NSP
Network Services Platform

Release 23.11

Network and Service Assurance Guide

3HE-18967-AAAA-TQZZA
Issue 1
December 2023

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Legal notice

Nokia is committed to diversity and inclusion. We are continuously reviewing our customer documentation and consulting with standards bodies to ensure that terminology is inclusive and aligned with the industry. Our future customer documentation will be updated accordingly.

This document includes Nokia proprietary and confidential information, which may not be distributed or disclosed to any third parties without the prior written consent of Nokia.

This document is intended for use by Nokia’s customers (“You”/”Your”) in connection with a product purchased or licensed from any company within Nokia Group of Companies. Use this document as agreed. You agree to notify Nokia of any errors you may find in this document; however, should you elect to use this document for any purpose(s) for which it is not intended, You understand and warrant that any determinations You may make or actions You may take will be based upon Your independent judgment and analysis of the content of this document.

Nokia reserves the right to make changes to this document without notice. At all times, the controlling version is the one available on Nokia’s site.

No part of this document may be modified.

NO WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY OF AVAILABILITY, ACCURACY, RELIABILITY, TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, IS MADE IN RELATION TO THE CONTENT OF THIS DOCUMENT. IN NO EVENT WILL NOKIA BE LIABLE FOR ANY DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL OR ANY LOSSES, SUCH AS BUT NOT LIMITED TO LOSS OF PROFIT, REVENUE, BUSINESS INTERRUPTION, BUSINESS OPPORTUNITY OR DATA THAT MAY ARISE FROM THE USE OF THIS DOCUMENT OR THE INFORMATION IN IT, EVEN IN THE CASE OF ERRORS IN OR OMISSIONS FROM THIS DOCUMENT OR ITS CONTENT.

Copyright and trademark: Nokia is a registered trademark of Nokia Corporation. Other product names mentioned in this document may be trademarks of their respective owners.

© 2023 Nokia.

Contents

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Displaying alarms 75

Investigating alarms 81

Managing alarms 84

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

About this document

Purpose

The *NSP Network and Service Assurance Guide* shows you how to monitor and troubleshoot your network for optimal performance. It introduces the Network Services Platform, or NSP, to technology officers and network operators by describing the tools used for network performance monitoring, including NE and service KPIs, alarm management, OAM testing, performance plots, and map views.

Scope

The NSP Network and Service Assurance Guide information primarily describes elements that are common to all NSP deployments, but may also include high-level information about optional NSP functions that are separately licensed and deployed.

Document support

Customer documentation and product support URLs:

- Documentation Center
- Technical support

How to comment

Please send your feedback to Documentation Feedback.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

1 Monitoring network health

Network Health view

1.1 What is the Network Health view?

1.1.1 What do I see in the Network Health view?

The Network Health view provides a dashboard of essential information relating to the proper function of your network. It presents an abbreviated view of equipment and service alarms, root cause alarms, graphical plots of service-affecting network object counts, and network object status.

You can cross-launch from objects in the dashboard to a variety of NSP functions. The function that is launched depends on the object context. For example, you can open the alarm list from an alarm object. Cross-launched functions open in a separate GUI.

Clicking on certain objects in the Network Health view takes you to a different within the view. For example, clicking on the Affected Services KPI icon in the Service Health dashlet takes you to a detailed list of affected services in the Network Inventory.

The data in all views of the Network Map and Health dashboard is updated every 30 seconds.

1.2 How do I get a quick view of my network health?

1.2.1 Network KPIs

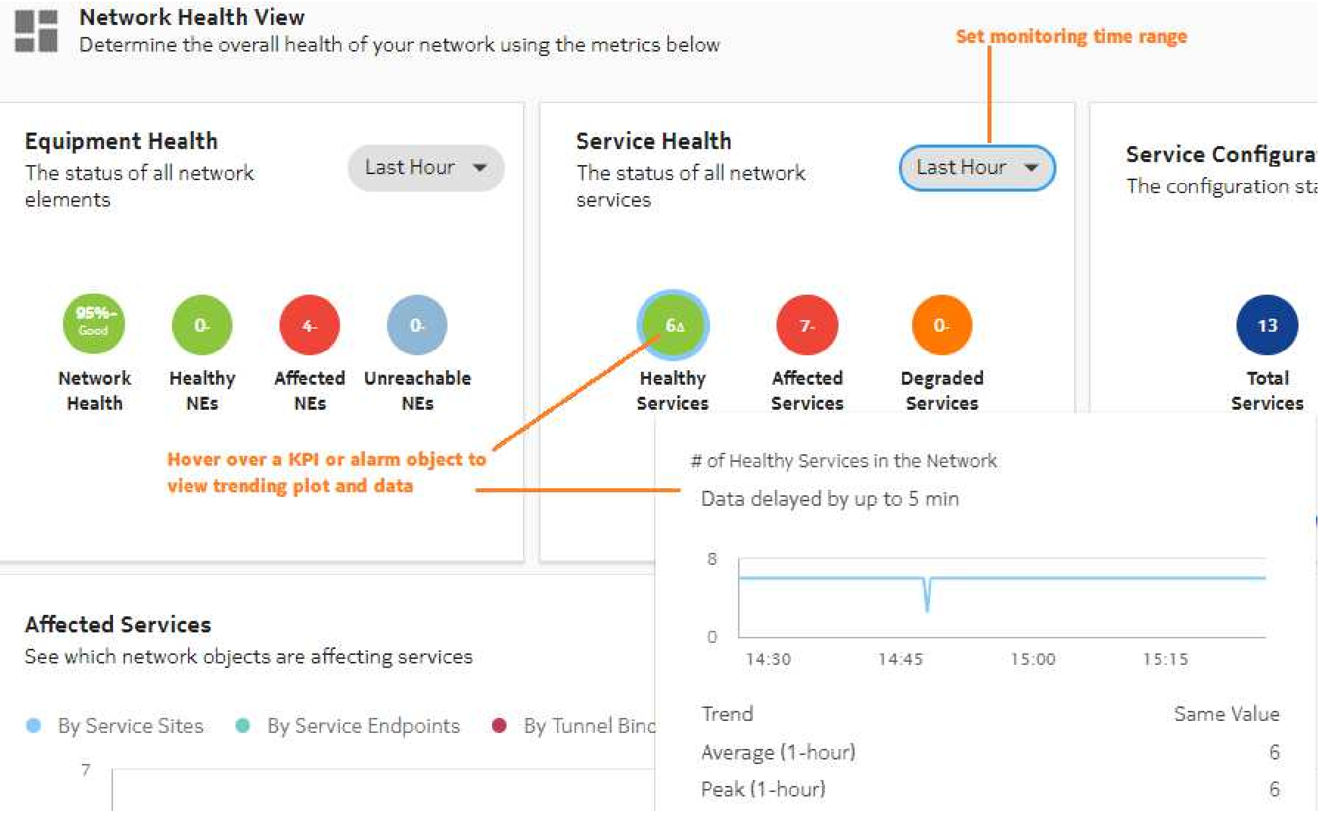
The Network Health view pulls KPI and alarm information from various NSP components to show you the status of your network equipment and services.

A selection of NE and service KPIs are displayed in dashlets:

- The **Network Health** KPI is a percentage calculated by dividing the number of healthy NEs by the total number of NEs (healthy, affected, and unreachable). Click on this KPI to go to the Network Elements list.
- The **Healthy NEs** or **Healthy Services** KPIs refer to the number of NE or service objects that have no associated components (cards, ports, service sites, service endpoints, or tunnel bindings) that are operationally down. Click on this KPI to go to the Network Elements list or Services list, filtered by the Affected Objects count (set to zero).
- The **Affected NEs** or **Affected Services** KPIs refer to the number of NE or service objects that have one or more components that are operationally down. Click on this KPI to go to the Network Elements list or Services list, filtered by the Affected Objects count.
- The **Degraded Services** KPI refers to the number of services
- The **Unreachable NEs** KPI refers to the number of NEs whose communication state is set to Partial or Down. Click on this count to go to the Network Elements list, filtered by Communication State set to either Partial or Down.

Information in the Network Health view is refreshed every 30 seconds.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms



1.2.2 Network monitoring workflow

Use the following dashboard features to expand on your network health investigation:

- **List network objects:** View all Network Elements for a KPI in the Network Inventory; see 1.3 “How do I list all objects for a KPI?” (p. 11).
- **List misaligned services:** See 1.4 “How do I list misaligned services?” (p. 11)
- **List alarms:** Investigate alarm KPIs; see 1.5 “How do I check network alarms?” (p. 12).
- **View KPI trending:** View a graphic plot of a KPI; see 1.6 “How do I check KPI trending?” (p. 12).
- **Cross-launch to another GUI:** See 1.7 “How do I cross-launch to another GUI?” (p. 13)

1.2.3 How does UAC affect objects in the Network Map and Health view?

An operator’s visibility of network equipment is based on User Access Control settings, which are configured by an administrator. Depending on your access settings, some equipment may not be visible. See your network administrator for more information.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

1.3 How do I list all objects for a KPI?

1.3.1 Purpose

You can list all of the network objects associated with a KPI indicator in a dashlet in the Network Health view.

1.3.2 Steps

1

Open Network Map and Health, Network Health View.

2

In the Equipment Health dashlet, click on a KPI icon.

You are taken to an expanded list of objects related to the KPI in the Network Inventory.

3

Return to the Network Health view by clicking the Previous View icon.

END OF STEPS

1.4 How do I list misaligned services?

1.4.1 Purpose

You can list all network services whose configuration in NSP is different from what is configured on NEs. The list open in Service Management.

1.4.2 Steps

1

Open Network Map and Health, Network Health View.

2

In the Service Configuration Health dashlet, click the **Misaligned Services** KPI icon to list misaligned services.

A list of misaligned services opens in Service Management.

3

Return to the Service Configuration Health dashlet by clicking the Previous View icon.

END OF STEPS

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

1.5 How do I check network alarms?

1.5.1 Purpose

You can cross-launch from the Alarm Summary dashlet to the Alarm List.

1.5.2 Steps

You can list network root cause alarms, filtered by severity.

1

Open Network Map and Health, Network Health View.

2

In the Alarm Summary dashlet, click an alarm KPI icon.

The alarm list opens, filtered by the KPI you clicked.

END OF STEPS

1.6 How do I check KPI trending?

1.6.1 Purpose

You can check the Trend value for KPI behavior from the present time, looking back over the period specified in the Time Range drop-down list.

1.6.2 Steps

1

Open Network Map and Health, Network Health View.

2

In the Equipment Health, Service Health, or Alarm Summary dashlet, hover over a KPI icon.

A graphic plot displays the KPI over the specified time range, along with KPI Trend, Average, and Peak values.

The Trend value can be:

- Increasing: more objects/resources have been affected over time
- Decreasing: fewer objects/resources have been affected over time
- Delta: the number of affected objects/resources has fluctuated over time, but is currently the same as the initial value (at the beginning of the time range)

Because the plot is meant to display average KPI values, the Peak value may not always appear.

END OF STEPS

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

1.7 How do I cross-launch to another GUI?

1.7.1 Purpose

Some Network Health dashlets include a cross-launch link to open the dashlet information in the NSP GUI it is sourced from.

1.7.2 Steps

1

Open Network Map and Health, Network Health View.

2

In a dashlet, click the **View in...** cross-launch link.

The dashlet data is displayed in expanded format in an external NSP GUI.

End of steps

1.8 How do I set my network monitoring time range?

1.8.1 Purpose

You can specify the time range over which each Network Health dashlet gathers network data.

1.8.2 Steps

1

Open Network Map and Health, Network Health View.

2

Click on a dashlet Last 6 Hours ▾ **Time Range** filter and select a time range from the drop-down list.

End of steps

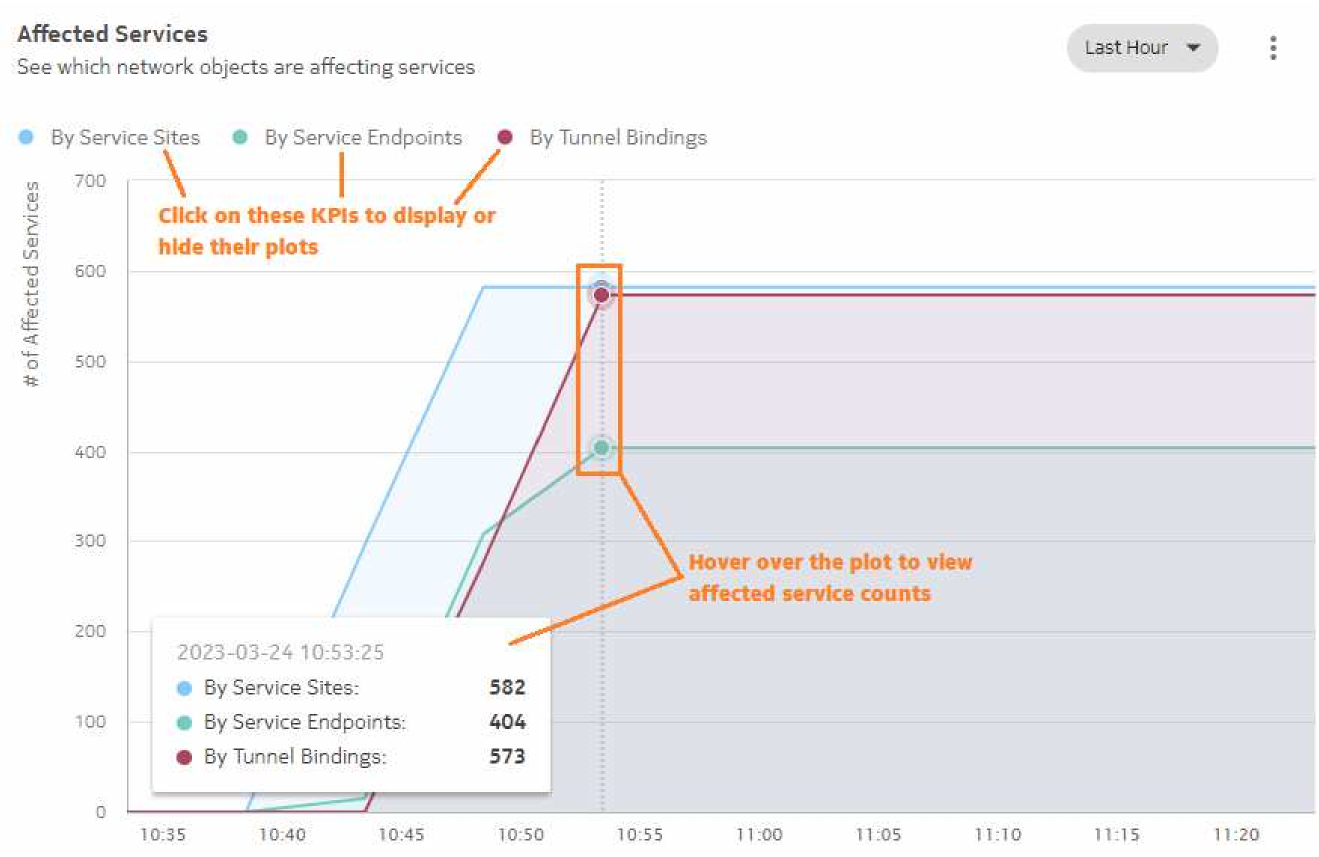
1.9 How do I track affected service levels?

1.9.1 Affected Services plot

The Affected Services dashlet tells you which network objects are affecting the function of your services. Service sites, service endpoints, and tunnel bindings are plotted separately against the number of services they are affecting over the specified time range.

You can display or hide plots by clicking on the **By Service Sites**, **By Service Endpoints**, or **By Tunnel Bindings** options to display or hide their plots on the graph.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms



1.9.2 To access the Affected Services dashlet

1

Open Network Map and Health, Network Health View.

The Affected Services dashlet appears at the bottom of the Network Health view.

End of steps

1.9.3 Network monitoring workflow

Use the following dashlet features to expand on your network health investigation:

- **Scan affected service counts:** Hover over the plot to view the affected service count by network object at a given time point. The affected service counts update as you move the cursor to the left or right along the plot.

  Because of the scale of the affected service plots, small fluctuations in affected service counts may not be visible in the plots.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- **List service-affecting objects:** view network objects that are affecting your services; see 1.10 “How do I list service-affecting network objects?” (p. 14)

1.10 How do I list service-affecting network objects?

1.10.1 Steps

1

Open Network Map and Health, Network Health View.

2

In the Affected Services dashlet, click ⋮ **More**, **Show [Service Sites | Service Endpoints | Tunnel Bindings] Affecting Services**.

A list of the selected object type opens in the Network Inventory.

3

Return to the Affected Services dashlet by clicking the Previous View ⬆ icon.

End of steps

1.11 What is Simplified RAN Transport?

1.11.1 SRT

The SRT is a solution for T-BTS management that merges management of RAN and transport components of a 4G/5G wireless network. Network monitoring components of SRT exist as a dashlet on the Network Map and Health dashboard to provide a single view of T-BTS transport features and RAN application bindings to IP transport services.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

News Feed

1.12 How do I view alarms in the News Feed?

1.12.1 Recent network events

The News Feed provides a live feed of unacknowledged root cause network alarms, as they occur in real time. Alarm severity levels of Warning, Minor, Major and Critical are displayed.

1.12.2 To access the News Feed

1

Open Network Map and Health, Network Health View.

The News Feed appears on the right-hand side of the Network Health view.

END OF STEPS

1.12.3 Troubleshooting workflow

You can cross-launch from an alarm object in the News Feed to an alternate NSP view to see more information about the alarm or the network object it originated from. Click More ⋮ on an alarm and select a cross-launch option. Cross-launch view availability varies depending on originating object for the alarm.

1.13 How do I stop/start automatic updates in the News Feed?

1.13.1 Purpose

The News Feed is automatically updated every 30 seconds. You can switch to manual updates.

1.13.2 Steps

1

Open Network Map and Health, Network Health View.

2

In the News Feed dashlet, click **More** ⋮, **Set To Manual Refresh** to stop automatic News Feed updates. A manual update button is added to the New Feed that you can click as needed.

When in manual update mode, you can click **More** ⋮, **Set To Auto Refresh** to return to automatic updates.

END OF STEPS

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

1.14 How do I change the News Feed sort order?

1.14.1 Steps

1

Open Network Map and Health, Network Health View.

2

In the News Feed dashlet, click on the **Sort** filter and select a sorting rule.

The News Feed is reordered according to the new sorting rule.

END OF STEPS

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Watchlist

1.15 How do I monitor network objects in the Watchlist?

1.15.1 Purpose

The Watchlist opens from the Network Map and Health dashboard or Object Troubleshooting dashboard to a separate browser tab. It allows you to monitor a shortlist of NEs and services that you want to keep under scrutiny and access easily. Objects in the Watchlist display basic KPIs, and the Trending indicator tells you if an object's condition is changing.

You add network objects to the Watchlist from the operational map view and from object lists in the Network Inventory.

Information in the Watchlist is refreshed every 30 seconds.

1.15.2 Object status trending

An object in the Watchlist displays a Trending indicator that tells you if the object is stable or affected by problems:

- An upward trending arrow ↗ means the object is impacted by new issues.
- A downward trending arrow ↘ means the number of issues impacting the object is diminishing.
- A flat trending indicator — means the object's condition has remained unchanged.

1.15.3 To open the Watchlist

1

Open Network Map and Health, Network Health View.

2

On the toolbar, click **Watchlist**.

3

The Watchlist opens in a separate browser tab, displaying network objects set for monitoring.

End of steps

1.15.4 Troubleshooting workflow

- From an affected object in the Watchlist click **More**, **View in Object Troubleshooting**.
  The Object Troubleshooting dashboard to displays complete status information for the object.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

1.16 How do I set the trending KPI for NEs in the Watchlist?

1.16.1 Purpose

You can specify which type of KPI is indicated by the Trending indicator for NE objects in the Watchlist.

1.16.2 Steps

1

Open Network Map and Health, Network Health View.

2

On the toolbar, click **Watchlist**.

3

On the toolbar, click ⚙**Watchlist Settings**.

4

In the Watchlist Settings form, select an NE KPI from the drop-down list.

5

Click **Save**.

END OF STEPS

1.17 How do I stop/start automatic updates in the Watchlist?

1.17.1 Purpose

The Watchlist is refreshed every 30 seconds. You can switch to manual updates.

1.17.2 Steps

1

Open Network Map and Health, Network Health View.

2

On the toolbar, click **Watchlist**.

3

In the Watchlist, click **List Actions** ⋮, **Set To Manual Refresh** to stop automatic Watchlist updates. A manual update button is added to the Watchlist that you can click as needed.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

When in manual update mode, you can click **List Actions ⋮**, **Set To Auto Refresh** to return to automatic updates.

END OF STEPS

1.18 How do I adjust the Watchlist contents?

1.18.1 Purpose

You can filter the Watchlist to display only certain object types, and you can change the sort order of the list.

1.18.2 Steps

1

Open Network Map and Health, Network Health View.

2

On the toolbar, click **Watchlist**.

3

Do either of the following:

- Click the **Filter** chip and select **Service**, **NE**, or **Service and NE** from the drop-down list.
  The list contents adjust to show only the object type(s) selected.
- Click the **Sort** chip and select **Object Type** or **Name** from the drop-down list.
  The list sort order changes to follow the selected criterion.

