NSP
Network Services Platform

Use Case Catalog Sample Procedures

3HE-20932-AAAA-TQZZA
Issue 4
May 2025

Legal notice

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

Contents

About this document

Purpose

The *NSP Use Case Catalog Sample Procedures* document is intended for NSP operators and administrators who need to understand or perform NSP device and service management processes.

This document describes the steps required to complete use cases found in the NSP Network Automation Use Case Catalog. For more information about the use case catalog, see (https://www.nokia.com/networks/ip-networks/network-services-platform/use-case-catalog/).

This guide is a multi-release document that provides tested procedures with release-specific sample commands from different NSP releases, depending on the use case.

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.

1 UCC-11: Brownfield Service Discovery

1.1 Overview

1.1.1 Purpose

This chapter describes the steps that are common to discovery of all brownfield services covered in this guide (i.e., E-LINE, E-LAN, C-LINE, IES, and L3 VPN (VPRN)) in NSP.

Configuration examples in this chapter show NSP Release 24.4 and SR OS 23.7.R2 NEs.

The following artifact bundles were used to test this use case:

- nsp-svc-assurance-bundle-2404.zip
- nsp-svc-fulfillment-bundle-2404.zip

See the NSP and NE documentation for more information.

1.1.2 Contents

Preparation

1.2 Prerequisites

1.2.1 Network configuration prerequisites

Before services can be configured and managed in NSP, the network configuration prerequisites must be met. The following table describes the requirements that can apply to service use cases, and indicates whether each prerequisite is required for this use case.

Where an NSP intent type is not available, CLI or MD-CLI must be used to perform configuration on the device.

Prerequisite	Documentation reference	Notes
Mandatory for Brownfield Service Discovery		
GRPC configuration 1. Generate security certificates 2. Configure security and enable GRPC on all devices 3. Apply security certificates on all devices	See SR TLS information here in the SR OS 24.3 R1 documentation: TLS	—
Netconf/SNMP provisioning: enable NETCONF and SNMP protocols on all devices	For more information about SNMP and NETCONF with SR OS, see SNMP and NETCONF in the *SR OS 24.3 R1 System Management Guide*.	—
NSP installation	Pathway for NSP system installation in the *NSP Installation and Upgrade Guide* How do I enable TLS for telemetry and gNMI on_change support? in the *NSP System Administrator Guide*.	Include the following in your deployment: • Feature packs: - platform-baseServices - platform-pluggableNetworkAdaptation - platform-loggingMonitoring - serviceActivationAndConfiguration-intentBasedServiceFulfillment - networkInfrastructureManagement-basicManagement - networkInfrastructureManagement-deviceConfig • Adaptor suites: - sros-common - sros-oc-logical-inventory - sros-23-7-r1

Prerequisite	Documentation reference	Notes
Download the required artifact bundles from the NSP software delivery site: • NSP predefined set for ICM (device configuration) • NSP product artifact bundle for Service Fulfillment	How do I install an artifact bundle? in the *NSP Network Automation Guide*	—
Device discovery	Pathway for device discovery in the *NSP Classic Management User Guide* How do I discover devices? in the *NSP Device Management Guide* Nokia Developer Portal for information about FTP mediation policy creation using API.	—
Cards and MDAs provisioning	ICM process in the *NSP Device Management Guide* for more information about using the Device Configuration views, and the other procedures in the *NSP Device Management Guide* for further detail. See the NSP ICM Intent Type Catalog for information about this and other device configuration intent types developed by Nokia.	The intent type required for this configuration is icm-equipment-card-mda.
Connectors and Ports provisioning		The intent types required for this configuration are: • icm-equipment-port-connector • icm-equipment-port-ethernet
OSPF/ISIS	CLI Reference Guides for SR OS	—
LDPs, MPLS and RSVP configuration	CLI Reference Guides for SR OS	For LDP to be operational, the IPv4 and IPv6 bindings must be configured manually using CLI.
Interfaces Provisioning	How do I create a physical configuration deployment? in the *NSP Device Management Guide*.	The intent type required for this configuration is icm-router-network-interface
Customer creation	How do I create a logical configuration deployment? in the *NSP Device Management Guide*.	The intent type required for this configuration is icm-service-customer
Optional		

Prerequisite	Documentation reference	Notes
Optional items to include in your NSP deployment	Pathway for NSP system installation in the *NSP Installation and Upgrade Guide*	• Optional feature packs: - pathControlAndOptimization - multilayerDiscoveryAndVisualization - NSP Analytics: Network Operations Analytics feature package with the networkOperationsAnalytics-analyticsReporting installation option - NSP Baseline Analytics: networkOperationsAnalytics-baselineAnalytics - networkInfrastructureManagement-performanceIndicatorsAndAlerts • VSR/NRC • An AuxDB • An NFM-P instance
Telemetry/OAM	*NSP Data Collection and Analysis Guide*	• NSP SR OS vendor-agnostic telemetry adaptation artifact bundle • networkInfrastructureManagement-gnmiTelemetry feature pack
BGP/EVPN	How do I create a logical configuration deployment? in the *NSP Device Management Guide*.	The intent type required for this configuration is icm-router-bgp_group
Segment Routing	CLI Reference Guides for SR OS	—
Scheduler QoS Policies	How do I create a logical configuration deployment? in the *NSP Device Management Guide*.	The intent types required for this configuration are: • icm-qos-schedulerpolicy-srqos • icm-qos-network-srqos • icm-qos-sapingress-srqos • icm-qos-sapegress-srqos
Network QoS Policies configuration		
SAP QoS Policies configuration		
PCEP configuration	CLI Reference Guides for VSR-NRC	Most of the connections required for PCEP are established during previous configuration steps.
LAGs and MC-LAG creation	How do I create a logical configuration deployment? in the *NSP Device Management Guide*.	The intent types required for this configuration are: • icm-logical-lag-access • icm-logical-mc_lag-access

1.3 Optional: create a restricted Service Management user

1.3.1 Purpose

Perform this optional procedure to create a user with access only to specified NSP functions.

Procedures in this chapter can be performed by the restricted user, or by an administrator.

This procedure is based on the procedures for the following in the *NSP System Administrator Guide*:

- Configuring a role
- Configuring a user group
- Creating an NSP local user
- Enabling User Access Control
- Configuring user access to an intent type

For example, the reference procedures in NSP Release 24.4 are:

- How do I configure a role?
- How do I configure a user group?
- How do I create an NSP local user?
- How do I enable User Access Control?
- How do I configure user access to an intent type?

1.3.2 Steps

Create a role

1

Log in to the NSP as an administrator.

2

Open **Users and Security**.

3

Select **Roles** from the drop-down list on the toolbar.

4

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

5

In the Identification panel, specify a role name and description.

The Role Name and Description fields can employ **only** the following special characters: `@ - _`.

The Role Name string must not contain *any* spaces, including a leading or trailing space.

6

To assign NSP functional access to the role, go to the Action Permissions panel and select an access level from the drop-down list for each NSP GUI you want to include in the role.

Action permissions group item	Permissions	Notes
Service Fulfillment	Read / Write / Execute	—
Network Intents	Read: Manage Intents	Required to import intent types into Service Management
Workflows	Read	Required to create service and tunnel templates
Optional: DCA Management	Read / Write / Execute	Only required for creating and plotting telemetry subscriptions
Optional: OAM Tests	Read / Write / Execute	Only required for generating and executing OAM tests

7

To assign network resource access to the role, go to the Resource Groups Access panel. (For a detailed explanation of the Resource Groups Access panel, see How do I set network resource access levels? in the *NSP System Administrator Guide*.)

You can assign resource group access globally, to resource group categories, to individual resource groups, or a combination of these. For service management it is recommended to grant access to all equipment and all services:

- **Access To All Equipment** assigns full permissions on all NE resource groups and port resource groups to the role.
- **Access To All Services** assigns full permissions on all service resource groups to the role.

8

Click **Create** to save your changes and return to the Roles list.

END OF STEPS

1.3.3 Create a user group

1

Open **Users and Security**.

2

Select **User Groups** from the drop-down list on the toolbar.

3

Click + **Create User Group**. The Create User Group form opens.

4

Specify a group name and description in the **Identification** panel.

The user group name you specify here must exactly match a corresponding user group name returned by your user repository.

The User Group Name and Description fields can employ **only** the following special characters: `@ - _`.

The User Group Name string must not contain *any* spaces, including a leading or trailing space.

5

To assign user roles to the group, click **+ Add Roles** on the Roles panel. The Add Roles form opens.

6

Enable the check box for each role you want to assign to the group and click **Done**. The roles are added to the Selected Roles list.

To remove a role item from the Selected Roles list, click **Delete** on the item.

7

Click **Create** to save your changes and return to the User Groups list.

END OF STEPS

1.3.4 Create a user

Note: This procedure describes how to create a local NSP user account in a system deployed using OAUTH2 authentication. It does not apply to users managed through external databases.

1

Open **Users and Security**.

2

Select **Users** from the drop-down list on the toolbar.

3

Click **+ Create User**.

4

In the Create User form, specify user identification information for the account in the Identification section. The **Username** and **User Group** fields are mandatory.

Note: Any uppercase characters in the username are saved as lowercase.

The **Username** value:

- can be 1 to 40 characters long
- cannot include a space
- cannot have a leading or trailing space
- can include only the following special characters:

- @ (at sign)
- - (hyphen)
- _ (underscore)
- . (period)

5

In the Password section, specify and confirm a password for the user account.

- If you want this password to be temporary, enable the **Force User to Change Password** option. The new user will be forced to change their password when they first login to NSP.
- Enable the **Show Password** option to see the password characters as you type them.
- Click on the **Password Requirements** link to view a list of minimum security requirements for the password.

6

Click **Create**.

END OF STEPS

1.4 Install the required artifact bundles

1.4.1 Purpose

Use this procedure to make the required intent types available to Service Management in NSP. This procedure is based on the procedure for installing an artifact bundle in the *NSP Network Automation Guide*.

For example, the reference procedure in NSP 24.4 is How do I install an artifact bundle?.

1.4.2 Steps

Install the artifact bundle in NSP

1

Log in to the NSP as the Service Management user.

2

Open **Artifacts**, **Artifact Bundles**.

3

Click **IMPORT & INSTALL**.

4

In the form that opens, drag and drop the artifact bundle that holds the intents provided for this use case, or click **Browse** and navigate to the files on your system.

5

To install the artifact bundle immediately, click **IMPORT & INSTALL**. To import without installing, click **IMPORT**.

The chosen operation is triggered immediately. The artifact bundle status is updated to Imported or Installed when NSP has confirmed the status of all artifacts in the artifact bundle.

6

To install a bundle in Imported status, choose **Install bundle** from the ⋮ (Table row actions) menu.

END OF STEPS

Service Configuration

1.5 Import intent types into Service Management

1.5.1 Purpose

Use this procedure to import the intent types you obtained in 1.4 “Install the required artifact bundles” (p. 18) to the Service Management views. This procedure is based on the procedure for importing an intent type into Service Management in the *NSP Service Management Guide*.

For example, the reference procedure in NSP Release 24.4 is How do I import an intent type into Service Management?.

Note: This procedure is not required in NSP 25.4 or later because intent types for Service Management will import directly into Service Management during artifact bundle installation.

The intent types required are `epipe`, `cpipe`, `evpn-vpls`, `ies`, and `vprn`.

1.5.2 Steps

1

Log in to the NSP as the Service Management user.

2

From the **Service Management, Intent Type Catalogue** view, click **IMPORT**.

A list of previously-defined intent types is displayed.

Note: Only intent types that have the Service Fulfillment label applied will be available to import.

Note: For a restricted user to be allowed to import intent types, they must have appropriate permissions configured for those intent types in Network Intents; see How do I configure user access to an intent type? in the *NSP Network Automation Guide*.
The permission needs to be granted to all applicable Intent Types.

3

Select the check boxes in-line with the intent types you wish to import and click **IMPORT**.

Depending on the service type that has to be covered, the corresponding Intent Type in the following list can be imported.

Intent types to be imported:

- epipe
- cpipe
- evpn-vpls
- ies

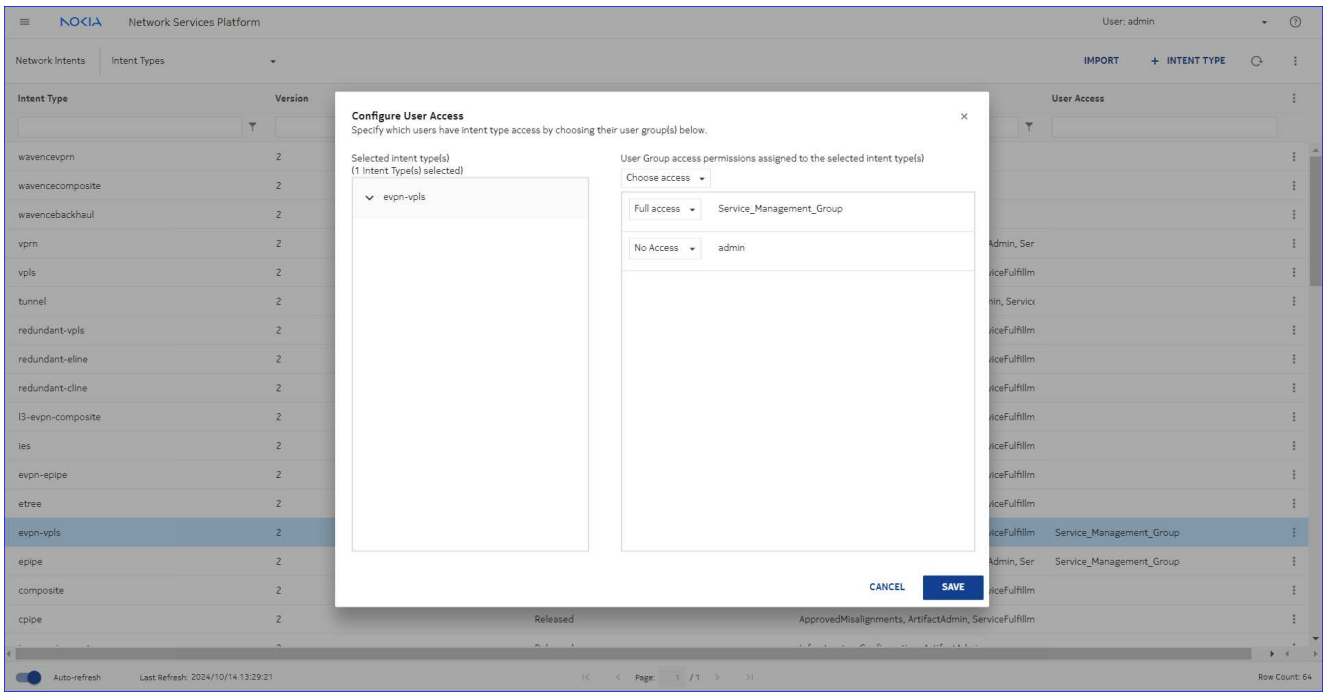
- vprn

The intent types are imported into service management. This may take a few minutes.

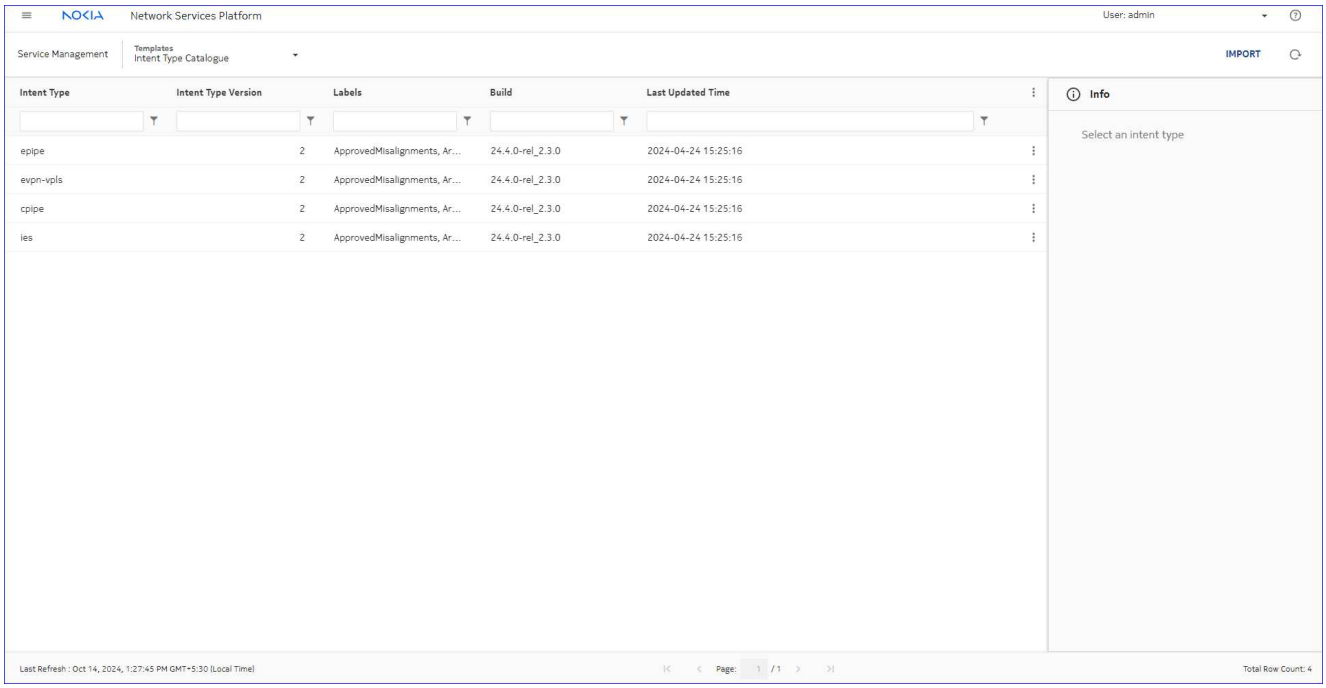
Note: Selecting an imported intent type from the list opens the Info panel, which displays historical information such as the last time the intent type was updated, the last time it was imported, and the last time the modules that compose the intent type were revised.

END OF STEPS

1.5.3 Example configuration of user access to evpn-vpls intent type



1.5.4 Example importing intent types into Service Management



1.6 Create a service template

1.6.1 Purpose

This procedure is based on the procedure to create a service template in the *NSP Service Management Guide*.

For example, the reference procedure in NSP 24.4 is How do I create a service template?.

1.6.2 Steps

1

Log in to the NSP as the Service Management user.

2

From the **Service Management, Service Templates** view, click **+ CREATE**.

The Create a service template form opens.

3

Configure the parameters, as required.

Parameter	Description
Template Name	Specifies the name of the template
Description	Describes the template
Service Intent Type	One of the following based on the service type: `epipe`, `cpipe`, `evpn-vpls`, `ies`, `vprn`
Intent Version	Specifies which version of the selected service intent type to associated with the template
State	**Released**
Config Form	Specifies the interface to be used with the template

4

If required, click **+ ADD** in the Workflows panel to add workflows to the service template.

The Add Workflows form opens.

5

Configure the parameters, as required:

Parameter	Description
Workflow Name	Specifies the workflow to be executed
Service Life Cycle State	Specifies the life cycle state of the service that will trigger workflow execution
Service Life Cycle Case	Specifies the case, Success or Fail, relative to the life cycle state that will trigger workflow execution
Blocking	Specifies whether unsuccessful execution of the workflow will prevent service life cycle state changes
Workflow Execution Timeout (seconds)	Specifies the length of time, in seconds, that unsuccessful execution of the workflow will prevent service life cycle state changes

6

Click **ADD**.

The Add Workflows form closes and the workflow is added to the service template.

7

If required, select a Default Service Category in the Bulk Association panel to specify a service type to which this service template can be applied in bulk.

8

Click **CREATE**.

The service template is created.

END OF STEPS

1.7 Stitch a brownfield service

1.7.1 IBSF service stitching

IBSF provides the functionality to stitch brownfield MDM managed service sites into a single service entity and persist them in the NSP database so they are visible (read-only) by IBSF. Then, the user may associate the service to a template which would enable full lifecycle management and CRUD support. In order to achieve this, a service stitching algorithm was developed to stitch sites together into a single service entity based on service type and algorithm. This service stitching can be triggered from the IBSF API or by enabling auto-stitch.

1.7.2 Prerequisites

The required artifacts for service stitching are in the svc-mgt-artifacts-common bundle. These artifacts include data-sync mapping and metadata files.

This is available on: (https://download-na.support.nokia.com/cgi-bin/Download.pl?hier_id=197305).

1.7.3 Service stitching API

The service stitching API takes 3 input parameters: service-type, algorithm, and sites. Only include MDM sites. The URL and body is as follows:

(https://{{server}}/restconf/data/nsp-service-intent:stitchservices)

```
{
   "input":{
   "service-type":<service-type>,
   "algorithm":<name-of-algorithm>,
   "sites":["2.2.2.2","3.3.3.3]
   }
}
```

1.7.4 Stitching procedures

Perform one of the following procedures to stitch a brownfield service:

- Service Stitching – EPIPE Services
- Service Stitching – ELAN Services
- Service Stitching – IES Services
- Service Stitching – L3 VPN Services

1.7.5 Auto-stitching

Perform the following procedure to auto-stitch a brownfield service:

- Auto-stitching a brownfield service

1.8 Service stitching – EPIPE/ELINE services

1.8.1 Service stitching algorithm for Epipe services

The following are the service stitching algorithm for Epipe services with their stitching criteria:

Algorithm	Stitching Criteria
route-target	sites must have inverse matching route-target values and inverse matching local/remote ac values
service-name	matching service-name
evi	sites must have matching evi values and inverse matching local/remote ac values
local	a single site with 2 access interfaces
vcid	site's tunnel binding must have matching vcid

Note: *Route-target* and *evi* algorithms are for EVPN-EPIPE and outside the scope of this document. Service stitching with the other 3 algorithms are documented below.

1.8.2 Service stitching with service-name algorithm

Services which are to be stitched with service-name algorithm should have same service names on the end sites.

1

Stitch the Epipe service created on MD NE using the following API:

POST: (https://{{server}}/restconf/data/nsp-service-intent:stitchservices)

BODY:

```
{
   "input":{
   "service-type":"eline",
   "algorithm":"service-name",
   "sites":["92.168.96.190","92.168.96.46"]
   }
}
```

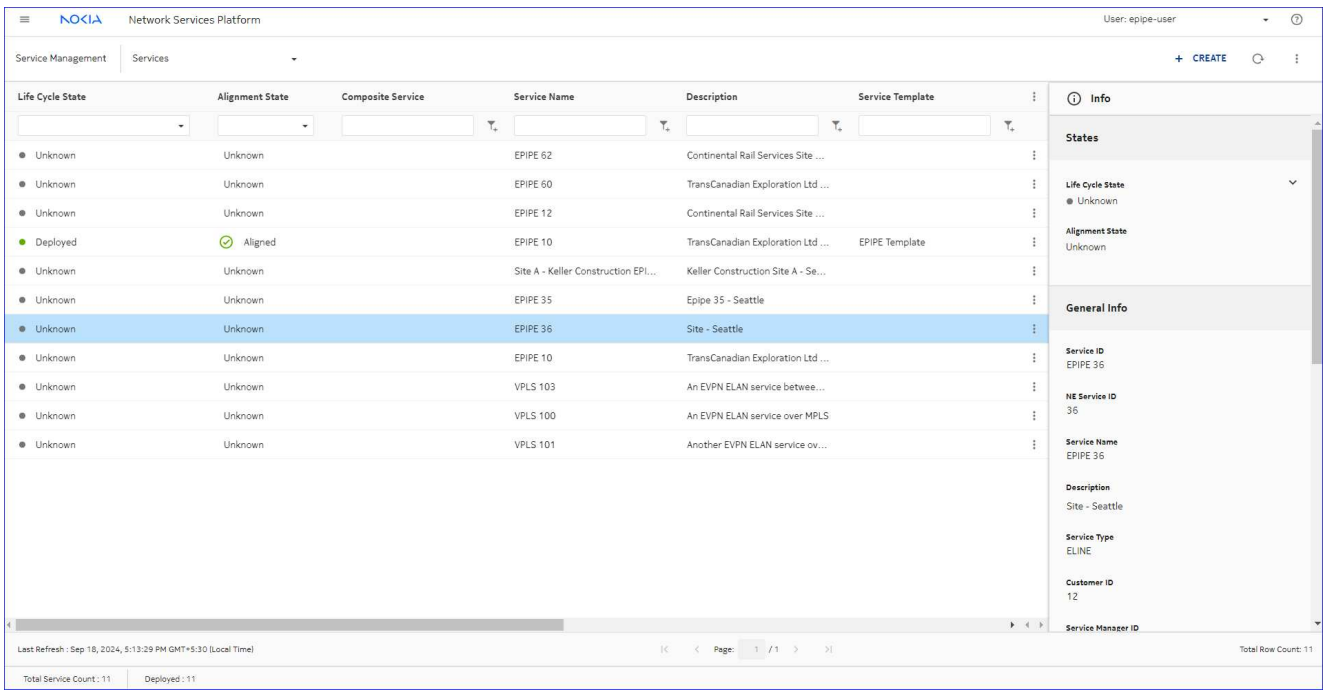
RESPONSE:

```
{
```

```
        "response": {
            "status": 0,
            "startRow": 0,
            "endRow": 0,
            "totalRows": 1,
            "data": "Successfully submitted to Job Manager for Service
Stitch processing with Job Name: eline_service-name-1726659802472",
            "errors": null
        }
    }
```

2

Ensure the service gets listed in the NSP Service Management in 'Unknown' state.



END OF STEPS

1.8.3 Service stitching with local algorithm

1

Stitch the Epipe service created on MD NE using the following API:

POST: (https://{{server}}/restconf/data/nsp-service-intent:stitchservices)

BODY:

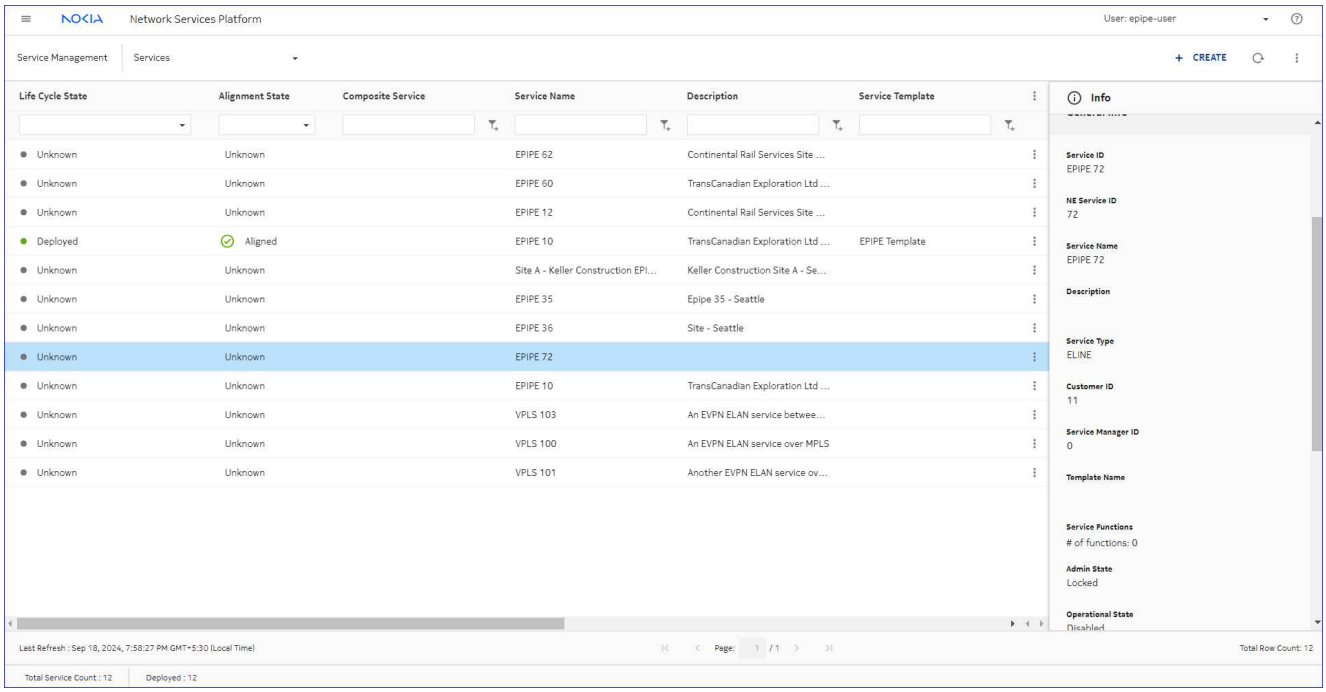
```
{
   "input":{
   "service-type":"eline",
   "algorithm":"local",
   "sites":["92.168.96.190"]
   }
}
```

RESPONSE:

```
{
   "response": {
      "status": 0,
      "startRow": 0,
      "endRow": 0,
      "totalRows": 1,
      "data": "Successfully submitted to Job Manager for Service
Stitch processing with Job Name:"eline_local-1726669622177",
      "errors": null
   }
}
```

2

Ensure the service gets listed in the NSP Service Management in 'Unknown' state.



END OF STEPS

1.8.4 Service stitching with vcid algorithm

1

Stitch the Epipe service created on MD NE using the following API.

POST: (https://{{server}}/restconf/data/nsp-service-intent:stitchservices)

BODY:

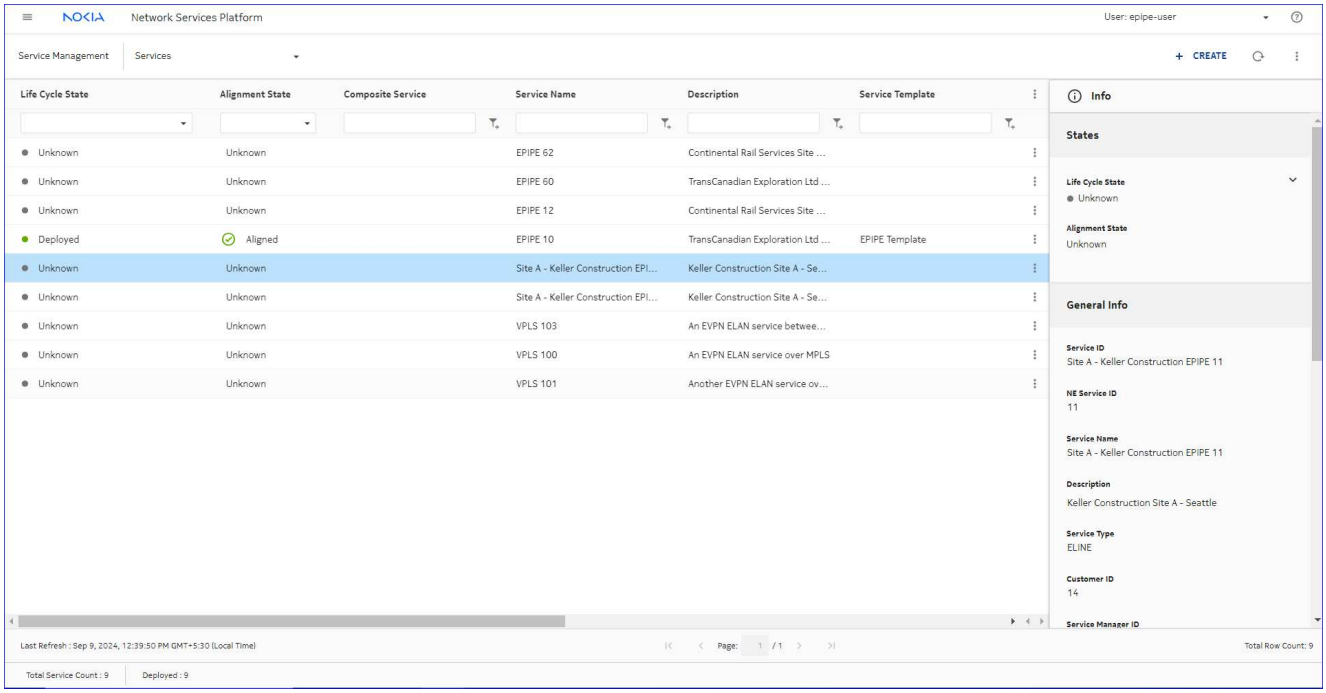
```
{
   "input":{
   "service-type":"eline",
   "algorithm":"vcid",
   "sites":["92.168.96.190","92.168.96.46"]
   }
}
```

RESPONSE:

```
{
   "response": {
      "status": 0,
      "startRow": 0,
      "endRow": 0,
      "totalRows": 1,
      "data": "Successfully submitted to Job Manager for Service
Stitch processing with Job Name: eline_vcid-1725863475919",
      "errors": null
   }
}
```

2

Ensure the service gets listed in the NSP Service Management in 'Unknown' state.



END OF STEPS

1.9 Service stitching – ELAN services

1.9.1 Service stitching algorithm for Elan services

The following are the service stitching algorithm for Elan services with their stitching criteria:

Algorithm	Stitching Criteria
route-target	sites must have inverse matching route-target values
service-name	matching service-name
evi	sites must have matching evi values and inverse matching local/remote ac values
vcid	site's tunnel binding must have matching vcid

1.9.2 Service stitching with service-name algorithm

1

Stitch the Elan service created on MD NE using the following API.

POST: (https://{{server}}/restconf/data/nsp-service-intent:stitchservices)

BODY:

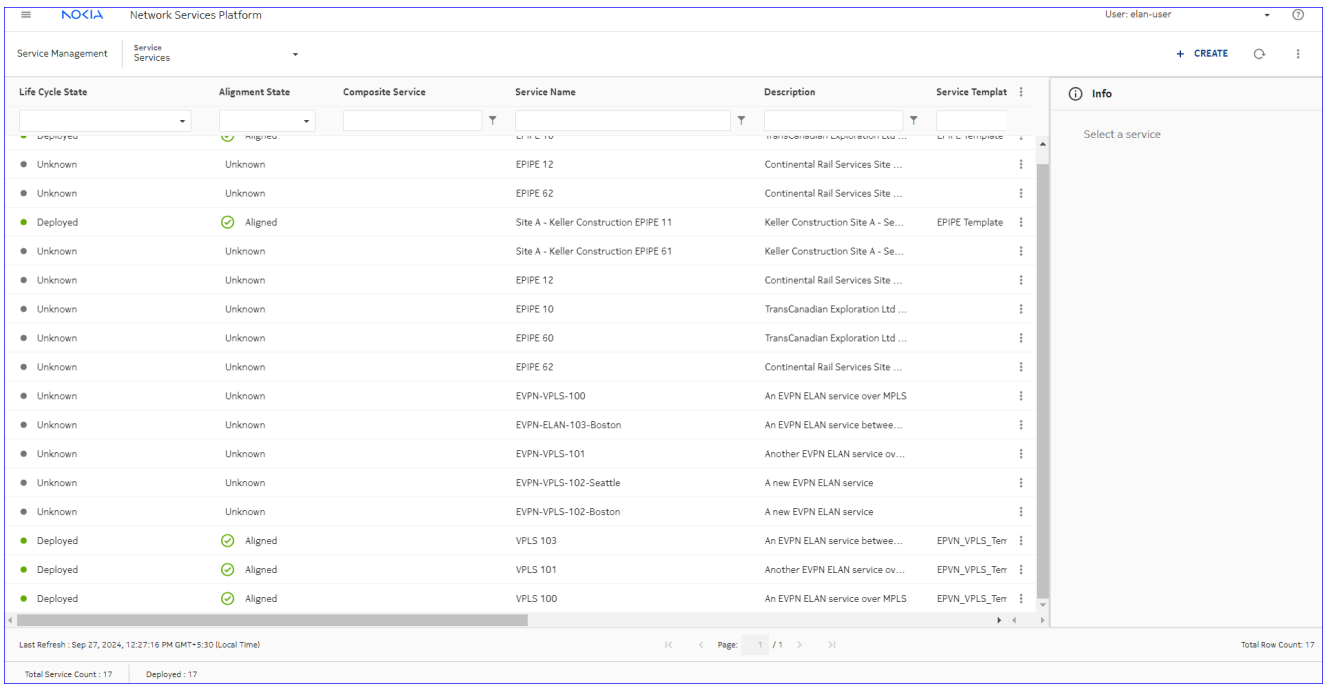
```
{
   "input":{
   "service-type":"elan",
   "algorithm":"service-name",
   "sites":["92.168.96.190","92.168.96.46"]
   }
}
```

RESPONSE:

```
{
   "response": {
      "status": 0,
      "startRow": 0,
      "endRow": 0,
      "totalRows": 1,
      "data": "Successfully submitted to Job Manager for Service
Stitch processing with Job Name: elan_service-name-1727419509598",
      "errors": null
   }
}
```

2

Ensure the service gets listed in the NSP Service Management in 'Unknown' state.



End of steps

1.9.3 Service stitching with evi algorithm

1

Stitch the Elan service created on MD NE using the following API:

POST: (https://{{server}}/restconf/data/nsp-service-intent:stitchservices)

BODY:

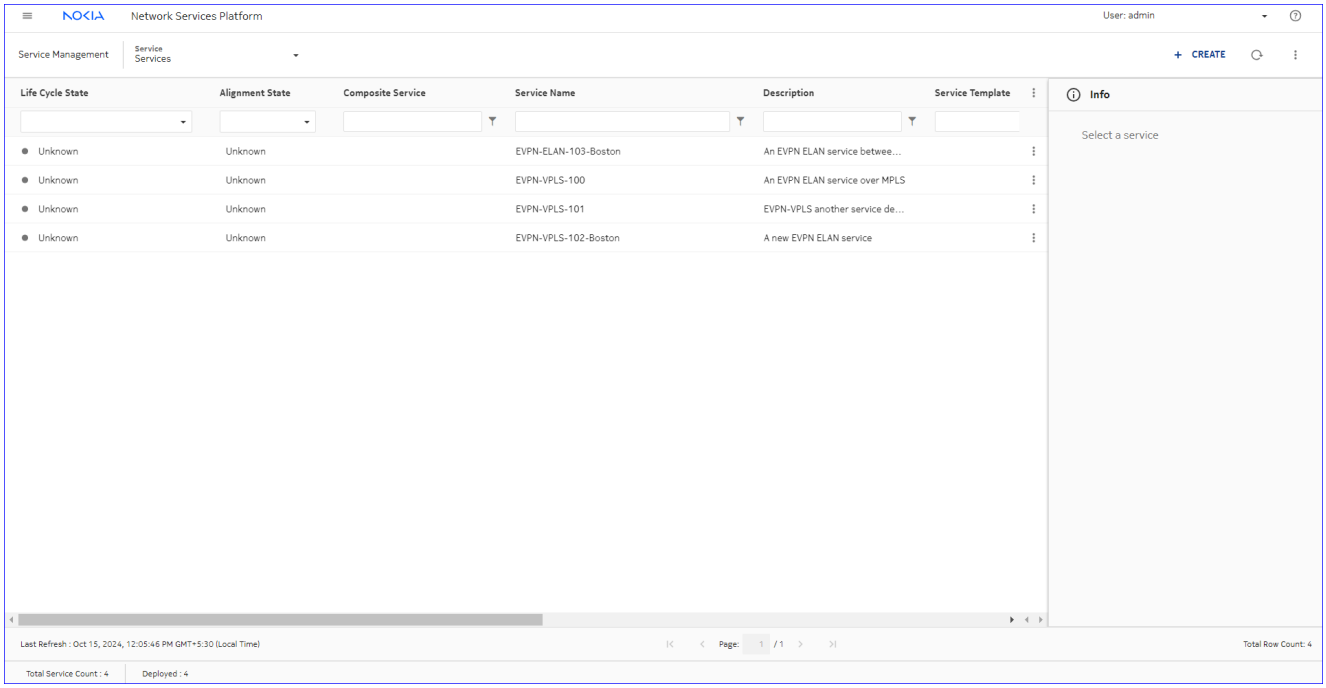
```
{
   "input":{
   "service-type":"elan",
   "algorithm":"evi",
   "sites":["92.168.96.190","92.168.96.46"]
   }
}
```

RESPONSE:

```
{
   "response": {
      "status": 0,
      "startRow": 0,
      "endRow": 0,
      "totalRows": 1,
      "data": "Successfully submitted to Job Manager for Service
Stitch processing with Job Name: elan_evi-1728379514781"
      "errors": null
   }
}
```

2

Ensure the service gets listed in the NSP Service Management in 'Unknown' state.



END OF STEPS

1.10 Service stitching – IES services

1.10.1 Service stitching algorithm for IES services

The following are the service stitching algorithm for IES services with their stitching criteria:

Algorithm	Stitching Criteria
service-name	matching service-name

1.10.2 IES service stitching with service-name algorithm

Services which are to be stitched with service-name algorithm should have same service names on the end sites.

1

Stitch the IES service created on MD NE using the following API:

POST: (https://{{server}}/restconf/data/nsp-service-intent:stitchservices)

BODY:

```
{
    "input":{
```

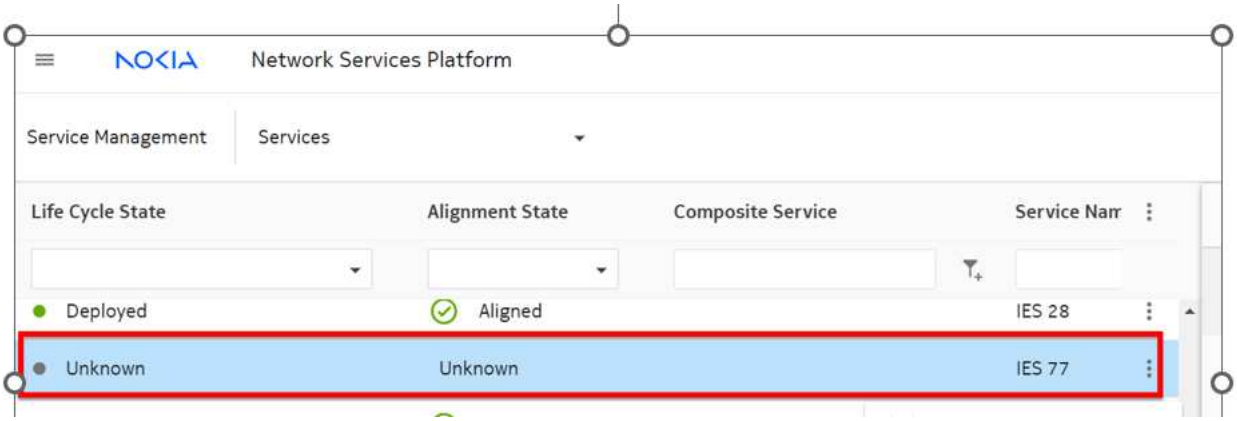
```
            "service-type":"ies",
            "algorithm":"service-name",
            "sites":["92.168.98.97","92.168.96.215"]
        }
}
```

RESPONSE:

```
{
    "response": {
            "status": 0,
            "startRow": 0,
            "endRow": 0,
            "totalRows": 1,
            "data": "Successfully submitted to Job Manager for Service
Stitch processing with Job Name: ies_service-name-1528357814456",
            "errors": null
        }
}
```

2

Once the IES service stitching is successful, ensure the service gets listed in the NSP Service Management in 'Unknown' state.



END OF STEPS

1.11 Service stitching – L3 VPN services

1.11.1 Service stitching algorithm for L3 VPN services

The following are the service stitching algorithm for L3 VPN services with their stitching criteria:

Algorithm	Stitching Criteria
route-target	Full mesh: sites must have inverse matching route-target values Hub and spoke: sites must have inverse matching route-target values. If the 'hub' site is stitched after the 'spoke' sites, the spoke sites will be merged to the hub site's service. When the algorithm detects the need for one site to be merged, the info will be persisted to the nsp db. In the event of a pod restart, the service merge will resume after the pod is up.
service-name	matching service-name

1.11.2 L3 VPN service stitching with route-target algorithm

1

Stitch the L3 VPN service created on MD NE using the following API:

POST: (https://{{server}}/restconf/data/nsp-service-intent:stitchservices)

BODY:

```
{
    "input":{
        "service-type":"l3vpn",
        "algorithm":"route-target",
        "sites":["92.168.96.46","92.168.96.190"]
    }
}
```

RESPONSE:

```
{
    "response": {
        "status": 0,
        "startRow": 0,
        "endRow": 0,
        "totalRows": 1,
        "data": "Successfully submitted to Job Manager for Service
Stitch processing with Job Name: L3 VPN_route-target-1726726571515",
        "errors": null
    }
}
```

2

Once the L3 VPN service stitching is successful, ensure the service gets listed in the NSP Service Management in 'Unknown' state.

END OF STEPS

1.12 Auto-stitching a brownfield service

1.12.1 Auto-stitching

By default, automatic stitching of services is disabled in IBSF. Users can either stitch a service type manually by following the above procedure or enable auto-stitching in which each service type will have a predefined list of supported stitching algorithms that can be selected to run automatically.

The auto-stitching is supported for service-types Eline, Elan, IES, and L3 VPN for the algorithms mentioned in the table below:

Service Type	Algorithm
Eline	vcid, evi, route-target, local and service-name
Elan	vcid, evi, route-target and service-name
IES	service-name
L3 VPN	route-target and service-name

The auto-stitching is disabled by default. The user has to enable the auto-stitching per service-type and specific algorithm type.

The different API calls for auto-stitching are mentioned below.

1.12.2 fetch auto-stitch-config:

restconf GET Url: (https://{{server}}/restconf/data/nsp-service-stitch:nsp-service-auto-stitch-configs/nsp-service-auto-stitch-config)

restconf GET Url for service-type (eline): (https://{{server}}/restconf/data/nsp-service-stitch:nsp-service-auto-stitch-configs/nsp-service-auto-stitch-config=eline)

1.12.3 patch auto-stitch-config:

restconf Patch Url for service-type (eline): (https://{{server}}/restconf/data/nsp-service-stitch:nsp-service-auto-stitch-configs/nsp-service-auto-stitch-config=eline)

payload:

```
{
    "nsp-service-stitch:nsp-service-auto-stitch-config": [
        {
            "admin-state": "unlocked",
            "algorithm-config": [
                {
                    "algorithm": "evi",
```

```
                    "admin-state": "unlocked"
                },
                {
                    "algorithm": "vcid",
                   "admin-state": "locked"
                },
                {
                    "algorithm": "route-target",
                    "admin-state": "locked"
                },
                {
                    "algorithm": "service-name",
                    "admin-state": "locked"
                },
                {
                    "algorithm": "local",
                    "admin-state": "locked"
                }
            ]
        }
    ]
}
```

1.12.4 put auto-stitch-config:

restconf Put Url for service-type (eline): (https://{{server}}/restconf/data/nsp-service-stitch:nsp-service-auto-stitch-configs/nsp-service-auto-stitch-config=eline)

payload:

```
{
    "nsp-service-stitch:nsp-service-auto-stitch-config": [
        {
            "service-type": "eline",
            "admin-state": "unlocked",
            "algorithm-config": [
                {
                    "algorithm": "evi",
                    "admin-state": "locked"
                },
                {
                    "algorithm": "vcid",
                    "admin-state": "locked"
                },
                {
                    "algorithm": "route-target",
                    "admin-state": "locked"
                },
                {
                    "algorithm": "service-name",
```

```
                    "admin-state": "unlocked"
                },
                 {
                    "algorithm": "local",
                    "admin-state": "locked"
                }
            ]
        }
    ]
}

** Unlocked – enabled
** locked - disabled
```

1.13 Associate a brownfield service to service template

1.13.1 Purpose

Perform this procedure to associate a brownfield service to a service template.

Brownfield services created in NFM-P can be brought under the management of NSP by associating the service to a matching service template created in NSP.

1.13.2 Steps

1

Log in to the NSP as the Service Management user.

2

From the **Service Management, Services** view, select a brownfield service.

3

Click ⋮ **Associate template**.

Figure 1-1 Example 1: EPIPE 10

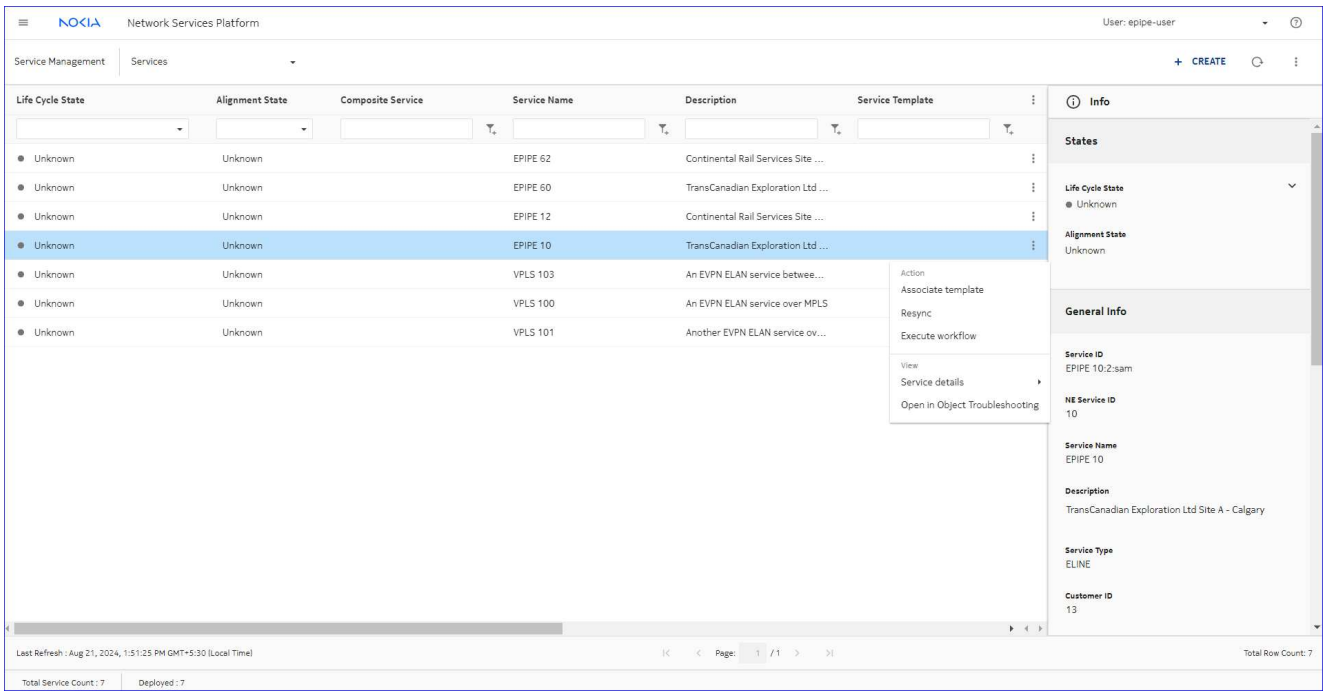
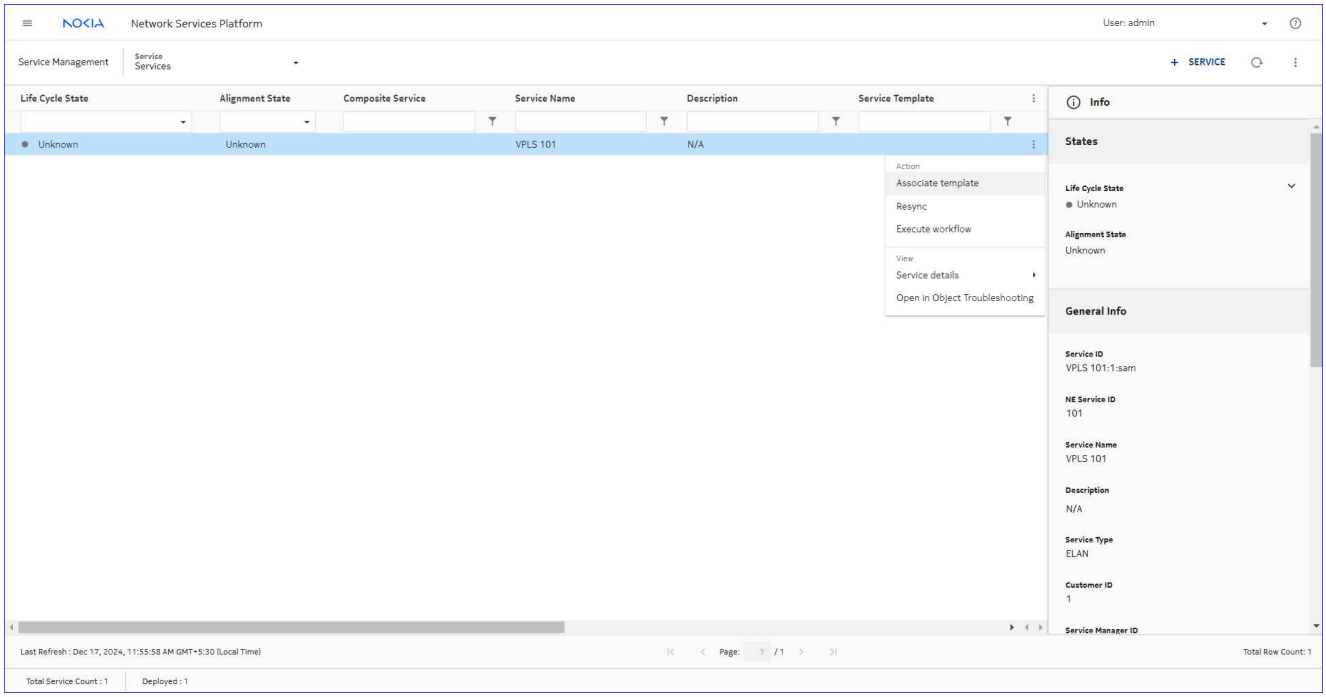


Figure 1-2 Example 2: VPLS 101



4

Select the corresponding brownfield service template to associate and click **CONFIRM**.

Figure 1-3 Example 1: EPIPE 10

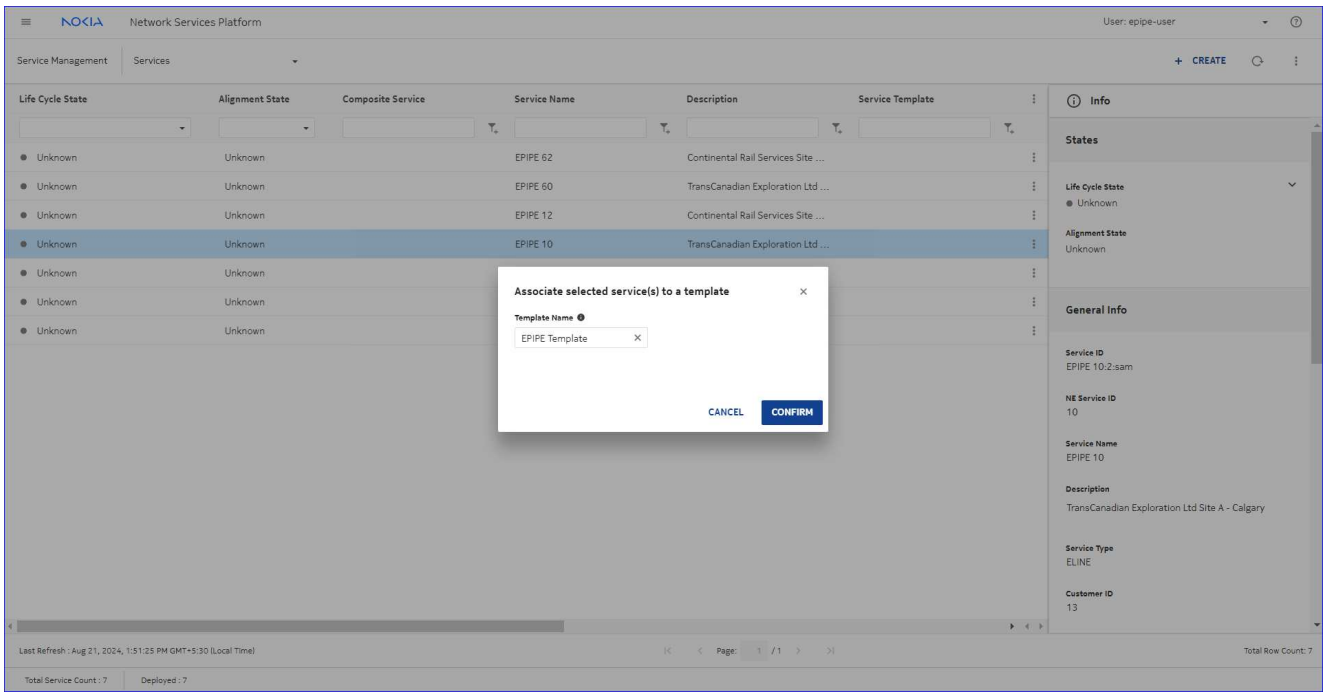
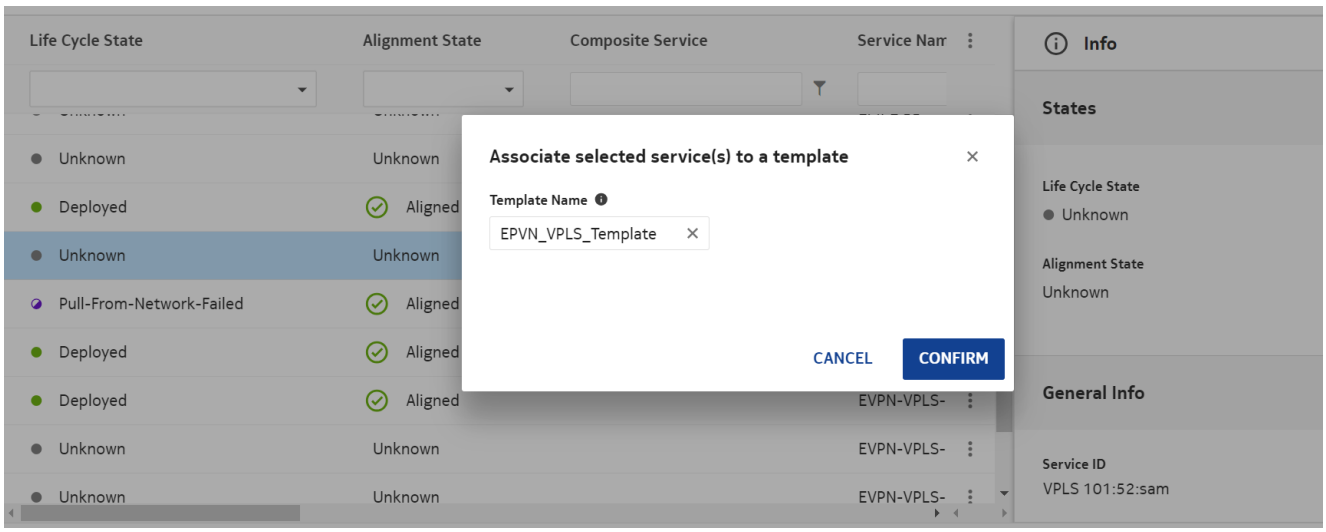


Figure 1-4 Example 2: VPLS 101



5

The service gets associated to the template. It may take a few minutes before it shows up as

Aligned and Deployed in the **Services** list.

Figure 1-5 Example 1: EPIPE 10

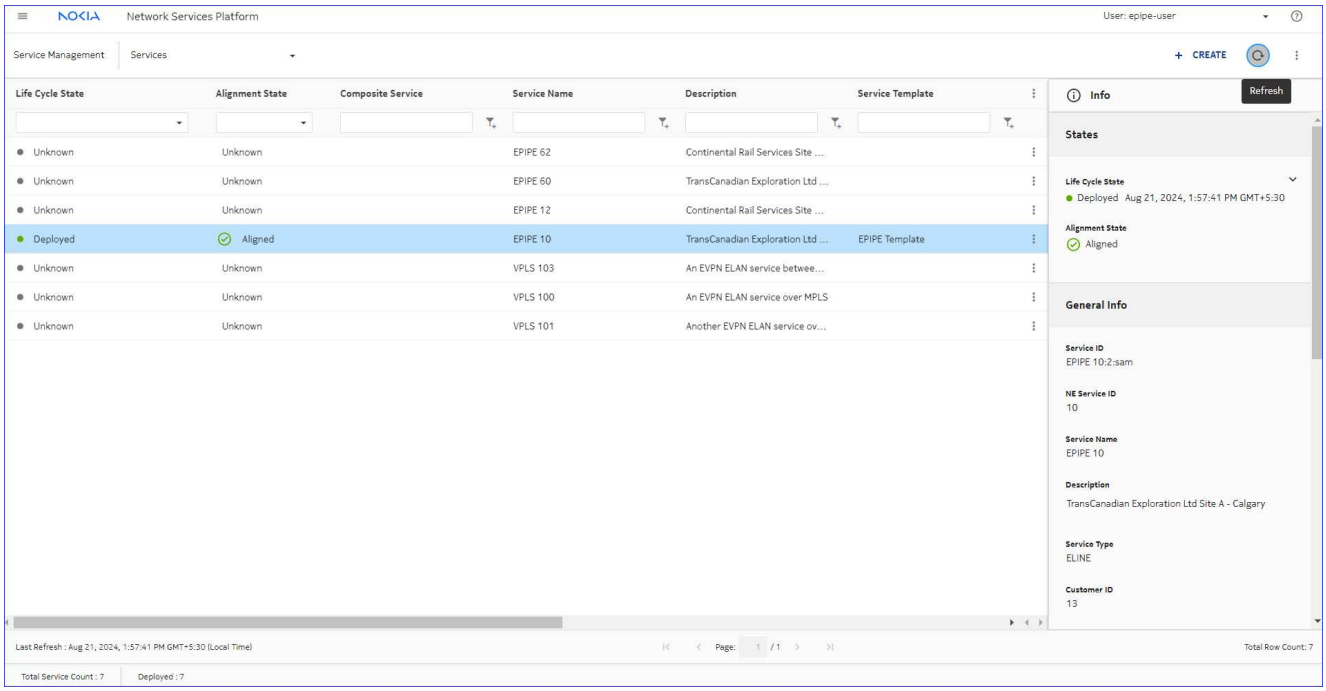
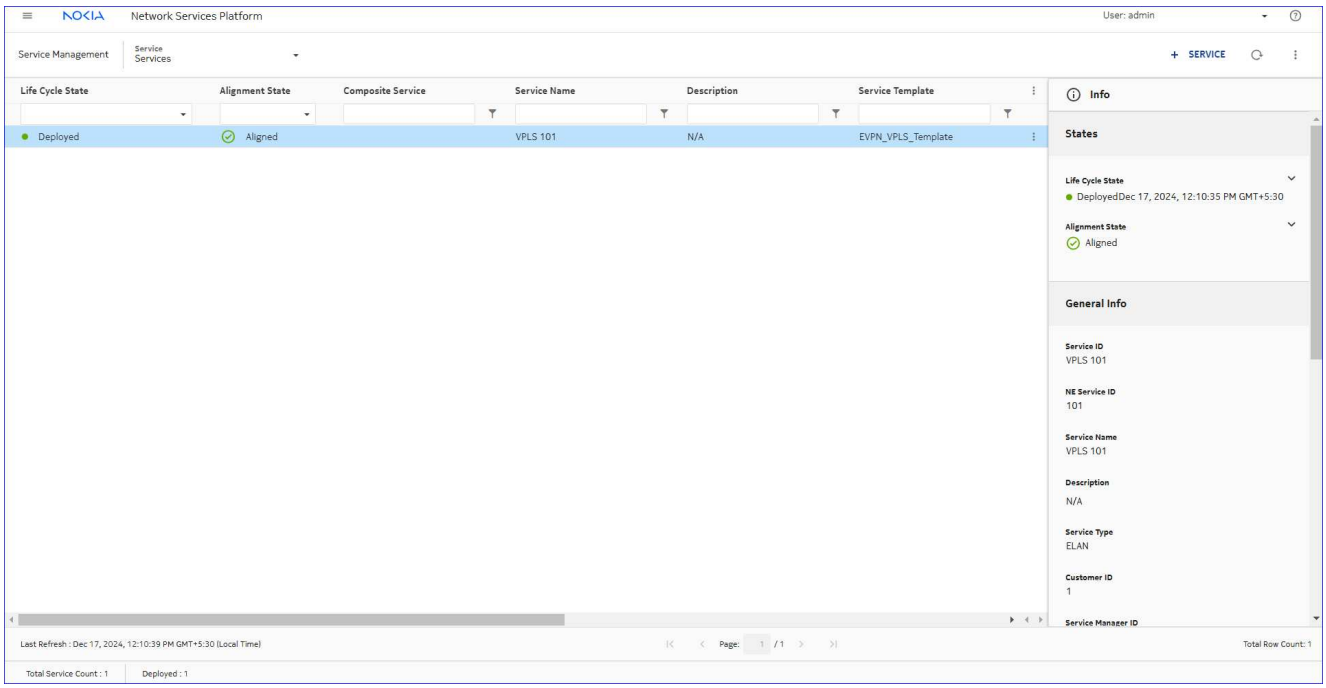


Figure 1-6 Example 2: VPLS 101



END OF STEPS

1.14 Modify a brownfield service

1.14.1 Purpose

The following procedure demonstrates how a brownfield Epipe service can be modified through using the example of modifying an endpoint of the service.

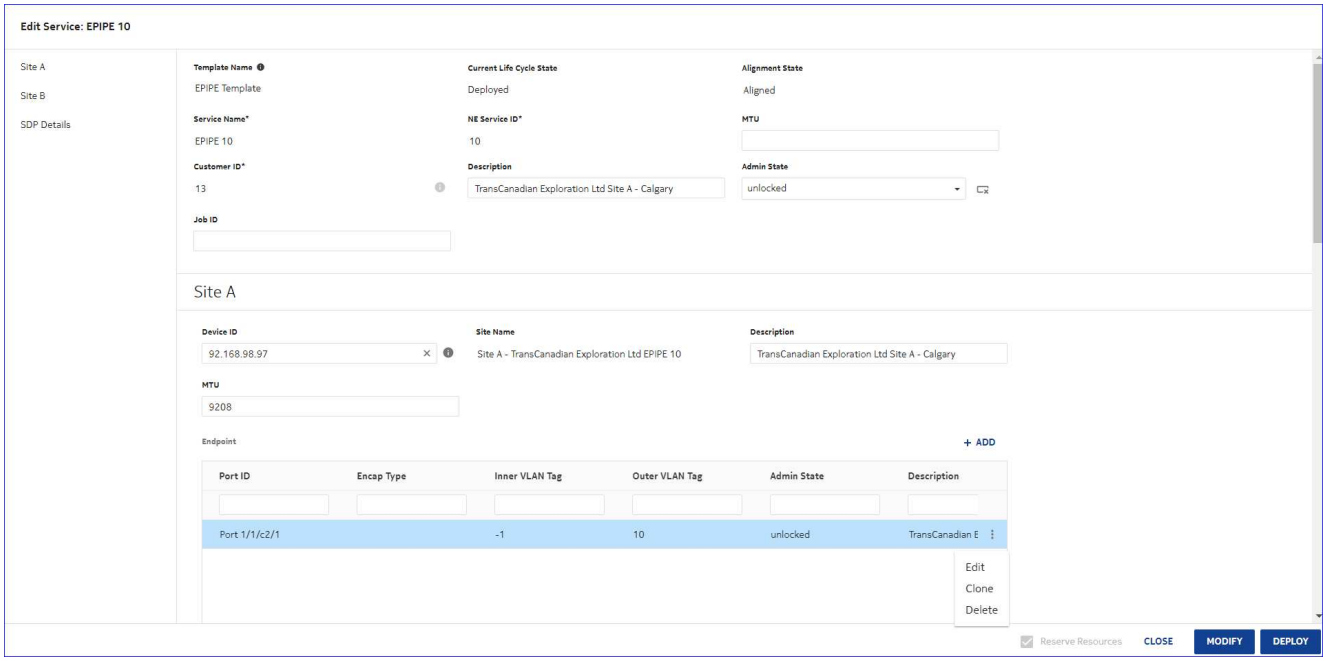
1.14.2 Steps

1

Log in to the NSP as the Service Management user.

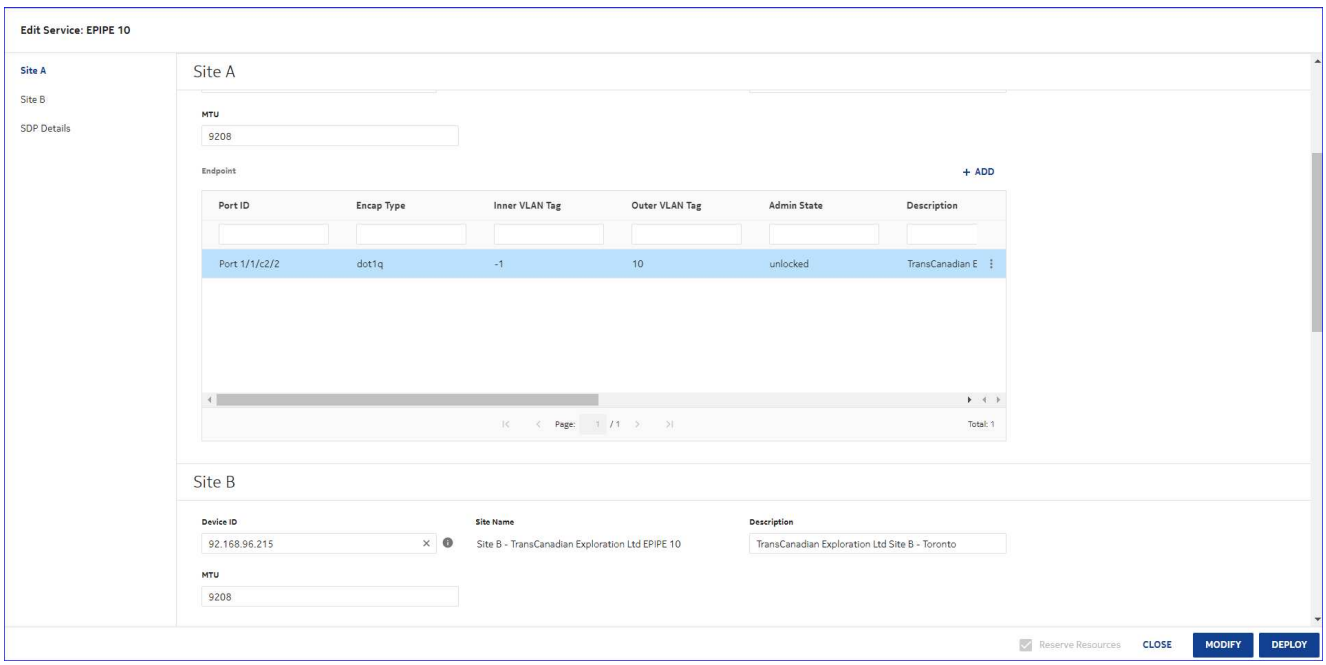
2

From the **Service Management, Services** view, select a brownfield Epipe service and choose **Edit** from the ⋮ (Table row actions) menu.



3

In the Edit Service form, delete the existing endpoint of Site A and add a new endpoint. Click **DEPLOY**.



4

Login to NFM-P and ensure the service is modified accordingly.

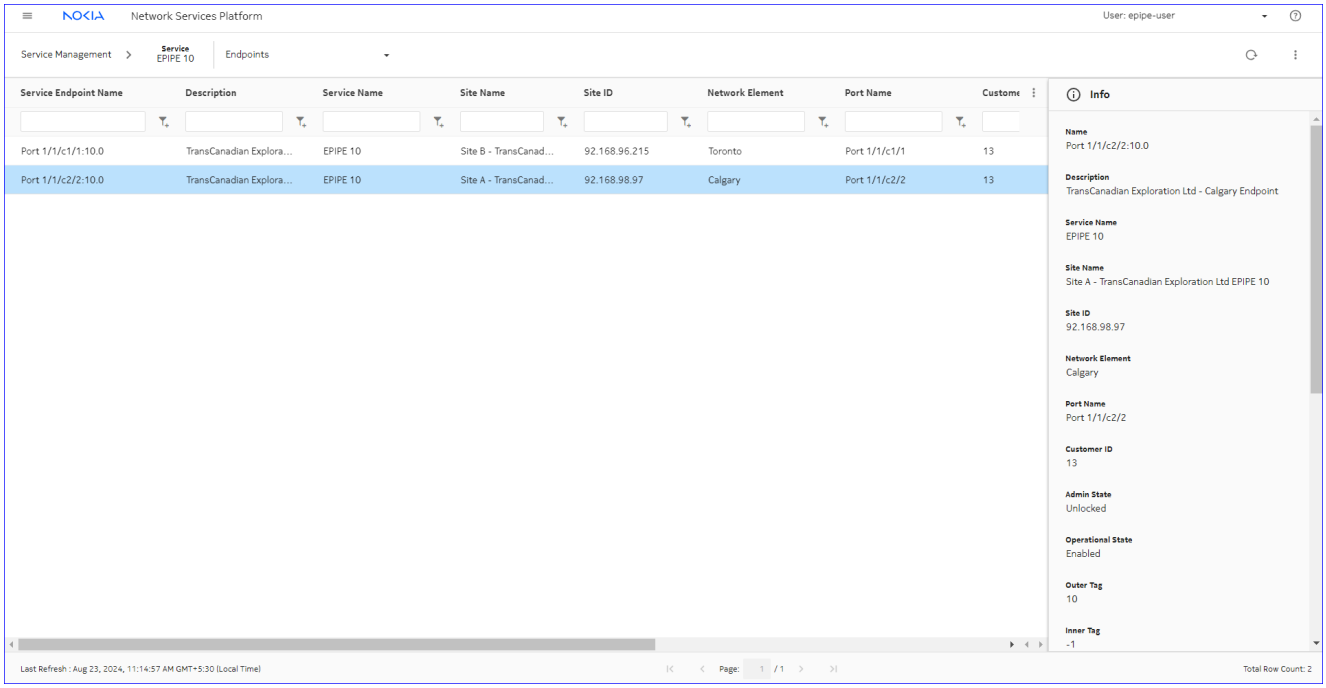
5

Login to the site NE and ensure the service is modified accordingly.

```
A:Calgary# configure service epipe 10
A:Calgary>config>service>epipe# info
----------------------------------------------
            description "TransCanadian Exploration Ltd Site A - Calgary"
            service-mtu 9208
            sap 1/1/c2/2:10 create
                description "TransCanadian Exploration Ltd - Calgary Endpoint"
                collect-stats
                accounting-policy 20
                no shutdown
            exit
            spoke-sdp 11:10 create
                description "TransCanadian Exploration Ltd - Service Tunnel to Toronto"
                no shutdown
            exit
            no shutdown
----------------------------------------------
```

6

Click on the modified service and select **Service Details, Components** from the ⋮ (Table row actions) menu. Ensure they show the modifications correctly.



END OF STEPS

1.15 Delete a brownfield service

1.15.1 Purpose

Use the following procedure to remove a brownfield service from the network and then delete the service permanently.

1.15.2 Steps

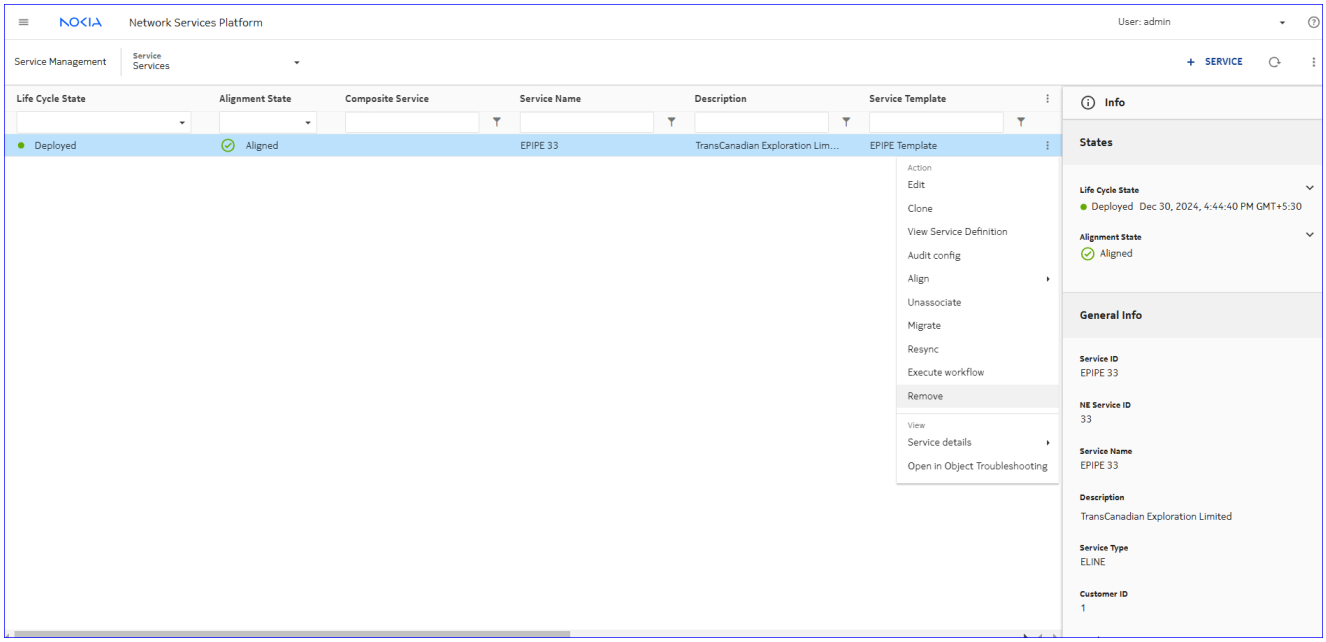
1

From the **Service Management**, **Services view**, select a service and click ⋮ (Table row actions), **Remove**.

The Remove Service From Network confirmation dialog opens.

2

Click **REMOVE** to remove the service from the network.



The Life Cycle State of the service is changed to Removed.

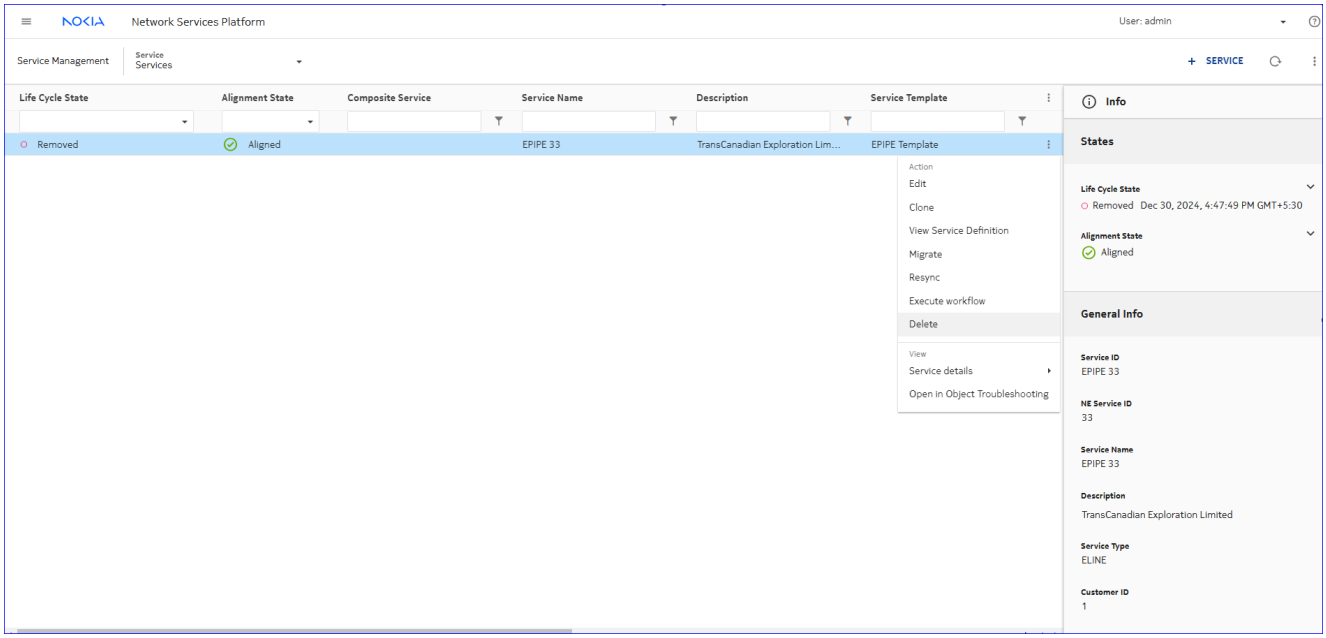
3

To delete the service permanently, proceed to the next step.

Note: If you prefer, you can leave the service in Removed state so that it can be deployed again later. To re-deploy the service to the network, select the service and click ⋮ (Table row actions), **DEPLOY**.

4

To delete the service, select the service and click ⋮ (Table row actions), **Delete**.



The Delete Service confirmation dialog opens.

Note: The Delete option only appears if the service is in Removed state.

5

Click DELETE to permanently delete the service from the NSP.

END OF STEPS

2 UCC-12: E-LINE/E-PIPE

2.1 Overview

2.1.1 Purpose

This chapter describes the process required to configure an Epipe service on SR OS NEs using NSP Service Management.

Configuration examples in this chapter show NSP Release 23.11 and SR OS 23.7.R2 NEs.

The following artifact bundles were used to test this use case:

- nsp-icm-intents-23.11.0-cam-bundle.zip
- nsp-svc-fulfillment-bundle-2311-v3.zip

See the NSP and NE documentation for more information.

2.1.2 Contents

Preparation

2.2 Prerequisites

2.2.1 Network configuration prerequisites

Before services can be configured and managed in NSP, the network configuration prerequisites must be met. The following table describes the requirements that can apply to service use cases, and indicates whether each prerequisite is required for this use case.

Where an NSP intent type is not available, CLI or MD-CLI must be used to perform configuration on the device.

Prerequisite	Documentation reference	Notes
Mandatory for E-LINE/E-PIPE		
GRPC configuration 1. Generate security certificates 2. Configure security and enable GRPC on all devices 3. Apply security certificates on all devices	See SR TLS information here in the SR OS 24.3 R1 documentation: TLS	—
Netconf/SNMP provisioning: enable NETCONF and SNMP protocols on all devices	For more information about SNMP and NETCONF with SR OS, see SNMP and NETCONF in the *SR OS 24.3 R1 System Management Guide*.	—
NSP installation	Pathway for NSP system installation in the *NSP Installation and Upgrade Guide* How do I enable TLS for telemetry and gNMI on_change support? in the *NSP System Administrator Guide*.	Include the following in your deployment: • Feature packs: - platform-baseServices - platform-pluggableNetworkAdaptation - platform-loggingMonitoring - serviceActivationAndConfiguration-intentBasedServiceFulfillment - networkInfrastructureManagement-basicManagement - networkInfrastructureManagement-deviceConfig • Adaptor suites: - sros-common - sros-oc-logical-inventory - sros-23-7-r1

Prerequisite	Documentation reference	Notes
Download the required artifact bundles from the NSP software delivery site: • NSP predefined set for ICM (device configuration) • NSP product artifact bundle for Service Fulfillment	How do I install an artifact bundle? in the *NSP Network Automation Guide*	—
Device discovery	Pathway for device discovery in the *NSP Classic Management User Guide* How do I discover devices? in the *NSP Device Management Guide* Nokia Developer Portal for information about FTP mediation policy creation using API.	—
Cards and MDAs provisioning	ICM process in the *NSP Device Management Guide* for more information about using the Device Configuration views, and the other procedures in the *NSP Device Management Guide* for further detail. See the NSP ICM Intent Type Catalog for information about this and other device configuration intent types developed by Nokia.	The intent type required for this configuration is icm-equipment-card-mda.
Connectors and Ports provisioning		The intent types required for this configuration are: • icm-equipment-port-connector • icm-equipment-port-ethernet
OSPF/ISIS	CLI Reference Guides for SR OS	—
LDPs, MPLS and RSVP configuration	CLI Reference Guides for SR OS	For LDP to be operational, the IPv4 and IPv6 bindings must be configured manually using CLI.
Interfaces Provisioning	How do I create a physical configuration deployment? in the *NSP Device Management Guide*.	The intent type required for this configuration is icm-router-network-interface
Customer creation	How do I create a logical configuration deployment? in the *NSP Device Management Guide*.	The intent type required for this configuration is icm-service-customer
Optional		

Prerequisite	Documentation reference	Notes
Optional items to include in your NSP deployment	Pathway for NSP system installation in the *NSP Installation and Upgrade Guide*	• Optional feature packs: - pathControlAndOptimization - multilayerDiscoveryAndVisualization - NSP Analytics: Network Operations Analytics feature package with the networkOperationsAnalytics-analyticsReporting installation option - NSP Baseline Analytics: networkOperationsAnalytics-baselineAnalytics - networkInfrastructureManagement-performanceIndicatorsAndAlerts • VSR/NRC • An AuxDB • An NFM-P instance
Telemetry/OAM	*NSP Data Collection and Analysis Guide*	• NSP SR OS vendor-agnostic telemetry adaptation artifact bundle • networkInfrastructureManagement-gnmiTelemetry feature pack
BGP/EVPN	How do I create a logical configuration deployment? in the *NSP Device Management Guide*.	The intent type required for this configuration is icm-router-bgp_group
Segment Routing	CLI Reference Guides for SR OS	—
Scheduler QoS Policies	How do I create a logical configuration deployment? in the *NSP Device Management Guide*.	The intent types required for this configuration are: • icm-qos-schedulerpolicy-srqos • icm-qos-network-srqos • icm-qos-sapingress-srqos • icm-qos-sapegress-srqos
Network QoS Policies configuration		
SAP QoS Policies configuration		
PCEP configuration	CLI Reference Guides for VSR-NRC	Most of the connections required for PCEP are established during previous configuration steps.
LAGs and MC-LAG creation	How do I create a logical configuration deployment? in the *NSP Device Management Guide*.	The intent types required for this configuration are: • icm-logical-lag-access • icm-logical-mc_lag-access

2.3 Optional: create a restricted Service Management user

2.3.1 Purpose

Perform this optional procedure to create a user with access only to specified NSP functions.

Procedures in this chapter can be performed by the restricted user, or by an administrator.

This procedure is based on the procedures for the following in the *NSP System Administrator Guide*:

- Configuring a role
- Configuring a user group
- Creating an NSP local user
- Enabling User Access Control
- Configuring user access to an intent type

For example, the reference procedures in NSP Release 23.11 are:

- How do I configure a role?
- How do I configure a user group?
- How do I create an NSP local user?
- How do I enable User Access Control?
- How do I configure user access to an intent type?

If a restricted user has already been created, verify that the user has the required permissions, as shown in Step 6.

2.3.2 Steps

Create a role

1

Log in to the NSP as an administrator.

2

Open **Users and Security**.

3

Select **Roles** from the drop-down list on the toolbar.

4

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

5

In the Identification panel, specify a role name and description.

The Role Name and Description fields can employ **only** the following special characters: `@ - _`.

The Role Name string must not contain *any* spaces, including a leading or trailing space.

6

To assign NSP functional access to the role, go to the Action Permissions panel and select an access level from the drop-down list for each NSP GUI you want to include in the role.

Action permissions group item	Permissions	Notes
Service Fulfillment	Read / Write / Execute	—
Network Intents	Read: Manage Intents	Required to import intent types into Service Management
Workflows	Read	Required to create service and tunnel templates
Optional: DCA Management	Read / Write / Execute	Only required for creating and plotting telemetry subscriptions
Optional: OAM Tests	Read / Write / Execute	Only required for generating and executing OAM tests

7

To assign network resource access to the role, go to the Resource Groups Access panel. (For a detailed explanation of the Resource Groups Access panel, see How do I set network resource access levels? in the *NSP System Administrator Guide*.)

You can assign resource group access globally, to resource group categories, to individual resource groups, or a combination of these. For service management it is recommended to grant access to all equipment and all services:

- **Access To All Equipment** assigns full permissions on all NE resource groups and port resource groups to the role.
- **Access To All Services** assigns full permissions on all service resource groups to the role.

8

Click **Create** to save your changes and return to the Roles list.

Create a user group

9

Open **Users and Security**.

10

Select **User Groups** from the drop-down list on the toolbar.

11

Click **+ Create User Group**. The Create User Group form opens.

12

Specify a group name and description in the **Identification** panel.

The user group name you specify here must exactly match a corresponding user group name returned by your user repository.

The User Group Name and Description fields can employ **only** the following special characters: `@ - _`.

The User Group Name string must not contain *any* spaces, including a leading or trailing space.

13

To assign user roles to the group, click **+ Add Roles** on the Roles panel. The Add Roles form opens.

14

Enable the check box for each role you want to assign to the group and click **Done**. The roles are added to the Selected Roles list.

To remove a role item from the Selected Roles list, click **Delete** on the item.

15

Click **Create** to save your changes and return to the User Groups list.

Create a user

16

Open **Users and Security**.

17

Select **Users** from the drop-down list on the toolbar.

18

Click **+ Create User**.

19

In the Create User form, specify user identification information for the account in the Identification section. The **Username** and **User Group** fields are mandatory.

Note: Any uppercase characters in the username are saved as lowercase.

The **Username** value:

- can be 1 to 40 characters long
- cannot include a space
- cannot have a leading or trailing space
- can include only the following special characters:
  - **@** (at sign)
  - **-** (hyphen)
  - **_** (underscore)
  - **.** (period)

20

In the Password section, specify and confirm a password for the user account.

- If you want this password to be temporary, enable the **Force User to Change Password** option. The new user will be forced to change their password when they first login to NSP.
- Enable the **Show Password** option to see the password characters as you type them.
- Click on the **Password Requirements** link to view a list of minimum security requirements for the password.

21

Click **Create**.

Enable user access control

22

Open **Users and Security**, **User Groups**.

23

Click ⋮ **More Actions**, **Settings**.

24

In the Access Control Settings form, enable the **NSP User Access Control** option.

25

Click **SAVE** to enable access control.

END OF STEPS

2.4 Install the required artifact bundles

2.4.1 Purpose

Use this procedure to make the required intent types available to Service Management in NSP. This procedure is based on the procedure for installing an artifact bundle in the *NSP Network Automation Guide*.

For example, the reference procedure in NSP 23.11 is How do I install an artifact bundle?.

2.4.2 Steps

Download the required intent types

1

Download the Service Fulfillment artifact bundle from the NSP software delivery site.

Navigate through the hierarchy to the folder of artifacts that can be imported using the Artifacts views, for example: NSP → 23.11 → Artifacts → Artifact_Admin_Import.

See the description to verify which bundle to download.

Install the artifact bundle in NSP

2

Log in to the NSP as the Service Management user.

3

Open **Artifacts**, **Artifact Bundles**.

4

Click **IMPORT & INSTALL**.

5

In the form that opens, drag and drop the zip file, or click **Browse** and navigate to the files on your system.

6

To install the artifact bundle immediately, click **IMPORT & INSTALL**. To import without installing, click **IMPORT**.

The chosen operation is triggered immediately. The artifact bundle status is updated to Imported or Installed when NSP has confirmed the status of all artifacts in the artifact bundle.

7

To install a bundle in Imported status, choose **Install bundle** from the ⋮ (Table row actions) menu.

END OF STEPS

2.5 Configure user access to the required intent types

2.5.1 Purpose

Use this procedure to provide the user access to intent types. If the restricted Service Management user will be performing configuration tasks, this procedure must be performed.

This procedure is based on the procedure for configuring user access to an intent type in the *NSP Network Automation Guide*.

For example, the reference procedure in NSP Release 23.11 is How do I configure user access to an intent type?.

2.5.2 Steps

1

Log in to the NSP as an administrator.

2

Open **Network Intents**, **Intent Types**.

3

Select the `tunnel` and `epipe` intent types.

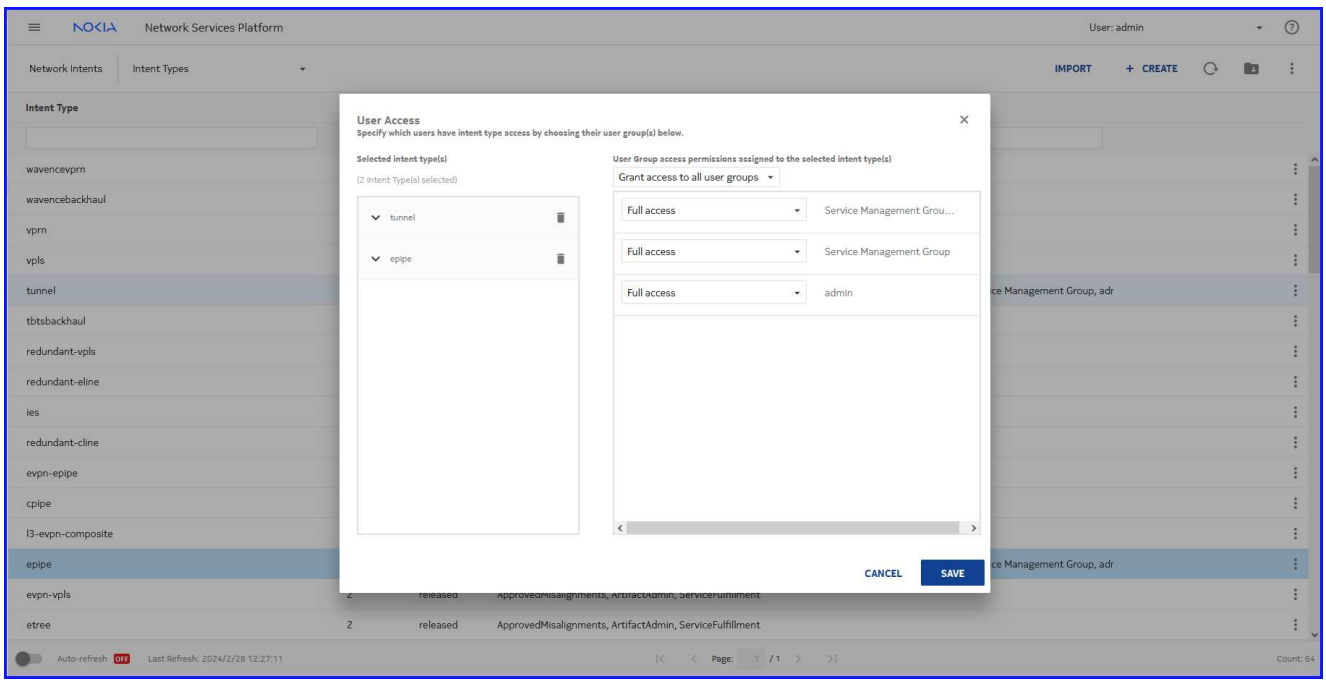
4

Click ⋮ (Table row actions), **User Access** to open the User Access form.

5

In the **User Access** form, choose **Grant access to all user groups** from the drop-down list at the top right of the form.

Choose **Full access** for the user group created in “Create a user group” (p. 54).



6

Click **SAVE**. The user access is updated.

END OF STEPS

Service Configuration

2.6 Import intent types into Service Management

2.6.1 Purpose

Use this procedure to import the intent types you obtained in 6.4 “Install the required artifact bundles” (p. 218) to the Service Management views. This procedure is based on the procedure for importing an intent type into Service Management in the *NSP Service Management Guide*.

For example, the reference procedure in NSP Release 23.11 is How do I import an intent type into Service Management?.

Note: This procedure is not required in NSP 25.4 or later because intent types for Service Management will import directly into Service Management during artifact bundle installation.

The intent types required are `tunnel` and `epipe`.

2.6.2 Steps

1

Log in to the NSP as the Service Management user.

2

From the **Service Management, Intent Type Catalogue** view, click **IMPORT**.

A list of previously-defined intent types is displayed.

Note: Only intent types that have the Service Fulfillment label applied will be available to import. Intent types to be used for tunnel template creation must also have the Tunnel label applied.

Note: For a restricted user to be allowed to import intent types, they must have appropriate permissions configured for those intent types in Network Intents; see How do I configure user access to an intent type? in the *NSP Network Automation Guide*.

3

Select the check boxes in-line with the intent types you wish to import and click **IMPORT**.

The intent types to import are:

- tunnel
- epipe

The intent types are imported into service management. This may take a few minutes.

Note: Selecting an imported intent type from the list opens the Info panel, which displays historical information such as the last time the intent type was updated, the last time it was imported, and the last time the modules that compose the intent type were revised.

END OF STEPS

2.7 Create a service tunnel template

2.7.1 Purpose

Perform this procedure to create the template that Service Management will use in the creation of a service tunnel.

This procedure is based on the procedure to create a tunnel template in the *NSP Service Management Guide*.

For example, the reference procedure in NSP 23.11 is How do I create a tunnel template?.

2.7.2 Steps

1

Log in to the NSP as the Service Management user.

2

From the **Service Management, Tunnel Templates** view, click **+ CREATE**.

The Create a tunnel template form opens.

3

Configure the parameters, as required.

Parameter	Description
Template Name	Specifies the name of the template
Description	Describes the template
Tunnel Intent Type	`tunnel`
Intent Version	Specifies which version of the selected tunnel intent type to associated with the template
State	Released
Config Form	Specifies the form to be used for the template

4

If required, click **+ ADD** in the Workflows panel to add workflows to the tunnel template.

The Add Workflows form opens.

5

Configure the parameters, as required:

Parameter	Description
Workflow Name	Specifies the workflow to be executed
Service Life Cycle State	Specifies the life cycle state of the tunnel that will trigger workflow execution
Service Life Cycle Case	Specifies the case, Success or Fail, relative to the life cycle state that will trigger workflow execution
Blocking	Specifies whether unsuccessful execution of the workflow will prevent tunnel life cycle state changes
Workflow Execution Timeout (seconds)	Specifies the length of time, in seconds, that unsuccessful execution of the workflow will prevent tunnel life cycle state changes

6

Click **ADD**.

The Add Workflows form closes and the workflow is added to the tunnel template.

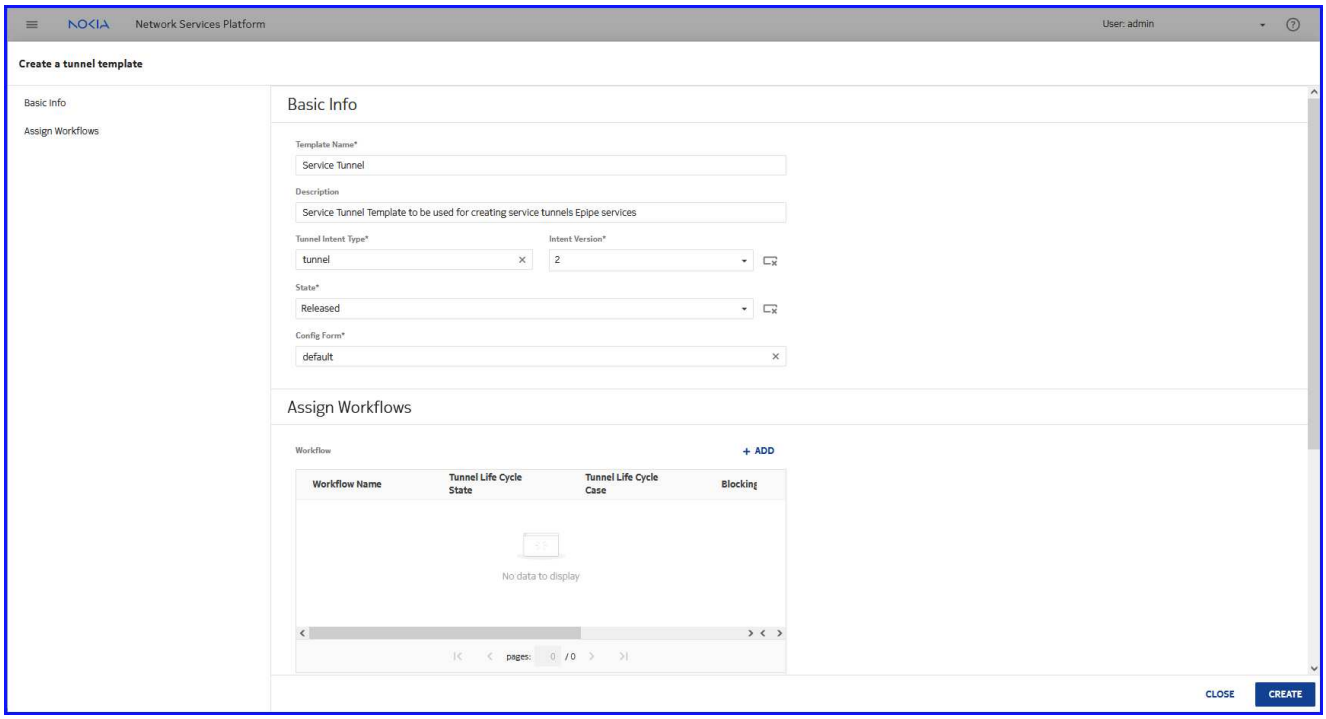
7

Click **CREATE**.

The tunnel template is created.

END OF STEPS

2.7.3 Example creation form without a workflow



2.8 Create and deploy service tunnels to the network

2.8.1 Purpose

Perform this procedure to create service tunnels. The creation of service tunnels is a prerequisite to creation of a service.

This procedure is based on the procedures for creating and auditing a service tunnel in the *NSP Service Management Guide*.

For example, the reference procedures in NSP Release 23.11 are:

- How do I create a service tunnel?
- How do I audit a service tunnel?

2.8.2 Steps

1

Log in to the NSP as the Service Management user.

2

Open the tunnel creation form:

1. From the **Service Management, Service Tunnels** view, click **+ CREATE**.

   The Select a tunnel template to start form opens displaying a list of tunnel templates.
2. Choose the template you created in 2.7 “Create a service tunnel template” (p. 61).

   The Create Tunnel form opens with the Template Name parameter populated.

3

Configure the parameters, as required.

4

If the Transport Type parameter was set to MPLS, configure the required parameters.

5

Configure the required Hello parameters.

6

If the Transport Type parameter was set to GRE, configure the Allow Fragmentation parameter (if required), which specifies whether or not fragmentation will be allowed for the tunnel.

7

Configure the required parameters.

8

Click **DEPLOY** to create the tunnel in a Deployed state.

9

Perform an audit to verify that the tunnel is deployed correctly:

1. From the **Service Management, Service Tunnels** view, click on the service tunnel in the list, then expand the Alignment State section in the info panel and click **AUDIT CONFIG**.

   The service tunnel is audited.
2. If an Audit Result form appears, one or more attributes and/or objects are misaligned. Review the results and click **OK**.

   The Audit Result form closes.

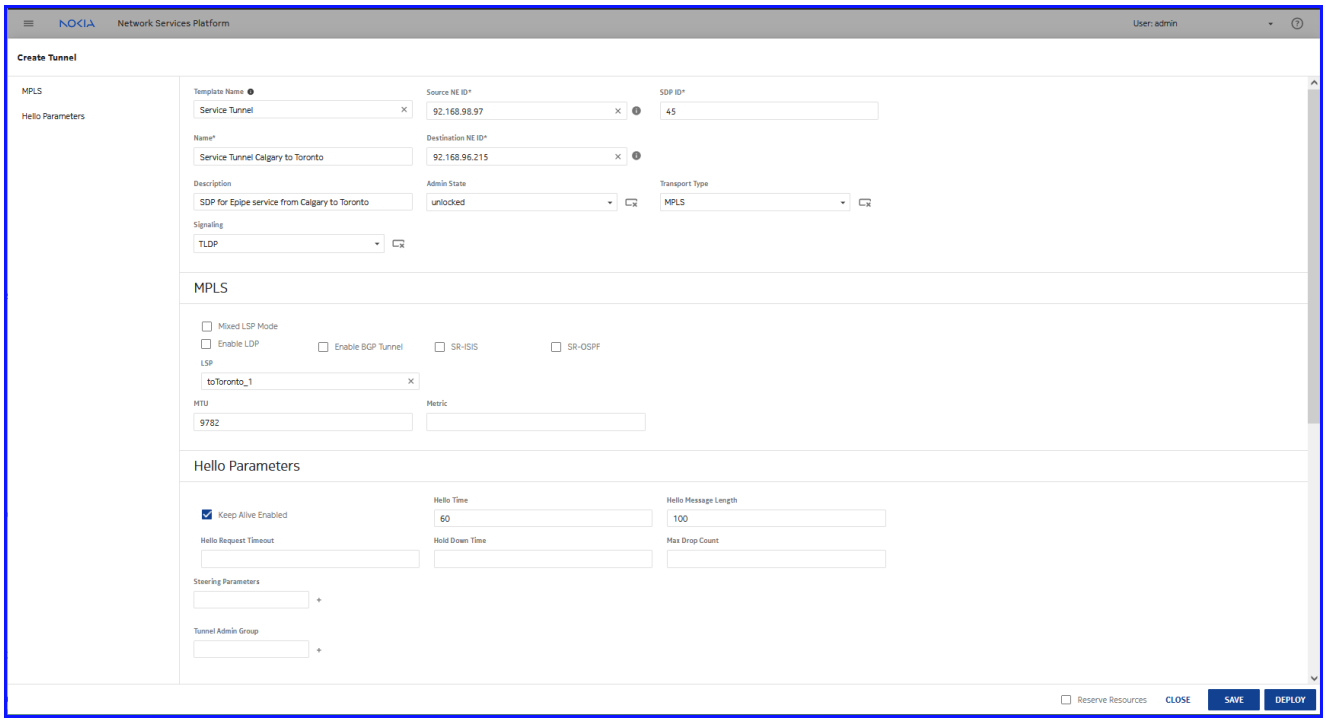
10

To revert to the expected value of a misaligned attribute, or to restore a misaligned object, click ⋮ (Table row actions), **Align**, **Push To Network** in-line with the previously audited service tunnel.

The service tunnel is synchronized with the network.

END OF STEPS

2.8.3 Tunnel creation example



2.9 Create an EPIPE service template

2.9.1 Purpose

This procedure is based on the procedure to create a service template in the *NSP Service Management Guide*.

For example, the reference procedure in NSP 23.11 is How do I create a service template?.

2.9.2 Steps

1

Log in to the NSP as the Service Management user.

2

From the **Service Management, Service Templates** view, click **+ CREATE**.

The Create a service template form opens.

3

Configure the parameters, as required.

Parameter	Description
Template Name	Specifies the name of the template
Description	Describes the template
Service Intent Type	`epipe`
Intent Version	Specifies which version of the selected service intent type to associated with the template
State	Released
Config Form	Specifies the interface to be used with the template

4

If required, click **+ ADD** in the Workflows panel to add workflows to the service template.

The Add Workflows form opens.

5

Configure the parameters, as required:

Parameter	Description
Workflow Name	Specifies the workflow to be executed
Service Life Cycle State	Specifies the life cycle state of the service that will trigger workflow execution
Service Life Cycle Case	Specifies the case, Success or Fail, relative to the life cycle state that will trigger workflow execution
Blocking	Specifies whether unsuccessful execution of the workflow will prevent service life cycle state changes
Workflow Execution Timeout (seconds)	Specifies the length of time, in seconds, that unsuccessful execution of the workflow will prevent service life cycle state changes

6

Click **ADD**.

The Add Workflows form closes and the workflow is added to the service template.

7

If required, select a Default Service Category in the Bulk Association panel to specify a service type to which this service template can be applied in bulk.

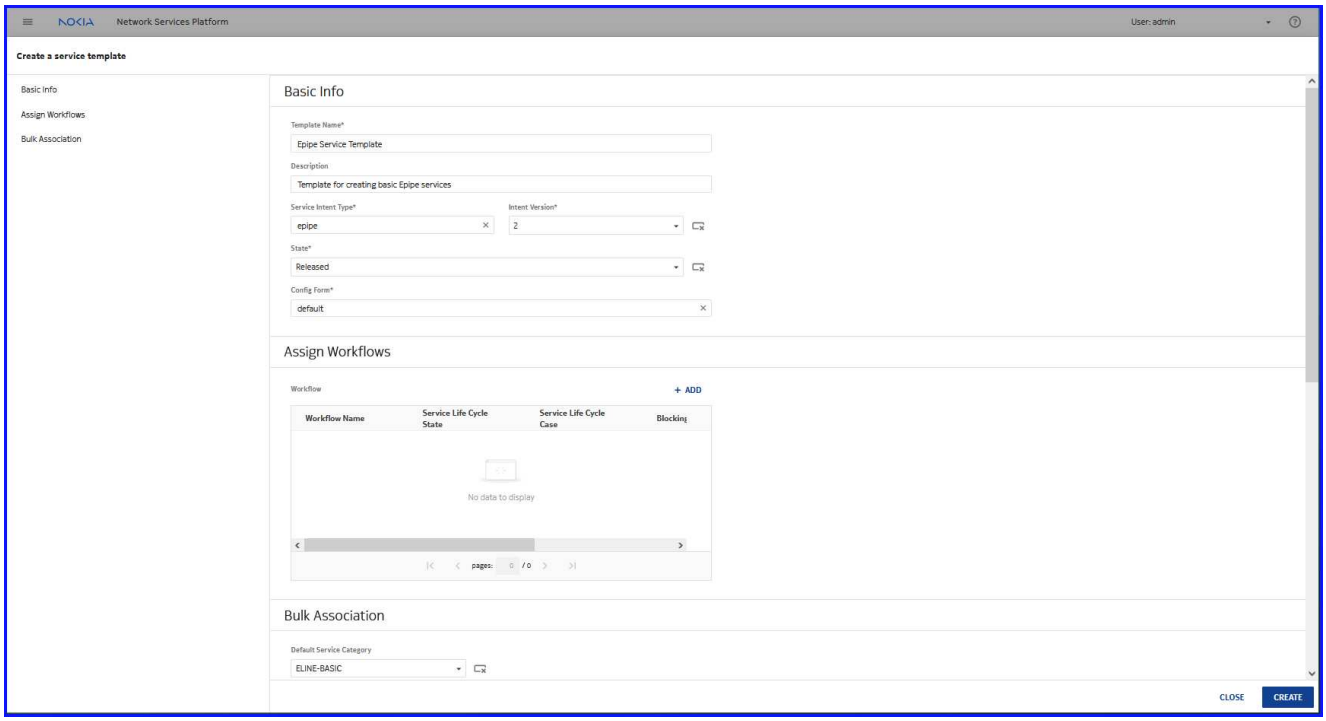
8

Click **CREATE**.

The service template is created.

END OF STEPS

2.9.3 Example creation form without a workflow



2.10 Create and deploy an EPIPE service to the network

2.10.1 Purpose

Perform this procedure to create the service.

This procedure is based on the procedures for creating and auditing a service in the *NSP Service Management Guide*.

For example, the reference procedures in NSP Release 23.11 are:

- How do I create an E-Line service?
- How do I audit a service?

2.10.2 Steps

1

Log in to the NSP as the Service Management user.

2

From the **Service Management, Services** view, click **+ CREATE**.

The Select a service template to start form opens displaying a list of service templates.

3

Click on an E-Line service template from the list.

The Create Service form opens with the Template Name parameter populated.

4

Configure the parameters, as required.

Continue to the Site A panel.

5

Configure the required parameters:

Note: If site names and descriptions are added, these will take precedence over any service name and description specified in Step 4, with the Site A name and description taking precedence over Site B. As such, these attributes will be displayed in various locations, such as NSP's Model Driven Configurator function and NFM-P.

6

Click **+ ADD**.

The Add Endpoint form opens.

7

Configure the parameters, as required.

8

Perform the following to specify an accounting policy to be used:

1. Click on the Accounting Policy field. The Select Accounting Policy form opens.
2. Click on an accounting policy in the list, then click **SELECT**. The Select Accounting Policy form closes.

9

Configure the parameters in the Cpu Protection panel, as required.

10

If QoS was enabled in Step 9, configure the parameters as required in both the ingress and egress panels:

11

If an IP/IPv6 filter was enabled in Step 9, configure the parameters as required in both the ingress and egress panels:

Click **ADD** to add the endpoint.

The Add Endpoint form closes.

12

In the Site B panel, repeat Step 5 to Step 11.

13

In the SDP Details panel, click + **ADD**.

The Add SDP form opens.

14

Configure the parameters, as required:

Click **ADD** to add the SDP binding.

The Add SDP form closes.

15

Click **DEPLOY** to create the service in a Deployed state.

16

Perform an audit to verify that the service is deployed correctly:

1. From the **Service Management, Services** view, click ⋮ (Table row actions), **Audit config** in-line with any service.

   The service is audited.

2. If an Audit Result form appears, one or more attributes and/or objects are misaligned. Review the results and click **OK**.

   The Audit Result form closes.

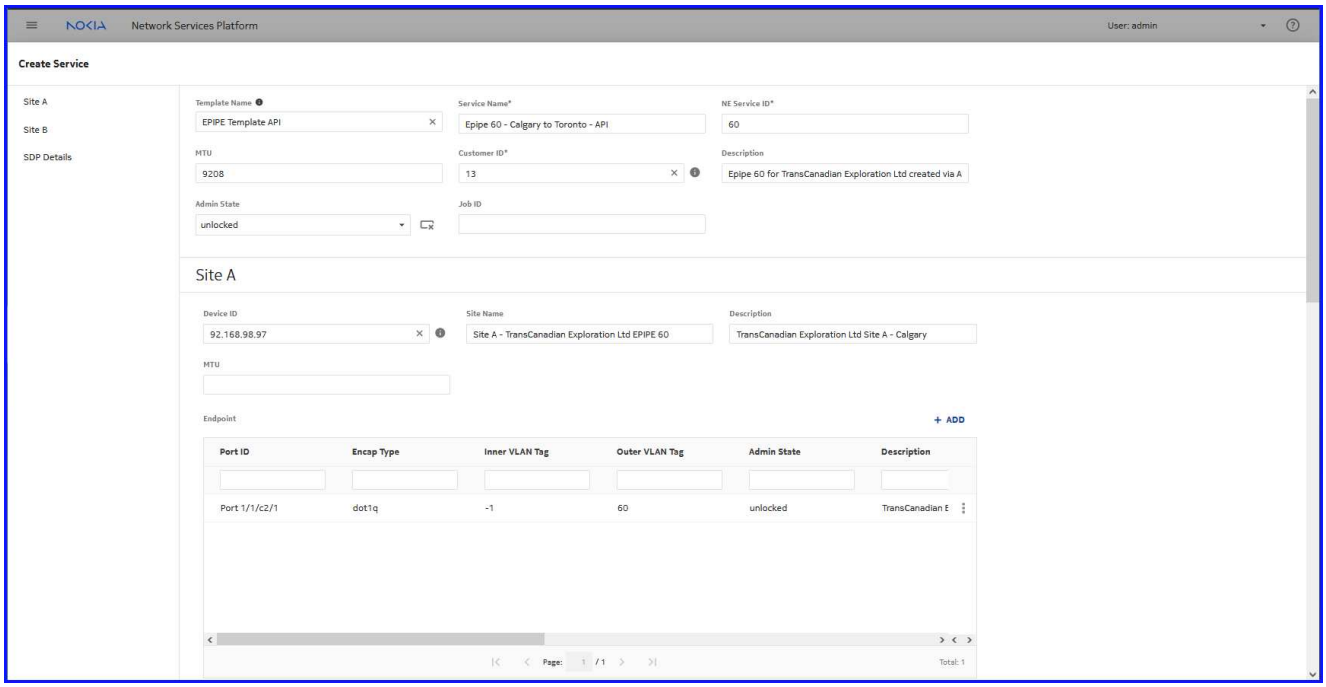
17

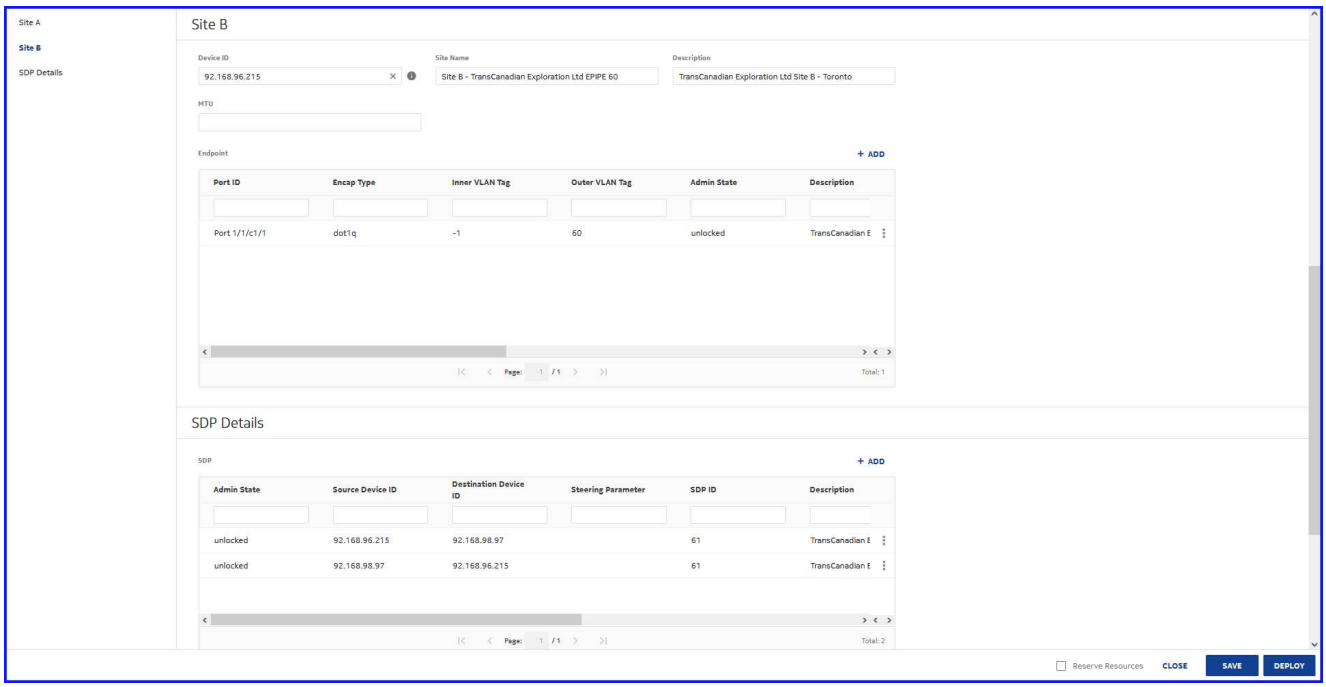
Click ⋮ (Table row actions), **Align**, and then either **Push to network** or **Pull from network** in-line with the previously audited service.

The service is synchronized with the network.

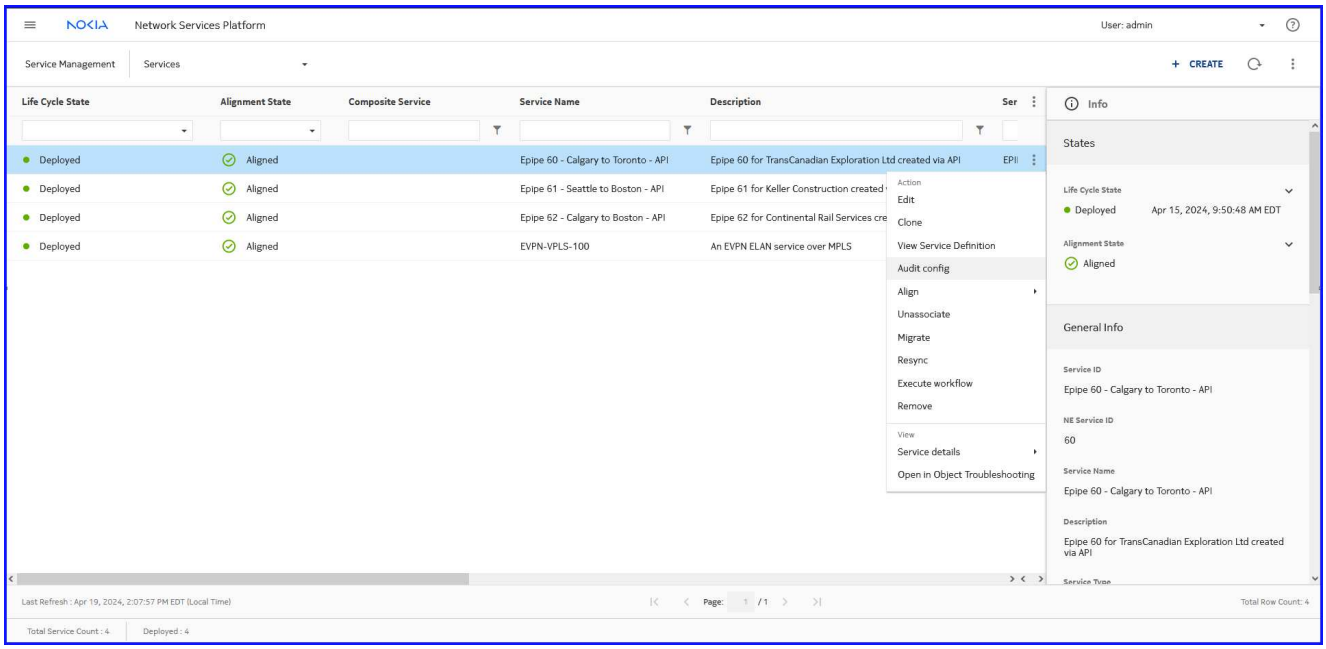
END OF STEPS

2.10.3 Example of a configured service





2.10.4 Services Table row actions menu showing audit and align



2.11 Modify or delete an EPIPE service

2.11.1 Purpose

Use this procedure if needed to modify configured parameters for an Epipe service, or to remove a service from the network and delete it.

2.11.2 Steps

Edit a service

1

Log in to the NSP as the Service Management user.

2

From the Service Management, Services view, select a service and choose **Edit** from the ⋮ (Table row actions) menu.

3

Modify the service, site, endpoint or SDP parameters as required.

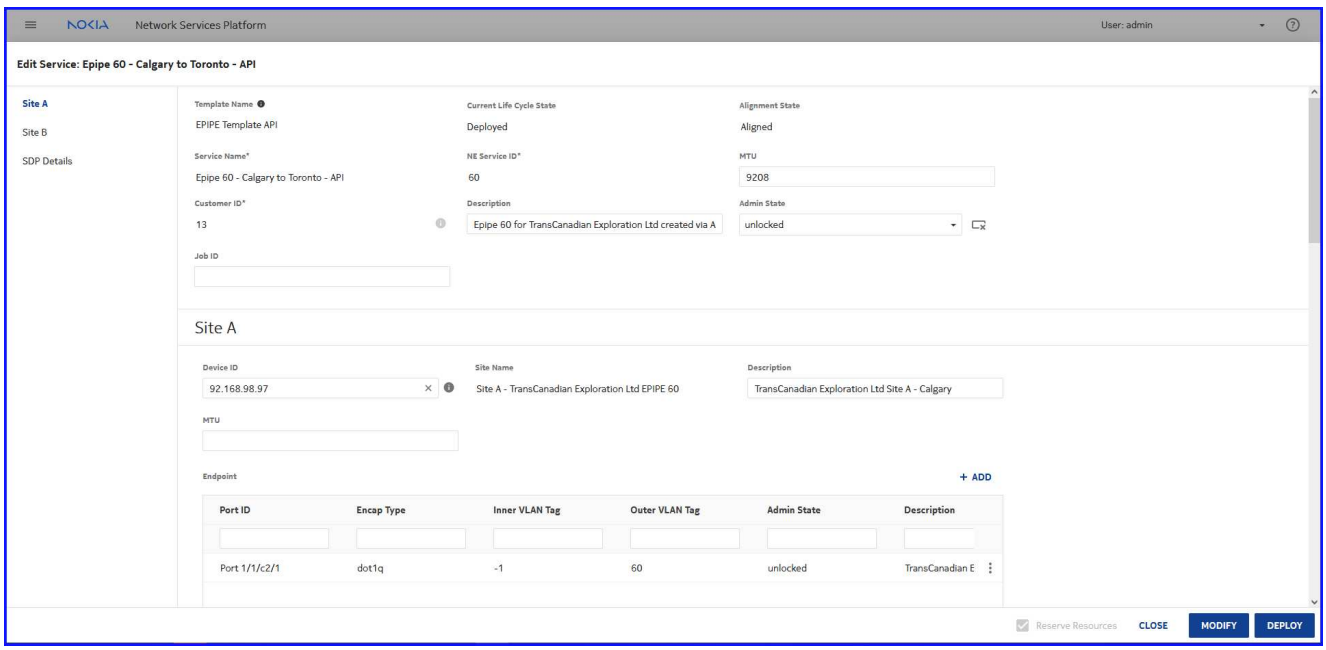
4

Perform one of the following:

a. Select the Reserve Resources check box and click **PLAN** to create the service in a Planned state.

b. Click **SAVE** to create the service in a Saved state.

c. Click **DEPLOY** to create the service in a Deployed state.



Delete a service

5

From the **Service Management**, **Services view**, select a service and click ⋮ (Table row actions), **Remove**.

The Remove Service From Network confirmation dialog opens.

6

Click **REMOVE** to remove the service from the network.

The Life Cycle State of the service is changed to Removed.

7

If you prefer, you can leave the service in Removed state so that it can be deployed again later. To delete the service permanently, proceed to the next step.

8

To delete the service, select the service and click ⋮ (Table row actions), **Delete**.

The Delete Service confirmation dialog opens.

