



NSP

Network Services Platform

Release 24.4

Device Management Guide

3HE-20005-AAAA-TQZZA
Issue 1
April 2024

© 2024 Nokia.

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

Legal notice

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

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

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

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

No part of this document may be modified.

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

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

© 2024 Nokia.

Contents

- About this document** 11
- Part I: Device management essentials** 13
- 1 Device support in NSP** 15
 - 1.1 How does NSP support devices? 15
 - 1.2 What devices are supported by NSP? 15
 - 1.3 What is an adaptor? 16
 - 1.4 Where can I find more information about adaptors? 16
 - 1.5 How does NSP support device telemetry? 17
 - 1.6 How do I configure and manage devices? 17
 - 1.7 How do I view adaptor information for an NE? 20
 - 1.8 What is NE resynchronization? 21
 - 1.9 What is a device management state? 21
- 2 Device discovery** 23
 - Discovering devices using NSP** 23
 - 2.1 How does device discovery work? 23
 - 2.2 What is a unified discovery rule? 24
 - 2.3 What is a classic discovery rule? 24
 - 2.4 What are discovery protocols and policies? 25
 - 2.5 What is flexible discovery for MDM devices? 26
 - 2.6 What is a domain controller? 27
 - Procedures for device discovery** 28
 - 2.7 How do I create a classic mediation policy? 28
 - 2.8 How do I create a mediation policy for MDM? 29
 - 2.9 How do I edit or delete a mediation policy? 30
 - 2.10 How do I create a classic reachability policy? 31
 - 2.11 How do I create a reachability policy for MDM ? 32
 - 2.12 How do I edit or delete a reachability policy? 32
 - 2.13 How do I create a classic discovery rule? 33
 - 2.14 How do I discover devices? 34
 - 2.15 How do I edit or delete a discovery rule? 36
 - 2.16 How do I stitch a classic device to a unified discovery rule? 37
 - 2.17 How do I discover a domain controller? 38
 - 2.18 How do I discover the NEs managed by a domain controller? 39

2.19	How do I edit or delete a domain controller?	40
3	NE maintenance	43
	NE backup and restore	43
3.1	How do I back up an NE?	43
3.2	How do I view backup files for an NE?	44
3.3	How do I compare two backup files for an NE?	44
3.4	How do I restore an NE from a backup?	45
	Part II: Advanced device management	47
4	Large-scale operations	49
	Overview	49
4.1	Operations	49
4.2	Operation views	51
4.3	Operation types provided by NSP	52
	Procedures	54
4.4	How do I change the life cycle state of an operation type?	54
4.5	How do I start or schedule a new operation?	54
4.6	How do I start or schedule a saved operation?	56
4.7	How do I view or manage scheduled operations?	57
4.8	How do I view current operations and executions?	57
4.9	How do I start, stop, or pause an operation?	58
4.10	How do I view the details of completed operations?	58
4.11	How do I view a history of operations performed on an NE?	59
4.12	How do I automate the cleanup of completed operations?	59
4.13	How do I view reports generated by an operation?	60
4.14	How do I retry an execution within a phase?	61
4.15	How do I terminate an execution in progress?	62
4.16	How do I retry a failed operation?	62
4.17	How do I perform a rollback on a target in an operation?	63
	Troubleshooting	65
4.18	Operation troubleshooting	65
5	NE software upgrades using NSP	67
	NE software upgrades using NSP	67
5.1	Upgrade operation requirements	67
5.2	Process for NE upgrade	68
5.3	How do I import an NE software image?	69

5.4	How do I upgrade software on an NE?	70
6	Zero Touch Provisioning	75
6.1	What is Zero Touch Provisioning?.....	75
6.2	How do I configure Zero Touch Provisioning?.....	77
6.3	Can I change ZTP parameters from NSP?	81
	Part III: Device configuration	83
7	Device object configuration	85
	Viewing NE parameters	85
7.1	How do I see what is configured on an NE?	85
	Model Driven Configurator	87
7.2	What tools can I use to configure NEs in NSP?	87
7.3	How do I open a device for configuration?	88
7.4	How do I configure device objects?	89
8	Network configuration	91
	Template-based configuration deployment	91
8.1	What is device configuration in NSP?	91
8.2	How does configuration deployment work?	92
	Configuration process	94
8.3	ICM process	94
	Configuration intent types	98
8.4	What is a configuration intent type?	98
8.5	How do I import a configuration intent type?.....	101
	Configuration templates	102
8.6	What is a configuration template?	102
8.7	What is the difference between deploying a template and associating a template?	105
8.8	How do I create a configuration template?.....	106
8.9	How do I update a template to apply intent type schema form changes?.....	107
8.10	What is migration?	107
8.11	How do I migrate a deployment to another template?	109
8.12	How do I deploy or associate a template to the network?	110
8.13	How do I associate a logical template to the network?	110
8.14	How do I associate a physical template to the network?	111
8.15	How do I retry a failed association?	112
8.16	How do I change the life cycle status of a template?	112
8.17	How do I edit a template?.....	113

8.18	How do I audit or align configurations?	113
	Configuration deployments	115
8.19	How do I create a deployment?.....	115
8.20	How do I create a logical configuration deployment?	115
8.21	How do I create a physical configuration deployment?	116
8.22	How do I edit a deployment?.....	118
8.23	How do I bulk edit multiple deployments?	119
8.24	How do I deploy a saved deployment?	121
8.25	How do I retry a failed deployment?.....	121
8.26	How do I distribute a logical configuration deployment?	122
8.27	How do I distribute a physical configuration deployment?	123
8.28	How do I delete a deployment?.....	124
8.29	How do I remove a deployment?	125
8.30	How do I audit or align a deployment?.....	125
8.31	How do I audit or align configurations for an NE?	126
	Part IV: Device management use cases	129
9	Use cases	131
9.1	Discovery of a 7750 SR device in NSP	131
9.2	NFM-P and NSP comparison: Port Configuration	138
9.3	NFM-P and NSP comparison: QoS.....	141
9.4	NFM-P and NSP comparison: LAG Configuration	146

List of tables

Table 8-1 Results of bulk edit based on handling of added table values120

List of figures

Figure 6-1 Zero Touch Provisioning process.....77

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

Chapter 1, Device support in NSP	15
Chapter 2, Device discovery	23
Chapter 3, NE maintenance	43

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.

1.2 What devices are supported by NSP?

1.2.1 Supported devices

Device support varies by management type.

Classic management

See 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 support, see the *NSP NFM-P Network Element Compatibility Guide*.

Model-driven management

Production adaptors are available for the following Nokia device types:

- SR OS
- SR Linux OS
- MAG-c
- AirFrame
- T-API
- T-BTS

- CBIS

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

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

1.3 What is an adaptor?

1.3.1 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.

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

Commercially available adaptors are released in adaptor suites (zip files) and updated on a regular basis, outside the NSP release cycle. 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.

1.3.2 SDK

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

1.4 Where can I find more information about adaptors?

1.4.1 Artifact guides for adaptor suites

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.

1.4.2 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.

1.5 How does NSP support device telemetry?

1.5.1 Telemetry support

SNMP telemetry for model driven devices is provided by MDM.

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

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

1.6 How do I configure and manage devices?

1.6.1 Device configuration overview

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

This workflow 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.

1.6.2 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?” \(p. 34\)](#).

Configure and manage the discovered device

16

Update parameters on a model-driven NE configuration or state schema tree; see [7.4 “How do I configure device objects?” \(p. 89\)](#).

17

Deploy NE configuration templates to one or more devices; see [8.19 “How do I create a deployment?” \(p. 115\)](#).

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. 43) and [3.4 “How do I restore an NE from a backup?”](#) (p. 45)
- 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.

1.7 How do I view adaptor information for an NE?

1.7.1 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.

1.7.2 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.

1.8 What is NE resynchronization?

1.8.1 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. The resync operation is supported for classic devices.

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 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.

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.

1.9 What is a device management state?

1.9.1 Management state

The management state parameter describes whether a discovered device is included in the managed network. Available actions in the Manage menu depend on the NE mode, management state, and resync status.


1.9.2 Unmanaging devices


You can unmanage a classic device from the NSP. Unmanaging excludes the device from the managed network. The unmanage function may be used for unusual conditions such as when the NSP requires a complete refresh of device data because of data corruption, or when NEs are decommissioned.

When a device is unmanaged, 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 this NE is not removed from the associated discovery rule, this NE will be re-managed in the next scanning interval.

If a device is unmanaged in the NFM-P, it is not removed from the NSP.

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

 **Note:** If you need to unmanage and re-manage an NE with a telemetry subscription configured, a delay may be required to ensure the telemetry subscription will be automatically reinstated. To ensure the telemetry subscription is created again, Nokia recommends waiting at least 15 minutes between unmanaging and re-managing the NE.

1.9.3 Deleting devices

Using the NSP to delete a device completely removes the device from the managed network. All management data is lost.

The next time the discovery rule scans the network, it discovers and manages the device again, or you can run the discovery rule manually.

1.9.4 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.

Management State	NE Mode	Available actions in the Manage menu
Managed, Unmanage Failed	Classic	Resync, Unmanage, Delete
Not Managed	Classic	Manage, Delete
Unmanage Requested, Delete Requested, Unknown	Classic	No actions
Not supported	MD	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 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 port, 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 synched from NFM-P to NSP and available in the Device Discovery or Device Management views. Devices in an unmanaged state are not automatically synched.

 **Important!** To use telemetry and reporting with a synched 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 stitch a classic device to a unified discovery rule?”](#) (p. 37).

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, and a host IP address cannot be included in a discovery rule if the rule includes a subnet the host IP address is in.

 **Note:** A unified discovery rule must include at least one MDM mediation policy and at least one MDM reachability policy, regardless of whether any model driven devices are in the specified IP ranges.

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.

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, CPM reachability

If discovery rules are present in the NFM-P, they are synched 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.

A unified discovery rule must include at least one reachability policy, and at least one mediation policy for each network communication protocol that is used to manage the NE.

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 should be 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, you can 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.

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 can include mediation information for SNMP, CLI, and/or file transfer.

Mediation policies for controller discovery

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

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.

A reachability check is a scheduled check that the NSP initiates via the configured protocol (SNMP or Ping ICMP echo request). If the NE responds, it is reachable from the NSP system. If the device becomes unreachable, an alarm is raised.

2.4.4 Policy synching from NFM-P

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

2.5 What is flexible discovery for MDM devices?

2.5.1 NE compatibility and flexible discovery

Some discovery adaptors allow for NE custom compatibility. With NE compatibility, you can discover and manage an NE without needing the adaptor for the NE version. A default compatibility rule is defined in the discovery adaptor. You can configure custom compatibility rules to override the default as needed.

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.

Discovered NE version	Adaptors and compatibility rules in place	Expected result
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	<ul style="list-style-type: none">• 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.

NE compatibility is managed using RESTCONF APIs. For information about managing compatibility; see the Device Administration and Mediation RESTCONF APIs documentation 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 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.

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 is used for controller discovery only, that is, the policy 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.

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 CPM. address 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 to be used to confirm reachability, for example, ping. The parameters vary based on the reachability type.
Timeout (seconds)	Specifies the length of time, in seconds, to wait for a response after attempting to reach the NE
Interval (minutes)	Specifies the length of time, in minutes, to wait before repeating an attempt to reach the NE
Admin State	Specifies the administrative state for the new policy Up means the policy is in effect.

5

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

END OF STEPS

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.

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](#).

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.

Parameter	Description
Description	User-provided description of the discovery rule
Admin State	Specifies the administrative state for the discovery rule
Management Protocol	Choose IPv4 or IPv6
Classic Mediation Policies	Select a policy for each access type as needed: <ul style="list-style-type: none">Click on the mediation policy field.In the form that opens, select a policy and click SELECT. To create a mediation policy, click + NEW ; see 2.7 "How do I create a classic mediation policy?" (p. 28).
Classic Reachability Policies	Select a policy for each reachability type as needed: Click in a reachability type field. In the form that opens, select a policy and click SELECT . To create a reachability policy, click + NEW ; see 2.10 "How do I create a classic reachability policy?" (p. 31).

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. 34).

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.



Note: At least one MDM mediation policy and at least one MDM reachability policy are mandatory for unified discovery rule creation, regardless of whether the rule will be used to discover model-driven devices.