END OF STEPS

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Network Map

1.19 How to I check network health in the Network Map?

1.19.1 Map view

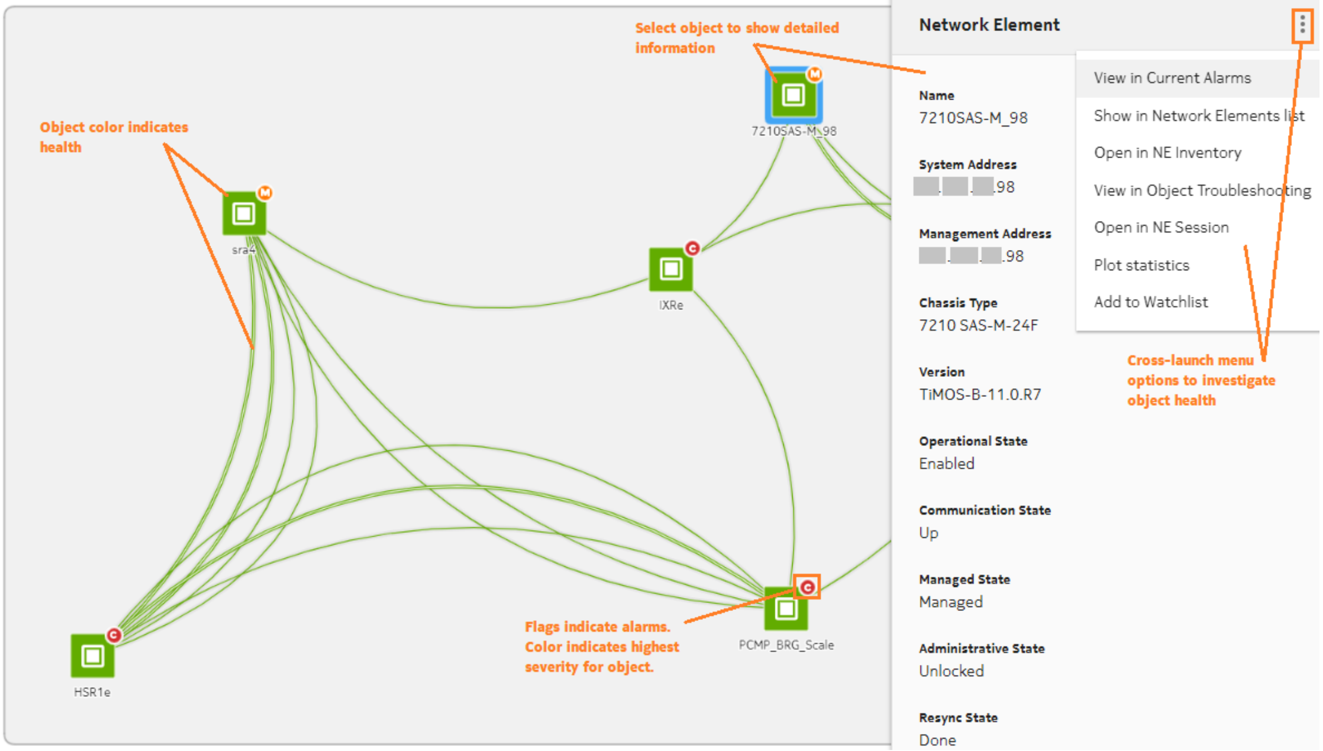
The Network Map is a geographical map of your network equipment. NEs are grouped into geographical regions and zones. The map can be zoomed out to the regional or continental level, or zoomed in to the city street level, providing precise information about network equipment locations.

> **Note:** Administrative users can view subnets and links to subnets as objects on the Network Map. Non-administrative users whose access rights are defined through UAC cannot view subnets and links to subnets because the Network Map is intended to display networking equipment. Subnets are not actual equipment.
>
> The Network Map does not support LLDP links with endpoints with the destination MAC address set to Nearest Customer.

Alarm and status information in the Network Map is automatically refreshed from the network every 30 seconds. You can update the map display manually by clicking ⟳ **Refresh**. The Refresh command can take significant time on large networks. Use it only if there have been changes to the NSP common map layout and you want them to appear in the Network Health view, or if the map data is stale (in which case you are prompted to refresh the map).

If a region titled NEs Without a Region appears on the map, it is an auto-created region containing NEs that exist in the Network but have not been not grouped under a specific region. Your administrator must place the NEs in a region.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms



Select object to show detailed information

Object color indicates health

Flags indicate alarms. Color indicates highest severity for object.

Cross-launch menu options to investigate object health

Network Element

Name
7210SAS-M_98

System Address
[redacted].[redacted].[redacted].98

Management Address
[redacted].[redacted].[redacted].98

Chassis Type
7210 SAS-M-24F

Version
TiMOS-B-11.0.R7

Operational State
Enabled

Communication State
Up

Managed State
Managed

Administrative State
Unlocked

Resync State
Done

1.19.2 Map object clustering for small networks

In small NSP deployments of fewer than 2000 NEs and 3000 links, where no common map layout is configured, map objects are automatically clustered, based on their proximity. If the object limits are exceeded, The Network Map displays an error message, indicating that the administrator must configure a common map layout, dividing NEs into regions.

1.19.3 Network monitoring workflow

Use the following dashlet features to expand on your network health investigation:

- Search for an object in the map; see 1.21 “How do I search for an object in the map?” (p. 23).
- Examine an NE in an external GUI; see 1.23 “How do I view information about an object in the map?” (p. 24).
- View network layers; see 1.20 “How do I view multiple network layers in the Network Map?” (p. 23).

1.20 How do I view multiple network layers in the Network Map?

1.20.1 Multi-layer map view

The Multi-layer map view shows the relationships between equipment objects in various layers of the network; for example, the physical layer and the IGP layer. The IGP layer is displayed for physical NEs contained in a single resource group where the corresponding IP links and routers can span over multiple administrative domains. You can see how problems in one layer may be affecting, or affected by, other layers.

The Multi-layer map view shares similar functionality (object information, view options) with the Operational map view.

To access the Multi-layer map view:

1. Open Network Map and Health, Network Map View.
2. Select **Multi-layer** from the **View** drop-down list.

1.21 How do I search for an object in the map?

1.21.1 Steps

1

Open Network Map and Health, Network Map View.

2

Click **Find in Map** ⌖. Select an object type from the drop-down list and type a search string. You can click on an entry in the results list to go to the object's location in the map layout.

END OF STEPS

1.22 How do I view the NEs in a map region?

1.22.1 Steps

1

Open Network Map and Health, Network Map View.

2

Double-click on a region to expand it and view its NEs.

To return to the top-level map view, click on the left-most item in the map breadcrumb.

END OF STEPS

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

1.23 How do I view information about an object in the map?

1.23.1 Purpose

You can view information about NEs or links in the map, either in short-form in a pop-up window, or in detail in separate NSP GUI.

1.23.2 Steps

1

Open Network Map and Health, Network Map View.

2

To display basic identification and status information for a map object, hover over the object.

The information appears in a pop-up window.

3

To view detailed information about an object in an external NSP view, right-click on the object and select one of the following options (options vary, according to object type):

Cross-launch options for NEs

- **View In Current Alarms** opens the Current Alarms list for the NE.
- **Show In Network Elements list** displays the NE in the Network Inventory, Network Element list.
- **Open In NE Inventory** displays an NE in the Device Management, NE Inventory on a separate browser tab, along with all configured objects.
- **Open in Object Troubleshooting** displays the NE in the Object Troubleshooting dashboard with detailed performance and alarm information.
- **Open in NE Session** opens a Telnet session with the NE.
- **Plot Statistics** displays KPI plots for the NE in the Data Collection and Analysis view.
- **Add to Watchlist** adds the NE to the Watchlist view for monitoring.

Cross-launch options for links

- **View In Current Alarms** opens the Current Alarms list for the link.
- **Show in Link List** displays the link in the Network Inventory, Link list.

END OF STEPS

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

1.24 How do I filter the map view?

1.24.1 Purpose

You can configure filters in the map to control the display of information and reduce clutter. The Operational map view allows filtering, with or without the Utilization option. You can add up to five filters.

1.24.2 Steps

1

In the map, click **Add Filter** and select one of the filter types. A chip filter Alarm Severity: Minor × is added to the map.

In the Operational map view, the filter types are Alarm Severity, Chassis Type, Network Type, Product Type, and Status. You can add up to three filters. If the Utilization option is enabled, the filter types are Utilization and Capacity.

2

Click **Filter** and select a criterion related to the filter type.

The chip filter is applied to the map.

3

Click × **Close** on a chip filter to remove it from the map.

END OF STEPS

1.25 How do I customize my map view?

1.25.1 Purpose

You can set your own zoom level and adjust the behaviour and appearance of the map and objects using the Map Palette controls. You can also save your personal map layout settings so that they are retained in your future NSP sessions, or restore the map to the default common layout.

1.25.2 Steps

Use the Map Palette controls on the map palette to adjust the map layout. When objects share the same physical location, the map shows a multi-layered icon shaded in blue. To see the co-located objects individually, drag them off of the multi-layered icon.

1

Open Network Map and Health, Network Map View.

2

Adjust the Map Pallette controls, as described in the table below.

Table 1-1 Map Palette controls

Fit to Screen	Click this option to zoom the map to fit the selected region to available screen area.
Clustering controls	Map cluster display options for **region-based** map (available when a common map layout is configured in NSP): • Options to display NE cluster health as a pie chart or a solid circle on the cluster. Object color indicates health. • Display or hide region and zone boundaries. Click **Show More** to access the following options: • Option to move all contained objects when moving a region or zone. • Group NEs external to a region or zone with their immediate parent zone or region; the map displays all connectors to zones or subzones that contain the external NEs. This option shows greater detail. • Group external NEs with their top-level region; the map displays a single connector to the region icon. This option shows less detail. Map cluster display options for **cluster-based** map (available in network of fewer than 2000 NEs and 3000 links, where no common map layout is configured in NSP): • Option to arrange NE into clusters, based on proximity • Options to display NE cluster health as a pie chart or a solid circle on the cluster. Object color indicates health. Click **Show More** to access the following options: • Option to adjust cluster inclusion range. • Option to adjust the cluster creation threshold for the entire network. • Option to adjust the cluster creation threshold for what is visible on the screen.
Adjust vertices	Adjust vertices as follows: • Show/hide text labels for map objects. • Adjust icon size for NEs, zones, and regions.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table 1-1 Map Palette controls (continued)

Adjust Links	Adjust link display as follows: • Show or hide links between NEs, zones, and regions. • Show or hide links when the objects they connect to are outside the map view. • Adjust link curvature (i.e., how deep of an arc) between objects. • Adjust link grouping threshold. Click **Show More** to access the following options: • Options to display link group health as a pie chart or a solid circle on the group. Object color indicates health. • Show or hide the number of links in a group.
Map View	Turn on Bird’s-eye View (shows the entire map in a small inset in the corner). Adjust the opacity of the background map.
− —●— + Zoom	Zoom into and out from the map.

END OF STEPS

1.25.3 Steps

Save your personalized map layout or restore it to the default layout.

1

Click **More** ⋮, **Save As My Layout** to save the map display settings as they are currently configured.

If you want to return to the default map display settings, click **More** ⋮, **Restore To Default Layout**.

END OF STEPS

1.26 How to do I check link utilization in the map?

1.26.1 Link utilization

The Network Map has a Utilization view option that shows how much available capacity is being utilized on network links. The Utilization view lets you quickly assess how efficiently your network is managing traffic, and identify links that are over- or under-utilized. Utilization is displayed as colored arrows on link objects. Network utilization can be analyzed in the Network Map for all links in a link group.

The Utilization view option supports a limit of five active users at any one time. If more than five users are accessing the Utilization view, You will see a notification.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Information in the Utilization view is based on port egress statistics collected for IP links on Ethernet physical ports. Statistics must be supported and available for utilization to be displayed; see 1.31 “How are utilization statistics collected?” (p. 32).

The Utilization view option displays usage data for the following link types:

- Point-to-Point (IP / IGP / CUPS)
- LAG
- Cross-domain
- Radio microwave
- Optical

The Utilization view option supports physical map layout and region-based clustering, but region and zone icons cannot be opened while in the Utilization view option is enabled.

The Utilization Map shows NEs connected by link lines that represent physical connections between endpoints. When you hover over a link, its utilization level is displayed in the object tooltip. The links have the following features:

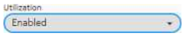
- **Thickness**. The relative capacity on the link is indicated by a thin, medium, or thick line. Thinner lines indicate lower capacity, thicker lines indicate higher capacity. Link capacity is based on the operational port speed configured for the port.
- **Color**. Physical links between endpoints 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.
- **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 about 5%) 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 utilization statistics are not supported on an NE, traffic may be present, but no utilization arrow is displayed.

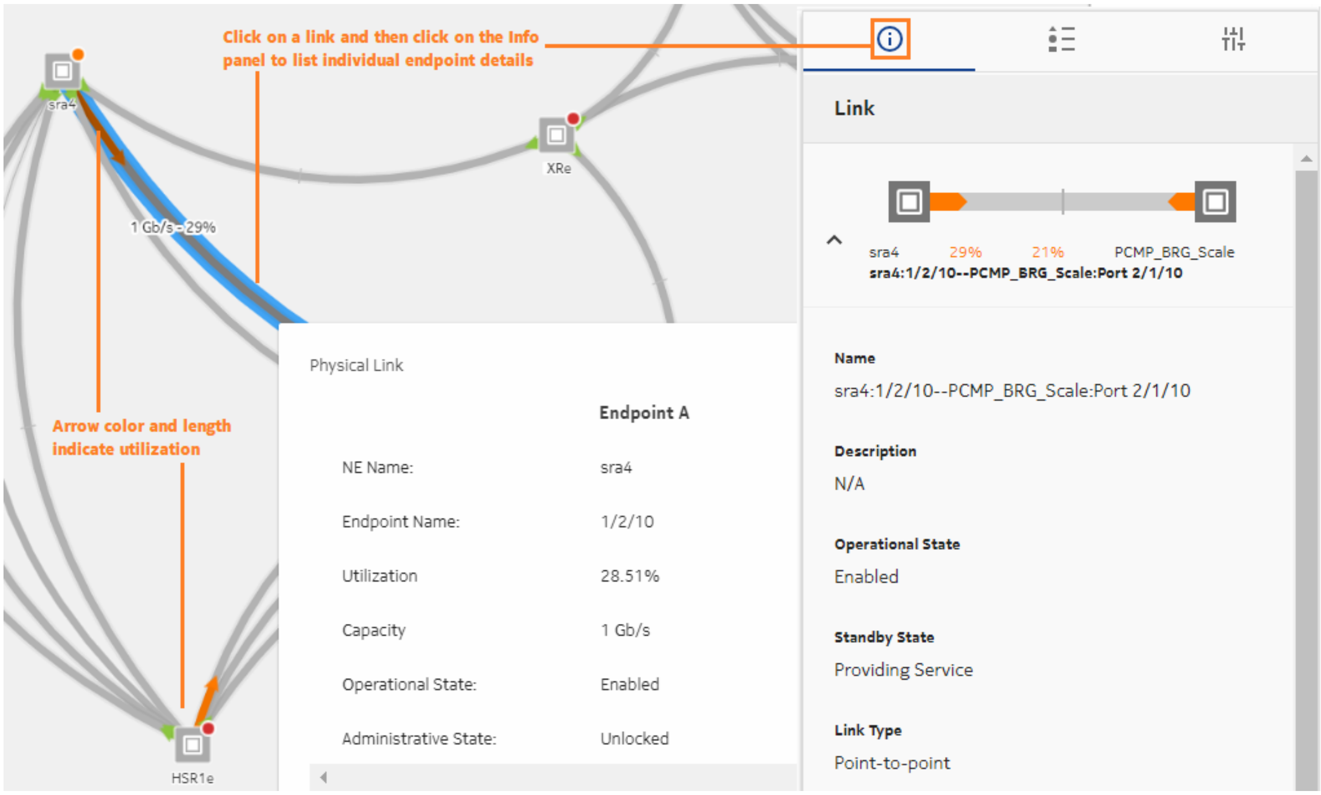
1.26.2 To display link utilization

1. Open Network Map and Health, Network Map View.
2. Double-click a region or zone object to display the links you want to monitor.
3. Click  **Utilization**, **Enabled** in the Network Map.

   Utilization data is displayed on the links.
4. Hover over a link to display its utilization information in brief, as a pop-up.

1.26.3 Detailed link information

You can click on a link and display detailed information relating to links and individual endpoints on the Info panel.



Click on a link and then click on the Info panel to list individual endpoint details

Arrow color and length indicate utilization

Physical Link

	Endpoint A
NE Name:	sra4
Endpoint Name:	1/2/10
Utilization	28.51%
Capacity	1 Gb/s
Operational State:	Enabled
Administrative State:	Unlocked

Link

sra4 29% 21% PCMP_BRG_Scale
sra4:1/2/10--PCMP_BRG_Scale:Port 2/1/10

Name
sra4:1/2/10--PCMP_BRG_Scale:Port 2/1/10

Description
N/A

Operational State
Enabled

Standby State
Providing Service

Link Type
Point-to-point

1.26.4 Managing link utilization map performance

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

- If the number of links in the resource group is large, there may be a delay before the **Utilization** view option if fully enabled.

  To maintain system performance and to avoid exhausting available statistics counters, consider creating groups of no more than 50 NEs for the purpose of link utilization monitoring. Your system administrator can create and modify resource groups.
- Statistics are collected by subscription from qualified ports. If there are too many qualified ports in the resource group, performance may be affected. For information about Utilization map scale limits, see the *NSP Planning Guide*.
- Be aware that Utilization map performance can also vary based on the number of subscriptions and on other telemetry gathering in the NSP system.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

1.27 How do I highlight links by type in the map?

1.27.1 Purpose

The Network Map provides an option to highlight selected link types, using colors to identify the type of link. View options are available in the Operational view of the map. You can highlight the following link types:

- Copper: Ethernet link using coaxial copper cable
- Fiber: Ethernet SFP link using optical fiber cable
- LAG N+0: LAG link without protected ports
- LAG N+N: LAG link with member ports protected (supported for Wavence NEs only)
- Protected: protected radio link (supported for Wavence NEs only)
- Unprotected: unprotected radio link (supported for Wavence NEs only)

1.27.2 Steps

1

Open Network Map and Health, Network Map View.

2

Click **Highlight** to open the Link Highlight Options panel.

3

Click on the link types in the list to **Enable** or **Disable** highlighting for each. The links on the map show colors indicating the link type.

END OF STEPS

1.28 How do I configure manual links in the Network Map?

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

1.28.1 Steps

1

Click ⋮ **More**, **Create Manual Link** to open a list of manually-created physical links in the Network Map.

2

In the Create Manual Link form, specify the **Name**, **Description**, **Latency**, and **Link Type** for the link.

3

Click **Add** to specify endpoints for the link.

4

Specify the endpoint type (NE or port) for the link.

5

In the Add Two Network Elements|Ports form, click on two items to select them in the left-hand list. You can search the list by specifying name or address strings in the fields at the top of the list.

As you select items in the list, they appear in the right-hand list.

6

When you have selected two endpoints, click **Add**.

7

In the Create Manual Link form, click **Create**.

END OF STEPS

1.29 How do I access cross-domain links in the Network Map?

1.29.1 Purpose

Cross-domain links between IP and optical equipment are shown on topology maps as dashed lines, and on multi-layer maps as solid lines. They are also included in the Network Inventory Links list.

You can access a list of optical services that terminate on the optical endpoint of a cross-domain link. The list shows information about those optical services, and provides additional options.

1.29.2 Steps

1

To open a list of optical services in the map:

1. Open Network Map and Health, Network Map View.
2. Select a cross-domain link on the map.
3. Open the ⓘInfo panel.
4. In the Info panel, click ⋮ **More**, **Show Optical Services**. A list of optical services that terminate on the optical endpoint of the cross-domain link is displayed.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2

To open a list of optical services from the Links dashlet:

1. Open Network Map and Health, Network Inventory.
2. Expand the Links list and select a cross-domain link in the list.
3. Click ⋮ **Table Row Actions** , **Show Optical Services**. A list of optical services that terminate on the optical endpoint of the cross-domain link is displayed.

END OF STEPS

1.30 How do I optimize map performance?

1.30.1 Map object limits

Consider the following performance information when working in map views.

Nokia recommends a maximum of 2000 NEs per region for the Operational map view. The Multi-layer map view is limited to a maximum of 4000 objects for the entire network.

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

1.31 How are utilization statistics collected?

1.31.1 Map statistics collection

Information in the Utilization map is based on port egress 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.

Utilization statistics are collected from NEs using SNMP for NFMP NEs and gRPC for MDM NEs.

When a user switches from the Operational Map to the Utilization Map, the first two telemetry subscriptions listed below are created. If LAG links are present on the map, the third subscription listed below is created.

1. Subscription for SNMP and MDM managed NEs and ports on the current map.

   SNMP-managed 7750 SR family NEs respond to the filter.

   The following MDM-managed NEs respond to the filter: 7750 SR, 7250 IXR / VSR(I), 7450 ESS, and 7950 XRS

   This subscription determines utilization directly from the output-utilization statistic counter.
2. Subscription for SNMP managed 7705 SAR and 7210 SAS NEs and ports on the current map.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

This subscription calculates utilization from the following statistics: operational-speed, transmitted-broadcast-packets-periodic, transmitted-multicast-packets-periodic, transmitted-octets-periodic, and transmitted-unicast-packets-periodic.

SNMP utilization statistics are calculated from NFM-P counters using this formula:

```
output-utilization(%) = (transmittedTotalOctetsPeriodic +
((transmitted-unicast-packets-periodic +
transmitted-multicast-packets-periodic +
transmitted-broadcast-packets-periodic) * 20)) *
8/t/operational-speed/1000 * 100
```

Where **t** is the collection interval in seconds, as specified in the Utilization Map preferences.

3. Subscription for SNMP-managed NEs and LAG links on the current map.

   This subscription calculates utilization from the following statistics: speed, transmitted-broadcast-packets-periodic, transmitted-multicast-packets-periodic, transmitted-octets-periodic, and transmitted-unicast-packets-periodic.

   SNMP utilization statistics are calculated from NFM-P counters using this formula:

   ```
   output-utilization = (transmitted-octets-periodic +
   ((transmitted-unicast-packets-periodic +
   transmitted-multicast-packets-periodic +
   transmitted-broadcast-packets-periodic) * 20)) *
   8/t/operational-speed/1000 * 100
   ```

   Where **t** is the collection interval in seconds, as specified in the Utilization Map preferences.

For SNMP, NEs must be managed by the NFM-P and reachable using SNMP. The following are used for utilization data:

- MIB name: TIMETRA-PORT-MIB
- MIB entry name: tmnxPortEtherEntry
- MIB counter name: tmnxPortEtherUtilStatsOutput
- Statistics group: Additional Ethernet Stats
- Counter: utilStatsOutput (in centi-percent)

The following NEs support the required SNMP statistics for the Utilization map:

- 7250 IXR
- 7450 ESS
- 7750 SR and VSR
- 7950 XRS

For MDM, the following gRPC schema path is used for utilization data:

- /state/port[port-id]/ethernet/statistics/out-utilization

SR OS NEs support the required MDM statistics for the Utilization map. The supporting chassis types are:

- 7250 IXR
- 7450 ESS

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- 7750 SR
- 7950 XRS

1.31.2 Utilization statistics for the 7705 SAR and 7210 SAS

The following (periodic) counters are used for utilization calculation for the 7705 SAR and 7210 SAS:

- MIB name: IF-MIB
- MIB entry name: ifXEntry
- MIB counter names: ifHCOutOctets, ifHCOutUcastPkts, ifHCOutMulticastPkts, ifHCOutBroadcastPkts
- NFMP statistics group: Interface Additional Statistics
- NFMP counters: transmittedBroadcastPackets, transmittedMulticastPackets, transmittedTotalOctets, transmittedUnicastPackets

The following information is used to establish a reference speed:

- MIB name: TIMETRA-PORT-MIB
- MIB entry name: tmnxPortEtherEntry
- MIB counter name: tmnxPortEtherOperSpeed (mbps)
- NFMP class: equipment.PhysicalPort
- NFMP counter: actualSpeed (kbps)

1.32 What is a Simplified Microwave Router?

1.32.1 Simplified microwave router

In networks where multiple Wavence UBT-SA devices are linked to a single 7250 IXR or 7705 SAR NE, the NSP provides a Simplified Microwave Router (SMR). To facilitate network monitoring, the SMR shows the router and its linked UBTs, including CA (Carrier Aggregated) UBTs, as a single logical site with the following display features:

- The Network Map shows the NE and its linked UBT-SAs as a single router NE; the UBT-SAs are not displayed.
- KPIs, and current and historical alarms on UBT-SAs are propagated to the linked router.
- The NE Inventory shows the UBT-SAs as child objects of the router, under Radio Equipment.
- You can cross-launch to the external EMS for UBT-SA devices by right-clicking on their object in the NE Inventory.
- You can search for a UBT-SA object using the object name or IP address.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

1.33 How do I open a CLI session with an NE?

1.33.1 Purpose

You can open an NE session from menus in the following Network Map and Health dashboard locations:

- the information panel for a selected NE on the Network Map
- NEs in the Network Inventory

There is typically a brief delay before the **Open in NE Session** menu item becomes active.

