



NSP

Network Services Platform

Release 25.8

Enterprise Guide

3HE-21453-AAAB-TQZZA

Issue 1

September 2025

© 2025 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.

© 2025 Nokia.

Contents

About this document	5
1 Overview	7
1.1 The Nokia Network Services Platform (NSP)	7
2 Installation	9
2.1 Installing Enterprise NSP	9
3 Enterprise NSP onboarding	11
3.1 What is onboarding and how do I start it?	11
3.2 How do I import artifacts?	11
3.3 How do I create unified discovery rules?	12
3.4 How do I discover nodes?	14
3.5 How do I create a background map layer?	15
3.6 How do I set statistics for nodes and links?	16
3.7 How do I create roles?	16
3.8 How do I create user groups?	17
3.9 How do I create users?	18
3.10 How do I complete the Setup Overview step?	19
4 Using Enterprise NSP	21
4.1 Enterprise NSP menus	21
5 Network viewing and monitoring	23
5.1 Network Map and Health	23
5.2 Network Inventory	24
6 Enterprise utilities - service management	25
6.1 Managing network services	25
6.2 Service Management menu	25
7 Device administration	27
7.1 Device Management	27
7.2 Device discovery	28
7.3 Model driven configurator	29

8	Data collection and analysis	31
8.1	Telemetry management using NSP	31
9	NSP administration and security	33
9.1	System health	33
9.2	Map layouts and groups.....	33
9.3	File server	34
9.4	Artifacts	34
9.5	Users and system security	34
9.6	Network Security	34
10	Procedures	35
10.1	Device discovery procedures	35

About this document

Purpose

The *NSP Enterprise Guide* describes the supported use-cases for Enterprise deployments of the NSP.

Scope

This document describes the enabling and management of NSP Enterprise functions.

Document support

Customer documentation and product support URLs:

- [Documentation Center](#)
- [Technical support](#)

How to comment

Please send your feedback to [Documentation Feedback](#).

1 Overview

1.1 The Nokia Network Services Platform (NSP)

1.1.1 What is NSP?

The Nokia NSP is a network management solution that provides network automation, assurance, service management, and configuration functions for small, medium, and large network deployments across multiple technology types. The NSP manages devices/nodes, links, network layers, and services as a fully functional Network Management System (NMS) from branch-level local networks up to carrier-level ISP networks.

1.1.2 What is Enterprise NSP?

Nokia Enterprise NSP is a simplified type of NSP deployment that provides domain-specific functions for:

- Utilities
- Defense (not supported in the current release)
- Transportation (not supported in the current release)
- Public Safety (not supported in the current release)

The functionality available to Enterprise NSP users is customized based on the use-case type. Each user type sees a unique, specific menu tree that provides the required functionality in a simplified, easy-to-understand format.

2 Installation

2.1 Installing Enterprise NSP

2.1.1 NSP system overview

The Enterprise NSP system is deployed as cluster of one or more VMs in the **Kubernetes container environment**. The NSP system consists of a **deployer host**, which holds the container image and Helm repositories and deploys the containerization environment for NSP clusters, and the NSP **cluster VMs**, which host the main NSP functions and load balance as needed. Within NSP cluster VMs, the NSP cluster host performs configuration operations.

Kubernetes is the orchestration system that hosts the NSP VM clusters and is included in the NSP software bundle. For more information about the NSP components described here, see the *NSP Installation and Upgrade Guide*.

2.1.2 Feature packages

Enterprise NSP requires the base *Platform* feature package as a minimum.

2.1.3 Enabling the Enterprise NSP UI

A typical NSP installation contains UI elements for a wide variety of functions. Enterprise NSP has a focused UI that only contains the relevant elements for the use-case type. In order to display the UI for the desired Enterprise NSP use-case, before installing NSP you must edit the `nsp-config.yml` configuration file as follows:

```
nsp:

  deployment:

    type: standard

    mode: enterprise-utilities
```

User access and permissions in the Enterprise UI

Admin users have full access and read/write/execute permissions for all options in the NSP menu tree. All other user types have their access defined according to Role Based Access Control, or RBAC. Enterprise NSP Admin users are required to use RBAC when configuring other user accounts to ensure that they have the permission levels that their duties require.

User configuration is described in the *NSP System Administrator Guide*.

2.1.4 Installing artifacts, adaptors, and intent types

Artifacts and adaptors are resource files that define network node characteristics and allow for management support in NSP by providing the mapping between node attributes and NSP attributes. Intent types, which define service characteristics, are also considered artifacts and can

be installed using the NSP UI. These files typically come in the form of zip bundles that you obtain from the [NSP software download site](#) and import using NSP.

You will have the option to install NSP artifacts as part of the onboarding process. After onboarding, if you need to import additional artifacts later, use the procedures in the *NSP Network Automation Guide* rather than the onboarding wizard. To discover and manage Nokia 7210 SAS and 7705 SAR nodes in an NSP Enterprise deployment that does not include the NFM-P component, artifact bundles are available for download from the [NSP software download site](#) and described in the *NSP Nokia Enterprise Artifact Guide*.

To view the SAS/SAR artifacts bundle, see the *NSP Nokia Enterprise Artifact Guide*.

Caution: Do **not** install the SAS/SAR artifact bundle if NFM-P is present in the deployment. The SAS/SAR adaptor artifacts are intended for use only when basic inventory and alarms are required, and provisioning is not required.

To install an intent type, see *How do I import an intent type from my computer?* in the *Network Automation Guide*.

3 Enterprise NSP onboarding

3.1 What is onboarding and how do I start it?


Enterprise NSP has an onboarding wizard that takes you through the basics of setting up the NSP managed network. You will import artifacts to enable node management, create discovery rules to scan the network, manage node discovery, configure map options, enable statistics collection, and set up user accounts that will grant users specific permissions. This chapter describes each major step of the onboarding wizard.