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

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
<i>General</i>	
Rule name	The name of the discovery rule
Description	User-provided description of the discovery rule
Network Scan Interval (minutes)	Specifies the interval, in minutes, at which the network scan repeats
Admin State	Specifies the administrative state for the discovery rule Up means the policy is in effect.
<i>Discovery Protocols and Policies</i>	
(First Second Third Fourth) discovery protocol	Specify the protocols to be used to communicate with the NE, in the order in which they should be used to attempt to reach the NE for discovery. Enter all the protocols that will be used for communication, regardless of whether they will be used for discovery.
Mediation Policies	Select a policy for each protocol: <ul style="list-style-type: none">Click on the policy field.In the form that opens, select a policy and click SELECT. To create a mediation policy, click + NEW ; see 2.8 "How do I create a mediation policy for MDM?" (p. 29).

Parameter	Description
Reachability Policies	The reachability types required for the selected discovery protocols appear in the Select Reachability Policies panel. Click in a reachability type field. In the form that opens, select a policy and click SELECT . To create a reachability policy, click + NEW ; see 2.11 "How do I create a reachability policy for MDM ?" (p. 32) .
Associate Classic Discovery Rule	Click in the Classic Discovery Rule field. In the form that opens, select a discovery rule and click SELECT . To create a classic discovery rule, click + NEW ; see 2.13 "How do I create a classic discovery rule?" (p. 33) .
<i>Discovery IP Ranges</i>	
Included IP Addresses	Click + ADD to specify an IP address and mask bits to search. Repeat to add additional ranges. Verify that the included IP address ranges include all the MDM and classic devices you need to discover.
Excluded IP Addresses	Click + ADD to specify an IP address and mask bits to exclude from discovery. Repeat to add additional ranges.



4

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

5

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

6

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

END OF STEPS

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, 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 stitch a classic device to a unified discovery rule?

2.16.1 Purpose


If classic devices are already discovered in the NFM-P (brownfield scenario), they are synchronized to the NSP and appear in the **Device Management, Managed Network Elements** view. This synchronization does not provide gRPC mediation, which is required for telemetry and reporting.

To enable telemetry and reporting in NSP, the classic devices must be stitched to a unified discovery rule with gRPC mediation.

This is a one-time manual procedure.

 **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. Disable equivalent MIB based statistics in NFM-P if gRPC telemetry is used.

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.

-
- 2 _____
Open **Device Discovery, Unified Discovery Rules**.
 - 3 _____
Select the discovery rule to associate the NE with 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 address of the NE is 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 to include the NE. The next time the discovery rule is run, the gRPC mediation information provided by the discovery rule is applied to the NE.

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
<i>General</i>	
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.

Parameter	Description
Primary IP Address	Specifies the primary IP address of the controller.
Standby IP Address	Enter the standby IP address, if applicable.
<i>Policies</i>	
Mediation Policies	<p>Policies that are mandatory for controller discovery are indicated with an asterisk (*).</p> <p>Select a policy for each protocol:</p> <ul style="list-style-type: none"> Click on the policy field. In the form that opens, select a policy and click SELECT. <p>To create a mediation policy, click + NEW; see 2.8 "How do I create a mediation policy for MDM?" (p. 29).</p>
Reachability Policies	<p>Policies that are mandatory for controller discovery are indicated with an asterisk (*).</p> <p>The reachability types required for the selected discovery protocols appear in the Select Reachability Policies panel.</p> <p>Click in a reachability type field.</p> <p>In the form that opens, select a policy and click SELECT.</p> <p>To create a reachability policy, click + NEW; see 2.11 "How do I create a reachability policy for MDM ?" (p. 32).</p>

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 [4.2.1 “Views” \(p. 51\)](#) for information about configuring operation types and performing large-scale operations.

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](#).

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.

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 , **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 restore an NE from a backup?

3.4.1 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.

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](#).

3.4.2 Steps


1

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

2

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

3

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.

4

Select the successful backup operation which you would like 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

Part II: Advanced device management

Overview

Purpose

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

Contents

Chapter 4, Large-scale operations	49
Chapter 5, NE software upgrades using NSP	67
Chapter 6, Zero Touch Provisioning	75

4 Large-scale operations

Overview

4.1 Operations

4.1.1 Overview

The Operation views are available if the Network Infrastructure Management - Basic Management feature package is included in the deployment. To complete operations, NSP executes workflows. You can view the workflows in the **Workflows**, **All Workflows** view if needed.

i **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 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.



4.2 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.


Term	Description	Navigation
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
7750 SR	—
7950 XRS	—
7450 ESS	—
7220 IXR SRLinux	—
7250 IXR	—
7250 IXR SRLinux	—
7210 SAS and variants: Mxp, D, Dxp, K, M, X, T, R, E, S/Sx	Classic mode only
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: <ul style="list-style-type: none"> • 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

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.

i **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” \(p. 67\)](#). 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 edit 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.

How do I view or manage scheduled operations?

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 manage scheduled operations?

4.7.1 Steps

1

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

2

Select an operation 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**.

END OF STEPS

4.8 How do I view current operations and executions?

4.8.1 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

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




4.9.1 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.

4.9.2 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 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 _____

4.10 How do I view the details of completed operations?

4.10.1 Steps

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

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

- 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 _____

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

4.11.1 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 _____

4.12 How do I automate the cleanup of completed operations?

4.12.1 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.

How do I view reports generated by an operation?

4.12.2 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 _____



4.13 How do I view reports generated by an operation?

4.13.1 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.

4.13.2 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

4.14 How do I retry an execution within a phase?

4.14.1 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.

4.14.2 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**. 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.

How do I terminate an execution in progress?

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

4.15 How do I terminate an execution in progress?

4.15.1 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.

4.15.2 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 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


4.16 How do I retry a failed operation?

4.16.1 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.

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

4.16.2 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 _____

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

4.17.1 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.

4.17.2 Steps

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

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


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

4.18 Operation troubleshooting

4.18.1 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 [4.8 “How do I view current operations and executions?” \(p. 57\)](#).
- **View details of completed operations.** Completed operations remain in the All Operations view until deleted. See [4.10 “How do I view the details of completed operations?” \(p. 58\)](#).
- **View reports generated by executions.** Some operations generate reports during certain phases. See [4.13 “How do I view reports generated by an operation?” \(p. 60\)](#).
- **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 [4.14 “How do I retry an execution within a phase?” \(p. 61\)](#).
- **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 [4.16 “How do I retry a failed operation?” \(p. 62\)](#).
- **Rollback a phase.** Some phases in an operation can be rolled back, depending on whether a rollback workflow exists for that phase. See [4.17 “How do I perform a rollback on a target in an operation?” \(p. 63\)](#).

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. For NEs managed using MDM, see [5.3 “How do I import an NE software image?” \(p. 69\)](#). 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:

- 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

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.

7x50 and ISSU upgrade path limitations

For 7x50 NEs, and for ISSU upgrades, the NSP only supports upgrading to a version that is up to two major releases later than the version currently installed on the NE. For example, an NE can be upgraded 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. The following requirements apply:

- The upgrade image must be imported into the NFM-P. See the *Classic Management User Guide*.
- Both CLI and FTP/SFTP mediation must be configured for the target NEs. For nodes managed through mixed-mode mediation, the following types of CLI access must be enabled, in the order shown: md-cli, and 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.

For the multi-phase upgrade operation type `nsp-ne-upgrade-with-phases`, the following three policies must be configured on the NFM-P with the settings specified below:

Policy name	Required settings
download	download=true, activate=false, reboot=false
activate	download=false, activate=true, reboot=false
reboot	download=false, activate=false, reboot=true (issu=true if issu upgrade triggered)

5.2 Process for NE upgrade

5.2.1 Stages

1

Verify the management type for the NE. The upgrade process will be different for MDM managed and NSP Classic managed NEs. 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?” \(p. 69\)](#).

3

Start the upgrade operation; see [4.5 “How do I start or schedule a new operation?” \(p. 54\)](#)

4

View the operation in the Operations tab to monitor it; see [4.8 “How do I view current operations and executions?” \(p. 57\)](#).

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 [4.9 “How do I start, stop, or pause an operation?”](#) (p. 58).

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 [4.10 “How do I view the details of completed operations?”](#) (p. 58)

8

To perform a rollback, see [4.17 “How do I perform a rollback on a target in an operation?”](#) (p. 63).

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 an 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.

i **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 which calls LSO_7x50_Upgrade_MD_Mixed_ Pre_Checks for MD mode	<ul style="list-style-type: none"> 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 which calls LSO_7x50_Upgrade_MD_Mixed_ Download for MD mode	<ul style="list-style-type: none"> 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
Activate	LSO_7x50__Activate which calls LSO_7x50_Upgrade_MD_Mixed_ Activate for MD mode	<ul style="list-style-type: none"> 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

Phase	Workflow	Process
Reboot	LSO_7x50_Reboot which calls LSO_7x50_Upgrade_MD_Mixed_ Reboot for mixed mode	<ul style="list-style-type: none">• 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. 69).
- 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 Basic Info panel, enter a name for the operation and an optional description.
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 TiMOS-xx.yy.Rz, for example, TiMOS-21.5.R1.
Is ISSU	Specifies whether the upgrade operation is an in service software upgrade. This parameter is only valid for MDM-managed NEs.
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: <ul style="list-style-type: none"> • 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.
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.	

Parameter	Description
<ul style="list-style-type: none">• Concurrency Count• Phase Timeout (minutes)• Average Execution Threshold (minutes)	<p>These parameters specify how the workflow executions will be managed. The pre-check steps themselves are defined in the applicable workflow.</p> <ul style="list-style-type: none">• 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

In the Schedule panel, configure scheduling for each phase of the upgrade. For example, you can configure the operation to run the pre-check phase immediately and the software download phase as soon as the pre-checks are complete, and complete the activation and reboot during a maintenance window.

For the pre-check phase: Set up the schedule.

- Click Run immediately, or
- Click Set up the schedule and configure the start and end times.

For each subsequent phase:

- Click Run manually to execute after the previous phase completes, or
- Click Set up the schedule and configure the start and end times.

13

Click **RUN**. The operation appears in the All Operations view and begins executing according to the schedule.

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.

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 by NSP or NFM-P.


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 and 7750 SR 14s NEs. Contact Nokia for assistance in using ZTP with any other NE type.

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 Nokia central resources; contact your Nokia representative for details
- An HTTP user must be created using the Create_HTTP_User intent type; see [6.2 “How do I configure Zero Touch Provisioning?” \(p. 77\)](#).
- A discovery rule for the NE must be created in NSP. The administrative state of the discovery rule must be Down.
- For classic devices, a discovery rule for the NE must be created in NFM-P in addition to the discovery rule in NSP. The administrative state of the discovery rule must be Down.
See the *NSP NFM-P Classic Management User Guide* for more information about discovery rule configuration in NFM-P.
- 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?” \(p. 69\)](#).
- 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” \(p. 77\)](#) 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?” \(p. 77\)](#).

Figure 6-1 Zero Touch Provisioning process



6.2 How do I configure Zero Touch Provisioning?

6.2.1 Note

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

- *NSP Network Automation Guide*
- *NSP System Administrator Guide*
- *NSP NFM-P Classic Management User 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 Process

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 **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 **Create Intent +**.

7

In the form that opens, configure the required parameters:

- Choose the management mode: classic, mixed, 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 the NE Type.

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 **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.
- Choose a discovery rule, and, for classic NEs, an NFM-P discovery rule.

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 NSP and NFM-P, turn the relevant discovery rules up.

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*.

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


Chapter 7, Device object configuration	85
Chapter 8, Network configuration	91

7 Device object configuration

Viewing NE parameters


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

7.1.1 NE inventory view

Select an NE from the list in **Device Management, Managed Network Elements** 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.


Individual inventory objects (child objects) show object names and basic administrative and operational state information. The color of an inventory object indicates its state.

 **Note:** The inventory details available in NSP depend on the adaptors installed and managed NE configuration.

NE inventory information is grouped by type of object:

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

Available actions

Select an inventory object and click  to open the tree item actions menu. Options in the tree item actions menu depend on the object.

- For the NE (top of the inventory):
 - **Open in Current Alarms:** opens the alarm list
 - **Open object** (available on model-driven NEs only):
Model Driven Configurator opens in a new browser tab, filtered to the object.
 - **Open NE session:** a CLI session with the NE opens in a new browser tab.
 - **Plot utilization statistics:** a set of utilization statistics charts opens in a new browser tab.
 - **Show in Event Timeline:** a filtered event timeline for the NE opens in a new browser tab.
- For a port:
 - **Open in Current Alarms**
 - **Open object** (available on model-driven NEs only)
 - **Plot utilization statistics**
- For other objects, the only options are **Open object** and **Expand all equipment tree items**.