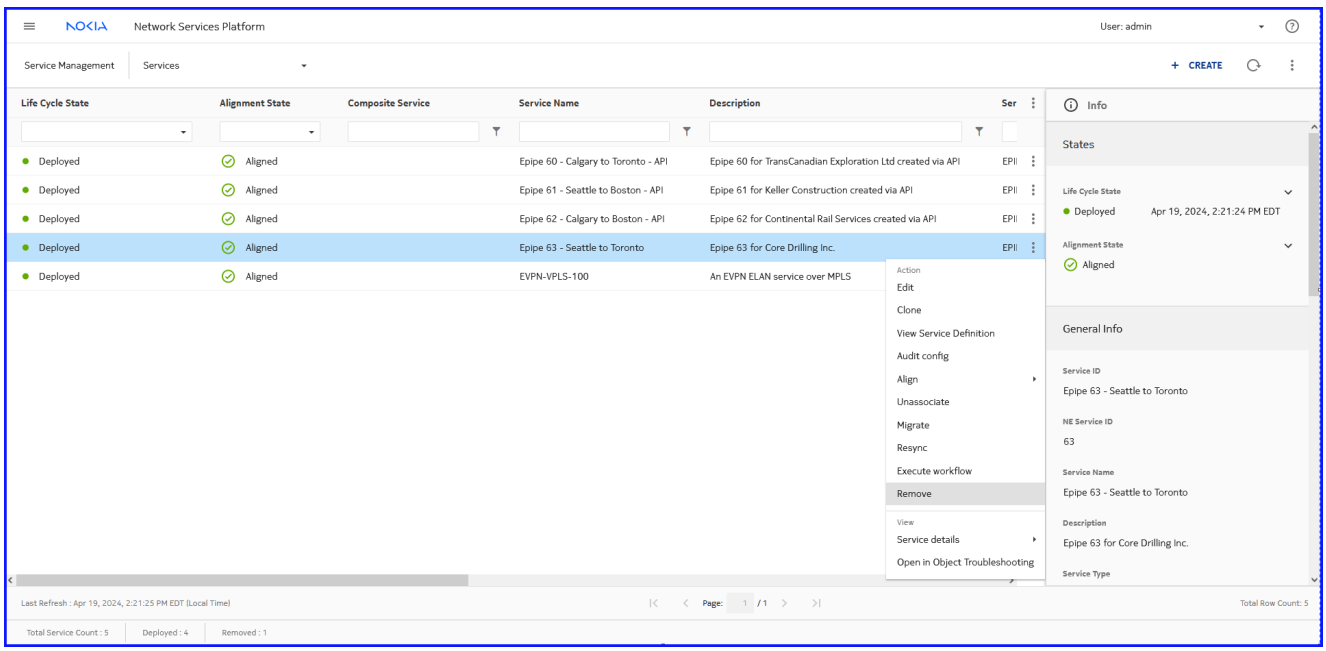
Note: The Delete option only appears if the service is in Removed state.

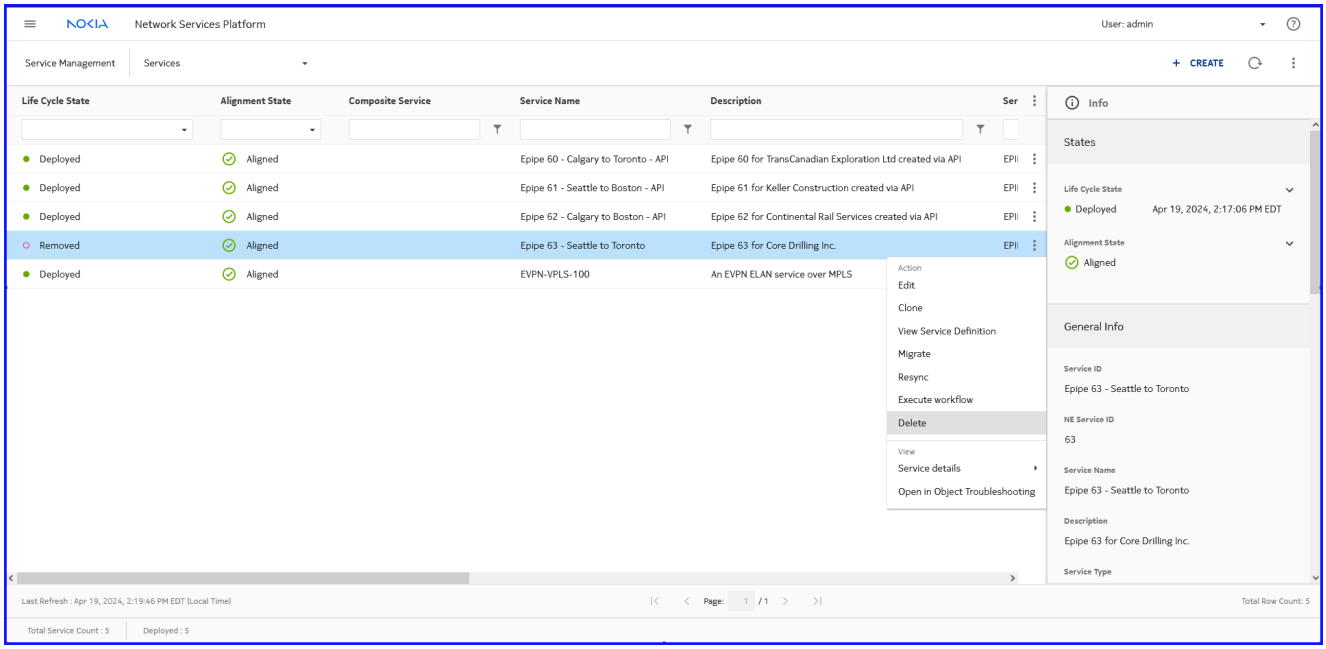
9

Click DELETE to permanently delete the service from the NSP.

END OF STEPS

2.11.3 Examples showing remove and delete





Optional procedures

2.12 Generate and execute OAM test suites

2.12.1 Purpose

Use one of the procedures in this section to generate and execute an OAM test suite against objects of a service. The procedures are based on the procedures for the following:

- Configuring an OAM test suite for a service, in the *NSP Network and Service Assurance Guide*
- Creating an OAM test suite, in the *NSP Data Collection and Analysis Guide*

For example, the reference procedures in NSP Release 23.11 are:

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

2.12.2 Steps

Create an OAM test suite from the Object Troubleshooting dashboard

1

Log in to the NSP as the Service Management user.

2

Open Object Troubleshooting and select a service to test.

3

Click **Create OAM Test Suite**.

The Select *Service Type* Endpoints form opens.

4

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

5

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

6

Generate the test suite.

a. To automatically execute the test suite after generation, enable Execute and click **GENERATE & EXECUTE**.

b. To create the test suite without automatically executing, disable Execute and click **GENERATE**.

Create an OAM test suite from Data Collection and Analysis Management

7

Open **Data Collection and Analysis Management**, **Test Suites**.

8

Click **+ SUITE**.

9

In the Generate OAM Tests form that opens, choose a Test type.

The list of templates in the Template field is updated based on your selection.

10

Choose a test template if needed.

If a template is not selected, an appropriate system template is automatically selected based on the value of the execute type field. If a template is selected, the value of the execute type field is imported from the template and is read-only in the form.

11

Add one or more entities:

1. Choose an entity type from the Entity type drop down.
2. Click **+ SELECT** to open a selection form.
3. Choose one or more entity objects from the list to add them to the Bin. Use the page selectors to navigate the list.
4. Verify the list of entity objects in the Bin and click **SELECT**.
5. To change the list of selected entities, repeat the previous steps to re-create the list.

12

Click on the Service field if applicable.

1. Select an attribute in the drop-down list, then enter values for that attribute in the field. As you type, the list is filtered for entities that match your input.
2. Click as required to add additional filter criteria.
3. Choose entities from the list and click **SELECT**.

13

Configure the test parameters as needed.

14

Generate the test suite.

a. To automatically execute the test suite after generation, enable Execute and click **GENERATE & EXECUTE**.

b. To create the test suite without automatically executing, disable Execute and click **GENERATE**.

END OF STEPS

2.13 Create telemetry subscriptions

2.13.1 Purpose

Perform this procedure to set up telemetry collection.

The bundle of vendor agnostic custom resources must be imported and installed to support telemetry collection. The bundle is found on the NSP software delivery site, in the Adaptors folder along with your NE adaptor suite, for example, NSP → 23.11 → Adaptors → Nokia_SROS. Choose the zip file with va and cr in the filename, for example, `nsp-telemetry-cr-va-sros-1.0.0-rel.10.zip`.

This procedure is based on the procedure for managing subscriptions in the *NSP Data Collection and Analysis Guide*.

For example, the reference procedure in NSP 23.11 is How do I manage subscriptions?.

See also the procedure to install telemetry artifacts in the *NSP Data Collection and Analysis Guide* to verify that telemetry prerequisites are in place. The reference procedure for this is in NSP 24.4: How do I install telemetry artifacts?.

CAUTION

Service Disruption

The name of an object, including subscriptions, baselines, indicators, templates, and chart profiles, cannot contain a semicolon (;) or backslash (\).

The use of these characters in an object identifier will result in corrupted data that must be deleted by Nokia support.

2.13.2 Steps

1

Log in to the NSP as the Service Management user.

2

Open **Data Collection and Analysis Management**, **Subscriptions**.

3

To create a subscription:

1. Click + **SUBSCRIPTION**.

2. In the Create Subscription form that opens, configure the General parameters as needed.
   - Enable database (DB) subscriptions as needed to save subscription information to the NSP database. For subscription data to be available to Analytics, the auxiliary database must be deployed.
   - The subscription is enabled by default: it will start running immediately.

     Choose **Disabled** in the **State** field if you want to enable your subscription later.
3. In the **Object Filter** field, enter filtering information as needed to filter the collected data.

   As you type, the field provides suggestions for available filters to match your input and identifies incorrect syntax.
4. Enter information in the Telemetry Type field. As you type, the field filters for available telemetry types to match your input.

   Choose the telemetry type you need from the list of matches.
5. When you enter a telemetry type, all counters are enabled by default.

   To customize the counters, enable the **Enable notifications and notification counters** check box.

   Click **Remove** to remove a counter.

   Click **+ COUNTERS** to add a counter that was removed.
6. Click **CREATE**.

   The subscription begins collection when it is enabled.

END OF STEPS

2.14 Create a telemetry chart and plot statistics

2.14.1 Purpose

Use this procedure to chart historical telemetry data. This procedure is based on the procedure for plotting a telemetry chart in the *NSP Data Collection and Analysis Guide*.

For example, the reference procedure in NSP 23.11 is How do I plot a telemetry chart?.

CAUTION

Service Disruption

The name of an object, including subscriptions, baselines, indicators, templates, and chart profiles, cannot contain a semicolon (;) or backslash (\).

The use of these characters in an object identifier will result in corrupted data that must be deleted by Nokia support.

2.14.2 Before you begin

When you create a telemetry chart, you configure a telemetry filter. For historical data to be displayed, the data must be available in the database; see 2.13 “Create telemetry subscriptions” (p. 77).

Charts are created by streaming to the plotter: historical data is queried and streamed to the plotter, then real time telemetry subscriptions are created and the data from these subscriptions is streamed to the plotter.

Data Collection and Analysis Visualizations times out if telemetry data is not received. The time-out limit is either double the collection interval or two minutes, whichever is greater.

2.14.3 Steps

Create a chart

1

Log in to the NSP as the Service Management user.

2

Open the New Chart window:

- From **Data Collection and Analysis Visualizations**, **Telemetry Charts**, click **+ CHART**.
- From **Data Collection and Analysis Management**, **Subscriptions**, choose a subscription and click ⋮ (Table row actions), **Open in Data Collection and Analysis Visualizations**.

3

In the window that opens, configure the parameters in the top panel:

1. Configure the **Collection Interval** parameter. If you are using NFM-P telemetry data, verify that the collection interval is long enough to allow time for Visualizations to receive the data before timing out.
2. From the **Time Range** drop-down list, choose the amount of historical data to display.
3. Click **Combine charts** to plot data from multiple data series on the same chart.

4

Click **+ DEFINITION**.

The telemetry and resource filter definition panels are displayed.

5

Enter information in the **Telemetry Type** field. As you type, the field filters for available telemetry types to match your input.

Choose the telemetry type from the list of matches.

6

Choose counters to display from the **Counters** drop-down list.

7

In the **Object Filter** field, enter filtering information to filter the collected data.

8

If you need to save the configuration as a chart:

1. Click **SAVE AS**.
2. In the window that opens, enter a name for the chart and add a description if needed.
3. Click **SAVE**.

The chart is added to the list.

9

Click **PLOT**.

END OF STEPS

2.14.4 Steps

Plot an existing chart

1

To plot an existing chart with no changes:

1. Open **Data Collection and Analysis Visualizations**, **Telemetry Charts**.
2. Choose a chart and click ⋮ (Table row actions), **Chart**.

2

To edit a chart and plot it, choose the chart and click ⋮ (Table row actions), **Edit**.

3

Edit the parameters as needed and click **PLOT**.

END OF STEPS

2.14.5 Result

Visualizations displays a chart view showing the streaming data. While data is streaming, you can configure the **Group by** parameter in the upper left of the chart view to change how the data is grouped or click **Configure** in the upper right to view or change the configuration of the chart.

Click ⓘ(Chart Details) to open the Chart Details panel on the right side of the chart view to show details about the resources.

3 UCC-13: C-LINE/C-PIPE

3.1 Overview

3.1.1 Purpose

This chapter describes the process required to configure a Cpipe service on SR OS NEs using NSP Service Management.

Configuration examples in this chapter show NSP Release 23.11 and SR OS (7750 SR-12) 20.10.R13 NEs.

The following artifact bundles were used to test this use case:

- nsp-icm-intents-23.11.0-cam-bundle.zip
- nsp-svc-fulfillment-bundle-2311-v3.zip

CPIPE/CLINE creation through NSP Service Management is supported on the following NE types:

- 7750 SR-12, version 21.2R1 or earlier, in classic mode
- 7705 SAR 8/18

See the NSP and NE documentation for more information.

3.1.2 Contents

Preparation

3.2 Prerequisites

3.2.1 Network configuration prerequisites

Before services can be configured and managed in NSP, the network configuration prerequisites must be met. The following table describes the requirements that can apply to service use cases, and indicates whether each prerequisite is required for this use case.

Where an NSP intent type is not available, CLI or MD-CLI must be used to perform configuration on the device.

Prerequisite	Documentation reference	Notes
Mandatory for C-LINE/C-PIPE		
GRPC configuration 1. Generate security certificates 2. Configure security and enable GRPC on all devices 3. Apply security certificates on all devices	See SR TLS information here in the SR OS 24.3 R1 documentation: TLS	—
Netconf/SNMP provisioning: enable NETCONF and SNMP protocols on all devices	For more information about SNMP and NETCONF with SR OS, see SNMP and NETCONF in the *SR OS 24.3 R1 System Management Guide*.	—
NSP installation	Pathway for NSP system installation in the *NSP Installation and Upgrade Guide* How do I enable TLS for telemetry and gNMI on_change support? in the *NSP System Administrator Guide*.	Include the following in your deployment: • Feature packs: - platform-baseServices - platform-pluggableNetworkAdaptation - platform-loggingMonitoring - serviceActivationAndConfiguration-intentBasedServiceFulfillment - networkInfrastructureManagement-basicManagement - networkInfrastructureManagement-deviceConfig • Adaptor suites: - sros-common - sros-oc-logical-inventory - sros-23-7-r1

Prerequisite	Documentation reference	Notes
Download the required artifact bundles from the NSP software delivery site: • NSP predefined set for ICM (device configuration) • NSP product artifact bundle for Service Fulfillment	How do I install an artifact bundle? in the *NSP Network Automation Guide*	—
Device discovery	Pathway for device discovery in the *NSP Classic Management User Guide* How do I discover devices? in the *NSP Device Management Guide* Nokia Developer Portal for information about FTP mediation policy creation using API.	—
Cards and MDAs provisioning	ICM process in the *NSP Device Management Guide* for more information about using the Device Configuration views, and the other procedures in the *NSP Device Management Guide* for further detail. See the NSP ICM Intent Type Catalog for information about this and other device configuration intent types developed by Nokia.	The intent type required for this configuration is icm-equipment-card-mda.
Connectors and Ports provisioning		The intent types required for this configuration are: • icm-equipment-port-connector • icm-equipment-port-ethernet
Channel configuration on access TDM ports	ICM process in the *NSP Device Management Guide* for more information about using the Device Configuration views, and the other procedures in the *NSP Device Management Guide* for further detail. See the NSP ICM Intent Type Catalog for information about this and other device configuration intent types developed by Nokia. CLI Reference Guides for SR OS	For 7705 SAR-8 and 7705 SAR-18 NEs, channels can be configured using Device Configuration in NSP. The intent type required for this configuration is icm-equipment-port-access-ce. For all other NE types, the configuration must be performed using CLI.
OSPF/ISIS	CLI Reference Guides for SR OS	—
LDPs, MPLS and RSVP configuration	CLI Reference Guides for SR OS	For LDP to be operational, the IPv4 and IPv6 bindings must be configured manually using CLI.
Interfaces Provisioning	How do I create a physical configuration deployment? in the *NSP Device Management Guide*.	The intent type required for this configuration is icm-router-network-interface
Customer creation	How do I create a logical configuration deployment? in the *NSP Device Management Guide*.	The intent type required for this configuration is icm-service-customer
Optional		

Prerequisite	Documentation reference	Notes
Optional items to include in your NSP deployment	Pathway for NSP system installation in the *NSP Installation and Upgrade Guide*	• Optional feature packs: - pathControlAndOptimization - multilayerDiscoveryAndVisualization - NSP Analytics: Network Operations Analytics feature package with the networkOperationsAnalytics-analyticsReporting installation option - NSP Baseline Analytics: networkOperationsAnalytics-baselineAnalytics - networkInfrastructureManagement-performanceIndicatorsAndAlerts • VSR/NRC • An AuxDB • An NFM-P instance
Telemetry/OAM	*NSP Data Collection and Analysis Guide*	• NSP SR OS vendor-agnostic telemetry adaptation artifact bundle • networkInfrastructureManagement-gnmiTelemetry feature pack
BGP/EVPN	How do I create a logical configuration deployment? in the *NSP Device Management Guide*.	The intent type required for this configuration is icm-router-bgp_group
Segment Routing	CLI Reference Guides for SR OS	—
Scheduler QoS Policies	How do I create a logical configuration deployment? in the *NSP Device Management Guide*.	The intent types required for this configuration are: • icm-qos-schedulerpolicy-srqos • icm-qos-network-srqos • icm-qos-sapingress-srqos • icm-qos-sapegress-srqos
Network QoS Policies configuration		
SAP QoS Policies configuration		
PCEP configuration	CLI Reference Guides for VSR-NRC	Most of the connections required for PCEP are established during previous configuration steps.
LAGs and MC-LAG creation	How do I create a logical configuration deployment? in the *NSP Device Management Guide*.	The intent types required for this configuration are: • icm-logical-lag-access • icm-logical-mc_lag-access

3.3 Optional: create a restricted Service Management user

3.3.1 Purpose

Perform this optional procedure to create a user with access only to specified NSP functions.

Procedures in this chapter can be performed by the restricted user, or by an administrator.

This procedure is based on the procedures for the following in the *NSP System Administrator Guide*:

- Configuring a role
- Configuring a user group
- Creating an NSP local user

For example, the reference procedures in NSP Release 23.11 are:

- How do I configure a role?
- How do I configure a user group?
- How do I create an NSP local user?
- How do I enable User Access Control?

If a restricted user has already been created, verify that the user has the required permissions, as shown in Step 6.

3.3.2 Steps

Create a role

1

Log in to the NSP as an administrator.

2

Open **Users and Security**.

3

Select **Roles** from the drop-down list on the toolbar.

4

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

5

In the Identification panel, specify a role name and description.

The Role Name and Description fields can employ **only** the following special characters: `@ - _`.

The Role Name string must not contain *any* spaces, including a leading or trailing space.

6

To assign NSP functional access to the role, go to the Action Permissions panel and select an access level from the drop-down list for each NSP GUI you want to include in the role.

Action permissions group item	Permissions	Notes
Service Fulfillment	Read / Write / Execute	—

Action permissions group item	Permissions	Notes
Network Intents	Read: Manage Intents	Required to import intent types into Service Management
Workflows	Read	Required to create service and tunnel templates
Optional: DCA Management	Read / Write / Execute	Only required for creating and plotting telemetry subscriptions
Optional: OAM Tests	Read / Write / Execute	Only required for generating and executing OAM tests

7

To assign network resource access to the role, go to the Resource Groups Access panel. (For a detailed explanation of the Resource Groups Access panel, see How do I set network resource access levels? in the *NSP System Administrator Guide*.)

You can assign resource group access globally, to resource group categories, to individual resource groups, or a combination of these. For service management it is recommended to grant access to all equipment and all services:

- **Access To All Equipment** assigns full permissions on all NE resource groups and port resource groups to the role.
- **Access To All Services** assigns full permissions on all service resource groups to the role.

8

Click **Create** to save your changes and return to the Roles list.

Create a user group

9

Open **Users and Security**.

10

Select **User Groups** from the drop-down list on the toolbar.

11

Click **+ Create User Group**. The Create User Group form opens.

12

Specify a group name and description in the **Identification** panel.

The user group name you specify here must exactly match a corresponding user group name returned by your user repository.

The User Group Name and Description fields can employ **only** the following special characters: `@ - _`.

The User Group Name string must not contain *any* spaces, including a leading or trailing space.

13

To assign user roles to the group, click **+ Add Roles** on the Roles panel. The Add Roles form opens.

14

Enable the check box for each role you want to assign to the group and click **Done**. The roles are added to the Selected Roles list.

To remove a role item from the Selected Roles list, click **Delete** on the item.

15

Click **Create** to save your changes and return to the User Groups list.

Create a user

16

Open **Users and Security**.

17

Select **Users** from the drop-down list on the toolbar.

18

Click **+ Create User**.

19

In the Create User form, specify user identification information for the account in the Identification section. The **Username** and **User Group** fields are mandatory.

Note: Any uppercase characters in the username are saved as lowercase.

The **Username** value:

- can be 1 to 40 characters long
- cannot include a space
- cannot have a leading or trailing space
- can include only the following special characters:
  - **@** (at sign)
  - **-** (hyphen)
  - **_** (underscore)
  - **.** (period)

20

In the Password section, specify and confirm a password for the user account.

- If you want this password to be temporary, enable the **Force User to Change Password** option. The new user will be forced to change their password when they first login to NSP.
- Enable the **Show Password** option to see the password characters as you type them.
- Click on the **Password Requirements** link to view a list of minimum security requirements for the password.

21

Click **Create**.

Enable user access control

22

Open **Users and Security**, **User Groups**.

23

Click ⋮ **More Actions**, **Settings**.

24

In the Access Control Settings form, enable the **NSP User Access Control** option.

25

Click **SAVE** to enable access control.

END OF STEPS

3.4 Install the required artifact bundles

3.4.1 Purpose

Use this procedure to make the required intent types available to Service Management in NSP. This procedure is based on the procedure for installing an artifact bundle in the *NSP Network Automation Guide*.

For example, the reference procedure in NSP 23.11 is How do I install an artifact bundle?.

3.4.2 Steps

Download the required intent types

1

Download the Service Fulfillment artifact bundle from the NSP software delivery site.

Navigate through the hierarchy to the folder of artifacts that can be imported using the Artifacts views, for example: NSP → 23.11 → Artifacts → Artifact_Admin_Import.

See the description to verify which artifact bundle to download.

Install the artifact bundle in NSP

2

Open **Artifacts**, **Artifact Bundles**.

3

Click **IMPORT & INSTALL**.

4

In the form that opens, drag and drop the zip file, or click **Browse** and navigate to the files on your system.

5

To install the artifact bundle immediately, click **IMPORT & INSTALL**. To import without installing, click **IMPORT**.

The chosen operation is triggered immediately. The artifact bundle status is updated to Imported or Installed when NSP has confirmed the status of all artifacts in the artifact bundle.

6

To install a bundle in Imported status, choose **Install bundle** from the ⋮ (Table row actions) menu.

END OF STEPS

3.5 Configure user access to the required intent types

3.5.1 Purpose

Use this procedure to provide the user access to intent types. If the restricted Service Management user will be performing configuration tasks, this procedure must be performed.

This procedure is based on the procedure for configuring user access to an intent type in the *NSP Network Automation Guide*.

For example, the reference procedure in NSP Release 23.11 is How do I configure user access to an intent type?.

3.5.2 Steps

1

Log in to the NSP as an administrator.

2

Open **Network Intents**, **Intent Types**.

3

Select the `tunnel` and `cpipe` intent types.

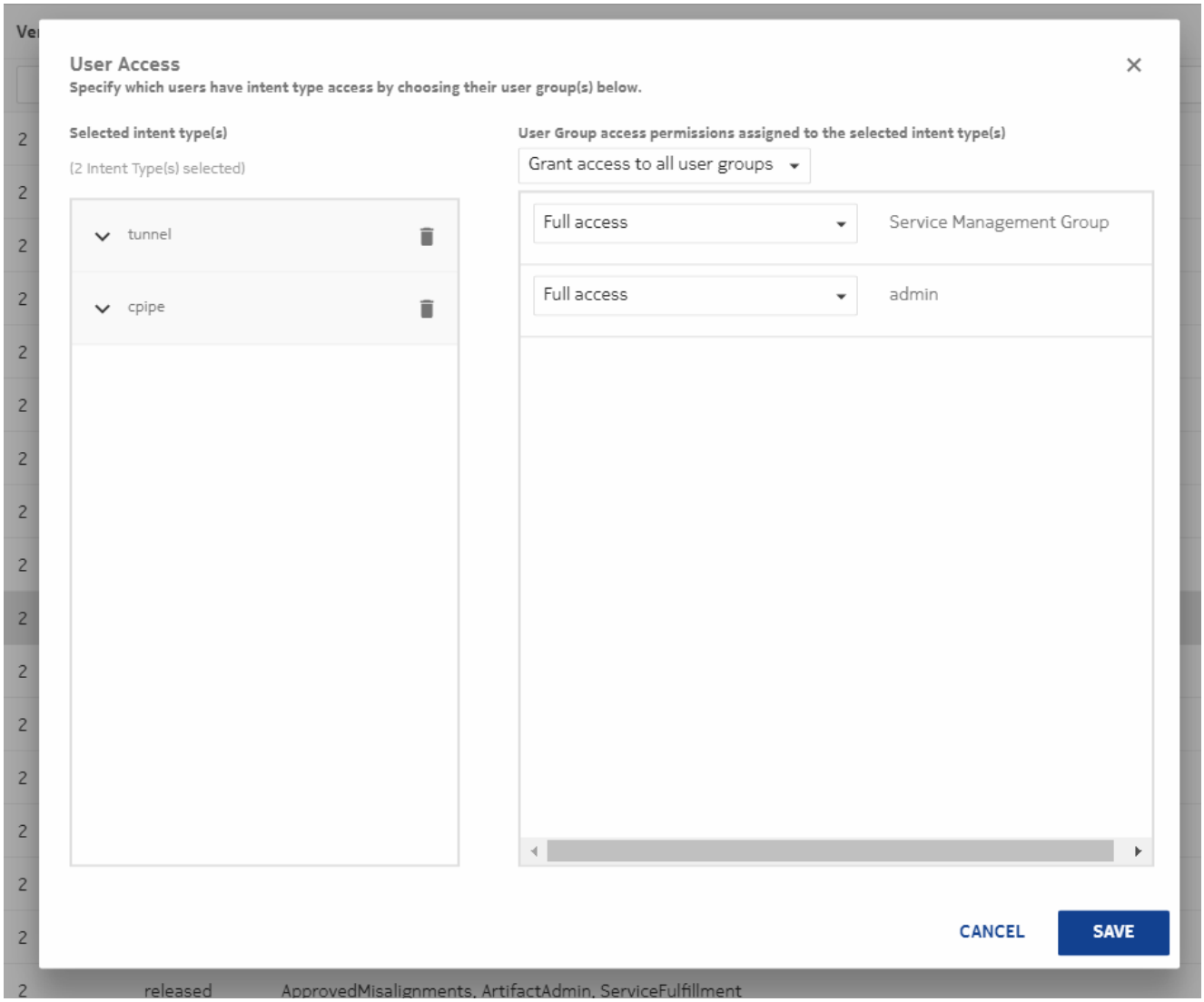
4

Click ⋮ (Table row actions), **User Access** to open the User Access form.

5

In the **User Access** form, choose **Grant access to all user groups** from the drop-down list at the top right of the form.

Choose **Full access** for the user group created in “Create a user group” (p. 54).



6

Click **SAVE**. The user access is updated.

END OF STEPS

Service Configuration

3.6 Import intent types into Service Management

3.6.1 Purpose

Use this procedure to import the intent types you obtained in 6.4 “Install the required artifact bundles” (p. 218) to the Service Management views. This procedure is based on the procedure for importing an intent type into Service Management in the *NSP Service Management Guide*.

For example, the reference procedure in NSP Release 23.11 is How do I import an intent type into Service Management?.

Note: This procedure is not required in NSP 25.4 or later because intent types for Service Management will import directly into Service Management during artifact bundle installation.

The intent types required are `tunnel` and `cpipe`.

3.6.2 Steps

1

Log in to the NSP as the Service Management user.

2

From the **Service Management, Intent Type Catalogue** view, click **IMPORT**.

A list of previously-defined intent types is displayed.

Note: Only intent types that have the Service Fulfillment label applied will be available to import. Intent types to be used for tunnel template creation must also have the Tunnel label applied.

Note: For a restricted user to be allowed to import intent types, they must have appropriate permissions configured for those intent types in Network Intents; see How do I configure user access to an intent type? in the *NSP Network Automation Guide*.

3

Select the check boxes in-line with the intent types you wish to import and click **IMPORT**.

The intent types to import are:

- tunnel
- cpipe

The intent types are imported into service management. This may take a few minutes.

Note: Selecting an imported intent type from the list opens the Info panel, which displays historical information such as the last time the intent type was updated, the last time it was imported, and the last time the modules that compose the intent type were revised.

END OF STEPS

3.7 Create a service tunnel template

3.7.1 Purpose

Perform this procedure to create the template that Service Management will use in the creation of a service tunnel.

This procedure is based on the procedure to create a tunnel template in the *NSP Service Management Guide*.

For example, the reference procedure in NSP 23.11 is How do I create a tunnel template?.

3.7.2 Steps

1

Log in to the NSP as the Service Management user.

2

From the **Service Management, Tunnel Templates** view, click **+ CREATE**.

The Create a tunnel template form opens.

3

Configure the parameters, as required.

Parameter	Description
Template Name	Specifies the name of the template
Description	Describes the template
Tunnel Intent Type	`tunnel`
Intent Version	Specifies which version of the selected tunnel intent type to associated with the template
State	Released
Config Form	Specifies the form to be used for the template

4

If required, click **+ ADD** in the Workflows panel to add workflows to the tunnel template.

The Add Workflows form opens.

5

Configure the parameters, as required:

Parameter	Description
Workflow Name	Specifies the workflow to be executed
Service Life Cycle State	Specifies the life cycle state of the tunnel that will trigger workflow execution
Service Life Cycle Case	Specifies the case, Success or Fail, relative to the life cycle state that will trigger workflow execution
Blocking	Specifies whether unsuccessful execution of the workflow will prevent tunnel life cycle state changes
Workflow Execution Timeout (seconds)	Specifies the length of time, in seconds, that unsuccessful execution of the workflow will prevent tunnel life cycle state changes

6

Click **ADD**.

The Add Workflows form closes and the workflow is added to the tunnel template.

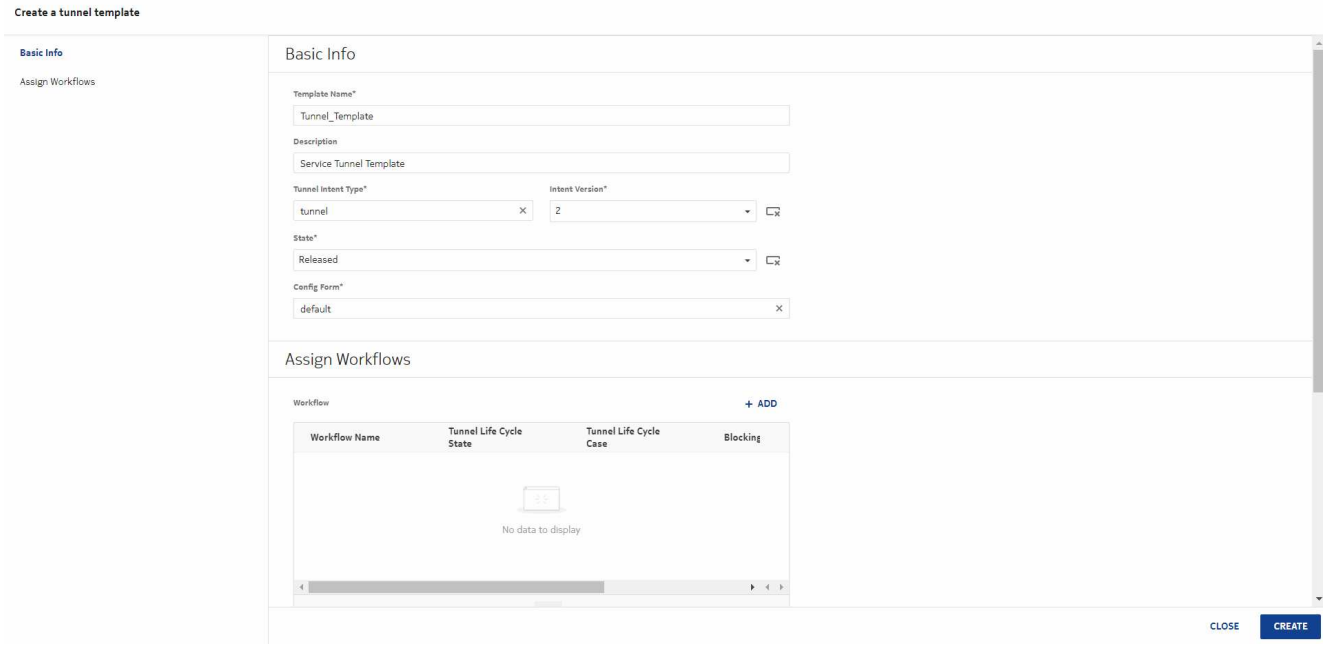
7

Click **CREATE**.

The tunnel template is created.

END OF STEPS

3.7.3 Example creation form without a workflow



3.8 Create and deploy service tunnels to the network

3.8.1 Purpose

Perform this procedure to create service tunnels. The creation of service tunnels is a prerequisite to creation of a service.

This procedure is based on the procedures for creating and auditing a service tunnel in the *NSP Service Management Guide*.

For example, the reference procedures in NSP Release 23.11 are:

- How do I create a service tunnel?
- How do I audit a service tunnel?

3.8.2 Steps

1

Log in to the NSP as the Service Management user.

2

Open the tunnel creation form:

1. From the **Service Management, Service Tunnels** view, click **+ CREATE**.

The Select a tunnel template to start form opens displaying a list of tunnel templates.

2. Choose the template you created in 3.7 “Create a service tunnel template” (p. 94).

   The Create Tunnel form opens with the Template Name parameter populated.

3

Configure the parameters, as required.

4

If the Transport Type parameter was set to MPLS, configure the required parameters.

5

Configure the required Hello parameters.

6

If the Transport Type parameter was set to GRE, configure the Allow Fragmentation parameter (if required), which specifies whether or not fragmentation will be allowed for the tunnel.

7

Configure the required parameters.

8

Click **DEPLOY** to create the tunnel in a Deployed state.

9

Perform an audit to verify that the tunnel is deployed correctly:

1. From the **Service Management, Service Tunnels** view, click on the service tunnel in the list, then expand the Alignment State section in the info panel and click **AUDIT CONFIG**.

   The service tunnel is audited.

2. If an Audit Result form appears, one or more attributes and/or objects are misaligned. Review the results and click **OK**.

   The Audit Result form closes.

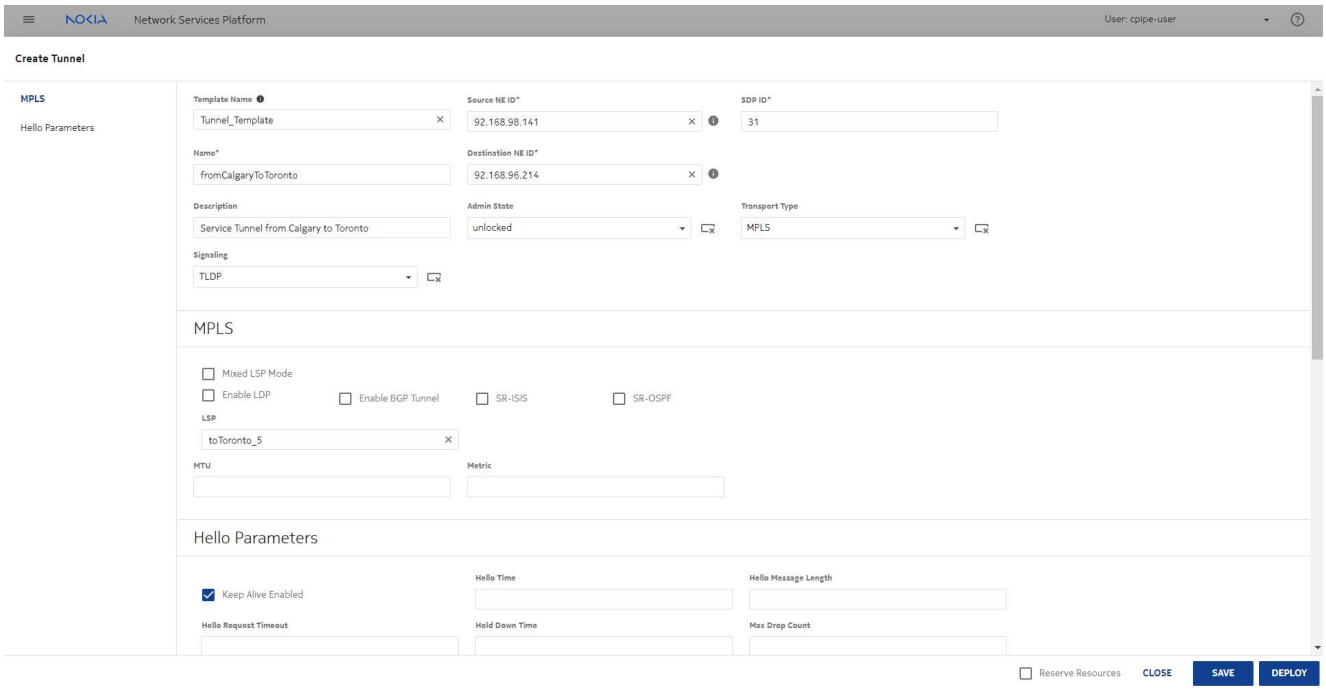
10

To revert to the expected value of a misaligned attribute, or to restore a misaligned object, click ⋮ (Table row actions), **Align**, **Push To Network** in-line with the previously audited service tunnel.

The service tunnel is synchronized with the network.

END OF STEPS

3.8.3 Tunnel creation example



3.9 Create a CPIPE service template

3.9.1 Purpose

This procedure is based on the procedure to create a service template in the *NSP Service Management Guide*.

For example, the reference procedure in NSP 23.11 is How do I create a service template?.

3.9.2 Steps

1

Log in to the NSP as the Service Management user.

2

From the **Service Management, Service Templates** view, click **+ CREATE**.

The Create a service template form opens.

3

Configure the parameters, as required.

Parameter	Description
Template Name	Specifies the name of the template
Description	Describes the template
Service Intent Type	`cpipe`
Intent Version	Specifies which version of the selected service intent type to associated with the template
State	Released
Config Form	Specifies the interface to be used with the template

4

If required, click **+ ADD** in the Workflows panel to add workflows to the service template.

The Add Workflows form opens.

5

Configure the parameters, as required:

Parameter	Description
Workflow Name	Specifies the workflow to be executed
Service Life Cycle State	Specifies the life cycle state of the service that will trigger workflow execution
Service Life Cycle Case	Specifies the case, Success or Fail, relative to the life cycle state that will trigger workflow execution
Blocking	Specifies whether unsuccessful execution of the workflow will prevent service life cycle state changes
Workflow Execution Timeout (seconds)	Specifies the length of time, in seconds, that unsuccessful execution of the workflow will prevent service life cycle state changes

6

Click **ADD**.

The Add Workflows form closes and the workflow is added to the service template.

7

If required, select a Default Service Category in the Bulk Association panel to specify a service type to which this service template can be applied in bulk.

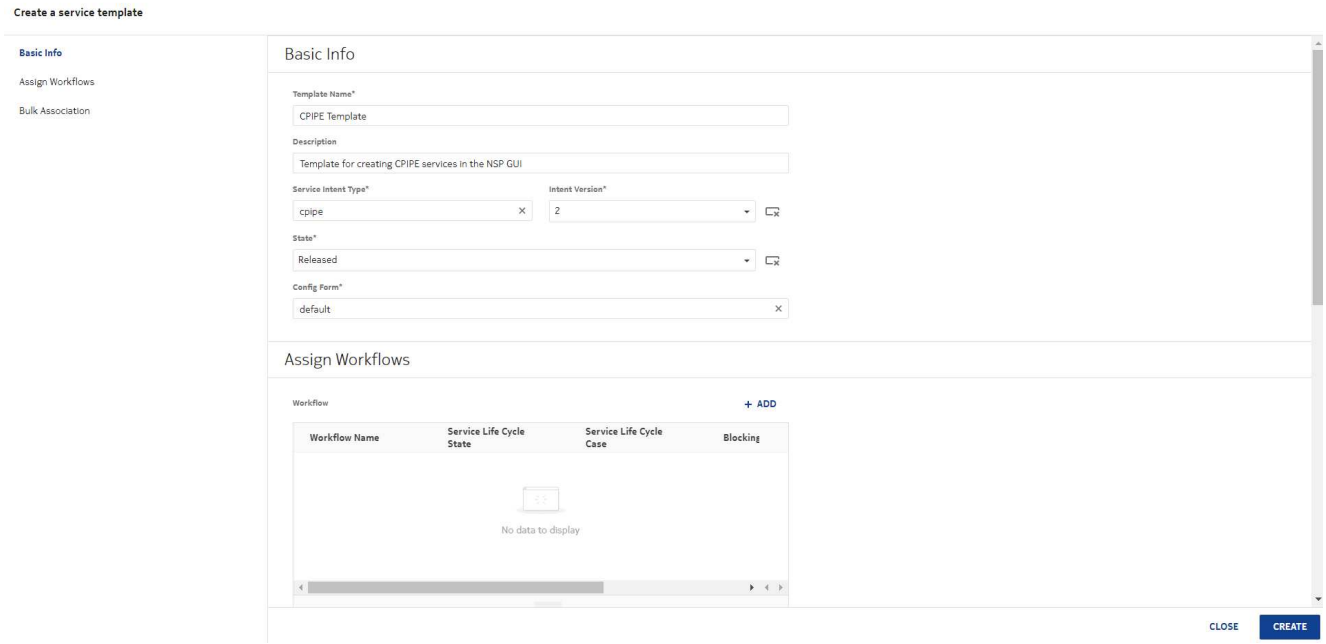
8

Click **CREATE**.

The service template is created.

END OF STEPS

3.9.3 Example creation form without a workflow



3.10 Create and deploy a CPIPE service to the network

3.10.1 Purpose

Perform this procedure to create the service.

This procedure is based on the procedures for creating and auditing a service in the *NSP Service Management Guide*.

For example, the reference procedures in NSP Release 23.11 are:

- How do I create a C-Line service?
- How do I audit a service?

3.10.2 Steps

1

Log in to the NSP as the Service Management user.

2

From the **Service Management, Services** view, click **+ CREATE**.

The Select a service template to start form opens displaying a list of service templates.

3

Click on a C-Line service template from the list.

The Create Service form opens with the Template Name parameter populated.

4

Configure the parameters, as required:

Parameter	Description
Service Name	Specifies the name of the service. Must be unique from other services created using NSP.
NE Service ID	Specifies the NE service ID
VC Type	Specifies the virtual circuit type
MTU	Specifies the service MTU
Customer ID	Specifies the customer ID
Description	Describes the service
Admin State	Specifies the initial administrative state of the service upon deployment
Job ID	Specifies the work-order number

Continue to the Site A panel.

5

Configure the required parameters:

Parameter	Description
Device ID	Specifies the device identifier
Site Name	Specifies the site name
Description	Describes the site

Note: If site names and descriptions are added, these will take precedence over any service name and description specified in Step 4, with the Site A name and description taking precedence over Site B. As such, these attributes will be displayed in various locations, such as NSP's Model Driven Configurator function and NFM-P.

6

Click **+ ADD**.

The Add Endpoint form opens.

7

Configure the parameters, as required:

Parameter	Description
Port ID	Specifies the port identifier
Time Slots	Specifies the time slot pattern to be used
Admin State	Specifies the administrative state of the service
Description	Describes the SAP

8

In the CEM panel, configure the parameters as required:

Parameter	Description
RTP Header	Specifies whether or not an RTP header is used when packets are transmitted to the Packet Service Network
Payload Size	Specifies the payload size (in bytes) of packets transmitted to the Packet Service Network
Jitter Buffer	Specifies the jitter buffer size (in milliseconds)
Asymmetric Delay Control	
Enable	Specifies whether or not asymmetric delay control is enabled
Samples	Specifies the number of packets that will be sampled during the sampling period
Repeat Period	Specifies the sampling period (in minutes)

9

Configure the parameters, as required:

Parameter	Description
Enable QoS	Specifies whether or not QoS is enabled

Parameter	Description
Enable IP/IPv6 Filter	Specifies whether or not an IP/IPv6 filter is enabled

10

If QoS was enabled in Step 9, configure the parameters as required in both the ingress and egress panels:

Parameter	Description
QoS	
Match QinQ Dot1p (ingress only)	Specifies the match QinQ Dot1p
QinQ Mark Top Only (egress only)	Specifies whether top Q-tags are marked
SAP Ingress	
Policy Name	Specifies the name of the ingress SAP policy
Queuing Type	Specifies the ingress queuing type
SAP Egress	
Policy Name	Specifies the name of the egress SAP policy
Queue (click **+ ADD**)	
Queue ID	Specifies the unique identifier for the queue
CBS	Specifies the CBS of the queue
MBS	Specifies the MBS of the queue
PIR	Specifies the PIR rate of the queue
CIR	Specifies the CIR rate of the queue
Policer (click **+ ADD**)	
Policer ID	Specifies the unique identifier for the policer
CBS	Specifies the CBS of the policer
MBS	Specifies the MBS of the policer
Policer Control Policy	
Policy Name	Specifies the name of the policer control policy
Scheduler Policy	
Policy Name	Specifies the name of the scheduler policy
Scheduler (click **+ ADD**)	

Parameter	Description
Scheduler Name	Specifies the name of the scheduler
PIR	Specifies the PIR rate of the scheduler
CIR	Specifies the CIR rate of the scheduler

11

If an IP/IPv6 filter was enabled in Step 9, configure the parameters as required in both the ingress and egress panels:

Parameter	Description
IP	Specifies the IP filter identifier
IPv6	Specifies the IPv6 filter identifier

Click **ADD** to add the endpoint. The Add Endpoint form closes.

12

Configure the PW Switching parameters, as required:

Parameter	Description
Primary Hub ID	Specifies the identifier of the primary hub
Secondary Hub ID	Specifies the identifier of the secondary hub

13

In the Site B panel, specify the Device ID, then click **+ ADD**.

The Add Endpoint form opens.

14

Repeat Step 5 to Step 12 for Site B.

15

In the SDP Details panel, click **+ ADD**.

The Add SDP form opens.

16

Configure the parameters, as required:

Parameter	Description
Admin State	Specifies the desired state of the service SDP binding

Parameter	Description
Source Device ID	Specifies the SDP source device identifier
Destination Device ID	Specifies the SDP destination device identifier
Steering Parameter	Specifies the steering parameter used by NSP
SDP ID	Specifies the SDP identifier
Description	Describes the SDP binding
Override VC-ID	Specifies whether or not the VC-ID will serve as the NE service ID for the SDP
VC ID	Specifies the SDP virtual circuit identifier

Click **ADD** to add the SDP binding. The Add SDP form closes.

17

Click **DEPLOY** to create the service in a Deployed state.

18

Perform an audit to verify that the service is deployed correctly:

1. From the **Service Management, Services** view, click ⋮ (Table row actions), **Audit config** in-line with any service.

   The service is audited.

2. If an Audit Result form appears, one or more attributes and/or objects are misaligned. Review the results and click **OK**.

   The Audit Result form closes.

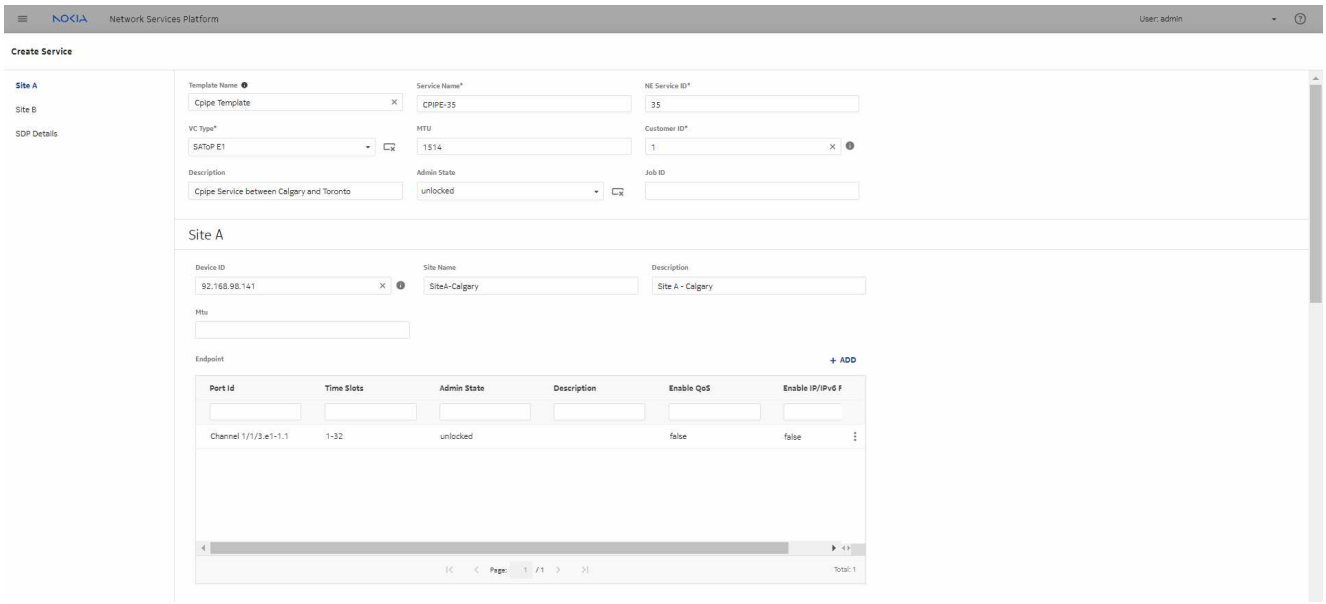
19

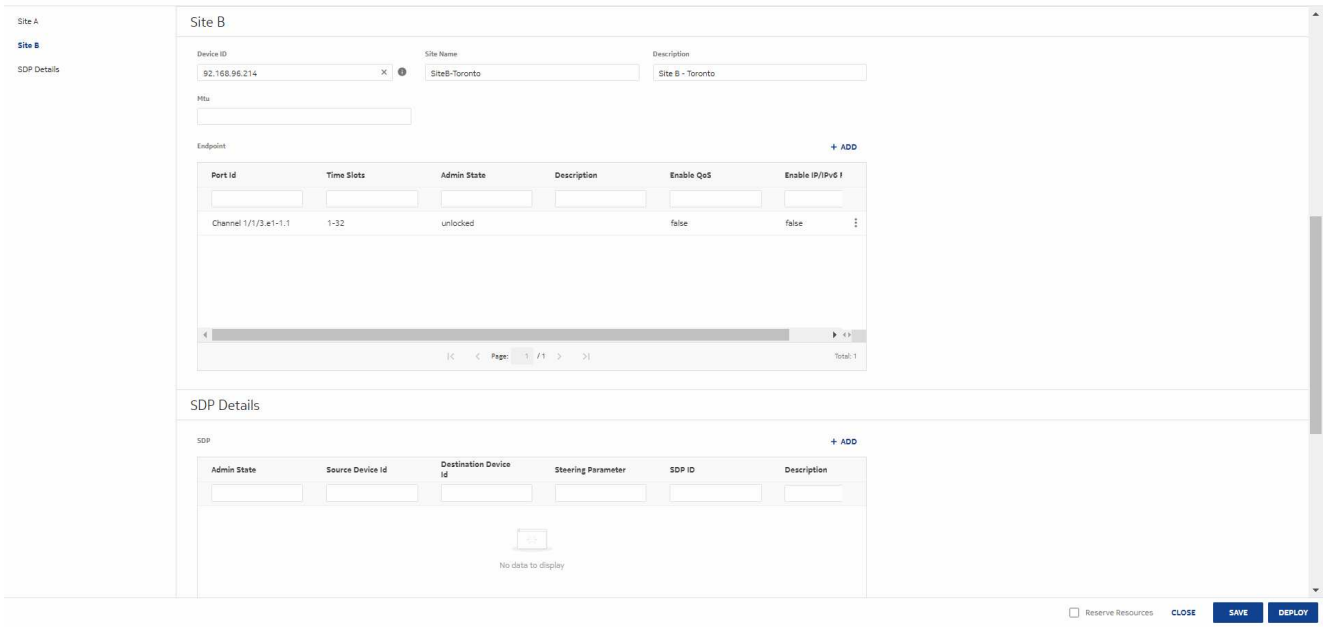
Click ⋮ (Table row actions), **Align**, and then either **Push to network** or **Pull from network** in-line with the previously audited service.

The service is synchronized with the network.

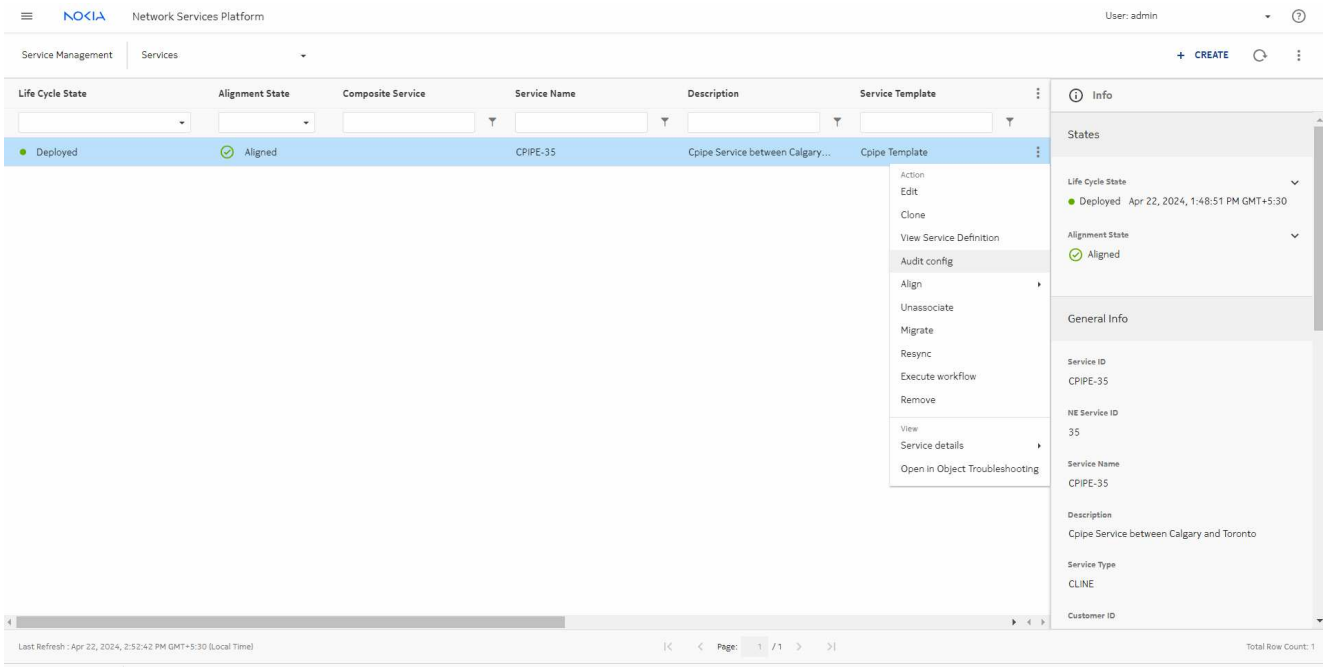
END OF STEPS

3.10.3 Example of a configured service





3.10.4 Services Table row actions menu showing audit and align



3.11 Modify or delete a CPIPE service

3.11.1 Purpose

Use this procedure if needed to modify configured parameters for a Cpipe service, or to remove a service from the network and delete it.

3.11.2 Steps

Edit a service

1

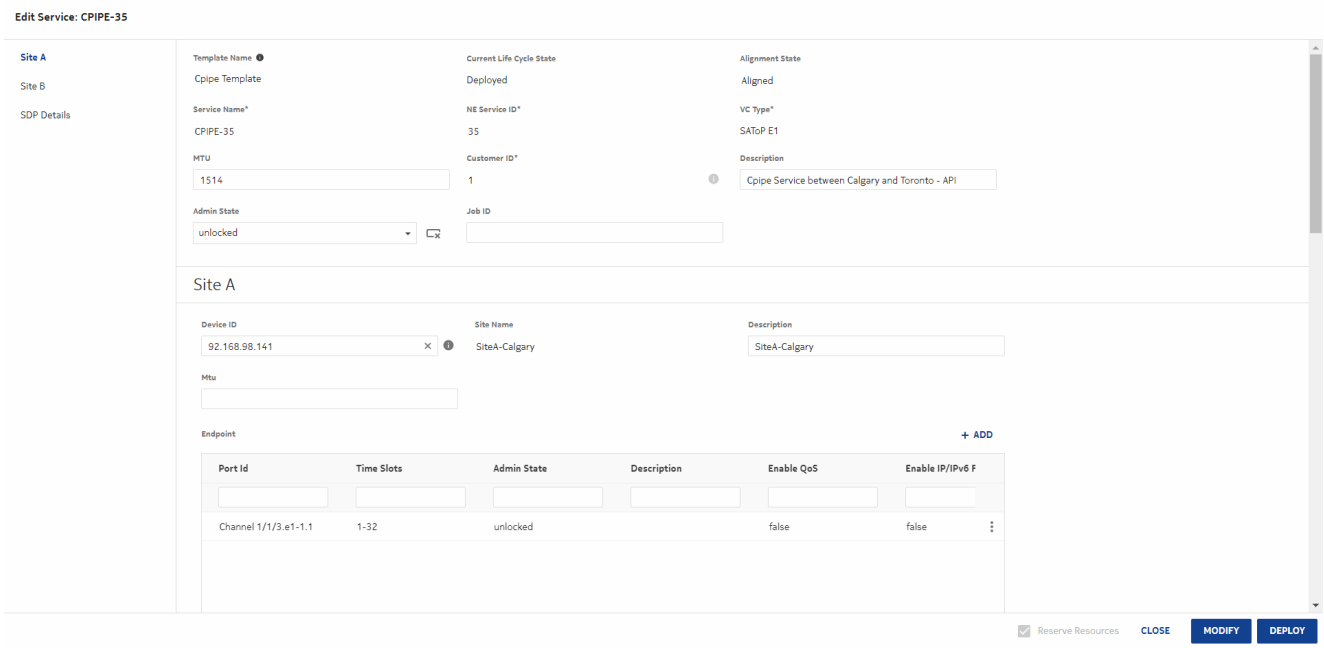
Log in to the NSP as the Service Management user.

2

From the **Service Management**, **Services** view, select a service and choose **Edit** from the ⋮ (Table row actions) menu.

3

Modify the service, site, endpoint or SDP parameters as needed and click **DEPLOY**.



Delete a service

4

From the **Service Management**, **Services view**, select a service and click ⋮ (Table row actions), **Remove**.

The Remove Service From Network confirmation dialog opens.

5

Click **REMOVE** to remove the service from the network.

The Life Cycle State of the service is changed to Removed.

6

If you prefer, you can leave the service in Removed state so that it can be deployed again later. To delete the service permanently, proceed to the next step.

7

To delete the service, select the service and click ⋮ (Table row actions), **Delete**.

The Delete Service confirmation dialog opens.

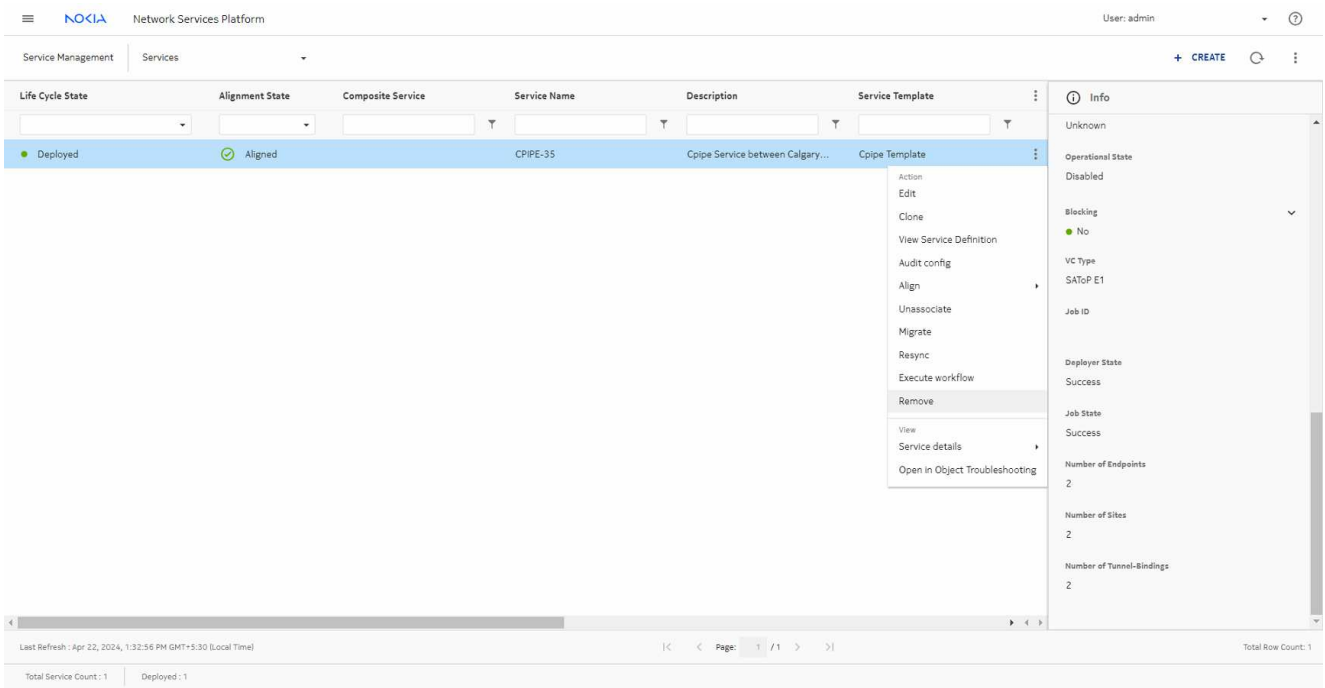
Note: The Delete option only appears if the service is in Removed state.

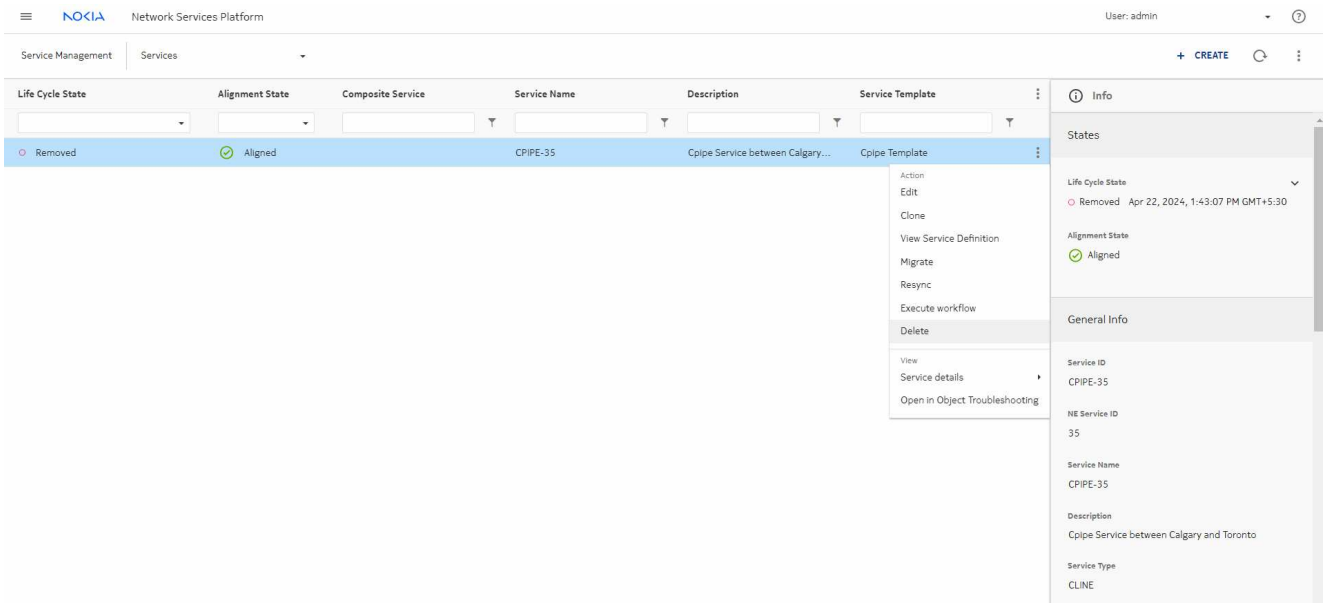
8

Click **DELETE** to permanently delete the service from the NSP.

END OF STEPS

3.11.3 Examples showing remove and delete





Optional procedures

3.12 Create telemetry subscriptions

3.12.1 Purpose

Perform this procedure to set up telemetry collection.

The bundle of vendor agnostic custom resources must be imported and installed to support telemetry collection. The bundle is found on the NSP software delivery site, in the Adaptors folder along with your NE adaptor suite, for example, NSP → 23.11 → Adaptors → Nokia_SROS. Choose the zip file with va and cr in the filename, for example, `nsp-telemetry-cr-va-sros-1.0.0-rel.10.zip`.

This procedure is based on the procedure for managing subscriptions in the *NSP Data Collection and Analysis Guide*.

For example, the reference procedure in NSP 23.11 is How do I manage subscriptions?.

See also the procedure to install telemetry artifacts in the *NSP Data Collection and Analysis Guide* to verify that telemetry prerequisites are in place. The reference procedure for this is in NSP 24.4: How do I install telemetry artifacts?.

CAUTION

Service Disruption

The name of an object, including subscriptions, baselines, indicators, templates, and chart profiles, cannot contain a semicolon (;) or backslash (\).

The use of these characters in an object identifier will result in corrupted data that must be deleted by Nokia support.

3.12.2 Steps

1

Log in to the NSP as the Service Management user.

2

Open **Data Collection and Analysis Management**, **Subscriptions**.

3

To create a subscription:

1. Click + **SUBSCRIPTION**.
2. In the Create Subscription form that opens, configure the General parameters as needed.
   - Enable database (DB) subscriptions as needed to save subscription information to the NSP database. For subscription data to be available to Analytics, the auxiliary database must be deployed.

- The subscription is enabled by default: it will start running immediately.
  Choose **Disabled** in the **State** field if you want to enable your subscription later.

3. In the **Object Filter** field, enter filtering information as needed to filter the collected data.
   As you type, the field provides suggestions for available filters to match your input and identifies incorrect syntax.
4. Enter information in the Telemetry Type field. As you type, the field filters for available telemetry types to match your input.
   Choose the telemetry type you need from the list of matches.
5. When you enter a telemetry type, all counters are enabled by default.
   To customize the counters, enable the **Enable notifications and notification counters** check box.
   Click **Remove** to remove a counter.
   Click **+ COUNTERS** to add a counter that was removed.
6. Click **CREATE**.
   The subscription begins collection when it is enabled.

END OF STEPS

3.13 Create a telemetry chart and plot statistics

3.13.1 Purpose

Use this procedure to chart historical telemetry data. This procedure is based on the procedure for plotting a telemetry chart in the *NSP Data Collection and Analysis Guide*.

For example, the reference procedure in NSP 23.11 is How do I plot a telemetry chart?.

CAUTION

Service Disruption

The name of an object, including subscriptions, baselines, indicators, templates, and chart profiles, cannot contain a semicolon (;) or backslash (\).

The use of these characters in an object identifier will result in corrupted data that must be deleted by Nokia support.

3.13.2 Before you begin

When you create a telemetry chart, you configure a telemetry filter. For historical data to be displayed, the data must be available in the database; see 2.13 “Create telemetry subscriptions” (p. 77).

Charts are created by streaming to the plotter: historical data is queried and streamed to the plotter, then real time telemetry subscriptions are created and the data from these subscriptions is streamed to the plotter.

Data Collection and Analysis Visualizations times out if telemetry data is not received. The time-out limit is either double the collection interval or two minutes, whichever is greater.

3.13.3 Steps

Create a chart

1

Log in to the NSP as the Service Management user.

2

Open the New Chart window:

- From **Data Collection and Analysis Visualizations**, **Telemetry Charts**, click **+ CHART**.
- From **Data Collection and Analysis Management**, **Subscriptions**, choose a subscription and click ⋮ (Table row actions), **Open in Data Collection and Analysis Visualizations**.

3

In the window that opens, configure the parameters in the top panel:

1. Configure the **Collection Interval** parameter. If you are using NFM-P telemetry data, verify that the collection interval is long enough to allow time for Visualizations to receive the data before timing out.
2. From the **Time Range** drop-down list, choose the amount of historical data to display.
3. Click **Combine charts** to plot data from multiple data series on the same chart.

4

Click **+ DEFINITION**.

The telemetry and resource filter definition panels are displayed.

5

Enter information in the **Telemetry Type** field. As you type, the field filters for available telemetry types to match your input.

Choose the telemetry type from the list of matches.

6

Choose counters to display from the **Counters** drop-down list.

7

In the **Object Filter** field, enter filtering information to filter the collected data.

8

If you need to save the configuration as a chart:

1. Click **SAVE AS**.
2. In the window that opens, enter a name for the chart and add a description if needed.
3. Click **SAVE**.

The chart is added to the list.

9

Click **PLOT**.

END OF STEPS

3.13.4 Steps

Plot an existing chart

1

To plot an existing chart with no changes:

1. Open **Data Collection and Analysis Visualizations**, **Telemetry Charts**.
2. Choose a chart and click ⋮ (Table row actions), **Chart**.

2

To edit a chart and plot it, choose the chart and click ⋮ (Table row actions), **Edit**.

3

Edit the parameters as needed and click **PLOT**.

END OF STEPS

3.13.5 Result

Visualizations displays a chart view showing the streaming data. While data is streaming, you can configure the **Group by** parameter in the upper left of the chart view to change how the data is grouped or click **Configure** in the upper right to view or change the configuration of the chart.

Click ⓘ(Chart Details) to open the Chart Details panel on the right side of the chart view to show details about the resources.

4 UCC-14: E-LAN/EVPN

4.1 Overview

4.1.1 Purpose

This chapter describes the process required to configure an E-LAN/EVPN service over MPLS on SR OS NEs using NSP Service Management.

Configuration examples in this chapter show NSP Release 23.11 and SR OS 23.7.R2 NEs.

The following artifact bundles were used to test this use case:

- nsp-icm-intents-23.11.0-cam-bundle.zip
- nsp-svc-fulfillment-bundle-2311-v3.zip

See the NSP and NE documentation for more information.

Note: The terms EVPN-VPLS and E-LAN EVPN are synonymous and are used interchangeably in NSP documentation.

4.1.2 Contents

Preparation

4.2 Prerequisites

4.2.1 Network configuration prerequisites

Before services can be configured and managed in NSP, the network configuration prerequisites must be met. The following table describes the requirements that can apply to service use cases, and indicates whether each prerequisite is required for this process.

Where an NSP intent type is not available, CLI or MD-CLI must be used to perform configuration on the device.

Prerequisite	Documentation reference	Notes
Mandatory for E-LAN/EVPN		
GRPC configuration 1. Generate security certificates 2. Configure security and enable GRPC on all devices 3. Apply security certificates on all devices	See SR TLS information here in the SR OS 24.3 R1 documentation: TLS	—
Netconf/SNMP provisioning: enable NETCONF and SNMP protocols on all devices	For more information about SNMP and NETCONF with SR OS, see SNMP and NETCONF in the *SR OS 24.3 R1 System Management Guide*.	—
NSP installation	Pathway for NSP system installation in the *NSP Installation and Upgrade Guide* How do I enable TLS for telemetry and gNMI on_change support? in the *NSP System Administrator Guide*.	Include the following in your deployment: • Feature packs: - platform-baseServices - platform-pluggableNetworkAdaptation - platform-loggingMonitoring - serviceActivationAndConfiguration-intentBasedServiceFulfillment - networkInfrastructureManagement-basicManagement - networkInfrastructureManagement-deviceConfig • Adaptor suites: - sros-common - sros-oc-logical-inventory - sros-23-7-r1

Prerequisite	Documentation reference	Notes
Download the required artifact bundles from the NSP software delivery site: • NSP predefined set for ICM (device configuration) • NSP product artifact bundle for Service Fulfillment	How do I install an artifact bundle? in the *NSP Network Automation Guide*	—
Device discovery	Pathway for device discovery in the *NSP Classic Management User Guide* How do I discover devices? in the *NSP Device Management Guide* Nokia Developer Portal for information about FTP mediation policy creation using API.	—
Cards and MDAs provisioning	ICM process in the *NSP Device Management Guide* for more information about using the Device Configuration views, and the other procedures in the *NSP Device Management Guide* for further detail. See the NSP ICM Intent Type Catalog for information about this and other device configuration intent types developed by Nokia.	The intent type required for this configuration is icm-equipment-card-mda.
Connectors and Ports provisioning		The intent types required for this configuration are: • icm-equipment-port-connector • icm-equipment-port-ethernet
OSPF/ISIS	CLI Reference Guides for SR OS	—
LDPs, MPLS and RSVP configuration	CLI Reference Guides for SR OS	For LDP to be operational, the IPv4 and IPv6 bindings must be configured manually using CLI.
Interfaces Provisioning	How do I create a physical configuration deployment? in the *NSP Device Management Guide*.	The intent type required for this configuration is icm-router-network-interface
BGP/EVPN	How do I create a logical configuration deployment? in the *NSP Device Management Guide*.	The intent type required for this configuration is icm-router-bgp_group
Customer creation	How do I create a logical configuration deployment? in the *NSP Device Management Guide*.	The intent type required for this configuration is icm-service-customer
Optional		

Prerequisite	Documentation reference	Notes
Optional items to include in your NSP deployment	Pathway for NSP system installation in the *NSP Installation and Upgrade Guide*	• Optional feature packs: - pathControlAndOptimization - multilayerDiscoveryAndVisualization - NSP Analytics: Network Operations Analytics feature package with the networkOperationsAnalytics-analyticsReporting installation option - NSP Baseline Analytics: networkOperationsAnalytics-baselineAnalytics - networkInfrastructureManagement-performanceIndicatorsAndAlerts • VSR/NRC • An AuxDB • An NFM-P instance
Telemetry/OAM	*NSP Data Collection and Analysis Guide*	• NSP SR OS vendor-agnostic telemetry adaptation artifact bundle • networkInfrastructureManagement-gnmiTelemetry feature pack
Segment Routing	CLI Reference Guides for SR OS	—
Scheduler QoS Policies	How do I create a logical configuration deployment? in the *NSP Device Management Guide*.	The intent types required for this configuration are: • icm-qos-schedulerpolicy-srqos • icm-qos-network-srqos • icm-qos-sapingress-srqos • icm-qos-sapegress-srqos
Network QoS Policies configuration		
SAP QoS Policies configuration		
PCEP configuration	CLI Reference Guides for VSR-NRC	Most of the connections required for PCEP are established during previous configuration steps.
LAGs and MC-LAG creation	How do I create a logical configuration deployment? in the *NSP Device Management Guide*.	The intent types required for this configuration are: • icm-logical-lag-access • icm-logical-mc_lag-access

4.3 Optional: create a restricted Service Management user

4.3.1 Purpose

Perform this optional procedure to create a user with access only to specified NSP functions.

Procedures in this chapter can be performed by the restricted user, or by an administrator.

This procedure is based on the procedures for the following in the *NSP System Administrator Guide* and *NSP Network Automation Guide*:

- Configuring a role
- Configuring a user group
- Creating an NSP local user
- Enabling User Access Control
- Configuring user access to an intent type

For example, the reference procedures in NSP Release 23.11 are:

- How do I configure a role?
- How do I configure a user group?
- How do I create an NSP local user?
- How do I enable User Access Control?
- How do I configure user access to an intent type?

If a restricted user has already been created, verify that the user has the required permissions, as shown in Step 6.

4.3.2 Steps

Create a role

1

Log in to the NSP as an administrator.

2

Open **Users and Security**.

3

Select **Roles** from the drop-down list on the toolbar.

4

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

5

In the Identification panel, specify a role name and description.

The Role Name and Description fields can employ **only** the following special characters: `@ - _`.

The Role Name string must not contain *any* spaces, including a leading or trailing space.

6

To assign NSP functional access to the role, go to the Action Permissions panel and select an access level from the drop-down list for each NSP GUI you want to include in the role.

Action permissions group item	Permissions	Notes
DCA Management	Read / Write / Execute	Only required for creating and plotting telemetry subscriptions
Network Intents	Read: Manage Intents	Required to import intent types into Service Management
OAM Tests	Read / Write / Execute	Only required for generating and executing OAM tests
Service Fulfillment	Read / Write / Execute	—
Workflows	Read	Required to create service and tunnel templates

7

To assign network resource access to the role, go to the Resource Groups Access panel. (For a detailed explanation of the Resource Groups Access panel, see How do I set network resource access levels? in the *NSP System Administrator Guide*.)

You can assign resource group access globally, to resource group categories, to individual resource groups, or a combination of these. For service management it is recommended to grant access to all equipment and all services:

- **Access To All Equipment** assigns full permissions on all NE resource groups and port resource groups to the role.
- **Access To All Services** assigns full permissions on all service resource groups to the role.

8

Click **CREATE** to save your changes and return to the Roles list.

Create a user group

9

Open **Users and Security**.

10

Select **User Groups** from the drop-down list on the toolbar.

11

Click **+ Create User Group**. The Create User Group form opens.

12

Specify a group name and description in the **Identification** panel.

The user group name you specify here must exactly match a corresponding user group name returned by your user repository.

The User Group Name and Description fields can employ **only** the following special characters: `@ - _`.

The User Group Name string must not contain spaces, including a leading or trailing space.

13

To assign user roles to the group, click **+ Add Roles** on the Roles panel. The Add Roles form opens.

14

Enable the check box for the role you configured in "Create a role" (p. 120) and click **Done**. The role is added to the Selected Roles list.

15

Click **CREATE** to save your changes and return to the User Groups list.

Create a user

16

Open **Users and Security**.

17

Select **Users** from the drop-down list on the toolbar.

18

Click **+ Create User**.

19

In the Create User form, specify user identification information for the account in the Identification section. The **Username** and **User Group** fields are mandatory.

Note: Any uppercase characters in the username are saved as lowercase.

The **Username** value:

- can be 1 to 40 characters long
- cannot include a space
- cannot have a leading or trailing space
- can include only the following special characters:
  - **@** (at sign)
  - **-** (hyphen)
  - **_** (underscore)
  - **.** (period)

20

In the **User Group** field, select the user group you created in "Create a user group" (p. 54).

21

In the Password section, specify and confirm a password for the user account.

- If you want this password to be temporary, enable the **Force User to Change Password** option. The new user will be forced to change their password when they first login to NSP.
- Enable the **Show Password** option to see the password characters as you type them.
- Click on the **Password Requirements** link to view a list of minimum security requirements for the password.

22

Click **CREATE**.

Enable user access control

23

Open **Users and Security**, **User Groups**.

24

Click **More Actions**, **Settings**.

25

In the Access Control Settings form, enable the **NSP User Access Control** option.

26

Click **SAVE** to enable access control.

END OF STEPS

4.4 Install the required artifact bundles

4.4.1 Purpose

Use this procedure to make the required intent types available to Service Management in NSP. This procedure is based on the procedure for installing an artifact bundle in the *NSP Network Automation Guide*.

For example, the reference procedure in NSP 23.11 is How do I install an artifact bundle?.

4.4.2 Steps

Download the required intent type bundles

1

Download the following artifact bundles from the NSP software delivery site.

- NSP product artifact bundle for Service Fulfillment
- NSP SR OS vendor-agnostic telemetry adaptation artifact bundle

Install the artifact bundle in NSP

2

Open **Artifacts**, **Artifact Bundles**.

3

Click **IMPORT & INSTALL**.

4

In the form that opens, drag and drop the zip file, or click **Browse** and navigate to the files on your system.

5

To install the artifact bundle immediately, click **IMPORT & INSTALL**. To import without installing, click **IMPORT**.

The chosen operation is triggered immediately. The artifact bundle status is updated to Imported or Installed when NSP has confirmed the status of all artifacts in the artifact bundle.

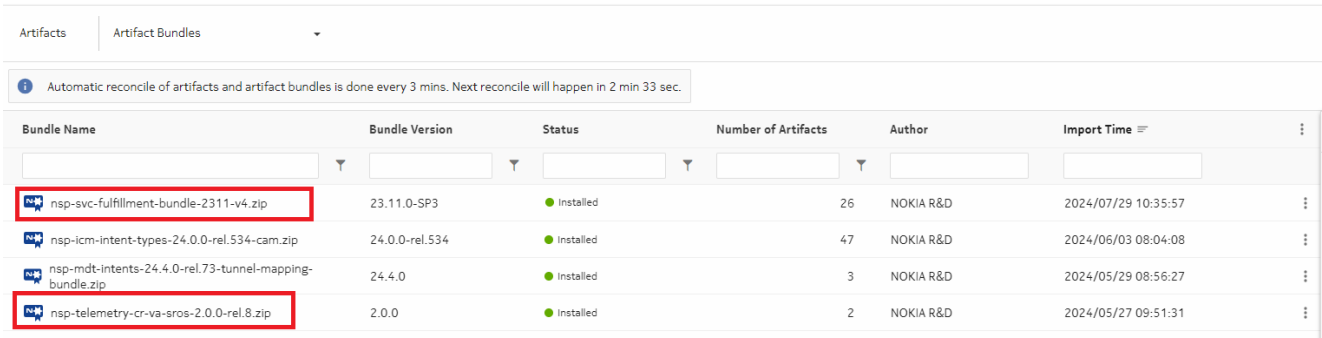
6

To install a bundle in Imported status, choose **Install bundle** from the ⋮ (Table row actions) menu.

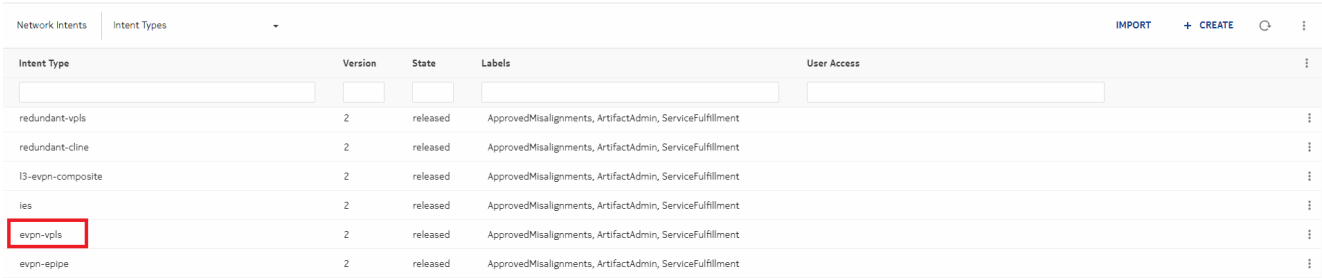
END OF STEPS

4.4.3 Result

The bundles appear in the **Artifacts**, **Artifact Bundles** view:



The service intent types, including the evpn-vpls intent type which is required for this use case, appear in the **Network Intents**, **Intent Types** view:



4.5 Configure user access to the required intent type

4.5.1 Purpose

Use this procedure to provide the user access to intent types. If the restricted Service Management user will be performing configuration tasks, this procedure must be performed.

This procedure is based on the procedure for configuring user access to an intent type in the *NSP Network Automation Guide*.

For example, the reference procedure in NSP Release 23.11 is How do I configure user access to an intent type?.

4.5.2 Steps

1

Log in to the NSP as an administrator.

2

Open **Network Intents**, **Intent Types**.

3

Select the `evpn-vpls` intent type.

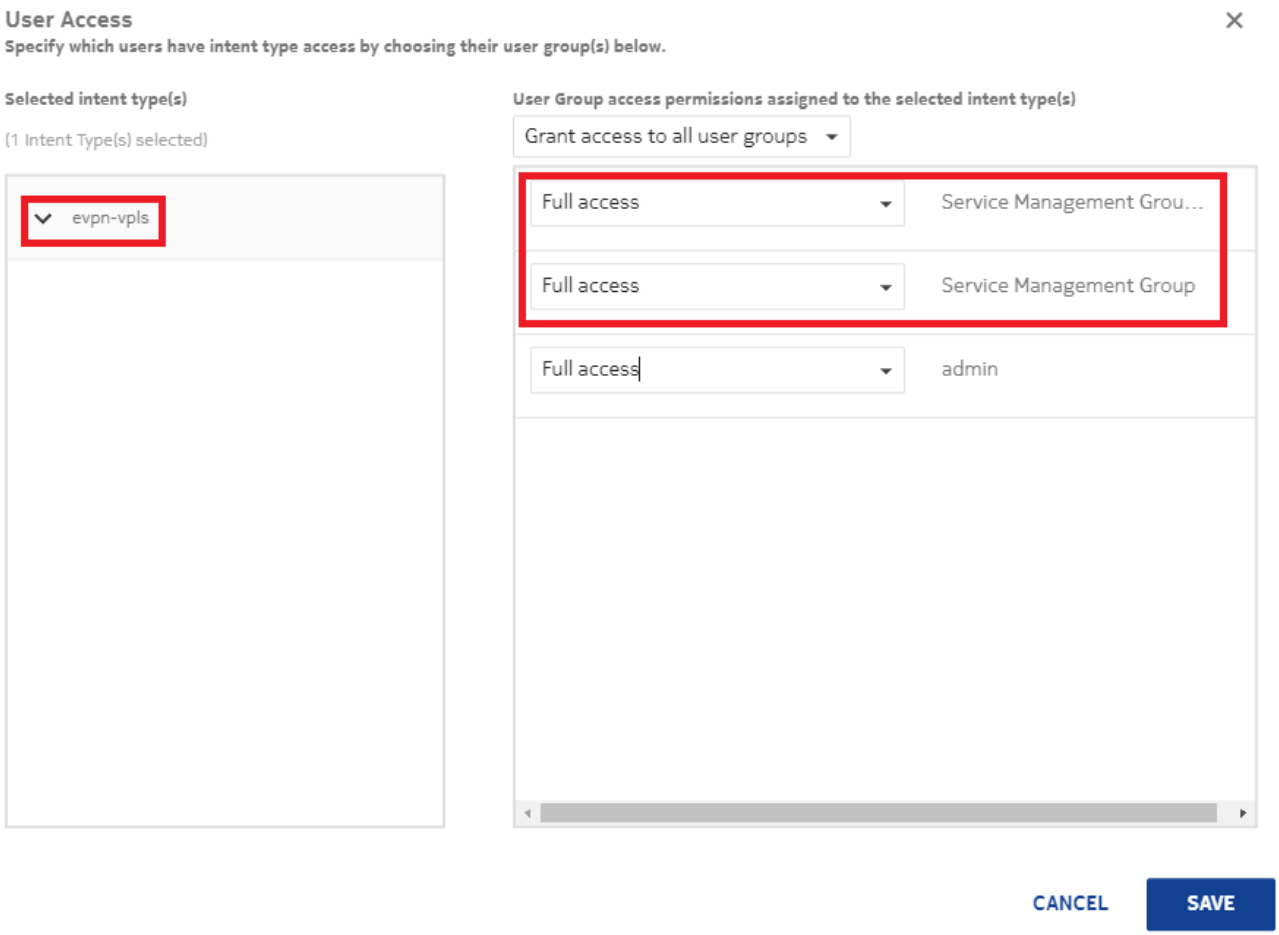
4

Click ⋮ (Table row actions), **User Access** to open the User Access form.

5

In the **User Access** form, choose **Grant access to all user groups** from the drop-down list at the top right of the form.

Choose **Full access** for the user group created in “Create a user group” (p. 54).



6

Click **SAVE**. The user access is updated.

END OF STEPS

Service configuration

4.6 Import the intent type into Service Management

4.6.1 Purpose

Use this procedure to import the intent types you obtained in 4.4 “Install the required artifact bundles” (p. 123) to the Service Management views. This procedure is based the procedure for importing an intent type into Service Management in the *NSP Service Management Guide*.

For example, the reference procedure in NSP Release 23.11 is How do I import an intent type into Service Management?.

The intent type required is `evpn-vpls`.

4.6.2 Steps

1

Log in to the NSP as the Service Management user.

2

From the **Service Management, Intent Type Catalogue** view, click **IMPORT**.

A list of previously defined intent types is displayed.

Note: Only intent types that have the Service Fulfillment label applied will be available to import.

3

Select the check boxes in-line with the intent types you wish to import and click **IMPORT**.

The intent type to import is `evpn-vpls`.

The intent type is imported into service management. This may take a few minutes.

Note: Selecting an imported intent type from the list opens the Info panel, which displays historical information such as the last time the intent type was updated, the last time it was imported, and the last time the modules that compose the intent type were revised.

END OF STEPS

4.7 Create an EVPN-VPLS service template

4.7.1 Purpose

Perform this procedure to create the template that Service Management will use in the creation of a EVPN-VPLS service.

This procedure is based on the procedure to create a service template in the *NSP Service Management Guide*.

For example, the reference procedure in NSP 23.11 is How do I create a service template?.

4.7.2 Steps

1

Log in to the NSP as the Service Management user.

2

From the **Service Management, Service Templates** view, select Service Polices from the drop-down menu and click **+ CREATE**.

The Create a service template form opens.

3

Configure the parameters, as required.

Parameter	Description
Template Name	Specifies the name of the template
Description	Describes the template
Service Intent Type	evpn-vpls
Intent Version	Specifies which version of the selected service intent type to associated with the template
State	Released
Config Form	default

4

Select NONE in the Default Service Category drop-down in the Bulk Association panel.

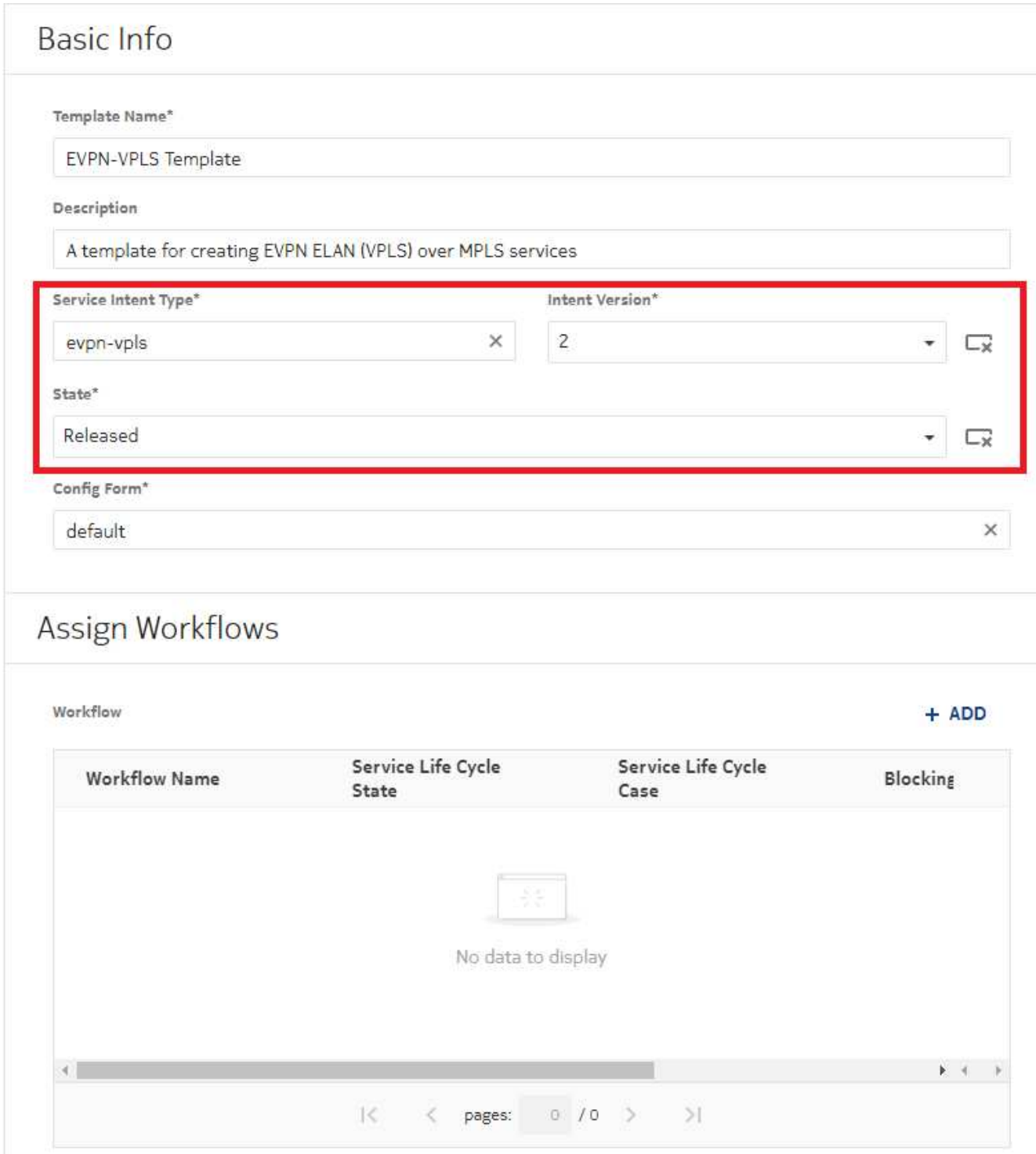
5

Click **CREATE**.

The service template is created.

END OF STEPS

4.7.3 Example creation form



4.8 Create an E-LAN EVPN (over MPLS) service

4.8.1 Purpose

Perform this procedure to create the service.

This procedure is based on the procedures for creating and auditing a service in the *NSP Service Management Guide*.

For example, the reference procedures in NSP Release 23.11 are:

- How do I create an EVPN VPLS service?
- How do I audit a service?

4.8.2 Steps

1

Log in to the NSP as the Service Management user.

2

From the **Service Management, Services** view, click **+ CREATE**.

The Select a service template to start form opens displaying a list of service templates.

3

Click on the EVPN-VPLS template from the list.

The Create Service form opens with the Template Name parameter populated.

4

Configure the parameters, as required:

- associate sites and endpoints to the service
- enter MPLS as the EVPN type
- select the transport protocols to use for tunnel binding
- associate the desired policies to the service, for example, QoS, CPU Protection

5

Click **DEPLOY** to create the service in a Deployed state.

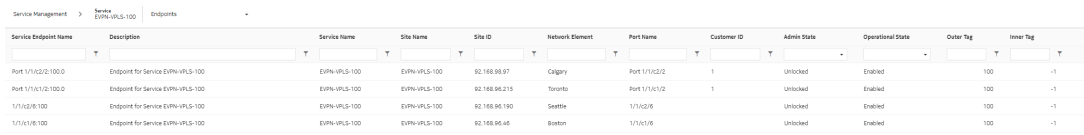
6

Verify the service details:

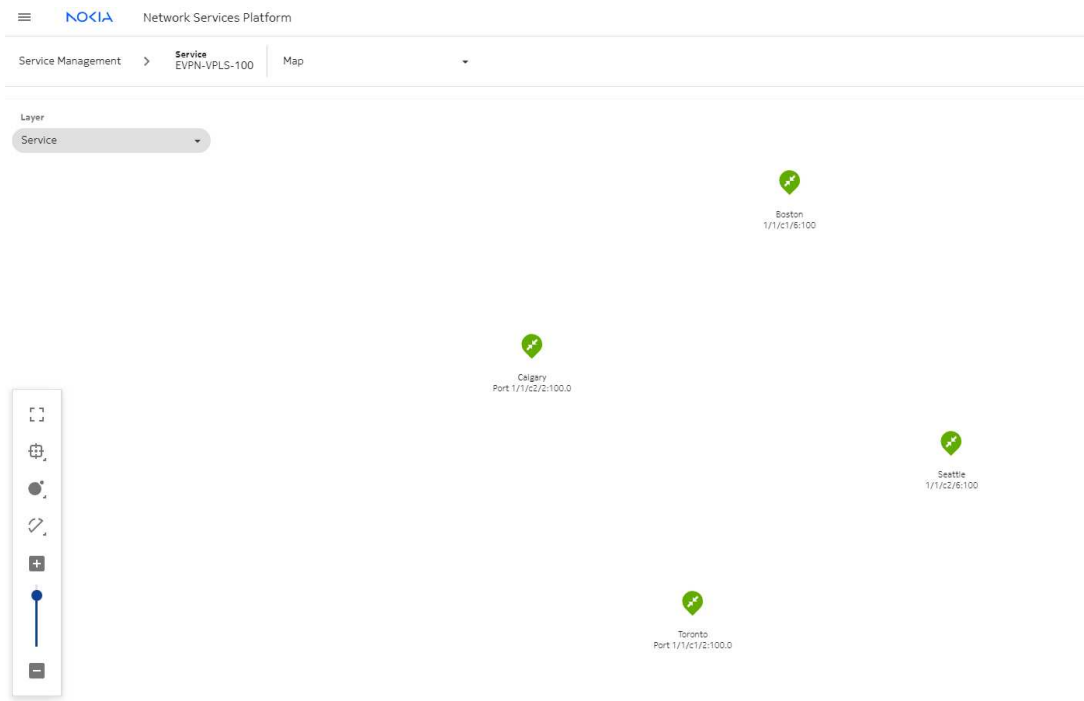
1. From the **Service Management, Services** view, select the new service and click ⋮ (Table row actions), **Service details**, **Components**.

   The list of sites in the service is displayed.

2. From the drop-down, select **Endpoints**.
3. Verify the configuration details for the endpoints.



4. From the drop-down, select **Map**.
5. Verify the details in the service map.



7

Perform an audit to verify that the service is deployed correctly:

1. From the **Service Management, Services** view, click ⋮ (Table row actions), **Audit config** in-line with any service.

   The service is audited.
2. If an Audit Result form appears, one or more attributes and/or objects are misaligned. Review the results and click **OK**.

   The Audit Result form closes.

8

If an object is misaligned, perform an align operation:

Click ⋮ (Table row actions), **Align**, and then either **Push to network** or **Pull from network** in-line with the previously audited service.

The service is synchronized with the network.

END OF STEPS

4.9 Modify the service configuration

4.9.1 Purpose

Perform this procedure to edit a service.

4.9.2 Steps

1

Log in to the NSP as the Service Management user.

2

From the **Service Management, Services** view, click ⋮ (Table row actions), **Edit** in-line with any service. The Edit service form opens.

3

Update the parameters as needed and click **DEPLOY**.

4

Verify the updated configuration.

END OF STEPS

4.10 Remove the service

4.10.1 Purpose

Perform this procedure to remove a service from the network. The service remains in the NSP database and can be re-deployed from the Services view.

4.10.2 Steps

1

Log in to the NSP as the Service Management user.

2

From the **Service Management, Services** view, click ⋮ (Table row actions), **Remove** in-line with any service.

3

In the form that opens, click **REMOVE** to confirm.

The Life Cycle State of the service is updated to Removed.

END OF STEPS

4.11 Delete the service

4.11.1 Purpose

Perform this procedure to delete a service. Before a service can be deleted it must be removed from the network; see 4.10 “Remove the service” (p. 132).

4.11.2 Steps

1

Log in to the NSP as the Service Management user.

2

From the **Service Management, Services** view, click ⋮ (Table row actions), **Delete** in-line with any service in the Removed state.

3

In the form that opens, click **DELETE** to confirm.

The service is deleted.

END OF STEPS

Optional procedures

4.12 Create an OAM test suite

4.12.1 Purpose

Use this optional procedure to create a collection of tests that are grouped together to allow for multiple tests to be executed together or run in sequence. The suite includes both the tests and, where applicable, instructions for running tests sequentially or in parallel. Test suites can provide improved automation for OAM testing.

The bundle of vendor agnostic custom resources must be imported and installed to support telemetry collection and OAM testing. The bundle is found on the NSP software delivery site, in the Adaptors folder along with your NE adaptor suite, for example, NSP → 23.11 → Adaptors → Nokia_SROS. Choose the zip file with va and cr in the filename, for example, `nsp-telemetry-cr-va-sros-1.0.0-rel.10.zip`.

This procedure is based on the procedure for creating a test suite in the *NSP Data Collection and Analysis Guide*.

For example, the reference procedure in NSP 23.11 is How do I create an OAM test suite?.

See also the procedure to install telemetry artifacts in the *NSP Data Collection and Analysis Guide* to verify that prerequisites for testing are in place. The reference procedure for this is in NSP 24.4: How do I install telemetry artifacts?.

4.12.2 Steps

1

Log in to the NSP as the Service Management user.

2

Open **Data Collection and Analysis Management**, **Test Suites**.

3

Click **+ SUITE**.

4

In the Generate OAM Tests form that opens, choose a Test type.

The list of templates in the Template field is updated based on your selection.

5

Choose a test template if needed.

If a template is not selected, an appropriate system template is automatically selected based on the value of the execute type field. If a template is selected, the value of the execute type field is imported from the template and is read-only in the form.

6

Add one or more entities:

1. Choose an entity type from the Entity type drop down.
2. Click **+ SELECT** to open a selection form.
3. Choose one or more entity objects from the list to add them to the Bin. Use the page selectors to navigate the list.
4. Verify the list of entity objects in the Bin and click **SELECT**.
5. To change the list of selected entities, repeat the previous steps to re-create the list.

7

Click on the Service field if applicable.

1. Select an attribute in the drop-down list, then enter values for that attribute in the field. As you type, the list is filtered for entities that match your input.
2. Click as required to add additional filter criteria.
3. Choose entities from the list and click **SELECT**.

8

Configure the test parameters as needed.

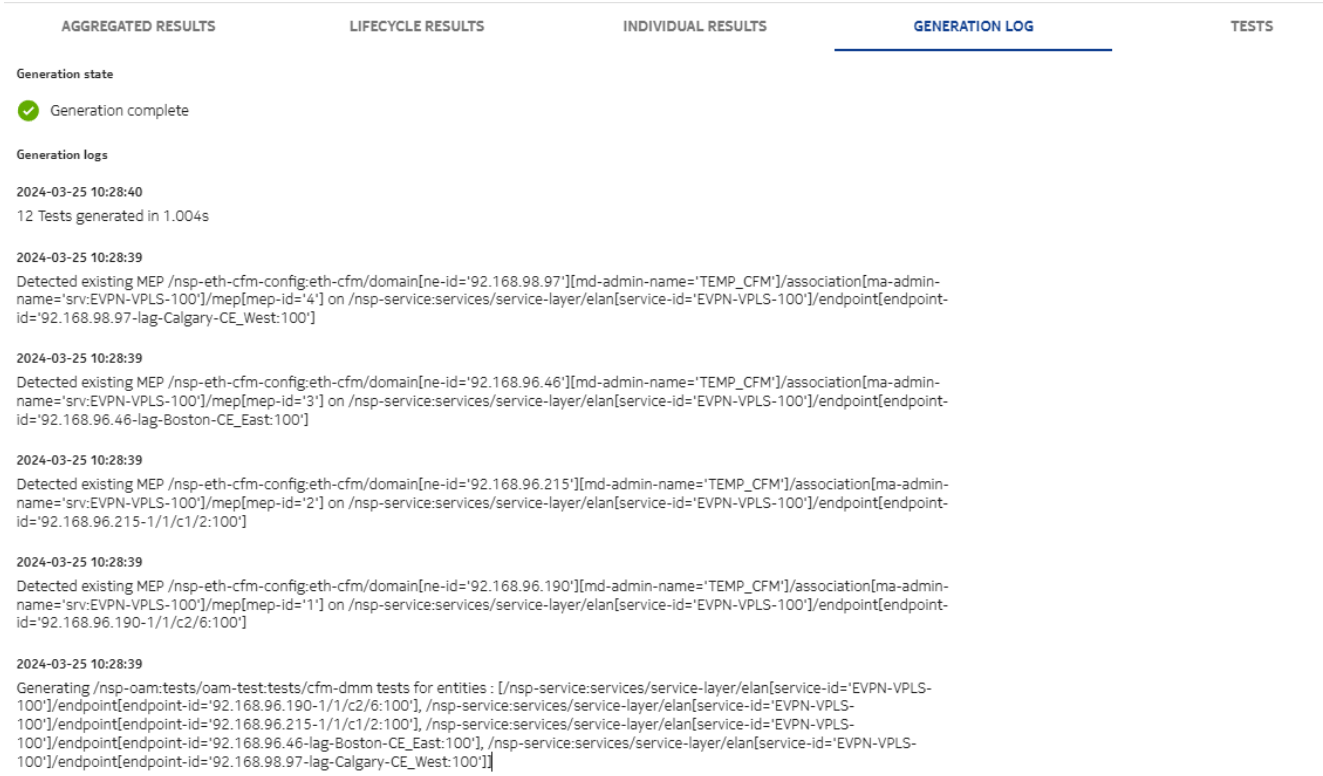
9

Generate the test suite.

a. To automatically execute the test suite after generation, enable Execute and click **GENERATE & EXECUTE**.

b. To create the test suite without automatically executing, disable Execute and click **GENERATE**.

The View Test Suite Details form opens. The Generation Log reports detection or creation of the objects required to run the test against the EVPN-VPLS service onto the network. In the following example, the CFM objects required for the tests were detected, and the DMM tests were deployed.



10

Click on the **LIFECYCLE RESULTS** tab to verify that the test suite was created successfully.

11

Click on the **TESTS** tab to view the list of tests in the suite.

12

Click **CLOSE** to return to the Test Suites view. The new test suite appears in the list.

END OF STEPS

4.13 Execute an OAM test suite

4.13.1 Purpose

Use this optional procedure to start all the tests in an OAM test suite. For on-demand test suites, there is no need to manually stop the test suite. The test suite will stop automatically based on the test duration value that is assigned to the on-demand delay streaming test template.

This procedure is based on the procedure for stopping or starting a test suite in the *NSP Data Collection and Analysis Guide*.

For example, the reference procedure in NSP 23.11 is How do I stop or start an OAM test suite?.

4.13.2 Steps

1

Log in to the NSP as the Service Management user.

2

Open **Data Collection and Analysis Management**, **Test Suites**.

3

Choose a test suite and click ⋮ (Table row actions), **Execute**.

4

In the form that opens, update the parameters if needed and click **EXECUTE**. The execution status is updated to Running.

Tip: Disable the **Publish results** parameter if you don't need results published to kafka. This may reduce processing impact.

5

To stop a test suite that is running, choose the test suite in the list and click ⋮ (Table row actions), **Stop**.

The test suite and all associated tests are stopped.

END OF STEPS

4.14 View OAM test results

4.14.1 Purpose

Use this optional procedure to view results of OAM tests. The examples in this procedure show a proactive Eth-CFM DMM test suite.

This procedure is based on the procedure to view test results in the NSP Data Collection and Analysis Guide.

For example, the reference procedure in NSP 23.11 is How do I view OAM test suite results?.

Note: After a test has executed, there is a brief processing delay before results are available. For tests that have just finished running, Nokia recommends that you wait a minimum of 5 s before viewing results.

4.14.2 Steps

1

Log in to the NSP as the Service Management user.

2

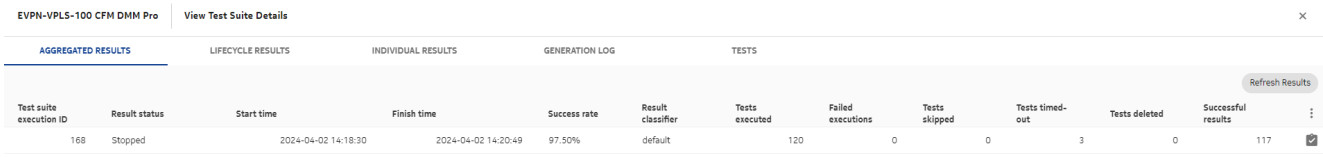
Open **Data Collection and Analysis Management**, **Test Suites**.

3

Choose the test suite and click ⋮ (Table row actions), **View Details**.

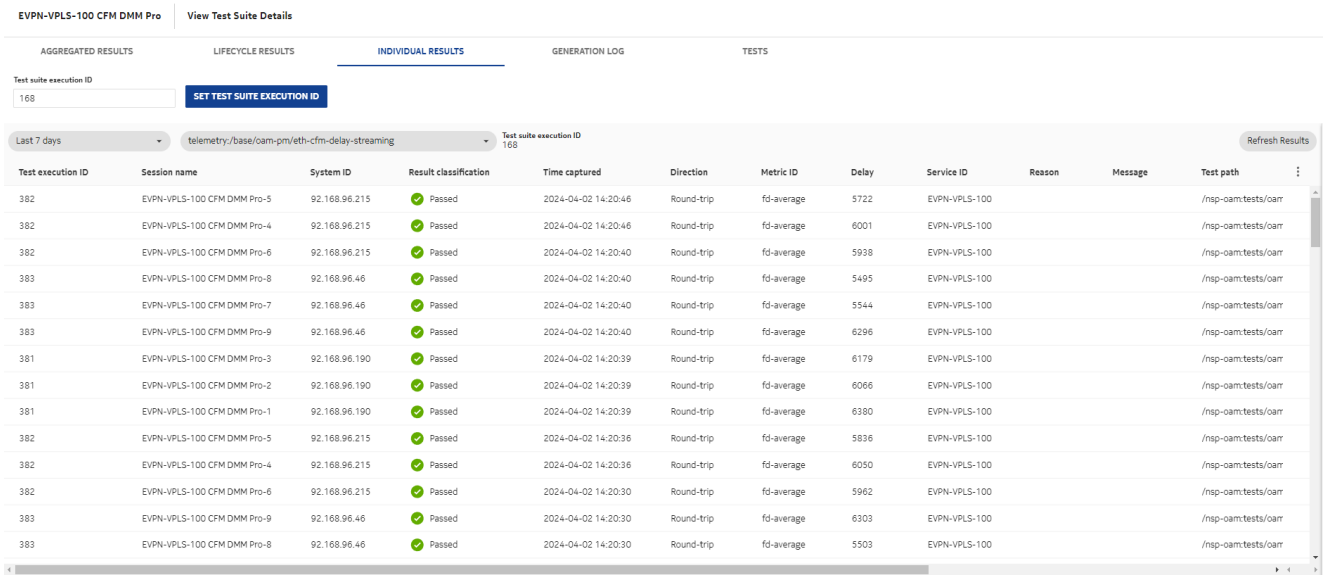
The View Test Suite Details page opens, showing the following:

Tab	Notes
AGGREGATED RESULTS	Each row of the aggregated results table corresponds to an execution of the test suite. Whenever the test suite is successfully started, a new aggregated results row is added. To view the individual results for a specific test suite execution, select the aggregated results row corresponding to the execution you are interested in and click **View individual results** .
LIFECYCLE RESULTS	The LIFECYCLE RESULTS table shows events from the execution of the test suite, such as stop and start timestamps and error events.
INDIVIDUAL RESULTS	The page displays the results of each test executed. By default, the results from the most recent test suite execution are shown, that is, the execution ID from the first row of the aggregated results table is chosen automatically. You can view results for other test suite executions by specifying another execution ID in the **Test suite execution ID** field or by returning to the AGGREGATED RESULTS tab and clicking **View individual results** . For more detailed information about a specific test, choose an execution and click **View Results** . **Note:** If a test suite was created from the NSP, the tests will all be the same type. If the test suite was created using RESTCONF, multiple test types could be included. To view results from a different type than is currently displayed, choose the telemetry type from the drop down list. See the **TESTS** tab for a list of tests in the suite.
GENERATION LOG	The page displays log information from the generation of the suite and tests.
TESTS	The page lists the test identifiers included in the suite. If the test suite is an on-demand suite, the TESTS tab shows the included tests grouped by stage. Stages are executed sequentially, but tests within each stage will be executed either sequentially or in parallel depending on how the stage is configured. For more detailed information about a specific test, double click on an execution or choose an execution and click **View Results** .



4

For more detailed information about a specific test, double click on an execution in the **TESTS** tab or choose an execution and click **View Results** .



For the example shown, the tests between service endpoints are passing, showing that there are no issues with service connectivity.

END OF STEPS

4.15 Delete an OAM test suite

4.15.1 Purpose

Use this optional procedure to delete an OAM test suite and all its associated tests from the NSP UI. This action cannot be undone.

Note: Test suites cannot be edited in the NSP UI.

4.15.2 Steps

1

Log in to the NSP as the Service Management user.

2

Open **Data Collection and Analysis Management**, **Test Suites**.

3

Choose a test suite and click ⋮ (Table row actions), **Delete**.

4

Click **DELETE** in the confirmation dialog to confirm.

The test suite and its tests are deleted from the NSP.

END OF STEPS

4.16 Create a telemetry subscription

4.16.1 Purpose

Perform this procedure to set up telemetry collection.

This procedure is based on the procedure for managing subscriptions in the *NSP Data Collection and Analysis Guide*.

For example, the reference procedure in NSP 23.11 is How do I manage subscriptions?.

CAUTION

Service Disruption

The name of an object, including subscriptions, baselines, indicators, templates, and chart profiles, cannot contain a semicolon (;) or backslash (\).

The use of these characters in an object identifier will result in corrupted data that must be deleted by Nokia support.

4.16.2 Steps

1

Log in to the NSP as the Service Management user.

2

Open **Data Collection and Analysis Management**, **Subscriptions**.

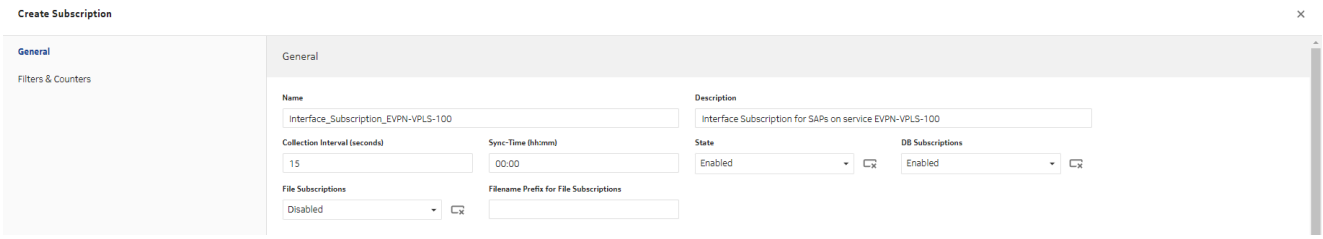
3

Click **+ SUBSCRIPTION**.

4

In the Create Subscription form that opens, configure the General parameters as needed:

- Enable database (DB) subscriptions as needed to save subscription information to the NSP database. For subscription data to be available to Analytics, the auxiliary database must be deployed.
- The subscription is enabled by default: it will start running immediately.



5

Configure filters and counters:

1. In the **Object Filter** field, enter filtering information as needed to filter the collected data.

   As you type, the field provides suggestions for available filters to match your input and identifies incorrect syntax.
2. Enter information in the Telemetry Type field. As you type, the field filters for available telemetry types to match your input.

   Choose the telemetry type you need from the list of matches.
3. When you enter a telemetry type, all counters are enabled by default.

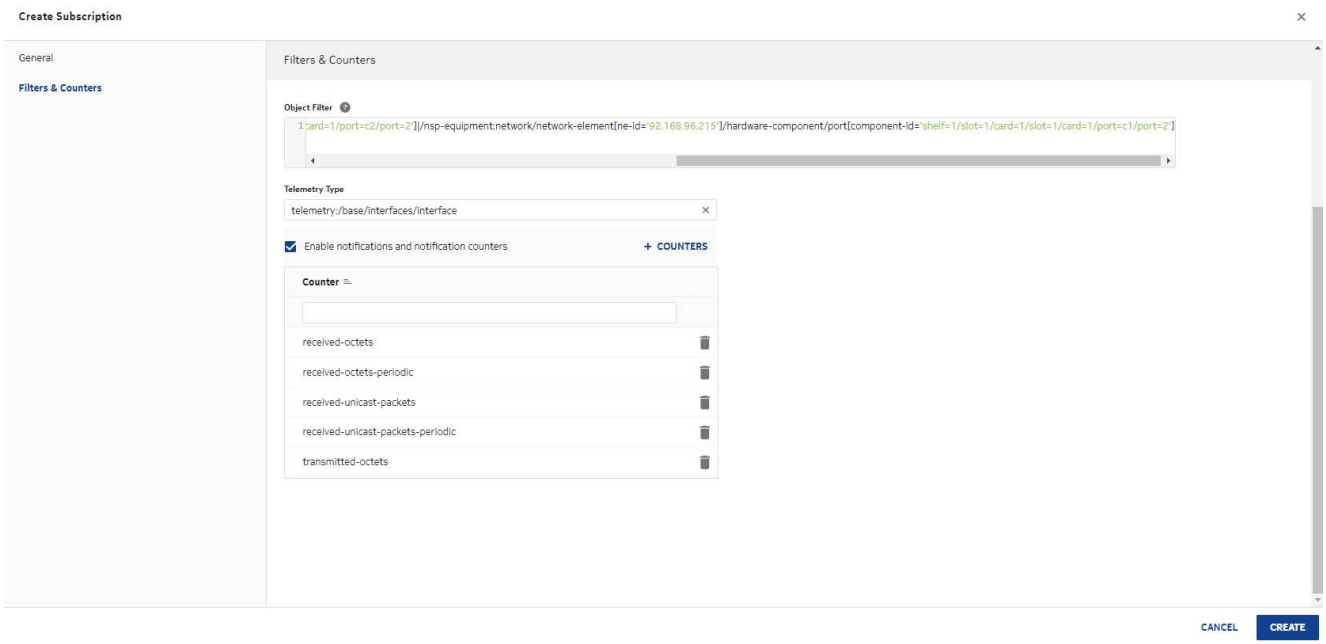
   To customize the counters, enable the **Enable notifications and notification counters** check box.

   Click **Remove** to remove a counter.

   Click **+ COUNTERS** to add a counter that was removed.

This example includes the following:

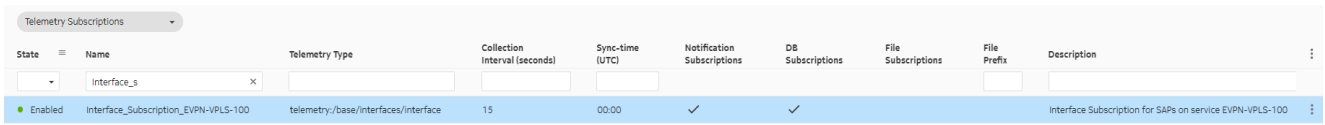
- Telemetry Type: telemetry:/base/interfaces/interface
- Counters:
  - received-octets-periodic
  - received-octets
  - received-unicast-packets
  - received-unicast-packets-periodic
  - transmitted-octets
- Object Filter (2 port objects used by two endpoints of the service): /nsp-equipment:network/network-element[ne-id='92.168.98.97']/hardware-component/port[component-id='shelf=1/slot=1/card=1/slot



6

Click **CREATE**.

The subscription appears in the subscriptions list.



Port throughput statistics from the sites and NEs found by the object filter are received and processed every 15 s (see Collection Interval value). The statistics will remain in the NSP database for a configured period of time, as defined in the ageout policy.

END OF STEPS

4.17 Modify a telemetry subscription

4.17.1 Purpose

Use this optional procedure to make changes to a telemetry subscription, for example, to change the list of counters.

This procedure is based on the procedure for managing subscriptions in the *NSP Data Collection and Analysis Guide*.

For example, the reference procedure in NSP 23.11 is How do I manage subscriptions?.

4.17.2 Steps

1

Log in to the NSP as the Service Management user.

2

Open **Data Collection and Analysis Management**, **Subscriptions**.

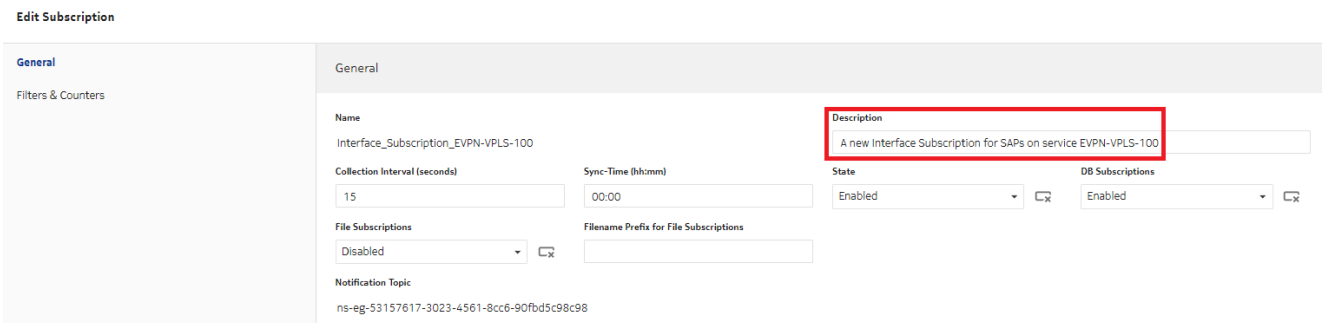
3

Choose a subscription and click ⋮ (Table row actions), **Edit**.

4

In the form that opens, update the parameters as needed.

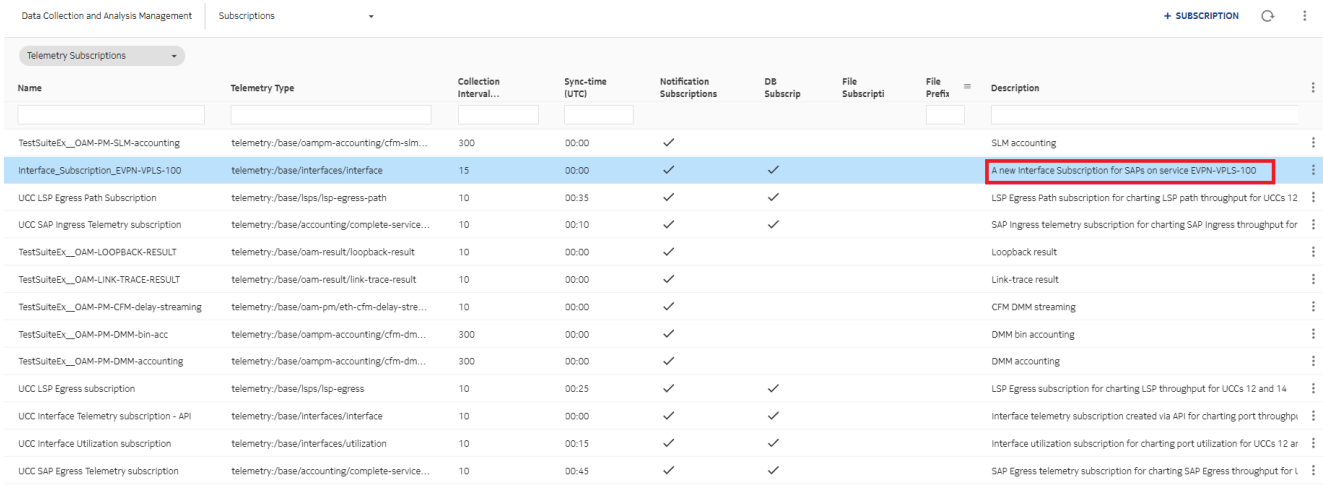
In this example, a new description is provided.



5

Click **UPDATE**

The updated subscription appears in the list.



END OF STEPS

4.18 Plot telemetry statistics

4.18.1 Purpose

Use this optional procedure to plot a chart of telemetry statistics. The steps for charting any type of telemetry statistic are the same: the example shows port throughput statistics.

This procedure is based on the procedure to plot a telemetry chart in the *NSP Data Collection and Analysis Guide*.

For example, the reference procedure in NSP 23.11 is How do I plot a telemetry chart?.

4.18.2 Before you begin

When you create a telemetry chart, you configure a telemetry filter. For historical data to be displayed, the data must be available in the database; see 4.16 “Create a telemetry subscription” (p. 140).

Charts are created by streaming to the plotter: historical data is queried and streamed to the plotter, then real time telemetry subscriptions are created and the data from these subscriptions is streamed to the plotter.

Data Collection and Analysis Visualizations times out if telemetry data is not received. The time-out limit is either double the collection interval or two minutes, whichever is greater.