The onboarding wizard starts automatically when you log into Enterprise NSP for the first time. If you close the onboarding wizard without finishing or skipping it, you can return to it by navigating to the following URL:


`https://nsp_ip_address/web/onboarding/home`

Once the onboarding wizard is open, you have the following options:

- **Get started**—Continue with the onboarding process to set up your managed network.
- **Set up in NSP**—Proceed to NSP to continue the setup.
- **Skip onboarding**—Skip the onboarding process.

 **Note:** When users select Set up in NSP and postpone the onboarding, the onboarding start page will reappear the next time they log in.

 **Note:** You cannot return to the onboarding wizard if you finish or skip the process. A warning stating this is displayed and must be confirmed before users can exit, skip, or finish the onboarding wizard.

 **Note:** When users complete the configuration in NSP and close the forms or log out, other users can access the onboarding process upon their next login and view the configurations made in NSP.

To proceed with the onboarding, click **Get Started** to begin.

While completing steps in the onboarding wizard, you can use the following buttons to navigate:

- **Previous step**—returns you to the previous step without saving changes.
- **Set up later**—skips the current step without saving changes and moves to the next step. You can return to a step that you skipped using Previous step, by clicking on it in the navigation tree, or during the final onboarding step (Setup Overview).
- **Continue**—saves the changes and moves to the next step.

3.2 How do I import artifacts?

In the first phase of onboarding, you will select and install artifact bundles, which provide translation capabilities that NSP needs to communicate with and manage network nodes.



Note: If you wish to install artifact bundles after the onboarding process, use the procedures in the *NSP Network Automation Guide*.

3.2.1 Prerequisites

You must download the artifacts included with the NSP feature package. You can also obtain the artifacts from the [Network Developer Portal](#) or Nokia support.

The artifact files must be made locally available on the NSP client workstation, which requires physically transferring them (using a thumb drive, for example) in cases where the NSP network is kept separated from the Internet.

3.2.2 Steps

1

Click **+ Import & Install Artifact Bundles**. The Import and Install Local Files window opens.

2

Drag and drop the files into the window, or click **Browse** to select the files. When you have added all the artifact files, click **Import & Install**.

If you just want to Import the artifacts and install them later, click **Import** instead.

3

Once imported, the files are displayed in a list. You can see the installation status of each artifact bundle in the **Status** column.

4

To manage the artifacts manually, you can click to choose to either **Install** or **Delete** an artifact bundle.

5

When you are finished this step, click **Continue** to proceed to the next step.

END OF STEPS

3.3 How do I create unified discovery rules?

In this step you will create a discovery rule, which is a policy object that contains a list of node IP addresses and the required communication protocols for each node. A “unified” discovery rule is the unity of an NSP discovery rule and an NFM-P discovery rule, for cases where Enterprise NSP is being installed on a network that includes NFM-P.

See the *NSP Device Management Guide* for more information about creating the policy types (ping, mediation) described here.

3.3.1 Steps

1

Click **+ Create Unified Discovery Rule**. The **Create Unified Discovery Rule** window opens.

2

Fill in the required information for the **General** part of the configuration form:

- **Rule Name**—the displayed name for the discovery rule that identifies it in lists and when selecting the rule from other forms.
- **Description**—notable information about the discovery rule, if required. For example, the geographic area covered by the discovery rule.
- **Network Scan Interval (min)**—the number of minutes between automatic scans of the IP addresses in the discovery rule.
- **Admin State**—the administrative state of a policy or network object determines whether it is *activated*, where Up is “on”, and Down is “off”.

3

Fill in the required information for the **Protocols and Policies** part of the configuration form. In this step, you are selecting the **First Discovery Protocol**, and up to three other protocols if needed. Node types require a specific communication protocol. Depending on the protocol selections you made, additional panels are displayed in the window.

Your options are the following:

- SNMP
- NETCONF
- gRPC
- CLI

4

Under **Select Mediation Policies**, click the field to select a mediation policy and click **Select**.

A mediation policy specifies various settings for communication over the selected protocol, and must match the protocols you specified in the previous step.

In the window to select a mediation policy, you can click **+ New**, if needed, which opens a new tab to create a policy. a mediation policy.

5

Under **Select Reachability Policies**, click the field to select at least one type of ping policy and click **Select**.

You can choose a policy for the protocol type, or a generic ping policy. A ping policy specifies how NSP connects to a node to determine *reachability*, that is, whether the node is actively responding to a ping request. Whether a node is reachable or not is a key criteria of node health.

In the window to select a ping policy, you can click **+ New**, if needed, which opens a new tab to create a policy.

6

Under **Associate Classic Discovery Rule**, you can select an existing NFM-P discovery rule (referred to as a “classic” discovery rule) to make this a unified discovery rule. The NSP will attempt to discover all nodes that are currently being managed by the NFM-P instance that is using this classic discovery rule.

In the window to select a classic rule, you can click **+ New**, if needed, which opens a new tab to create a new classic discovery rule.

7

Under **Discovery IP Ranges**, click **+ Add** for “Included IP Addresses”. The **Add Included IP Addresses** window opens.

8

Fill in the required information for the following:

- **IP Address**—the IP address for the node in IPv4 or IPv6 format.
- **Mask Bits**—the mask bits of the IP address, with a valid range of 24-32 for IPv4 and 120-128 for IPv6.

If required, enable **Create Another** to queue up another IP address, and click **Add**. The IP address that you entered is displayed in the list of included IP addresses.

9

If you need to exclude IP addresses, under **Discovery IP Ranges**, click **+ Add** for “Excluded IP Addresses”. Fill in the required information in the same manner as the previous step.

10

Click **Create**. The discovery rule is displayed in the list of discovery rules.

11

When you are finished this step, click **Continue** to proceed to the next step.

