NSP
Network Services Platform
Release 25.4

Device Management Guide

3HE-21452-AAAA-TQZZA
Issue 2
July 2025

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 *Device Management Guide* provides information about device management using NSP to operators and administrators by describing usage and features. For information about device management using NFM-P, see the *NSP NFM-P Classic Management User Guide*.

Scope

The guide covers the full set of features for device management using NSP. Device management using NFM-P (classic management) is documented by the *NSP NFM-P Classic Management User Guide*.

Some feature sets require the purchase and configuration of additional feature packages. See the *NSP System Architecture Guide* for more information about feature packages and installation options.

Device Management functions are available for OSS using programmable APIs. For general information about developer support, see the API documentation page on the Network Developer Portal.

For specific documentation about REST APIs for device management, including management of NEs behind a controller, click on API Reference in the Device Administrator row.

Safety information

For your safety, this document contains safety statements. Safety statements are given at points where risks of damage to personnel, equipment, and operation may exist. Failure to follow the directions in a safety statement may result in serious consequences.

Document support

Customer documentation and product support URLs:

- Documentation Center
- Technical support

How to comment

Please send your feedback to documentation.feedback@nokia.com.

Part I: Device management essentials

Overview

Purpose

Provides information about managing NEs using NSP.

Contents

1 Device support in NSP

1.1 How does NSP support devices?

1.1.1 Device support overview

NSP supports two types of device management: classic and model-driven.

Classic management

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.

For information about NFM-P devices, classic discovery, management, all other information about using NFM-P, see the *NSP NFM-P Classic Management User Guide*.

Model-driven management (MDM)

The NSP supports model-driven management of Nokia and multivendor devices. Device support is provided by adaptors installed in the NSP.

MDM provides mediation between certain NSP functions and Nokia or third-party NEs.

1.1.2 Support artifacts

Downloadable artifacts are available to support NSP functions for both classic and MD managed NEs.

Adaptor artifacts support model-driven mediation. Other types of artifacts, such as intent types and telemetry files, support classic, MD, or both, depending on the artifact.

Device artifact bundles and documentation are available from the Nokia NSP software download site. For Nokia devices, select the NSP release, then the NE family, for example, SR_OS, to see the list of available artifact bundles and documentation.

Artifact guides are provided for each NE family and NSP release. For example, the Nokia SR OS Artifact Guide for Release 23.11 lists and describes the artifacts delivered to support management of Nokia SR OS devices by NSP Release 23.11, including artifacts for model-driven management and ones that support other NSP functions.

See the following for more information:

- The *NSP Device Configuration Intent Type Catalog* describes available intent type bundles
- The *NSP Network Automation Guide* describes artifact installation

1.2 What devices are supported by NSP?

1.2.1 Supported device types

Device support varies by management type.

Classic management

See the device support chapter in the *NSP NFM-P Classic Management User Guide* for information about supported NE families.

By default, for most core-network device types, the NFM-P supports the current software release and a limited number of immediately preceding major releases. For detailed information about NFM-P device compatibility, see the *NSP NFM-P Network Element Compatibility Guide*.

Model-driven management

Production adaptor artifacts are available in the support of the following device types:

- Nokia SR Linux OS-based routers
- Nokia SR OS-based routers
- Nokia MAG-c solution
- Nokia T-API model-based Optical Domain Controllers
- Ciena T-API model-based Optical Domain Controllers
- Nokia Enterprise devices

Documentation delivered with these artifacts identifies the release compatibility.

For SR Linux OS, SR OS, and MAG-c devices, the production adaptor artifacts enable management between NSP and the NEs within a target N-3 and N+2 compatibility range. The following table provides a simplified view of the compatibility targets when “N” is Release 24.x for NSP and the 7750 SR, as an example:

Table 1-1 Sample compatibility range for 7750 SR

NE compatibility release targets	NE release examples	NSP release example
N-4 or more	Not supported	NSP Release “N” = 24.x
N-3	21.x	
N-2	22.x	
N-1	23.x	
Nokia SR release “N”	24.x	
N+1	25.x	
N+2	26.x	
N+3 or more	Not supported	

In this example, to know the specific certified NE releases supported by the latest available SR adaptor artifacts, you would consult the latest NSP 24.x SR OS Artifact Guide, “Compatible and certified software releases” table.

Nokia-provided adaptors for various NEs, including all Nokia device types listed above, are available for download from the Nokia support software download site.

Note: If the Management Operational Mode on the device is set to mixed, the device is discovered and managed as a model driven NE.

Extended Services Appliance

An Extended Services Appliance (ESA) is a server that attaches to a host 7750 SR NE over standard system interface ports, and which has one to four Virtual Machine (VM) instances to perform multiservice processing. An ESA connected to a model-driven 7750 SR NE appears in the NE Inventory view for the NE. NSP communicates with the host NE, not directly with the ESA. For more information about ESA hardware and configuration, see the NE documentation.

1.3 What is the NE ID?

1.3.1 NE IDs

The NE ID is a unique identifier used by NSP, in both model-driven and classic management, to identify a managed network element. The NE ID can be an IP address, a hostname, or some other identifying string depending on the NSP device adaptation. The required configuration must be present on the NE prior to its discovery.

For the SR OS family of NEs, including SR, ESS, XRS, SAR, SAS, and IXR, this unique NE ID set to the NE’s system interface loopback address. System interfaces can be single stack (IPv4 or IPv6) or dual stack (IPv4 and IPv6). Which address is designated as the NE ID is defined in “Classic management NE IDs” (p. 13) and “MDM SR OS NE IDs” (p. 13).

Classic management NE IDs

Single stack classic SR OS have their NE IDs set to the system interface IPv4 or the IPv6 address depending on which is present. NEs with single-stack IPv4 system interfaces retain their current NE ID when the IPv6 address is added to the system interface.

Classic SR OS with dual stack system interfaces select the IPv4 address as the NE ID.

MDM SR OS NE IDs

Single-stack MD SR OS have their NE IDs set to the system interface IPv4 or the IPv6 address depending on which is present.

MD SR OS with dual-stack system interfaces will select the IPv6 address as the NE ID.

1.4 What is an adaptor?

1.4.1 Adaptor artifacts

Adaptors provide mapping between devices and the NSP. All MDM functions in NSP require adaptor files to be installed by an NSP administrator. In general, anything you want to do with an MDM -managed device, including discovery, requires an adaptor.

Note: Some NSP functions, such as telemetry, require other artifacts, such as mapping files, to be installed in addition to adaptors.

Note: The fault management alarms are provided by two mechanisms: an MDM alarm adaptor and NSP alarm rules mapping artifact. To obtain full alarm support, both the alarm adaptor (which is included in the adaptor suite) and the NSP alarm rules mapping artifact must be installed. The alarm rules artifact is delivered on the software download site with a name that starts with *nsp-mdm-act-alarm-rules* and must be installed using the procedure “How do I install an artifact bundle?” in the *NSP Network Automation Guide*.

Commercially available adaptors are released in adaptor suites (zip files) and updated on a regular basis, outside the NSP release cycle. The latest adaptor suite is always recommended; however, customers may choose to stay on a set of adaptors and skip available updates, depending on their operational requirements. Adaptors and adaptor documentation are available from **Electronic Delivery**, **Downloads** on the Nokia NSP software download site.

You can engage Nokia to build adaptors for specific NEs and feature sets. Development versions of these customer-specific adaptors are shared with the customer through the Network Developer Portal.. Once they have passed user-acceptance testing, final versions are delivered on the software download site of the Support Portal in a customer-restricted folder hierarchy: Network Services Platform/Adaptors/Customer-specific/<customername>.

Navigate through the hierarchy:

- For Nokia device adaptors, select the NSP release, then the NE family, for example, SR_OS, to see the list of available adaptor suites and documentation.
- For custom multi-vendor adaptors, access your adaptor folder

Nokia recommends that you install all adaptor files in any given suite.

1.4.2 SDK

You can use an SDK to build your own adaptors or customize reference adaptors for your requirements; see the *NSP Network Automation Guide*.

1.5 Where can I find more information about adaptors?

1.5.1 Artifact guides for NE types

Device artifact bundles and documentation are available from the Nokia NSP software download site.

Artifact guides are provided with the adaptors for each NE family and NSP release. For example, the Nokia SR OS Artifact Guide for Release 23.11 lists and describes the adaptor suites delivered

to support management of Nokia SR OS devices by NSP Release 23.11 over model-driven interfaces. The artifact guides also contain information about the NSP functionality supported by the adaptors, NE compatibility with those NSP functions, NE commissioning information and a view of active issues.

1.5.2 Adaptors in the NSP documentation

See the *NSP System Architecture Guide* for general information about MDM.

For information about installing and managing adaptors, mapping files, and NE model definition files, see the MDM administration section in the *NSP System Administrator Guide*.

To see which adaptors are installed on your NSP, see “How do I install adaptor artifacts that are not supported in the Artifacts view?” in the *NSP System Administrator Guide* for script instructions.

1.6 How does NSP support device telemetry?

1.6.1 Telemetry support

SNMP telemetry for model driven devices is provided by MDM.

NSP supports CN telemetry (cloud native telemetry) for gNMI telemetry and accounting file collection, for model-driven and classic devices. To enable CN telemetry for gNMI, a gRPC mediation policy must be present on the discovery rule associated with the device.

For accounting collection, a file transfer mediation policy must be included in the discovery rule used to discover the NE. Classic discovery rules include file transfer policies for classic NEs. For model-driven NEs, a file transfer policy for MDM must be included in the unified discovery rule.

For more information about telemetry, see the *NSP Data Collection and Analysis Guide*.

1.7 Pathway: configure and manage devices

1.7.1 Device configuration overview

The following is a generic flow of the high-level tasks that are typically used to configure and manage supported devices using the NSP. As appropriate, review the pathway associated with each task for detailed instructions.

This process is common to all MDM devices but not all tasks apply to all device types.

See the *NSP NFM-P Classic Management User Guide* for the high-level process for classic management.

1.7.2 Stages

Prerequisite tasks

1

Plan your deployment for managing devices by determining the following:

- the number of NEs you need to manage, the redundancy requirements and the hardware required for the system
- the management network latency and management network bandwidth requirements
- the naming conventions for objects that you create

See the *NSP Planning Guide* for the full list of deployment considerations.

2

Integrate the NSP with other EMS, as required.

3

Review the adaptor artifact guides for release-specific information about the compatibility of NSP functions with the adaptors.

4

Install the physical device as per the appropriate device-specific hardware user documentation.

5

Install the required NE adaptors on the NSP; see “How do I install adaptor artifacts that are not supported in the Artifacts view?” in the *NSP System Administrator Guide*.

6

Download and install any additional required artifacts, such as intent types, alarm rules, and mapping files. See “How do I install an artifact bundle?” in the *NSP Network Automation Guide*.

7

If you will be managing classic devices, verify that the NFM-P is running and fully operational.

Review GUI basics for managing devices

8

Familiarize yourself with GUI operations for configuring and managing devices such as navigating the GUI, performing searches, and customizing the GUI user preferences; see “NSP UI overview” in the *NSP User Guide*.

9

Launch the on-product user documentation to access the customer documentation and search tools.

10

Familiarize yourself with available OSS functions using programmable APIs; see the API documentation page on the Network Developer Portal.

Perform account and security tasks

11

Set up all required user accounts and user groups with the required scope of command roles, span of control permissions, and the ongoing monitoring and management of those accounts. See “NSP user security” in the *NSP System Administrator Guide* for more information.

12

For greater security, enable two-way client authentication using mTLS between the NSP and the managed NEs; perform “How do I enable mTLS on the NSP mediation interface?” in the *NSP System Administrator Guide*.

Note: For information about generating the required TLS root CA and client certificates, see the device documentation.

13

Verify that a gRPC certificate has been implemented in the NSP; see “How do I enable TLS for telemetry and gNMI on_change support?” in the *NSP System Administrator Guide*.

Prepare network devices for NSP management

14

Configure the following on the device:

- device identification—NE name used for NSP filtering, configuration and monitoring
- management interface protocol configuration—authentication and communication parameters for device management interface

See the device and adaptor artifact guides for information.

15

Discover the device and verify the device management; see 2.14 “How do I discover devices?” (p. 35).

Configure and manage the discovered device

16

Update parameters on a model-driven NE configuration or state schema tree; see 8.3 “How do I configure device objects?” (p. 101).

17

Deploy NE configuration templates to one or more devices; see 9.23 “How do I create a deployment?” (p. 139).

Create services over devices

18

Configure services as required using service templates; see the *NSP Service Management Guide*.

Monitor, maintain, and troubleshoot devices

19

Configure alarm settings, and monitor incoming alarms to check the type and characteristics of the alarms, and to resolve the network problems or physical equipment failures identified by the alarms; see the *NSP Network and Service Assurance Guide*.

20

Configure OAM testing to troubleshoot network problems and for SLA verification; see “OAM tests” in the *NSP Data Collection and Analysis Guide* .

21

Familiarize yourself with the Network Map and Health dashboard; see “Monitoring network health” in the *NSP Network and Service Assurance Guide* .

22

Collect statistics to monitor network and service performance, compile equipment usage and billing data, and ensure SLA compliance; see the *NSP Data Collection and Analysis Guide*.

Configure charts and Analytics reports as needed; see the *NSP Data Collection and Analysis Guide* and the *Analytics Report Catalog*.

23

Perform device maintenance functions, as required, for example:

- configuration backups and restores; see 3.1 “How do I back up an NE?” (p. 45) and 3.5 “How do I restore an NE from a backup?” (p. 48)
- software upgrades; see Chapter 5, “NE software upgrades using NSP”

24

Identify and resolve performance issues in the network or on a system as required. See “Troubleshooting network objects” in the *NSP Network and Service Assurance Guide* for a starting point.

1.8 How do I view adaptor information for an NE?

1.8.1 Adaptors list

The adaptors list for a managed NE provides information about the installed adaptors relevant to the selected NE.

Adaptors are sorted by purpose: the Used For column in the adaptors view shows the NSP function the adaptor is designed to support. You can filter the list by use, adaptor name, or adaptor version as needed.

Select an NE from the list in **Device Management**, **Managed Network Elements** and click ⋮ (Table row actions), **View applicable adaptors**.

The Applicable Adaptors list is displayed.

1.8.2 Adaptor compatibility notes

- Adaptors from a previous NSP release can be used, but they do not provide access to any features added to the NSP in subsequent NSP releases.
- The same adaptor may work for more than one NE type or version. This means that you may see the same adaptor file name in NSP for two NEs that have different software releases or chassis types.
- The adaptor filename may refer to an earlier NE version than your NE is running. This means that the adaptor was created for the earlier version and is still applicable.

1.9 What is NE resynchronization?

1.9.1 NE resynchronization

The Manage, Resync option in the Table row actions menu performs a reachability check and verifies the information displayed in the Summary panel, including the software version, upgrade status, and backup status.

For NEs managed by a domain controller, NSP displays the reachability state of the NEs from the point of view of the controller. If the controller itself is not reachable, the NEs are not reachable.

Note: The NSP resync operation for classic devices reads all data from the device, not only recently changed data. Therefore the resync operation in NSP may take longer than a force resync in NFM-P.

For MD devices, the data to be read from the device on resync is defined in the device model.

The Summary panel displays the resync status, last resync time, and resync duration.

The Resync status value is one of the following:

- Done—a resynchronization has successfully completed
- Failed—a resynchronization attempt has failed

  If the NE is unreachable, the value in the Reachability column is updated to Unreachable and the icon color changes to red.
- In Progress—a resynchronization is in progress
- Not Attempted—no resynchronization has been requested
- Requested—the resynchronization request is queued for processing.

If an operator has not performed a manual resync, the Last Manual Resync time will display the time the initial synchronization was completed after discovery.

1.10 What is device reachability?

1.10.1 Reachability

The reachability status of a managed device indicates the results of the last reachability check.

A reachability check is a scheduled check that the NSP initiates via the configured protocols. The reachability status parameter in the NSP reflects the results of the reachability check:

- If the NE responds via all configured protocols, it is reachable from the NSP system.
- If more than one protocol is configured and some checks fail and others pass, the NE is partially reachable.
- If all checks fail, the NE is unreachable.

  If the NE becomes unreachable or partially unreachable, an alarm is raised.

For classic NEs, reachability is determined by the ping result of the active management IP address. This can be the in-band or out-of-band IP address: if the active management IP address is the in-band IP address, the in-band reachability policy will be used to perform reachability checks, and vice versa.

1.11 What is a device management state?

1.11.1 Management state

Management state is applicable to classic devices only. The Management State parameter appears as a dash (—) for MDM devices, to indicate that it is not applicable.

The management state parameter describes whether a discovered classic device is included in the managed network.

Available actions in the Manage menu depend on the NE mode, management state, and resync status.

1.11.2 Deleting devices

Using the NSP to delete a device completely removes the device from the managed network. All current and historical management data is removed, for example, physical links, statistics, and backup files. If the device is discovered again, the data is not restored.

For model-driven NEs, the NE IP address remains in the discovery rule after the NE is deleted. The next time the discovery rule scans the network, it discovers and manages the device again, or you can run the discovery rule manually.

Classic NE IP addresses are removed from the classic discovery rule after the device is deleted from the NSP. These devices will not be rediscovered automatically.

Managing backups

If you are using NFM-P to back up your classic devices, you can configure retention of backups after NE deletion; see “How do I configure backup-file retention for deleted NEs?” in the *NSP System Administrator Guide*.

If you are using backup operations within NSP to create backups, backup files remain in the File Server after the NE is deleted. The NE must be re-discovered and managed before a backup can be restored.

1.11.3 Unmanaging devices (classic only)

You can unmanage a classic device from the NSP. Unmanage is not supported for model-driven NEs.

When a user selects Unmanage in the NSP UI, the NE is unmanaged in NFM-P. All current and historical management data is removed, for example, physical links, statistics, and backup files. If the device is managed again, the data is not restored.

If the IP address of the NE is not removed from the associated discovery rule, this NE will be re-managed in the next scanning interval.

To unmanage or re-manage a classic device, select the device in the **Device Management**, **Managed Network Elements** view. Click ⋮ (Table row actions), **Manage**, **Unmanage** or **Manage**.

Note: If you need to unmanage and re-manage an NE with telemetry subscriptions configured, a delay of up to 15 min may occur before all telemetry subscription are reinstated.

Managing backups

When a device is unmanaged, the NFM-P deletes the backup files. Retention cannot be configured.

If you are using backup operations within NSP to create backups, backup operations are still available in the **Device Management**, **Operations** views and backup files remain in the File Server after the NE is unmanaged. The NE must be re-discovered and managed before a backup can be restored.

1.11.4 Changing management states

Available actions in the Manage menu depend on the NE mode and management state. If a management operation is in progress, actions may not be available.

The following table shows available options.

NE Mode	Management State	Available actions in the Manage menu
Classic	Managed, Unmanage Failed	Resync, Unmanage, Delete
	Discovered, Not Managed	Manage, Delete
	Unmanage Requested, Delete Requested, Unknown	No actions
MDM	Not applicable (—)	Resync, Delete

2 Device discovery

Discovering devices using NSP

2.1 How does device discovery work?

2.1.1 Functional description

The NSP discovers devices using user-specified protocols and stores the device properties in the database. To discover one or more devices in your network, you create a discovery rule and then scan the network for devices according to the IP address ranges specified in the discovery rule.

A discovery rule contains lists of IP addresses or subnets are to be included in, or excluded from, the discovery process. For example, you can configure one subnet under included IP addresses for discovery, and another under excluded IP addresses. This allows you to provide a focused list of IP addresses for faster discovery scanning.

A discovery rule includes a network scan interval, for example, 60 min. This means that, if the discovery rule is active, NSP scans the network every 60 min to look for devices that match the information specified in the discovery rule and make them available for management by the NSP.

Discovery checks are also used to determine if an NE has been rebooted or if the software version has been upgraded. When a software upgrade is complete, the NE reboots and raises a reboot alarm. The reboot alarm triggers an NE-specific discovery scan. When the discovery scan detects a version change, the NE information is updated.

The management IP address is used to discover a device. The IP address provided for discovery must be reachable by the NSP.

Device discovery using IPv6

NSP supports the discovery of devices that use IPv6 IP addresses. In order for the NSP to discover and manage a device that uses IPv6, the device must have an IPv6 address on the management interface, and the NSP cluster must be configured for IPv6 mediation; see “Multi-interface configuration” in the *NSP Installation and Upgrade Guide.*

Note: IPv4 and IPv6 addresses must be discovered using different discovery rules.

2.1.2 Synching from NFM-P

Discovery rules, policies, and managed devices are synced from NFM-P to NSP and available in the Device Discovery or Device Management views. Devices in an unmanaged state are not automatically synced.

Classic discovery rules cannot be run from NSP. To use a classic discovery rule in NSP, it must be associated with a unified discovery rule; see 2.15 “How do I edit or delete a discovery rule?” (p. 38).

Important! To use telemetry and reporting with a synced NE, the classic discovery rule used to discover the device must be stitched to a unified discovery rule with gRPC mediation configured. This is a one-time manual process; see 2.16 “How do I enable NSP telemetry and reporting for NFM-P-managed classic devices?” (p. 39).

2.2 What is a unified discovery rule?

2.2.1 Unified discovery rules

A unified discovery rule can be used to discover model-driven and classic devices in specified IP address ranges, so that you can manage them in NSP.

The discovery rule provides the protocols and policies required to discover model-driven devices.

To use the unified discovery rule to discover classic devices, you must associate a 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.

When the unified discovery rule scans the network, it performs discovery using both MDM and classic:

- For host addresses (/32), NSP first tries to discover the devices in the IP address ranges using MDM. If MDM discovery fails, the IP addresses are pushed to NFM-P for classic discovery.
- For subnet discovery, the subnet IP address will be sent to both NFM-P and NSP MDM for NE discovery at the same time.

Note: NSP does not support IP address overlap in discovery rules: an IP address cannot be included in more than one discovery rule.

Select a discovery rule in the **Device Discovery**, **Unified Discovery Rules** view to see rule components, discovered NEs and any errors that occurred during discovery.

Note: Nokia AIM devices serve as controllers for MAG-c a2 appliances. You can discover an AIM using a unified discovery rule.

Specifying IP addresses for discovery

You can use an IP prefix to identify a range of IP addresses when you create a discovery rule. NSP discovery scans the range, with the exception of IP addresses typically reserved for the network address or broadcast address of a subnet.

For example, for the included IP address `10.0.1.0/25` NSP will scan the following range to discover devices: `10.0.1.1 – 10.0.1.126`.

To avoid this issue, specify specific (/32) IP addresses to include in the discovery rule for each expected IP address of an device that you want to discover.

2.3 What is a classic discovery rule?

2.3.1 Classic discovery rules

A classic discovery rule contains the IP management, mediation and reachability information required to discover and manage classic devices. The rule includes the following:

- IP management protocol: IPv4 or IPv6
- mediation policies: read access, write access, trap access, and security access
- reachability policies: in band management, out of band management, SNMP reachability

If discovery rules are present in the NFM-P, they are synced to the NSP and appear in the **Device Discovery**, **Classic Discovery Rules** view. For a classic discovery rule to be used to discover devices in NSP, it must be used by a unified discovery rule. Click on a discovery rule to see the unified discovery rule in the Summary panel.

Classic discovery rule parameters not currently supported in NSP

Some parameters that appear in discovery rules in the NFM-P are not currently supported in NSP.

Contact Nokia for support with any of the following:

- OLC State and Revert OLC State
- Scan Interval
- Group NE
- Discovery protocol other than SNMP, for example, TL1, NWI3 or NE3S
- External EMS
- Auto Discovery Rule Elements ACL
- MIB Statistics Policy
- Discovered Routers to Span(s)
- Backup Policy
- NE Self Config Policies
- EM Systems
- Post Discovery Action

2.4 What are discovery protocols and policies?

2.4.1 Protocols and policies

A unified discovery rule defines up to four protocols for MDM to use to discover the device. NSP scans the specified IP address ranges using each protocol in the order defined in the discovery rule. For example, you can use the same discovery rule to discover devices using both SNMP and CLI by selecting SNMP as the first discovery protocol and CLI as the second.

For MDM discovery, a unified discovery rule must include at least one mediation policy for each network communication protocol that is used to manage the NE. When a mediation policy is present, at least one reachability policy must also be included. You can select a ping reachability policy, a policy for the mediation protocol, or both. For example, if you have selected gRPC and NETCONF for mediation, you can select any combination of ping, NETCONF or gRPC reachability policies.

If the discovery rule will be used for classic discovery only, you can associate the classic discovery rule and leave the **Select Protocols** fields blank.

You must create mediation policies for all required protocols before discovery, regardless of which protocols are used to discover the devices.

After MDM discovery is completed, NSP discovers classic devices in the specified IP address ranges as applicable, using the classic discovery rule associated with the unified discovery rule.

Adding a domain controller also requires mediation and reachability policies. The protocols for discovery of a controller are often different from those used to discover NEs.

2.4.2 Mediation policies

To discover and manage devices in your network, you must create one or more mediation policies to setup the security and communication infrastructure between the NSP and each device.

A mediation policy defines how the NSP uses a communication type to interact with an NE. The policy specifies the communication settings, and the credentials for security functions. The order in which the policies are added to the discovery rule specifies the order in which they are used to attempt to reach the NE for discovery.

Model driven mediation policies

If the Classic Mediation parameter in a mediation policy is set to No, the mediation policy is for model-driven mediation. Each MDM policy provides mediation information for one protocol, for example, NETCONF.

If a protocol should be used only for NE management and never for discovery, set the Use for Discovery parameter to false.

The protocols required to manage an NE using MDM are listed in the artifact guide for the NE family, along with any applicable recommendations about the order in which the protocols should be used.

Select a policy in the **Device Discovery**, **Mediation Policies** view to see policy components, including the discovery rules, controllers, and NEs, if available, that use the mediation policy. If a mediation policy is in use, it cannot be deleted.

File transfer policies

FTP and SFTP policies for MDM are configured in the **Device Discovery**, **Mediation Policies** view and included in the discovery rule.

Device adaptor artifacts must be present in the NSP before an MDM file transfer policy can be configured.

Note: If a file transfer policy is present on the NE before discovery, the file transfer policy in the discovery rule overwrites the policy on the NE. If there is a file transfer policy on the NE and no file transfer policy in the discovery rule, the policy on the NE is deleted by the discovery process.

Classic mediation policies

If the Classic Mediation parameter in a mediation policy is set to Yes, the mediation policy is for mediation with classic devices. A classic mediation policy includes mediation information for SNMP, CLI, and file transfer. Therefore, all classic discovery rules include mediation information for all three mediation types, and all classic devices discovered in NSP have SNMP, CLI, and FTP or SFTP policies in place.

Mediation policies for controller discovery

Certain model-driven mediation protocols can be used for discovery of domain controllers only.

Device adaptor artifacts must be present in the NSP before controller mediation policies can be configured.

2.4.3 Reachability policies

A reachability policy defines a way for the NSP to perform a reachability check. The policy specifies the communication type to be used to reach the NE, for example SNMP, how often to attempt to reach the NE, and how long to wait for a response.

If a discovery protocol is selected, at least one reachability policy must be selected.

2.4.4 Anti-theft policies

Configuring an anti-theft policy in NSP allows the NSP to communicate with an NE in anti-theft mode.

The anti-theft policy provides the password information to the NSP, it does not configure anti-theft on the NE. Anti-theft configuration must be performed on the NE using CLI. The password configured in the anti-theft policy must match the OS password configured on the NE.

See “Network security in the NSP UI” in the *NSP Security Hardening Guide* for more information about anti-theft mode, and procedures to configure anti-theft policies.

Including an anti-theft policy in a discovery rule applies the anti-theft password to all NEs associated with the discovery rule.

Select a policy in the **Network Security**, **Anti-theft Policies** view to see policy components, including the discovery rules and NEs, if available, that use the anti-theft policy. If an anti-theft policy is in use, it cannot be deleted.

2.4.5 Policy synching from NFM-P

If mediation and reachability policies are present in the NFM-P, they are synced to the NSP and appear in the **Device Discovery**, **Mediation Policies** and **Device Discovery**, **Reachability Policies** views.

2.4.6 Protocols and policies in the Info panel

After devices have been discovered, you can select an NE in the **Device Management**, **Managed Network Elements** view to see the Info panel for the NE. Click (Mediation Policies), (Reachability Policies), or (Network Security). The Info panel displays the policies applied to the NE. From the Network Security tab, you can click to cross-launch to the relevant view.

The mediation and reachability policies applied to an NE depend on the discovery rule and the mediation type: the policies in the classic discovery rule are applied to classic devices, and the MDM policies in the universal discovery rule are applied to MDM devices. Network Security policies apply to all compatible NEs discovered by the discovery rule.

2.5 What are the principles for NSP compatibility with MDM devices?

2.5.1 NE compatibility

The NSP adaptor artifact program is designed to provide compatibility with MD SR OS and SRL NE releases on an N-3 and N+2 basis. For example, NSP 25.4 supports NE releases 22.x, 23.x, and 24.x, as well as NE releases 26.x and 27.x when released. As the NE model evolves, NSP delivers adaptor artifacts in support of those changes.

2.5.2 Flexible discovery

NSP supports flexible discovery of NEs managed via MDM artifacts. Flexible discovery means that NSP can use existing artifacts to discover an NE that has been upgraded to a new maintenance release. If you elect to use this capability and skip the installation of new artifacts, NSP will only be aware of the NE model objects (MDC, device telemetry, alarms) defined for the NE version for which the artifact was designed. To get support for new models in the latest NE version, you must update to the artifact bundle associated with that NE version.

The following example uses the fictitious NE 9999 ABC, release 12.x:

Discovered NE version	Adaptors and compatibility rules in place	Expected result
12.1 R1	No 12.x adaptors installed	NE is not certified and cannot be discovered or managed.
12.1 R1	12.1 adaptors installed with explicit support for 12.1.R1 defined in the metadata	NE is certified, that is, it can be discovered and managed without use of a compatibility rule.
12.1.R2	12.1 adaptors installed but 12.1.R2 is not defined explicitly in the metadata	• If the adaptors have a default compatibility rule defined, NE is compatible and can be discovered or managed at the level of 12.1.R1. • If the adaptors do not have a default compatibility rule defined, NE is not compatible and cannot be managed.
12.2.R1	12.1 adaptors installed No adaptors available for 12.2 Custom compatibility rule is in place listing 12.1.R1 as the compatible version for 12.2.R1	NE is compatible, that is, it is discovered and managed according to a compatibility rule. The NE will be managed at the 12.1.R1 level.

The NE compatibility rules for artifacts are defined in the discovery adaptor and extrapolated to the artifact documentation. For multi-vendor NEs, you can override the default NE compatibility rules using RESTCONF APIs as described on the Network Developer Portal.

For more details about the applicability and/or any restrictions of the NE compatibility feature to specific devices, consult the NSP adaptor artifact guides for those devices.

2.6 What is a domain controller?

2.6.1 Domain controllers

A domain controller is an external element manager that is managing NEs. By adding the controller to your NSP, you can view and manage the controller's NEs in your NSP.

In the current release, the only supported type of domain controller is another NSP.

Procedures for device discovery

2.7 How do I create a classic mediation policy?

2.7.1 Purpose

Use this procedure to set up security and communication infrastructure between the NSP and classic devices in your network. The policy, along with other components of a unified discovery rule, will be used to discover and manage the devices in NSP.

2.7.2 Steps

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
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

2.8 How do I create a mediation policy for MDM?

2.8.1 Purpose

Use this procedure to configure communication with model-driven devices or domain controllers, using a selected communication type or protocol.

The policy consists of a network communication profile, which contains information such as port number and timeouts, and a network user, which is a user name and password. You can associate users or communication profiles with multiple policies.

For example, if two different network users (that is, two sets of credentials) might be used to log in to the same port using CLI over Telnet, create a policy of type CLI for each user. When you create the second policy, associate the communication profile you created for the first policy. This applies the same CLI parameters to the policy for the other user.

Note: To create a file transfer mediation policy for MDM, device adaptor artifacts must be present in the NSP.

2.8.2 Steps

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, leave the **Classic Mediation** check box unchecked.

4

Configure the general parameters.

Parameter	Description
Policy type	Specifies the communication type the mediation policy is for, for example, SNMPV3. **Note:** For gNMI-based discovery, select the gRPC mediation policy type.
Policy name	The name of the mediation policy
Description	User-provided description of the policy
Use For Discovery	Disable this parameter if the communication type is not to be used to discover the NE, for example, if the communication type is for telemetry collection only. This parameter does not appear if the policy type cannot be used to discover devices.

5

Configure the communication parameters.

6

Click **CREATE**. The mediation policy is automatically assigned a policy ID and is added to the list.

END OF STEPS

2.9 How do I edit or delete a mediation policy?

2.9.1 Purpose

CAUTION

Communication problems

If a mediation policy is edited when it is in use by a discovery rule, communication with devices may be affected.