Chart limit

Up to 10 objects can be charted at a time. The number of objects is the number of resources returned by the object filter, multiplied by the number of counters.

If your object filter returns one resource, for example, one NE, you can chart up to 10 counters for the resource.

4.18.3 Steps

CAUTION

Service Disruption

The name of an object, including subscriptions, baselines, indicators, templates, and chart profiles, cannot contain a semicolon (;) or backslash (\).

The use of these characters in an object identifier will result in corrupted data that must be deleted by Nokia support.

Create a chart

1

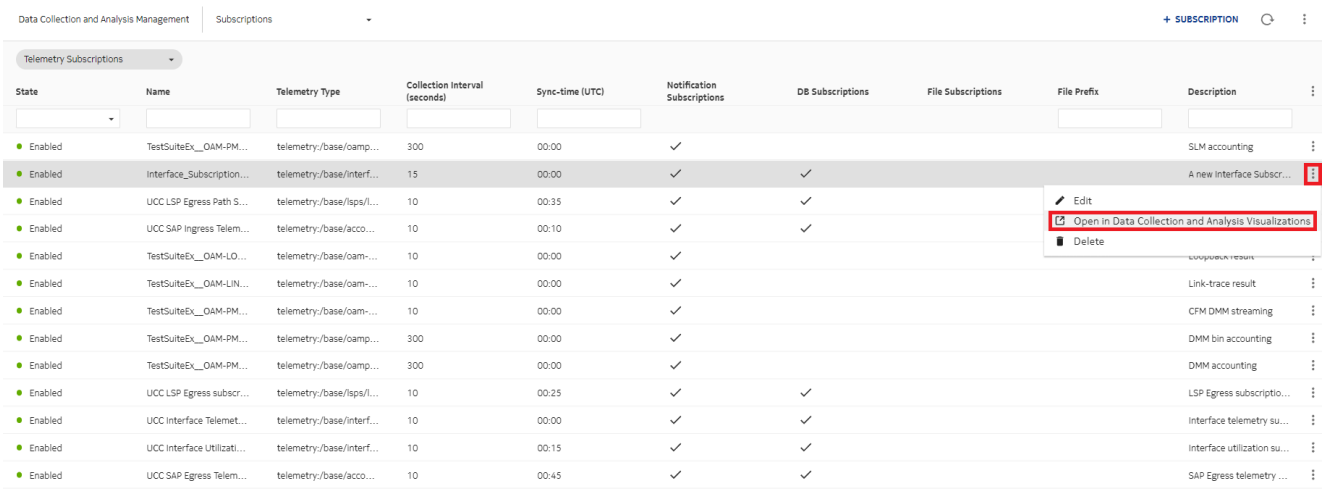
Log in to the NSP as the Service Management user.

2

Open **Data Collection and Analysis Management**, **Subscriptions**.

3

Choose a subscription and click ⋮ (Table row actions), **Open in Data Collection and Analysis Visualizations**.



The **Data Collection and Analysis Visualizations** view opens in a new browser tab.

4

In the window that opens, configure the parameters in the top panel:

1. Configure the **Collection Interval** parameter. If you are using NFM-P telemetry data, verify that the collection interval is long enough to allow time for Visualizations to receive the data before timing out.
2. From the **Time Range** drop-down list, choose the amount of historical data to display.
3. Click **Combine charts** to plot data from multiple data series on the same chart.

5

Click **+ DEFINITION**.

The telemetry and resource filter definition panels are displayed.

6

Enter information in the **Telemetry Type** field. As you type, the field filters for available telemetry types to match your input.

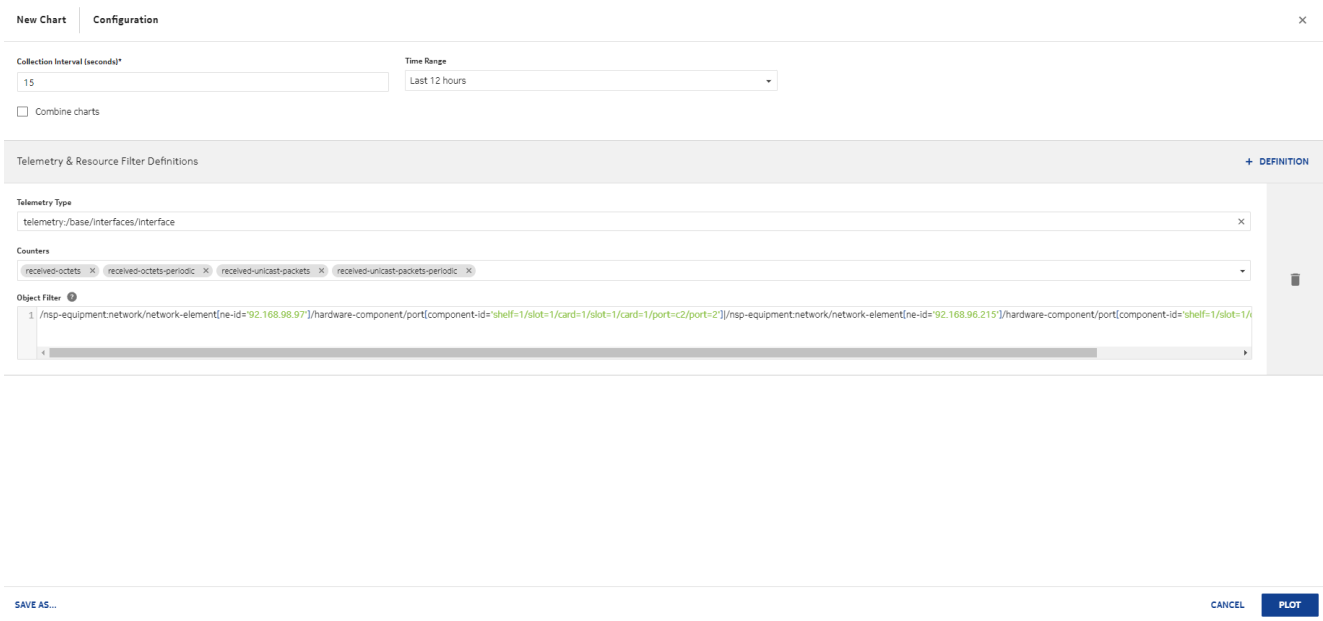
Choose the telemetry type from the list of matches.

7

Choose counters to display from the **Counters** drop-down list.

8

In the **Object Filter** field, enter filtering information to filter the collected data.



9

Save the configuration as a chart:

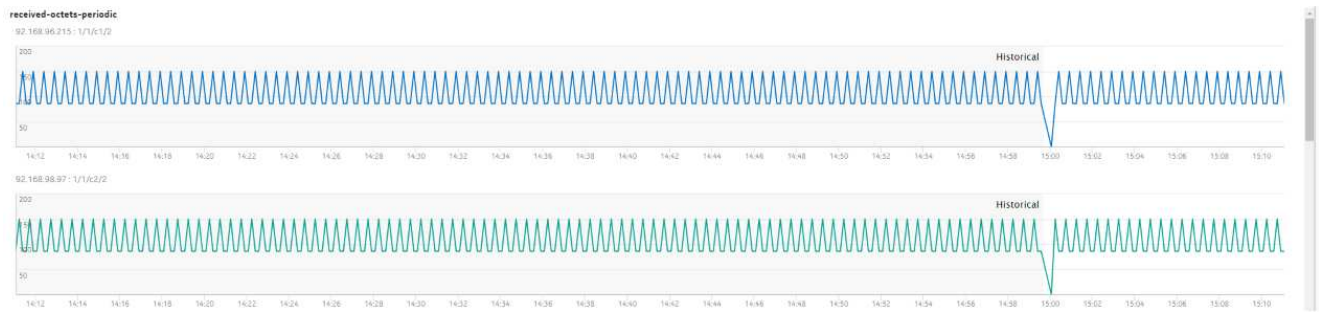
1. Click **SAVE AS**.
2. In the window that opens, enter a name for the chart and add a description.
3. Click **SAVE**.

In a few seconds, the chart is added to the list.

10

Click **PLOT**.

NSP begins plotting data. In a few moments, data will be visualized in the chart.



11

Close the chart window. The saved telemetry chart appears in the list, ready to be plotted again as needed.

END OF STEPS

4.19 Delete a telemetry subscription

4.19.1 Purpose

Use this optional procedure to remove a telemetry subscription from the NSP. This action cannot be undone.

This procedure is based on the procedure for managing subscriptions in the *NSP Data Collection and Analysis Guide*.

For example, the reference procedure in NSP 23.11 is How do I manage subscriptions?.

4.19.2 Steps

1

Log in to the NSP as the Service Management user.

2

Open **Data Collection and Analysis Management**, **Subscriptions**.

3

To delete a subscription:

Choose a subscription and click ⋮ (Table row actions), **Delete**.

The subscription is removed immediately.

Note: Removing a subscription does not remove data from the database. The data collected by the subscription is retained according to the database retention policy.

END OF STEPS

5 UCC-15: L3 VPN

5.1 Overview

5.1.1 Purpose

This chapter describes the process required to configure an L3 VPN service over MPLS on SR OS NEs using NSP Service Management.

Configuration examples in this chapter show NSP Release 24.4 and SR OS 23.7.R2 NEs.

The following artifact bundles were used to test this use case:

- nsp-icm-intents-24.4.0-cam-bundle.zip
- nsp-svc-fulfillment-bundle-2404.zip

See the NSP and NE documentation for more information.

5.1.2 Contents

Preparation

5.2 Prerequisites

5.2.1 Network configuration prerequisites

Before services can be configured and managed in NSP, the network configuration prerequisites must be met. The following table describes the requirements that can apply to service use cases, and indicates whether each prerequisite is required for this process.

Where an NSP intent type is not available, CLI or MD-CLI must be used to perform configuration on the device.

Prerequisite	Documentation reference	Notes
Mandatory for L3 VPN		
GRPC configuration 1. Generate security certificates 2. Configure security and enable GRPC on all devices 3. Apply security certificates on all devices	See SR TLS information here in the SR OS 24.3 R1 documentation: TLS	—
Netconf/SNMP provisioning: enable NETCONF and SNMP protocols on all devices	For more information about SNMP and NETCONF with SR OS, see SNMP and NETCONF in the *SR OS 24.3 R1 System Management Guide*.	—
NSP installation	Pathway for NSP system installation in the *NSP Installation and Upgrade Guide* How do I enable TLS for telemetry and gNMI on_change support? in the *NSP System Administrator Guide*.	Include the following in your deployment: • Feature packs: - platform-baseServices - platform-pluggableNetworkAdaptation - platform-loggingMonitoring - serviceActivationAndConfiguration-intentBasedServiceFulfillment - networkInfrastructureManagement-basicManagement - networkInfrastructureManagement-deviceConfig • Adaptor suites: - sros-common - sros-oc-logical-inventory - sros-23-7-r1

Prerequisite	Documentation reference	Notes
Download the required artifact bundles from the NSP software delivery site: • NSP predefined set for ICM (device configuration) • NSP product artifact bundle for Service Fulfillment	How do I install an artifact bundle? in the *NSP Network Automation Guide*	—
Device discovery	Pathway for device discovery in the *NSP Classic Management User Guide* How do I discover devices? in the *NSP Device Management Guide* Nokia Developer Portal for information about FTP mediation policy creation using API.	—
Cards and MDAs provisioning	ICM process in the *NSP Device Management Guide* for more information about using the Device Configuration views, and the other procedures in the *NSP Device Management Guide* for further detail. See the NSP Device Configuration Intent Type Catalog for information about this and other device configuration intent types developed by Nokia.	The intent type required for this configuration is icm-equipment-card-mda.
Connectors and Ports provisioning		The intent types required for this configuration are: • icm-equipment-port-connector • icm-equipment-port-ethernet
OSPF/ISIS	CLI Reference Guides for SR OS	—
LDPs, MPLS and RSVP configuration	CLI Reference Guides for SR OS	For LDP to be operational, the IPv4 and IPv6 bindings must be configured manually using CLI.
Interfaces Provisioning	How do I create a physical configuration deployment? in the *NSP Device Management Guide*.	The intent type required for this configuration is icm-router-network-interface
BGP/EVPN	How do I create a logical configuration deployment? in the *NSP Device Management Guide*.	The intent type required for this configuration is icm-router-bgp_group
Customer creation	How do I create a logical configuration deployment? in the *NSP Device Management Guide*.	The intent type required for this configuration is icm-service-customer
Optional		

Prerequisite	Documentation reference	Notes
Optional items to include in your NSP deployment	Pathway for NSP system installation in the *NSP Installation and Upgrade Guide*	• Optional feature packs: - pathControlAndOptimization - multilayerDiscoveryAndVisualization - NSP Analytics: Network Operations Analytics feature package with the networkOperationsAnalytics-analyticsReporting installation option - NSP Baseline Analytics: networkOperationsAnalytics-baselineAnalytics - networkInfrastructureManagement-performanceIndicatorsAndAlerts • VSR/NRC • An AuxDB • An NFM-P instance
Telemetry/OAM	*NSP Data Collection and Analysis Guide*	• NSP SR OS vendor-agnostic telemetry adaptation artifact bundle • networkInfrastructureManagement-gnmiTelemetry feature pack
Segment Routing	CLI Reference Guides for SR OS	—
Scheduler QoS Policies	How do I create a logical configuration deployment? in the *NSP Device Management Guide*.	The intent types required for this configuration are: • icm-qos-schedulerpolicy-srqos • icm-qos-network-srqos • icm-qos-sapingress-srqos • icm-qos-sapegress-srqos
Network QoS Policies configuration		
SAP QoS Policies configuration		
PCEP configuration	CLI Reference Guides for VSR-NRC	Most of the connections required for PCEP are established during previous configuration steps.
LAGs and MC-LAG creation	How do I create a logical configuration deployment? in the *NSP Device Management Guide*.	The intent types required for this configuration are: • icm-logical-lag-access • icm-logical-mc_lag-access

5.3 Optional: create a restricted Service Management user

5.3.1 Purpose

Perform this optional procedure to create a user with access only to specified NSP functions.

Procedures in this chapter can be performed by the restricted user, or by an administrator.

This procedure is based on the procedures for the following in the *NSP System Administrator Guide* and *NSP Network Automation Guide*:

- Configuring a role
- Configuring a user group
- Creating an NSP local user
- Enabling User Access Control
- Configuring user access to an intent type

For example, the reference procedures in NSP Release 24.4 are:

- How do I configure a role?
- How do I configure a user group?
- How do I create an NSP local user?
- How do I enable User Access Control?
- How do I configure user access to an intent type?

If a restricted user has already been created, verify that the user has the required permissions, as shown in Step 6.

5.3.2 Steps

Create a role

1

Log in to the NSP as an administrator.

2

Open **Users and Security**.

3

Select **Roles** from the drop-down list on the toolbar.

4

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

5

In the Identification panel, specify a role name and description.

The Role Name and Description fields can employ **only** the following special characters: `@ - _`.

The Role Name string must not contain *any* spaces, including a leading or trailing space.

6

To assign NSP functional access to the role, go to the Action Permissions panel and select an access level from the drop-down list for each NSP GUI you want to include in the role.

Action permissions group item	Permissions	Notes
Service Fulfillment	Read / Write / Execute	—
Network Intents	Read: Manage Intents	Required to import intent types into Service Management
Workflows	Read	Required to create service and tunnel templates
DCA Management	Read / Write / Execute	Optional: Only required for creating and plotting telemetry subscriptions
OAM Tests	Read / Write / Execute	Optional: Only required for generating and executing OAM tests

7

To assign network resource access to the role, go to the Resource Groups Access panel. (For a detailed explanation of the Resource Groups Access panel, see How do I set network resource access levels? in the *NSP System Administrator Guide*.)

You can assign resource group access globally, to resource group categories, to individual resource groups, or a combination of these. For service management it is recommended to grant access to all equipment and all services:

- **Access To All Equipment** assigns full permissions on all NE resource groups and port resource groups to the role.
- **Access To All Services** assigns full permissions on all service resource groups to the role.

8

Click **CREATE** to save your changes and return to the Roles list.

Create a user group

9

Open **Users and Security**.

10

Select **User Groups** from the drop-down list on the toolbar.

11

Click **+ Create User Group**. The Create User Group form opens.

12

Specify a group name and description in the **Identification** panel.

The user group name you specify here must exactly match a corresponding user group name returned by your user repository.

The User Group Name and Description fields can employ **only** the following special characters: `@ - _`.

The User Group Name string must not contain spaces, including a leading or trailing space.

13

To assign user roles to the group, click **+ Add Roles** on the Roles panel. The Add Roles form opens.

14

Enable the check box for the role you configured in "Create a role" (p. 154) and click **Done**. The role is added to the Selected Roles list.

15

Click **CREATE** to save your changes and return to the User Groups list.

Create a user

16

Open **Users and Security**.

17

Select **Users** from the drop-down list on the toolbar.

18

Click **+ Create User**.

19

In the Create User form, specify user identification information for the account in the Identification section. The **Username** and **User Group** fields are mandatory.

Note: Any uppercase characters in the username are saved as lowercase.

The **Username** value:

- can be 1 to 40 characters long
- cannot include a space
- cannot have a leading or trailing space
- can include only the following special characters:
  - **@** (at sign)
  - **-** (hyphen)
  - **_** (underscore)
  - **.** (period)

20

In the **User Group** field, select the user group you created in “Create a user group” (p. 155).

21

In the Password section, specify and confirm a password for the user account.

- If you want this password to be temporary, enable the **Force User to Change Password** option. The new user will be forced to change their password when they first login to NSP.
- Enable the **Show Password** option to see the password characters as you type them.
- Click on the **Password Requirements** link to view a list of minimum security requirements for the password.

22

Click **CREATE**.

Enable user access control

23

Open **Users and Security**, **User Groups**.

24

Click ⋮ **More Actions**, **Settings**.

25

In the Access Control Settings form, enable the **NSP User Access Control** option.

26

Click **SAVE** to enable access control.

END OF STEPS

5.4 Install the required artifact bundles

5.4.1 Purpose

Use this procedure to make the required intent types available to Service Management in NSP. This procedure is based on the procedure for installing an artifact bundle in the *NSP Network Automation Guide*.

For example, the reference procedure in NSP 24.4 is How do I install an artifact bundle?.

5.4.2 Steps

Download the required intent type bundles

1

Download the following artifact bundles from the NSP software delivery site.

- NSP product artifact bundle for Service Fulfillment
- NSP SR OS vendor-agnostic telemetry adaptation artifact bundle

Install the artifact bundle in NSP

2

Open **Artifacts**, **Artifact Bundles**.

3

Click **IMPORT & INSTALL**.

4

In the form that opens, drag and drop the zip file, or click **Browse** and navigate to the files on your system.

5

To install the artifact bundle immediately, click **IMPORT & INSTALL**. To import without installing, click **IMPORT**.

The chosen operation is triggered immediately. The artifact bundle status is updated to Imported or Installed when NSP has confirmed the status of all artifacts in the artifact bundle.

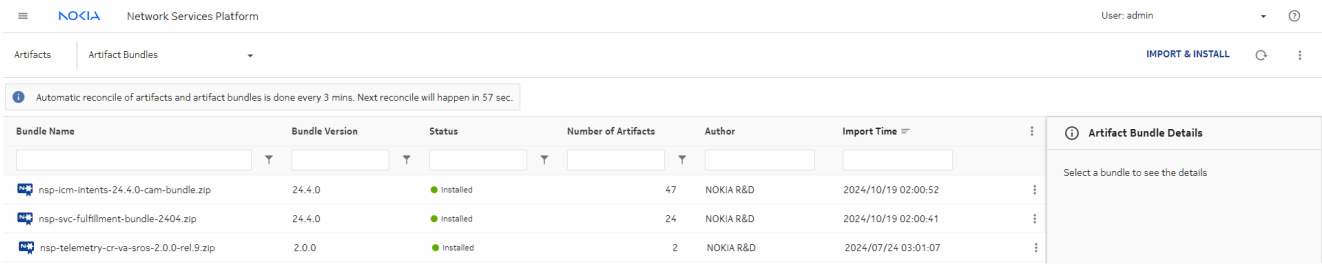
6

To install a bundle in Imported status, choose **Install bundle** from the ⋮ (Table row actions) menu.

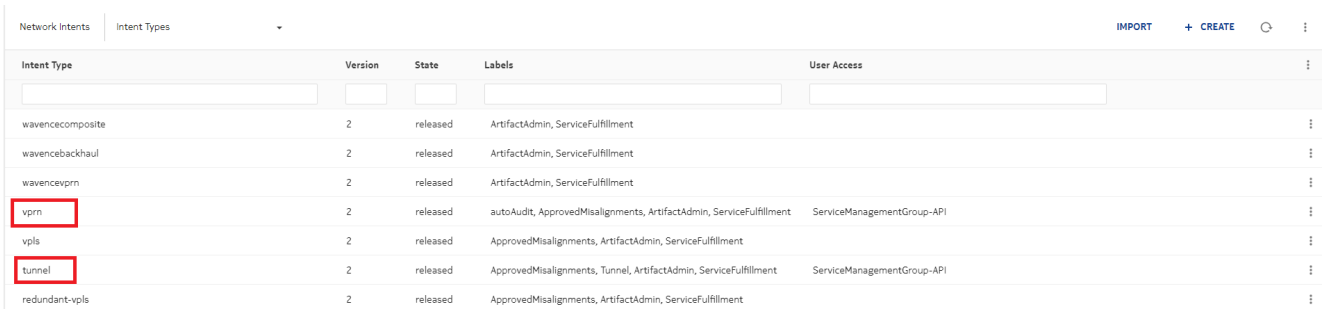
END OF STEPS

5.4.3 Result

The bundles appear in the **Artifacts**, **Artifact Bundles** view:



The service intent types, including the `tunnel` and `vprn` intent types which are required for this use case, appear in the **Network Intents**, **Intent Types** view.



5.5 Configure user access to the required intent type

5.5.1 Purpose

Use this procedure to provide the user access to intent types. If the restricted Service Management user will be performing configuration tasks, this procedure must be performed.

This procedure is based on the procedure for configuring user access to an intent type in the *NSP Network Automation Guide*.

For example, the reference procedure in NSP Release 24.4 is How do I configure user access to an intent type?.

5.5.2 Steps

1

Log in to the NSP as an administrator.

2

Open **Network Intents**, **Intent Types**.

3

Ctrl+click to select the `tunnel` and `vprn` intent types.

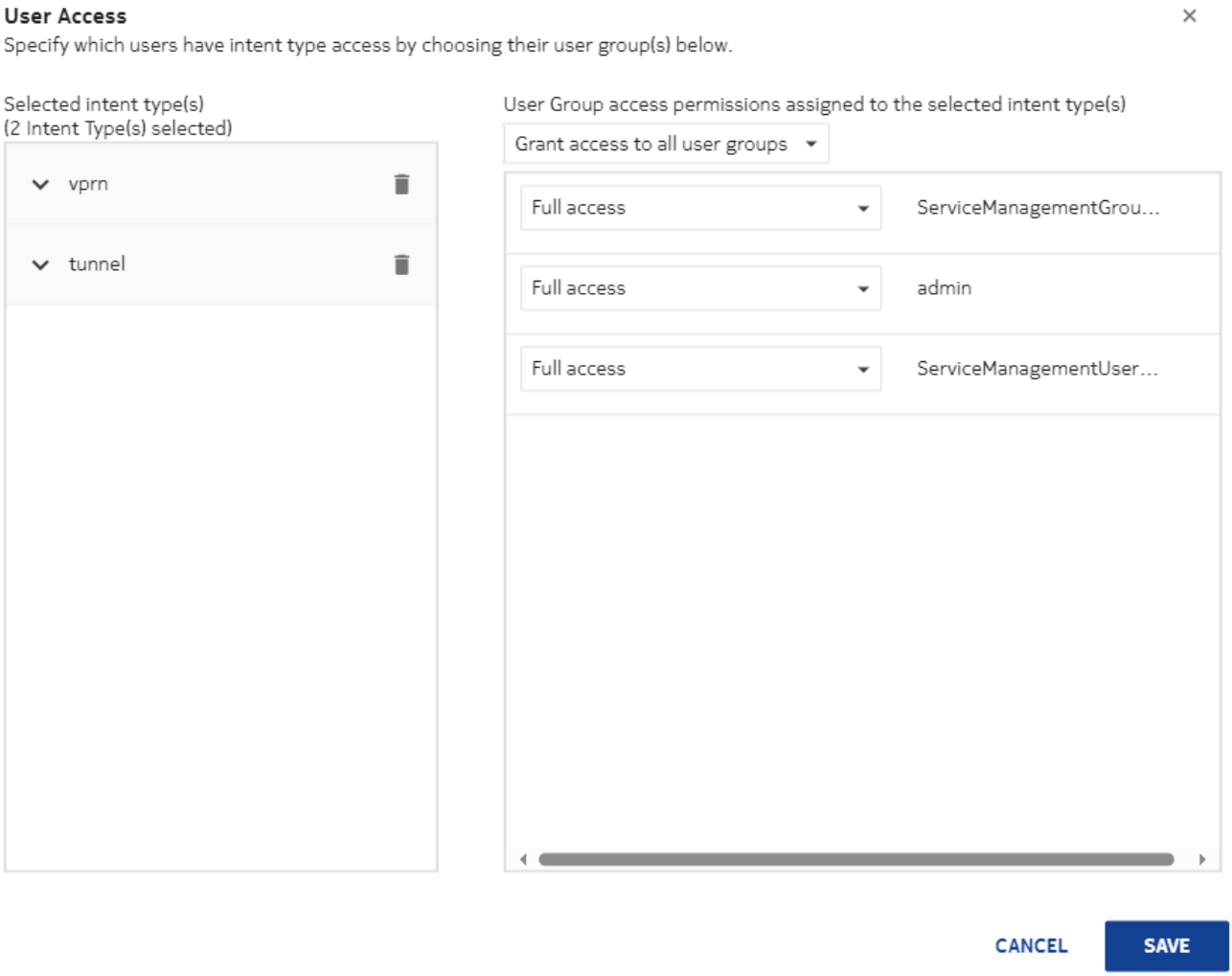
4

Click **User Access** at the top right of the view to open the User Access form.

5

In the **User Access** form, choose **Grant access to all user groups** from the drop-down list at the top right of the form.

Choose **Full access** for the user group created in “Create a user group” (p. 155).



6

Click **SAVE**. The user access is updated.

END OF STEPS

Service configuration

5.6 Import the intent type into Service Management

5.6.1 Purpose

Use this procedure to import the intent types you obtained in 5.4 “Install the required artifact bundles” (p. 157) to the Service Management views. This procedure is based the procedure for importing an intent type into Service Management in the *NSP Service Management Guide*.

For example, the reference procedure in NSP Release 24.4 is How do I import an intent type into Service Management?.

The intent types required are `tunnel` and `vprn`.

5.6.2 Steps

1

Log in to the NSP as the Service Management user.

2

From the **Service Management, Intent Type Catalogue** view, click **IMPORT**.

A list of previously defined intent types is displayed.

Note: Only intent types that have the Service Fulfillment label applied will be available to import.

3

Select the check boxes in-line with the intent types you wish to import and click **IMPORT**.

The intent types to import are `tunnel` and `vprn`.

The intent types are imported into service management. This may take a few minutes.

Note: Selecting an imported intent type from the list opens the Info panel, which displays historical information such as the last time the intent type was updated, the last time it was imported, and the last time the modules that compose the intent type were revised.

END OF STEPS

5.7 Create a service tunnel template

5.7.1 Purpose

Perform this procedure to create the template that Service Management will use in the creation of a service tunnel.

This procedure is based on the procedure to create a tunnel template in the *NSP Service Management Guide*.

For example, the reference procedure in NSP 24.4 is How do I create a tunnel template?.

5.7.2 Steps

1

Log in to the NSP as the Service Management user.

2

From the **Service Management, Tunnel Templates** view, click **+ CREATE**.

The Create a tunnel template form opens.

3

Configure the parameters, as required.

Parameter	Description
Template Name	Specifies the name of the template
Description	Describes the template
Tunnel Intent Type	`tunnel`
Intent Version	Specifies which version of the selected tunnel intent type to associated with the template
State	Released
Config Form	Specifies the form to be used for the template

4

If required, click **+ ADD** in the Workflows panel to add workflows to the tunnel template.

The Add Workflows form opens.

5

Configure the parameters, as required:

Parameter	Description
Workflow Name	Specifies the workflow to be executed
Service Life Cycle State	Specifies the life cycle state of the tunnel that will trigger workflow execution
Service Life Cycle Case	Specifies the case, Success or Fail, relative to the life cycle state that will trigger workflow execution
Blocking	Specifies whether unsuccessful execution of the workflow will prevent tunnel life cycle state changes
Workflow Execution Timeout (seconds)	Specifies the length of time, in seconds, that unsuccessful execution of the workflow will prevent tunnel life cycle state changes

6

Click **ADD**.

The Add Workflows form closes and the workflow is added to the tunnel template.

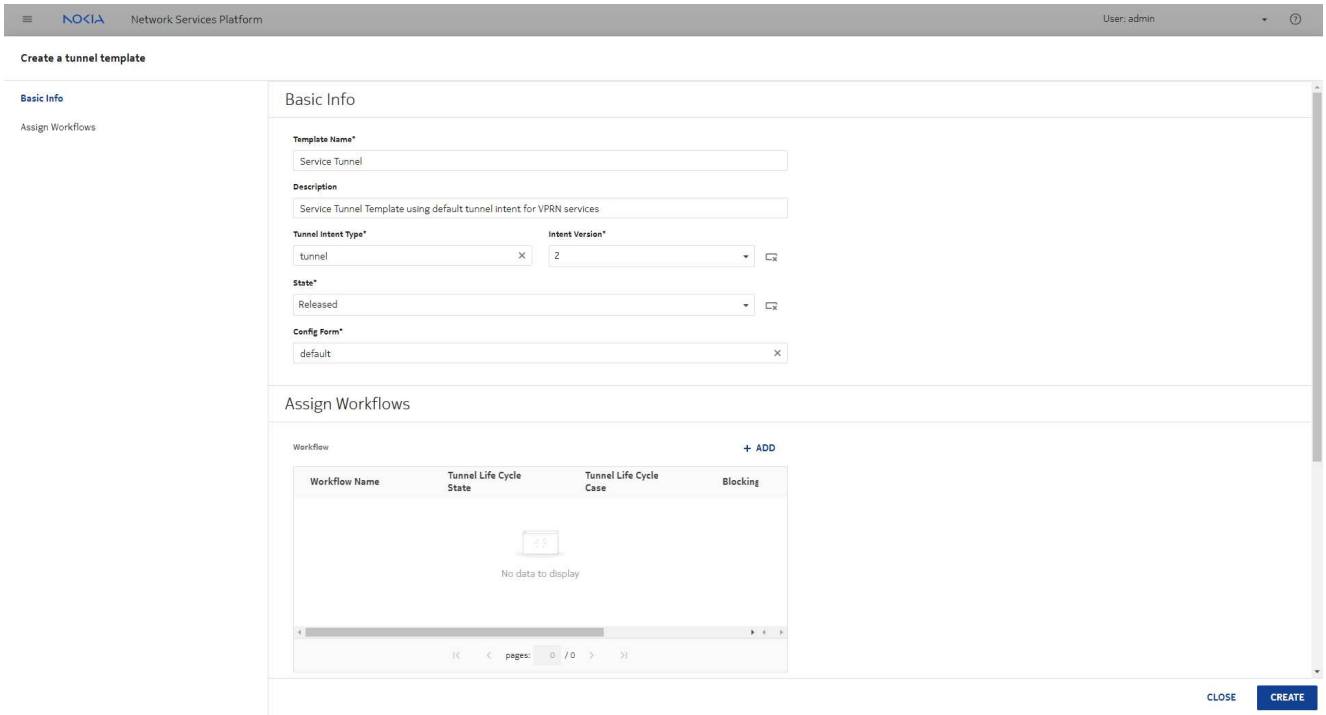
7

Click **CREATE**.

The tunnel template is created.

END OF STEPS

5.7.3 Example creation form without a workflow



5.8 Create and deploy service tunnels to the network

5.8.1 Purpose

Perform this procedure to create service tunnels. The creation of service tunnels is a prerequisite to creation of a service.

This procedure is based on the procedures for creating and auditing a service tunnel in the *NSP Service Management Guide*.

For example, the reference procedures in NSP Release 24.4 are:

- How do I create a service tunnel?
- How do I audit a service tunnel?

5.8.2 Steps

1

Log in to the NSP as the Service Management user.

2

Open the tunnel creation form:

1. From the **Service Management, Service Tunnels** view, click **+ CREATE**.

   The Select a tunnel template to start form opens displaying a list of tunnel templates.
2. Choose the template you created in 5.7 “Create a service tunnel template” (p. 162).

   The Create Tunnel form opens with the Template Name parameter populated.

3

Configure the parameters, as required.

4

If the Transport Type parameter was set to MPLS, configure the required parameters.

5

Configure the required Hello parameters.

6

If the Transport Type parameter was set to GRE, configure the Allow Fragmentation parameter (if required), which specifies whether or not fragmentation will be allowed for the tunnel.

7

Configure the required parameters.

8

Click **DEPLOY** to create the tunnel in a Deployed state.

9

Perform an audit to verify that the tunnel is deployed correctly:

1. From the **Service Management, Service Tunnels** view, click on the service tunnel in the list, then expand the Alignment State section in the info panel and click **AUDIT CONFIG**.

   The service tunnel is audited.
2. If an Audit Result form appears, one or more attributes and/or objects are misaligned. Review the results and click **OK**.

The Audit Result form closes.

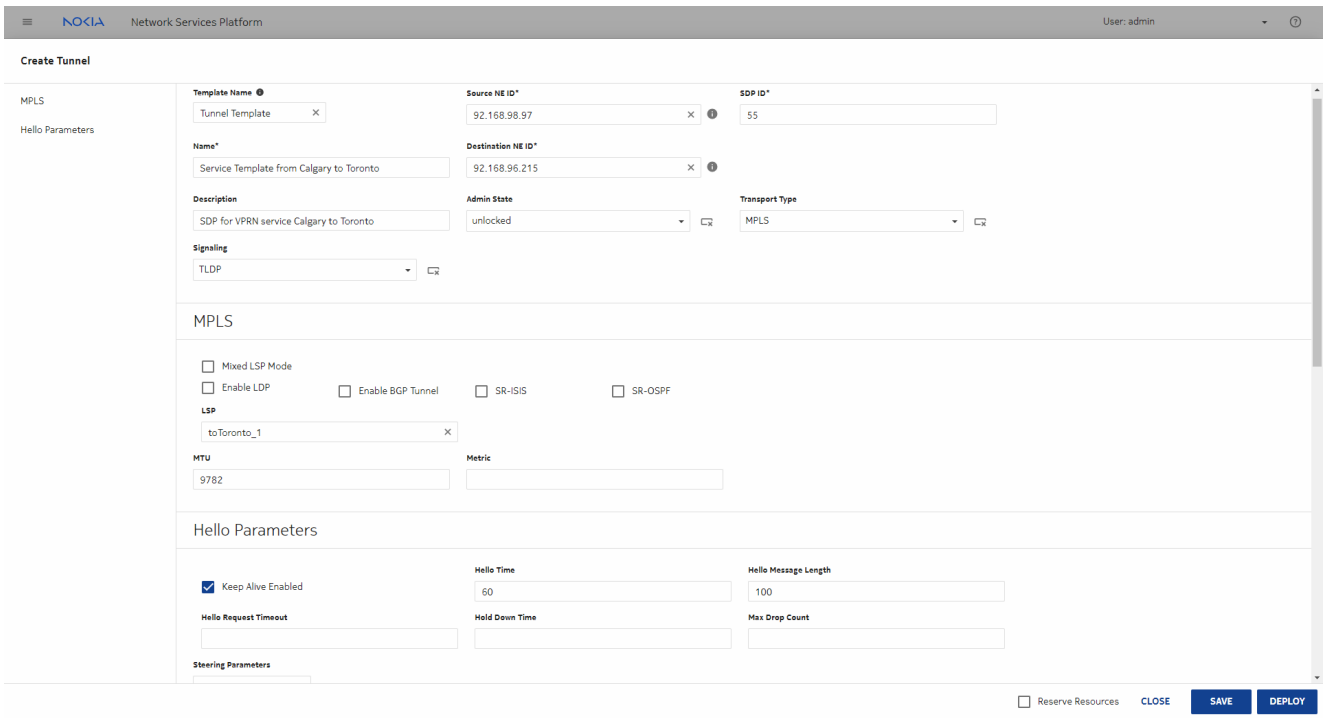
10

To revert to the expected value of a misaligned attribute, or to restore a misaligned object, click ⋮ (Table row actions), **Align**, **Push To Network** in-line with the previously audited service tunnel.

The service tunnel is synchronized with the network.

END OF STEPS

5.8.3 Tunnel creation example



5.9 Create a VPRN service template

5.9.1 Purpose

Perform this procedure to create the template that Service Management will use in the creation of a VPRN (L3 VPN) service.

This procedure is based on the procedure to create a service template in the *NSP Service Management Guide*.

For example, the reference procedure in NSP 24.4 is How do I create a service template?.

5.9.2 Steps

1

Log in to the NSP as the Service Management user.

2

From the **Service Management, Service Templates** view, click **+ CREATE**.

The Create a service template form opens.

3

Configure the parameters, as required.

Parameter	Description
Template Name	Specifies the name of the template
Description	Describes the template
Service Intent Type	vprn
Intent Version	Specifies which version of the selected service intent type to associated with the template
State	Released
Config Form	default

4

Select L3VPN in the Default Service Category drop-down in the Bulk Association panel.

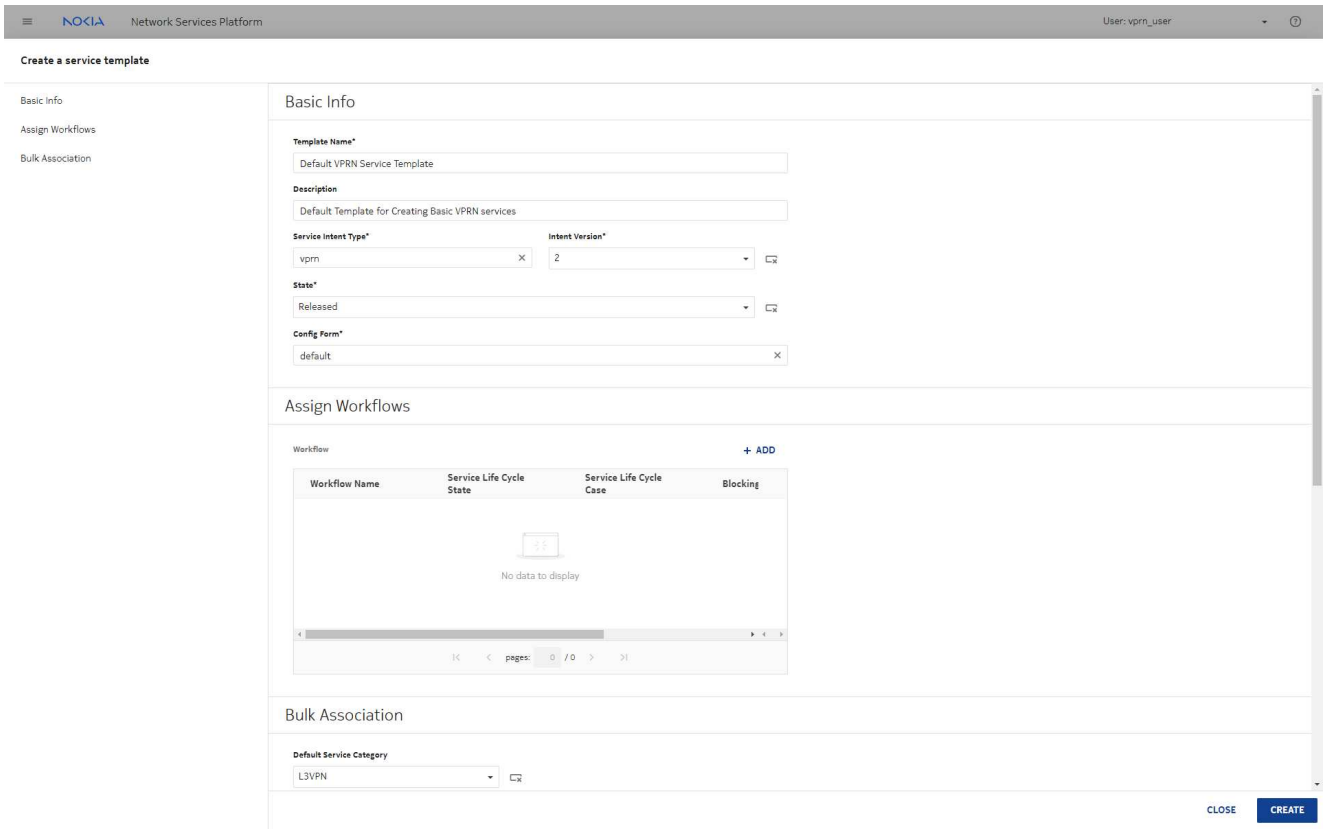
5

Click **CREATE**.

The service template is created.

END OF STEPS

5.9.3 Example creation form



5.10 Create and deploy a VPRN service to the network

5.10.1 Purpose

Perform this procedure to create the service.

This procedure is based on the procedures for creating and auditing a service in the *NSP Service Management Guide*.

For example, the reference procedures in NSP Release 24.4 are:

- How do I create a L3 VPN service?
- How do I audit a service?

5.10.2 Steps

1

Log in to the NSP as the Service Management user.

2

From the **Service Management, Services** view, click **+ CREATE**.

The Select a service template to start form opens displaying a list of service templates.

3

Click on a VPRN service template from the list, such as the one created in 5.9 “Create a VPRN service template” (p. 166).

The Create Service form opens with the Template Name parameter populated.

4

In the Site Details panel, click **+ ADD**.

The Add Site form opens.

5

Configure the parameters, as required:

Parameter	Description
Device ID	Specifies the assigned queue group redirect list
VRF Name	Specifies the name of the VRF
Description	Describes the VRF
MTU	Specifies the service MTU
NE Service ID	Specifies the NE service ID
Autonomous System	Specifies the AS number advertised to peers for this router
ECMP	Specifies the maximum number of ECMP routes
Router ID	Specifies the unique identifier of the router in the autonomous system
Export Inactive BGP	Specifies whether or not to export the best BGP route as a VPN-IP route, even if inactive due to a preferred route from another PE
Route Distinguisher Type	Specifies the route distinguisher type
Route Distinguisher	Specifies the route distinguisher
VRF Import	Specifies the name of the VRF import policy
VRF Export	Specifies the name of the VRF export policy

Parameter	Description
BGP IPVPN Admin State	Specifies the BGP IPVPN administrative state. Only applicable on SROS 21.x devices.
Route Target (click **+ ADD**)	
Target Type	Specifies the type of route target
Target Value	Specifies the route target value

6

In the Auto Bind Tunnel panel, configure the required parameters:

Parameter	Description
Resolution	Specifies the MBS of the queue
Enforce Strict Tunnel Tagging	Specifies the PIR rate of the queue
Resolution Filter	
BGP	Specifies the BGP type for the autobind tunnel
GRE	Specifies whether GRE is enabled for the autobind tunnel
LDP	Specifies whether LDP is enabled for the autobind tunnel
RSVP	Specifies whether RSVP is enabled for the autobind tunnel
SR ISIS	Specifies whether SR ISIS is enabled for the autobind tunnel
SR OSPF	Specifies whether SR OSPF is enabled for the autobind tunnel
SR-TE	Specifies whether SR-TE is enabled for the autobind tunnel
UDP	Specifies the UDP type for the autobind tunnel
RIB API	Specifies whether RIB API is enabled for the autobind tunnel
MPLS Fwd Policy	Specifies whether MPLS Fwd policy is enabled for the autobind tunnel
SR Policy	Specifies whether SR policy is enabled for the autobind tunnel

Parameter	Description
SR OSPF3	Specifies whether segment routing OSPF3 is used for next hop resolution

7

As required, click the **Enable EVPN MPLS** check box in the BGP EVPN panel and configure the parameters:

Parameter	Description
Admin State	Specifies the administrative state of BGP-EVPN MPLS
Route Distinguisher	Specifies the route distinguisher
VRF Import Policy	Specifies the name of the VRF import policy
VRF Export Policy	Specifies the name of the VRF export policy
Route Target (click **+ ADD**)	
Target Type	Specifies the type of route target
Target Value	Specifies the route target value
Auto Bind Tunnel	
Resolution	Specifies the MBS of the queue
Enforce Strict Tunnel Tagging	Specifies the PIR rate of the queue
Resolution Filter	
BGP	Specifies the BGP type for the autobind tunnel
GRE	Specifies whether GRE is enabled for the autobind tunnel
LDP	Specifies whether LDP is enabled for the autobind tunnel
RSVP	Specifies whether RSVP is enabled for the autobind tunnel
SR ISIS	Specifies whether SR ISIS is enabled for the autobind tunnel
SR OSPF	Specifies whether SR OSPF is enabled for the autobind tunnel
SR-TE	Specifies whether SR-TE is enabled for the autobind tunnel

Parameter	Description
UDP	Specifies the UDP type for the autobind tunnel
RIB API	Specifies whether RIB API is enabled for the autobind tunnel
MPLS Fwd Policy	Specifies whether MPLS Fwd policy is enabled for the autobind tunnel
SR Policy	Specifies whether SR policy is enabled for the autobind tunnel
SR OSPF3	Specifies whether segment routing OSPF3 is used for next hop resolution

8

As required, click the **Enable Maximum Routes** check box in the BGP EVPN panel and configure the parameters:

Parameter	Description
Maximum IPv4 Routes	
Max Number of Routes	Specifies the maximum number of IPv4 routes that are configured on the virtual router
Log Only	Specifies whether action is taken when the maximum number of IPv4 routes, held within a VRF context, is reached
Mid Route Threshold	Specifies the mid-level water marker for the number of IPv4 routes that the VRF holds
Maximum IPv6 Routes	
Max Number of Routes	Specifies the maximum number of IPv6 routes that are configured on the virtual router
Log Only	Specifies whether action is taken when the maximum number of IPv6 routes, held within a VRF context, is reached
Mid Route Threshold	Specifies the mid-level water marker for the number of IPv6 routes that the VRF holds
Mc Maximum Routes	
Max Number of MCast Routes	Specifies the maximum number of multicast routes that are configured on the virtual router

Parameter	Description
Log Only	Specifies whether action is taken when the maximum number of multicast routes, held within a VRF context, is reached
Mid Route MCast Threshold	Specifies the mid-level water marker for the number of multicast routes that the VRF holds

9

Configure the parameters in the Route Aggregation panel, as required:

Parameter	Description
Aggregate (click **+ADD**)	
Ip Prefix	Specifies the destination IP address prefix of the aggregate route
Community	Specifies the community name that is added to the aggregate route
Summary Only	Specifies whether or not to advertise the aggregate route only
Next Hop	Specifies the address of the next hop
SNMP Community	Specifies the SNMP v1/v2c community name associated with the VPRN
Ignore NH Metric	Specifies whether or not to ignore next hop metric

10

Configure the parameters in the Bgp Vpn Backup panel, as required:

Parameter	Description
Ipv4	Specifies whether or not to allow BGP-VPN to be used as backup for IPv4 prefixes
Ipv6	Specifies whether or not to allow BGP-VPN to be used as backup for IPv6 prefixes

11

At the bottom of the form, configure the parameters, as required:

Parameter	Description
Enable eBGP	Specifies whether or not the eBGP protocol is enabled
Enable Static Route	Specifies whether or not the static routes protocol is enabled
Enable IS-IS	Specifies whether or not the IS-IS protocol is enabled
Enable BGP	Specifies whether or not the BGP protocol is enabled
Enable RIP	Specifies whether or not the RIP protocol is enabled

12

In the Interface Details panel, click **+ ADD**.

The Add Interface form opens.

13

Configure the parameters, as required:

Parameter	Description
Interface Name	Specifies the name of the interface
Description	Describes the interface
Administrative State	Specifies the administrative state of the interface
Loopback	Specifies whether to use the interface as a loopback interface
IP MTU	Specifies the interface IP MTU
Ingress Stats	Specifies whether or not ingress statistics will be collected
Monitor Oper Group	Specifies the operational group to monitor

14

If IS-IS was enabled in Step 11, configure the required parameters in the IS-IS panel:

Parameter	Description
IS-IS Instance	Specifies the instance ID for the IS-IS instance
Admin State	Specifies the administrative state of the IS-IS interface
Passive	Specifies the passive interface
Level Capability	Specifies the routing level for instance
Interface Type	Specifies the interface type; broadcast or point-to-point

15

If OSPF was enabled in Step 11, configure the required parameters in the OSPF panel:

Parameter	Description
Area ID	Specifies the area identifier
Interface Type	Specifies the interface type, broadcast or point-to-point
Passive	Specifies whether to allow the interface to be advertised as an OSPF interface without running the OSPF protocol
Metric	Specifies the explicit route cost metric that is applied to the interface
Authentication Key	Specifies the authentication key
Authentication Type	Specifies the authentication type used on OSPF interface
BFD Liveliness (click check box)	
Remain Down On Failure	Specifies whether or not to force adjacency down on failure until session returns
Admin State	Specifies the administrative state of the OSPF interface

16

If RIP was enabled in Step 11, configure the required parameter in the RIP panel:

Parameter	Description
Group Name	Specifies the group name

17

In the IPv4 panel, configure the required parameters:

Parameter	Description
Primary	
Address	Specifies the primary IPv4 address assigned to the interface
Prefix Length	Specifies the primary IPv4 address prefix length
Secondary (**+ ADD**)	
Address	Specifies the secondary IPv4 address assigned to the interface
Prefix Length	Specifies the secondary IPv4 address prefix length
VRRP (**+ ADD**)	
Virtual Router ID	Specifies the virtual router identifier for the VRRP virtual router instance
Passive	Specifies whether or not to suppress the processing of VRRP advertisement messages
Admin State	Specifies the administrative state of VRRP
Backup	Specifies virtual router IP addresses for the interface
Priority	Specifies the base priority for the VRRP
Message Interval	Specifies the interval for sending VRRP advertisement messages
Ping Reply	Specifies whether or not to allow non-owner master to reply to ICMP echo requests
Traceroute Reply	Specifies whether or not to allow non-owner master to reply to traceroute requests
Standby Forwarding	Specifies whether or not to allow standby router to forward traffic

Parameter	Description
Neighbor Discovery	
Timeout	Specifies the timeout for an ARP entry learned on the interface
Retry Timer	Specifies the ARP retry interval
Learn Unsolicited	Specifies whether or not to learn new entries from any received NA message
Proactive Refresh	Specifies whether or not to send a single refresh message before entry timeout
Populate	Specifies whether or not to allow static and dynamic hosts to be populated in system ARP cache
Local Proxy Arp	Specifies whether or not to enable local proxy ARP on interface
Proxy Arp Policy	Specifies the proxy ARP policy name
Populate (click **+ADD**)	
Route Type	Specifies the type of ARP or ND entries that generate host routes
Route Tag	Specifies the tag value used with the host route from an ARP/ND entry
Limit	
Max Entries	Specifies the maximum number of entries learned on an IP interface
Log Only	Specifies whether or not to generate log entries only if limit is reached
Threshold	Specifies the threshold value that triggers a warning message
BFD	
Admin State	Specifies the administrative state of BFD sessions
Transmit Interval	Specifies the BFD transmit interval over this interface
Receive	Specifies the BFD receive interval over this interface
Multiplier	Specifies the number of consecutive BFD messages missed from the peer

Parameter	Description
Echo Receive	Specifies the minimum echo interval over this interface
Type	Specifies the local termination point for the BFD session
ICMP - Redirects	
Admin State	Specifies the administrative state of sending ICMP redirect messages
Number	Specifies the maximum number of ICMP redirect messages to send
Seconds	Specifies the time used to limit the number of ICMP redirect messages
ICMP - Unreachables	
Admin State	Specifies the administrative state of sending unreachable messages
Number	Specifies the maximum number of unreachable messages to send
Seconds	Specifies the time used to limit the number of ICMP unreachable messages
DHCP	
Admin State	Specifies the administrative state of DHCP
Server	Specifies the IP addresses for DHCP server requests

18

In the SAP panel, configure the following parameters for both ingress and egress, as required:

Parameter	Description
Port ID	Specifies the port identifier
Inner VLAN Tag	Specifies the inner VLAN tag
Outer VLAN Tag	Specifies the outer VLAN tag
Admin State	Specifies the administrative state of the service
Description	Describes the SAP
Collect Accounting Statistics	Specifies whether or not accounting statistics will be collected

Parameter	Description
Multi Service Site	Specifies the multi service site name

19

Perform the following to specify an accounting policy to be used:

1. Click on the Accounting Policy field. The Select Accounting Policy form opens.
2. Click on an accounting policy in the list, then click **SELECT**. The Select Accounting Policy form closes.

20

Configure the parameters in the Cpu Protection Panel, as required:

Parameter	Description
Policy Id	Specifies the CPM protection policy
Enable QoS	Specifies whether or not QoS is enabled
Enable IP/IPv6 Filter	Specifies whether or not an IP/IPv6 filter is enabled

21

If QoS was enabled in Step 20, configure the required QoS parameters in both the Ingress and Egress sections:

Parameter	Description
QoS	
Match QinQ Dot1p (ingress only)	Specifies the match QinQ Dot1p
QinQ Mark Top Only (egress only)	Specifies whether top Q-tags are marked
SAP Ingress	
Policy Name	Specifies the name of the ingress SAP policy
Queuing Type	Specifies the ingress queuing type
SAP Egress	
Policy Name	Specifies the name of the egress SAP policy
Queue (click **+ ADD**)	
Queue ID	Specifies the unique identifier for the queue
CBS	Specifies the CBS of the queue

Parameter	Description
MBS	Specifies the MBS of the queue
PIR	Specifies the PIR rate of the queue
CIR	Specifies the CIR rate of the queue
Policer (click **+ ADD**)	
Policer ID	Specifies the unique identifier for the policer
CBS	Specifies the CBS of the policer
MBS	Specifies the MBS of the policer
Stat Mode	Specifies the mode of statistics collected by the policer
Policer Override Rate	Specifies the policer override rate
Policer Control Policy	
Policy Name	Specifies the name of the policer control policy
Overrides (click check box)	
Max rate	Specifies the maximum rate
Min Thresh Separation	Specifies the minimum threshold separation
Priority (click **+ADD**)	
Priority Level	Specifies the priority level
Mbs Contribution	Specifies the minimum amount of cumulative buffer space allowed
Scheduler Policy	
Policy Name	Specifies the name of the scheduler policy
Scheduler (click **+ ADD**)	
Scheduler Name	Specifies the name of the scheduler
PIR	Specifies the PIR rate of the scheduler
CIR	Specifies the CIR rate of the scheduler
Weight	Specifies the relative weight of the scheduler to feed the queue
Cir Weight	Specifies the weight used at the within-CIR port priority level
Aggregate Policer (ingress only)	

Parameter	Description
Rate	Specifies the enforced aggregate rate for all queues
Burst	Specifies the aggregate policer burst
Cir	Specifies the aggregate policer CIR
Cbs	Specifies the aggregate policer CBS
Vlan Qos Policy (egress only)	
Policy Name	Specifies the Egress VLAN QoS policy name
Port Redirect	Specifies whether or not to enable Egress VLAN QoS policy port redirect
Egress Remark Policy (egress only)	
Policy Name	Specifies the Egress Remark policy name
Agg Rate or Percent Agg Rate	Specifies the enforced aggregate rate for all queues

22

If a filter was enabled in Step 20, configure the required filter parameters:

Parameter	Description
Aggregate Policer (ingress only)	
Rate	Specifies the enforced aggregate rate for all queues
Burst	Specifies the aggregate policer burst
Cir	Specifies the aggregate policer CIR
Cbs	Specifies the aggregate policer CBS
IP/IPv6 Filter	
IP	Specifies the IP filter identifier
IPv6	Specifies the IPv6 filter identifier

23

In the Routed VPLS panel, configure the required parameters:

Parameter	Description
VPLS Name	Specifies the name of the VPLS service

Parameter	Description
EVPN Tunnel	Specifies whether or not to configure the interface as a VPLS EVPN tunnel
ARP	
Learn Dynamic	Specifies whether or not dynamic entries learning is enabled
Advertise Static	Specifies whether or not advertise static is enabled
Advertise Static Route Tag	Specifies the advertise static route tag
Advertise Dynamic	Specifies whether or not advertise dynamic is enabled
Advertise Dynamic Route Tag	Specifies the advertise dynamic route tag

24

In the IPv6 Details panel, configure the required parameters:

Parameter	Description
IPv6 (**+ ADD**)	
IPv6 Address	Specifies the IPv6 address assigned to the interface
Prefix Length	Specifies the IPv6 address prefix length

Click **ADD** to add the interface.

The Add Interface form closes.

25

In the IP Transports panel, click **+ADD**.

The Add IP Transport form opens.

26

Configure the parameters, as required:

Parameter	Description
Transport Port ID	Specifies the Transport Port Identifier
Admin State	Specifies the administrative state for this IP Transport entry
Description	Description of this IP Transport
Local Host	

Parameter	Description
Local Host IP Address	Specifies the IP address of the IP Transport Local Host
Local Host Port Number	Specifies the Internet socket port number
Local Host Protocol	Specifies the IP protocol that the Local Host
Session Details	
DSCP	Specifies the Differentiated Services Code Point (DSCP) for all packets sent to Remote Hosts (within the same IP Transport)
Forwarding Class	Specifies the Forwarding Class (FC) for all packets sent to Remote Hosts (within the same IP Transport)
Filter Unknown Host	Specifies whether to allow a connection/session with an unknown remote host
Profile	Specifies the profile marking for all packets sent to Remote Hosts (within the same IP Transport)
TCP	
TCP Max Retries	Specifies the maximum number of consecutive attempts to establish a TCP connection
TCP Retry Interval	Specifies the period of time between consecutive attempts to establish a TCP connection
TCP In Active Timeout	Specifies the maximum period of time a TCP connection can remain idle before tear-down is initiated
Remote Host (click **+ADD**)	
Remote Host Id	Specifies the identifier for this IP Transport Remote Host
Name	Specifies the name assigned to this IP Transport Remote Host
Description	Specifies the description of this IP Transport Remote Host
Remote Host Ip Address	Specifies the IP address of the IP Transport Remote Host
Remote Host Port Number	Specifies the number of a TCP or UDP port

Parameter	Description
Check TCP	Specifies the TCP connection test to be initiated

Click **ADD** to add the IP Transport.

The Add IP Transport form closes.

27

If eBGP was enabled in Step 11, configure the required parameters:

Parameter	Description
Loop Detect	Specifies the strategy for loop detection in the AS path
Peer IP Tracking	Specifies whether or not to enable BGP peer tracking
Router ID	Specifies the Router ID for the BGP instance in the AS
Local AS	
As Number	Specifies the Local (or virtual) BGP AS number
Rapid Withdrawal	Specifies whether or not to send BGP withdrawal UPDATE messages immediately
Min Route Advertisement	Specifies the minimum time before a prefix can be advertised to peer
Next Hop Resolution	Specifies whether BGP routes can be used to resolve BGP nexthop
Best Path Selection	
Compare Origin Validation State	Specifies whether the origin validation state is used in the BGP decision process
Deterministic MED	Specifies whether paths will be grouped based on AS before MED attribute comparison
Origin Invalid Unusable	Specifies whether routes that have an origin validation state of 'Invalid' can be used
Ignore NH Metric	Specifies whether next-hop distance will be ignored during best path selection
Ignore Router ID	Specifies whether router ID will be ignored during best path selection

Parameter	Description
Always Compare MED	
MED Value	Specifies the Always Compare MED context
Strict AS	Specifies whether MED attributes will be compared from same-neighbor AS routes only
AS Path Ignore	
IPv4	Specifies whether AS path length will be ignored for unlabeled unicast IPv4 routes
IPv6	Specifies whether AS path length will be ignored for unlabeled unicast IPv6 routes
Label IPv4	Specifies whether AS path length will be ignored for labeled unicast IPv4 routes
Ebgp Ibgp Equal	
IPv4	Specifies whether to consider EBGP and IBGP labeled IPv4 routes equal
IPv6	Specifies whether to consider EBGP and IBGP labeled IPv6 routes equal
Label IPv4	Specifies whether to consider EBGP and IBGP unlabeled IPv4 routes equal
Group (**+ ADD**)	
Group Name	Specifies the group name
Damping	Specifies whether BGP route damping is used to reduce route flap
Authentication Key	Specifies the BGP authentication key for all peers
Peer AS	Specifies the peer AS number
Peer IP Tracking	Specifies whether BGP peer tracking is enabled
Prefix Limit (click **+ADD**)	
Family	Specifies the address family to which the limit applies
Maximum	Specifies the maximum number of routes to be learned from a peer
Threshold	Specifies the percentage threshold that triggers a warning message

Parameter	Description
Idle Timeout	Specifies the time which BGP peering remains idle before reconnecting
Admin State	Specifies the administrative state of the BGP group
Export (click check box)	
Policy	Specifies the export policy name
Import (click check box)	
Policy	Specifies the export policy name
Type	Specifies the BGP peer type
Family (click check box)	
Ipv4	Specifies whether or not to add support for the IPv4 address family
Ipv6	Specifies whether or not to advertise MP-BGP support for the IPv6 address family
Mcast Ipv4	Specifies whether or not to advertise support for the MCAST-IPv4 address family
Flow Ipv4	Specifies whether or not to advertise support for the flowspec-IPv4 address family
Flow Ipv6	Specifies whether or not to advertise support for the flowspec-IPv6 address family
Mcast Ipv6	Specifies whether or not to advertise support for the MCAST-IPv6 address family
Label Ipv4	Specifies whether or not to advertise support for the label-IPv4 address family
Neighbor (**+ ADD**)	
Import Policy	Specifies the import policy name
Export Policy	Specifies the export policy name
IP Address	Specifies the IP address that the neighbor uses to communicate with BGP peers
Group Name	Specifies the group name
Peer AS	Specifies the peer AS number
Admin State	Specifies the administrative state of the BGP neighbor

Parameter	Description
Split Horizon	Specifies whether to prevent routes being reflected back to best-route peer
Authentication Key	Specifies the BGP authentication key for peer
Description	Describes the BGP neighbor
AS Override	Specifies whether the peer's ASN will be replaced by the local ASN in AS Path
Type	Specifies the BGP peer type
Family (click check box)	
Ipv4	Specifies whether or not to add support for the IPv4 address family
Ipv6	Specifies whether or not to advertise MP-BGP support for the IPv6 address family
Mcast Ipv4	Specifies whether or not to advertise support for the MCAST-IPv4 address family
Flow Ipv4	Specifies whether or not to advertise support for the flowspec-IPv4 address family
Flow Ipv6	Specifies whether or not to advertise support for the flowspec-IPv6 address family
Mcast Ipv6	Specifies whether or not to advertise support for the MCAST-IPv6 address family
Label Ipv4	Specifies whether or not to advertise support for the label-IPv4 address family

28

If Enable Static Route was enabled in Step 11, click **+ ADD** in the Static Route Details panel.

The Add Static Route form opens.

29

Configure the parameters, as required.

Parameter	Description
IP Prefix	Specifies the IP prefix for the static route
Prefix Length	Specifies the prefix length for the static route
Route Type	Specifies the static route type
Tag	Specifies the static route tag

Parameter	Description
Is Blackhole	Specifies whether the prefix is a blackhole route
Next Hop (**+ ADD**)	
IP Address	Specifies the IP address of the next hop
Preference	Specifies the priority of this static route over routes from different sources
Tag	Specifies the static route tag
BFD Liveness	Specifies whether or not to use Bidirectional Forwarding Detection on this static route
Admin State	Specifies the administrative state of next hop
Indirect (**+ ADD**)	
IP Address	Specifies the IP address of the next hop
Preference	Specifies the priority of this static route over routes from different sources
Tag	Specifies the static route tag
Admin State	Specifies the administrative state of next hop

Click **ADD** to add the static route.

The Add Static Route form closes.

30

If Enable IS-IS was enabled in Step 11, click **+ ADD** in the IS-IS panel.

The Add IS-IS form opens.

31

Configure the parameters, as required.

Parameter	Description
IS-IS Instance	Specifies the instance ID for the IS-IS instance
Admin State	Specifies the administrative state of the IS-IS instance
Export Policy	Specifies the export policies that determine exported routes
Import Policy	Specifies the import policy names for routes from IGP to route table

Parameter	Description
Level Capability	Specifies the routing level for the instance
Advertise Router Capability	Specifies the router capabilities advertisement to neighbors

Click **ADD** to add the IS-IS instance.

The Add IS-IS form closes.

32

If Enable OSPF was enabled in Step 11, configure the parameters as required:

Parameter	Description
Compatible RFC-1583	Enables OSPF summary and external route calculations
Overload On Boot (click check box)	
Timeout	Specifies the time during which the router operates in overload state before reestablishing normal operations
Export Policy	Specifies the export policies that determine exported routes
Import Policy	Specifies the import policy names for routes from IGP to route table
Timers	
Incremental SPF Wait	Specifies the delay time before an incremental SPF calculation starts
LSA Accumulate	Specifies the delay to gather LSAs before advertising to neighbors
LSA Arrival	Specifies the minimum delay between receipt of same LSAs from neighbors
Redistribute Delay	Specifies the hold down timer for external routes into OSPF
LSA Generate	
Max LSA Wait	Specifies the maximum time between two LSAs being generated
LSA Initial Wait	Specifies the first wait period between OSPF LSA generation
LSA Second Wait	Specifies the hold time between the first and second LSA generation

Parameter	Description
Spf Wait	
Max SPF Wait	Specifies the maximum interval between two consecutive SPF calculations
SPF Initial Wait	Specifies the initial SPF calculation delay after a topology change
SPF Second Wait	Specifies the hold time between the first and second SPF calculation
Graceful Restart (click check box)	
Helper Mode	Enables graceful restart helper for OSPF
Strict Lsa Checking	Enables strict LSA checking during graceful restart helper

33

If Enable RIP was enabled in Step 11, configure the parameters as required:

Parameter	Description
Export Policy	Specifies the export policies that determine exported routes
Import Policy	Specifies the import policy names for routes from IGP to route table
Metric In	Specifies the metric added to routes received from a RIP neighbor
Metric Out	Specifies the metric added to routes exported into RIP
Preference	Specifies the route preference
Propagate Metric	Enables the BGP MED used to configure the RIP metric
Receive	Specifies the accepted version on received packets
Send	Specifies the RIP version and method used to send RIP updates
Admin State	Specifies the administrative state of the IS-IS instance
Timers	
Update	Specifies the timer that controls the frequency of updates

Parameter	Description
Timeout	Specifies the RIP timeout timer
Flush	Specifies the RIP flush timer
Group (click **+ADD**)	
Group Name	Specifies the group name
Admin State	Administrative state of the RIP group
Export Policy	Specifies the export policies that determine exported routes
Import Policy	Specifies the import policy names for routes from IGP to route table
Metric In	Specifies the metric added to routes received from a RIP neighbor
Metric Out	Specifies the metric added to routes exported into RIP
Preference	Specifies the route preference
Propagate Metric	Enables the BGP MED used to configure the RIP metric
Receive	Specifies the accepted version on received packets
Send	Specifies the RIP version and method used to send RIP updates
Timers	
Update	Specifies the timer that controls the frequency of updates
Timeout	Specifies the RIP timeout timer
Flush	Specifies the RIP flush timer

34

Click **ADD** to add the site.

The Add Site form closes.

35

In the SDP Details panel, click **+ ADD**.

The Add SDP form opens.

36

Configure the parameters, as required:

Parameter	Description
Source Device ID	Specifies the SDP source device identifier
Destination Device ID	Specifies the SDP destination device identifier
Steering Parameter	Specifies the steering parameter used by NSP
SDP ID	Specifies the SDP identifier
Description	Describes the SDP binding
Interface	Species the name of the interface
Override VC-ID	Specifies whether or not the VC-ID will serve as the NE service ID for the SDP
VC ID	Specifies the SDP virtual circuit identifier

Click **ADD** to add the SDP binding. The Add SDP form closes.

37

Click **DEPLOY** to create the service in a Deployed state.

38

Perform an audit to ensure that the service is properly deployed.

Perform one of the following to start the audit:

a. From the **Service Management, Services** view, click ⋮ (Table row actions), **Audit config** in-line with any service.

Note: Users can select up to 10 services at a time to run the Audit Config action against.

b. From the **Service Management, Services** view, click on a service in the list, then expand the Alignment State section in the info panel and click **AUDIT CONFIG**.

The service is audited.

39

If an Audit Result form appears, one or more attributes and/or objects are misaligned. Review the results and click **OK**.

The Audit Result form closes.

40

To revert to the expected value of a misaligned attribute, or to restore a misaligned object, perform one of the following:

a. Click ⋮ (Table row actions), **Align**, and then either **Push to network** or **Pull from network** in-line with the previously-audited service.

b.

1. Click on a service in the list, then expand the Alignment State section in the info panel and click **ALIGN**. The select alignment form opens.
2. Select the **Push to network** or **Pull from network** radio button, then click **CONTINUE**. The select alignment form closes.

The service is synchronized with the network.

END OF STEPS

5.11 Modify the service configuration

5.11.1 Purpose

Perform this procedure to edit a service.

5.11.2 Steps

1

Log in to the NSP as the Service Management user.

2

From the **Service Management, Services** view, click ⋮ (Table row actions), **Edit** in-line with any service. The Edit service form opens.

3

Update the parameters as needed and click **DEPLOY**.

4

Verify the updated configuration.

END OF STEPS

5.12 Remove the service

5.12.1 Purpose

Perform this procedure to remove a service from the network. The service remains in the NSP database and can be re-deployed from the Services view.

5.12.2 Steps

1

Log in to the NSP as the Service Management user.

2

From the **Service Management, Services** view, click ⋮ (Table row actions), **Remove** in-line with any service.

3

In the form that opens, click **REMOVE** to confirm.

The Life Cycle State of the service is updated to Removed.

END OF STEPS

5.13 Delete the service

5.13.1 Purpose

Perform this procedure to delete a service. Before a service can be deleted it must be removed from the network; see 5.12 “Remove the service” (p. 193).

5.13.2 Steps

1

Log in to the NSP as the Service Management user.

2

From the **Service Management, Services** view, click ⋮ (Table row actions), **Delete** in-line with any service in the Removed state.

3

In the form that opens, click **DELETE** to confirm.

The service is deleted.

END OF STEPS

Optional procedures

5.14 Create an OAM test suite

5.14.1 Purpose

Use this optional procedure to create a collection of tests that are grouped together to allow for multiple tests to be executed together or run in sequence. The suite includes both the tests and, where applicable, instructions for running tests sequentially or in parallel. Test suites can provide improved automation for OAM testing.

The bundle of vendor agnostic custom resources must be imported and installed to support telemetry collection and OAM testing. The bundle is found on the NSP software delivery site, in the Adaptors folder along with your NE adaptor suite, for example, NSP → 24.4 → Adaptors → Nokia_SROS. Choose the zip file with va and cr in the filename, for example, `nsp-telemetry-cr-va-sros-2.0.0-rel.9.zip`.

This procedure is based on the procedure for creating a test suite in the *NSP Data Collection and Analysis Guide*.

For example, the reference procedure in NSP Release 24.4 is How do I create an OAM test suite?.

See also the procedure to install telemetry artifacts in the *NSP Data Collection and Analysis Guide* to verify that prerequisites for testing are in place. The reference procedure for this in NSP Release 24.4 is: How do I install telemetry artifacts?.

5.14.2 Steps

1

Log in to the NSP as the Service Management user.

2

Open **Data Collection and Analysis Management**, **Test Suites**.

3

Click **+ SUITE**.

4

In the Generate OAM Tests form that opens, choose a Test type.

The list of templates in the Template field is updated based on your selection.

5

Choose a test template if needed.

If a template is not selected, an appropriate system template is automatically selected based on the value of the execute type field. If a template is selected, the value of the execute type field is imported from the template and is read-only in the form.

6

Add one or more entities:

1. Choose an entity type from the Entity type drop down.
2. Click **+ SELECT** to open a selection form.
3. Choose one or more entity objects from the list to add them to the Bin. Use the page selectors to navigate the list.
4. Verify the list of entity objects in the Bin and click **SELECT**.
5. To change the list of selected entities, repeat the previous steps to re-create the list.

7

Click on the Service field if applicable.

1. Select an attribute in the drop-down list, then enter values for that attribute in the field. As you type, the list is filtered for entities that match your input.
2. Click as required to add additional filter criteria.
3. Choose entities from the list and click **SELECT**.

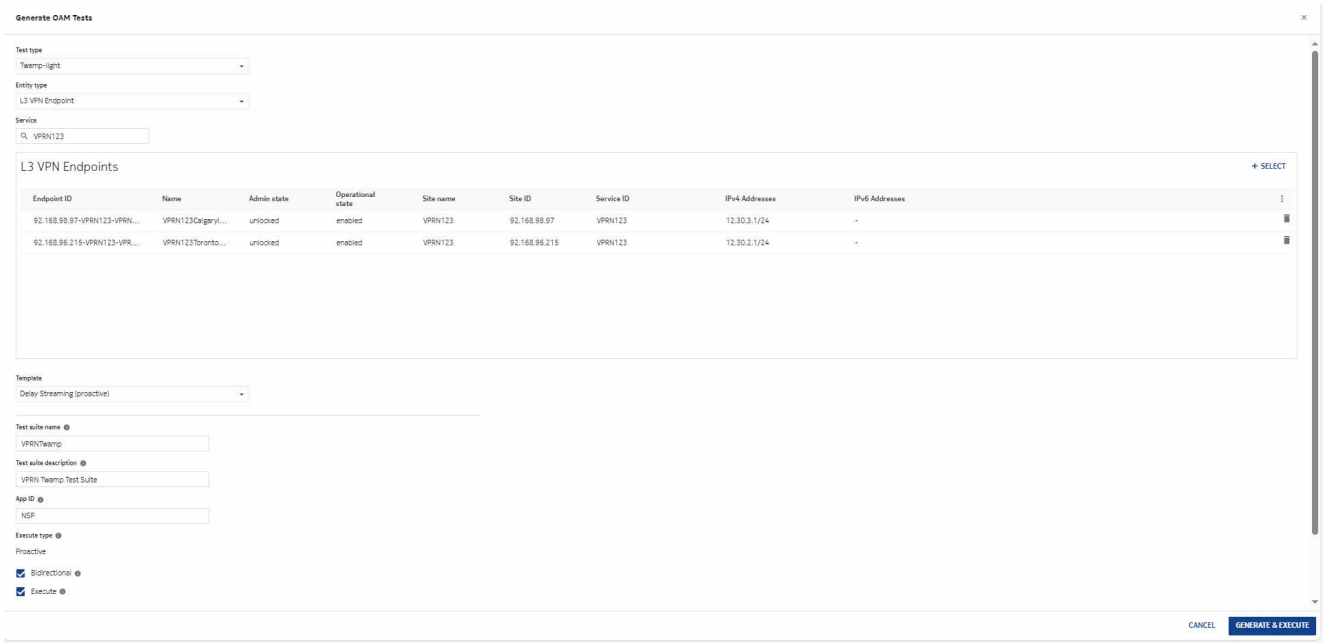
8

Configure the test parameters as needed.

9

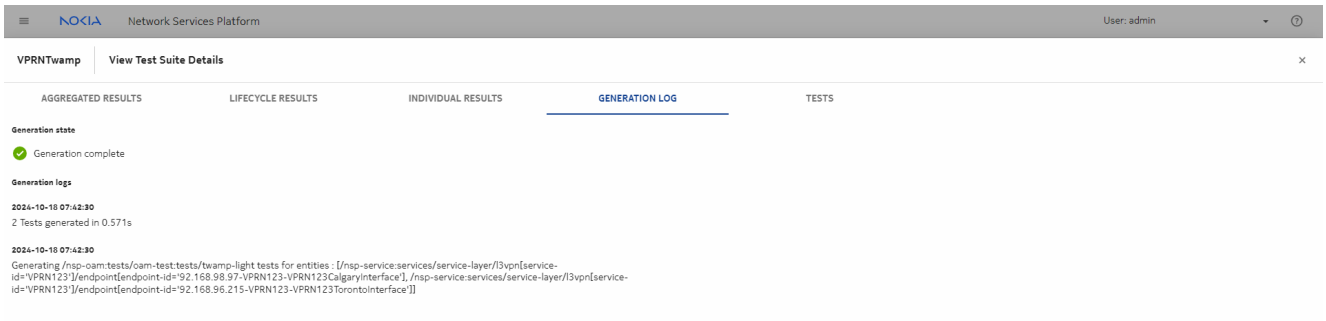
Generate the test suite.

a. To automatically execute the test suite after generation, enable Execute and click **GENERATE & EXECUTE**.



b. To create the test suite without automatically executing, disable Execute and click **GENERATE**.

The View Test Suite Details form opens. The Generation Log reports creation of the TWAMP objects required to run the test against the VPRN service onto the network were deployed.



10

Click on the **LIFECYCLE RESULTS** tab to verify that the test suite was created successfully.

11

Click on the **TESTS** tab to view the list of tests in the suite.

12

Click **CLOSE** to return to the Test Suites view. The new test suite appears in the list.

END OF STEPS

5.15 Execute an OAM test suite

5.15.1 Purpose

Use this optional procedure to start all the tests in an OAM test suite. For on-demand test suites, there is no need to manually stop the test suite. The test suite will stop automatically based on the test duration value that is assigned to the on-demand delay streaming test template.

This procedure is based on the procedure for stopping or starting a test suite in the *NSP Data Collection and Analysis Guide*.

For example, the reference procedure in NSP 24.4 is How do I stop or start an OAM test suite?.

5.15.2 Steps

1

Log in to the NSP as the Service Management user.

2

Open **Data Collection and Analysis Management**, **Test Suites**.

3

Choose a test suite and click ⋮ (Table row actions), **Execute**.

4

In the form that opens, update the parameters if needed and click **EXECUTE**. The execution status is updated to Running.

Tip: Disable the **Publish results** parameter if you don’t need results published to kafka. This may reduce processing impact.

5

To stop a test suite that is running, choose the test suite in the list and click ⋮ (Table row actions), **Stop**.

The test suite and all associated tests are stopped.

END OF STEPS

5.16 View OAM test results

5.16.1 Purpose

Use this optional procedure to view results of OAM tests. The examples in this procedure show a proactive Eth-CFM DMM test suite.

This procedure is based on the procedure to view test results in the NSP Data Collection and Analysis Guide.

For example, the reference procedure in NSP 24.4 is How do I view OAM test suite results?.

Note: After a test has executed, there is a brief processing delay before results are available. For tests that have just finished running, Nokia recommends that you wait a minimum of 5 s before viewing results.

5.16.2 Steps

1

Log in to the NSP as the Service Management user.

2

Open **Data Collection and Analysis Management**, **Test Suites**.

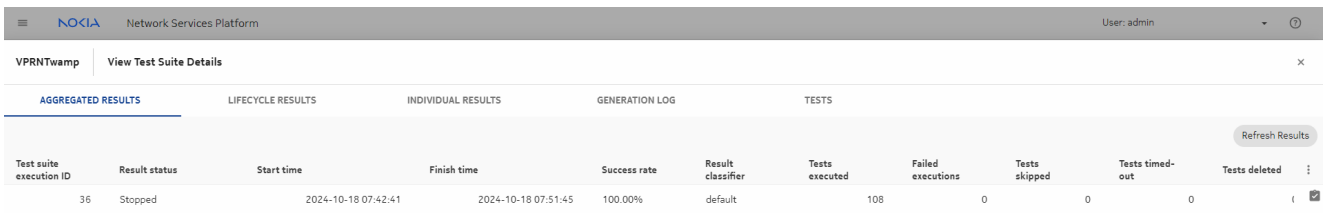
3

Choose the test suite and click ⋮ (Table row actions), **View Details**.

The View Test Suite Details page opens, showing the following:

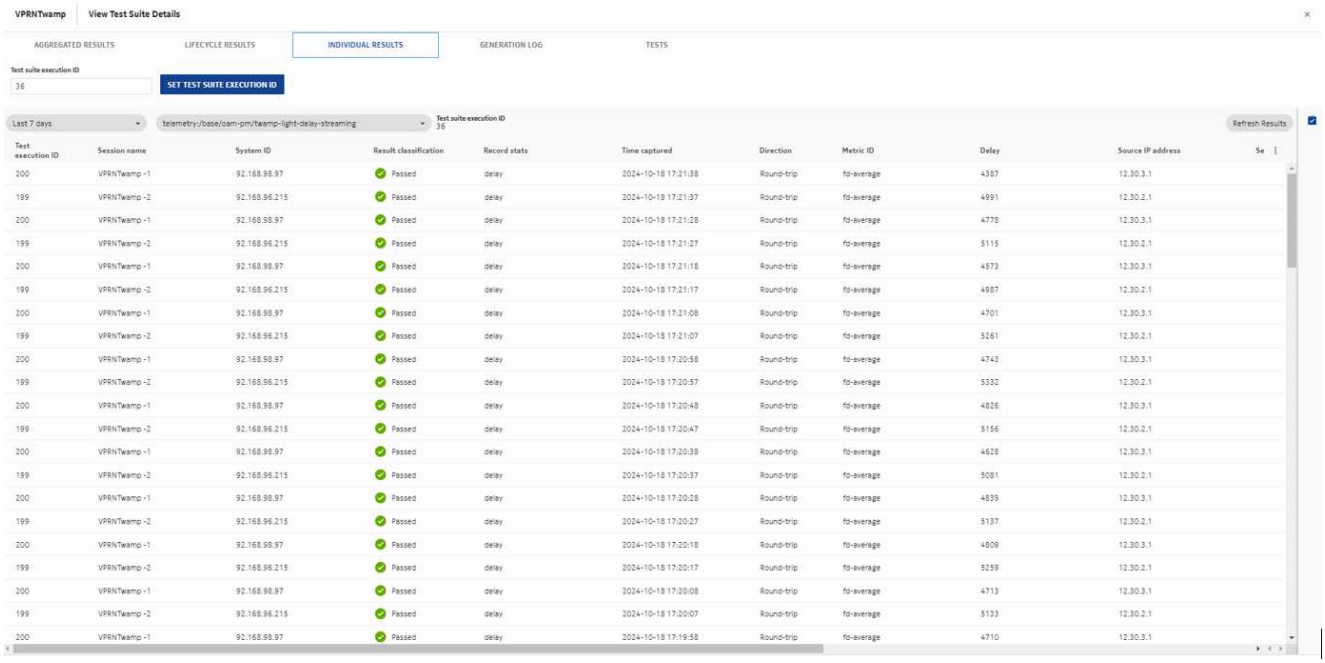
Tab	Notes
AGGREGATED RESULTS	Each row of the aggregated results table corresponds to an execution of the test suite. Whenever the test suite is successfully started, a new aggregated results row is added. To view the individual results for a specific test suite execution, select the aggregated results row corresponding to the execution you are interested in and click **View individual results**.
LIFECYCLE RESULTS	The LIFECYCLE RESULTS table shows events from the execution of the test suite, such as stop and start timestamps and error events.

Tab	Notes
INDIVIDUAL RESULTS	The page displays the results of each test executed. By default, the results from the most recent test suite execution are shown, that is, the execution ID from the first row of the aggregated results table is chosen automatically. You can view results for other test suite executions by specifying another execution ID in the **Test suite execution ID** field or by returning to the AGGREGATED RESULTS tab and clicking **View individual results** . For more detailed information about a specific test, choose an execution and click **View Results** . **Note:** If a test suite was created from the NSP, the tests will all be the same type. If the test suite was created using RESTCONF, multiple test types could be included. To view results from a different type than is currently displayed, choose the telemetry type from the drop down list. See the **TESTS** tab for a list of tests in the suite.
GENERATION LOG	The page displays log information from the generation of the suite and tests.
TESTS	The page lists the test identifiers included in the suite. If the test suite is an on-demand suite, the TESTS tab shows the included tests grouped by stage. Stages are executed sequentially, but tests within each stage will be executed either sequentially or in parallel depending on how the stage is configured. For more detailed information about a specific test, double click on an execution or choose an execution and click **View Results** .



4

For more detailed information about a specific test, double click on an execution in the **TESTS** tab or choose an execution and click **View Results** .



For the example shown, the tests between service endpoints are passing, showing that there are no issues with service connectivity.

END OF STEPS

5.17 Delete an OAM test suite

5.17.1 Purpose

Use this optional procedure to delete an OAM test suite and all its associated tests from the NSP UI. This action cannot be undone.

Note: Test suites cannot be edited in the NSP UI.

5.17.2 Steps

1

Log in to the NSP as the Service Management user.

2

Open **Data Collection and Analysis Management**, **Test Suites**.

3

Choose a test suite and click ⋮ (Table row actions), **Delete**.

4

Click **DELETE** in the confirmation dialog to confirm.

The test suite and its tests are deleted from the NSP.

END OF STEPS

5.18 Create a telemetry subscription

5.18.1 Purpose

Perform this procedure to set up telemetry collection.

This procedure is based on the procedure for managing subscriptions in the *NSP Data Collection and Analysis Guide*.

For example, the reference procedure in NSP 24.4 is How do I manage subscriptions?.

CAUTION

Service Disruption

The name of an object, including subscriptions, baselines, indicators, templates, and chart profiles, cannot contain a semicolon (;) or backslash (\).

The use of these characters in an object identifier will result in corrupted data that must be deleted by Nokia support.

5.18.2 Steps

1

Log in to the NSP as the Service Management user.

2

Open **Data Collection and Analysis Management**, **Subscriptions**.

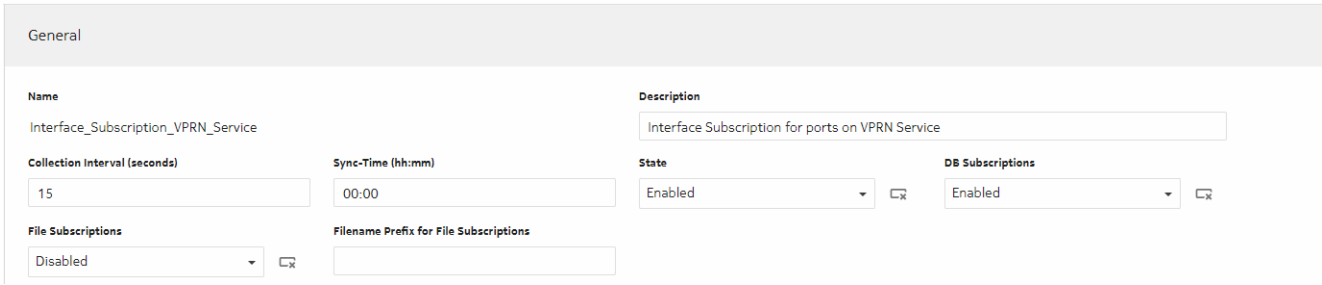
3

Click **+ SUBSCRIPTION**.

4

In the Create Subscription form that opens, configure the General parameters as needed:

- Enable database (DB) subscriptions as needed to save subscription information to the NSP database. For subscription data to be available to Analytics, the auxiliary database must be deployed.
- The subscription is enabled by default: it will start running immediately.



5

Configure filters and counters:

1. In the **Object Filter** field, enter filtering information as needed to filter the collected data.

   As you type, the field provides suggestions for available filters to match your input and identifies incorrect syntax.

2. Enter information in the Telemetry Type field. As you type, the field filters for available telemetry types to match your input.

   Choose the telemetry type you need from the list of matches.

3. When you enter a telemetry type, all counters are enabled by default.

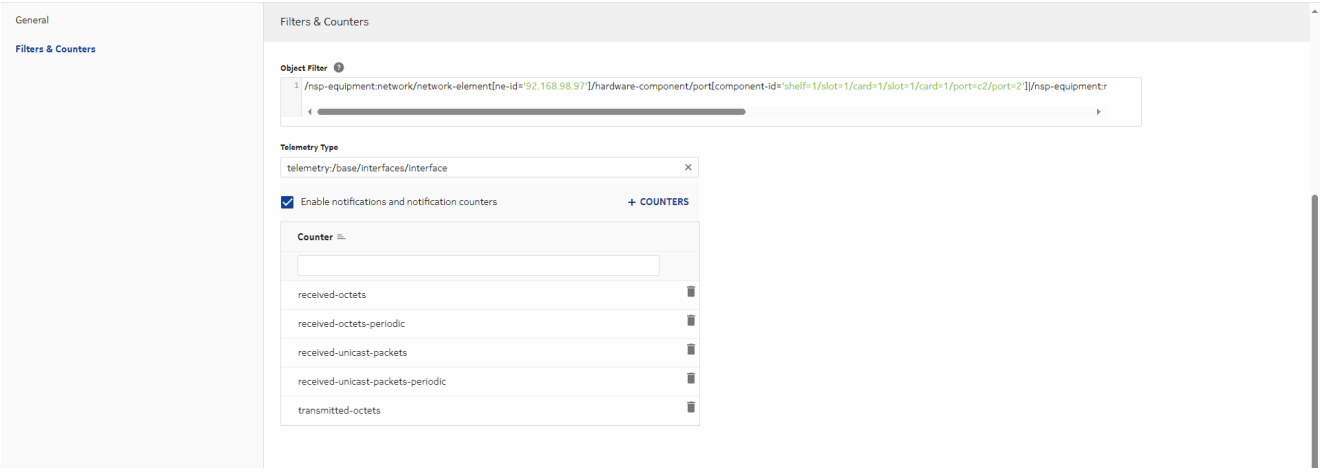
   To customize the counters, enable the **Enable notifications and notification counters** check box.

   Click **Remove** to remove a counter.

   Click **+ COUNTERS** to add a counter that was removed.

This example includes the following:

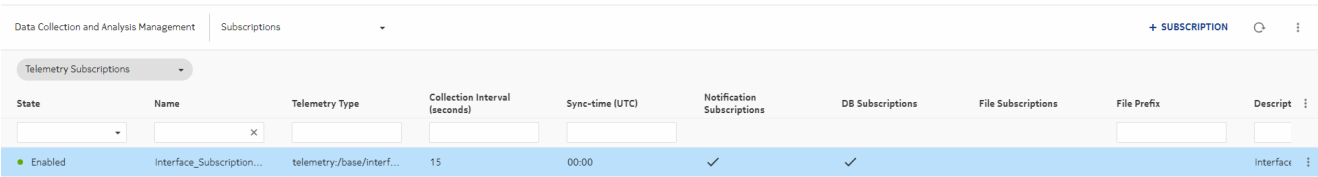
- Telemetry Type: telemetry:/base/interfaces/interface
- Counters:
  - received-octets-periodic
  - received-octets
  - received-unicast-packets
  - received-unicast-packets-periodic
  - transmitted-octets
- Object Filter (2 port objects used by two endpoints of the service): /nsp-equipment:network/network-element[ne-id='92.168.98.97']/hardware-component/port[component-id='shelf=1/slot=1/card=1/slot



6

Click **CREATE**.

The subscription appears in the subscriptions list.



Port throughput statistics from the sites and NEs found by the object filter are received and processed every 15 s (see Collection Interval value). The statistics will remain in the NSP database for a configured period of time, as defined in the ageout policy.

END OF STEPS

5.19 Modify a telemetry subscription

5.19.1 Purpose

Use this optional procedure to make changes to a telemetry subscription, for example, to change the list of counters.

This procedure is based on the procedure for managing subscriptions in the *NSP Data Collection and Analysis Guide*.

For example, the reference procedure in NSP 24.4 is How do I manage subscriptions?.

5.19.2 Steps

1

Log in to the NSP as the Service Management user.

2

Open **Data Collection and Analysis Management**, **Subscriptions**.

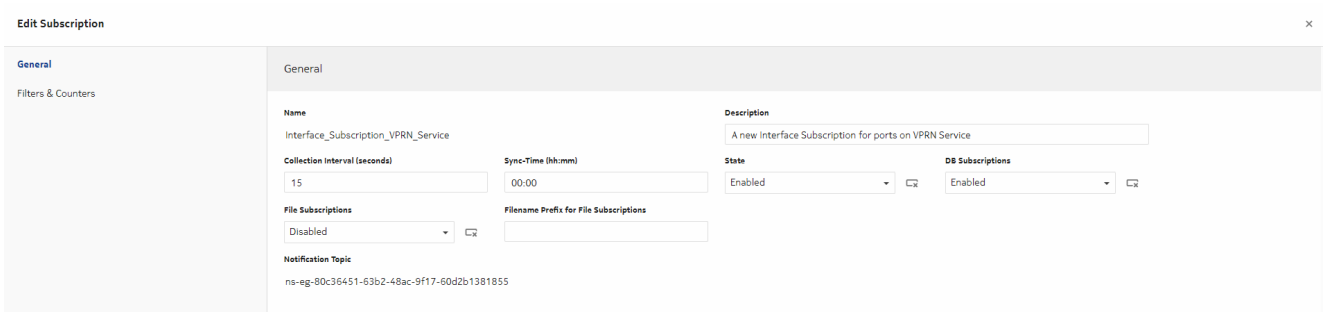
3

Choose a subscription and click ⋮ (Table row actions), **Edit**.

4

In the form that opens, update the parameters as needed.

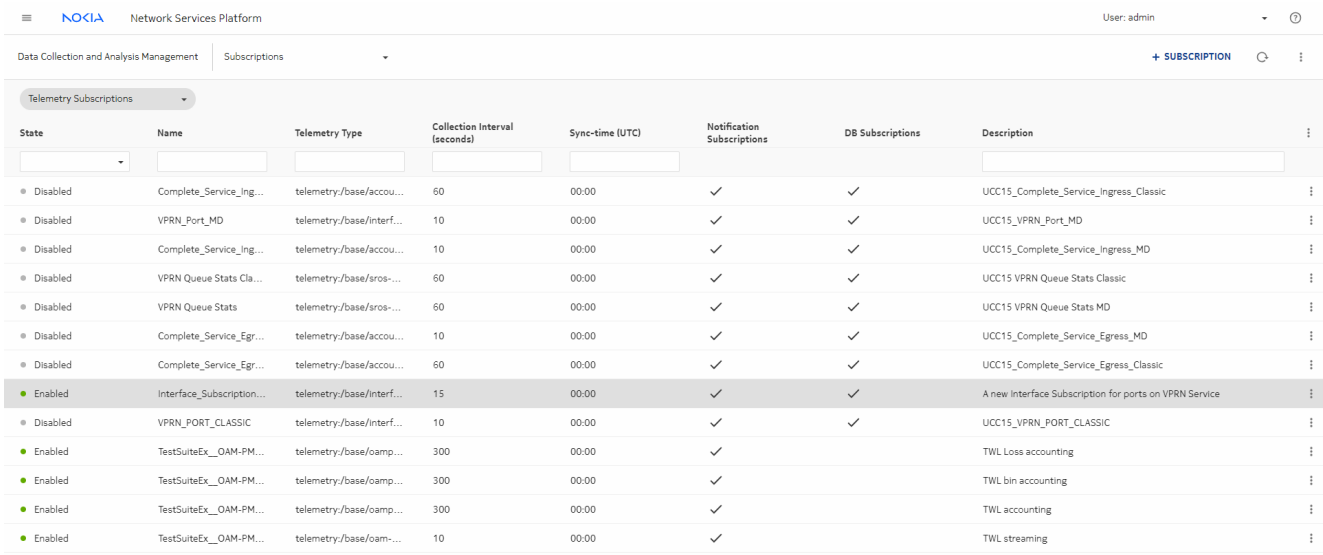
In this example, a new description is provided.



5

Click **UPDATE**

The updated subscription appears in the list.



State	Name	Telemetry Type	Collection Interval (seconds)	Sync-time (UTC)	Notification Subscriptions	DB Subscriptions	Description
Disabled	Complete_Service_Ing...	telemetry:/base/accou...	60	00:00	✓	✓	UCC15_Complete_Service_Ingress_Classic
Disabled	VPRN_Port_MD	telemetry:/base/interf...	10	00:00	✓	✓	UCC15_VPRN_Port_MD
Disabled	Complete_Service_Ing...	telemetry:/base/accou...	10	00:00	✓	✓	UCC15_Complete_Service_Ingress_MD
Disabled	VPRN Queue Stats Cla...	telemetry:/base/sros-...	60	00:00	✓	✓	UCC15 VPRN Queue Stats Classic
Disabled	VPRN Queue Stats	telemetry:/base/sros-...	60	00:00	✓	✓	UCC15 VPRN Queue Stats MD
Disabled	Complete_Service_Egr...	telemetry:/base/accou...	10	00:00	✓	✓	UCC15_Complete_Service_Egress_MD
Disabled	Complete_Service_Egr...	telemetry:/base/accou...	60	00:00	✓	✓	UCC15_Complete_Service_Egress_Classic
Enabled	Interface_Subscription...	telemetry:/base/interf...	15	00:00	✓	✓	A new Interface Subscription for ports on VPRN Service
Disabled	VPRN_PORT_CLASSIC	telemetry:/base/interf...	10	00:00	✓	✓	UCC15_VPRN_PORT_CLASSIC
Enabled	TestSuiteEx__OAM-PM...	telemetry:/base/oamp...	300	00:00	✓		TWL Loss accounting
Enabled	TestSuiteEx__OAM-PM...	telemetry:/base/oamp...	300	00:00	✓		TWL bin accounting
Enabled	TestSuiteEx__OAM-PM...	telemetry:/base/oamp...	300	00:00	✓		TWL accounting
Enabled	TestSuiteEx__OAM-PM...	telemetry:/base/oam-...	10	00:00	✓		TWL streaming

END OF STEPS

5.20 Plot telemetry statistics

5.20.1 Purpose

Use this optional procedure to plot a chart of telemetry statistics. The steps for charting any type of telemetry statistic are the same: the example shows port throughput statistics.

This procedure is based on the procedure to plot a telemetry chart in the *NSP Data Collection and Analysis Guide*.

For example, the reference procedure in NSP 24.4 is How do I plot a telemetry chart?.

5.20.2 Before you begin

When you create a telemetry chart, you configure a telemetry filter. For historical data to be displayed, the data must be available in the database; see 5.18 “Create a telemetry subscription” (p. 202).

Charts are created by streaming to the plotter: historical data is queried and streamed to the plotter, then real time telemetry subscriptions are created and the data from these subscriptions is streamed to the plotter.

Data Collection and Analysis Visualizations times out if telemetry data is not received. The time-out limit is either double the collection interval or two minutes, whichever is greater.

Chart limit

Up to 10 objects can be charted at a time. The number of objects is the number of resources returned by the object filter, multiplied by the number of counters.

If your object filter returns one resource, for example, one NE, you can chart up to 10 counters for the resource.

5.20.3 Steps

CAUTION

Service Disruption

The name of an object, including subscriptions, baselines, indicators, templates, and chart profiles, cannot contain a semicolon (;) or backslash (\).

The use of these characters in an object identifier will result in corrupted data that must be deleted by Nokia support.

Create a chart

1

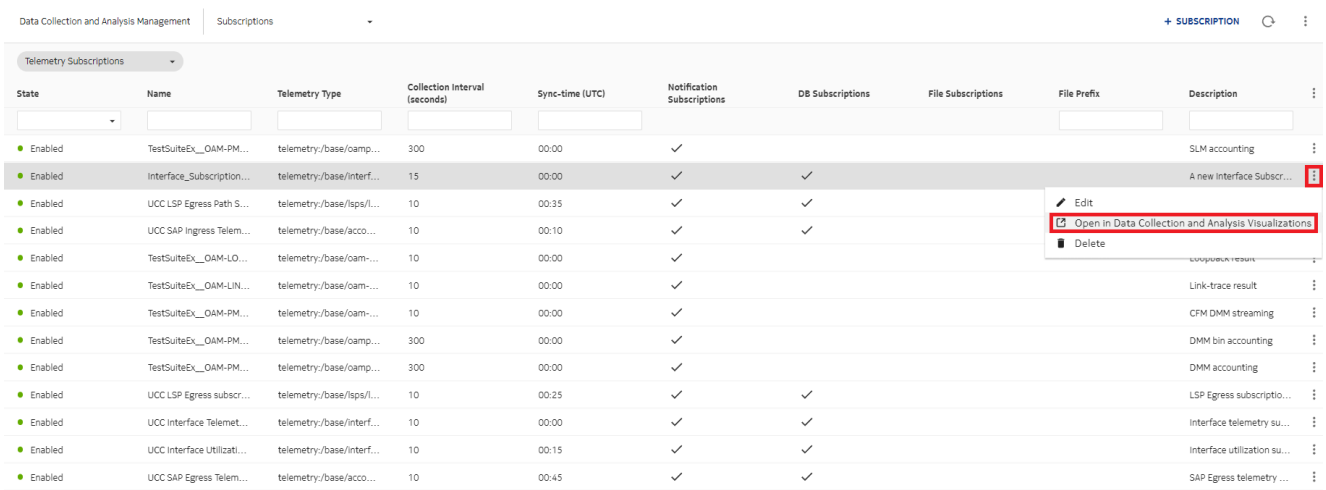
Log in to the NSP as the Service Management user.

2

Open **Data Collection and Analysis Management**, **Subscriptions**.

3

Choose a subscription and click ⋮ (Table row actions), **Open in Data Collection and Analysis Visualizations**.



The **Data Collection and Analysis Visualizations** view opens in a new browser tab.

4

In the window that opens, configure the parameters in the top panel:

1. Configure the **Collection Interval** parameter. If you are using NFM-P telemetry data, verify that the collection interval is long enough to allow time for Visualizations to receive the data before timing out.
2. From the **Time Range** drop-down list, choose the amount of historical data to display.
3. Click **Combine charts** to plot data from multiple data series on the same chart.

5

Click **+ DEFINITION**.

The telemetry and resource filter definition panels are displayed.

6

Enter information in the **Telemetry Type** field. As you type, the field filters for available telemetry types to match your input.

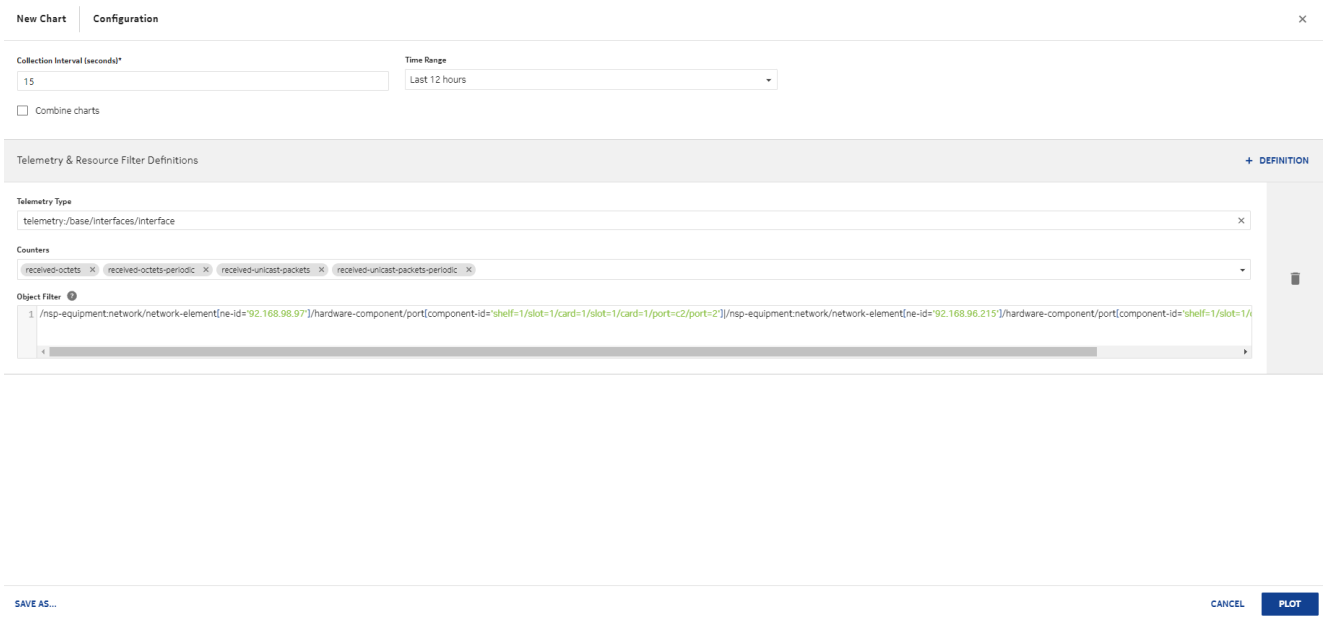
Choose the telemetry type from the list of matches.

7

Choose counters to display from the **Counters** drop-down list.

8

In the **Object Filter** field, enter filtering information to filter the collected data.



9

Save the configuration as a chart:

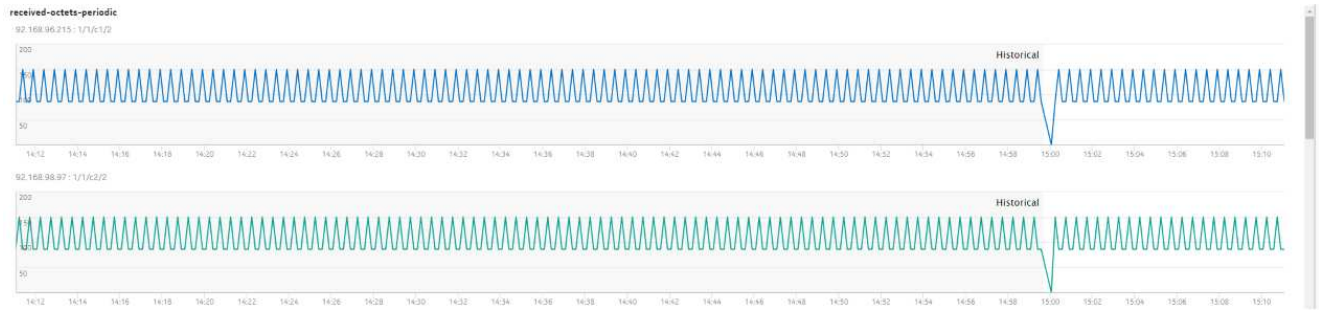
1. Click **SAVE AS**.
2. In the window that opens, enter a name for the chart and add a description.
3. Click **SAVE**.

In a few seconds, the chart is added to the list.

10

Click **PLOT**.

NSP begins plotting data. In a few moments, data will be visualized in the chart.



11

Close the chart window. The saved telemetry chart appears in the list, ready to be plotted again as needed.

END OF STEPS

5.21 Delete a telemetry subscription

5.21.1 Purpose

Use this optional procedure to remove a telemetry subscription from the NSP. This action cannot be undone.

This procedure is based on the procedure for managing subscriptions in the *NSP Data Collection and Analysis Guide*.

For example, the reference procedure in NSP 24.4 is How do I manage subscriptions?.

5.21.2 Steps

1

Log in to the NSP as the Service Management user.

2

Open **Data Collection and Analysis Management**, **Subscriptions**.

3

To delete a subscription:

Choose a subscription and click ⋮ (Table row actions), **Delete**.

The subscription is removed immediately.

Note: Removing a subscription does not remove data from the database. The data collected by the subscription is retained according to the database retention policy.

END OF STEPS

6 UCC-16: IES

6.1 Overview

6.1.1 Purpose

This chapter describes the process required to configure an IES on SR OS NEs using NSP Service Management.

Configuration examples in this chapter show NSP Release 23.11 and SR OS 23.7.R2 NEs.

The following artifact bundles were used to test this use case:

- nsp-icm-intents-23.11.0-cam-bundle.zip
- nsp-svc-fulfillment-bundle-2311-v3.zip

See the NSP and NE documentation for more information.

6.1.2 Contents

Preparation

6.2 Prerequisites

6.2.1 Network configuration prerequisites

Before services can be configured and managed in NSP, the network configuration prerequisites must be met. The following table describes the requirements that can apply to service use cases, and indicates whether each prerequisite is required for this use case.

Where an NSP intent type is not available, CLI or MD-CLI must be used to perform configuration on the device.

Prerequisite	Documentation reference	Notes
Mandatory for IES		
GRPC configuration 1. Generate security certificates 2. Configure security and enable GRPC on all devices 3. Apply security certificates on all devices	See SR TLS information here in the SR OS 24.3 R1 documentation: TLS	—
Netconf/SNMP provisioning: enable NETCONF and SNMP protocols on all devices	For more information about SNMP and NETCONF with SR OS, see SNMP and NETCONF in the *SR OS 24.3 R1 System Management Guide*.	—
NSP installation	Pathway for NSP system installation in the *NSP Installation and Upgrade Guide* How do I enable TLS for telemetry and gNMI on_change support? in the *NSP System Administrator Guide*.	Include the following in your deployment: • Feature packs: - platform-baseServices - platform-pluggableNetworkAdaptation - platform-loggingMonitoring - serviceActivationAndConfiguration-intentBasedServiceFulfillment - networkInfrastructureManagement-basicManagement - networkInfrastructureManagement-deviceConfig • Adaptor suites: - sros-common - sros-oc-logical-inventory - sros-23-7-r1

Prerequisite	Documentation reference	Notes
Download the required artifact bundles from the NSP software delivery site: • NSP predefined set for ICM (device configuration) • NSP product artifact bundle for Service Fulfillment	How do I install an artifact bundle? in the *NSP Network Automation Guide*	—
Device discovery	Pathway for device discovery in the *NSP Classic Management User Guide* How do I discover devices? in the *NSP Device Management Guide* Nokia Developer Portal for information about FTP mediation policy creation using API.	—
Cards and MDAs provisioning	ICM process in the *NSP Device Management Guide* for more information about using the Device Configuration views, and the other procedures in the *NSP Device Management Guide* for further detail. See the NSP ICM Intent Type Catalog for information about this and other device configuration intent types developed by Nokia.	The intent type required for this configuration is icm-equipment-card-mda.
Connectors and Ports provisioning		The intent types required for this configuration are: • icm-equipment-port-connector • icm-equipment-port-ethernet
OSPF/ISIS	CLI Reference Guides for SR OS	—
LDPs, MPLS and RSVP configuration	CLI Reference Guides for SR OS	For LDP to be operational, the IPv4 and IPv6 bindings must be configured manually using CLI.
Interfaces Provisioning	How do I create a physical configuration deployment? in the *NSP Device Management Guide*.	The intent type required for this configuration is icm-router-network-interface
Customer creation	How do I create a logical configuration deployment? in the *NSP Device Management Guide*.	The intent type required for this configuration is icm-service-customer
Optional		

Prerequisite	Documentation reference	Notes
Optional items to include in your NSP deployment	Pathway for NSP system installation in the *NSP Installation and Upgrade Guide*	• Optional feature packs: - pathControlAndOptimization - multilayerDiscoveryAndVisualization - NSP Analytics: Network Operations Analytics feature package with the networkOperationsAnalytics-analyticsReporting installation option - NSP Baseline Analytics: networkOperationsAnalytics-baselineAnalytics - networkInfrastructureManagement-performanceIndicatorsAndAlerts • VSR/NRC • An AuxDB • An NFM-P instance
Telemetry/OAM	*NSP Data Collection and Analysis Guide*	• NSP SR OS vendor-agnostic telemetry adaptation artifact bundle • networkInfrastructureManagement-gnmiTelemetry feature pack
BGP/EVPN	How do I create a logical configuration deployment? in the *NSP Device Management Guide*.	The intent type required for this configuration is icm-router-bgp_group
Segment Routing	CLI Reference Guides for SR OS	—
Scheduler QoS Policies	How do I create a logical configuration deployment? in the *NSP Device Management Guide*.	The intent types required for this configuration are: • icm-qos-schedulerpolicy-srqos • icm-qos-network-srqos • icm-qos-sapingress-srqos • icm-qos-sapegress-srqos
Network QoS Policies configuration		
SAP QoS Policies configuration		
PCEP configuration	CLI Reference Guides for VSR-NRC	Most of the connections required for PCEP are established during previous configuration steps.
LAGs and MC-LAG creation	How do I create a logical configuration deployment? in the *NSP Device Management Guide*.	The intent types required for this configuration are: • icm-logical-lag-access • icm-logical-mc_lag-access

6.3 Optional: create a restricted Service Management user

6.3.1 Purpose

Perform this optional procedure to create a user with access only to specified NSP functions.

Procedures in this chapter can be performed by the restricted user, or by an administrator.

This procedure is based on the procedures for the following in the *NSP System Administrator Guide*:

- Configuring a role
- Configuring a user group
- Creating an NSP local user
- Enabling User Access Control
- Configuring user access to an intent type

For example, the reference procedures in NSP Release 23.11 are:

- How do I configure a role?
- How do I configure a user group?
- How do I create an NSP local user?
- How do I enable User Access Control?
- How do I configure user access to an intent type?

If a restricted user has already been created, verify that the user has the required permissions, as shown in Step 6.

6.3.2 Steps

Create a role

1

Log in to the NSP as an administrator.

2

Open **Users and Security**.

3

Select **Roles** from the drop-down list on the toolbar.

4

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

5

In the Identification panel, specify a role name and description.

The Role Name and Description fields can employ **only** the following special characters: `@ - _`.

The Role Name string must not contain *any* spaces, including a leading or trailing space.

6

To assign NSP functional access to the role, go to the Action Permissions panel and select an access level from the drop-down list for each NSP GUI you want to include in the role.

Action permissions group item	Permissions	Notes
Service Fulfillment	Read / Write / Execute	—
Network Intents	Read: Manage Intents	Required to import intent types into Service Management
Workflows	Read	Required to create service and tunnel templates
Optional: DCA Management	Read / Write / Execute	Only required for creating and plotting telemetry subscriptions
Optional: OAM Tests	Read / Write / Execute	Only required for generating and executing OAM tests

7

To assign network resource access to the role, go to the Resource Groups Access panel. (For a detailed explanation of the Resource Groups Access panel, see How do I set network resource access levels? in the *NSP System Administrator Guide*.)

You can assign resource group access globally, to resource group categories, to individual resource groups, or a combination of these. For service management it is recommended to grant access to all equipment and all services:

- **Access To All Equipment** assigns full permissions on all NE resource groups and port resource groups to the role.
- **Access To All Services** assigns full permissions on all service resource groups to the role.

8

Click **Create** to save your changes and return to the Roles list.

Create a user group

9

Open **Users and Security**.

10

Select **User Groups** from the drop-down list on the toolbar.

11

Click **+ Create User Group**. The Create User Group form opens.

12

Specify a group name and description in the **Identification** panel.

The user group name you specify here must exactly match a corresponding user group name returned by your user repository.

The User Group Name and Description fields can employ **only** the following special characters: `@ - _`.

The User Group Name string must not contain *any* spaces, including a leading or trailing space.

13

To assign user roles to the group, click **+ Add Roles** on the Roles panel. The Add Roles form opens.

14

Enable the check box for each role you want to assign to the group and click **Done**. The roles are added to the Selected Roles list.

To remove a role item from the Selected Roles list, click **Delete** on the item.

15

Click **Create** to save your changes and return to the User Groups list.

Create a user

16

Open **Users and Security**.

17

Select **Users** from the drop-down list on the toolbar.

18

Click **+ Create User**.

19

In the Create User form, specify user identification information for the account in the Identification section. The **Username** and **User Group** fields are mandatory.

Note: Any uppercase characters in the username are saved as lowercase.

The **Username** value:

- can be 1 to 40 characters long
- cannot include a space
- cannot have a leading or trailing space
- can include only the following special characters:
  - **@** (at sign)
  - **-** (hyphen)
  - **_** (underscore)
  - **.** (period)

20

In the Password section, specify and confirm a password for the user account.

- If you want this password to be temporary, enable the **Force User to Change Password** option. The new user will be forced to change their password when they first login to NSP.
- Enable the **Show Password** option to see the password characters as you type them.
- Click on the **Password Requirements** link to view a list of minimum security requirements for the password.

21

Click **Create**.

Enable user access control

22

Open **Users and Security**, **User Groups**.

23

Click ⋮ **More Actions**, **Settings**.

24

In the Access Control Settings form, enable the **NSP User Access Control** option.

25

Click **SAVE** to enable access control.

END OF STEPS

6.4 Install the required artifact bundles

6.4.1 Purpose

Use this procedure to make the required intent types available to Service Management in NSP. This procedure is based on the procedure for installing an artifact bundle in the *NSP Network Automation Guide*.

For example, the reference procedure in NSP 23.11 is How do I install an artifact bundle?.

6.4.2 Steps

Download the required intent types

1

Download the Service Fulfillment artifact bundle from the NSP software delivery site.

Navigate through the hierarchy to the folder of artifacts that can be imported using the Artifacts views, for example: NSP → 23.11 → Artifacts → Artifact_Admin_Import.

See the description to verify which bundle to download.

Install the artifact bundle in NSP

2

Log in to the NSP as the Service Management user.

3

Open **Artifacts**, **Artifact Bundles**.

4

Click **IMPORT & INSTALL**.

5

In the form that opens, drag and drop the zip file, or click **Browse** and navigate to the files on your system.

6

To install the artifact bundle immediately, click **IMPORT & INSTALL**. To import without installing, click **IMPORT**.

The chosen operation is triggered immediately. The artifact bundle status is updated to Imported or Installed when NSP has confirmed the status of all artifacts in the artifact bundle.

7

To install a bundle in Imported status, choose **Install bundle** from the ⋮ (Table row actions) menu.

END OF STEPS

6.5 Configure user access to the required intent types

6.5.1 Purpose

Use this procedure to provide the user access to intent types. If the restricted Service Management user will be performing configuration tasks, this procedure must be performed.

This procedure is based on the procedure for configuring user access to an intent type in the *NSP Network Automation Guide*.

For example, the reference procedure in NSP Release 23.11 is How do I configure user access to an intent type?.

6.5.2 Steps

1

Log in to the NSP as an administrator.

2

Open **Network Intents**, **Intent Types**.

3

Select the `ies` intent type.

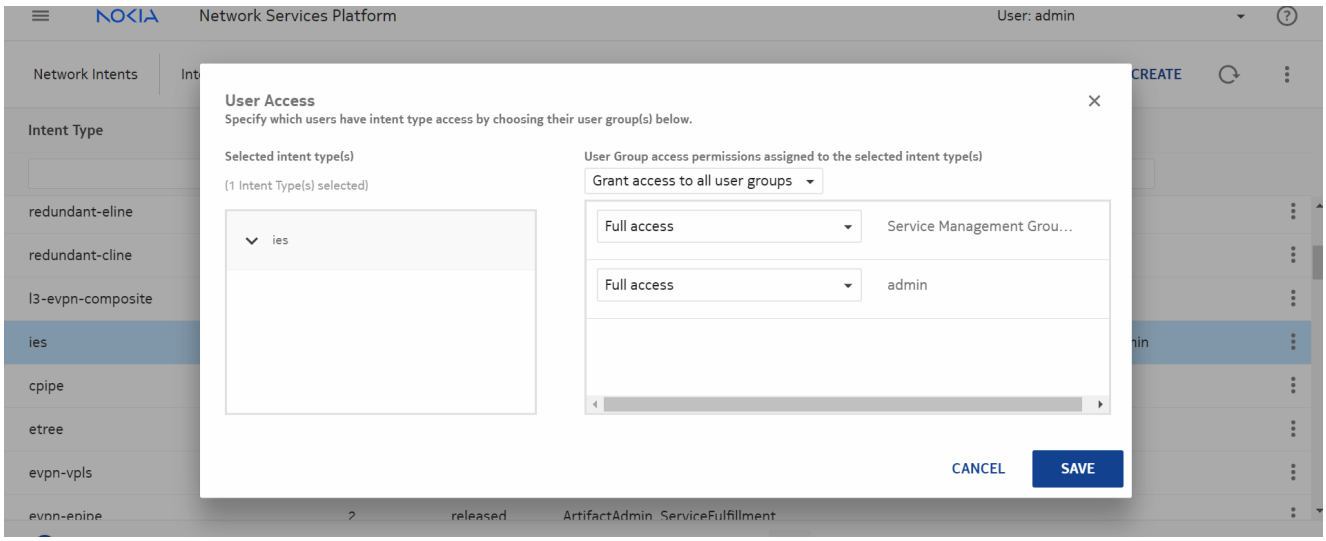
4

Click ⋮ (Table row actions), **User Access** to open the User Access form.

5

In the **User Access** form, choose **Grant access to all user groups** from the drop-down list at the top right of the form.

Choose **Full access** for the user group created in “Create a user group” (p. 54).



6

Click **SAVE**. The user access is updated.

END OF STEPS

Service Configuration

6.6 Import intent types into Service Management

6.6.1 Purpose

Use this procedure to import the intent types you obtained in 6.4 “Install the required artifact bundles” (p. 218) to the Service Management views. This procedure is based on the procedure for importing an intent type into Service Management in the *NSP Service Management Guide*.

For example, the reference procedure in NSP Release 23.11 is How do I import an intent type into Service Management?.

Note: This procedure is not required in NSP 25.4 or later because intent types for Service Management will import directly into Service Management during artifact bundle installation.

The intent type required is `ies`.

6.6.2 Steps

1

Log in to the NSP as the Service Management user.

2

From the **Service Management, Intent Type Catalogue** view, click **IMPORT**.

A list of previously-defined intent types is displayed.

Note: Only intent types that have the Service Fulfillment label applied will be available to import. Intent types to be used for tunnel template creation must also have the Tunnel label applied.

Note: For a restricted user to be allowed to import intent types, they must have appropriate permissions configured for those intent types in Network Intents; see How do I configure user access to an intent type? in the *NSP Network Automation Guide*.

3

Select the check boxes in-line with the intent types you wish to import and click **IMPORT**.

The intent type to import is ies.

The intent type is imported into service management. This may take a few minutes.

Note: Selecting an imported intent type from the list opens the Info panel, which displays historical information such as the last time the intent type was updated, the last time it was imported, and the last time the modules that compose the intent type were revised.

End of steps

6.7 Create an IES service template

6.7.1 Purpose

This procedure is based on the procedure to create a service template in the *NSP Service Management Guide*.

For example, the reference procedure in NSP 23.11 is How do I create a service template?.

6.7.2 Steps

1

Log in to the NSP as the Service Management user.

2

From the **Service Management, Service Templates** view, click **+ CREATE**.

The Create a service template form opens.

3

Configure the parameters, as required.

Parameter	Description
Template Name	Specifies the name of the template
Description	Describes the template
Service Intent Type	`ies`
Intent Version	Specifies which version of the selected service intent type to associated with the template
State	Released
Config Form	Specifies the interface to be used with the template

4

If required, click **+ ADD** in the Workflows panel to add workflows to the service template.

The Add Workflows form opens.

5

Configure the parameters, as required:

Parameter	Description
Workflow Name	Specifies the workflow to be executed
Service Life Cycle State	Specifies the life cycle state of the service that will trigger workflow execution

Parameter	Description
Service Life Cycle Case	Specifies the case, Success or Fail, relative to the life cycle state that will trigger workflow execution
Blocking	Specifies whether unsuccessful execution of the workflow will prevent service life cycle state changes
Workflow Execution Timeout (seconds)	Specifies the length of time, in seconds, that unsuccessful execution of the workflow will prevent service life cycle state changes

6

Click **ADD**.

The Add Workflows form closes and the workflow is added to the service template.

7

If required, select a Default Service Category in the Bulk Association panel to specify a service type to which this service template can be applied in bulk.

8

Click **CREATE**.

The service template is created.

END OF STEPS

6.8 Create and deploy an IES service to the network

6.8.1 Purpose

Perform this procedure to create the service.

This procedure is based on the procedures for creating and auditing a service in the *NSP Service Management Guide*.

For example, the reference procedures in NSP Release 23.11 are:

- How do I create an IES service?
- How do I audit a service?

6.8.2 Steps

1

Log in to the NSP as the Service Management user.

2

From the **Service Management, Services** view, click **+ CREATE**.

The Select a service template to start form opens displaying a list of service templates.

3

Click on an IES service template from the list.

The Create Service form opens with the Template Name parameter populated.

4

Configure the parameters, as required:

Parameter	Description
Service Name	Specifies the name of the service. Must be unique from other services created using NSP.
Customer ID	Specifies the customer ID
Description	Describes the service
Admin State	Specifies the initial administrative state of the service upon deployment
Job ID	Specifies the work-order number
NE Service ID	Specifies the NE service ID

5

In the Site Details panel, click **+ ADD**.

The Add Site form opens.

6

Configure the required parameters:

Parameter	Description
Device ID	Specifies the device identifier
Site Name	Specifies the site name
Description	Describes the site

Note: If site names and descriptions are added, these will take precedence over any service name and description specified in Step 4, with the first-configured site's name and description taking precedence over all others. As such, these attributes will be displayed in various locations, such as NSP's Model Driven Configurator function and NFM-P.

7

Click **+ ADD**.

The Add Interface form opens.