END OF STEPS

3.4 How do I discover nodes?

In this step you will initiate a scan of the node IP addresses in the selected discovery rules. NSP will then attempt to *manage* the nodes, establishing a durable communication link and adding them to list of nodes and network map. Any nodes that are already managed by an existing classic NFM-P discovery rule will appear in the list as well.

3.4.1 Steps

1


Click the check boxes beside the discovery rules to select one or more discovery rules, and click **Discover**.

The windows changes to display “Discovered Nodes” as NSP starts scanning the node IP addresses listed in the discovery rule and attempting to manage the nodes according to the protocol type specified by the mediation policy.

2

This list will continue to update as the node discovery is in process in the background. Discovered nodes appear in the list and can be viewed according to their Reachability and Management State. Successfully managed nodes will display as “Reachable” and “Managed”, respectively.


3

You can manually scan (or re-scan) a discovery rule by returning to the discovery rule list, clicking , and selecting **Discover** for the required discovery rule. You can also choose to delete the discovery rule.



Note: You cannot delete a discovery rule while it is actively scanning the network.

4

If you need to unmanage and delete a node, you can click  to remove it from the managed network.

5

When you are finished this step, click **Continue** to proceed to the next step.

END OF STEPS

3.5 How do I create a background map layer?

In this step, you will create a background map layer by specifying a tile server and configuring the Map Settings.

3.5.1 Steps

1

Fill in the required information to create a background map layer:

- **Background Map Layer URL**—URL of a map server available under an open license. Use this format:
`https://tile_server/path/file.png`
- **Background Map Layer Attribution**—For crediting an open license provider for legal purposes.

2

When you are finished this step, click **Continue** to proceed to the next step.

END OF STEPS

3.6 How do I set statistics for nodes and links?

In this step you will select which statistic types to enable. NSP collects metrics through statistics counters, which measure various aspects of managed nodes. The statistics that you can enable here are percentage based, for example, CPU usage for each node expressed from 0-100%.

You can hover the cursor over the info icon beside each statistic counter to see a tooltip explaining more about what the counter does.

Enabling a statistic creates a *subscription* for that counter type. Creating a subscription causes NSP to start collecting that counter type from the node at the configured time interval. You can view statistics subscriptions in **Data Collection and Analysis, Management**.

3.6.1 Steps

1

Click the  icon for the statistics counter types that you want to enable.

2

When you are finished this step, click **Continue** to proceed to the next step.

END OF STEPS

3.7 How do I create roles?

In this step, you will create roles which specify access rights to specific NSP functions and network resources. Roles are assigned to user groups, providing access rights defined in the roles, including read, write, and execute permissions.

3.7.1 Steps

1

Click **+ Create Role**. The Create Role window opens.

2

Fill in the required information for the **Identification** part of the window:

- **Role Name**—the name for the role, with no spaces. Required.
- **Description**

3

In the **Characteristics** part of the window, click the **Administrator** check box if you want to grant full access to all resource groups and applications.



Note: Checking this box will disable the Action Permissions and Resource Group Access sections, as the options are predefined. If selected, you can skip the next two steps.

4

Fill in the required permissions for the **Action Permissions** part of the window:

- **Analytics Reports**
- **Data Collection and Analysis Management**
- **Device Management**
- **File Server**
- **Network Intents**
- **NE Inventory**
- **IP/Optical Coordination**
- **Path Control**
- **Model Driven Configurator**

Permissions are configured per module and will include some or all of None, Read, Read and Write, Read and Execute, Read, Write, and Execute.

5

Fill in the required permissions for the **Resource Group Access** part of the window:

- **Access to all Equipment**—Grants full read, write, and execute permissions to all equipment resource groups.
- **Access to all Services**—Grants full read, write, and execute permissions to all services resource groups.
- **Permissions**—Grants specific access permissions to equipment and services.
- **Group Category**—Filters which resource group the applied access permissions affect.



Note: Permissions and Group Category work together when one or neither of the Access to all Equipment and Access to all Services options are selected.

6

Click **Create**. The role is displayed in the list of roles.

END OF STEPS

3.8 How do I create user groups?

In this step, you will create user groups which define the roles and associated access rights. When a role is assigned to a user group, all access rights tied to that role are automatically applied to the user group.

3.8.1 Steps

1

Click **+ User Groups**. The **Create User Group** window opens.

2

Fill in the required information for the **Identification** part of the window:

- **User Group Name**—the name for the user group, with no spaces. Required.
- **Description**

3

In the **Roles** part of the configuration form, click **+ Roles** to add a role to the user group. You can only assign one role to the user group.

4

Click **Create**. The user group is displayed in the list of user groups.

END OF STEPS

3.9 How do I create users?

In this step, you will create user accounts that can manage various functional areas based on their assigned user group, which is configured with specific roles defining their access and permissions to NSP Enterprise main menu options. Each user account should correspond to a real person and not be shared among multiple people.

3.9.1 Steps

1

Click **+ Users**. The **Create User** window opens.

2

Fill in the required information for the **Identification** part of the window (scroll down as needed):

- **Username**—the name for the user account, with no spaces. Required.
- **First Name**
- **Last Name**
- **Description**
- **Account State**—"Active" or "Suspended".
- **User Group**—the user group for the user account. Required.
- **Auth Source**
- **Email Address**—the email address associated with the user account.

3

Fill in the required information for the **Password** part of the window:

- **Force User to Change Password**—enabling this option forces the user to change their password on initial login, which is recommended.
- **Password**
- **Confirm Password**

You can click **Show Password** to view the characters entered for the two password fields, or click **Password requirements** to view the requirements list for user passwords.

4

When you are finished, click **Create** to create the admin user account.

5

When you are finished this step, click **Continue** to proceed to the next step.

END OF STEPS

3.10 How do I complete the Setup Overview step?

This step allows you to view everything that has been completed in the onboarding wizard and make some changes, if required.