Verify that the updated protocol credentials match the configuration on the NE.

The default classic mediation policy can be edited but cannot be deleted.

Note: The special characters *;* and \ can appear in classic policy names that have been synced from NFM-P. These characters are not allowed in NSP. Policies with these characters in their names cannot be edited or deleted in NSP.

2.9.2 Steps

1

Open **Device Discovery**, **Mediation Policies**.

The system displays the list of configured mediation policies.

2

To edit a mediation policy:

1. Choose a policy and click ⋮ (Table row actions), **Edit**.
2. Configure the parameters and click **UPDATE**.

3

To delete a mediation policy, choose a policy and click ⋮ (Table row actions), **Delete**, and confirm.

A policy cannot be deleted if it is in use by a discovery rule.

END OF STEPS

2.10 How do I create a classic reachability policy?

2.10.1 Purpose

Use this procedure to create a management ping policy to specify how the NSP checks the connection to device management IP addresses on classic devices.

Note: You must enable scheduling for a ping policy to be active. When scheduling is not enabled, and an assigned managed device is not reachable, management connection alarms may not be raised.

During creation of a discovery rule, reachability policies are assigned for in-band management, out of band management, and SNMP reachability.

2.10.2 Steps

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

2.11 How do I create a reachability policy for MDM ?

2.11.1 Steps

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 or protocol to be used to confirm reachability, for example, Ping.
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

2.12 How do I edit or delete a reachability policy?

2.12.1 Purpose

Use this procedure to make changes to a reachability policy.

The default policy can be edited but cannot be deleted.

Note: The special characters *;* and \ can appear in classic policy names that have been synced from NFM-P. These characters are not allowed in NSP. Policies with these characters in their names cannot be edited or deleted in NSP.

2.12.2 Steps

1

Open **Device Discovery**, **Reachability Policies**.

The system displays the list of configured reachability policies.

2

To edit a reachability policy:

1. Choose a policy and click ⋮ (Table row actions), **Edit**.
2. Configure the parameters and click **UPDATE**.

3

To delete a reachability policy, choose a policy and click ⋮ (Table row actions), **Delete**, and confirm.

END OF STEPS

2.13 How do I create a classic discovery rule?

2.13.1 Purpose

To discover classic devices, NSP requires a classic discovery rule. The classic discovery rule is associated with a unified discovery rule. NSP performs scans of the network to look for devices matching specifications provided in active unified discovery rules. You can also launch a discovery manually.

RESTCONF APIs are also available for device discovery and management; see the Device Administration and Mediation RESTCONF APIs documentation on the Network Developer Portal.

Note: The special characters *;* and \ can appear in the names of classic discovery rules that have been synced from NFM-P. These characters are not allowed in NSP. Rules with these characters in their names cannot be edited or deleted in NSP.

2.13.2 Steps

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 2.7 “How do I create a classic mediation policy?” (p. 29).
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 2.10 “How do I create a classic reachability policy?” (p. 32).

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 2.14 “How do I discover devices?” (p. 35).

END OF STEPS

2.14 How do I discover devices?

2.14.1 Purpose

To discover devices, create a unified discovery rule. NSP performs scans of the network to look for devices matching specifications provided in active discovery rules. You can also launch a discovery manually.

The association of a classic discovery rule provides information for discovery of classic devices. The discovery protocols and policies parameters in the discovery rule provide information for discovery and management of MDM devices. When associating a classic discovery rule from NFM-P to a unified discovery rule, verify that the list of IP addresses in the unified discovery rule matches the list of IP addresses from the NFM-P classic discovery rule.

RESTCONF APIs are also available for device discovery and management; see the Device Administration and Mediation RESTCONF APIs documentation on the Network Developer Portal.

Note: To prevent performance issues with discovery:

- A discovery rule must not contain more than 512 IP addresses.
- The protocol to be used to discover the devices should be the first protocol choice in the discovery rule. For example, if the node is discoverable through NETCONF then NETCONF should be selected as first protocol choice in the discovery rule. See the artifact guide for the NE family for the recommended order.
- Mediation polices which are not used for discovery should have the “Use For Discovery” flag set to false.
- If subnets are used in the discovery rule, most of the IP addresses should be reachable. Any unreachable IP addresses should be added into the exclude list.

  Having a lot of undiscoverable IP addresses in the discovery rule would lead to a timeout error.

2.14.2 Steps

1

Open **Device Discovery**, **Unified Discovery Rules**.

The system displays the list of configured discovery rules.

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	

Parameter	Description
(First|Second|Third|Fourth) discovery protocol	Specify the protocols to be used to communicate with the NE, in the order in which they should be used to attempt to reach the NE for discovery. The protocol to be used to discover the NE should be the first protocol selected; see the artifact guide for the NE family for the recommended order. Enter all the protocols that will be used for communication, regardless of whether they will be used for discovery. After at least one protocol is selected, the **Select Mediation Policies** panel displays, with fields for the selected protocols. If device adaptor artifacts are installed in the NSP, a file transfer field also appears. Required policies are indicated with an asterisk (*).
Mediation Policies	Select a policy for each discovery protocol you selected, and, if needed, for file transfer: 1. Click on the policy field. 2. In the form that opens, select a policy and click **SELECT**. To create a mediation policy, click **+ NEW**; see 2.8 “How do I create a mediation policy for MDM?” (p. 30).
Reachability Policies	The **Select Reachability Policies** panel displays fields for the selected discovery protocols and for Ping. If a discovery protocol has been selected, at least one reachability policy must be selected. The policy can be specific to the discovery protocol, or a Ping policy. 1. Click on a policy field. 2. In the form that opens, select a policy and click **SELECT**. To create a reachability policy, click **+ NEW**; see 2.11 “How do I create a reachability policy for MDM ?” (p. 33).
Associate Classic Discovery Rule	1. Click in the Classic Discovery Rule field. 2. In the form that opens, select a discovery rule and click **SELECT**. To create a classic discovery rule, click **+ NEW**; see 2.13 “How do I create a classic discovery rule?” (p. 34).
Network Security	
Anti-theft Policy	1. Click on the policy field. 2. In the form that opens, select a policy and click **SELECT**. To create an anti-theft policy, click **+ NEW**; see “How do I create an anti-theft policy?” in the *NSP Security Hardening Guide*.

Parameter	Description
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. If any IP addresses in the included ranges are unreachable, add the unreachable IP addresses to the Excluded IP Addresses list. Searching many unreachable IP addresses may cause discovery to time out.

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

2.15 How do I edit or delete a discovery rule?

2.15.1 Purpose

You can edit a discovery rule to change the admin state or scan interval, add mediation protocols and policies, for example, to add a gRPC mediation policy for telemetry, to associate or remove a classic discovery rule, or to change the lists of included or excluded IP ranges.

If a discovery rule is deleted, the discovered NEs are not removed from the NSP. However, the IP ranges for affected devices must be added to a remaining discovery rule to prevent loss of communication.

2.15.2 Steps

1

Open **Device Discovery**, **Unified Discovery Rules** or **Device Discovery**, **Classic Discovery Rules**

2

To edit a discovery rule:

1. Choose a discovery rule and click ⋮ (Table row actions), **Edit**.
2. Configure the parameters and click **UPDATE**.

3

To delete a discovery rule, choose a rule and click ⋮ (Table row actions), **Delete**, and confirm.

END OF STEPS

2.16 How do I enable NSP telemetry and reporting for NFM-P-managed classic devices?

2.16.1 Purpose

If classic devices are already discovered in the NFM-P, for example, in a brownfield scenario or after an upgrade from a previous release, the classic discovery rules, policies, and managed devices are automatically synced from NFM-P to NSP and are visible in the Device Discovery or Device Management views. Devices in an unmanaged state are not automatically synced.

To use NSP telemetry and reporting with a synced NE, the classic discovery rule used to discover the device must be associated with a unified discovery rule with gRPC mediation configured. The NSP uses the gRPC mediation policy configured in the unified discovery rule to collect statistics. Performing this procedure enables gRPC mediation for all classic devices discovered by a classic discovery rule.

Note: Only one classic discovery rule can be associated with a selected unified discovery rule. See 2.14 “How do I discover devices?” (p. 35)to create additional unified discovery rules if needed.

Note: If statistics collection is set up in both NFM-P and NSP, the telemetry framework may receive the same information twice. The duplication could result in incorrect reports or duplicated TCAs. To avoid duplication, disable equivalent MIB based statistics in NFM-P if gRPC telemetry is used, or see “Troubleshooting duplicate data collection” in the *NSP Troubleshooting Guide* for more options.

2.16.2 Steps

1

Obtain required information about the NE:

- Open **Device Management**, **Managed Network Elements**.
- Note the management IP address of the NE.
- Click on the NE to open the Summary panel, and Click on the Discovery Rules pane ( ) to find the associated classic discovery rule.

Associate the classic discovery rule to the unified discovery rule

2

Open **Device Discovery**, **Unified Discovery Rules**.

3

Select a discovery rule and click ⋮ (Table row actions), Edit.

4

In the Edit Discovery Rule form, click in the Classic Discovery Rule field.

In the form that opens, select a discovery rule and click **SELECT**.

5

Verify that the IP addresses of the classic devices are in one of the included IP ranges.

If needed, click + **ADD** to specify an IP address and mask bits.

6

Click **UPDATE**.

The discovery rule is updated. The next time the discovery rule is run, the gRPC mediation information provided by the discovery rule is applied.

Note: Only one classic discovery rule can be associated with a selected unified discovery rule. See 2.14 “How do I discover devices?” (p. 35)to create additional unified discovery rules if needed.

Restore collection and reporting

7

If you have upgraded your system from 23.11 or earlier, restore classic telemetry collection. See the **Restore classic telemetry collection** step in “To upgrade an NSP cluster” in the *NSP Installation and Upgrade Guide*.

8

Verify the age-out policies for the telemetry types as needed.

After an upgrade from 23.11 or earlier, the NE IDs for dual stack NEs have been changed, causing existing telemetry records to become stale. The stale records will be deleted according to the age-out policy for each telemetry type.

See “How do I edit an age-out policy?” in the *NSP Data Collection and Analysis Guide* to update the policies as needed.

9

If you created baselines in NSP using NFM-P statistics collection, and will be using NSP to collect statistics in future, create the baselines again.

See “How do I create baselines?” in the *NSP Data Collection and Analysis Guide*.

10

Update any object filter elements that include `nokia-nsp-source:fdn`, for example, `"networkDeviceId":"/network-device-mgr:network-devices/network-device[name='1.1.1.1']/root/nokia-nsp-source:fdn[id='fdn:realm:sam:network:1.1.1.1:shelf-1:cardSlot-12:card:port-4']"`, to device yang format, for example, `"networkDeviceId":"/network-device-mgr:network-devices/network-device[name='1.1.1.1']/root/nokia-state:state/port[port-id='B/4']"`.

11

If you have saved charts using baselines or object filters you recreated in steps Step 9 and Step 10, plot and save the charts again.

See the procedures to plot charts in the *NSP Data Collection and Analysis Guide*.

END OF STEPS

2.17 How do I discover a domain controller?

2.17.1 Steps

1

Open **Device Discovery**, **Domain Controllers**.

The system displays the list of configured domain controllers.

2

Click **+ CONTROLLER**.

3

In the form that opens, configure the required parameters.

Parameter	Description
General	
Name	The name of the controller
Type	NSP is the only type of domain controller currently supported.
Version	Specifies the NSP release the external NSP is running.
Primary IP Address	Specifies the primary IP address of the controller.
Standby IP Address	Enter the standby IP address, if applicable.
Policies	

Parameter	Description
Mediation Policies	Policies that are mandatory for controller discovery are indicated with an asterisk (*). 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 2.8 “How do I create a mediation policy for MDM?” (p. 30).
Reachability Policies	Policies that are mandatory for controller discovery are indicated with an asterisk (*). 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 2.11 “How do I create a reachability policy for MDM ?” (p. 33).

4

Click **CREATE**. The domain controller is added to the list.

END OF STEPS

2.18 How do I discover the NEs managed by a domain controller?

2.18.1 Steps

1

Open **Device Discovery**, **Domain Controllers**.

The system displays the list of configured domain controllers.

2

Verify the reachability of the controller whose devices you want to discover. The controller must be reachable for its devices to be discovered.

3

Choose a controller and click ⋮ (Table row actions), **Discover NEs**.

4

In the form that opens, enter the NE IDs of the NEs managed by the controller:

1. Click **+ ADD**

2. Enter an NE ID. If you will be entering more NE IDs, click the **Create another** check box.
3. When you have entered your last NE ID, disable the check box and click **ADD**.

5

Click **DISCOVER & CLOSE** to launch the discovery and remain in the **Device Discovery**, **Domain Controllers** view, or **DISCOVER & VIEW** to launch discovery and switch to the **Device Management**, **Managed Network Elements** view.

6

To view results of a discovery, select the controller and click **Summary** ⓘ to view the Summary panel. In the panel at the right of the screen, the number of NEs discovered is displayed.

Click **OPEN** to view the NEs in the **Device Management**, **Managed Network Elements** view.

END OF STEPS

2.19 How do I edit or delete a domain controller?

2.19.1 Purpose

You can edit a domain controller to change the mediation policies.

A controller cannot be deleted while discovered NEs managed by the controller are managed in the NSP.

2.19.2 Steps

1

Open **Device Discovery**, **Domain Controllers**

2

To edit a domain controller:

1. Choose a controller and click ⋮ (Table row actions), **Edit**.
2. Configure the parameters and click **UPDATE**.

3

To delete a domain controller:

1. Choose the controller you need to delete and click ⋮ (Table row actions), **Open discovered NEs in Device Management**. A filtered list of the NEs appears in a new tab.
2. For each NE, choose the NE and click ⋮ (Table row actions), **Manage**, **Delete** and confirm.

   The NEs are removed from the local NSP but continue to be managed by the controller.
3. Return to **Device Discovery**, **Domain Controllers**, choose the controller and click ⋮ (Table row actions), **Delete**, and confirm.

END OF STEPS

3 NE maintenance

NE backup and restore

3.1 How do I back up an NE?

3.1.1 Purpose

You can back up an NE, provided there is an operation type configured for the selected NE. Backup is only supported for primary configurations. To back up multiple NEs simultaneously, you can use an operation. See Chapter 4, “Operations” for information about configuring operation types and performing operations.

The NE must have an NE Name configured, you cannot perform a backup on an NE with no NE name (a null name is displayed as N/A). The NE Name must be unique in the NSP network; backup or restore operations may fail if the NE Name is shared with any other NE.

An FTP mediation policy must be assigned to the NE before you can perform a backup. FTP mediation policies are created and assigned either using the NSP or a REST API. For information about configuring mediation policies using the NSP see “Procedures for device discovery” (p. 29); for information about using a REST API see the Device Management tutorials on the Network Developer Portal.

An NDX file is required to perform a backup on nodes configured in classic or mixed mode. The backup operation fails if an NDX file with the same name as the configuration file defined in the bof file is not present in the same folder.

You can configure a backup to include debug files located on the same cf as the configuration file.

Note: An NE cannot be backed up if its Anti-theft Lock Status is Locked. To unlock an NE in anti-theft mode, the correct password must be configured in the anti-theft policy; see the *NSP Security Hardening Guide*.

3.1.2 Steps

1

Open **Device Management**, **Managed Network Elements**.

2

From the Managed Network Elements list, select the NE you need to back up.

3

Click ⋮ (Table row actions), Backup. The backup operation is added to the operations queue.

4

You can view the status of the backup in the Backup section of the details panel for the selected NE, or you can click ⋮ (Table row actions), **Operation History** to view completed backups.

END OF STEPS

3.2 How do I view backup files for an NE?

3.2.1 Steps

1

Open **Device Management**, **Managed Network Elements**.

2

From the Managed Network Elements list, select the NE you need to manage.

3

To view backup files for a specific backup operation, perform the following:

1. Click ⋮ (Table row actions), **Review backups, View backup history**. The backup history view appears, displaying a list of backup operations performed on the selected NE.
2. Select an operation and click (Table row actions), **View Files**. A list of backup files appears; you can select a file and click **View File Content** to display the contents of each file.

4

To view all backup files for an NE, perform the following:

1. Click (Table row actions), **Review Backups, View all backup files**. A list of all backup files stored in the NSP for the selected NE appears.
2. Select a backup file and click **View Zip Content** to explore the files in the archive.

END OF STEPS

3.3 How do I compare two backup files for an NE?

3.3.1 Purpose

You can view two files from two separate backups in a side-by-side comparison window that highlights differences. You can only compare files for backups that were performed from the NSP.

3.3.2 Steps

1

Open **Device Management**, **Managed Network Elements**.

2

From the Managed Network Elements list, select the NE you need to manage.

3

To compare a previous backup with the most recent backup, perform the following:

1. Click ⋮ (Table row actions), **Review backups, View backup history**. The backup history view appears, displaying a list of backup operations performed on the selected NE.
2. Select a successful backup operation and click (Table row actions), **Compare with latest backup**. A file compare window appears.
3. Select the files you need to compare from the drop-down lists. File comparison panels appear, displaying the contents of the files with any differences highlighted.

4

To compare any two backup files, perform the following:

1. Click (Table row actions), **Review Backups, View all backup files**. A list of all backup files stored in the NSP for the selected NE appears.
2. Select two backup files, and click on **File Compare.** A file compare window appears.
3. Select the files you need to compare from the drop-down lists. File comparison panels appear, displaying the contents of the files with any differences highlighted.

End of steps

3.4 How do I compare the current NE configuration with a backup?

3.4.1 Backup file comparison

You can compare files from a previous backup to the current NE's configuration, either the most recent backup or an older backup.

3.4.2 Steps

1

Open **Device Management**, **Managed Network Elements**.

2

From the Managed Network Elements list, select the NE you need to manage.

3

To compare with the most recent backup, perform the following:

1. In the details panel, expand the Backup section.
2. Beside the backupFilename parameter, click ⋮ (Table row actions), **Compare with current NE config**. The NSP begins comparing the files and a File Compare window opens when the comparison is ready.

4

To compare with a previous backup, perform the following:

1. Click ⋮ (Table row actions), **Review backups, View backup history**. The backup history view appears, displaying a list of backup operations performed on the selected NE.
2. Select the backup you need to compare, and click ⋮ (Table row actions), **Compare with current NE config**. The NSP begins comparing the files and a File Compare window opens when the comparison is ready.

5

In the file compare window, select the files you need to compare from the drop-down lists. File comparison panels appear, displaying the contents of the files with any differences highlighted.

END OF STEPS

3.5 How do I restore an NE from a backup?

3.5.1 Purpose

If you backed up an NE from NSP, you can restore to that backup from **Device management**, **Managed Network Elements**. The current NE version must match the version installed when the backup was made. The NE Name of the NE must be unique in the NSP; restore operations may fail if the NE Name is shared with another NE.

An FTP mediation policy must be assigned to the NE before you can perform a backup. FTP mediation policies are created and assigned using a REST API; see the Device Management tutorials on the Network Developer Portal.

3.5.2 Steps

1

Open **Device Management**, **Managed Network Elements**.

2

From the Managed Network Elements list, select the NE you need to restore.

3

Perform one of the following to find the backup you need to restore:

a. To select from a list of completed backup operations, click ⋮ (Table row actions), **Review backups, View backup history**. The backup history view appears, displaying a list of backup operations performed on the selected NE.

b. To select from a list of backup files, click ⋮ (Table row actions), **Review backups, View all backup files**. The backup file view appears, displaying a list of the backup files stored for the selected NE.

4

Select the successful backup operation or backup file which you need to restore, and click ⋮, **Restore**. If a default restore operation type is configured, then a restore operation is created and starts immediately; otherwise, the Restore NE form opens.

5

If required, choose a restore operation type from the drop-down list in the Restore NE form, then click Restore.

6

You can view the status of the Restore operation on the Operations tab, and view a record of the completed Restore operation in the Operation History view.

END OF STEPS

3.6 How do I configure automatic cleanup of backup files?

3.6.1 Purpose

By default, NSP policies are configured to automatically delete backup executions that are older than one day, and backup files that are older than 30 days. You can configure the policies to alter or disable the automated file cleanup. The backup file cleanup policy only applies to backup files that are stored in the NSP file system; backup files stored in other locations (for example, on the NE) are not affected.

3.6.2 Steps

To configure the automated cleanup of backup executions

1

Open **Workflows, Policies**.

2

Select the Lsom-Backup-Purge-Policy and click on ⋮ (Table row actions),**Update**. The Update Policy form opens.

3

Configure the Older Than (Days) parameter to specify how many days to keep backup executions before they are deleted. Configure the other parameters as required.

4

Click Update to save and update the policy.

To configure the automated cleanup of backup files

5

Open **File Server**.

6

Click **File Server Settings.** The File Server Settings page opens.

7

In the Override Policies section of the Purge Settings panel, select the /lsom/neBackup policy and click on ⋮ (Table row actions),**Edit**. The Update Purge Settings page opens.

8

Configure the Retention Period (Days) parameter to specify the number of days to keep backup files before they are deleted. Configure the other parameters as required.

END OF STEPS

Part II: Advanced device management

Overview

Purpose

Provides information about advanced and large-scale options for managing NEs using NSP.

Contents

4 Operations

Overview

4.1 Operations

4.1.1 Overview

The Operation views are available in the Device Management view; this function is sometimes referred to as large-scale operations because they are performed on groups of NEs. To complete operations, NSP executes workflows. You can view the workflows in the **Workflows**, **All Workflows** view if needed.

Note: Before performing an operation on a group of NEs, you must define NE groups; see the *NSP System Administrator Guide*.

An operation is composed of a series of workflows, organized in phases, which are performed on a scope of NEs. Each phase of an operation is associated with a workflow. When the workflow for a phase is performed on an NE, it creates an execution within the operation, which is an instance of that phase's workflow being performed on that NE. The workflows, phases, and other details for an operation are defined in an operation type.

You can create an operation to perform a task on large numbers of NEs concurrently; for example, upgrading all SR NEs in a network to the latest SR OS release. To complete the task, the NSP performs the actions that are defined in workflows; the specific workflows used can vary depending on the target NE, and each operation type contains a mapping profile which specifies which workflow to use on an NE for each phase in the operation. For example, an upgrade operation may contain a phase for copying files to the target NE; the specific workflow called may be different for a 7450 ESS and a 7950 XRS, but at the end of the phase the files are copied.

4.1.2 Operation types

An operation type is the blueprint used to create an operation. Each operation type is intended to perform a general task, such as upgrading software, and combines an operation model and a mapping profile, which are used to find the appropriate workflows to be performed on the NEs specified in the operation. The mapping profile matches workflows to NEs based on NE identifiers (for example, NE family or version). The operation model extends the base operation model defined in the NSP for each operation type.

Phases

Each operation is divided into phases, which are high-level steps in the process of the operation. Phases vary depending on the operation, and some operations have only a single phase. Some operations contain an Initial-Phase phase, which is performed against the NSP system to ensure the NSP is ready to proceed with the operation.

Phases which are waiting for your attention are noted in the **Device Management**, **All Operations** view.

Executions

An execution is the implementation of a phase on a specific NE. You can view the progress of individual phases by double-clicking on an operation in **Device Management**, **All Operations** view.

Executions can generate reports for you to review; report outputs are defined in the workflows used by the operation, so can vary between operations. Some operations generate reports in multiple phases, and provide an option for comparing reports - for example, an operation may have a pre-check phase and a post-check phase, with both phases generating reports that can be compared to highlight differences. Which reports are comparable is defined in the mapping profile for the operation. For assistance in developing workflows and operations that generate reports, please contact your support representative.

Creating and updating operation types

Operation types are stored in the NSP as artifacts and managed using Artifacts. Adding a new operation type or updating an existing one requires installing an artifact bundle. For information about installing an artifact bundle, see “How do I install an artifact bundle?” in the *NSP Network Automation Guide*. For information about creating artifact packages, contact your Nokia support representative.

Note: Before upgrading an operation type to a new major version by installing an updated artifact package, configure the lifecycle of the operation type to Withdrawn.

4.1.3 Operation models

An operation model is a .yang file which can be used to extend the base operation model of each operation type. For example, the operation model included in the default NE Backup operation type extends the model to include the backup-file parameter, which retrieves the name of the backup file created by the operation and includes it in the task result summary as a parameter.

Operation inputs can be stated in an operation model, and values for those inputs configured when the operation is created.

4.1.4 Mapping profiles

A mapping profile is a .yaml file that maps nodes to workflows, using node parameters such as node family and node software version. Qualifiers can be nested to produce more specific results, for example:

```
phases:

  - phase: 'Backup'

    description: 'Single phase backup'

    concurrency_count: 20

    ne_families:

       - family_type: 7750 SR, 7950 XRS
```

```
ne_versions:

 - version: all

   workflow_name: LSO_7x50_Backup

   workflow_inputs:

   backup_certificates: no
```

You can use a mapping profile to call different workflows for different nodes, or provide different inputs for the same workflow.

4.1.5 Operation schedules

You can schedule an operation to occur at a later date, or on a repeating schedule. A scheduled operation appears in the **Operation schedule** view, where you can view and edit the operation's details. Scheduled operations can be in one of four states:

State	Icon	Description
Scheduled		The operation is ready to start at the scheduled time.
Paused		The operation is manually paused. Operations that have been generated by this schedule that are already in progress complete normally, but future operations do not proceed until the schedule is resumed.
Ended		The end date for the operation has passed and the operation schedule has ended. You can edit the operation schedule with a new end date to return it to the Scheduled state.
Cancelled		The operation schedule has encountered an error that prevents it from starting the operation, and been cancelled; for example, the targets of the operation cannot be found.

4.1.6 Model-driven and mixed-mode operations

For operations performed on nodes discovered through mixed-mode or model-driven management, CLI access management must be enabled on the node. The following types of CLI access must be enabled, in the order shown: md-cli, and classic-cli.

For SR OS device commissioning information, see the Management Interface Protocol Configuration section in the adaptor artifact guide. For additional information if needed, see the NE documentation.

4.1.7 Operation behavior after a service interruption

After a service interruption that shuts down the NSP server, for example a switchover from a primary NSP server to a backup, any operations currently in progress are marked as failed and

must be manually restarted or resumed. Scheduled operations are unaffected, only operations currently in progress when the interruption occurs are disrupted.

4.2 Operation views

4.2.1 Views

The Operations group includes the following views: All Operations, Operation Schedules, Operation Types, and Node Images. Use the drop-down to switch from one view to another.

The following table describes device operations terms.

Term	Description	Navigation
Operation	An operation is a series of executions, organized in phases, which are performed on a scope of NEs. An operation is a job: it is composed of an operation type, a selected series of targets, inputs, and schedule.	Choose **All Operations** from the drop-down. This is the primary view, showing operations that are currently executing, scheduled, or completed.
Operation schedule	A schedule allows you to configure an to execute in the future, either once or repeatedly.	Choose **Operation Schedules** to view a list of scheduled future operations, and saved draft operations. You can delete scheduled operations from this list, and schedule or modify saved draft operations.
Operation type	An operation type provides the general definition of a task, such as upgrading software. The operation type combines an operation model and a mapping profile.	Choose **Operation Types** from the drop-down to view the list of configured operation types.
Operation model	An operation model is a .yang file which can be used to extend the base operation model of each operation type. For example, the operation model included in the NE upgrade operation type extends the model to include a description of the required format of the target software version.	From the Operation Types view, select an operation type and click ⋮ (Table row actions), View Operation Model.
Mapping profile	A mapping profile is a .yang file that is used to load the appropriate workflows to be performed to complete the operation. The mapping profile matches workflows to NEs based on NE identifiers (for example, NE family or version).	From the Operation Types view, select an operation type and click ⋮ (Table row actions), View Mapping Profile. **Note:** You can view the workflows in the Workflows menu for more information about the detailed steps performed. You do not need to access Workflows to complete the upgrade.
Node image	Node software image stored in the NSP database for use by operations	Choose **Node Images** from the drop-down to view the list of imported software images, divided into tabs by node family. You can upload new images using the **+ IMPORT** button.

4.3 Operation types provided by NSP

4.3.1 Default operation types

The NSP provides default operation types that allow you to perform backup, restore, upgrade, and audit operations. You can create additional operation types for use with your network. Default operation types are available for the nodes listed in the following table.

Node	Note
7210 SAS and variants: Mxp, D, Dxp, K, M, X, T, R, E, S/Sx	Classic mode only
7215 IXS SRLinux	—
7220 IXR SRLinux	—
7250 IXR	—
7250 IXR SRLinux	—
7450 ESS	—
7730 SXR SRLinux	—
7750 SR	—
7950 XRS	—
MAG-c Appliance	Supports backup, restore, upgrade, and audit operations with the following requirements: • A CLI mediation policy with a common username and password attached to both MAG-c a2 Appliance NE and MAG-c NE • An FTP mediation policy attached to both MAG-c a2 Appliance NE and MAG-c NE using the NSP UI • The MAG-c a2 Appliance NE name must be unique in the NSP • For upgrade operations, the MAG-c a2 Appliance NE must be Release 24.3 R1 or later. • When performing an upgrade operation, only select the active MAG-c a2 Appliance NE as the target.

MAG-u	Supports upgrade operations with the following considerations:
	• Before starting the upgrade, predefined BNG queries must be configured on the connected MAG-c using the following commands:
	`/configure mobile-gateway system bng queries session fwa user-access-type fwa`
	`/configure mobile-gateway system bng queries session "fwa" output-options count`
	• When using the single-phase upgrade operation (nsp-ne-upgrade), the reboot action should not be triggered, as it may result in the loss of only FWA sessions.
	• Do not modify the PFCP configuration of the MAG-u in the 10 minutes before starting an upgrade
	• Only FWA sessions are drained during an upgrade

Node	Note
Wavence SM, SA, MSS-8/MSS-4 coreEvo	Classic mode upgrade only

Note: Audit operations can be performed on any node, provided the backup being audited was created using the nsp-ne-backup operation type.

4.3.2 Upgrade operation types

The NSP provides signed upgrade operation types for some NEs.

The following table describes the upgrade operations provided with NSP.

Operation name	Description	Supported NE types
nsp-ne-upgrade-with-phases	Operation for Multi-Phase Upgrade The operation phases are: • Pre-checks for NE upgrade • Software image download to NE • Software image activation on NE • Reboot NE or perform CPM switchover to complete upgrade Each phase is a workflow.	SR OS NEs, including 7750 SR, 7950 XRS, 7450 ESS, 7250 IXR, 7705 SAR, and 7210 SAS SR Linux NEs: 7220 IXR SRLinux, 7250 IXR SRLinux Upgrade is available to versions for which node software images can be found on the support portal.
nsp-ne-upgrade-eth-sat	Operation for Ethernet Satellite Upgrade	
nsp-ne-wavence-upgrade	Operation for Wavence NE Multi-Phase Upgrade	Wavence NEs
nsp-magc-appl-upgrade-phases	Operation for MAG-c a2 Appliance NE upgrade	MAG-c a2 Appliance NEs

See the Device Management tutorials on the Network Developer Portal for information about working with Operations APIs.

Each operation calls one or more workflows. See the Workflows tutorial on the Network Developer Portal for information about updating workflows.

Important! Operation types and workflows provided with the NSP for NE upgrade are signed by Nokia. Signed artifacts cannot be modified. If you choose to manually clone, edit and re-deploy a signed artifact, the clone is not signed.

Procedures

4.4 How do I change the life cycle state of an operation type?

4.4.1 Purpose

You can withdraw an operation type from service, or return an operation type to the released state. Withdrawn types do not appear in the list of options when choosing an operation to perform on an NE.

4.4.2 Steps

1

Open **Device Management**, **Operation Types**.

A list of existing operation types appears.

2

Select an operation type and select a life-cycle state from the drop-down menu in the Life Cycle column.

END OF STEPS

4.5 How do I start or schedule a new operation?

4.5.1 Purpose

You can start an operation on a group or list of NEs using the Operations views. NE groups are configured using the Map Layout; for information about creating NE groups, see the *NSP System Administrator Guide*.

Operations with a single phase can be scheduled to start at a later time, and can be configured to repeat (for example, a repeating backup operation). Schedule options depend on the type of operation. Operations with multiple phases, and single-phase upgrade operations, cannot be scheduled and instead run once when started. You can save an unscheduled operation and start or schedule it later.

Operations with multiple phases that are in the categories Upgrade or Other can be configured to proceed on a per-phase or per-target basis. When configured for per-phase progression, all targets must finish the current phase before any target can proceed to the next phase. When configured for per-target progression, a target can proceed to the next phase immediately regardless of the progression of other targets.

Note: Node upgrade operations have further requirements; see 5.1 “Upgrade operation requirements” (p. 73). If a node upgrade fails, the upgrade operation will restore the node software to the version that was installed previously.

4.5.2 Steps

1

Open **Device Management**, **All Operations**.

2

Click **+ OPERATION**. The Create Operation form opens.

