can select a soft or hard reboot.

The read-only Task State parameter on the VNF component shows whether the component has any NFM-P component operations in progress. VNF component can be triggered only if the Task State parameter is Deployed. The read-only VM State parameter displays the OpenStack VM state. VNF component operations — such as reboot — can be performed only if the VM State parameter is Active, ShutOff, or Rescued.

---

### 27.1.9 VNF component evacuation

You can perform VNF component evacuation to move a VNF component to a new compute host. This functionality is useful if a VNF component goes down due to a compute host failure. This action does not reboot the VNF.

VNF component evacuation is available from the VNF Manager REST API only.

### 27.1.10 VNFD redundancy

The NFM-P supports redundancy for the HOT files that define the lifecycle management tasks performed by the VNF Manager application. These files are kept in the `<NFMP_INSTALL_DIR>/os` directory and require NFM-P administrator read/write privileges. Whenever an rsync operation is triggered, files in the directory with a `.yaml`, `.txt`, `.sh`, and `.json` extension are duplicated into a standby file server. Changes in the `<NFMP_INSTALL_DIR>/os` directory on the active server are duplicated every 30 minutes by default.

### 27.1.11 REST API

The VNF Manager application publishes a set of URLs which point to resources, or web services, managed by them. The URLs that are available to users are documented. These URLs can be accessed through a browser by any authorized user, including OSSs which can use them to cross launch from their own application. To view the published URLs of a given application:

```
http(s) ://<host>/VNFManager/api-docs
```

Where *host* is the hostname or IP address which hosts the application.



---

## 28 Device Administrator

### 28.1 Overview

#### 28.1.1

The Device Administrator application allows a user to define mediation policies and discovery rules so that network elements can be discovered through MDM in NSP and used by MDM-aware NSP applications. See the *NSP Deployment and Installation Guide* for information about how to manage device adaptation in MDM.

Network scans are performed at intervals configured in NE discovery rules, or discovery can be triggered manually.

### 28.2 Workflow for using the Device Administrator application

#### 28.2.1

This workflow outlines the sequence of actions required to discover NEs in Device Administrator.

- 1 \_\_\_\_\_  
Configure the node to enable discovery by NSP; see the node documentation.
- 2 \_\_\_\_\_  
Create an NE Reachability Policy; see [28.3 "To create an NE reachability policy" \(p. 270\)](#).
- 3 \_\_\_\_\_  
Create a mediation policy for each protocol you will use to communicate with the NE; see [28.4 "To create a mediation policy" \(p. 271\)](#).  
**NOTE:** A mediation policy is required for each protocol that will be used to manage the NE, regardless of which protocols will be used for the discovery.
- 4 \_\_\_\_\_  
Create an NE discovery rule; see [28.5 "To create an NE discovery rule" \(p. 272\)](#).
- 5 \_\_\_\_\_  
View discovered NEs; see [28.6 "To view discovered NEs" \(p. 274\)](#).
- 6 \_\_\_\_\_  
View or edit policies; see [28.7 "To view or edit policies" \(p. 274\)](#).

---

7

View or edit discovery rules; see 28.8 “To view or edit NE discovery rules” (p. 275).

END OF STEPS

---

## 28.3 To create an NE reachability policy

### 28.3.1

1

In the Device Administrator application, click on Reachability Policies. The system displays the list of existing reachability policies.

2

Click CREATE REACHABILITY POLICY. The Create Reachability Policy form opens.

3

Configure the required parameters.

Parameter	Description
Policy Name	The name of the Reachability policy
Reachability Type	Specifies the communication type to be used to confirm reachability, for example, ping
Interval (minutes)	Specifies the length of time, in minutes, to wait before repeating an attempt to reach the NE
Timeout (seconds)	Specifies the length of time, in seconds, to wait for a response after attempting to reach the NE
Admin State	Specifies the administrative state for the new policy
Description	User-provided description of the policy

4

Click Create. The reachability policy is auto-assigned a policy ID and added to the list.

END OF STEPS

---

## 28.4 To create a mediation policy

### 28.4.1

A mediation policy is required for each network communication protocol that will be used to manage the NE. Mediation policies for all required protocols must be created before discovery, regardless of which protocols will be used to discover the NE.

A mediation policy consists of a network user and a network communication profile, or set of communication parameters. You can associate users or communication profiles with multiple policies. For example, if two different network users (that is, two sets of credentials) might be used to log in to the same port using CLI over Telnet, create a policy of type CLI for each user. When you create the second policy, associate the communication profile you created for the first policy. This will apply the same CLI parameters to the policy for the other user.

1 \_\_\_\_\_

In the Device Administrator application, click on Mediation Policies. The system displays the list of existing mediation policies.

2 \_\_\_\_\_

Click CREATE MEDIATION POLICY. The Create Mediation Policy form opens.

3 \_\_\_\_\_

Configure the required parameters.