There is an **Edit** button available at the top-right corner of most sections that allows you to return to that step and perform additional configuration or node discovery tasks.

Click **Finish** to complete the onboarding process. A confirmation pop-up appears stating you that you will not be able to return to the onboarding wizard.

The onboarding confirmation page appears with links to each module. You can download a PDF summarizing the completed configurations, providing links to each module.

4 Using Enterprise NSP

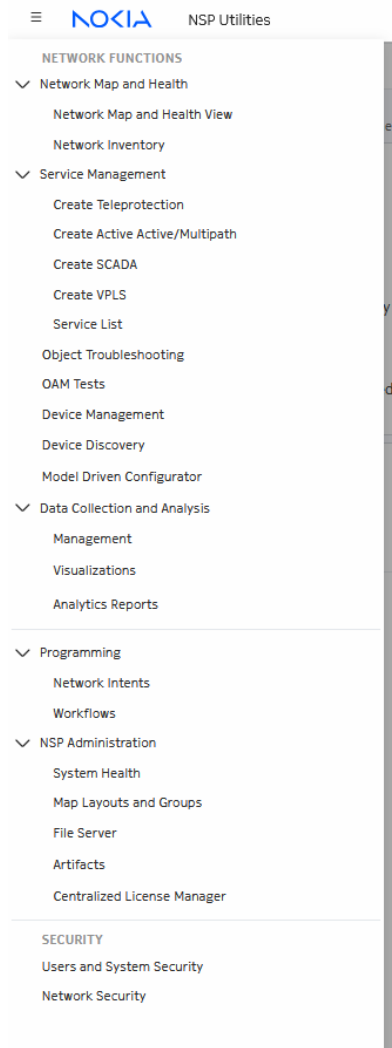
4.1 Enterprise NSP menus

Enterprise NSP features a streamlined menu structure that includes only the most relevant NSP functions for the selected use-case.

Enterprise Utilities features the following options and sub-options:

- **Network Map and Health**—network monitoring and health KPIs, network map, and network inventory. See [Chapter 5, “Network viewing and monitoring”](#).
- **Service Management**—service template configuration and deployment. See [Chapter 6, “Enterprise utilities - service management”](#).
- **Data Collection and Analysis**—network statistics collection and analysis functions. See [Chapter 8, “Data collection and analysis”](#).
- **Device Management**—View managed devices. See [7.1 “Device Management” \(p. 27\)](#).
- **Device Discovery**—node discovery and management controls. See [7.2 “Device discovery” \(p. 28\)](#).
- **Model Driven Configurator**—configure parameters and view state information. See [7.3 “Model driven configurator” \(p. 29\)](#).
- **Programming**—advanced functions for network programming and automation. See the Nokia Network Developer Portal at <https://network.developer.nokia.com/api-documentation> and the *NSP Network Automation Guide*.
- **NSP Administration and Security**—administrator functions for system status/health, map configuration, user configuration, file system management, and artifact management. See [Chapter 9, “NSP administration and security”](#).

Figure 4-1 NSP Utilities menu



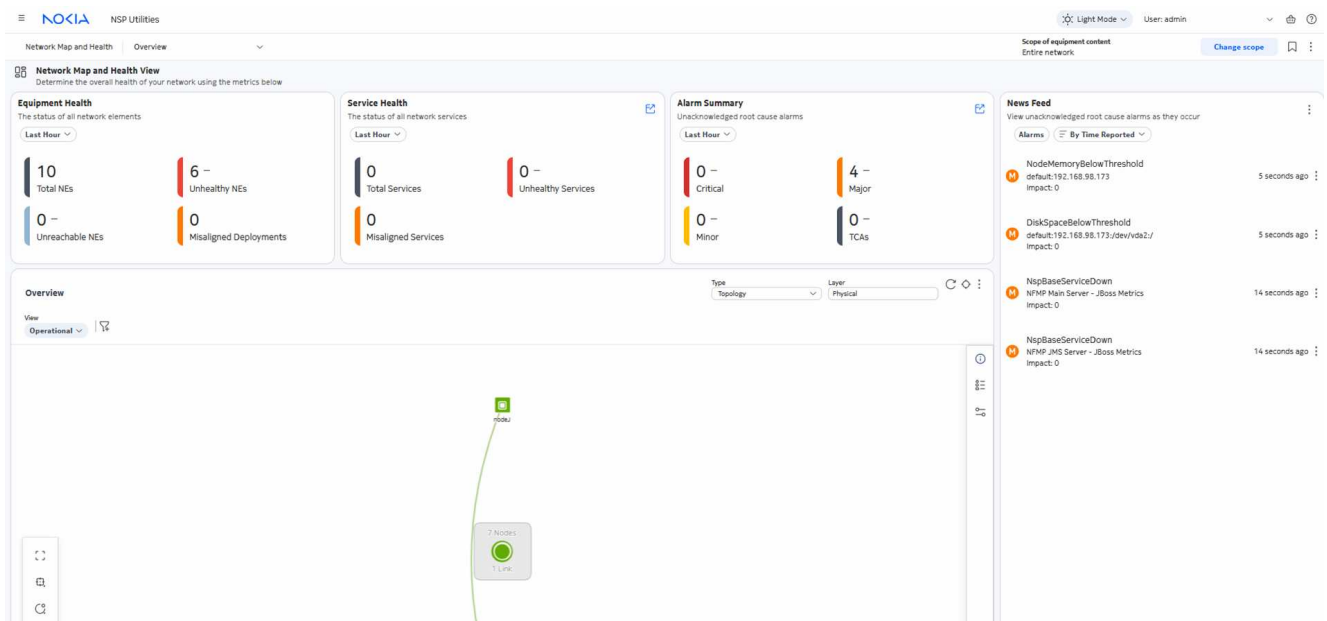
5 Network viewing and monitoring

5.1 Network Map and Health

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 tab.