3

Click **+ OPERATION TYPE**, choose an operation type from the list that appears, and click **ADD.** To change the chosen operation type, click **REPLACE** and choose a different operation type.

4

In the General panel, provide a name and description for the operation, and configure the other attributes as required. Under Operation Control, choose per phase or per target progression, if available. Some operations support specifying a product family in the Targeted Product Family drop-down; specifying a product family restricts operation targets to that family and prevents incorrect targets from being chosen.

5

Click **+ SELECT** in the Select Targets panel. You can choose to select an individual resource, or a predefined group. The Select Network Elements window opens.

6

Search for a resource or resource group using the list and filters provided. You can filter and order the list using the column headers. Select one or more entries from the list and click **ADD.**

7

Configure the parameters in the Operation Inputs panel as required. The Advanced Inputs section allows you to configure the operation to end when certain thresholds are crossed. These can be specified separately for each phase. Click on the checkbox to enable an advanced input, and configure the value; unchecked inputs are not evaluated.

Note: When configuring an upgrade operation, the Target Software Version parameter must be in TiMOS-20.10.R2 format. The Window Size parameter should not exceed the number of nodes that are a part of the operation. The Concurrency Count parameter is applied per phase and not to the operation overall.

8

Configure the parameters in the Schedule panel to specify when to start the phases of the operation. The available options depend on the operation type chosen, and whether the operation is configured to proceed per-phase or per-target (when available). Proceeding per-

target generally supports configuring a different option for each phase of the operation, which are triggered when a target reaches that phase.

Scheduling options can include:

- To schedule the operation to start at a later time, choose **Set up the schedule** and configure the scheduling options. This option is only available for single-phase operations, excluding upgrade operations.
- To start the phase immediately, choose **Run Immediately**.
- To configure the phase to wait to be started manually, choose **Run manually.**
- To configure the phase to wait for a specified amount of time before starting, choose **Run after a delay (min)** and specify a time in minutes.

9

Perform one of the following to finish creating the operation. Enable the Create Another option to create the operation and return to the Configure Operation panel to start a new operation.

a. Click **RUN** to start the operation or add it to the schedule, as configured in the Schedule panel.

b. Click **SAVE** to save the operation as a draft. You can select saved operations in the Operation Schedules view and configure or start the operation at a later time.

END OF STEPS

4.6 How do I start or schedule a saved operation?

Tip: You can start a saved operation immediately, or schedule one to start at a later time.

4.6.1 Steps

1

Open **Device Management**, **Operation Schedules**. A list of scheduled and saved operations appears.

2

To start a saved operation immediately, choose an operation, click **More** ⋮ and select **Run**.

3

To edited a saved operation before starting, or schedule it for a later time, perform the following:

1. Choose an operation, click **More** ⋮ and select **Edit**.
2. Configure the parameters, as required.
3. To perform the operation immediately, choose **Run Immediately** in the Schedule panel.
4. To add a single-phase operation to the schedule, choose **Set up the schedule** in the Schedule panel and configure a date and time.

5. Click **RUN** to start the operation or add it to the schedule, as configured in the Schedule panel.

End of steps

4.7 How do I view or edit operation schedules?

4.7.1 Steps

1

Open **Device Management**, **Operation Schedules**. A list of scheduled operations appears.

2

Select a scheduled operation to view detailed information in the Info panel.

3

To view the network elements affected by the operation, scroll to the Included Resources section of the Operation Summary panel and click **View.**

4

To edit the operation, click **More** ⋮ and select **Edit**. The Edit Operation panel appears. You can configure or reschedule the operation, then click **Update** to save the changes.

End of steps

4.8 How do I pause an operation schedule?

4.8.1 Purpose

You can pause an operation schedule and prevent it from triggering new operations until resumed. When an operation schedule is paused, operations created from that schedule which are already in progress continue normally, while operations that have not started yet do not start until the schedule resumes.

4.8.2 Steps

1

Open **Device Management**, **Operation Schedules**. A list of scheduled operations appears.

2

Select an operation schedule to view detailed information in the Info panel.

3

To pause an operation schedule, click **More** ⋮, and select **Pause.** The operation status changes to Paused.

4

To resume the paused operation later, click **More** ⋮, and select **Resume**. The operation status changes to Scheduled, and operations start as scheduled.

End of steps

4.9 How do I view current operations and executions?

4.9.1 Steps

1

Open **Device Management**, **All Operations**. A list of current operations appears.

2

To view the details of an operation, including an overview of phases and executions, click on the operation and review the information in the Operation Summary panel.

3

To view the network elements affected by the operation, scroll to the Included Resources section of the Operation Summary panel and click **View.**

4

To view detailed information about phases and executions in an operation, click **More** ⋮, and select **View**, or click on the View button in a phase in the Operation Summary panel. The View Included Executions view appears. Phases are shown in tabs at the top of the view, and executions that are part of the selected phase appear in the list.

End of steps

4.10 How do I start, stop, or pause an operation?

4.10.1 Purpose

You can stop or pause an existing operation, and start or stop a phase within an operation. Operations can be paused manually by a user, or automatically by crossing a configured threshold (for example, percentage of failed executions). Phases that are waiting can be manually started, and a phase that is in progress can be stopped or paused. An operation that is configured to proceed per-target cannot be paused.

When an operation is paused, any executions in progress continue to completion, and no more executions are launched until the operation is started or stopped. Starting a paused operation continues the current phase.

When an operation is stopped, any executions in progress continue to completion, and any executions remaining in the phase are cancelled and marked as failed. Starting a stopped operation starts the next phase, if one exists.

4.10.2 Steps

1

Open **Device Management**, **All Operations**. A list of current and completed operations appears.

2

To pause an operation, choose an operation and click **More** ⋮, and select **Pause**. Executions already in progress continue to completion, and no more executions are started.

3

To start a phase of an operation, choose an operation and and click **More** ⋮, and select **Start next phase**; or, click **Start** in the Operation Summary panel, under the section for the next phase. You can also schedule when to start the phase by clicking **Schedule**.

4

To stop an operation in progress, choose an operation and click **More** ⋮, and select **Stop**, or select a phase in the Operation Summary panel and click **Stop**. Executions already in progress continue to completion, and any executions that have not started are marked as failed.

END OF STEPS

4.11 How do I view the details of completed operations?

4.11.1 Steps

1

Open **Device Management**, **All Operations**. A list of current and completed operations appears.

2

Select an operation from the list to view detailed information about that operation in the Info panel.

3

To view the network elements affected by the operation, scroll to the Included Resources section of the Operation Summary panel and click **View.**

4

To remove the record from the list permanently, click ⋮ (Table row actions), Delete.

5

Click ⋮ (Table row actions), View Included Executions to see the executions performed as a part of the selected operation.

6

Select an execution from the list to view information about that execution in the Info panel.

END OF STEPS

4.12 How do I view a history of operations performed on an NE?

4.12.1 Steps

1

Open **Device Management**, **Managed Network Elements.**. A list of network elements appears.

2

In the row for the NE you need to manage, click (Table row actions), Operation History. A list of operations performed on that NE appears.

END OF STEPS

4.13 How do I automate the cleanup of completed operations?

4.13.1 Purpose

You can create Operation Clean-up policies to automatically delete operations after a specified time. A policy can apply to all operations, or only operations of specific types. The default clean-up policy removes operations that are older than 30 days, triggering once a day at 07:30 am.

Note: You can create multiple policies for the same filter, but the lifecycle of duplicate policies should be closely managed. Cleanup is not applied to operations created as a part of importing node images during the nsp-ne-sw-import operation.

4.13.2 Steps

1

Open **Device Management**, **All Operations**. A list of current and completed operations appears.

2

Click on Settings. The Device Operations Settings panel appears, displaying a list of clean-up policies.

3

Create a new policy by clicking **+ Policy**, or edit an existing policy by clicking (Table row actions), **Edit**.

4

Specify a name for the policy, and click Enable Policy to make the policy active.

5

In the Operations older than (days) field, specify how old, in days, an operation must be before the policy removes the operation.

6

To restrict the policy to clean up only certain types of operations, click on the Filter (Operation types) drop-down and select operation types from the list. You can click multiple times to select multiple types.

7

Configure a schedule to specify when the policy checks the current age of all operations and performs a clean up. You can select daily, monthly, or weekly cleanups, or provide a cron expression.

8

Click Save to save the policy and close the form.

END OF STEPS

4.14 How do I view reports generated by an operation?

4.14.1 Purpose

You can view reports generated by an operation that is in progress or has been completed using the View Reports action. .

Note: Some workflows do not generate reports. The View Report action is only available if a report is available for review.

4.14.2 Steps

1

Open **Device Management**, **All Operations**. A list of current and completed operations appears.

2

Choose an operation and click **More** ⋮, and select **View Executions**. A list of executions appears.

3

Select a phase at the top of the list, choose an execution, then click **More** ⋮, and select **View Reports**. The report for the chosen execution appears.

4

For operations that generate reports for two different phases, you can compare the reports for an NE by clicking on Compare Reports in the execution summary panel. The initial and final reports appear in a differential view. Whether two reports can be compared is defined in the mapping profile for the operation; for information about developing reports, contact your service representative.

End of steps

4.15 How do I retry an execution within a phase?

4.15.1 Purpose

You can rerun executions in a paused or in-progress operation using the Rerun action, repeating the workflow for the selected targets. Only executions for the current phase can be rerun, and after a new phase has started, executions for the previous phase cannot be rerun. When you rerun an execution, the next phase cannot be started until the reruns are complete. Executions in a completed operation cannot be rerun.

4.15.2 Steps

1

Open **Device Management**, **All Operations**. A list of current and completed operations appears.

2

Choose an operation and click **More** ⋮, and select **View**. A list of executions appears.

3

Click on the chip filter for the phase containing the execution you need to retry. The list displays the executions for that phase.

4

Choose one or more executions, then click **More** ⋮, and select **Rerun**. The chosen executions are repeated from the beginning of the phase.

End of steps

4.16 How do I terminate an execution in progress?

4.16.1 Purpose

You can use the Terminate action to end an execution in progress. When an execution is terminated, the workflow ends, no further commands are processed, and the execution is placed in a failed state. You can retry a terminated execution.

Note: If the Terminate action is triggered while the final task in an execution is in progress or completing, then the execution completes normally and is not placed in a failed state.

4.16.2 Steps

1

Open **Device Management**, **All Operations**. A list of current and completed operations appears.

2

Choose an operation and click **More** ⋮, and select **View**. A list of executions appears.

3

Click on the chip filter for the phase containing the execution you need to terminate. The list displays the executions for that phase.

4

Choose an executions, then click **More** ⋮, and select **Terminate**. The chosen execution is terminated, and the state changes to failed.

END OF STEPS

4.17 How do I retry a failed operation?

4.17.1 Purpose

You can retry an operation that has one or more failed executions using the **Clone with failed executions** action. A new operation is created, targeting the nodes where the previous executions failed.

4.17.2 Steps

1

Open **Device Management**, **All Operations**. A list of current and completed operations appears.

2

Choose an operation with failed executions from the list and click **More** ⋮, then select **Clone with failed executions**. The Create Operation form appears, with the values cloned from the chosen operation.

3

Configure the Name parameter with a new name. Reconfigure other parameters as required.

4

Click **RUN** to start the operation or add it to the schedule; click **SAVE** to save the operation as a draft.

END OF STEPS

4.18 How do I perform a rollback on a target in an operation?

4.18.1 Purpose

You can trigger the rollback action on an execution in an operation, which will perform the rollback workflow defined for the operation on the target of that execution. After a rollback has been performed, the target of the rollback is marked as failed for the remainder of the operation, no further executions can be performed on the target, and previous executions cannot be retried.

Before you can perform the rollback action, a rollback workflow must be defined in the mapping file for the operation, and the rollback_allowed parameter must be true. When you perform a rollback on an execution in a completed phase, the phase enters the in-progress state, and other phases cannot start until the rollback is complete.

Some operations can be configured to automatically perform a rollback on failed targets, using the Rollback Type setting. Automatic rollback is only available for operations with the rollback_type parameter in the mapping file for the operation configured to automatic. Not all operations support automatic rollback. Contact a Nokia support representative for assistance with modifying an operation to use automatic rollback.

4.18.2 Steps

1

Open **Device Management**, **All Operations**. A list of current and completed operations appears.

2

Choose an operation and click **More** ⋮, and select **View**. A list of executions appears.

3

Click on the chip filter for the phase containing the execution you need to rollback. The list displays the executions for that phase.

4

Choose one or more executions, then click **More** ⋮, and select **Rollback**. The chosen executions are placed in an in-progress state, and the rollback workflow defined in the operation is performed on the chosen targets.

END OF STEPS

Troubleshooting

4.19 Operation troubleshooting

4.19.1 All Operations view

The All Operations view displays information about operations at every stage, whether ready, paused, in progress, or complete. In the event that an operation encounters problems, there are actions you can perform to investigate or manage troubled operations:

- **View current operations**. Operations that require attention or have encountered errors are marked in the All Operations view. See 4.9 “How do I view current operations and executions?” (p. 63).
- **View details of completed operations.** Completed operations remain in the All Operations view until deleted. See 4.11 “How do I view the details of completed operations?” (p. 64).
- **View reports generated by executions.** Some operations generate reports during certain phases. See 4.14 “How do I view reports generated by an operation?” (p. 66).
- **Retry failed executions.** You can re-run some executions in the most recent phase of an operation. Executions from previous phases cannot be re-run after the operation has moved to a new phase. See 4.15 “How do I retry an execution within a phase?” (p. 67).
- **Retry failed operations.** You can retry an operation, creating a new operation of the same type that targets elements that failed the original operation. See 4.17 “How do I retry a failed operation?” (p. 68).
- **Rollback a phase.** Some phases in an operation can be rolled back, depending on whether a rollback workflow exists for that phase. See 4.18 “How do I perform a rollback on a target in an operation?” (p. 69).

5 NE software upgrades using NSP

NE software upgrades using NSP

5.1 Upgrade operation requirements

5.1.1 Prerequisites

Performing an upgrade operation on an NE requires the fulfillment of certain prerequisites, depending on the NE configuration and management. Before you perform an NE upgrade operation, you must import an NE software image; see 5.3 “How do I import an NE software image?” (p. 75). NE software images can be downloaded from the Nokia Support Portal for the NE type and release.

For NEs managed using MDM, the adaptors for the new software version must be present on the NSP; see “How do I install adaptor artifacts that are not supported in the Artifacts view?” in the *NSP System Administrator Guide*.

The following additional general requirements apply to all upgrades:

- each node must have a unique NE Name identifier; backup or restore operations may fail if the NE Name of the target is shared with any other node in the NSP
- do not delete NE software images from the NSP during an upgrade operation
- both primary and secondary images should be stored on the same flash drive number (for example, cf3 or cf1)
- bof.cfg should be stored on the same cf where the primary image is stored
- backout files are stored locally on the NE, and are required if an upgrade fails
- pre-check removes images not referenced in the BOF configuration. If insufficient space is freed up, the upgrade cannot proceed.
- tertiary images are not supported
- the primary image cannot be set to a remote FTP location in the BOF configuration

An upgrade operation can fail if a workflow task times out, for example fetching upgrade status or validating downloads and CPM synchronization. You may need to customize the upgrade workflow for your network; see the *NSP Network Automation Guide* for information about modifying workflows.

ISSU upgrade path limitations

Before performing an upgrade operation, consult the NE documentation to confirm that the upgrade you need to perform is supported on that NE. For example, a 7750 NE only supports upgrades to releases one or two major releases later than the current release: from Release 21.x to Release 22.x or 23.x, but not to Release 24.x or later.

NSP classically-managed NEs

You can use the NSP to upgrade NEs managed through NSP Classic mediation using a classic mediation policy and the unified discovery rule. The following requirements apply:

- The upgrade image must be imported into the NFM-P. See the *Classic Management User Guide*.
- Both CLI Telnet/SSH and FTP/SFTP mediation must be configured for the target NEs. For classically-managed nodes, classic-cli must be enabled first, then md-cli if applicable. For nodes using mixed management, md-cli must be enabled first, then classic-cli.
- NFM-P upgrade policies should have the Validate Disk Space parameter enabled. The upgrade policy used by the upgrade operation is specified in the operation mapping file.
- Confirm that the components installed on the node support the planned upgrade. When you perform an upgrade operation on a 7x50, 7210 SAS, or 7705 SAR NE that is managed using NSP Classic Management, the NSP does not check for deprecated or unsupported components (for example, switch fabric cards or ethernet satellites).

5.2 Pathway: NE upgrade

5.2.1 Stages

1

Verify the management type for the NE. See the Prerequisites section for information about differing requirements.

For SR OS device commissioning information, see the Management Interface Protocol Configuration section in the adaptor artifact guide. For additional information if needed, see the NE documentation.

2

Import NE software images as needed; see 5.3 “How do I import an NE software image?” (p. 75).

3

Start the upgrade operation; see 4.5 “How do I start or schedule a new operation?” (p. 59)

4

View the operation in the Operations tab to monitor it; see 4.9 “How do I view current operations and executions?” (p. 63).

5

You can stop or pause an existing operation, and start or stop a phase within an operation. Operations can be paused manually by a user, or automatically by crossing a configured threshold (for example, percentage of failed executions). Phases that are waiting can be manually started, and a phase that is in progress can be stopped or paused.

- Pause: Executions already in progress continue to completion, and no more executions are started. The operation remains in the All Operations view, and can be unpaused using the Resume action.
- Stop: Executions already in progress continue to completion, and any executions that have not started are marked as failed.

See 4.10 “How do I start, stop, or pause an operation?” (p. 63).

6

When the upgrade is complete, the NE reboots and raises a reboot alarm. The reboot alarm triggers an NE-specific discovery scan. When the discovery scan detects a version change, the NE information is updated.

7

After the upgrade is complete, you can check the History list to verify success, troubleshoot failures, or check schedules for future operations. See 4.11 “How do I view the details of completed operations?” (p. 64)

8

To perform a rollback, see 4.18 “How do I perform a rollback on a target in an operation?” (p. 69).

5.3 How do I import an NE software image?

5.3.1 Purpose

You can upload a NE software image to use in upgrade operations for supported NEs.

Note: For 7x50 image import, the software bundle name and contents must not be modified after downloading it from the Nokia support page.

5.3.2 Steps

1

Open **Device Management**, **Node Images**.

2

Click **Import**. The Import Node Software Images form opens.

3

Specify the image name, the product type, and the md5 checksum for the software image. The md5 checksum for an image is displayed on the Nokia support page where the file was downloaded.

4

Drag and drop the node software image file into the Software Bundle field, or click browse to select the file in a file browser.

5

Click **Import** to upload the node software image to the NSP.

END OF STEPS

5.4 How do I upgrade software on a 7750 SR NE?

5.4.1 Purpose

This procedure shows the process of upgrading software on an MDM-managed 7750 SR NE. Before performing this procedure, verify that the NE to be upgraded is reachable, and that adaptors for the new software version are installed on the NSP.

Nokia recommends using the nsp-ne-upgrade-with-phases operation type to upgrade a 7750 SR. When you create an operation with this operation type and NE type, the parameter values are provided as input for the upgrade workflow. NSP monitors the status of workflow executions.

Note: Scale limits apply for number of concurrent executions and number of targets per operation; see Scale limits for large-scale operations in the *NSP Planning Guide*.

The following table shows the general process for this example procedure.

Phase	Workflow	Process
Pre-checks	`LSO_7x50_Pre_Checks`	• Checks current software version: if the update is already done, no workflow is called • Checks the BOF • Checks on CPM redundancy • Checks availability of adaptors and supported equipment • Checks for deprecated cards and MDAs on the node • Retrieves details of the target software image • Runs a cleanup of stale images on the the /images/ folder
Download	`LSO_7x50__Download`	• Reads and processes the BOF • Creates a directory on the NE and transfers the image files • Confirms the file integrity and sends a success message

Phase	Workflow	Process
Activate	`LSO_7x50__Activate`	• Saves the updated configuration on the NE and performs an admin save • Synchronizes the CPM • Resets redundancy settings as needed and sends a success message
Reboot	`LSO_7x50_Reboot`	• Checks BOF instructions for reboot and CPM redundancy requirements • Processes redundancy • Triggers a reboot and checks the device version. • Sends a success message.

5.4.2 Steps

1

Perform 5.3 “How do I import an NE software image?” (p. 75).

2

Open **Device Management**, **All Operations**.

3

Click **+ OPERATION**.

4

In the form that opens, click **+ OPERATION TYPE**.

5

In the Select an Operation Type form, choose **nsp-ne-upgrade-with-phases** and click **ADD**.

Fields required for the operation appear in the Operation Inputs panel.

6

In the General panel, enter a name for the operation and an optional description, and configure Operation Control.

You can identify the operation by the name you enter.

7

In the Select Targets panel, click **+ SELECT**, Resources, Network Elements.

8

In the Select Network Elements form, choose one or more NEs to add them to the Bin on the right of the form.

Use the fields above the list of NEs to filter the list as needed.

9

Click **ADD**. The NEs you selected appear in the Select Targets panel.

You can change the list of selected targets if needed:

- Click **+ SELECT** to reopen the Select Network Elements form and add additional NEs.
- Choose an NE and click (Delete) to remove the NE from the list of targets.
- Click **CLEAR** to clear the list.

10

In the Operation Inputs panel, configure the mandatory parameters:

Parameter	Description
Target Software Version	Specifies the node software version you are upgrading to. For a 7750 SR NE, the format of the software version must be must be TiMOS-xx.yy.Rz, for example, TiMOS-21.5.R1.
Is ISSU	Specifies whether the upgrade operation is an in service software upgrade.
Auto Cleanup	Specifies whether automatic flash cleanup should be performed on the NE as part of the operation.
Free Space Post Upgrade (Enter a Number)	Specifies the expected free disk space after upgrade, as a percentage. Enter a number.

11

Configure the Advanced Inputs as needed:

Parameter	Description
Window Size Failure Threshold	These two parameters work together to define an automatic stopping point for the operation due to failed workflow executions: • Window size specifies the sample size to use when calculating whether a threshold has been crossed. • Failure threshold specifies the percentage of executions failed that will trigger the automatic stop. For example, with a window size of 200 and a failure threshold of 50%, the operation will automatically stop after 100 failed executions. The phase and operation are paused and any not-started executions remain in not-started status.

Parameter	Description
The following parameters can be configured separately for each phase of the operation: pre-checks, software download, software activation, and NE reboot or CMP switchover.	
• Concurrency Count • Phase Timeout (minutes) • Average Execution Threshold (minutes)	These parameters specify how the workflow executions will be managed. The pre-check steps themselves are defined in the applicable workflow. • Concurrency Count: maximum number of executions to run concurrently • Phase Timeout and Average Execution Threshold: if these parameters are configured, the operation automatically stops after the specified time. The phase and operation are paused and any not-started executions remain in not-started status.

12

If you selected Per Target execution for Operation Control in the General panel, configure phase execution scheduling in the View/Edit Schedule panel. You can specify for each phase what happens when a target reaches that phase.

13

Perform one of the following to finished creating the operation.

a. To start the operation immediately, click **RUN**. The operation appears in the All Operations view and begins executing the first phase.

b. To save the operation for later, click **SAVE**. The operation appears in the Operation Schedules view, and you can configure or start the operation at a later time.

END OF STEPS

6 Zero Touch Provisioning

6.1 What is Zero Touch Provisioning?

6.1.1 Zero Touch Provisioning

Zero Touch Provisioning (ZTP) is an SR OS feature that automatically configures a node by obtaining the required information from the network and provisioning the device with minimal manual intervention and configuration. When new devices that support ZTP are connected and boot up, the device is auto-provisioned.

Note: ZTP is not supported over IPv6.

For more information about ZTP and the specific devices on which it is supported, see the ZTP information in the device documentation: *Nokia 7450 Ethernet Services Switch, 7750 Service Router, 7950 Extensible Routing System, and Virtualized Service Router Basic System Configuration Guide.*

RESTCONF APIs are also available for ZTP; see the API documentation on the Network Developer Portal.

NSP Zero Touch Provisioning provides tools to generate ZTP files for device provisioning, and adds device information to discovery rules, reducing manual work required for device discovery.

ZTP NE details can be exported from NSP in JSON format. The exported data can facilitate the automation of the DHCP server configuration.

NSP uses the following intent types to facilitate ZTP:

- create_http_user: creates a user identity to connect with the NSP file server
  Note: creation of an HTTP user is a one time operation. Only one HTTP user is supported.
- ztp-profile: saves a set of NE information and discovery information that can be applied to multiple devices. For example, you can create a profile for MDM managed 7250 IXR devices and one for classically managed 7250 IXR devices.
  Create a ZTP profile for each set of generic parameters you need.
- day-0-ztp: takes the parameters provided in a ZTP profile and parameters that are unique to a device and creates configuration and provisioning files for the device on the NSP file server.
  Create a Day-0 intent for each device.

When the intents have been executed, the device is added to the list in the **Device Management**, **ZTP Process list** view. The device can then be powered on and discovery can be initiated.

The ZTP process list can be cleaned up using a workflow.

Important! NSP Zero Touch Provisioning has been tested with 7250 IXR-e, 7250 IXR-s and 7750 SR 14s NEs. Contact Nokia for assistance in using ZTP with any other NE type.

ZTP performed on certain releases of SR OS may fail due to an HTTP chunking issue. The affected SR OS releases are 21.2 R1-R2, 21.5 R1-R2, 21.7 R1-R2, 20.10 R3-R10 21.10 R1-R3 and 22.2 R1-R2.

6.1.2 NSP ZTP Prerequisites

NSP ZTP requires the following prerequisites:

- Prerequisites for device ZTP must be in place; see the NE documentation.
- The ZTP intents zip files must be downloaded from the Nokia NSP software download site.
- An HTTP user must be created using the create_http_user intent type; see 6.2 “How do I configure Zero Touch Provisioning?” (p. 83).
- A unified discovery rule for the NE must be created in NSP. The administrative state of the unified discovery rule must be Down.
- For classic devices, a classic discovery rule for the NE must be created in NSP and associated to the unified discovery rule. The administrative state of the classic discovery rule must be Down.
- If you plan to upgrade your device as part of the ZTP process, for example if you purchased a device with Release 20.7 software and want to use it with Release 20.10, you must import the new software image to the NSP file server before performing ZTP. If you do this, you can configure the new target software version as part of the ZTP profile intent.

  See the 5.3 “How do I import an NE software image?” (p. 75).
- If you plan to use an IP resource pool for IP address assignment, the IP resource pool must be created in NSP.

  See the *NSP System Administrator Guide* for information about using IP resource pools. Also see the Resource Administration tutorial on the Network Developer Portal.

6.1.3 Process

Figure 6-1, “Zero Touch Provisioning process” (p. 83) shows the ZTP process with NSP.

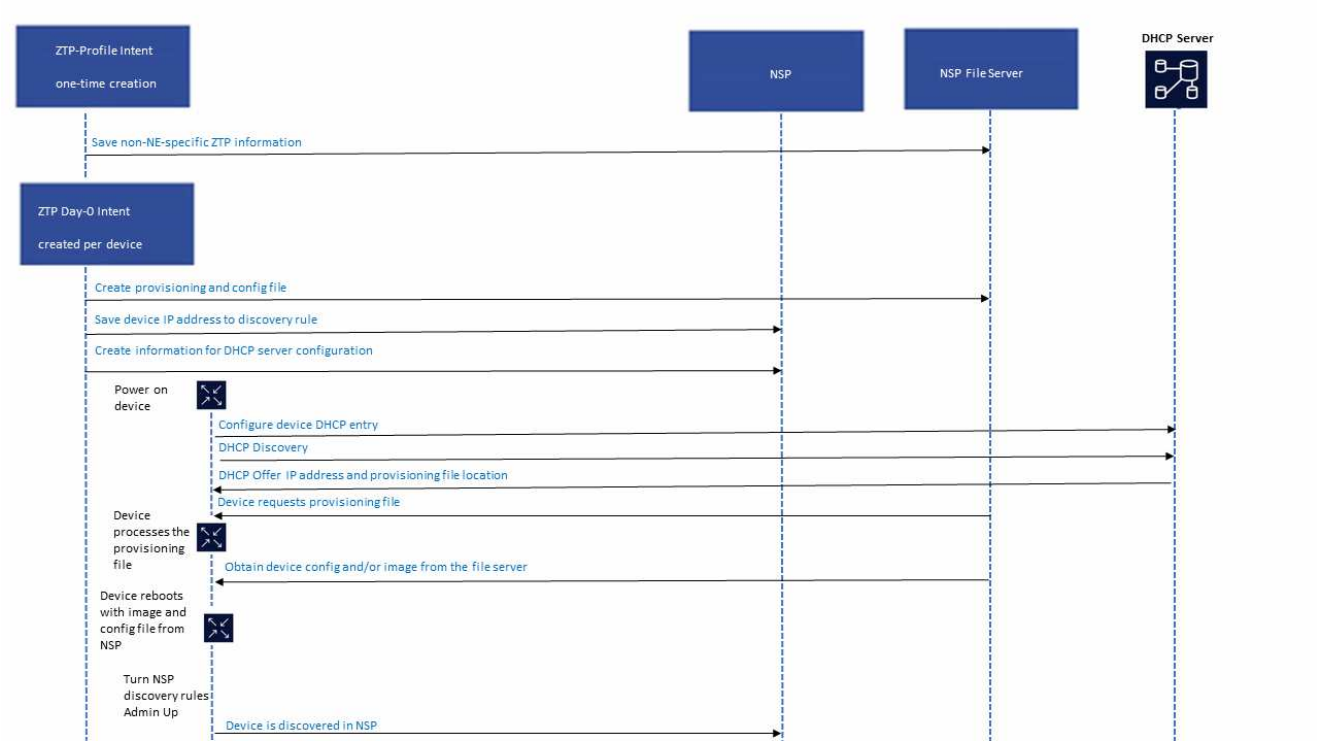
When the ZTP Day-0 intent is created and synchronized:

- Configuration and provisioning files are created and stored on the file server
- Paths and filenames for the configuration and provisioning files are saved to the database
- Device IP addresses is added to the relevant discovery rules
- The device is added to the list of ZTP Process network elements in NSP.

If all ZTP intents are synchronized, the operator turns up the discovery rule and powers on the node. The node completes ZTP and reboots.

After rebooting, MDM managed devices are ready to manage. For classic devices, a setting must be changed in CLI to prepare the device for discovery; see 6.2 “How do I configure Zero Touch Provisioning?” (p. 83).

Figure 6-1 Zero Touch Provisioning process



6.2 How do I configure Zero Touch Provisioning?

6.2.1 Before you begin

This procedure requires the use of multiple functions within NSP. For complete configuration details, you may need to consult the following documents:

- *NSP Network Automation Guide*
- *NSP System Administrator Guide*
- NE documentation: *Nokia 7450 Ethernet Services Switch, 7750 Service Router, 7950 Extensible Routing System, and Virtualized Service Router Basic System Configuration Guide*

6.2.2 Steps

Import intent types

1

Download the ZTP zip file to your computer.

Three intent types are included in the zip file: create_http_user, ztp-profile, and day-0-ztp.

2

Import the intent types to NSP:

1. Open **Network Intents**, **Intent Types**.
2. Click **Import**.
3. In the form that opens, navigate to the file you want and click Open.

3

Evaluate and update the day-0-ztp intent type to ensure that it will generate the correct information in the provisioning and day-0 config files.

The primary image file in the bof portion of the provisioning file generated from the intent type must match the information on the compact flash of the device.

Contact Nokia for assistance with this step.

Create an HTTP user

4

An HTTP user is required to connect to the NSP file server. This step only needs to be performed once.

The file server only supports one HTTP User.

In **Network Intents**, **Intent Types**, select the create_http_user intent type and click ⋮ (Table row actions), **Create Intent**.

5

In the form that opens, configure the parameters and click **Create**.

Create at least one ZTP profile

6

A ZTP profile contains template values that can apply to multiple devices.

In **Network Intents**, **Intent Types**, select the ztp-profile intent type and click ⋮ (Table row actions), **Create Intent**.

7

In the form that opens, configure the required parameters:

- Choose the NE Type.
- Choose the management mode: classic or model driven.
- Choose the management connection, for example, in-band.
  For model-driven management, only in-band and out-of-band are available.

For classic management, the drop-down includes in-band, out-of-band, and in-band-embedded-config. With in-band-embedded-config, the day-0 configuration parameters will be part of the provisioning file. Embedded configuration is only available with supported releases of the 7250 IXR.

- Choose a discovery rule.

8

Configure additional parameters as needed.

Attention: Static routes are only supported with the out-of-band management connection type.

9

Click **Create.**

The ZTP profile is now available.

10

Create additional ZTP profiles as needed for each set of device parameters.

Create a ZTP intent for each device you want to provision

11

The ZTP intent will create the provisioning and configuration files.