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.

7.1.2 Configured Attributes view

[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.

Model Driven Configurator

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

7.2.1 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 .
Infrastructure Configuration Management (ICM)	With ICM, 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 8, "Network configuration"
Large-scale operations (LSO)	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, "Large-scale operations"



Function	Description	Path in NSP	Documentation reference
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	<i>NSP Service Management Guide</i>

7.3 How do I open a device for configuration?

7.3.1 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

7.4 How do I configure device objects?

7.4.1 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.

7.4.2 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.

7.4.3 Steps

1

Navigate to the configuration schema; perform [7.3 “How do I open a device for configuration?” \(p. 88\)](#).

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

8 Network configuration

Template-based configuration deployment

8.1 What is device configuration in NSP?

8.1.1 NSP Infrastructure Configuration Management

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

RESTCONF APIs are also available for ICM; see the API documentation on the [Network Developer Portal](#).

ICM 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 ICM Intent Types Delivery notes 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). ICM 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.

8.2 How does configuration deployment work?

8.2.1 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 ICM 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: <ul style="list-style-type: none"> • Network Intents function is currently unavailable • the required intent type is not found • the Opensearch subsystem is down • A function downstream of ICM 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

8.3 ICM process

8.3.1 Purpose

This process describes the general steps of ICM. 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 ICM intent type 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 resource 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
- Open **Device Management, Configuration Deployments**.
 - Click **+ DEPLOYMENT** and choose **Logical** or **Physical**.
 - 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:

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

8.4 What is a configuration intent type?

8.4.1 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**.

i **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, called views or schema forms in Network Intents. Configuration forms define 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.

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.

8.4.2 ICM 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 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.
target-xpath	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.

Attribute	Mandatory	Default value	Available values	Description
targets	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.

Notes:

1. If the targets parameter is set in the descriptor file, the select-template parameter defaults to **single**.

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.

8.4.3 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.

8.4.4 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

8.4.5 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.

i **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.

8.5 How do I import a configuration intent type?

8.5.1 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.

i **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 [8.4.2 “ICM descriptor resource file” \(p. 98\)](#) for information about the requirements for the descriptor file.

8.5.2 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.

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

END OF STEPS _____

Configuration templates


8.6 What is a configuration template?

8.6.1 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.

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.

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 [8.20 “How do I create a logical configuration deployment?” \(p. 115\)](#) and [8.20 “How do I create a logical configuration deployment?” \(p. 115\)](#).

NSP supports up to 20 000 deployments per configuration template.

8.6.2 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.
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.
Role	Physical	The target is a physical object such as a port.
	Logical	The target is a configured object such as QoS.

Parameter	Predefined values	Notes
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.
	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.

8.6.3 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

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

- 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

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

8.6.4 Differences between classic NEs and model-driven NEs

If you are using Nokia predefined ICM 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.

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

8.7.1 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.

i **Attention:** For ICM 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.

8.8 How do I create a configuration template?

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

8.8.1 Steps

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

2 _____
Click **+ CONFIGURATION TEMPLATE**.

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

i **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 _____

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

8.9.1 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.

8.9.2 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

8.10 What is migration?

8.10.1 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.

i **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.

8.10.2 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
<ul style="list-style-type: none"> • MTU: 1500 • encaptype: qinq 	<ul style="list-style-type: none"> • MTU: 1600 • administrative state: enabled 	<ul style="list-style-type: none"> • MTU: 1600 • encaptype: qinq • administrative state: enabled

8.11 How do I migrate a deployment to another template?

8.11.1 Steps


1

Perform [8.9 “How do I update a template to apply intent type schema form changes?”](#) (p. 107) 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

8.12 How do I deploy or associate a template to the network?

8.12.1 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:

- [8.20 “How do I create a logical configuration deployment?”](#) (p. 115)
- [8.21 “How do I create a physical configuration deployment?”](#) (p. 116)
- [8.13 “How do I associate a logical template to the network?”](#) (p. 109)
- [8.14 “How do I associate a physical template to the network?”](#) (p. 111)

8.13 How do I associate a logical template to the network?

8.13.1 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 [8.20 “How do I create a logical configuration deployment?”](#) (p. 115)

8.13.2 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 _____

8.14 How do I associate a physical template to the network?


8.14.1 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 [8.21 “How do I create a physical configuration deployment?”](#) (p. 116)

8.14.2 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 _____

8.15 How do I retry a failed association?

8.15.1 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:
- To retry a single association:
 - From the  (Table row actions) menu, choose **Retry association**.
 - From the **Deployment Details** panel, click **RETRY ASSOCIATION**.
 - To retry multiple associations, click  **Retry** above the details panel.
The retry operation proceeds.

END OF STEPS _____

8.16 How do I change the life cycle status of a template?

8.16.1 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 _____

8.17 How do I edit a template?

i **Note:** If you need to apply changes from an updated config form, see [8.9 “How do I update a template to apply intent type schema form changes?”](#) (p. 107)

8.17.1 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 _____

8.18 How do I audit or align configurations?

8.18.1 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 [8.30 “How do I audit or align a deployment?”](#) (p. 125). To audit or align all the deployments on an NE, see [8.31 “How do I audit or align configurations for an NE?”](#) (p. 126).


8.18.2 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 check the Template Details panel for process information.

 **Note:** If you are using Nokia predefined ICM 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

8.19 How do I create a deployment?

8.19.1 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:

- [8.20 “How do I create a logical configuration deployment?”](#) (p. 115)
- [8.21 “How do I create a physical configuration deployment?”](#) (p. 116)

8.20 How do I create a logical configuration deployment?

i **Important!** A configuration template of the required role must be created before a deployment can be created.

8.20.1 Steps

1

Open the **Deploy Logical Configuration** form:

- a. Open **Device Management, Configuration Deployments**.
- b. Click **+ CONFIGURATION 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

8.21 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.

8.21.1 Steps

1

Open the **Deploy Physical Configuration** form:

- a. Open **Device Management, Configuration Deployments**.
- b. Click **+ CONFIGURATION 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** 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

8.22 How do I edit a deployment?

8.22.1 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.

i **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 [8.11 “How do I migrate a deployment to another template?” \(p. 109\)](#). To edit parameters for multiple deployments based on the same flexible template; see [8.23 “How do I bulk edit multiple deployments?” \(p. 119\)](#).

8.22.2 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

8.23 How do I bulk edit multiple deployments?

8.23.1 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.

8.23.2 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 8-1 Results of bulk edit based on handling of added table values

Handling option	Deployment 1	Deployment 2
Do Nothing	No queues, no forwarding classes	<ul style="list-style-type: none"> one queue: Queue ID 5, Queue Type expedited, Queue Mode priority one forwarding class: FC Name be, Profile in, Queue 5
Append All	<ul style="list-style-type: none"> no queues forwarding classes: FC Name be, Profile in, Queue 2 FC Name af, Profile none, Queue 2 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> no queues forwarding classes: FC Name be, Profile in, Queue 2 FC Name af, Profile none, Queue 2 	<ul style="list-style-type: none"> no queues forwarding classes: FC Name be, Profile in, Queue 2 FC Name af, Profile none, Queue 2

8.23.3 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

8.24 How do I deploy a saved deployment?

8.24.1 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

8.25 How do I retry a failed deployment?

8.25.1 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:

- To retry a single deployment:
 - From the  (Table row actions) menu, choose **Retry deployment**.
 - From the **Deployment Details** panel, click **RETRY DEPLOYMENT**.
- To retry multiple deployments, click  **Retry selected deployments** above the details panel.


The retry operation proceeds.

END OF STEPS

8.26 How do I distribute a logical configuration deployment?


8.26.1 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:

- Click **+ TARGET** and choose **NEs** or **Predefined Groups** from the drop-down list.
- 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.
- Verify the list of targets in the Bin and click **ADD**.
- 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.

- Click **VIEW/EDIT TEMPLATE CONFIG** to open the **View/Edit Template Config** form.
- 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

8.27 How do I distribute a physical configuration deployment?

8.27.1 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

8.28 How do I delete a deployment?

8.28.1 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

8.29 How do I remove a deployment?

8.29.1 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.

8.29.2 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

8.30 How do I audit or align a deployment?

 **Note:** If you are using Nokia predefined ICM 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.


8.30.1 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 _____

8.31 How do I audit or align configurations for an NE?

8.31.1 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

Chapter 9, Use cases	131
--------------------------------------	-----

9 Use cases

9.1 Discovery of a 7750 SR device in NSP

9.1.1 Purpose

This use case shows how to use NSP to discover a model-driven 7750 SR.

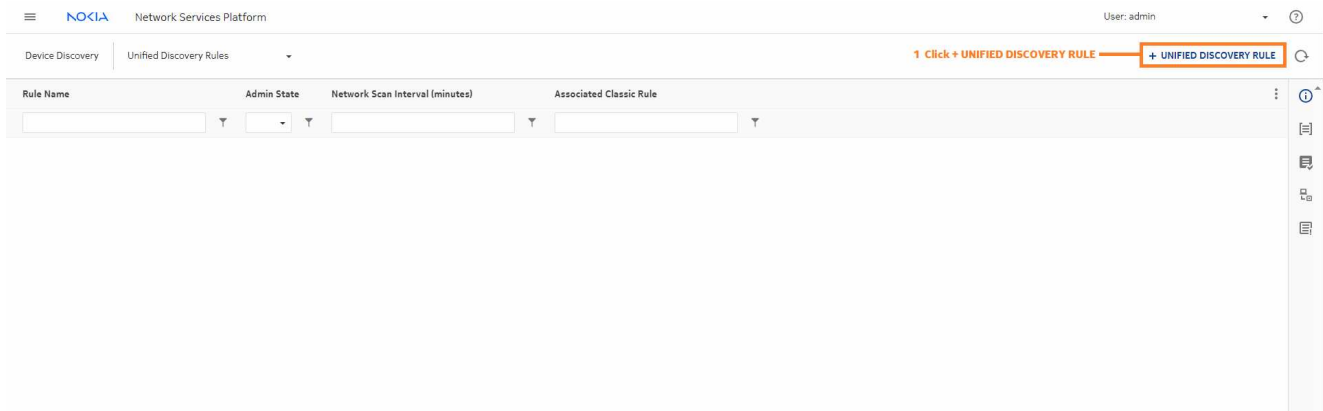
Click on a figure to enlarge it.

9.1.2 Steps

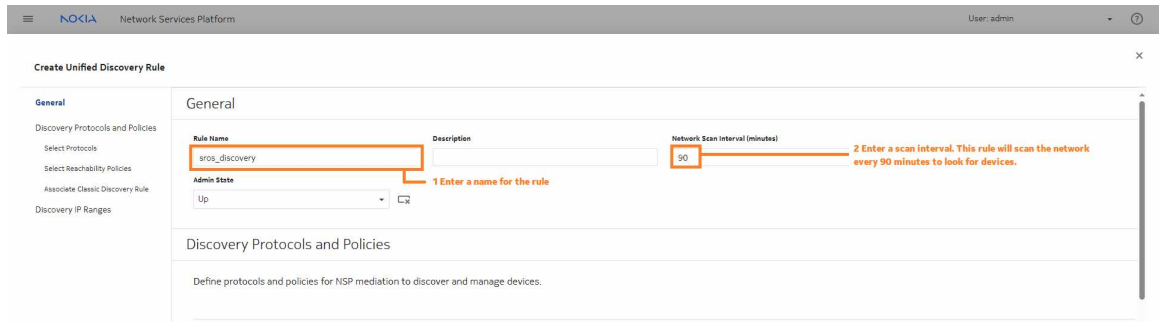
1

The first step is creating a unified discovery rule.