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

Figure 5-1 Network Map and Health view



5.1.1 Network Map

The Network Map is a graphical display of your network equipment and its interconnections. If the view is configured with a background map layer, equipment can be positioned on the map, based on its actual physical location. Nodes are grouped into geographical regions and zones. The map can be zoomed out to view equipment from a broad perspective, or zoomed in to view only a handful of nodes.

5.2 Network Inventory

The Network Inventory view displays all managed nodes, service sites, ports, services, and tunnel bindings. You can access the Network Inventory view by selecting **Network Map and Health**, **Network Inventory**, or by selecting **Network Inventory** from the **Network Map and Health** drop-down in the navigation menu.

The **Network Elements** view opens by default and displays the following information:

- **Name**—the name of the node.
- **Operational State**—displays the operational status of the node, indicating whether the node is running correctly (enabled), or has encountered an issue (disabled).
- **System Address**—the primary IP address of the node.
- **Management Address**—the IP address that NSP uses to communicate with the node for network management.
- **Product**—the type of node (for example, 7705 SAR).
- **Chassis Type**—the chassis type, which indicates the hardware variant of the node.

Other network inventory information can be found by clicking , and includes the following:

Equipment Inventory

- **Shelves**—physical chassis details of network devices.
- **Fans**—cooling component details and status.
- **Power Supplies**—details and status of device of device power units.
- **Slots**—device slot details with identifiers and status.
- **Cards**—Installed card details with identifiers and status.
- **Modules**—Installed modules providing specific device functions with identifiers and status.
- **Ports**—node ports with identifiers (NE name and ID) and status.
- **LAGs**—group of node ports with identifiers (NE name and ID) and status.
- **Pluggables**—transceiver details (assembly, part numbers, serials, deviations).
- **Port Adaptors**—adaptor details (assembly, part numbers, serials, deviations).

Service Inventory

- **Services**—configured services with type and status.
- **Service Sites**—service objects that exist on nodes and status.
- **Service Endpoints**—service endpoints with site, IP address, port, NE and status.
- **Tunnel Bindings**—service bindings between nodes with source and destination identifiers and status.

Network Topology

- **Links**—links between nodes with type and status.

See the *NSP Classic Management Guide* for more information on network inventory.

6 Enterprise utilities - service management

6.1 Managing network services

NSP manages network services using a library of a predefined set of service models including L3 VPN, EVPN, C-Line, E-LAN, E-TREE, E-Line and IES services. These service models can be installed and utilized by the built-in, intent-based engine (NSP Network Intents views) to provide assurance that service configuration is as planned/requested, and also easy adaptability for custom service model requests. New service models to support custom needs can also be developed with aid of the NSP automation practice team using the NSP programmability suite.

Service management uses the following pathway:

1. Obtain the required network intent .zip archives from Nokia and make them available on your local machine.
2. Import the network intents under **Artifacts, Artifact Bundles**.
3. Import the network intents into Service Management under **Service Management, Services, Intent Type Catalogue**.
4. Create a service template under **Service Management, Service Templates**.
5. Create a service under **Service Management, Services** or select the service from the **Service Management** drop-down in the navigation menu.

See the *NSP Service Management Guide* for more information about managing services.

6.2 Service Management menu

6.2.1 Overview

The Service Management menu includes the following options, each opening a different service creation form:

- Create Teleprotection—Opens service creation for “cpipe”.
- Create Active Active/Multipath—Opens a service creation for “redundant cpipe”.
- Create SCADA—Opens a service creation for “scada”.
- Create VPLS—Opens a service creation for “vpls”.
- Service List—Opens the default service management view.

For details on using NSP Utilities service intents and templates, see [6.2.2 “Service templates and intent types” \(p. 26\)](#).

6.2.2 Service templates and intent types

Service templates must be created before provisioning a service. To create a service template, see “How do I create a service template?” in the *NSP Service Management Guide*.

To utilize the NSP Utilities service intents, users are required to:

- Create a service template using the intent type listed in [Table 6-1, “Supported intent types and view configurations for each service template”](#) (p. 25).
- Ensure the service template name aligns with the corresponding entry in [Table 6-2, “Template names for each service”](#) (p. 26).

Customized view configurations are supported across applicable service intents and are visible in the svc-intents and svc-unified intents views. To align the view configuration with the following intent types and service templates, use the following mappings:

Table 6-1 Supported intent types and view configurations for each service template

Intent type	View config	Service template
cpipe	StandardRelayTemplate	Standard_Relay
cpipe	SCADA	Standard_Scada
Redundant-cline	AMP	Standard_MP_R_Cpipe
vpls	default	Standard_VPLS

To sync the service template to the appropriate service, use the following template names:

Table 6-2 Template names for each service

Service	Template name
Create Teleprotection	Standard_Relay
Create Active Active/Multipath	Standard_MP_R_Cpipe
Create SCADA	Standard_Scada
Create VPLS	Standard_VPLS

7 Device administration

7.1 Device Management

7.1.1 What are devices?

“Device” is another term for node, commonly used in the core NSP documentation set and NSP UI. Devices are also referred to as Network Elements (NEs) in the context of the managed NSP network. There is no functional difference between the terms and they are interchangeable.

7.1.2 Viewing managed devices

Managed devices are displayed under **Device Management, Managed Network Elements**. The table view is similar to the one displayed by Network Inventory, and displays the following unique information:

- **Reachability**—displays the network reachability status of the node (reachable or unreachable).
- **Management State**—for classically managed nodes, the management state is typically “managed” when the node is discovered and communicating with NSP, or “unmanaged” when management has been manually disabled. The management state of MDM nodes is not set.
- **NE Mode**—the management mode of the node, “Classic” or “MDM”.
- **Management IP**—the IP address that NSP uses to communicate with the node for management.
- **NE ID**—the site IP address of the node that acts as a node identifier.
- **Product**—the type of node (for example, 7705 SAR).
- **Chassis**—the chassis type, which indicates the hardware variant of the node (for example, 7705 SAR-18).
- **Software Version**—the currently running software version of the node
- **Resync Status**—the status of the most recent resync attempt.
- **Discovered By**—the discovery rule that triggered the discovery of the node.
- **Domain Controller**—displays if the node is a domain controller, an external network management system that manages nodes of its own.