8

Configure the parameters, as required:

Parameter	Description
Interface Name	Specifies the name of the interface
Interface Type	Specifies the interface type (SAP, SDP, or Loopback)
Admin State	Specifies the administrative state of the interface
IP MTU	Describes the interface IP MTU
IPv4	
Address	Specifies the primary IPv4 address to be assigned to the interface
Prefix Length	Specifies the primary IPv4 address prefix length
Secondary (click **+ ADD**)	
Address	Specifies the secondary IPv4 address to be assigned to the interface
Prefix Length	Specifies the secondary IPv4 address prefix length
IPv6 (click **+ ADD**)	
Address	Specifies the IPv6 address to be assigned to the interface
Prefix Length	Specifies the IPv6 address prefix length
SAP	
Port ID	Specifies the port identifier
Admin State	Specifies the administrative state of the service
Description	Describes the SAP
Collect Accounting Statistics	Specifies whether or not accounting statistics will be collected
Enable QoS	Specifies whether or not QoS is enabled
Enable IP/IPv6 Filter	Specifies whether or not an IP/IPv6 filter is enabled
VPLS	
VPLS Name	Specifies the name of the VPLS service

9

Perform the following to specify an accounting policy to be used:

1. Click on the Accounting Policy field. The Select Accounting Policy form opens.
2. Click on an accounting policy in the list, then click **SELECT**. The Select Accounting Policy form closes.

10

In both the IPv4 and IPv6 panels, click **+ ADD** to configure the VRRP parameters as required:

Parameter	Description
Virtual Router ID	Specifies the virtual router identifier (VRID) for the VRRP virtual router instance
Backup	Specifies virtual router IP addresses for the interface
Priority	Specifies the base priority for the VRRP
MAC	Specifies a MAC address to be used by the virtual router instance, overriding the VRRP default derived from the VRID
Ping Reply	Specifies whether or not the non-owner can reply to ICMP echo requests directed to the virtual router instance IP addresses

11

If QoS was enabled in Step 8, configure the parameters as required in both the ingress and egress panels:

Parameter	Description
QoS	
Match QinQ Dot1p (ingress only)	Specifies the match QinQ Dot1p
QinQ Mark Top Only (egress only)	Specifies whether top Q-tags are marked
SAP Ingress	
Policy Name	Specifies the name of the ingress SAP policy
Queuing Type	Specifies the ingress queuing type
SAP Egress	
Policy Name	Specifies the name of the egress SAP policy
Queue (click **+ ADD**)	

Parameter	Description
Queue ID	Specifies the unique identifier for the queue
CBS	Specifies the CBS of the queue
MBS	Specifies the MBS of the queue
PIR	Specifies the PIR rate of the queue
CIR	Specifies the CIR rate of the queue
Policer (click **+ ADD**)	
Policer ID	Specifies the unique identifier for the policer
CBS	Specifies the CBS of the policer
MBS	Specifies the MBS of the policer
Policer Control Policy	
Policy Name	Specifies the name of the policer control policy
Scheduler Policy	
Policy Name	Specifies the name of the scheduler policy
Scheduler (click **+ ADD**)	
Scheduler Name	Specifies the name of the scheduler
PIR	Specifies the PIR rate of the scheduler
CIR	Specifies the CIR rate of the scheduler

12

If an IP/IPv6 filter was enabled in Step 8, configure the parameters as required in both the ingress and egress panels:

Parameter	Description
IP	Specifies the IP filter identifier
IPv6	Specifies the IPv6 filter identifier

Click **ADD** to add the interface. The Add Interface form closes.

13

Repeat Step 6 to Step 12 to add additional interfaces.

Click **ADD** to add the site(s). The Add Site form closes.

14

Perform one of the following:

a. Select the Reserve Resources check box and click **PLAN** to create the service in a Planned state.

b. Click **SAVE** to create the service in a Saved state.

c. Click **DEPLOY** to create the service in a Deployed state.

END OF STEPS

6.9 Modify or delete an IES service

6.9.1 Purpose

Use this procedure if needed to modify configured parameters for an IES service, or to remove a service from the network and delete it.

6.9.2 Steps

Edit a service

1

Log in to the NSP as the Service Management user.

2

From the Service Management, Services view, select a service and choose **Edit** from the ⋮ (Table row actions) menu.

3

Modify the service, site, endpoint or SAP parameters as required.

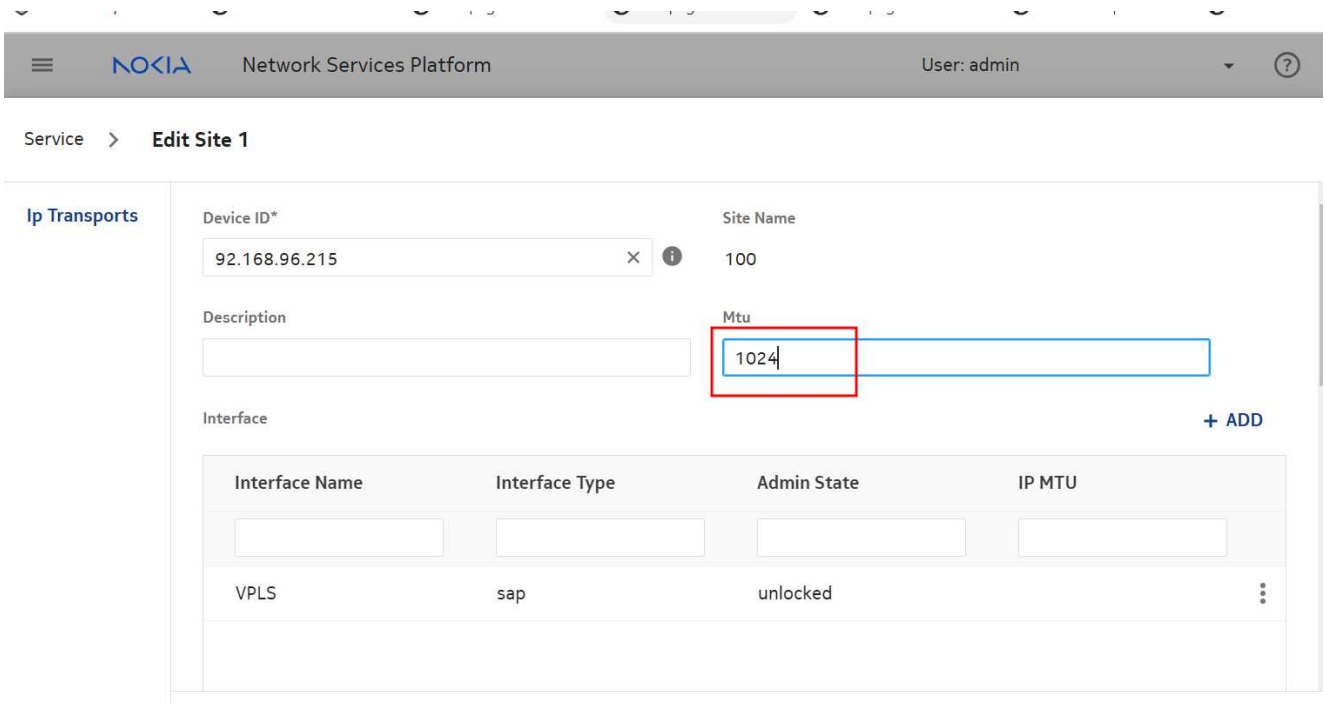
4

Perform one of the following:

a. Select the Reserve Resources check box and click **PLAN** to create the service in a Planned state.

b. Click **SAVE** to create the service in a Saved state.

c. Click **DEPLOY** to create the service in a Deployed state.



Delete a service

5

From the **Service Management**, **Services view**, select a service and click ⋮ (Table row actions), **Remove**.

The Remove Service From Network confirmation dialog opens.

6

Click **REMOVE** to remove the service from the network.

The Life Cycle State of the service is changed to Removed.

7

If you prefer, you can leave the service in Removed state so that it can be deployed again later. To delete the service permanently, proceed to the next step.

8

To delete the service, select the service and click ⋮ (Table row actions), **Delete**.

The Delete Service confirmation dialog opens.

Note: The Delete option only appears if the service is in Removed state.

9

Click DELETE to permanently delete the service from the NSP.

END OF STEPS

Optional procedures

6.10 Create telemetry subscriptions

6.10.1 Purpose

Perform this procedure to set up telemetry collection.

The bundle of vendor agnostic custom resources must be imported and installed to support telemetry collection. The bundle is found on the NSP software delivery site, in the Adaptors folder along with your NE adaptor suite, for example, NSP → 23.11 → Adaptors → Nokia_SROS. Choose the zip file with va and cr in the filename, for example, `nsp-telemetry-cr-va-sros-1.0.0-rel.10.zip`.

This procedure is based on the procedure for managing subscriptions in the *NSP Data Collection and Analysis Guide*.

For example, the reference procedure in NSP 23.11 is How do I manage subscriptions?.

See also the procedure to install telemetry artifacts in the *NSP Data Collection and Analysis Guide* to verify that telemetry prerequisites are in place. The reference procedure for this is in NSP 24.4: How do I install telemetry artifacts?.

CAUTION

Service Disruption

The name of an object, including subscriptions, baselines, indicators, templates, and chart profiles, cannot contain a semicolon (;) or backslash (\).

The use of these characters in an object identifier will result in corrupted data that must be deleted by Nokia support.

6.10.2 Steps

1

Log in to the NSP as the Service Management user.

2

Open **Data Collection and Analysis Management**, **Subscriptions**.

3

To create a subscription:

1. Click + **SUBSCRIPTION**.
2. In the Create Subscription form that opens, configure the General parameters as needed.
   - Enable database (DB) subscriptions as needed to save subscription information to the NSP database. For subscription data to be available to Analytics, the auxiliary database must be deployed.

- The subscription is enabled by default: it will start running immediately.
  Choose **Disabled** in the **State** field if you want to enable your subscription later.

3. In the **Object Filter** field, enter filtering information as needed to filter the collected data.

   As you type, the field provides suggestions for available filters to match your input and identifies incorrect syntax.

   Object filter example: `/nsp-equipment:network/network-element[ne-id='<nedid>']`

4. Enter information in the Telemetry Type field. As you type, the field filters for available telemetry types to match your input.

   Choose the telemetry type you need from the list of matches.

   Telemetry type example: `telemetry:/base/interfaces/interface`

5. When you enter a telemetry type, all counters are enabled by default.

   To customize the counters, enable the **Enable notifications and notification counters** check box.

   Click **Remove** to remove a counter.

   Click **+ COUNTERS** to add a counter that was removed.

6. Click **CREATE**.

   The subscription begins collection when it is enabled.

END OF STEPS

6.11 Create a telemetry chart and plot statistics

6.11.1 Purpose

Use this procedure to chart historical telemetry data. This procedure is based on the procedure for plotting a telemetry chart in the *NSP Data Collection and Analysis Guide*.

For example, the reference procedure in NSP 23.11 is How do I plot a telemetry chart?.

CAUTION

Service Disruption

The name of an object, including subscriptions, baselines, indicators, templates, and chart profiles, cannot contain a semicolon (;) or backslash (\).

The use of these characters in an object identifier will result in corrupted data that must be deleted by Nokia support.

6.11.2 Before you begin

When you create a telemetry chart, you configure a telemetry filter. For historical data to be displayed, the data must be available in the database; see 2.13 “Create telemetry subscriptions” (p. 77).

Charts are created by streaming to the plotter: historical data is queried and streamed to the plotter, then real time telemetry subscriptions are created and the data from these subscriptions is streamed to the plotter.

Data Collection and Analysis Visualizations times out if telemetry data is not received. The time-out limit is either double the collection interval or two minutes, whichever is greater.

6.11.3 Steps

Create a chart

1

Log in to the NSP as the Service Management user.

2

Open the New Chart window:

- From **Data Collection and Analysis Visualizations**, **Telemetry Charts**, click **+ CHART**.
- From **Data Collection and Analysis Management**, **Subscriptions**, choose a subscription and click ⋮ (Table row actions), **Open in Data Collection and Analysis Visualizations**.

3

In the window that opens, configure the parameters in the top panel:

1. Configure the **Collection Interval** parameter. If you are using NFM-P telemetry data, verify that the collection interval is long enough to allow time for Visualizations to receive the data before timing out.
2. From the **Time Range** drop-down list, choose the amount of historical data to display.
3. Click **Combine charts** to plot data from multiple data series on the same chart.

4

Click **+ DEFINITION**.

The telemetry and resource filter definition panels are displayed.

5

Enter information in the **Telemetry Type** field. As you type, the field filters for available telemetry types to match your input.

Choose the telemetry type from the list of matches.

6

Choose counters to display from the **Counters** drop-down list.

7

In the **Object Filter** field, enter filtering information to filter the collected data.

8

If you need to save the configuration as a chart:

1. Click **SAVE AS**.
2. In the window that opens, enter a name for the chart and add a description if needed.
3. Click **SAVE**.

The chart is added to the list.

9

Click **PLOT**.

End of steps

6.11.4 Steps

Plot an existing chart

1

To plot an existing chart with no changes:

1. Open **Data Collection and Analysis Visualizations**, **Telemetry Charts**.
2. Choose a chart and click ⋮ (Table row actions), **Chart**.

2

To edit a chart and plot it, choose the chart and click ⋮ (Table row actions), **Edit**.

3

Edit the parameters as needed and click **PLOT**.

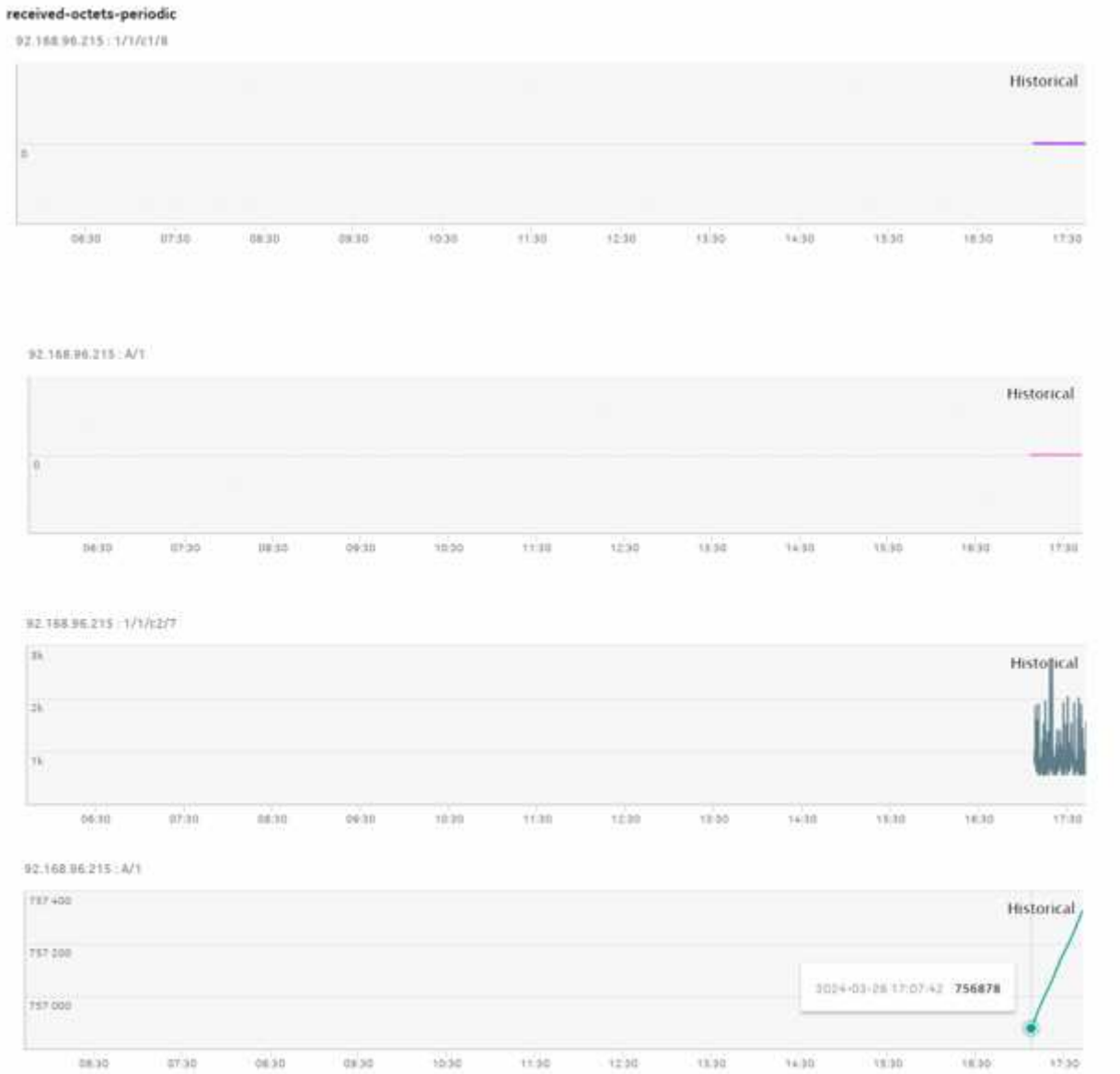
End of steps

6.11.5 Result

Visualizations displays a chart view showing the streaming data. While data is streaming, you can configure the **Group by** parameter in the upper left of the chart view to change how the data is grouped or click **Configure** in the upper right to view or change the configuration of the chart.

Click ⓘ(Chart Details) to open the Chart Details panel on the right side of the chart view to show details about the resources.

Example charts:



7 UCC-20: NE Provisioning - Day/Phase 1 configuration

7.1 Overview

7.1.1 Purpose

This chapter describes the steps that are required to complete the Day/Phase 1 configuration on an NE that has its Day/Phase 0 configuration complete and discovered in NSP. Day/Phase 1 involves network infrastructure configuration of network interfaces, IGP, BGP and IP/MPLS, which enables the control planes to start functioning between discovered network elements.

Configuration examples in this chapter show NSP Release 24.11.

The following NE variants/versions were used to test this use case:

- 7750 SR 14s Classic [Version 23.7R2 and 23.10 R7]
- 7750 SR 14s Model Driven [Version 23.7R2 and 23.10 R7]
- 7250 IXR-6 Model Driven [Version 23.7 R2]

The following NSP device configuration artifact bundles were used to test this use case:

- NSP device configuration product artifacts for SROS (Classic) based nodes [e.g. device-config-artifacts-csros-23-10-1-nsp-23-11-0-cam-v6.zip]
- NSP device configuration product artifacts for SROS Classic and Model Driven nodes with deeper attribute coverage [e.g. device-config-artifacts-gsros-23-10-1-nsp-23-11-0-cam-v4.zip]
- NSP device configuration product artifacts for SROS (Model Driven) based nodes [e.g. device-config-artifacts-msros-23-10-1-nsp-23-11-0-cam-v6.zip]
- NSP device configuration product artifacts for SROS Classic and Model Driven nodes [e.g. device-config-artifacts-usros-23-10-1-nsp-23-11-0-cam-v4.zip]

Note: The configurations described in this guide are generic and actual user configurations might differ based on specific requirements/scenarios.

7.1.2 Contents

Preparation

7.2 Prerequisites

7.2.1 Network configuration prerequisites

Before services can be configured and managed in NSP, the network configuration prerequisites must be met. The following table describes the requirements that can apply to service use cases, and indicates whether each prerequisite is required for this use case.

Note: The NE must be discovered in NSP as a prerequisite to start the Day/Phase 1 configuration. NSP Intents have been used for NE configuration in Day/Phase 1 in most of the places in this chapter. Where an NSP intent type is not available, CLI or MD-CLI must be used to perform configuration on the device.

Prerequisite	Documentation reference	Notes
Mandatory for Brownfield Service Discovery		
GRPC configuration 1. Generate security certificates 2. Configure security and enable GRPC on all devices 3. Apply security certificates on all devices	See SR TLS information here in the SR OS 24.3 R1 documentation: TLS	—
Netconf/SNMP provisioning: enable NETCONF and SNMP protocols on all devices	For more information about SNMP and NETCONF with SR OS, see SNMP and NETCONF in the *SR OS 24.3 R1 System Management Guide*.	—

Prerequisite	Documentation reference	Notes
NSP installation	Pathway for NSP system installation in the *NSP Installation and Upgrade Guide* How do I enable TLS for telemetry and gNMI on_change support? in the *NSP System Administrator Guide*.	Include the following in your deployment: • Feature packs: - platform-baseServices - platform-pluggableNetworkAdaptation - platform-loggingMonitoring - serviceActivationAndConfiguration-intentBasedServiceFulfillment - networkInfrastructureManagement-basicManagement - networkInfrastructureManagement-deviceConfig • Adaptor suites: - sros-common - sros-oc-logical-inventory - sros-23-7-r1
Download the required artifact bundles from the NSP software delivery site: • NSP predefined set for ICM (device configuration)	How do I install an artifact bundle? in the *NSP Network Automation Guide*	—
Device discovery	Pathway for device discovery in the *NSP Classic Management User Guide* How do I discover devices? in the *NSP Device Management Guide* Nokia Developer Portal for information about FTP mediation policy creation using API.	—

Day/Phase 1 configuration

7.3 Cards/MDA

7.3.1 Prerequisites:

- Users must provision power-modules in CLI on 7250 and 7750 nodes or else cards remain in booting / Lo Power state.
- Users must provision SFM in CLI; there is no intent.

7.3.2 To provision power in CLI:

7750 Classic

```
/configure system power-shelf 1 power-shelf-type "ps-a10-shelf-dc"
/configure system power-shelf 1 power-module 1 power-module-type
"ps-a-dc-6000"
/configure system power-shelf 1 power-module 2 power-module-type
"ps-a-dc-6000"
/configure system power-shelf 1 power-module 3 power-module-type
"ps-a-dc-6000"
/configure system power-shelf 1 power-module 4 power-module-type
"ps-a-dc-6000"
/configure system power-shelf 1 power-module 5 power-module-type
"ps-a-dc-6000"
/configure system power-shelf 1 power-module 6 power-module-type
"ps-a-dc-6000"
/configure system power-shelf 1 power-module 7 power-module-type
"ps-a-dc-6000"
/configure system power-shelf 1 power-module 8 power-module-type
"ps-a-dc-6000"
/configure system power-shelf 1 power-module 9 power-module-type
"ps-a-dc-6000"
/configure system power-shelf 1 power-module 10 power-module-type
"ps-a-dc-6000"
/admin save
```

7750 MD

```
/edit-config private
/configure chassis router chassis-number 1 power-shelf 1 power-shelf-type
ps-a10-shelf-dc
/configure chassis router chassis-number 1 power-shelf 1 power-module 1
power-module-type ps-a-dc-6000
/configure chassis router chassis-number 1 power-shelf 1 power-module 2
power-module-type ps-a-dc-6000
/configure chassis router chassis-number 1 power-shelf 1 power-module 3
power-module-type ps-a-dc-6000
/configure chassis router chassis-number 1 power-shelf 1 power-module 4
```

```
power-module-type ps-a-dc-6000
/configure chassis router chassis-number 1 power-shelf 1 power-module 5
power-module-type ps-a-dc-6000
/configure chassis router chassis-number 1 power-shelf 1 power-module 6
power-module-type ps-a-dc-6000
/configure chassis router chassis-number 1 power-shelf 1 power-module 7
power-module-type ps-a-dc-6000
/configure chassis router chassis-number 1 power-shelf 1 power-module 8
power-module-type ps-a-dc-6000
/configure chassis router chassis-number 1 power-shelf 1 power-module 9
power-module-type ps-a-dc-6000
/configure chassis router chassis-number 1 power-shelf 1 power-module 10
power-module-type ps-a-dc-6000
/commit
/admin save
/quit-config
```

```
A:admin@Boston#  show chassis power-shelf 1 power-module

===============================================================================
Power Shelf Summary
===============================================================================
Slot       Provisioned Type            Admin Operational   Zone   Input Output
               Equipped Type (if diff) State State                   Mode
-------------------------------------------------------------------------------
1          ps-a10-shelf-dc             up    up            1      60A   on
===============================================================================


===============================================================================
Power Module Summary
===============================================================================
Slot       Provisioned Type            Admin Operational   Input  Zone
               Equipped Type (if diff) State State         A B
-------------------------------------------------------------------------------
1          ps-a-dc-6000                up    up            Y Y    1
2          ps-a-dc-6000                up    up            Y Y    1
3          ps-a-dc-6000                up    up            Y Y    1
4          ps-a-dc-6000                up    up            Y Y    1
5          ps-a-dc-6000                up    up            Y Y    1
6          ps-a-dc-6000                up    up            Y Y    1
7          ps-a-dc-6000                up    up            Y Y    1
8          ps-a-dc-6000                up    up            Y Y    1
9          ps-a-dc-6000                up    up            Y Y    1
10         ps-a-dc-6000                up    up            Y Y    1
===============================================================================
```

7250 MD

```
/edit-config private
/configure chassis router chassis-number 1 power-module 2
```

```
power-module-type ixr-dc-3000
/configure chassis router chassis-number 1 power-module 3
power-module-type ixr-dc-3000
/configure chassis router chassis-number 1 power-module 4
power-module-type ixr-dc-3000
/configure chassis router chassis-number 1 power-module 5
power-module-type ixr-dc-3000
/configure chassis router chassis-number 1 power-module 6
power-module-type ixr-dc-3000
/commit
/admin save
/quit-config
```

```
A:admin@CE_West# show chassis power-module

===============================================================================
Power Module Summary
===============================================================================
Slot       Provisioned Type            Admin Operational   Input  Zone
               Equipped Type (if diff) State State         A B
-------------------------------------------------------------------------------
1          (not provisioned)           up    unprovisioned Y -    1
               ixr-dc-3000
2          ixr-dc-3000                 up    up            Y -    1
3          ixr-dc-3000                 up    up            Y -    1
4          ixr-dc-3000                 up    up            Y -    1
5          ixr-dc-3000                 up    up            Y -    1
6          ixr-dc-3000                 up    up            Y -    1
===============================================================================
```

7.3.3 To provision SFM:

7750 Classic

```
/configure sfm 1 sfm-type sfm-s
/configure sfm 2 sfm-type sfm-s
/configure sfm 3 sfm-type sfm-s
/configure sfm 4 sfm-type sfm-s
/configure sfm 5 sfm-type sfm-s
/configure sfm 6 sfm-type sfm-s
/configure sfm 7 sfm-type sfm-s
/configure sfm 8 sfm-type sfm-s
/admin save
```

7750 MD

```
/edit-config private
/configure sfm 1 sfm-type sfm-s
```

```
/configure sfm 2 sfm-type sfm-s
/configure sfm 3 sfm-type sfm-s
/configure sfm 4 sfm-type sfm-s
/configure sfm 5 sfm-type sfm-s
/configure sfm 6 sfm-type sfm-s
/configure sfm 7 sfm-type sfm-s
/configure sfm 8 sfm-type sfm-s
/commit
/admin save
/quit-config
```

```
A:admin@Boston# show sfm

===============================================================================
SFM Summary
===============================================================================
Slot      Provisioned Type                          Admin Operational   Comments
              Equipped Type (if different)          State State
-------------------------------------------------------------------------------
1         sfm-s                                     up    up
2         sfm-s                                     up    up
3         sfm-s                                     up    up
4         sfm-s                                     up    up
5         sfm-s                                     up    up
6         sfm-s                                     up    up
7         sfm-s                                     up    up
8         sfm-s                                     up    up
===============================================================================
```

7250 MD

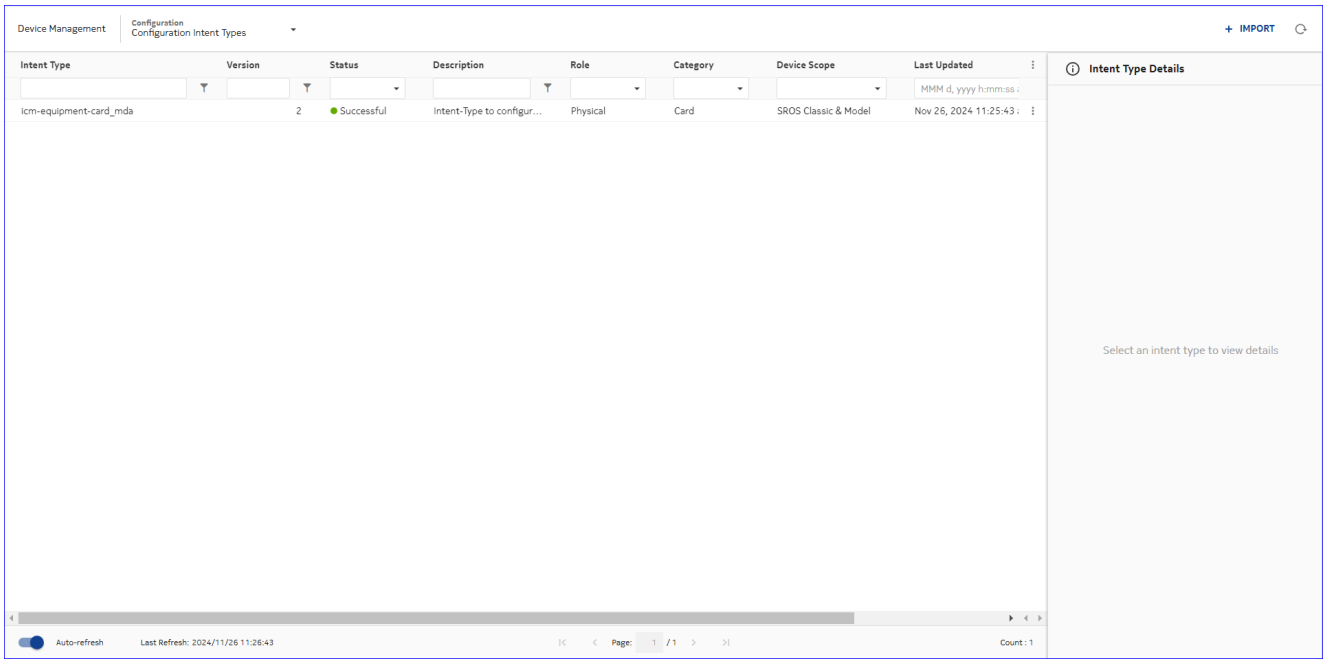
```
/edit-config private
/configure sfm 1 sfm-type sfm-ixr-6
/configure sfm 2 sfm-type sfm-ixr-6
/configure sfm 3 sfm-type sfm-ixr-6
/configure sfm 4 sfm-type sfm-ixr-6
/configure sfm 5 sfm-type sfm-ixr-6
/configure sfm 6 sfm-type sfm-ixr-6
/commit
/admin save
/quit-config
```

```
A:admin@CE_West# show sfm

===============================================================================
SFM Summary
===============================================================================
Slot      Provisioned Type                          Admin Operational   Comments
              Equipped Type (if different)          State State
-------------------------------------------------------------------------------
1         sfm-ixr-6                                 up    up
2         sfm-ixr-6                                 up    up
3         sfm-ixr-6                                 up    up
4         sfm-ixr-6                                 up    up
5         sfm-ixr-6                                 up    up
6         sfm-ixr-6                                 up    up
===============================================================================
```

7.3.4 To configure Card/MDA using icm-equipment-card_mda intent

1

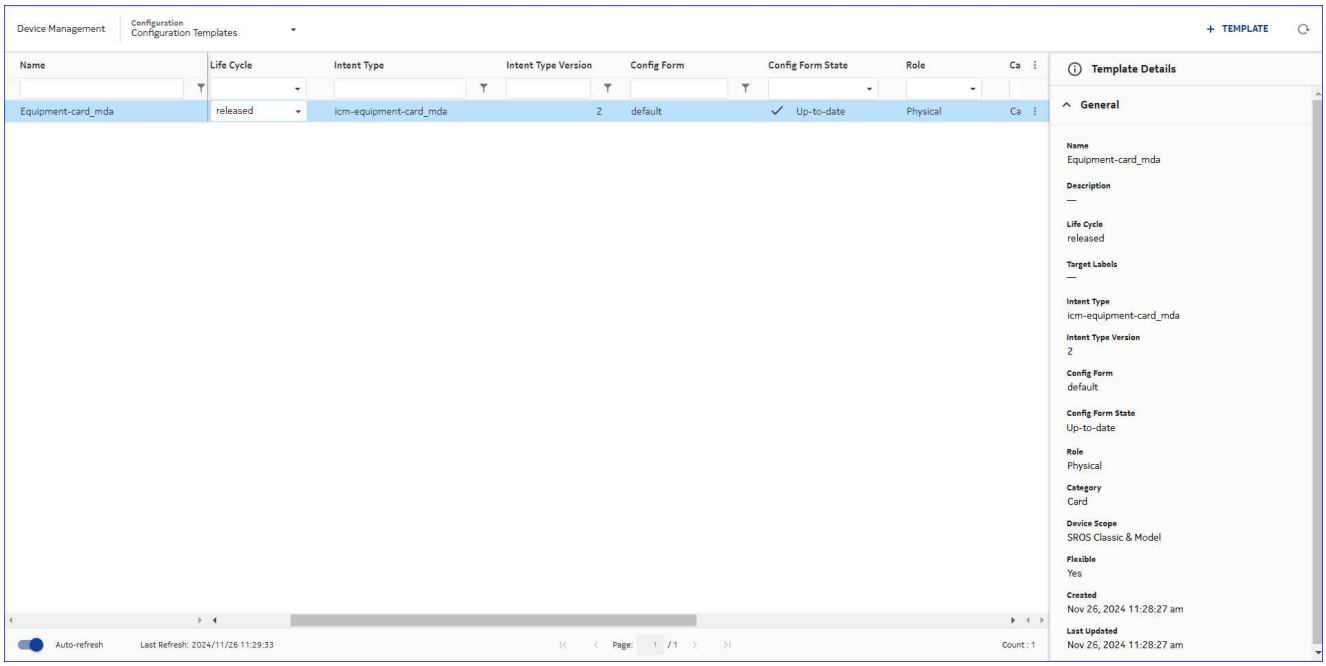
Import the intent type **icm-equipment-card_mda** into **Device Management**, **Configuration Intent Types**.



2

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

For example, the configuration template created below is named as **Equipment-card_mda**.



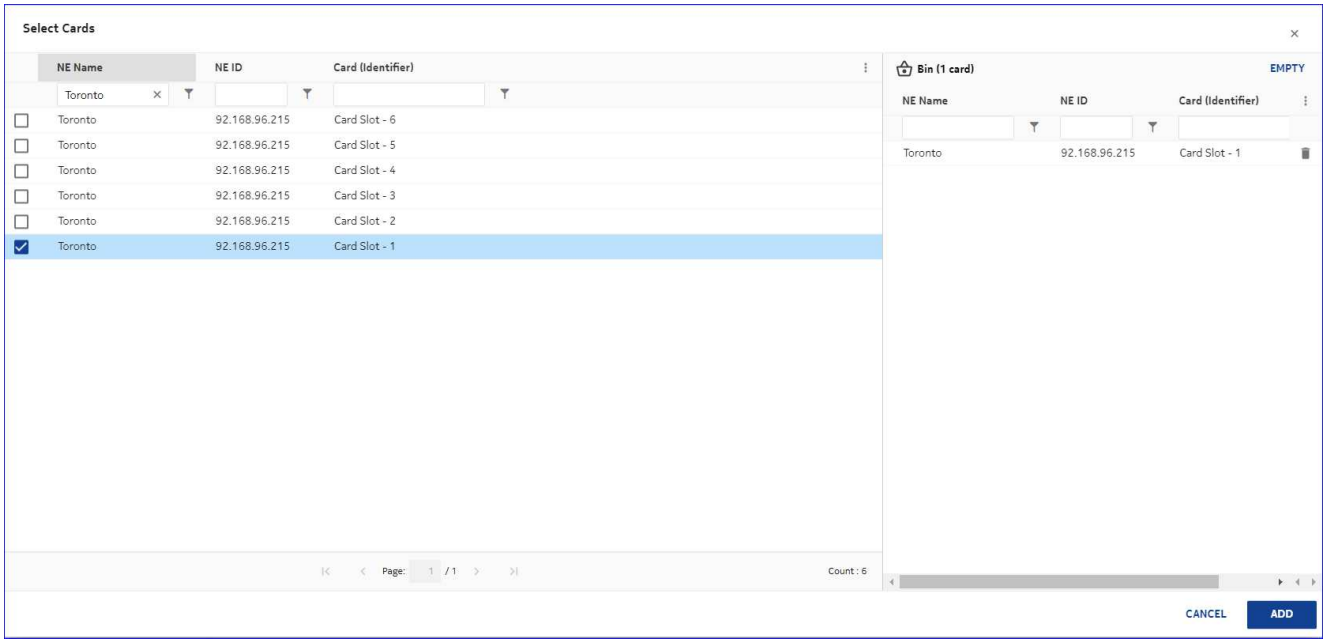
3

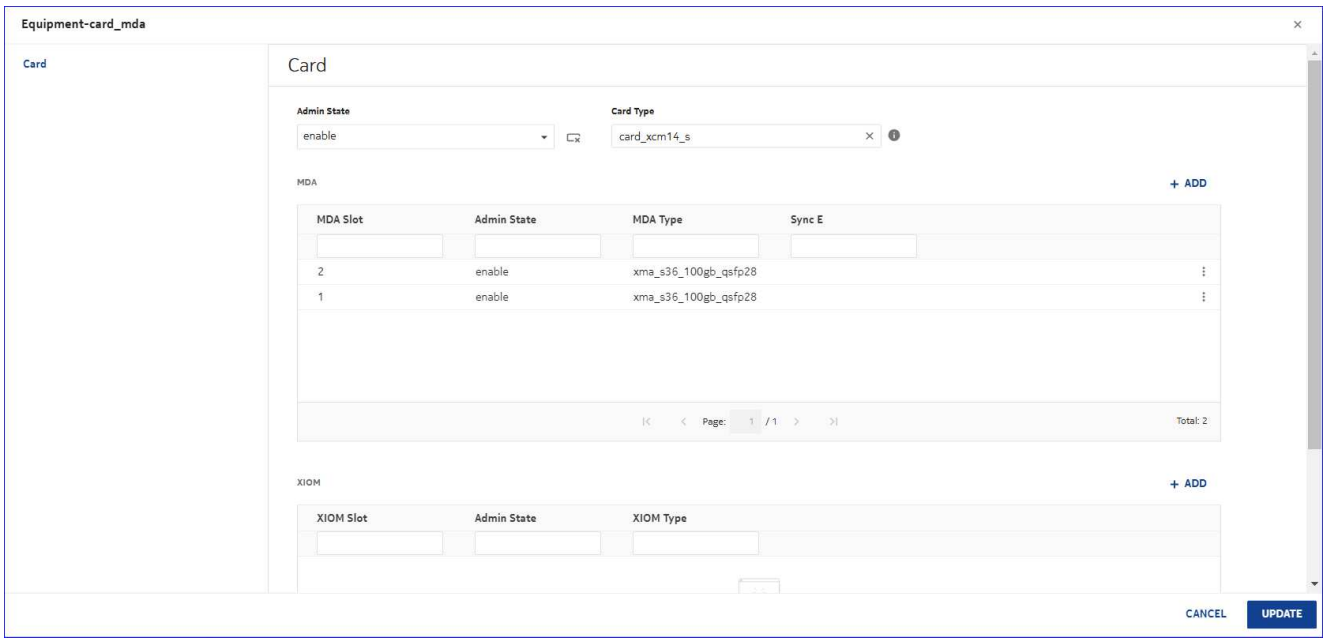
Create configuration deployments with the above configuration template. The following example uses 7750 (SR-14s variant):

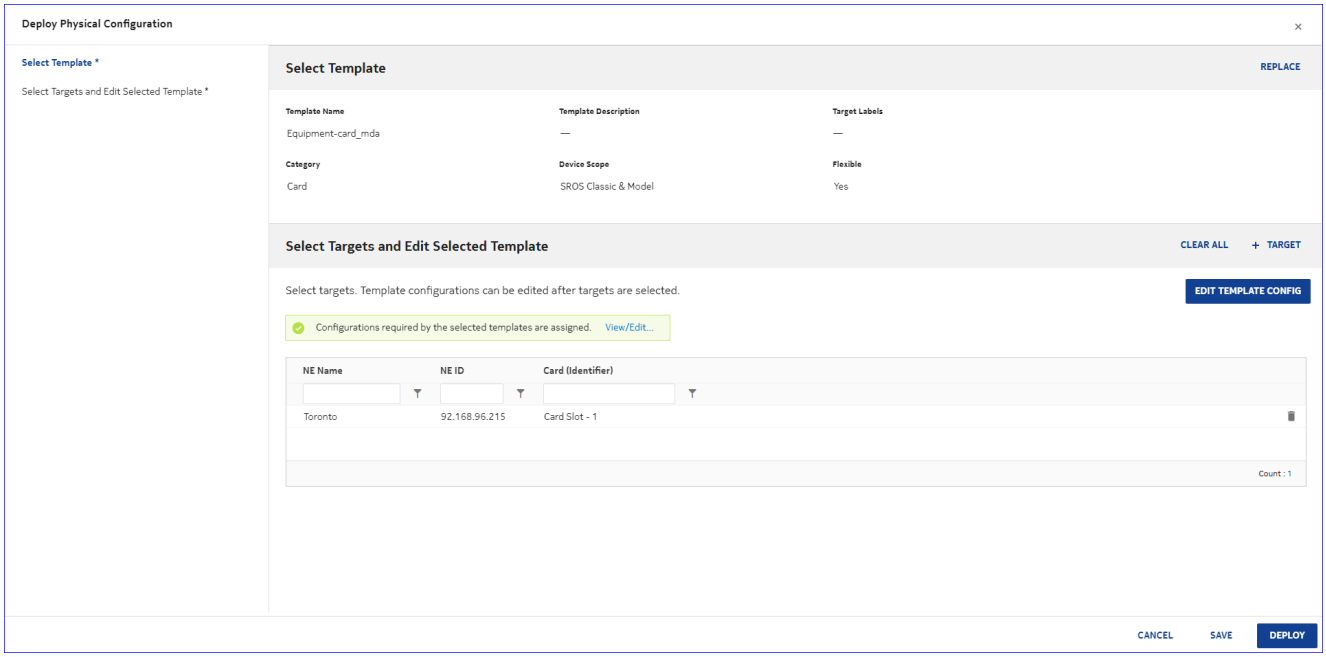
Card slot 1: card_xcm14_s (xcm-14s on MD)

MDA slot 1 and 2: xma_s36_100gb_qsfp28 (s36-100gb-qsfp28 on MD)

Ex. 7750 Classic







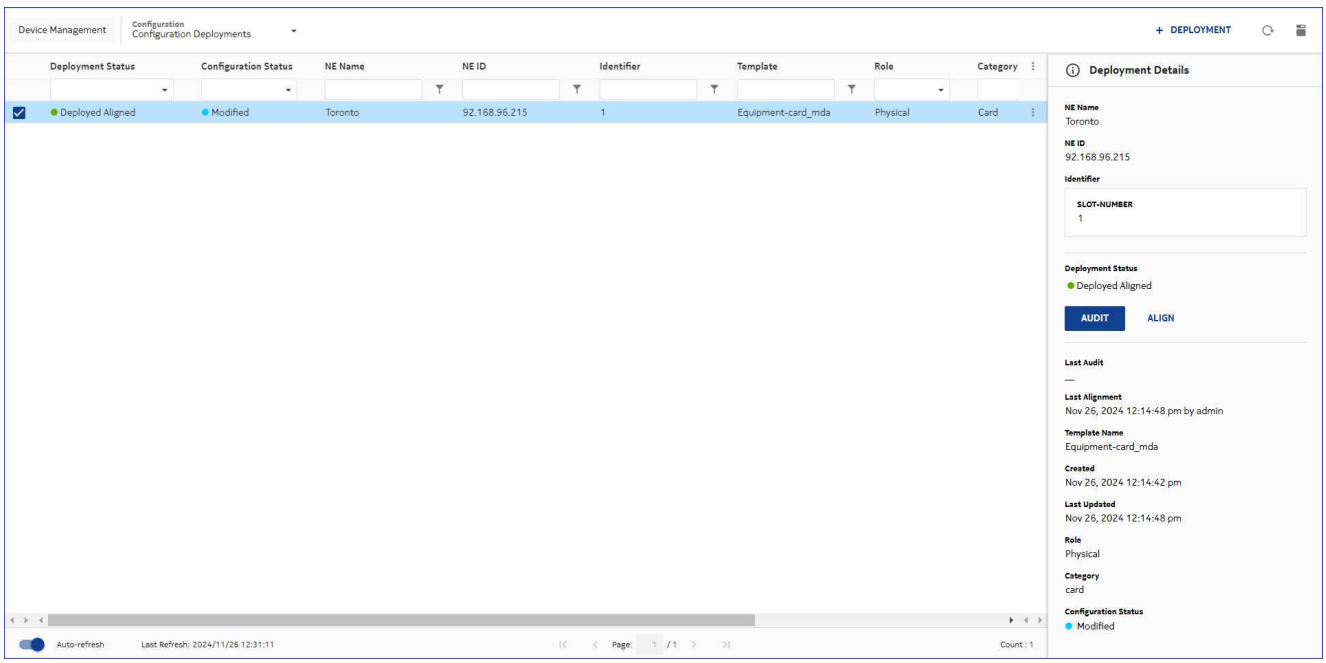
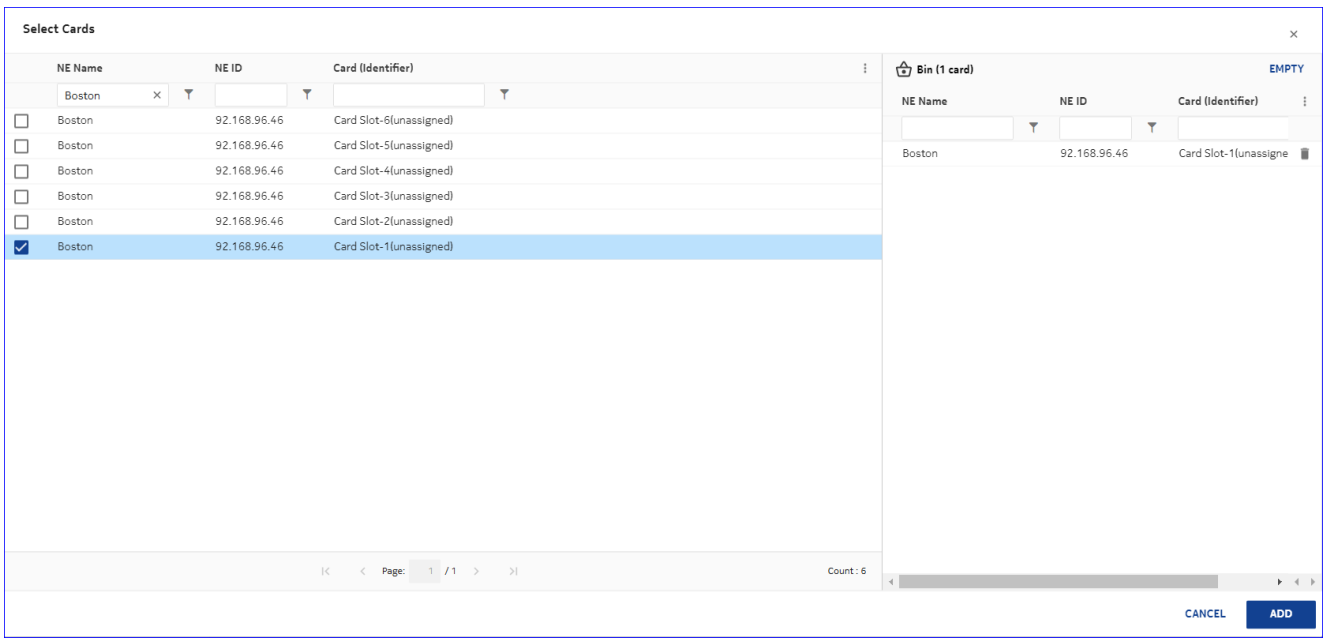
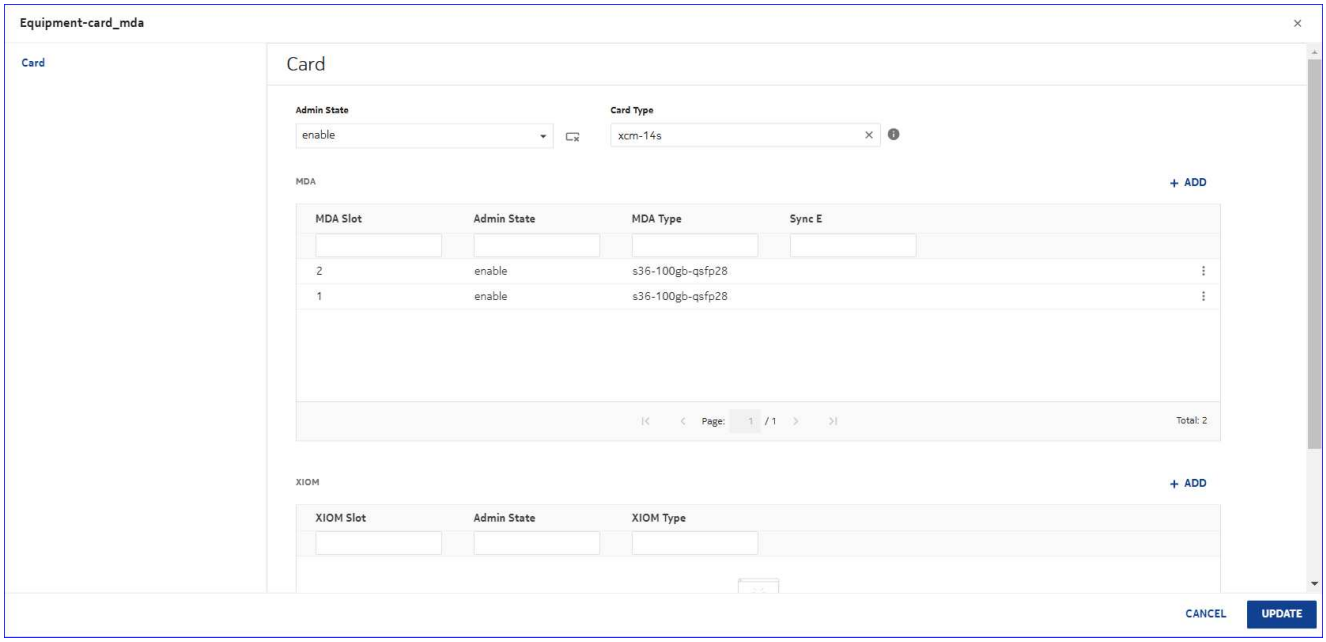


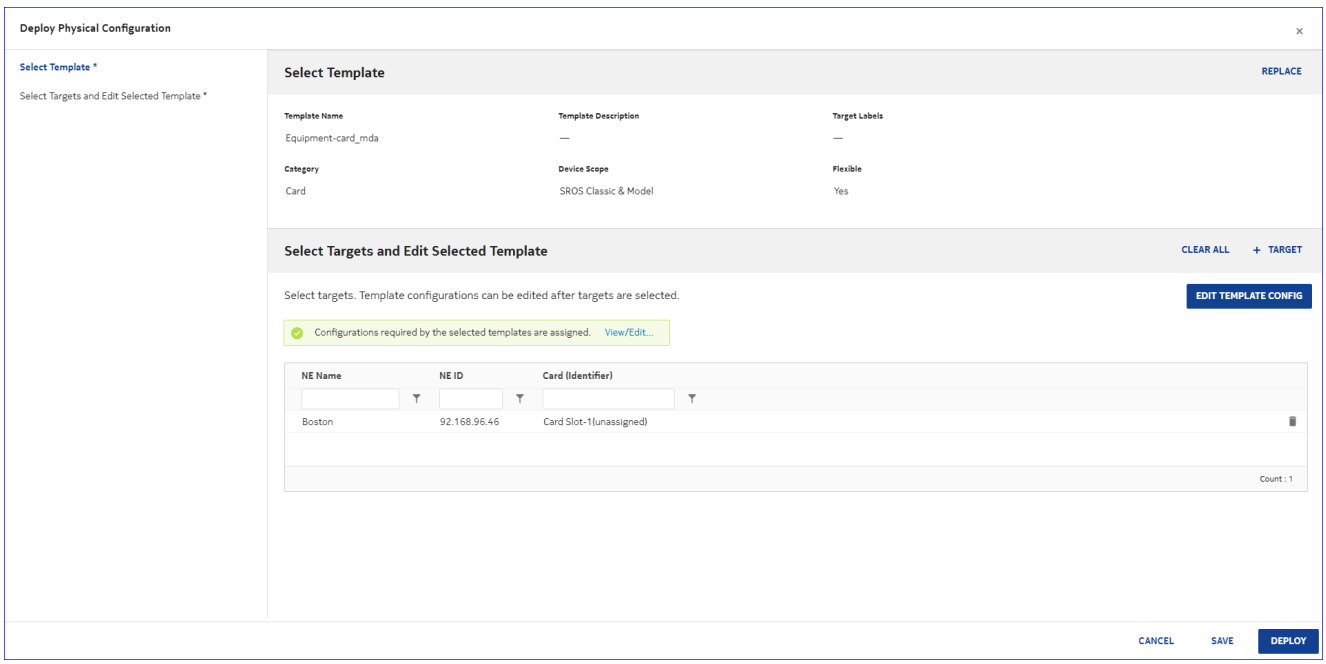
Figure 7-1 NE CLI check after deployment

```
A:Toronto# show card state

===============================================================================
Card State
===============================================================================
Slot/  Provisioned Type                    Admin Operational   Num   Num Comments
Id         Equipped Type (if different)    State State         Ports MDA
-------------------------------------------------------------------------------
1      xcm-14s                             up    up                  2
1/1    s36-100gb-qsfp28:he2400g+           up    up            36
1/2    s36-100gb-qsfp28:he2400g+           up    up            36
A      cpm-s                               up    up                      Active
B      cpm-s                               up    down                    Standby
           (not equipped)
===============================================================================
```

Ex. 7750 MD







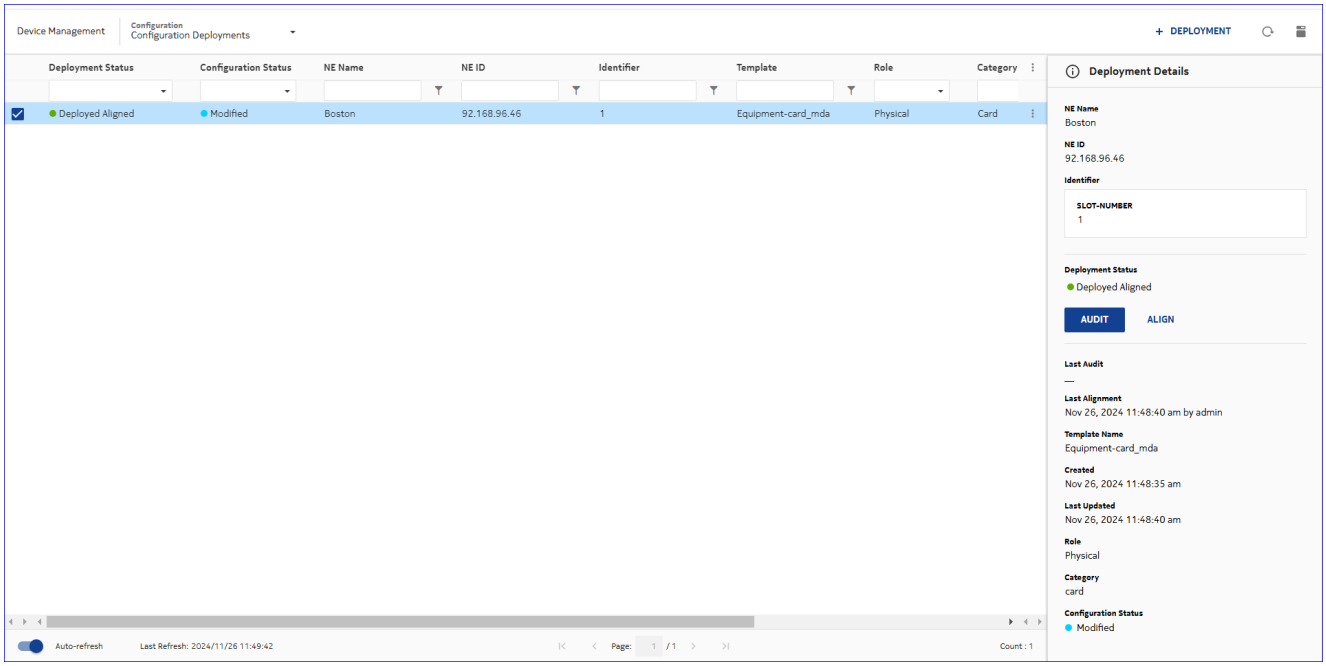


Figure 7-2 NE CLI check after deployment

```
A:admin@Boston# show card state

===============================================================================
Card State
===============================================================================
Slot/  Provisioned Type                  Admin Operational    Num    Num Comments
Id         Equipped Type (if different)  State State          Ports  MDA
-------------------------------------------------------------------------------
1      xcm-14s                           up    up                    2
1/1    s36-100gb-qsfp28:he2400g+         up    up             36
1/2    s36-100gb-qsfp28:he2400g+         up    up             36
A      cpm-s                             up    up                          Active
B      cpm-s                             up    down                        Standby
           (not equipped)
===============================================================================
```

END OF STEPS

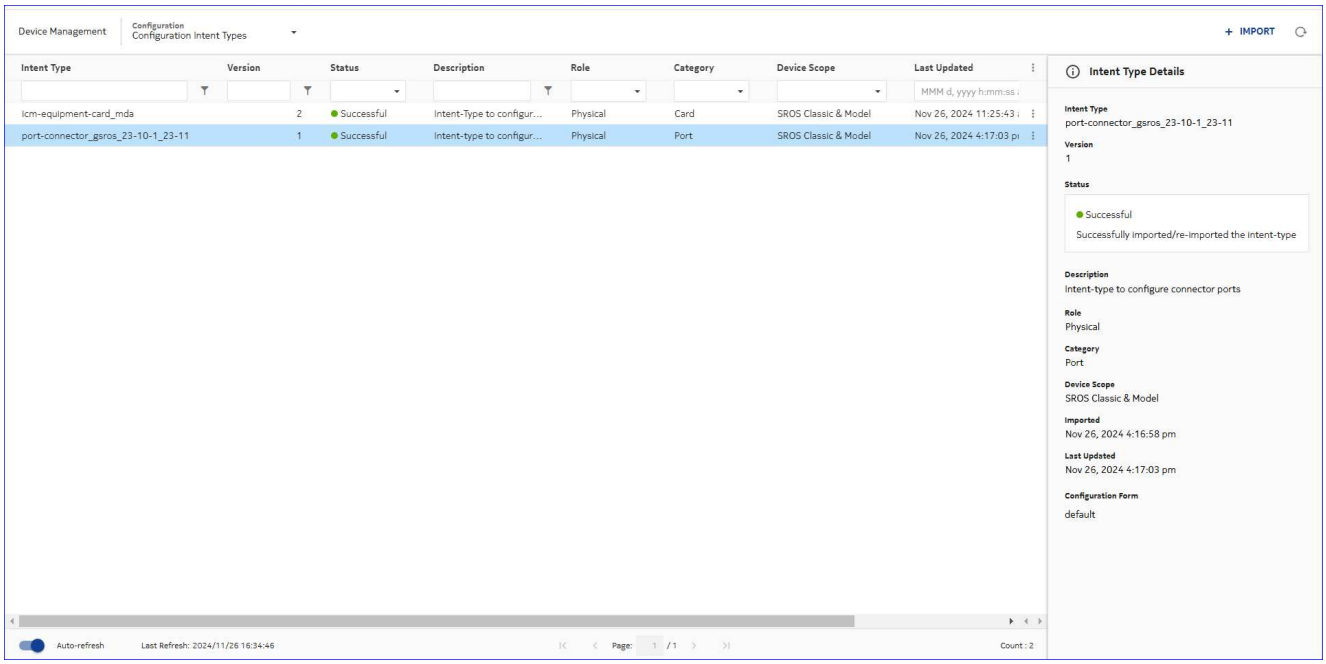
7.4 Port/Connector

7.4.1 To configure Port and Connectors using intent port-connector_gsros_23-10-1_23-11

port-connector_gsros_23-10-1_23-11 intent supports configuration of Breakout Type on connector port.

1

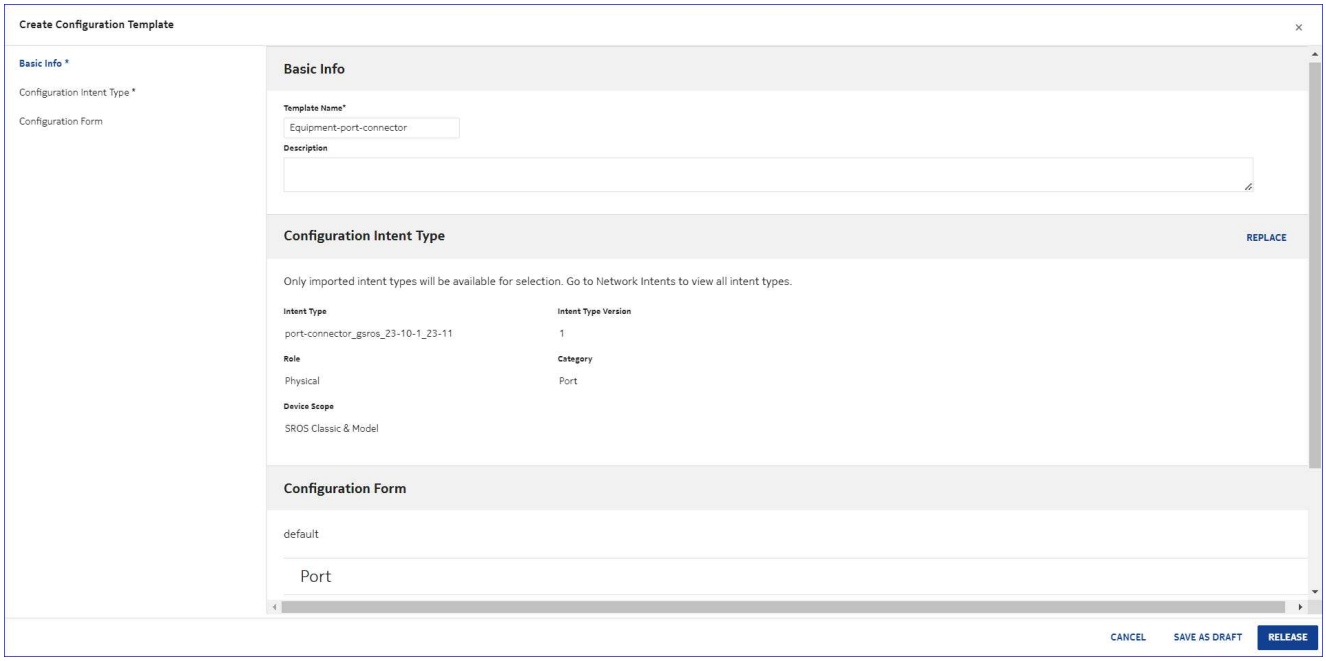
Import the intent type **port-connector_gsros_23-10-1_23-11** into **Device Management**, **Configuration Intent Types**.

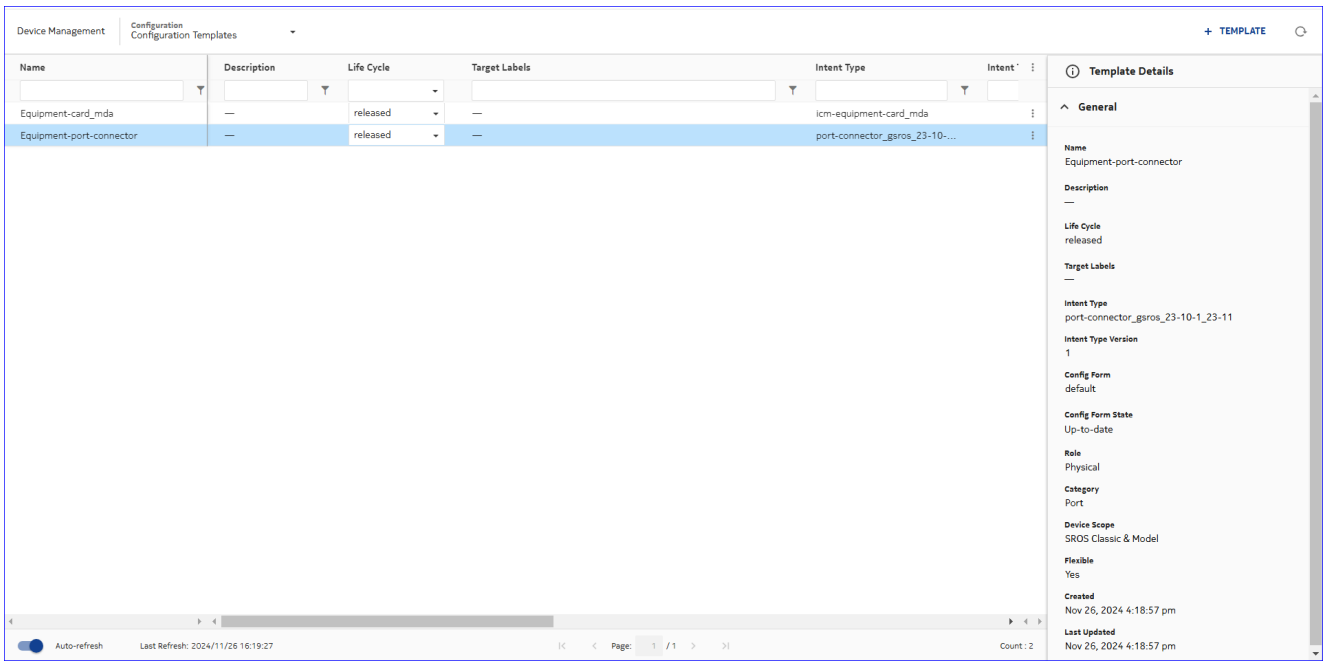


2

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

For example, the configuration template created below is named as **Equipment-port-connector**.



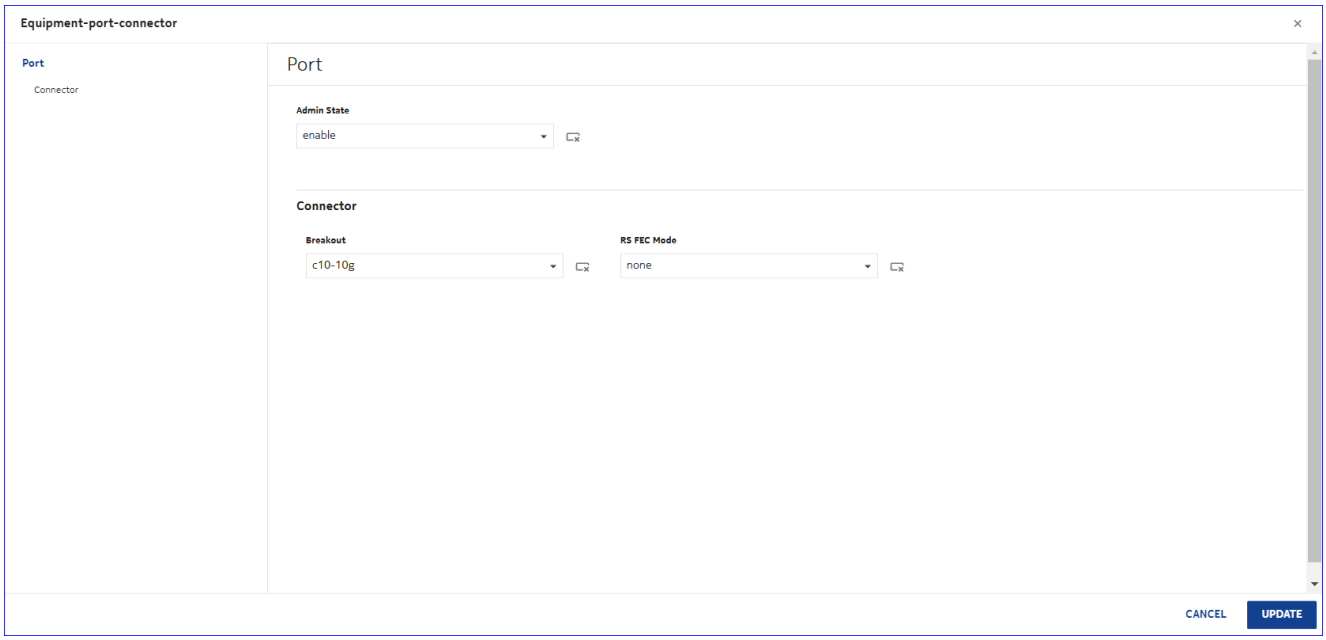


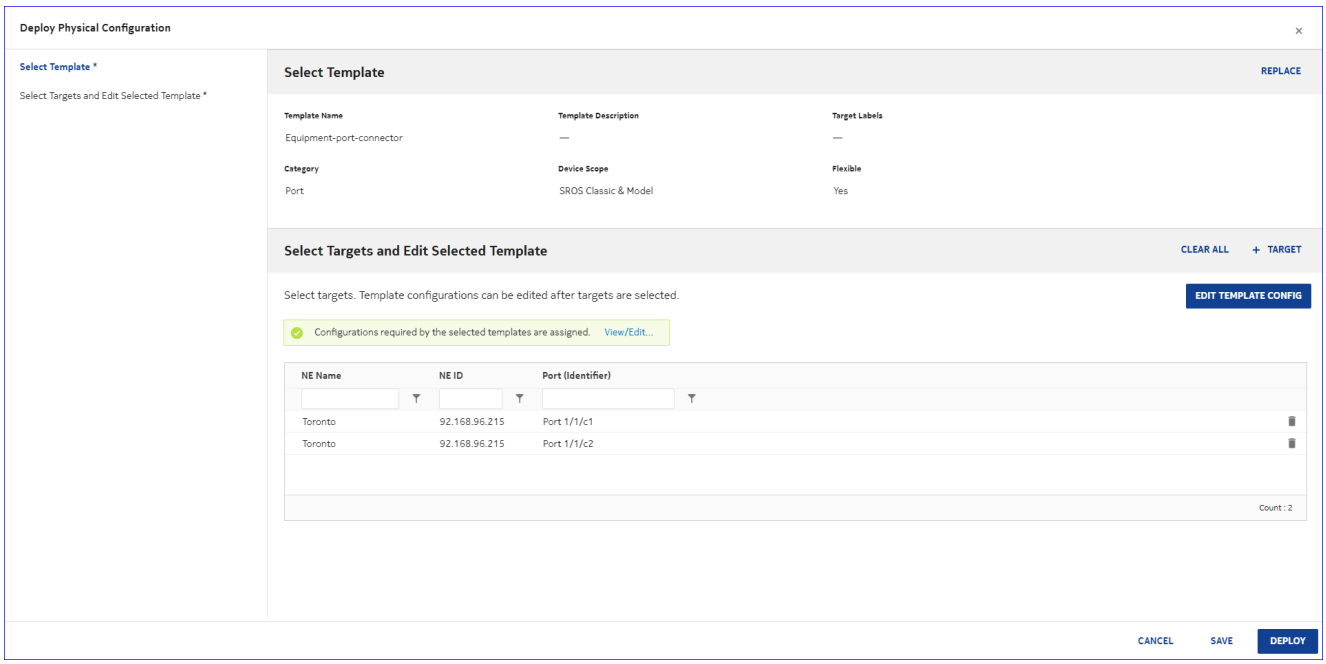
3

Create configuration deployments using the above configuration template.

For the following examples, targets are 1/1/c1 and 1/1/c2 for 7750 classic and MD nodes; selected c10-10g breakout on classic 7750 SR.

Ex. 7750 Classic





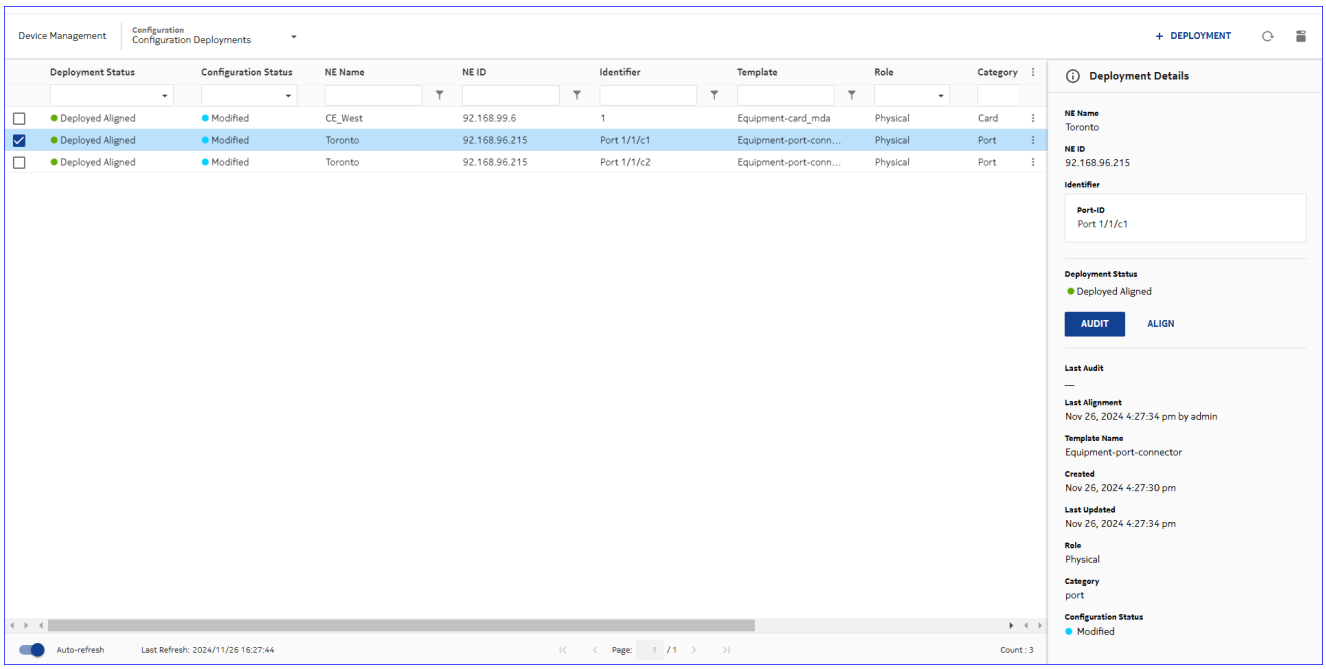
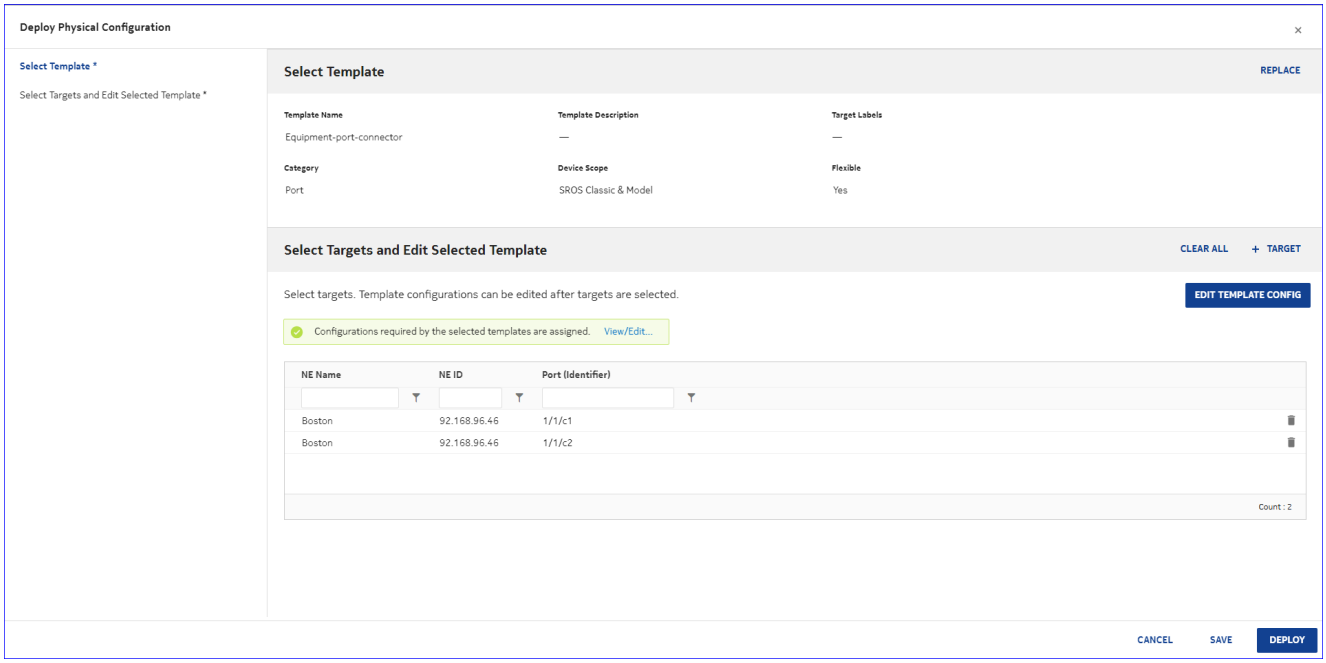


Figure 7-3 NE CLI check after deployment

```
*A:Toronto>config# /show port

===============================================================================
Ports on Slot 1
===============================================================================
Port          Admin Link Port    Cfg  Oper LAG/ Port Port Port   C/QS/S/XFP/
Id            State      State   MTU  MTU  Bndl Mode Encp Type   MDIMDX
-------------------------------------------------------------------------------
1/1/c1        Up         Link Up                          conn   100GBASE-LR4*
1/1/c1/1      Up    Yes  Up      8704 8704    - netw null xgige
1/1/c1/2      Up    Yes  Up      8704 8704    - netw null xgige
1/1/c1/3      Up    Yes  Up      8704 8704    - netw null xgige
1/1/c1/4      Up    Yes  Up      8704 8704    - netw null xgige
1/1/c1/5      Up    No   Down    8704 8704    - netw null xgige
1/1/c1/6      Up    No   Down    8704 8704    - netw null xgige
1/1/c1/7      Up    No   Down    8704 8704    - netw null xgige
1/1/c1/8      Up    No   Down    8704 8704    - netw null xgige
1/1/c1/9      Up    No   Down    8704 8704    - netw null xgige
1/1/c1/10     Up    No   Down    8704 8704    - netw null xgige
1/1/c2        Up         Link Up                          conn   100GBASE-LR4*
1/1/c2/1      Up    Yes  Up      8704 8704    - netw null xgige
1/1/c2/2      Up    Yes  Up      8704 8704    - netw null xgige
1/1/c2/3      Up    Yes  Up      8704 8704    - netw null xgige
1/1/c2/4      Up    Yes  Up      8704 8704    - netw null xgige
1/1/c2/5      Up    Yes  Up      8704 8704    - netw null xgige
1/1/c2/6      Up    Yes  Up      8704 8704    - netw null xgige
1/1/c2/7      Up    Yes  Up      8704 8704    - netw null xgige
1/1/c2/8      Up    Yes  Up      8704 8704    - netw null xgige
1/1/c2/9      Up    No   Down    8704 8704    - netw null xgige
1/1/c2/10     Up    No   Down    8704 8704    - netw null xgige
1/1/c3        Up         Down                             conn   100GBASE-LR4*
1/1/c4        Up         Down                             conn   100GBASE-LR4*
1/1/c5        Up         Down                             conn   100GBASE-LR4*
```

Ex. 7750 MD



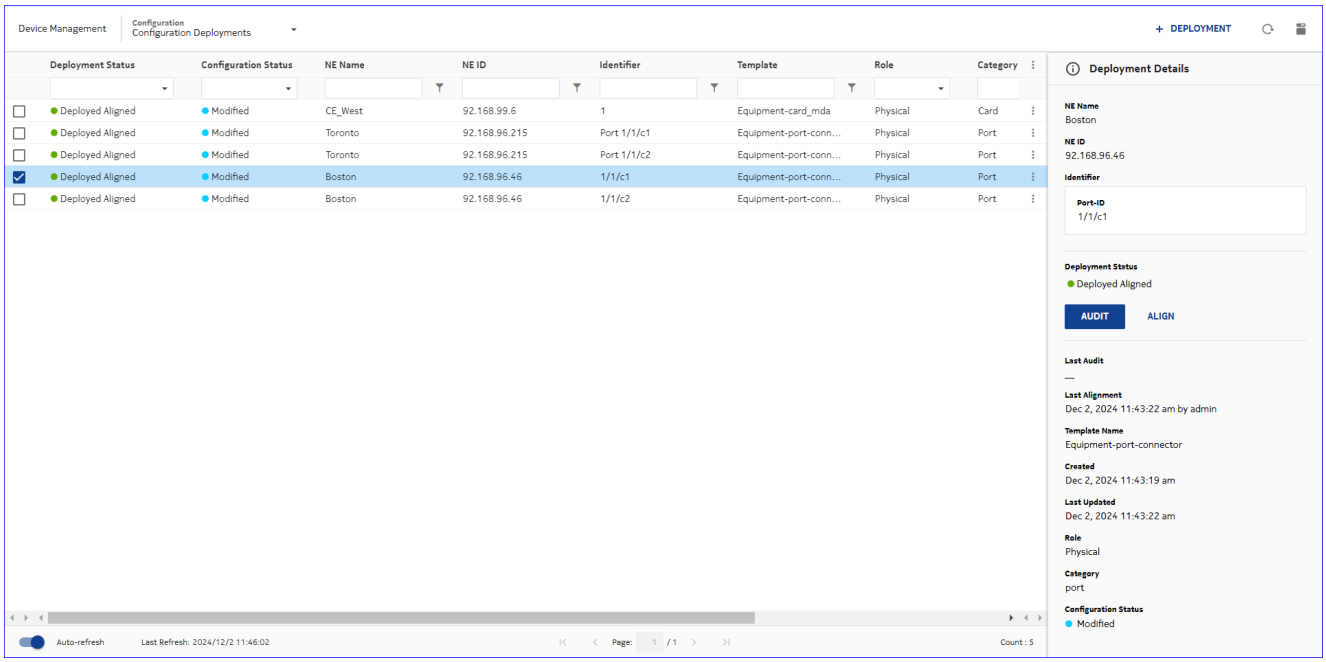


Figure 7-4 NE CLI check after deployment

```
A:admin@Boston# show port

===============================================================================
Ports on Slot 1
===============================================================================
Port          Admin Link Port    Cfg  Oper LAG/ Port Port Port   C/QS/S/XFP/
Id            State      State   MTU  MTU  Bndl Mode Encp Type   MDIMDX
-------------------------------------------------------------------------------
1/1/c1        Up         Link Up                          conn   100GBASE-LR4*
1/1/c1/1      Down  No   Down    8704 8704    - netw null xgige
1/1/c1/2      Down  No   Down    8704 8704    - netw null xgige
1/1/c1/3      Down  No   Down    8704 8704    - netw null xgige
1/1/c1/4      Down  No   Down    8704 8704    - netw null xgige
1/1/c1/5      Down  No   Down    8704 8704    - netw null xgige
1/1/c1/6      Down  No   Down    8704 8704    - netw null xgige
1/1/c1/7      Down  No   Down    8704 8704    - netw null xgige
1/1/c1/8      Down  No   Down    8704 8704    - netw null xgige
1/1/c1/9      Down  No   Down    8704 8704    - netw null xgige
1/1/c1/10     Down  No   Down    8704 8704    - netw null xgige
1/1/c2        Up         Link Up                          conn   100GBASE-LR4*
1/1/c2/1      Down  No   Down    8704 8704    - netw null xgige
1/1/c2/2      Down  No   Down    8704 8704    - netw null xgige
1/1/c2/3      Down  No   Down    8704 8704    - netw null xgige
1/1/c2/4      Down  No   Down    8704 8704    - netw null xgige
1/1/c2/5      Down  No   Down    8704 8704    - netw null xgige
1/1/c2/6      Down  No   Down    8704 8704    - netw null xgige
1/1/c2/7      Down  No   Down    8704 8704    - netw null xgige
1/1/c2/8      Down  No   Down    8704 8704    - netw null xgige
1/1/c2/9      Down  No   Down    8704 8704    - netw null xgige
1/1/c2/10     Down  No   Down    8704 8704    - netw null xgige
1/1/c3        Down       Down                             conn   100GBASE-LR4*
1/1/c4        Down       Down                             conn   100GBASE-LR4*
1/1/c5        Down       Down                             conn   100GBASE-LR4*
```

END OF STEPS

7.4.2 To configure Port using intent icm-equipment-port-ethernet

icm-equipment-port-ethernet intent type deployment can be created on ethernet ports. For this use case, after connector deployment, ethernet port configuration was tested on some of the newly created ports.

1

Prerequisites:

For Classic NE:

- Accounting policy

```
/configure log accounting-policy 36 record complete-ethernet-port
/configure log accounting-policy 36 no shutdown
```

```
/admin save
```

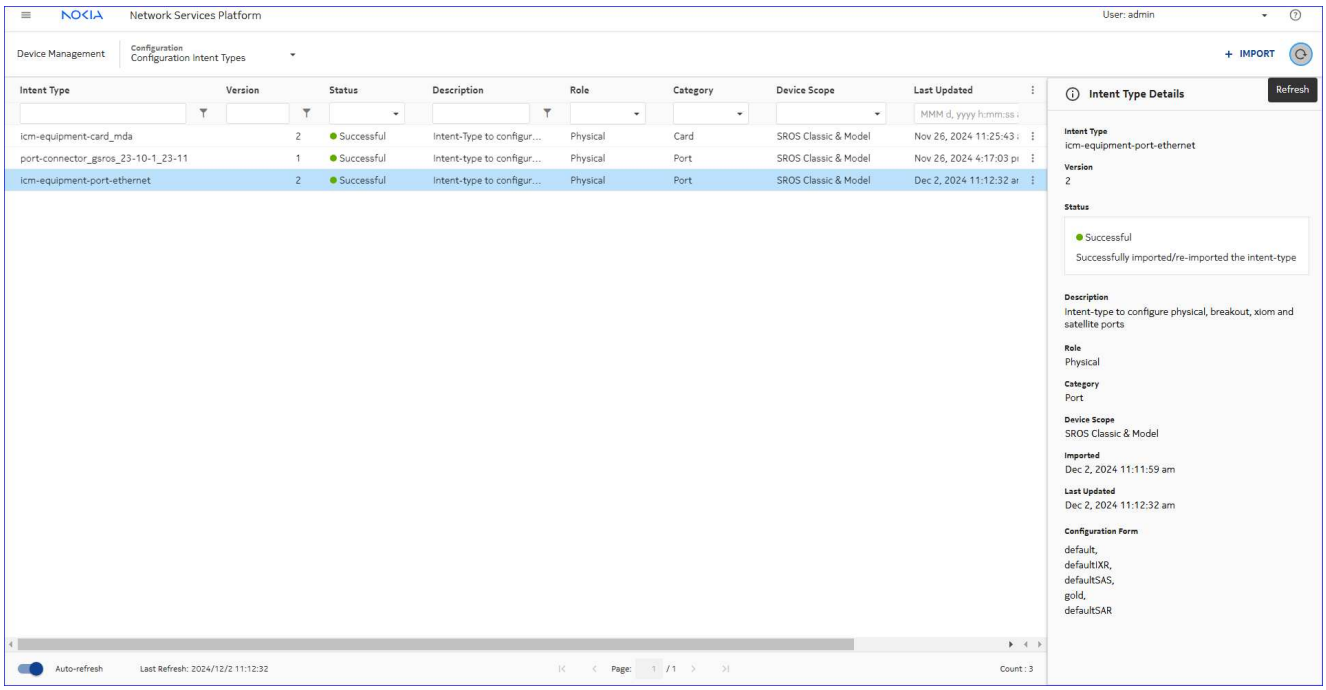
For MD NE:

- Accounting policy

```
/edit-config private
/configure log accounting-policy 36 record complete-ethernet-port
/commit
/quit-config
```

2

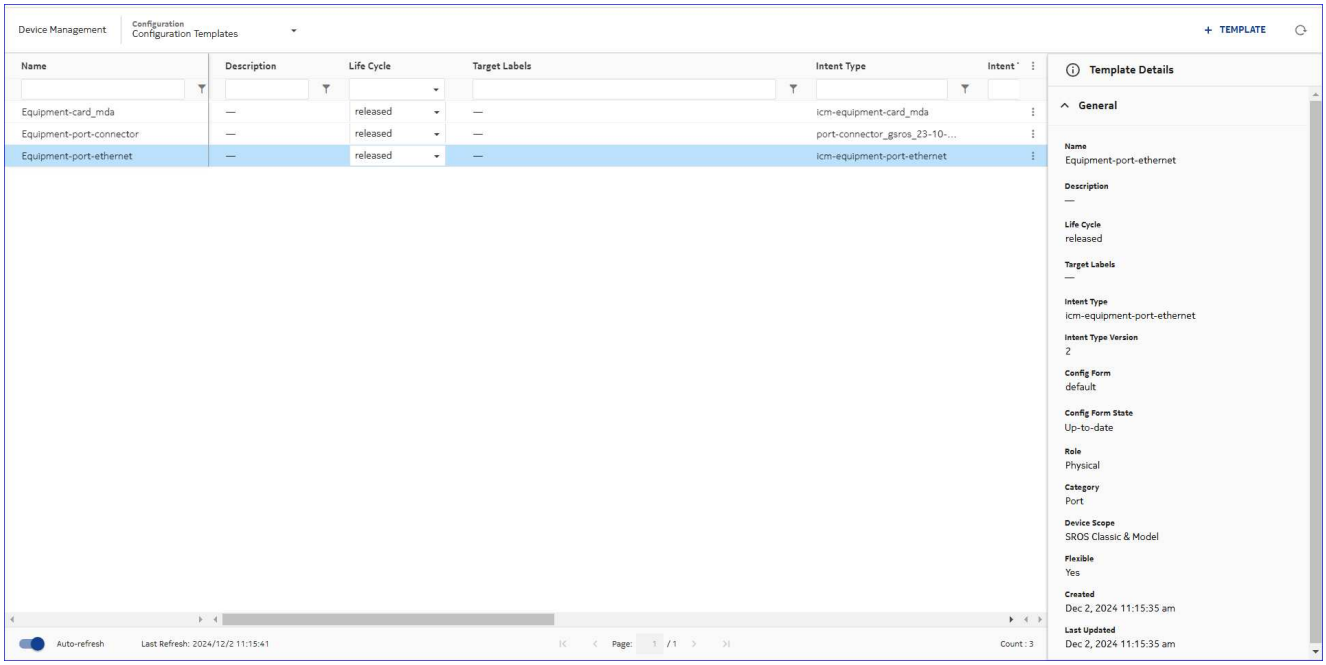
Import the intent type **icm-equipment-port-ethernet** into **Device Management**, **Configuration Intent Types**.



3

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

For example, the configuration template created below is named as **Equipment-port-ethernet**.



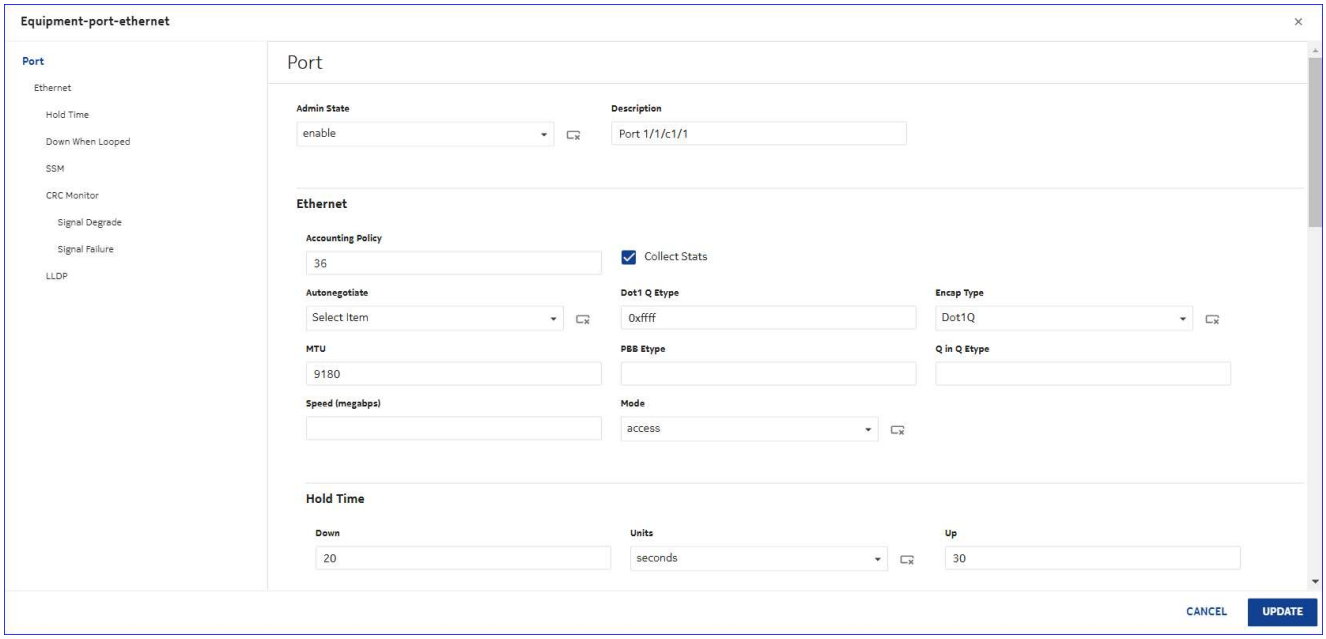
4

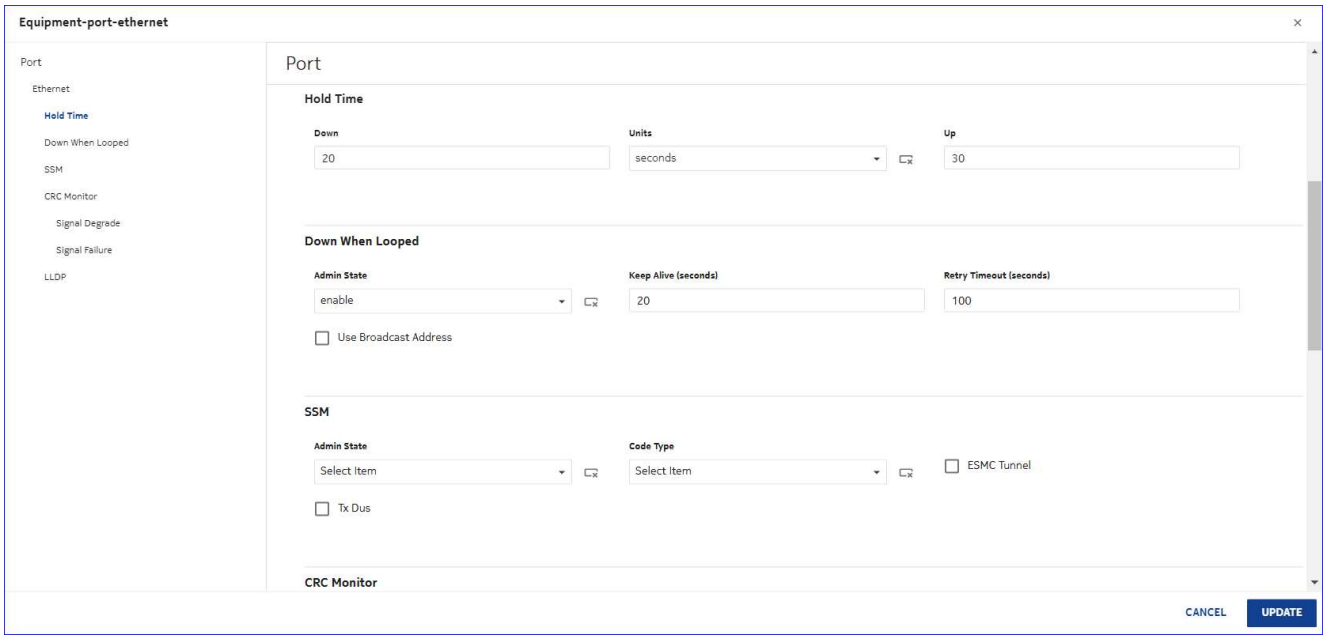
Create configuration deployments using the above configuration template.

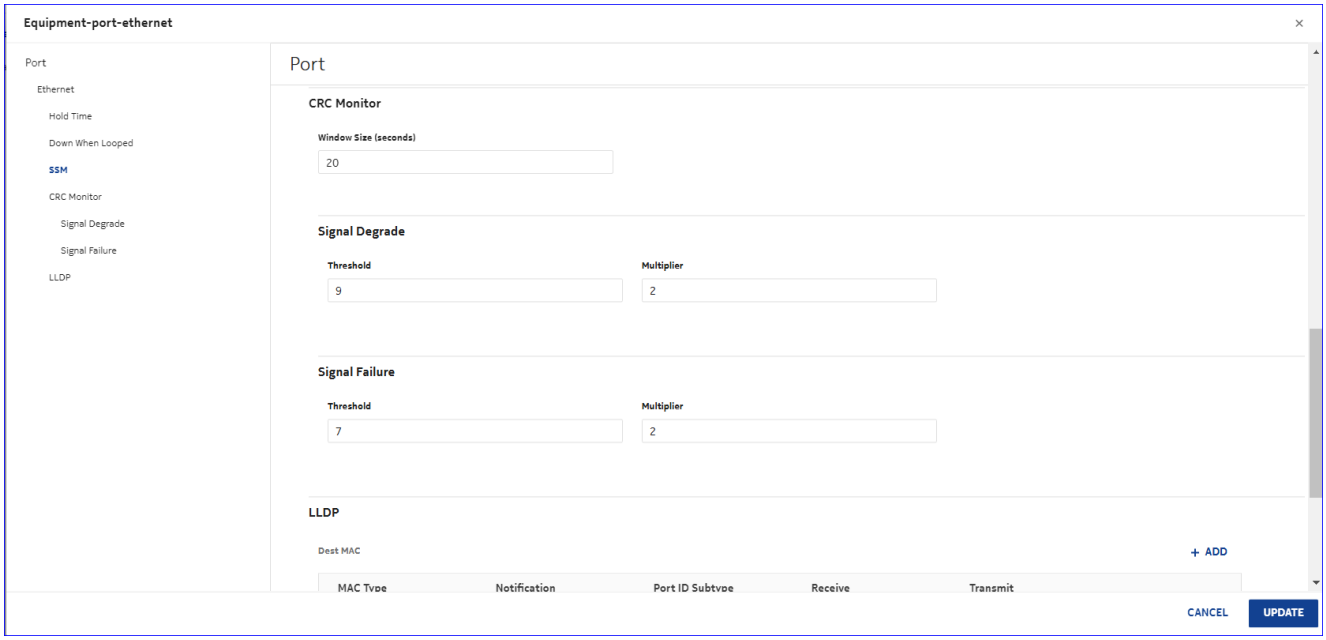
For the following examples, targets are 1/1/c1/1 for 7750 classic and MD nodes.

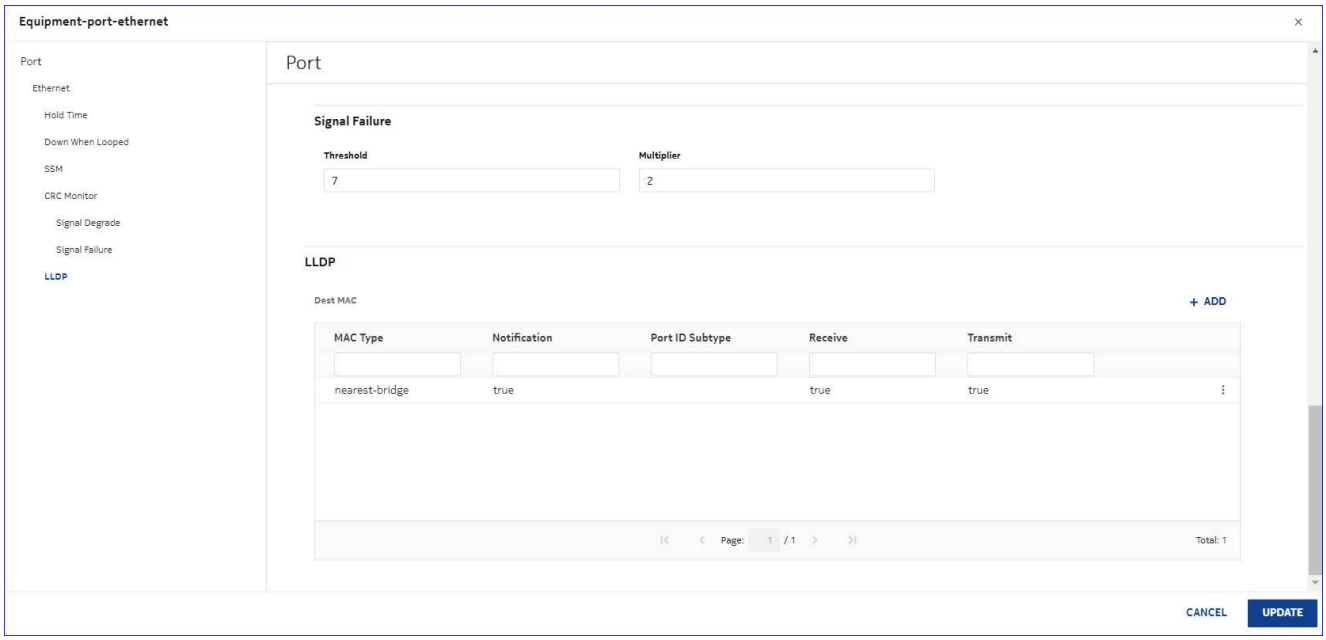
Ex. 7750 Classic

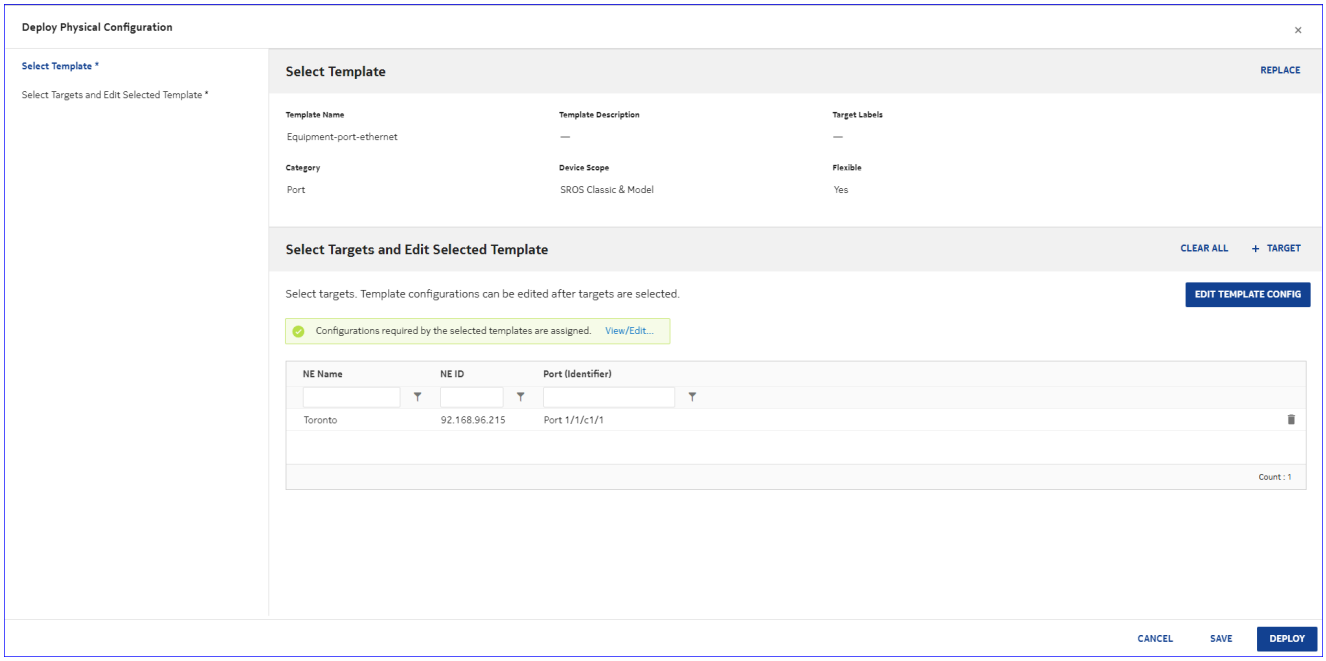
Deployment form attribute values:











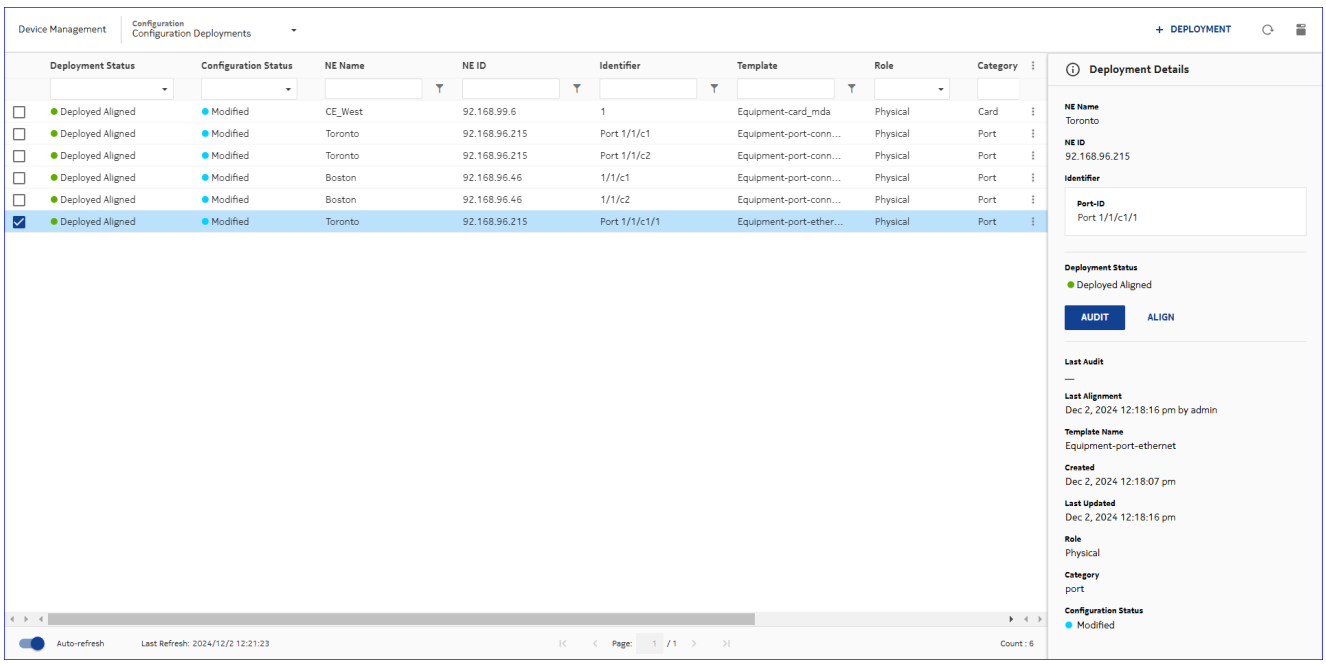


Figure 7-5 NE CLI after deployment

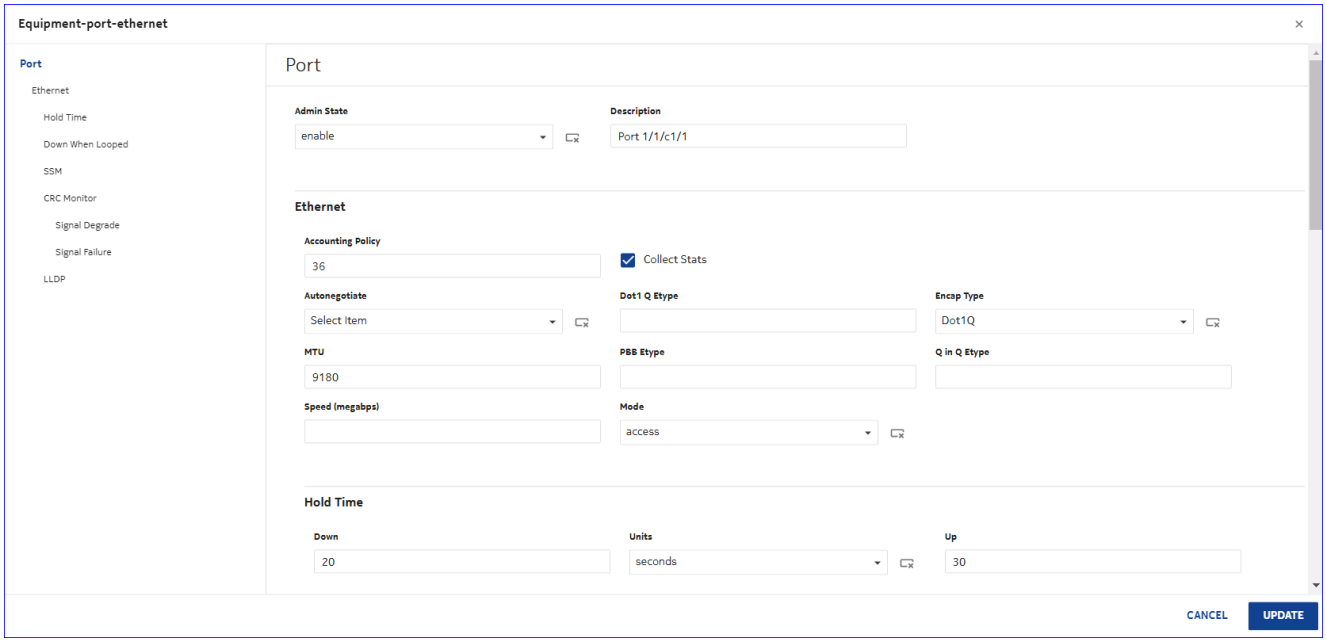
```
A:Toronto>config>port# /configure port 1/1/c1/1
A:Toronto>config>port# info
----------------------------------------------
        description "Port 1/1/c1/1"
        ethernet
            mode access
            encap-type dot1q
            mtu 9180
            crc-monitor
                sd-threshold 9 multiplier 2
                sf-threshold 7 multiplier 2
                window-size 20
            exit
            down-when-looped
                keep-alive 20
                retry-timeout 100
                no shutdown
            exit
            accounting-policy 36
            collect-stats
            lldp
                dest-mac nearest-bridge
                    admin-status tx-rx
                    notification
                    tx-tlvs port-desc sys-name sys-desc sys-cap
                exit
            exit
            hold-time up 30 down 20
            dot1q-etype 0xffff
        exit
        no shutdown
----------------------------------------------
```

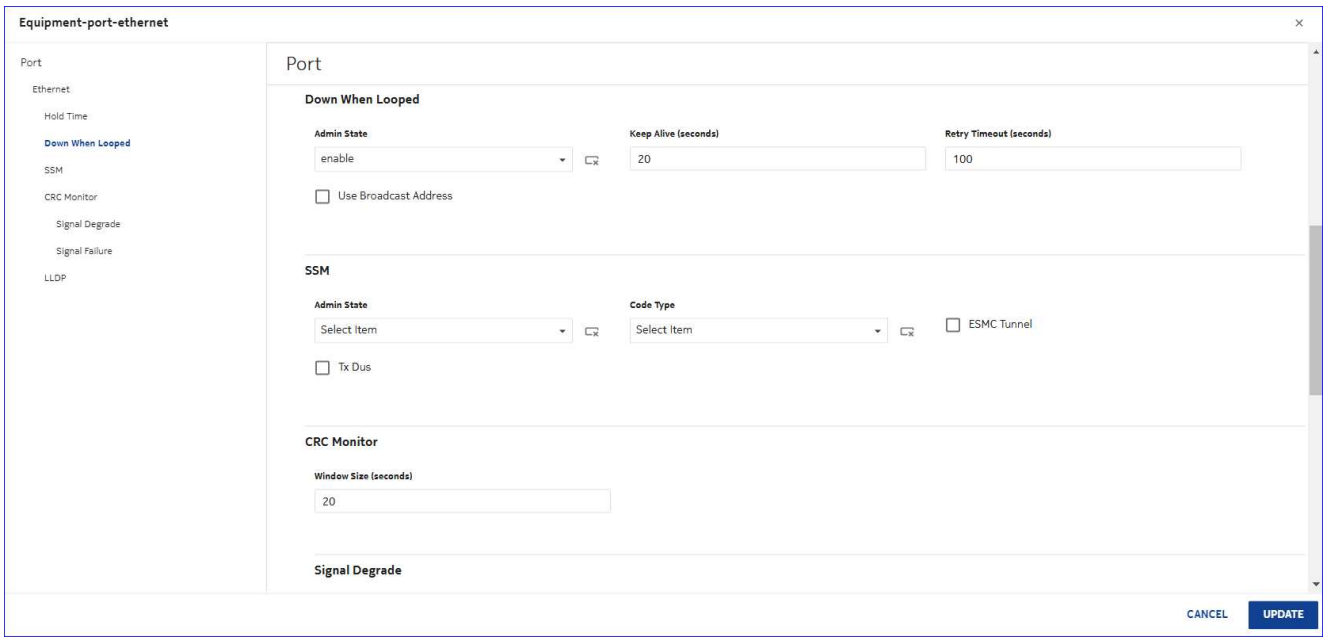
Figure 7-6 NE CLI after deployment

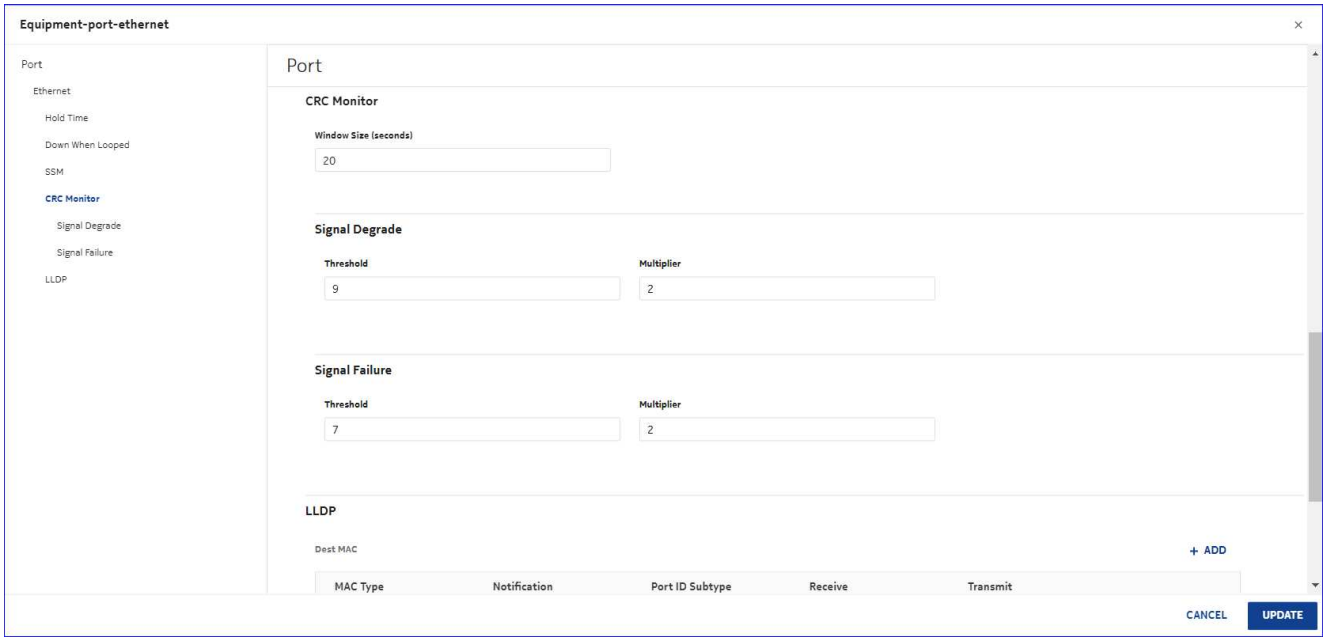
```
A:Toronto# show port

===============================================================================
Ports on Slot 1
===============================================================================
Port          Admin Link Port    Cfg  Oper LAG/ Port Port Port   C/QS/S/XFP/
Id            State      State   MTU  MTU  Bndl Mode Encp Type   MDIMDX
-------------------------------------------------------------------------------
1/1/c1        Up         Link Up                        conn   100GBASE-LR4*
1/1/c1/1      Up    Yes  Up      1518 1518    - accs dotq xgige
1/1/c1/2      Up    Yes  Up      8704 8704    - netw null xgige
1/1/c1/3      Up    Yes  Up      8704 8704    - netw null xgige
1/1/c1/4      Up    Yes  Up      8704 8704    - netw null xgige
1/1/c1/5      Up    No   Down    8704 8704    - netw null xgige
1/1/c1/6      Up    No   Down    8704 8704    - netw null xgige
1/1/c1/7      Up    No   Down    8704 8704    - netw null xgige
1/1/c1/8      Up    No   Down    8704 8704    - netw null xgige
1/1/c1/9      Up    No   Down    8704 8704    - netw null xgige
1/1/c1/10     Up    No   Down    8704 8704    - netw null xgige
1/1/c2        Up         Link Up                        conn   100GBASE-LR4*
1/1/c2/1      Up    Yes  Up      1514 1514    - accs null xgige
1/1/c2/2      Up    Yes  Up      8704 8704    - netw null xgige
1/1/c2/3      Up    Yes  Up      8704 8704    - netw null xgige
1/1/c2/4      Up    Yes  Up      8704 8704    - netw null xgige
1/1/c2/5      Up    Yes  Up      8704 8704    - netw null xgige
1/1/c2/6      Up    Yes  Up      8704 8704    - netw null xgige
1/1/c2/7      Up    Yes  Up      8704 8704    - netw null xgige
1/1/c2/8      Up    Yes  Up      8704 8704    - netw null xgige
1/1/c2/9      Up    No   Down    8704 8704    - netw null xgige
1/1/c2/10     Up    No   Down    8704 8704    - netw null xgige
1/1/c3        Up         Down                           conn   100GBASE-LR4*
1/1/c4        Up         Down                           conn   100GBASE-LR4*
1/1/c5        Up         Down                           conn   100GBASE-LR4*
1/1/c6        Up         Down                           conn   100GBASE-LR4*
1/1/c7        Up         Down                           conn   100GBASE-LR4*
1/1/c8        Up         Down                           conn   100GBASE-LR4*
```

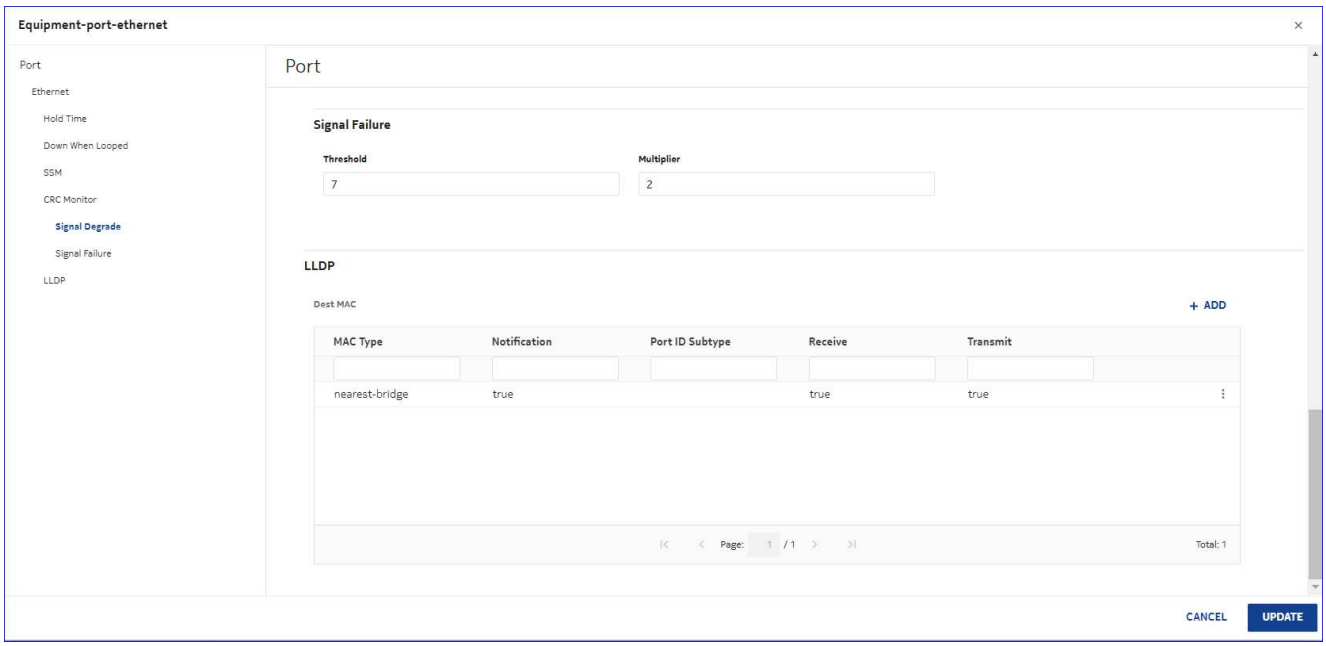
Ex. 7750 MD

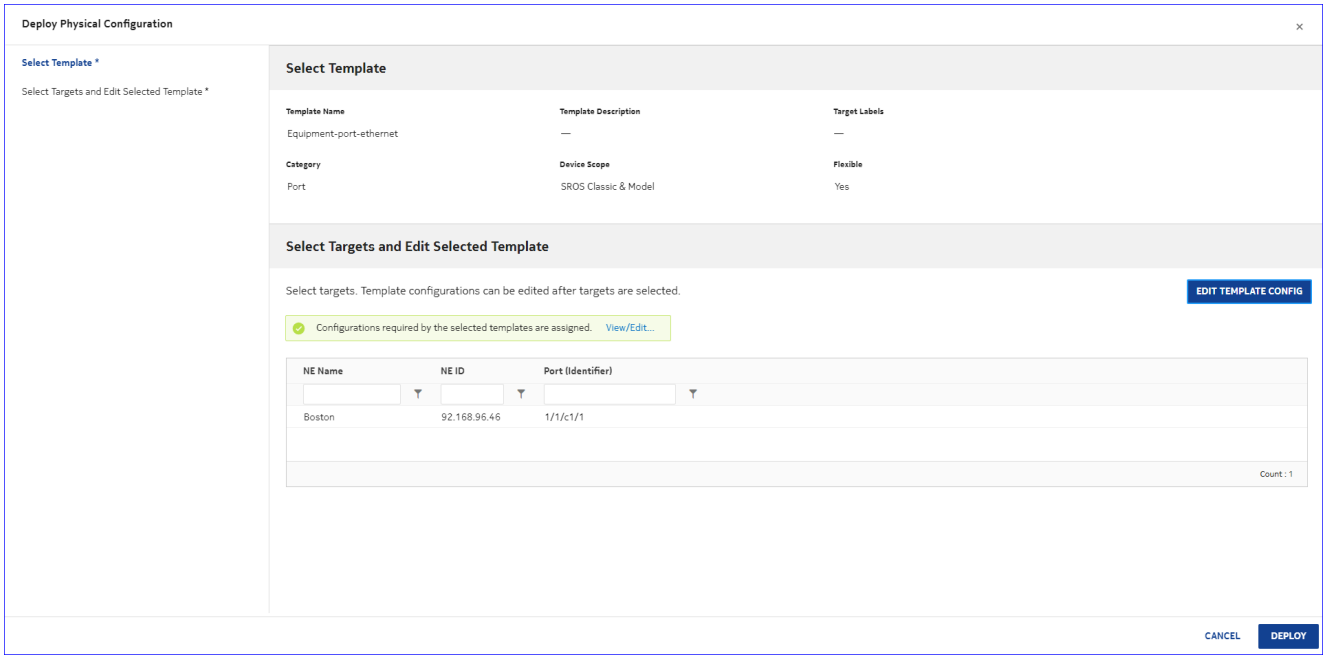
Deployment form attribute values:











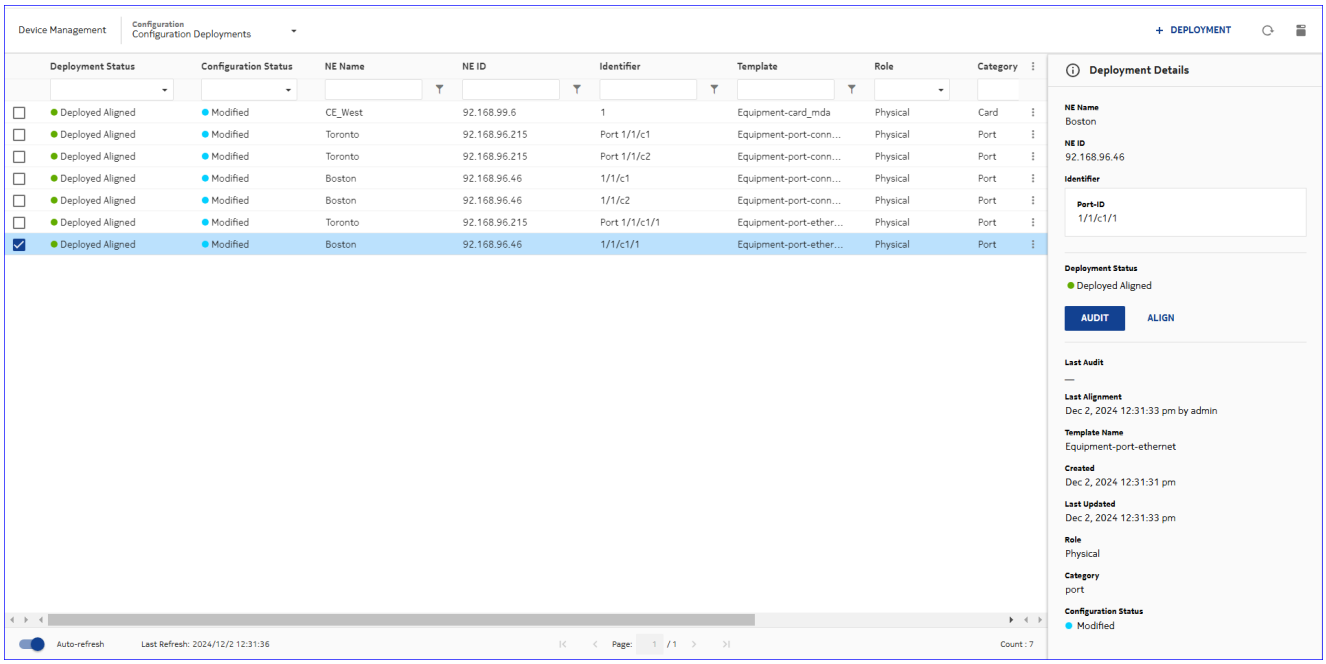


Figure 7-7 NE CLI after deployment

```
(pr)[/configure port 1/1/c1/1]
A:admin@Boston# info
    admin-state enable
    description "Port 1/1/c1/1"
    ethernet {
        accounting-policy 36
        collect-stats true
        mode access
        encap-type dot1q
        mtu 9180
        hold-time {
            units seconds
            up 30
            down 20
        }
        crc-monitor {
            window-size 20
            signal-degrade {
                threshold 9
                multiplier 2
            }
            signal-failure {
                threshold 7
                multiplier 2
            }
        }
        down-when-looped {
            admin-state enable
            keep-alive 20
            retry-timeout 100
        }
        lldp {
            dest-mac nearest-bridge {
                notification true
                receive true
                transmit true
                tx-tlvs {
                    port-desc true
                    sys-name true
                    sys-desc true
                    sys-cap true
                }
                tx-mgmt-address system {
                    admin-state enable
                }
            }
        }
    }
```

Figure 7-8 NE CLI after deployment

```
A:admin@Boston# show port

===============================================================================
Ports on Slot 1
===============================================================================
Port          Admin Link Port    Cfg  Oper LAG/ Port Port Port   C/QS/S/XFP/
Id            State      State   MTU  MTU  Bndl Mode Encp Type   MDIMDX
-------------------------------------------------------------------------------
1/1/c1        Up         Link Up                          conn   100GBASE-LR4*
1/1/c1/1      Up    No   Down    1518 1518    - accs dotq xgige
1/1/c1/2      Up    No   Down    8704 8704    - netw null xgige
1/1/c1/3      Up    No   Down    8704 8704    - netw null xgige
1/1/c1/4      Up    No   Down    8704 8704    - netw null xgige
1/1/c1/5      Up    Yes  Up      8704 8704    - netw null xgige
1/1/c1/6      Up    Yes  Up      8704 8704    - netw null xgige
1/1/c1/7      Down  No   Down    8704 8704    - netw null xgige
1/1/c1/8      Down  No   Down    8704 8704    - netw null xgige
1/1/c1/9      Down  No   Down    8704 8704    - netw null xgige
1/1/c1/10     Down  No   Down    8704 8704    - netw null xgige
1/1/c2        Up         Link Up                          conn   100GBASE-LR4*
1/1/c2/1      Down  No   Down    8704 8704    - netw null xgige
1/1/c2/2      Down  No   Down    8704 8704    - netw null xgige
1/1/c2/3      Down  No   Down    8704 8704    - netw null xgige
1/1/c2/4      Down  No   Down    8704 8704    - netw null xgige
1/1/c2/5      Down  No   Down    8704 8704    - netw null xgige
1/1/c2/6      Down  No   Down    8704 8704    - netw null xgige
1/1/c2/7      Down  No   Down    8704 8704    - netw null xgige
1/1/c2/8      Down  No   Down    8704 8704    - netw null xgige
1/1/c2/9      Down  No   Down    8704 8704    - netw null xgige
1/1/c2/10     Down  No   Down    8704 8704    - netw null xgige
1/1/c3        Down       Down                             conn   100GBASE-LR4*
1/1/c4        Down       Down                             conn   100GBASE-LR4*
```

END OF STEPS

7.4.3 To configure Ethernet Port using intent port-eth_msros_23-10-1_24-4

port-eth_msros_23-10-1_24-4 supports configuration of ethernet port on MD NE.