1. Open **Device Discovery, Unified Discovery Rules**.
2. Click **+ UNIFIED DISCOVERY RULE**.

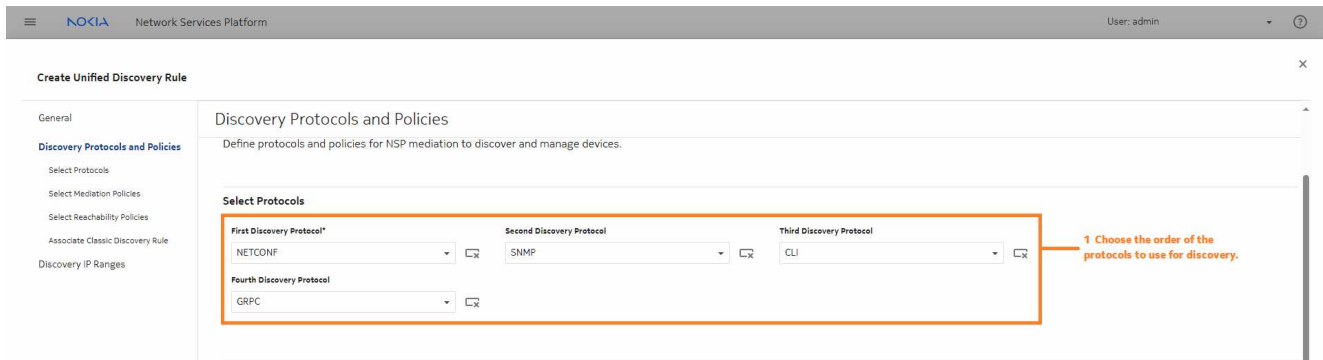


First, we'll configure the general settings for the discovery rule. Enter a name for the rule and a scan interval. This rule will scan the network every 90 minutes to look for devices and device updates.



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.



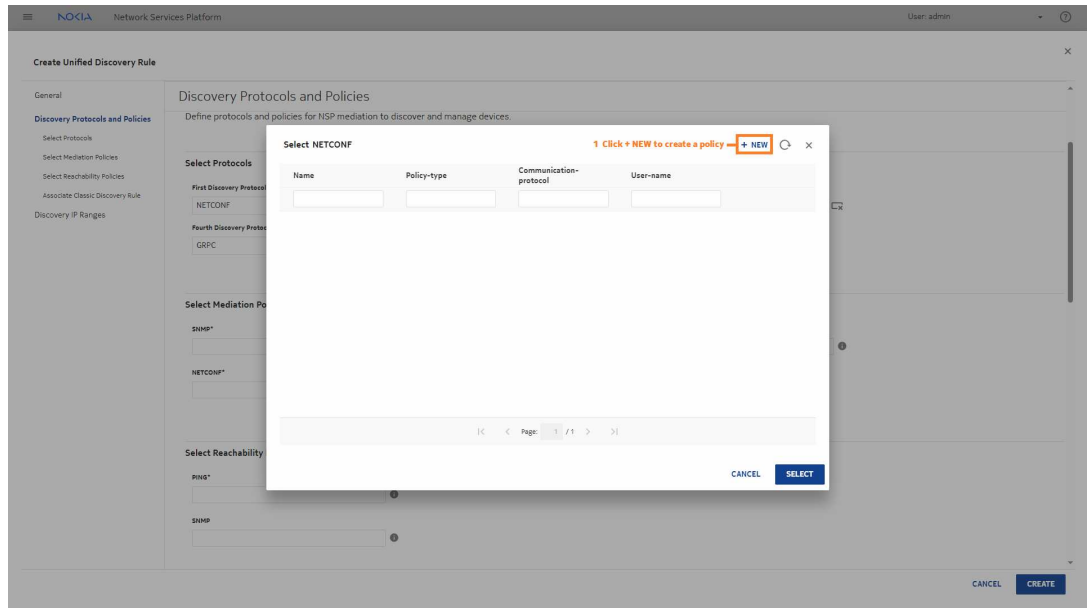
3

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.

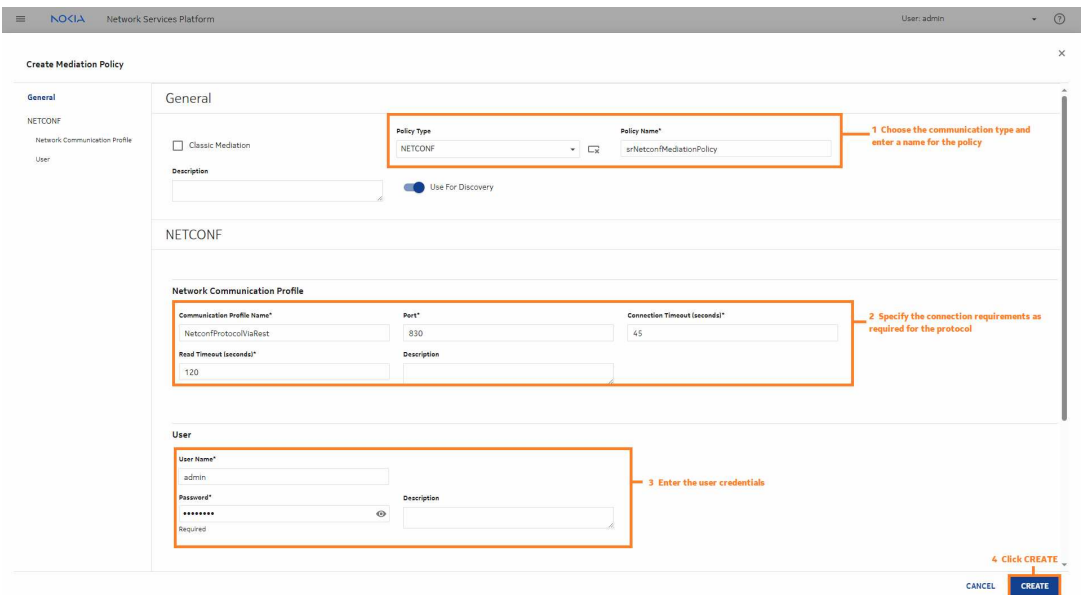
These steps need to be done for each mediation protocol we selected. We'll use NETCONF as an example.

1. Click in the NETCONF field in the Select Mediation Policies panel to open the Select


NETCONF policy form.

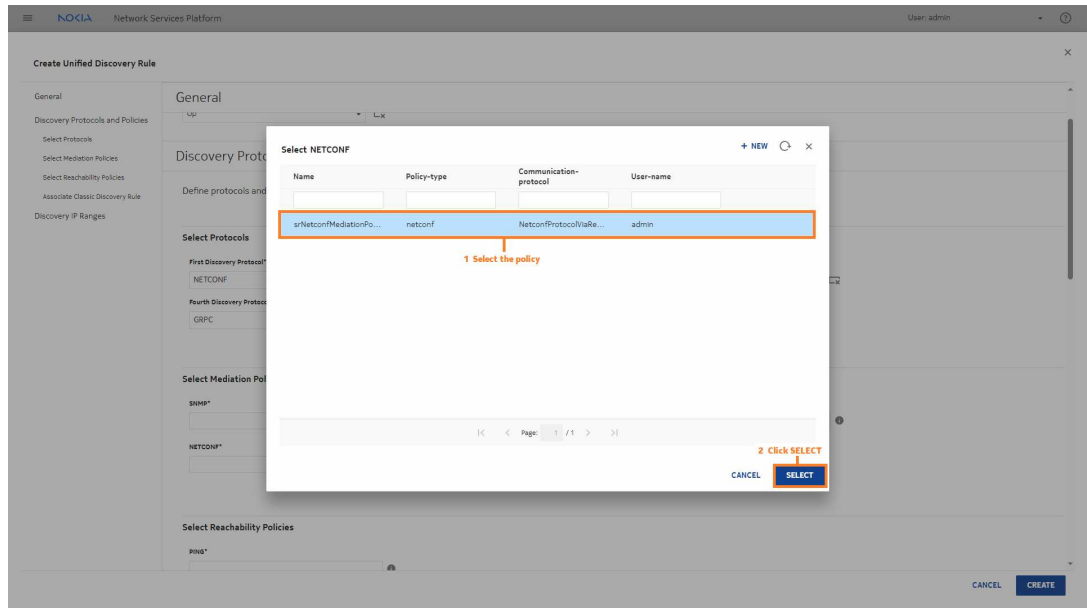


2. Click **+ NEW** to open the **Create Mediation Policy** form in a new browser tab.



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.

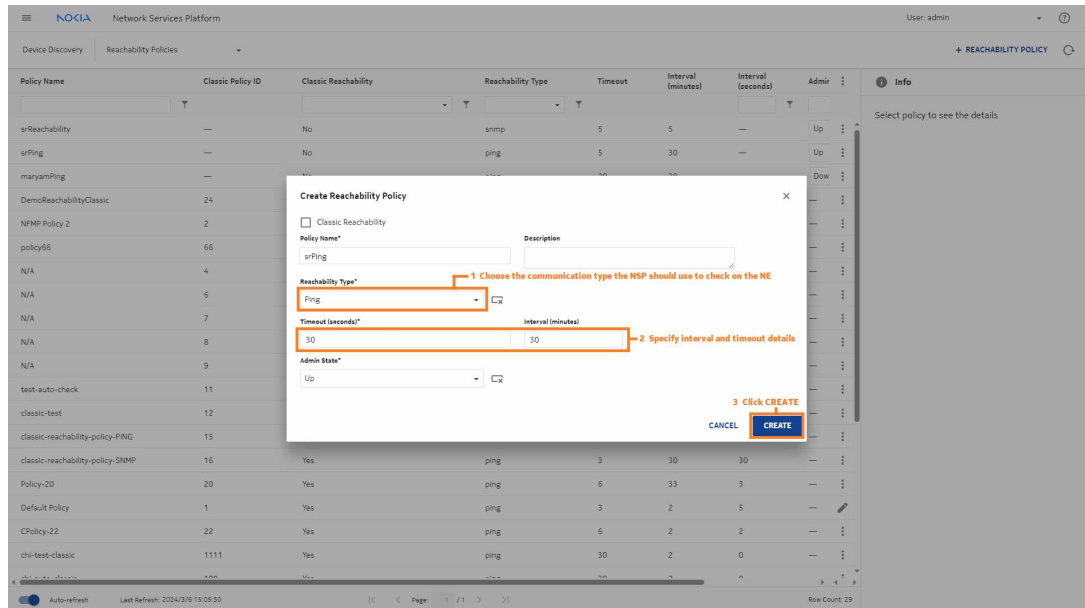
4

The last part of the protocol and policy setting is creating the reachability policies.

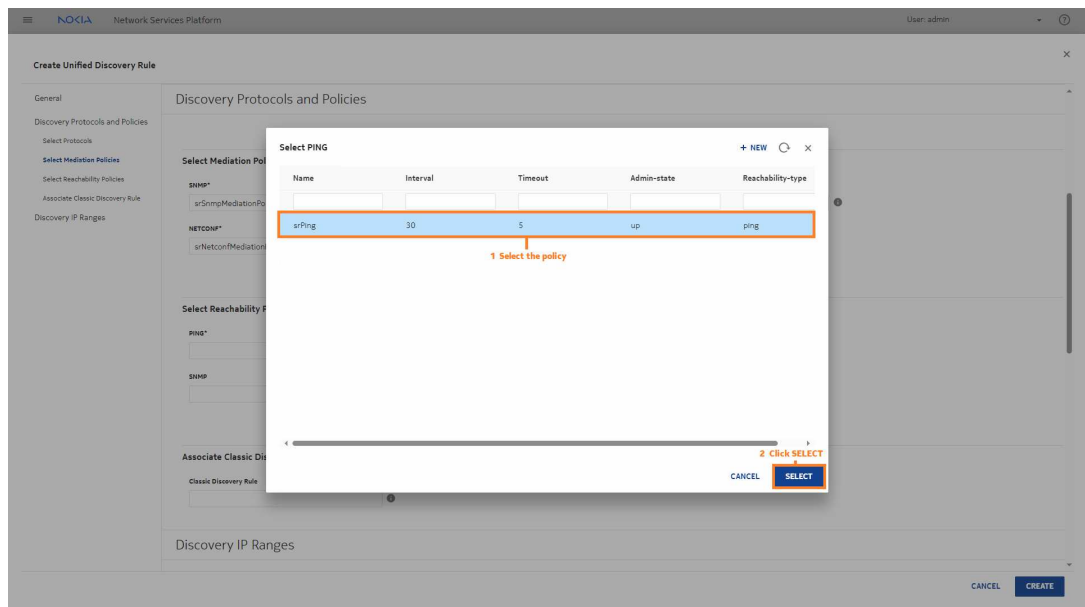
We'll follow a similar process: creating the policies we need and associating each with the discovery rule. This time we'll use Ping as an example.

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.



- 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.