In **Network Intents**, **Intent Types**, select the day-0-ztp intent type and click ⋮ (Table row actions), **Create Intent**.

12

In the form that opens, configure the parameters:

- Enter the DHCP client address for the NE in the ZTP ID field
- Choose the ZTP profile to apply the template values
- Enter a unique NE name.
- Configure the System and Management IP addresses. Enter the IP addresses manually or choose IP Resource Pool for automated IP address assignment. IP resource pools can be created in the Resource Manager menu.

  Note: The System IP address and Management IP address must be different.

13

Click **Create**.

The provisioning and configuration files are created and a new rule element is added to the relevant discovery rule.

14

Verify and update the day–0 configuration and provisioning files to match network settings, NE card type and port settings. Contact Nokia for assistance.

Verify the information and discover the device

15

Open **Device Management**, **ZTP Process** from the drop-down.

The list of devices for which ZTP is configured is displayed.

16

Click on an NE to see the details.

17

Click **Export** to save the NE information to a JSON file if needed.

18

Power on the device.

The device completes ZTP and reboots. The discovery status in the **ZTP Process** list is updated.

19

In the **Device Discovery** view, set the unified and, if applicable, the classic discovery rules Admin State to Up to initiate device discovery.

Configure cleanup of the ZTP Process list

20

Import the ZTP_Purge_Workflow and ZTP_Artifacts_Cleanup workflows from the ZTP zip file into NSP.

21

Open **Workflows**, **All Workflows**.

22

Choose ZTP_Purge_Workflow.

Note: The ZTP_Purge_Workflow runs ZTP_Artifacts_Cleanup during its operation. Both workflows must be present in NSP.

23

From the menu at the end of the row, choose **More** ⋮ **Execute**.

24

Update the retentionDays parameter as needed and click **Execute**.

The cleanup removes NEs with Success status from the ZTP Process NEs list that have been discovered longer than the configured number of days.

25

Schedule execution of the ZTP_Purge_Workflow for automated cleanup if needed; see “How do I schedule a workflow?” in the *NSP Network Automation Guide*.

END OF STEPS

6.3 Can I change ZTP parameters from NSP?

6.3.1 ZTP list is read-only

No: the ZTP Process list is read-only. If you find an error, change the configuration in the intent type.

To remove NEs from the ZTP list, open **Device Management**, **ZTP Process**, choose one or more NEs, and click **Delete** .

To delete the configuration files, open **Network Intents**, **Intent Types**, and delete the intents created for the device.

Note: ZTP profiles can be changed by editing the ZTP profile intent. If you have changed a ZTP profile you must resync the day-0-ztp intents that use the profile to apply the changes. If you do not resync the intents, the ZTP profile changes are not applied.

Part III: Device configuration

Overview

Purpose

Provides overview and procedures for configuring devices using NSP.

Contents

7 NE inventory

7.1 How do I see what is configured on an NE?

7.1.1 NE inventory view

The NE Inventory view is one of the primary ways to see what is configured on an NE. Configured NE objects are displayed in the NE Inventory view in a graphical tree format.

To open the NE Inventory view from Device Management, select an NE from the **Device Management**, **Managed Network Elements** list and click ⋮ (Table row actions), **View NE Inventory**. The NE inventory tree view opens in a new browser tab.

NE child objects are displayed in an expandable/collapsible hierarchy. Click on an inventory object to show object properties in the Information panel.

NE inventory information is also available using RESTCONF APIs; see the Network Inventory RESTCONF APIs documentation on the Network Developer Portal.

7.1.2 Configured Attributes view in Model Driven Configurator

Another way to see NE configuration is to view the model details in Model Driven Configurator. Open the Model Driven Configurator view for the NE to see the parameters defined in the NE adaptation schema.

NE parameters are displayed using a tree structure, derived from the YANG model of the NE. The schema trees displayed vary based on the NE adaptors that are installed. For example, the 7750 SR device supports nokia-conf, nokia-state and openconfig models. The state schema is read-only.

Choose Configured Attributes View from the drop-down list at the top of the page to view only the configured parameters on the NE. Choose All Attributes View to view all of the available parameters, including parameters with default values.

7.2 What can I see in the NE Inventory view?

7.2.1 NE child objects

The NE Inventory view shows a tree structure of individual inventory objects (child objects). Object names and basic administrative and operational state information are displayed. The color of an inventory object indicates its state.

NE inventory information is grouped by type of object:

- Equipment inventory: objects configured on the NE, such as shelves, cards, and ports, are grouped in the inventory view as an Equipment Group.

  If an Extended Services Appliance (ESA) is configured on a model-driven NE, an ESA group appears in the Equipment Group, showing all configured ESAs with their VMs and virtual ports.
- Logical inventory: if applicable, supported logical entities such as LAGs and routing instances are also displayed, grouped as a Logical Group. The Logical Group appears below the Equipment Group in the inventory tree.

The inventory details available in NSP depend on adaptor artifacts installed, NSP installation options and managed NE configuration:

- the Logical inventory tree requires the networkInfrastructureManagement-basicManagement installation option
- Device Configuration options for ports require the networkInfrastructureManagement-deviceConfig installation option

7.2.2 Available equipment objects

The following object types are supported in the Equipment Group. The hierarchy depends on the NE type.

- Shelf
- Card
- Port
- Module
- Fan
- Power Supply
- Radio
- Radio Folder
- Extended Services Appliance
- VM (virtual machine)
- Virtual Port

7.2.3 Available logical objects

The following object types are supported in the Logical Group:

- Link Aggregation Groups
  - MC LAGs
- Routing Instances
  - Routers
    - - Interfaces
    - - - IPv4 Addresses
    - - - IPv6 Addresses
    - - BGP Instances
    - - - BGP Peer Groups
    - - - - BGP Peers
    - - OSPFv2 Instances
    - - - OSPFv2 Areas
    - - - - OSPFv2 Interfaces
    - - - - - OSPFv2 Neighbors
    - - - - OSPFv2 Sham Links
    - - - - OSPFv2 Virtual Links
    - - OSPFv3 Instances
    - - - OSPFv3 Areas
    - - - - OSPFv3 Interfaces
    - - - - - OSPFv3 Neighbors
    - - - - OSPFv3 Virtual Links

- - ISIS Instances
- - - ISIS Levels
- - - ISIS Interfaces
- - PIM Instances
- - - PIM Rendezvous Points
- - - PIM Interfaces
- - MPLS
- - - MPLS Instances
- - - MPLS Interfaces
- - RSVP
- - - RSVP Interfaces
- - - RSVP Neighbors
- - LDP
- - - LDP Instances
- - - LDP Interfaces
- - - LDP Neighbors

  − L3 Routing Instances
  - - BGP Peer Groups
  - - - BGP Peers
  - - OSPFv2 Instances
  - - - OSPFv2 Areas
  - - - - OSPFv2 Interfaces
  - - - - - OSPFv2 Neighbors
  - - - - OSPFv2 Sham Links
  - - - - OSPFv2 Virtual Links
  - - OSPFv3 Instances
  - - - OSPFv3 Areas
  - - - - OSPFv3 Interfaces
  - - - - - OSPFv3 Neighbors
  - - - - OSPFv3 Virtual links
  - - ISIS Instances
  - - - ISIS Levels
  - - - ISIS Interfaces
  - - PIM Instances
  - - - PIM Rendezvous Points
  - - - PIM Interfaces

- ACL Sets
  − ACL v4 Sets
  - - ACL v4 Entries
  − ACL v6 Sets
  - - ACL v6 Entries
  − ACL L2 Sets

- - ACL L2 Entries

- BFD
  - BFD Templates
  - BFD Reflectors

7.2.4 Filtering object lists

At the top of the NE Inventory view, choose Equipment type filters or Logical type filters, click (Add filter) to choose filter criteria, and click **APPLY FILTERS**. When a filter is applied, objects that don't match the filter are dimmed.

Note: If you filter on Ports, virtual ports are included in the results if present.

You can apply type filters, state filters, or a combination, for example, cards with operational state enabled.

Equipment type filters

The following equipment type filters are supported:

- Shelf
- Slot
- Card
- Port
- Module
- Fan
- Power Supply
- Rack
- Radio

Choose an equipment type from the drop-down list. The default filtering logic is All, for example, all shelves. Click on a type to refine the filter, for example, to add a number.

Logical type filters

The following logical type filters are supported. Choose a type filter and click (Add filter) again to add a sub-type filter, for example, to filter by interface, choose Router, add another filter, and choose Interface. Click on a type or sub-type to refine the filter, for example, to add a number.

- Router
  - Interface
  - IPv4 Address
  - IPv6 Address
  - BGP Instance
  - OSPFv2 Interface
  - OSPFv2 Neighbor
  - OSPFv3 Interface
  - OSPFv3 Neighbor

  - MPLS Interface
  - LDP Interface
- L3 Routing Instance
  - L3 Routing Instance
  - BGP Instance
  - OSPFv2 Interface
  - OSPFv2 Neighbor
  - OSPFv3 Interface
  - OSPFv3 Neighbor
- LAG
- LAG Port
- MC LAG Peer
- MC Lag

State filters

You can add filters for Operational State, Administrative State, and, for ports, Configuration Deployment Status. Add a type filter, then choose a state from the drop-down list. Available criteria depends on the filter types.

7.2.5 Expanding object lists

In the equipment inventory tree, you can select an inventory object and click ⋮ to open the tree item actions menu.

From the Equipment Group object, you can expand or export all objects in the equipment group:

- **Expand all**: shows all objects in the equipment inventory tree.
- **Export all**: download a file to your local computer, containing the equipment inventory of the NE. The export file is in .xlsx format, with a sheet for each object type configured on the NE.

  For example, if there are ports configured, the export file includes a sheet called ports, populated with the ports and their properties.
- **Export filtered**: this action is available if a filter is applied in the NE Inventory view. The export filtered option allows you to download an inventory file of the filtered data.

From any other equipment object, **Expand all** shows all child objects of the selected object.

7.2.6 Accessing related views

Select an inventory object and click ⋮ to open the tree item actions menu. Options in the tree item actions menu depend on the object. The following table lists the commands available for various objects, and the NSP view that opens for each command.

The Configure commands allow you to perform device configuration actions on ports from the NE Inventory tree. See Chapter 9, “Network configuration” for more information about the Device Configuration views.

Table 7-1 Action options from NE Inventory objects

Menu option	Action	Available for objects
Open in Current Alarms	Opens Current Alarms List	NE, Port
Open object	Opens Model Driven Configurator, filtered to the object.	Any equipment object on a model-driven NE
Open NE Session	Opens a CLI session	NE
Plot Utilization Statistics	Opens a new chart of utilization statistics for the port in Data Collection and Analysis Visualizations, with default parameters selected See “How do I plot a telemetry chart?” in the *NSP Data Collection and Analysis Guide* for information about changing the chart configuration.	Port
Show in Event Timeline	Object Troubleshooting event timeline, filtered to the NE	NE
Configure		
Configure, Deploy[1]	Opens a Deploy Physical Configuration form with the port selected as a target. See 9.25 “How do I create a physical configuration deployment?” (p. 140) to create the deployment. The Configuration Deployment Status is displayed for the port when the deployment process completes.	Ports with no Configuration Deployment Status These ports are not a target of a configuration deployment.
Configure, Retry deployment[1]	Retries the failed deployment. This option does not open a form, however, you can check the process of the retry operation in Device Management. The Configuration Deployment Status is displayed for the port when the deployment process completes.	Ports with a Configuration Deployment Status of Deployment Failed
Configure, Associate[1]	Opens an Associate Template form with the port selected as a target. See 9.16 “How do I associate a physical template to the network? ” (p. 132) to create the deployment. The Configuration Deployment Status is displayed for the port when the deployment process completes.	Ports with no Configuration Deployment Status These ports are not a target of a configuration deployment.
Configure, Retry association[1]	Retries the failed association. This option does not open a form, however, you can check the process of the retry operation in Device Management. The Configuration Deployment Status is displayed for the port when the deployment process completes.	Ports with a Configuration Deployment Status of Association Failed

Table 7-1 Action options from NE Inventory objects (continued)

Menu option	Action	Available for objects
Configure, Edit	Opens a Deploy Physical Configuration form. Click **EDIT TEMPLATE CONFIG** to change the parameters, and click **DEPLOY** to deploy the updated parameters to the port.	Ports with a Configuration Deployment Status These ports are a target of at least one configuration deployment.
Configure, Audit	Launches an audit operation on the deployment in Device Configuration. An audit checks whether the target configuration matches the template, but does not change the target configuration. Click CONTINUE to launch the operation. Open the **Device Management**, **Configuration Deployments** view to see the progress and status.	
Configure, Align	Launches an align operation on the deployment in Device Configuration. An align operation updates the target configuration if it does not match the configuration template. Click CONTINUE to launch the operation. Open the **Device Management**, **Configuration Deployments** view to see the progress and status.	
Configure, Open config deployment	Opens the **Device Management**, **Configuration Deployments** view, filtered to show the deployments on the port.	

Notes:

1. Both the Deploy and Associate actions create a configuration deployment in the **Device Management**, **Configuration Deployments** view. Deploy overwrites target parameter values with template values if a mismatch is found; associate does not. See 9.8 “What is the difference between deploying a template and associating a template?” (p. 126) for details.

If an option in the object tree item actions menu is dimmed, the action is not available.

If this occurs, check the following:

- adaptors:
  - MDC adaptors must be present for the NE for Model Driven Configurator to be opened
  - an alarm adaptor must be present for NSP to display alarms
  - telemetry mappings must be present to plot statistics
- Mediation: for NE session, a CLI mediation policy must be configured in the discovery rule used to manage the NE.

If the problem persists, contact Nokia support.

8 Device object configuration

8.1 What tools can I use to configure NEs in NSP?

8.1.1 Configuration tools

The following table describes functions within NSP that can be used to perform configuration tasks.

Function	Description	Path in NSP	Documentation reference
Model Driven Configurator	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.	**Model Driven Configurator**	This chapter RESTCONF APIs are also available for MDM managed NEs; see the Device Configuration API documentation on the Network Developer Portal. **Note:** APIs for NE management are derived from the NE model and evolve with NE versions. See the NE model and NE documentation for updates about NE model changes that may affect the APIs.
Configuration	In the Configuration views, you can define reusable configuration templates covering physical configurations such as cards and ports, and logical configurations such as QoS. These templates can be deployed to the network with fixed or flexible attributes.	**Device Management**, **Configuration Deployments**	Chapter 9, “Network configuration”

Function	Description	Path in NSP	Documentation reference
Operations	An operation is a series of executions, organized in phases, which are performed on a scope of NEs. You can use an operation to perform executions on large numbers of NEs concurrently; for example, upgrading all SR NEs in a network to the latest SR OS release.	**Device Management**, **All Operations**	Chapter 4, “Operations”
Service Management	Service Management allows for service provisioning and activation across networks accessible to the NSP, enabling users to make service requests that deploy services to the network using the NSP’s mediation framework. A library exists with a predefined set of service models for both classic and model-mode SR OS networks. These service models can be installed and utilized by NSP to provide assurance that service configuration is as planned/requested, and also provides adaptability for custom service model requests.	**Service Management**, **Service List**	*NSP Service Management Guide*

8.2 How do I open a device for configuration?

8.2.1 Steps

1

To open a specified NE object:

1. Open **Device Management**, **Managed Network Elements**.
2. Select an NE and click ⋮ (Table row actions), **Open inventory**. The NE inventory tree view opens in a new browser tab.
3. Select an object in the inventory tree and click and click ⋮ **Open object**

The Configured Attributes view for the object opens in a new browser tab.

2

To navigate to an NE schema from the main menu:

1. Open **Model Driven Configurator**.
2. Click in the **Search for a Network Element** field.

   Enter search terms in the filter fields at the top of the page to find a specific NE using NE ID, NE Name, Node Type, or Version.
3. Double-click on an NE. A list of available schemas for the NE appears.
4. Click on a schema in the list to view the specific attributes of the schema.

END OF STEPS

8.3 How do I configure device objects?

8.3.1 Configuring model-driven NE parameters

Use this procedure to configure parameters on a model-driven NE.

Note: The **Refresh** icon fetches the latest values from the NE. The schema views do not automatically refresh.

Note: Mandatory fields have an asterisk (*) next to the attribute name.

8.3.2 Config basket

The config basket lets you create a list of configuration changes and submit multiple changes at the same time.

The config basket displays the list of changes, with links to the schema where the changes will be made. You can validate, cancel, or submit the changes, or click the link to return to the schema and edit the change. From the config basket, click **CONTINUE EDITING** to return to the schema.

The following restrictions apply.

- The config basket can only be used for one NE at a time. Changes cannot be pushed from the config basket to multiple NEs.
- If two YANG models are supported by the same adaptor, changes to both can be submitted at the same time.
- The config basket contents are only populated for the duration of the session; they cannot be saved for later use.

8.3.3 Steps

1

Navigate to the configuration schema; perform 8.2 “How do I open a device for configuration?” (p. 100).

2

Navigate through the branches of the schema to the object you want to configure.

To navigate to a previous configuration window, click on the object in the **Root** path.

3

To create an object:

1. Click **CREATE** *object* and configure the applicable parameters.

   where *object* is the object type you want to create.

2. Once the object instance parameters are configured, click **ADD TO CONFIG BASKET**.

   The newly created object is added to the config basket. It appears in the list marked with a change bar; however, it is not yet committed.

4

To modify an object:

1. Configure the required parameters in the branch you navigated to.

   The change is marked by a white bullet.

2. Click **ADD TO CONFIG BASKET**.

   Your configured changes are added to the list in the config basket. The bullet marking the change becomes a solid bullet.

3. If required, navigate to another branch and add additional changes to the config basket.

5

To delete an object:

Select the object and click **Delete** . The deletion is added to the config basket.

The change is marked by a red change bar.

6

Click **CONFIG BASKET** to review your list of changes.

Click **Delete** to remove a change from the config basket if needed.

7

To update your changes:

a. To return to the last branch you viewed and make further changes, click **CONTINUE EDITING**.

b. To remove a change, select a change from the list and click **Delete** .

c. To modify a change, delete it, click **CONTINUE EDITING**, and make the change again with the new value.

8

Click **VALIDATE**.

If validation fails:

1. Delete the failed change from the config basket.

2. Click **CONTINUE EDITING** to return to the branch.
3. Make your change again, click **CONFIG BASKET**, and validate again.

9

Click **SUBMIT** to commit the changes in the config basket.

END OF STEPS

9 Network configuration

Template-based configuration deployment

9.1 What is device configuration in NSP?

9.1.1 NSP Device Configuration

Device Configuration helps to define and deploy infrastructure configurations to an NSP managed network. With Device Configuration, the network engineer can easily define reusable configuration templates covering such areas as card, port, QoS, security, and routing policy configurations. Device Configuration is found in Device Management, in the Configuration views, if Network Infrastructure Management - Device Config is included in the deployment.

RESTCONF APIs are also available; see the API documentation on the Network Developer Portal.

Greenfield configuration of third-party equipment is supported and has been tested for Juniper card configuration. Brownfield configuration of third-party equipment has not been tested.

Intent types

NSP uses intent types to build configuration templates, which are then used to build configurations.

The intent type defines the parameters that will be set when the configuration template is deployed. The configuration form can provide a parameter value or leave the value blank, to be set during deployment. If a parameter is not included in the configuration form, deploying the configuration template will not set that parameter on the target.

Users can create custom intent types in NSP or download predefined intent types from the Artifacts directory on the NSP software download site. Nokia recommends using predefined intent types where applicable.

Predefined intent types are delivered to the software download site outside the NSP release cycle. The intent types are delivered in zip files, which include a readme file for each intent type. See the NSP Device Configuration Intent Type Catalogue document in the Artifacts directory for the list and descriptions of the intent types in the collection.

Configuration templates

Operators use the configuration templates to deploy the configurations to the network either in bulk or on an individual target basis (NE or card/port). Device Configuration provides full feedback on the success (aligned) or failure (misaligned) of the deployment request, so that the operator is aware if the defined configuration is present and running in the network. The operator can audit and monitor for configuration drift that may occur over time and realign the network configuration back to the intended and defined configuration.

Templates can be defined with fixed or flexible attribute definitions. Certain attributes can be set with a fixed value (for example, MTU = 1500) that cannot be changed by the operator, or can be set with a default value that can be modified in the deployment phase.

9.2 How does configuration deployment work?

9.2.1 Creation of a configuration deployment

A configuration deployment is created when a template is deployed or associated to the network. The deployment object represents the application of a configuration template to a target in the network.

The deployment provides inputs to the template parameters as needed, and executes the configuration on a target in the network.

Some intent types can be deployed to multiple targets, or to a group. See the *NSP System Administrator Guide* for information about creating groups.

A template must be created before a deployment can be created.

The following table shows the Configuration Deployment parameters.

Parameter	Predefined values	Notes
Deployment Status	Not-Started	The deployment is created in Device Configuration and is in a queue for deployment
	Saved	The configuration has been created and is waiting for a user to deploy it to the network.
	Aligning	An alignment operation is ongoing
	Auditing	An audit operation is ongoing
	Migrating	A migration operation is ongoing.
	Deployed Aligned	The deployment is completed and the network configuration matches the defined configuration.
	Deployed Misaligned	The deployment is completed and the network configuration does not match the defined configuration.
	Deployment Failed	The deployment could not be completed. Deployments may fail for several reasons: • Network Intents function is currently unavailable • the required intent type is not found • the Opensearch subsystem is down • A function downstream of Device Configuration is not responding
	Association Failed	Associating a template to the network could not be completed.

Parameter	Predefined values	Notes
Configuration Status	Modified	The deployment includes user-configured parameters
	Default	All parameters are set by the template
NE Name	—	—
NE ID	—	—
Identifier	—	For a physical deployment, the identifier is the network object that is configured by the deployment, for example, a port number. For a logical deployment, the identifier depends on the template, for example, LAG name and ID. The identifier is entered by the user at deployment creation.
Template	—	The configuration template in use
Role	Physical	The target is a physical object such as a port
	Logical	The target is a configured object such as QoS
Category	—	The type of physical or logical object being configured The category is defined in the configuration intent type.
Last Updated	—	The date and time of the most recent modification or operation performed.

Configuration process

9.3 Pathway: device configuration

9.3.1 Purpose

This pathway describes the general steps of intent-based device configuration. For complete configuration details, you may need to consult the *NSP Network Automation Guide*, or the tutorials on the Network Developer Portal.

Import or create intent types

1

Download the device type bundle from the NSP software download site. Intent types are available in artifact bundles (zip files).

If you prefer to create your own intent types, proceed to Stage 3.

2

Import the downloaded artifact bundles into NSP; see “How do I install an artifact bundle?” in the *NSP Network Automation Guide*.

3

To create intent types, see the Network Intents tutorial on the Network Developer Portal for developer information.

Note the following:

- The `InfrastructureConfiguration` label must be present
- The intent type must include a resource file, `icm_descriptor.json`, that provides the role:
  - Physical (for example, port and card configuration) or
  - Logical (for example, QoS or routing)

    For intent types with the logical role, this resource file also defines whether the template can be deployed to multiple targets in a deployment flow, and whether it can be deployed with other templates in a deployment flow.
  - The intent type must include at least one schema form and viewConfig file.
  - Other resource files may be required depending on the operations performed by the intent type.

Import the intent types

4

Open **Device Management**, **Configuration Intent Types**.

5

Click **+ IMPORT**

6

Choose the intent types from the list and click **IMPORT**.

Create a configuration template

7

Open **Device Management**, **Configuration Templates**.

8

Click **+ TEMPLATE**

9

Configure the parameters and click **RELEASE**.

Deploy the configuration

10

a. Open **Device Management**, **Configuration Deployments**.

b. Click **+ DEPLOYMENT** and choose **Logical** or **Physical**.

c. From the **Configuration Templates** list, choose a template and click ⋮ (More actions) **Deploy to Network**.

11

Configure the parameters and click **DEPLOY**.

The configuration is sent to the targets, and the deployment details are added to the **Configuration Deployments** list.

Audit

12

You can perform an audit at the deployment level for a single target, at the template level for all deployments using the template, or at the NE level for all configurations deployed to the NE.

An audit checks whether the target configuration matches the template, but does not change the target configuration.

Note: an audit at the template level checks all deployments using the template. The operation may take a long time. During the audit, you can click **VIEW DETAILS** for process information.

To audit a deployment:

1. Open **Device Management**, **Configuration Deployments**.
2. Choose a deployment.
3. Click ⓘ if needed to open the **Deployment Details** panel.

Click **VIEW RESULT** in the **Deployment Details** panel to see the results of the last audit.

4. Click **AUDIT CONFIG**. The audit results and alignment status information are updated.

13

To audit a template:

1. Open **Device Management**, **Configuration Templates**.
2. Choose a template and click ⓘ if needed to open the **Template Details** panel.

   The **Template Details** panel shows the number of deployments and the number that were aligned and misaligned after the last audit.
3. Click **AUDIT ALL CONFIG** and click **CONTINUE** to confirm. The alignment status information is updated.

14

To audit an NE:

1. Click (Audit/Align an NE). The Audit/Align an NE form opens.
2. Click in the **Select an NE** field. The Select an NE form opens with a list of NEs.
3. Choose an NE and click **SELECT**. The NE ID appears in the Audit/Align an NE form.
4. Click **AUDIT**. The **Device Management**, **Configuration Deployments** view is filtered to show the deployments for the NE with updated alignment status information.

Align

15

You can perform an align at the deployment, template, or NE level.

An align operation updates the target configuration if it does not match the configuration template.

To align a template:

1. Open **Device Management**, **Configuration Templates**.
2. Choose a template.
3. Click ⓘ if needed to open the **Template Details** panel.

   The **Template Details** panel shows the number of deployments and the number that were aligned and misaligned after the last audit.
4. Click **ALIGN ALL CONFIG** and click **CONTINUE** to confirm.

16

To align a deployment:

1. Open **Device Management**, **Configuration Deployments**.
2. Choose a deployment.

   Click ⓘ if needed to open the **Deployment Details** panel.

   The **Deployment Details** panel shows the results of the last audit.

3. Click **ALIGN CONFIG**. The alignment is performed and the alignment status information is updated.

17

To align an NE:

1. Click (Audit/Align an NE). The Audit/Align an NE form opens.
2. Click in the **Select an NE** field. The Select an NE form opens with a list of NEs.
3. Choose an NE and click **SELECT**. The NE ID appears in the Audit/Align an NE form.
4. Click **ALIGN**. The **Device Management**, **Configuration Deployments** view is filtered to show the deployments for the NE with updated alignment status information.

Configuration intent types

9.4 What is a configuration intent type?

9.4.1 Overview

NSP uses intent types to build configuration templates, which are then used to build configurations. Users can create custom intent types or import predefined intent types into NSP. Nokia provided intent types are available from the Nokia software support download site. Nokia recommends using predefined intent types where applicable.

When an intent type is imported to NSP, it is available in **Network Intents**, **Intent Types**. To be used as a configuration intent type, the intent type must be imported to **Device Management**, **Configuration Intent Types**.

Note:

- The intent type must have the `InfrastructureConfiguration` label to be used as a configuration intent type.
- The first container name in the intent type YANG must be the same as the module name.
- View files for predefined intent types can be added or edited in the **Network Intents**, **Intent Types** view; see “How do I add or change a View file?” in the *NSP Network Automation Guide*. No other changes can be made to predefined intent types.

The configuration intent type includes one or more configuration forms, which are defined by the viewConfig file of the intent type. Configuration forms define the parameters that will be set when the configuration template is deployed. The viewConfig file defines both the configuration form the user sees in the UI and the API payload that is sent to deploy the template.

The configuration form can provide a parameter value or leave the value blank, to be set during deployment. If a parameter is not included in the configuration form, deploying the configuration template will not set that parameter on the target.

The use of multiple configuration forms allows one intent type to be used to create multiple configuration templates with different configuration parameters and different parameter values.

For example, an intent type called `access port` could include a default configuration form with ten blank parameters, and a simple configuration form with two parameters with set values. All configuration templates created from this intent type will configure access ports. However, you can create multiple templates, for example, one to set the two parameters to predefined values, and one or more to set the ten parameters to values of your choosing.

9.4.2 Device-specific intent type artifacts

Device-specific intent types are created by Nokia for a particular NE release and NE mode. The intent type is designed to configure as many as possible of the attributes supported by the device for a specific area, for example, SAP QoS or Ethernet port configuration. An example intent type artifact is SAP QoS for model-driven SR OS Release 23.7.

If a new NE release offers new features or new or updated attributes in a particular area, a new device-specific intent type will be available.

When an NE is upgraded to a new NE release, you can migrate the NE configurations to a template created from the new intent type; see 9.6 “How do I update an NE configuration to use a newer intent type? ” (p. 119).

9.4.3 Descriptor resource file

The configuration intent type also includes a resource file, `icm_descriptor.json`, that provides parameters for the configuration templates created from the intent type. For intent types with the logical role, this resource file also defines whether the template can be deployed to multiple targets in one deployment, and whether it can be deployed with other templates in one deployment.

The following table describes attributes that can be provided in the `icm_descriptor.json` file.

Attribute	Mandatory	Default value	Available values	Description
category	Yes	—	Any string, such as Port, Card, or QoS	The category is used primarily for logical grouping of the templates created using the intent type.
role	Yes	—	**physical** **logical**	The physical role refers to physical configurations such as ports, while logical refers to logical configurations, such as QoS.
description	No	—	Any string	—
device-scope	Yes	—	mdm classic mdm-and-classic srl wavence third-party all	The device scope declares the device types the templates are intended for.
select-template[1]	No	**multiple** for logical role **single** for physical role	**multiple** **single**	This parameter declares whether the template can be deployed along with other templates in the same deployment.
select-target	No	**multiple**	**multiple** **single**	This parameter declares whether the user will be able to select single or multiple targets when the template is deployed.

Attribute	Mandatory	Default value	Available values	Description
target-xpath[2]	No	**NEs** for logical role For physical role, the default varies based on category.	Any valid network inventory x-path	The x-path is used to fetch the list of targets during deployment creation.
targets[1]	No	—	targets = [{"NSP", "NSP"}]	The targets parameter allows a target to be provided that differs from the role defaults. For example, for NGE configuration, the target is NSP. The parameter is configured as a key-value pair.

target-labels[2]	No	—	JSON string with target-specific content:
			target-labels: {
			"type": "*NE type*",
			"product": "*product name*",
			"version": "*NE release version*"
			}
			Example:
			target-labels : {
			"type": "7750 SR-12",
			"product": "7750 SR",
			"version": "TiMOS-C-20.5.R2, TiMOS-C-22.10.R8"}[3]
				The target-labels parameter allows the targets presented in the deployment creation form to be filtered according to the requirements of the intent type.
				Example: `"target-labels": {"type": "7750 SR-12", "product": "7750 SR", "version": "TiMOS-C-20.5.R2"}`
				When a template created from the intent type is selected and the user opens the Add Target form, the list of available targets is filtered to show only 7750 SR NEs, running version 20.5 R2.

Attribute	Mandatory	Default value	Available values	Description
labels	No	—	String with comma separated values Example: labels: "s168_96_99_acpm, SR-7750, 22.10.R8.AA1, 7750 SR, 7750 SR-12“[3]	The labels parameter allows the templates presented in the deployment creation form to be filtered according to the requirements of the intent type. Example: `"labels": "7750 SR-12",` When the user selects a 7750 SR-12 NE as a target and opens the Add Template form, the templates created from the intent type will be part of the filtered list of available templates. Templates with no labels will also appear in the list.

Attribute	Mandatory	Default value	Available values	Description
isPayloadWithMandatoryAttribute	No	false	true false	This parameter relates to brownfield discovery. If the intent type includes a mandatory value with no default value set, and this parameter is set to true, a computed default value is sent during discovery: • For enum, the computed value is one of the available values (usually the first one) • For integer, the computed value is the first value in the range(if present) else 0 • For string, the computed value is a dummy string in the range(if present) else dummy
full-class-name	No	—	Any valid NFM-P class path, as a key:value pair Example: "full-class-name": "rp.PolicyStatement"	This parameter relates to mass deployment discovery. Providing the full class name of the network object to be discovered allows NSP to query the NFM-P to discover the objects. The full-class-name parameter must match the class name of the object in NFM-P.[4]

Notes:

1. If the targets parameter is set in the descriptor file, the select-template parameter must be **single**.
2. Target filtering is defined by either the `target-xpath` or `target-labels` parameters. If `target-xpath` is configured, `target-labels` is ignored.
3. Partial strings are supported: for example, `7750 SR` will show 7750 SR-1 and 7750 SR-12 NEs,

if present. Wildcard characters are not supported.

4. You can obtain the class path for the network object from the XML API Reference, available from the API Documentation page in the Network Developer Portal.

See “What are the components of an intent type?” in the *NSP Network Automation Guide* for more information about configuring intent types, and the Intent Based Networking Framework and Input Forms tutorials on the Network Developer Portal for developer information, including use of resource files.

