NSP
Network Services Platform
Release 24.8

Enterprise Guide

3HE-20418-AAAA-TQZZA
Issue 1
August 2024

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.

Contents

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 network layers, nodes, links, 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 cluster, and the NSP **cluster VMs**, which host the main NSP functions and load balance as needed. Within the 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 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: "deployment_type"
```

where *deployment_type* is the required use-case type

In the current NSP release, the following values are supported for deployment type:

- *standard*—the standard non-Enterprise deployment type for NSP, and is the default value.
- *enterprise-utilities*—the utilities-focused Enterprise NSP deployment type.

User access and permissions in the Enterprise UI

Admin users have full access and read/write/execute permissions for all options in the Enterprise 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*.

2.1.3 Installing artifacts and adaptors

Artifacts and adaptors are resource files that define network device characteristics and allow for management support in NSP by providing the mapping between device attributes and NSP

attributes. Intent types, which define service characteristics, are also considered artifacts and can be installed using the artifact manager. These files typically come in the form of zip archives that are imported using NSP.

Installing the NSP Enterprise artifacts is described in the *NSP Nokia Enterprise Artifact Guide*.

General artifact and adaptor management is described in the *NSP Network Automation Guide*.

3 Network discovery and management workflow

3.1 Enterprise NSP workflow

Perform the following tasks to install Enterprise NSP and manage the network.

1. Enable the Enterprise UI for the required use-case. See 2.1.2 “Enabling the Enterprise NSP UI” (p. 9).
2. Install Enterprise NSP. Follow the standard system deployment procedure in *NSP Installation and Upgrade Guide*.
3. Obtain and install the required adaptors and intent types. See 2.1.3 “Installing artifacts and adaptors” (p. 9).
4. Create users. See 8.4 “User and security” (p. 24).
5. Discover and manage devices. See 7.1.2 “Discovering devices in Enterprise NSP” (p. 19).
6. Manage services. See 5.1 “Managing network services” (p. 15).

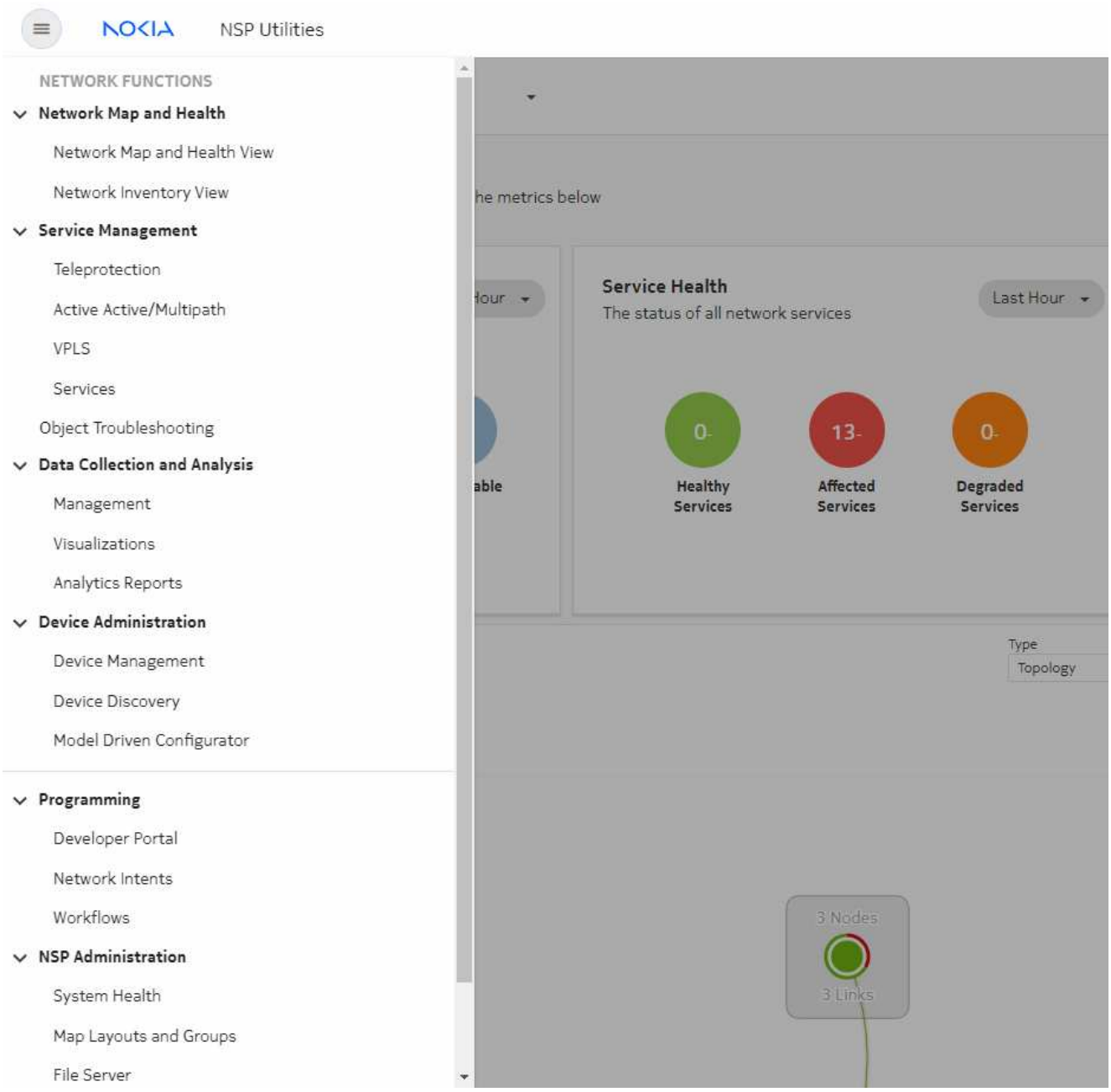
3.2 Enterprise NSP menus

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 4.1 “Network Map and Health” (p. 13).
- **Service Management**—service template configuration and deployment. See 5.1 “Managing network services” (p. 15).
- **Data Collection and Analysis**—network statistics collection and analysis functions. See Chapter 6, “Data collection and analysis”.
- **Device Administration**—device discovery and management controls. See Chapter 7, “Device administration”.
- **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**—administrator functions for system status/health, map configuration, user configuration, file system management, and artifact management. See Chapter 8, “NSP administration”.

Figure 3-1 NSP Utilities menu



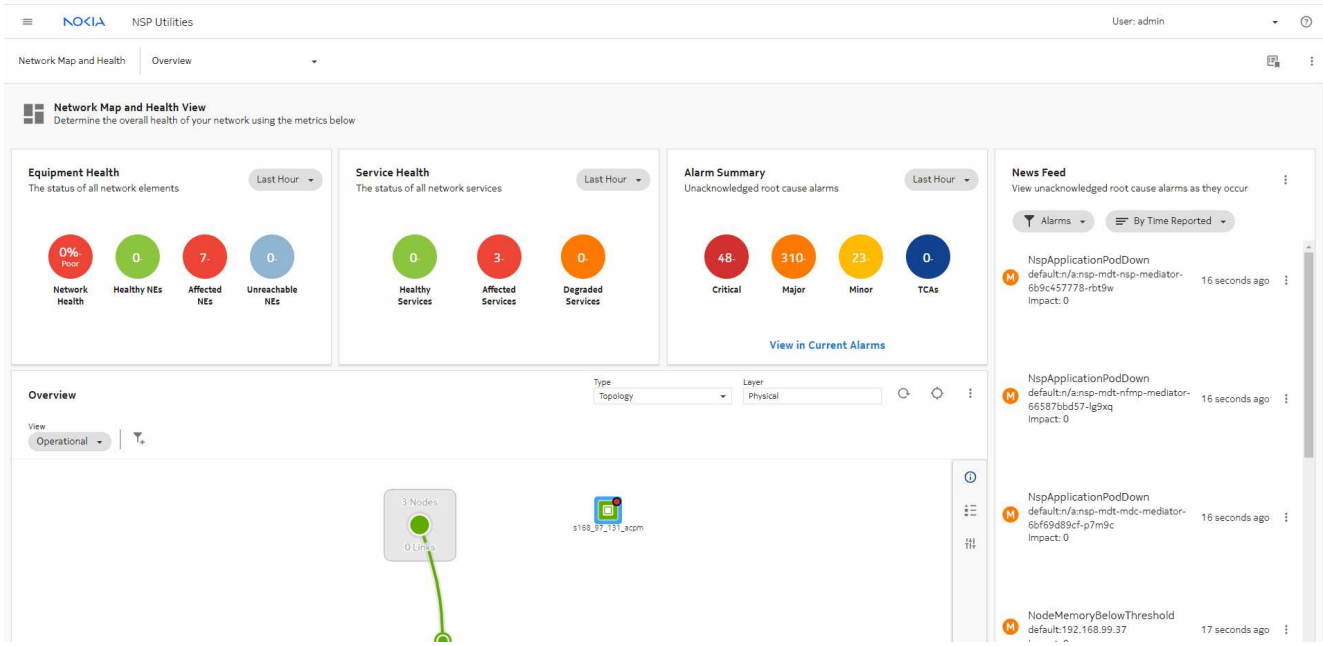
4 Network viewing and monitoring

4.1 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 4-1 Network Map and Health view



4.1.1 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. NEs 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 devices.