Figure 7-1 Managed network elements

Device Management

Devices
Managed Network Elements

NE Name	Reachability	Management State	NE Mode	Product	Chassis
nodeB	● Reachable	—	MDM	7210 SAS	7210 SAS-Mxp 22F2C 4SF...
nodeC	● Reachable	—	MDM	7210 SAS	7210 SAS-R12
s168_97_124_Both	● Reachable	—	MDM	7705 SAR	7705 SAR-18
s168_97_149_Both	● Reachable	—	MDM	7705 SAR	7705 SAR-18
s168_97_19_Both	● Reachable	—	MDM	7705 SAR	7705 SAR-18
s168_97_215_Both	● Reachable	—	MDM	7705 SAR	7705 SAR-Hmc
s168_98_218_Both	● Reachable	—	MDM	7705 SAR	7705 SAR-18
s168_98_223_Both	● Reachable	—	MDM	7705 SAR	7705 SAR-Hm
s168_99_180_acpm	● Reachable	—	MDM	7750 SR	7750 SR-12
SAR8-145	● Reachable	—	MDM	7705 SAR	7705 SAR-8
SAR8-145	● Reachable	Managed	Classic	7705 SAR	7705-SAR8

7.1.3 Management actions

You can select  (Table row actions), for a managed node to open the NE inventory or perform management tasks, including:

- resync
- unmanage
- delete

See the *NSP Device Management Guide* for more information about using the Device Management view to perform node management tasks.

7.2 Device discovery

7.2.1 What is device discovery and how does it work?

Device discovery is the process where NSP is provided with the management IP address of a supported node, establishes communication with the node, and adds the node to the network. Once the node has been discovered, it becomes “managed”.

NSP supports two main types of discovery and management:

- Model-driven management (MDM) is how NSP manages Nokia and multivendor nodes. Support is provided by adaptors installed in the NSP that provide mediation between certain NSP functions and Nokia/third-party node database models that defines the object and parameter structure of the node.

- Classic management is provided by the optionally deployable NSP component, NFM-P. Classic nodes are discovered in the NSP and managed by the NFM-P in the background. To ensure alignment between NSP and NFM-P, Nokia recommends that all management operations be performed in the NSP.

i **Note:** If a node is managed through both an MDM NSP discovery rule and a classic discovery rule, a duplicate entry for the node will appear in the managed network.

Discovery rules

Discovery rules define the protocols and IP address ranges used that NSP uses in node discovery. A “unified” discovery rule supports the discovery of both MDM and classic nodes, allowing you to perform both types of discovery with a single configuration form. Discovery of classic nodes is provided by a linking between the unified rule and a previously-defined classic discovery rule. The classic discovery rule contains the mediation and reachability policy information required to discover and manage the classic nodes in the specified IP address ranges.

See [10.1 “Device discovery procedures” \(p. 35\)](#) for procedures on creating the policies required to discover nodes.

7.2.2 Discovering devices in Enterprise NSP

The onboarding wizard (see [Chapter 3, “Enterprise NSP onboarding”](#)) provides an opportunity to set up node discovery and manage nodes when first setting up NSP. You can manage node discovery manually with the following pathway:

1. Create a list of nodes to be managed and record their management IP addresses for use in a discovery rule.
2. Create a unified discovery rule and set the Admin State of the discovery rule to “Up”. See [10.1.1 “Creating a unified discovery rule” \(p. 35\)](#)
3. Verify the management state of nodes. See [7.1.2 “Viewing managed devices” \(p. 27\)](#).

7.3 Model driven configurator

The Model Driven Configurator allows you to configure parameters and view state information defined in the NE adaptation schema. Model Driven Configurator is applicable to nodes managed by MDM for which MDC adaptors have been installed in the MDM server. The built-in nodal models are used; that is, Model Driven Configurator does not perform any model conversion. This enables compatibility with future NE releases without the need to upgrade the NSP. All that is required is installation of the new adaptors.

RESTCONF APIs are also available for MDM managed NEs; see the Device Configuration API documentation on the [Network Developer Portal](#).

8 Data collection and analysis

8.1 Telemetry management using NSP

8.1.1 Definition

NSP Data Collection and Analysis (DCA) functions provide collection, processing, and analysis for MDM and Cloud Native (CN) telemetry. NSP supports configuring telemetry subscriptions and using baseline analytics, NSP indicators, and OAM tests for anomaly detection, metric customization, and network tests.

The type and scope of statistics support is dependent on the source. NSP provides the following statistics support by node type:

- **MDM-based telemetry**—SNMP protocol for multi-vendor nodes
- **Cloud Native telemetry**—gNMI protocol for Nokia and multi-vendor nodes
- **Classically managed NEs**—SNMP protocol for Nokia classically-managed nodes, described in the *NFM-P Statistics Management Guide*.

The DCA functions of NSP are described in detail in the *NSP Data Collection and Analysis Guide*.

8.1.2 Functionality

NSP provides the following DCA functions using collected telemetry data:

- visualization, in the form of telemetry charts
- aggregation, rules to combine stats for consumption by Analytics
- baseline analytics and anomaly detection, defining trends using telemetry data and identifying outliers
- NSP indicators, customized metrics to define and track KPIs
- OAM tests, template-based tests

The DCA telemetry functions described in this document are distinct from:

- Cflowd AA stats and other flow statistics collected via Flow Collectors
- Analytics report catalogs, though stats collected using DCA aggregation functions are available in Analytics. See the *NSP Analytics Report Catalog* for information about report generation and visualizations, and reference lists of the available report catalogs. Baseline analytics and analytics reporting are different functions, each with their own installation options.