ⓘ **Note:** Opening an NE session requires that your access privileges include execute permission for the selected NE. See your network administrator for more information.

1.33.2 Steps

1

Open Network Map and Health, Network Health View.

2

Perform one of the following:

a. To open a session from the Network Map: Click on the NE in the map, then click ⓘ **Info** to open the Information panel. Click ⋮ **More**, **Open in NE Session**.

b. To open a session from the Network Inventory, Network Elements list: On a list item, click ⋮ **More**, **Open NE Session**.

An NE Session form opens in a new tab.

3

Click **CONNECT**. NEs that are managed using MDM only use the session type configured in the CLI mediation policy. For SSH sessions with NEs managed using NFM-P, a Login window appears.

4

Enter the username and password for the NE in the Login window for an SSH session, or in the terminal window for a Telnet session.

5

Click **DISCONNECT** when your session is finished to log out and close the session.

END OF STEPS

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Network Inventory

1.34 What does the Network Inventory show me?

1.34.1 Access network objects

The Network Inventory is a repository of network objects, categorized and listed with basic information in dashlets. You can view the contents of an object list by expanding its dashlet to full screen width, displaying the full list with full status information.

The data in the Network Inventory is updated every 30 seconds. You can switch to manual updates in the enlarged object list views.

1.34.2 Expanded object lists

You can expand an object list dashlet to the full width of your browser window, with detailed data displayed for each list item in columnar format. The auto-refresh function is turned off by default when you switch to expanded or full-screen display.

To expand a Network Inventory dashlet: Click ⤢**Expand Size** to display an object list dashlet in a larger format with more information. When in expanded display, you can click ⋮ **Size Settings and Actions**, **Restore Size** to return to compact display.

The expanded object list has a variety of tools available to help you control what you see, including sorting and filtering options:

- **Enable automatic updates:** Click ⋮ **Size Settings and Actions**, **Set to Auto Refresh** to start automatic data updates.

  When in automatic update mode, you can click ⋮ **Size Settings and Actions**, **Set to Manual Refresh** to return to manual data updates. In manual update mode, a chip at the top of the list displays the most recent data update. Click on the chip for a manual data update.
- **View detailed information about a list item:** On a list item, click ⋮ **Table Row Actions** and select the NSP GUI in which to view the object.
- **Filter the object list under a specific column:** Type a text string in the text field or select a filter option at the top of a column.

  The object list automatically updates with filter results as you type your filter string.

  Where applicable, click ▼ **Filter Menu** next to the text field, select an operator from the drop-down list, and type a filter string.

  Next to the column headers, click **Table Setting and Actions** ⋮ , **Clear Filters** to clear column filters.
- **Sort the object list under a specific column:** Click on a column header to sort the list under that column. Click on the header again to toggle between ascending and descending sorting.

  Next to the column headers, click ⋮ **Table Setting and Actions**, **Clear Sorting** to clear column sorting.
- **Export the object list:** Next to the column headers, click ⋮ , **Table Setting and Actions**, **Export Selected** to export the current page or selected rows to a CSV, XLXS, or XML file.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

1.34.3 Network monitoring workflow

You can cross-launch from objects in Network Inventory expanded lists to other NSP views. Cross-launch availability varies depending on the object type. The following table lists the cross-launch commands available for various objects, and the NSP view that opens for each command.

Table 1-2 Cross-launch options from Network Inventory objects

Cross-launch command	Opens NSP view	Available for objects
View In Current Alarms	Current Alarms List	NEs, Links, Ports, Service Sites, Service Endpoints, Tunnel Bindings
Open In NE Inventory	Device Management, Inventory view	NEs, Ports
Show In Network Map[1]	Network Map	NEs and Links
View in Object Troubleshooting	Object Troubleshooting dashboard	NEs, Links, Ports, Service Sites, Service Endpoints, Tunnel Bindings
Open in NE Session	CLI	NEs
Plot Statistics	Data Collection and Analysis Visualizations	NEs
Plot Utilization Statistics	Data Collection and Analysis Visualizations	Links and Ports
Plot Error Statistics	Data Collection and Analysis Visualizations	Links and Ports

Notes:

1. The Network Map does not support cross-launch for LLDP links with endpoints with the destination MAC address set to Nearest Customer.

1.35 How do I manage LSPs in the Network Inventory?

1.35.1 Purpose

You can monitor and create LSPs from the LSPs dashlet in the Network Inventory. The LSPs dashlet is hidden by default. You must modify the Network Map and Health dashboard to display the LSPs dashlet in the Network Inventory; see “How do I customize a dashboard?” in the *NSP User Guide*.

The LSPs dashlet can display up to 50 000 LSPs.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

1.35.2 Prerequisites

Before you can perform this procedure, the following prerequisites must be completed.

1. Obtain the Predefined IETF Intents zip file and the data sync artifact bundle (nsp-mdt-intents-23.11.*xx*-rel.*xx*-tunnel-mapping-bundle.zip).
2. Import the IETF intent types into NSP; see “How do I import an intent type from my computer?” in the *NSP Network Automation Guide*.
3. Install the data sync artifact bundle; see “How do I install an artifact bundle?” in the *NSP Network Automation Guide*.
4. If you will be creating LSPs through the IETF-TE-TUNNEL model, run the IETF_Yang_Intent_Mapping request by selecting the IntentMapping.json from Postman.
5. Create a configuration template using the `icm-te-tunnel` intent type. The name of the template must be DefaultLspTemplate. See “How do I create a configuration template” in the *NSP Device Management Guide.*

1.35.3 To create an LSP

1

Open Network Map and Health, Network Inventory View.

2

In the LSPs dashlet, click ⋮ **Size Settings and Actions**, **Create LSP**.

The Deploy Logical Configuration form opens in Device Management, with the DefaultLspTemplate selected.

3

Configure your LSP; see “How do I create a logical configuration deployment?” in the *NSP Device Management Guide*.

END OF STEPS

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Subscriber Monitoring

1.36 What is the Subscriber Monitoring view?

1.36.1 Subscriber monitoring

The Subscriber Monitoring View provides you with KPIs and statistics for BNG/FWA CUPS NEs with MD interfaces. The Subscriber Monitoring View lets you see NE information in the control and user planes, and provides subscriber session statistics. Sites are listed by subscriber count, and by OSDA pools usage.

Note: The Subscriber Monitoring view is hidden by default. You must modify the Network Map and Health dashboard to display the Subscriber Monitoring dashlets; see “How do I customize a dashboard?” in the *NSP User Guide*.

The view displays subscriber information through the following dashlets

- BNG/FWA CUPS Summary - the number of control plane (active and standby) and user plane NEs in the network.
- User Plane Peer Connectivity - the number of user plane NE Peer Connections at CP level that are operationally Up versus Down.
- Subscriber Performance Metrics - total number of active subscribers. Click the Number of Subscribers KPI to list the associated subscriber sites in an expanded Sites by Subscriber Count list.
- Sites by Subscriber Count - list of active control plane and user plane sites by subscriber count.
- BNG/FWA CUPS Network Elements - list of BNG/FWA CUPS NEs.
- PFCP Peer View - list of PFCP peers.
- Sites by ODSA pools usage - list of active control plane sites by ODSA pool usage.
- RADIUS Group Peer Usage - usage statistics for RADIUS group peers.
- RADIUS Group Peer Metrics - list of control plane active sites by RADIUS group peer metrics.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2 Troubleshooting network objects

2.1 What is the Object Troubleshooting dashboard?

2.1.1 Object troubleshooting

The Object Troubleshooting dashboard allows you to check the performance of a selected service object or piece of network equipment. The view allows you to view summarized performance information, and to drill down into specific objects and view performance details, opening objects in external views where necessary.

The data in the Object Troubleshooting dashboard is updated every 30 seconds.

You can search for objects to troubleshoot under the following contexts:

- Network Elements
- Services
- Ports
- Links
- Radio planes

2.2 How do I troubleshoot a network object?

2.2.1 Purpose

When you open the Object Troubleshooting view, you must specify what type of object you want to troubleshoot and then select a specific object. Once you have selected an object, you are taken to a troubleshooting dashboard with performance details for the object.

If you are already in an object troubleshooting summary dashboard and want to examine a different object, click **Change Target** an select a new object as described from Step 2 below. If you want to return to an object you had previously opened in the Object Troubleshooting dashboard, click ⟲**History** and select an object from the drop-down list.

2.2.2 Steps

1

Open Object Troubleshooting.

The Select a Troubleshooting Target form opens in the Troubleshooting Summary dashboard.

2

Select the type of object you want to troubleshoot from the **Target Type** drop-down list.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3

To filter the Troubleshooting Target list contents, select a search criterion from the drop-down list Port Name ▾, type a search string in the field and click **Add Filter**.

The list is reduced to the filtered items. You can configure up to two more filters if needed.

4

Select the object you want to troubleshoot from the Troubleshooting Target list.

5

Click **Choose**.

A Troubleshooting Summary dashboard opens. Depending on the type of object you selected, the dashboard contains different selections of dashlets and views.

END OF STEPS

2.3 How do I examine an NE in the Troubleshooting Summary dashboard?

2.3.1 NE troubleshooting

The NE Troubleshooting Summary dashboard consists of a selection of dashlets intended to show an overall picture of a selected network element, providing the necessary information to troubleshoot it. On alarm dashlets, you can click on an alarm KPI to open the related alarms in a list view.

For information on displaying and hiding dashlets, see the *NSP User Guide*.

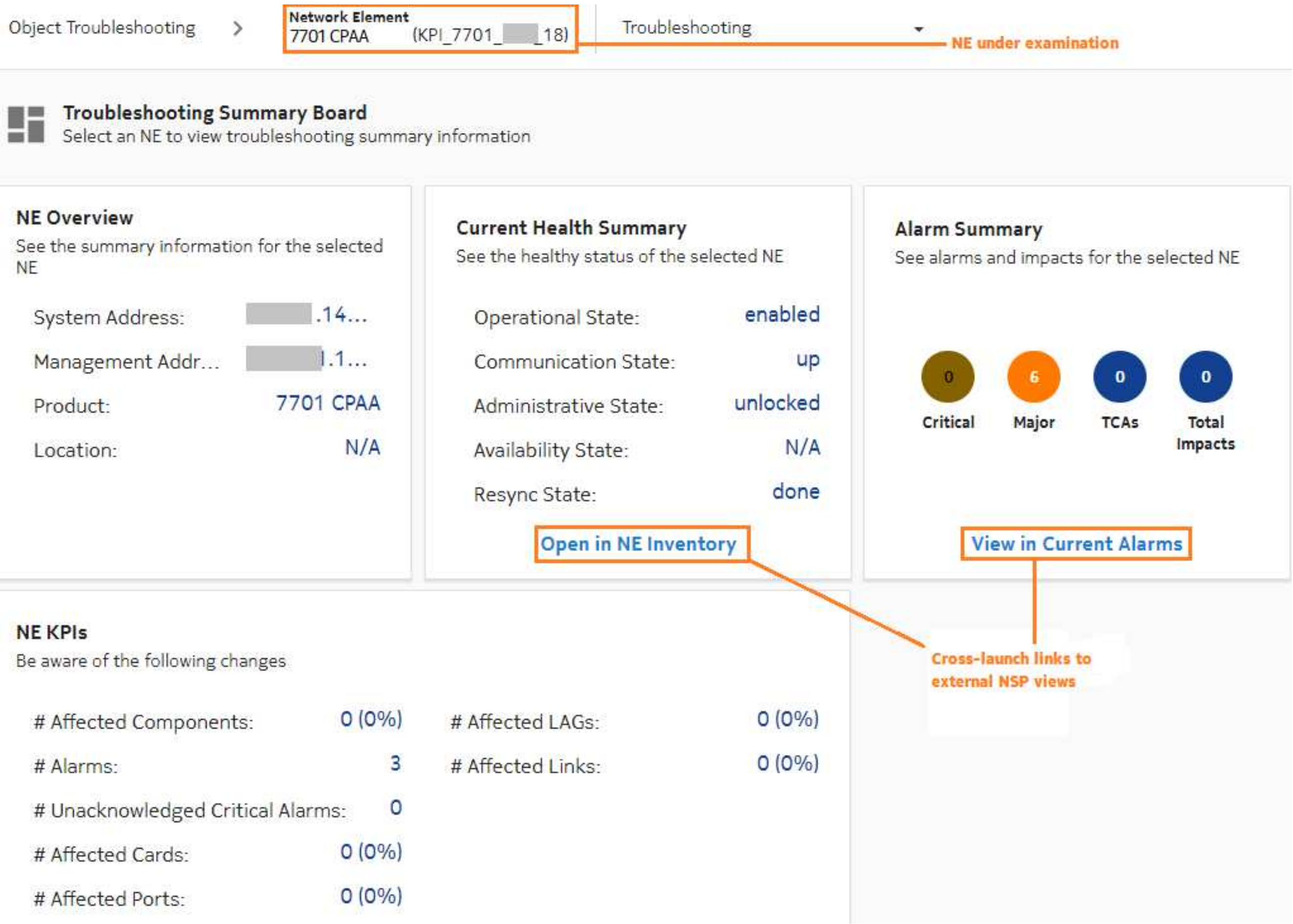
The Troubleshooting Summary dashboard provides information in a series of common dashlets that appear for all object types:

- NE Overview - IP address, model, and location information for the selected NE
- Current Health Summary - operational status of the selected NE
- Alarm Summary - alarm counts for the selected NE
  Click on an alarm KPI to view the alarms in the Current Alarms list, filtered to the KPI.
- Analytics reports - a list of Analytics reports that can be run on the selected NE
- NE KPIs - performance data for the selected NE
- Event Timeline Summary
- Troubleshooting Map

If you need to refer back to an object you had previously opened in the Object Troubleshooting dashboard, click **Target History** and select an object from the drop-down list.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Figure 2-1 Sample Troubleshooting Summary for an NE



Object Troubleshooting >

Network Element
7701 CPAA (KPI_7701_[redacted]18)

Troubleshooting

NE under examination

Troubleshooting Summary Board
Select an NE to view troubleshooting summary information

NE Overview
See the summary information for the selected NE

System Address: [redacted].14...
Management Addr... [redacted].1...
Product: 7701 CPAA
Location: N/A

Current Health Summary
See the healthy status of the selected NE

Operational State: enabled
Communication State: up
Administrative State: unlocked
Availability State: N/A
Resync State: done

Open in NE Inventory

Alarm Summary
See alarms and impacts for the selected NE

Critical	Major	TCAs	Total Impacts
0	6	0	0

View in Current Alarms

Cross-launch links to external NSP views

NE KPIs
Be aware of the following changes

Affected Components: 0 (0%)
Alarms: 3
Unacknowledged Critical Alarms: 0
Affected Cards: 0 (0%)
Affected Ports: 0 (0%)
Affected LAGs: 0 (0%)
Affected Links: 0 (0%)

2.3.2 Troubleshooting workflow

Use the following dashboard features to troubleshoot an NE:

- View all alarms for an NE KPI in the Alarms list; see 2.7 “How do I check alarms for a KPI?” (p. 46).
- View all alarms for the NE; in the Alarm Summary dashlet, click **View In Current Alarms**.
- Run Analytics reports for the NE.
- Plot statistics for the NE; see 2.18 “How do I plot performance statistics for an object?” (p. 58)
- View equipment on the NE; in the Current Health Summary dashlet, click **Open In NE Inventory** to display the NE in the NE Inventory, in the context of its related equipment (shelves, cards, ports).

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2.4 How do I examine a service in the Troubleshooting Summary dashboard?

2.4.1 Service troubleshooting

The service Troubleshooting Summary dashboard consists of a selection of dashlets intended to show an overall picture of a selected service, providing the necessary information to troubleshoot it. On alarm dashlets, you can click on an alarm KPI to open the related alarms in a list view. Cross-launch to alternate views is not possible if the related object is not part of a resource group.

The dashboard provides information in a series of dashlets:

- Service Overview - customer and service type information for the selected service
- Current Health Summary - overall operational status of the selected service
- Sites Health Summary - operational status of service sites
- Endpoints Health Summary - operational status of service tunnel endpoints
- Tunnel Bindings Health Summary - operational status of service tunnel bindings
- Alarm Summary - alarm counts for the selected service
- Event Timeline Summary
- Service Connectivity Map
- Analytics reports - a list of Analytics reports that can be run on the selected service

If you need to refer back to an object you had previously opened in the Object Troubleshooting dashboard, click **Target History** and select an object from the drop-down list.

2.4.2 Service Inventory

The Service Inventory displays operational information relating to service objects:

- Service Sites - list all sites for the selected service
- Service Endpoints - list all endpoints for the selected service
- Tunnel Bindings - list all tunnel bindings for the selected service, or for a selected site

2.4.3 Troubleshooting workflow

Use the following dashboard features to troubleshoot a service:

- View all alarms for a service KPI in the Alarms list; see 2.7 “How do I check alarms for a KPI?” (p. 46).
- View all alarms for the service; in the Alarm Summary dashlet, click **View In Current Alarms**.
- Run Analytics reports for the service
- View OAM test results for a service; see 2.17 “How do I run an OAM test from a service?” (p. 57)

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2.5 How do I examine a port in the Troubleshooting Summary dashboard?

2.5.1 Port troubleshooting

The port Troubleshooting Summary dashboard consists of a selection of dashlets intended to show an overall picture of a selected port, providing the necessary information to troubleshoot it. On alarm dashlets, you can click on an alarm KPI to open the related alarms in a list view. Cross-launch to an alternate view via links or alarm circles is not possible if the related object is not part of a resource group.

The Port Summary dashboard provides NE information in a series of dashlets:

- Port Overview - type and address information for the selected port
- Current Health Summary - overall operational status of the selected port
- Alarm Summary - alarm counts for the selected port
- Analytics reports - a list of Analytics reports that can be run on the selected port
- Equipment Overview - equipment model and version information for the selected port

If you need to refer back to an object you had previously opened in the Object Troubleshooting dashboard, click ⟲**Target History** and select an object from the drop-down list.

2.5.2 Troubleshooting workflow

Use the following dashboard features to troubleshoot a port:

- View all alarms for a port KPI in the Alarms list; see 2.7 “How do I check alarms for a KPI?” (p. 46).
- View all alarms for the port; in the Alarm Summary dashlet, click **View In Current Alarms**.
- Run Analytics reports for the port
- Plot utilization or error statistics for the port; see 2.18 “How do I plot performance statistics for an object?” (p. 58)
- In the Current Health Summary dashlet, click **Open In NE Inventory** to display the port in the NE Inventory on a separate browser tab, in the context of its related equipment (card, shelf, NE).

2.6 How do I examine a link in the Troubleshooting Summary dashboard?

2.6.1 Link troubleshooting

The link Troubleshooting Summary dashboard consists of a selection of dashlets intended to show an overall picture of a link, providing the necessary information to troubleshoot it. On alarm dashlets, you can click on an alarm KPI to open the related alarms in a list view. Cross-launch to an alternate view via links or alarm circles is not possible if the related object is not part of a resource group.

The Link Summary dashboard provides information in a series of dashlets:

- Link Endpoints Overview - port and address information for the selected link
- Current Health Summary - overall operational status of the selected link
- Alarm Summary - Link - alarm counts for the selected link
- Alarm Summary - Endpoints - alarm counts for the selected link endpoints

If you need to refer back to an object you had previously opened in the Object Troubleshooting dashboard, click **Target History** and select an object from the drop-down list.

2.6.2 Troubleshooting workflow

Use the following dashboard features to troubleshoot a link:

- View all alarms for a link KPI in the Alarms list; see 2.7 “How do I check alarms for a KPI?” (p. 45).
- View all alarms for the link; in the Alarm Summary dashlet, click **View In Current Alarms**.
- Open the link in IP Optical Coordination; see 2.8 “How do I open a link in IP Optical Coordination?” (p. 47)
- Plot utilization or error statistics for the link; see 2.18 “How do I plot performance statistics for an object?” (p. 58)

2.7 How do I check alarms for a KPI?

2.7.1 Purpose

You can cross-launch from a KPI in an Alarm Summary dashlet to the Current Alarms list. The alarm list is filtered to display only alarms related to the KPI you clicked.

2.7.2 Steps

You can list network root cause alarms, filtered by severity.

1

Open Object Troubleshooting.

2

select an object to troubleshoot as described in 2.2 “How do I troubleshoot a network object?” (p. 41)

3

In the Alarm Summary dashlet, click an alarm KPI icon.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Current Alarms opens with the list filtered by the KPI you clicked.

END OF STEPS

2.8 How do I open a link in IP Optical Coordination?

2.8.1 Steps

1

Open Object Troubleshooting.

2

select a link as described in 2.2 “How do I troubleshoot a network object?” (p. 41)

Scroll down to the map view.

3

Click **More** ⋮ , **Open in IP Optical Coordination**.

END OF STEPS

2.9 How do I examine a radio plane in the Troubleshooting Summary view?

2.9.1 Radio plane troubleshooting

The Radio Plane Troubleshooting view is component of the NE Troubleshooting Summary dashboard. It provides information for T-BTS radio planes. The view is disabled by default. You must edit the NE Troubleshooting Summary dashboard to display the following dashlets:

- Radio Plane Bindings Summary - radio plane bindings performance KPIs
- Radio Plane Bindings - list of radio plane bindings relating to a KPI in the Radio Plane Bindings Summary

If you need to refer back to an object you had previously opened in the Object Troubleshooting dashboard, click ↺**Target History** and select an object from the drop-down list.

2.10 What is the Troubleshooting map?

2.10.1 View object information

The Troubleshooting map displays an NE or link in a graphical context, in relation to associated objects. You can view information about NEs and links, either in short-form in a pop-up window, or in detail in separate NSP GUI.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

> **Note:** The Troubleshooting Map does not support LAG link members, LLDP links with endpoints with the destination MAC address set to Nearest Customer, or links to unmanaged endpoints.

2.10.2 Troubleshooting workflow

1

Open Object Troubleshooting.

2

select an NE as described in 2.2 “How do I troubleshoot a network object?” (p. 41).

Scroll down to the map view.

3

To display basic identification and status information for an NE, hover over the object.