Template filtering

The `labels` parameter allows filtering of templates in the deployment creation form. The `device-scope`, `target-xpath` and `target-labels` parameters work together to filter targets, see 9.7.3 “Target filtering” (p. 123).

If both target and template filtering parameters are configured, filtering is based on the order in which the user selects the target or template:

- If the template is selected first, the list of targets is filtered according to the target filtering parameters.

  Example: `"target-labels": {"type": "7750 SR-12", "product": "7750 SR", "version": "TiMOS-C-20.5.R2"}`

  When a template created from the intent type is selected and the user opens the Add Target form, the list of available targets is filtered to show only 7750 SR NEs, running version 20.5 R2.

- If the target is selected first, the list of templates is filtered according to the `labels` parameter.

  Example: `"labels": "7750 SR-12",`

  When the user selects a 7750 SR-12 NE as a target and opens the Add Template form, the templates created from the intent type will be part of the filtered list of available templates.

You can make changes to the label and target label values after the intent type is in use in Device Configuration. After updating the `icm_descriptor` resource file, re-import the intent type in Device Configuration to apply the changes. Any new templates created using the intent type include the updated parameter values.

Existing templates are updated as follows:

- Adding values: re-importing the intent type adds the new values to all existing templates. When the template is deployed, the template labels are update with NE details: ne-id, ne-name, type, product and version. Added details are appended to any details already present in the template labels.
- Updating values: re-importing the intent type imports the changed values to the existing templates. Partial updates are allowed, for example, you can change one value in a target-label string. However, each label and target-label will be computed as unique.
- Deleting values: if labels, target-labels, or both are removed from the `icm_descriptor` resource file, re-importing the intent type removes the values from existing templates. If the last deployment with the deleted values is deleted from a template, the labels are removed from the template.

The following limitations apply:

- Filtering of targets is not supported when multiple templates are selected.
- Filtering of templates is not supported when multiple targets are selected.

9.4.4 Intent type configuration form

You can update an intent type to change one of the existing schema forms or add a new schema form. For details, see the viewConfig Forms tutorial on the Network Developer Portal.

If templates were created using the old schema form of the intent type, they will have a Config Form State of Outdated after the intent type is updated and re-imported. If a required schema form has been deleted in NSP, the Config Form State is updated to Detached. Audit or align operations on an outdated or detached template will be performed using the previous values.

The only available operations for a detached template are audit and align: no new deployments can be created, and deployments cannot be migrated to the template.

9.4.5 Intent type details

Select an intent type and click (Intent Type Details) to view information about the intent type.

From the (Table row actions) menu, you can:

- Open the intent type in Network Intents to make any changes required
- Remove the intent type from the list of configuration intent types, if it is not in use by a template
- Re-import the intent type from Network Intents

Changes to views are automatically imported.

Perform a re-import for any of the following.

- To import changes made to an intent type other than changes to views
- To import changes of any kind made outside NSP

9.4.6 Re-importing intent types

If a view or schema form in an intent type has been added, deleted, or edited in the **Network Intents**, **Intent Types** view, it is automatically updated in the Device Management configuration views.

If other changes have been made to the intent type, for example, a change to the YANG, the intent type is not automatically synched. You need to re-import the intent type to see the changes.

Important! The only changes that are automatically synched are changes made to the view files.

If a change has been made in Network Intents other than a change to a view, or if a change has been made to the intent type code or files outside NSP, for example, in a text editor, you must re-import the intent type to access the changes.

9.5 How do I import a configuration intent type?

9.5.1 Before you begin

Before you can import an intent type, the intent type must be present in the NSP with the `InfrastructureConfiguration` label. You can import a bundle of intent types into NSP; see “How do I install an artifact bundle?” in the *NSP Network Automation Guide*.

Intent types that have already been imported appear dimmed in the import form. To import changes to an intent type, perform a re-import from the **Table row actions** menu.

Note: The intent type must include an `icm_descriptor` resource file. If the resource file is missing a mandatory attribute, the import fails with the error message “Invalid descriptor file. Missing *attributes*” where *attributes* is the list of mandatory attributes that are missing from the file. See 9.4.3 “Descriptor resource file” (p. 113) for information about the requirements for the descriptor file.

9.5.2 Steps

1

Open **Device Management**, **Configuration Intent Types**.

2

Click **+ IMPORT**.

3

In the form that opens, choose the intent types and click **IMPORT**.

The list of intent types is updated.

Note: The more schema form content an intent type has, the longer it takes to import.

END OF STEPS

9.6 How do I update an NE configuration to use a newer intent type?

9.6.1 Purpose

Use this procedure to migrate the configurations for an NE from one configuration template to another, for example, when a new device-specific intent type is available for the device.

The device specific intent type bundles include the workflow, `icm-workflow-ne-migrate-multiple`, required to migrate the configurations.

Only deployments in Deployed Aligned or Deployed Misaligned status are migrated.

Note: This procedure does not support migration from classic management to MDM.

9.6.2 Steps

1

Create a template using the new intent type.

1. Obtain the new intent type artifact bundle from the Nokia NSP software delivery site.
2. Import the artifact bundle into NSP; see “How do I install an artifact bundle?” in the *NSP Network Automation Guide*

3. Import the intent type into Device Management; see 9.5 “How do I import a configuration intent type?” (p. 118)
4. Create a configuration template using the intent type; see 9.10 “How do I create a configuration template?” (p. 127).
5. Repeat the preceding steps as needed to create configuration templates for all the intent types you need to migrate to.

2

Open **Workflows**, **All Workflows**.

3

Select the `icm-workflow-ne-migrate-multiple` workflow and click ⋮ (Table row actions), **Execute**.

4

In the Create Execution form that opens, configure the migration parameters.

1. Enter an optional description in the **Description** field.

   You can filter on the description in the Workflow Executions view.
2. Click in the **NE ID** field and choose the NE ID.
3. Click + **ADD** above the **Source and Target Template Pair** field.
4. Click in the **Source Template** field, select a template, and click **SELECT**.
5. Click in the **Target Template** field, select the template to migrate to, and click **SELECT**.
6. Click **EXECUTE**.

The workflow executes, replacing deployments on the NE that used the source template with deployments using the target template.

5

Open **Workflows**, **Workflow Executions** to monitor the progress of the workflow.

As the workflow proceeds, the list of deployments in Device Management, Configuration Deployments is updated to show the new template.

END OF STEPS

Configuration templates

9.7 What is a configuration template?

9.7.1 Overview

A configuration template is a reusable set of parameter values that implements a configuration based on the associated intent type configuration form. The intent type and the configuration form must be created before the template can be created.

You can create a template for each configuration form in each intent type, or create templates for different use cases.

Note: If a user has multiple versions of an intent type and a template is created for each, the same target object can be created under each template, which will cause the target configurations to overwrite each other in the network.

Templates can be fixed or flexible. A fixed template has preset or default values for all parameters. A flexible template includes parameters that can be changed by the operator at deployment time.

Note: Validation of parameters is performed by the NSP when a template is deployed. However, for MTU in particular, non-numerical values cannot be detected by NSP due to an HTML5 behavior.

You can deploy a configuration template from the configuration templates list by clicking ⋮ (Table row actions), **Deploy to Network**, or from the deployments list, see 9.24 “How do I create a logical configuration deployment?” (p. 139) and 9.24 “How do I create a logical configuration deployment?” (p. 139).

NSP supports up to 20 000 deployments per configuration template.

9.7.2 Parameters

In NSP you can create configuration templates for physical configuration such as card or port configuration, or logical configuration such as QoS, LAGs, and routing policy configurations. Configuration templates are based on configuration intent types. The template inherits some properties defined in the intent type, and others are defined as part of template configuration.

The following table shows the Configuration Template parameters.

Parameter	Predefined values	Notes
Name	—	—
Description	—	If no description has been configured, the Description column displays a dash. The Description column can only be filtered on configured contents.

Parameter	Predefined values	Notes
Life Cycle	draft	The template can be edited but cannot be deployed to the network.
	released	The template is active. It can be used to deploy configuration to the network. The template cannot be edited or deleted. The status of the template cannot be changed to draft if it has been deployed.
	obsolete	The template is inactive and cannot be used to deploy new configurations to the network, but maintains existing configuration instances.
Target Labels[1]	—	The target-label values configured in the `icm_descriptor` resource file in the configuration intent type Target labels, combined with device scope, filter template targets by NE.
Intent Type	—	The configuration intent type the template is based on
Intent Type version	—	The version number of the intent type
Config Form	—	The intent type schema form the template is using. The intent type can have one or more schema forms: a template incorporates one form.
Config Form State	Up-to-date	The config form in use by the template matches the schema form in the intent type.
	Outdated	The config form in use by the template is no longer aligned with the intent type as a result of an intent type update. Operational actions, such as audits, will be performed against the previous version, not the updated version. The template can be cloned with the new values to create a copy of the template that incorporates the new schema form.
	Detached	The schema form used to create this template is deleted or otherwise unusable by the template. The template can still be audited or aligned, but it cannot be cloned, and new deployments cannot be created, including by migration.
	Processing	An update to the config form state is ongoing.

Parameter	Predefined values	Notes
Role	Physical	The target is a physical object such as a port.
	Logical	The target is a configured object such as QoS.
Category[1]	—	The type of physical or logical object being configured.
Device Scope[1]	SROS Model	The template is intended for model driven SR OS devices.
	SROS Classic	The template is intended for classically managed SR OS devices.
	SROS Classic and Model	The template can be used for both classic and model driven SR OS devices.
	SRL Only	The template is intended for SRL devices.
	Wavence	The template is intended for Wavence devices.
	Third Party	The template is intended for non-Nokia NEs.
	All	The template can be used for any device or management type.
Flexible	True	A flexible template includes parameters that can be changed by the operator at deployment time.
	False	If all parameters are read only and have default values, the Flexible parameter is set to False.
Last Updated	—	The date and time of the most recent modification or operation performed.

Notes:

1. This parameter is defined in the `icm_descriptor` resource file in the configuration intent type.

9.7.3 Target filtering

When a template is deployed, the available targets are filtered based on the `device-scope`, `target-xpath` and `target-labels` parameters, respectively. The parameters are configured in the `icm_descriptor` resource file in the configuration intent type; see 9.4.3 “Descriptor resource file” (p. 113). Each of these parameters is optional, but at least one must be configured for the target list to be filtered.

Device scope

The Device Scope value shown in the **Device Management**, **Configuration Templates** view is based on the value of the `device-scope` parameter in the `icm_descriptor` file. The device scope parameter filters based on management type: classic or MDM.

Target x-path

Nokia predefined intent types often include a target x-path in the `icm_descriptor` file.

The target x-path value can be any valid network inventory x-path. For example, `/nsp-equipment:network/network-element[product = '7750 SR' or product = '7450 ESS' or product = '7950 XRS']` specifies that the target must be an SR OS NE.

Target label

The target label value is not set in Nokia predefined intent types.

The target label defines the NE type, product, and version to show in the targets list.

For example:

```
"target-labels": {"type": "7750 SR-12", "product": "7750 SR", "version":
"TiMOS-C-20.5.R2"}
```

When a template created from the intent type is selected and the user opens the Add Target form, the list of available targets is filtered to show only 7750 SR-12 NEs, running version 20.5 R2.

Partial strings are supported: for example, `"type": 7750 SR` will show 7750 SR-1 and 7750 SR-12 NEs, if present. It is not required to configure all three components, for example, if `version` is not configured, all 7750 SR-12 NEs are shown.

The `target-xpath` parameter takes precedence over the `target-labels` parameter: if `target-xpath` is configured, `target-labels` is ignored.

Combining parameters to create a filtered list

Filtering of targets in Device Configuration is based on the combined values of `device-scope` and `target-xpath` or `target-labels`, as described in the following table. The device scope parameter filters based on management type: classic or MDM. The target list is then filtered based on the `target-xpath` if available, or, if `target-xpath` is not configured, `target-labels`.

If the target filtering parameters are not configured correctly for your needs, the filtering may return undesired targets. For example:

- if the `device-scope` parameter is `third-party` but the `target-labels` includes `"product": "SR Linux"`, the filtered target list will include SR Linux NEs, although SR Linux is not a third party NE.
- if the `target-xpath` states `[product = '7750 SR']` and the `target-labels` states `"product": "7950 XRS"` the filtered target list will include only 7750 SR NEs because `target-xpath` takes precedence.

device-scope parameter in icm_descriptor	target definition in icm_descriptor	Targets shown
mdm	`"product":` includes SR OS NEs, such as 7750 SR	Model driven SR OS devices
classic	`"product":` includes SR OS NEs, such as 7750 SR	Classically managed SR OS devices
mdm_and_classic	`"product":` includes SR OS NEs, such as 7750 SR	Classic and model driven SR OS devices
srl	`"product": "SR Linux"` is included in the value	SRL devices
wavence	`"product": "Wavence SA"` or `"product": "Wavence SM"` is included in the value	Wavence devices
third-party	`"product":` includes non-Nokia products, for example, `"product": "Cisco"`	Devices with the specified product names, for example, Cisco
all	not configured	No filtering - all NEs are available to select

9.7.4 Template options

Select a template and click ⓘ(Template Details) to view information about the template.

From the ⋮ (Table row actions) menu, you can:

- View/Edit the template
  If the template Life Cycle status is draft or obsolete, it can be opened for editing from the Table row actions menu. If it is in released status, a read-only View page can be opened.
- View the list of deployments using the template
- Migrate deployments to another template
- Deploy the template to the network
- Associate the template to the network
- Audit/Align deployments:
  - Audit all config
    Audit deployments for configuration drift that may occur over time
  - Align config
    Realign the network configuration back to the intended and defined configuration
  - Align misaligned only
- Delete
  Delete the template. Note: the template cannot be deleted if the Life Cycle status is released.
- Open in Network Intents
  Open the template intent type in Network Intents to make any changes required

Attention: Be cautious when invoking bulk actions at the template level with many thousands of configuration instances as this may take many hours to complete.

9.7.5 Differences between classic NEs and model-driven NEs

If you are using Nokia predefined intent types audits will behave differently between classic SR OS and MD SR OS NEs.

In the case of classic SR OS targets, only those attributes defined in the associated configuration form and with a user entered value will be audited. In the case of MD SR OS targets, all attributes in the target configuration tree are audited and attributes not even in the intent type YANG tree are checked.

For example, if the deployment has two targets:

- with classic SR OS NEs: the configured values of the user entered attributes on each target are checked to verify whether they match the configuration form. The alignment status is based on this check.
- with MD SR OS NEs: the values of all attributes on each target are checked to verify whether they match the configuration form and each other. The alignment status is based on matching both the configuration form and the other target.

Alignments also behave differently between classic NEs and MD NEs. For MD NEs, an alignment is marked misaligned if the NE is unreachable. For classic NEs, the alignment operation checks the configuration in the NFM-P database. If the database matches the deployment configuration, the status will be aligned, regardless of the NE's reachability.

9.8 What is the difference between deploying a template and associating a template?

9.8.1 Mismatch handling

Both associating and deploying a template create a deployment of the template to the NSP network.

The difference between the two processes is in how they handle a mismatch between the template configuration and configuration already present on the target:

- If the template is deployed to the network, the deployment will apply the template values to the target.
- If the template is associated to the network, the deployment will not overwrite target values with template values.
  - If the mismatched value is flexible in the template, the template value will be set to the value on the target.
  - If the template has fixed attributes and the target attribute values do not match a fixed attribute, then the configuration instance will be declared misaligned.
  - If the value is flexible in the template and not set on the target, the target will be updated with the template value.

Attention: For NSP to discover the target configuration when you associate the template, the target NE must be configured using MD-CLI.

If an attribute on the target NE was not configured using MD-CLI, it will be marked misaligned when the template is associated. In the Audit Result form, the Actual Value field will show the value as undefined.

9.9 What is mass deployment discovery?

9.9.1 Large-scale brownfield association

You can perform a mass deployment discovery to associate multiple logical network objects for multiple classic NEs in a brownfield scenario.

Devices must be discovered and managed by NFM-P.

A mass deployment discovery can be initiated from a logical intent type, or from a logical template.

If the operation is initiated from the intent type, a template based on the selected intent type is associated to the entire network. For example, all egress QoS policies on classic NEs are discovered by NSP and marked aligned or misaligned against the same template. If the operation is initiated from the template, you can select specific NEs and/or targets to associate to the template. For example, if you have two templates for egress QoS policies, you can associate each template to the NEs or policies that align with that template.

The `full-class-name` parameter must be configured in the intent type `icm_descriptor` file; see 9.4.3 “Descriptor resource file” (p. 113).

9.10 How do I create a configuration template?

Important! A configuration intent type must be imported before a template can be created.

9.10.1 Steps

1. Open **Device Management**, **Configuration Templates**.
2. Click **+ CONFIGURATION TEMPLATE**.
3. In the form that opens, enter a name for the template.

   Note: Template names cannot start or end with a space, or contain special characters other than spaces, underscores, or hyphens.
4. Click **+ INTENT TYPE** and choose an intent type.
5. Choose a configuration form from the drop-down list.

6

Click **SAVE AS DRAFT** to create the template in draft state, or **RELEASE** to create the template in released state.

The configuration template is added to the list.

END OF STEPS

9.11 How do I update a template to apply intent type schema form changes?

9.11.1 Purpose

Use this procedure if a schema form in the intent type used by a template has been changed, that is, the Config Form State is Outdated, and you need to use the updated config form. To do this, create a clone of the template with the updated schema form values.

9.11.2 Steps

1

Open **Device Management**, **Configuration Templates**.

2

Choose an outdated template and click ⋮ (Table row actions), **Clone with updated config form**.

3

In the form that opens, enter a name for the cloned template.

4

Click **SAVE AS DRAFT** to create the clone in draft state, or **RELEASE** to create the clone in released state.

The cloned template is created with a Config Form State of Up-to-date.

END OF STEPS

9.12 What is migration of a deployment?

9.12.1 Applying schema form changes to an existing deployment

If you have updated an intent type schema form, you can apply the updated intent type values to an existing deployment.

To do this, migrate the deployments from a template created with the old schema form, the source template, to a template created with the new schema form, the target template.

Important! Migrating configuration deployments between templates is only available if the

source and target templates meet the following criteria.

- the same Role and Category
- based on the same intent type with the same schema form
- the same target identifiers defined

The following is an example scenario.

- Template `set_mtu` was created with intent type `port_config`, using the viewConfig form `gold_ports.viewConfig`
- Template `set_mtu` was deployed to the network, configuring ports on NE1 and NE2.
- `gold_ports.viewConfig` was updated, automatically updating the schema form and causing the config form state of the `set_mtu` template to become outdated.
- Template `set_mtu` was cloned to create `set_mtu2`.

To apply the updates in the new version of `gold_ports.viewConfig` to the ports on the NEs, migrate the deployments from template `set_mtu` to template `set_mtu2`.

After migration, NSP automatically aligns the deployments with the new template, pushing the new template configuration to the targets.

Note: Deployments with a Deployment Status of Not-started, Saved, Auditing, Aligning, or Association Failed cannot be migrated. These deployments will not appear in the **Migrate Deployments** form.

9.12.2 Modified attributes

When modifying the viewConfig file in Network Intents, you can make changes to some attributes. This includes adding and removing attributes, changing attribute values, and changing attributes from fixed to flexible or vice versa. Attributes can be modified if their values are entered into a field or selected from a dropdown. Table and list attributes cannot be modified during a migration. For example, in a QoS configuration template, the **Default FC** parameter can be changed, but a queue cannot be added.

Migration is not a service impacting operation. The migration operation deploys the new template to the existing configuration, merging the existing configuration and the new configuration. Note that values can be updated either due to changes in fixed values in the target template, or to changes made to flexible attributes when the migration is performed.

- If the source and target templates have the same attributes and only attribute values have changed, the new deployment has the updated attribute values.
- If the target template has added attributes, the new deployment has the target template values for all attributes, including the additional ones.
- If the target template has deleted attributes that appeared in the source template, the new deployment keeps the existing configuration value for the deleted attribute and applies the target template values for the attributes in the target template.

The following table shows an example. In this example, one attribute is changed, one is added, and one is deleted.

Existing deployment values configured by source template	Attribute values applied by migration	New deployment values
• MTU: 1500 • encaptype: qinq	• MTU: 1600 • administrative state: enabled	• MTU: 1600 • encaptype: qinq • administrative state: enabled

9.13 How do I migrate a deployment to another template?

9.13.1 Steps

1

Perform 9.11 “How do I update a template to apply intent type schema form changes?” (p. 128) to create a target template.

2

Open **Device Management**, **Configuration Templates**.

3

Choose the source template, click ⋮ (Table row actions), **Migrate deployments** and click **CONTINUE** to confirm.

The **Migrate Deployments** form opens with the template already selected.

4

Select the target template:

1. Click + **TEMPLATE**
2. Choose the new template from the templates list and click **ADD**.

   Click **View configuration** if needed for a read-only preview of the configuration parameters.
3. If you have chosen a flexible template, .click **View/Edit Template Config** to verify or update template parameters, and click **UPDATE**.

5

Select the deployments to migrate:

1. Click + **DEPLOYMENTS**
2. Choose one or more deployments from the list to add them to the Bin. You can use Shift-click to choose a range of deployments.
3. Verify the list of targets in the Bin.

   If **Select all deployments** is clicked, the deployment list and Bin cannot be rendered.
4. Click **ADD**.

6

Click **MIGRATE** .

The template field in the **Device Management**, **Configuration Deployments** list is updated. You can align the network configuration to apply the configuration changes to the targets.

END OF STEPS

9.14 How do I deploy or associate a template to the network?

9.14.1 Procedures differ for physical and logical templates

You can deploy a template from the **Device Management**, **Configuration Deployments** view or from the **Device Management**, **Configuration Templates** view. You can only associate a template from the **Device Management**, **Configuration Templates** view.

The steps vary depending on the role. See the following:

- 9.24 “How do I create a logical configuration deployment?” (p. 139)
- 9.25 “How do I create a physical configuration deployment?” (p. 140)
- 9.15 “How do I associate a logical template to the network? ” (p. 130)
- 9.16 “How do I associate a physical template to the network? ” (p. 132)

9.15 How do I associate a logical template to the network?

9.15.1 Purpose

Associating a template to the network creates a deployment. Template parameters that are already configured on the target are preserved.

To create a logical template deployment where the template parameters will overwrite target configuration, see 9.24 “How do I create a logical configuration deployment?” (p. 139)

9.15.2 Steps

1

Open **Device Management**, **Configuration Templates**.

2

Choose a logical template and click ⋮ (Table row actions), **Associate to network**.

The **Associate Template** form opens with the template already selected.

3

Add one or more targets:

1. Click + **TARGET** and choose **NEs** from the drop-down list.
2. Choose one or more targets from the list to add them to the Bin. You can use Shift-click to choose a range of targets.

3. Verify the list of targets in the Bin and click **ADD**.
4. To add additional targets, repeat the previous steps and click **UPDATE**.

4

If needed, click the **VIEW TEMPLATE CONFIG** button for a read-only preview of the configuration parameters. If any configuration in a fixed template conflicts with the configuration in the target, the deployment will be misaligned.

5

Identifier fields appear in the form for each selected template. Enter information in each field.

Attention: Your input can't contain the hash symbol (#).

6

Click **ASSOCIATE** to apply the configuration to the targets.

END OF STEPS

9.16 How do I associate a physical template to the network?

9.16.1 Purpose

Associating a template to the network creates a deployment. Template parameters that are already configured on the target are preserved.

To create a physical template deployment where the template parameters will overwrite target configuration, see 9.25 "How do I create a physical configuration deployment?" (p. 140)

9.16.2 Steps

1

Open **Device Management**, **Configuration Templates**.

2

Choose a physical template and click ⋮ (Table row actions), **Associate to network**.

The **Associate Template** form opens with the template already selected.

3

Add one or more targets:

1. Click + **TARGET** and choose **Ports**.
2. Choose one or more targets from the list to add them to the Bin. You can use Shift-click to choose a range of targets.
3. Verify the list of targets in the Bin and click **ADD**.
4. To add additional targets, repeat the previous steps and click **UPDATE**.

Note: All targets must be the same type: you can't deploy to ports and groups in the same deployment.

4

If needed, click the **VIEW TEMPLATE CONFIG** button for a read-only preview of the configuration parameters. If any configuration in a fixed template conflicts with the configuration in the target, the deployment will be misaligned.

5

Click **ASSOCIATE** to apply the configuration to the targets.

END OF STEPS

9.17 How do I perform a mass deployment discovery from an intent type?

9.17.1 Purpose

Use this procedure to associate a logical template to NFM-P managed brownfield devices in the network.

This procedure allows you to associate a template based on the intent type to all classic devices at one time. To associate the template to selected targets or target identifiers instead of the entire network, see 9.18 "How do I perform a mass deployment discovery from a template?" (p. 134).

The `full-class-name` parameter must be configured in the intent type `icm_descriptor` file; see 9.4.3 "Descriptor resource file" (p. 113).

Note: Performing a mass deployment discovery on more than 5 000 deployments may result in some deployments in Association Failed status. You can retry the failed associations from the Configuration Deployments view, or using the API.

9.17.2 Steps

1

Open **Device Management**, **Configuration Intent Types**.

2

Choose a logical intent type and click ⋮ (Table row actions), **Associate to Network (Classic Only)**.

3

In the form that opens, click in the **Configuration Template** field.

The **Select a Configuration Template** form opens, showing the available templates based on the selected intent type.

4

Select a template:

a. Choose a template from the list and click **SELECT**.

b. Create a template.

1. Click **+ NEW**. The template creation form opens in a new tab, with the intent type selected.
2. Configure the template parameters and click **RELEASE**.
3. Click in the **Select a Configuration Template** form.
4. Choose your new template and click **SELECT**.

5

Click **ASSOCIATE**.

A deployment for the template is created for each target and identifier, for example, for each policy on each NE.

END OF STEPS

9.18 How do I perform a mass deployment discovery from a template?

9.18.1 Purpose

Use this procedure to associate a logical template to NFM-P managed brownfield devices in the network.

This procedure allows you to associate the template to selected devices, and/or to select target identifiers, for example, a subset of the QoS egress policies configured in the NFM-P. To associate a template to the entire network without selecting targets or identifiers, see 9.17 “How do I perform a mass deployment discovery from an intent type?” (p. 133).

The `full-class-name` parameter must be configured in the intent type `icm_descriptor` file; see 9.4.3 “Descriptor resource file” (p. 113).

Note: To associate target identifiers to more than one target, you need to enter the identifier numbers in the form, for example, the policy names and IDs. Ensure that you have this information available when performing this procedure.

Note: Performing a mass deployment discovery on more than 5 000 deployments may result in some deployments in Association Failed status. You can retry the failed associations from the Configuration Deployments view, or using the API.

9.18.2 Steps

1

Open **Device Management**, **Configuration Templates**.

2

Choose a logical template and click ⋮ (Table row actions), **Associate to Network, Associate selected classic instances**.

3

Add additional templates if required:

1. In the **Associate selected classic instances** form, click + **TEMPLATE**
2. Choose one or more templates from the templates list to add them to the Bin. You can use Shift-click to choose a range of templates.
3. Verify the list of templates in the Bin and click **UPDATE**.

If more than one template is added, all targets and identifiers are automatically selected. Proceed to Step 7.

4

Add one or more targets:

1. Click + **TARGET** and choose **Select targets** or **All targets in the network** from the drop-down list.
2. If you chose **All targets in the network**, proceed to Step 5.
3. If you chose **Select targets**, a Select Target form opens. Choose one or more targets from the list to add them to the Bin.
4. Verify the list of targets in the Bin and click **ADD**.
5. To add additional targets, repeat the previous steps and click **UPDATE**.
6. Proceed to Step 6.

5

Add one or more identifiers. If you have selected more than one target, perform the following:

1. Enter an identifier in the **Target Identifier** field and click + . The identifier appears below the field.
2. Enter additional identifiers as needed.
3. Proceed to Step 7.

6

Add one or more identifiers. If you have selected a single target, perform the following:

1. Click + **IDENTIFIER** and choose **Select identifiers** or **All identifiers** from the drop-down list.
2. If you chose **All targets in the network**, proceed to Step 7.
3. If you chose **Select identifiers**, a Select identifiers form opens. Choose one or more identifiers from the list to add them to the Bin.

   You can use Shift-click to choose a range of items.
4. Verify the list of identifiers in the Bin and click **ADD**.
5. To add additional targets, repeat the previous step.

6. Proceed to Step 7.

7

Click **ASSOCIATE**.

A deployment for the template is created for each target and identifier, for example, for each policy on each NE.

END OF STEPS

9.19 How do I retry a failed association?

9.19.1 Steps

1

Open **Device Management**, **Configuration Deployments**

2

Filter the list if needed: in the **Deployment Status** drop-down list, choose **Association Failed**.

3

Choose one or more deployments with the Association Failed status. You can use Shift-click to choose a range of deployments.

4

Retry the association:

a. To retry a single association:
   - From the ⋮ (Table row actions) menu, choose **Retry association**.
   - From the **Deployment Details** panel, click **RETRY ASSOCIATION**.

b. To retry multiple associations, click **Retry** above the details panel.

The retry operation proceeds.

END OF STEPS

9.20 How do I change the life cycle status of a template?

9.20.1 Steps

1

A template can be in draft, released, or obsolete status.

To change the status of the template, choose the status from the drop-down list in the **Life Cycle** column and click **CONTINUE** to confirm.

END OF STEPS

9.21 How do I edit a template?

Note: If you need to apply changes from an updated config form, see 9.11 “How do I update a template to apply intent type schema form changes?” (p. 128)

9.21.1 Steps

1

Open **Device Management**, **Configuration Templates**.

2

Choose a template in draft status.

3

Choose ⋮ (Table row actions), **View/Edit**.

4

Configure the parameters and click **UPDATE**.

END OF STEPS

9.22 How do I audit or align configurations?

9.22.1 Purpose

Use this procedure to audit or align all the deployments based on a specified template. To audit or align configuration for a single deployment, see 9.34 “How do I audit or align a deployment?” (p. 149). To audit or align all the deployments on an NE, see 9.35 “How do I audit or align configurations for an NE?” (p. 150).

9.22.2 Steps

1

Open **Device Management**, **Configuration Templates** view, choose a template.

2

Click ⓘ if needed to open the **Template Details** panel.

The **Template Details** panel shows the number of deployments and the number that were aligned and misaligned after the last audit.

3

In the **Template Details** panel, click **VIEW ALL**.

The system displays a list of the deployments based on the template.

Choose a deployment to view deployment details as needed.

4

To audit configurations:

1. From **Device Management**, **Configuration Templates**, choose a template. Choose ⋮ (Table row actions), **Audit/Align deployments** > **Audit all config**.
2. Click **CONTINUE** to confirm. The alignment status information is updated.

Note: An audit at the template level checks all deployments using the template. The operation may take a long time. During the audit, you can you can check the Template Details panel for process information.

Note: If you are using Nokia predefined intent types audits will behave differently between classic SROs and MD SROS NEs.
In the case of classic SROS targets, only those attributes defined in the associated configuration form and with a user entered value will be audited. In the case of MD SROS targets, all attributes in the target configuration tree are audited and so attributes not even in the intent type YANG tree are checked.

5

To align configurations:

1. From **Device Management**, **Configuration Templates**, choose a template. Choose ⋮ (Table row actions), **Audit/Align deployments** > **Align config**.
2. By default, only misaligned deployments are aligned. Choose **Align all deployments regardless of alignment status** if needed. Note that aligning all deployments may take much longer than aligning only misaligned deployments.
3. Click **ALIGN** to confirm.

Note: An alignment at the template level updates all misaligned deployments using the template. The operation may take a long time. During the operation, you can check the Template Details panel for process information.

END OF STEPS

Configuration deployments

9.23 How do I create a deployment?

9.23.1 Procedures differ for physical and logical deployments

A deployment is created by deploying or associating a template to the network.

You can deploy a template from the **Device Management**, **Configuration Deployments** view or from the **Device Management**, **Configuration Templates** view. You can only associate a template from the **Device Management**, **Configuration Templates** view.

The steps vary depending on the role. See the following:

- 9.24 “How do I create a logical configuration deployment?” (p. 139)
- 9.25 “How do I create a physical configuration deployment?” (p. 140)

9.24 How do I create a logical configuration deployment?

Important! A configuration template of the required role must be created before a deployment can be created.

9.24.1 Steps

1

Open the **Deploy Logical Configuration** form:

a. Open **Device Management**, **Configuration Deployments**.

b. Click **+ DEPLOYMENT** and choose **Logical** from the drop-down list.

c.

1. From **Device Management**, **Configuration Templates**, choose a logical template and click ⋮ (Table row actions), **Deploy to network**.

   The form opens with the template already selected.