4.2 Network inventory

The Network Inventory provides easy-to-read dashlets that display all managed devices, service sites, ports, services, and tunnel bindings. You can access Network Inventory using **Network Map and Health**, **Network Inventory View**, or scroll to the bottom of the Network Map and Health view.

The **Network Elements** dashlet displays the following information:

- **Name**—the name of the device.
- **Operational State**—displays the operational status of the device, indicating whether the device is running correctly (enabled), or has encountered an issue (disabled).
- **# Affected Objects**—the number of service objects that have one or more components that are operationally down.
- **System Address**—the primary IP address of the device.
- **Management Address**—the IP address that NSP uses to communicate with the device for management.
- **Product**—the type of device (for example, 7705 SAR).
- **Chassis Type**—the chassis type, which indicates the hardware variant of the device.

The other available dashlets include the following:

- **Links**—links between devices with type and status.
- **Ports**—device ports with identifiers (NE name and ID) and status.
- **Services**—configured services with type and status.
- **Service Sites**—service objects that exist on devices and status.
- **Service Endpoints**—service endpoints with site, IP address, port, NE and status.
- **Tunnel Bindings**—service bindings between devices with source and destination identifiers and status.

Each dashlet can be expanded to full screen width to view all the available columns.

5 Enterprise utilities - service management

5.1 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 workflow:

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**.

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

5.2 Service management menu

The Service Management includes the following options, each opening a different service type template:

- **Teleprotection**—opens service template creation for “cpipe”.
- **Active Active/Multipath**—opens service template creation for “redundant cpipe”.
- **VPLS**—opens service template creation for “vpls”.

The **Services** menu options opens the default service management view.

6 Data collection and analysis

6.1 Telemetry management using NSP

6.1.1 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 NE source. NSP provides the following statistics support by NE type:

- **MDM-based telemetry**—SNMP protocol for multi-vendor NEs
- **Cloud Native telemetry**—gNMI protocol for Nokia and multi-vendor NEs
- **Classically managed NEs**—SNMP protocol for Nokia classically managed NEs, 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*.

6.1.2 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.

6.1.3 Telemetry artifacts

The telemetry types for NEs 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.

6.1.4 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 Kafka subscription, which is used to transfer telemetry data from the NE to NSP.

7 Device administration

7.1 Device discovery

7.1.1 What is device management and how does it work

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

NSP supports two main types of device discovery and management:

- Model-driven management (MDM) is how NSP manages Nokia and multivendor devices. Device 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 device.
- Classic management is provided by the optionally deployable NSP component, NFM-P. Classic devices 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.

Discovery rules

Discovery rules define the protocols and IP address ranges used that NSP uses in device discovery. A “unified” discovery rule supports the discovery of both MDM and classic devices, allowing you to perform both types of discovery with a single configuration form. Discovery of classic devices 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 devices in the specified IP address ranges.

See 9.1 “Device discovery procedures” (p. 25) for procedures on creating the policies required to discover devices.