The information appears in a pop-up window.

4

To display further details, click on the object and click ⓘ**Details**.

The Information panel opens, with expanded object information.

5

To view further information about an object, right-click on the object and select one of the following options (options vary, according to object type):

Troubleshooting options for NEs

- **Explore** displays all links terminating at the NE
- **View In Current Alarms** opens the Current Alarms list for the NE.
- **Open In NE Inventory** displays an NE in the Device Management, NE Inventory on a separate browser tab, along with all configured objects.
- **View in Object Troubleshooting** for a map object that is not currently displayed in the Object Troubleshooting dashboard, this option opens the object for troubleshooting.
- **Open in NE Session** opens a Telnet session with the NE.
- **Add to Watchlist** adds the NE to the Watchlist view for monitoring.

Cross-launch options for links

- **View In Current Alarms** opens the Current Alarms list for the link.
- **View in Object Troubleshooting** for a link object that is not currently displayed in the Object Troubleshooting dashboard, this option opens the link for troubleshooting.

End of steps

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2.11 What is the Service Troubleshooting map?

2.11.1 Service troubleshooting

The Service Troubleshooting map displays a service object in a graphical context, in relation to associated objects. The map can be useful in identifying a service segment that is experiencing problems. The map lets you trace services in the network through various layers, such as service tunnels, MPLS, and IGP.

2.11.2 Troubleshooting workflow

Use the following Service Troubleshooting Map features to troubleshoot service objects:

- View map object details; see 2.13 “How do I view information about an object in the Service Troubleshooting map?” (p. 51).
- View the map in separate network layers; see 2.12 “What is the multi-layer map?” (p. 48)

2.12 What is the multi-layer map?

2.12.1 Multi-layer map

The multi-layer map is a display option on the Service Troubleshooting map. It allows you to view services through a series of separate network layers.

Note: The MPLS, IGP, and Physical layers are sourced through either CPAM/CPAA or VSR/NRC (NRC-P), which must be configured in NSP in order for the map to display services on managed NEs.

2.12.2 Troubleshooting workflow

Use the following Multi-layer Map features to troubleshoot map objects:

- View map object details; see 2.13 “How do I view information about an object in the Service Troubleshooting map?” (p. 51).

2.12.3 Tunnel support

The table below lists the different supported tunnel types in which an LSP path can be determined based on the IGP topology source (CPAM or VSR-NRC) to populate the IGP layer in the multi-layer map.

Table 2-1 Multi-layer map tunnel support

SDP or auto-bind	Tunnel type	Support notes

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table 2-1 Multi-layer map tunnel support (continued)

SDP	GRE	CPAM/CPAA runs SPF protocol to get actual path of LSP recorded in NFM-P. Both endpoints need to be in the same admin domain. VSR-NRC runs NRC-P path calculation. Endpoints do not need to be in the same admin domain.
	MPLS – LDP	CPAM/CPAA runs SPF protocol to get actual path of LSP recorded in NFM-P. Both endpoints need to be in the same admin domain. VSR-NRC runs NRC-P path calculation. Endpoints do not need to be in the same admin domain.
	MPLS – LSP	CPAM/CPAA runs SPF protocol to get actual path of LSP recorded in NFM-P. Both endpoints need to be in the same admin domain. VSR-NRC returns PCEP related path discovered by NRC-P. If no PCEP related path is available, NRC-P runs path calculation to determine path. Endpoints do not need to be in the same admin domain.
	MPLS – SR-TE-LSP	VSR-NRC returns PCEP related path discovered by NRC-P. If no PCEP related path is available, NRC-P runs path calculation to determine path. Endpoints do not need to be in the same admin domain.
	MPLS – SR-ISIS	VSR-NRC runs NRC-P path calculation. Endpoints do not need to be in the same admin domain.
	MPLS – SR-OSPF	VSR-NRC runs NRC-P path calculation. Endpoints do not need to be in the same admin domain.
	RSVP/TE (PCE)	CPAM/CPAA runs SPF protocol to get actual path of LSP recorded in NFM-P. Both endpoints need to be in the same admin domain. VSR-NRC returns PCEP related path discovered by NRC-P. If no PCEP related path is available, NRC-P runs path calculation to determine path. Endpoints do not need to be in the same admin domain.
	L2TPv3 MPLS – BGP Tunnel MPLS – Class forwarding MPLS – Mixed LSP Mode Eth-GRE-Bridged Static	Not supported.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table 2-1 Multi-layer map tunnel support (continued)

Auto-bind	LDP	CPAM/CPAA runs SPF protocol to get actual path of LSP recorded in NFM-P. Both endpoints need to be in the same admin domain. VSR-NRC runs NRC-P path calculation. Endpoints do not need to be in the same admin domain.
	SR – ISIS SR – OSPF UDP BGP RIB – API RSVP SR – Policy SR – TE MPLS Forwarding Policy	Not supported.

2.13 How do I view information about an object in the Service Troubleshooting map?

2.13.1 Purpose

You can view information about objects in the Service Troubleshooting map, either in short-form in a pop-up window, or in detail in separate NSP GUI.

2.13.2 Steps

1

Open Object Troubleshooting.

2

select a service as described in 2.2 “How do I troubleshoot a network object?” (p. 41).

Scroll down to the map view.

3

To display basic identification and status information for a service, hover over the object.

The information appears in a pop-up window.

4

To display further details, click on the object and click ⓘ**Details**.

The Information panel opens, with expanded object information.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

5

To display an object in the Multi-layer Map, right-click on the object and select **Show in Multi-layer Map**.

END OF STEPS

2.14 How do I view past events on an object?

2.14.1 Event Timeline

The Event Timeline displays events related to alarms, configuration, OAM test failures and state change notifications, to help determine the root cause of a problem with an NE or service. The Event Timeline is displayed as a summary in the Troubleshooting dashboard. The timeline is displayed as a plot along the bottom of the view, and event categories, such as alarms or updates, are listed with total event counts.

When you are troubleshooting an NE, the timeline shows events on equipment, physical links originating or terminating on the NE, service site, service endpoint, tunnel bindings, tunnels, and LSPs originating on the NE.

When you are troubleshooting a service, the timeline shows events on services sites, endpoints, tunnel bindings, supporting LSPs, physical links, LAGs and supporting ports (for endpoints).

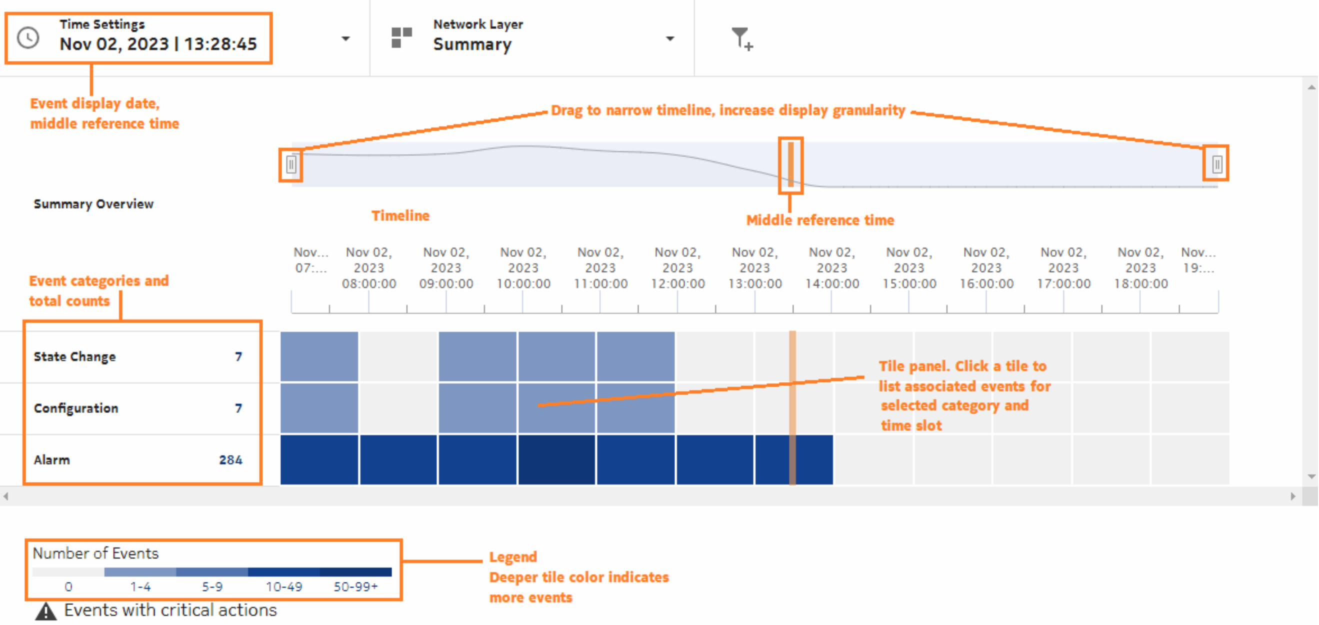
View events that occurred prior to a hardware problem or an alarm being raised to determine a possible cause (for example, an object configuration change).

To open a more detailed view, click **View in Expanded Event Timeline** for event details by category in shorter time frames, with associated events listed.

2.14.2 Expanded view

The timeline is displayed across the top of the view, and event categories, such as alarms or updates, are listed on the left. Event counts are displayed as colored tiles. A deeper color indicates a high number of events, or critical events such as OAM test failures, alarm threshold crossings, and critical alarms.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms



2.14.3 Troubleshooting workflow

- **Show event details:** click on a tile in the tile panel to list events for the selected time slot and category.

2.15 How do I set the event time frame?

2.15.1 Purpose

You can specify the date for which the Event Timeline displays events, and set the mid-point time of the displayed time frame. By default, the Event Timeline displays event for 12 hours before and 12 hours after the specified date and time. This time frame can be narrowed to view the tile panel in greater detail.

2.15.2 Steps

1

Open an object in the Object Troubleshooting dashboard as described in 2.2 “How do I troubleshoot a network object?” (p. 41)

.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2

In the Event Timeline, click 📅**Time Settings** and choose and option **Select Date**.

- Choose **Today** to set the timeline to display the current day, with the current time as the mid-point of the collection time frame.
- Choose **Select Date** to set the timeline to display a specific date and mid-point time. You can set the mid-point time by hour, minute, and second.

3

Click **Save**.

END OF STEPS

2.16 How are NSP assurance events retrieved and recorded?

2.16.1 Assurance events

Assurance events are used as a troubleshooting tool to give the user insight into the events that led to a certain state. For example, an operator could examine events that occurred on an NE or service prior to a critical alarm and see if there was a configuration change that resulted in an alarm.

Assurance events are sequential historical events recorded on NE or service objects and their hierarchical sub-components. The type of events that can generate an assurance event are:

- object creation, including alarm creation (AlarmRaised)
- attribute change, which can include configuration change (ConfigurationChange) and state change (StateChange), depending on which attributes have changed
- object deletion, including alarm deletion (AlarmCleared)
- alarm update

2.16.2 Assurance event recording in NSPOS

For objects managed by MDM or WS-NOC, event logging is implemented using time series model recording.

You enable event logging globally for NSP from the NSP settings page. Click **User**, **NSP Settings**, **Event Logging Policy**. This setting is for NSP event logging only. It applies to non-NFM-P-managed objects.

The assurance event framework detects changes on common model objects by listening to corresponding **`nsp-db-<model>`** topics (e.g., **`nsp-db-equipment`**, **`nsp-db-service`**, **`nsp-db-alarm`**) which report any change committed to the common model database. If the change is detected on any one of the pre-configured objects, an assurance event is created and published it to a Kafka topic. The nspos-ts-data-manager-app listens for assurance events and adds them to the ts.AssuranceEvent table.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2.16.3 Assurance event format

Each NFM-P or NSPOS event contains the following information:

Table 2-2 Assurance event information components

Event component	Description
managedObjecFdn	Derived FDN of the ancestor MO to the MO that generated the event (e.g., Service FDN).
eventFdn	FDN of the MO that generated the event (e.g., Site FDN).
creationTime	Event creation time.
eventType	Can be any of: AlarmRaisedEvent, AlarmUpdateEvent, AlarmClearedEvent, CreationEvent, ConfigurationEvent, StateChangeEvent, DeletionEvent, TestFailureEvent, AnomalyEvent, ThresholdCrossedEvent, ScaleOutEvent, ScaleInEvent, HealingEvent, CustomEvent, UpgradeEvent, CustomOperationEvent, InstantiateEvent
eventRecord	json-encoded event data.

2.16.4 Assurance event recording in NFM-P

Assurance events for NFM-P-managed objects are recorded using NFM-P event generation (JMS). The assurance event recorder subscribes to the JMS events. If an event is on an object of interest, it is translated into an assurance event record and logged using the event logging framework.

By default, assurance events are recorded in an Oracle database, but if the customer has configured an auxiliary database, the recording is automatically routed to the auxiliary database.

An NFM-P Event policy allows you to enable/disable event recording (Admin State Up/Down) and the log retention time. To configure an Event policy, open NFM-P, click **Tools** menu, **Events**, **Event Policies**. The framework also provides tools to purge events.

Event log retention time defaults and minimum/maximum values depend on the type of database you are using.

Table 2-3 Event log retention time defaults and minimum/maximum values

Database type	**Default retention time**	**Minimum retention time**	**Maximum retention time**
Oracle	168 hours (one week)	One hour	720 hours (1one month)
Auxiliary	720 hours (one month)	One day	8760 hours (one year)

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

In addition to NFM-P Event Policy configuration, you must enable event recording in the Timeline Settings form. Click ⋮ **More**, **Timeline Settings**. You can enable event recording for specific objects:

Table 2-4 Objects with event recording

Object type	NFM-P class
Network Element	netw.NetworkElement
Link	netw.AbstractPhysicalLink
Card	equipment.Card
Port	equipment.Port
Site	rtr.ProtocolSite
Network Interface	rtr.NetworkInterface
LAG Interface	lag.Interface
Site Sync	sonet.SiteSync
MPLS	rsvp.Interface
IGP	isis.Interface
IGP	ospf.Interface
VNF Instance	nfv.VNFInstance
VNF Component	nfv.VNFComponent

2.16.5 Assurance events retrieval

NSP retrieves events from the appropriate database (NFM-P or NSPOS), based on the original source of the object.

Assurance events are retrieved using API commands from the web component library (assurance-share-md), which provides web components to display events on a timeline. Assurance events are recorded and stored on a server that is accessible from NSP using the web component library.

The web component library provides:

- Retrieve events from the NFM-P or NSPOS database, based on the source of the referenced object.
- Display events in a timeline view. Events are grouped into categories in the display, and multiple categories are presented on the same event timeline.
- Ability to filter assurance events based on the source object type or category.
- Ability to select individual events and examine event details.
- Ability to select a set of events to form a pattern, and then searching the Event Timeline for a similar pattern of events.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

The Event Timeline will display events for multiple objects at the same time if all of the selected objects are part of the same object hierarchy, and all of the objects are at the same level in the hierarchy (for example, multiple service sites for the same service).

2.17 How do I run an OAM test from a service?

2.17.1 Purpose

Use this procedure to run an OAM test on a service. 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.

For information about OAM tests, see the *NSP Data Collection and Analysis Guide*.

2.17.2 Steps

1

Open Object Troubleshooting and select a service to test, as described in 2.2 “How do I troubleshoot a network object?” (p. 41).

2

Click ⋮ **More**, **View OAM Test Results**.

The service is opened in Data Collection and Analysis Management.

3

Select a test in the list and click ⋮ **Table Row Actions**, **Execute** on the selected item.

4

In the Run OAM Test form, configure the available OAM test options.

5

Enable the check box for each object in the list that you want to test.

6

Click **Execute**.

7

The test results are displayed in Data Collection and Analysis.

End of steps

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2.18 How do I plot performance statistics for an object?

2.18.1 Purpose

Use this procedure to test an object in the Object Troubleshooting dashboard for errors or performance. For information about OAM tests, see the *NSP Data Collection and Analysis Guide*.

2.18.2 Steps

1

Open Object Troubleshooting and select an object to test, as described in 2.2 “How do I troubleshoot a network object?” (p. 41).

2

Click ⋮ **More**, **Plot Statistics**.

The component is opened as a statistics plot in Data Collection and Analysis Visualizations.

END OF STEPS

2.19 How do I configure an OAM test suite for a service?

2.19.1 Purpose

Use this procedure to configure an OAM test suite for a service. For information about OAM test suites, see the *NSP Data Collection and Analysis Guide*.

2.19.2 Steps

1

Open Object Troubleshooting and select a service to test, as described in 2.2 “How do I troubleshoot a network object?” (p. 41).

2

Click 📋 **Create OAM Test Suite**.

The Select L3 VPN Endpoints form opens.

3

Select the endpoints you want to test and click **Select**.

4

In the Generate OAM Tests form, specify a name and description for the test suite and configure parameters as required.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

5

Click **Generate and Execute**.

The test suite is generated in Data Collection and Analysis Management.

End of steps

2.20 How do I view historical OAM test results for a service?

2.20.1 Purpose

Use this procedure to examine past OAM test results for a service. This functionality applies to MDM services on MDM-managed NEs only. For information about OAM tests, see the *NSP Data Collection and Analysis Guide*.

2.20.2 Steps

1

Open Object Troubleshooting and select a service component to test, as described in 2.2 “How do I troubleshoot a network object?” (p. 41).

2

Click ⋮ **More**, **View OAM Test Results**.

A list of tests opens in Data Collection and Analysis Management.

3

Select a test item in the list and click ⋮ **Table Row Actions**, **View Results** on the selected item.

A list of test results opens.

4

Select a test result and click **Retrieve**.

End of steps

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3 Network health alarm views

3.1 How does the NSP manage alarms?

3.1.1 NSP fault management

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

The alarm lists display 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. There are three categories of alarm lists, available from the drop-down list:

- The **current alarm list** displays all active alarms in the network, or for specific NEs. The global current alarm list is kept updated in real-time. Current alarm lists accessed from the Top Unhealthy NEs or Top Problems views are updated on demand.
- The **merged alarm list** displays all active and previously-active alarms in the network (or for specific NEs) over a specified time period.
- The **historical alarm list** displays all previously-active alarms in the network (or for specific NEs) over a specified time period.

3.1.2 Alarm severity levels

The NSP supports the following alarm severity levels:

- Cleared
- Indeterminate
- Info
- Condition
- Warning
- Minor
- Major
- Critical

Alarm severity levels are color-coded. An administrator can change the colors assigned to each severity level; see the *NSP System Administrator Guide* for information about modifying alarm severity colors. You can manually change the severity of an alarm, or configure the NSP to change the severity of an alarm when it is received; see 4.18 “How do I automate alarm management using a policy?” (p. 86).

3.1.3 Role-based access control for alarms

Alarm-related navigation actions require write or execute access to the object affected by the alarm. Opening an NE Session requires execute access to the corresponding NE.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Role-based access is not supported on the historical and merged alarms lists, or on historical alarm REST and RESTCONF requests, which may show alarms outside of a user's assigned role. Role-based access for optical trail alarms is only supported in deployments that include the NRC-X.

3.1.4 Alarm reload behavior

When alarm messages from MDM and WS-NOC sources are modified or deleted in NSP, the change is recorded in the NSP database, but not at the alarm source. If alarms are bulk-reloaded from an MDM or WS-NOC source to the NSP, 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.

3.2 How do I view current alarms?

3.2.1 Current alarm lists

The **current alarm list** displays all active alarms in the network, or for specific NEs. The global current alarm list is kept updated in real-time.

3.2.2 What can I do in the alarm lists?

Perform the following operations to manage the order and content of your alarm list:

- **Filter by severity.** Click on an alarm severity level icon in the Severity filter selector to display only alarms of that particular severity level. Click on the Clear Filter button ⊗to clear filters.
- **Filter the Current Alarm List to show or exclude root cause alarms.** Click on the Filter button and select Root Causes. A chip filter appears at the top of the list. Choose an option from the drop-down list to configure the filter. Select True to show only root cause alarms, False to exclude root cause alarms, or Unknown to show alarms where the root cause status is being determined. Click on the close button ⊗to clear the Root Causes filter.
- **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 Close button ⊗to remove the filter.
- **Filter the alarm list under a specific column using a quick filter.** Click on the Filter button in a column header. Choose an operator and enter a value in the search field and press Enter, or use the date picker or drop-down list (where available) and press Enter. Click on the Filter button and click Reset to clear the filter.
- **Pause real-time updates.** Click on the Live Data toggle in the lower left of the Current Alarms view to pause the real-time updating of alarms. While updates are paused, the time elapsed since the last update is displayed in the banner next to the Pause toggle.
- **Refresh the alarm list manually.** Click the Refresh button. ↻

Selecting multiple alarms

You can select up to 100 alarms from the alarm list, from among currently displayed alarms. You can select alarms in batches, but cannot make a selection that includes alarms that have not been loaded into the NSP alarm list (for example, by starting a selection, then scrolling past the currently loaded alarms). Selecting large numbers of alarms from a long list is not recommended; see4.5 “How do I create an advanced alarms filter?” (p. 77) for information about filtering alarms.

Note: If a selected alarm is deleted during the selection process, the deleted alarm is not included in the action performed on the other selected alarms.

3.2.3 What can I do with the Watched Filters list?

The Watched Filters list is a part of Current Alarms, and shows a summary of up to ten saved filters. You can add or remove saved filters from the list, and click on a filter in the list to display that filter in the Alarm List panel. Perform the following operations to manage filters displayed in the list:

- **Display the Watched Filters list.** Click the Watched Filters button in the details panel to open the Watched Filters list.
- **Add a saved filter to the list.** Click Add and select one or more filters from the displayed list, then click Add.
- **Remove a saved filter from the list.** Hover over a filter in the list, and click on the Delete button.
- **Edit a saved filter.** Select a filter in the list, and click on the Edit button. The Advanced Filter window appears, with the selected filter displayed.
- **Move a saved filter in the list.** Click and drag a filter row, and move it to a new location in the list.
- **Apply a saved filter to the alarm list.** Click on a filter in the list. The selected filter is applied to the alarm list.
- **Stop applying a saved filter to the alarm list.** Click on the Clear Selection button. The alarm list is returned to an unfiltered state.
- **Choose which columns appear in the list.** Click More > Columns and select the columns to display in the Watched Filters list.

3.2.4 What can I do with the alarm squelch page?

The squelch settings page shows you the squelch status of all ports or NEs monitored by NSP. You can squelch an object or a to discard all new alarms on the squelched object, and service endpoints associated with a squelched port.

Alarms that are squelched in the NSP are not squelched at their originating data source (for example NFM-P or WS-NOC) and continue to appear in their respective clients. Squelched alarms are dropped when received by the NSP, and do not appear in current alarm lists or as historical events.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Note: Squelching is not supported in WS-NOC standalone deployments. Squelching resource groups is not supported in NFM-P standalone deployments. Squelched alarms received from the NFM-P are not displayed in the Current alarm list, but are displayed in the Merged and Historical alarm lists.