2

Add one or more templates if required:

1. In the **Deploy Logical Configuration** form, click **+ TEMPLATE**
2. Choose one or more templates from the templates list to add them to the Bin. You can use Shift-click to choose a range of templates.
3. Verify the list of templates in the Bin and click **ADD**.

3

Add one or more targets:

1. Click **+ TARGET** and choose **NEs** or **Predefined Groups** from the drop-down list.

2. Choose one or more targets from the list to add them to the Bin. You can use Shift-click to choose a range of targets.
3. Verify the list of targets in the Bin and click **ADD**.
4. To add additional targets, repeat the previous steps and click **UPDATE**.
5. Verify that the list of targets is correct. Repeat this sequence to change the list if needed.

Note: All targets must be the same type, that is, you can't deploy to NEs and Predefined Groups in the same deployment.

4

If the template is flexible, the **VIEW/EDIT TEMPLATE CONFIG** button is available.

1. Click **VIEW/EDIT TEMPLATE CONFIG** to open the **View/Edit Template Config** form.
2. Choose a template and click **Edit Configuration**.
3. In the form that opens, configure the template parameters.
4. Click **UPDATE** if you made changes, or click **CANCEL** to close the **Edit Configuration** form.
5. Update additional template configurations as needed.
6. Click **SAVE** if you made changes, or click **CANCEL** to close the **View/Edit Template Config** form.

If the template is fixed, click the **VIEW TEMPLATE CONFIG** button for a read-only preview of the configuration parameters.

5

Identifier fields appear in the form for each selected template. Enter information in each field.

Attention: Your input can't contain the hash symbol (#).

6

Complete the creation of the deployment:

a. Click **SAVE** to add the deployment to the list in Saved status, but not apply the configuration to the targets.

b. Click **DEPLOY** to apply the configuration to the targets.

END OF STEPS

9.25 How do I create a physical configuration deployment?

Important! A configuration template of the required role must be created before a deployment can be created.

9.25.1 Steps

1

Open the **Deploy Physical Configuration** form:

a. Open **Device Management**, **Configuration Deployments**.

b. Click **+ DEPLOYMENT** and choose **Physical** from the drop-down list.

c.

1. From **Device Management**, **Configuration Templates**, choose a physical template and click ⋮ (Table row actions), **Deploy to network**.

   The form opens with the template already selected.

2

In the **Deploy Physical Configuration** form, add or change the template as needed:

1. To add a template, click **+ TEMPLATE**.
2. Select a template and click **ADD**.
3. To use a different template, click **REPLACE**, select the new template and click **ADD**.

3

Add one or more targets:

1. Click **+ TARGET** and choose **Ports**, **Cards**, or **Predefined Groups** from the drop-down list.
2. Choose one or more targets from the list to add them to the Bin. You can use Shift-click to choose a range of targets.
3. Verify the list of targets in the Bin and click **ADD**.
4. To add additional targets, repeat the previous steps and click **UPDATE**.
5. Verify that the list of targets is correct. Repeat this sequence to change the list if needed.

Note: All targets must be the same type, that is, you can’t deploy to Ports and Predefined Groups in the same deployment.

4

If the template is flexible, the **VIEW/EDIT TEMPLATE CONFIG** button is available.

1. Click **VIEW/EDIT TEMPLATE CONFIG** to open the **View/Edit Template Config** form.
2. Choose a template and click **Edit Configuration**.
3. In the form that opens, configure the template parameters.
4. Click **UPDATE** if you made changes, or click **CANCEL** to close the **Edit Configuration** form.
5. Update additional template configurations as needed.
6. Click **SAVE** if you made changes, or click **CANCEL** to close the **View/Edit Template Config** form.

If the template is fixed, click the **VIEW TEMPLATE CONFIG** button for a read-only preview of the configuration parameters.

5

Complete the creation of the deployment:

a. Click **SAVE** to add the deployment to the list in Saved status, but not apply the configuration to the targets.

b. Click **DEPLOY** to apply the configuration to the targets.

END OF STEPS

9.26 How do I edit a deployment?

9.26.1 Purpose

You can edit a deployment to change the template or parameters and deploy again to the same target. A deployment can only be edited if its deployment status is saved, deployed aligned, or deployed misaligned.

Note: You can use this procedure to make changes to a single deployment. To change multiple deployments based on the same template to another template, see 9.13 “How do I migrate a deployment to another template?” (p. 130). To edit parameters for multiple deployments based on the same flexible template; see 9.27 “How do I bulk edit multiple deployments?” (p. 143).

9.26.2 Steps

1

Open **Device Management**, **Configuration Deployments**.

2

Choose a deployment.

Click if needed to open the **Deployment Details** panel.

3

Click (Table row actions), **View/Edit**.

4

The form that opens depends on the role:

a. In the **Deploy Physical Configuration** form, click **REPLACE** to change the template, and **EDIT CONFIGURATION** to change the parameters.

b. In the **Deploy Logical Configuration** form, click **VIEW/EDIT TEMPLATE CONFIG** to change the parameters.

5

Click **DEPLOY**.

END OF STEPS

9.27 How do I bulk edit multiple deployments?

9.27.1 Purpose

You can edit up to ten deployments at one time. The following criteria must be met:

- The deployments must be from the same template.
- The template must be flexible.
- All deployments must have a compatible deployment status: saved, deployed aligned, or deployed misaligned.

9.27.2 Adding values to lists or tables

Some parameters, such as queues and forwarding classes in a QoS template, appear in list or table format in a configuration form. Existing table parameters can't be displayed in the edit form, however, you can add them in the edit form.

Added values can be handled in the following ways:

- Do Nothing: ignore all added table or list parameters and keep the existing values.
- Append All: keep the existing values in the deployments and add the values that were added during editing.
  If a value is added that already existed on a deployment, the new value will overwrite the old.
- Replace All: replace the entire table on all deployments with the table of values added during editing. If no values are added, the tables are empty after the edit.

Example

Deployment 1 has no queues and no forwarding classes.

Deployment 2 has:

- one queue: Queue ID 5, Queue Type expedited, Queue Mode priority
- one forwarding class: FC Name be, Profile in, Queue 5

The deployments are edited. The edit operation includes adding the following:

- no queues
- forwarding classes:
  FC Name be, Profile in, Queue 2
  FC Name af, Profile none, Queue 2

The following table shows the results of the edit based on the chosen handling of added values.

Table 9-1 Results of bulk edit based on handling of added table values

Handling option	Deployment 1	Deployment 2
Do Nothing	No queues, no forwarding classes	• one queue: Queue ID 5, Queue Type expedited, Queue Mode priority • one forwarding class: FC Name be, Profile in, Queue 5
Append All	• no queues • forwarding classes: FC Name be, Profile in, Queue 2 FC Name af, Profile none, Queue 2	• one queue: Queue ID 5, Queue Type expedited, Queue Mode priority • forwarding classes: FC Name be, Profile in, Queue 2 FC Name af, Profile none, Queue 2
Replace All	• no queues • forwarding classes: FC Name be, Profile in, Queue 2 FC Name af, Profile none, Queue 2	• no queues • forwarding classes: FC Name be, Profile in, Queue 2 FC Name af, Profile none, Queue 2

9.27.3 Steps

1

View a list of deployments from the same template:

a. Open **Device Management**, **Configuration Deployments** and filter the list by template name.

b.

1. Open **Device Management**, **Configuration Templates**.
2. Click on a template and choose ⋮ (Table row actions), **View all deployments**.

The view displays a list of deployments from the template.

2

Select up to ten deployments.

3

From the header at the top of the view, choose ⋮ (More), **Edit**.

An edit form opens, showing the template parameters. If a field parameter has the same value for all selected deployments, the value is shown in the form.

4

Update the parameters and click **CONTINUE**.

5

In the confirmation form that opens, select the way you want to handle added values and click **UPDATE**.

END OF STEPS

9.28 How do I deploy a saved deployment?

9.28.1 Steps

1

Open **Device Management**, **Configuration Deployments**.

2

Filter the list if needed: in the **Deployment Status** drop-down list, choose **Saved**.

3

Choose one or more deployments with the Saved status. You can use Shift-click to choose a range of deployments.

4

Complete the deployment:

a. For a single deployment:
- From the ⋮ (Table row actions) menu, choose **Deploy**.
- From the **Deployment Details** panel, click **DEPLOY**.

b. To retry multiple deployments, click **Deploy** at the top of the page.

The deployment proceeds.

END OF STEPS

9.29 How do I retry a failed deployment?

9.29.1 Steps

1

Open **Device Management**, **Configuration Deployments**.

2

Filter the list if needed: in the **Deployment Status** drop-down list, choose **Deployment Failed**.

3

Choose one or more deployments with the Deployment Failed status. You can use Shift-click to choose a range of deployments.

4

Retry the deployment:

a. To retry a single deployment:
   - From the ⋮ (Table row actions) menu, choose **Retry deployment**.
   - From the **Deployment Details** panel, click **RETRY DEPLOYMENT**.

b. To retry multiple deployments, click **Retry selected deployments** above the details panel.

The retry operation proceeds.

END OF STEPS

9.30 How do I distribute a logical configuration deployment?

9.30.1 Steps

1

Open **Device Management**, **Configuration Deployments**.

2

Choose a logical deployment and click ⋮ (Table row actions), **Distribute**.

The form opens with the template already selected and an identifier already assigned.

3

Add one or more targets:

1. Click + **TARGET** and choose **NEs** or **Predefined Groups** from the drop-down list.
2. Choose one or more targets from the list to add them to the Bin. You can use Shift-click to choose a range of targets.
3. Verify the list of targets in the Bin and click **ADD**.
4. To add additional targets, repeat the previous steps and click **UPDATE**.

Note: All targets must be the same type, that is, you can't deploy to NEs and Predefined Groups in the same deployment.

4

If the template is flexible, the **VIEW/EDIT TEMPLATE CONFIG** button is available.

1. Click **VIEW/EDIT TEMPLATE CONFIG** to open the **View/Edit Template Config** form.
2. Choose a template and click **Edit Configuration**.

3. In the form that opens, configure the template parameters.
4. Click **UPDATE** if you made changes, or click **CANCEL** to close the **Edit Configuration** form.
5. Update additional template configurations as needed.
6. Click **SAVE** if you made changes, or click **CANCEL** to close the **View/Edit Template Config** form.

If the template is fixed, click the **VIEW TEMPLATE CONFIG** button for a read-only preview of the configuration parameters.

5

Complete the creation of the new deployment:

a. Click **SAVE** to add the deployment to the list in Saved status, but not apply the configuration to the targets.

b. Click **DEPLOY** to apply the configuration to the targets.

END OF STEPS

9.31 How do I distribute a physical configuration deployment?

9.31.1 Steps

1

Open **Device Management**, **Configuration Deployments**.

2

Choose a physical deployment and click ⋮ (Table row actions), **Distribute**.

The form opens with the template already selected.

3

In the **Deploy Physical Configuration** form, change the template as needed:

Click **REPLACE**, select the new template and click **ADD**.

4

Add one or more targets:

1. Click + **TARGET** and choose **Ports** or **Predefined Groups** from the drop-down list.
2. Choose one or more targets from the list to add them to the Bin. You can use Shift-click to choose a range of targets.
3. Verify the list of targets in the Bin and click **ADD**.
4. To add additional targets, repeat the previous steps and click **UPDATE**.

Note: All targets must be the same type, that is, you can't deploy to Ports and Predefined Groups in the same deployment.

5

If the template is flexible, the **VIEW/EDIT TEMPLATE CONFIG** button is available.

1. Click **VIEW/EDIT TEMPLATE CONFIG** to open the **View/Edit Template Config** form.
2. Choose a template and click **Edit Configuration**.
3. In the form that opens, configure the template parameters.
4. Click **UPDATE** if you made changes, or click **CANCEL** to close the **Edit Configuration** form.
5. Update additional template configurations as needed.
6. Click **SAVE** if you made changes, or click **CANCEL** to close the **View/Edit Template Config** form.

If the template is fixed, click the **VIEW TEMPLATE CONFIG** button for a read-only preview of the configuration parameters.

6

Complete the creation of the new deployment:

a. Click **SAVE** to add the deployment to the list in Saved status, but not apply the configuration to the targets.

b. Click **DEPLOY** to apply the configuration to the targets.

END OF STEPS

9.32 How do I delete a deployment?

9.32.1 Steps

1

Open **Device Management**, **Configuration Deployments**..

2

Choose one or more deployments. You can use Shift-click to choose a range of deployments.

3

a. To delete a single deployment, from the ⋮ (Table row actions) menu, choose **Delete**.

b. To delete multiple deployments, click ⋮ **Delete** at the top of the page.

4

In the form that opens, choose how you want to delete the configuration:

- From NSP and Network: remove the configuration from the targets and remove the deployment from the **Configuration Deployments** list.
- From NSP: remove the deployment from the **Configuration Deployments** list without making any changes to the targets.
- Undeploy to Saved status: remove the configuration from the targets. Keep the deployment in the **Configuration Deployments** list in Saved status.

Note: Failed associations can only be deleted from NSP. Other deletion options are dimmed.
Deletion of a failed deployment from the network may fail. If this happens, consider deleting from NSP only.

END OF STEPS

9.33 How do I remove a deployment?

9.33.1 Purpose

Use this procedure to remove values that were configured by a deployment.

For example, if the MTU value on a port is set to 1600, then is changed to 1700 by a deployment, removing the deployment will result in no MTU value on the port.

9.33.2 Steps

1

Open **Device Management**, **Configuration Deployments**.

2

Choose one or more deployments. You can use Shift-click to choose a range of deployments.

3

a. To undeploy a single deployment, from the ⋮ (Table row actions) menu, choose **Undeploy to Saved status**.

b. To undeploy multiple deployments, click ⋮ **Undeploy to Saved status** at the top of the page.

The configuration is removed from the targets. The deployment status is changed to Saved.

END OF STEPS

9.34 How do I audit or align a deployment?

Note: If you are using Nokia predefined intent types audits will behave differently between classic SR OS and MD SROS NEs.

In the case of classic SR OS targets, only those attributes defined in the associated configuration form and with a user entered value will be audited. In the case of MD SROS targets, all attributes in the target configuration tree are audited and attributes not even in the intent type YANG tree are checked.

For example, if the deployment has two targets:

- with classic SR OS NEs: the configured values of the user entered attributes on each target are checked to verify whether they match the configuration form. The alignment status is based on this check.
- with MD SR OS NEs: the values of all attributes on the each target are checked to verify whether they match the configuration form and each other. The alignment status is based on matching both the configuration form and the other target.

9.34.1 Steps

1

Open **Device Management**, **Configuration Deployments**.

2

Choose a deployment. Click ⓘ if needed to open the **Deployment Details** panel.

Click **VIEW RESULT** in the **Deployment Details** panel to see the results of the last audit.

3

Choose an action:

a. Click **AUDIT**. The audit results and alignment status information are updated.

b. Click **ALIGN**. The alignment is performed and the alignment status information is updated.

END OF STEPS

9.35 How do I audit or align configurations for an NE?

9.35.1 Steps

1

Open **Device Management**, **Configuration Deployments**.

2

Click (Audit/Align an NE). The Audit/Align an NE form opens.

3

Click in the **Select an NE** field. The Select an NE form opens with a list of NEs.

4

Choose an NE and click **SELECT**. The NE ID appears in the Audit/Align an NE form.

5

Choose an action:

a. Click **AUDIT**. The audit results and alignment status information are updated.

b. Click **ALIGN** . The alignment is performed and the alignment status information is updated.

The **Device Management**, **Configuration Deployments** view is filtered to show the deployments for the NE with updated alignment status information.

END OF STEPS

Part IV: Device management use cases

Overview

Purpose

Describes use cases for Device Management functions.

Contents

10 Use cases

10.1 Discovery of a 7750 SR device in NSP

10.1.1 Purpose

This use case shows how to use NSP to discover a model-driven 7750 SR.

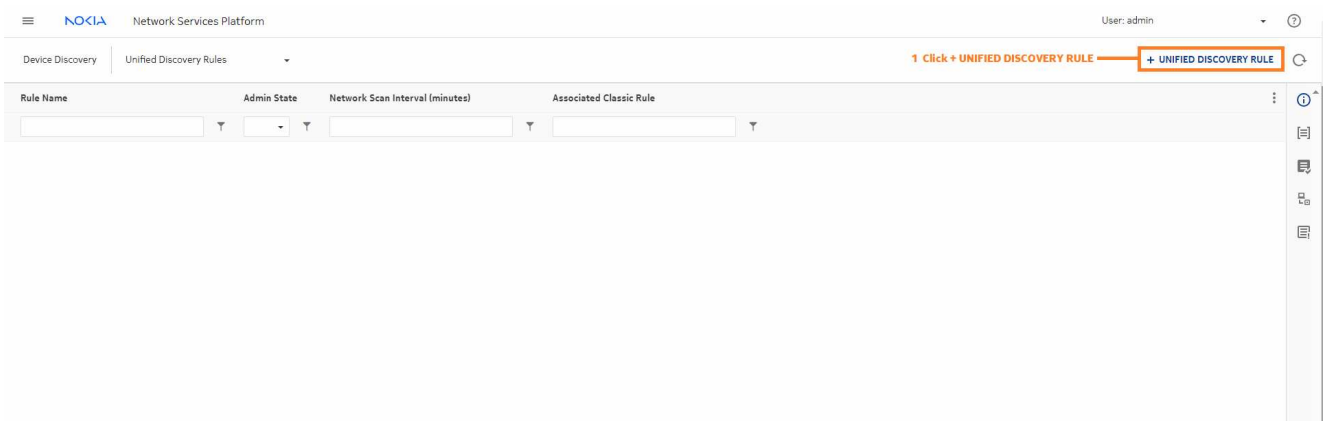
Click on a figure to enlarge it.

10.1.2 Steps

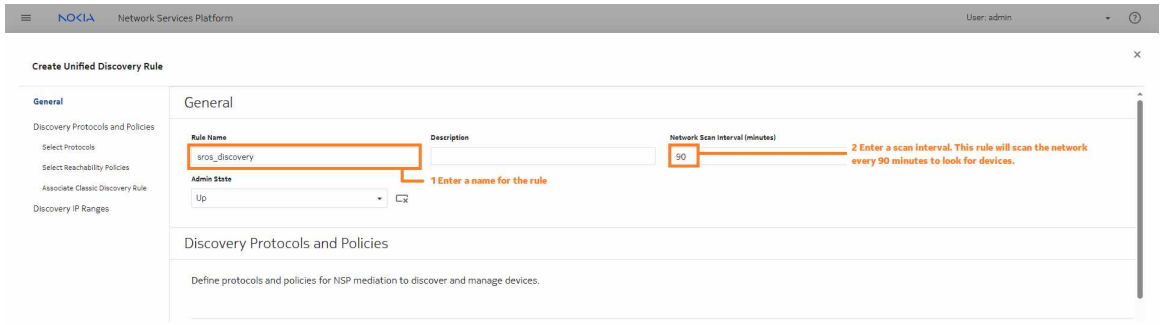
1

The first step is creating a unified discovery rule.

1. Open **Device Discovery**, **Unified Discovery Rules**.
2. Click **+ UNIFIED DISCOVERY RULE**.

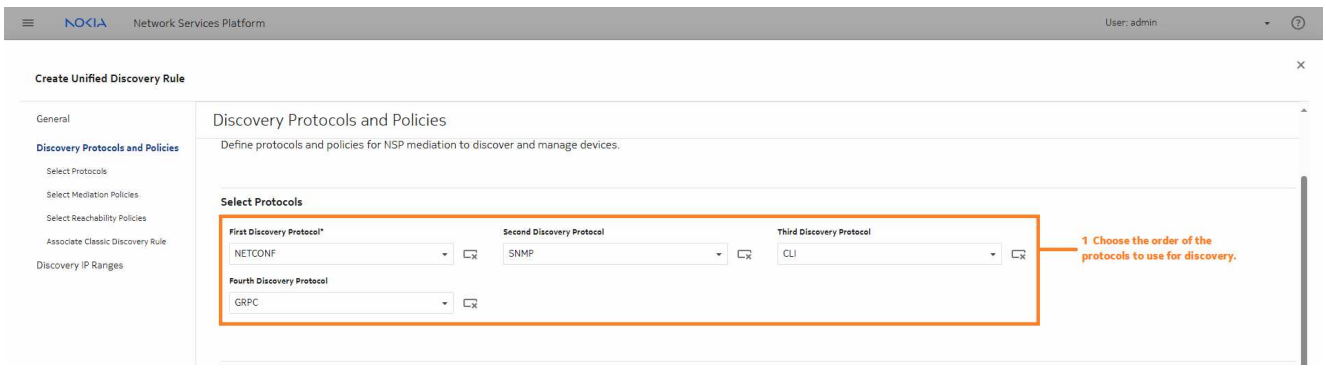


First, we'll configure the general settings for the discovery rule. Enter a name for the rule and a scan interval. This rule will scan the network every 90 minutes to look for devices and device updates.



2

To configure Discovery Protocols and Policies, we'll choose the order of the protocols to use for discovery, and create and associate the required mediation and reachability policies. In this example, we don't need the gRPC protocol for discovery, but we'll include it for telemetry communication after the NE is managed.



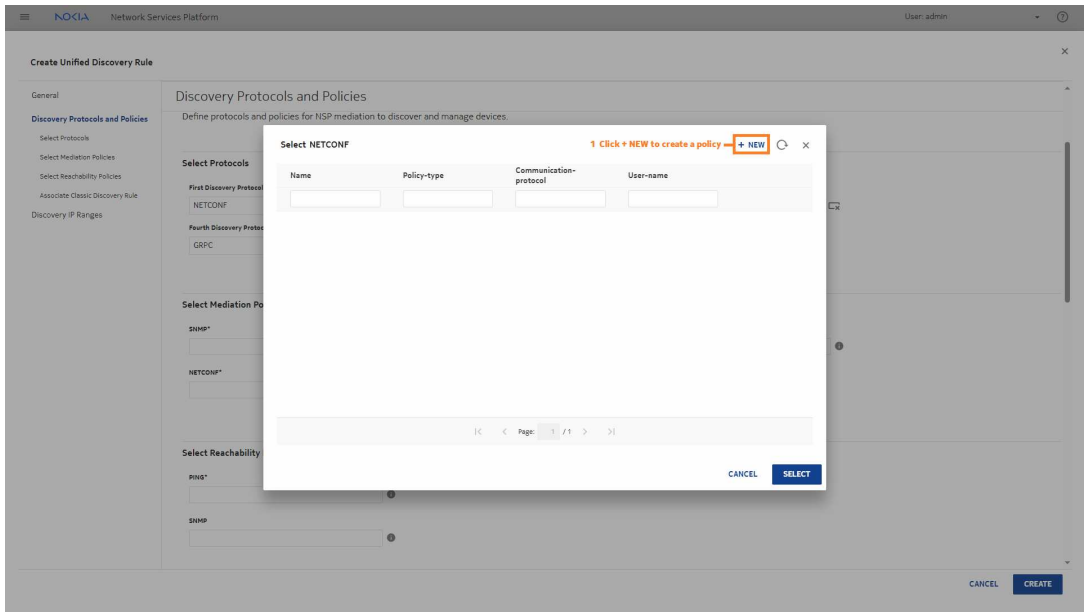
3

Now we will create mediation policies for the protocols we'll need to use to discover and manage the NE, and associate them with the discovery rule.

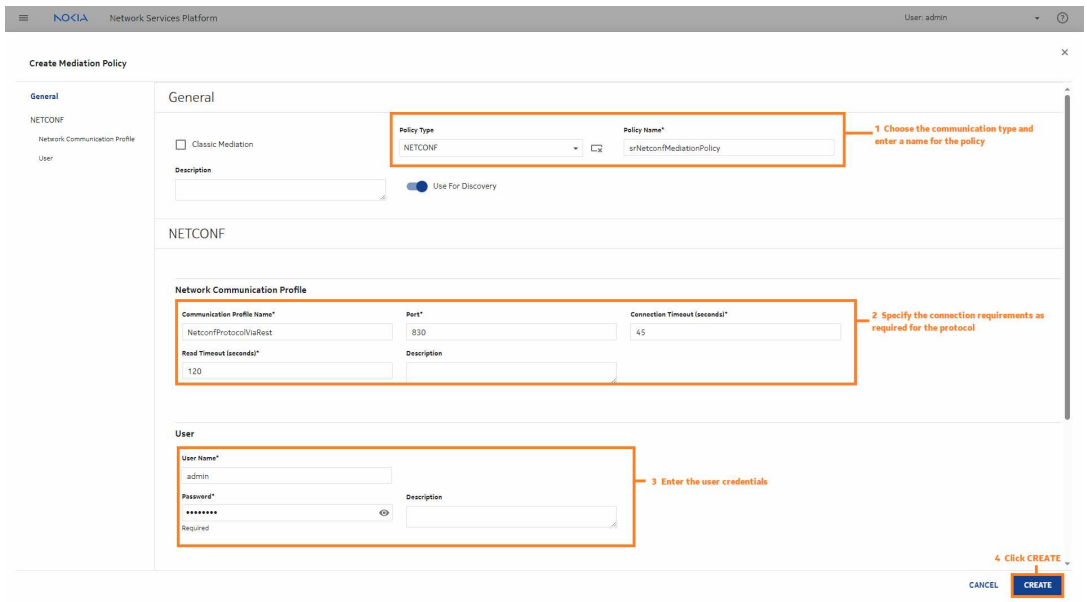
These steps need to be done for each mediation protocol we selected. We'll use NETCONF as an example.

1. Click in the NETCONF field in the Select Mediation Policies panel to open the Select

NETCONF policy form.

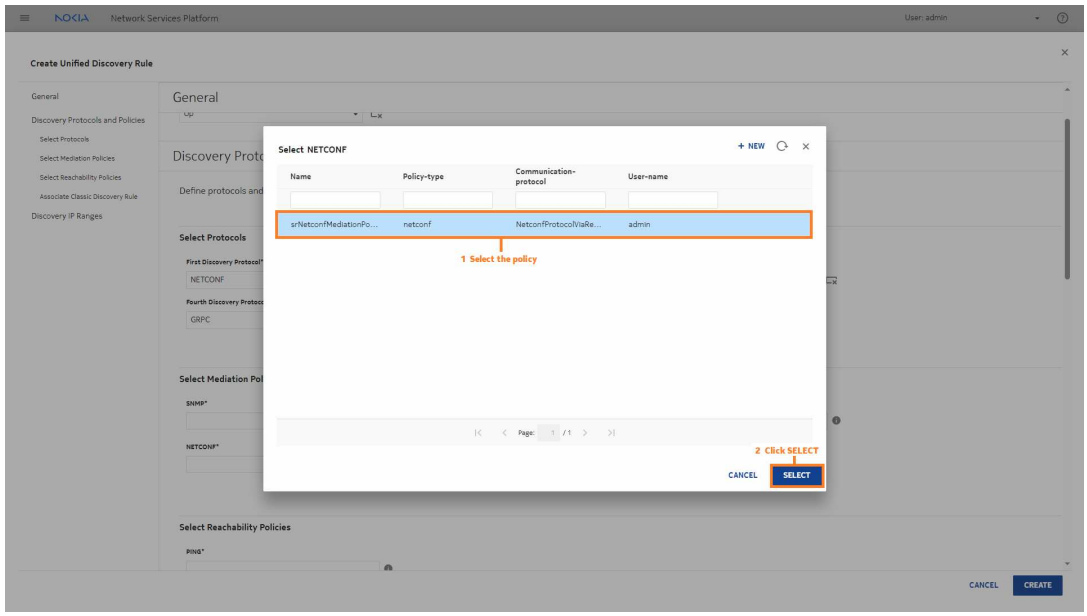


2. Click + **NEW** to open the **Create Mediation Policy** form in a new browser tab.



3. When the policy is created, return to the previous browser tab and click refresh (

) in the select form. Click the policy you created and click **SELECT**.



Repeat this step with the other mediation policies.

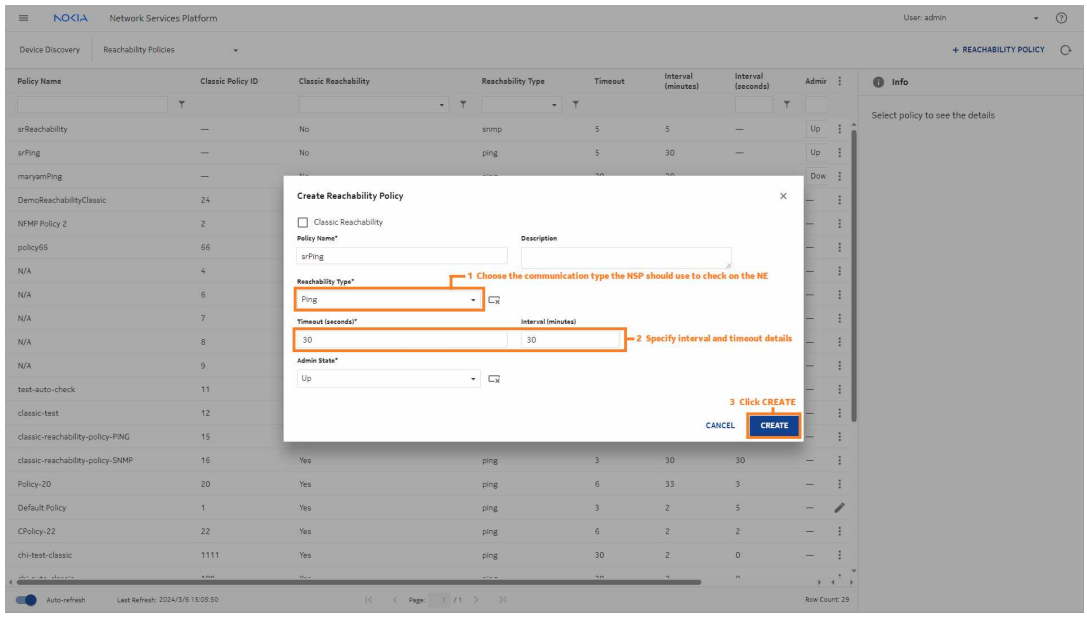
4

The last part of the protocol and policy setting is creating the reachability policies.

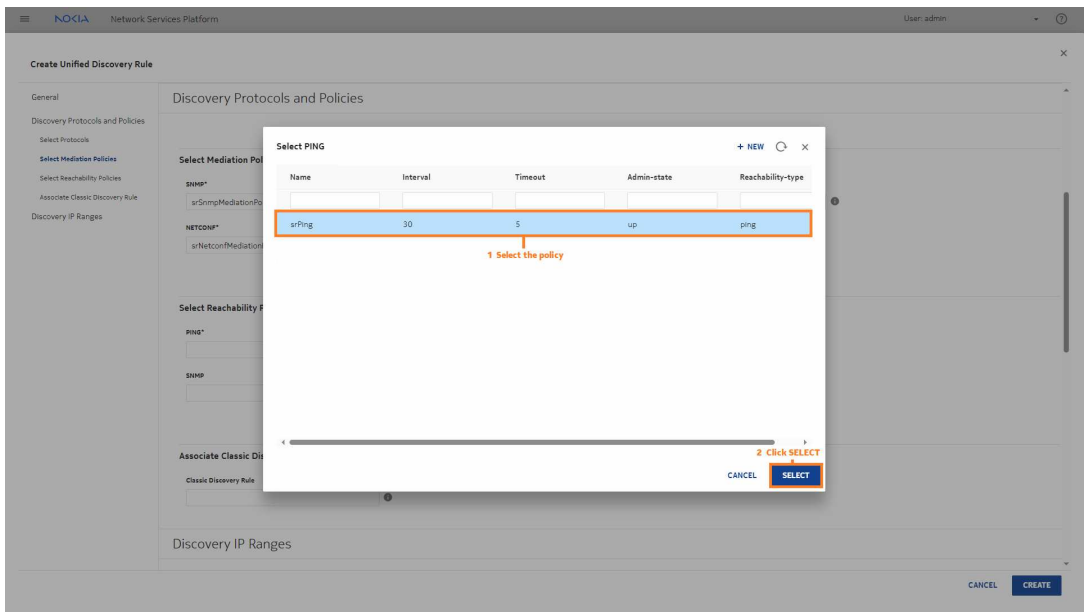
We'll follow a similar process: creating the policies we need and associating each with the discovery rule. This time we'll use Ping as an example.

1. Click in the PING field in the Select Reachability Policies panel to open the Select PING policy form.
2. Click + **NEW** in the Select PING policy form to open the **Create Reachability Policy** form

in a new browser tab.



3. When the policy is created, return to the previous browser tab and click refresh ( ) in the select form. Click the policy you created and click **SELECT**.



Repeat this step with other reachability policies.