The screenshot shows the 'Create Unified Discovery Rule' window. The 'Discovery IP Ranges' section is expanded, showing a table for 'Included IP Addresses' with columns for 'IP Address' and 'Mask Bits'. A red box highlights the '+ ADD' button in the top right corner of this section. Below it is a table for 'Excluded IP Addresses' with the same columns and a '+ ADD' button. The interface also features a sidebar with navigation options and a bottom right area with 'CANCEL' and 'CREATE' buttons.

In the form that opens, enter the IP address and mask bits, and click **ADD**.

Create Unified Discovery Rule > Create Included IP Addresses

IP Address* 198.51.100.20 Mask Bits* 32

1 Enter an IP address and mask to specify an IP range or subnet. The rule will scan the range to look for devices.

2 Click ADD

CANCEL ADD CANCEL CREATE

7

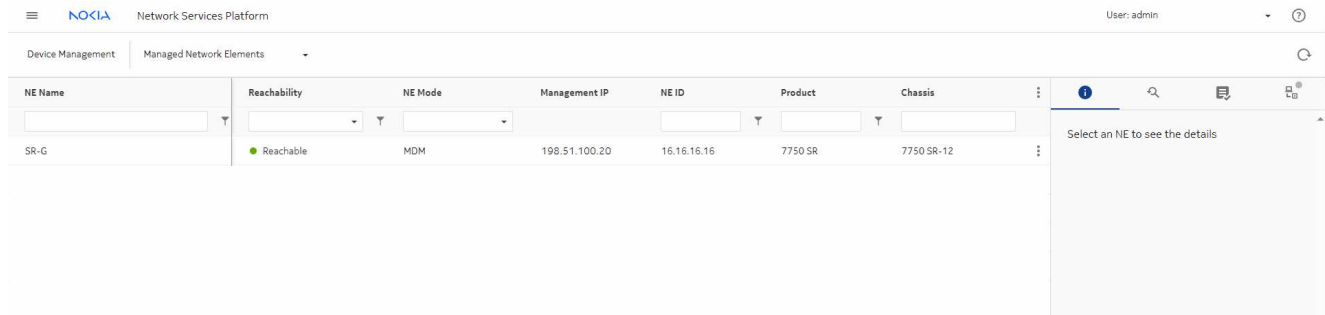
After you click **CREATE**, the discovery rule appears in the list. Choose Discover from the Table row actions menu to run the discovery rule manually.

Rule Name	Admin State	Network Scan Interval (minutes)	Associated Classic Rule
srNetconfDiscoveryRule	Up	5	-

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.

9.2 NFM-P and NSP comparison: Port Configuration

9.2.1 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 [8.5 “How do I import a configuration intent type?”](#) (p. 101) and [8.8 “How do I create a configuration template?”](#) (p. 106).

Use this procedure to use this template to configure the ports.

9.2.2 Steps

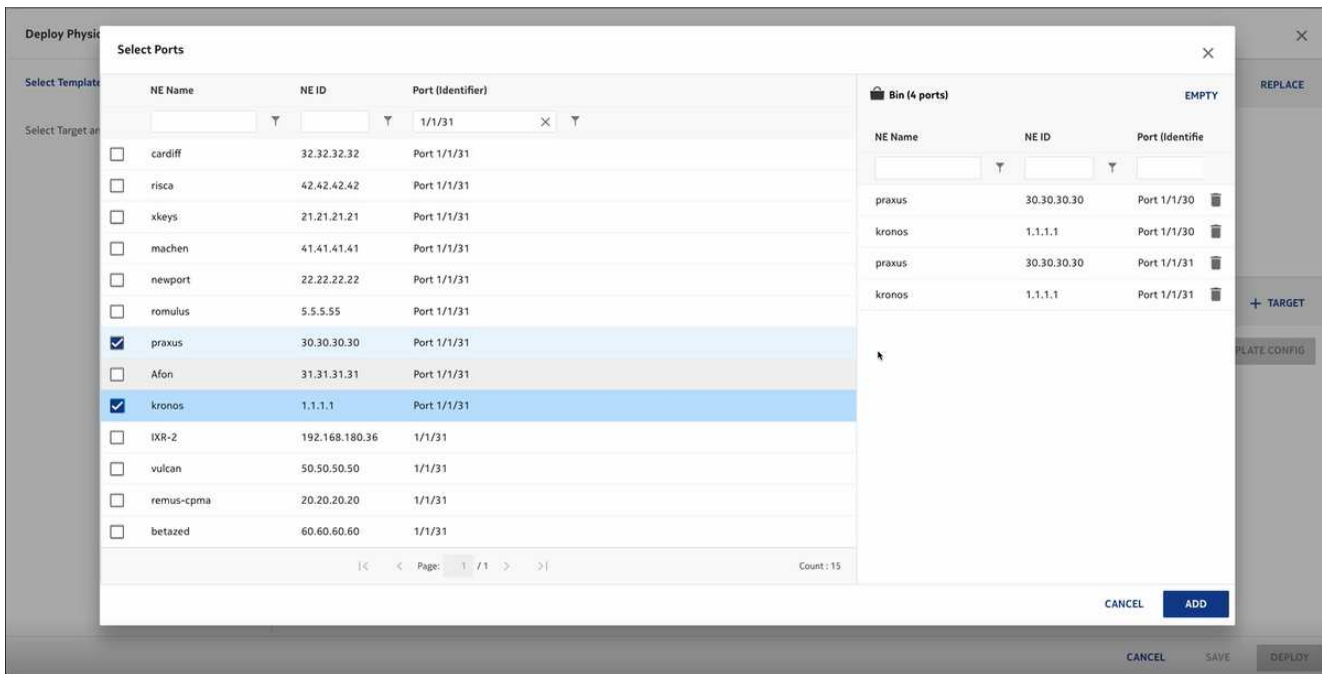
1 _____
Open **Device Management, Configuration Templates**.

2 _____
Select **Ready_Access_Ports_4_LAG** from the list of configuration templates and click **⋮** (Table row actions), **Deploy to Network**.

Name	Description	Life Cycle	Intent Type	Intent Type Version	Config Form	Config Form State	Role	Category	Service Scope	Flexible	Last Updated
Statement		released	com-nokia-ops-configuration-...	2	default	✓ up-to-date	Logical	Router	SD-WAN Clients & Model	Yes	Nov 10, 2022 3:49:08 pm
Ready_Access_Ports_4_LAG		released	com-nokia-ops-configuration-...	2	default	✓ up-to-date	Physical	Port	SD-WAN Clients & Model	Yes	Nov 16, 2022 7:47:24 am
Ugreen_OIG		released	com-nokia-ops-configuration-...	2	default	✓ up-to-date	Logical	DSL	SD-WAN Clients & Model	Yes	Nov 10, 2022 3:09:39 pm
Sub_Ports		released	com-nokia-ops-configuration-...	2	gold	✓ up-to-date	Physical	Port	SD-WAN Clients & Model	No	Nov 10, 2022 3:00:23 pm
Ugreen_OIG		released	com-nokia-ops-configuration-...	2	default	✓ up-to-date	Logical	DSL	SD-WAN Clients & Model	Yes	Nov 10, 2022 3:09:37 pm
Customer		released	com-nokia-ops-configuration-...	2	default	✓ up-to-date	Logical	Service	All	Yes	Nov 14, 2022 11:29:24 pm

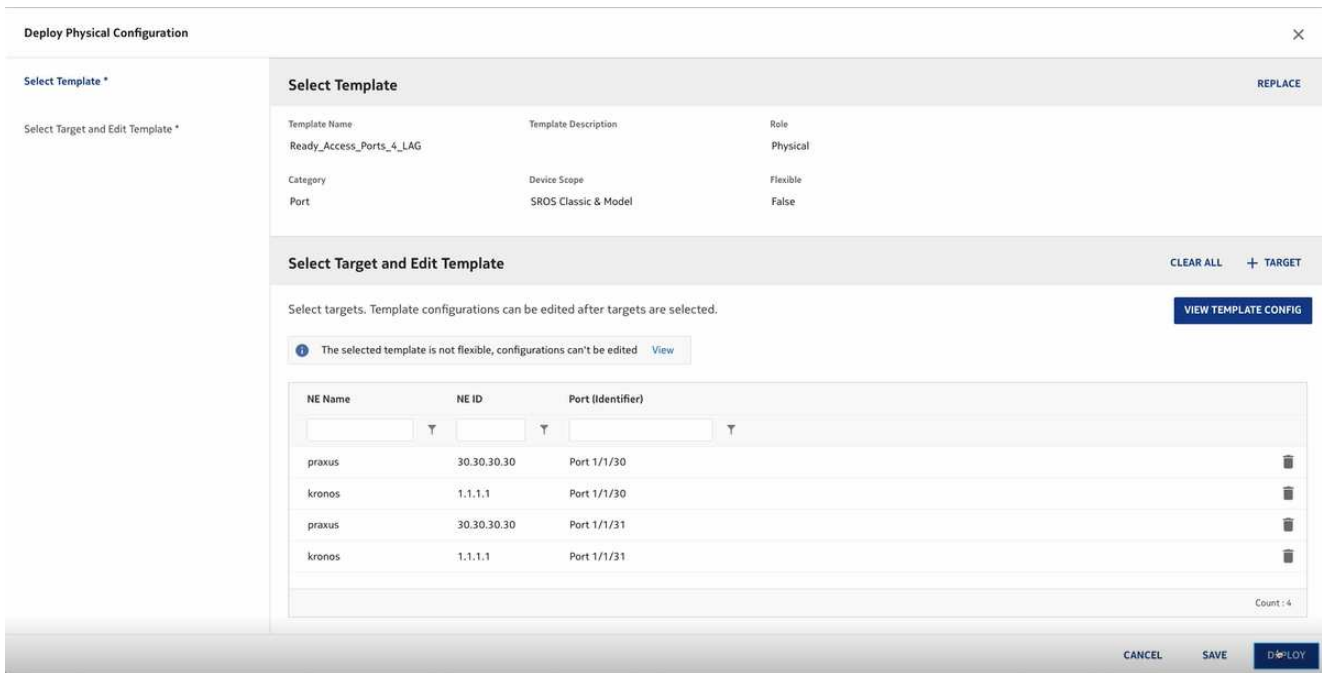
3 _____
In the form that opens, click **+ TARGET** and choose Ports.

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

9.3 NFM-P and NSP comparison: QoS

9.3.1 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 [8.5 “How do I import a configuration intent type?” \(p. 101\)](#) and [8.8 “How do I create a configuration template?” \(p. 106\)](#).

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.

9.3.2 Steps

1

Select **SAP Egress Policy** from the list of configuration templates and click **⋮** (Table row actions), **Associate to Network**.

Name	Description	Life Cycle	Intent Type	Intent Type Version	Config Form	Config Form State	Rule	Category	Device Scope	Flexible	Last Updated
Stratagem		Released	network-policy/stratagem-...	3	default	Up-to-date	Logical	Route	SRX2 Class & Model	Yes	Nov 10, 2023 9:00:00 pm
SAP Egress Policy		Released	network-management/egress...	3	default	Up-to-date	Logical	QoS	SRX2 Class & Model	Yes	Nov 16, 2023 10:43:34 am
Ready_Series_Ports_1_4G		Released	network-management/...	3	default	Up-to-date	Physical	Port	SRX2 Class & Model	Yes	Nov 16, 2023 9:47:34 am
Ingress_QoS		Released	network-management/...	3	default	Up-to-date	Logical	QoS	SRX2 Class & Model	Yes	Nov 16, 2023 9:08:33 pm
QoS_Ports		Released	network-management/...	3	gold	Up-to-date	Physical	Port	SRX2 Class & Model	Yes	Nov 16, 2023 9:08:33 pm
Egress_QoS		Released	network-management/...	3	default	Up-to-date	Logical	QoS	SRX2 Class & Model	Yes	Nov 16, 2023 9:08:37 pm
Extranet		Released	network-management/...	3	default	Up-to-date	Logical	Service	All	Yes	Nov 14, 2023 11:39:34 am

2

In the form that opens, click **+ TARGET** and choose NEs.

3

Choose the NE where the new policy is added and click **ADD**.