Note: You can individually squelch up to 1000 NEs and 1000 ports. You can use resource groups to squelch up to 250,000 objects (both ports and NEs combined).

Manage squelched objects using the following tasks:

- **View squelch status of ports.** In the **Network Map and Health, Current Alarms** view, click on the More, Settings button and select Alarm Squelch in the left panel.
- **View squelch status of NEs.** In the Alarm Squelch page, click on the NE tab.
- **View squelch status of a resource group.** In the Alarm Squelch page, click on the Resource Group tab.
- **Filter objects in the list.** Use the filters at the top of each column to filter the list of displayed objects.
- **Squelch alarms.** Select an object in the list and click on the Squelch button. To squelch multiple objects, select up to 80 objects in the list and click on Squelch Selected in the banner that appears.
- **Unsquelch alarms.** Select an entry in the list and click on the Unsquelch button. To unsquelch multiple objects, select up to 80 objects in the list and click on Unsquelch Selected in the banner that appears.

Alarm squelching behavior

NSP discards alarms on squelched objects based on the Affected Object and Site ID parameters of the alarm. Squelching an NE discards alarms with a Site ID that matches the squelched NE. Squelching a port discards alarms with an Affected Object parameter that matches the squelched port. Squelching a port also discards alarms for service endpoints associated with the port.

Resource groups

The Resource Group panel on the Alarm Squelch page displays existing network supervision, network element, and equipment resource groups. For more information about using group directories and resource groups, see the *NSP System Administrator Guide*.

3.3 How do I view current and previous alarms?

3.3.1 Merged alarm lists

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

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3.3.2 What can I do with the Merged Alarm list?

Perform the following operations to manage the order and content of your alarm list:

- **Filter the 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 using a quick filter.** Choose an operator and enter a value in the search field at the top of a column and press Enter, or use the date picker or drop-down list (where available) and press Enter.
- **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. ↻

3.4 How do I view historical alarms?

3.4.1 Historical Alarm lists

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

3.4.2 What can I do with the Historical Alarm list?

Perform the following operations to manage the order and content of your alarm list:

- **Filter the Merged Alarm List.** Click on the Filter button to configure a filter.
- **Filter the alarm list under a specific column using a quick filter.** Click on the filter button in a column header, then choose an operator and enter a value in the search field at the top of a column and press Enter, or use the date picker or drop-down list (where available) and press Enter.
- **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. ↻

3.5 How do I manage alarm messages?

3.5.1 Interacting with alarms in the alarm list

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

- **Acknowledge or unacknowledge an alarm.** Select one or more alarms, then click (Table row actions) ⋮ , Edit Alarm(s) and configure the Acknowledge parameter.

  If you select multiple NFM-P alarms, you can configure the Assigned Severity, and Acknowledgement Note. If you select multiple WS-NOC alarms, you can configure the Acknowledgement Note. If you select both NFM-P and WS-NOC alarms, you can configure the Acknowledgement Note.

- **Delete or clear an alarm.** Select one or more alarms and click (Table row actions) ⋮ , Delete Alarm(s) or Clear Alarm(s).
- **Assign alarm severity.** Select one or more alarms, then click (Table row actions) ⋮ , Edit Alarm(s) and configure the Severity parameter.
- **Assign alarm admin state.** Select one or more alarms, then click (Table row actions) ⋮ , Edit Alarm(s) and configure the Admin State parameter.
- **Edit alarm custom text.** Select one or more alarms, then click (Table row actions) ⋮ , Edit Alarm(s) and configure the Custom Text parameter.

3.6 How do I investigate an alarm?

3.6.1 Viewing further information about alarms in the alarm list

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

- **Show alarm details.** A selected alarm shows expanded information in the Details panel on the right-hand side of the GUI.
- **Show alarm impacts.** Click (Table row actions) ⋮ , View Impacts to open the Impact Diagram for the selected alarm.

  Note: This function is not available for alarm messages that are not involved in correlation.
- **Show the root cause of an alarm.** Click (Table row actions) ⋮ , View Root Cause to open the Root Cause diagram for the selected alarm.

  Note: This function is not available for alarm messages that are not involved in correlation.
- **Show the objects impacted by an alarm.** Click (Table row actions) ⋮ , View Object Impacts to view the objects that are impacted by the alarm.
- **Open an NE session with the affected NE** Click (Table row actions) ⋮ , Open in NE Session to open a session with the affected NE.

3.7 How do I view root cause distribution in the network?

3.7.1 Alarm Distribution diagram

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.

3.7.2 What can I do with the Alarm Distribution diagram?

Select Alarm Distribution from the drop-down list in the Network Map and Health dashboard. 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.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

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 it has been scaled due to high impact counts.

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, site ID, product, topology group, or saved filter). Depending on what you select, additional filters options appear.

  The filters appear as chip filters Product: 7750 SR ⊗ 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, then click Refresh to hide acknowledged alarms or maintenance (admin state) alarms.
- **Hide alarms of specific severity.** Click More ⋮ and de-select the appropriate severity options, then click Refresh.

3.8 How do I view network alarms as a chart?

3.8.1 Using the Alarm Statistics chart

The Alarm Statistics chart displays network alarm counts by alarm severity. Select Alarm Statistics from the Network Map and Health dashboard to see the chart. Click on a bar in the graph to navigate to the Current Alarms view.

3.9 How do I view which NEs have the most alarms?

3.9.1 Unhealthy NEs view

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

3.9.2 What can I do from the Top Unhealthy NEs view?

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 the options to filter the matrix.

  The filters appear as chip filters Product: 7750 SR ⊗ 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:
  - # of Alarms - NE tiles are sorted by the number of alarms against them.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

  - # of Unacknowledged Alarms - NE tiles are sorted by the number of unacknowledged alarms against them.
  - # of Impacts - 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 NE tile and click on the More button then select View in Current Alarms.
- **View current and historical alarms on an NE.** Hover over the NE tile and click on the More button then select View in Merged Alarms.
- **View historical alarms on an NE.** Hover over the NE tile and click on the More button then select View in Historical Alarms.
- **View additional details and KPIs.** Hover over the NE tile and click on the More button then select View Details
- **Open an NE session.** Hover over the NE tile and click on the More button then select Open in NE Session.

3.10 How do I view which alarms are occurring the most?

3.10.1 Top Problems view

The Top Problems view helps identify the largest problems in your network by displaying issues in the form of a bar chart. By default, the view displays the alarm types with the most occurrences in the network. Each bar represents a specific alarm type, and its size represents the 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 settings page.

You can configure the graph to instead display alarms grouped by probable cause or specific cause, and count by total number of alarms, total alarm occurrences, or total NEs affected.

3.10.2 What can I do with the Top Problems view?

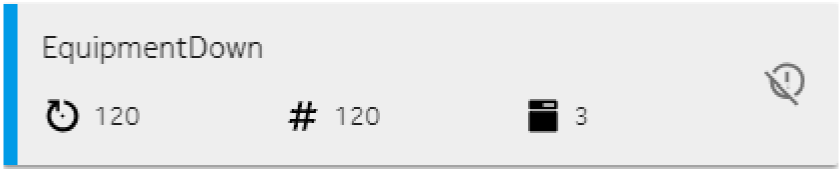
When you hover over a bar in the chart, the corresponding alarm type in the list is highlighted.

- **Configure the graph.** Use the drop-down menus at the top of the graph to configure what bars are displayed, and what criteria are counted for the bars
- **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 list. 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.

3.10.3 What can I do with the Alarm 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.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms


EquipmentDown

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).

3.11 How do I change alarm view settings?

3.11.1 Alarm settings

This section describes configuration options for alarm appearance and behavior. To access the settings page, click on the More button in any alarm list and choose Settings.

Note: Alarm settings can only be configured by an administrator.

3.11.2 What can I configure on the Current Alarms settings panel?

The Current Alarms settings panel manages settings related to the alarm database and alarms in the alarm list. These settings apply to NSP, WS-NOC, and MDM alarms. NFM-P alarm settings are configured in NFM-P; see the *NFM-P Administrator Guide*. Using this panel, you can:

- **Enable alarm aging** Enable the Aging Settings option and configure the number of days after which an alarm is deleted in the Delete After (days) parameter. You can also configure aging for a specific alarm using an alarm policy.
- **Configure when an overflow warning is triggered** Configure the Warning Threshold (%) parameter
- **Purge alarms in the event of an overflow** Select Wrap from the Overflow Action drop-down list, then configure the percentage of the database to purge in the Purge Amount parameter, and which alarms to purge first in the Purge Policy parameter.
- **Halt alarm collection in the event of an overflow** Select Halt from the Overflow Action drop-down list.

3.11.3 What can I configure on the Historical alarms settings panel?

The Historical Alarms settings page manages settings related to the historical alarm database. These settings apply to NSP, WS-NOC, and MDM alarms. NFM-P alarm settings are configured in NFM-P; see the *NFM-P Administrator Guide*. Using this page, you can:

- **Configure archive settings** Enable the Archive Settings pattern and select either the Log on Change or Log on Deletion options.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- **Specify overflow actions** Specify the maximum alarm count, then specify warning and critical thresholds as a percentage of the maximum, and the number of alarms to purge when each threshold is reached.

3.11.4 What can I configure on the Global Alarm Policies page?

The System settings page manages settings related to NSP, WS-NOC, and MDM alarms. Using this page, you can:

- **Enable manual changes to alarms** Enable the Manual Settings parameter, then enable options to allow users to promote, demote, or clear alarms.
- **Configure when users can delete alarms** Enable the Alarm Deletion Settings and Manual Alarm Deletion Settings parameters, then choose an option that specifies when a user can delete a system alarm (for example, only after it has been acknowledged, or anytime without restriction).
- **Enable notifications for deleting correlated alarms** Enable the Alarm Deletion Settings and Correlated Alarm Settings for Manually Deleted Alarms parameters, then choose an option that specifies whether an alert is displayed when correlated alarms would be deleted by manually deleting a system alarm.
- **Configure automatic deletion of alarms** Enable the Alarm Deletion Settings and Automatic Alarm Deletion Settings parameters, then choose an option that specifies when to automatically delete alarms.
- **Configure automatic acknowledgement of correlated alarms.** Enable the Alarm Acknowledgement Policy and Correlated Alarm Settings for Manually Acknowledged Alarms parameters to automatically acknowledge any correlated alarms when a system alarm is manually acknowledged, and specify whether a GUI notification occurs when the correlated alarms are acknowledged.
- **Configure automatic acknowledgement of cleared alarms.** Enable the Alarm Acknowledgement Policy and Acknowledge alarms when cleared parameters to automatically acknowledge any alarms when they are cleared.

3.11.5 What can I configure on the Individual Alarm Policies page?

The Alarm Policies page manages policies related to NSP, WS-NOC, and MDM alarms. When the NSP receives an alarm for the first time, an alarm policy is created for the received alarm. You can use an alarm policy to perform automatic operations on an alarm when it is received. Changes to alarm policies are not retroactive, and only apply to alarms received in the future; to modify existing alarms, use the Alarm List view.

You can filter and sort the list using the columns, and select multiple policies at a time to perform mass configurations. Select one or more alarm policies, click on the More ••• button, select Edit, and configure the parameters as required. Alarm properties you can configure using an alarm policy are:

- **Squelch alarms**. Enable the Squelch parameter to squelch all alarms of this type.
- **Assign severity**. Select a severity in Initial Assignment Severity to change the alarm’s type when it is raised.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- **Acknowledge alarms**. Enable the Auto Acknowledge parameter to acknowledge the alarm when it is raised.
- **Disable historical alarm archiving.** Disable the History parameter to disable archiving of the alarm.
- **Apply custom text.** Configure the Custom Text parameter to set the custom text of the alarm when it is raised. This will overwrite any other custom text on the alarm.
- **Restore default values.** Click Restore to Default to return all parameters to their default values.
- **Enable alarm debouncing.** Enable the Alarm Debouncing parameter. Alarm debouncing is only available for implicitly cleared alarms.
- **Configure automatic escalation and de-escalation.** Configure the Escalation Policies parameters to enable alarm escalation.

You can delete an alarm policy by clicking on the More ••• button, and selecting Delete. Stale alarm policy entries may occur due to drift in alarm dictionary keys; it is safe to delete these stale policies.

3.11.6 What can I configure on the E-mail Policies page?

The e-mail policy feature allows administrative users to configure e-mail notification policies for specific alarm messages in NFM-P, WS-NOC, 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 alarms, 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 10) that can be sent over a one-hour period. The recipients are notified when the maximum has been reached.

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

E-mails are not sent for alarm attribute change events, only for alarm creation. For example, if an alarm is created with a severity of major, and the severity is subsequently changed to critical, alarm e-mail policy filters for critical alarms will not include this alarm.

In order for NSP to send e-mail notifications, you must configure connection information for an e-mail server through the NSP settings page.

Using the E-Mail Policies settings page, you can:

- **Create an e-mail policy** Click on the + Email Policy button and configure the parameters. See 4.13 "How do I configure an e-mail policy?" (p. 82).
- **Configure an e-mail policy** Select an e-mail policy and configure the parameters in the details panel.
- **Disable an e-mail policy** Select an e-mail policy and disable the Enable parameter in the details panel.
- **Delete an e-mail policy** Select an e-mail policy and click the Delete button at the end of the row.

Example e-mail notification

The e-mail sent by the NSP consists of a link to the affected alarm, and a set of information about the alarm. The following is an example e-mail sent for a single NSP system alarm:

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

> Subject: NSP Notification - New NSP Health-Alarm Received
>
> Select the link(s) below to launch the filtered alarm list for each alarm. To view the alarm you will be required to have access to an NSP system and to use your existing credentials for log in.
>
> https://233.252.0.0:443/FaultManagement/?view=alarmListImpacts & alarmId;= fdn%3Amodel%3Afm%3AAlarm%3A213673
>
> Severity: major
>
> Alarm Name: NspApplicationPodDown
>
> Alarm Type: communicationsAlarm
>
> Alarm ID: fdn:model:fm:Alarm:213673
>
> Probable Cause: systemFailed
>
> Alarmed Object ID: fdn:app:server:cam-im-deployer-app-1676634176763-job-rr2sr:233.252.0.0
>
> Alarmed Object Type: NmsSystem
>
> Alarmed Object Name: cam-im-deployer-app-1676634176763-job-rr2sr:233.252.0.0
>
> Last Time Detected: 2023/02/17 11:46:04 159 UTC
>
> Is Service Affecting: false
>
> Site ID: cam-im-deployer-app-1676634176763-job-rr2sr:233.252.0.0
>
> Site Name: cam-im-deployer-app-1676634176763-job-rr2sr:233.252.0.0
>
> Implicitly Cleared: false
>
> Administrative State: unknown
>
> Source Type: nsp
>
> Source System: fdn:app:server
>
> Additional Text: null
>
> Custom Text: N/A

When the NSP has reached the configured maximum number of e-mails permitted in one hour, the following statement is added:

> The configured maximum number of e-mail notifications has been reached for this e-mail notification filter. NSP will not send further notifications for up to one hour. Open the FM App to verify current alarm information.

When there are more than 10 new alarms to be included in the e-mail, the following statement is added:

> A set of 10 or more alarms exist for this e-mail notification policy. This e-mail notification only displays 10 of the reported set. Open the FM App to verify all the current alarm information.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3.12 How do I configure current alarm list settings?

3.12.1 Purpose

Configure aging and overflow settings for the current alarm list. These settings apply to WS-NOC, NSP, and MDM alarms. NFM-P alarm settings are configured in NFM-P; see the *NFM-P Administrator Guide*.

You must have administrator privileges to configure alarm settings.

3.12.2 Steps

1

In the **Network Map and Health, Current Alarms** view, click the More button ⋮ and select 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 for alarms from sources other than the NFM-P is 250000 alarms if WS-NOC and NFM-P are deployed in shared mode, or 300000 alarms if WS-NOC 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

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3.13 Fault management API and tools support

3.13.1 Fault management API developer portal documentation

NSP fault management functions are available for OSS using programmable APIs. For general information about developer support, visit the Network Developer Portal (https://network.developer.nokia.com/). For API documentation, see the NSP API documentation portal (https://network.developer.nokia.com/api-documentation/).

For specific documentation about REST APIs for fault management, see:

https://*nsp-server-ip*/FaultManagement/**api-docs**.

3.13.2 Alarm correlation rules

To see the available correlation rules or rules that have been evicted for NSP, navigate to:

https://*nsp-server-ip*/FaultManagement/api-docs/rules.html

Speak with your Nokia customer relations representative for information about creating and applying custom correlation rules, or enabling and disabling existing rules.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4 Managing network alarms

Displaying alarms

4.1 How do I configure historical alarm list settings?

4.1.1 Purpose

Configure logging and overflow settings for the historical alarm list. These settings apply to NSP, WS-NOC and MDM alarms. NFM-P alarm settings are configured in NFM-P; see the *NFM-P Administrator Guide*.

You must have administrator privileges to configure alarm settings.

4.1.2 Steps

1

In the **Network Map And Health**, **Historical Alarms** view, click the More button ⋮ and select Settings. The Alarm Settings form opens, with the Historical Alarms panel displayed.

2

Enable the Archive Settings option and enable either or both of the Log on Change and Log on Deletion options.

3

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

4

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.

5

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.

6

Save your changes.

END OF STEPS

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4.2 How do I configure which columns are displayed in an alarm list?

4.2.1 Steps

1

In any alarm list, click on the More ⋮ button at the end of the column headers and select Manage columns.

2

Click on the names of the columns that you want to display.

3

Click Apply to save your changes and close the form.

END OF STEPS

4.3 How do I pause the current alarm list?

4.3.1 Purpose

The current alarm list is updated in real-time. You can pause the updates using the pause toggle. While updates are paused, the time elapsed since the last update is displayed next to the toggle.

ℹ **Note:** When you scroll down the current alarm list far enough to load alarms that have not yet been displayed, information about those alarms is loaded from the NSP alarm database. The information is current to the time it was loaded, and not to the time when alarm updating was paused. The last refresh time is updated when this occurs.

4.3.2 Steps

1

In the **Network Map And Health, Current Alarms** view click on the Pause toggle in the lower left. The indicator changes from “Live data” to “Last refresh” and a count of the time elapsed since updates were paused.

2

To resume alarm updates, click on the toggle again.

END OF STEPS

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4.4 How do I apply a quick alarms filter?

4.4.1 Purpose

You can use the search fields in a column header to filter the current alarms list. If you have an advanced filter applied, you can combine the quick filter and the advanced filter to create a new advanced filter.

4.4.2 Steps

1

In the **Network Map And Health, Current Alarms** view click on the filter symbol in the header and select an operator. The available filters vary by column.

2

In the search field in the column header, enter a value or choose one from the drop-down list, and press Enter.

3

To save the quick filter as an advanced filter, click on the Filter button and select Advanced Filter. Enter a name for the filter and click Save Filter.

END OF STEPS

4.5 How do I create an advanced alarms filter?

4.5.1 Purpose

You can create and save an advanced search filter. Advanced search filters are more detailed than simple search filters. After applying an advanced filter, you can further refine the results using quick filters and save the refinements to a new filter.

4.5.2 Steps

1

In the **Network Map And Health, Current Alarms** view click on the Filter button to open the advanced filter configuration form.

2

Enter a filter name and description, and specify whether you want the filter to be public or private. Multiple filter properties in an advanced search filter are combined using Boolean operators.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3

Choose a Boolean operation from the drop-down list:

- AND - When you combine properties using the AND operator, the search returns objects that meet both or all of the specified criteria
- OR - When you combine properties using the OR operator, the search returns objects that meet at least one of the specified criteria
- NOT - When a filter property is preceded by the NOT operator, items that meet the criteria in that filter property are excluded from the results

4

Choose an alarm attribute from the drop-down list, choose a search function, such as equals, between, or is not null, for example, and then choose or enter a value. You can click on the + or - button to add or remove clauses. Click on the +{} button to add sub-clauses.

5

To share the filter with other users, enable the Public option.

6

Click Apply or Save Filter. Advanced search filters that you save appear in the Saved Filters list.

End of steps

4.6 How do I delete a saved alarms filter?

4.6.1 Purpose

You can delete a saved filter you have created, including public filters. An administrator can delete public filters created by other users.

4.6.2 Steps

1

In the **Network Map And Health, Current Alarms** view click on the Filter button and click Saved Filter.

2

Select the filter you need to delete from the drop-down list and click on the Delete button. A confirmation dialog appears listing any users or objects affected by deleting the filter.

Note: Deleting a public filter that is currently in use by a watched filters list or an e-mail policy disables them when the filter is deleted. You must have permission to edit e-mail policies to delete a filter being used by an e-mail policy.

End of steps

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4.7 How do I combine an advanced filter and a quick filter?

4.7.1 Purpose

You can apply a quick filter to an advanced filter to create a new filter.

4.7.2 Steps

1

In the **Network Map And Health, Current Alarms** view click on the Filter button and click Saved Filter to load an existing filter, or Advanced Filter to create a new filter. See 4.5 “How do I create an advanced alarms filter?” (p. 77) for more information about using advanced filters.

2

Apply a quick filter to the results of the advanced filter. See 4.4 “How do I apply a quick alarms filter?” (p. 77) for more information about using quick filters.

3

Click on the advanced filter chip filter. The Advanced Filter form opens with the quick filters you applied included in the filter expression.

4

Enter a new name for the filter.

5

Click Save Filter to save the new filter, then click on Apply to return to the alarm list.

END OF STEPS

4.8 How do I create a watched filters list or alarm sublist?

4.8.1 Purpose

You can use the Watched Filters list to display a summary of up to ten saved filters and apply those filters to the Alarm List with a click. Perform the following to add saved filters to the Watched Filters list.

4.8.2 Steps

1

In the **Network Map And Health, Current Alarms** view click the Watched Filters button in the details panel to open the Watched Filters list.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2

Click Add in the Watched Filters panel and select one or more saved filters from the displayed list.

3

Click Add in the list of filters to add the selected filters to the Watched Filters list.

4

Click on a filter in the Watched Filters list to apply the selected filter to the Alarm List.

5

Click and drag a filter row in the Watched Filters list to move the filter in the list.

End of steps

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Investigating alarms

4.9 How do I find the object affected by an alarm?

4.9.1 Steps

1

Click More ⋮ on the right side of a row and choose Open Affected Object to open the affected object of the alarm for configuration in a separate GUI.

> **Note:** When you choose View Affected Object for an optical alarm on a WS-NOC-managed NE, the WS-NOC web client opens.

End of steps

4.10 How do I list other objects impacted by an alarm?

4.10.1 Steps

1

In any **Network Map and Health** alarm view, click on the More button and select View Object Impacts on the right side of a row to open the Object Impacts list for the selected alarm.

> **Note:** This function is not available for alarm messages that are not involved in correlation.

End of steps

4.11 How do I display the root cause of an alarm?

4.11.1 Steps

1

In the **Network Map And Health, Current Alarms** view click on the More button and select View Root Causes on to open the Root Causes diagram for the selected alarm.