NSP telemetry aggregation is configured using DCA functions, though only when an auxiliary database is installed.

8.1.3 Telemetry artifacts

The telemetry types for nodes are defined using YANG files in the NE artifact bundles. NSP uses custom resource (CR) definitions to translate the YANG data, map incoming telemetry to managed

objects in the network, and output data to Postgres, Vertica, and Kafka as required. These resource definition files can be viewed as part of the artifact archive. For information about the CRs that accompany your NE adaptors, see the relevant artifact guide.



Note: You must install the relevant adaptors before managing the associated NE types to use the telemetry definitions. NSP also includes a limited, generic set of default telemetry. Without installing adaptors, you will only see the default telemetry.

8.1.4 Telemetry subscriptions

A subscription defines the parameters of telemetry collection and uses a filter definition to select the NEs/objects. NSP deploys the specified data to the NE and registers the subscription, which is used to transfer telemetry data from the NE to NSP.

9 NSP administration and security

9.1 System health

9.1.1 Description

The NSP System Health dashboard displays a number of system KPI representations. The default view includes a graphical representation of the number of system pods in each state, such as Running or Pending, for quick identification of problems. The view also lists relevant information for each pod, such as the pod uptime, host NSP cluster node, and number of pod restarts.

9.1.2 What are the System Health functions?

Monitoring NSP

From the NSP System Health dashboard, you can monitor NSP to quickly determine the overall operational quality of the system. To view more detailed information about aspects of NSP operation, you can use Grafana and NSP Log Viewer.

Log Viewer Dashboards and Grafana

You can invoke the following logging and monitoring functions from the System Health dashboard:

- **Log Viewer**—local OpenSearch instance with dashboards for viewing and analyzing NSP application log data
- **Grafana**—local Grafana instance that draws on various data sources to provide visualizations and alerts

Log Viewer Dashboards and Grafana are third-party functions that are built-in to the NSP. Each function displays a dashboard that displays system status and logging information. The Log Viewer collects, analyzes, and displays NSP application log information by invoking a local OpenSearch instance called OpenSearch Dashboards.

NSP user credentials are required to view the tools. Additionally, Grafana has Admin, Editor, and Viewer roles that can be assigned through Users and Security.

See the *NSP System Administrator Guide* for more information about system health functions.

9.2 Map layouts and groups

A map layout is a map comprised of assembled map elements, in this case a background image overlaid with graphical NE and path elements. The Map Layout function lets administrators specify a common map layout for use in NSP map views. In the physical map layer, NEs are grouped into geographical regions and zones that are organized against a map background. NSP Enterprise uses the Physical layer for map display.

See the *NSP System Administrator Guide* for more information about configuring map layouts and using the map.

9.3 File server

The NSP File Server is a file import and management utility that facilitates NSP artifact management for NSP functions such as Device Management, Workflows, and Network Intents. Typical uses for the File Server include:

- organizing software images for NE upgrades
- managing input for mass operations such as migrations
- NE backup storage
- managing files used for Zero Touch Provisioning (ZTP)
- debug and troubleshooting file storage

See the *NSP System Administrator Guide* for more information about the NSP file server.

9.4 Artifacts

The artifact view is how you can manage the importing and installation of artifacts and bundles. Typically, an artifact or bundle comes in the form of a zip archive that you have available locally on your machine. Using the **Import & Install** function, you can install them in NSP by browsing your local file system or by dragging and dropping them in the window.

See the *NSP Network Automation Guide* for more information.

9.5 Users and system security

The Users and System Security view of NSP allows administrators to perform the following tasks:

- **Session monitoring**—you can view a list of all active user sessions, send messages to users, and terminate user sessions.
- View **User Activity Logs**—this view displays a list of all user activity, including user names and actions. This list also displays API connections, the type of actions taken over API, and the results.
- Create/modify/delete **Users**—this view allows you to manage user accounts and specify the access level that each user account has.
- Perform **Access Control** functions—these views allow you to create user ground and user roles to further refine permission levels. User Access Control (UAC) is disabled by default in NSP.

See the *NSP System Administrator Guide* for more information about NSP user security.

9.6 Network Security

Network Security allows you to create, edit, delete and update anti-theft policies. These policies enable the NSP to manage a model-driven NE even when anti-theft mode is active. Each policy defines the password the NSP uses to unlock the NE if it becomes locked due to anti-theft protection.

For more information on Network Security, see the *NSP Security Hardening Guide*.

10 Procedures

10.1 Device discovery procedures

10.1.1 Creating a unified discovery rule

1

Open **Device Management, Device Discovery**.

The system opens the **Unified Discovery Rules** view.

2

Click **+Unified Discovery Rule**.

3

In the form that opens, configure the required parameters.


Parameter	Description
<i>General</i>	
Rule name	The name of the discovery rule
Description	User-provided description of the discovery rule
Network Scan Interval (minutes)	Specifies the interval, in minutes, at which the network scan repeats
Admin State	Specifies the administrative state for the discovery rule Up means the policy is in effect.
<i>Discovery Protocols and Policies</i>	
(First Second Third Fourth) discovery protocol	Specify the protocols to be used to communicate with the NE, in the order in which they should be used to attempt to reach the NE for discovery. Enter all the protocols that will be used for communication, regardless of whether they will be used for discovery.
Mediation Policies	Select a policy for each protocol: <ul style="list-style-type: none"> Click on the policy field. In the form that opens, select a policy and click Select. To create a mediation policy, click +New ; see 10.1.4 "Creating a classic mediation policy" (p. 38) and 10.1.3 "Creating an MDM mediation policy" (p. 37) .