Associate Template

Select Template: 1. SAP Egress Policy

Select Target as: []

Assign Identifier: []

NE Name	NE ID	Management IP	Product
<input type="checkbox"/> vN7750-104	63.130.123.104	172.20.149.104	7750 SR
<input type="checkbox"/> romulus	5.5.5.55	172.20.149.129	7750 SR
<input type="checkbox"/> remus-cpma	20.20.20.20	172.20.149.180	7750 SR
<input type="checkbox"/> praxus	30.30.30.30	172.20.149.181	7750 SR
<input checked="" type="checkbox"/> kronos	1.1.1.1	172.20.149.128	7750 SR
<input type="checkbox"/> SR-14s	92.168.96.244	135.249.210.34	7750 SR
<input type="checkbox"/> MEO	172.25.100.56	135.86.186.167	7750 SR
<input type="checkbox"/> IXR227	fdef:fade:face:ff...	135.249.220.120	7250 IXR
<input type="checkbox"/> IXR-2	192.168.180.36	172.20.149.36	7250 IXR
<input type="checkbox"/> IXR-1	192.168.180.35	172.20.149.35	7250 IXR

Bin (1 NE) EMPTY

NE Name	NE ID
kronos	1.1.1.1

Count: 1

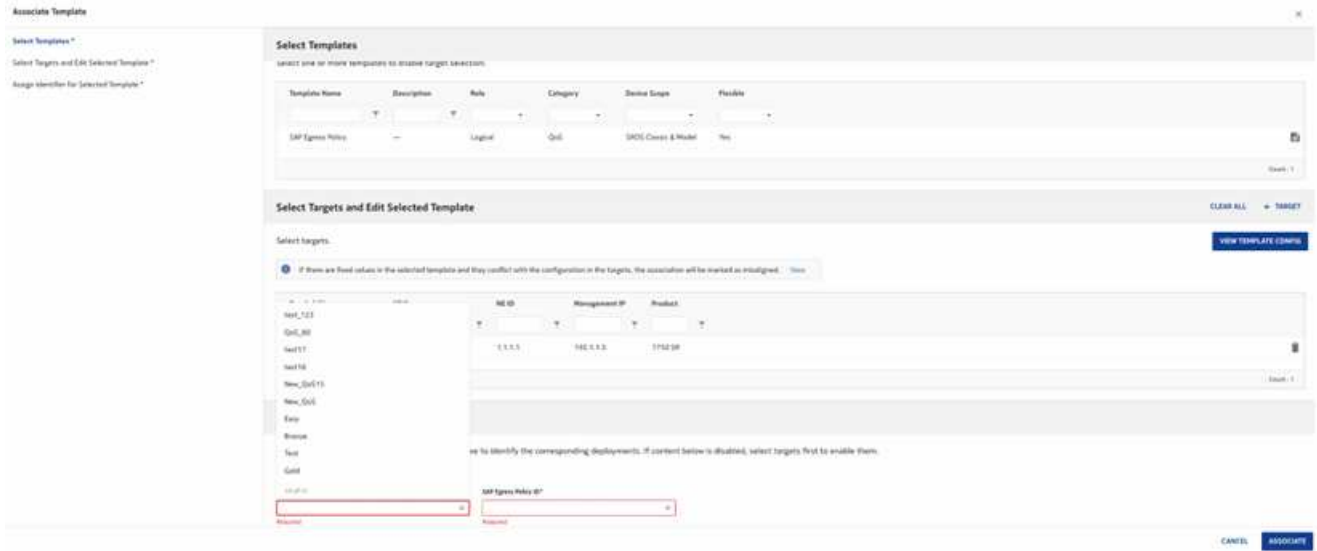
+ TARGET

PLATE CONFIG

CANCEL **ADD**

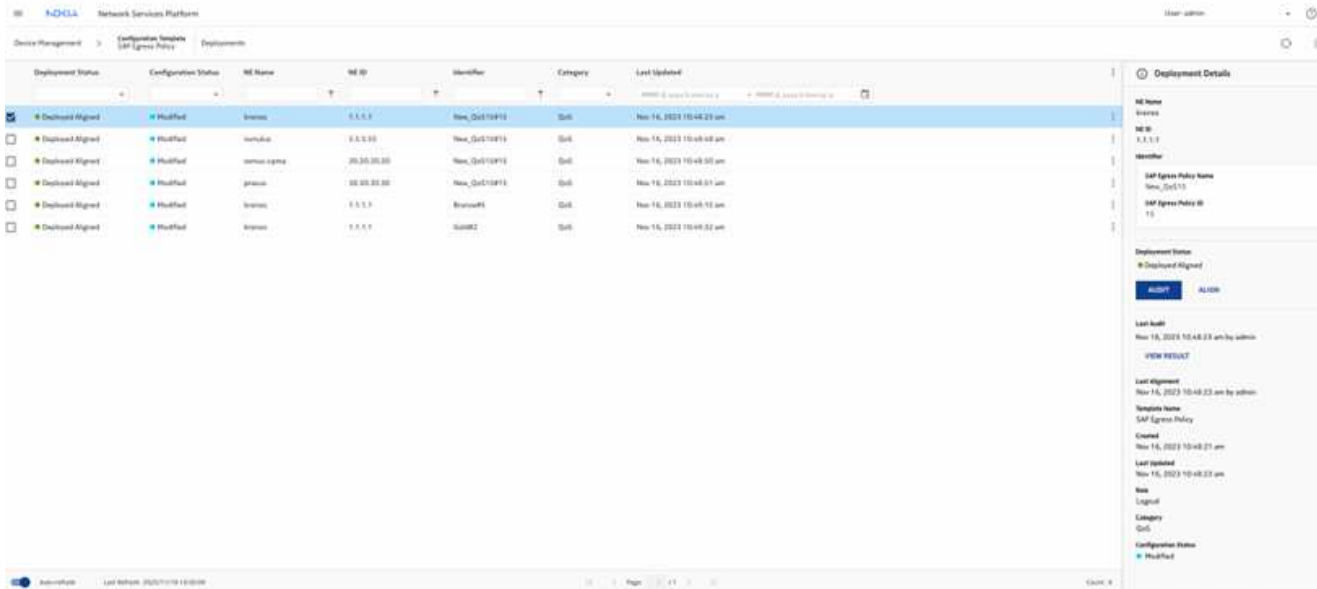
4

Select the existing policy name and ID for the NE and click **ASSOCIATE**.



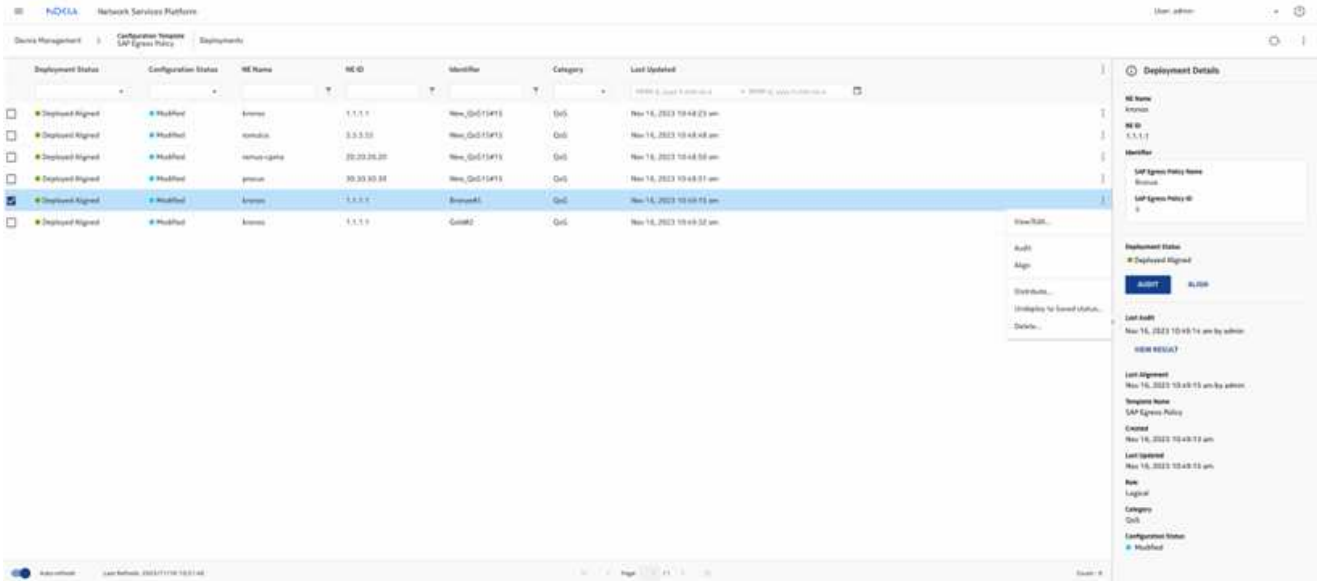
5

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.

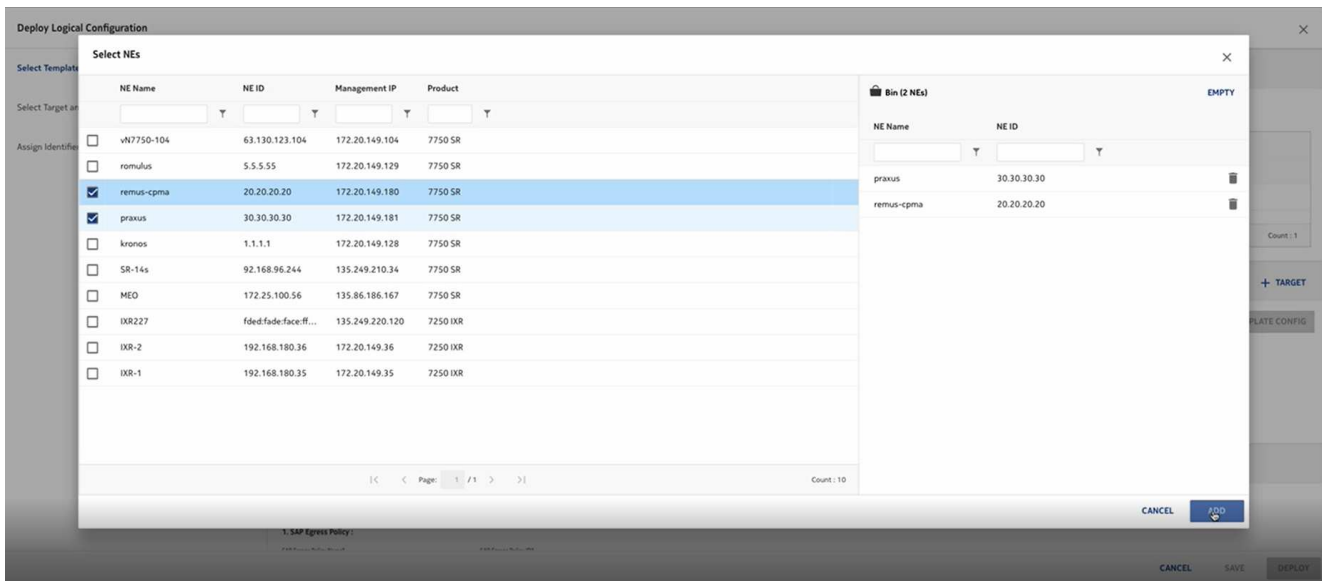


7

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.

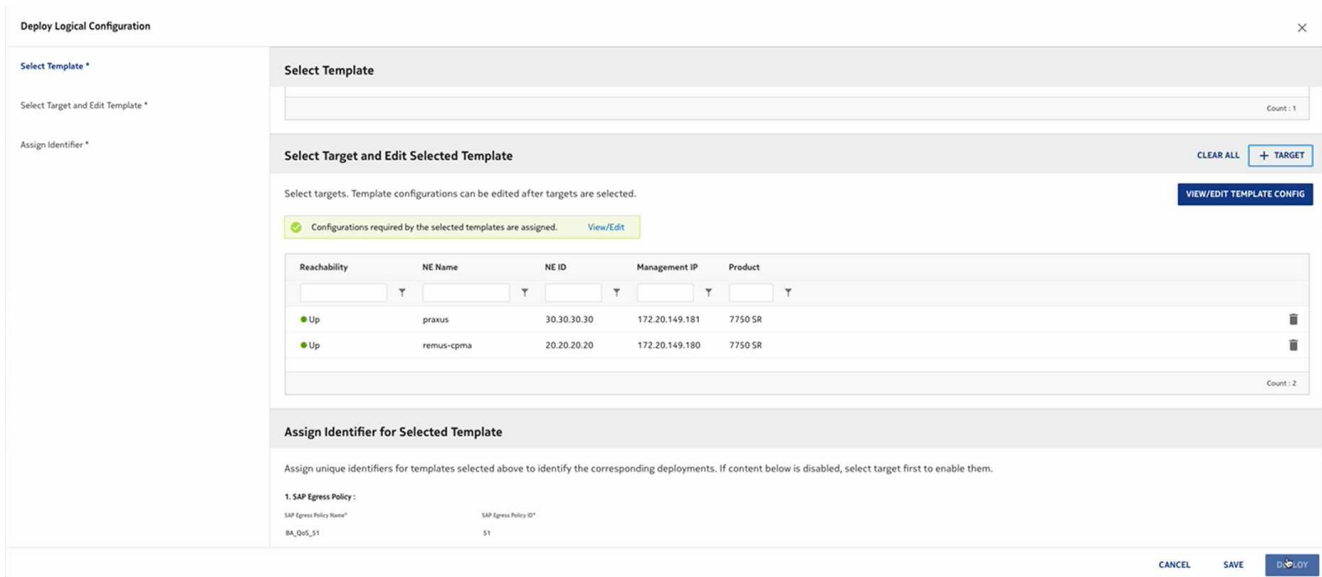
8

Select the NEs you want to distribute the policy to and click ADD.