> **Note:** This function is not available for alarm messages that are not involved in correlation.

End of steps

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4.12 How do I export high-severity alarms to a file?

4.12.1 Steps

1

In any **Network Map and Health** alarm view click on an alarm severity level icon in the Severity filter selector C 2 M 8 m 3 W 0 to display only alarms of that severity level.

2

Click on the More ⋮ button and select an export option to save the displayed alarms to a CSV file.

End of steps

4.13 How do I configure an e-mail policy?

4.13.1 Purpose

The e-mail policy feature allows administrative users to configure e-mail notification policies for specific alarm messages in NFM-P, WS-NOC, MDM, and NSP. See 3.11.6 “What can I configure on the E-mail Policies page?” (p. 71) for information about e-mail policies.

4.13.2 Steps

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

1

In the **Network Map And Health, Current Alarms** view click the More button ⋮ and select Settings. The Alarm Settings form opens.

2

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

3

Click on the **+ Email Policy** button ⊕.

4

Type a name for the policy.

5

Select Enabled or Disabled in the Policy Status drop-down menu.

6

Select an alarm filter.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

The Alarm Filter menu is populated with public advanced filters configured and saved in the Current Alarms list; see 3.2.2 “What can I do in the alarm lists?” (p. 62).

7

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

8

In the Recipient List field, specify the e-mail addresses of the intended recipients for the alarm notification. You can specify up to 20 recipients.

9

Click Save to save the e-mail policy.

END OF STEPS

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Managing alarms

4.14 How do I configure system alarm settings?

4.14.1 Purpose

Use this procedure to configure alarm handling options for alarm messages originating from the NSP system. These settings apply to NSP, WS-NOC, and MDM alarms. NFM-P alarm settings are configured in the NFM-P GUI; see the *NFM-P Administrator Guide*.

You must have administrator privileges to configure alarm settings.

4.14.2 Steps

1

In the **Network Map And Health, Current Alarms** view click the More button ⋮ and select Settings. The Alarm Settings form opens.

2

Click System Settings on the left-hand panel to configure system-wide alarm settings.

3

Enable the Alarm Severity Settings option and then configure manual 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

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4.15 How do I acknowledge an alarm?

4.15.1 Steps

1

In the **Network Map And Health, Current Alarms** view click More ⋮ on the right side of a row and choose Edit Alarm(s).

2

Set the Acknowledge parameter to Acknowledge.

3

You can acknowledge or unacknowledge multiple alarms by using the Ctrl key and selecting the rows before using Edit Alarms(s). When you select multiple alarms, the following limitations apply:

- When you select multiple NFM-P alarms, you can configure the Severity, and Acknowledgement Note.
- When you select multiple NSP, WS-NOC, or MDM alarms, you can configure the Acknowledgement Note.
- When you select a mix of NFM-P and NSP, WS-NOC, or MDM alarms, you can configure the Acknowledgement Note.

4

As required, configure the Severity and Acknowledgement Note and click Save. For NSP, WS-NOC, or MDM alarms, configure the Acknowledgement Note and click Save.

End of steps

4.16 How do I delete or clear an alarm?

4.16.1 Steps

1

In the **Network Map And Health, Current Alarms** view click More ⋮ on the right side of a row and choose Delete Alarm(s) to remove or Clear Alarm(s) to clear the alarm or alarms. You can delete or clear multiple alarms by using the Ctrl key and selecting the alarms.

ℹ **Note:** If the Delete Alarm(s) or Clear Alarm(s) actions are not available, an administrator may need to enable manual alarm deletion or clearing.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2

Click OK on the dialog box to confirm the action, or Cancel to close the dialog box without deleting or clearing the alarms.

END OF STEPS

4.17 How do I edit alarm custom text?

4.17.1 Steps

1

In the **Network Map And Health, Current Alarms** view click More ⋮ on the right side of a row and choose Edit Alarm(s). You can edit custom alarm text for multiple alarms by using the Ctrl key and selecting the alarms.

2

Enter text in the Custom Text field and click SAVE. You can enter a URL, for example: http://www.example.com.

END OF STEPS

4.18 How do I automate alarm management using a policy?

4.18.1 Purpose

When the NSP receives an alarm for the first time, the NSP creates an alarm policy for that alarm. You can use an alarm policy to perform operations automatically on future instances of the alarm. See 3.11.5 “What can I configure on the Individual Alarm Policies page?” (p. 70) for more information.

4.18.2 Steps

1

In the **Network Map And Health, Current Alarms** view, click on the More ⋮ button in the title banner of the current tab and select Settings.

2

Click on Individual Alarm Policies in the left panel. A list of alarm policies appears.

3

Select one or more alarm policies. You can use the column headers to filter or sort the list of alarm policies.

4

Click (Table row actions), Edit. The following table describes the alarm policy parameters.

Parameter	Effect
General Actions	
Squelch	Hides future instances of this alarm. Squelched alarms are not displayed in the Alarm List.
Initial Severity Assignment	Assigns the chosen severity to the alarm when it is received, overriding the severity assigned by the source.
Auto Acknowledge	Acknowledges the alarm when it is received.
History	Disables or enables historical alarm archiving for the alarm.
Custom Text	Applies the specified custom text to the alarm when it arrives, overwriting any custom text assigned by the source.
Escalation Policies	
Escalation Policy	Enable to configure an escalation policy for the alarm. An escalation policy changes the severity of the alarm when a specified threshold is crossed.
Severity	Specifies the severity to assign to the alarm when the threshold is crossed.
Threshold Type	Specifies the type of threshold to use; for example, the number of occurrences.
Threshold Value	The value that must be exceeded in order to trigger escalation; for example, 50 occurrences.
Escalation Policies	
De-escalation Policy	Enable to configure a de-escalation policy for the alarm. A de-escalation policy changes the severity of the alarm when the number of occurrences drops below a specified number.
Severity	Specifies the new severity to assign to the alarm when the policy is triggered.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Parameter	Effect
Threshold Value	Specifies the number of occurrences for the de-escalation threshold. When the number of occurrences of the alarm drops below this value, the de-escalation policy is triggered.
Alarm Debouncing	
Alarm Debouncing	Enables debouncing for the alarm. When alarm debouncing is enabled, alarm clear events are held until the specified hold period expires instead of being processed immediately. If an alarm raise event occurs before the hold period expires, the existing debounced alarm is updated with the new occurrence and the event is processed immediately. This prevents unnecessary historical alarm logging and lowers the frequency of alarm NBI notifications for highly active (flapping) alarms.

5

Click on the Save button to save your changes.

End of steps

4.19 How do I suppress all alarms raised on a port, NE, or resource group?

4.19.1 Purpose

You can use the NSP to squelch all new alarms raised against an NE or a port, or all NEs and ports in a resource group, including service endpoints associated with the port. Squelched alarms are dropped when received, and do not appear as historical events. Squelched alarms received from an NFM-P do not appear in the current alarm list, but continue to appear in the historical and merged alarm lists.

4.19.2 Steps

1

In the **Network Map And Health, Current Alarms** view, click on the More ⋮ button in the title banner of the current tab and select Settings.

2

Select Alarm Squelch in the left panel. The Alarm Squelch panel opens.

3

Click on the Port, NE, or Resource Group tab in the Alarm Squelch panel. A list of objects appears.

4

Select one or more objects and click on (Table row actions), Squelch to squelch the selected objects.

END OF STEPS

4.20 How do I open an SSH or Telnet session with an NE?

4.20.1 Purpose

You can use the NSP to open an SSH or Telnet session with an NE in a browser window. You can open a session from an alarm entry or NE tile in any view. You can only open a session with NEs that are managed using the NFM-P or MDM.

ℹ **Note:** The NSP supports up to 100 concurrent NE sessions. Opening a session with an NE requires that your user privileges include execute permission for the selected NE. See your network administrator for more information.

4.20.2 Steps

1

Perform one of the following:

a. To open a session from the Unhealthy NEs view, click **Show More** ⋮, **Open in NE Session**.

b. To open a session from any alarm list, click **(Table row actions)** ⋮, **Open in NE Session**.

An NE session form opens in a new tab.

2

Select the type of session in the drop-down list, if required, and click **CONNECT**. NEs that are managed using MDM only use the session type configured in the CLI mediation policy. For SSH sessions with nodes managed using the NFM-P, a Login window appears.

3

Enter the username and password for the NE in the Login window for a SSH session, or in the terminal window for a Telnet session.

4

Click the Theme toggle to switch the appearance of the session to black text on a white background.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

5

Click **DISCONNECT** when your session is finished to log out and close the session.

> **Note:** You can click **CONNECT** to open the session again, or enter an IP address in the IP field and click **CONNECT** to open another session with a different NE.

END OF STEPS

4.21 How do I automate escalating or de-escalating alarms?

4.21.1 Purpose

You can use an alarm policy to automatically escalate or de-escalate an alarm based on configurable triggers. These settings apply to NSP, WS-NOC, and MDM alarms. NFM-P alarm settings are configured in the NFM-P GUI; see the *NFM-P Administrator Guide*.

You must have administrator privileges to configure alarm settings.

4.21.2 Steps

1

In the **Network Map and Health, Current Alarms** view, click on the More ⋮ button in the title banner of the current tab and select Settings.

2

Click on Individual Alarm Policies in the left panel. A list of alarm policies appears.

3

Select one or more alarm policies. You can use the column headers to filter or sort the list of alarm policies.

4

Click on (Table row action), Edit. The Alarm Policy edit form appears.

5

Navigate to the Escalation Policy panel and enable the Escalation Policy parameter.

6

Configure the Severity parameter to specify a different severity to be applied to the alarm when the frequency threshold is reached.

7

Select an Escalation Threshold Type. The following table describes the escalation threshold types. De-escalation policies only support the Frequency threshold type.

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Threshold type	Description
Frequency	How many times the alarm has occurred in the last 24 hours.
Number of Occurrences	How many occurrences of the alarm have been reported.
Days without Ack/Clear	How many days have elapsed without the alarm being acknowledged or cleared.

8

Configure the Escalation Threshold Value parameter for the selected escalation threshold type.

9

Enable the De-Escalation Policy parameter.

10

Configure the Severity parameter to a new severity to apply to the alarm when the alarm is de-escalated, and a De-Escalation Threshold Value.

11

Click Save. The new policy is applied to the alarm.

END OF STEPS

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

A Assurance application evolution

A.1 How has assurance changed in NSP?

A.1.1 Overview

The NSP has significantly evolved its user interface in Release 23.11. The purpose of this appendix is to demonstrate graphically the evolution of the assurance applications in 23.11 and help customers who are upgrading to 23.11 to adapt quickly to the new layout and navigation.

Note: Starting with upgrades to NSP 23.11, any customizations to assurance applications that you may have saved as preferences will have to be reconfigured.

See the *NSP User Guide* for more information on the UI evolution and common behaviors of the new UI in 23.11.

A.2 Managing alarms

A.2.1 What do I use instead of the NFM-P Alarm Window or NSP Alarm Views?

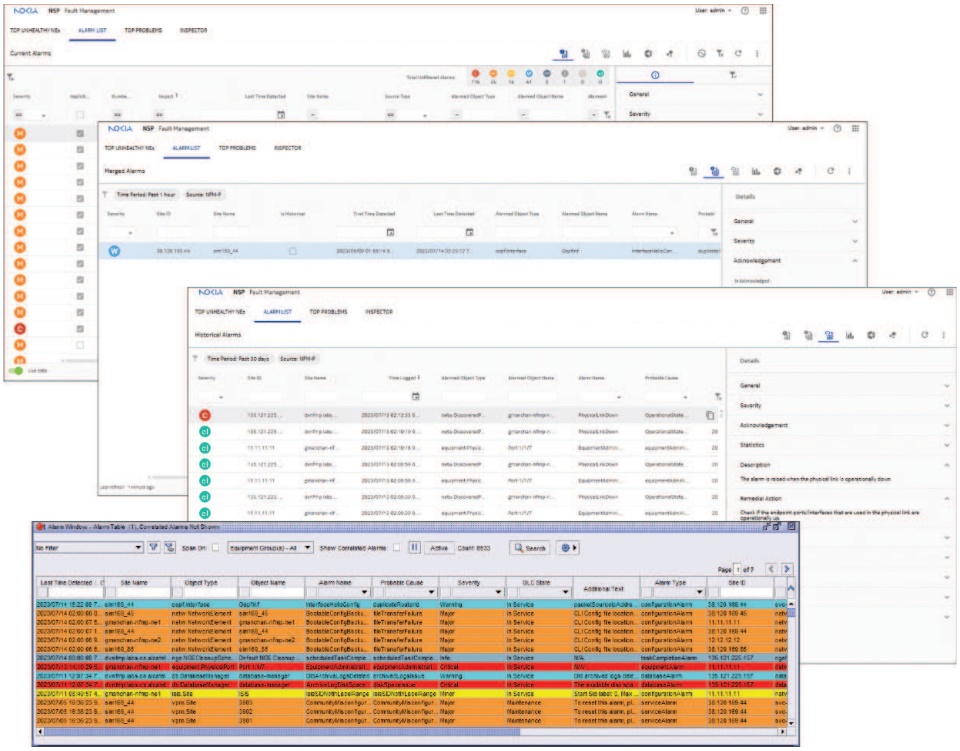
All of the alarm management features available in pre-23.11 NSP releases remain available in 23.11. You can now use Current Alarms, or the Network Health or Troubleshooting dashboards to access alarm management features.

New navigation

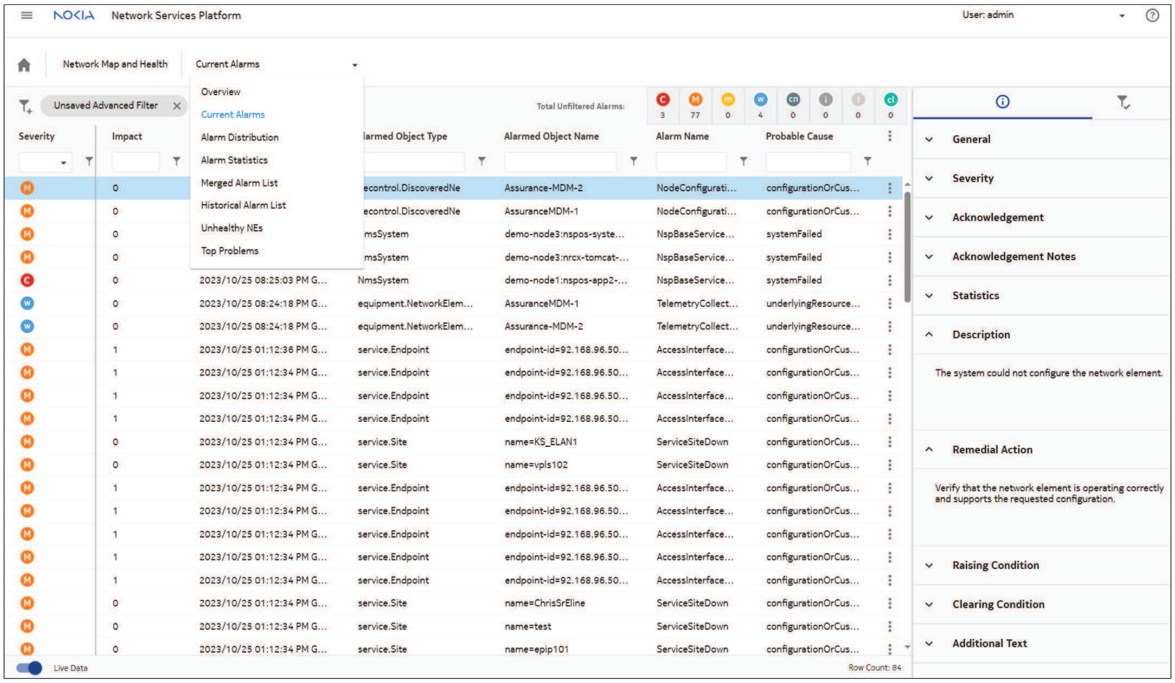
Open **Network Map and Health**, or open **Current Alarms**

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Fault Management Alarms Views + NFM-P Alarm window (pre 23.11)



Current Alarms (23.11)



Total Unfiltered Alarms:

C	M	m	w	cn	i	i	cl
3	77	0	4	0	0	0	0

Severity	Impact		larmed Object Type	Alarmed Object Name	Alarm Name	Probable Cause
M	0		econtrol.DiscoveredNe	Assurance-MDM-2	NodeConfigurati...	configurationOrCus...
M	0		econtrol.DiscoveredNe	AssuranceMDM-1	NodeConfigurati...	configurationOrCus...
M	0		msSystem	demo-node3:nspos-syste...	NspBaseService...	systemFailed
M	0		msSystem	demo-node3:nrcx-tomcat-...	NspBaseService...	systemFailed
C	0	2023/10/25 08:25:03 PM G...	NmsSystem	demo-node1:nspos-app2-...	NspBaseService...	systemFailed
W	0	2023/10/25 08:24:18 PM G...	equipment.NetworkElem...	AssuranceMDM-1	TelemetryCollect...	underlyingResource...
W	0	2023/10/25 08:24:18 PM G...	equipment.NetworkElem...	Assurance-MDM-2	TelemetryCollect...	underlyingResource...
M	1	2023/10/25 01:12:36 PM G...	service.Endpoint	endpoint-id=92.168.96.50...	AccessInterface...	configurationOrCus...
M	1	2023/10/25 01:12:34 PM G...	service.Endpoint	endpoint-id=92.168.96.50...	AccessInterface...	configurationOrCus...
M	1	2023/10/25 01:12:34 PM G...	service.Endpoint	endpoint-id=92.168.96.50...	AccessInterface...	configurationOrCus...
M	1	2023/10/25 01:12:34 PM G...	service.Endpoint	endpoint-id=92.168.96.50...	AccessInterface...	configurationOrCus...
M	0	2023/10/25 01:12:34 PM G...	service.Site	name=KS_ELAN1	ServiceSiteDown	configurationOrCus...
M	0	2023/10/25 01:12:34 PM G...	service.Site	name=vpls102	ServiceSiteDown	configurationOrCus...
M	1	2023/10/25 01:12:34 PM G...	service.Endpoint	endpoint-id=92.168.96.50...	AccessInterface...	configurationOrCus...
M	1	2023/10/25 01:12:34 PM G...	service.Endpoint	endpoint-id=92.168.96.50...	AccessInterface...	configurationOrCus...
M	1	2023/10/25 01:12:34 PM G...	service.Endpoint	endpoint-id=92.168.96.50...	AccessInterface...	configurationOrCus...
M	1	2023/10/25 01:12:34 PM G...	service.Endpoint	endpoint-id=92.168.96.50...	AccessInterface...	configurationOrCus...
M	1	2023/10/25 01:12:34 PM G...	service.Endpoint	endpoint-id=92.168.96.50...	AccessInterface...	configurationOrCus...
M	0	2023/10/25 01:12:34 PM G...	service.Site	name=ChrisSrEline	ServiceSiteDown	configurationOrCus...
M	0	2023/10/25 01:12:34 PM G...	service.Site	name=test	ServiceSiteDown	configurationOrCus...
M	0	2023/10/25 01:12:34 PM G...	service.Site	name=epip101	ServiceSiteDown	configurationOrCus...

Row Count: 84

General

Severity

Acknowledgement

Acknowledgement Notes

Statistics

Description

The system could not configure the network element.

Remedial Action

Verify that the network element is operating correctly and supports the requested configuration.

Raising Condition

Clearing Condition

Additional Text

38883

A.2.2 How have the fault management diagrams changed?

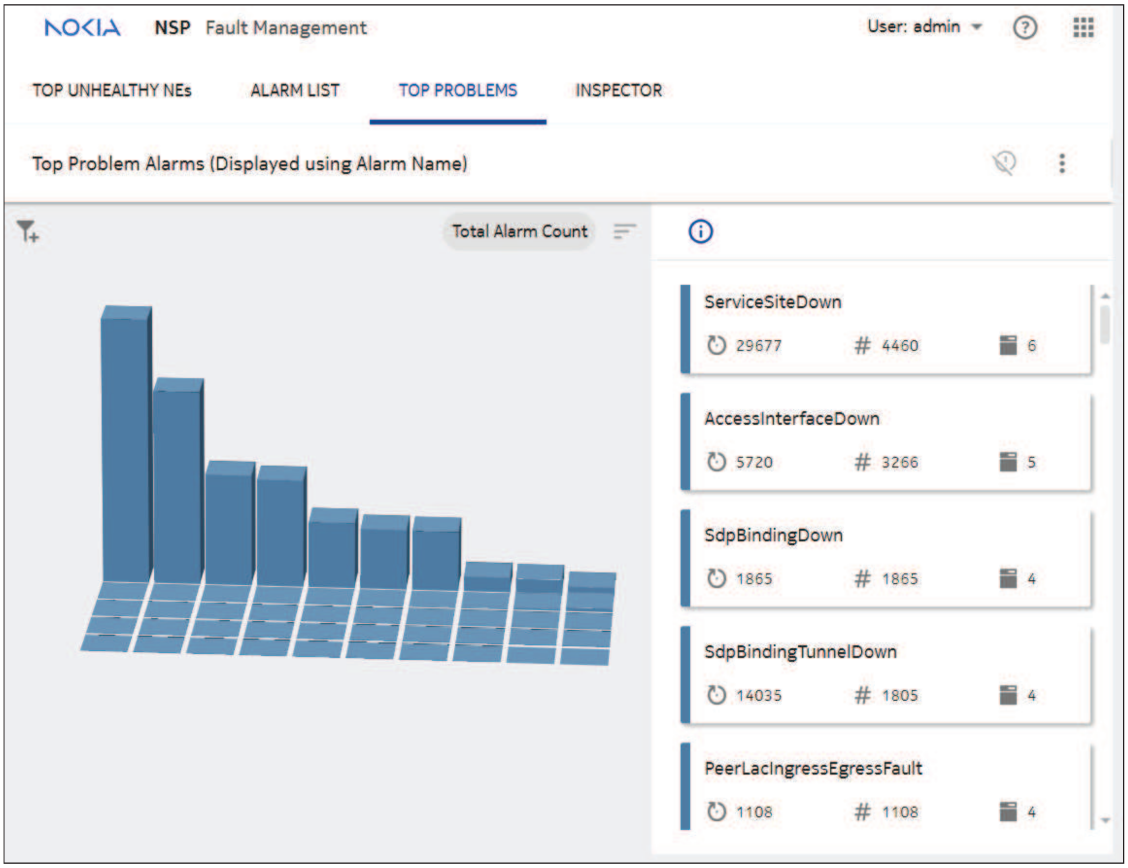
In NSP 23.11, the fault management diagrams have been simplified to improve readability, labelling, and zooming features. See examples: Top Problems, Impact Diagram.