1

Pre-configuration:

oper-group

- `/configure service oper-group "OperGroup-1"`

dist-cpu-protection

- `/configure system security dist-cpu-protection policy "port-cpu-protect-1" type port`

accounting-policy

- `/configure log accounting-policy 20`

port scheduler policy

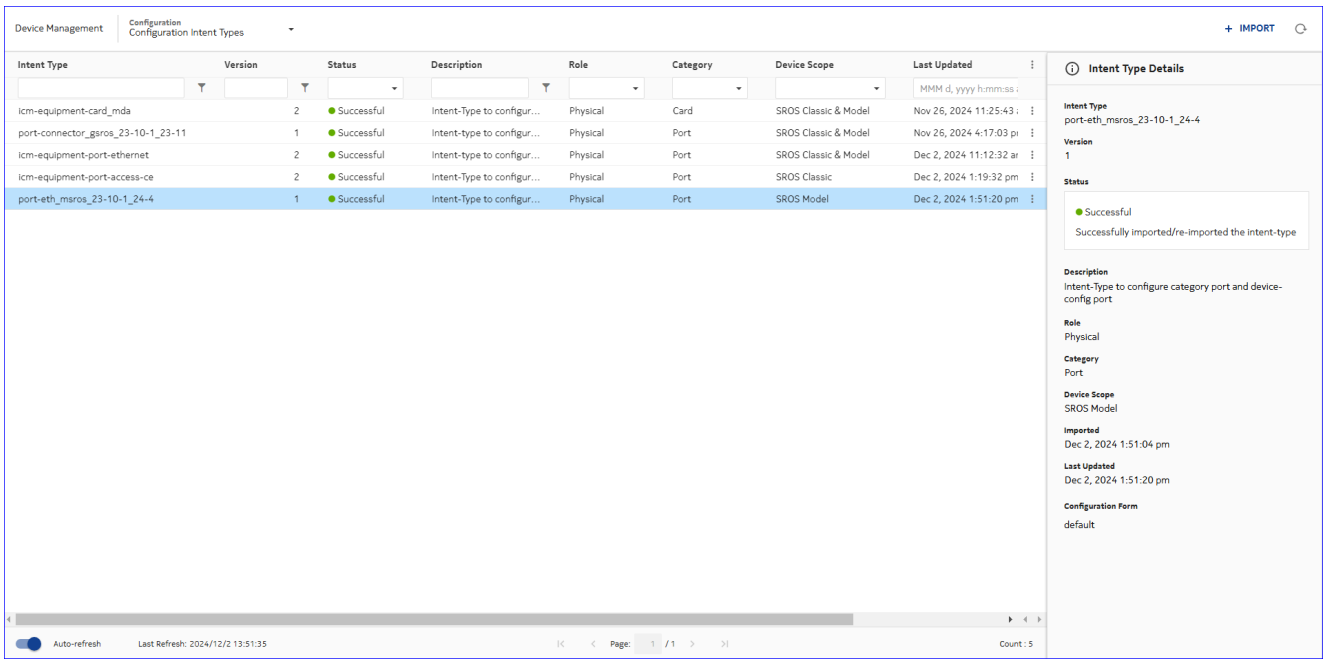
- `/configure qos port-scheduler-policy "port-sch-policy-1"`

hw-agg-shaper-scheduler-policy

- `/configure qos hw-agg-shaper-scheduler-policy "hw-agg-shaper-sch-pol-1"`

2

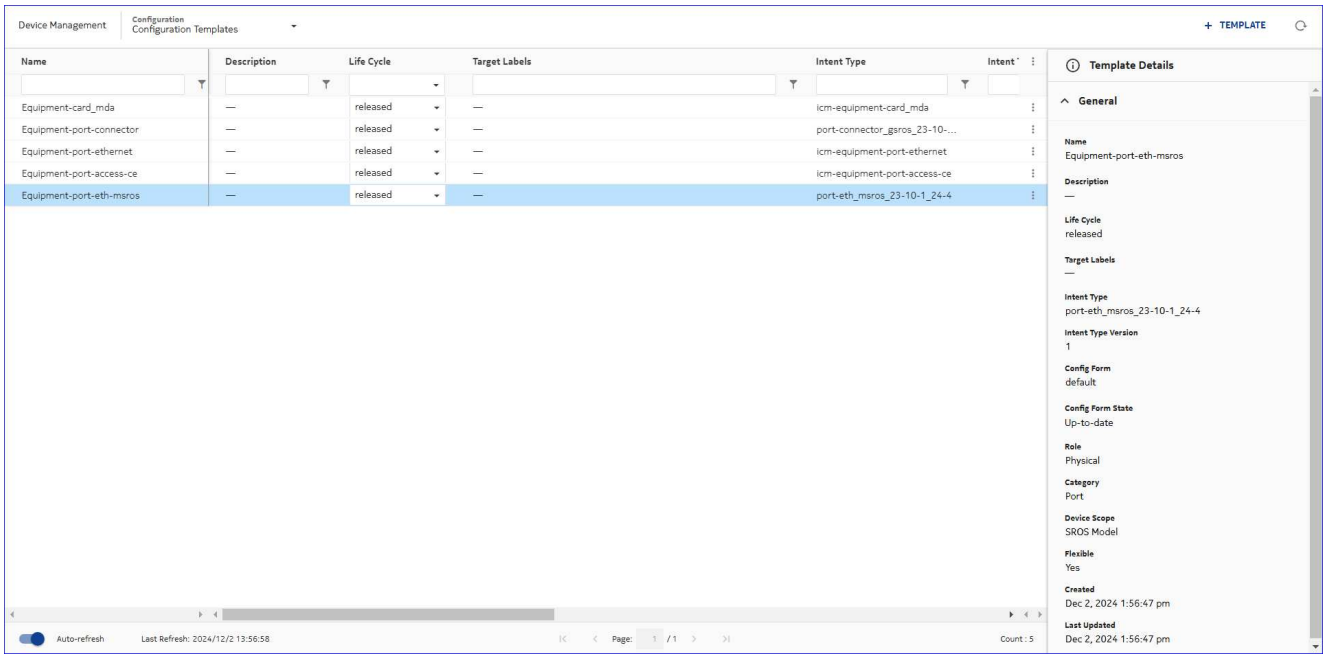
Import intent type **port-eth_msros_23-10-1_24-4** into **Device Management**, **Configuration Intent Types**.



3

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

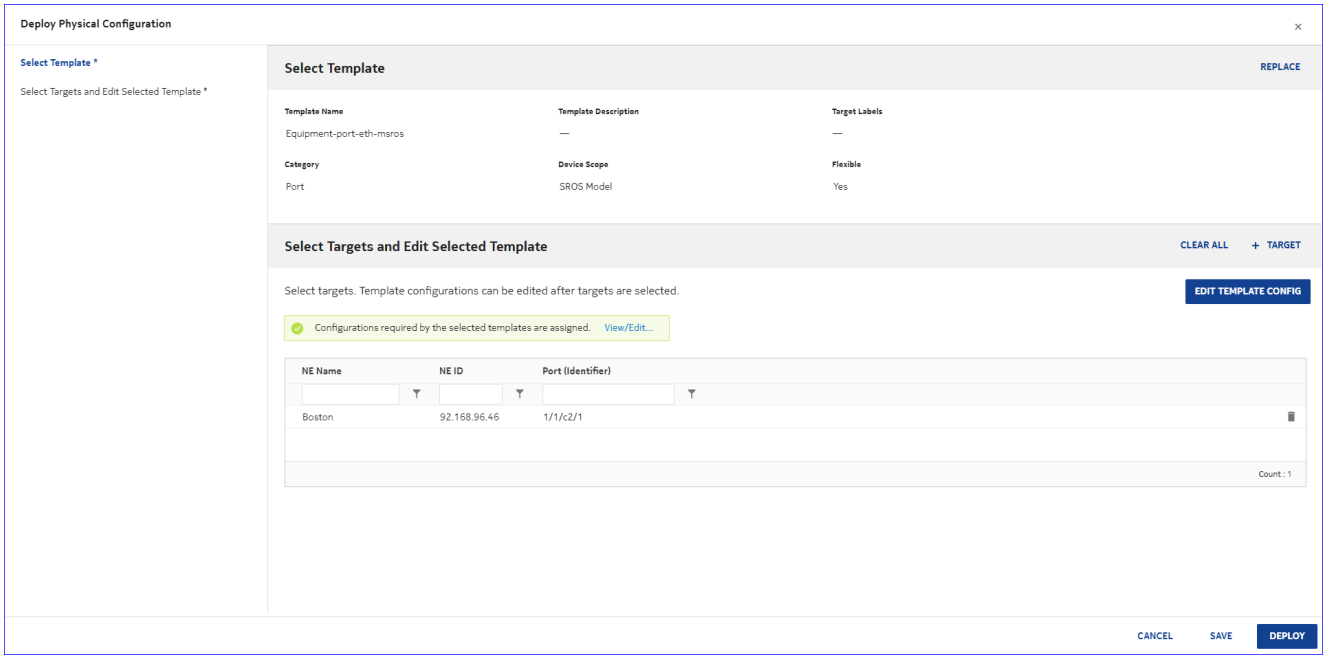
For example, the configuration template created below is named as **Equipment-port-eth-msros**.



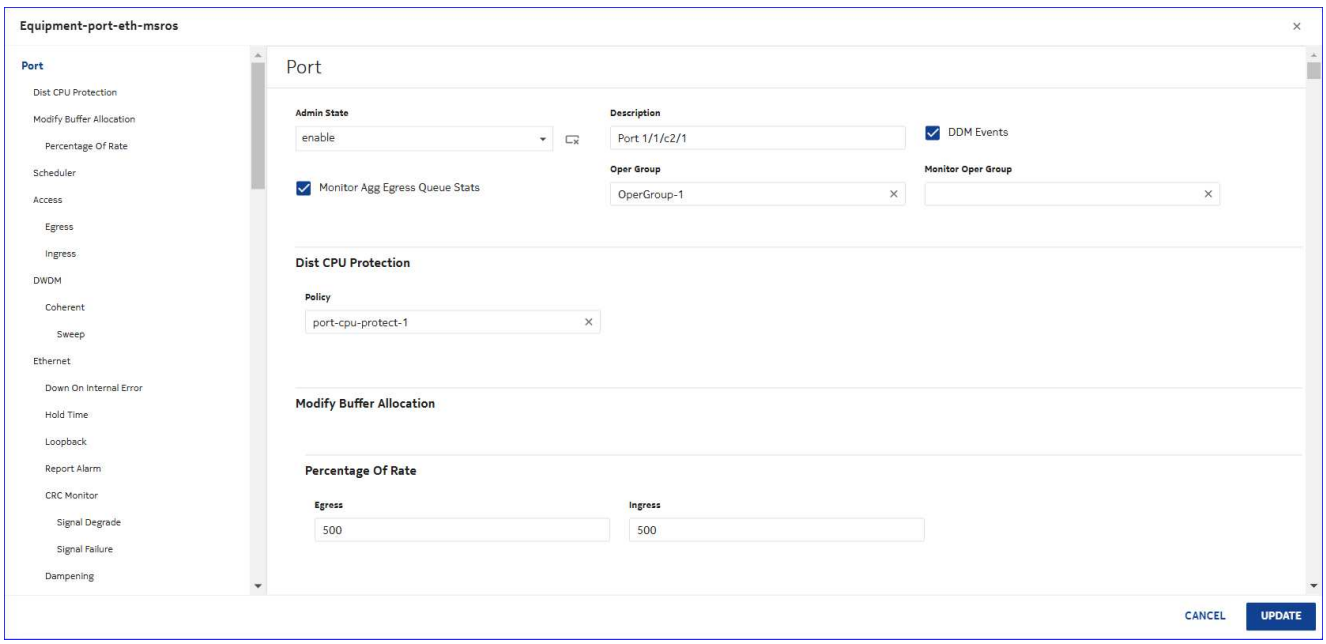
4

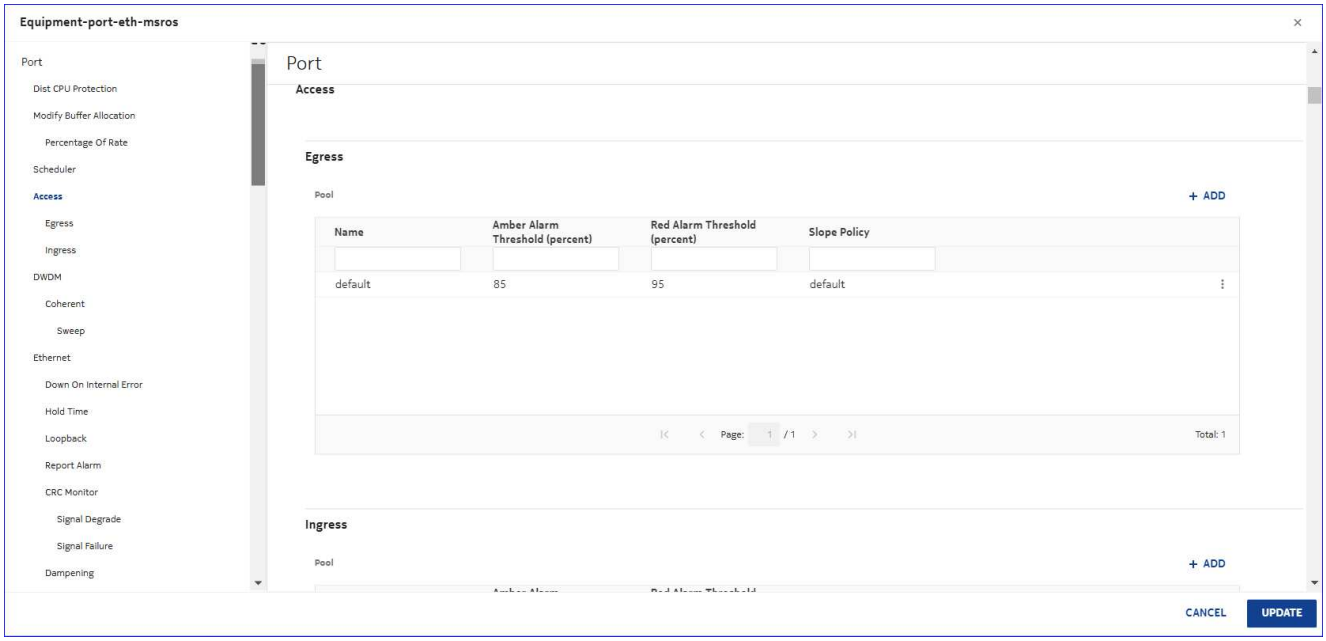
Create configuration deployments using the above configuration template.

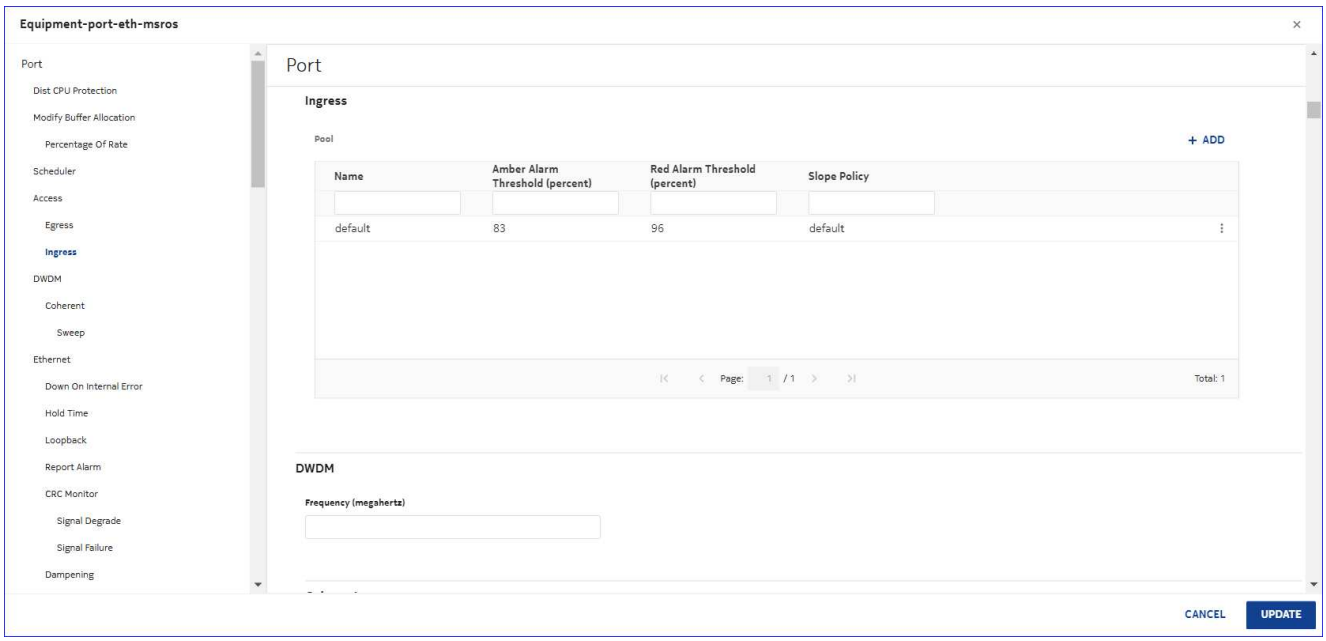
For the following example, targets are 1/1/c2 /1 for 7750 MD nodes.

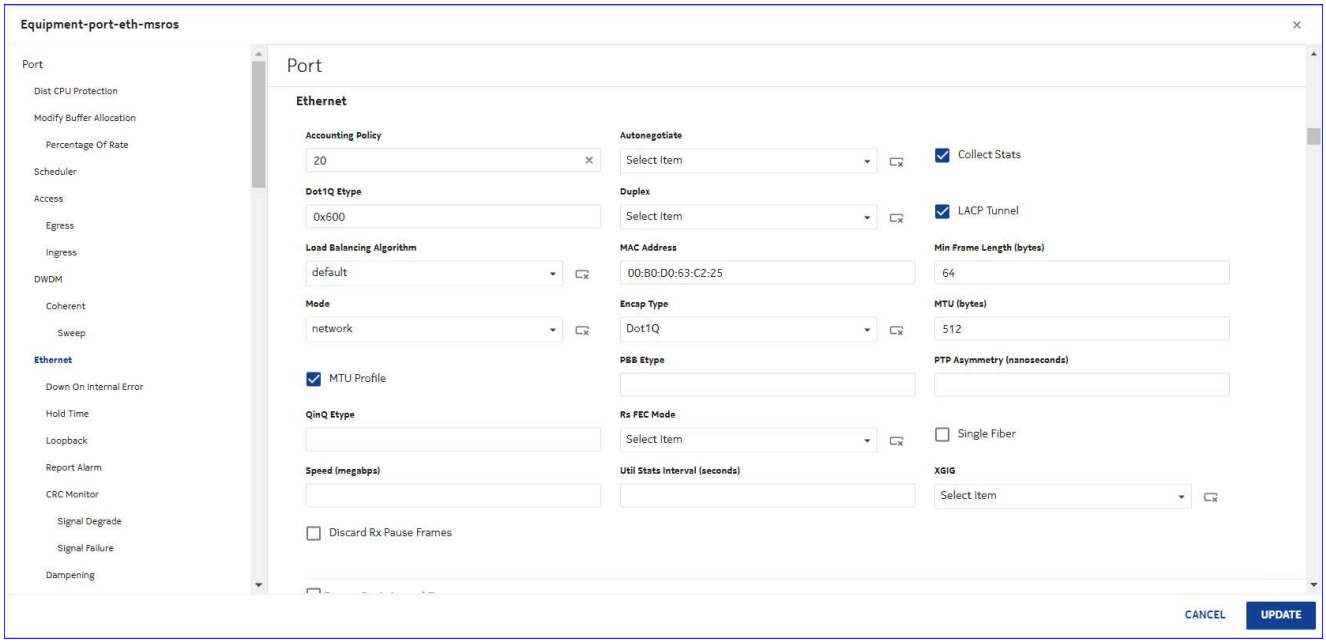


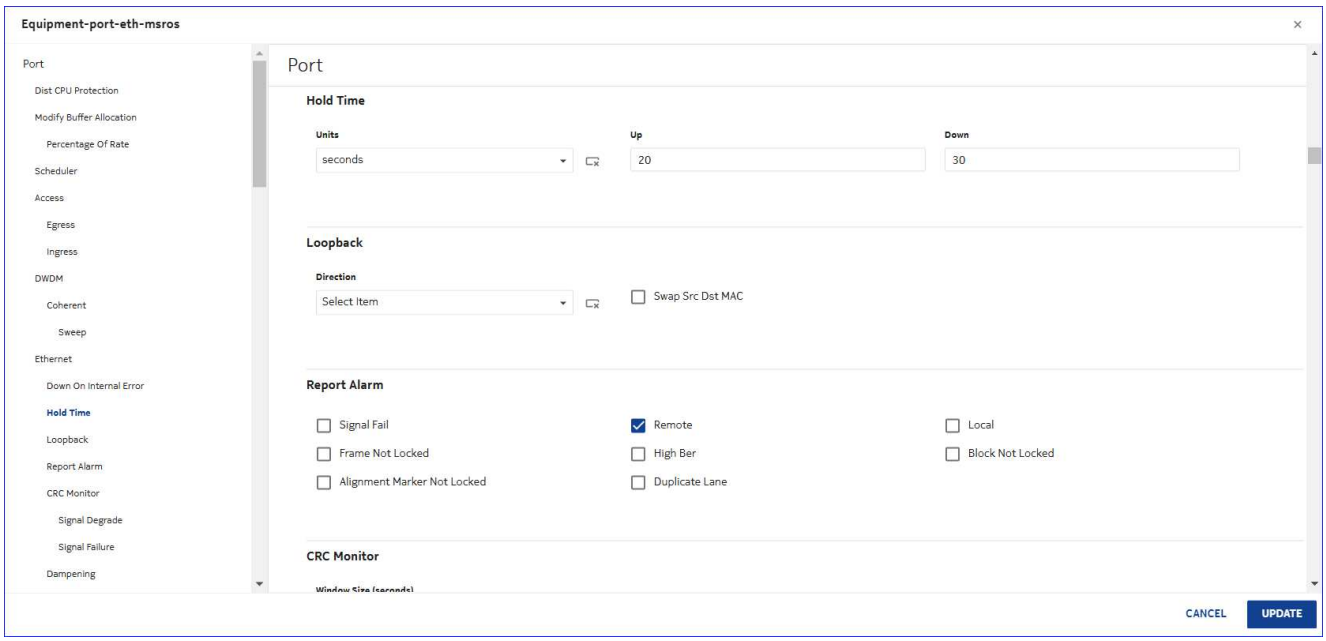
Attribute values in the configuration deployment form:

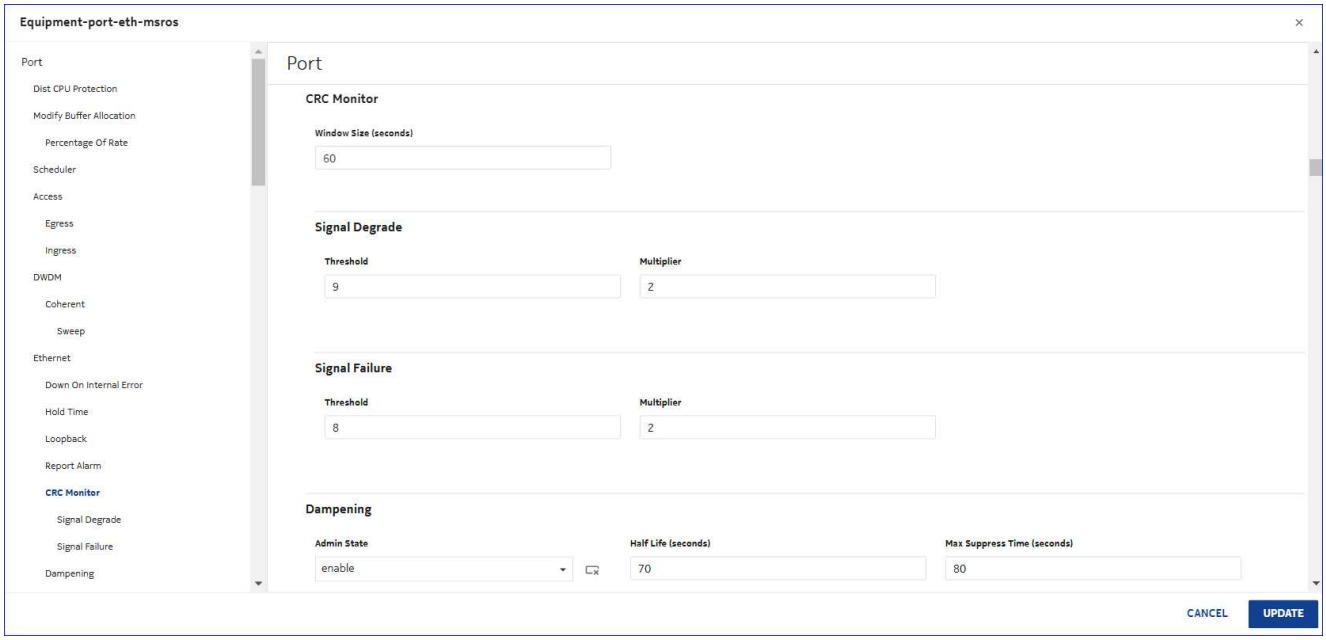


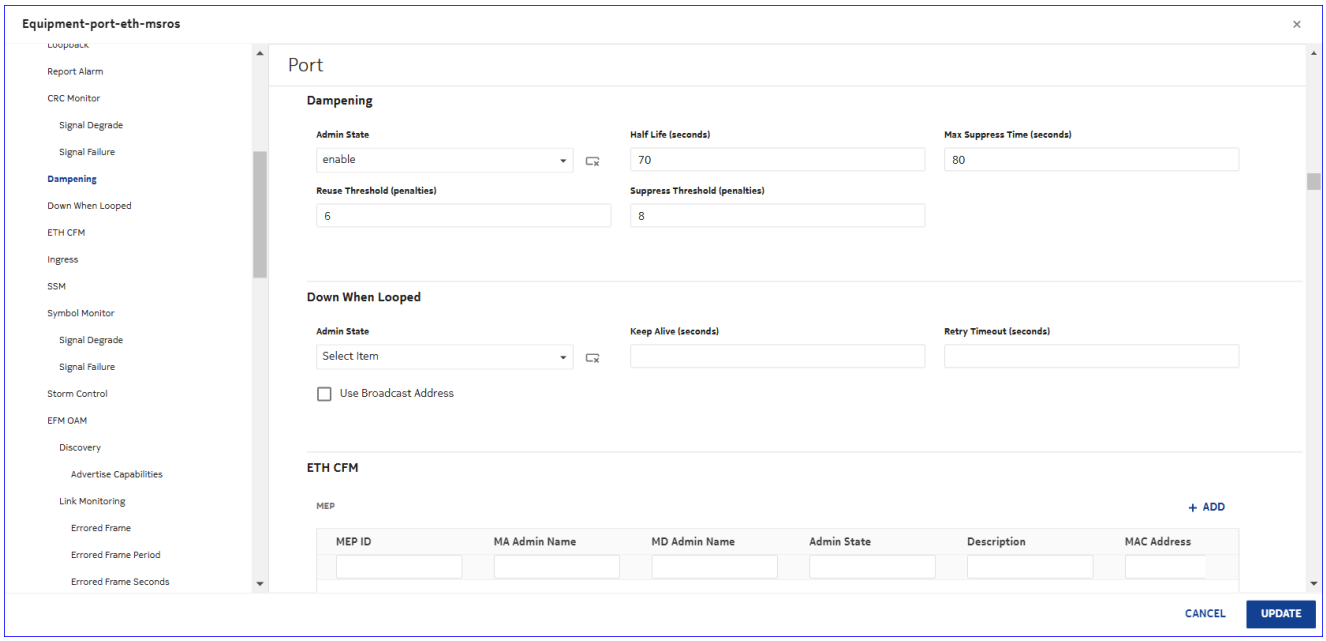


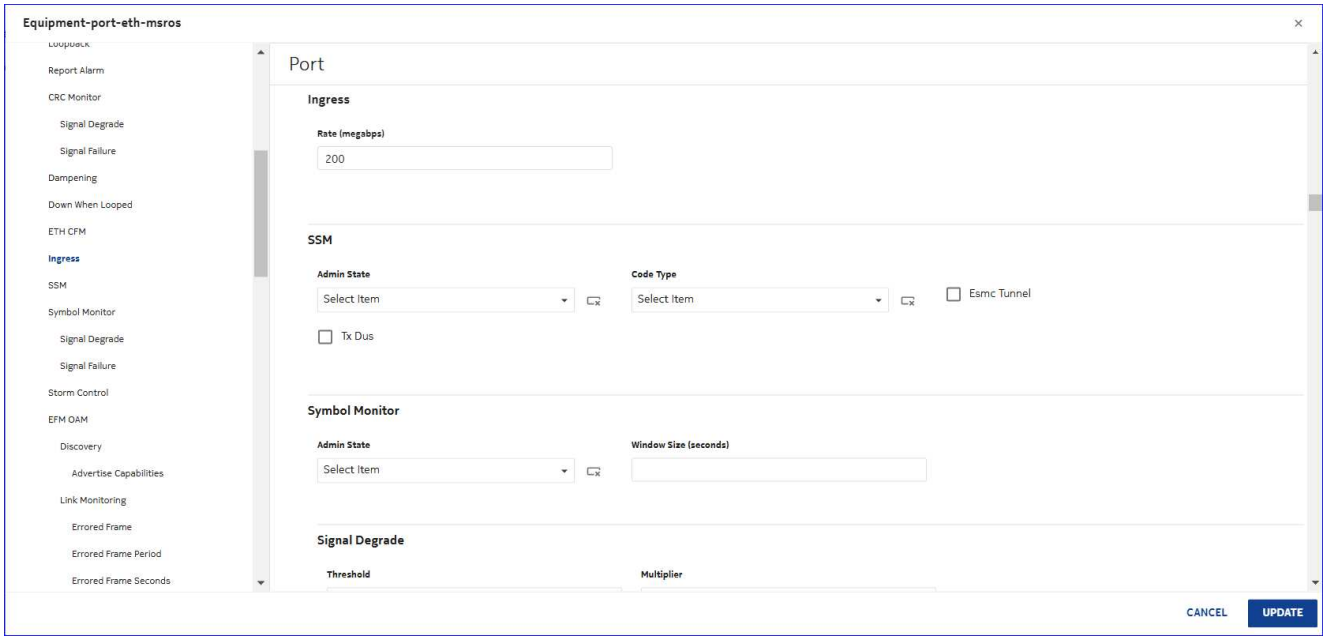


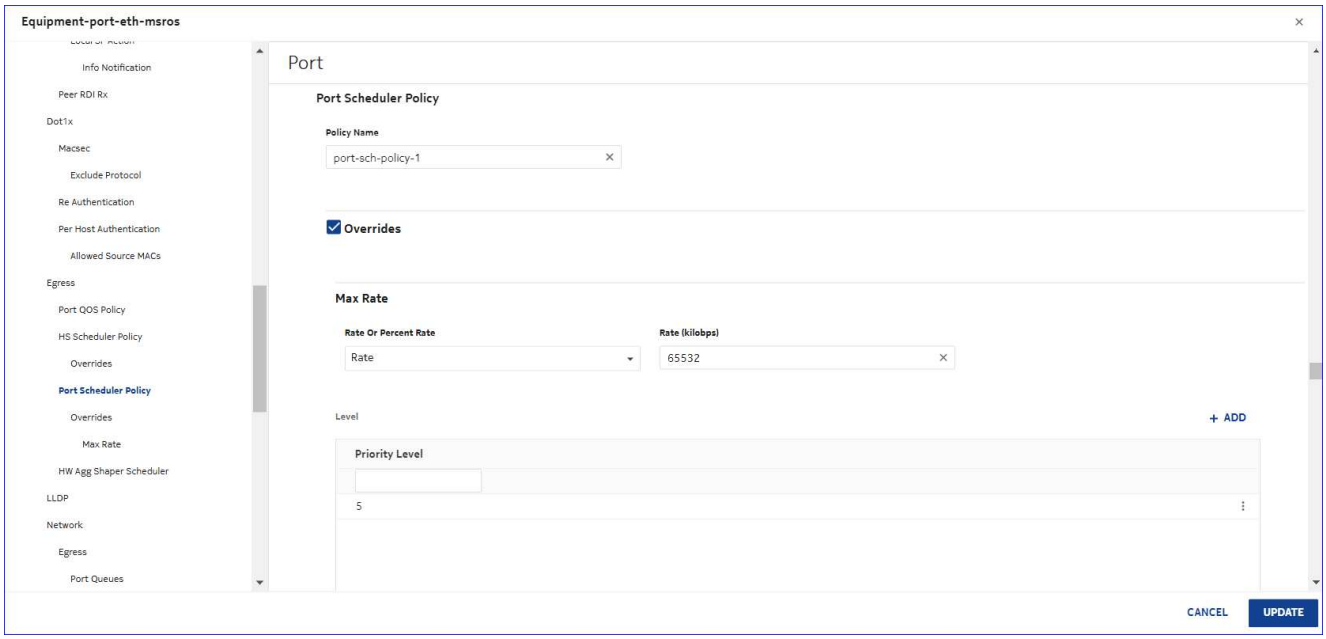


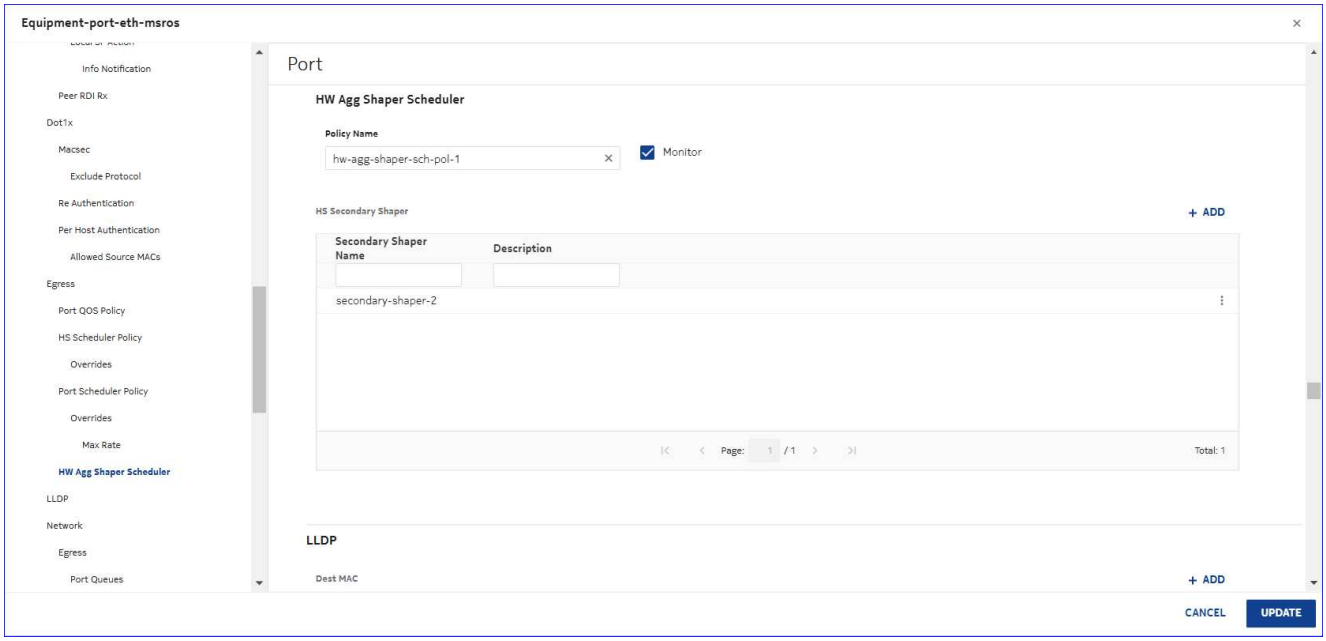


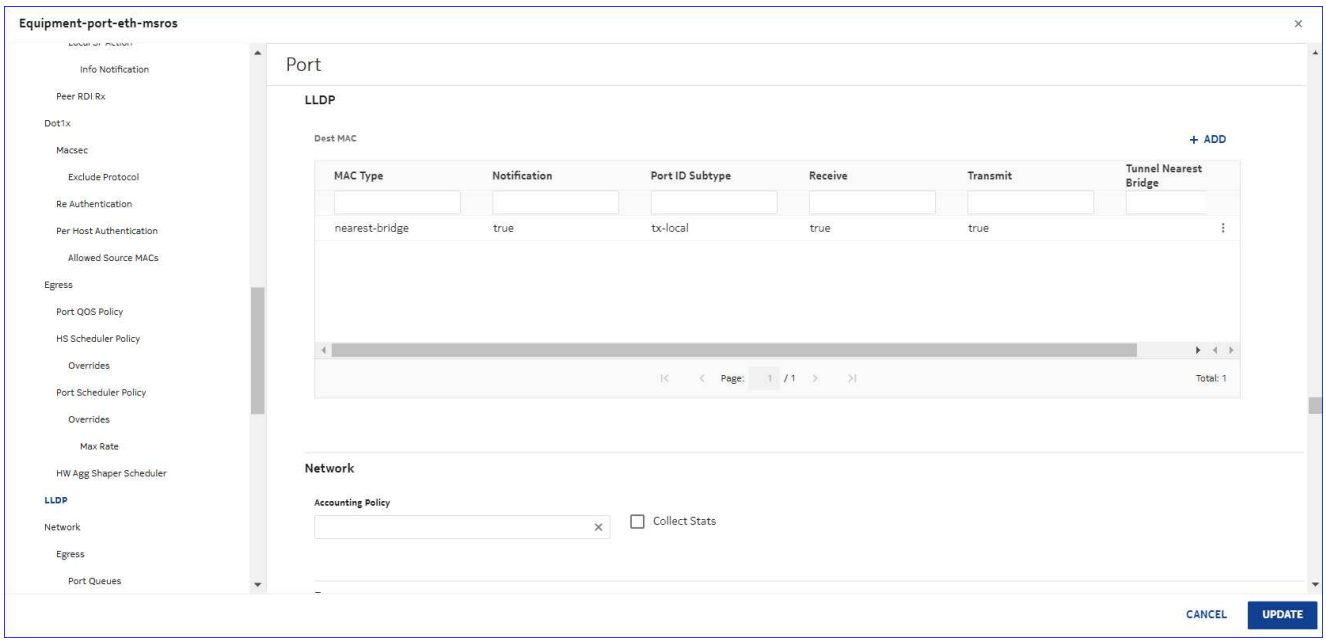












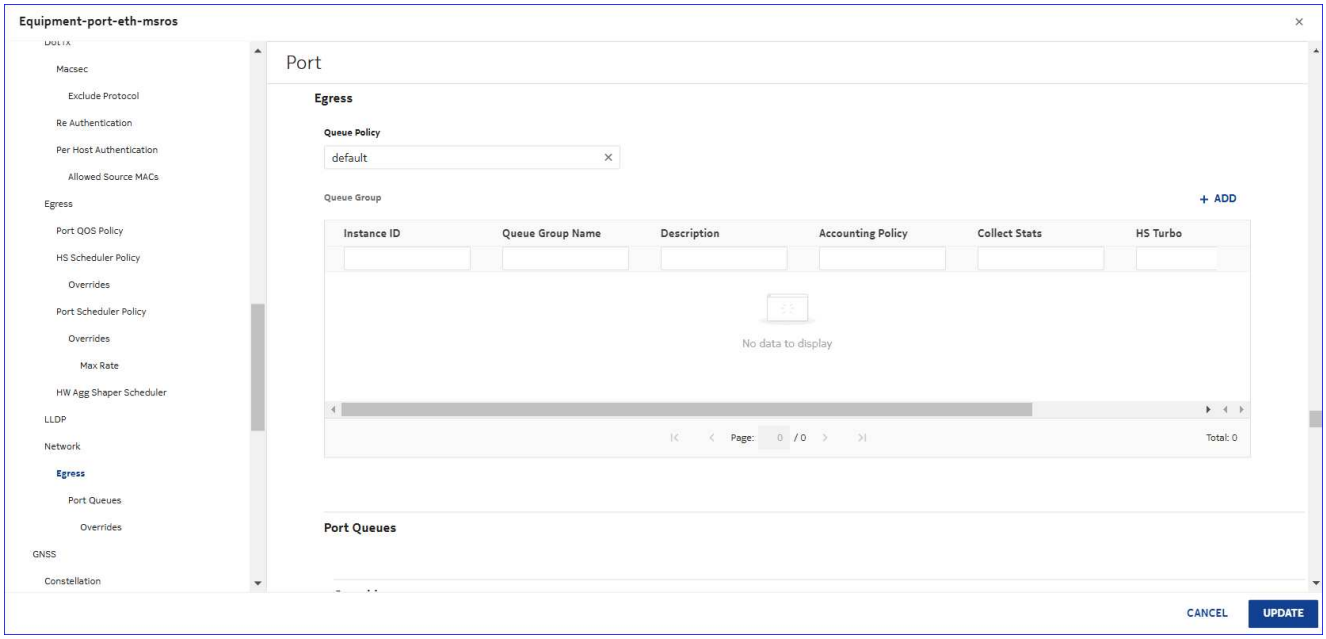


Figure 7-9 Final successful deployment

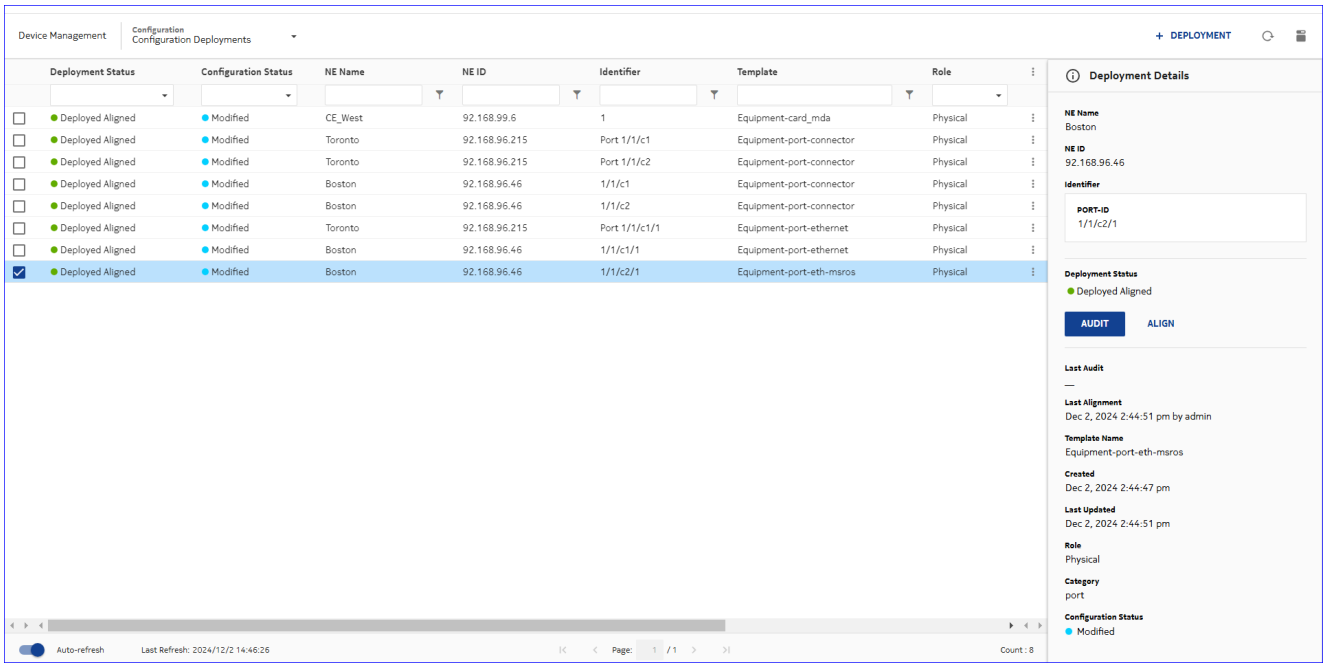


Figure 7-10 NE CLI after deployment

```
*(pr)[/configure port 1/1/c2/1]
A:admin@Boston# info
    admin-state enable
    description "Port 1/1/c2/1"
    ddm-events true
    monitor-agg-egress-queue-stats true
    oper-group "OperGroup-1"
    dist-cpu-protection {
        policy "port-cpu-protect-1"
    }
    modify-buffer-allocation {
        percentage-of-rate {
            egress 500
            ingress 500
        }
    }
    access {
        egress {
            pool "default" {
                amber-alarm-threshold 85
                red-alarm-threshold 95
                slope-policy "default"
                resv-cbs {
                    cbs 87
                    amber-alarm-action {
                        step 78
                        max 93
                    }
                }
            }
        }
        ingress {
            pool "default" {
                amber-alarm-threshold 83
                red-alarm-threshold 96
                slope-policy "default"
                resv-cbs {
                    cbs 79
                    amber-alarm-action {
                        step 75
                        max 95
                    }
                }
            }
        }
    }
```

Figure 7-11 NE CLI after deployment

```
ethernet {
    dot1q-etype 0x600
    lacp-tunnel true
    load-balancing-algorithm default
    mac-address 00:b0:d0:63:c2:25
    min-frame-length 64
    mode network
    encap-type dot1q
    mtu 512
    hold-time {
        units seconds
        up 20
        down 30
    }
    report-alarm {
        signal-fail false
        remote true
        frame-not-locked false
        duplicate-lane false
    }
    crc-monitor {
        window-size 60
        signal-degrade {
            threshold 9
            multiplier 2
        }
        signal-failure {
            threshold 8
            multiplier 2
        }
    }
    dampening {
        admin-state enable
        half-life 70
        max-suppress-time 80
        reuse-threshold 6
        suppress-threshold 8
    }
    ingress {
        rate 200
    }
    ssm {
        tx-dus false
    }
```

Figure 7-12 NE CLI after deployment

```
        egress {
            port-scheduler-policy {
                policy-name "port-sch-policy-1"
                overrides {
                    max-rate {
                        rate 65532
                    }
                    level 5 {
                        rate {
                            pir 6000
                            cir 5000
                        }
                    }
                }
            }
            hw-agg-shaper-scheduler {
                policy-name "hw-agg-shaper-sch-pol-1"
                monitor true
            }
        }
        lldp {
            dest-mac nearest-bridge {
                notification true
                port-id-subtype tx-local
                receive true
                transmit true
                tx-tlvs {
                    port-desc true
                    sys-name true
                    sys-desc true
                }
                tx-mgmt-address system {
                    admin-state enable
                }
            }
        }
        network {
            collect-stats false
            egress {
                queue-policy "default"
            }
        }
    }
```

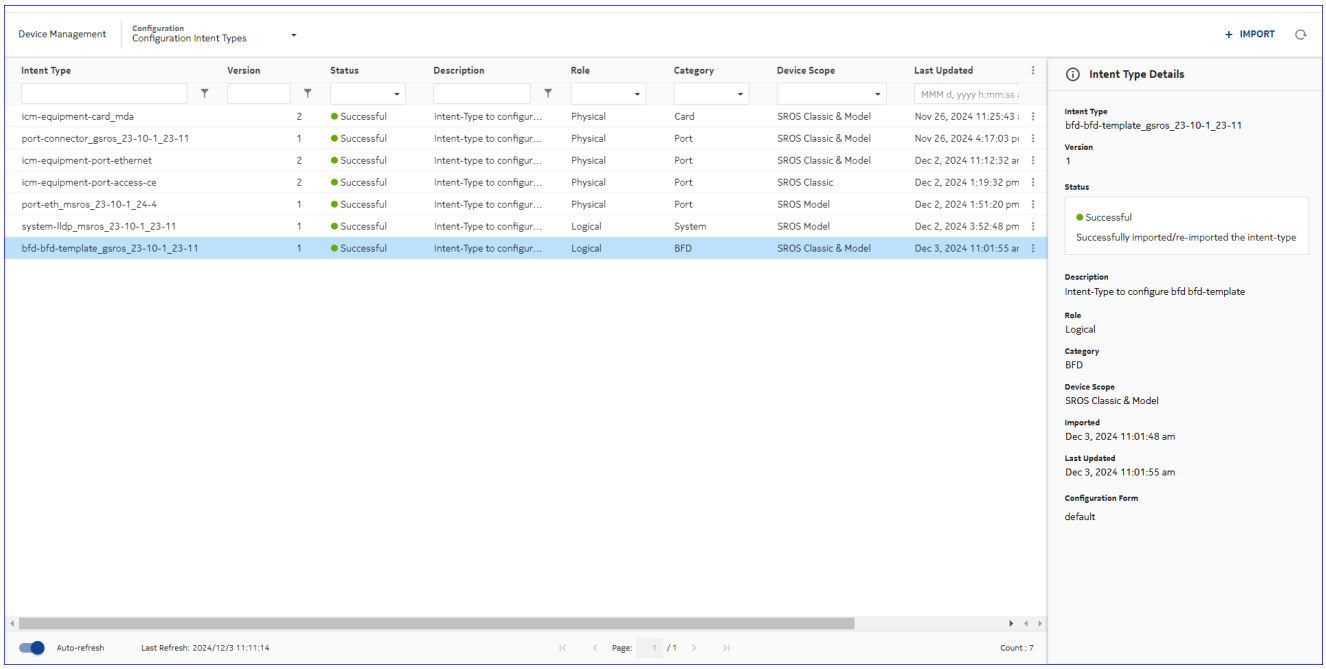
END OF STEPS

7.5 BFD Templates

7.5.1 To configure BFD Templates using bfd-bfd-template_gsros intent

1

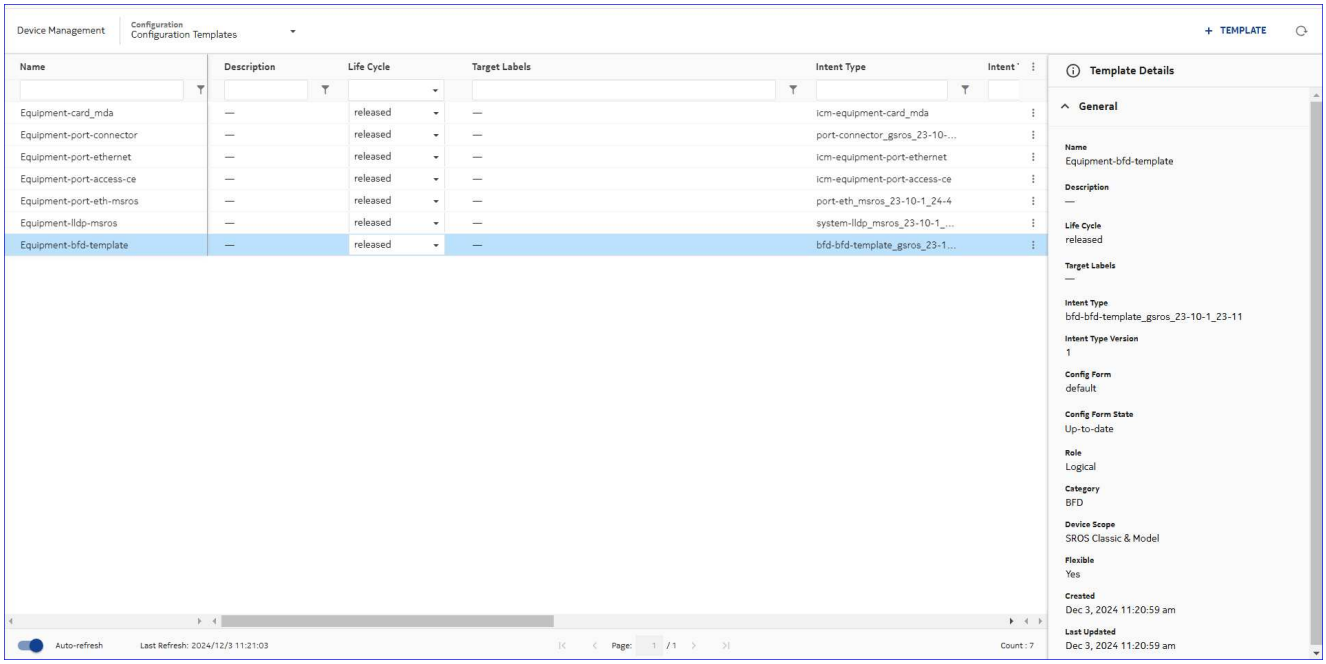
Import intent type **bfd-bfd-template_gsros_23-10-1_23-11** into **Device Management**, **Configuration Intent Types**.



2

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

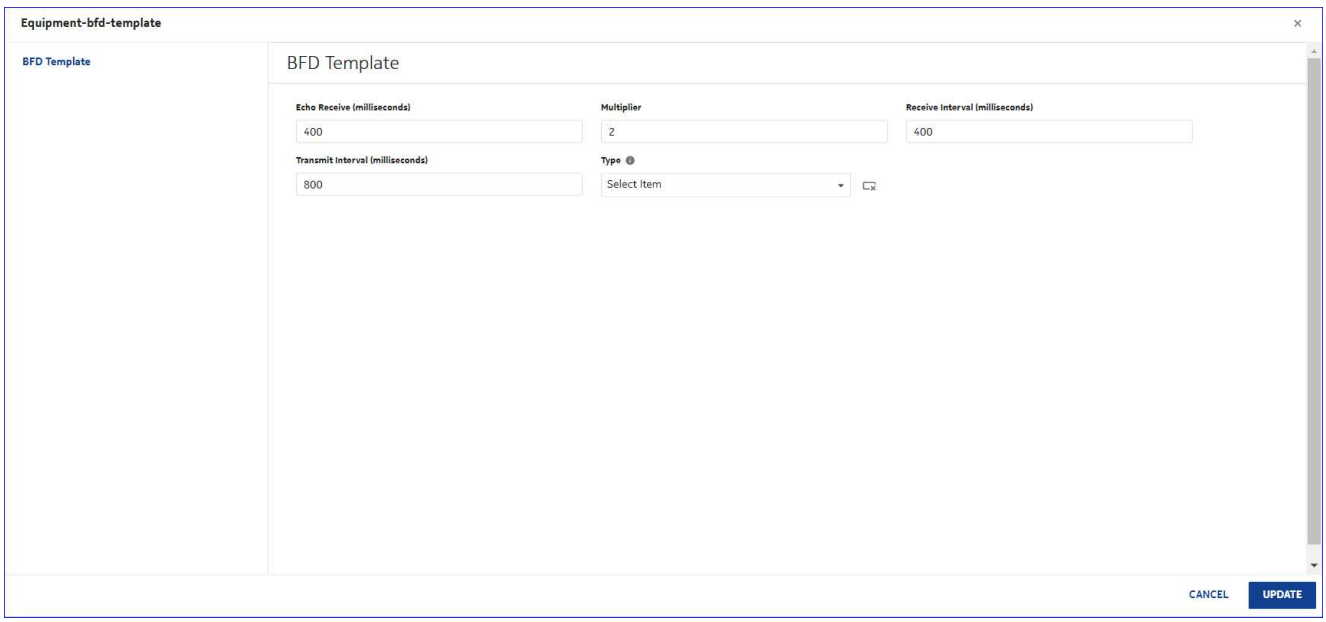
For example, the configuration template created below is named as **Equipment-bfd-template**.

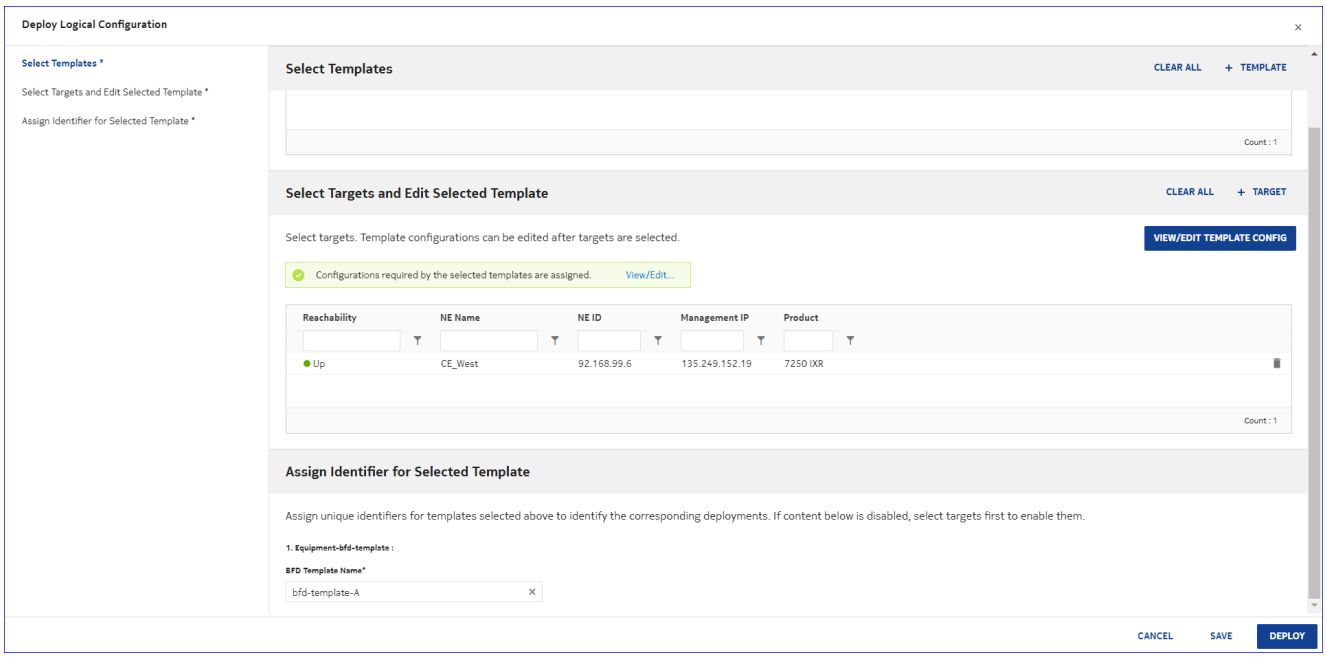


3

Create configuration deployments using the above configuration template.

Example 1: On 7250 IXR-6 node in MD mode





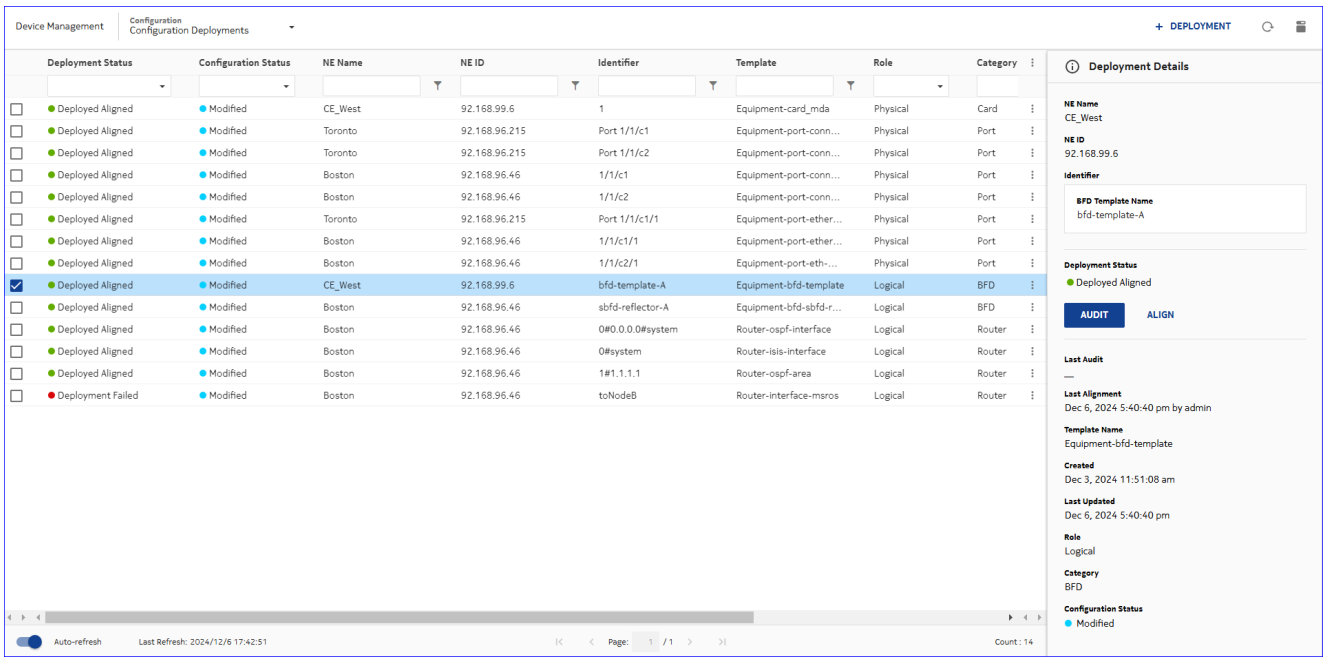
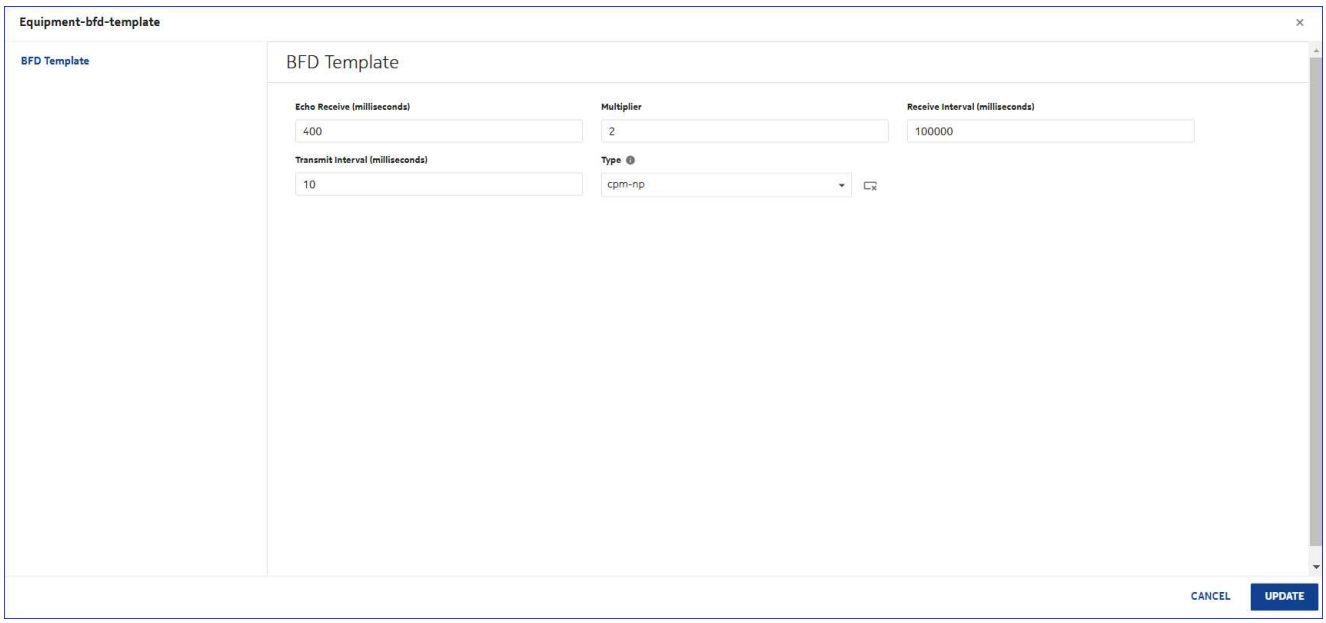


Figure 7-13 NE CLI after deployment

```
(pr)[/configure bfd]
A:admin@CE_West# info
    bfd-template "bfd-template-A" {
        echo-receive 400
        multiplier 2
        receive-interval 400
        transmit-interval 800
    }

(pr)[/configure bfd]
```

Example 2: On 7750 SR-14s node in MD mode



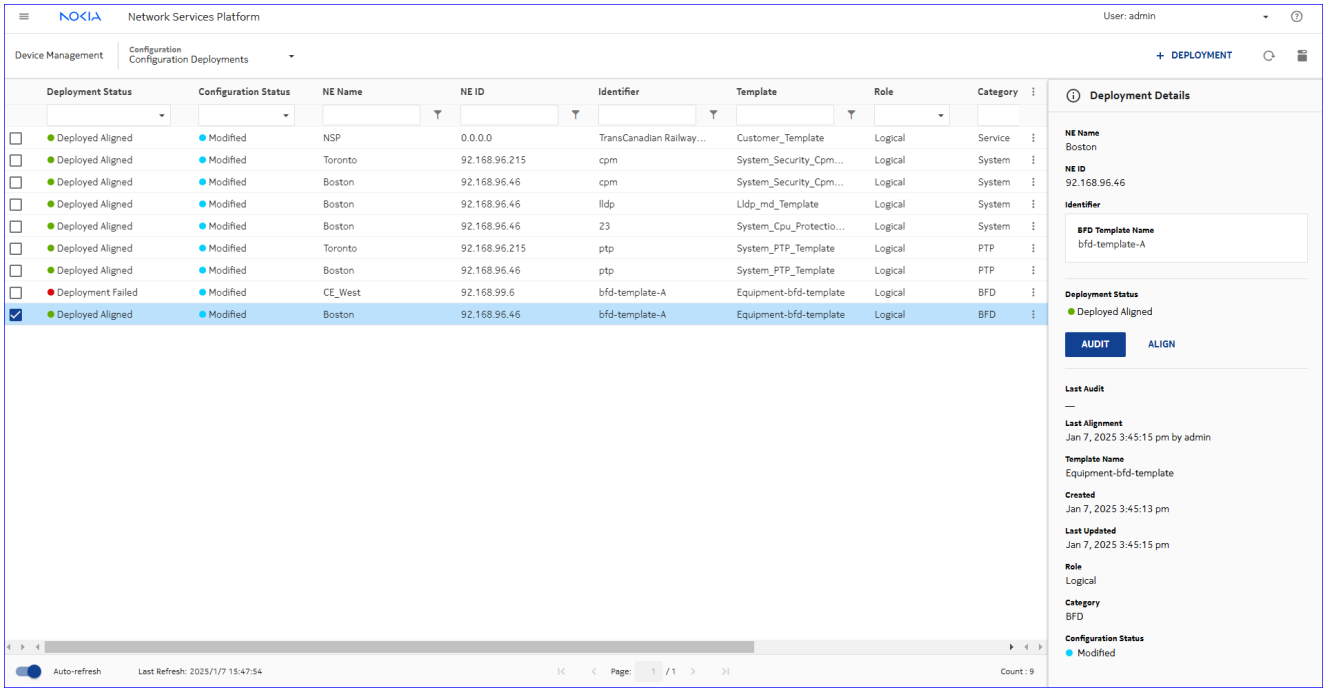


Figure 7-14 NE CLI after deployment

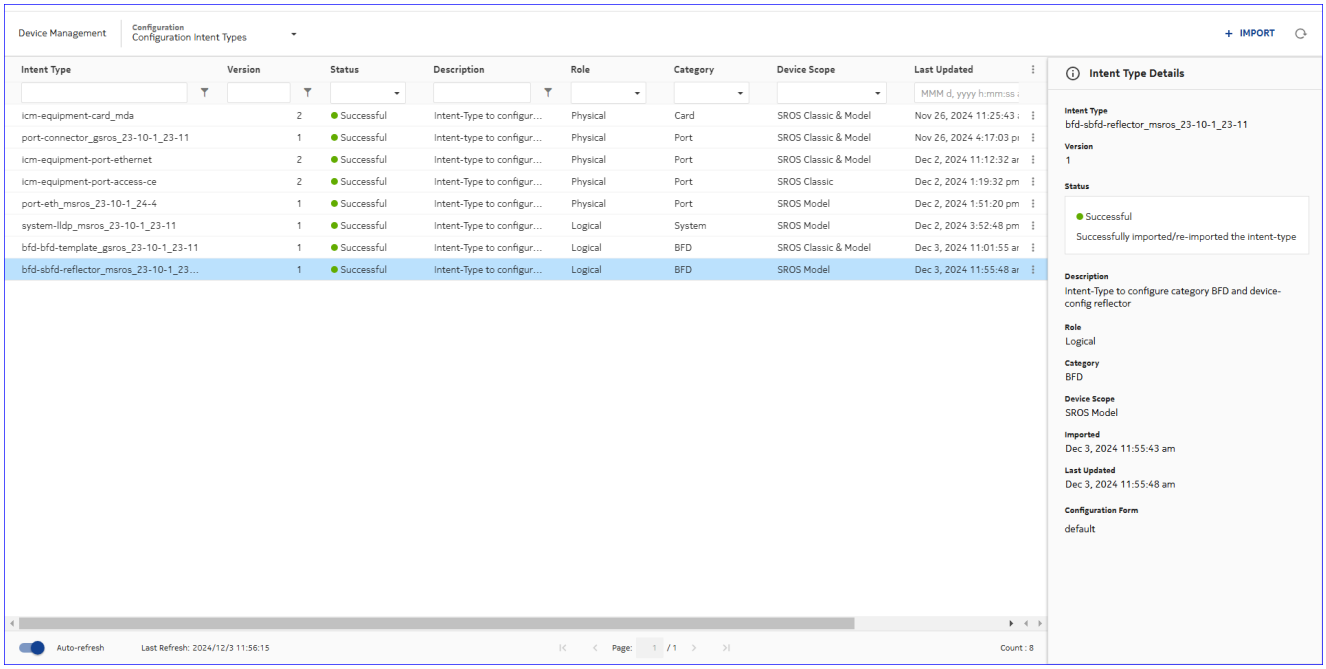
```
(pr)[/configure bfd bfd-template "bfd-template-A"]
A:admin@Boston# info
    echo-receive 400
    multiplier 2
    receive-interval 100000
    transmit-interval 10
    type cpm-np

(pr)[/configure bfd bfd-template "bfd-template-A"]
```

END OF STEPS

7.5.2 Configure BFD Templates using bfd-sbfd-reflector-msros intent

1

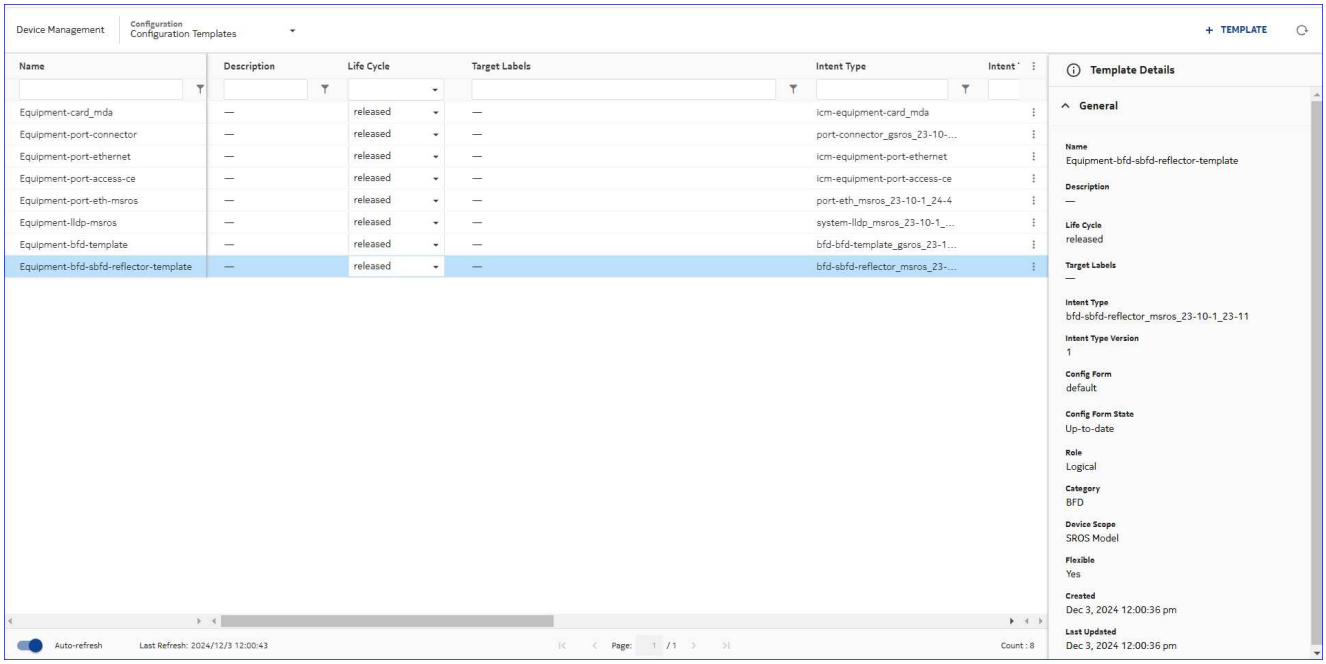
Import intent type **bfd-sbfd-reflector_msros_23-10-1_23-11** into **Device Management**, **Configuration Intent Types**.



2

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

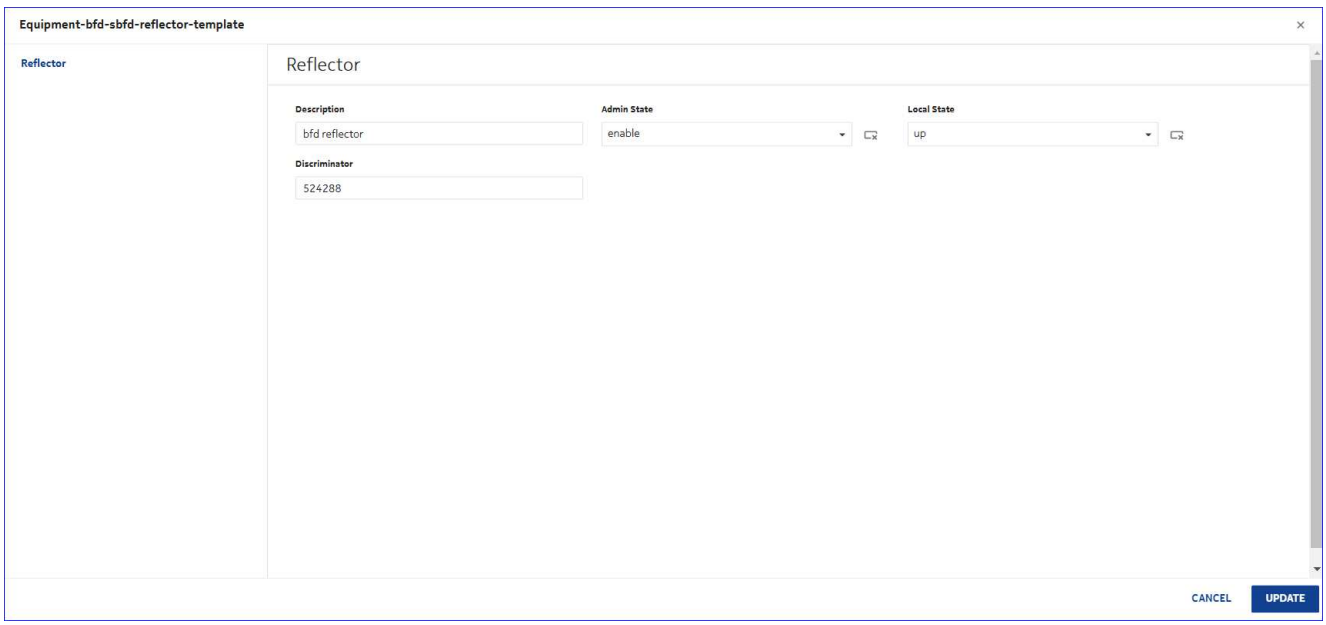
For example, the configuration template created below is named as **Equipment-bfd-sbfd-reflector-template**.

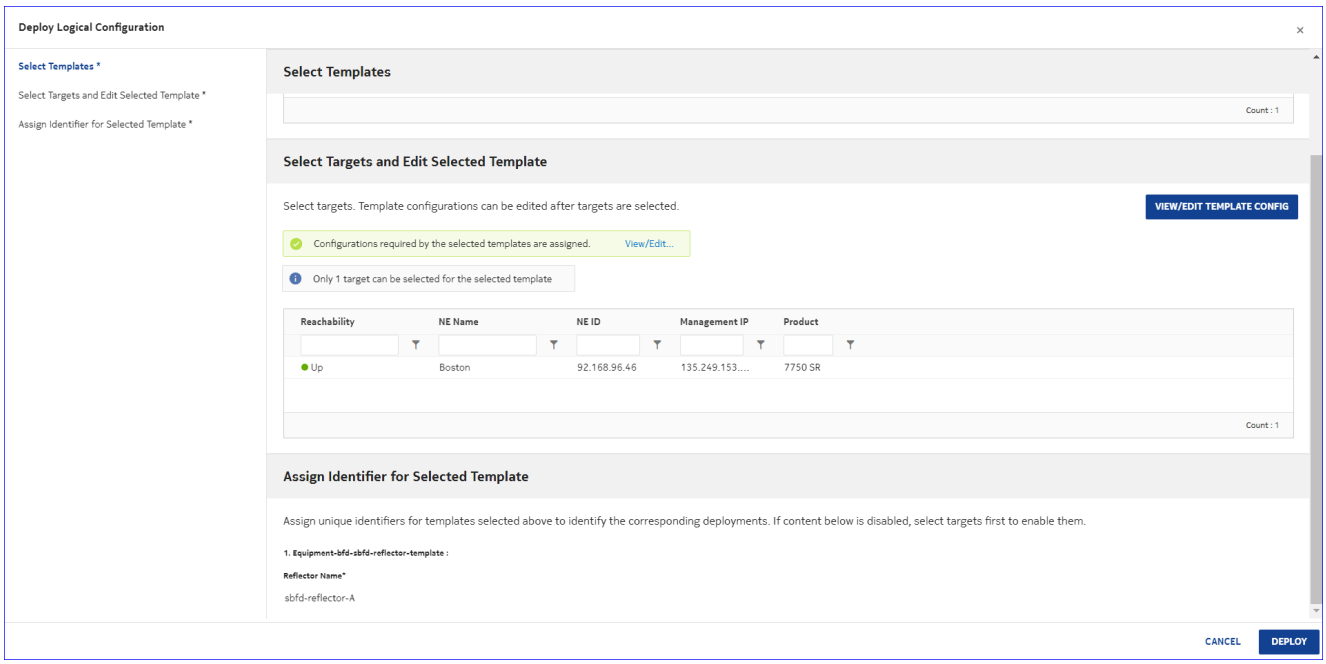


3

Create configuration deployments using the above configuration template.

The following example uses 7750 SR-14s in MD mode.





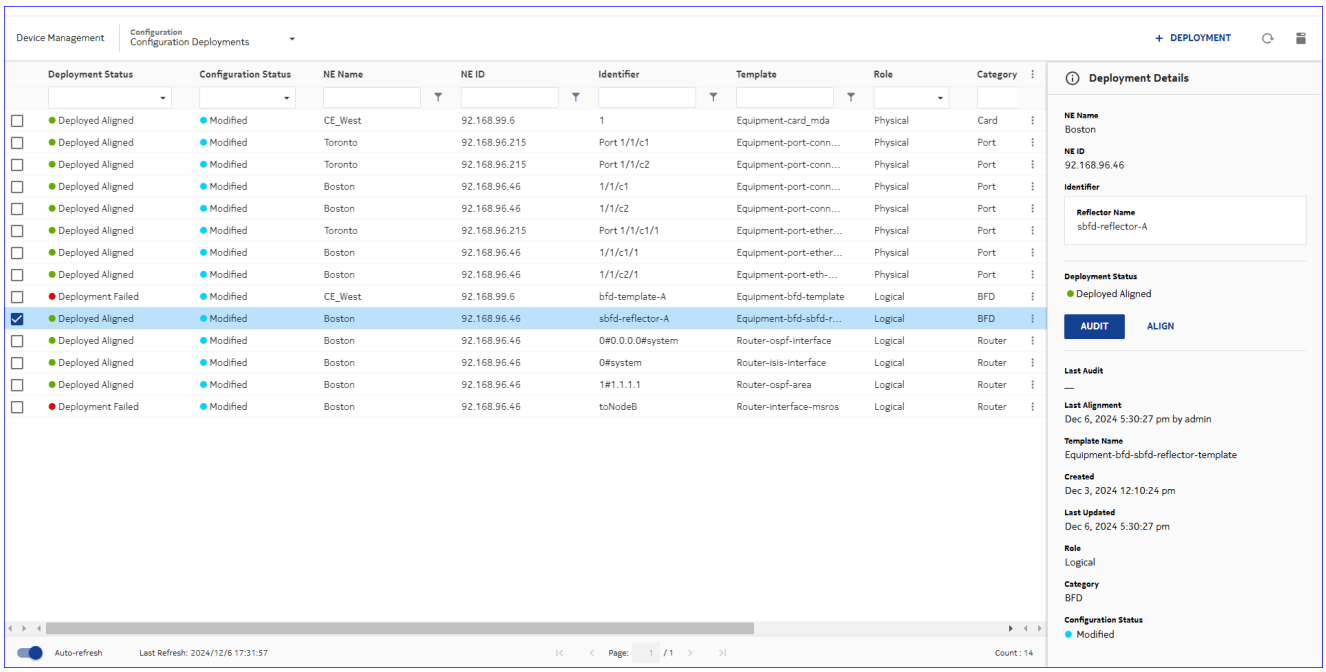


Figure 7-15 NE CLI after deployment

```
(pr)[/configure bfd]
A:admin@Boston# info
    bfd-template "bfd-template-A" {
    }
    seamless-bfd {
        reflector "sbfd-reflector-A" {
            admin-state enable
            description "bfd reflector"
            discriminator 524288
            local-state up
        }
    }

(pr)[/configure bfd]
```

END OF STEPS

7.6 OSPF/ISIS

7.6.1 To configure OSPF Area on MD NEs with router-ospf-area_msros_23-10-1_24-4 intent

router-ospf-area_msros_23-10-1_24-4 intent can be used to create OSPF instance and area, and also configure the same on MD NEs.

1

Prerequisites:

Note: The following prerequisites are unique to the example deployment below.

Configure import and export policies:

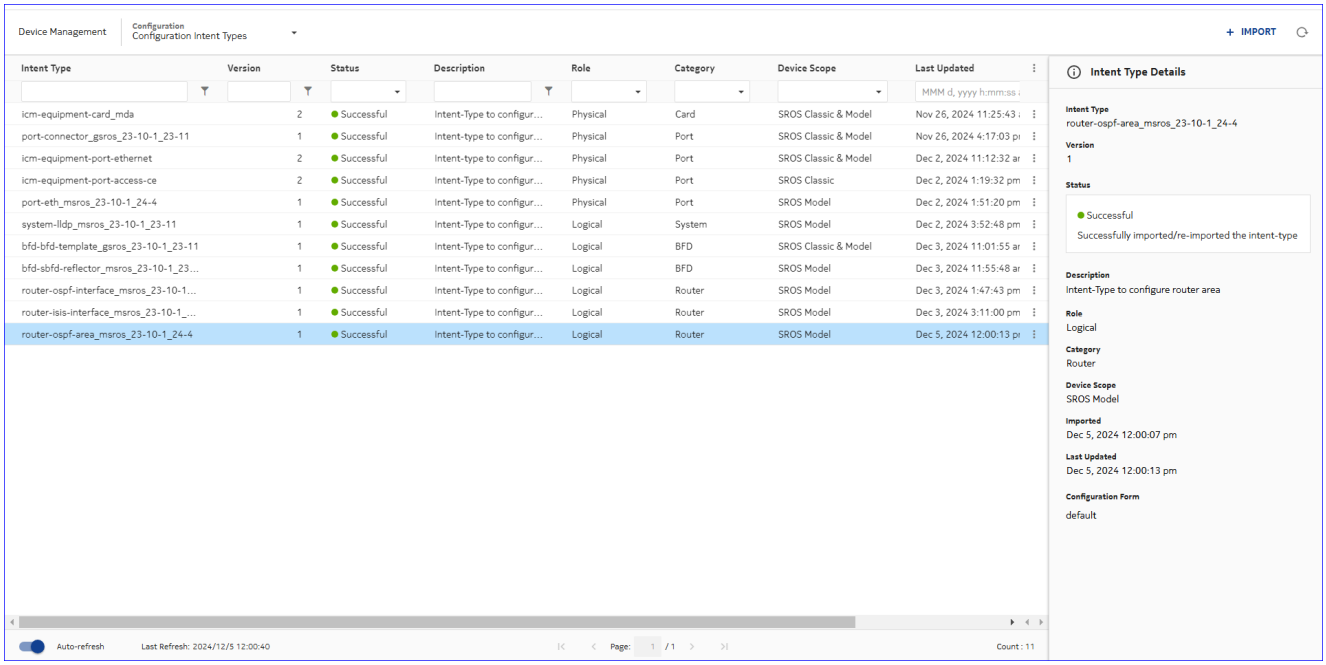
- `/configure policy-options policy-statement "export_policy"`
  `/configure policy-options policy-statement "import_policy"`

Configure BIER template:

- `/configure router "Base" bier template "BIER_Template_1"`

2

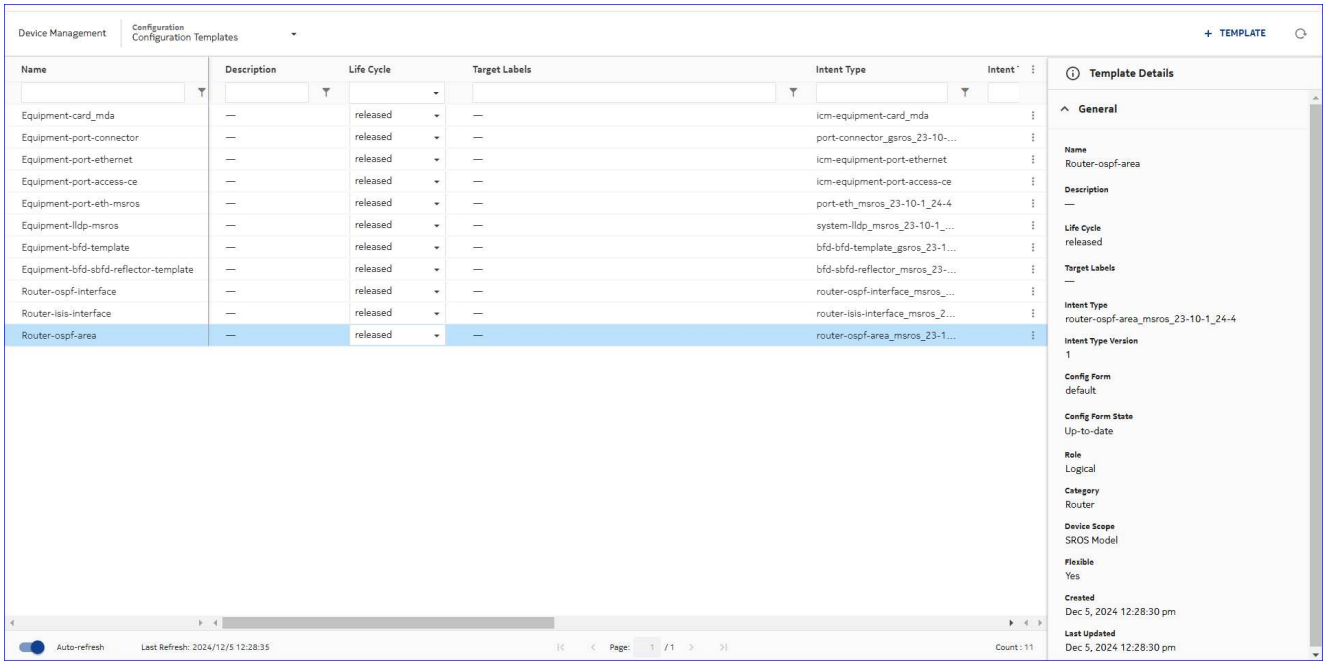
Import the intent type **router-ospf-area_msros_23-10-1_24-4** into **Device Management**, **Configuration Intent Types**.



3

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

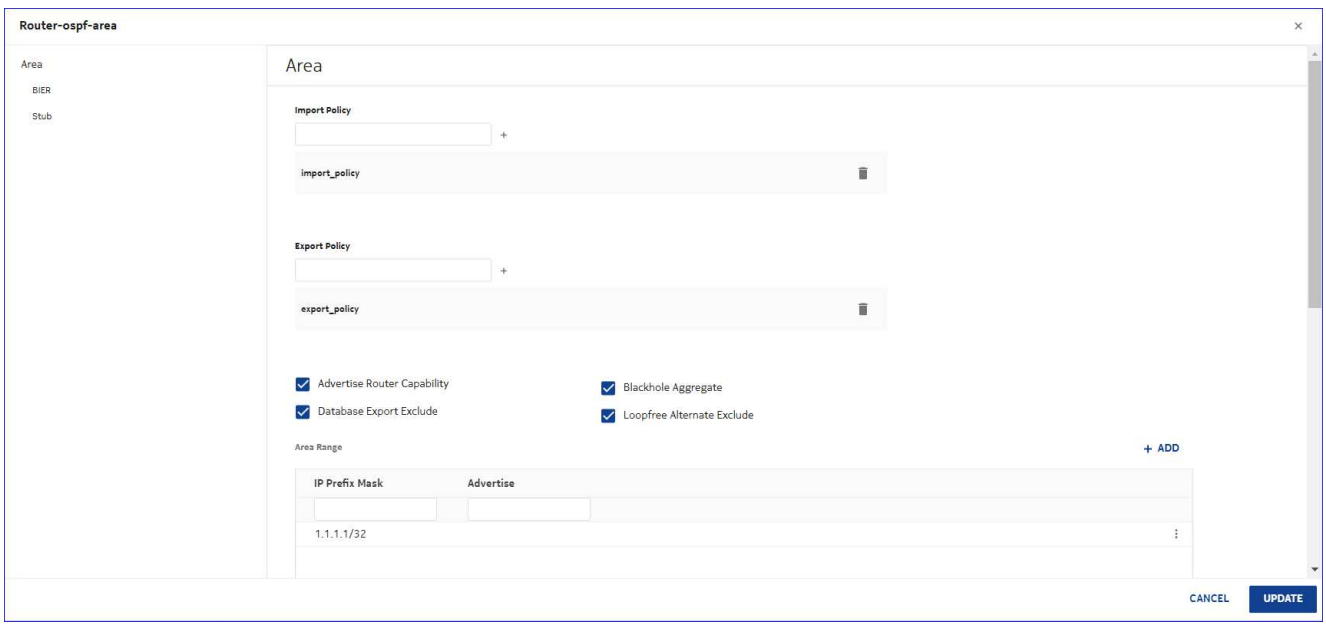
For example, the configuration template created below is named as **Router-ospf-area**.

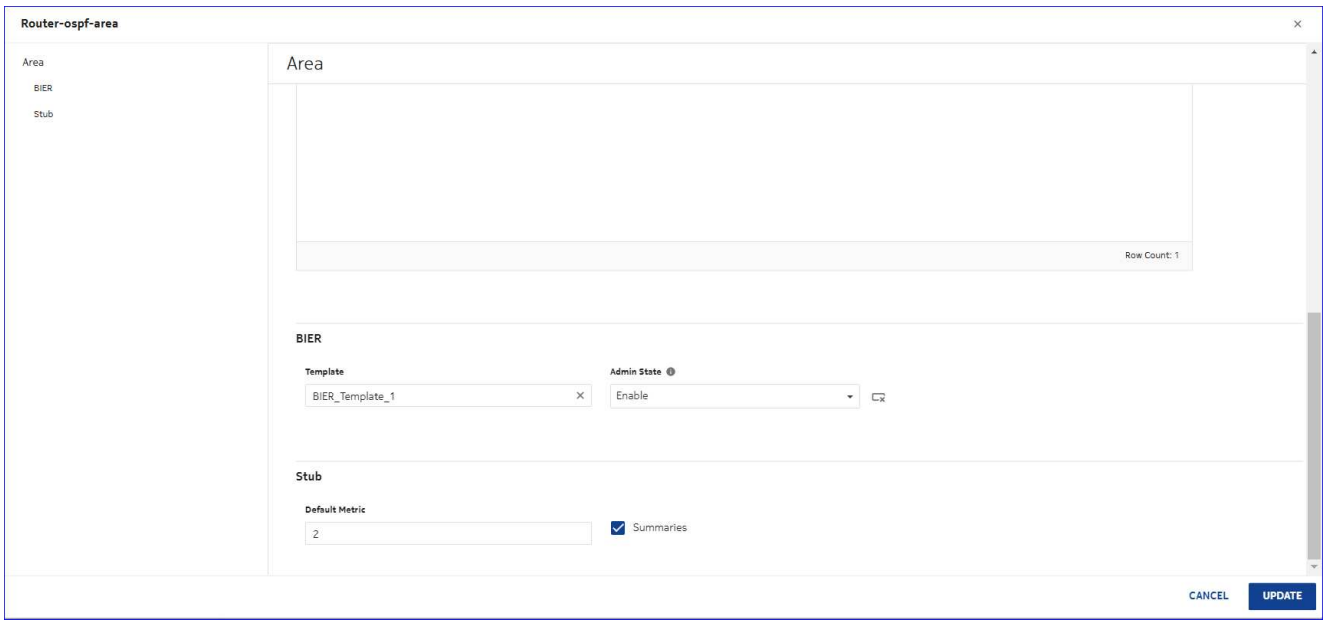


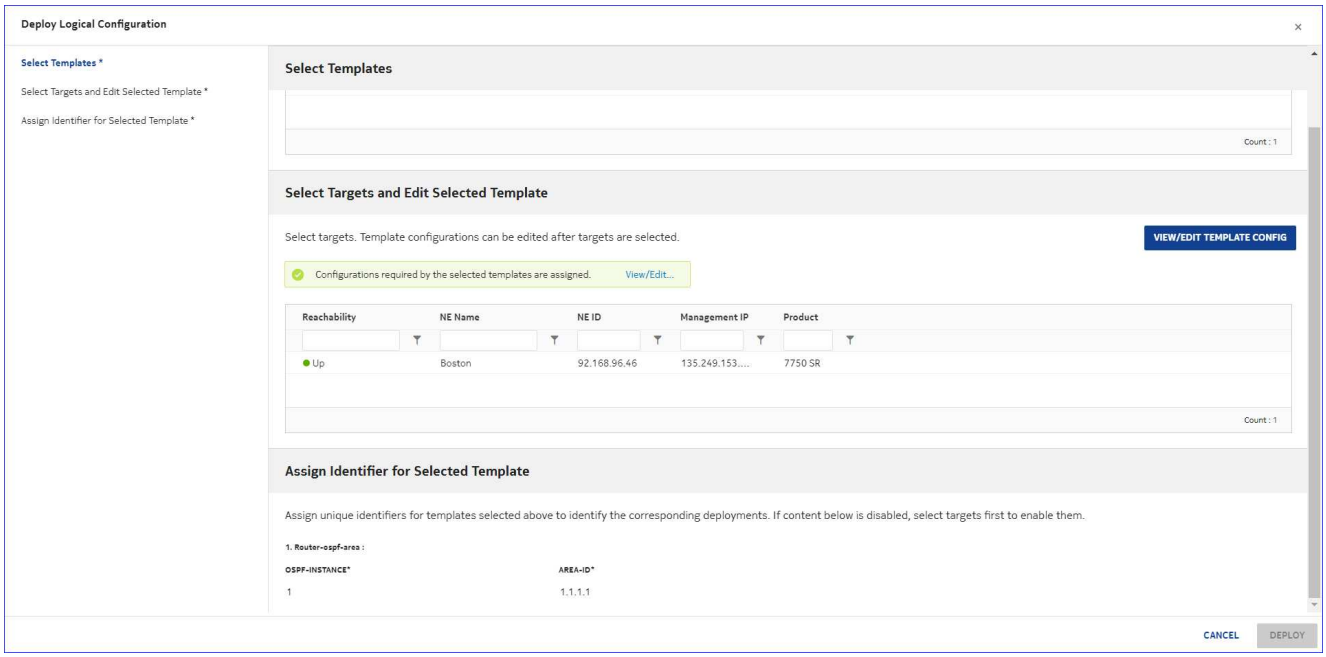
4

Create configuration deployments using the above configuration template.

The following example uses 7750 SR-14s MD.







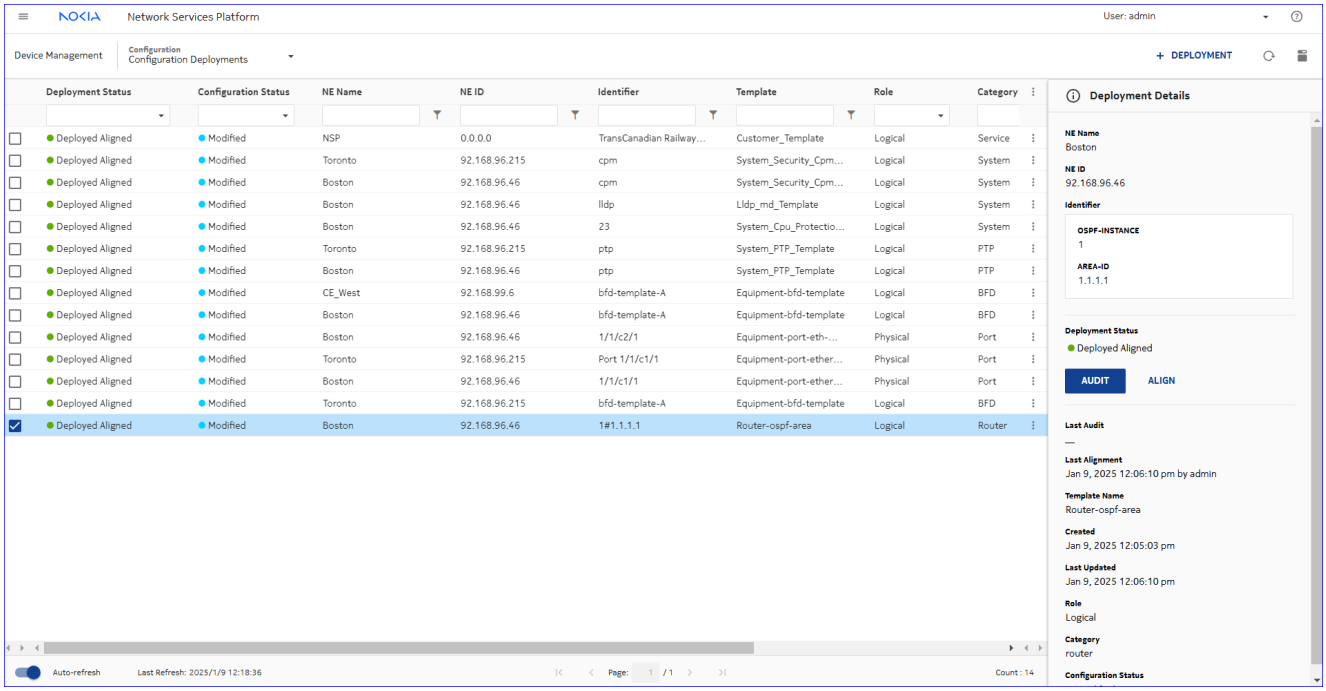


Figure 7-16 NE CLI after deployment

```
(pr)[/configure router "Base" ospf 1]
A:admin@Boston# info
    area 1.1.1.1 {
        advertise-router-capability true
        blackhole-aggregate true
        export-policy ["export_policy"]
        import-policy ["import_policy"]
        loopfree-alternate-exclude true
        database-export-exclude true
        stub {
            default-metric 2
            summaries true
        }
        bier {
            admin-state enable
            template "BIER_Template_1"
        }
        area-range 1.1.1.1/32 {
        }
    }
```

END OF STEPS

7.6.2 To configure OSPF Area on Classic NEs with router-ospf-area_csros_23-10-1_24-4 intent

router-ospf-area_csros_23-10-1_24-4 intent can be used to create and configure OSPF instance and area on classic NEs.

1

Prerequisites:

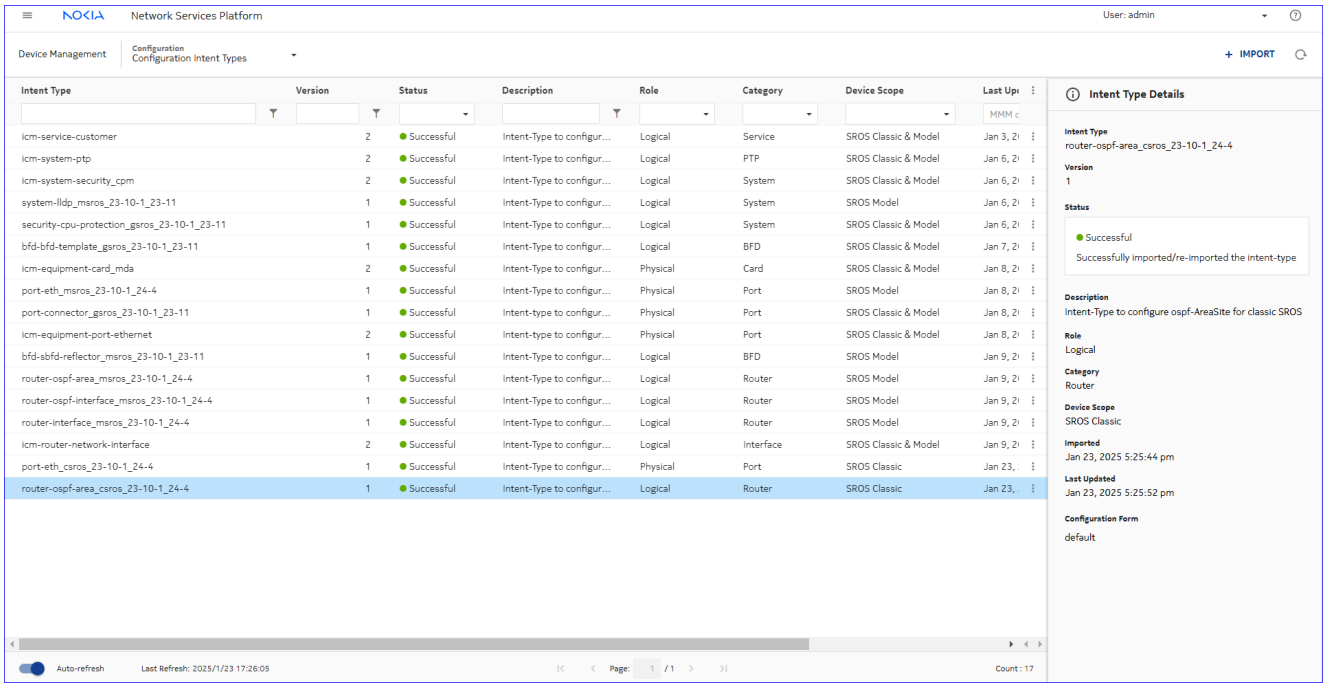
Note: The following prerequisites are unique to the example deployment below.

Configure BIER template:

- `/configure router "Base" bier template "BIER_Template_1"`

2

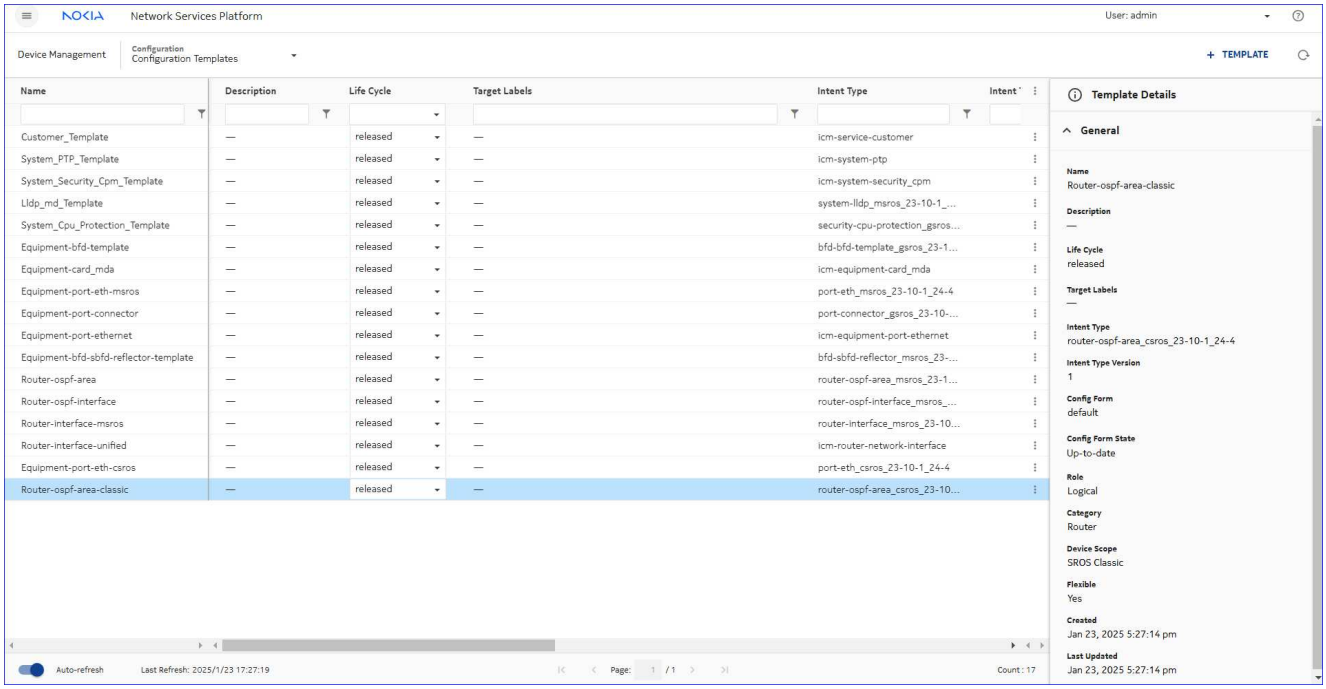
Import the intent type **router-ospf-area_csros_23-10-1_24-4** into **Device Management**, **Configuration Intent Types**.



3

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

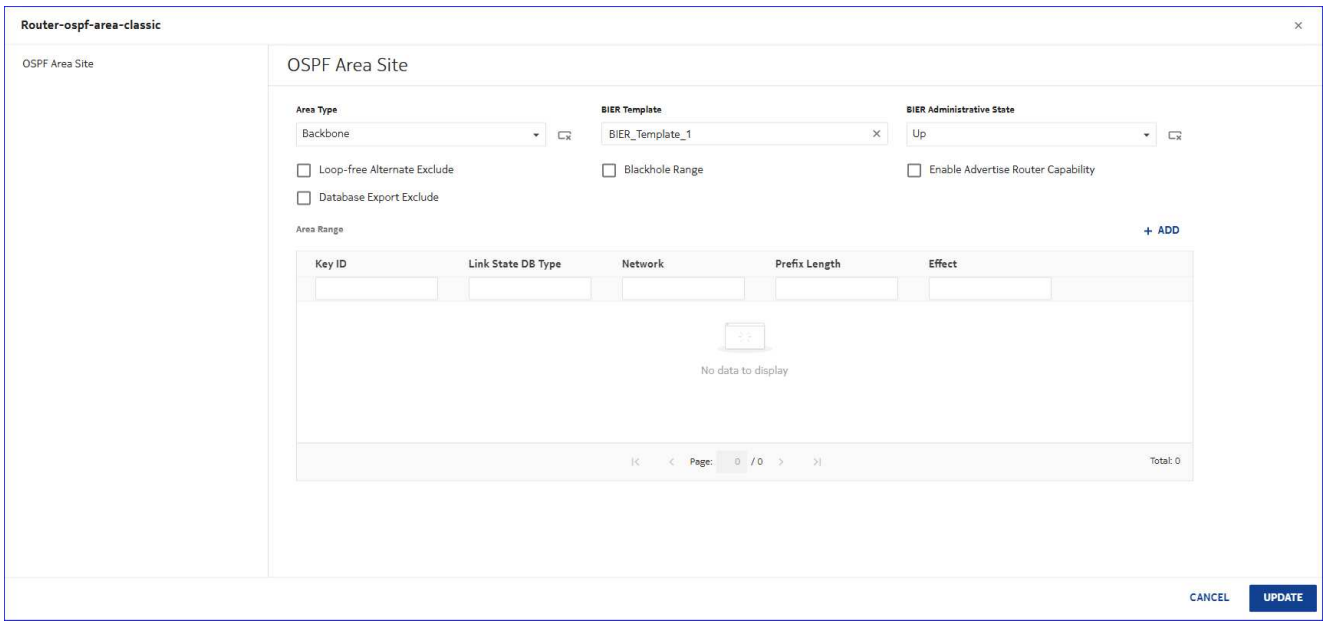
For example, the configuration template created below is named as **Router-ospf-area-classic**.

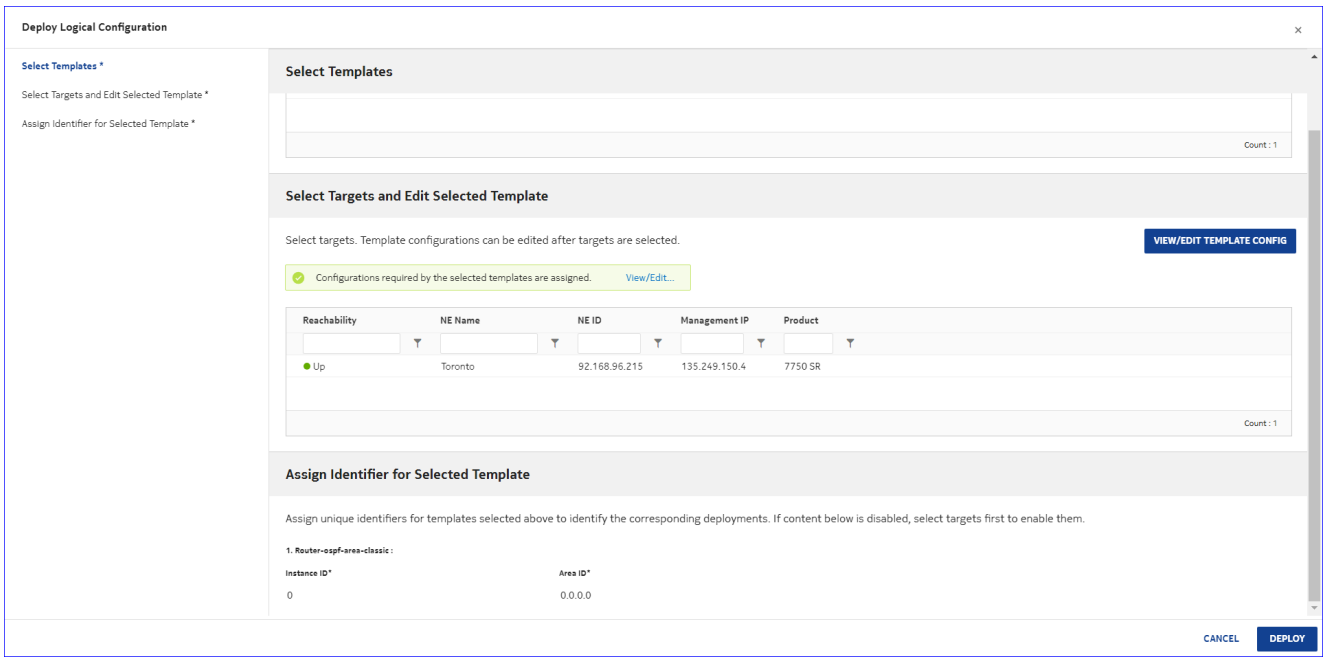


4

Create configuration deployments using the above configuration template.

The following example deploys on 7750 SR-14s classic NE.





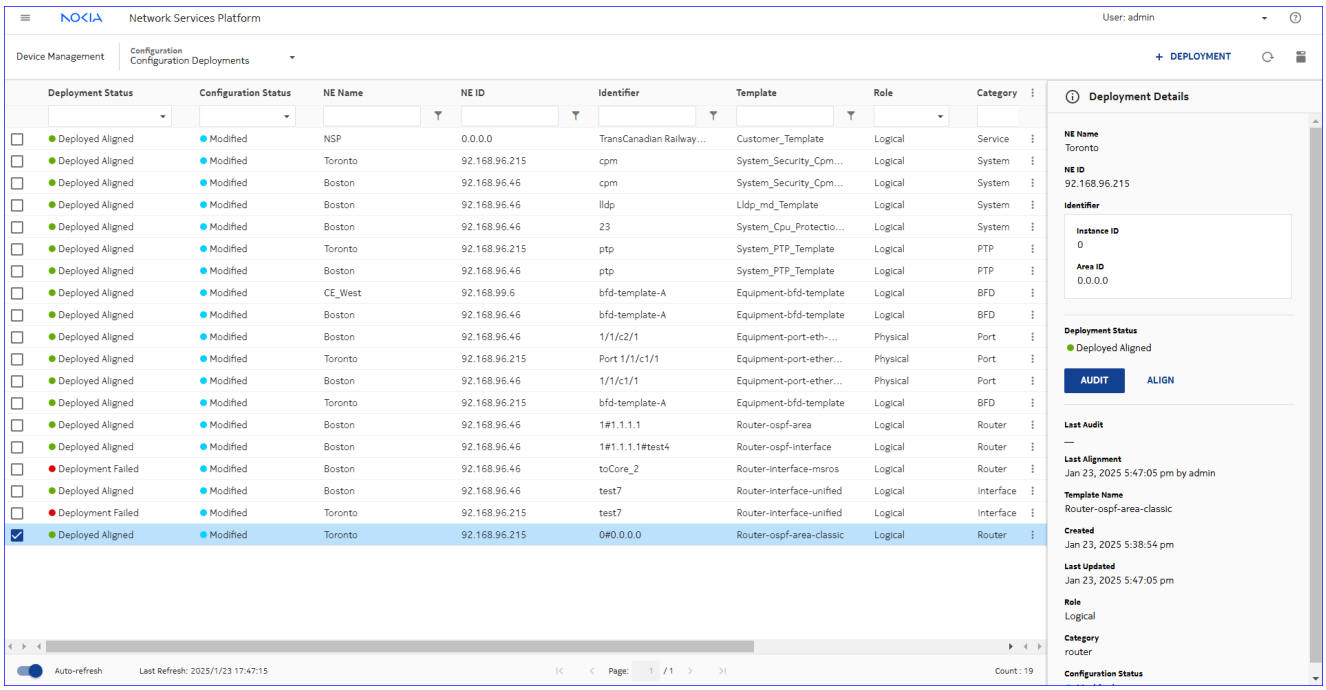


Figure 7-17 NE CLI after deployment

```
A:Toronto>config>router>ospf# info
----------------------------------------------
            traffic-engineering
            advertise-router-capability area
            segment-routing
                prefix-sid-range global
                no shutdown
            exit
            area 0.0.0.0
                no advertise-router-capability
                no blackhole-aggregate
                bier
                    template "BIER_Template_1"
                    no shutdown
                exit
                interface "system"
                    node-sid label 20000
                    no shutdown
                exit
            exit
            no shutdown
----------------------------------------------
```

END OF STEPS

7.6.3 To configure OSPF Interface on MD NEs using router-ospf-interface-msros intent

1

Prerequisites:

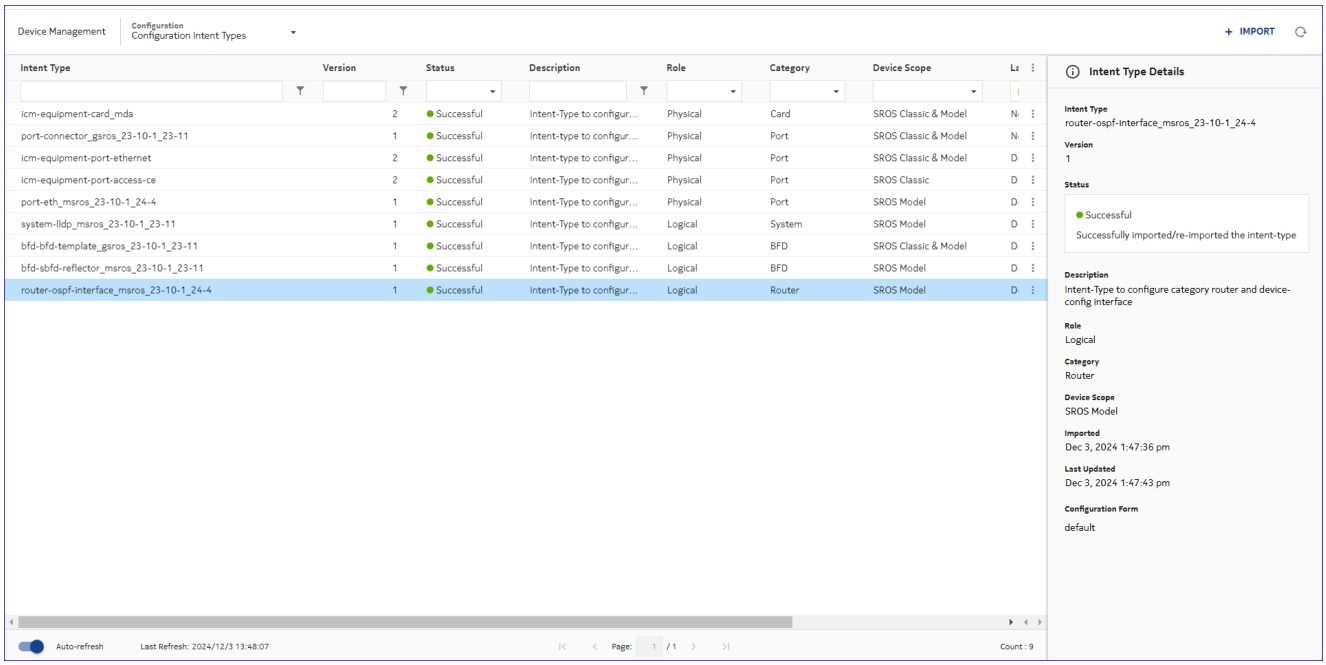
Note: The following prerequisites are unique to the example deployment below.

- OSPF area should be created (see 7.6.2 “To configure OSPF Area on Classic NEs with router-ospf-area_csros_23-10-1_24-4 intent” (p. 298) for details)
- Authentication keychain should be configured:

  `/configure system security keychains keychain "keychain-1"`

2

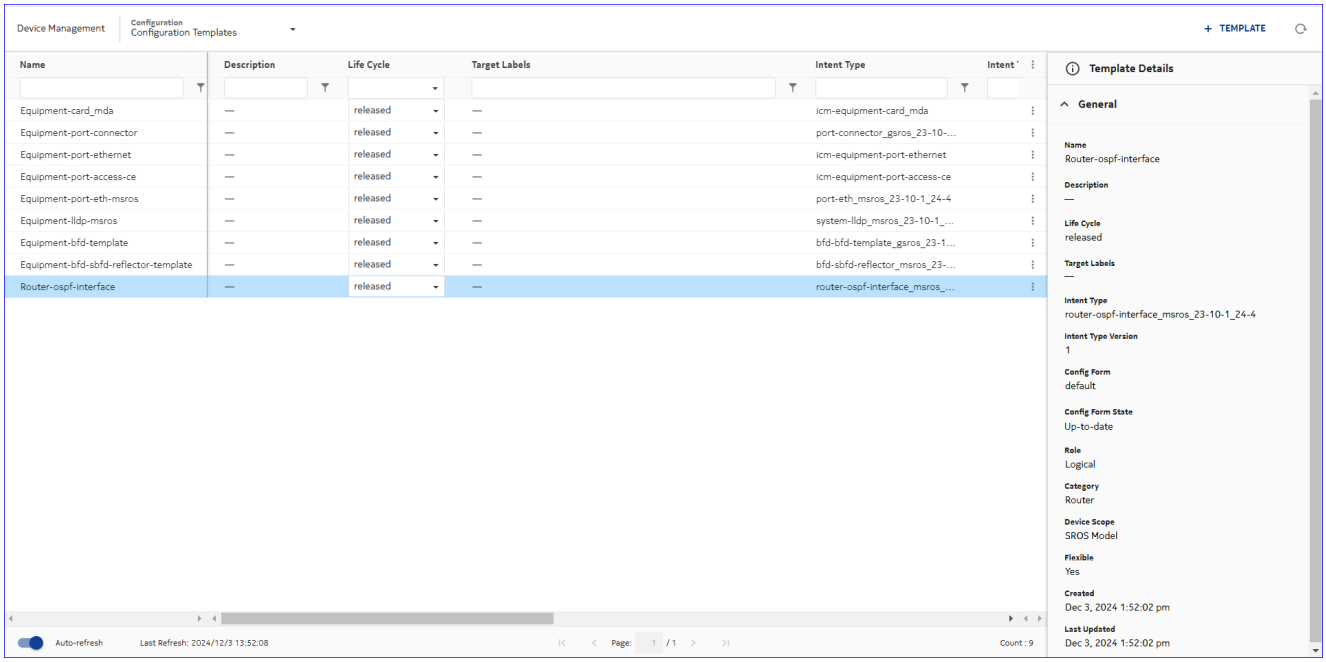
Import the intent type **router-ospf-interface_msros_23-10-1_24-4** into **Device Management**, **Configuration Intent Types**.