9

Click **DEPLOY**.



END OF STEPS

9.4 NFM-P and NSP comparison: LAG Configuration

9.4.1 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 [8.5 “How do I import a configuration intent type?” \(p. 101\)](#) and [8.8 “How do I create a configuration template?” \(p. 106\)](#).

- **Gold_Ports** , which uses the predefined icm-equipment-port-ethernet intent type
- **Gold-LAGs** , which uses the predefined icm-logical-lag-access intent type

9.4.2 Steps

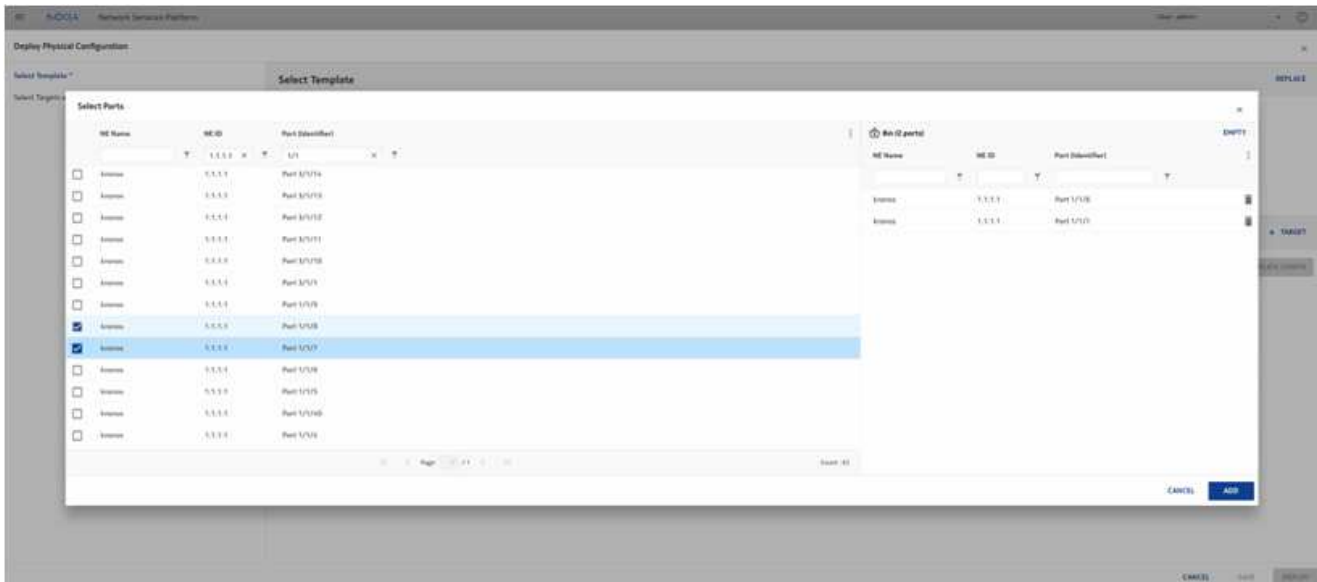
Configure the ports

- 1 _____
Open **Device Management, Configuration Templates**.
- 2 _____
Select **Gold_Ports** from the list of configuration templates and click **⋮** (Table row actions), **Deploy to Network**.

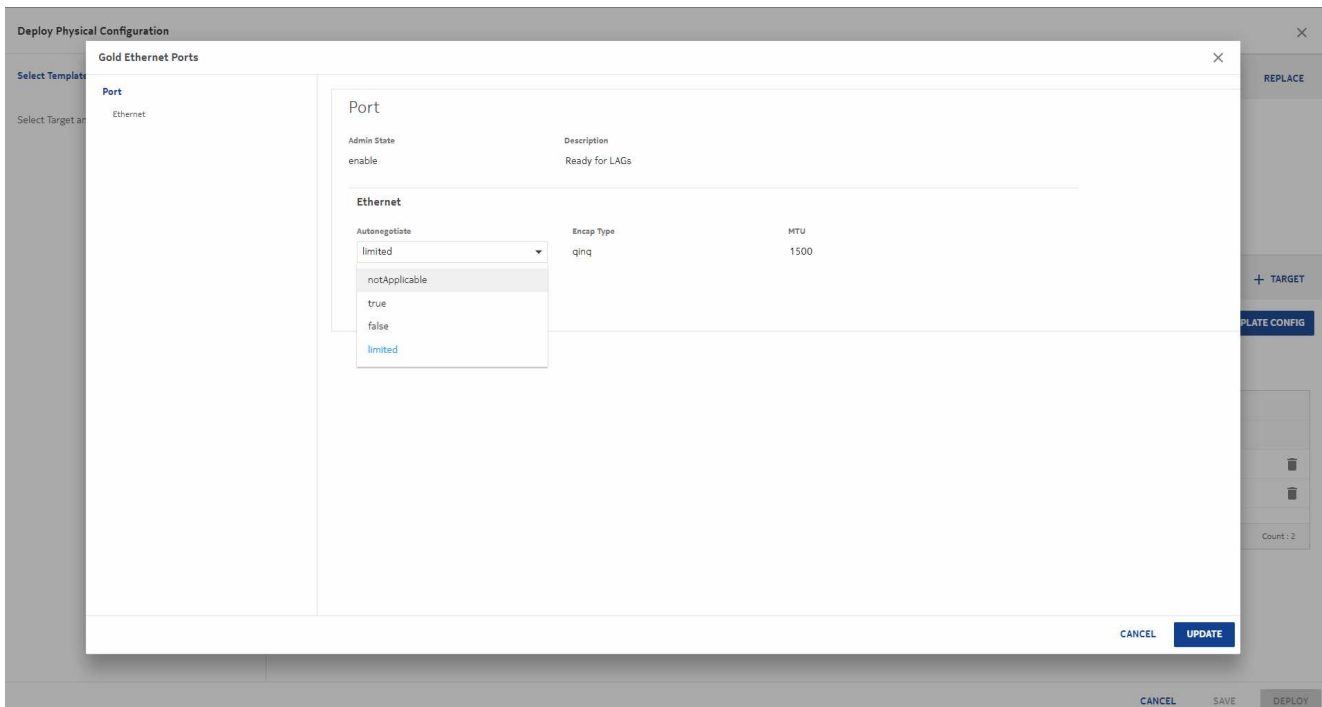
Name	Description	Life Cycle	Intent Type	Intent Type Version	Config Form	Config Form State	Role	Category	Device Scope	Flexible	List L
Gold_Ports		released	icm-equipment-port-ethernet	2	gold	Up-to-date	Physical	Port	SRDS Classic & Model	No	None
Ingress_OuS		released	icm-ops-suppress-egress	2	default	Up-to-date	Logical	Out	SRDS Classic & Model	No	View all deployments...
Egress_OuS		released	icm-ops-suppress-egress	2	default	Up-to-date	Logical	Out	SRDS Classic & Model	No	Migrate deployments...
Statement		released	icm-router-policystatement-eg...	2	default	Up-to-date	Logical	Router	SRDS Classic & Model	No	Audit/Sign Deployments...
Customer		released	icm-service-customer	2	default	Up-to-date	Logical	Service	All	No	Deploy to network...
Ready_Access_Ports_A...		released	icm-equipment-port-ethernet	2	default	Up-to-date	Physical	Port	SRDS Classic & Model	No	Associate to network...
SAP Egress Policy		released	icm-ops-suppress-egress	2	default	Up-to-date	Logical	Out	SRDS Classic & Model	No	View...

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.

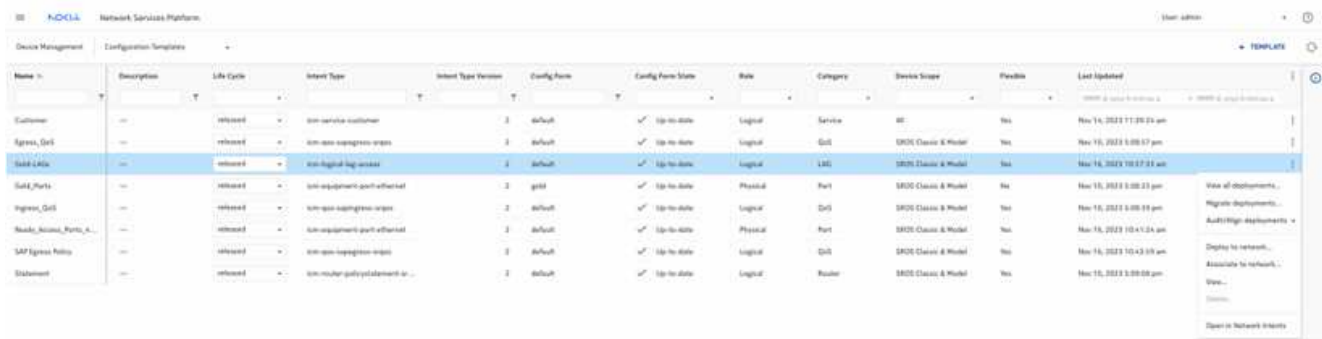


Click **UPDATE** to close the View form, and **DEPLOY** to send the configuration to the ports.

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**.

Deploy Logical Configuration > View/Edit Template Config

Below are templates selected in the "Select Template" section of the previous page. Click on each of them to view or modify configurations that come with it.

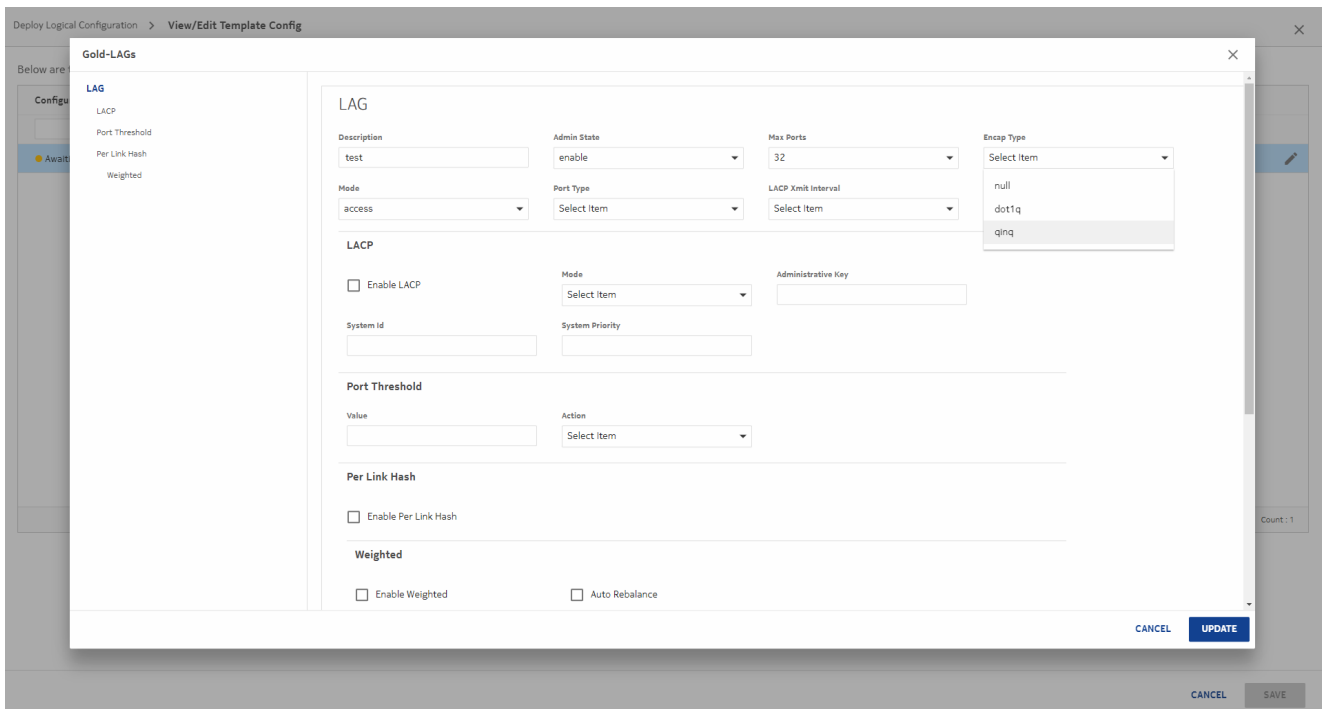
Configuration Status	Template Name	Description	Role	Category	Device Scope	Flexible
Awaiting user input	Gold-LAGs	N/A	Logical	LAG	SROS Classic & Model	True