7.1.2 Discovering devices in Enterprise NSP

Discovering devices uses the following workflow:

1. Create a list of devices 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 9.1.1 “Creating a unified discovery rule” (p. 25)
3. Verify the management state of devices. See 7.2.1 “Viewing managed devices” (p. 20).

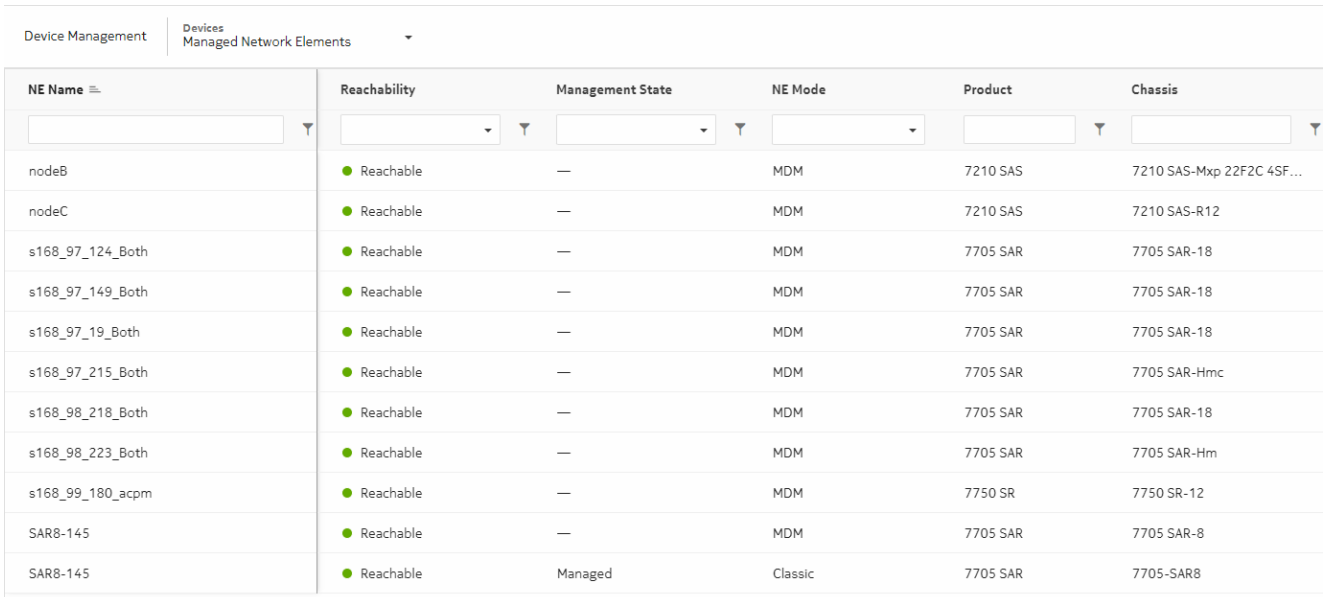
7.2 Managed Network Elements

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

Figure 7-1 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

7.2.2 Management actions

You can select ⋮ (Table row actions), for a managed device 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 device management tasks.

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 devices managed by MDM for which MDC adaptors have been installed in the MDM server. The built-in device 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 NSP administration

8.1 System health

8.1.1 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.

8.1.2 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.

8.2 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.

8.3 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.

8.4 User and security

The Users and 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.

8.5 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 Procedures

9.1 Device discovery procedures

9.1.1 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
General	
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.
Discovery Protocols and Policies	
(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: • Click on the policy field. • In the form that opens, select a policy and click **SELECT**. To create a mediation policy, click + **NEW**; see 9.1.4 “Creating a classic mediation policy” (p. 28) and 9.1.3 “Creating an MDM mediation policy” (p. 27).

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 9.1.6 “Creating a classic reachability policy” (p. 30) and 9.1.5 “Creating an MDM reachability policy” (p. 29).
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 9.1.2 “Creating a classic discovery rule” (p. 26).
Discovery IP Ranges	
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 devices 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

9.1.2 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: • 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 9.1.4 “Creating a classic mediation policy” (p. 28).
Classic Reachability Policies	Select a policy for each reachability type as needed: 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 9.1.5 “Creating an MDM reachability policy” (p. 29).

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 devices, see 9.1.1 “Creating a unified discovery rule” (p. 25).

END OF STEPS

9.1.3 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

9.1.4 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

9.1.5 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

9.1.6 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