5

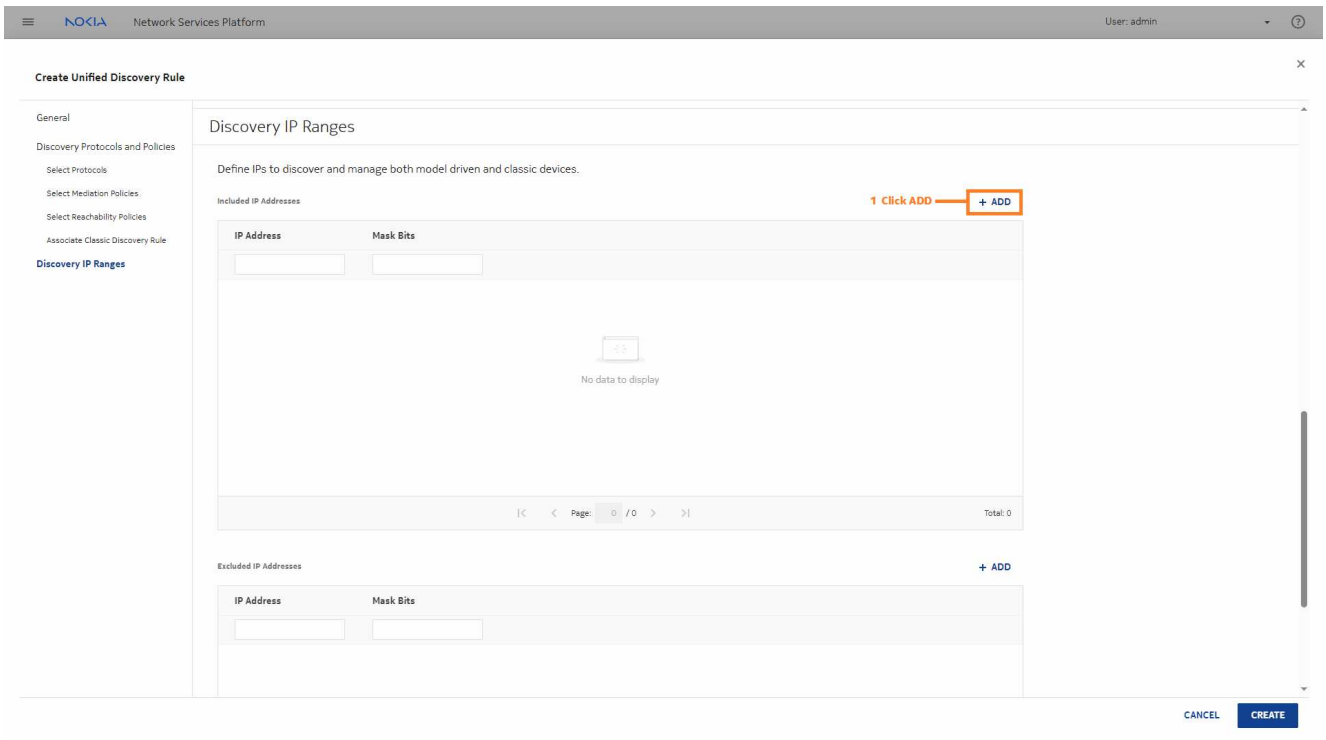
To use this unified discovery rule to discover classic devices, we need to associate a classic discovery rule. This discovery rule will be for model-driven devices only, so we can skip this field.

6

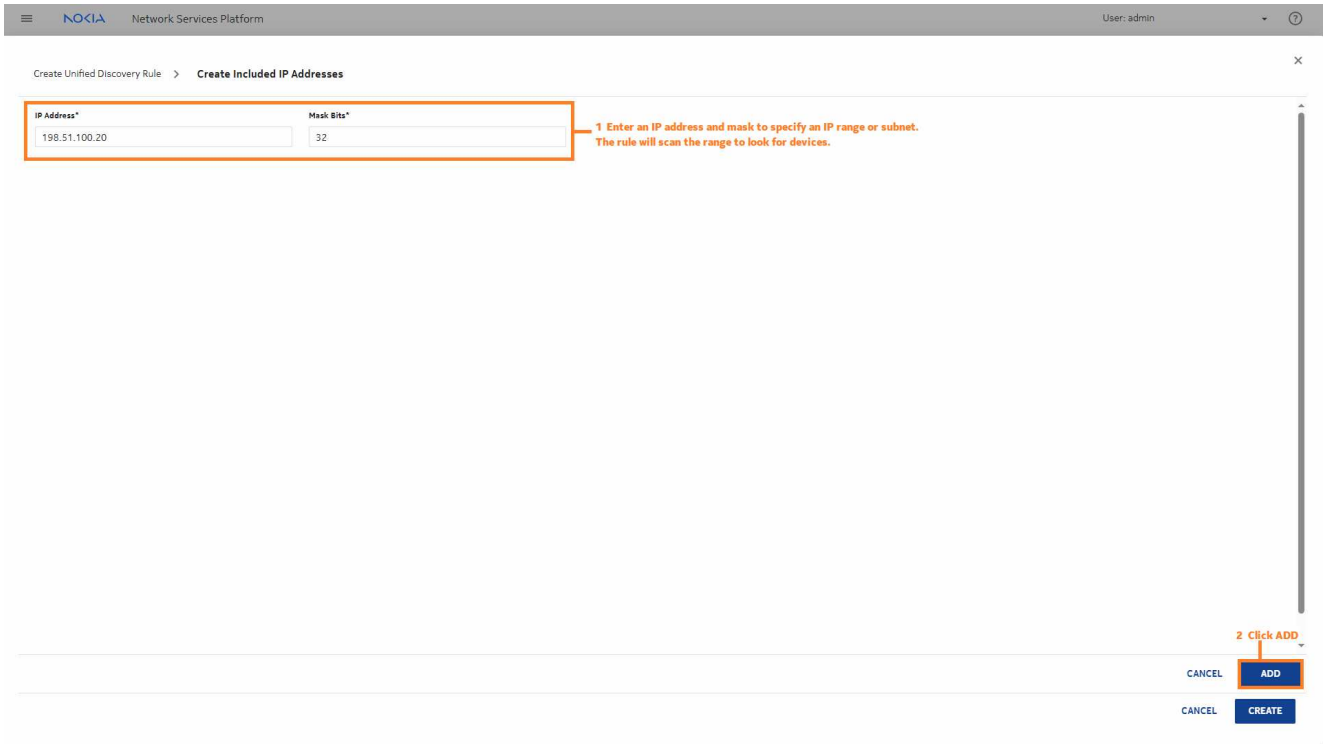
Next, we'll add an IP range or subnet for discovery. The device we want to discover must be in this range.

When the discovery rule performs a network scan in the future, it will search the IP range.

Click **+ ADD** in the Included IP Addresses area.

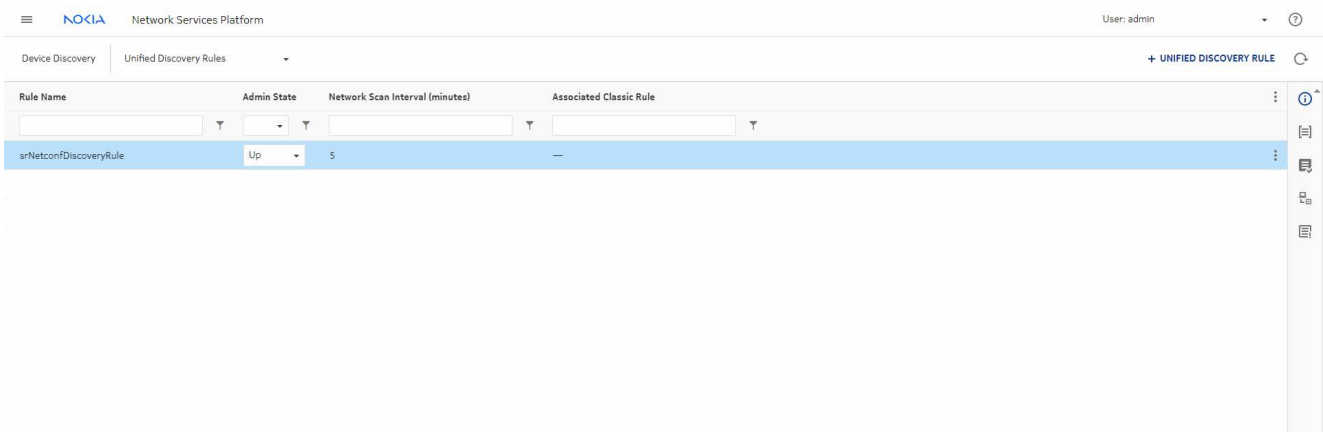


In the form that opens, enter the IP address and mask bits, and click **ADD**.



7

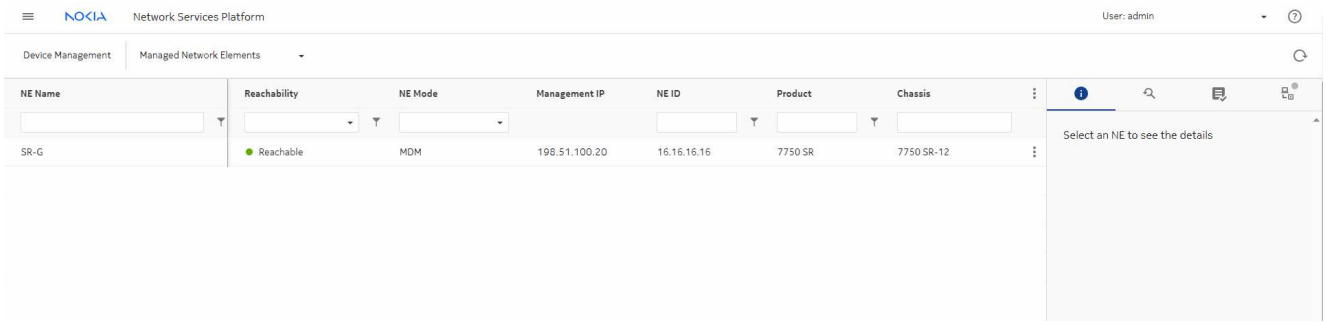
After you click **CREATE**, the discovery rule appears in the list. Choose Discover from the Table row actions menu to run the discovery rule manually.



END OF STEPS

Result

When the NE is discovered, the NE appears in the **Device Management**, **Managed Network Elements** view.



The NE has been discovered.

10.2 NFM-P and NSP comparison: Port Configuration

10.2.1 Before you begin

This use case shows how to use Infrastructure Configuration Management in NSP to configure ports in preparation for LAG and MC-LAG creation.

Click on a figure to enlarge it.

NFM-P method

For comparison, here are the steps we would have performed in the NFM-P to configure the ports.

1. On the equipment tree, expand Network→*NE*→Shelf→Card Slot *n*→Daughter Card Slot *n*→Port *n/n/n*.
2. Right-click on the Port icon and choose Properties. The Physical Port (Edit) form opens.
3. Update the parameters as required and click Apply.
4. Save your changes and close the form.

This procedure needs to be performed for each port you need to configure, on each NE that will be part of the LAG or MC-LAG.

Infrastructure Configuration Management method

You can configure all the ports in one operation by deploying a configuration template.

In this example, the configuration template **Ready_Access_Ports_4_LAG** has been created using the predefined `icm-equipment-port-access` intent type; see 9.5 “How do I import a configuration intent type?” (p. 118) and 9.10 “How do I create a configuration template?” (p. 127).

Use this procedure to use this template to configure the ports.

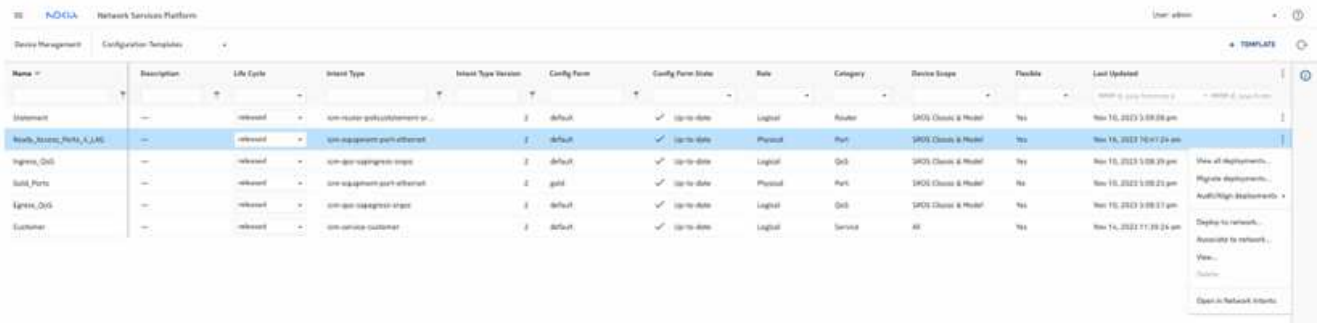
10.2.2 Steps

1

Open **Device Management**, **Configuration Templates**.

2

Select **Ready_Access_Ports_4_LAG** from the list of configuration templates and click ⋮ (Table row actions), **Deploy to Network**.

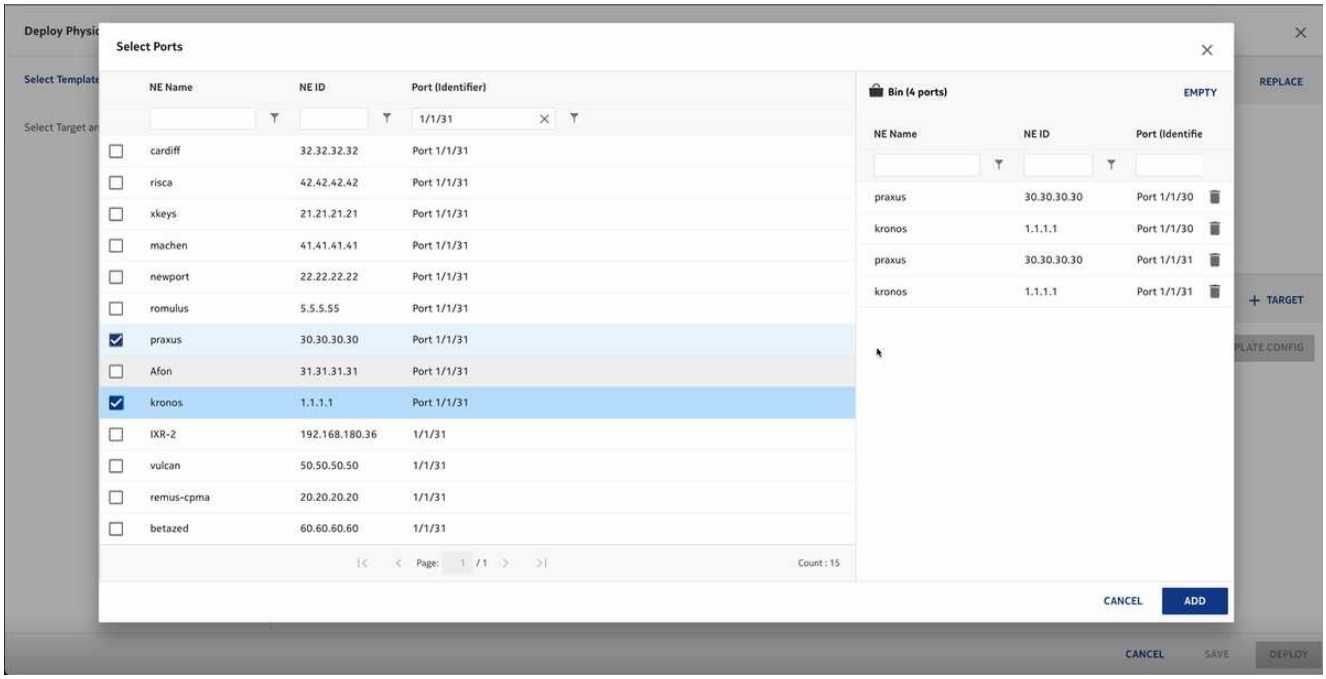


3

In the form that opens, click + **TARGET** and choose Ports.

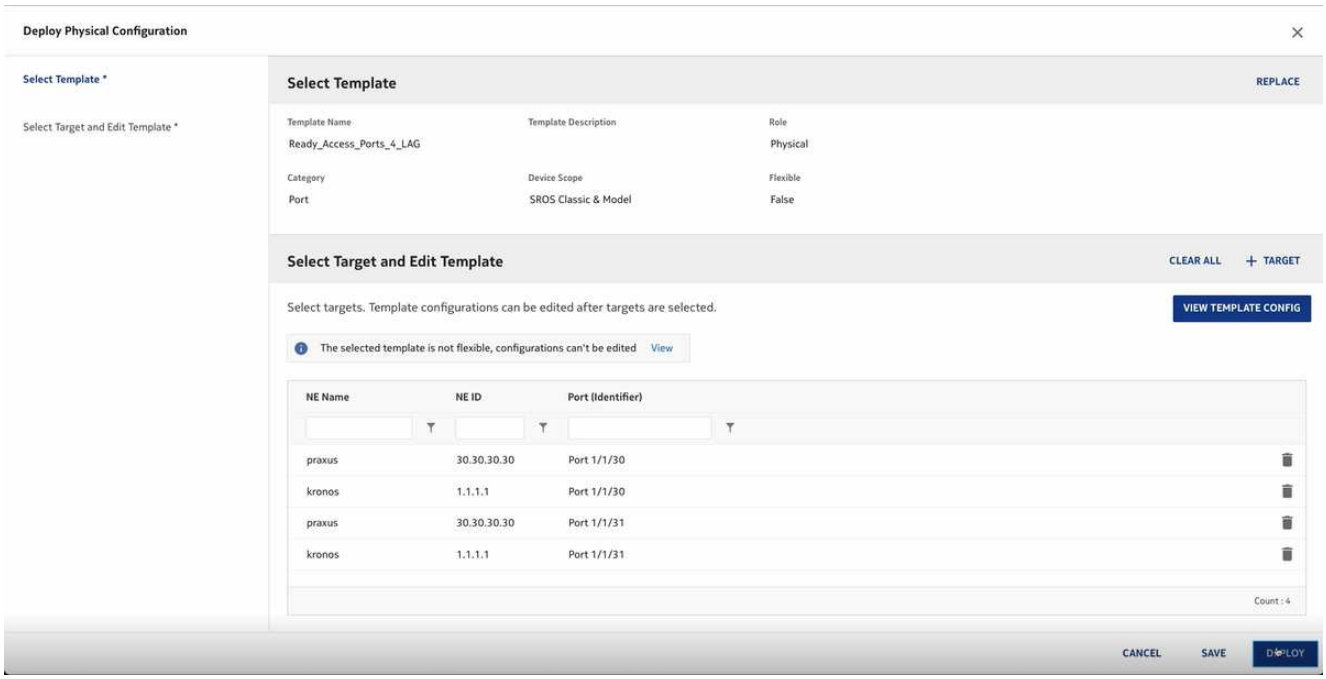
4

Filter on the port numbers to find the ports you want to configure, and click **ADD** to add them to the list of targets.



5

Click **DEPLOY** to send the configuration to all the ports you selected.



End of steps

10.3 NFM-P and NSP comparison: QoS

10.3.1 Before you begin

This use case shows how to use Infrastructure Configuration Management in NSP to discover an existing QoS policy from a device and synchronize it to other NEs in the network..

Click on a figure to enlarge it.

NFM-P method

For comparison, here are the steps we would have performed in the NFM-P to distribute the policy to multiple NEs.

1. Create the policy on the NE using CLI.
2. Choose Policies→QoS→SROS QoS→Access Egress→SAP Access Egress from the NFM-P main menu.
3. Click Search and select the new policy.
4. Double-click on the policy to open the Edit form.

   The new policy is a local policy, in Draft configuration mode.
5. Click More Actions, Synchronize.
6. Choose the NE to which the policy is to be synchronized from the Available Local Policies list and click on the right-arrow. The chosen NE moves to the Selected Source Local Policy panel of the form.
7. Click Synchronize. The new local policy definition is synchronized with the global policy.
8. From the Edit form, click Switch Mode to release the policy and distribute it to other NEs.
9. Select the NEs for distribution in the Available Object panel and click on the right-arrow button.
10. Click Distribute.

The policy is now available on the selected NEs.

Infrastructure Configuration Management method

You can discover, release and distribute the new policy to classic or model driven NEs by deploying a configuration template.

In this example, the QoS policy has been created on the node using CLI.

The configuration template **SAP Egress Policy** has been created using the predefined `icm-qos-sapegress-srqos` intent type; see 9.5 “How do I import a configuration intent type?” (p. 118) and 9.10 “How do I create a configuration template?” (p. 127).

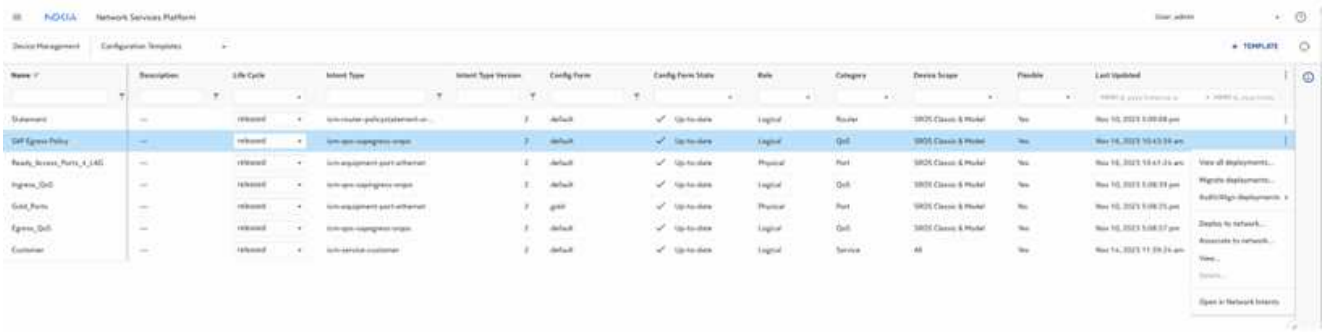
To use this template to discover and distribute the new policy:

For this scenario, we will associate the template to the network. Associating the template ensures that no existing QoS policy values on the NE will be overwritten with template values.

10.3.2 Steps

1

Select **SAP Egress Policy** from the list of configuration templates and click ⋮ (Table row actions), **Associate to Network**.

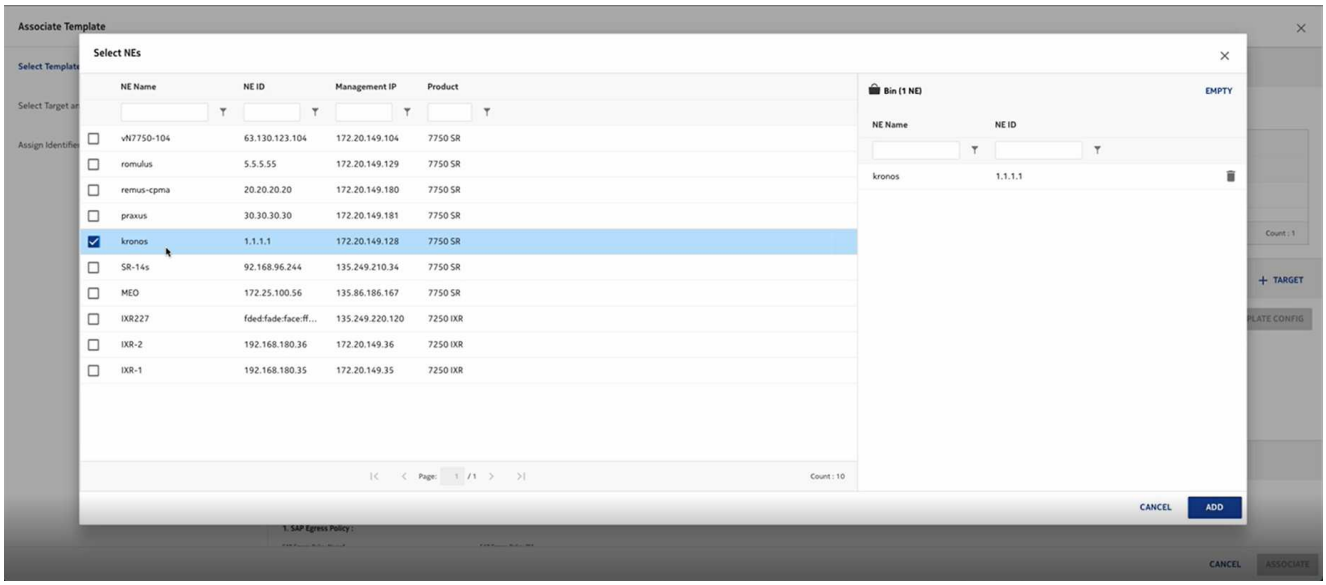


2

In the form that opens, click **+ TARGET** and choose NEs.

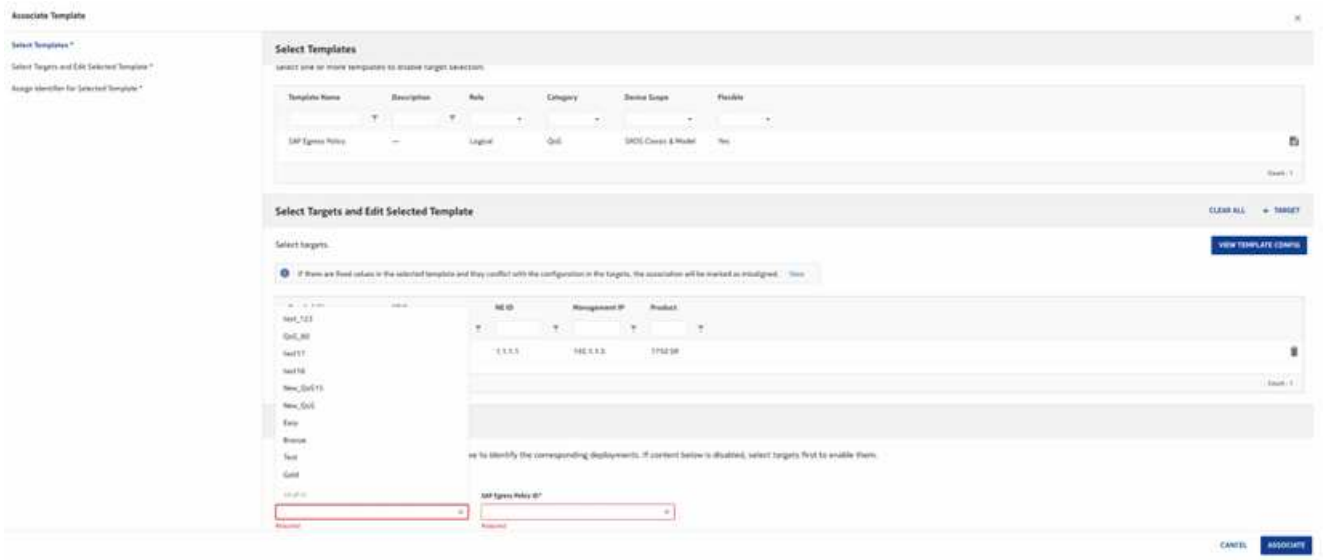
3

Choose the NE where the new policy is added and click **ADD**.



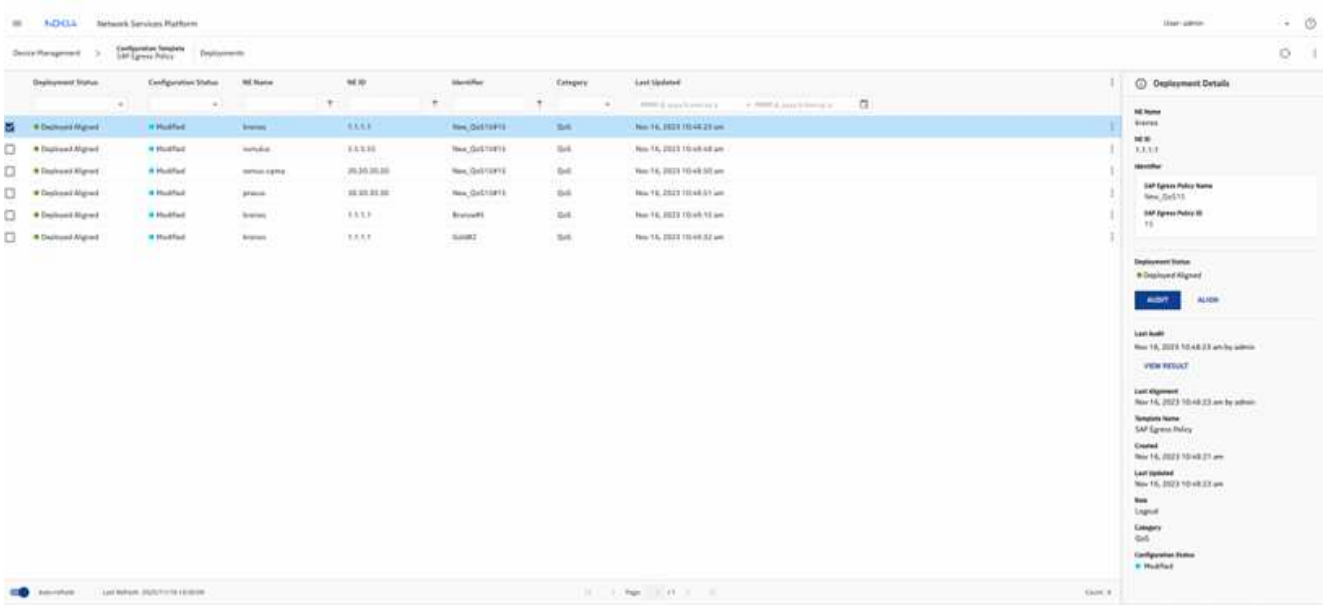
4

Select the existing policy name and ID for the NE and click **ASSOCIATE**.



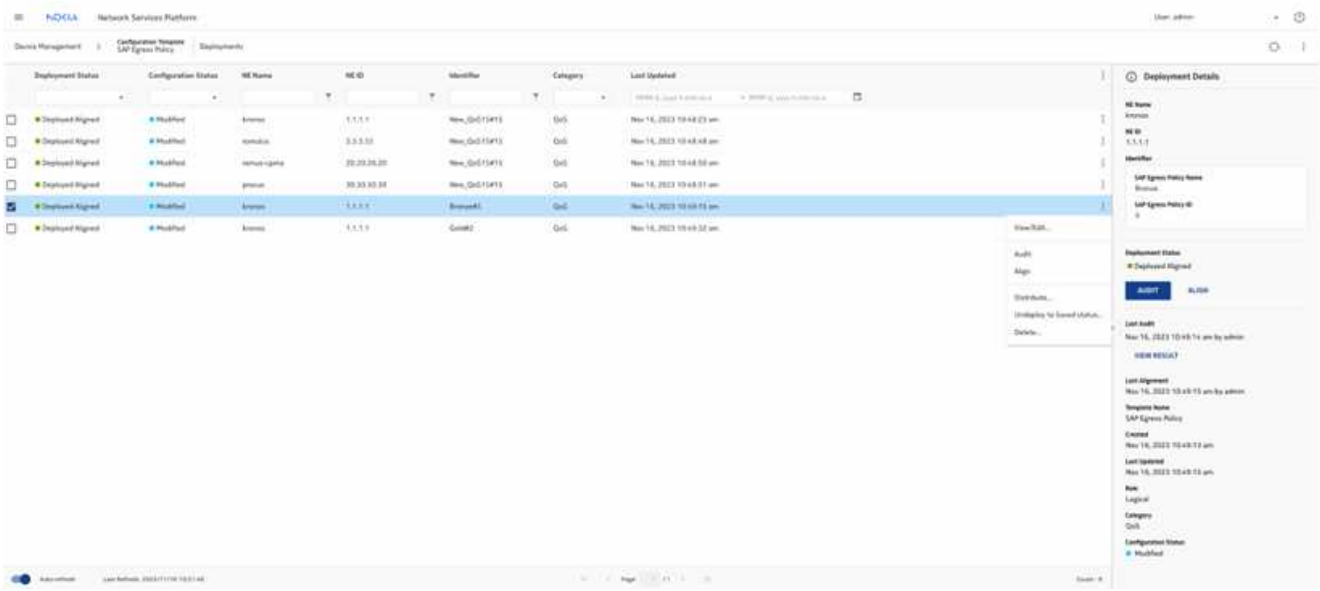
5

The template has now been deployed. Double-click on the template to see the deployment in the list of deployments for the template.



6

Choose the deployment and click ⋮ (Table row actions), Distribute.