3

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

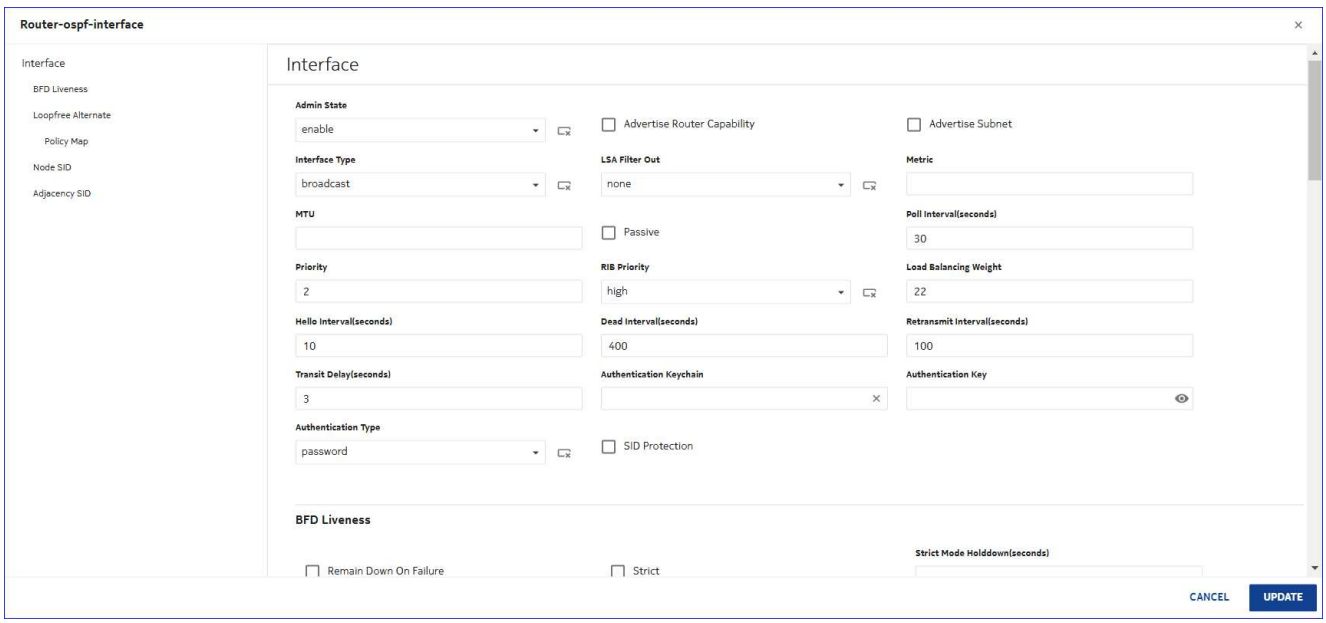
For example, the configuration template created below is named as **Router-ospf-interface**.

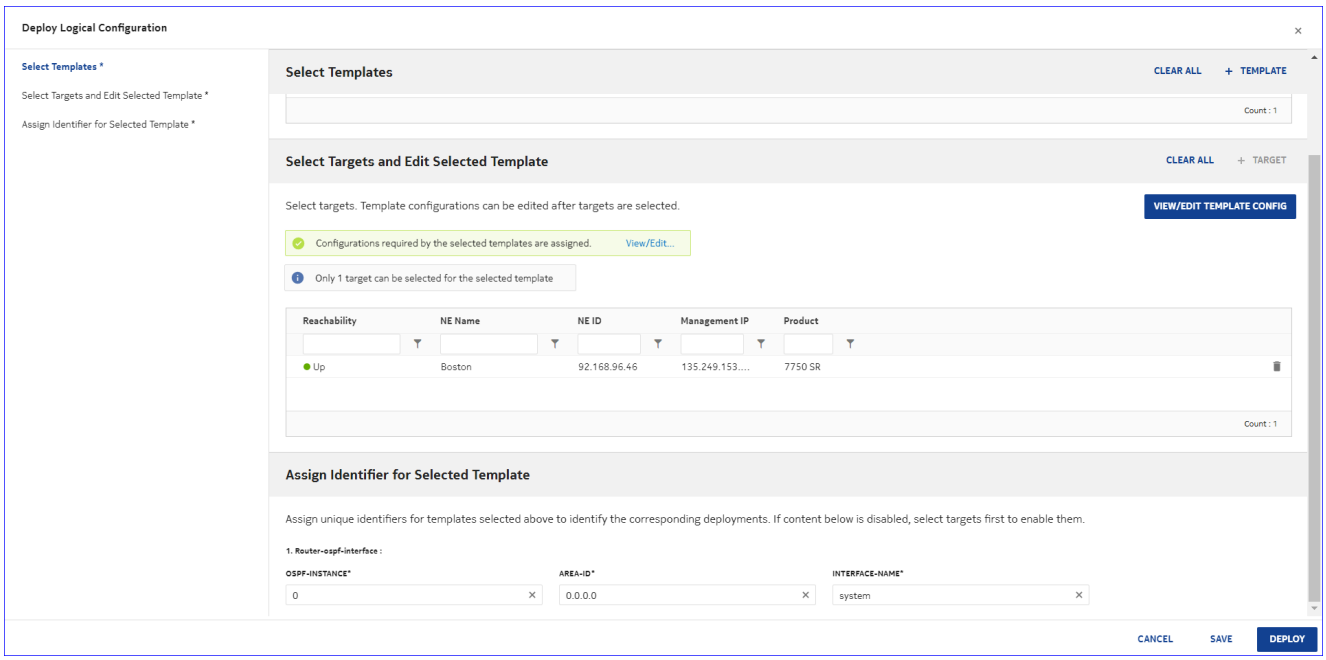


4

Create configuration deployments using the above configuration template.

Example deployment 1: On 7750 SR-14s MD - Router Base OSPF instance 0 area 0.0.0.0





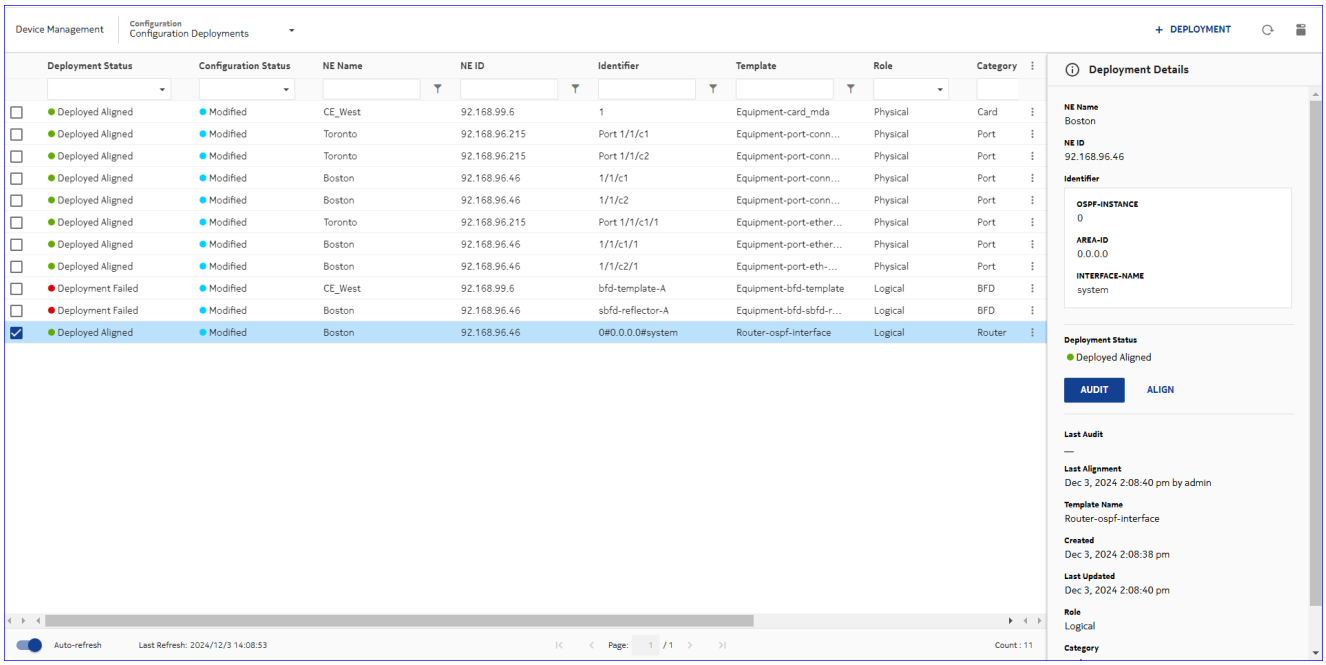
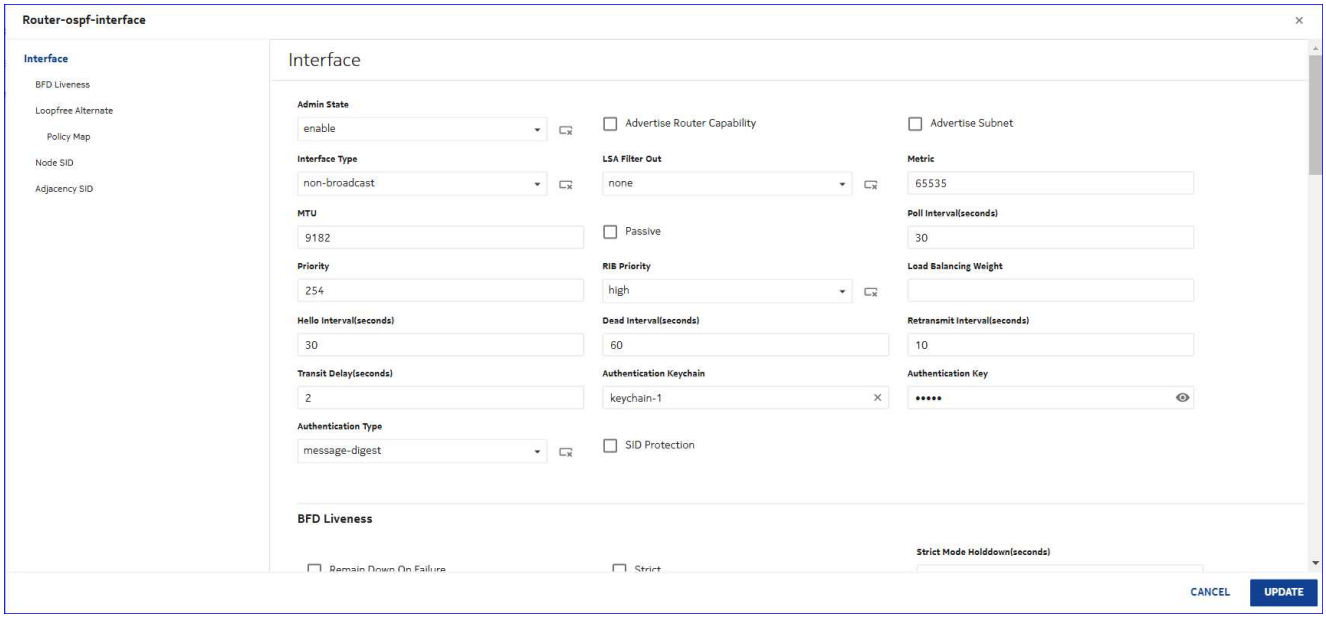
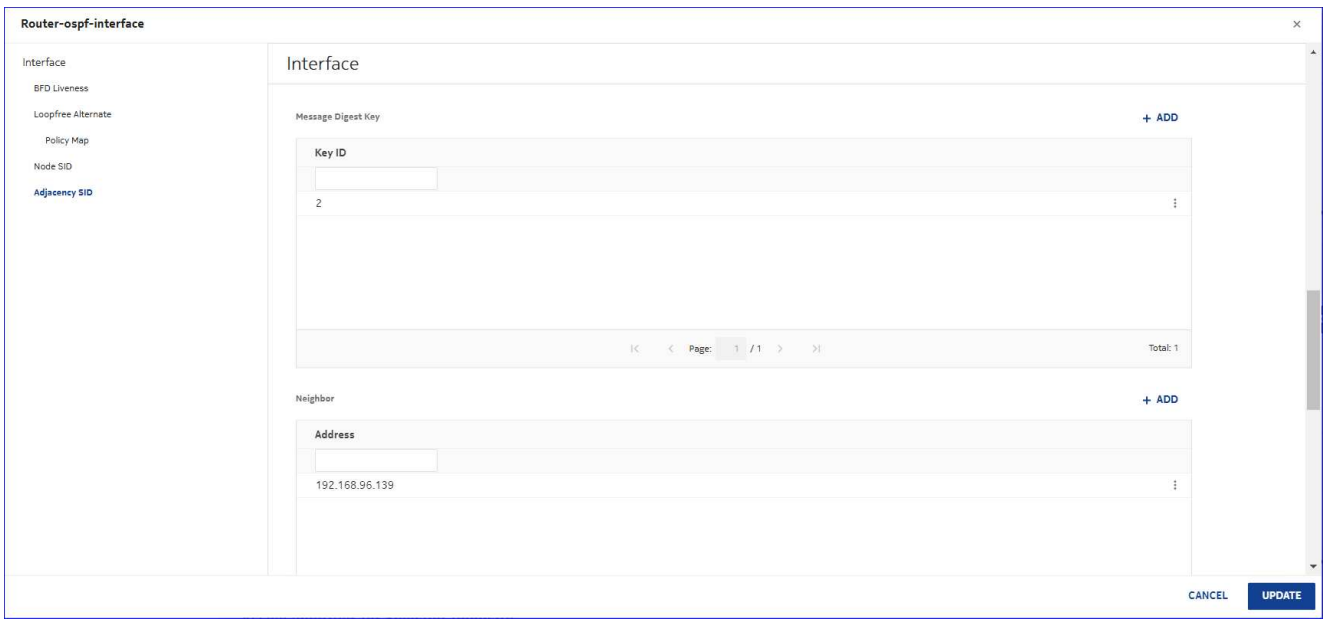


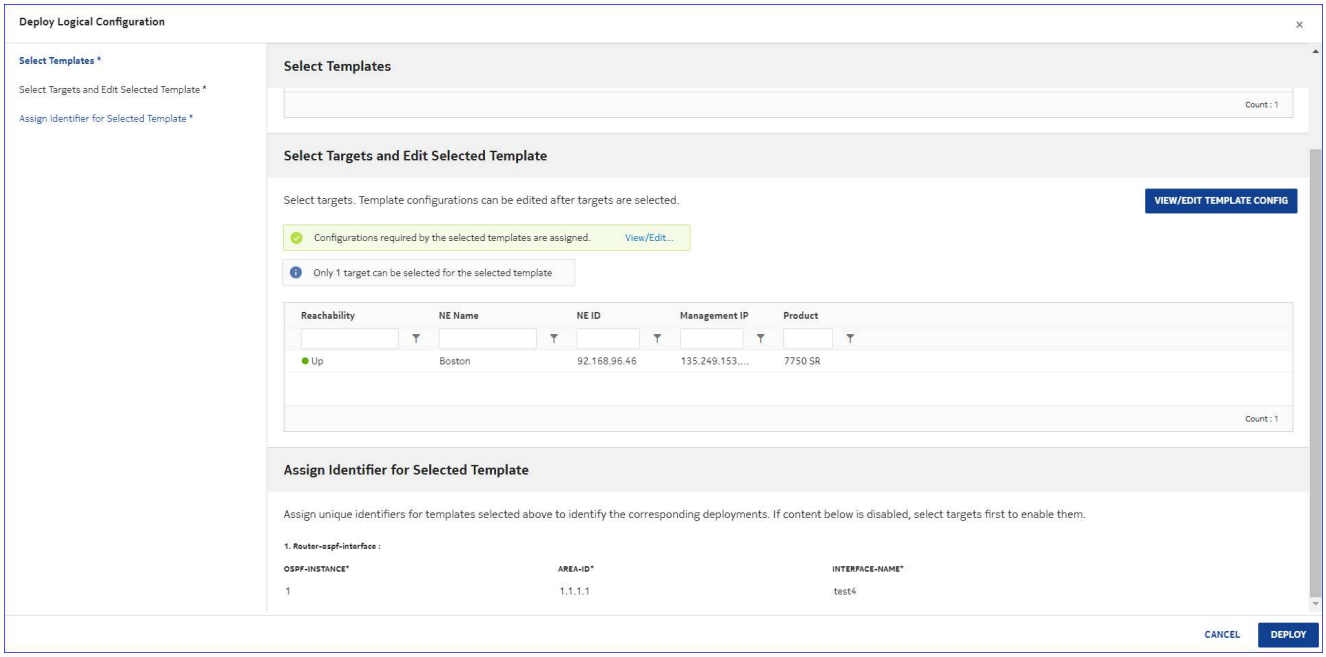
Figure 7-18 NE CLI after deployment

```
(pr)[/configure router "Base" ospf 0 area 0.0.0.0]
A:admin@Boston# info
    interface "system" {
        admin-state enable
        interface-type broadcast
        lsa-filter-out none
        poll-interval 30
        priority 2
        rib-priority high
        load-balancing-weight 22
        hello-interval 10
        dead-interval 400
        retransmit-interval 100
        transit-delay 3
        authentication-type password
        bfd-liveness {
        }
    }

(pr)[/configure router "Base" ospf 0 area 0.0.0.0]
```

Example deployment 2: On 7750 SR-14s MD - Router Base OSPF instance 1 area 1.1.1.1 with a different set of attributes







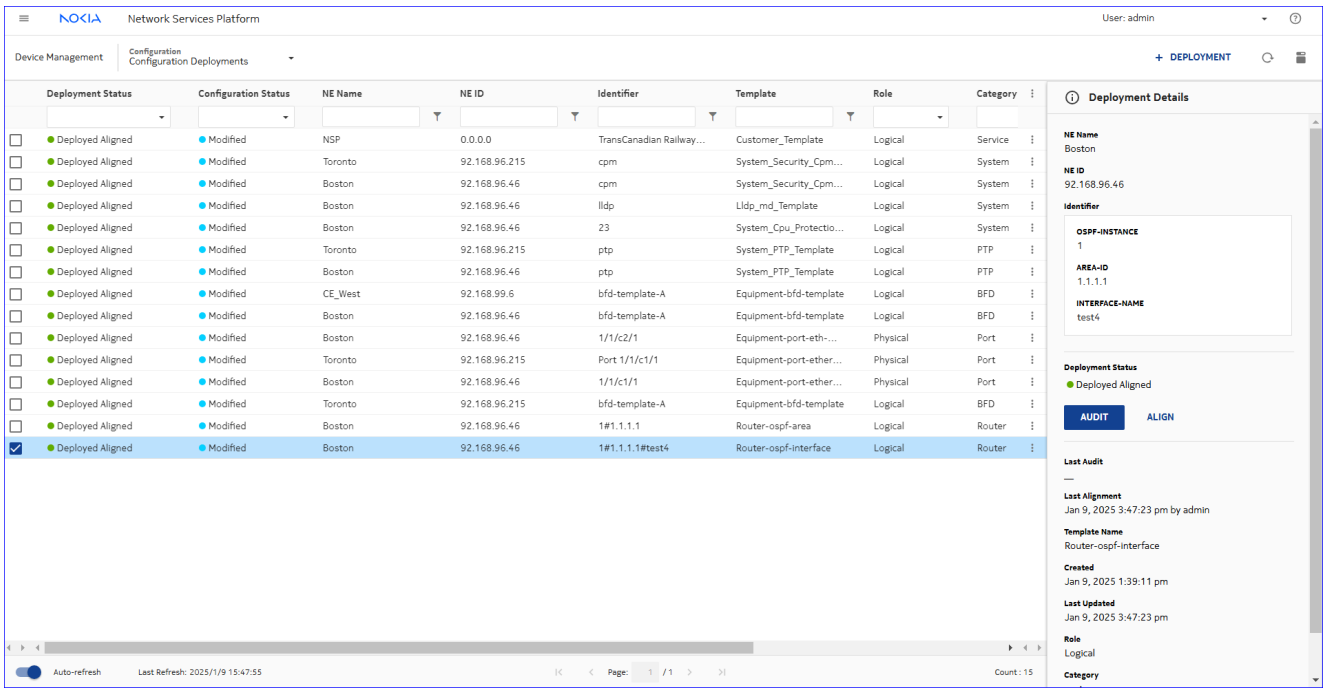


Figure 7-19 NE CLI after deployment

```
(pr)[/configure router "Base" ospf 1 area 1.1.1.1 interface "test4"]
A:admin@Boston# info
    admin-state enable
    advertise-router-capability false
    advertise-subnet false
    interface-type non-broadcast
    lsa-filter-out none
    metric 65535
    mtu 9182
    poll-interval 30
    priority 254
    rib-priority high
    hello-interval 30
    dead-interval 60
    retransmit-interval 10
    transit-delay 2
    authentication-keychain "keychain-1"
    authentication-key "fDawqd7d4RnHUWWVfGycGAJSzOGT hash2"
    authentication-type message-digest
    bfd-liveness {
        remain-down-on-failure false
    }
    message-digest-key 2 {
        md5 "ydwfsMCJlzNo0b/NVEI5yFSscWo= hash2"
    }
    neighbor 192.168.96.139 { }
```

END OF STEPS

7.6.4 To configure OSPF Interface on MD NEs using router-ospf-interface-msros intent

router-ospf-interface_csros_23-10-1_24-4 intent can be used to configure OSPF interface on classic SR NEs.

1

Prerequisites:

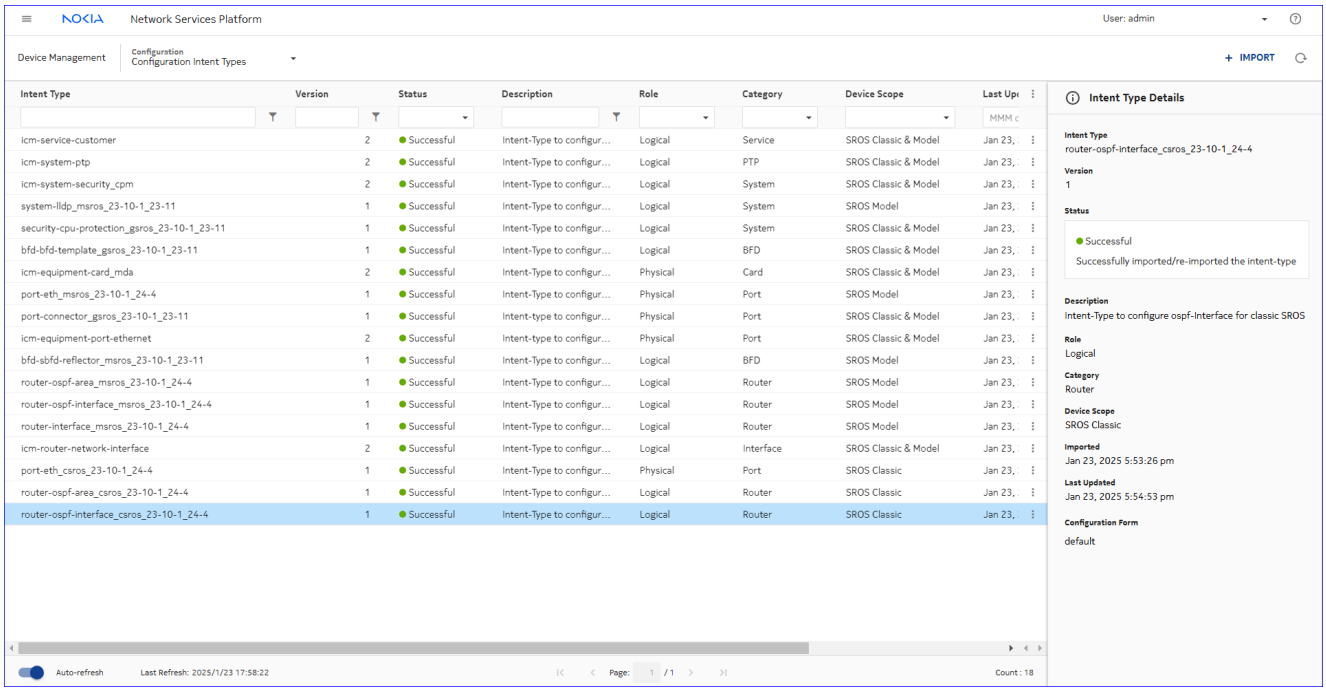
Note: The following prerequisites are unique to the example deployment below.

- OSPF area should be created (see 7.6.2 “To configure OSPF Area on Classic NEs with router-ospf-area_csros_23-10-1_24-4 intent” (p. 298) for details)
- Authentication keychain should be configured:

  `/configure system security keychain "keychain-1"`

2

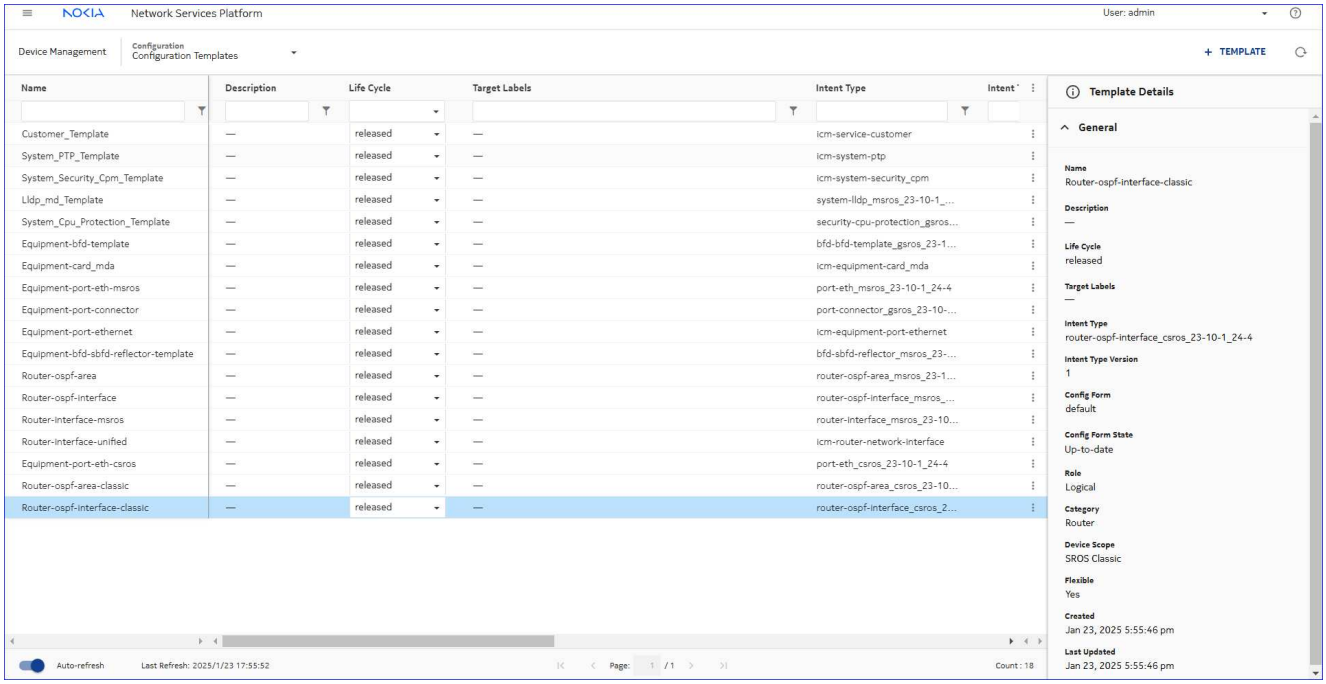
Import the intent type **router-ospf-interface_csros_23-10-1_24-4** into **Device Management**, **Configuration Intent Types**.



3

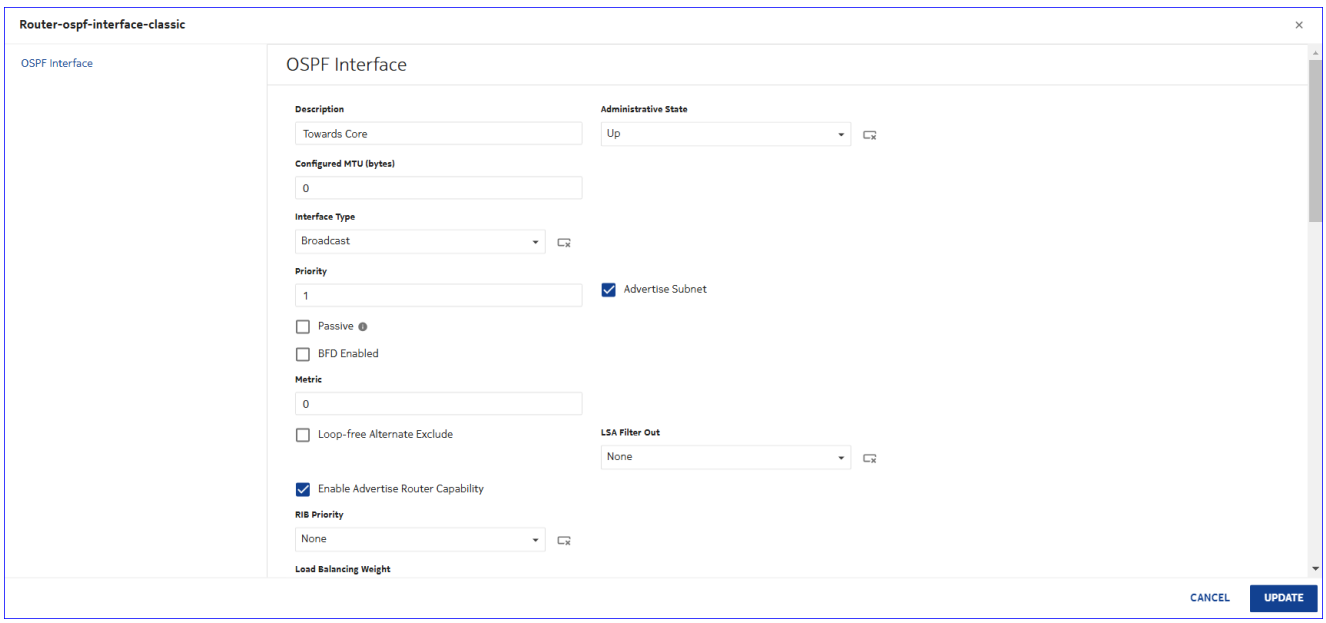
Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

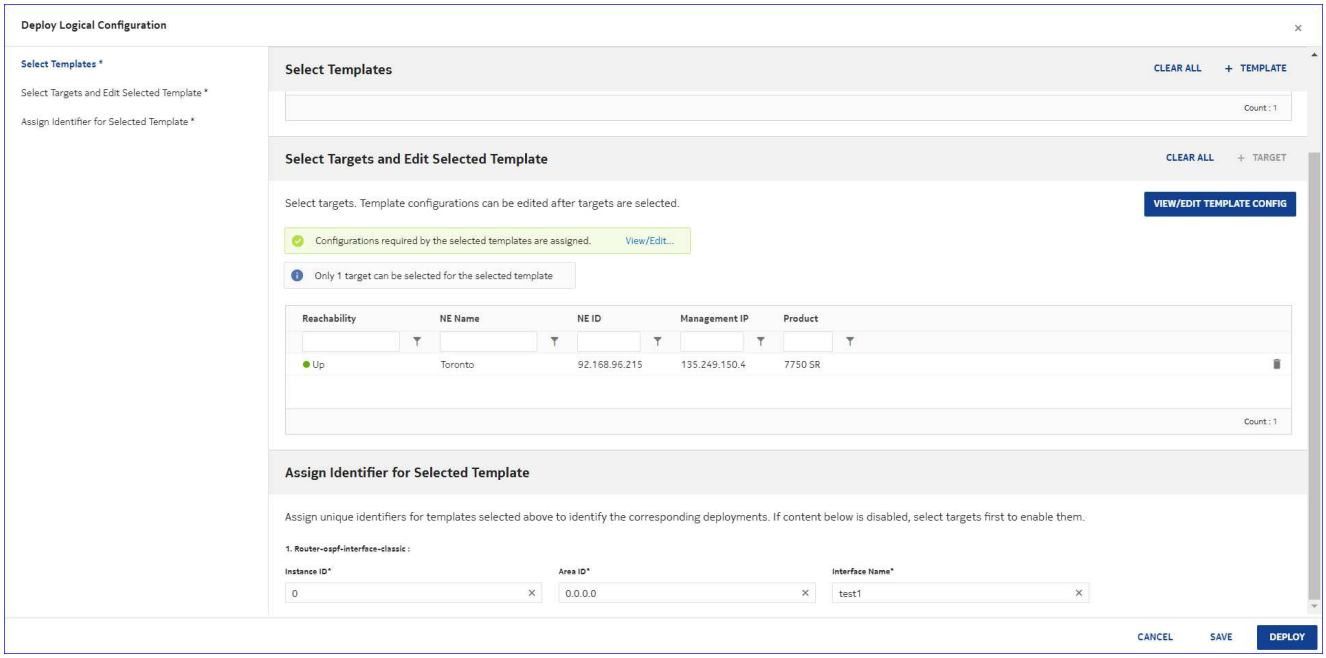
For example, the configuration template created below is named as **Router-ospf-interface-classic**.



4

Create configuration deployments using the above configuration template.





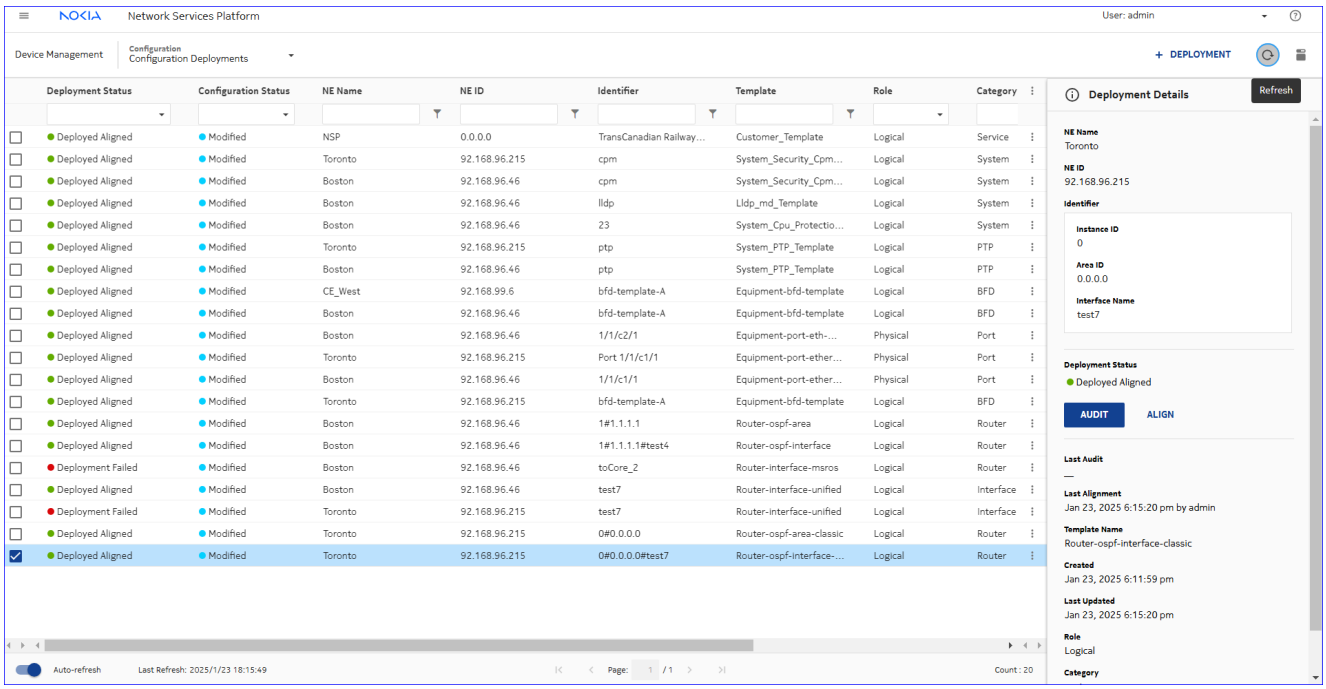


Figure 7-20 NE CLI after deployment

```
-----------------------------------------------
A:Toronto>config>router>ospf# info
-----------------------------------------------
            traffic-engineering
            advertise-router-capability area
            segment-routing
                prefix-sid-range global
                no shutdown
            exit
            area 0.0.0.0
                no advertise-router-capability
                no blackhole-aggregate
                bier
                    template "BIER_Template_1"
                    no shutdown
                exit
                interface "system"
                    node-sid label 20000
                    no shutdown
                exit
                interface "test7"
                    no shutdown
                exit
                interface "test1"
                    interface-type broadcast
                    no shutdown
                exit
            exit
            no shutdown
-----------------------------------------------
```

END OF STEPS

7.6.5 To configure ISIS Interface on MD NEs using router-isis-interface-msros intent

1

Prerequisites:

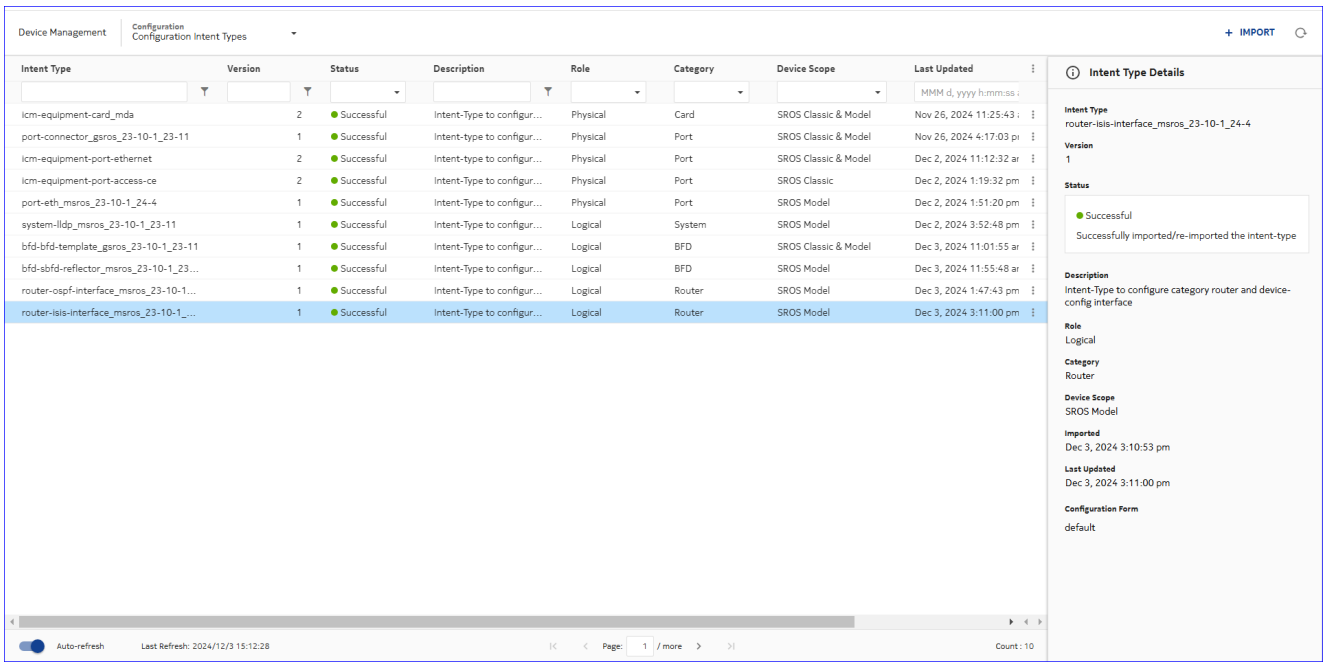
Note: The following prerequisites are unique to the example deployment below.

- ISIS instance and area should be created. This has to be done via NE CLI as there is no intent for this:

```
/edit-config private
/configure router isis 0 admin-state enable
/configure router isis 0 area-address 49.0001
/configure router isis 0 level-capability 2
/configure router isis 0 advertise-router-capability as
/commit
/quit-config
```

2

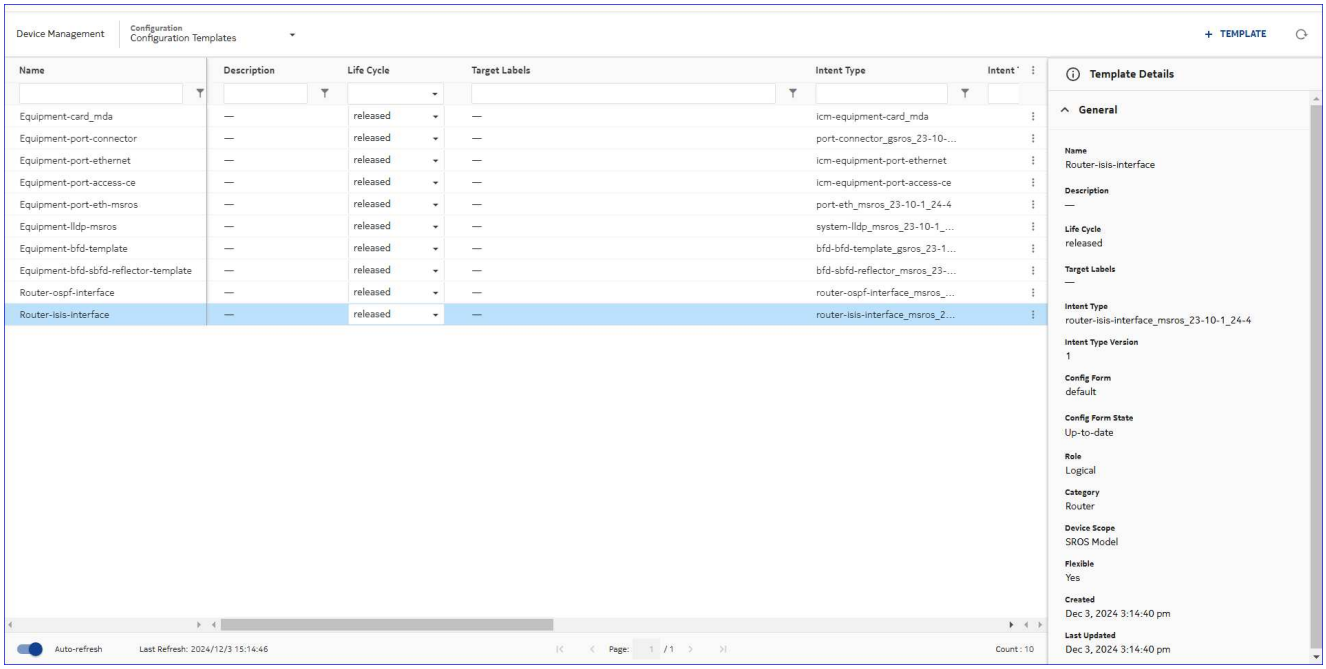
Import the intent type **router-isis-interface_msros_23-10-1_24-4** into **Device Management**, **Configuration Intent Types**.



3

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

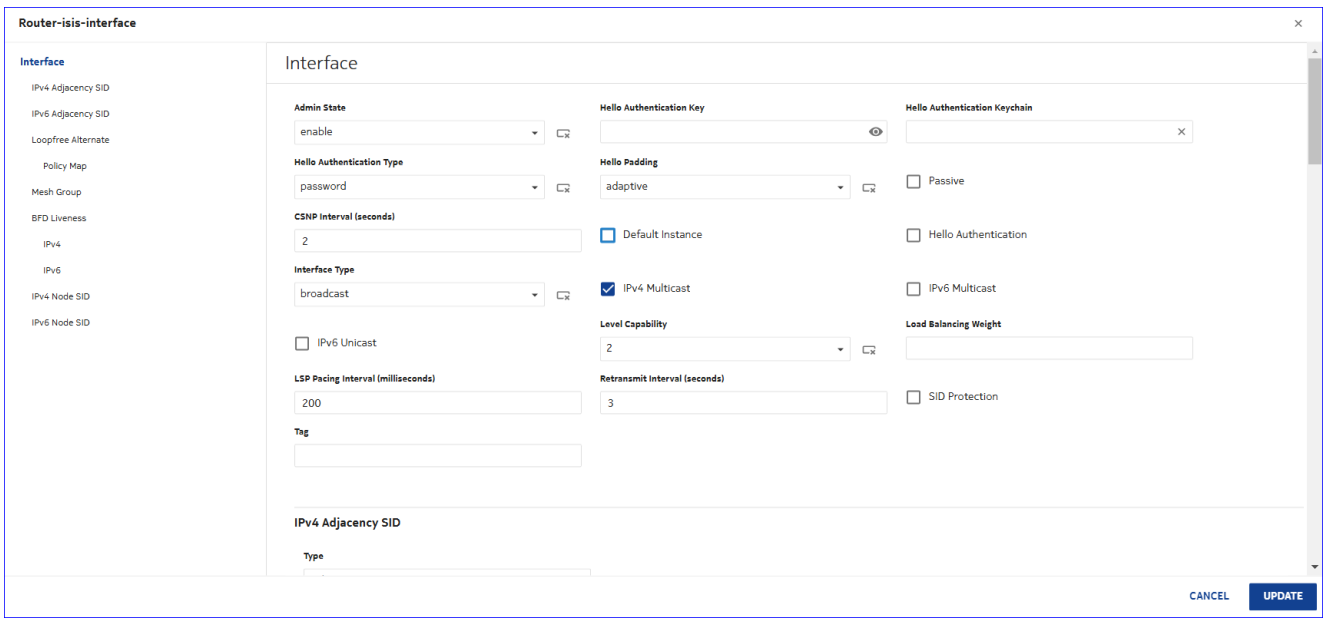
For example, the configuration template created below is named as **Router-isis-interface**.

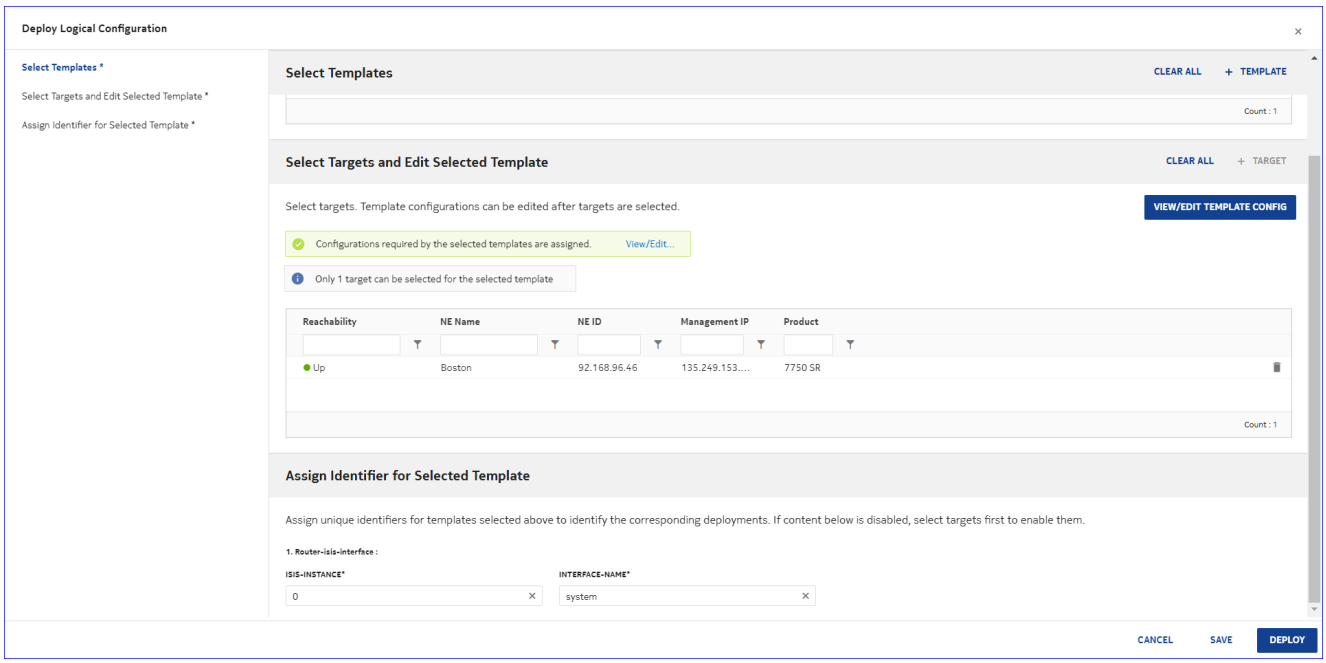


4

Create configuration deployments using the above configuration template.

The following example uses 7750 SR-14s MD.





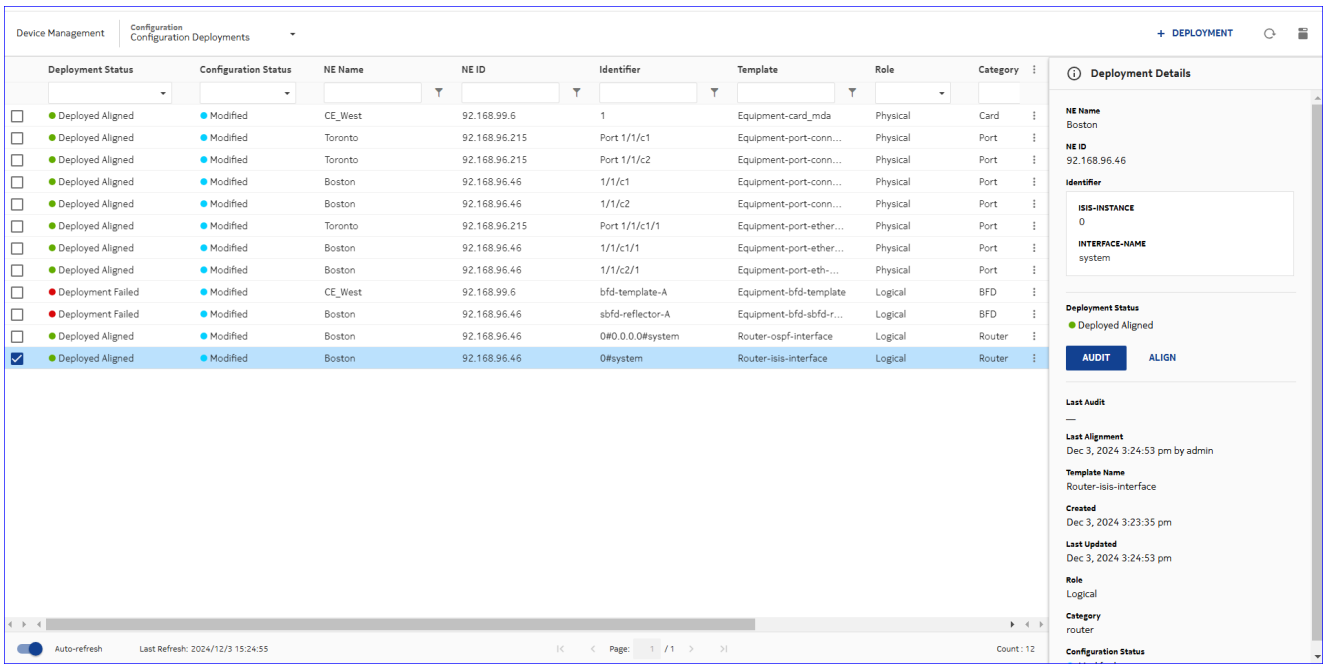
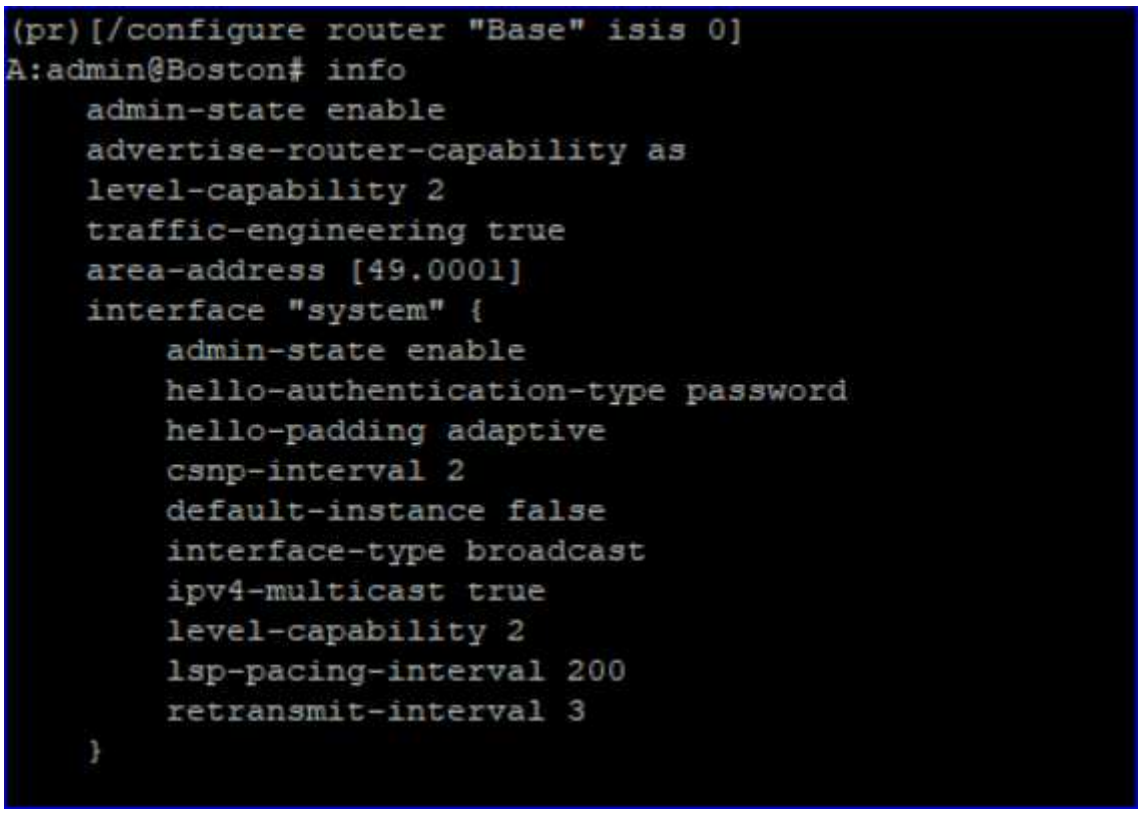


Figure 7-21 NE CLI after deloyment

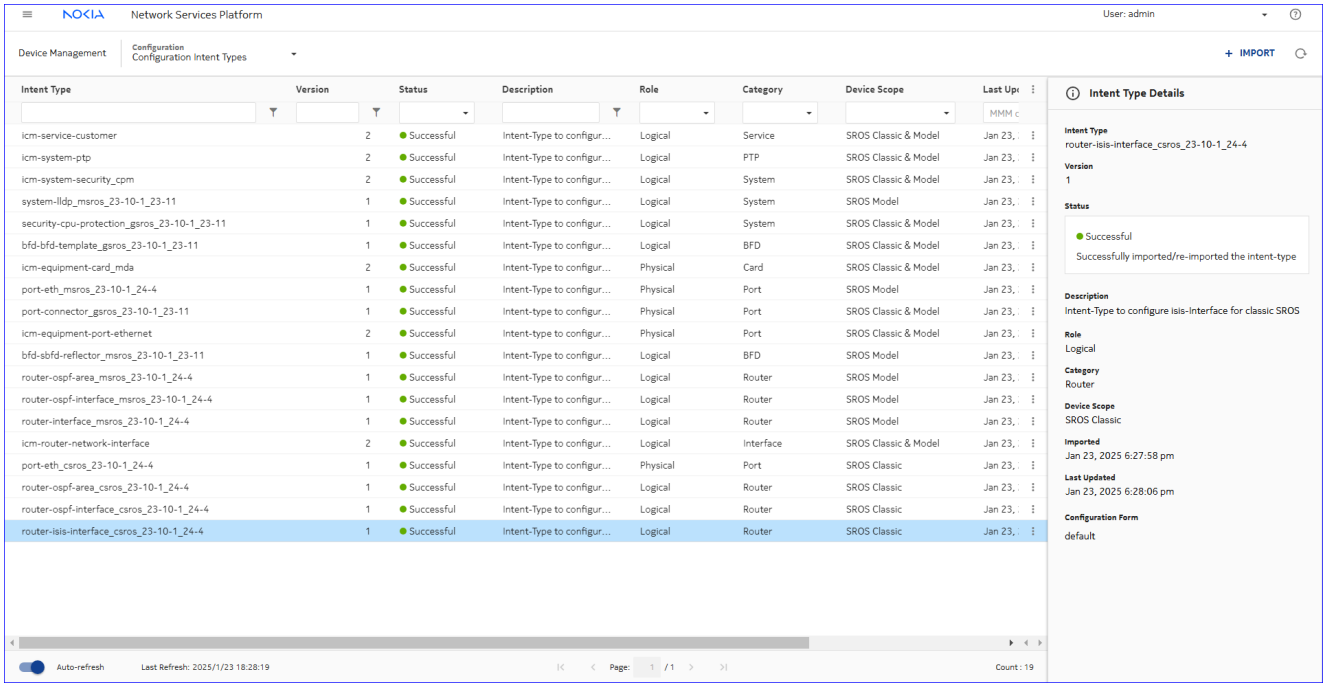


END OF STEPS

7.6.6 To configure ISIS Interface on classic NEs using router-isis-interface-csros intent

1

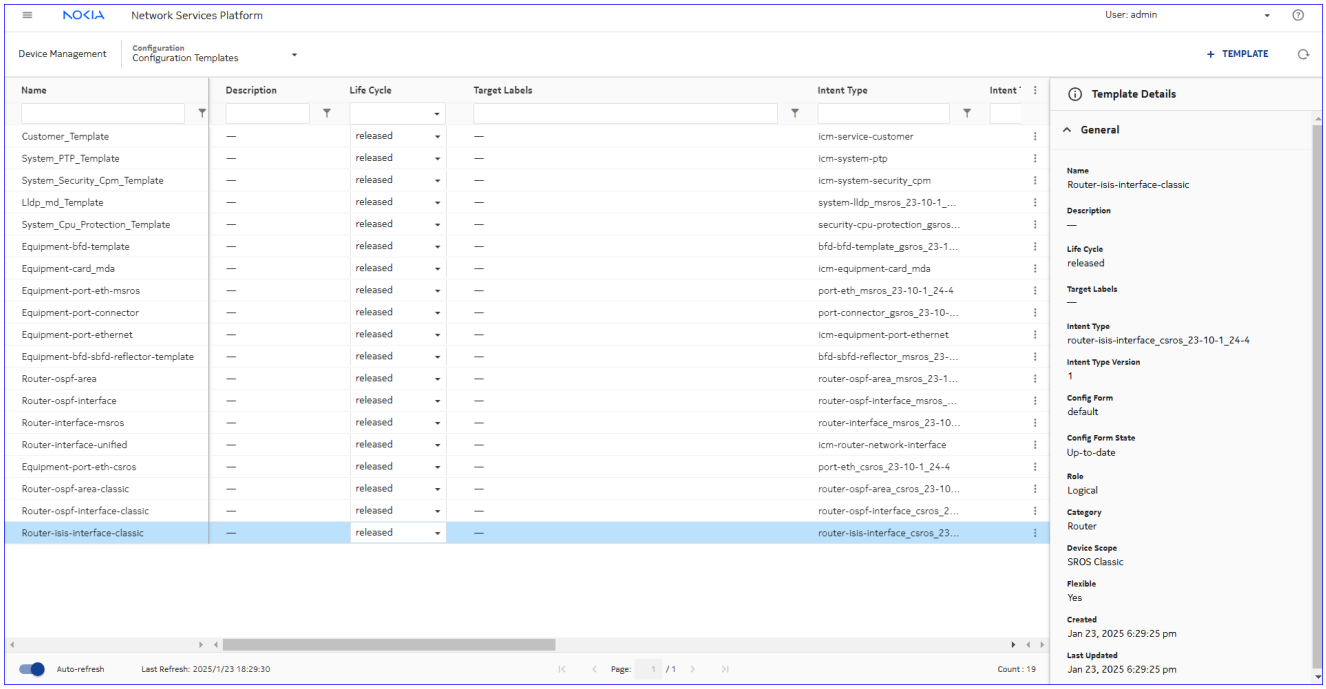
Import the intent type **router-isis-interface_csros_23-10-1_24-4** into **Device Management**, **Configuration Intent Types**.



2

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

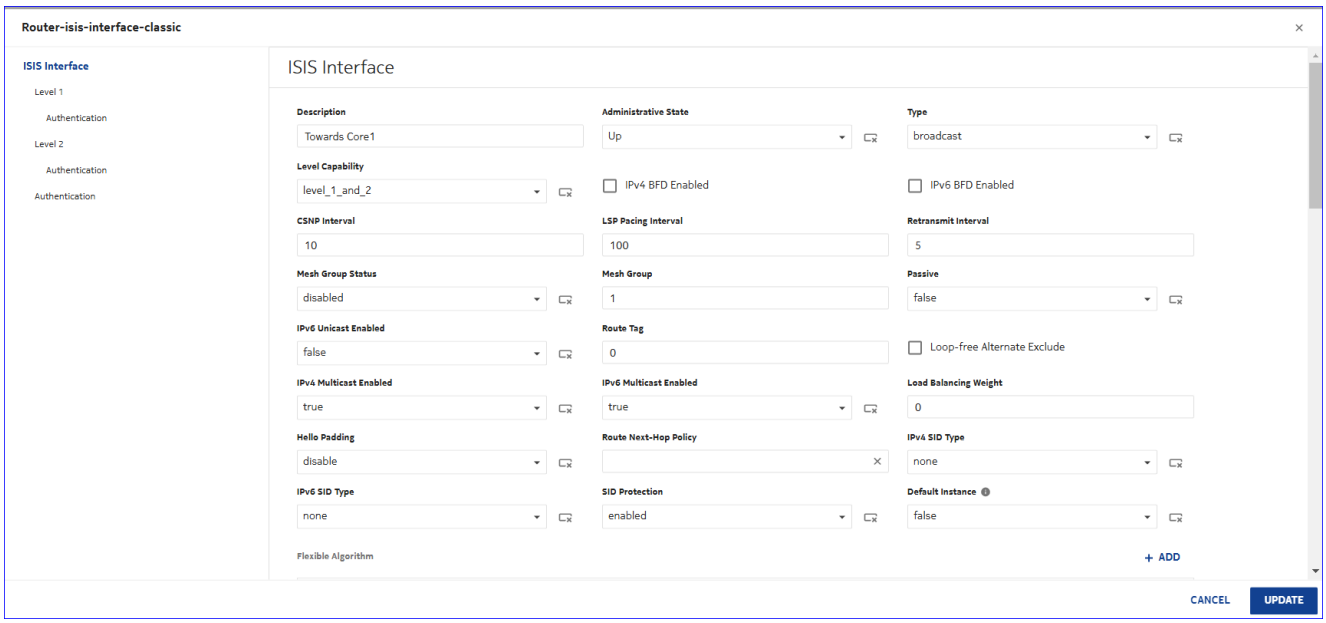
For example, the configuration template created below is named as **Router-isis-interface-classic**.

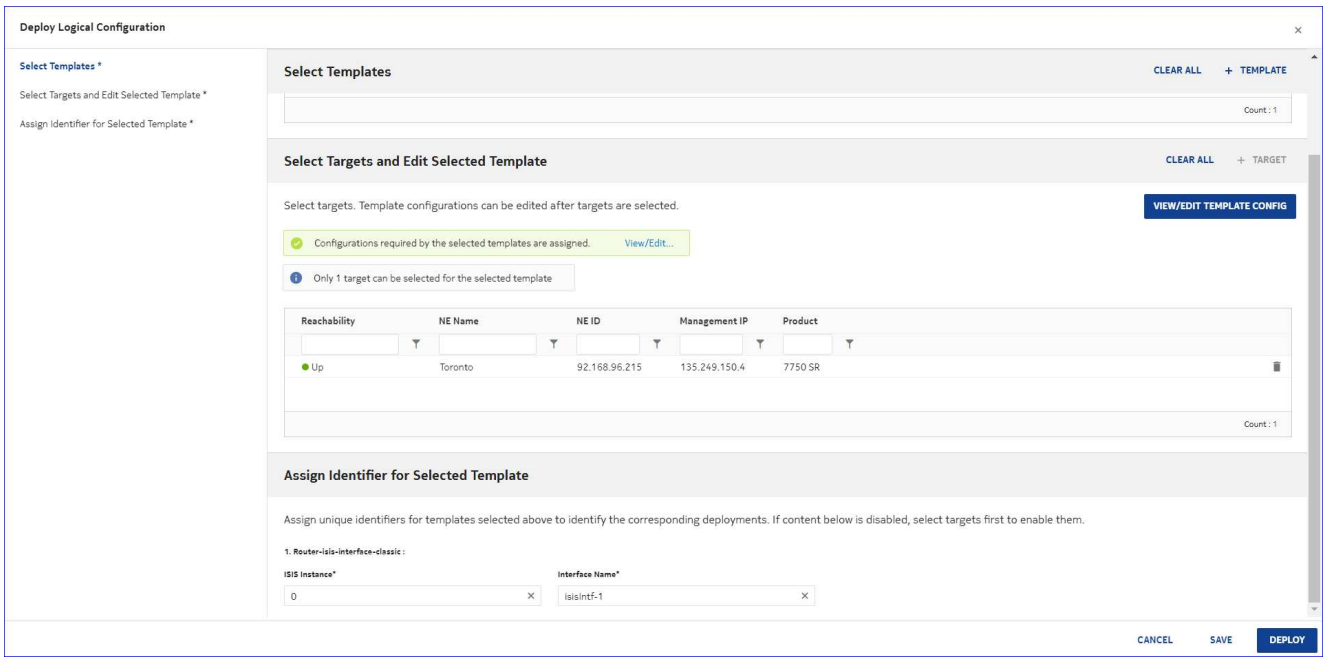


3

Create configuration deployments using the above configuration template.

The following example deploys on 7750 SR-14s classic NE.





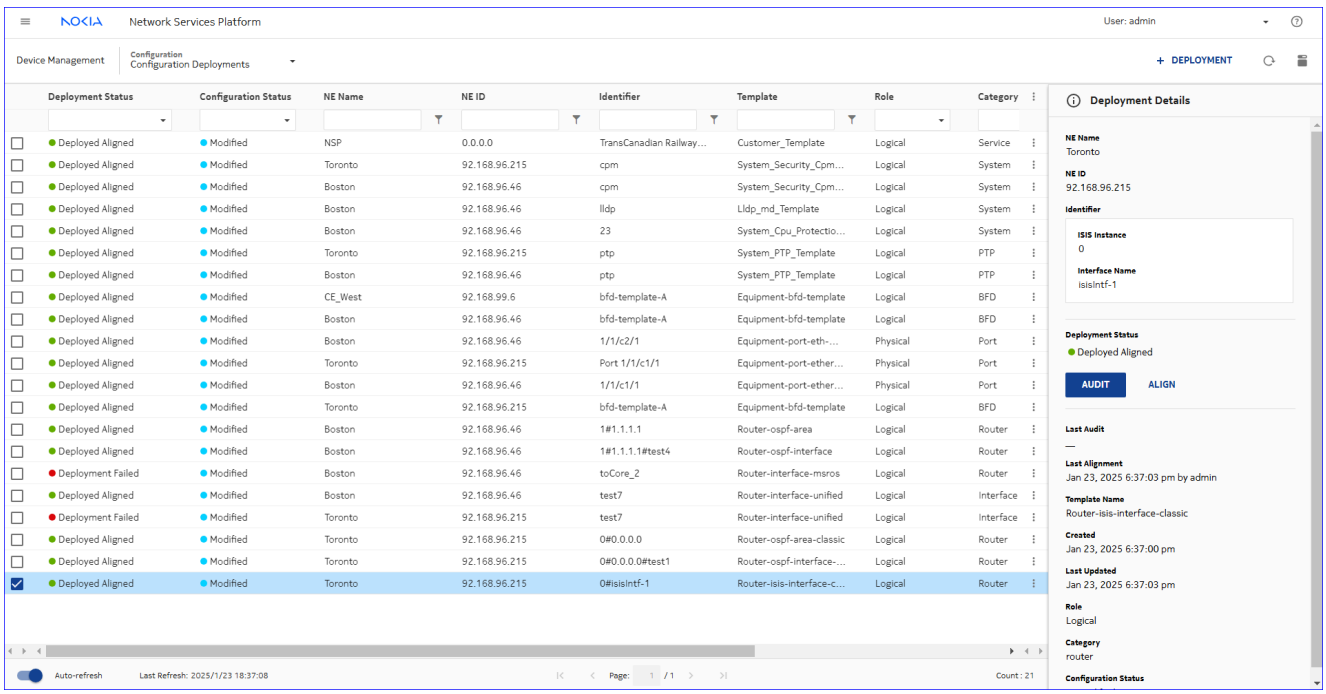


Figure 7-22 NE CLI after deployment

```
A:Toronto>config>router>isis# info
----------------------------------------------
            shutdown
            traffic-engineering
            advertise-router-capability as
            segment-routing
                prefix-sid-range global
                no shutdown
            exit
            interface "system"
                ipv4-node-sid label 20006
                no shutdown
            exit
            interface "isisIntf-1"
                interface-type broadcast
                ipv6-unicast-disable
                no shutdown
            exit
----------------------------------------------
```

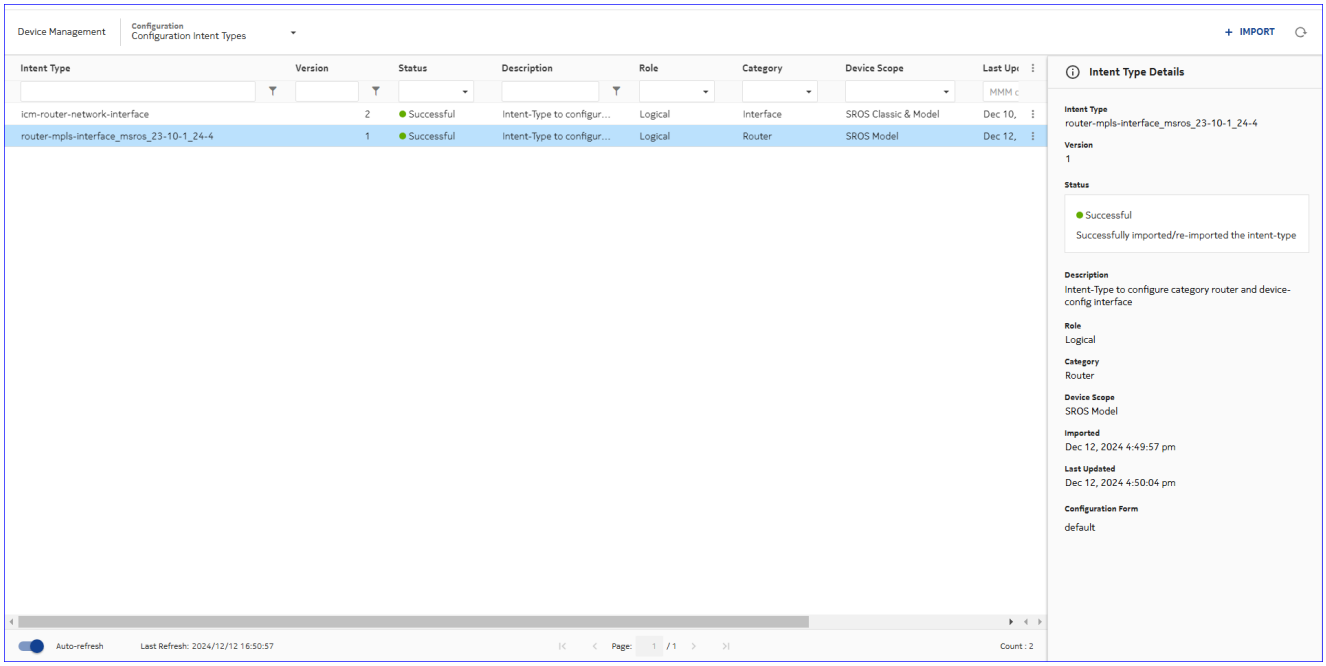
END OF STEPS

7.7 MPLS/RSVP Interfaces

7.7.1 To configure MPLS interface on MD NEs using router-mpls-interface-msros

1

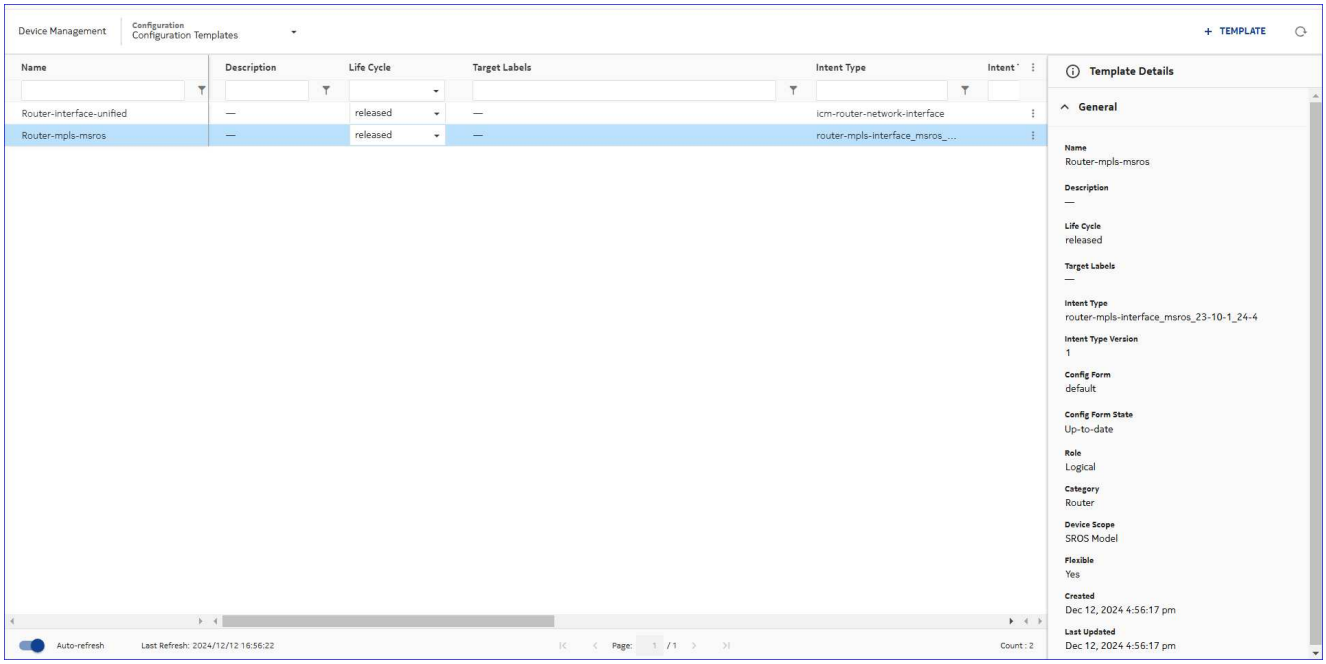
Import the intent type **router-mpls-interface_msros_23-10-1_24-4** into **Device Management**, **Configuration Intent Types**.



2

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

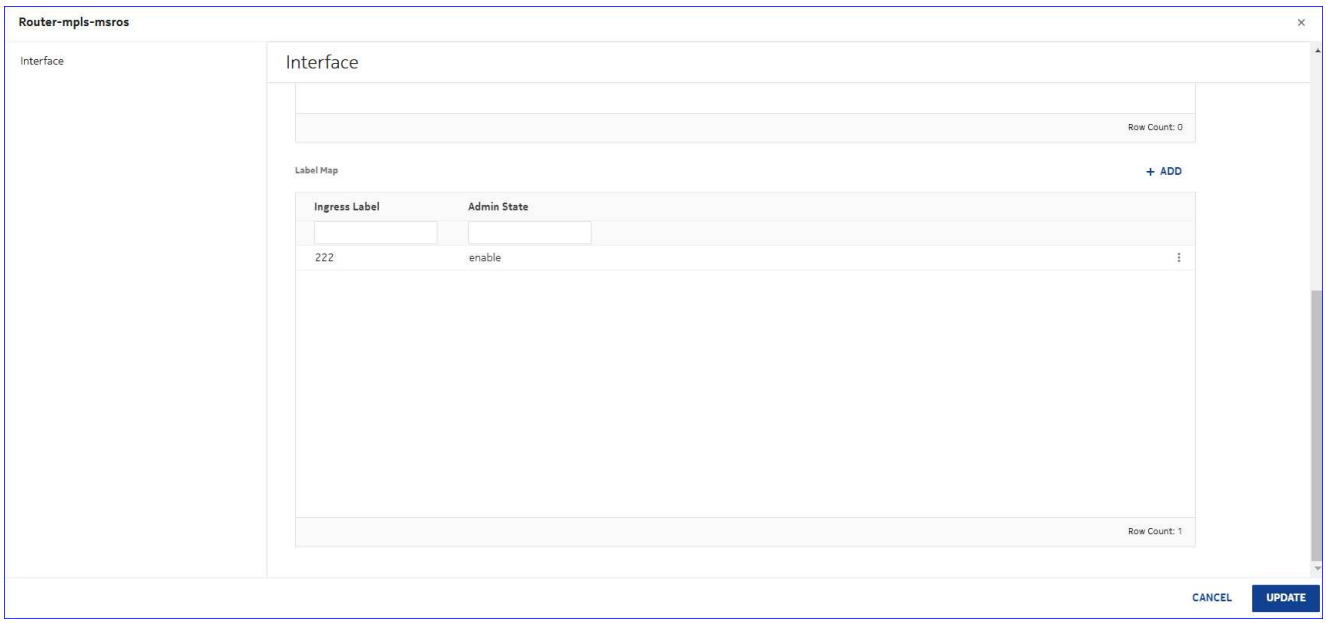
For example, the configuration template created below is named as **Router-mpls-msros**.



3

Create configuration deployments using the above configuration template.

The following example uses 7750 MD.



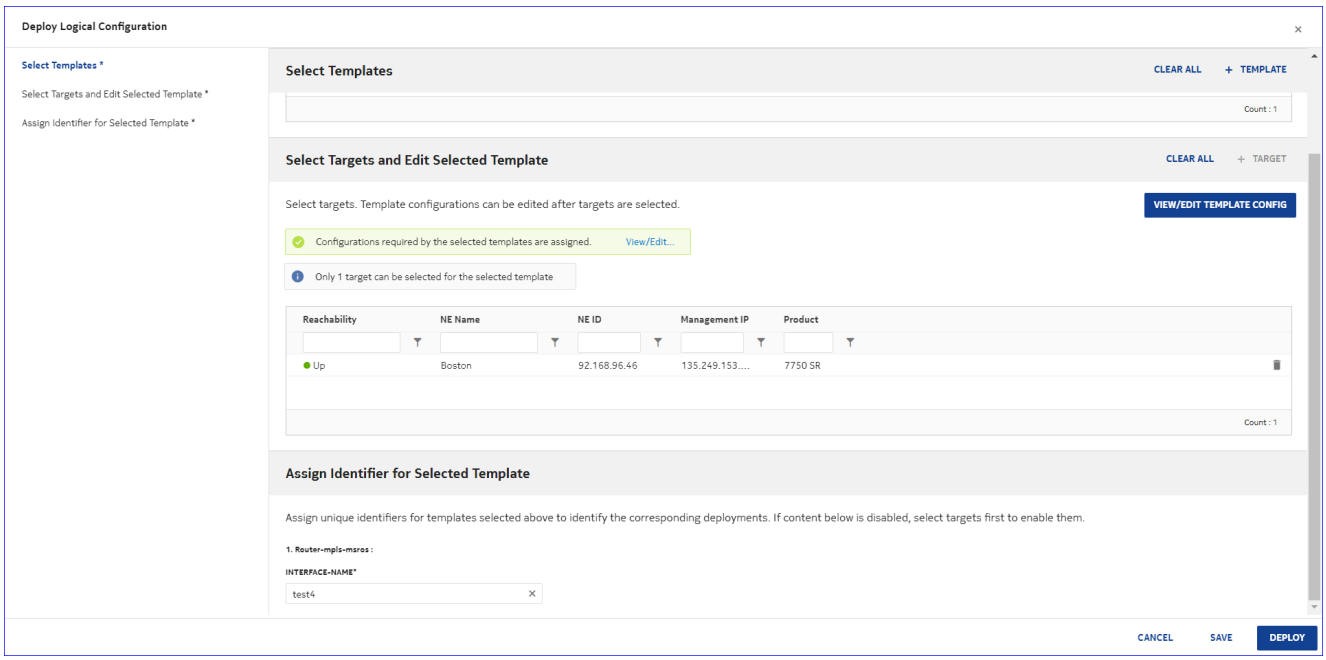
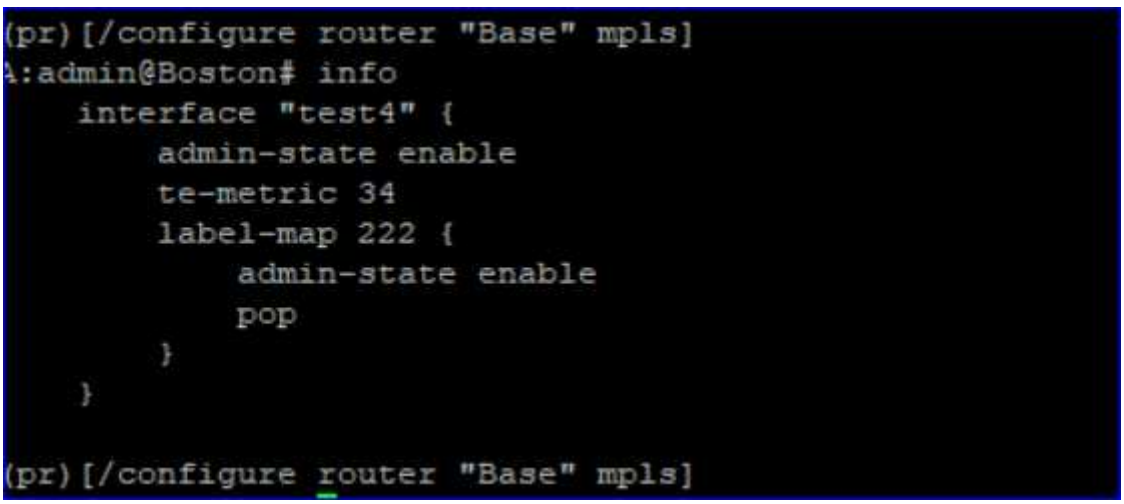


Figure 7-23 NE CLI after deployment



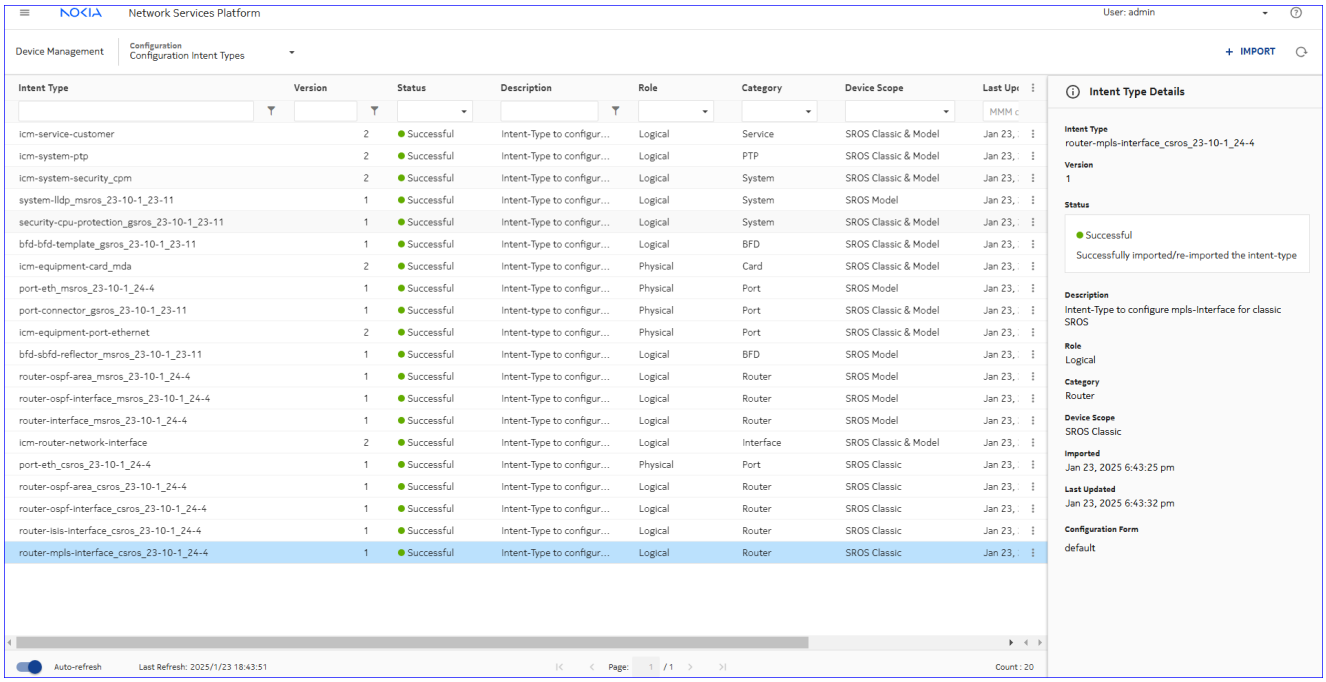
END OF STEPS

7.7.2 To configure MPLS interface on Classic NEs using router-mpls-interface-csros

router-mpls-interface_csros_23-10-1_24-4 intent can be used for MPLS interface configuration on classic NEs.

1

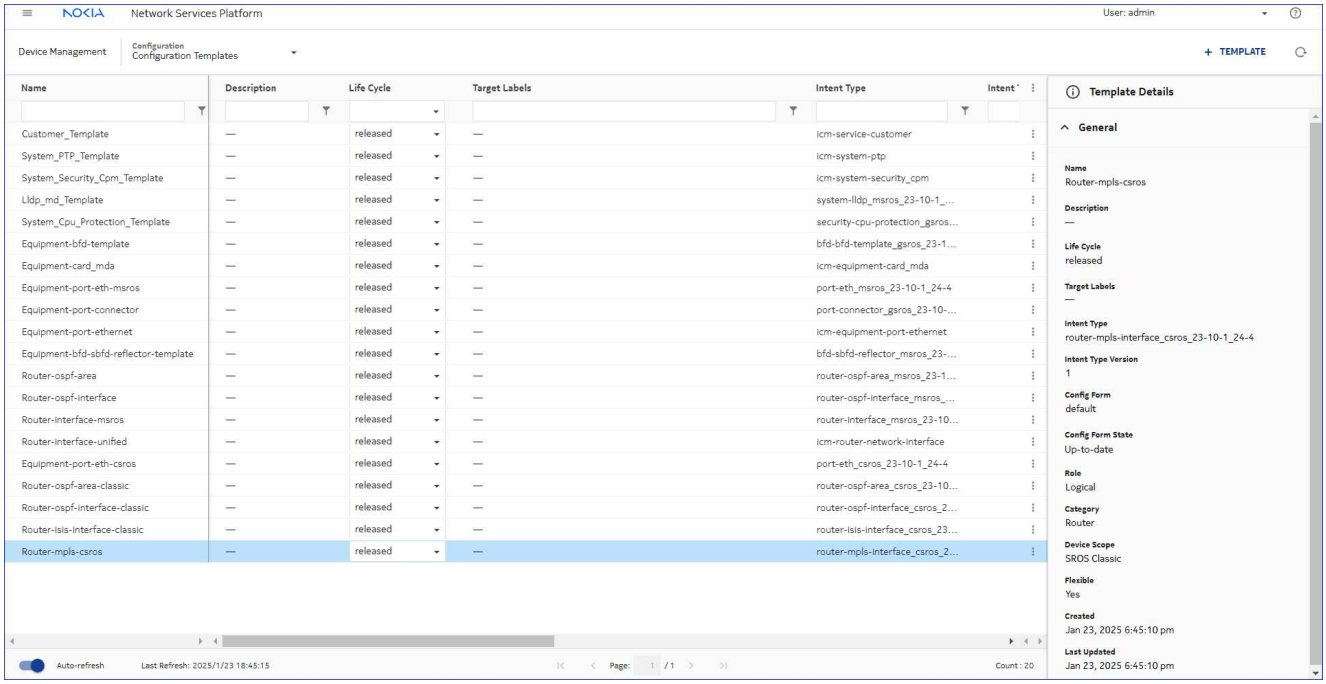
Import the intent type **router-mpls-interface_csros_23-10-1_24-4** into **Device Management**, **Configuration Intent Types**.



2

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

For example, the configuration template created below is named as **Router-mpls-csros**.



3

Create configuration deployments using the above configuration template.

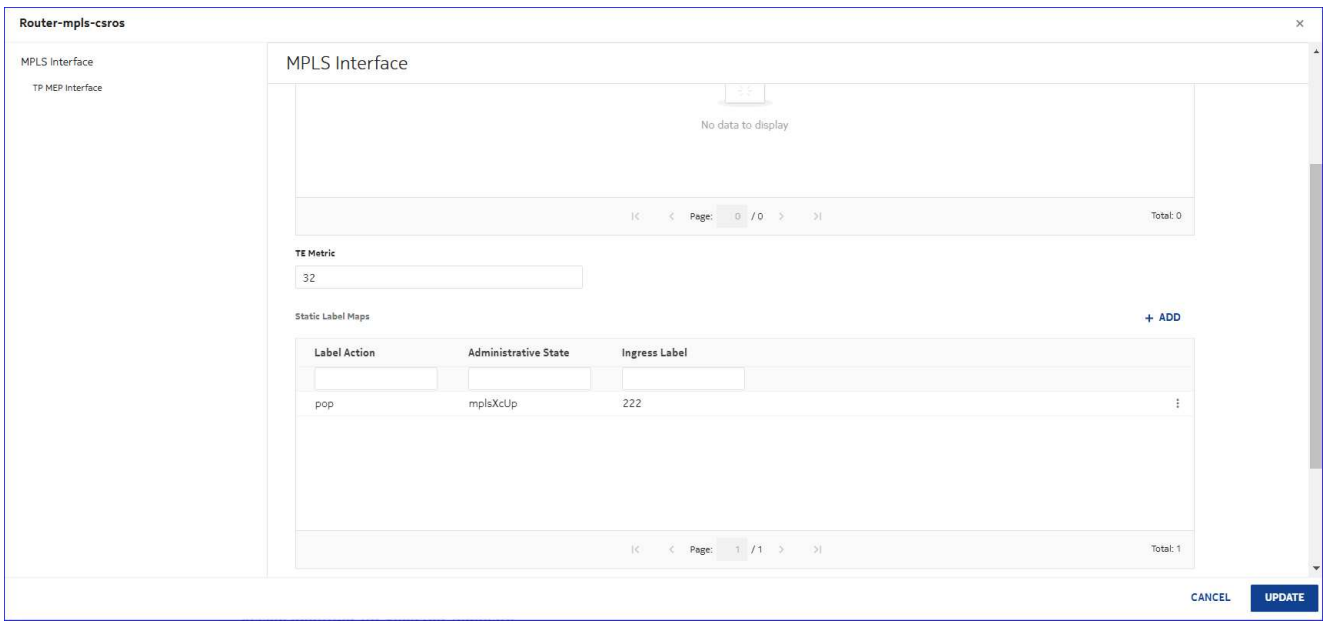


Figure 7-24 NE CLI after deployment

```
A:Toronto>config>router>mpls# info
----------------------------------------------
            interface "system"
                no shutdown
            exit
            interface "test7"
                te-metric 32
                label-map 222
                    pop
                    no shutdown
                exit
                no shutdown
            exit
            no shutdown
----------------------------------------------
```

END OF STEPS

7.7.3 To configure RSVP interface on MD NEs using router-rsvp-interface_msros_23-10-1_24-4

1

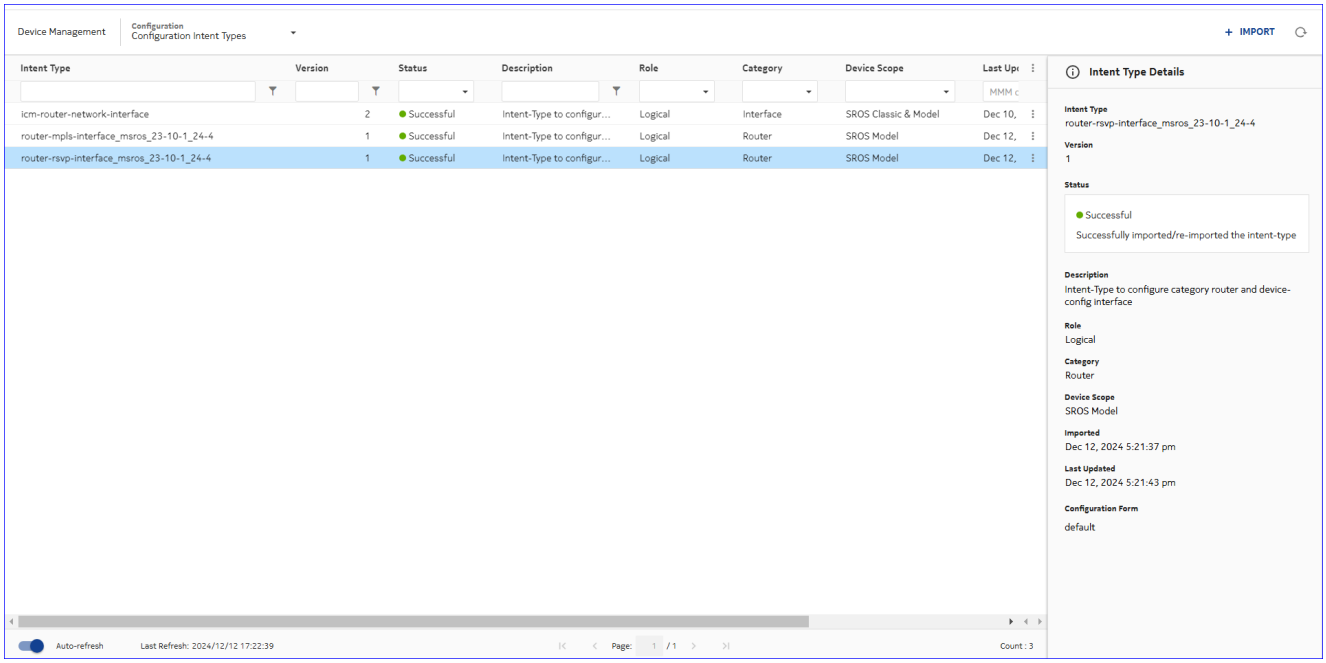
Prerequisites:

- diffserv-te must be enabled:

```
(pr)[/configure router "Base" rsvp diffserv-te]
A:admin@Boston# info
admission-control-model rdm
```

2

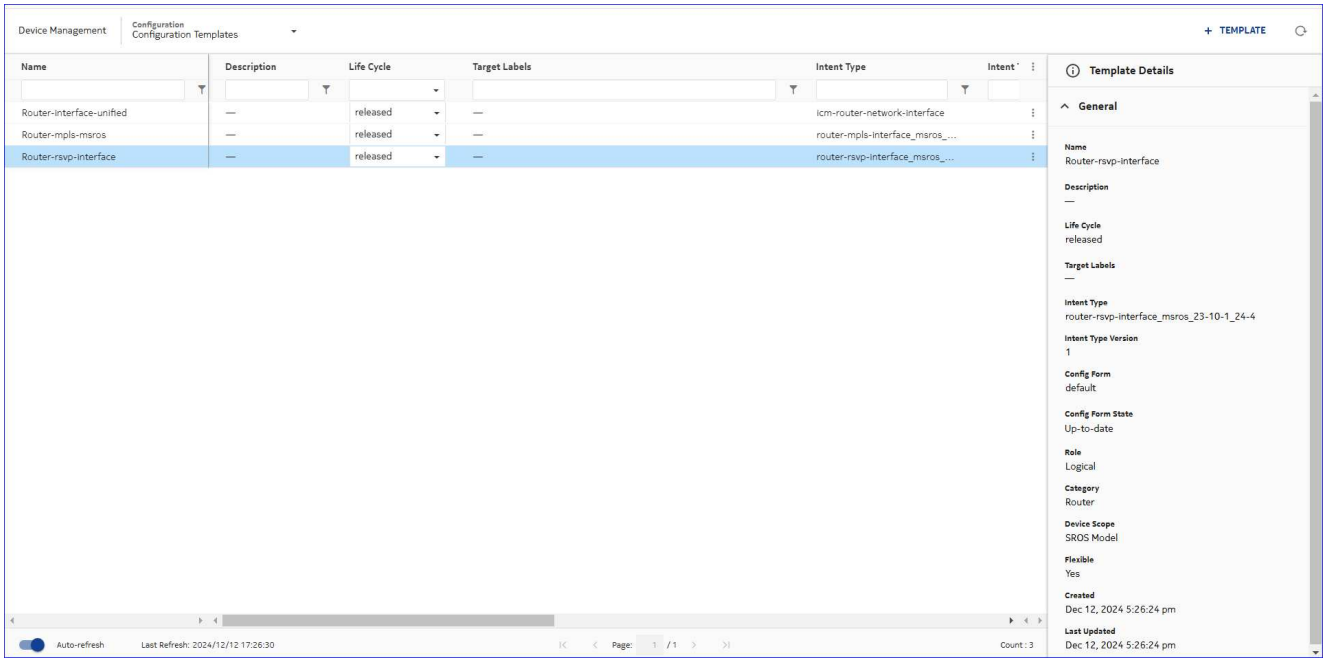
Import the intent type **router-rsvp-interface_msros_23-10-1_24-4** into **Device Management**, **Configuration Intent Types**.



3

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

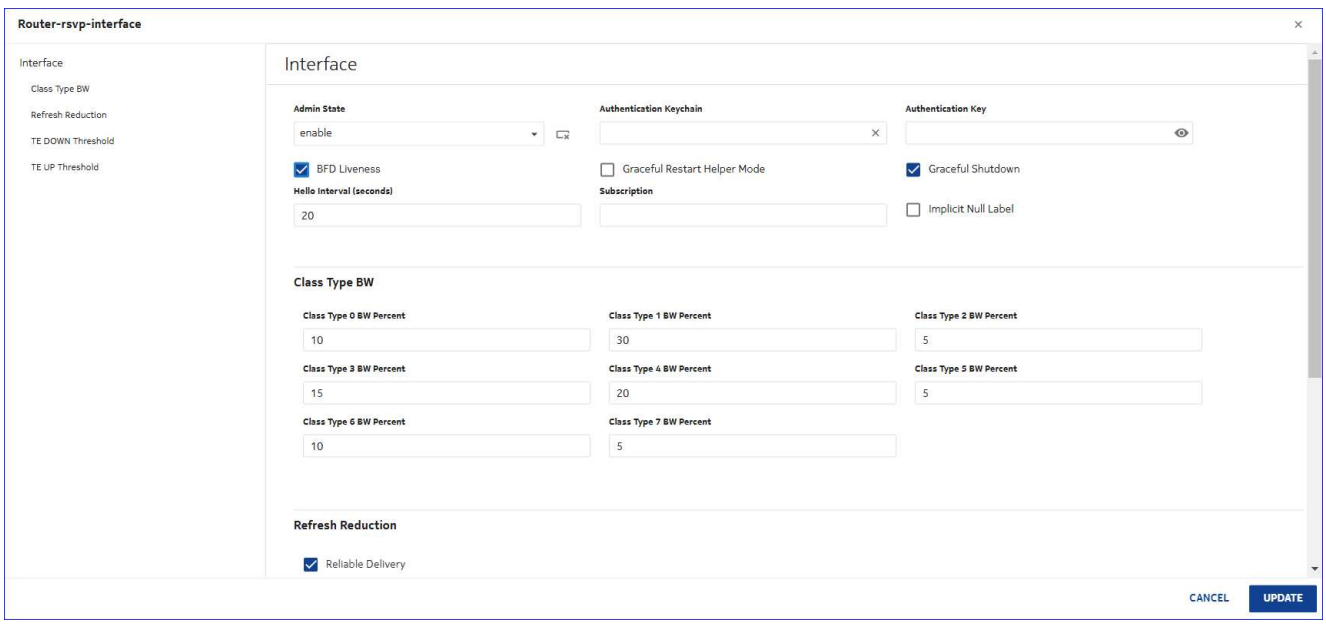
For example, the configuration template created below is named as **Router-rsvp-interface**.



4

Create configuration deployments using the above configuration template.

The following example uses 7750 MD.



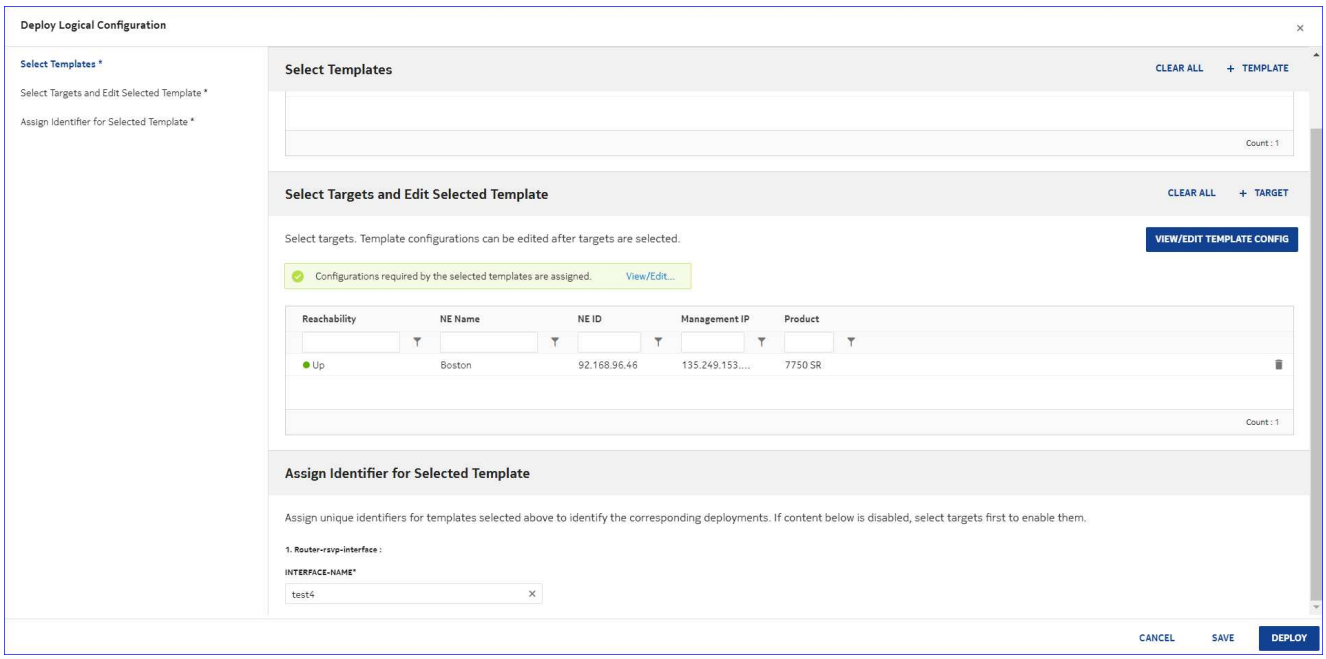


Figure 7-25 NE CLI after deployment

```
A:admin@Boston# info
    diffserv-te {
        admission-control-model rdm
    }
    interface "test4" {
        admin-state enable
        bfd-liveness true
        graceful-shutdown true
        hello-interval 20
        class-type-bw {
            ct0 10
            ct1 30
            ct2 5
            ct3 15
            ct4 20
            ct5 5
            ct6 10
            ct7 5
        }
        refresh-reduction {
            reliable-delivery true
        }
    }

(pr)[/configure router "Base" rsvp]
```

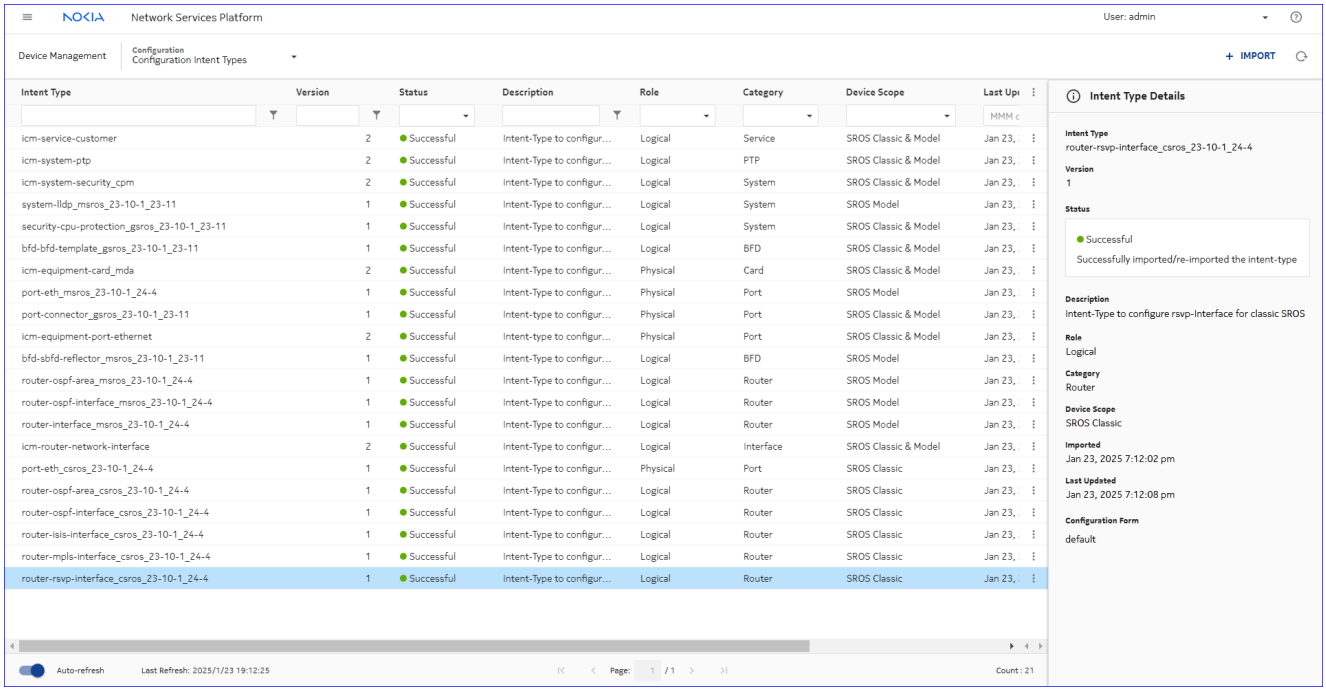
END OF STEPS

7.7.4 To configure RSVP interface on Classic NEs using router-rsvp-interface_ msros_23-10-1_24-4

router-rsvp-interface_csros_23-10-1_24-4 intent can used for the configuration of RSVP on classic NEs.

1

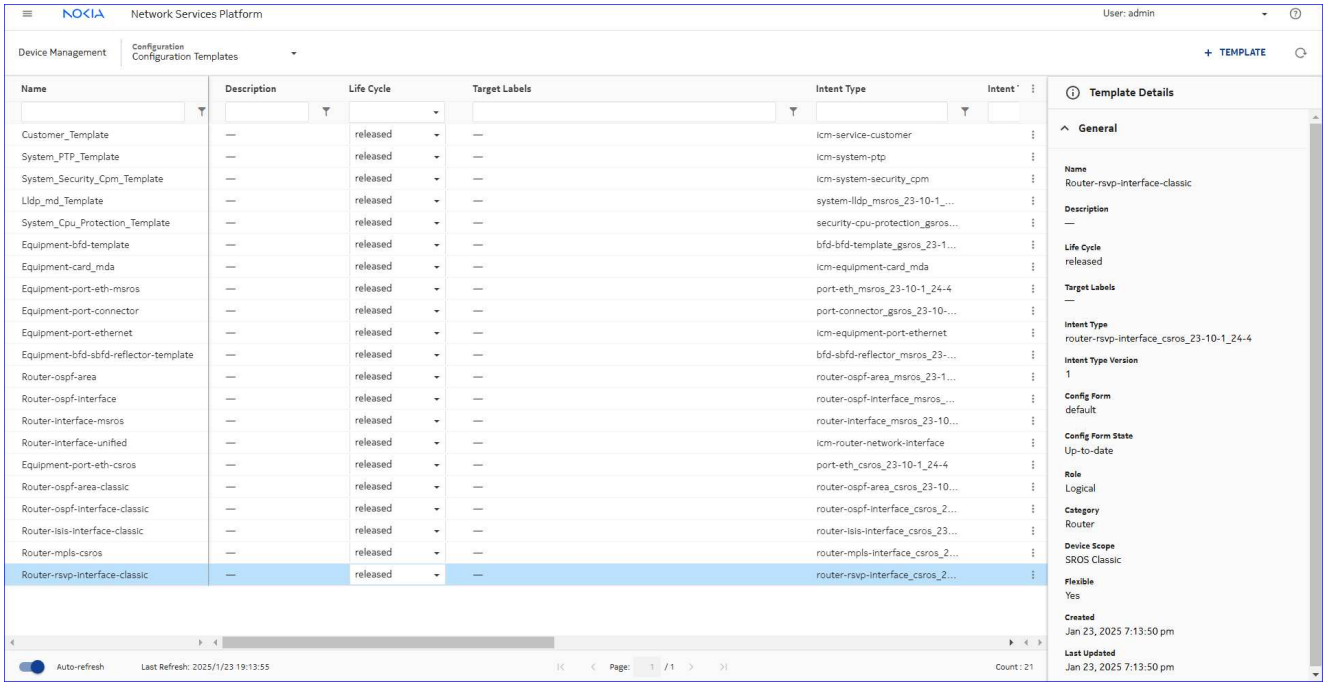
Import the intent type **router-rsvp-interface_csros_23-10-1_24-4** into **Device Management**, **Configuration Intent Types**.



2

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

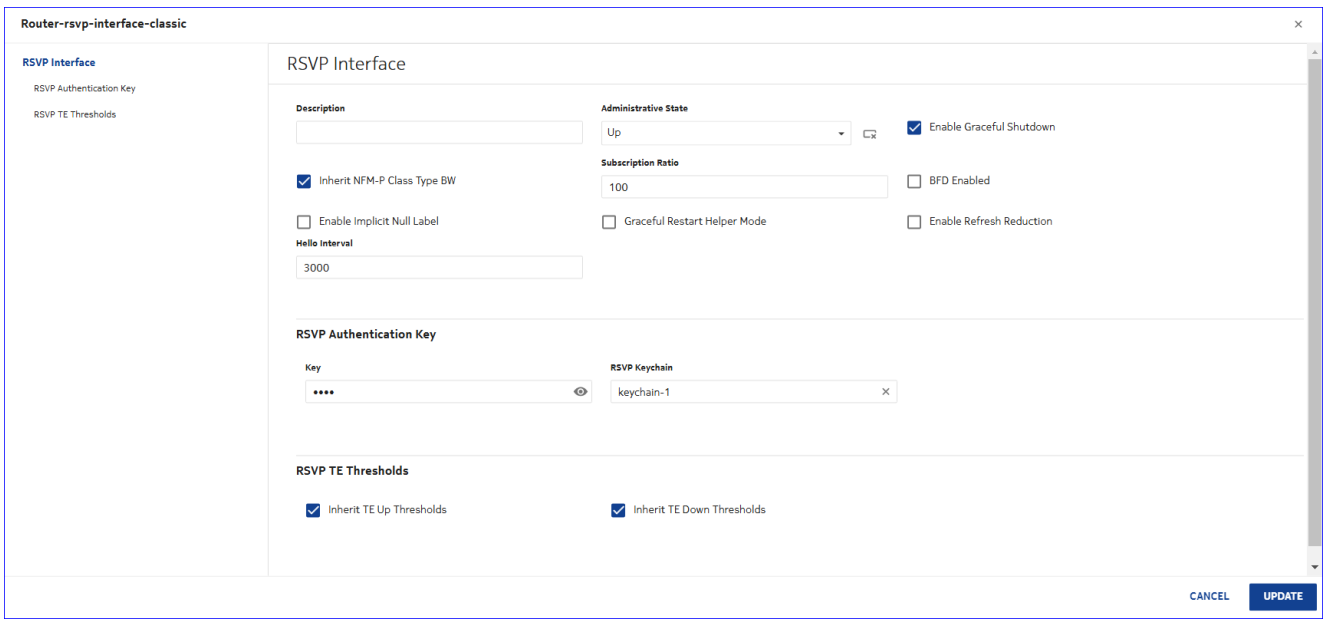
For example, the configuration template created below is named as **Router-rsvp-interface-classic**.

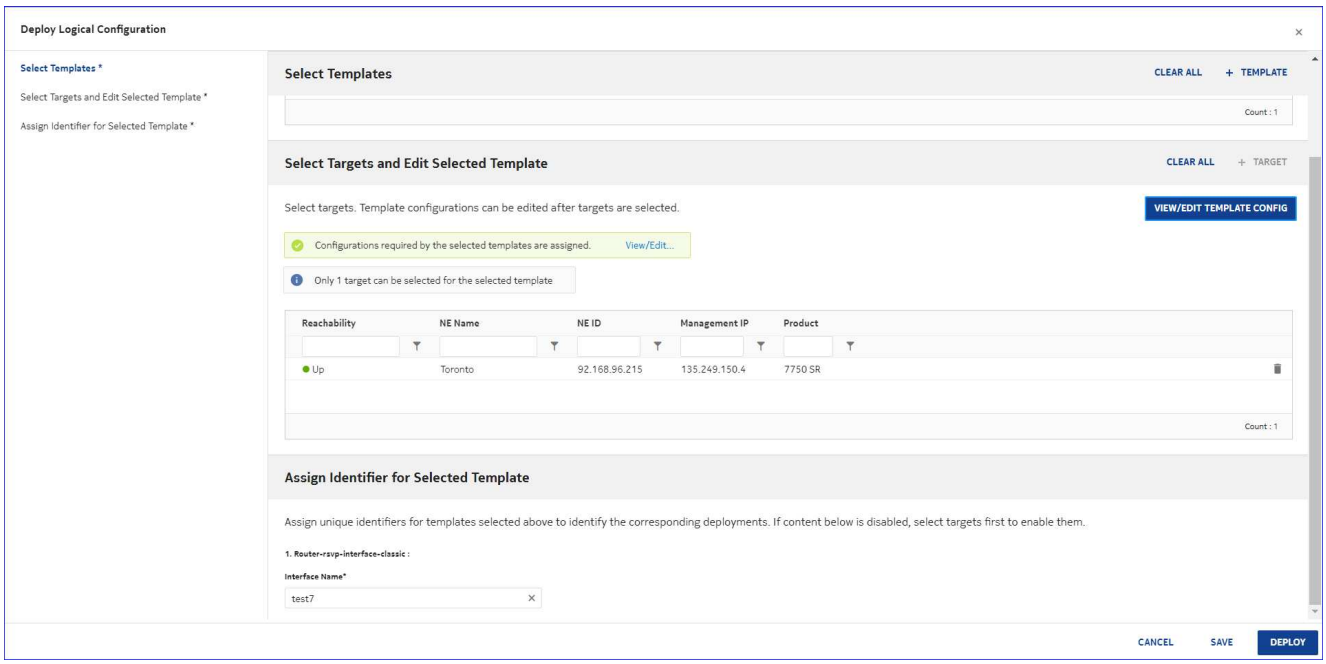


3

Create configuration deployments using the above configuration template.

The following example uses 7750 MD.





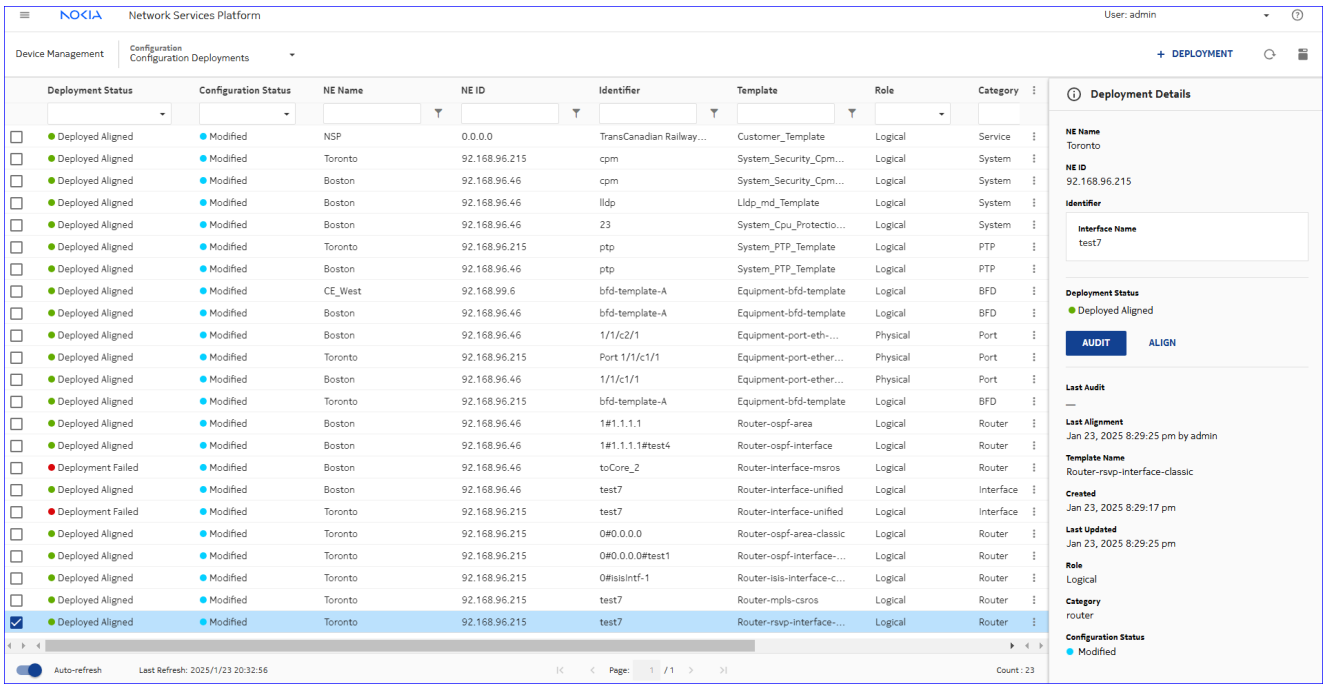


Figure 7-26 NE CLI after deployment

```
A:Toronto>config>router>rsvp# info
----------------------------------------------
            shutdown
            diffserv-te mam
            exit
            interface "system"
                no shutdown
            exit
            interface "test7"
                authentication-key "iNQmb9TmM40TuEX88olXneVBF8k=" hash2
                auth-keychain "keychain-1"
                graceful-shutdown
                no shutdown
            exit
----------------------------------------------
```

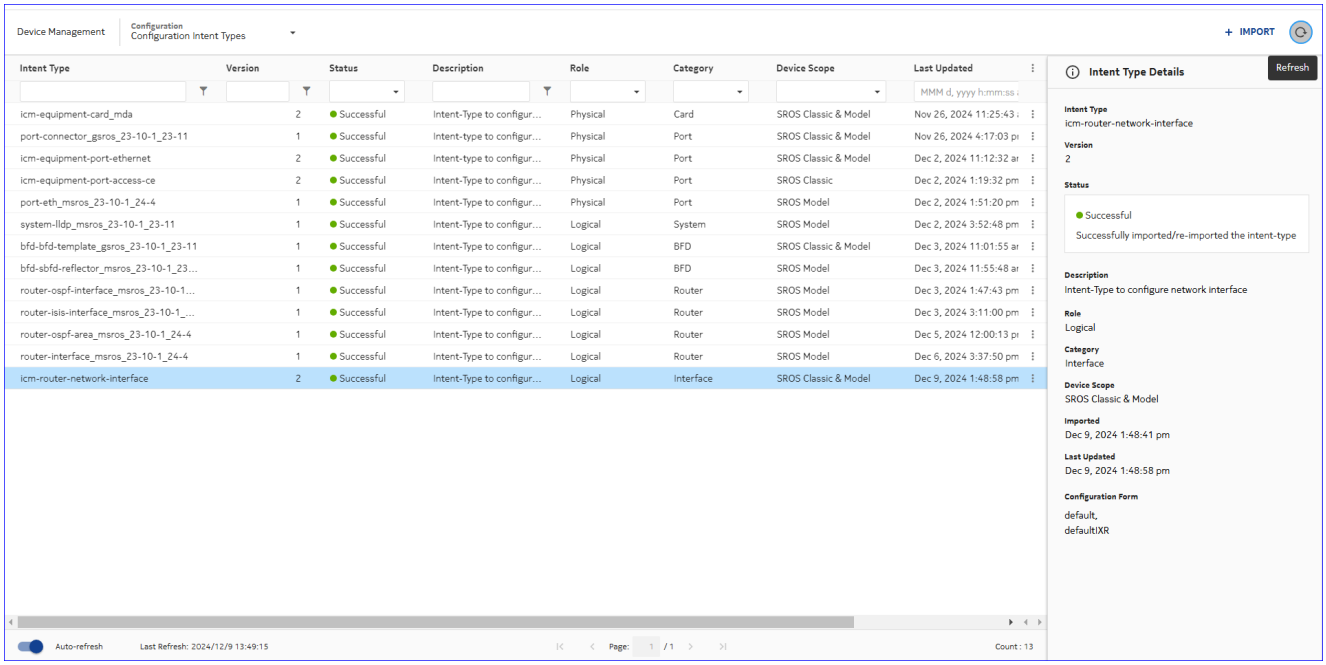
END OF STEPS

7.8 Interfaces

7.8.1 To configure router interface with icm-router-network-interface intent

1

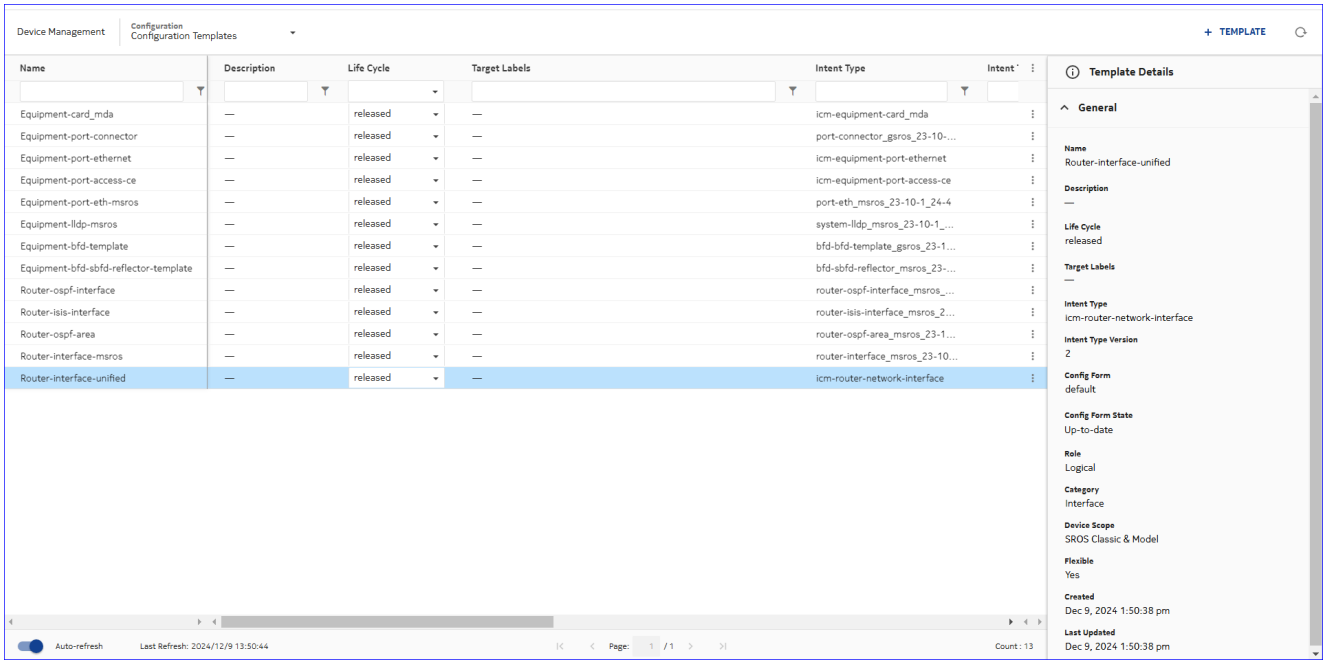
Import the intent type **icm-router-network-interface** into **Device Management**, **Configuration Intent Types**.