Parameter	Description
Reachability Policies	The reachability types required for the selected discovery protocols appear in the Select Reachability Policies panel. Click in a reachability type field. In the form that opens, select a policy and click Select . To create a reachability policy, click +New ; see 10.1.6 "Creating a classic reachability policy" (p. 40) and 10.1.5 "Creating an MDM reachability policy" (p. 39) .
Associate Classic Discovery Rule	Click in the Classic Discovery Rule field. In the form that opens, select a discovery rule and click Select . To create a classic discovery rule, click +New ; see 10.1.2 "Creating a classic discovery rule" (p. 36) .
<i>Discovery IP Ranges</i>	
Included IP Addresses	Click +Add to specify an IP address and mask bits to search. Repeat to add additional ranges. Verify that the included IP address ranges include all the MDM and classic nodes you need to discover.
Excluded IP Addresses	Click +Add to specify an IP address and mask bits to exclude from discovery. Repeat to add additional ranges.



4

Click **Create**. The discovery rule is automatically assigned a rule ID and is added to the list.

5

To run a discovery rule click on your discovery rule in the list and click  (Table row actions), **Discover**.

6

To view results of a discovery, select the discovery rule and click **Summary**  to view the Summary panel. In the panel at the right of the screen, click **Errors**  to see details about any errors that occurred the most recent time the discovery rule was run.

END OF STEPS

10.1.2 Creating a classic discovery rule

1

Open **Device Discovery, Classic Discovery Rules**.

The system displays the list of configured discovery rules.

2

Click **+Classic Discovery Rule**.

3

In the form that opens, configure the required parameters.

Parameter	Description
Rule ID	Enter a rule ID or check the Auto assign classic rule ID check box.
Description	User-provided description of the discovery rule
Admin State	Specifies the administrative state for the discovery rule
Management Protocol	Choose IPv4 or IPv6
Classic Mediation Policies	Select a policy for each access type as needed: <ul style="list-style-type: none"> Click on the mediation policy field. In the form that opens, select a policy and click Select. To create a mediation policy, click +New ; see 10.1.4 "Creating a classic mediation policy" (p. 38) .
Classic Reachability Policies	Select a policy for each reachability type as needed: <ul style="list-style-type: none"> Click in a reachability type field. In the form that opens, select a policy and click Select. To create a reachability policy, click +New ; see 10.1.5 "Creating an MDM reachability policy" (p. 39) .

4

Click **Create**. The classic discovery rule is added to the list.

5

To associate the classic discovery rule with a unified discovery rule and discover nodes, see [10.1.1 "Creating a unified discovery rule" \(p. 35\)](#).

END OF STEPS

10.1.3 Creating an MDM mediation policy

1

Open **Device Discovery, Reachability Policies**.

The system displays the list of configured reachability policies.

2

Click **+Reachability Policy**.

3

In the form that opens, leave the **Classic Reachability** check box unchecked.

4

Configure the required parameters.

Parameter	Description
Policy Name	The name of the reachability policy
Description	User-provided description of the policy
Reachability Type	Specifies the communication type to be used to confirm reachability, for example, ping. The parameters vary based on the reachability type.
Timeout (seconds)	Specifies the length of time, in seconds, to wait for a response after attempting to reach the NE
Interval (minutes)	Specifies the length of time, in minutes, to wait before repeating an attempt to reach the NE
Admin State	Specifies the administrative state for the new policy Up means the policy is in effect.

5

Click **Create**. The reachability policy is auto-assigned a policy ID and added to the list.

END OF STEPS

10.1.4 Creating a classic mediation policy

1

Open **Device Discovery, Mediation Policies**.

The system displays the list of configured mediation policies.

2

Click **+Mediation Policy**.

3

In the form that opens, click the **Classic Mediation** check box.

The form displays panel headers that include the word Classic, for example, Classic SNMP.

4

Configure the required parameters. Parameters vary based on the mediation type.

Parameter	Description
Policy Name	User-provided name for the policy

Parameter	Description
Classic Policy ID	Enter a policy ID or click the Auto assign classic policy ID check box.
Classic SNMP	Select the security model and configure the parameters.
Classic CLI	Select the communication protocol and configure the parameters.
Classic FTP	Select the file transfer type and configure the parameters.

5

Click **Create**. The mediation policy is added to the list.

END OF STEPS

10.1.5 Creating an MDM reachability policy

1

Open **Device Discovery, Reachability Policies**.

The system displays the list of configured reachability policies.

2

Click **+Reachability Policy**.

3

In the form that opens, leave the **Classic Reachability** check box unchecked.

4

Configure the required parameters.

Parameter	Description
Policy Name	The name of the reachability policy
Description	User-provided description of the policy
Reachability Type	Specifies the communication type to be used to confirm reachability, for example, ping. The parameters vary based on the reachability type.
Timeout (seconds)	Specifies the length of time, in seconds, to wait for a response after attempting to reach the NE
Interval (minutes)	Specifies the length of time, in minutes, to wait before repeating an attempt to reach the NE
Admin State	Specifies the administrative state for the new policy Up means the policy is in effect.

5

Click **Create**. The reachability policy is auto-assigned a policy ID and added to the list.

END OF STEPS

10.1.6 Creating a classic reachability policy

1

Open **Device Discovery, Reachability Policies**.

The system displays the list of configured reachability policies.

2

Click **+Reachability Policy**.

3

In the form that opens, click the **Classic Reachability** check box.

4

Configure the required parameters.

Parameter	Description
Policy Name	The name of the Reachability policy
Classic Policy ID	Enter a policy ID or click the Auto assign policy ID check box.
Timeout (seconds)	Specifies the length of time, in seconds, to wait for a response after attempting to reach the NE
Schedule enabled	Schedule enabled means the policy is in effect.
Interval	Specifies the length of time, in minutes and seconds, to wait before repeating an attempt to reach the NE

5

Click **Create**. The reachability policy is added to the list.

END OF STEPS