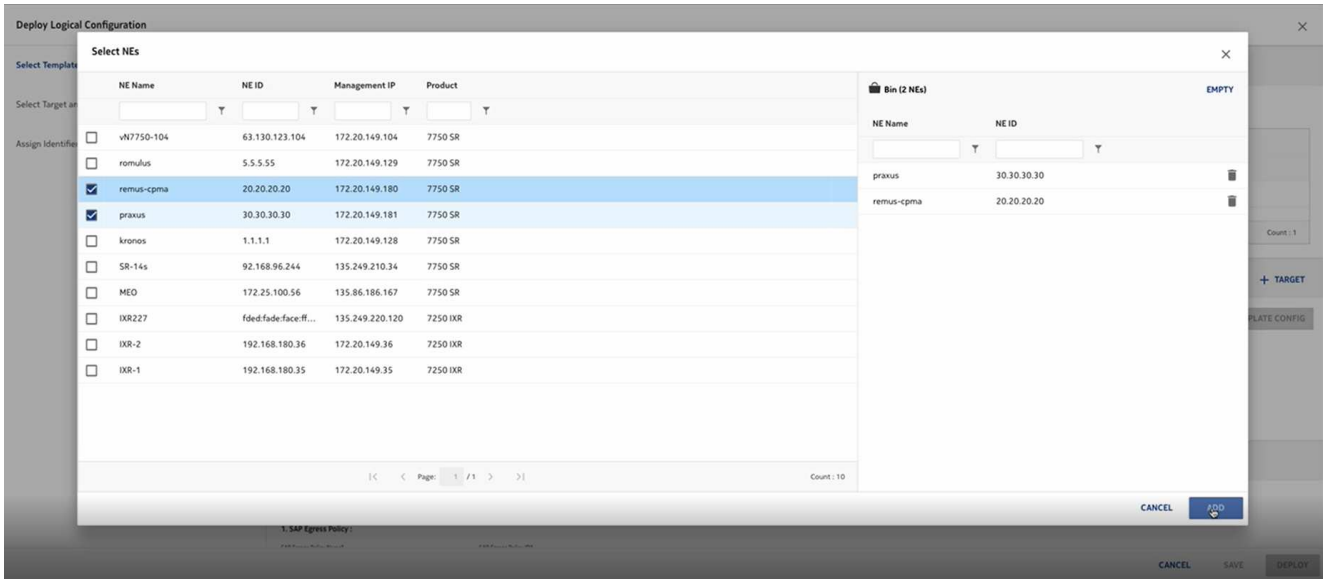
7

In the Deploy Logical Configuration form that opens, click + **TARGET** and choose NEs.

All compatible managed NEs appear in the list, regardless of management type.

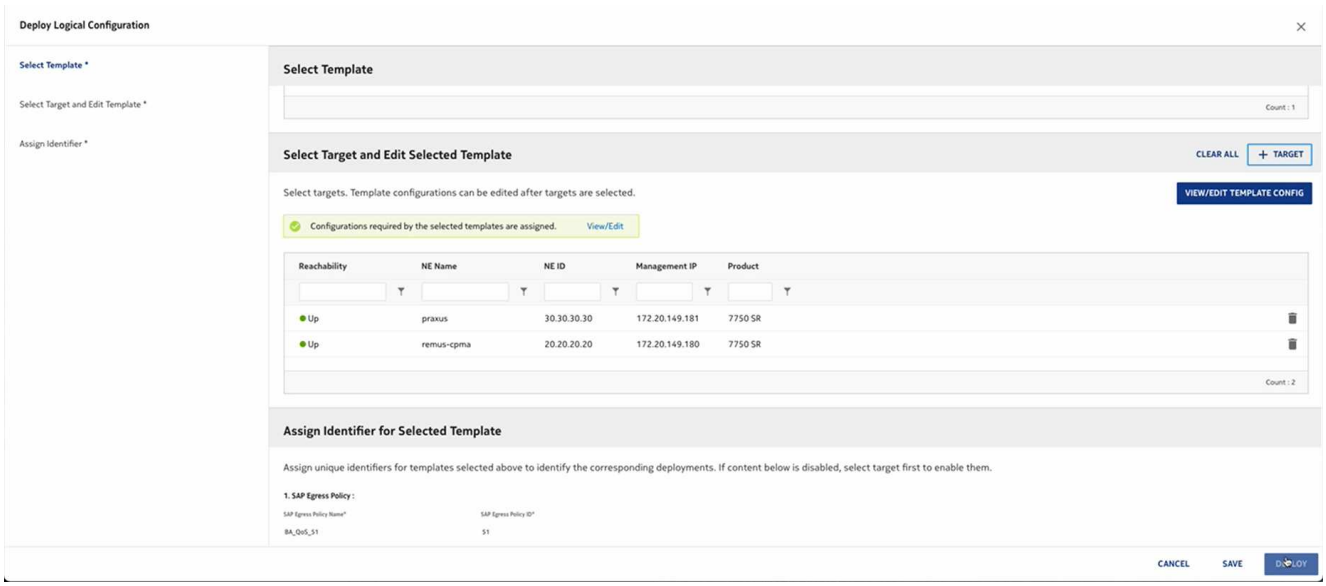
8

Select the NEs you want to distribute the policy to and click ADD.



9

Click **DEPLOY**.



END OF STEPS

10.4 NFM-P and NSP comparison: LAG Configuration

10.4.1 Before you begin

This use case shows how to use Infrastructure Configuration Management in NSP to create a LAG.

Click on a figure to enlarge it.

NFM-P method

For comparison, here are the steps we would have performed in the NFM-P to create a LAG.

1. Prepare the ports:
   a. On the equipment tree, expand Network→*NE*→Shelf→Card Slot *n*→Daughter Card Slot *n*→Port *n/n/n*.
   b. Multi-select the required ports, right-click and choose Properties. The Physical Port (Multiple Instances) (Edit) form opens.
   c. Update the parameters as required and click Apply.
   d. Save your changes and close the form.
2. On the equipment tree, expand Network→*NE*→Logical Groups→LAGs.
3. Right-click on LAGs and choose Create LAG.
4. Proceed through the wizard, configuring parameters as required, and click Finish.

Infrastructure Configuration Management method

You can configure all the ports in one operation by deploying a configuration template. Deploy another template to create the LAG.

In this example, the following configuration templates have been created; see 9.5 “How do I import a configuration intent type?” (p. 118)and 9.10 “How do I create a configuration template?” (p. 127).

- **Gold_Ports** , which uses the predefined `icm-equipment-port-ethernet` intent type
- **Gold-LAGs** , which uses the predefined `icm-logical-lag-access` intent type

10.4.2 Steps

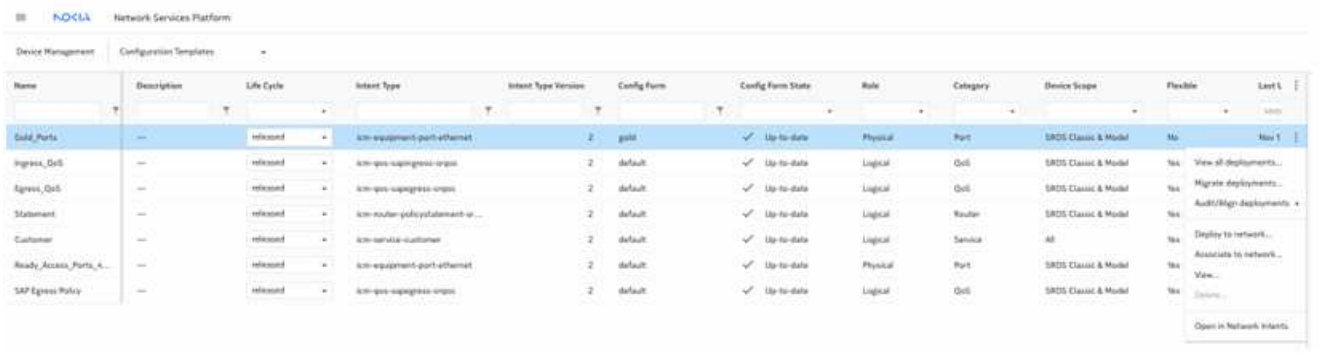
Configure the ports

1

Open **Device Management**, **Configuration Templates**.

2

Select **Gold_Ports** from the list of configuration templates and click ⋮ (Table row actions), **Deploy to Network**.

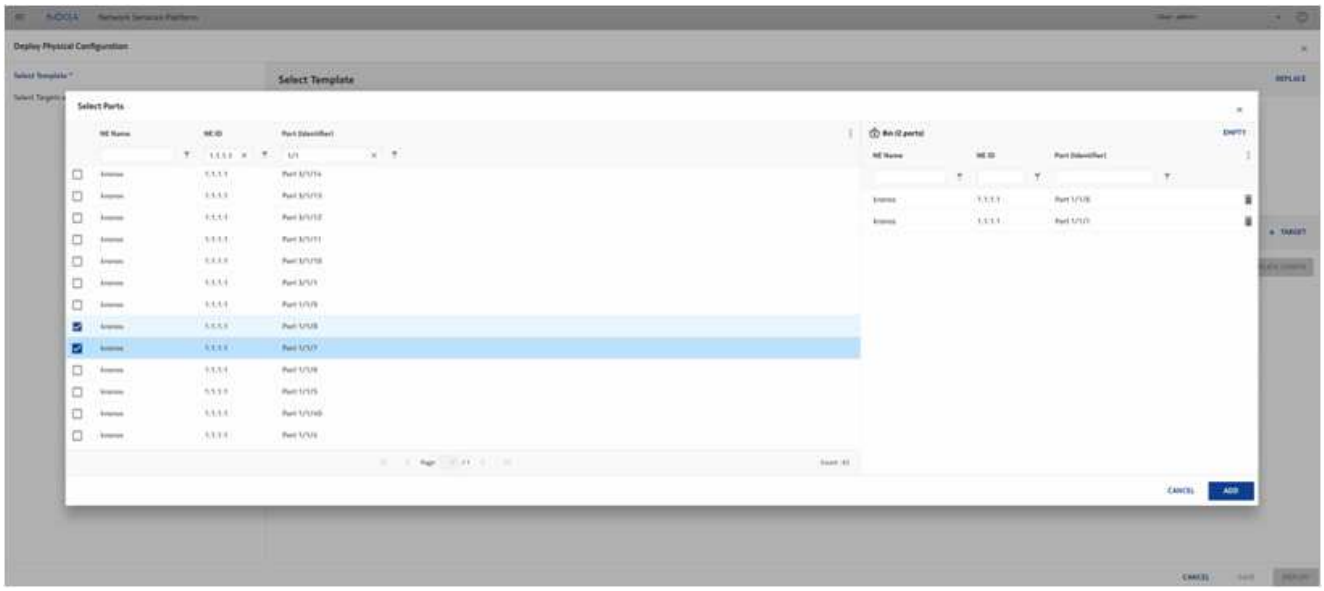


3

In the form that opens, click **+ TARGET** and choose Ports.

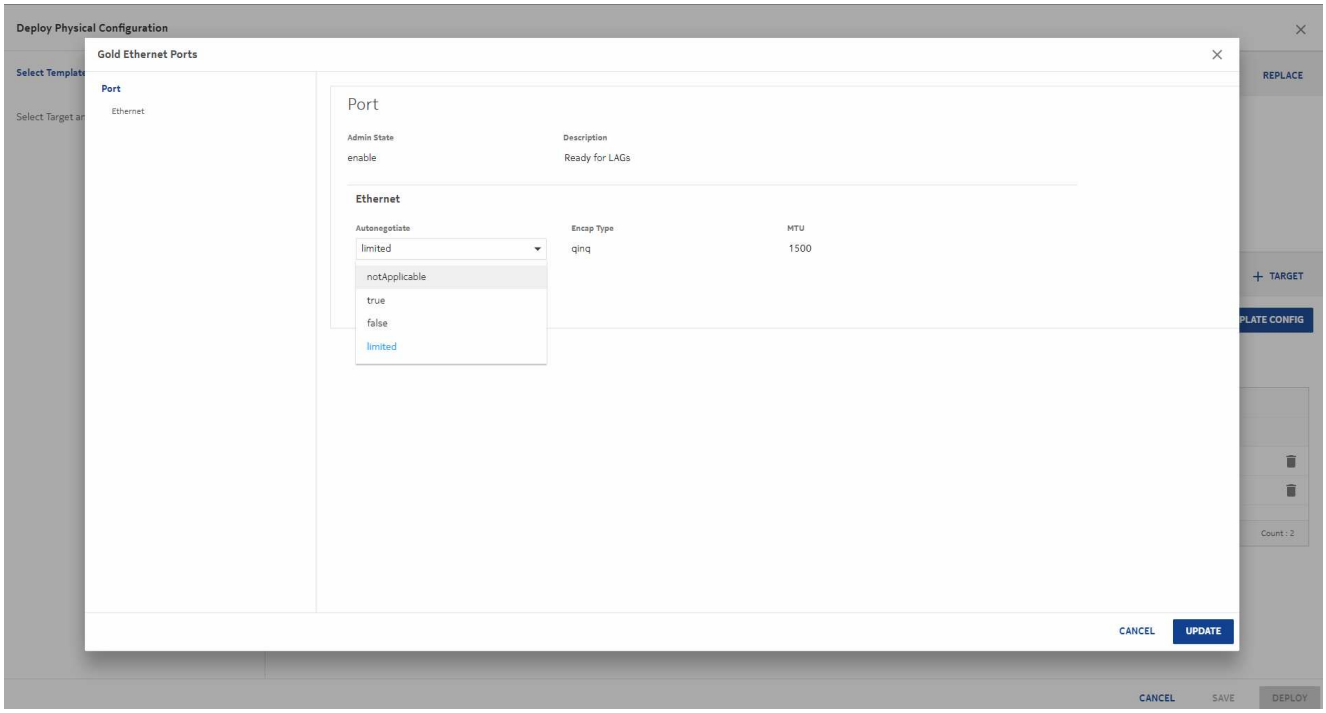
4

Filter on the NE name and port numbers to find the ports you want to configure, and click **ADD** to add them to the list of targets.



5

This template is flexible: you can click **View/Edit Template Config** to verify the configuration and update it if needed.

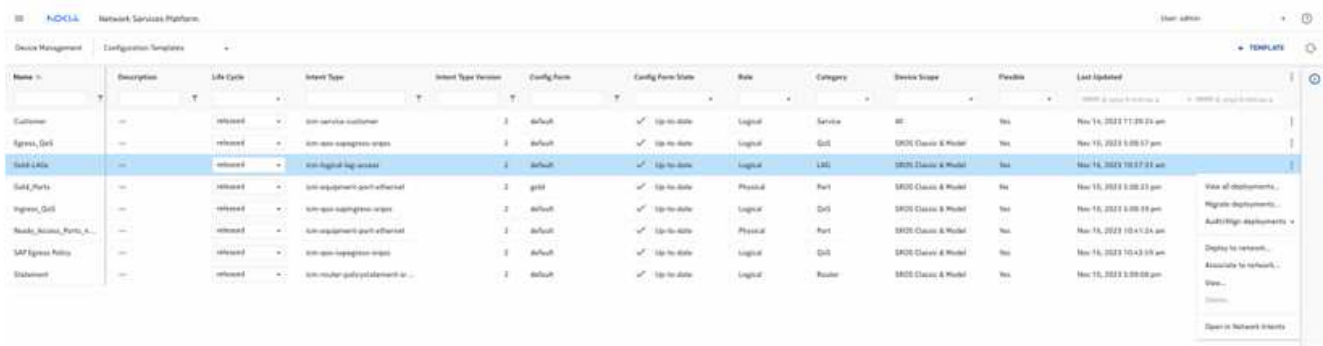


Click **UPDATE** to close the View form, and **DEPLOY** to send the configuration to the ports.

Configure the LAG

6

Select **Gold-LAGs** from the list of configuration templates and click ⋮ (Table row actions), **Deploy to Network**.



7

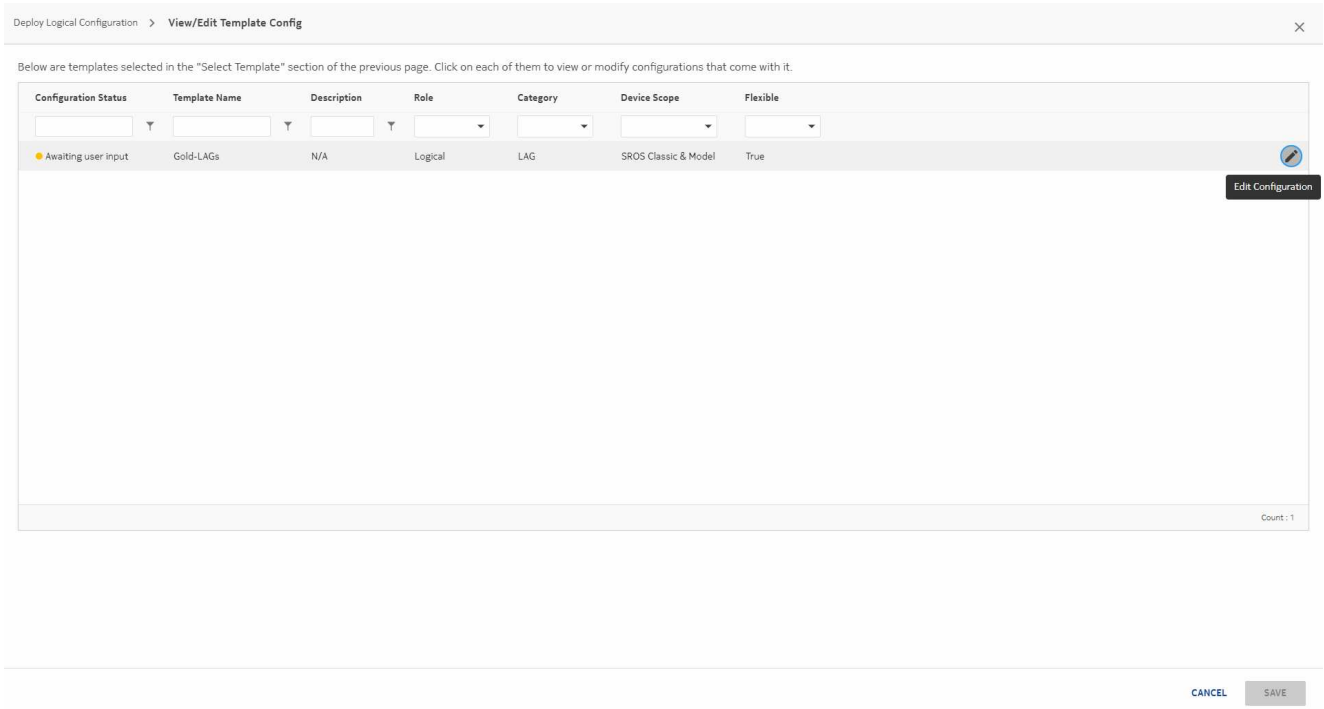
The template only accepts one target. Click **+ TARGET** and choose NEs.

Select the NE in the form that opens.

8

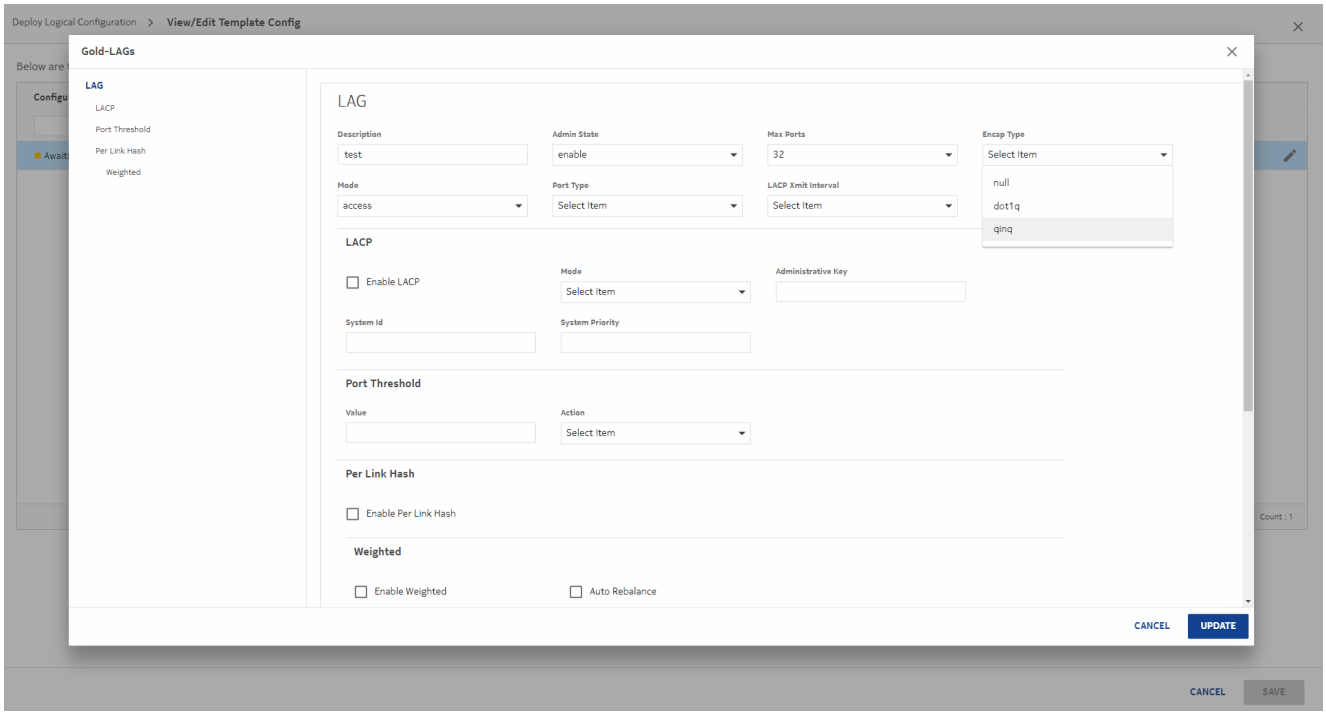
Click **View/Edit Template Config** to view and set the LAG parameters.

In the form that opens, select the template and click **Edit Configuration**.



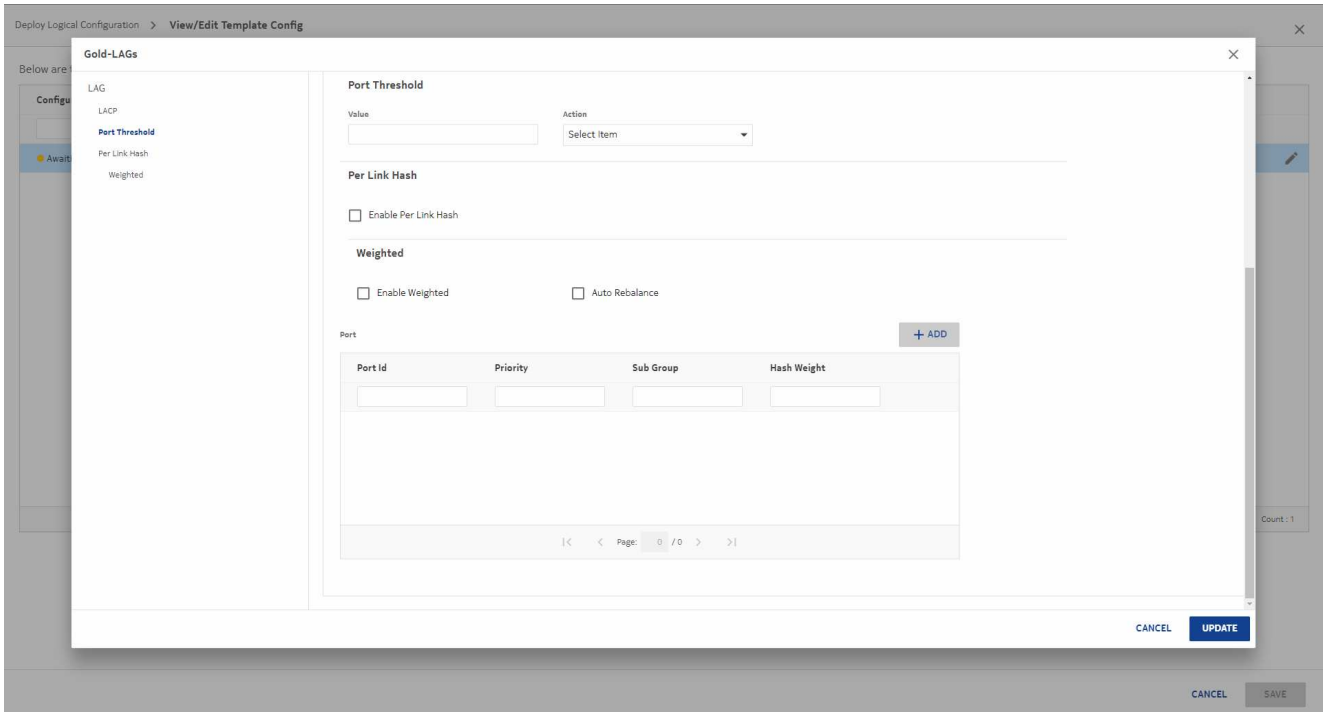
9

Configure the LAG parameters as needed.



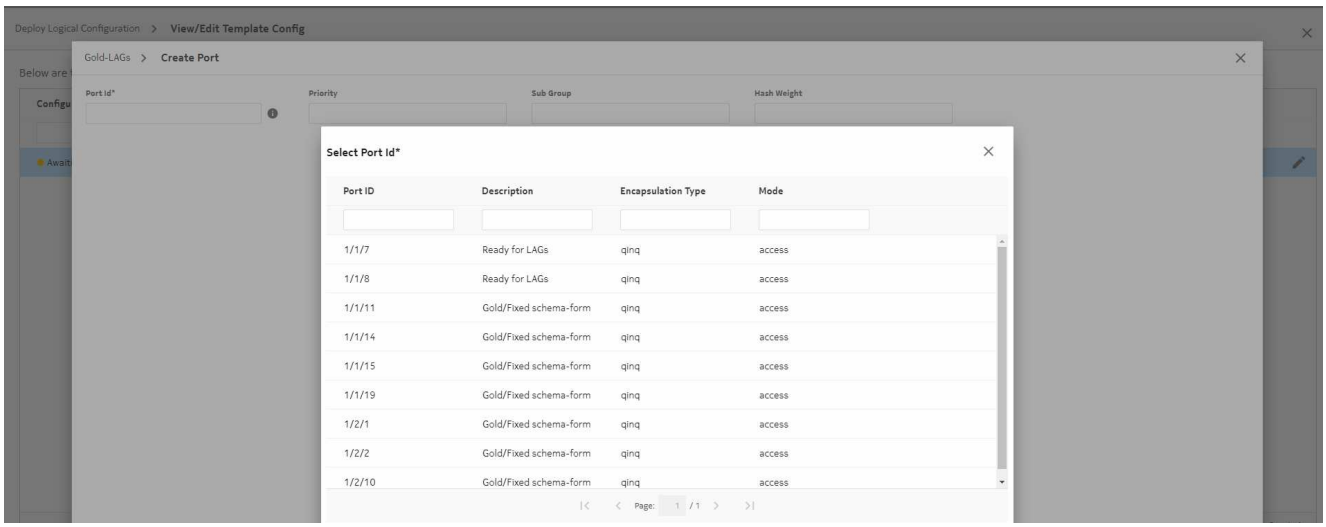
10

Click + **ADD** to add the ports you configured with the previous template.



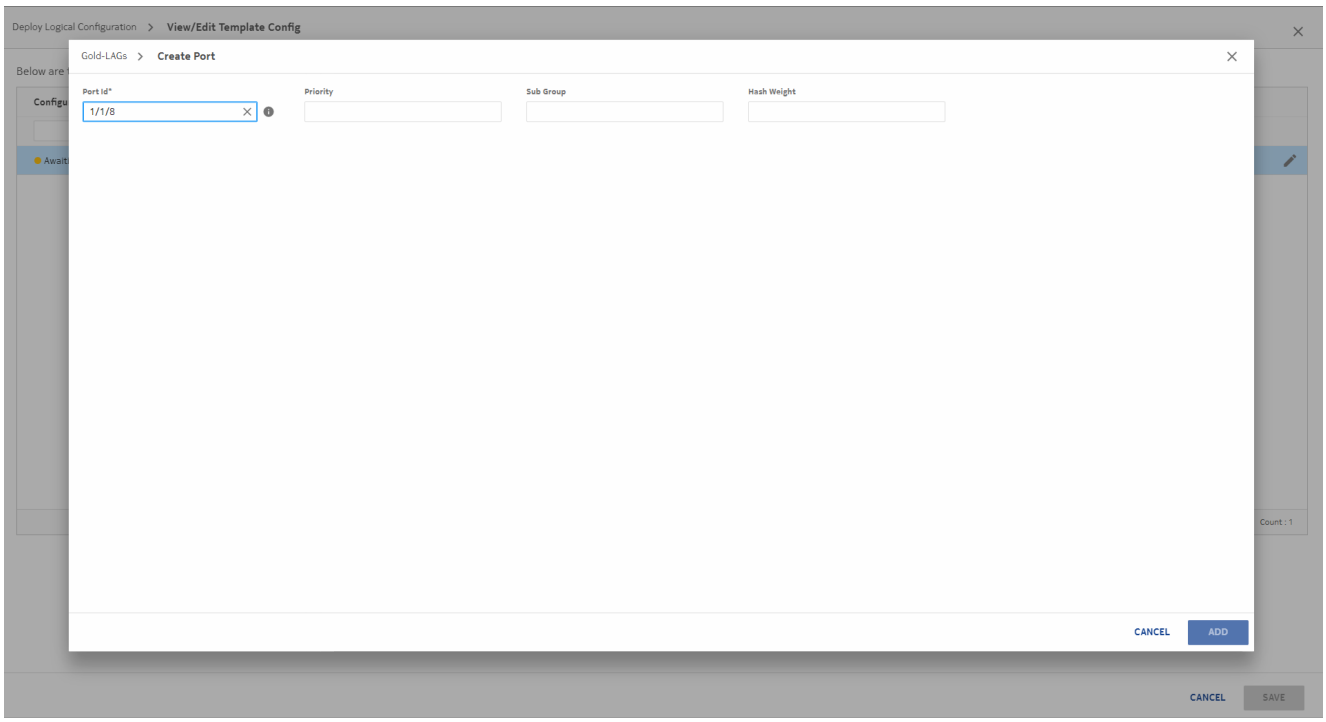
11

In the form that opens, select a port and click **SELECT**.



12

Configure port parameters as needed and click **ADD**.

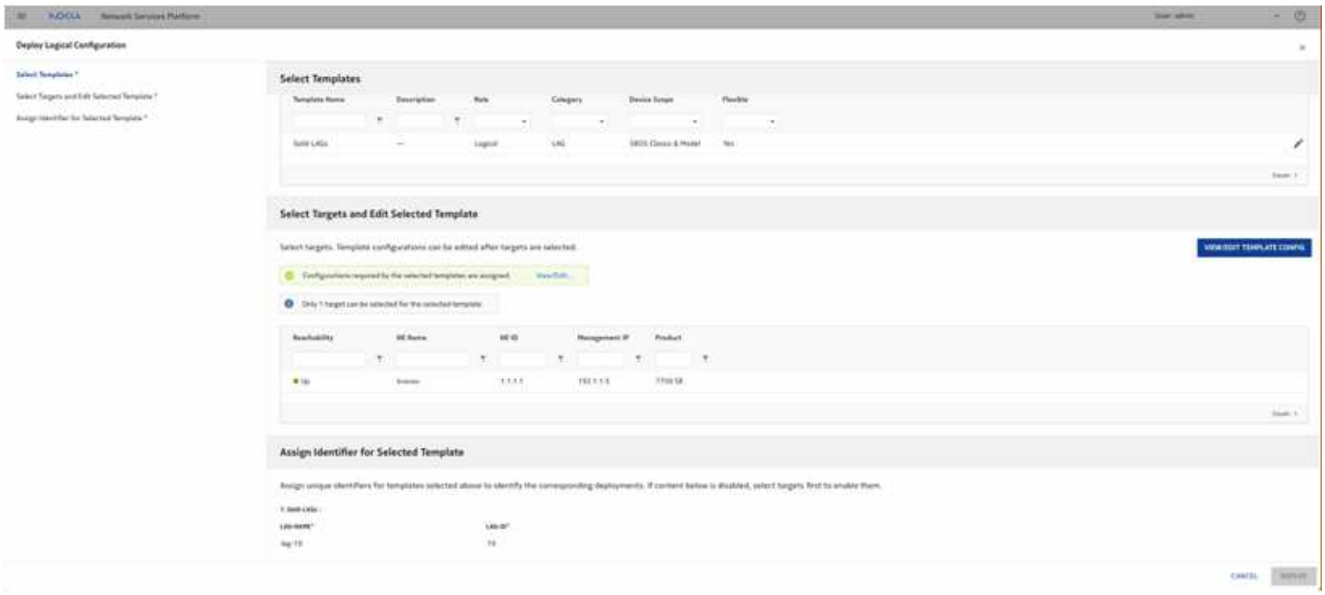


13

Repeat the steps to add the other port and click **UPDATE**. Click **SAVE** to exit the View/Edit form.

14

Enter a name and ID for the LAG and click **DEPLOY**.



END OF STEPS

Result

Double click on **Gold-LAGs** in the template list to see the deployments and show the newly created LAG.