2

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

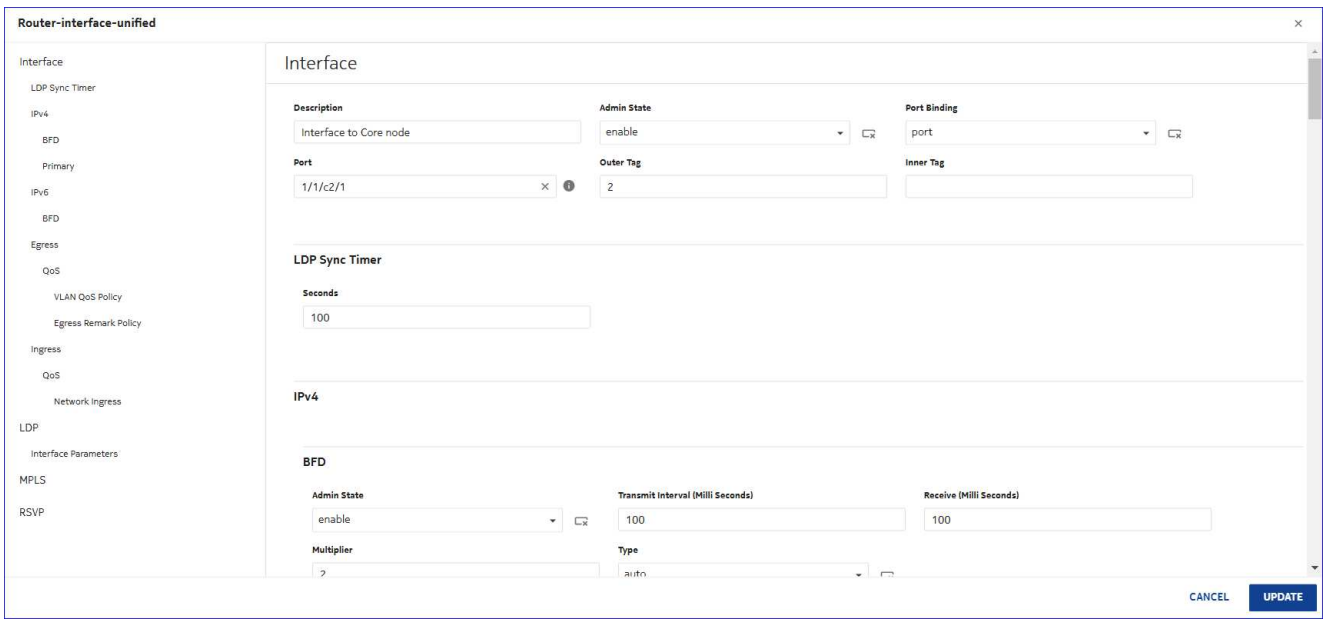
For example, the configuration template created below is named as **Router-interface-unified**.

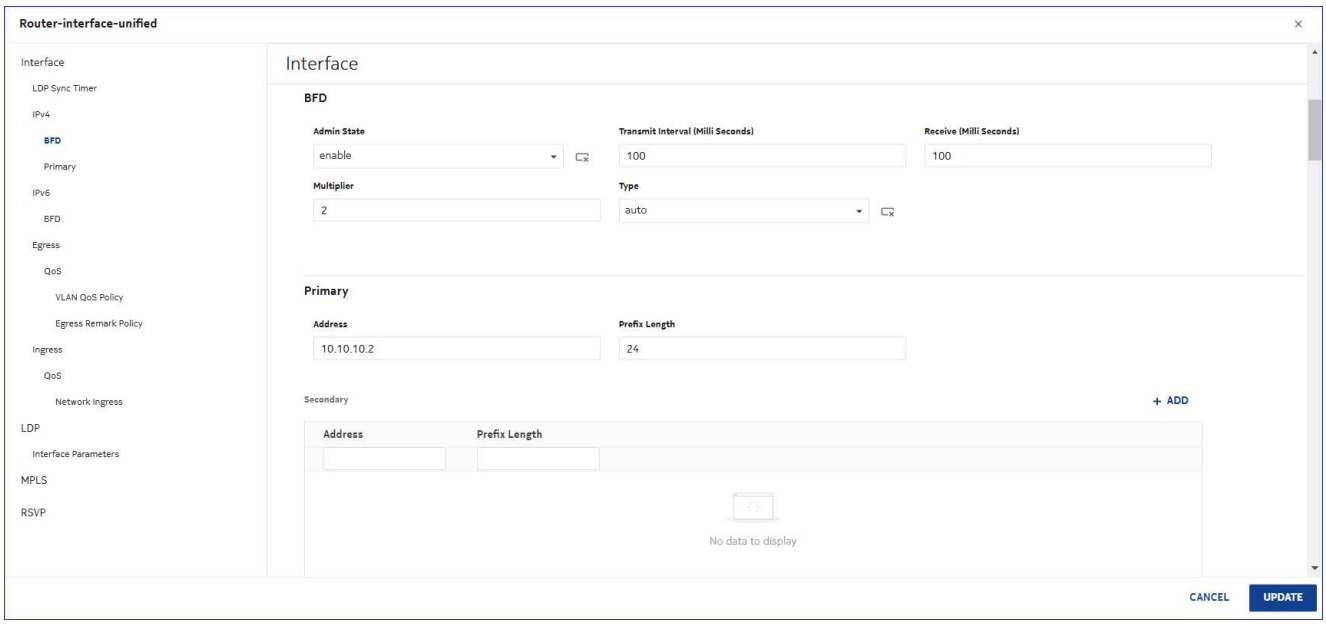


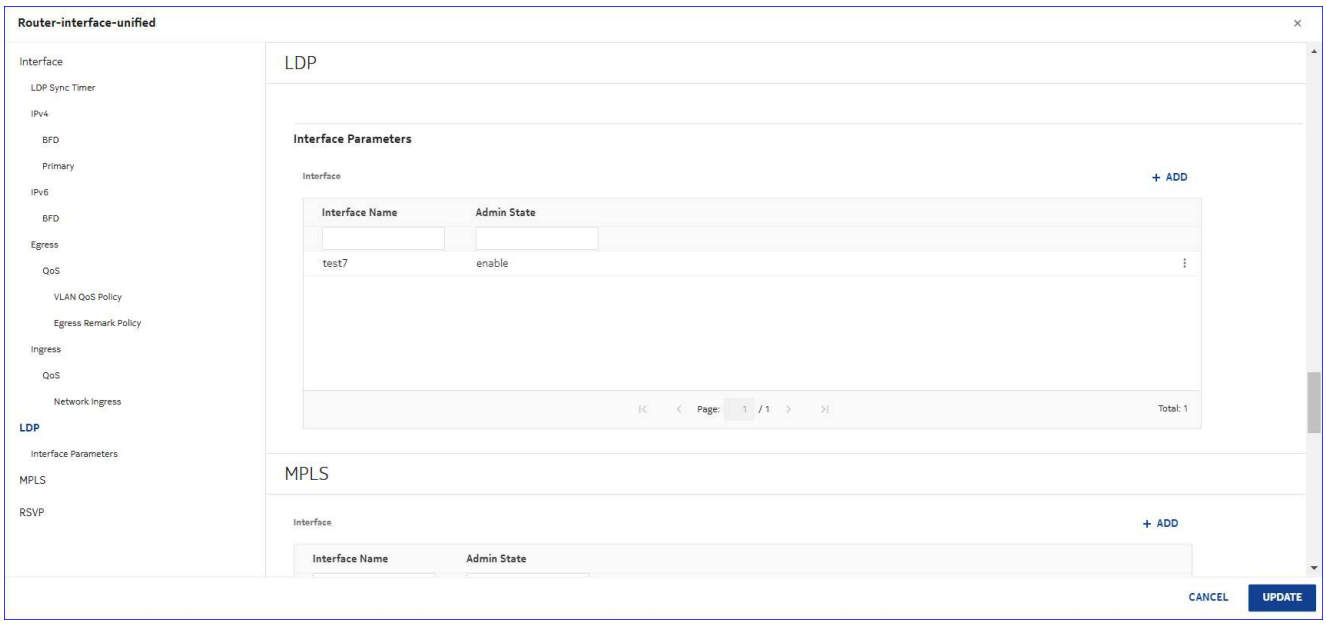
3

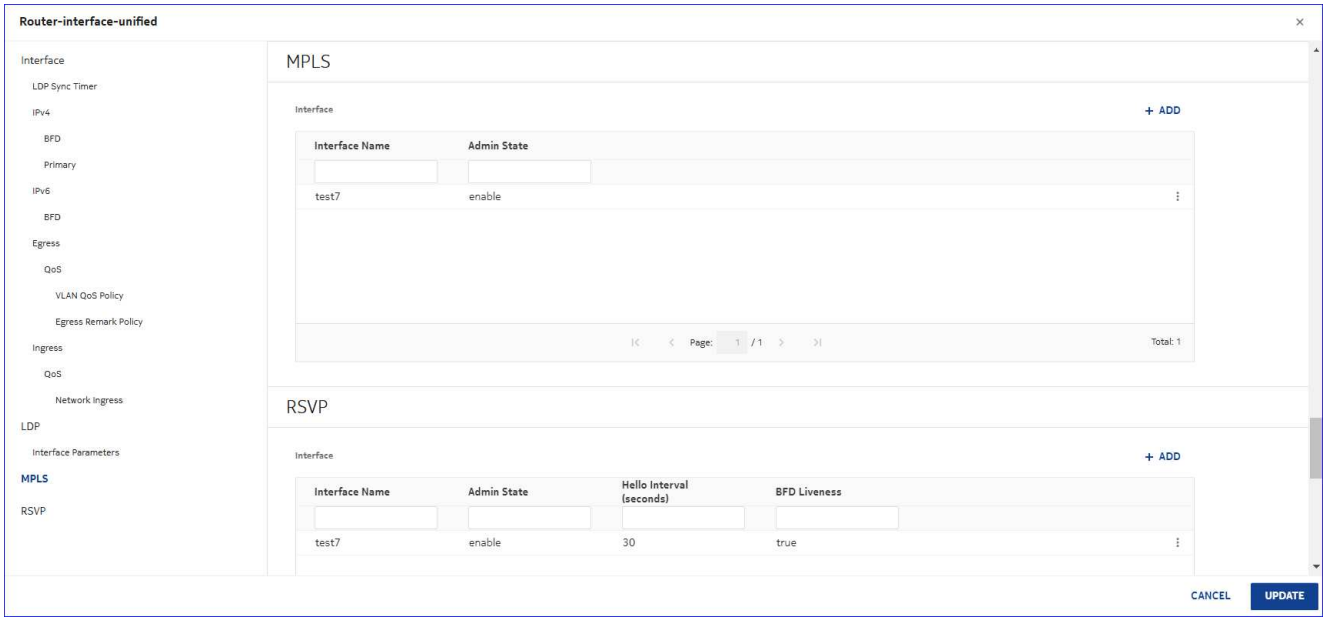
Create configuration deployments using the above configuration template.

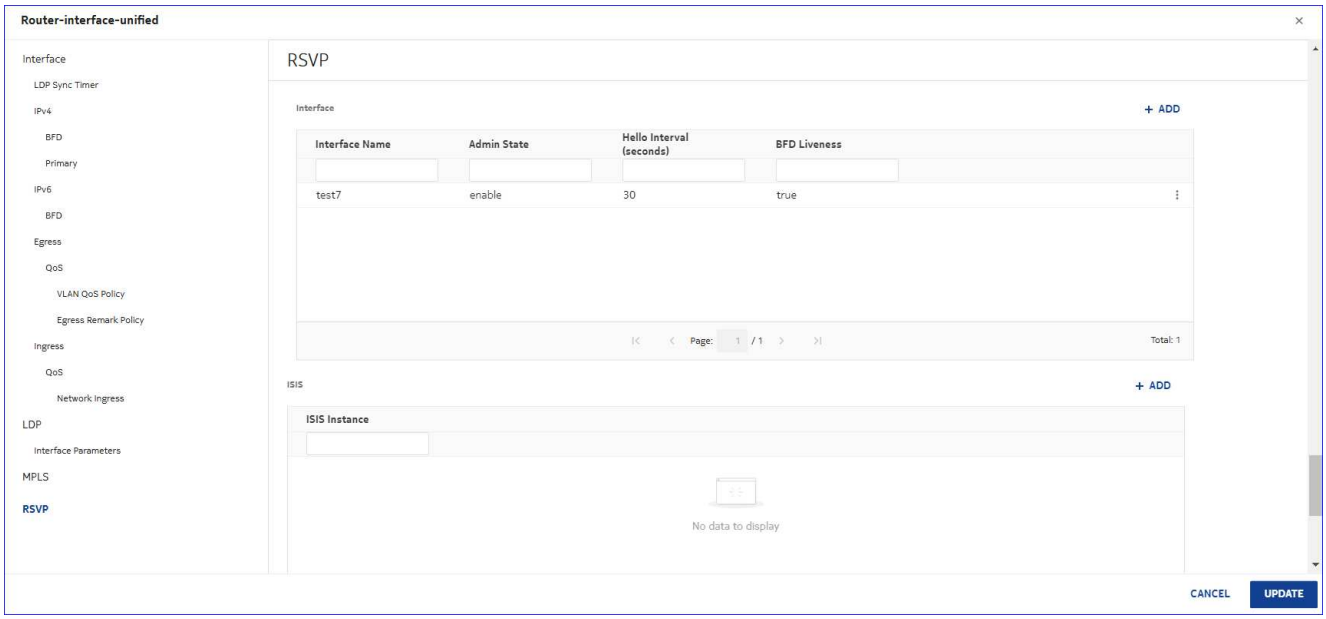
Example 1: 7750 SR-14s MD

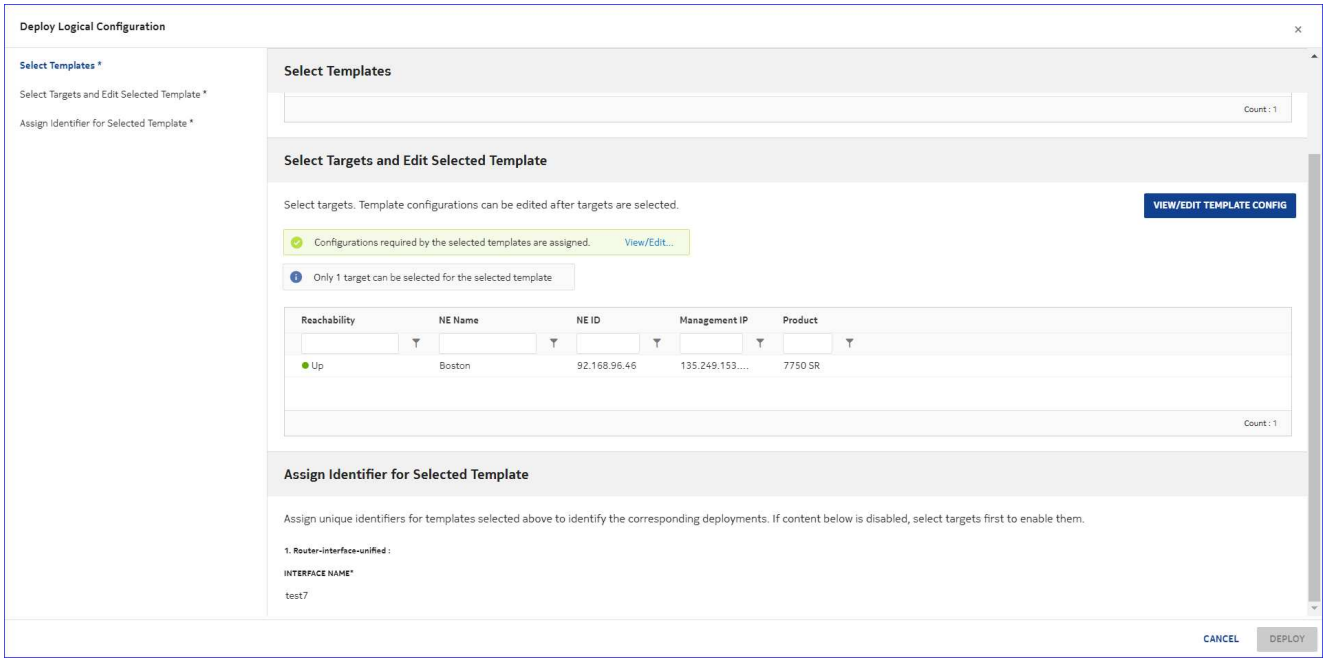












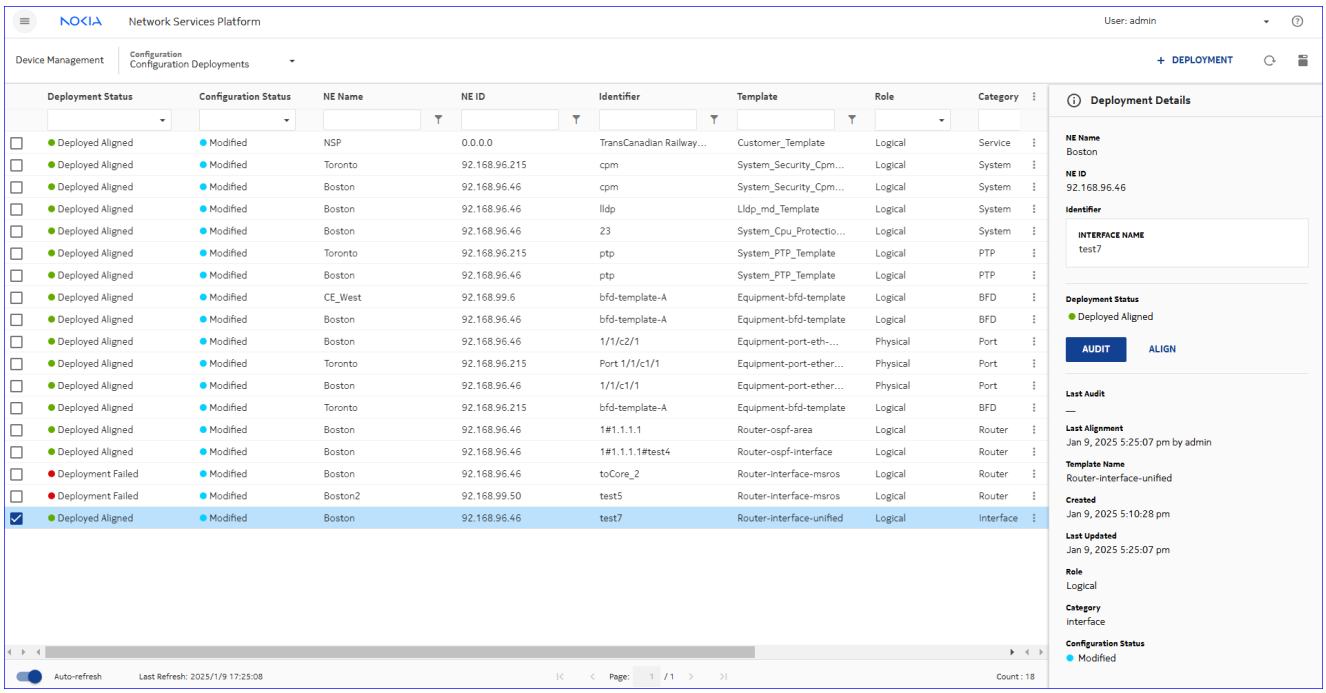
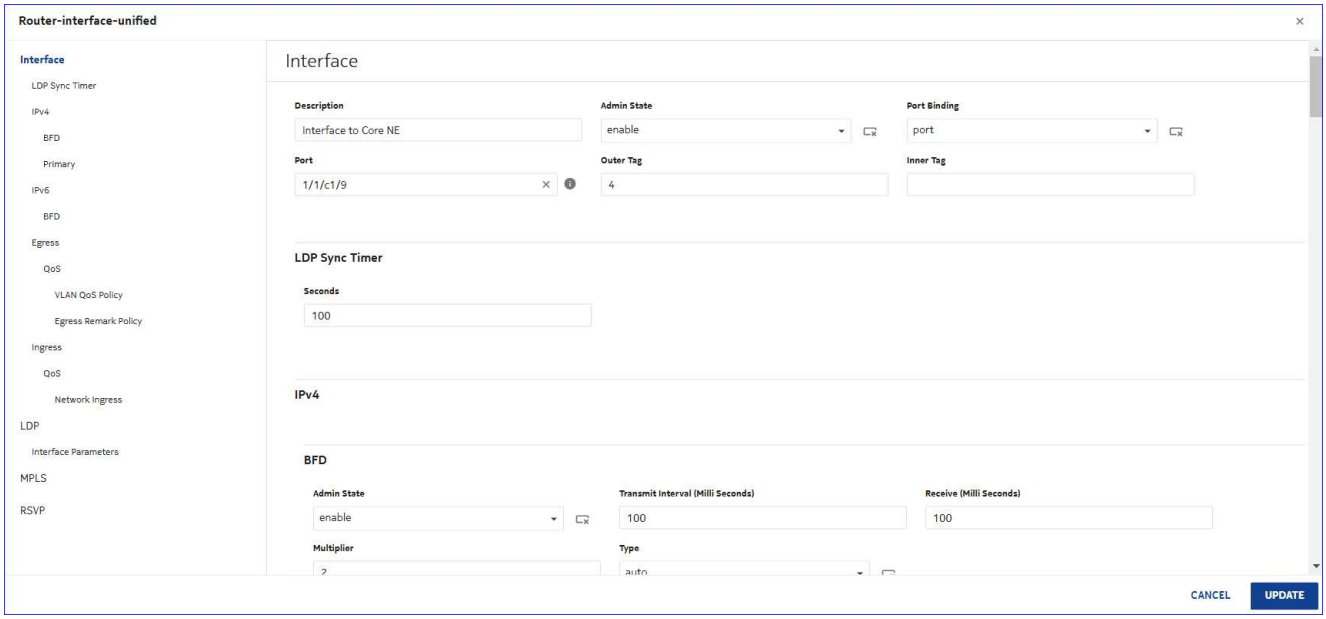
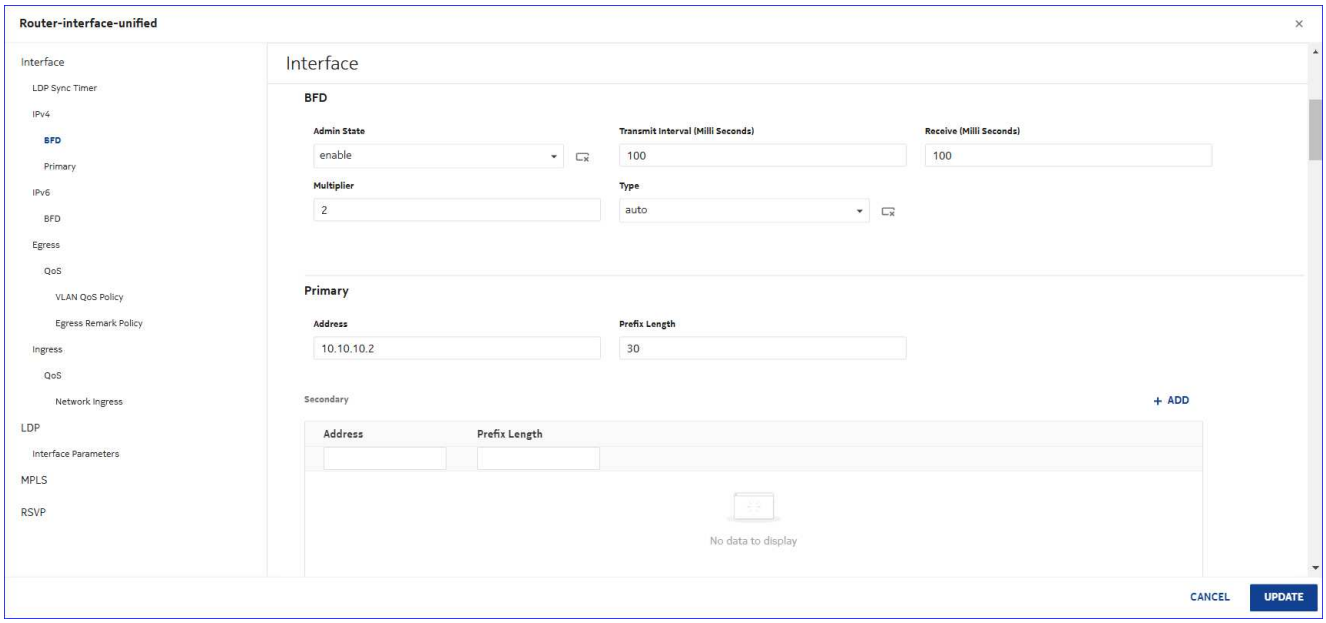


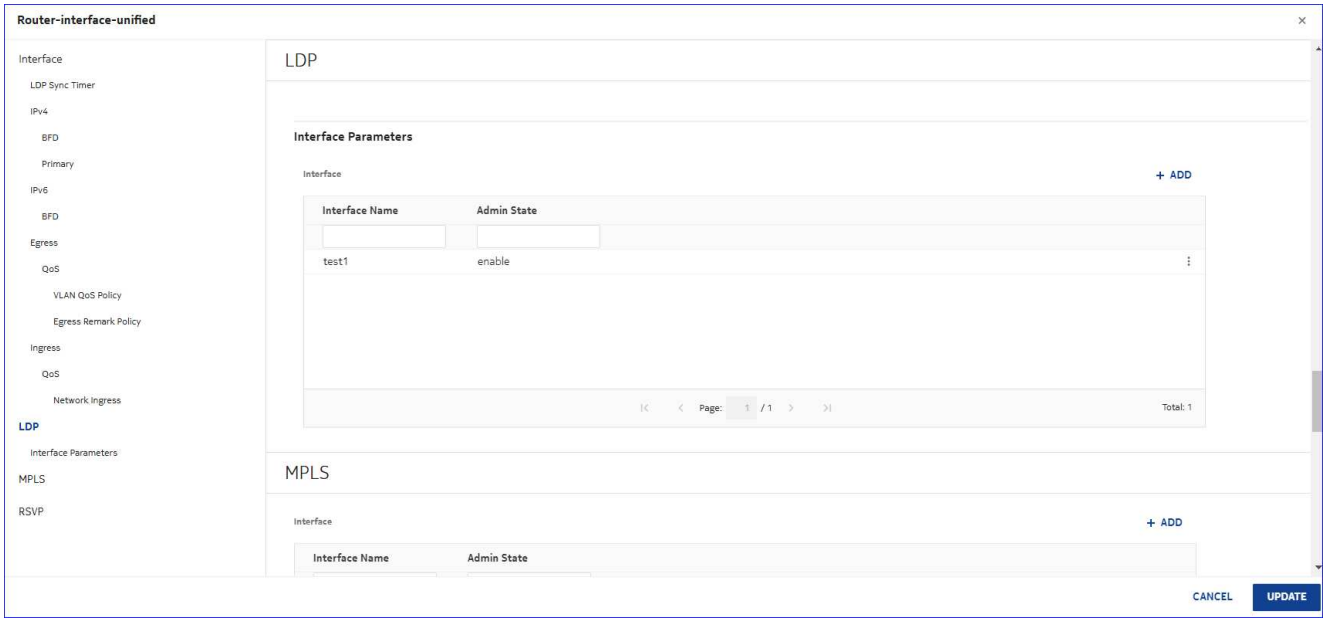
Figure 7-27 NE CLI after deployment

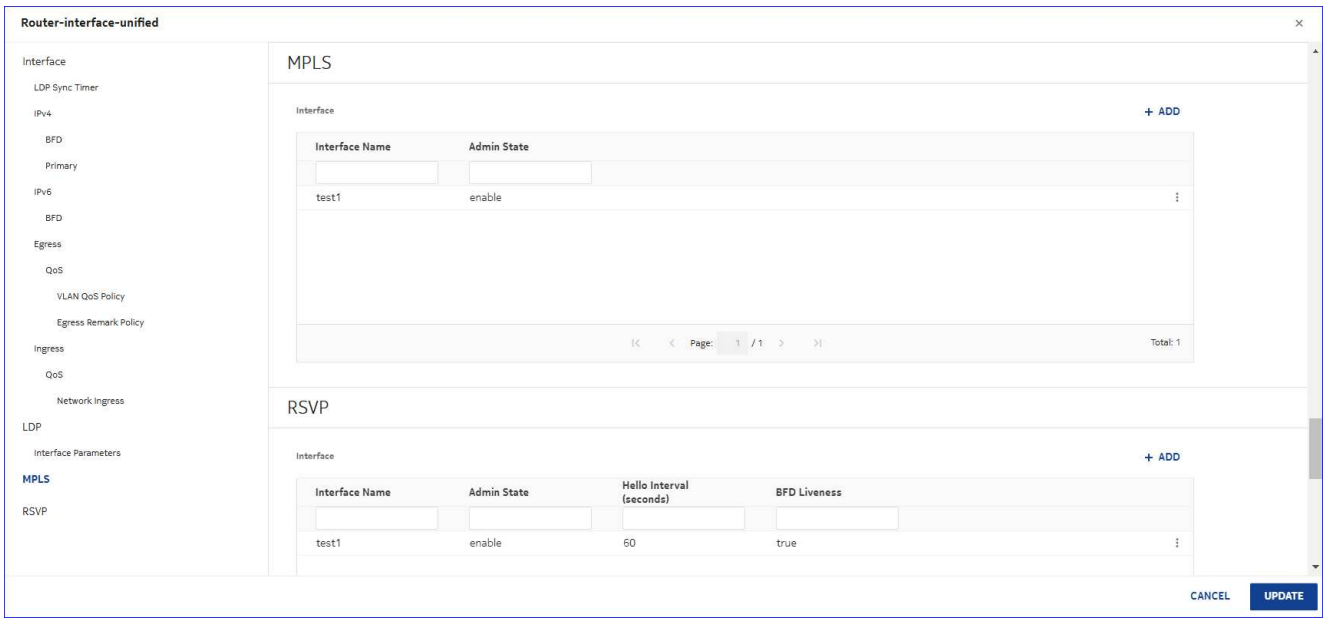
```
(pr)[/configure router "Base" interface "test7"]
A:admin@Boston# info
    admin-state enable
    description "Interface to Core node"
    port 1/1/c2/1:2
    ldp-sync-timer {
        seconds 100
    }
    ipv4 {
        bfd {
            admin-state enable
            transmit-interval 100
            receive 100
            multiplier 2
            type auto
        }
        primary {
            address 10.10.10.2
            prefix-length 24
        }
    }
```

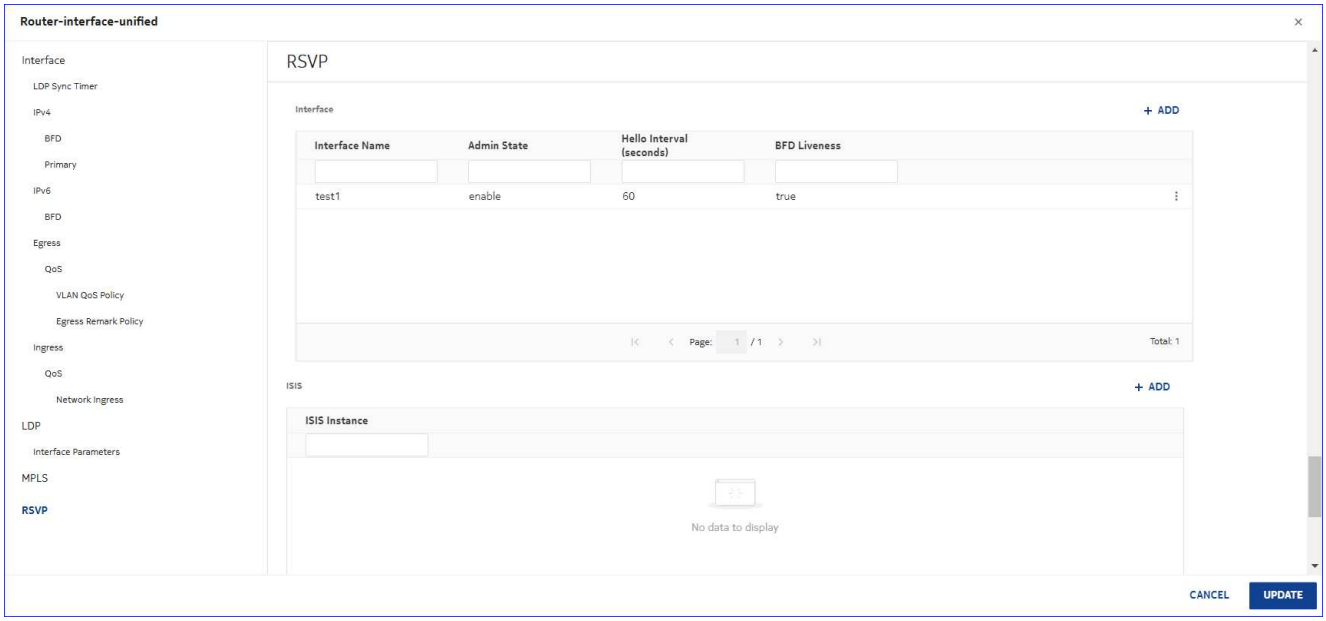
Example 2: 7750 SR-14s Classic











Note: The deployment works without the primary IPv4 address, MPLS, and RSVP configurations on the 7750 SR-14s classic NE, and the interface is created on the classic NE.

Figure 7-28 NE CLI after deployment

```
A:Toronto>config>router>mpls# /configure router interface "test1"
A:Toronto>config>router>if# info
----------------------------------------------
            description "Interface to Core NE"
            ldp-sync-timer 100
            port 1/1/c1/9:4
            bfd 100 receive 100 multiplier 2
            no shutdown
----------------------------------------------
```

END OF STEPS

7.9 LDP

7.9.1 LDP protocol

LDP (Label Distribution Protocol) is a protocol used in Multiprotocol Label Switching (MPLS) networks to establish label-switched paths (LSPs).

Configuration must be performed in CLI because there is no intent to enable or configure LDP. The CLI commands below are the minimum required to enable this protocol.

7.9.2 Configuring LDP

1

Configure LDP on nodes.

Classic nodes:

```
/configure router ldp
```

MD nodes:

```
/edit-config private
/configure router ldp admin-state enable
/commit
/admin save
/exit all
/quit-config
```

2

Check the status of the protocols on all nodes:

```
/show router ldp status
```

Note: For LDP to be operational, users need to configure the IPv4 and IPv6 bindings manually via CLI. The bindings are not attributes users can select/configure via the intent type.

3

Log in to each router via CLI.

4

Add the IPv4 and/or IPv6 bindings to the protocol traffic-engineering on OSPF, IS-IS, or both via CLI since it cannot be done through NSP via an ICM pre-defined intent:

Classic:

```
/configure router ldp interface-parameters interface "<interface_
name>" ipv4 no shutdown
/configure router ldp interface-parameters interface "<interface_
name>" ipv6 no shutdown
```

MD:

```
/configure router ldp interface-parameters interface "<interface_
name>" ipv4
/configure router ldp interface-parameters interface "<interface_
name>" ipv6
```

5

Repeat Step 4 for all interfaces under the LDP context.

Figure 7-29 Ex. Classic

```
#--------------------------------------------------
echo "LDP Configuration"
#--------------------------------------------------
        ldp
            import-pmsi-routes
            exit
            tcp-session-parameters
            exit
            interface-parameters
                interface "test7" dual-stack
                    ipv4
                        no shutdown
                    exit
                    no shutdown
                exit
            exit
            targeted-session
            exit
            no shutdown
        exit
#--------------------------------------------------
```

Note: The IPv4 binding should be configured by default even though this attribute is not part of the intent type for classic NEs only.

END OF STEPS

7.10 BGP

7.10.1 BGP-EVPN

Note: The following configurations must be done manually on a router before BGP can be configured.

1

Log in to the router via CLI.

2

Configure the autonomous system parameter on the routers:

Classic:

```
/configure router autonomous-system <ID>
```

Example: `/configure router autonomous-system 65100`

MD:

```
/configure router autonomous-system <ID>
```

Example: `/configure router autonomous-system 65100`

3

For classic NEs, the BGP context or instance must be created first. This is not necessary for model-driven NEs.

Classic:

```
/configure router bgp
```

4

Log in to NSP.

5

Import the intent type **icm-router-bgp_group** into **Device Management**, **Configuration Intent Types**.

6

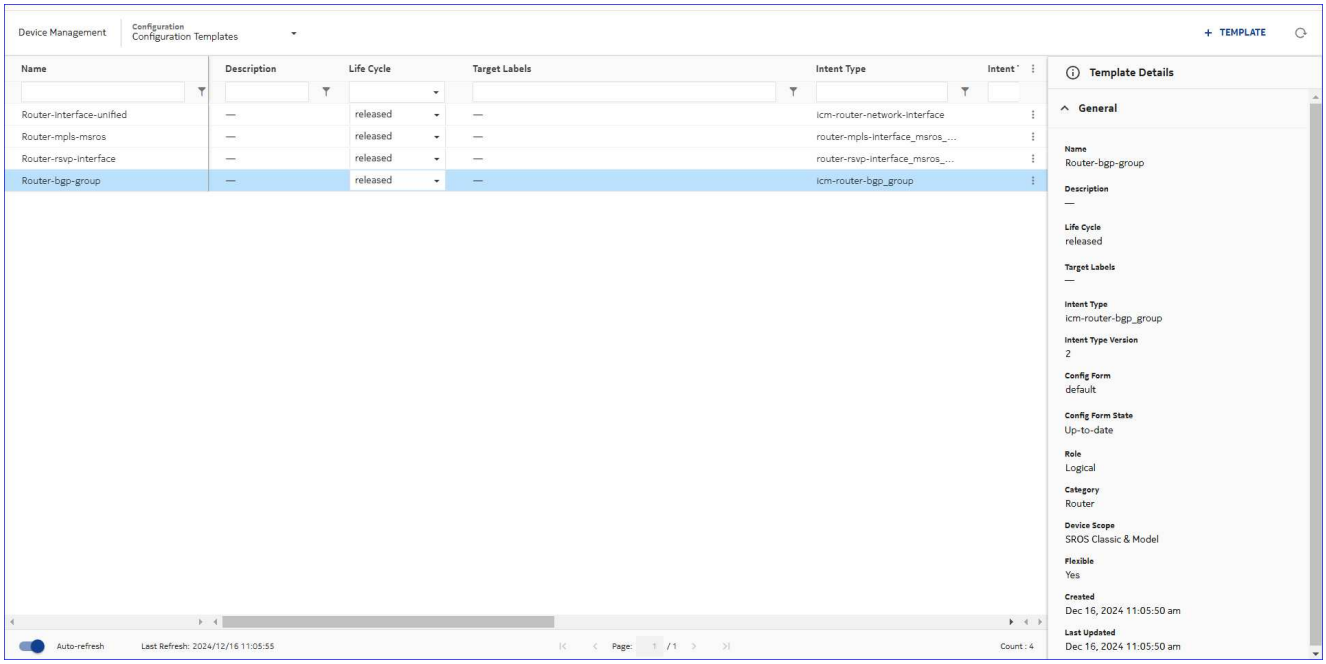
Navigate to **Device Management**, **Configuration Templates**.

7

Create a configuration template (ex. Router-bgp-group) and associate **icm-router-bgp_group** intent type. Use the default schema form.

8

Release the BGP group template.



9

Navigate to **Device Management**, **Configuration Deployments**.

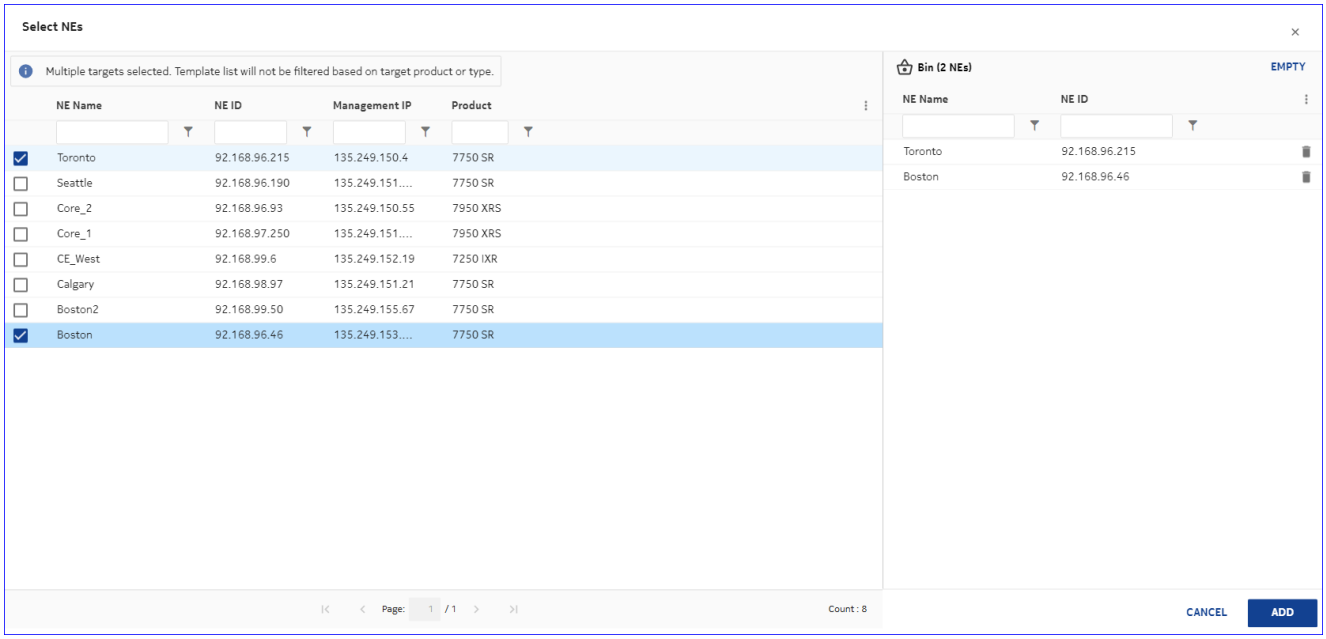
10

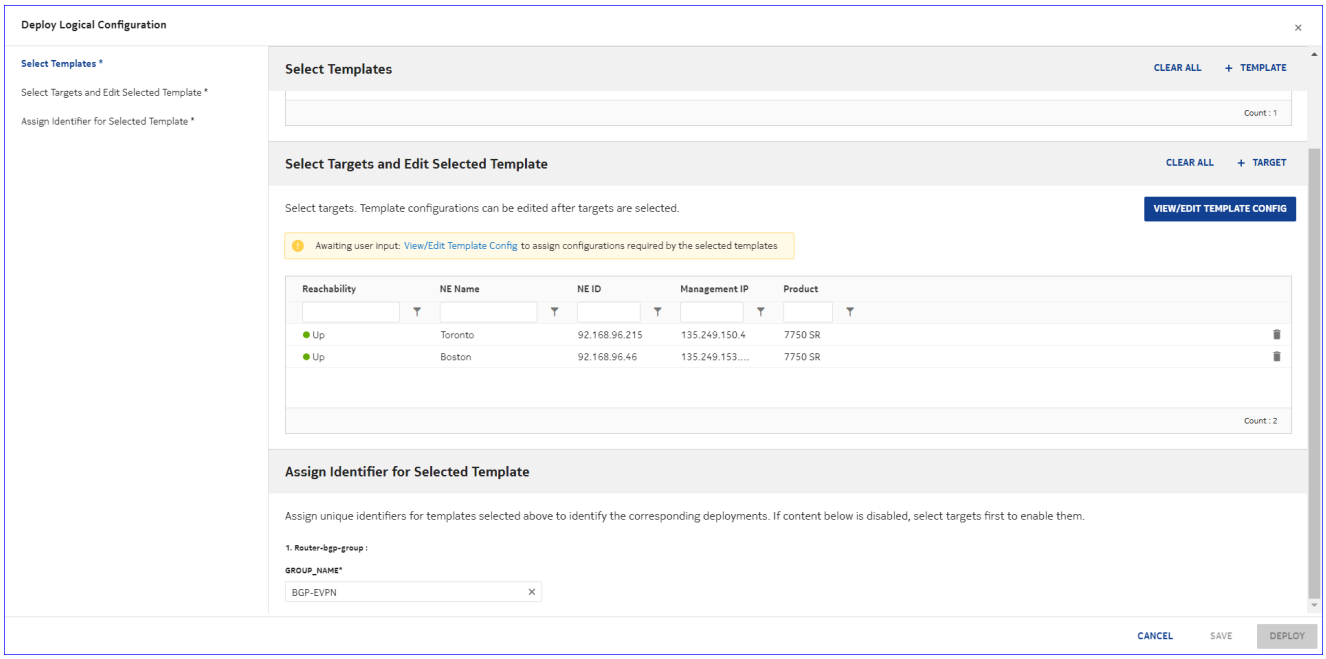
Create a logical deployment and select the BGP group template.

11

Select the target NE.

For the following example, both 7750 SR-14s classic and MD NEs were selected as deployment targets.

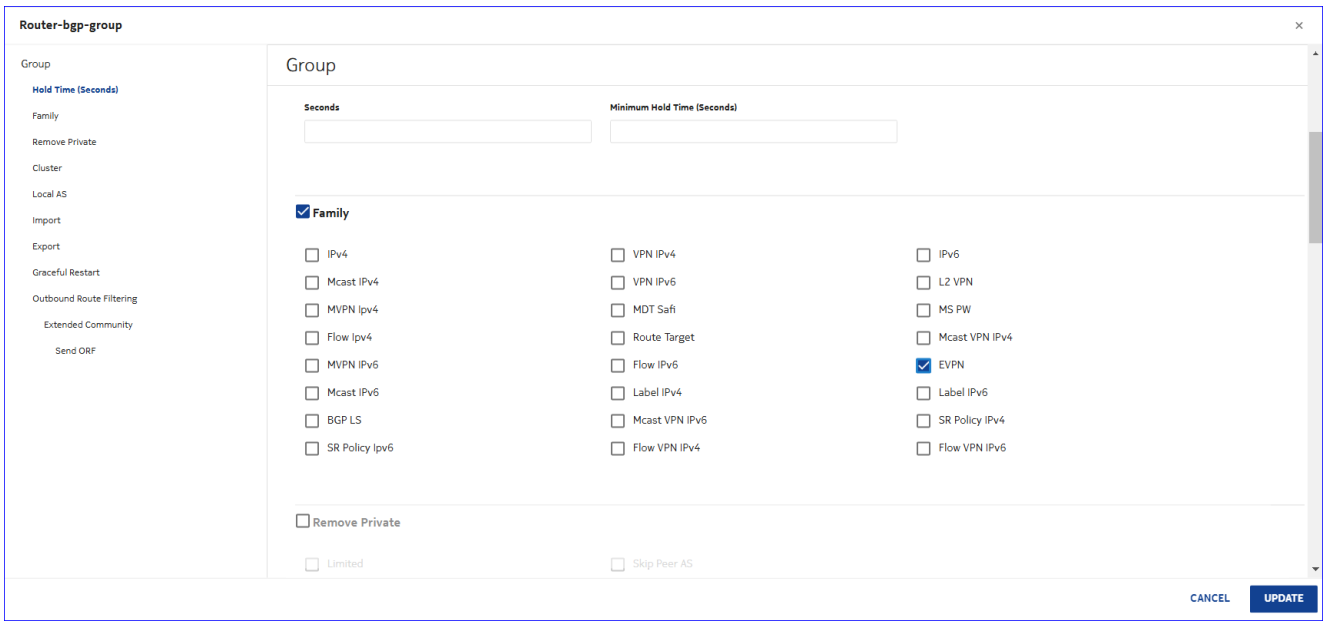




12

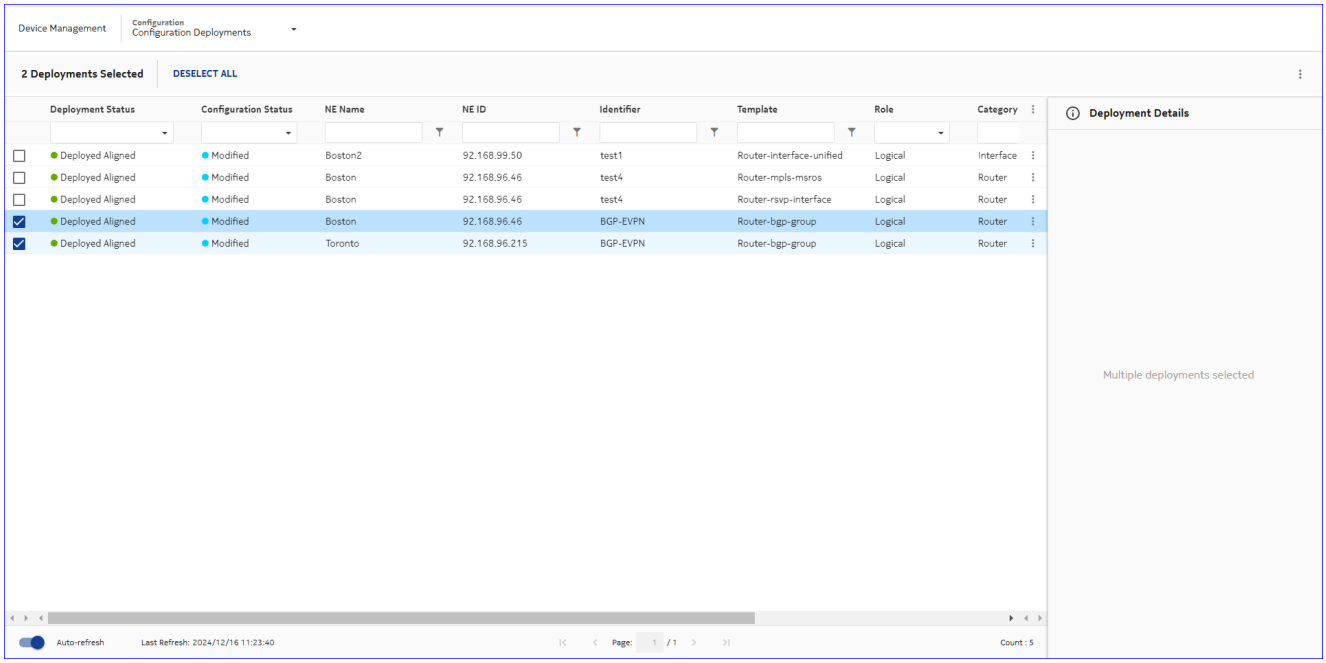
Click on **VIEW/EDIT TEMPLATE CONFIG** and enter the BGP group parameters that are common to all targets. At minimum, select the family.

Note: For BGP-EVPN, EVPN must be selected.



13

Deploy the configurations and verify that all the deployments have been successful.



After deployment:

Figure 7-30 Classic NE

```
#--------------------------------------------------
echo "BGP Configuration"
#--------------------------------------------------
        bgp
            group "BGP-EVPN"
                family evpn
                disable-client-reflect
                disable-4byte-asn
            exit
            no shutdown
        exit
--------------------------------------------------
```

Figure 7-31 MD NE

```
(pr)[/configure router "Base" bgp]
A:admin@Boston# info
    group "BGP-EVPN" {
        admin-state enable
        family {
            evpn true
        }
    }
```

14

Add the peers to each BGP group instance (and add the corresponding attributes):

1. Select the first BGP group deployment and click **View/Edit...**.
2. On the Deploy Logical Configuration form, click **VIEW/EDIT TEMPLATE CONFIG**.
3. In the “Neighbor” section, add all neighbors (i.e other PE routers) to that particular group and configure the “peer” as attribute (which should be equal to the autonomous system ID).

Figure 7-32 Classic NE

```
A:Toronto>config>router>bgp# info
----------------------------------------------
            group "BGP-EVPN"
                family evpn
                disable-client-reflect
                disable-4byte-asn
                neighbor 92.168.96.46
                    disable-client-reflect
                    disable-4byte-asn
                    peer-as 65100
                    disable-capability-negotiation
                exit
                neighbor 92.168.96.190
                    disable-client-reflect
                    disable-4byte-asn
                    peer-as 65100
                    disable-capability-negotiation
                exit
            exit
            no shutdown
----------------------------------------------
```

Figure 7-33 MD NE

```
(pr)[/configure router "Base" bgp]
A:admin@Boston# info
    group "BGP-EVPN" {
        admin-state enable
        family {
            evpn true
        }
    }
    neighbor "92.168.96.190" {
        admin-state enable
        group "BGP-EVPN"
        peer-as 65100
        family {
            evpn true
        }
    }
    neighbor "92.168.96.215" {
        admin-state enable
        group "BGP-EVPN"
        peer-as 65100
        family {
            evpn true
        }
    }

(pr)[/configure router "Base" bgp]
```

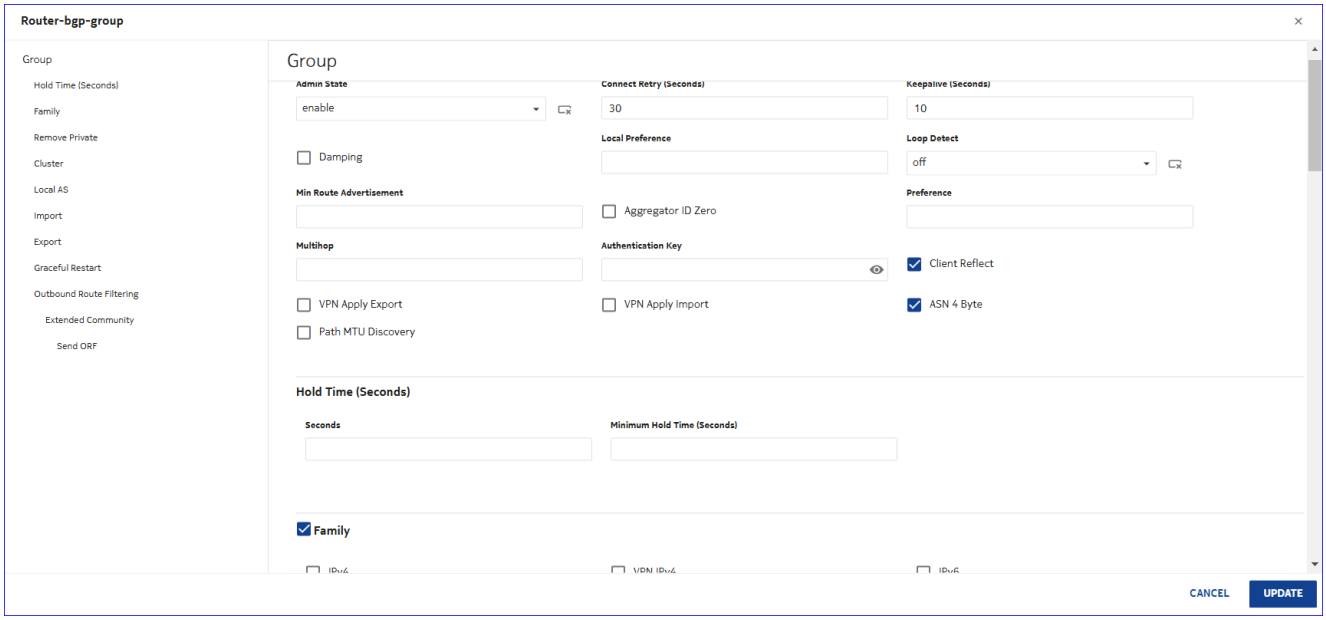
END OF STEPS

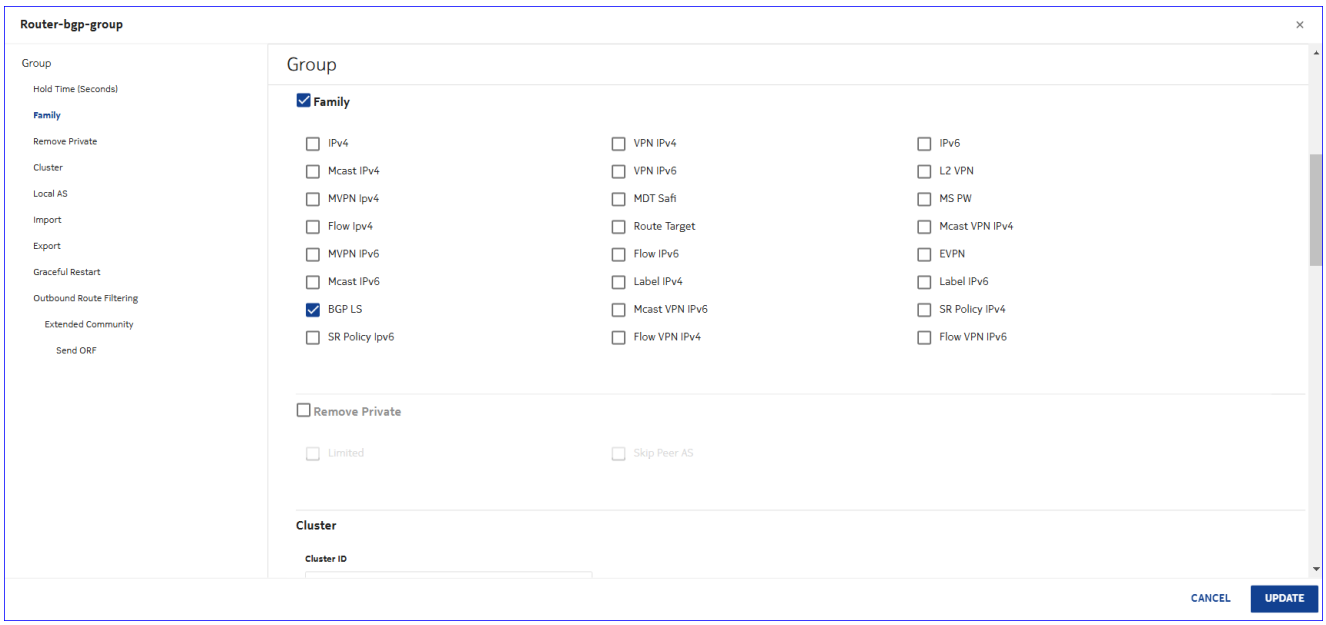
7.10.2 BGP-LS

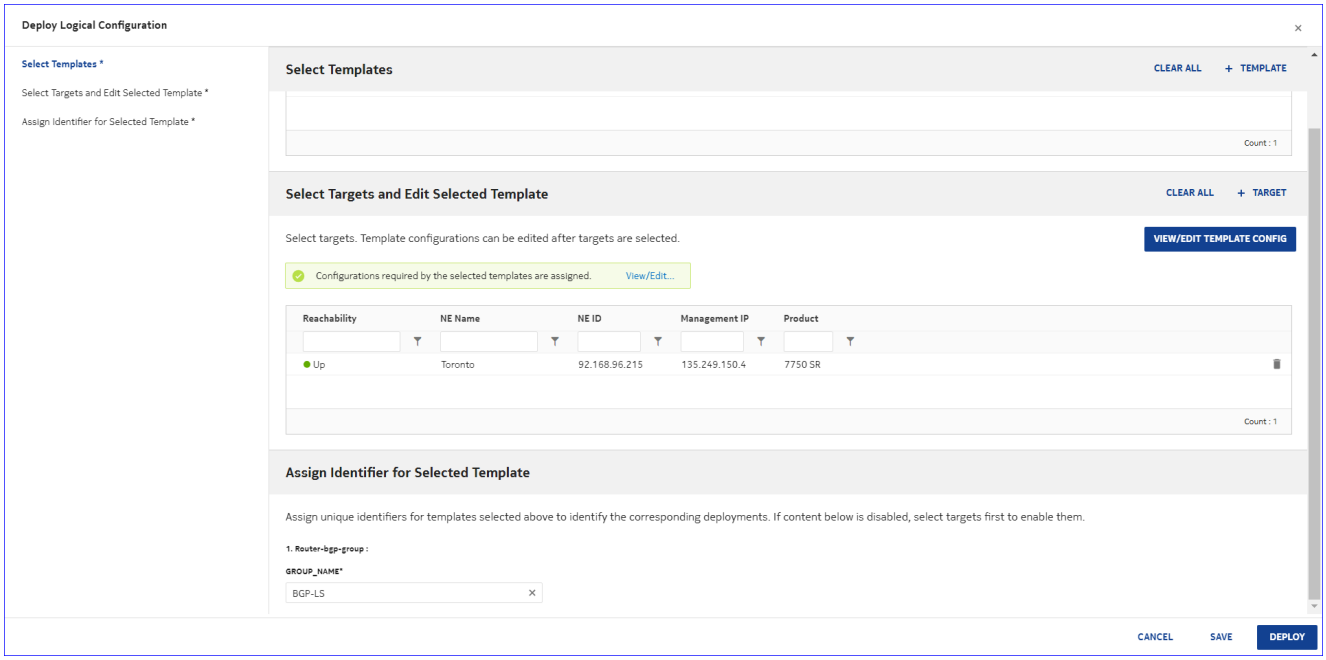
A different router BGP group can be configured with the same **icm-router-bgp_group** intent type. The following procedure describes this process. The same configuration template **Router-bgp-group** can be used for this configuration deployment.

1

The following attribute can be filled for the **Router-bgp-group** template deployment form for configuring BGP-LS.





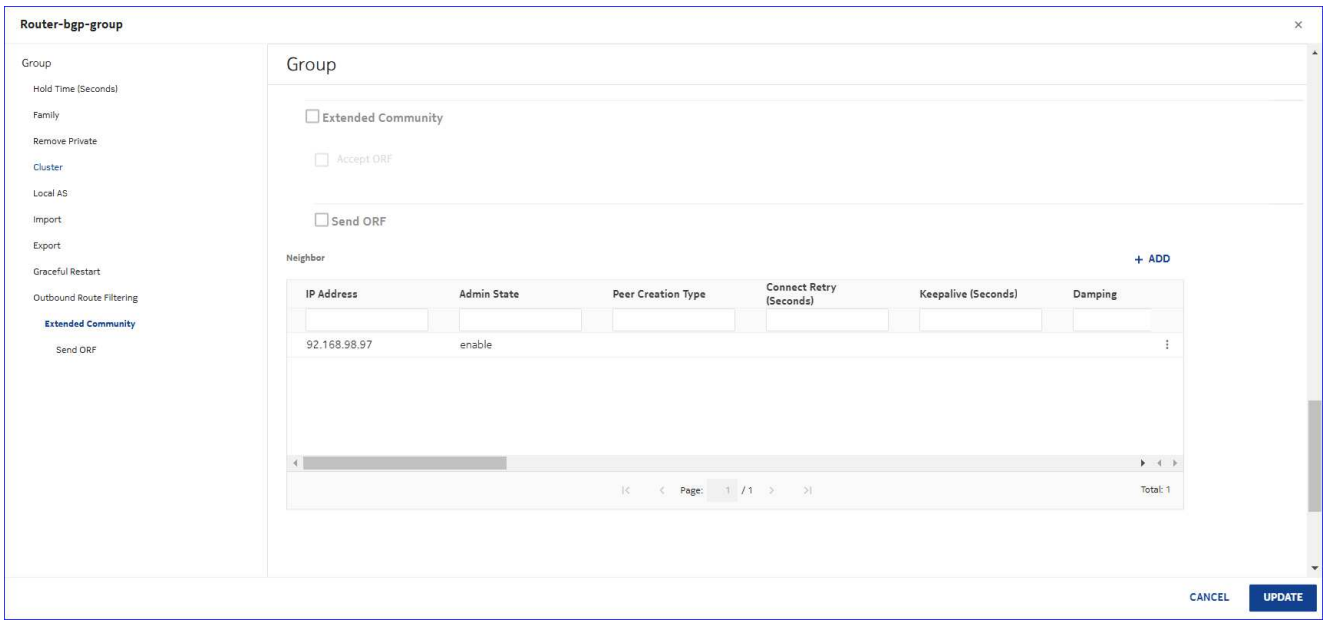


NE CLI after successful deployment of BGP-LS group configuration:

```
A:Toronto>config>router>bgp# info
----------------------------------------------
            group "BGP-LS"
                family bgp-ls
                connect-retry 30
                keepalive 10
                loop-detect off
            exit
            group "BGP-EVPN"
                family evpn
                neighbor 92.168.96.46
                    peer-as 65100
                exit
                neighbor 92.168.96.190
                    peer-as 65100
                exit
            exit
            no shutdown
----------------------------------------------
```

2

Configuring neighbors in the BGP-LS group can be done through a re-deployment of the same template by adding the neighbor to the deployment form.



NE CLI after addition of neighbor to the "BGP-LS" group through the above deployment:

```
-----------------------------------------------
A:Toronto>config>router>bgp# info
-----------------------------------------------
            group "BGP-LS"
                family bgp-ls
                connect-retry 30
                keepalive 10
                loop-detect off
                neighbor 92.168.98.97
                exit
            exit
            group "BGP-EVPN"
                family evpn
                neighbor 92.168.96.46
                    peer-as 65100
                exit
                neighbor 92.168.96.190
                    peer-as 65100
                exit
            exit
            no shutdown
-----------------------------------------------
```

END OF STEPS

7.11 Segment Routing

Note: To enable and configure Segment Routing (SR) on the NEs, users need to use CLI as there is no NSP ICM intent type that can provision or configure SR on the NEs in the network. Segment Routing is a prerequisite for creating SR-TE LSPs.

7.11.1 Steps

1

Log in to the router via CLI.

2

Configure the IGP instance (OSPF, IS-IS, or both) to signal the router capability TLVs (advertisements). “Area” should be used for OSPF and “AS” should be used for IS-IS.

Classic:

```
/configure router ospf advertise-router-capability area
/configure router isis advertise-router-capability as
```

MD:

```
/configure router ospf advertise-router-capability area
/configure router isis advertise-router-capability as
/commit
```

3

Through CLI, define the Segment Routing Global Block (SRGB) to reserve a range of labels to Prefix-SIDs:

Note: In the following example, the range used is [20000, 30000].

Classic:

```
/configure router mpls-labels sr-labels start 20000 end 30000
```

MD:

```
/configure router mpls-labels sr-labels start 20000 end 30000
/commit
```

4

If not already done, enable traffic engineering using CLI. This is also not configurable through the use of the pre-defined intent types.

Note: If RSVP has already been configured on the network, this step can be skipped.

Classic:

```
/configure router ospf traffic-engineering
/configure router isis traffic-engineering
```

MD:

```
/configure router ospf traffic-engineering
/configure router isis traffic-engineering
/commit
```

5

Through CLI, enable Segment Routing in the IGP instance (OSPF, IS-IS, or both). Also define the “start-label” for the “Prefix-SID” range as well as the “index-range”. Here, if the user chooses “global” as the value, the “'start-label” is equal to the lowest label value in the SRGB and max-index is equal to the range size of the SRGB.

Classic:

```
/configure router ospf segment-routing prefix-sid-range global
/configure router ospf segment-routing no shutdown
```

```
/configure router isis segment-routing prefix-sid-range global
/configure router isis segment-routing no shutdown
```

MD:

```
/configure router ospf segment-routing prefix-sid-range global
/configure router ospf segment-routing admin-state enable
/configure router isis segment-routing prefix-sid-range global
/configure router isis segment-routing admin-state enable
/commit
```

6

A node-SID index or label value is normally assigned to the NE's primary address (such as a “system” or “loopback” address). The address must be in the GRT (Global Routing Table). Use CLI to configure the index or label to the interface in the IGP instance (OSPF, IS-IS, or both). If both IGP instances are to be configured, a different label/index value must be used as the same value cannot be used. Each router must have a unique label/index value.

Example: Defined SRGB: [20000, 30000]

Classic NE (e.g. 'Calgary NE'):

```
/configure router ospf 0 area 0.0.0.0 interface "system"
node-sid label 20000
/configure router isis 0 interface "system" ipv4-node-sid label 20006
```

MD NE (e.g. 'Seattle NE'):

```
/configure router ospf 0 area 0.0.0.0 interface "system" node-sid
label 20005
/configure router isis 0 interface "system" ipv4-node-sid label 20011
/commit
```

Note: The label/index node-SID value assignment must be different and unique. The chosen value must be a value within the SRGB.

END OF STEPS

7.12 LSP

7.12.1 To configure RSVP-TE LSPs and Paths onto the network

1

Log in to the router via CLI.

2

Configure traffic-engineering on OSPF, IS-IS, or both via CLI since it cannot be done through NSP via an ICM pre-defined intent:

Classic:

```
/configure router ospf traffic-engineering
/configure router isis traffic-engineering
```

MD:

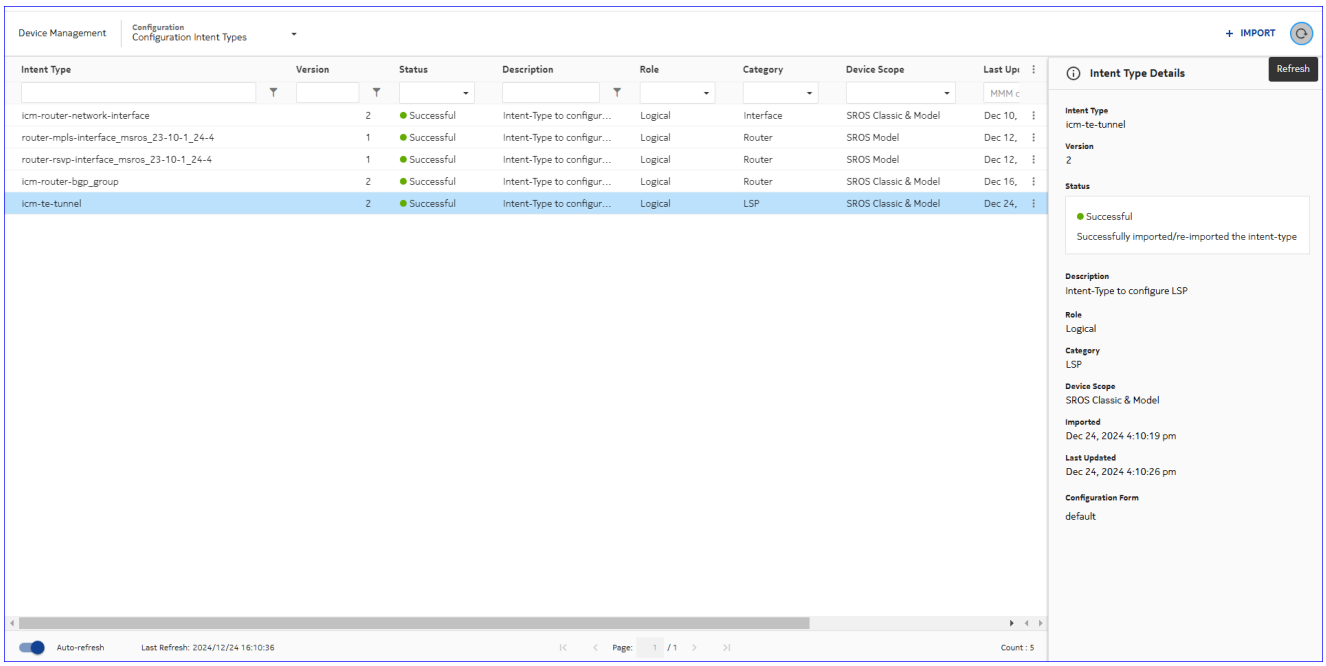
```
/configure router ospf traffic-engineering
/configure router isis traffic-engineering
/commit
```

3

Log in to NSP.

4

Import the intent type **icm-te-tunnel** into **Device Management**, **Configuration Intent Types**.



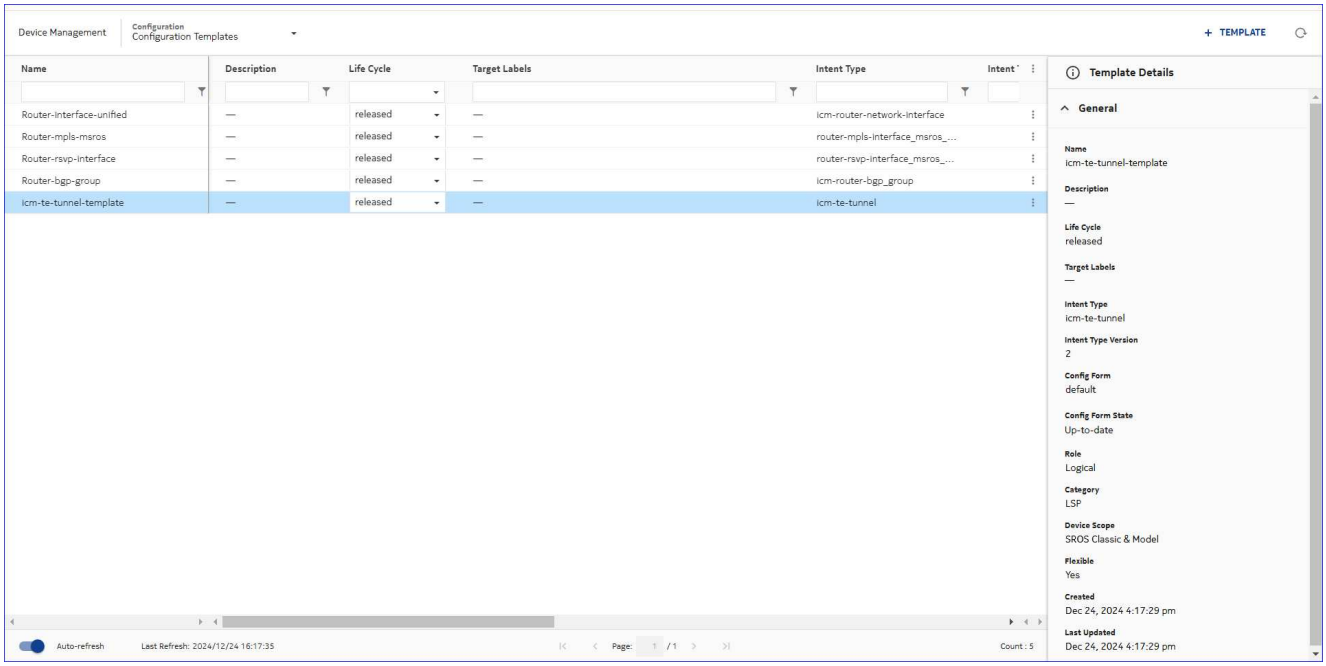
5

Navigate to **Device Management**, **Configuration Templates**.

6

Create a configuration template and associate the **icm-te-tunnel** intent type.

For example, the configuration template created below is named as **icm-te-tunnel-template**.

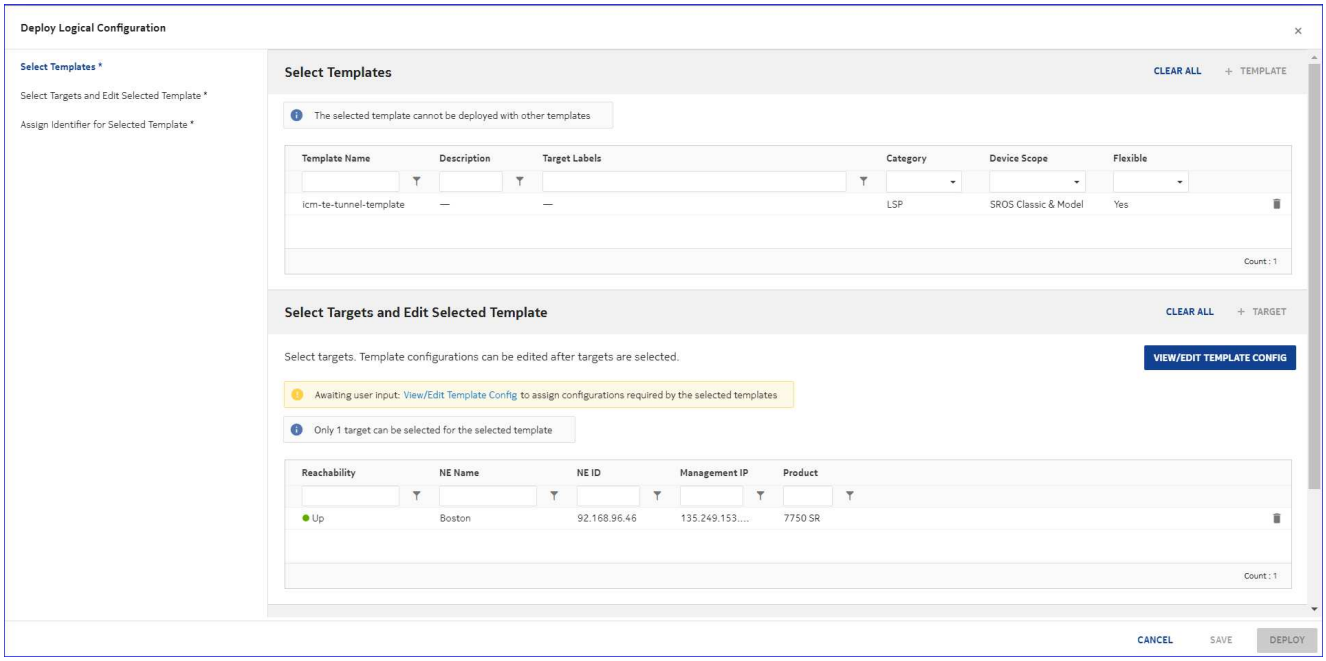


7

Navigate to **Device Management**, **Configuration Deployments**.

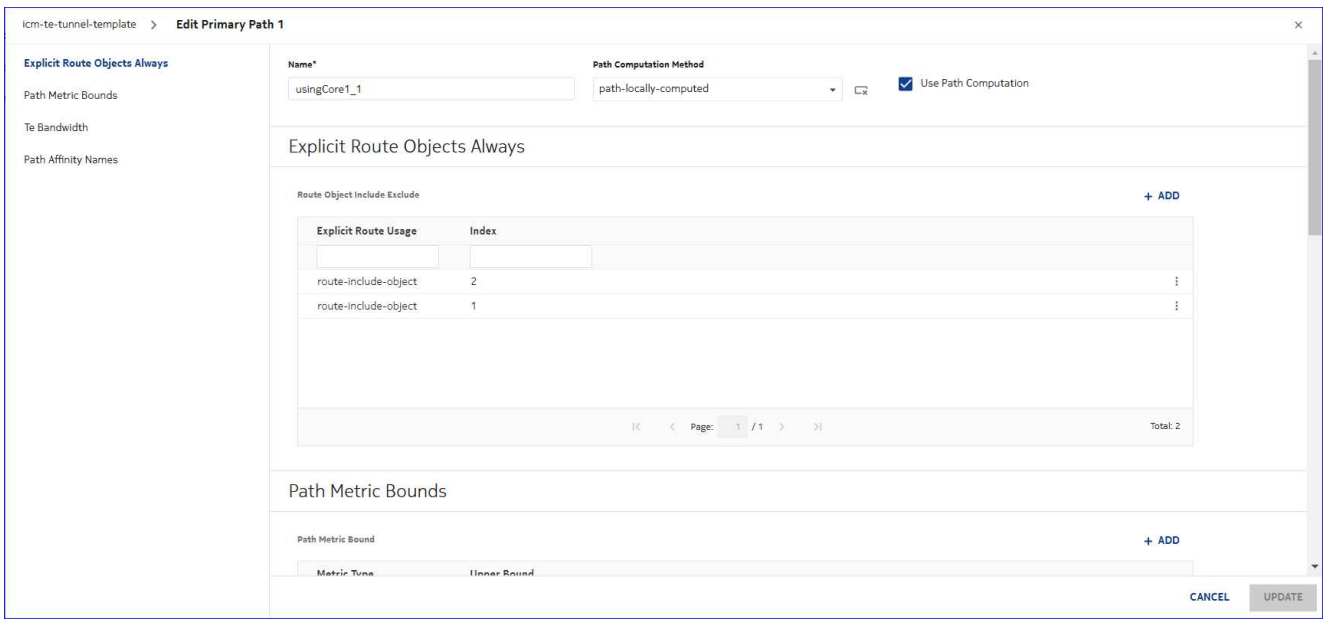
8

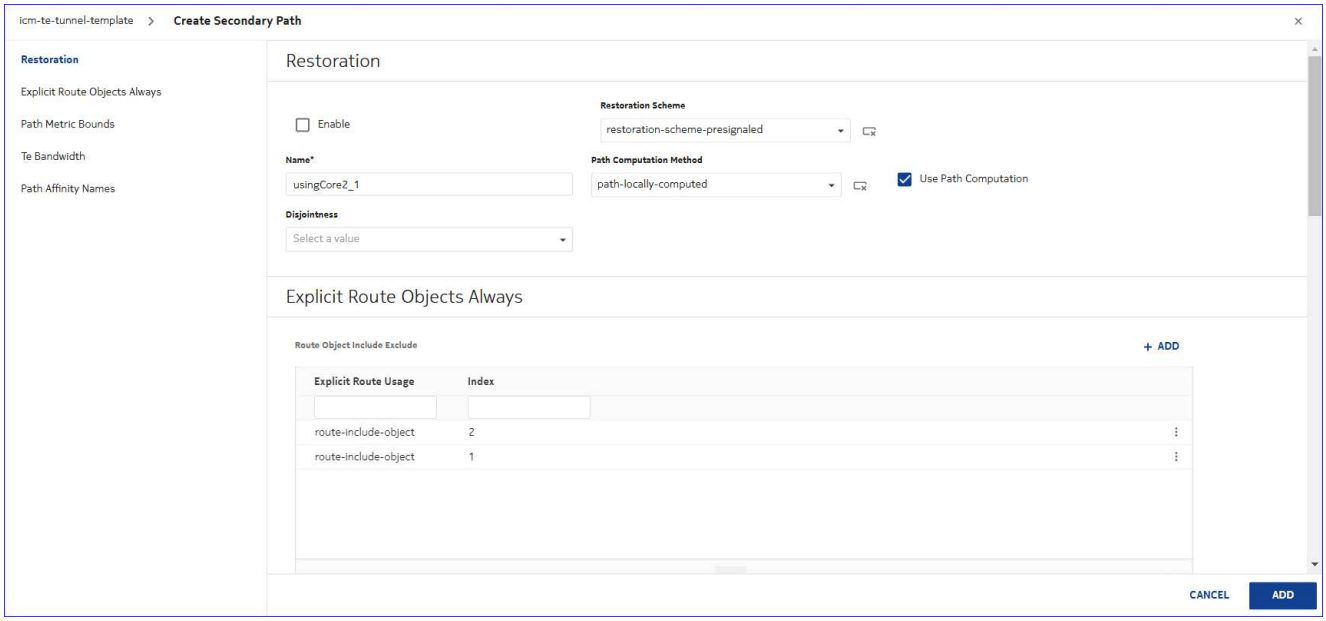
Create a logical deployment and select the TE tunnel (LSP) template.

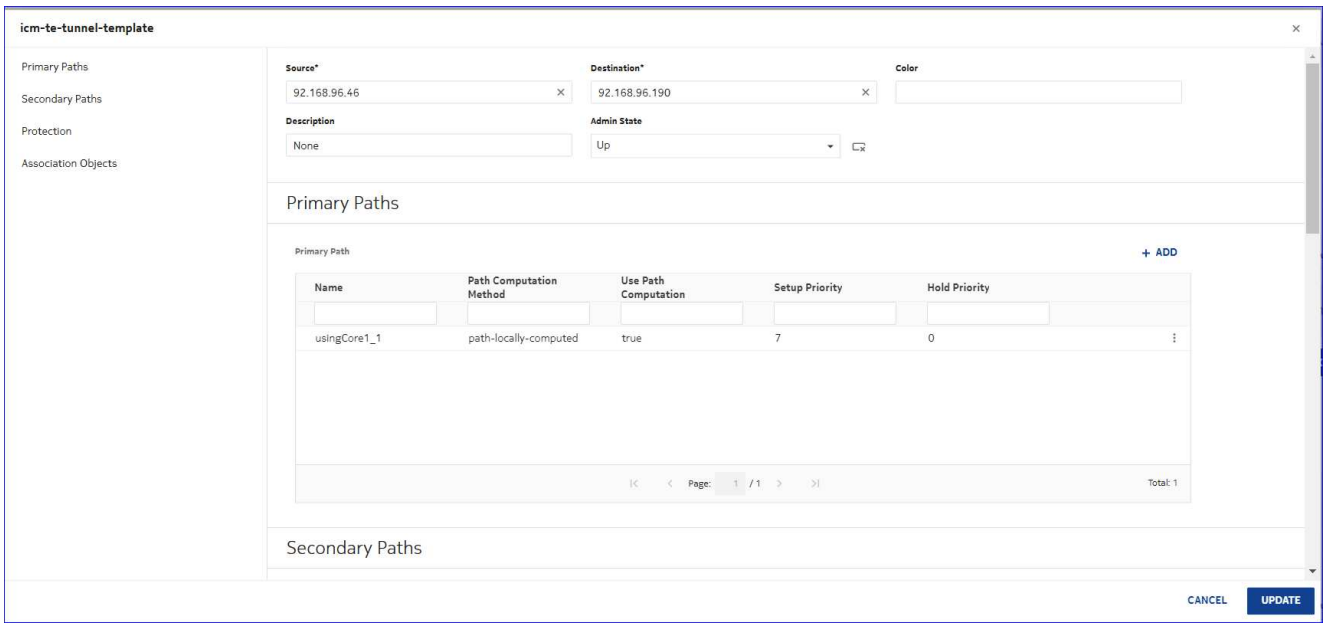


9

Click on **VIEW/EDIT TEMPLATE CONFIG** and enter the LSP and LSP path parameters (source, destination, signaling-type (RSVP vs. SR-TE) path-computation method, primary and secondary paths, hop limits and conditions, etc.).







10

Click **UPDATE**.

11

Give LSP Tunnel a name and click **DEPLOY**.

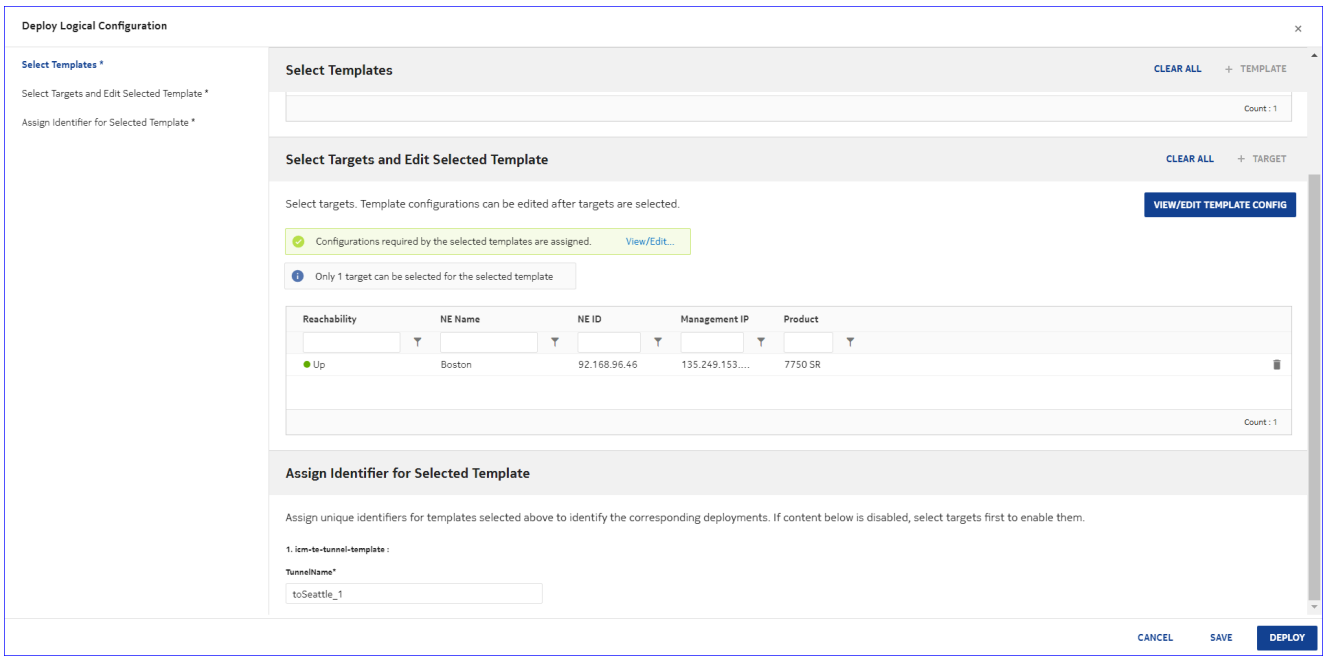


Figure 7-34 NE CLI after deployment

```
A:admin@Boston# configure router mpls lsp "toSeattle_1"

(pr)[/configure router "Base" mpls lsp "toSeattle_1"]
A:admin@Boston# info
    admin-state enable
    type p2p-rsvp
    from 92.168.96.46
    to 92.168.96.190
    pce-control true
    pce-report true
    path-computation-method pce
    egress-statistics {
        admin-state enable
    }
    primary "toSeattle_1_usingCore1_1" {
        bandwidth 0
        priority {
            setup-priority 7
            hold-priority 0
        }
    }
    secondary "toSeattle_1_secondary_usingCore2_1" {
        bandwidth 0
        srlg false
        standby false
        priority {
            setup-priority 7
            hold-priority 0
        }
    }

(pr)[/configure router "Base" mpls lsp "toSeattle_1"]
```

END OF STEPS

7.13 Customers

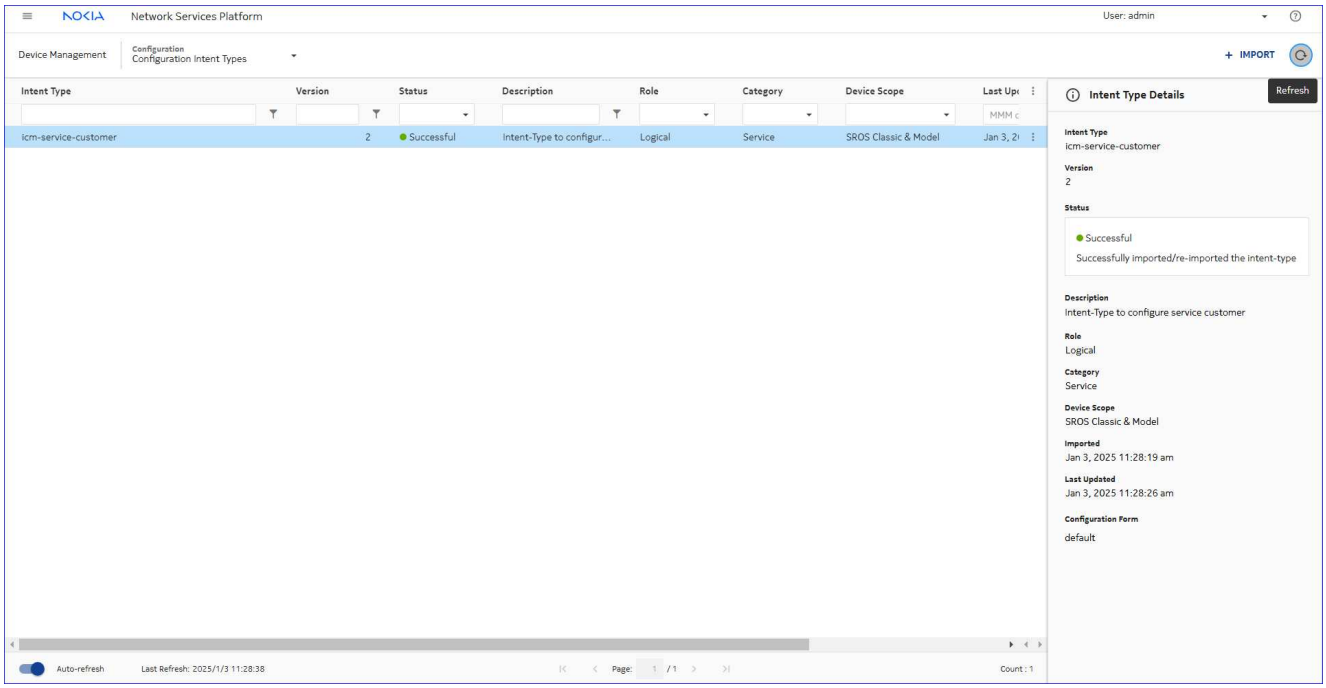
7.13.1 To configure customers using service customer intent

1

Log in to NSP.

2

Import the intent type **icm-service-customer** into **Device Management**, **Configuration Intent Types**.



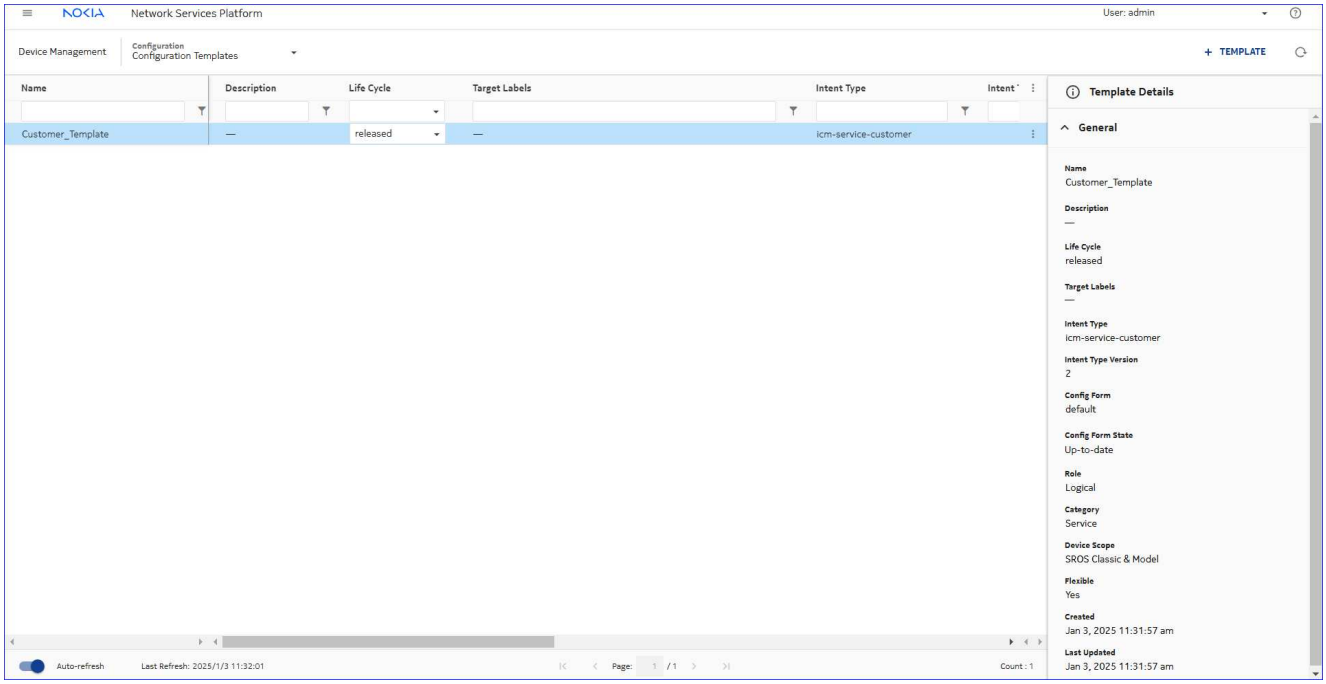
3

Navigate to **Device Management**, **Configuration Templates**.

4

Create a configuration template and associate the **icm-service-customer** intent type.

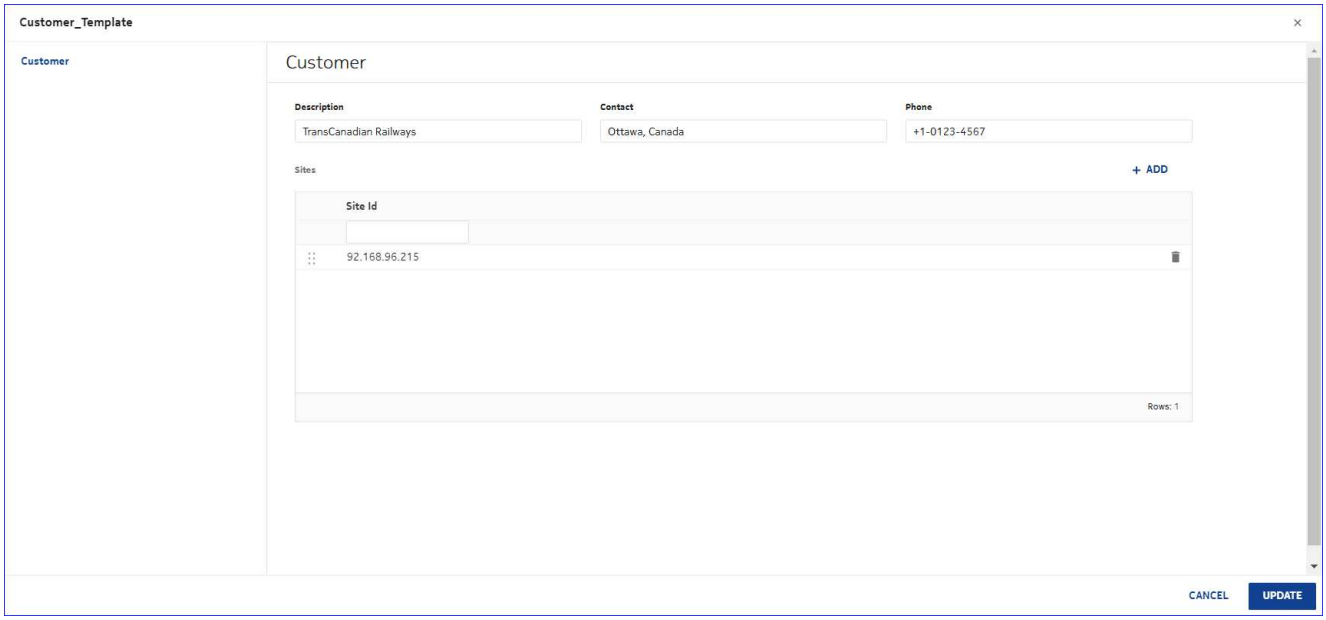
For example, the configuration template created below is named as **Customer_Template**.

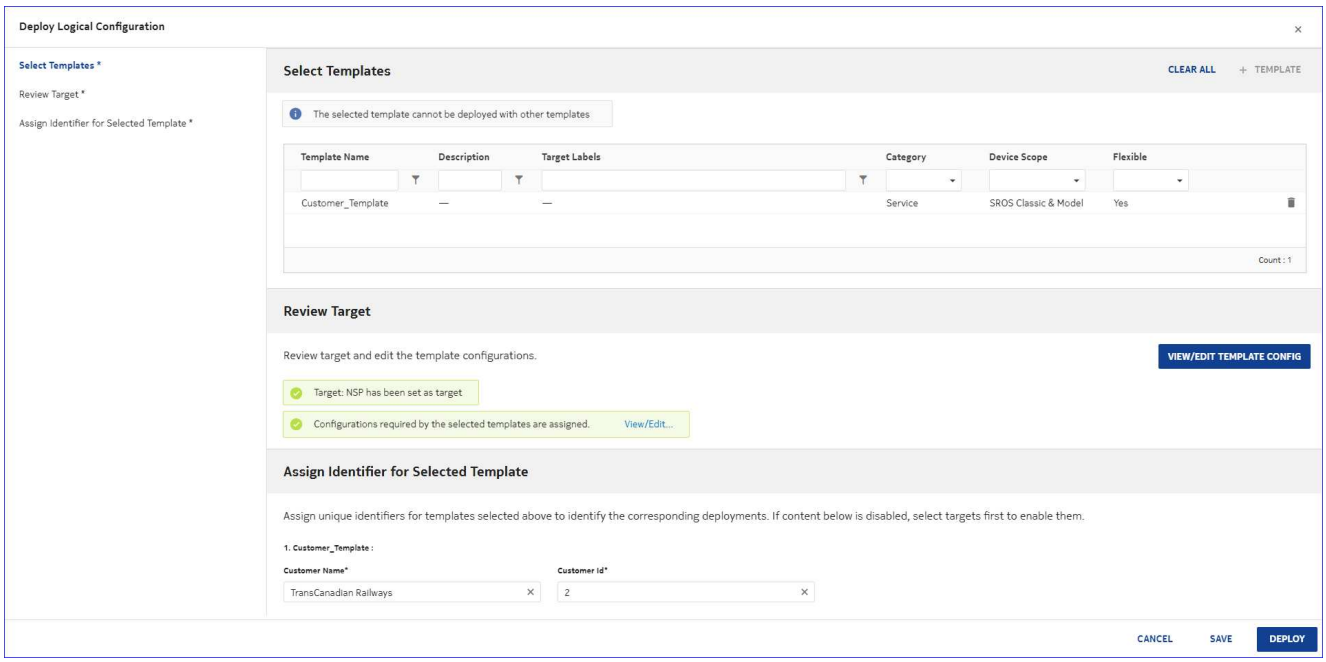


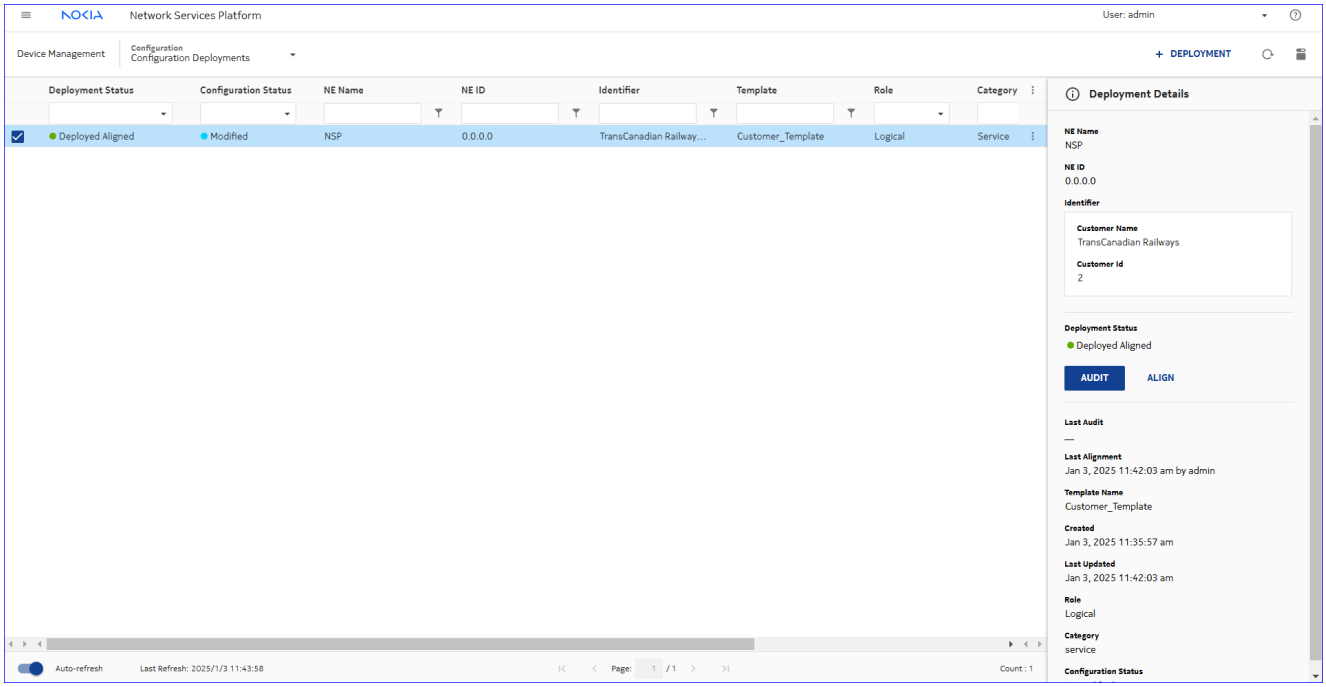
5

Navigate to **Device Management**, **Configuration Deployments**.

Note: NSP is always the target for this deployment. While configuring the customer, users can choose to deploy it to one or more sites or leave it to Service Management to configure the customer on the requisite sites when a service is provisioned.







6

Check the NE:

```
A:Toronto>config>service>cust# /configure service customer 2
A:Toronto>config>service>cust# info
----------------------------------------------
            description "TransCanadian Railways"
            contact "Ottawa, Canada"
            phone "+1-0123-4567"
----------------------------------------------
```

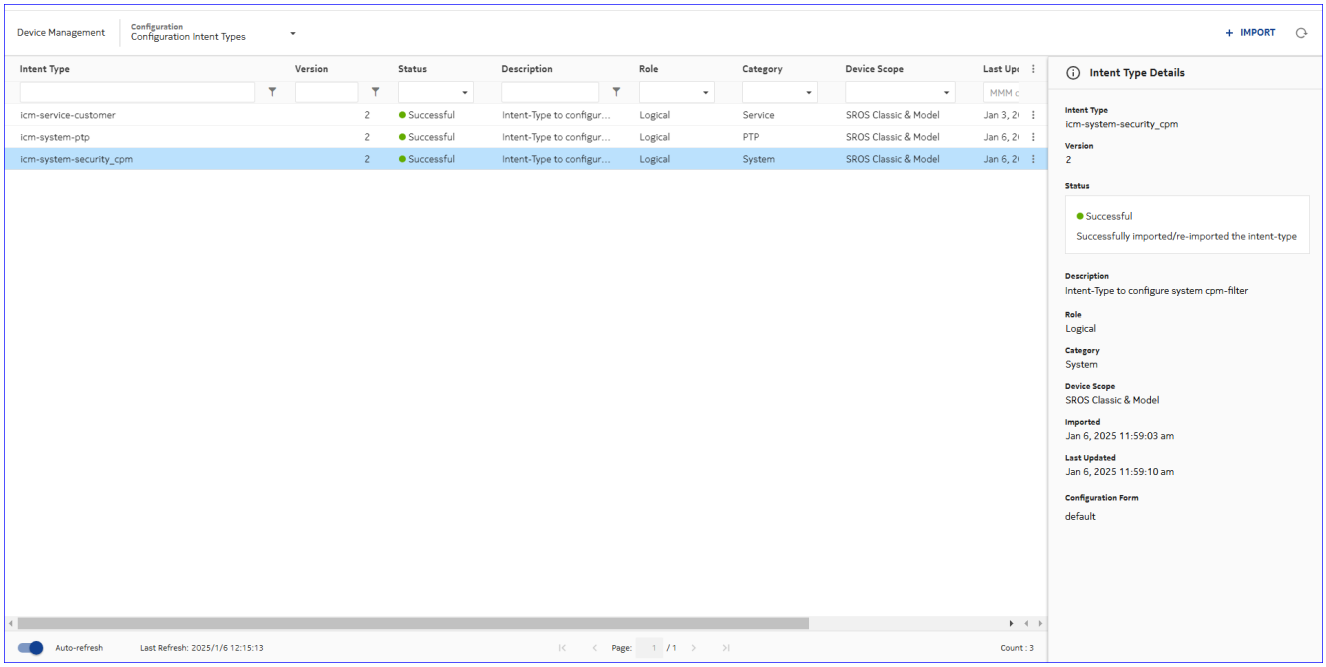
END OF STEPS

7.14 Other configurations

7.14.1 To configure using icm-system-security-cpm intent type

1

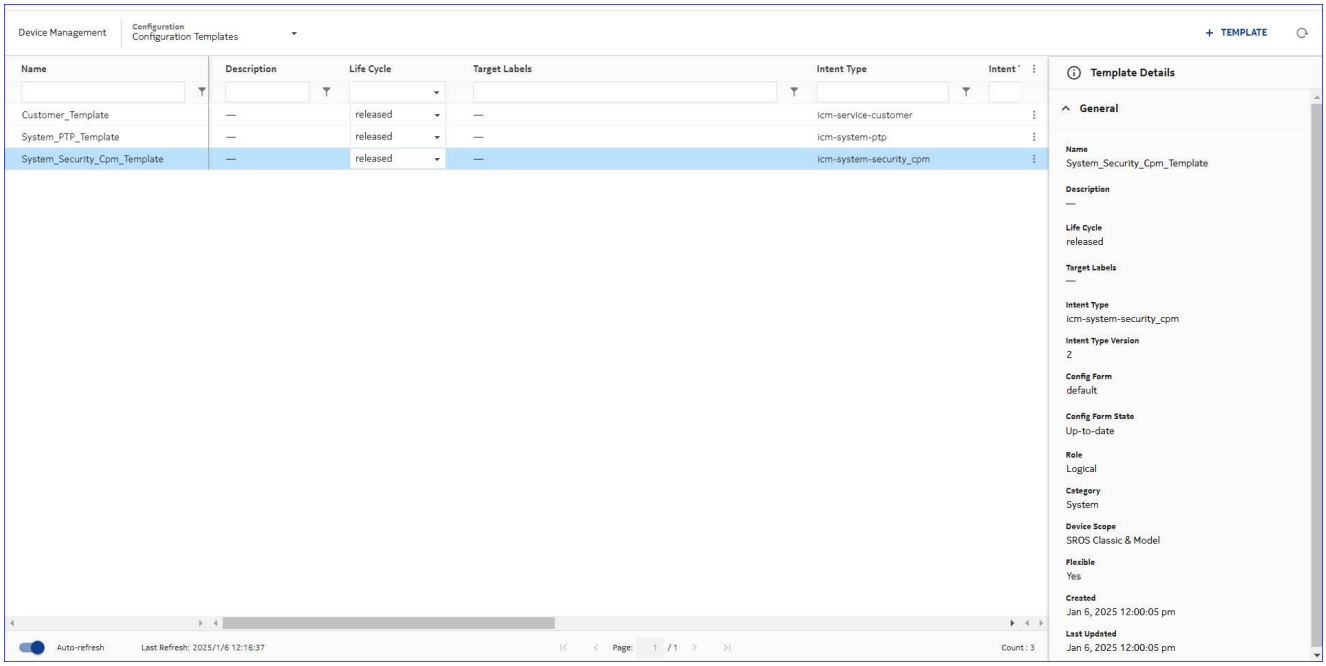
Import the intent type **icm-system-security-cpm** into **Device Management**, **Configuration Intent Types**.



2

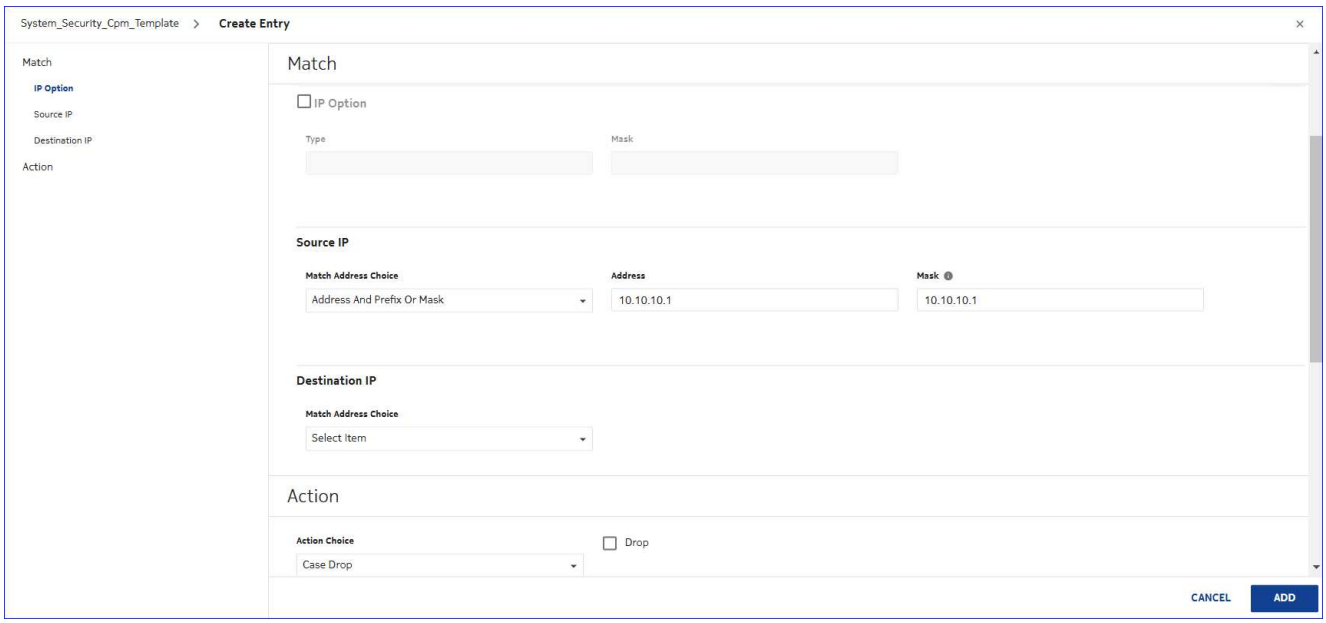
Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

For example, the configuration template created below is named as **System_Security_Cpm_Template**.

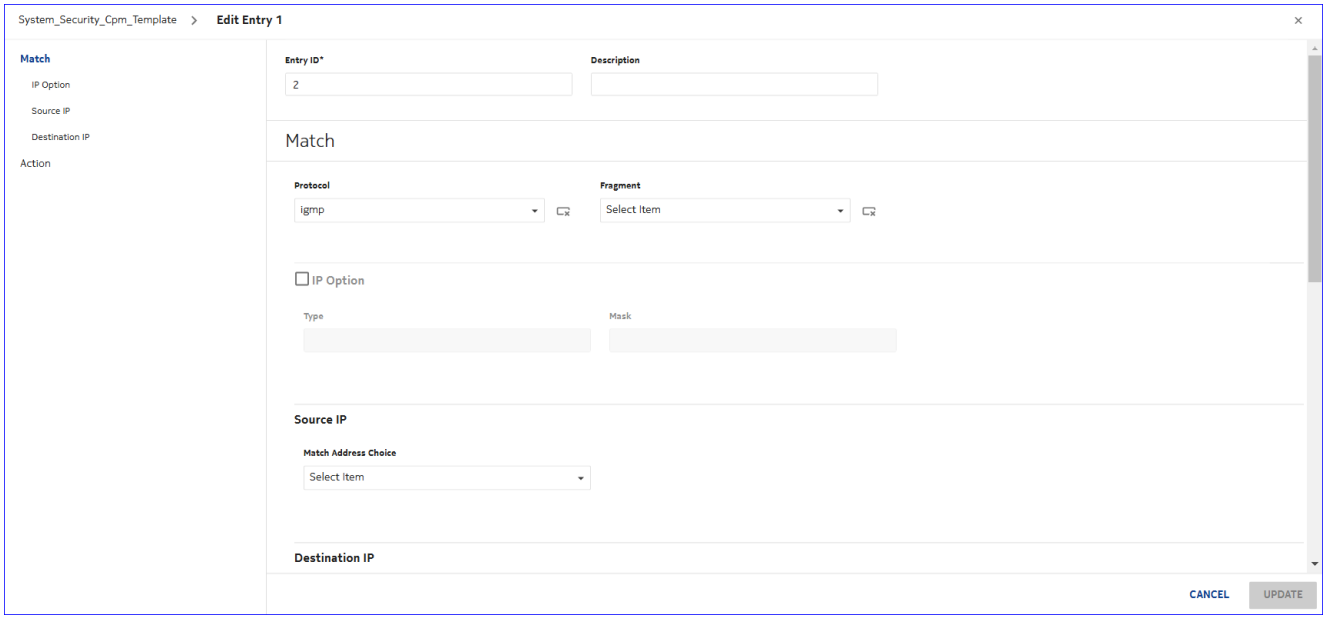


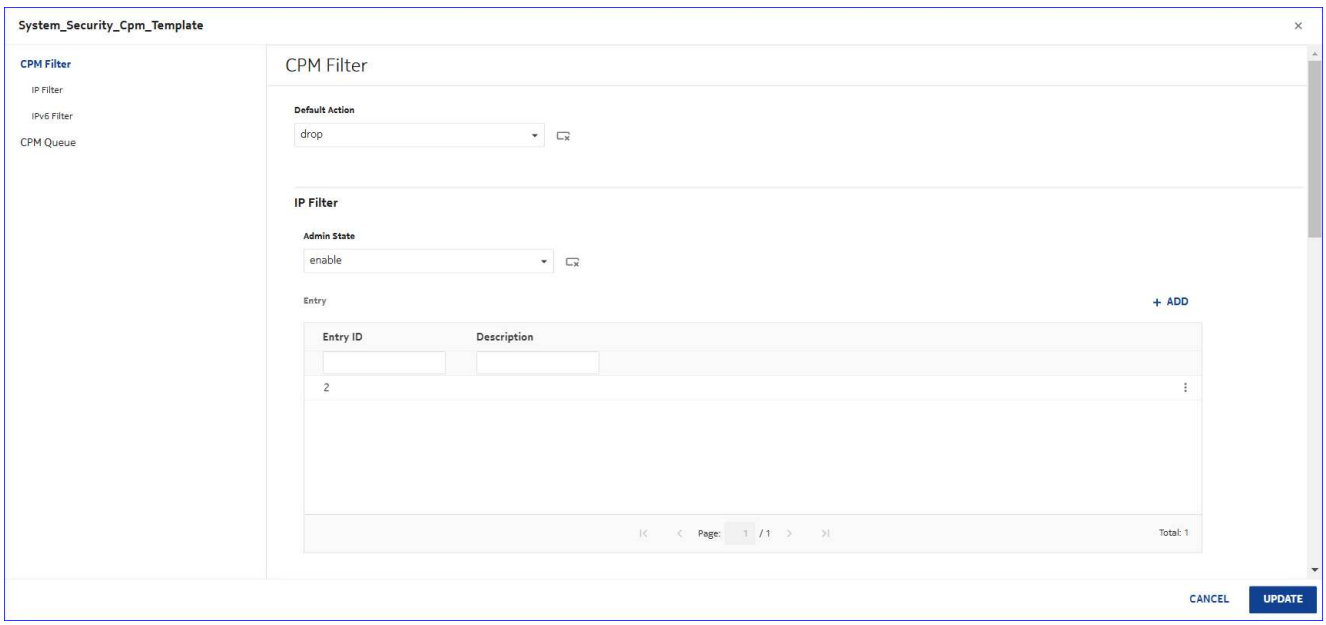
3

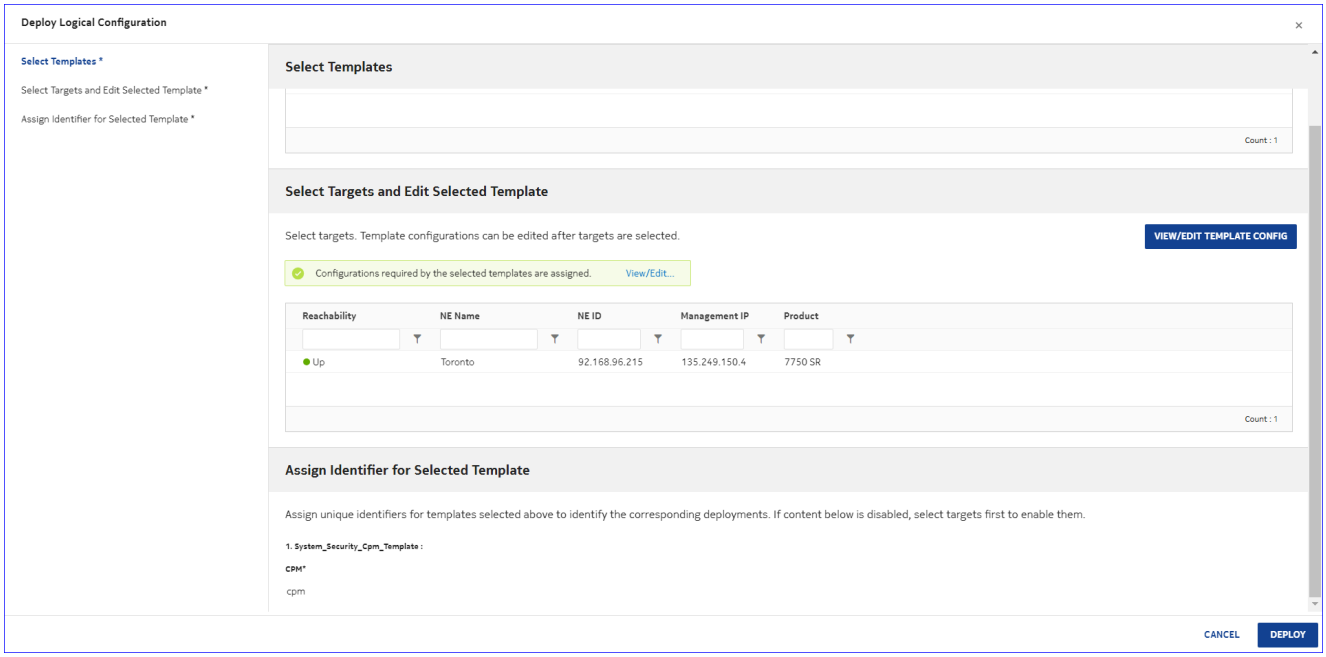
Create configuration deployments using the above configuration template.



Successful deployment:







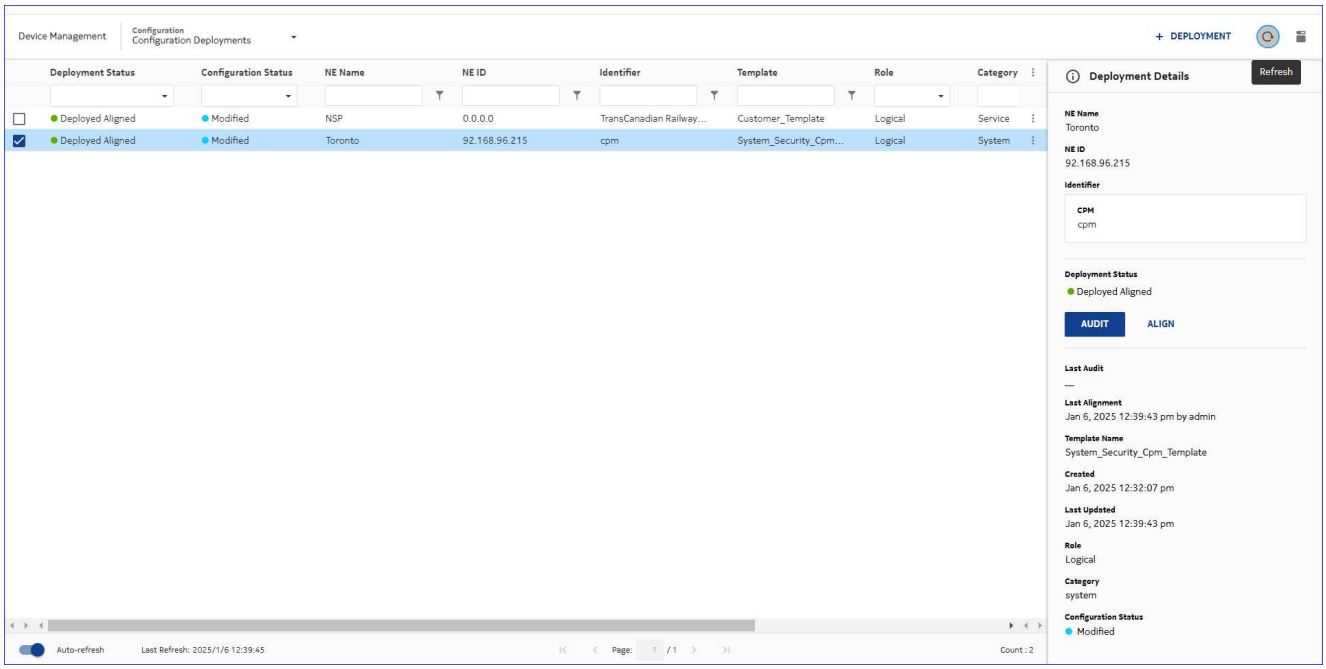


Figure 7-35 On Classic NE:

```
A:Toronto>config>sys>security>cpm-filter# info
----------------------------------------------
                default-action drop
                ip-filter
                    entry 2 create
                        action drop
                        match protocol 2
                        exit
                    exit
                    no shutdown
                exit
----------------------------------------------
```

Figure 7-36 On MD NE:

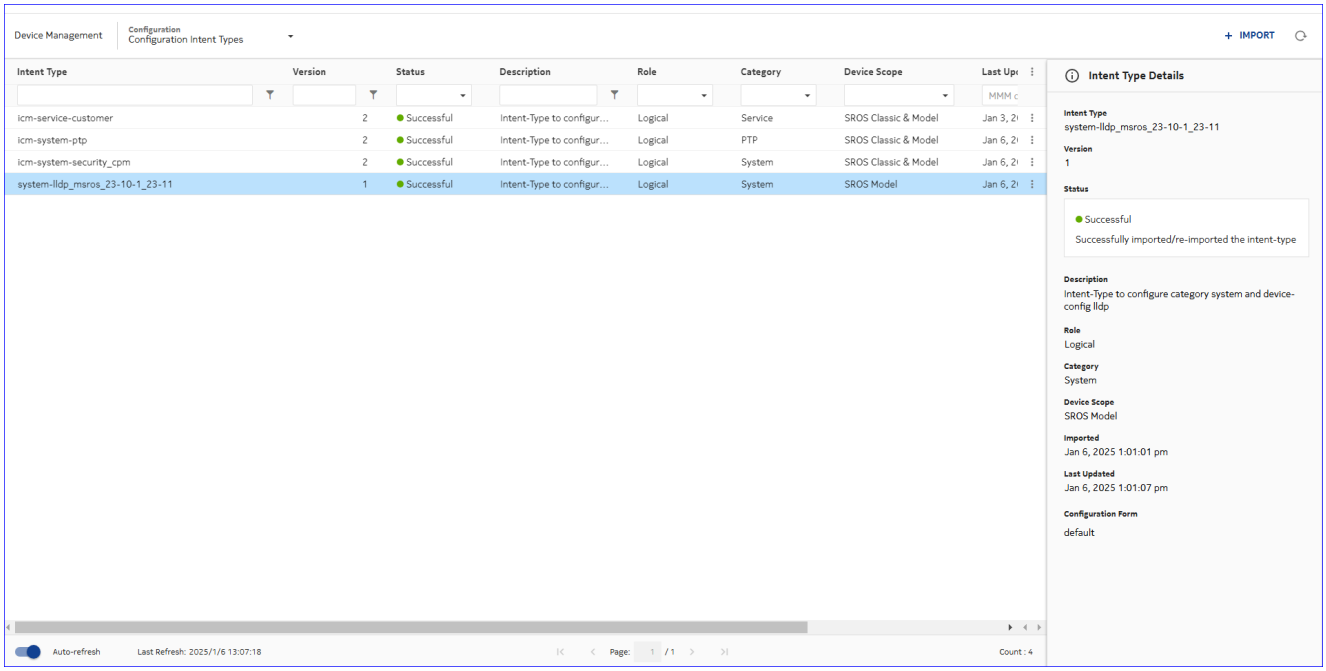
```
(pr)[/configure system security cpm-filter]
A:admin@Boston# info
    default-action drop
    ip-filter {
        admin-state enable
        entry 2 {
            match {
                protocol igmp
            }
        }
    }

(pr)[/configure system security cpm-filter]
```

END OF STEPS

7.14.2 To configure using system-lldp-msros intent type

1

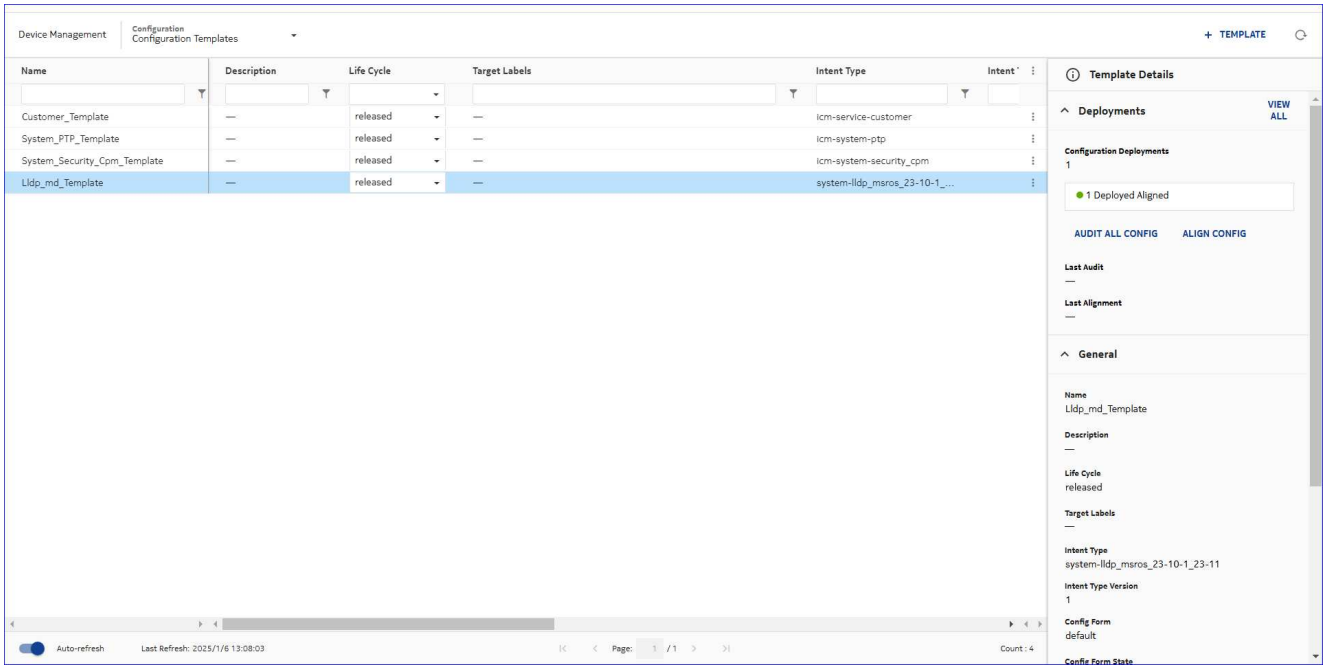
Import the intent type **system-lldp-msros** into **Device Management**, **Configuration Intent Types**.