Parameter	Description
<b>Left panel</b>	
Mediation policy type	Specifies the communication type the mediation policy is for, for example, SNMPv3.
Mediation policy name	The name of the mediation policy
Description	User-provided description of the policy
<b>Middle panel</b>	
Associate network communication profile (radio button)	Configure this radio button to use the communication profile parameters from an existing mediation policy. Use the Search field to find the name of the associated profile you want to use.
Create new network communication profile (radio button)	Configure this radio button to configure new communication protocol parameters. The parameters will vary based on the mediation policy type.
<b>Right panel</b>	

Parameter	Description
Associate network user (radio button)	Configure this radio button to use a network user from an existing mediation policy. Use the Search field to find the name of the network user you want to use.
Create new network user (radio button)	Configure this radio button to configure a new network user. The parameters will vary based on the mediation policy type.

4

Click Create. The mediation policy is auto-assigned a policy ID and added to the list.

END OF STEPS

## 28.5 To create an NE discovery rule

### 28.5.1

1

In the Device Administrator application, click on NE Discovery Rules. The system displays the list of existing discovery rules.

2

Click CREATE DISCOVERY RULE. The Create NE Discovery Rule step form opens.

3

Configure the required parameters. Click Continue to proceed to the next set of parameters.

Parameter	Description
<b>1: Settings and Discovery Protocol Order</b>	
<i>Settings</i>	
Rule name	The name of the discovery rule
Description	User-provided description of the discovery rule
Network Scan Interval (minutes)	Specifies the interval, in minutes, at which the network scan repeats
Admin State	Specifies the administrative state for the discovery rule
<i>Discovery Protocol Order</i>	

Parameter	Description
(First Second Third Fourth) discovery protocol	Specify the protocols to be used to communicate with the NE, in the order in which they should be used to attempt to reach the NE for discovery  Enter all the protocols that will be used for communication, regardless of whether they will be used for discovery.
<b>2: Set Discovery IP Range</b>	
Include	Click Add IP Range to specify an IP address and mask bits to include. Repeat to add additional ranges.
Exclude	Click Add IP Range to specify an IP address and mask bits to exclude from discovery. Repeat to add additional ranges.
<b>3: Associate Mediation Policies</b>	
Mediation Policies	Click on each protocol listed in the left panel. Mediation policies for the protocol are listed in the right panel. Select a policy for each protocol by clicking the plus sign at the right of the panel.  You can create a mediation policy from this view if needed; see <a href="#">28.4 "To create a mediation policy"</a> (p. 271).
<b>4: Associate Reachability Policies</b>	
Reachability Policies	Click on each reachability type listed in the left panel. Reachability policies are listed in the right panel. Select a policy for each type by clicking the plus sign at the right of the panel.  You can create a reachability policy from this view if needed; see <a href="#">28.3 "To create an NE reachability policy"</a> (p. 270).

4

Click Finish. The NE discovery rule is auto-assigned a rule ID and added to the list.

END OF STEPS

---

## 28.6 To view discovered NEs

### 28.6.1

- 1 \_\_\_\_\_  
In the Device Administrator application, click on Discovered Nodes. The system displays the list of discovered NEs.
- 2 \_\_\_\_\_  
To filter the list, enter information in any filter field in the top panel.
- 3 \_\_\_\_\_  
To remove a filter, delete information from the filter field.
- 4 \_\_\_\_\_  
Hover your mouse over an NE to see the Unmanage and Resync icons at the right of the screen. Click on an icon to unmanage or resync the NE.  
If a device is unmanaged, it is removed from the list. The NE can be discovered again if a compatible discovery process is performed.

END OF STEPS \_\_\_\_\_

## 28.7 To view or edit policies

### 28.7.1

- 1 \_\_\_\_\_  
In the Device Administrator application, click on Mediation Policies or Reachability Policies. The system displays the list of configured policies of the selected policy type.
- 2 \_\_\_\_\_  
To filter the list, enter information in any filter field in the top panel.
- 3 \_\_\_\_\_  
To remove a filter, delete information from the filter field.
- 4 \_\_\_\_\_  
Hover your mouse over an NE to see the Edit, Delete, and Show Detail icons.
  - Click Edit to change policy parameters.  
Click Update to save your changes.
  - Click Delete to delete the policy.
  - Click Show Detail to display a read-only panel with the policy parameters.

---

Mediation policy details include the number of NEs using the policy as a read, read and write, or trap policy. Click on an item to display a filtered list of NEs using the policy in the selected manner.

END OF STEPS

---

## 28.8 To view or edit NE discovery rules

### 28.8.1

1

---

In the Device Administrator application, click on NE Discovery Rules. The system displays the list of configured NE discovery rules.

2

---

To filter the list, enter information in any filter field in the top panel.

3

---

To remove a filter, delete information from the filter field.

4

---

Hover your mouse over an NE to see the Edit, Delete, Show Detail, and More icons.

- Click Edit to change discovery rule parameters.  
Click Update to save your changes.
- Click Delete to delete the rule.
- Click Show Detail to display a read-only panel with the rule parameters. Click on the icons at the top of the panel to display IP ranges or policies.
- From the More menu you can edit, delete, or show detail. The More menu also includes Discover and Show Discovered NEs.
  - Choose Discover to manually launch a discovery.
  - Choose Show Discovered NEs to display a filtered list of NEs discovered using the selected NE discovery rule.

END OF STEPS

---