Count: 1

CANCEL SAVE

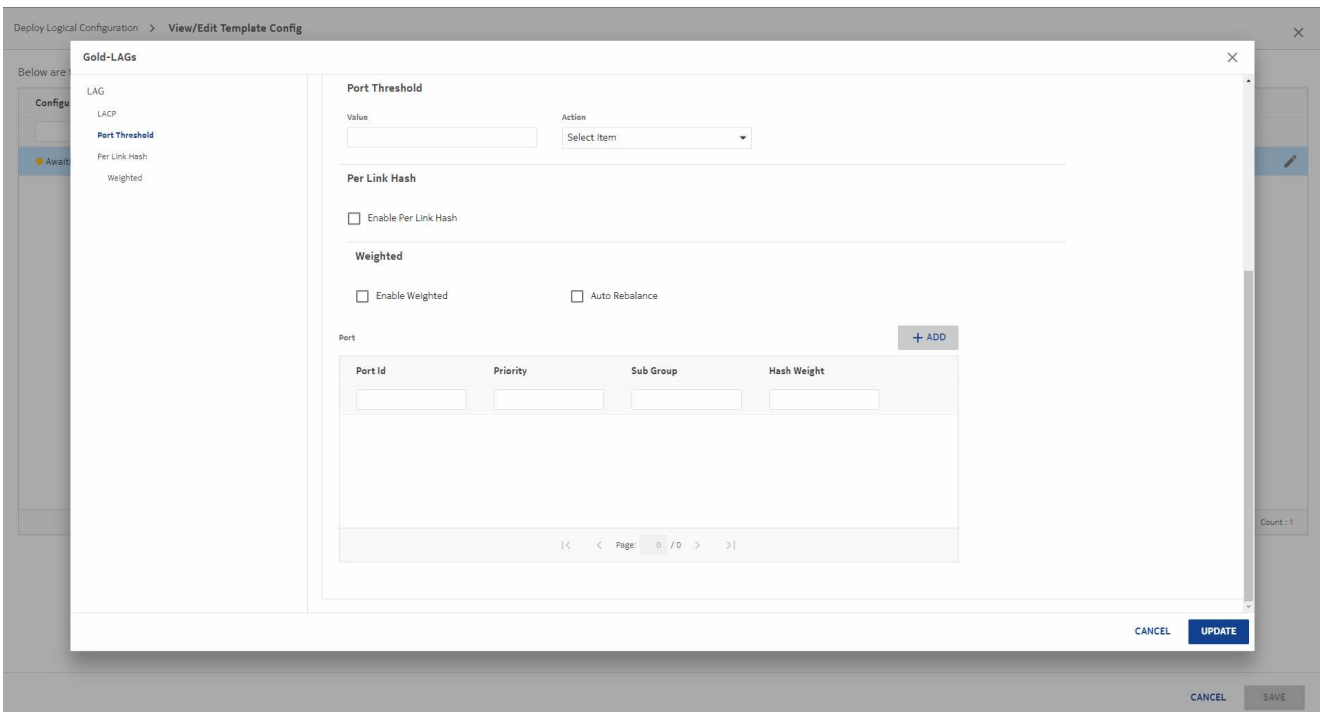
9

Configure the LAG parameters as needed.



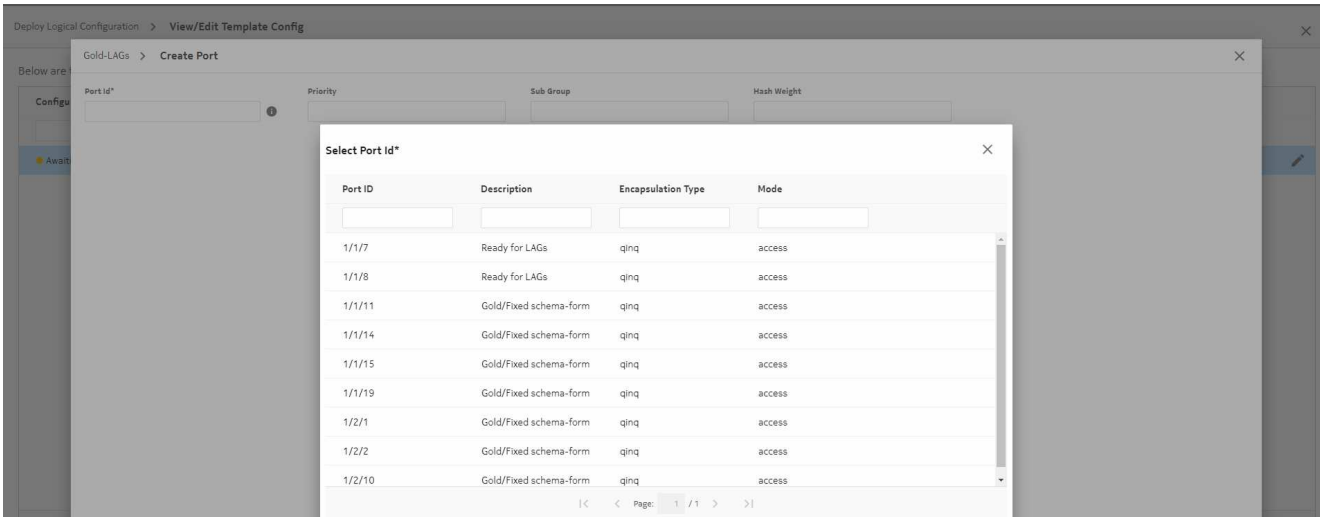
10

Click **+ ADD** to add the ports you configured with the previous template.



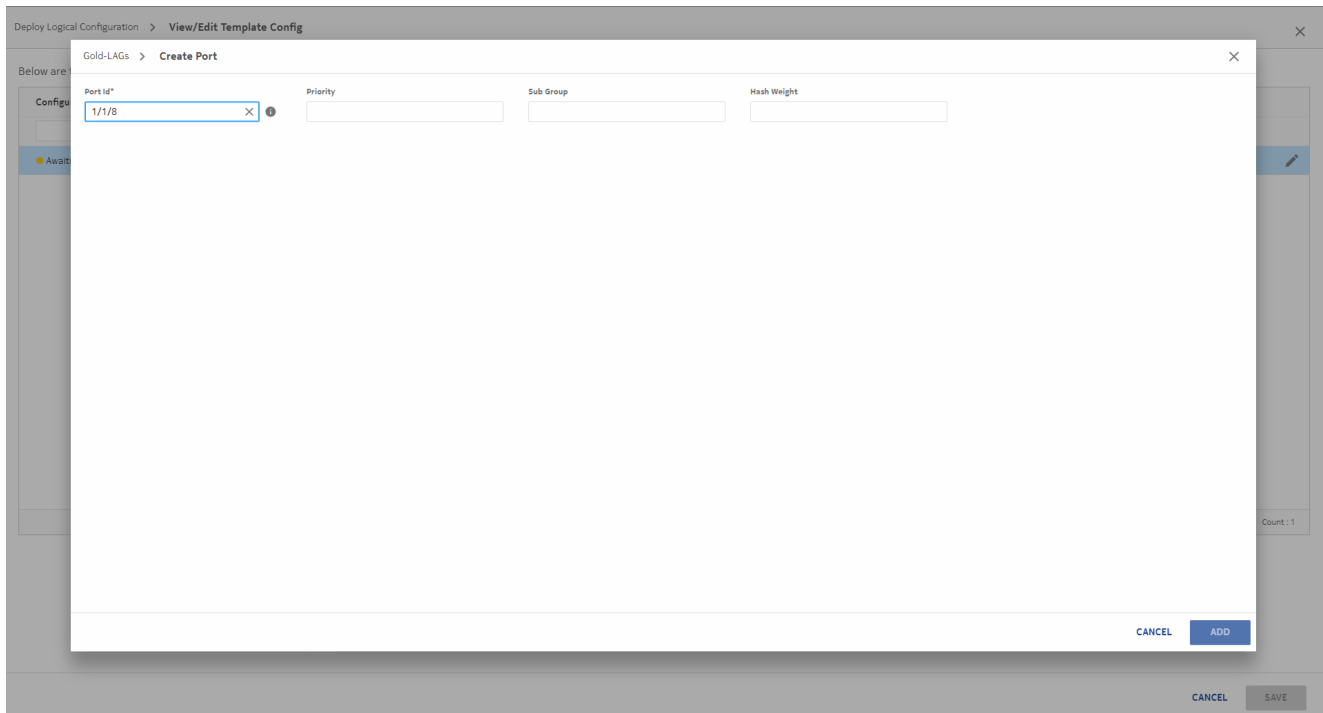
11

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



12

Configure port parameters as needed and click **ADD**.

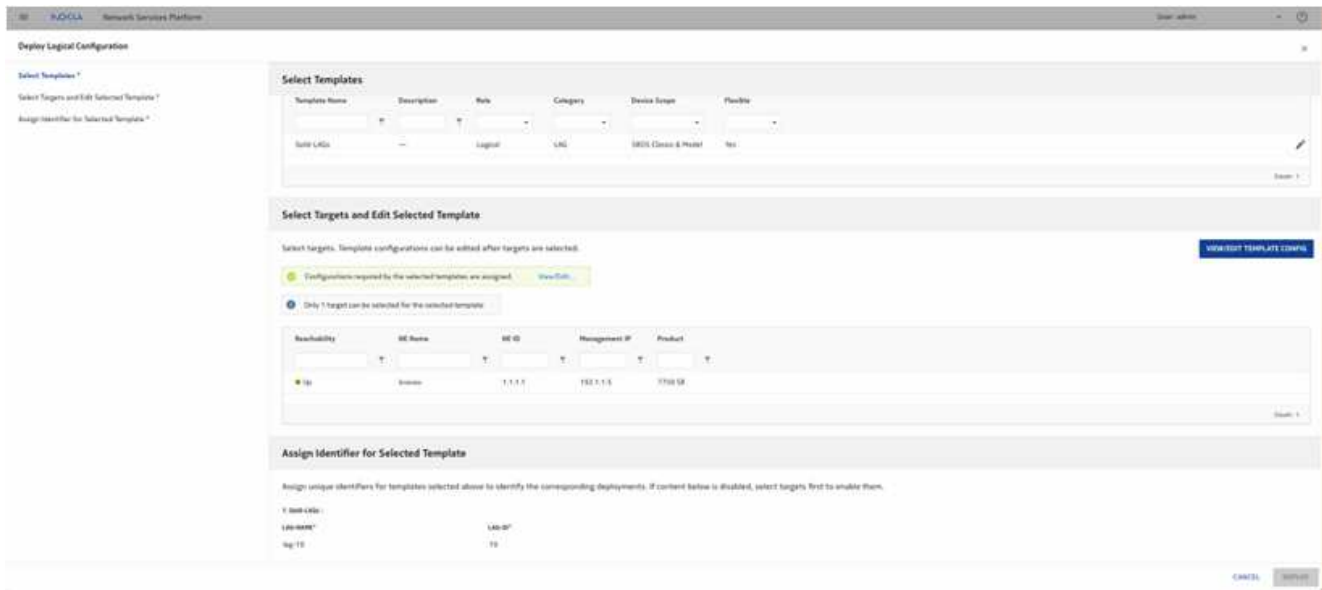


13

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.