New navigation: Top Problems

Open **Network Map and Health, Top Problems**

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Top Problems view (pre 23.11)



Top Problem Alarms (Displayed using Alarm Name)

ServiceSiteDown
29677 # 4460 6

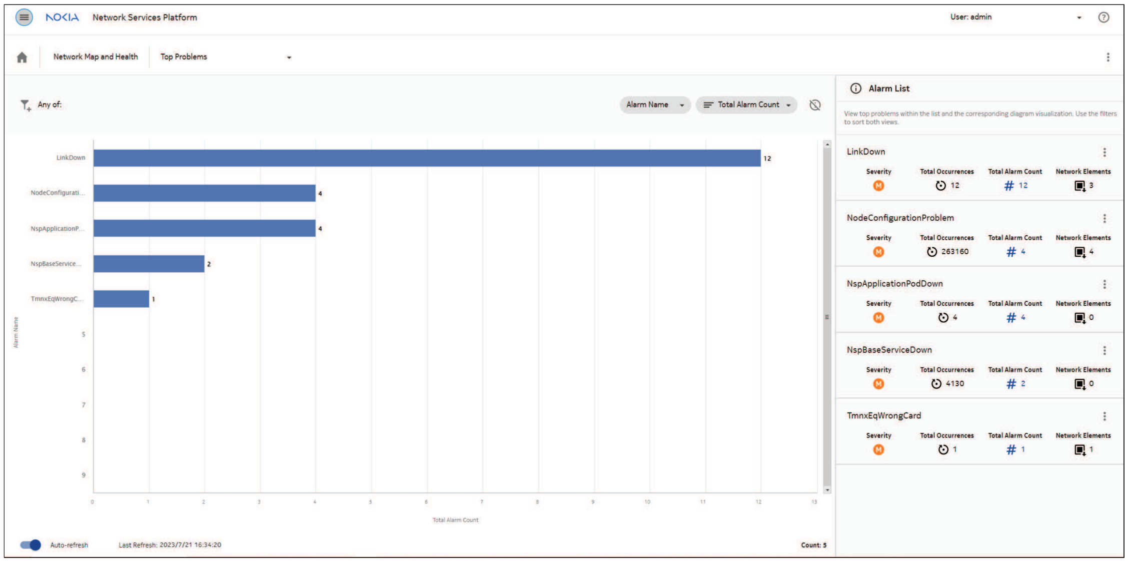
AccessInterfaceDown
5720 # 3266 5

SdpBindingDown
1865 # 1865 4

SdpBindingTunnelDown
14035 # 1805 4

PeerLacIngressEgressFault
1108 # 1108 4

Top Problems view (23.11)



Last Refresh: 2023/7/21 16:34:20

Count: 5

Alarm List

View top problems within the list and the corresponding diagram visualization. Use the filters to sort both views.

	Severity	Total Occurrences	Total Alarm Count	Network Elements
LinkDown	M	12	# 12	3
NodeConfigurationProblem	M	263160	# 4	4
NspApplicationPodDown	M	4	# 4	0
NspBaseServiceDown	M	4130	# 2	0
TmnxEqWrongCard	M	1	# 1	1

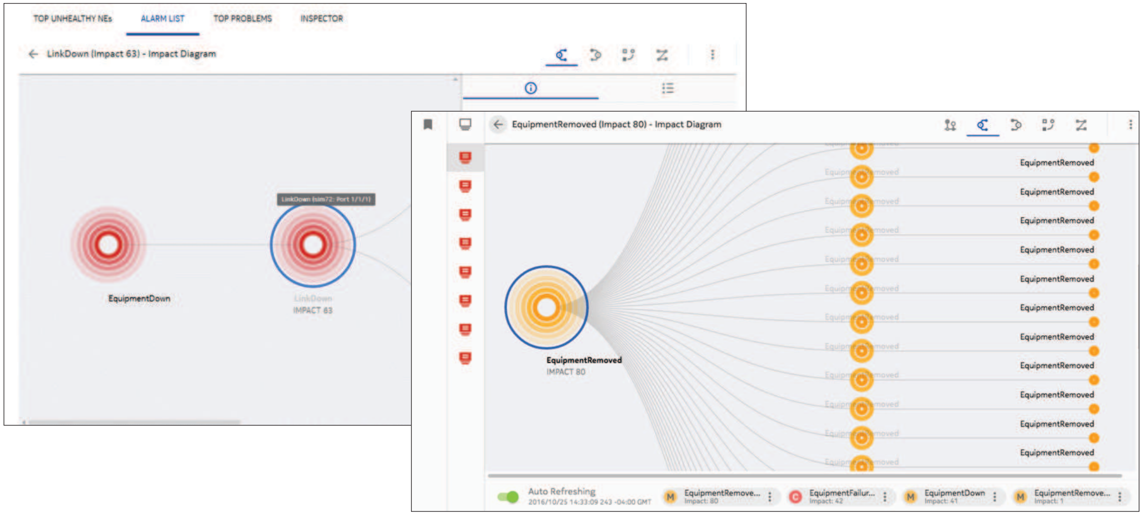
38882

New navigation: Impact Diagram

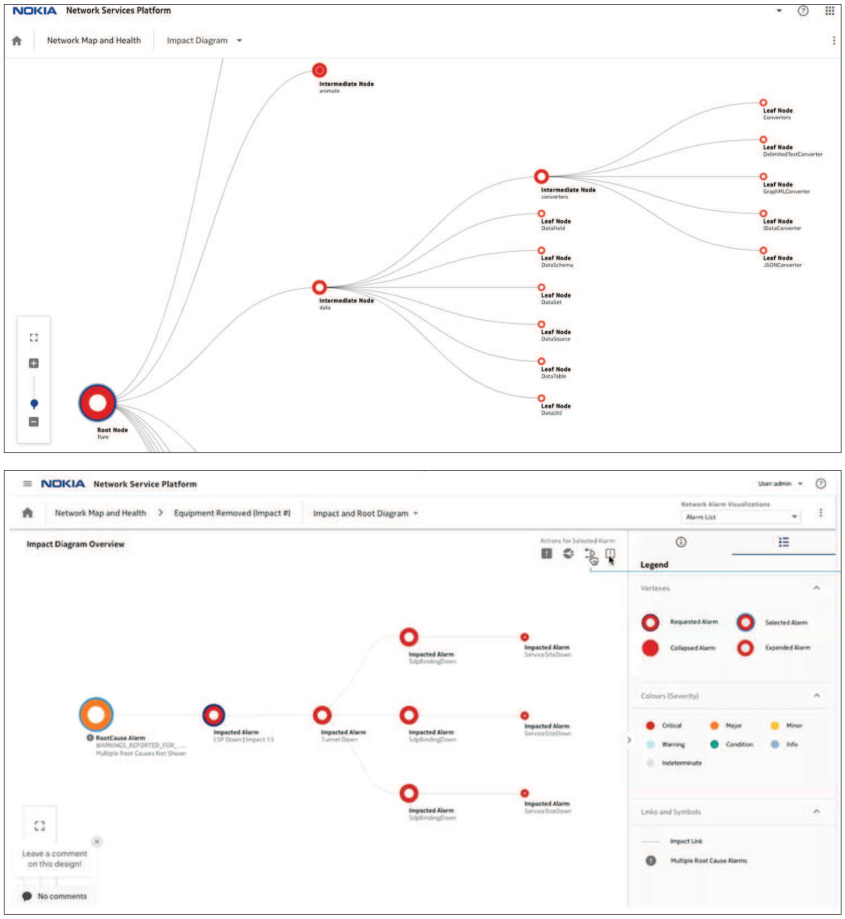
Open **Network Map and Health**, select an alarm that has impacts, click ⋮ **Table Row Actions** , **Impact Diagram**

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Root cause and impact diagrams (pre 23.11)


TOP UNHEALTHY NEs
ALARM LIST
TOP PROBLEMS
INSPECTOR
LinkDown (Impact 63) - Impact Diagram
EquipmentDown
LinkDown
IMPACT 63
EquipmentRemoved (Impact 80) - Impact Diagram
EquipmentRemoved
IMPACT 80
EquipmentRemoved
Auto Refreshing
EquipmentRemove... Impact: 80
EquipmentFailur... Impact: 42
EquipmentDown Impact: 41
EquipmentRemove... Impact: 1

Root cause and impact diagrams (23.11)



39006

A.2.3 Where is the Current Alarm Hierarchy?

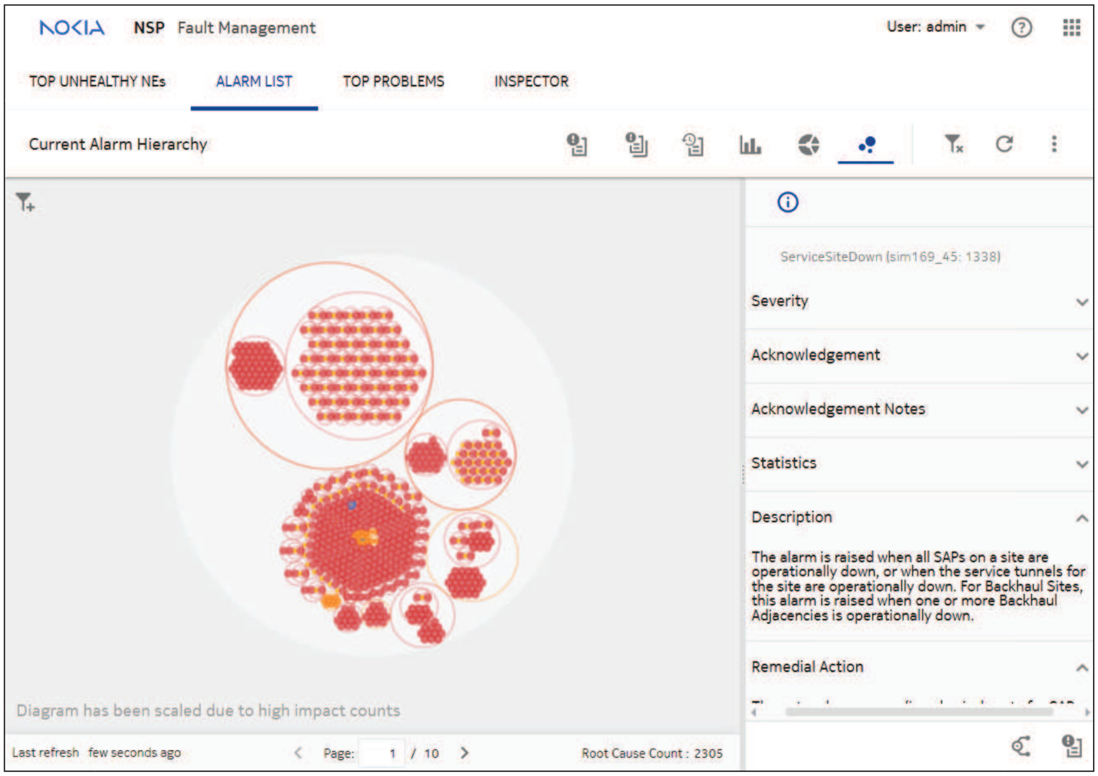
In NSP 23.11, Current Alarm Hierarchy has been removed and replaced by the Distribution Diagram.

New navigation

Open **Network Map and Health, Distribution Diagram**

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Current Alarm Hierarchy (pre 23.11)

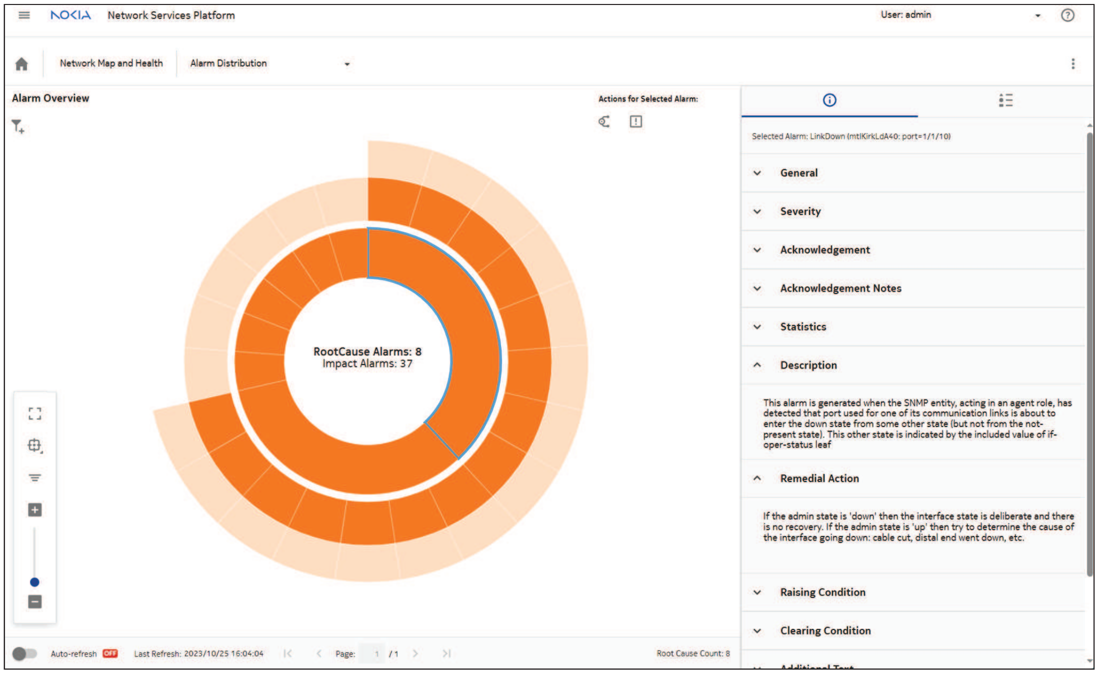


ServiceSiteDown (sim169_45: 1338)

The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.

Diagram has been scaled due to high impact counts

Distribution Diagram (23.11)



Selected Alarm: LinkDown (mtlKirkLdA40: port=1/1/10)

This alarm is generated when the SNMP entity, acting in an agent role, has detected that port used for one of its communication links is about to enter the down state from some other state (but not from the not-present state). This other state is indicated by the included value of if-oper-status leaf

If the admin state is 'down' then the interface state is deliberate and there is no recovery. If the admin state is 'up' then try to determine the cause of the interface going down: cable cut, distal end went down, etc.

38884

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

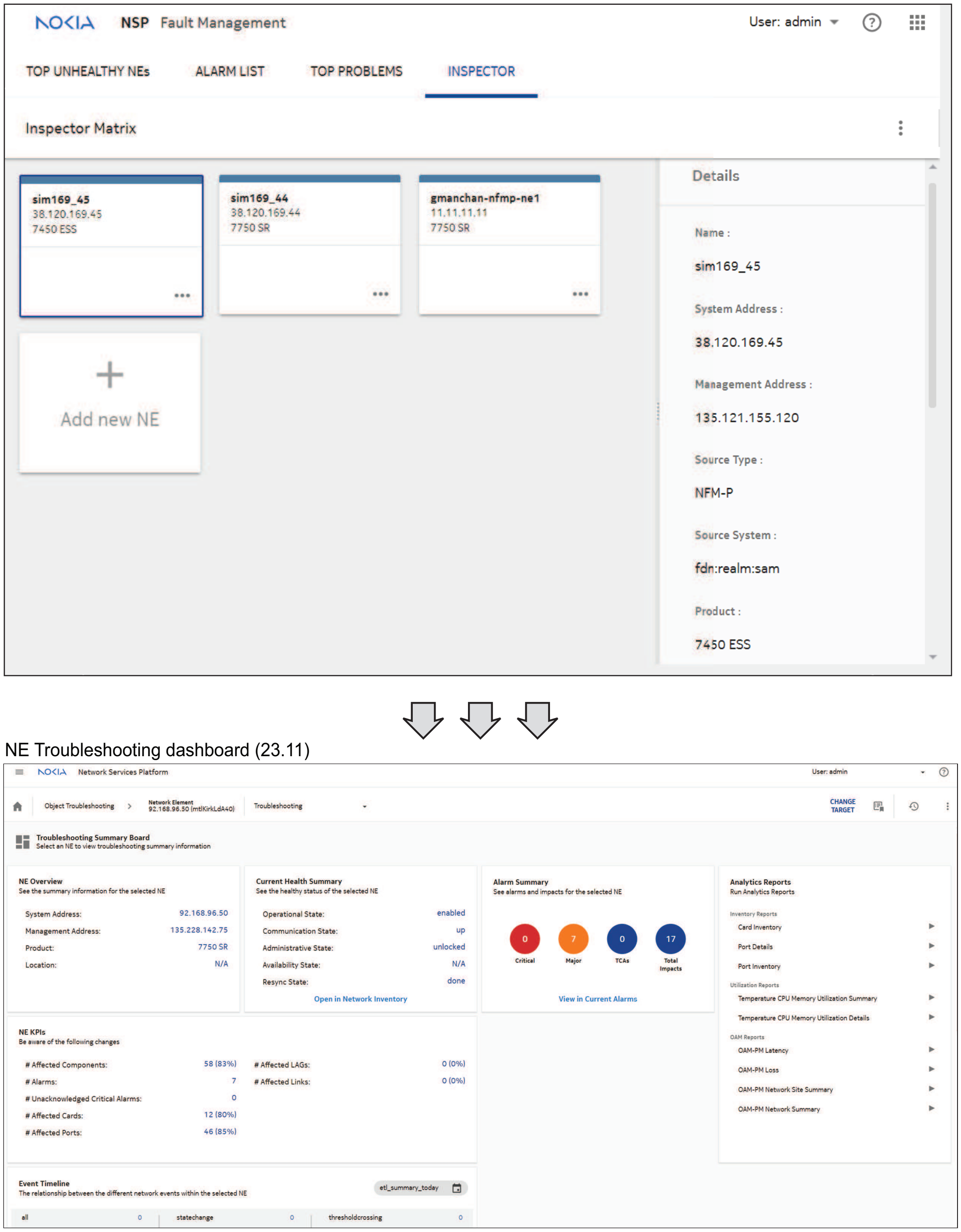
A.2.4 Where is the Inspector Matrix?

In NSP 23.11, Inspector Matrix has been removed and replaced by the NE Troubleshooting dashboard.

New navigation:

Open **Object Troubleshooting, Network Element**

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms



Inspector Matrix (pre 23.11)

NOKIA NSP Fault Management

User: admin

TOP UNHEALTHY NEs | ALARM LIST | TOP PROBLEMS | INSPECTOR

Inspector Matrix

sim169_45
38.120.169.45
7450 ESS

sim169_44
38.120.169.44
7750 SR

gmanchan-nfmp-ne1
11.11.11.11
7750 SR

+ Add new NE

Details

Name :
sim169_45

System Address :
38.120.169.45

Management Address :
135.121.155.120

Source Type :
NFM-P

Source System :
fdn:realm:sam

Product :
7450 ESS

NE Troubleshooting dashboard (23.11)

NOKIA Network Services Platform

User: admin

Object Troubleshooting > Network Element 92.168.96.50 (mtlKirkLdA40) | Troubleshooting

CHANGE TARGET

Troubleshooting Summary Board
Select an NE to view troubleshooting summary information

NE Overview
See the summary information for the selected NE

System Address:	92.168.96.50
Management Address:	135.228.142.75
Product:	7750 SR
Location:	N/A

Current Health Summary
See the healthy status of the selected NE

Operational State:	enabled
Communication State:	up
Administrative State:	unlocked
Availability State:	N/A
Resync State:	done

Open in Network Inventory

Alarm Summary
See alarms and impacts for the selected NE

Critical	Major	TCAs	Total Impacts
0	7	0	17

View in Current Alarms

Analytics Reports
Run Analytics Reports

Inventory Reports
- Card Inventory ▶
- Port Details ▶
- Port Inventory ▶

Utilization Reports
- Temperature CPU Memory Utilization Summary ▶
- Temperature CPU Memory Utilization Details ▶

OAM Reports
- OAM-PM Latency ▶
- OAM-PM Loss ▶
- OAM-PM Network Site Summary ▶
- OAM-PM Network Summary ▶

NE KPIs
Be aware of the following changes

# Affected Components:	58 (83%)	# Affected LAGs:	0 (0%)
# Alarms:	7	# Affected Links:	0 (0%)
# Unacknowledged Critical Alarms:	0		
# Affected Cards:	12 (80%)		
# Affected Ports:	46 (85%)		

Event Timeline
The relationship between the different network events within the selected NE

etl_summary_today

all	0	statechange	0	thresholdcrossing	0

38885

A.3 Monitoring the network and services

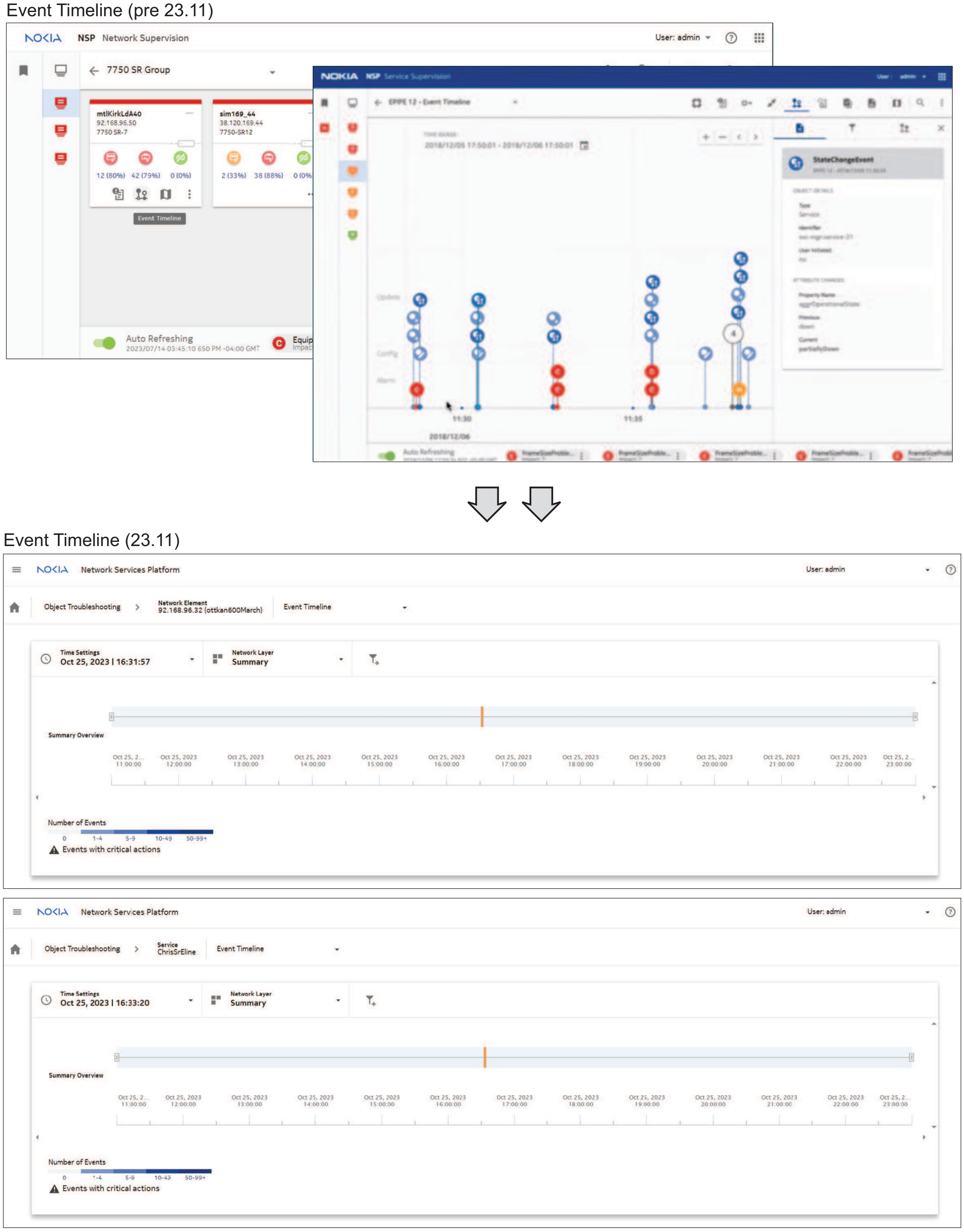
A.3.1 How has Event Timeline changed?

In NSP 23.11, this view has been updated to a simplified graphic to address scale issues and improve panning, zooming, and time scale labels. The Event Timeline has been moved to the NE and Service Troubleshooting dashboards.

New navigation

Open **Object Troubleshooting, Network Element or Service, Event Timeline**

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms



Time Settings
Oct 25, 2023 | 16:31:57

Network Layer
Summary

Time Settings
Oct 25, 2023 | 16:33:20

Network Layer
Summary

38837

A.3.2 How has service supervision changed?

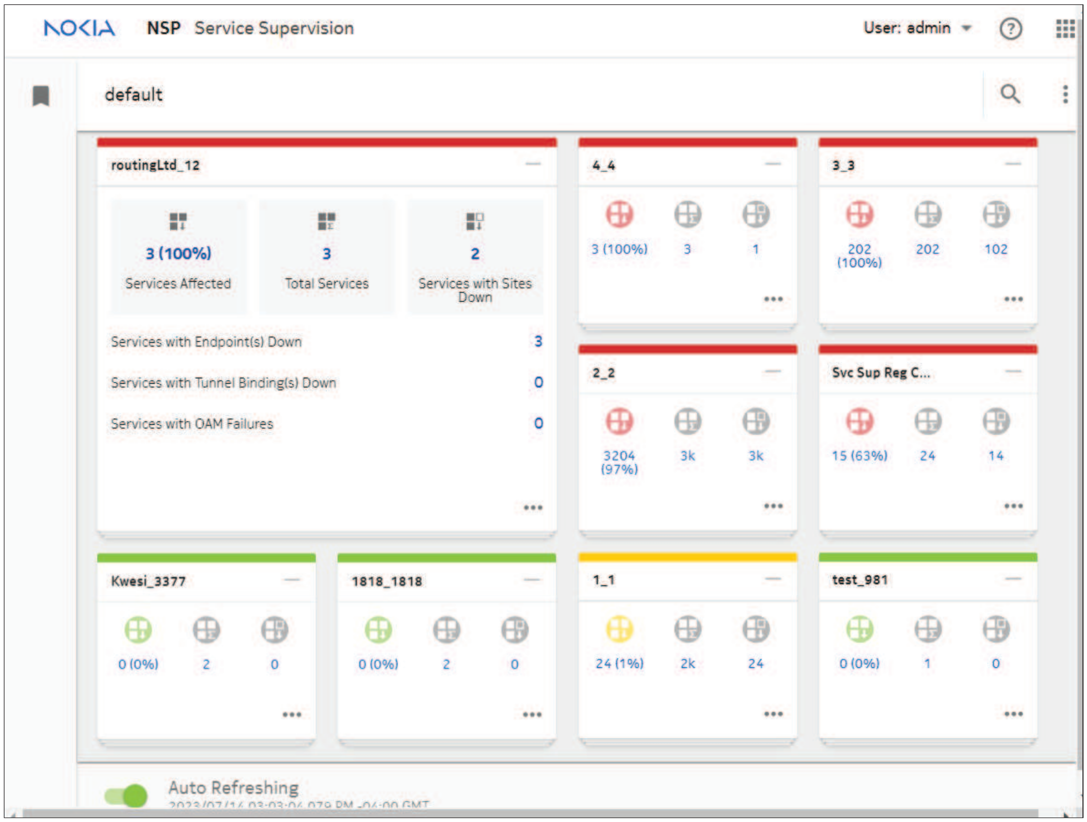
In NSP 23.11, the functionality previously delivered by the Service Supervision application (including Service health KPIs, Tunnel bindings, etc.) has been migrated to the Service Troubleshooting dashboard.

New navigation

Open **Object Troubleshooting, Service**

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Service Supervision dashboard (pre 23.11)

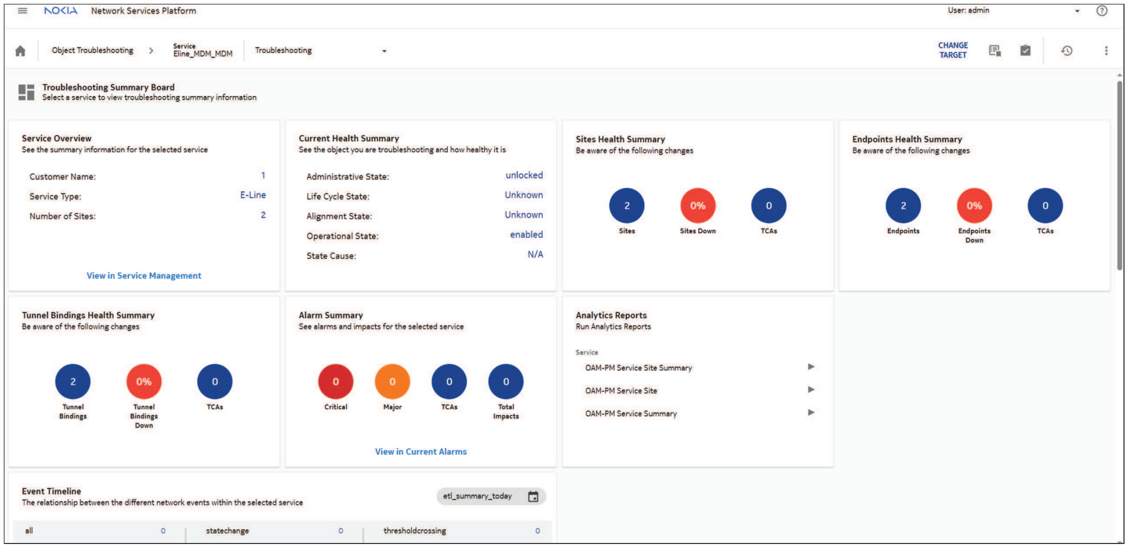


Services with Endpoint(s) Down 3

Services with Tunnel Binding(s) Down 0

Services with OAM Failures 0

Service Troubleshooting dashboard (23.11)



Troubleshooting Summary Board
Select a service to view troubleshooting summary information

Service Overview
See the summary information for the selected service

Customer Name: 1
Service Type: E-Line
Number of Sites: 2

Current Health Summary
See the object you are troubleshooting and how healthy it is

Administrative State: unlocked
Life Cycle State: Unknown
Alignment State: Unknown
Operational State: enabled
State Cause: N/A

Sites Health Summary
Be aware of the following changes

Endpoints Health Summary
Be aware of the following changes

Tunnel Bindings Health Summary
Be aware of the following changes

Alarm Summary
See alarms and impacts for the selected service

Analytics Reports
Run Analytics Reports

Service
- OAM-PM Service Site Summary ▶
- OAM-PM Service Site ▶
- OAM-PM Service Summary ▶

Event Timeline
The relationship between the different network events within the selected service

all 0 | statechange 0 | thresholdcrossing 0

38881

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

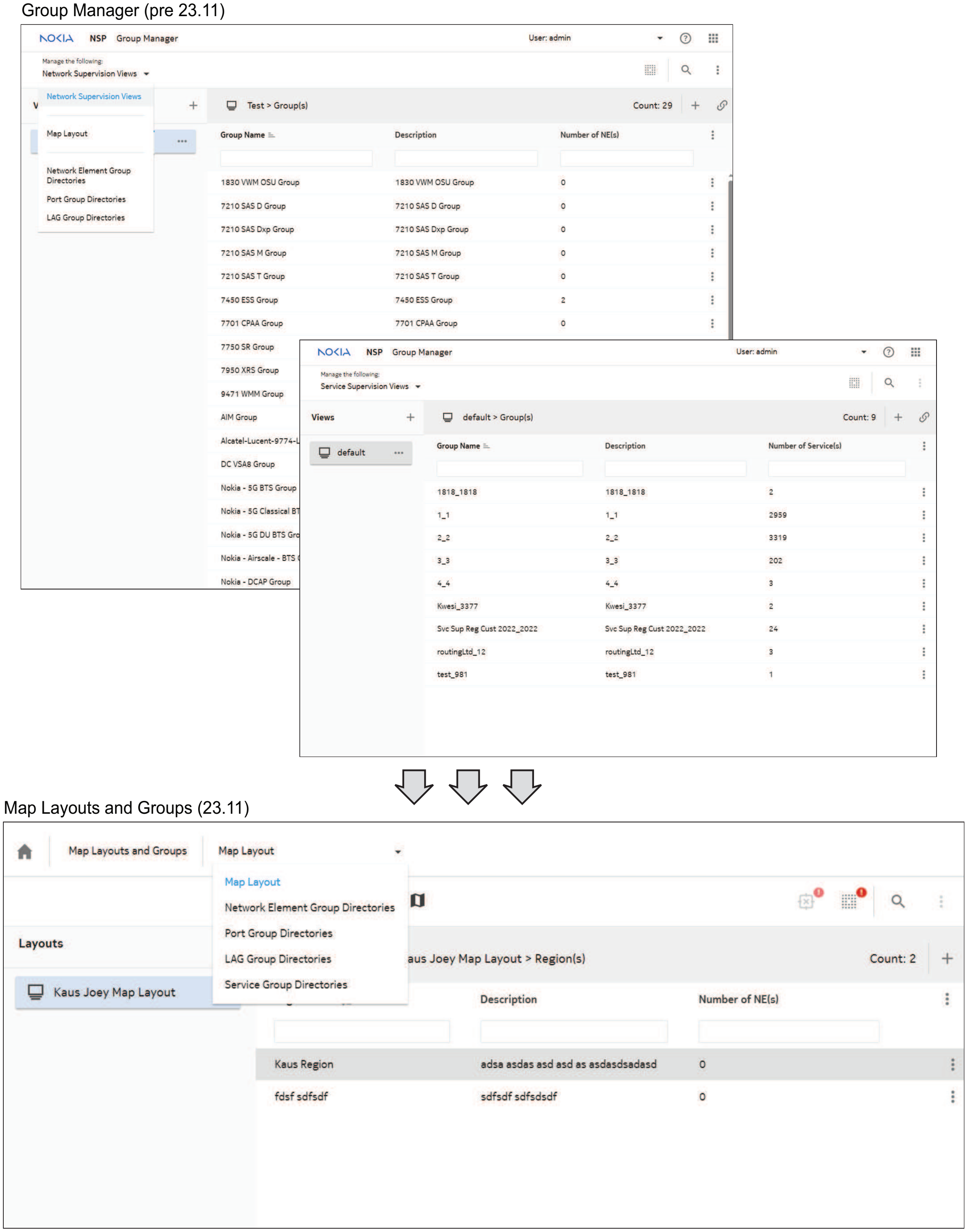
A.3.3 How have supervision views and groups changed?

In NSP 23.11, Network and Service Supervision views and groups that were available in the former Group Manager application are not included in Map Layouts and Groups. In Map Layouts and Groups, you can configure a common map layout for use in all NSP map views, and you can configure resource group directories and resource groups for use in the Network Functions GUI views. For more information, see "Network resource groups" in the *NSP System Administrator Guide*.

New navigation

Open **Map Layouts and Groups, Map Layout**

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms



Group Manager (pre 23.11)

Group Name	Description	Number of NE(s)
1830 VWM OSU Group	1830 VWM OSU Group	0
7210 SAS D Group	7210 SAS D Group	0
7210 SAS Dxp Group	7210 SAS Dxp Group	0
7210 SAS M Group	7210 SAS M Group	0
7210 SAS T Group	7210 SAS T Group	0
7450 ESS Group	7450 ESS Group	2
7701 CPAA Group	7701 CPAA Group	0
7750 SR Group		
7950 XRS Group		
9471 WMM Group		
AIM Group		
Alcatel-Lucent-9774-L		
DC VSA8 Group		
Nokia - 5G BTS Group		
Nokia - 5G Classical BT		
Nokia - 5G DU BTS Gro		
Nokia - Airscale - BTS (		
Nokia - DCAP Group		

Group Name	Description	Number of Service(s)
1818_1818	1818_1818	2
1_1	1_1	2959
2_2	2_2	3319
3_3	3_3	202
4_4	4_4	3
Kwesi_3377	Kwesi_3377	2
Svc Sup Reg Cust 2022_2022	Svc Sup Reg Cust 2022_2022	24
routingLtd_12	routingLtd_12	3
test_981	test_981	1

Map Layouts and Groups (23.11)

	Description	Number of NE(s)
Kaus Region	adsa asdas asd asd as asdasdsadasd	0
fdsf sdfsdf	sdfsdf sdfsdsdf	0

38914

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

A.4 Combining views

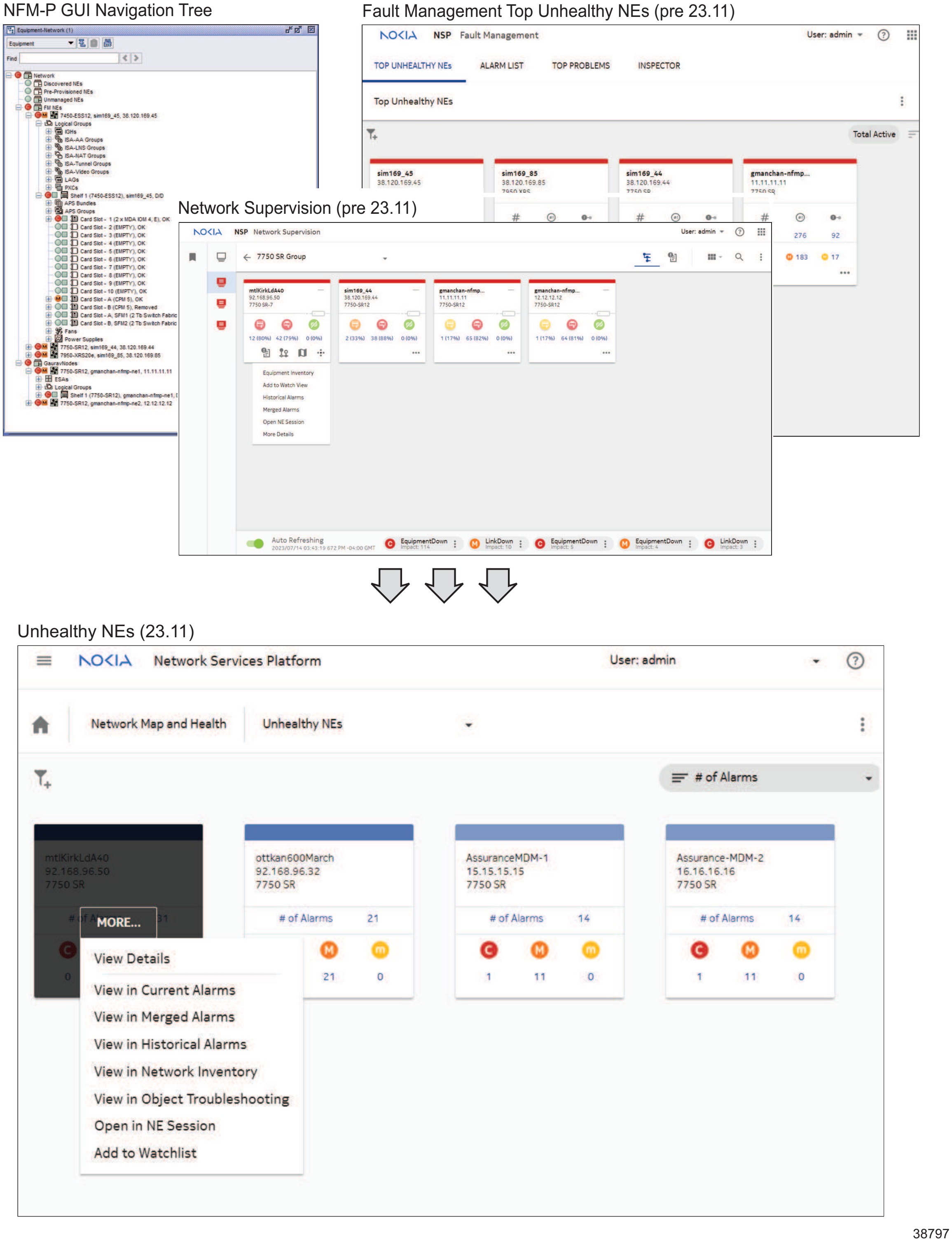
A.4.1 How do I view unhealthy NEs?

Before 23.11, you viewed top unhealthy NEs through the Top Unhealthy NEs matrix in Fault Management or Network Supervision. In NSP 23.11, the Fault Management and Network Supervision matrixes have been combined into one simplified and focused matrix as part of the Network Map and Health dashboard.

New navigation

Open **Network Map and Health, Unhealthy NEs**

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms


NFM-P GUI Navigation Tree
Fault Management Top Unhealthy NEs (pre 23.11)
Network Supervision (pre 23.11)
Unhealthy NEs (23.11)
NOKIA
Network Services Platform
User: admin
Network Map and Health
Unhealthy NEs
# of Alarms
mtlKirkLdA40
92.168.96.50
7750 SR
MORE...
View Details
View in Current Alarms
View in Merged Alarms
View in Historical Alarms
View in Network Inventory
View in Object Troubleshooting
Open in NE Session
Add to Watchlist
ottkan600March
92.168.96.32
7750 SR
# of Alarms
21
21
0
AssuranceMDM-1
15.15.15.15
7750 SR
# of Alarms
14
1
11
0
Assurance-MDM-2
16.16.16.16
7750 SR
# of Alarms
14
1
11
0
38797

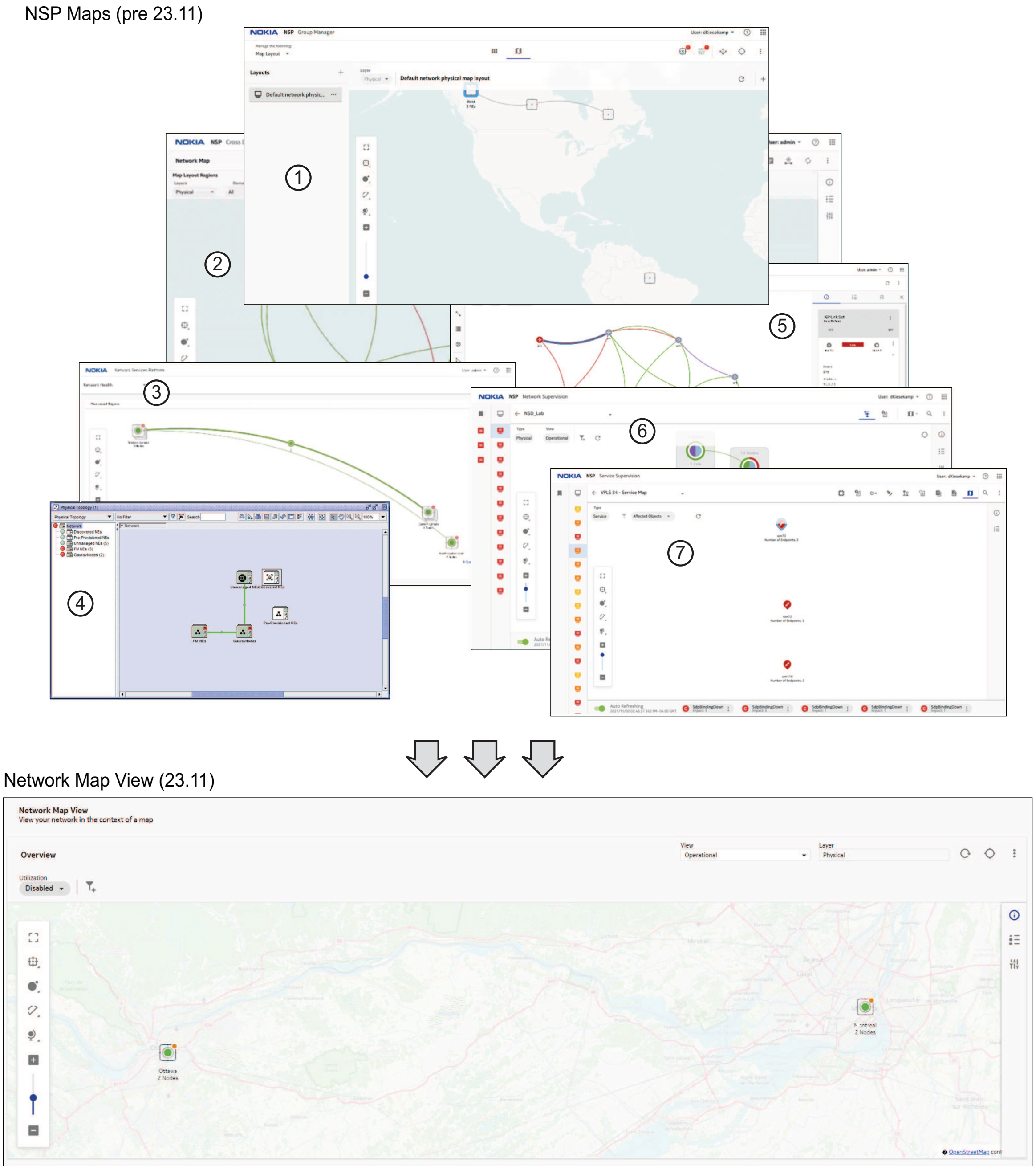
A.4.2 How have maps changed?

In NSP 23.11, all existing NSP maps have been consolidated to simplify and enhance users' experience through improved labeling and layout of information.

New navigation

Open **Network Health View, Network Map View**

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms



38836

Figure legend: NSP Maps (pre 23.11)

1. Group Manager Map Layout
2. Cross Domain Coordinator Network Map

3. NSP Network Health
4. NFM-P GUI Physical Topology
5. IP/MPLS Optimization Network Map
6. Network Supervision Map
7. Service Supervision Service Map

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms

© 2023 Nokia.
Use subject to Terms available at: www.nokia.com/terms