2

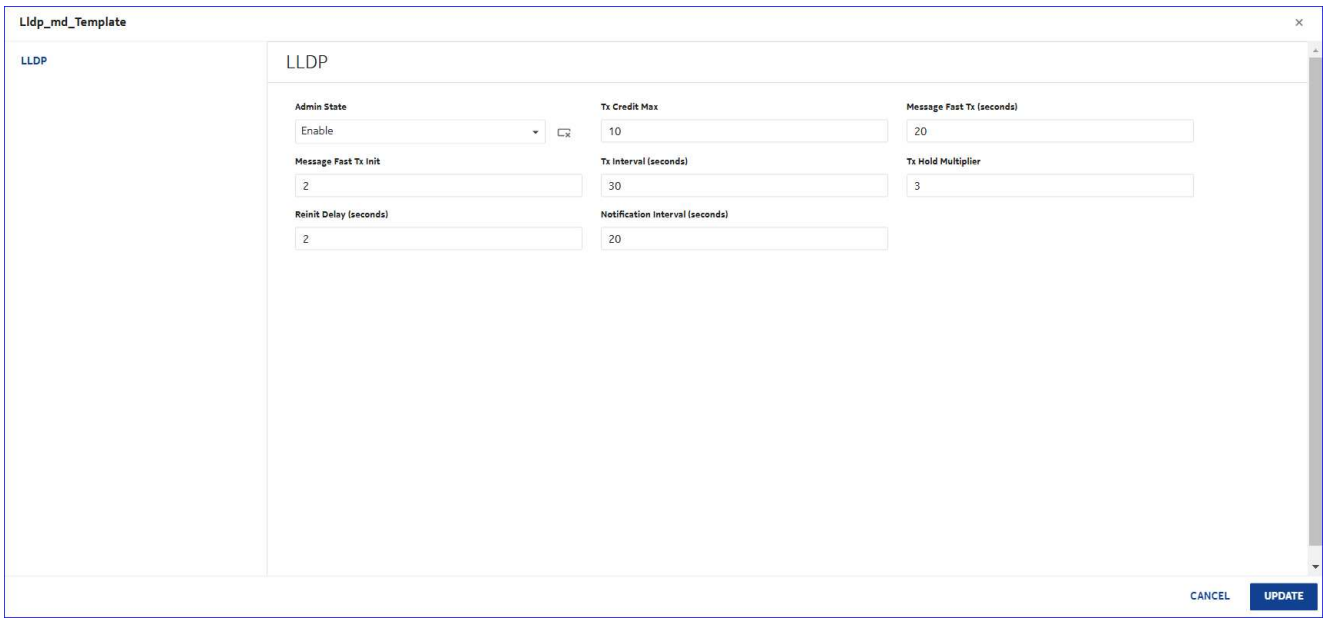
Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

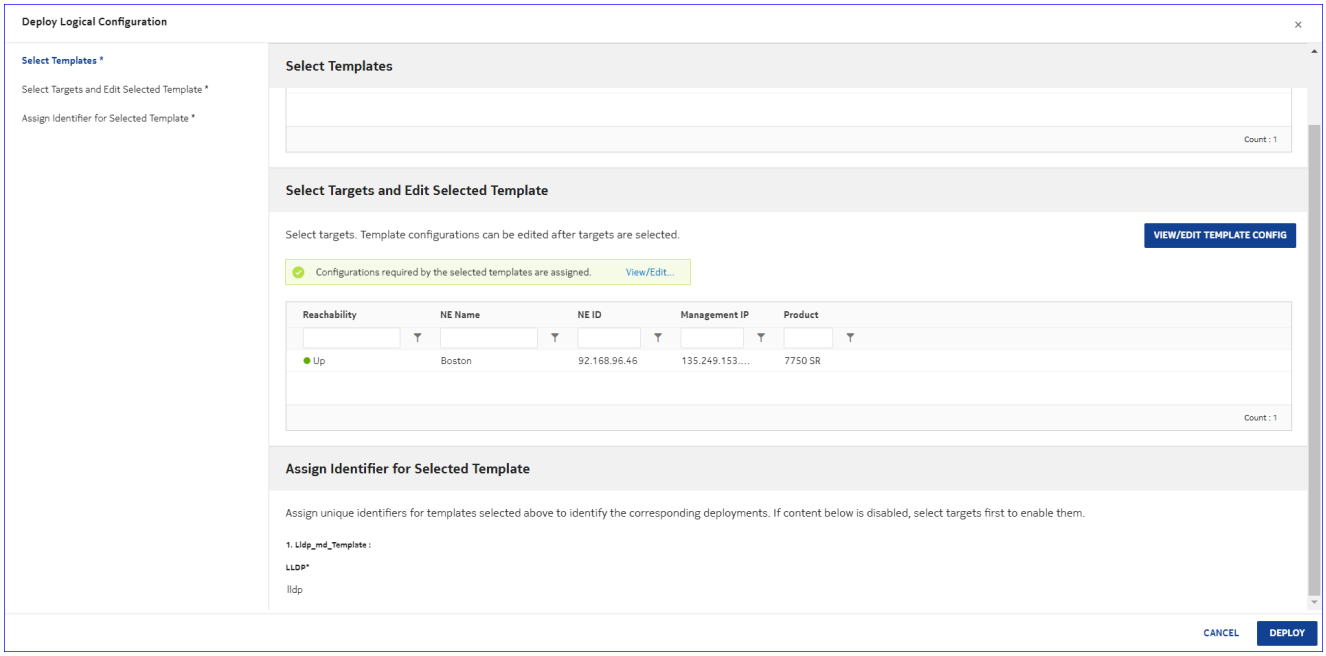
For example, the configuration template created below is named as **Lldp_md_Template**.



3

Create configuration deployments using the above configuration template.





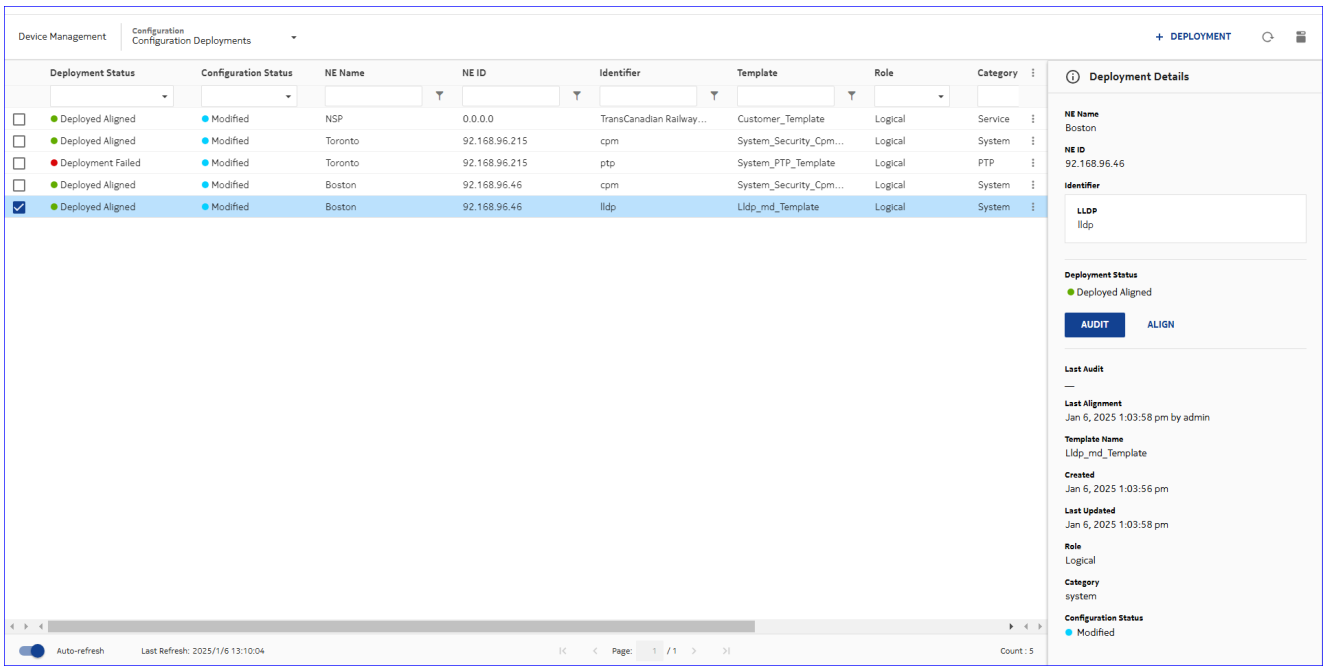
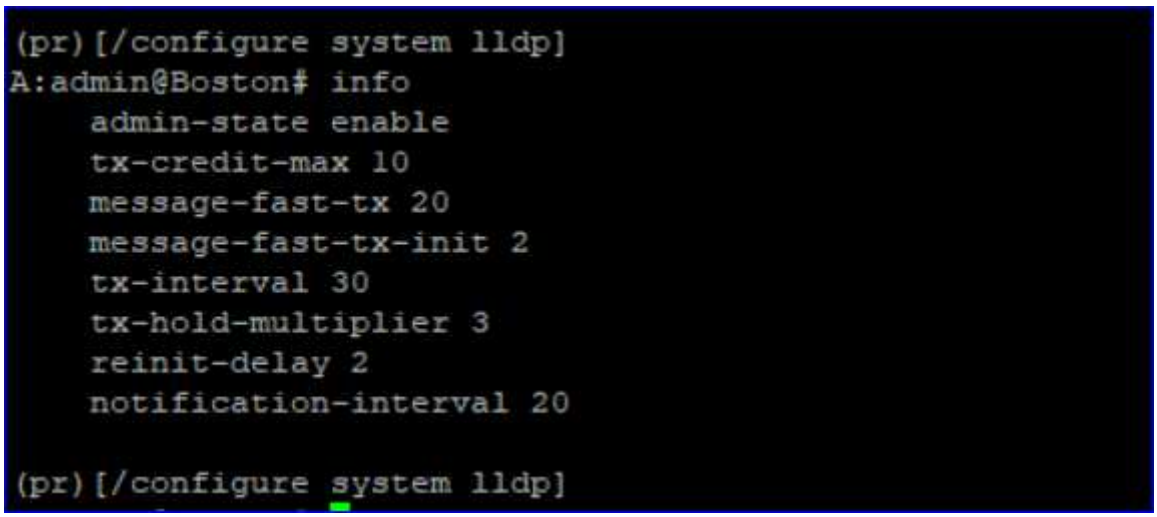


Figure 7-37 NE CLI after deployment:

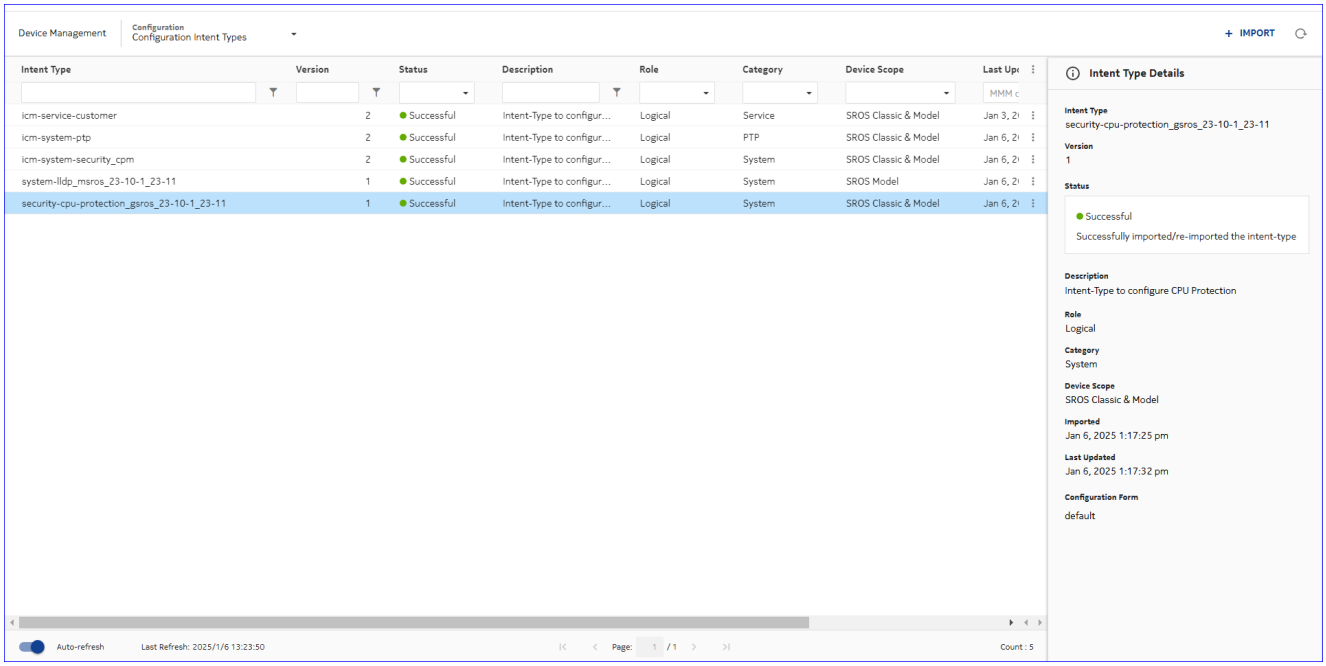


END OF STEPS

7.14.3 To configure using security-cpu-protection-gsros intent type

1

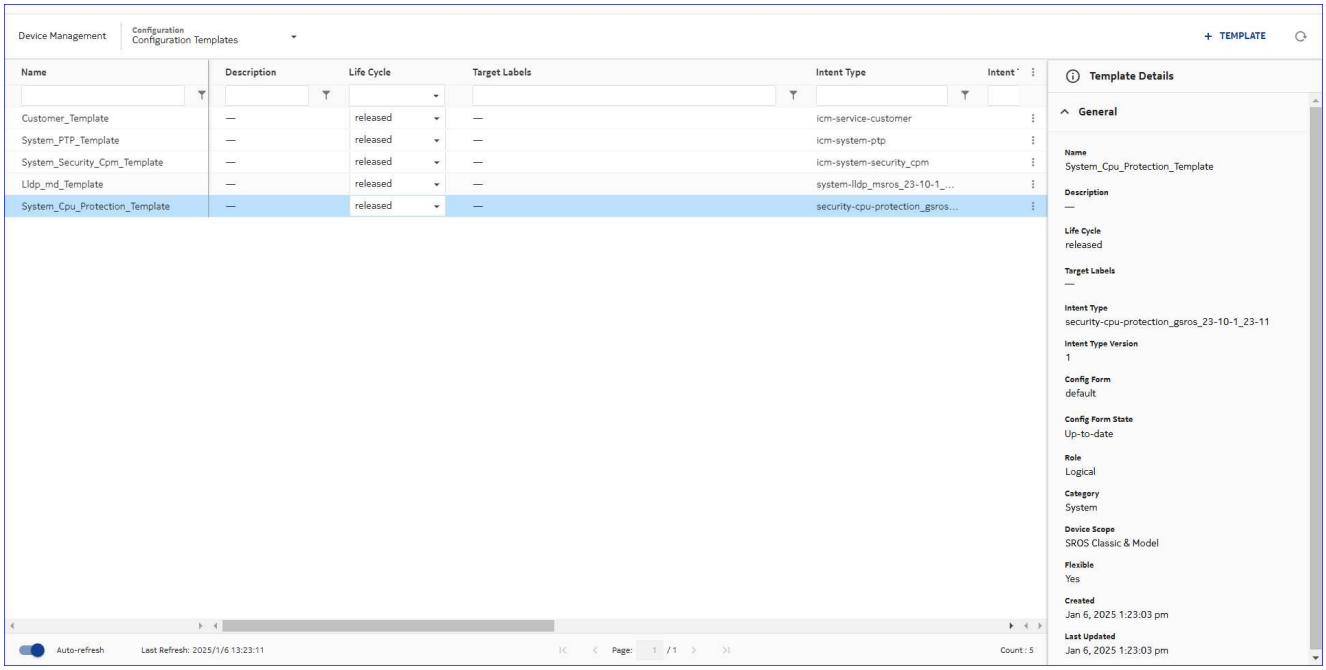
Import the intent type **security-cpu-protection-gsros** into **Device Management**, **Configuration Intent Types**.



2

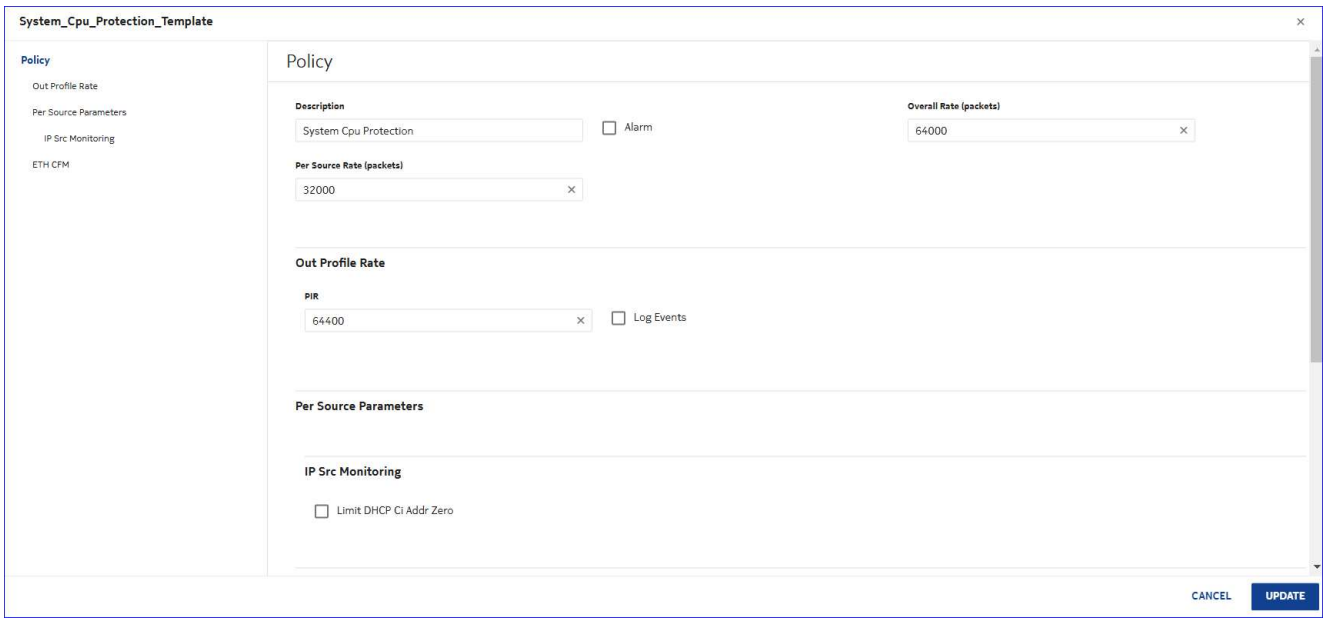
Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

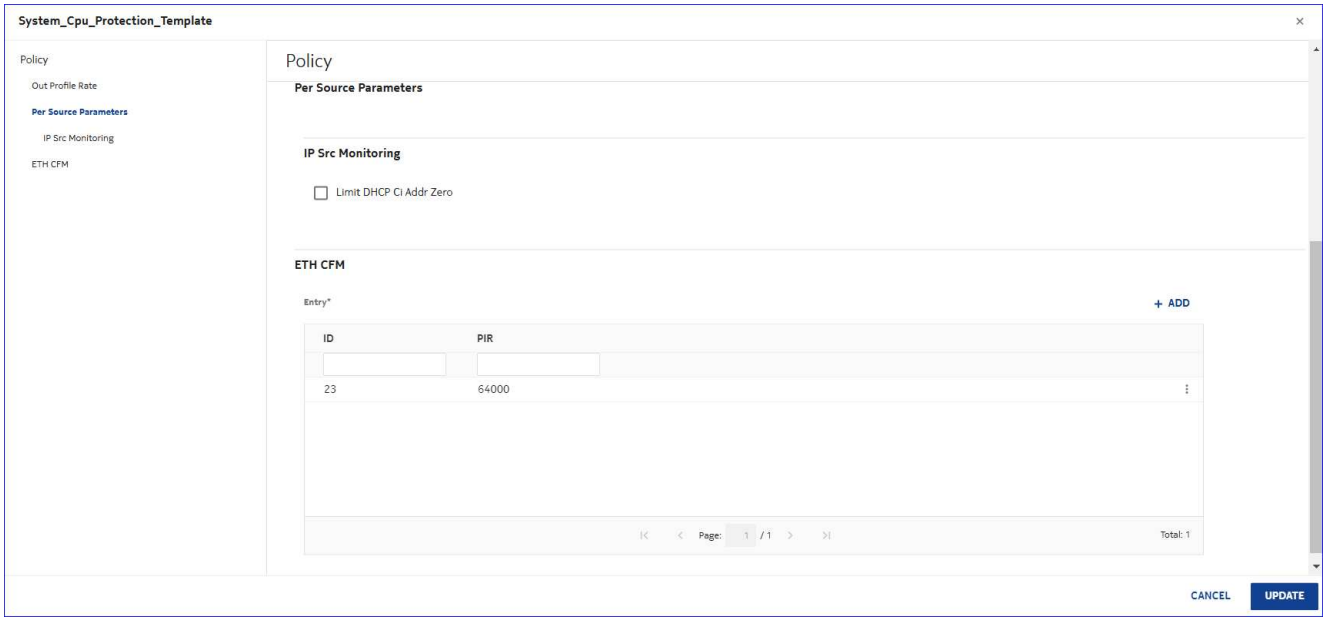
For example, the configuration template created below is named as **System_Cpu_Protection_Template**.

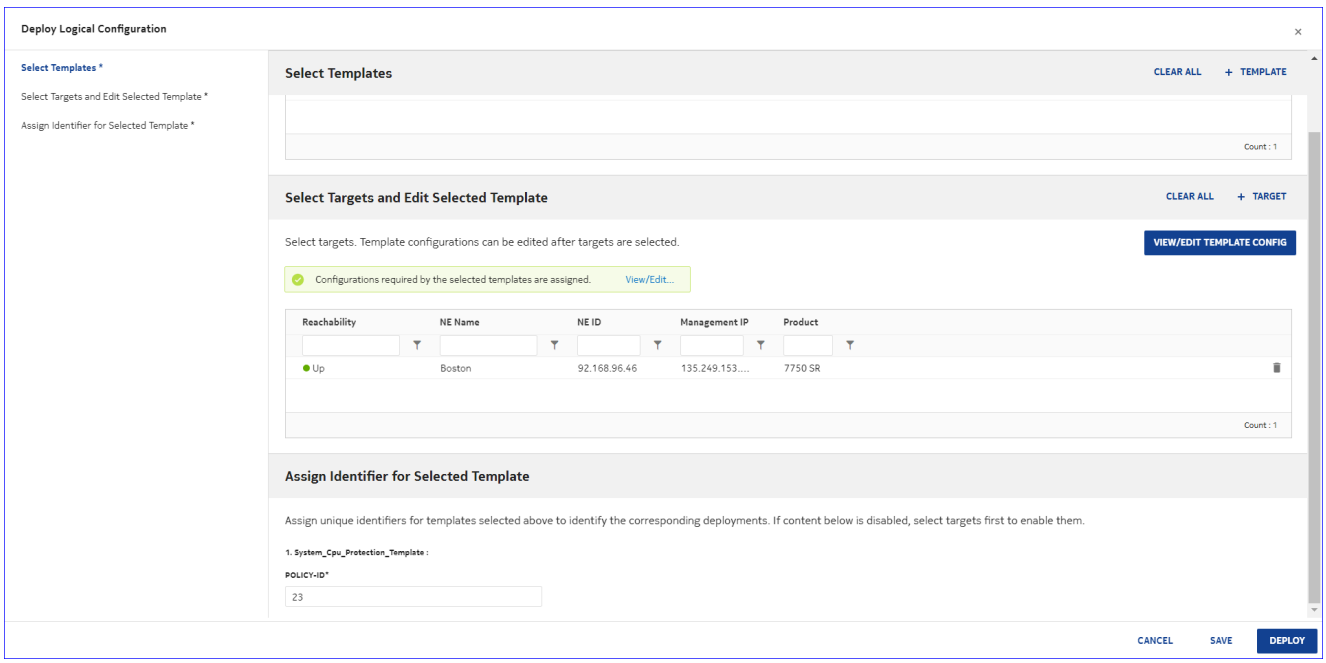


3

Create configuration deployments using the above configuration template.







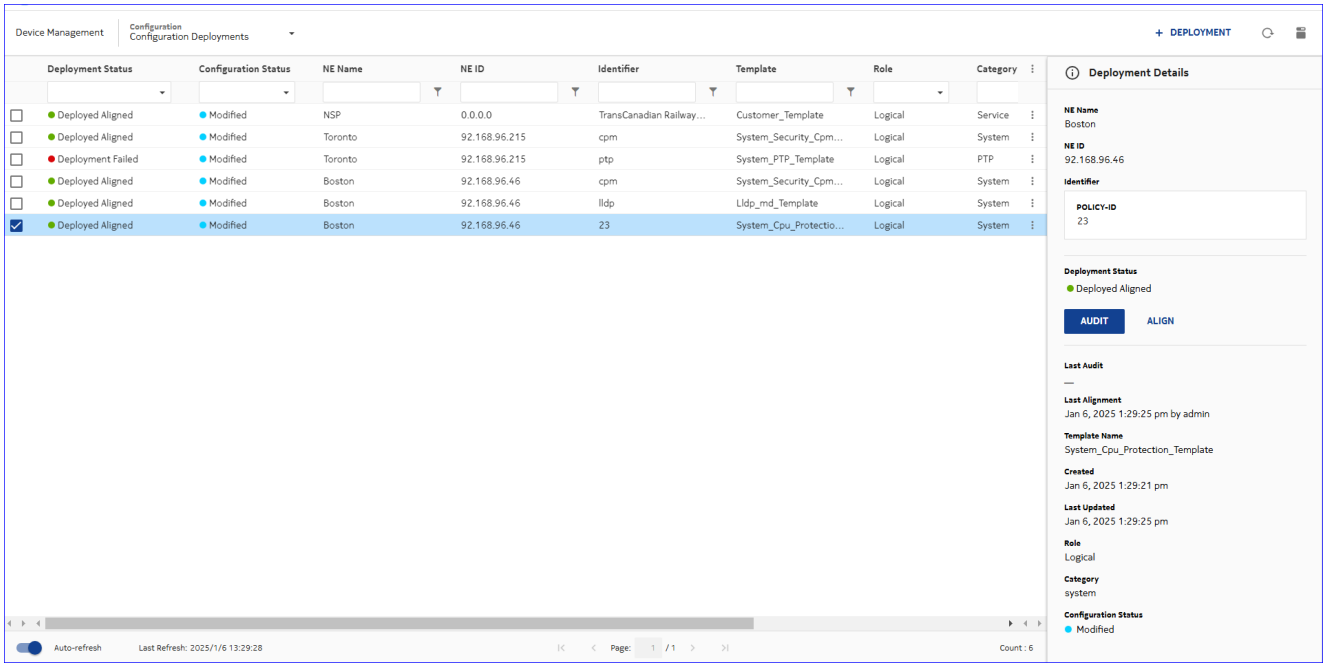


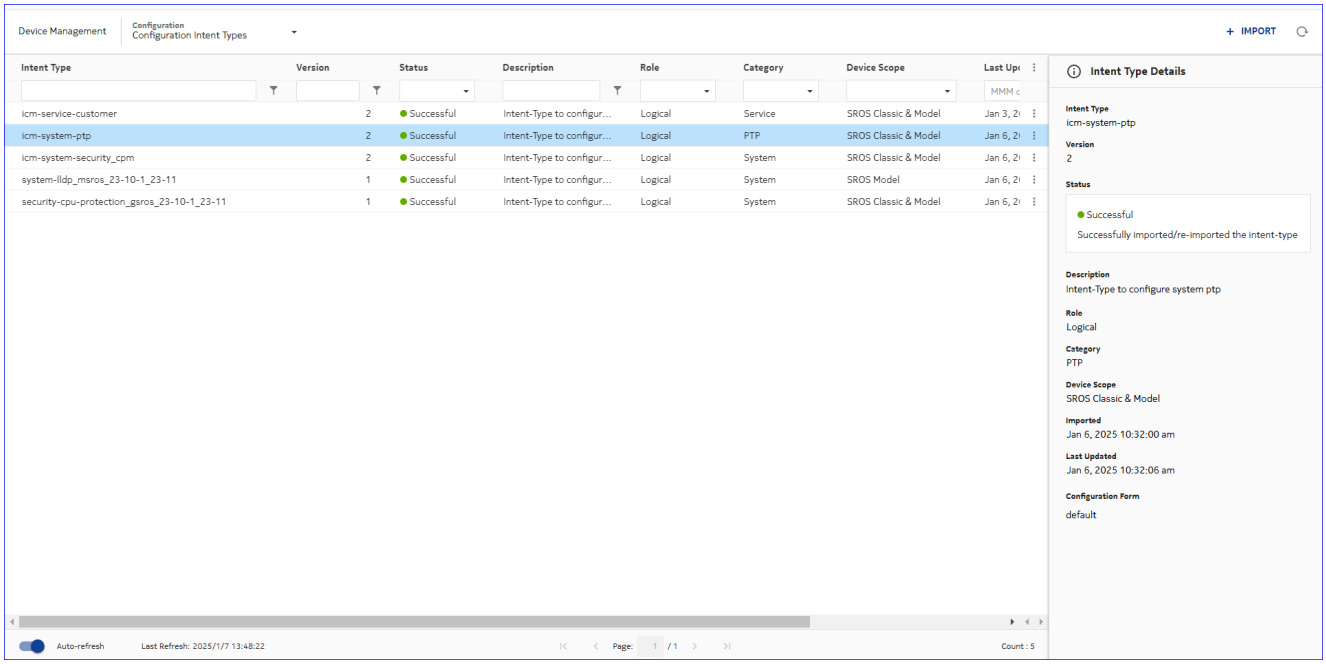
Figure 7-38 NE CLI after deployment:

END OF STEPS

7.14.4 To configure using icm-system-ptp intent type

1

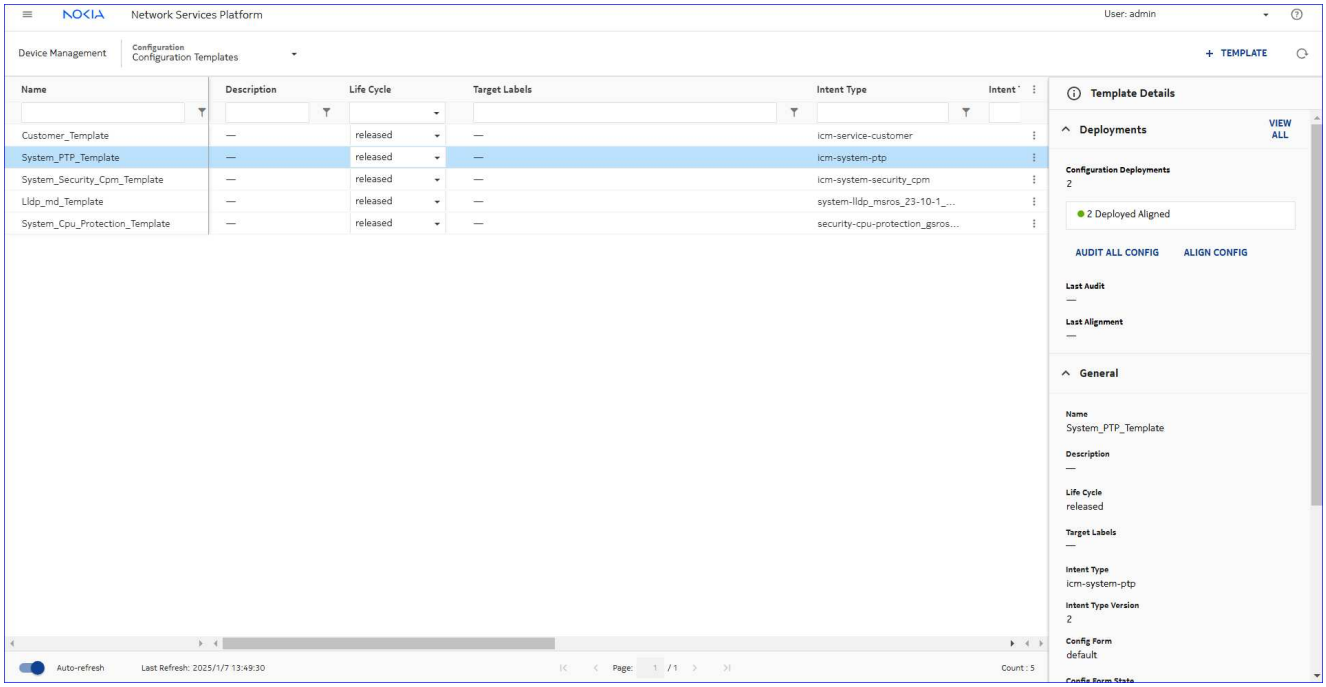
Import the intent type **icm-system-ptp** into **Device Management**, **Configuration Intent Types**.



2

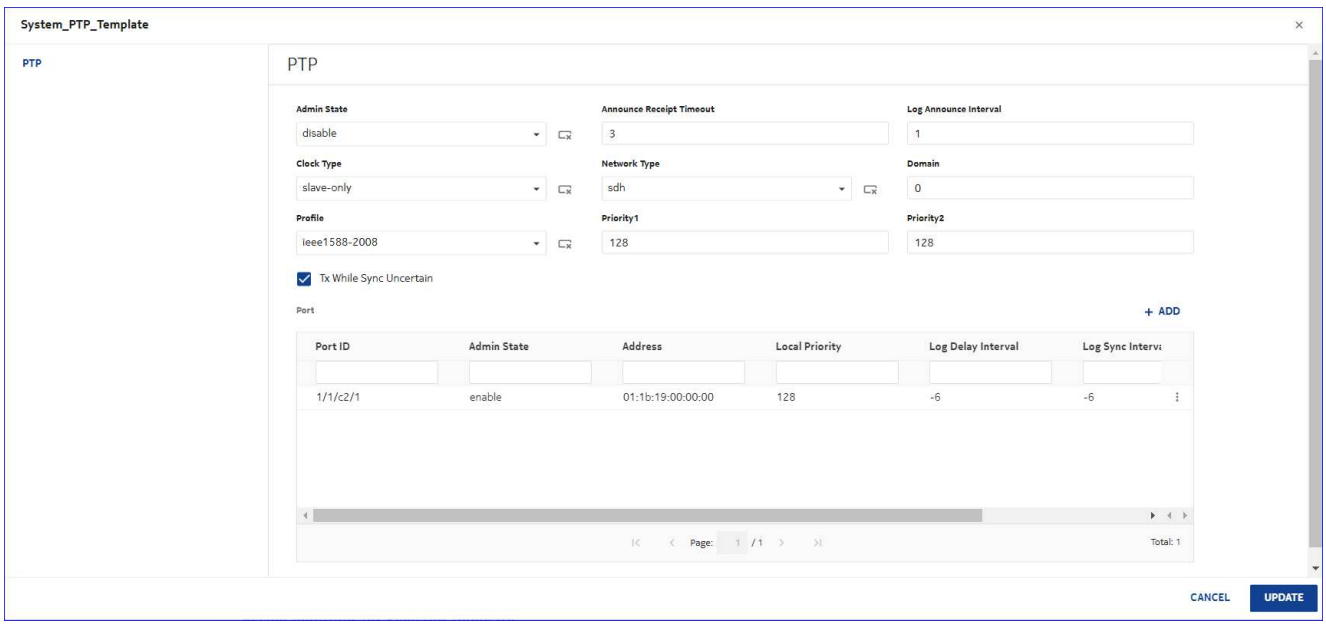
Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

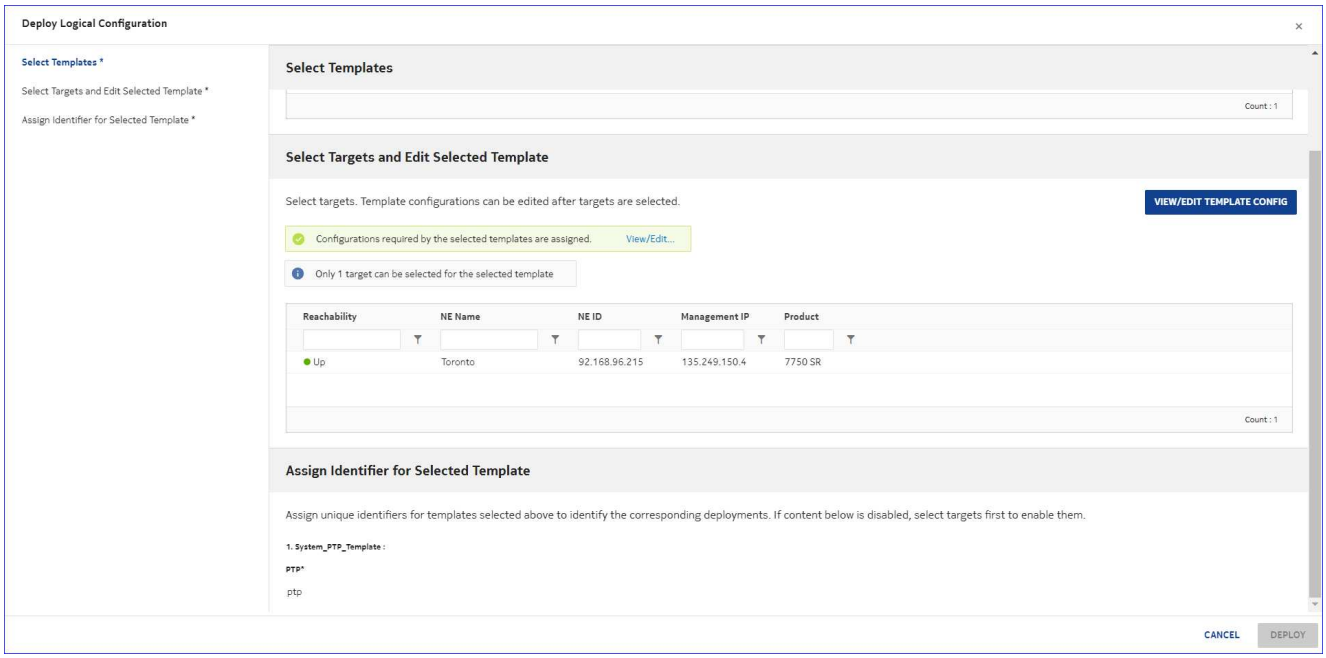
For example, the configuration template created below is named as **System_PTP_Template**.



3

Create configuration deployments using the above configuration template.





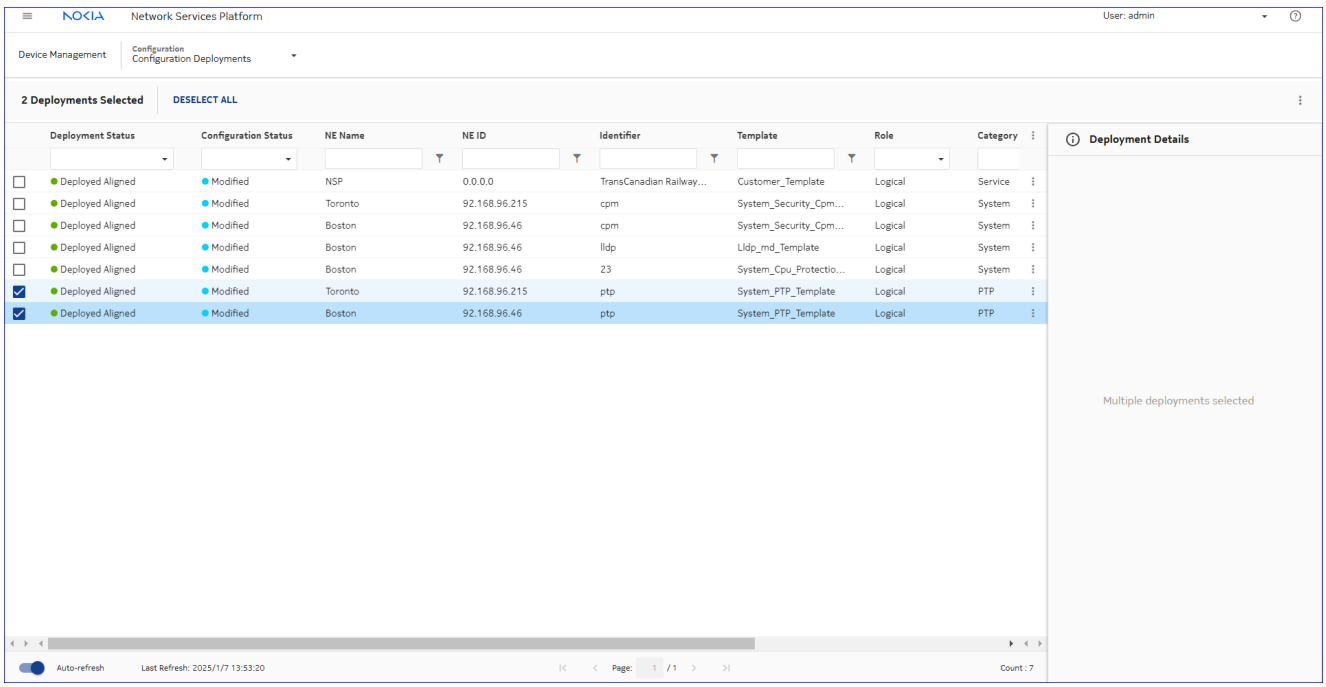


Figure 7-39 Classic NE CLI after deployment:

```
A:Toronto# configure system ptp
A:Toronto>config>system>ptp# info
----------------------------------------------
            shutdown
            profile ieee1588-2008
            port 1/1/c2/1 create
                no shutdown
            exit
----------------------------------------------
```

Figure 7-40 MD NE CLI after deployment:

```
A:admin@Boston# /configure system ptp

(pr)[/configure system ptp]
A:admin@Boston# info
    admin-state enable
    announce-receipt-timeout 4
    clock-type slave-only
    domain 1
    profile ieee1588-2008
    log-announce-interval 4
    network-type sonet
    priority1 23
    priority2 34
    tx-while-sync-uncertain true
    port 1/1/c1/3 {
        address 01:80:c2:00:00:0e
    }

(pr)[/configure system ptp]
```

END OF STEPS

8 UCC-26: NE Upgrades

8.1 Overview

8.1.1 Purpose

This chapter describes the process required to perform and manage NE software upgrades on both classic and model-driven SR nodes.

Testing for this chapter was completed on NSP Release 24.8 GA load and NFM-P Openstack setup.

The NE upgrades for this use case were done using the following nodes:

- 7750 SR-2se dual cpm
- 7250 IXR-R6dl dual cpm

The NE was upgraded from version 23.10 R2 to 24.7 R2 using both classic node (7750) and model-driven (7250).

8.1.2 Artifact bundles

Upgrade artifacts included in the NSP installation are shown below. All default artifacts are certified and cannot be modified.

The following node upgrade artifacts are included with the installation of the networkInfrastructureManagement-basicManagement feature pack:

- nsp-ne-upgrade-with-phases
- nsp-ne-upgrade

The **nsp-ne-upgrade-with-phases** is used for multi-phase of SR OS, SR OS 7210, SR OS 7705, SR Linux.

The **nsp-ne-upgrade** is used for single phase upgrade of SR OS, SR OS 7210, SR OS 7705, SR Linux.

Note: Nokia recommends using the **nsp-ne-upgrade-with-phases** operation type to upgrade a 7750 SR.

Phase	Workflow	Process

Pre-check	SR OS 7x50: • LSO_7x50_Pre_Checks • LSO_7x50_Upgrade_ Cleanup_Redundant_CPM • LSO_7x50_Upgrade_ Cleanup_Single_CPM	• 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 for md nodes • Checks for deprecated cards and MDAs on the node • Retrieves details of the target software image • Runs a cleanup of stale images on the /images/ folder is autoCleanup option is set to True
	SR OS 7210: • LSO_7210_PreChecks • LSO_7210_Upgrade_ Cleanup_Redundant_CPM • LSO_7210_Upgrade_ Cleanup_Single_CPM	
	SR OS 7705: • LSO_7705_PreChecks • LSO_7705_Upgrade_ Cleanup_Redundant_CPM • LSO_7705_Upgrade_ Cleanup_Single_CPM	
	SR Linux: • LSO_SRLinux_Pre_Checks	
Download	SR OS 7x50: • LSO_7x50_Download	• Reads and processes the BOF • Creates a directory on the NE and transfers the image files • Confirms the file integrity and sends a success message
	SR OS 7210: • LSO_7210_Download	
	SR OS 7705: • LSO_7705_Download	
	SR Linux: • LSO_SRLinux_Download	

Activate	SR OS 7x50: • LSO_7x50_Activate • LSO_7x50_Upgrade_ Rollback_ActivatePhase	• Saves the updated configuration on the NE and performs an admin save • Updates the Bof • Synchronizes the CPM • Resets redundancy settings as needed and sends a success message
	SR OS 7210: • LSO_7210_Activate • LSO_7210_Upgrade_ Rollback_ActivatePhase	
	SR OS 7705: • LSO_7705_Activate • LSO_7705_Upgrade_ Rollback_ActivatePhase	
	SR Linux: • LSO_SRLinux_Activate	
Reboot	SR OS 7x50: • LSO_7x50_Reboot • LSO_7x50_ISSU • LSO_7x50_Upgrade_ Rollback_RebootPhase	• Checks BOF instructions for reboot and CPM redundancy requirements • Processes redundancy • Triggers a reboot and checks the device version • Sends a success message
	SR OS 7210: • LSO_7210_Reboot • LSO_7210_ISSU • LSO_7210_Upgrade_ Rollback_RebootPhase	
	SR OS 7705: • LSO_7705_Reboot • LSO_7705_ISSU • LSO_7705_Upgrade_ Rollback_RebootPhase	
	SR Linux: • LSO_SRLinux_Reboot	

8.1.3 Contents

Preparation

8.2 Prerequisites

8.2.1 Network configuration prerequisites

Before NE upgrades can be configured and managed in NSP, the network configuration prerequisites must be met.

Prerequisite	Documentation reference	Notes
Mandatory for NE Upgrades		
Netconf/SNMP provisioning: enable NETCONF and SNMP protocols on all devices	For more information about SNMP and NETCONF with SR OS, see SNMP and NETCONF in the *SR OS 24.3 R1 System Management Guide*.	—
NSP installation	Pathway for NSP system installation in the *NSP Installation and Upgrade Guide*	Include the following in your deployment: Feature packs: • networkInfrastructureManagement-basicManagement
Device discovery	Pathway for device discovery in the *NSP Classic Management User Guide* How do I discover devices? in the *NSP Device Management Guide* Nokia Developer Portal for information about FTP mediation policy creation using API.	—
Check *SR OS Software Release Notes*	Check the *SR OS Software Release Notes* for the node type and version you are upgrading to.	—

8.3 Pre-upgrade checks

8.3.1 Node pre-checks

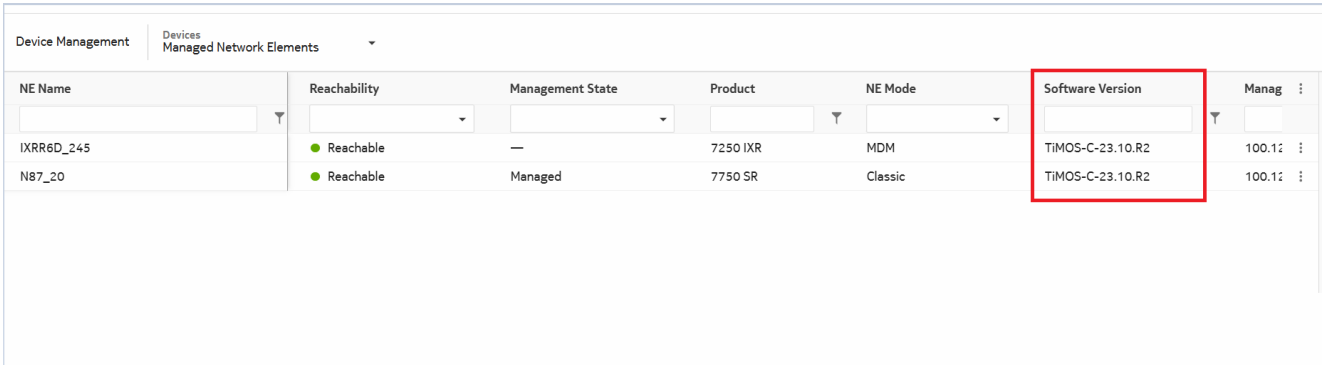
Users can run some show commands on the routers to compare with the node post-upgrade.

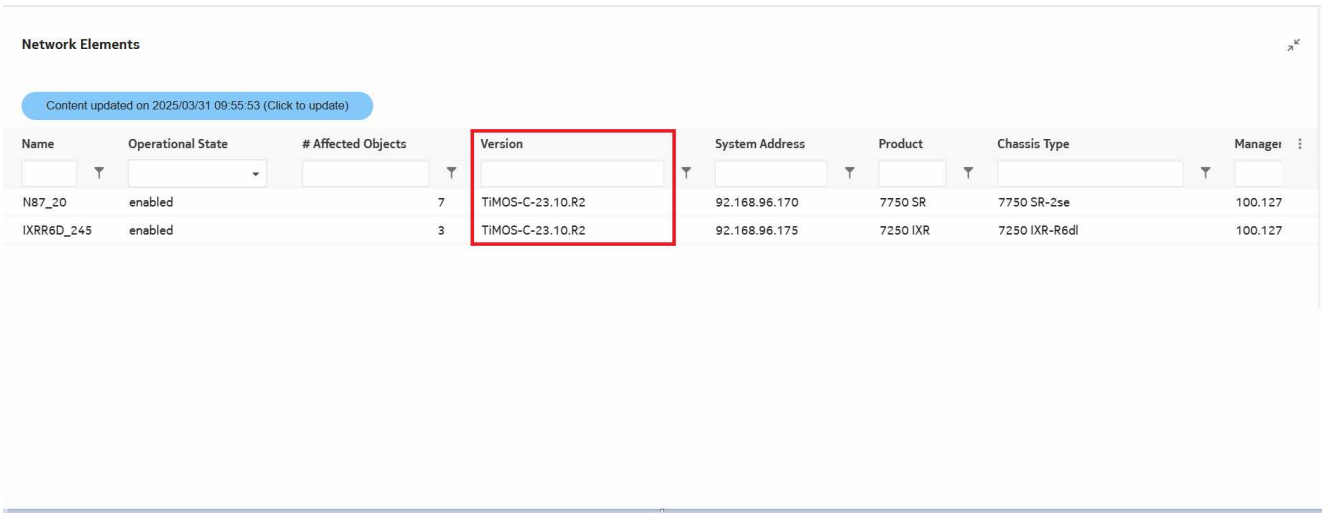
The following is an example of suggested commands users can run on a node before an upgrade. Users can run any additional commands needed. Save the output in a file for comparison post-upgrade.

```
show card
show chassis
show mda
show version
show bof
show service service-using
show service sdp-using
show oam-pm tests
```

```
show system lldp neighbor
show router interface
show router rsvp neighbor
show router ospf neighbor
show system netconf connection
show system grpc connection
show port
show system information
```

Check node version in the **Device Management and Network Health** dashboard.





```
[/]
A:admin@IXRR6D_245# show version
TiMOS-C-23.10.R2 cpm/x86hops64 Nokia 7250 IXR Copyright (c) 2000-2023 Nokia.
All rights reserved. All use subject to applicable license agreements.
Built on Mon Dec 11 23:45:58 UTC 2023 by builder in /builds/2310B/R2/panos/main/sros

[/]
A:admin@IXRR6D_245#
```

8.3.2 NSP pre-configs and checks

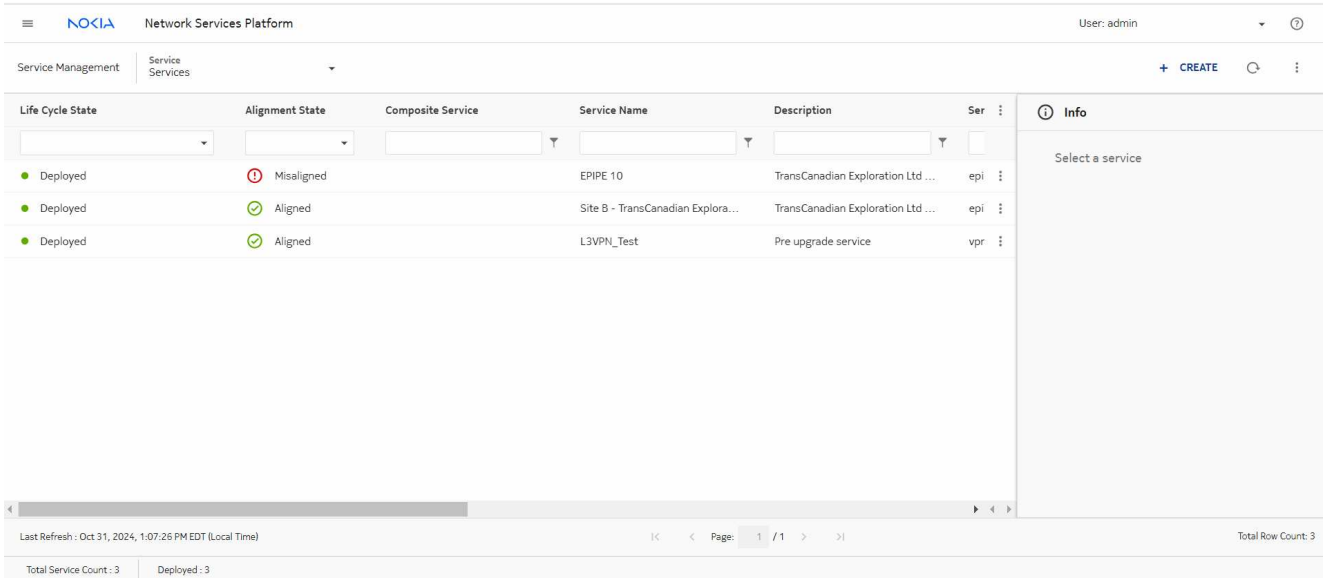
See the following for a list of services and checks:

Service Management

The following is a created L3VPN service through Service Management using intents and an associated brownfield epipe service with an intent.

```
B:admin@IXRR6D_245# show service service-using


===============================================================================

Services

===============================================================================

ServiceId    Type      Adm  Opr  CustomerId Service Name

-------------------------------------------------------------------------------

10           Epipe     Up   Up   13         Site B - TransCanadian
Exploration*

100          VPRN      Up   Up   12         L3VPN_Test

-------------------------------------------------------------------------------

Matching Services : 2

-------------------------------------------------------------------------------
```

```
================================================================================

* indicates that the corresponding row element may have been truncated.


[/]

B:admin@IXRR6D_245#
```



ICM

The following objects were configured through ICM:

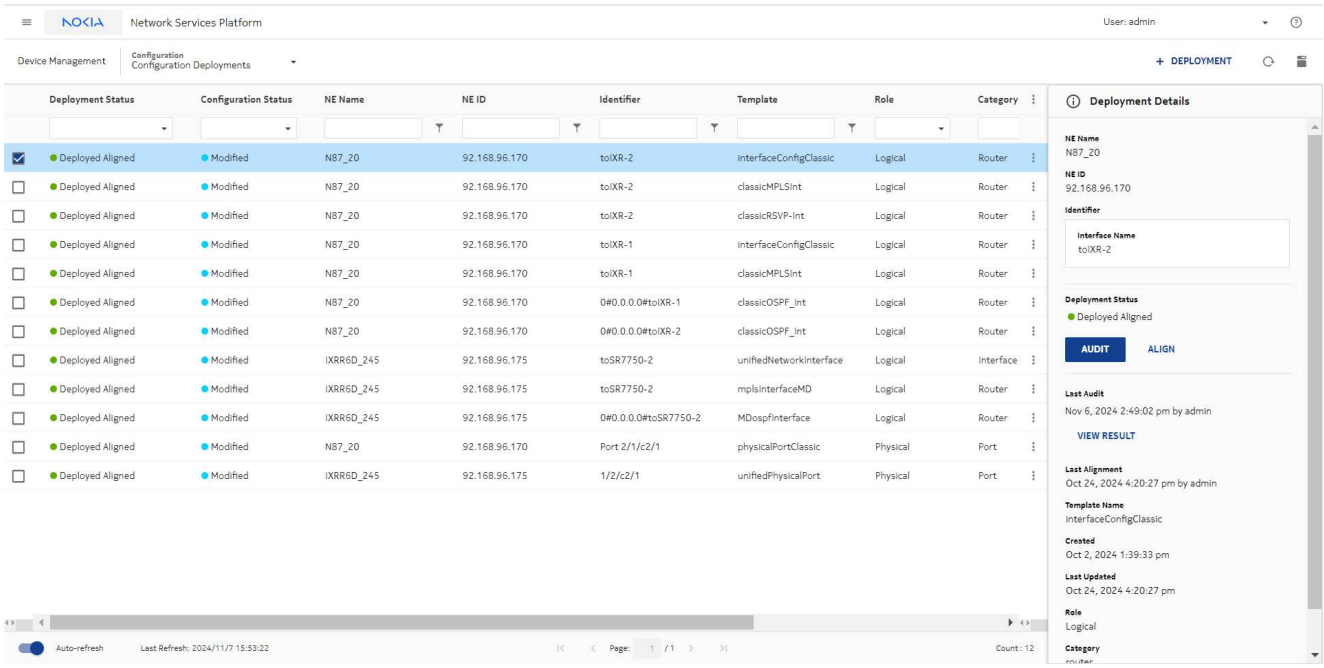
- Classic 7750 Node - using device specific intents
  - Logical router interface
  - Logical router mpls interface
  - Logical router rsvp interface
  - Logical ospf interface

  MD Node IXR - using md device specific intents, except for router interface which was not supported on IXR
  - Logical router interface
  - Logical router mpls interface

- Logical ospf interface

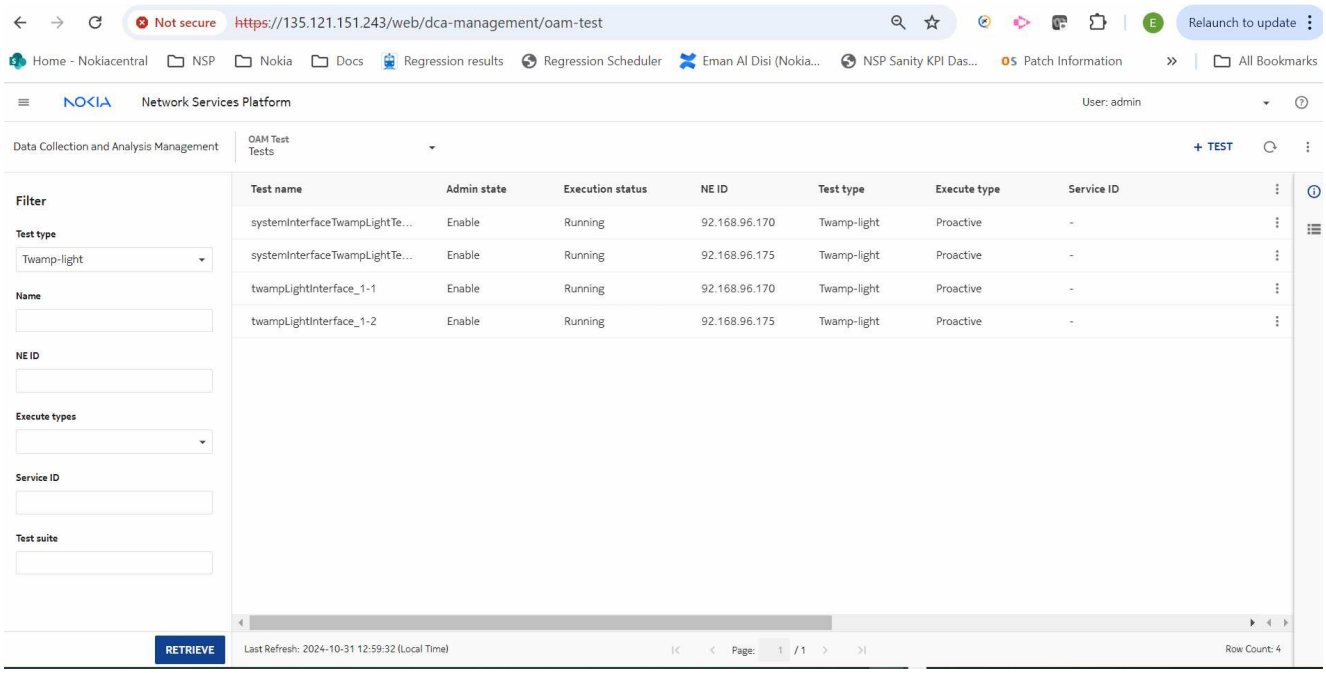
Associate to network (Brownfield Discovery)

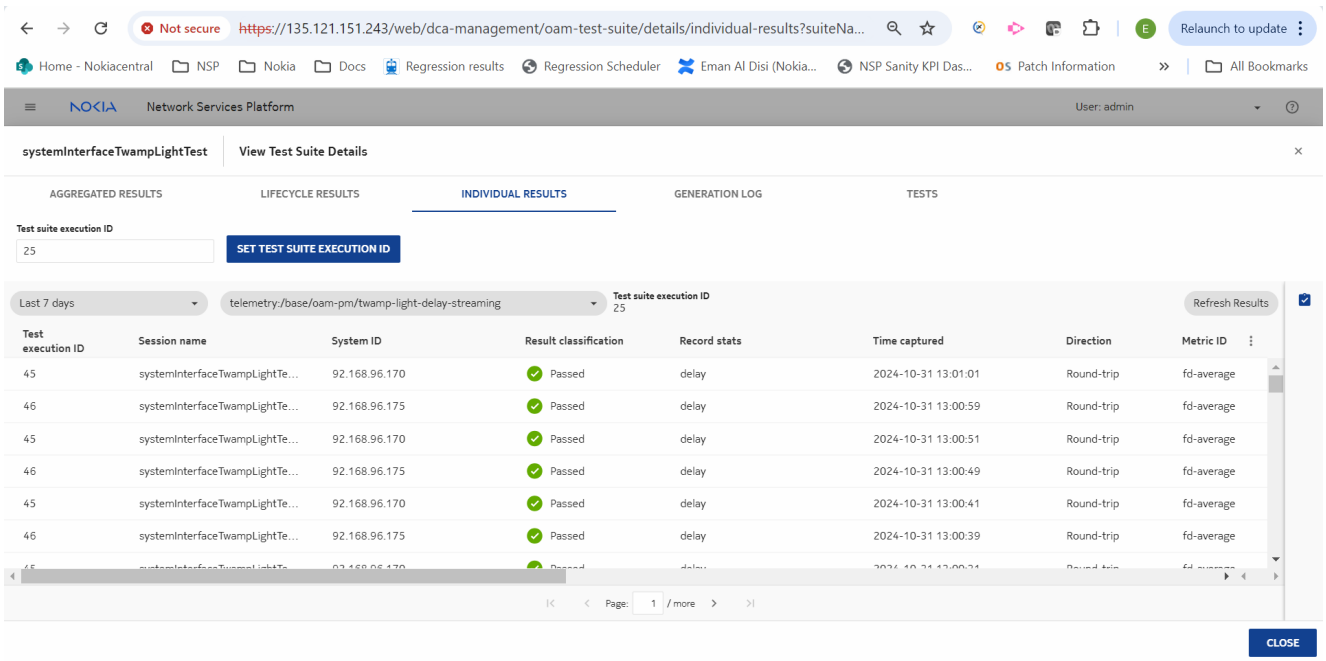
- Classic Physical port
- MD Physical port

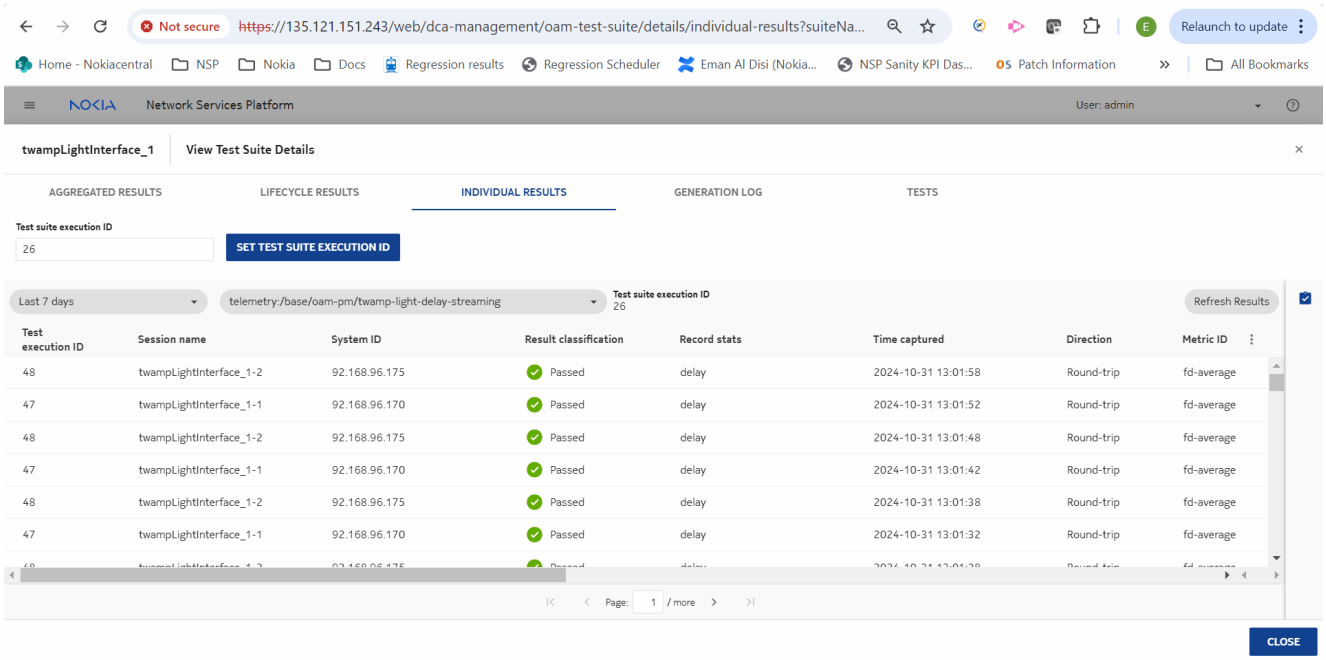


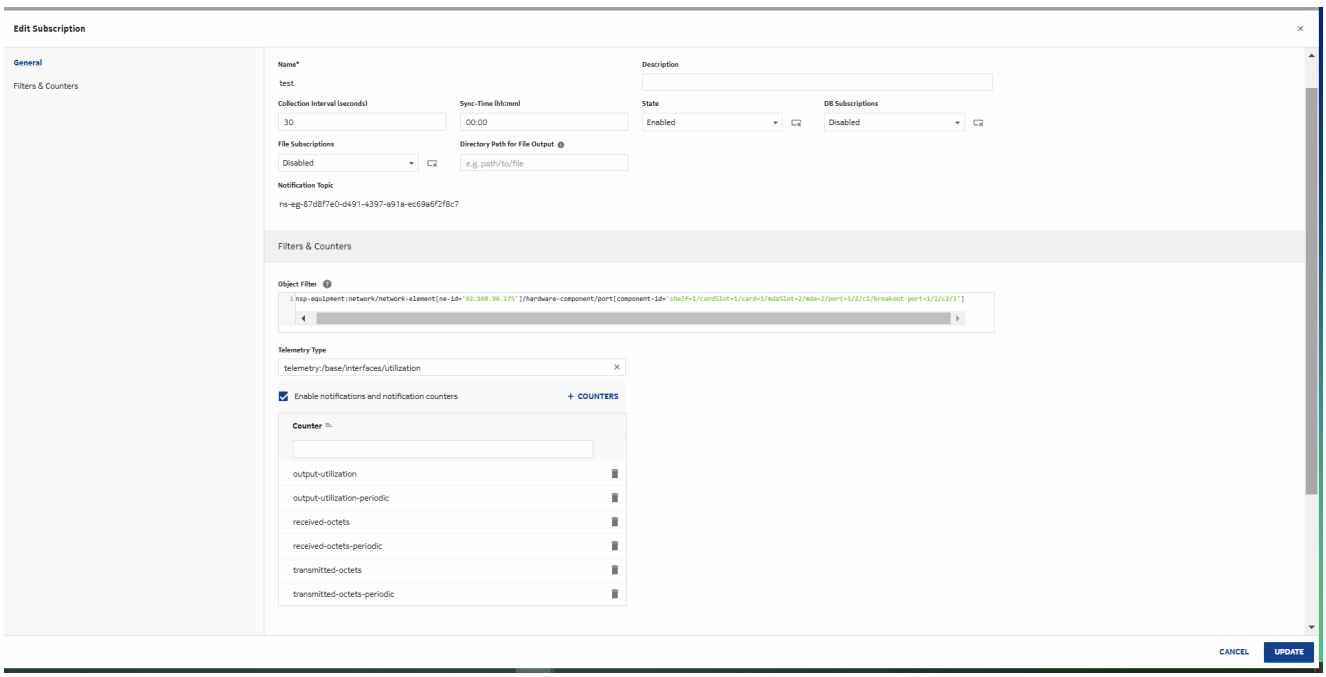
OAM/Telemetry

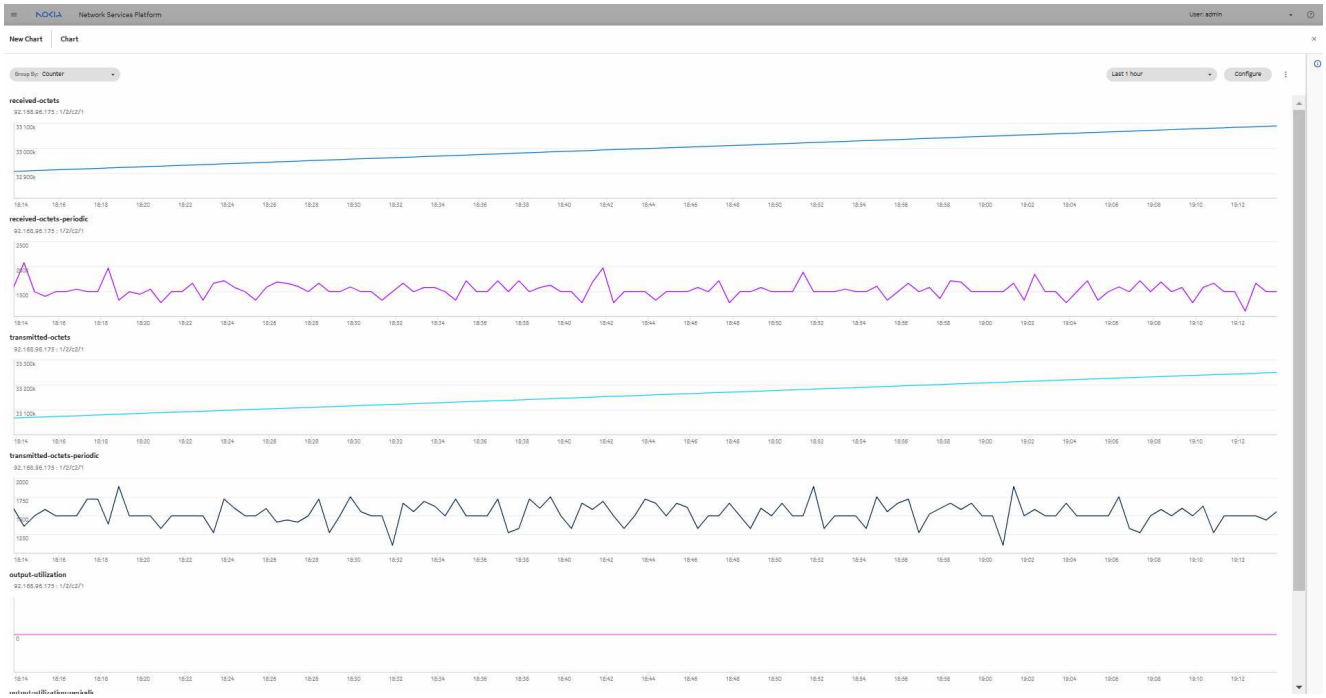
Created Twamp light interface tests on both nodes:











8.4 Download and upload NE software

8.4.1 Steps

1

NE software images can be downloaded from the Nokia Support Portal for the NE type and release.

2

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

7750 SR (Service Router) > 24.7 > R2 > Nokia-7750_SR-TiMOS-24.7.R2

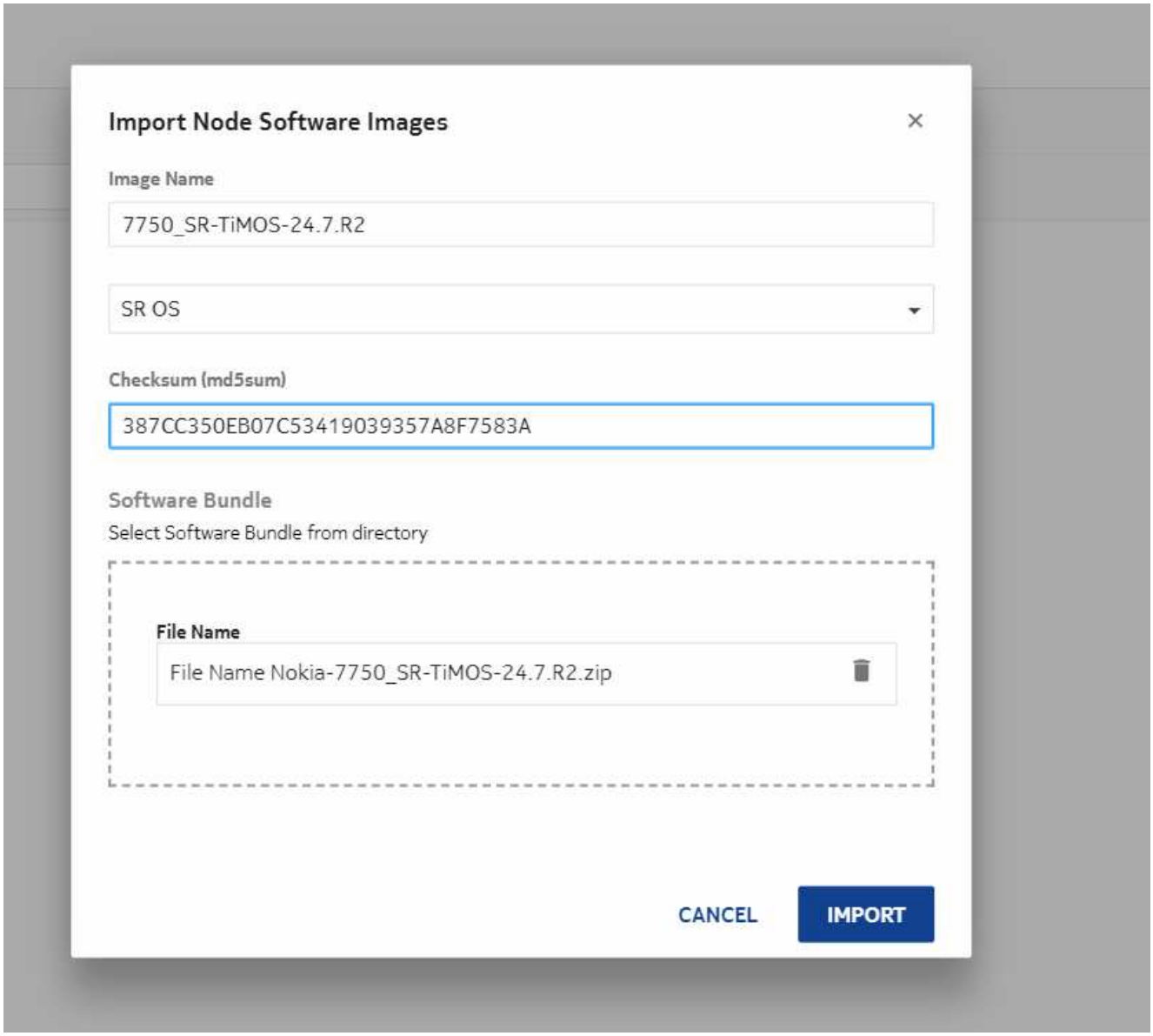
When using:	Browserdownload	Please verify the file(s) you have downloaded by generating either an MD5 hash value or an SHA-256 hash value and compare your generated values with the values provided here:
File	Size	Hash Values
Nokia-7750_SR-TiMOS-24.7.R2.zip	2,422,840,510	MD5: 387cc350eb07c53419039357a8f7583a SHA-256: 502c00db5ab3b4eed06040c1cbdd7bfdf603572a20939d745b0f92a61129e6a6

3

Import the image to NSP:

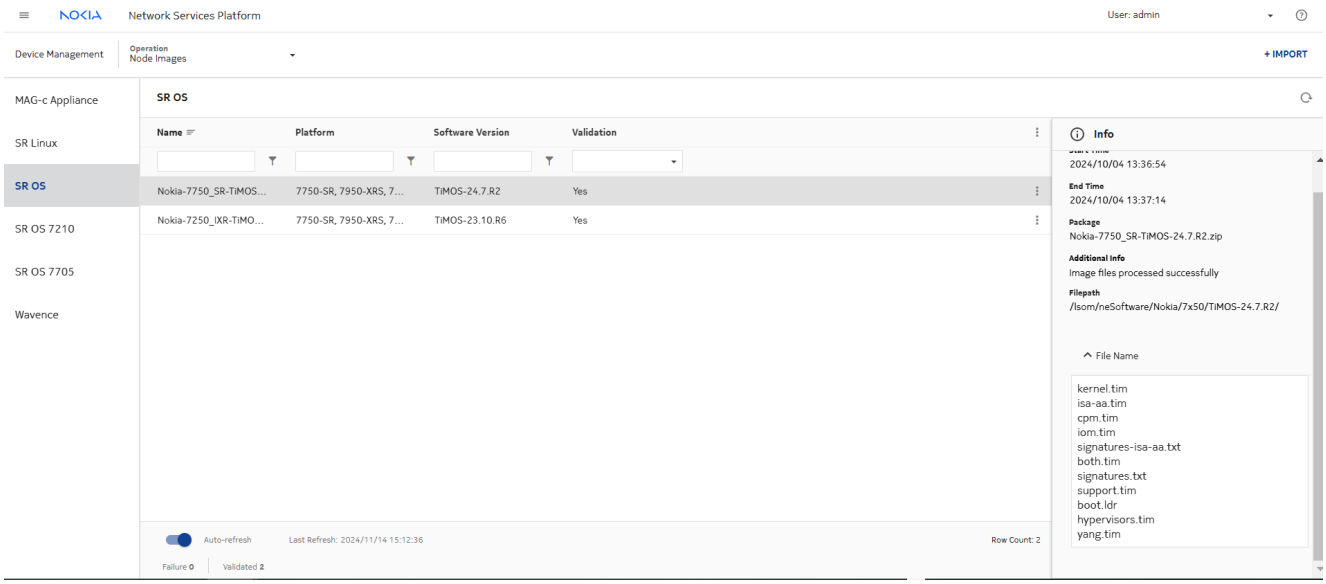
Note: For 7x50 image import, the software bundle name and contents must not be modified after downloading it from the Nokia support page.

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.



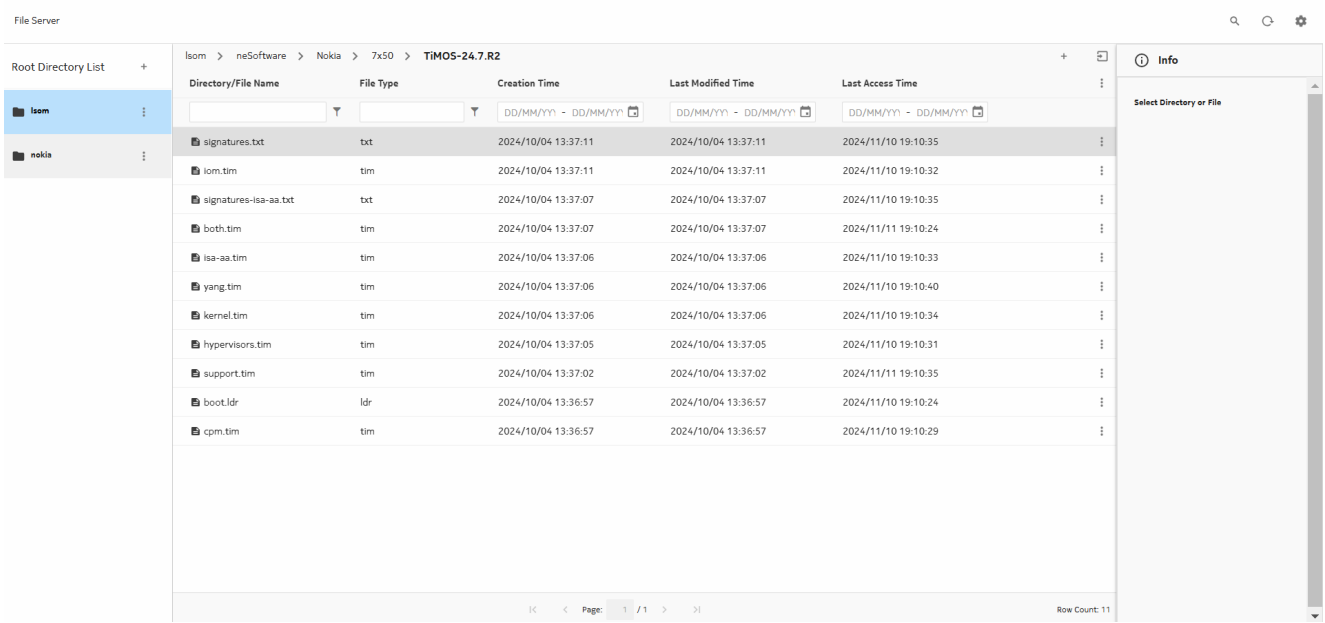
4

Images can be viewed from **Node Images**, with the content displayed in the info panel on the right.



5

Images can also be viewed from the **File Server** application.



END OF STEPS

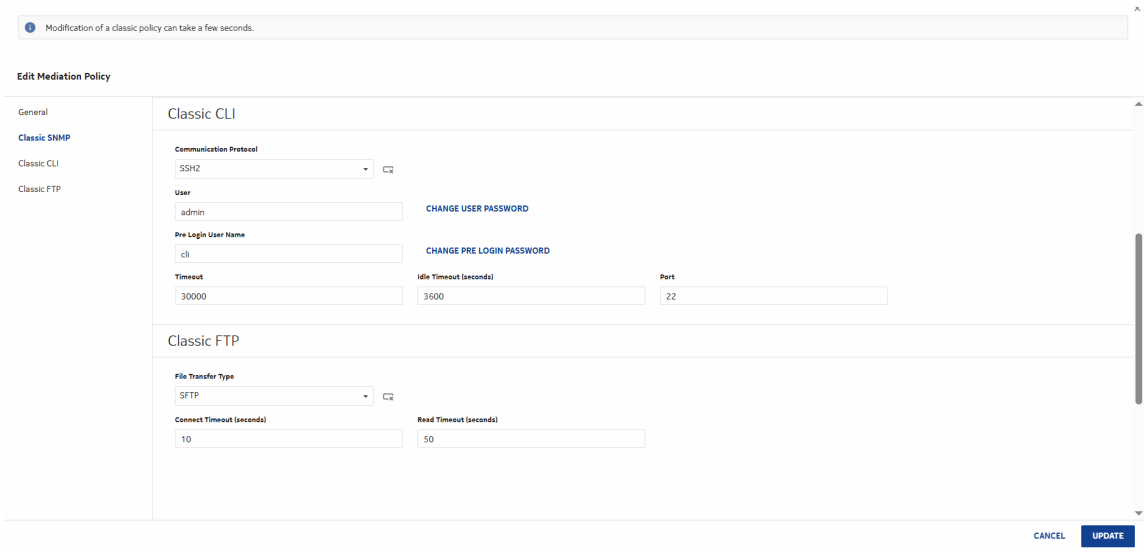
Upgrades

8.5 Upgrade prerequisites

8.5.1 For classic nodes upgrade

Complete the following prior to running a classic node upgrade:

- Verify that the classic mediation policy is correctly set in NSP.



8.5.2 For MD nodes upgrade

Complete the following prior to running an MD node upgrade:

1. Install adaptors for the new node version; Pre-check will fail if adaptors are not installed. See “How do I install adaptor artifacts that are not supported in the Artifacts view?” in the *NSP System Administrator Guide* for more information.
2. Configure FTP policy:

   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.

8.5.3 Additional requirements

The following additional general requirements apply to all upgrades:

- Make sure there is enough space on the node for the upgrade.
- 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.

8.5.4 ISSU upgrade path limitations

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

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

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

8.6 Backing up the node configs

Note: Perform this step prior to the upgrade.

8.6.1 To backup configs:

1

Log in to the NSP.

2

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

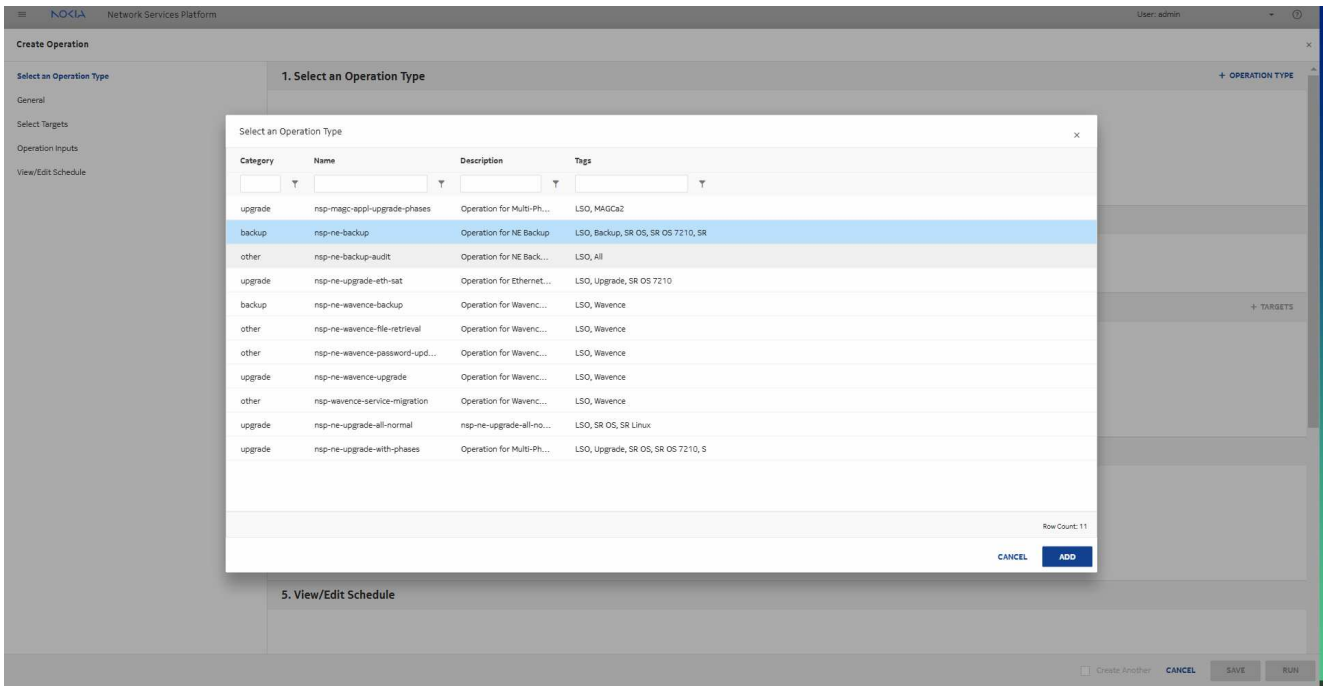
3

Select **Create an Operation**.

4

Select the right backup for your nodes: i.e. "nsp-ne-backup" for SR OS, SR OS 7210, SR.

Note: 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.



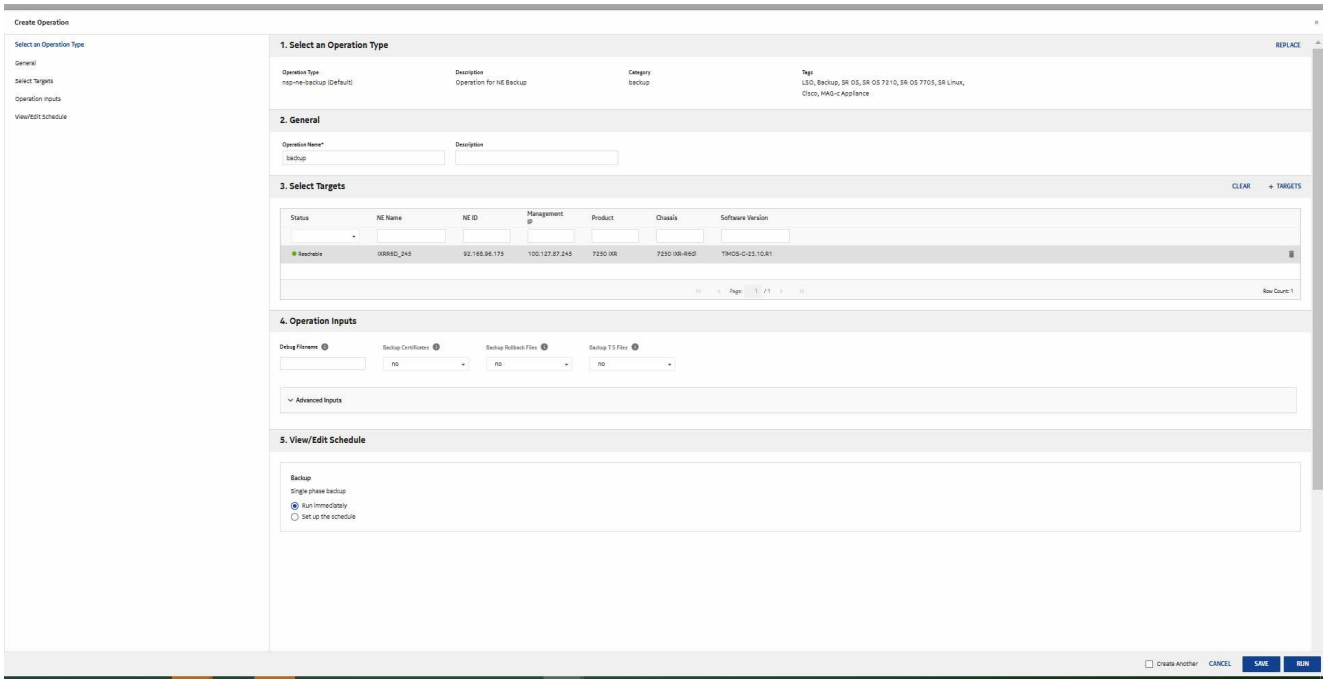
5

Select + **TARGETS** and select either **NEs** or **Predefined NE groups**.

6

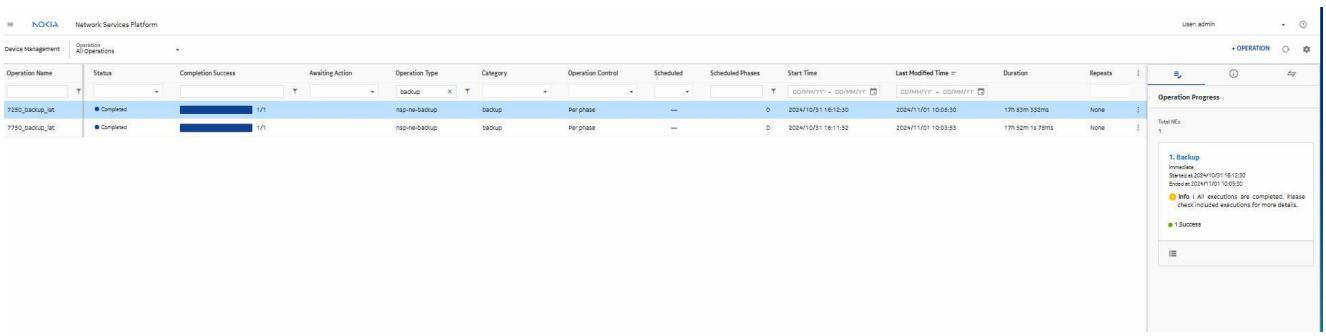
Select all options required.

Under **View/Edit Schedule**, select either “Run immediately” or “Setup up the schedule”.



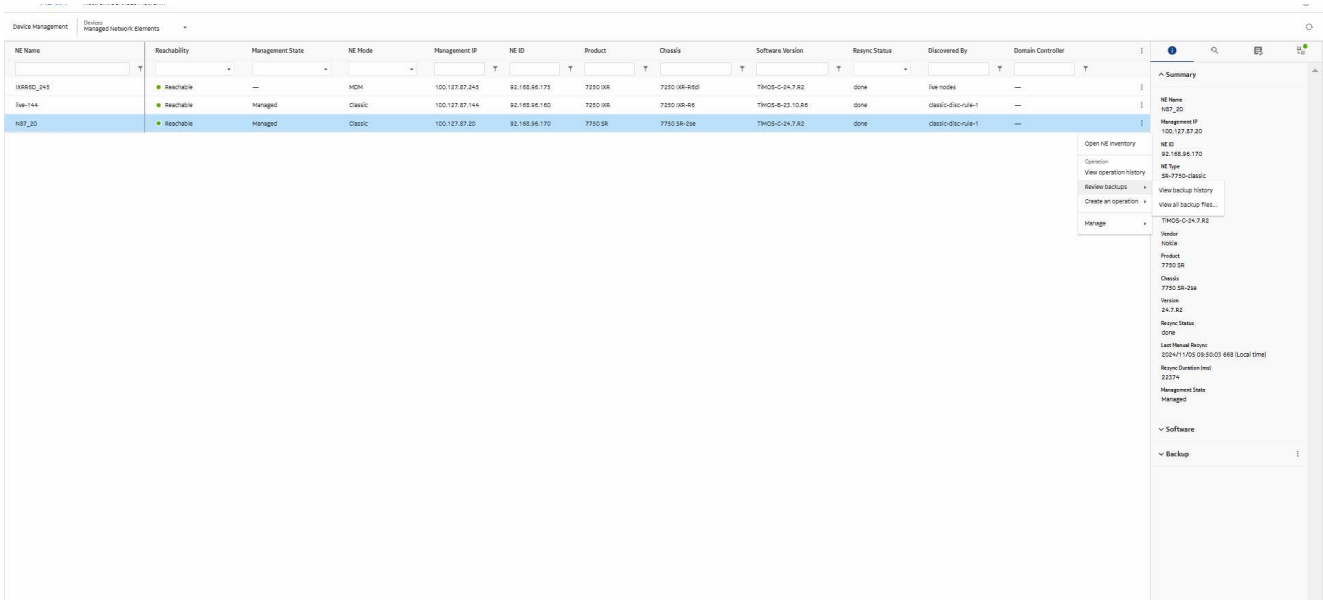
7

You can view the backup status from **Device Management**, **All Operations**.



8

Backup files can be viewed from **Device Management**, **Managed Network Elements**. Click on the NE and then select ⋮ **Review backups**, **View all backup files**.



END OF STEPS

8.7 Multi-phase upgrade: preparing the upgrade

8.7.1 Steps

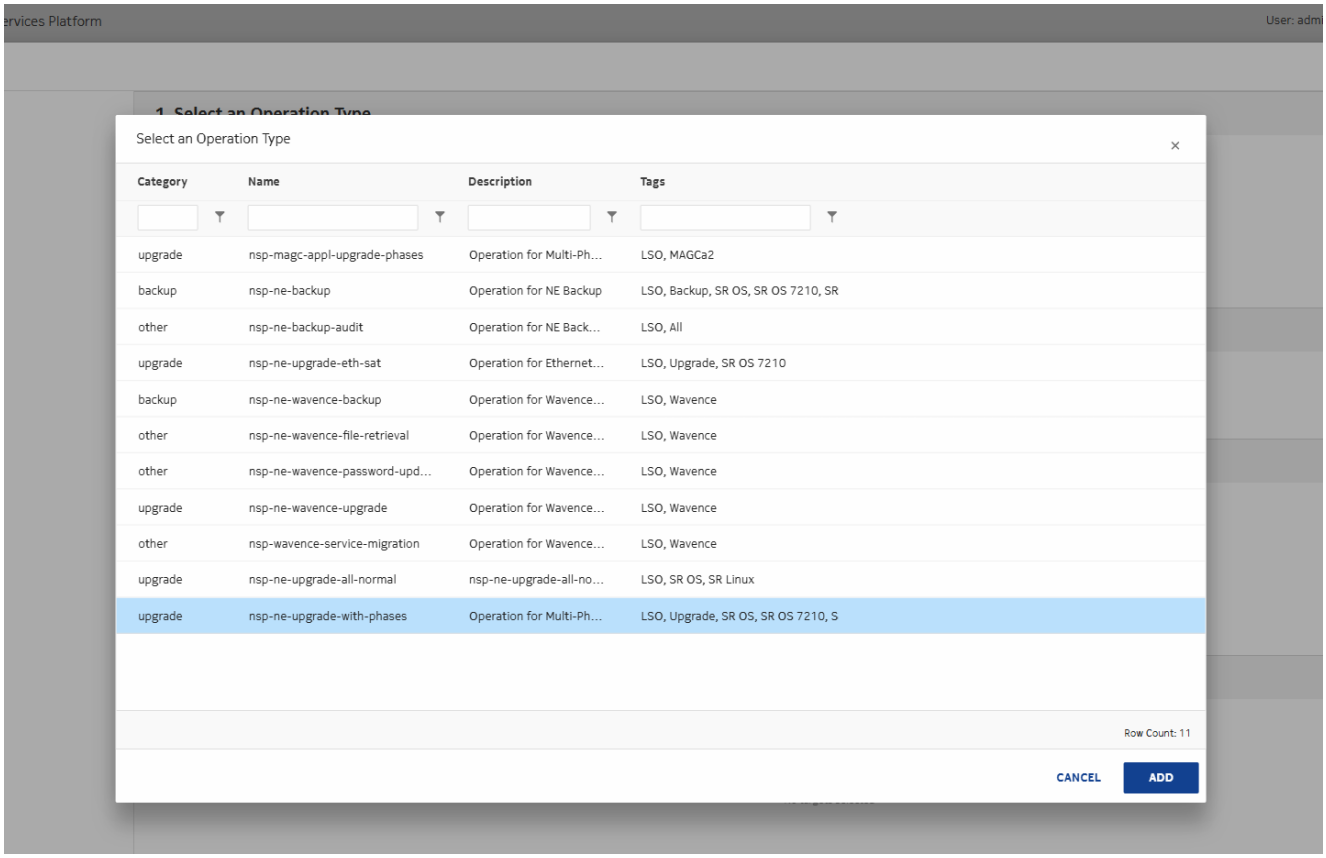
The following example shows a 7250 IXR model-driven node multi-phase upgrade from 23.10 to 24.7 R2.

1

Node upgrade can be created from two different locations: **Device Management, All Operations** or **Device Management, Node Images**. Navigate to either location to begin this procedure.

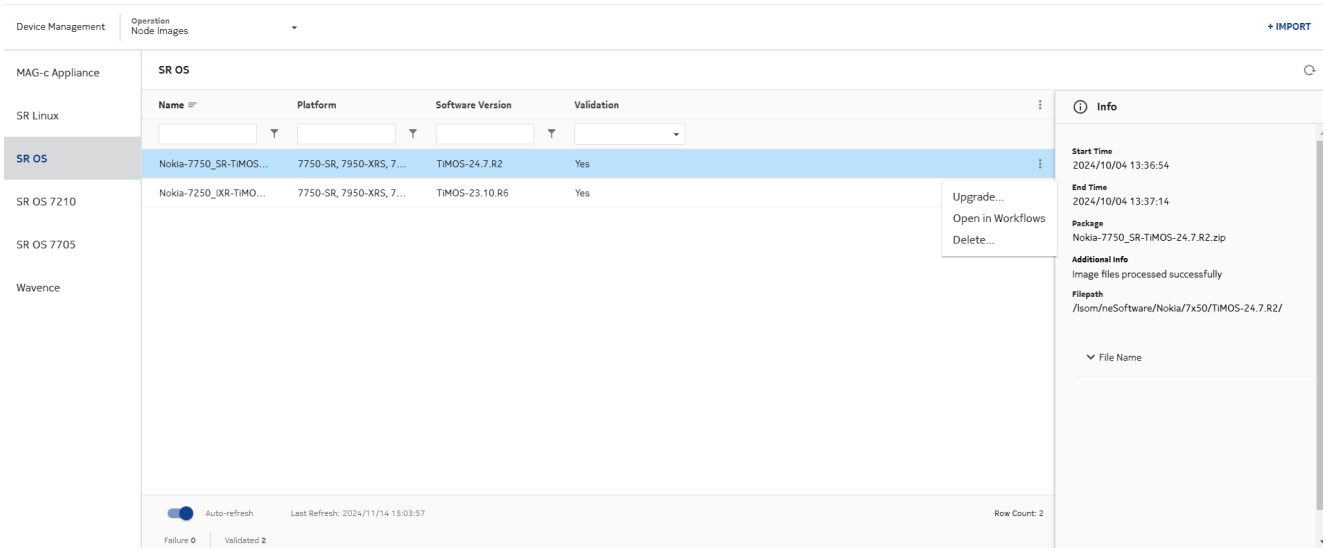
2

If you navigated to **All Operations**, select **Operation**, **Operation Type** and choose "nsp-ne-upgrade-with-phases" from the list.

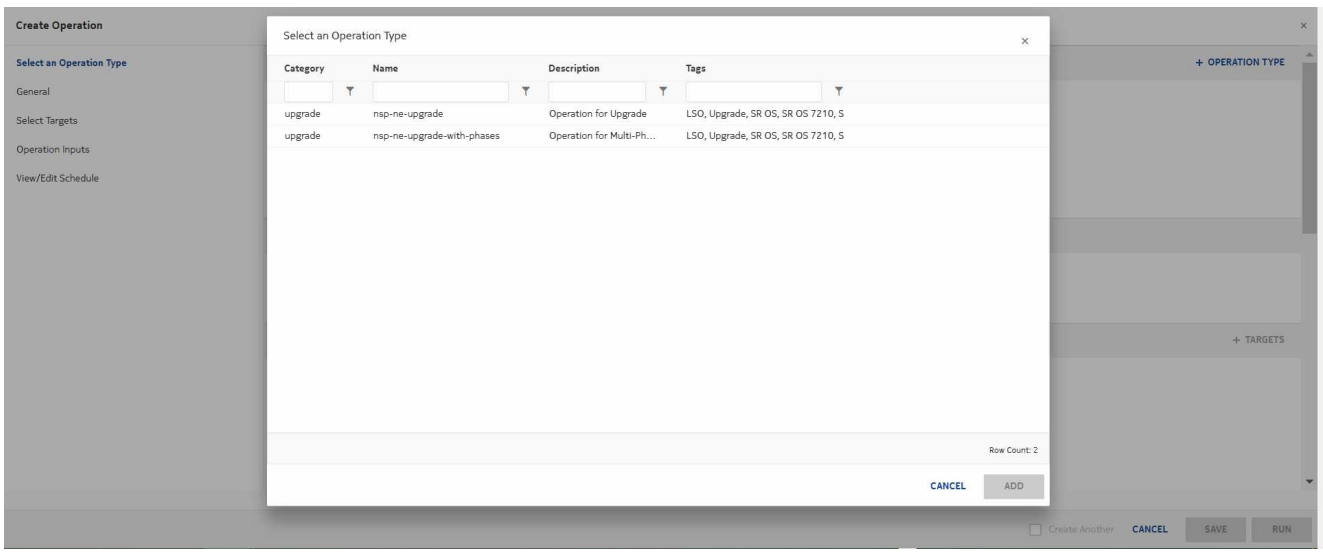


3

If you navigated to **Node Images**, locate the **SR OS** tab and click ⋮, **Upgrade...**



Select **Operation**, **Operation Type** and choose "nsp-ne-upgrade-with-phases" from the list.

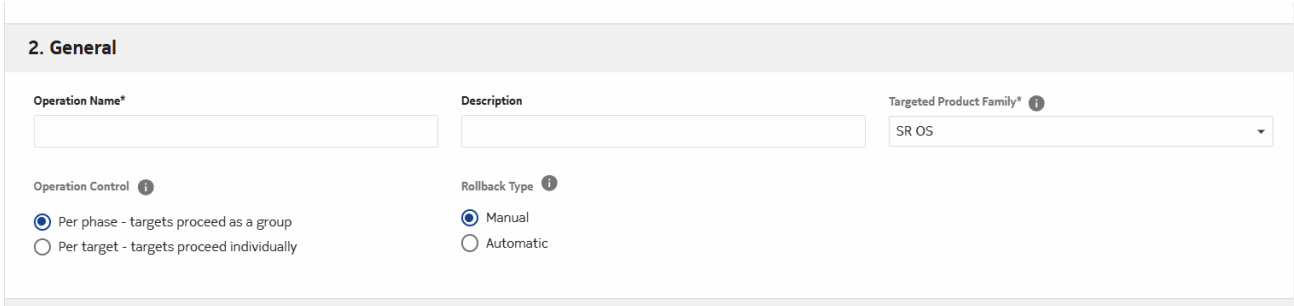


4

Select Target family product and all other options:

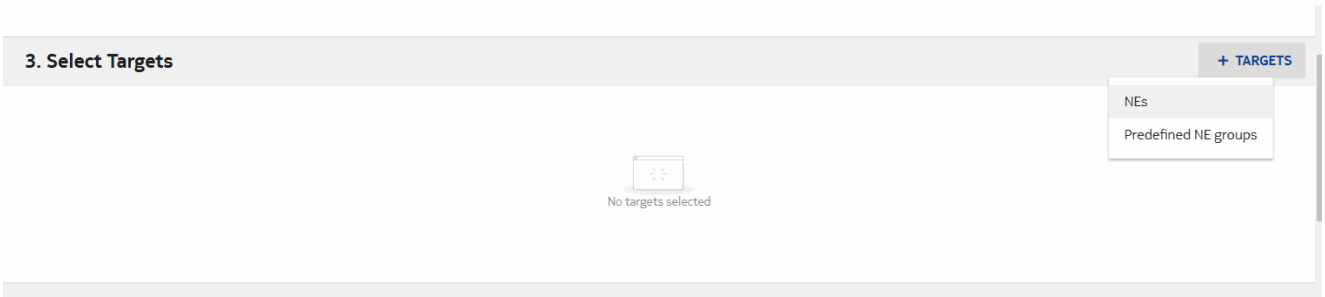
Operation Control: When upgrading multiple NEs at the same time, users can select "Per Phase" if targets (nodes) proceed as a group - which means all nodes must complete the current phase before proceeding to the next - OR "Per target" target and proceed to the next phase immediately regardless if the other targets are complete or not.

Rollback Type: Applicable for phases that support rollback - Activate and Reboot.



5

Select + **TARGETS**, **NEs** or **Predefined NE groups**.



6

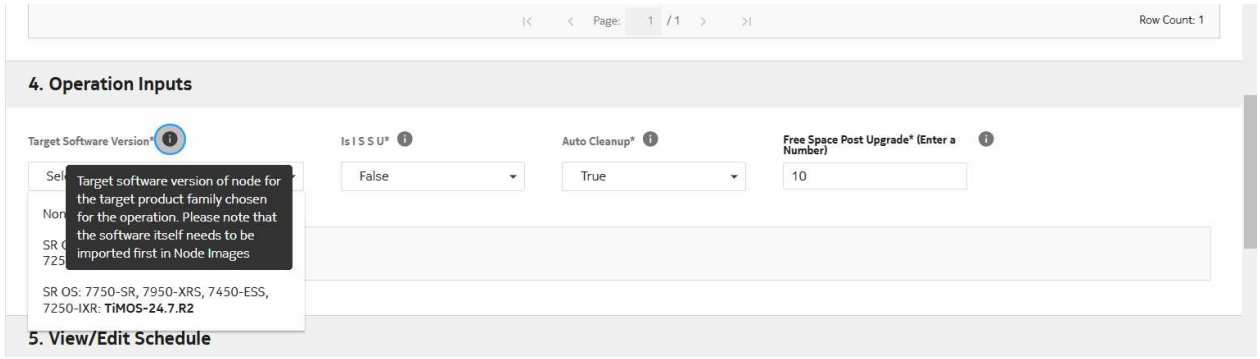
Select Operation Inputs:

Target Software Version: Select the version of the image from the list; the images that show in the drop down are the ones imported to Node Images.

Is ISSU: Defaulted to False, set to True only for nodes that support ISSU. Check the "SR OS Software Release Notes" documentation for the node chassis types that support ISSU.

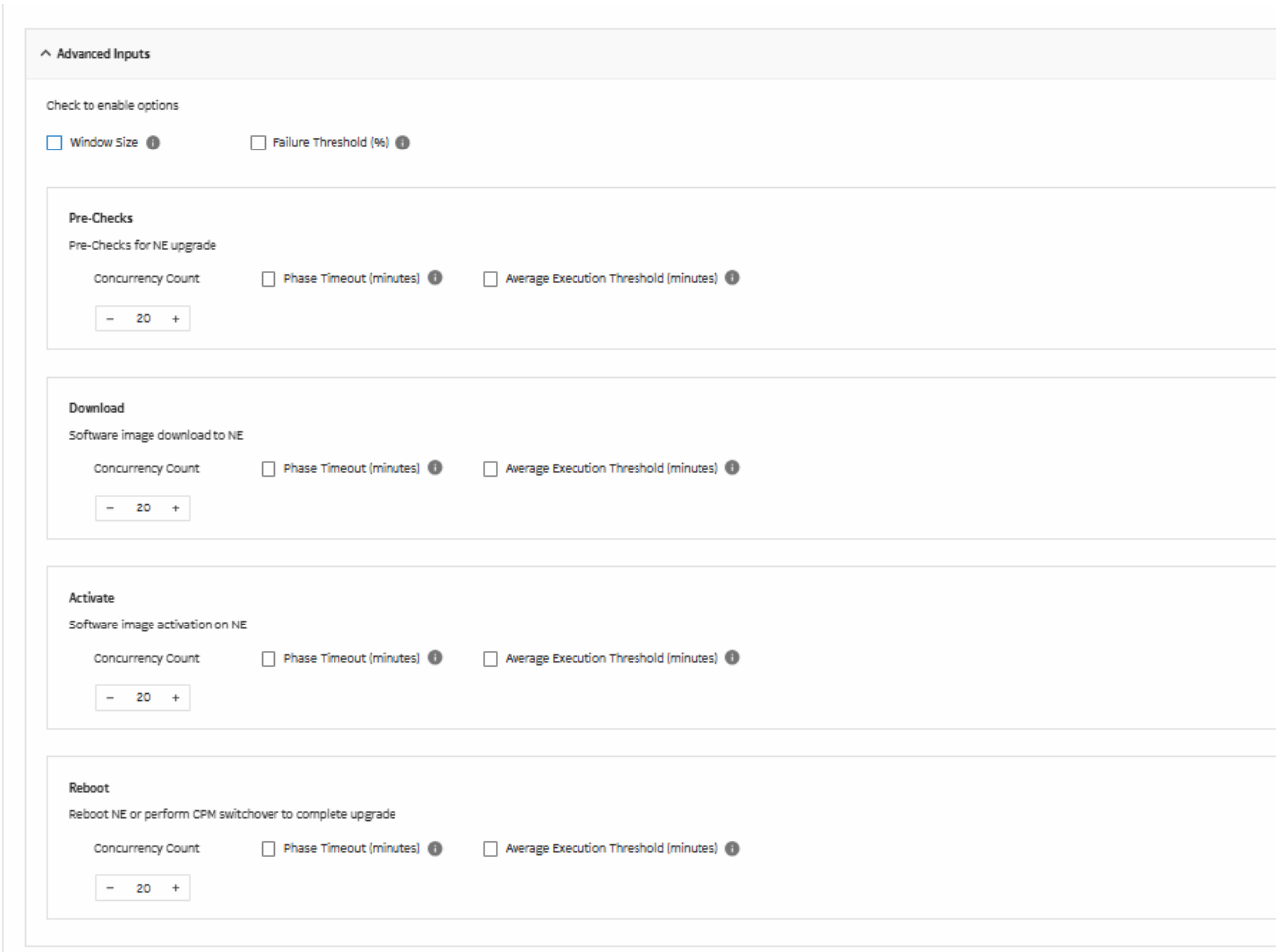
Auto Cleanup: Defaulted to True. When set to True, it will auto-delete all images in the images directory that are not referenced in the bof.

Free Space Post Upgrade: The expected free disk space % after upgrade, and only used when autoCleanup is set to True.



7

Users can select any of these optional Advanced Inputs for each of the phases:



Configure the Advanced Inputs as needed:

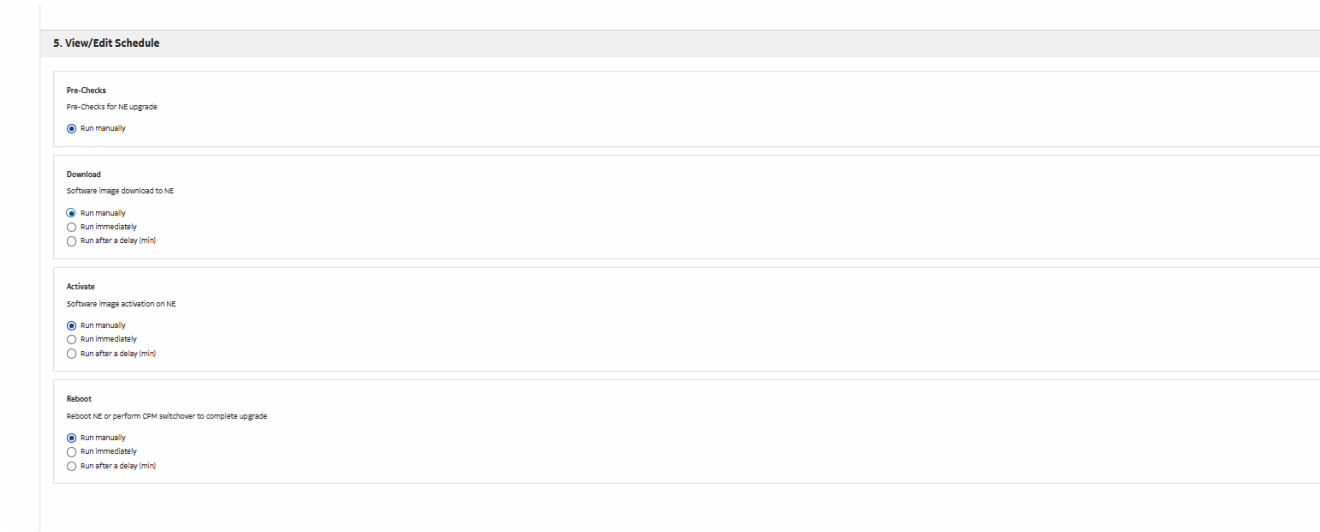
Parameter	Description
Window Size Failure Threshold	These two parameters work together to define an automatic stopping point for the operation due to failed workflow executions: • Window size specifies the sample size to use when calculating whether a threshold has been crossed. • Failure threshold specifies the percentage of executions failed that will trigger the automatic stop. For example, with a window size of 200 and a failure threshold of 50%, the operation will automatically stop after 100 failed executions. The phase and operation are paused and any not-started executions remain in not-started status.
The following parameters can be configured separately for each phase of the operation: pre-checks, software download, software activation, and NE reboot or CMP switchover.	
• Concurrency Count • Phase Timeout (minutes) • Average Execution Threshold (minutes)	These parameters specify how the workflow executions will be managed. The pre-check steps themselves are defined in the applicable workflow. • Concurrency Count: maximum number of executions to run concurrently. • Phase Timeout and Average Execution Threshold: if these parameters are configured, the operation automatically stops after the specified time. The phase and operation are paused and any not-started executions remain in not-started status.

8

View/Edit Schedule:

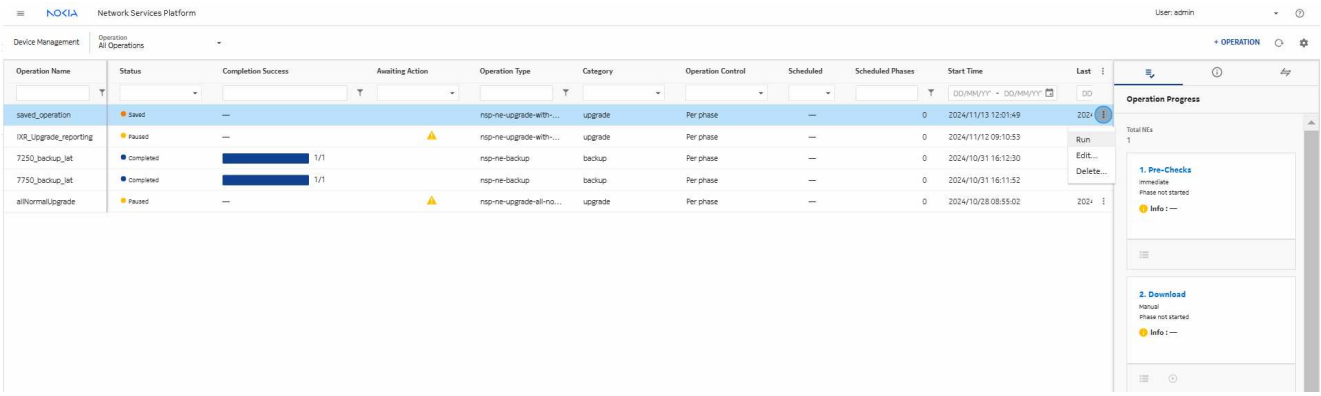
If the user selected Operational Control - "Per phase" in Step 3, the phases will only have the option to run manually.

If the user selected Operation Control - "Per target" in Step 3, they can select to run each phase manually, immediately, or after a delay (min).



9

After selecting all the options for an upgrade, users can Run or Save. A saved operation can be viewed from **Device Management**, **All Operations** with Saved status. Users can start operation at any time.



END OF STEPS

8.8 Multi-phase upgrade: performing the upgrade

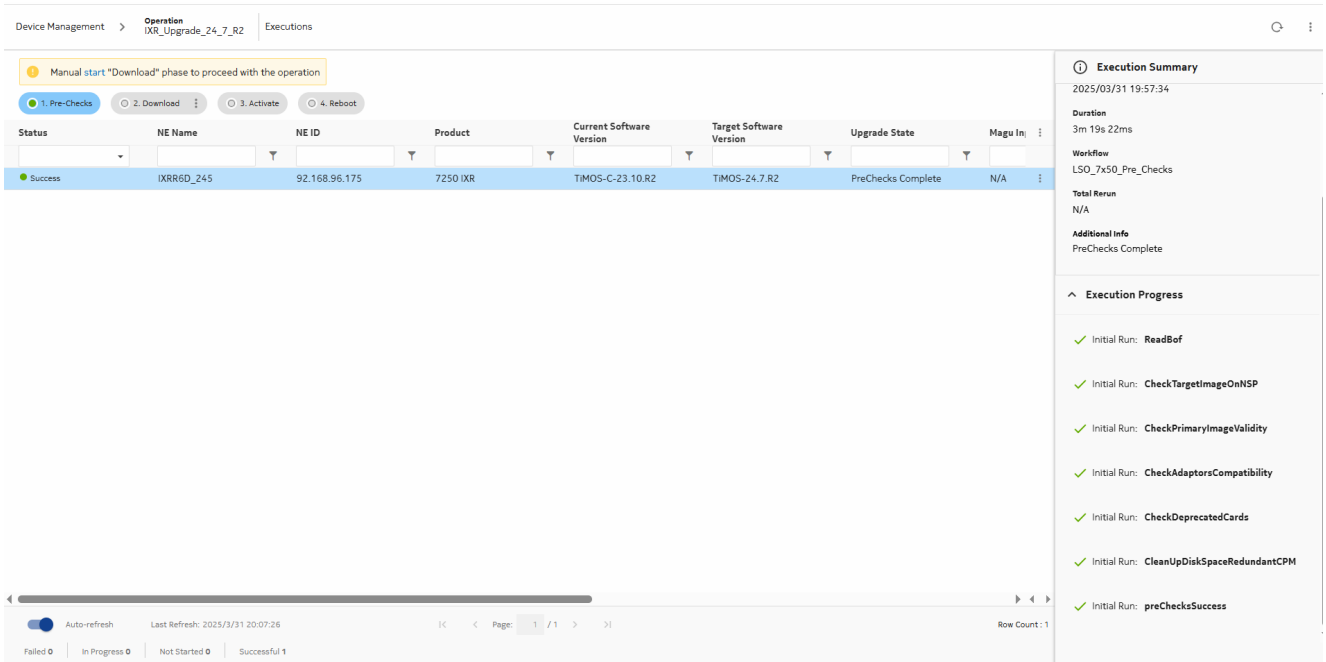
8.8.1 Encountering failures

In the event of a failure at any phase in the upgrade process, troubleshoot and complete the necessary tasks based on the failure message, then re-run the phase. To re-run the phase, click ⋮ and select **Rerun**.

8.8.2 Phase 1: Pre-check

In the Pre-check phase, the node is assessed to verify it is prepared and ready for upgrade.

Note: Pre-check will fail if Cleanup is set to True and there is not enough space on the node. Users can manually delete old files on the node and rerun the phase.



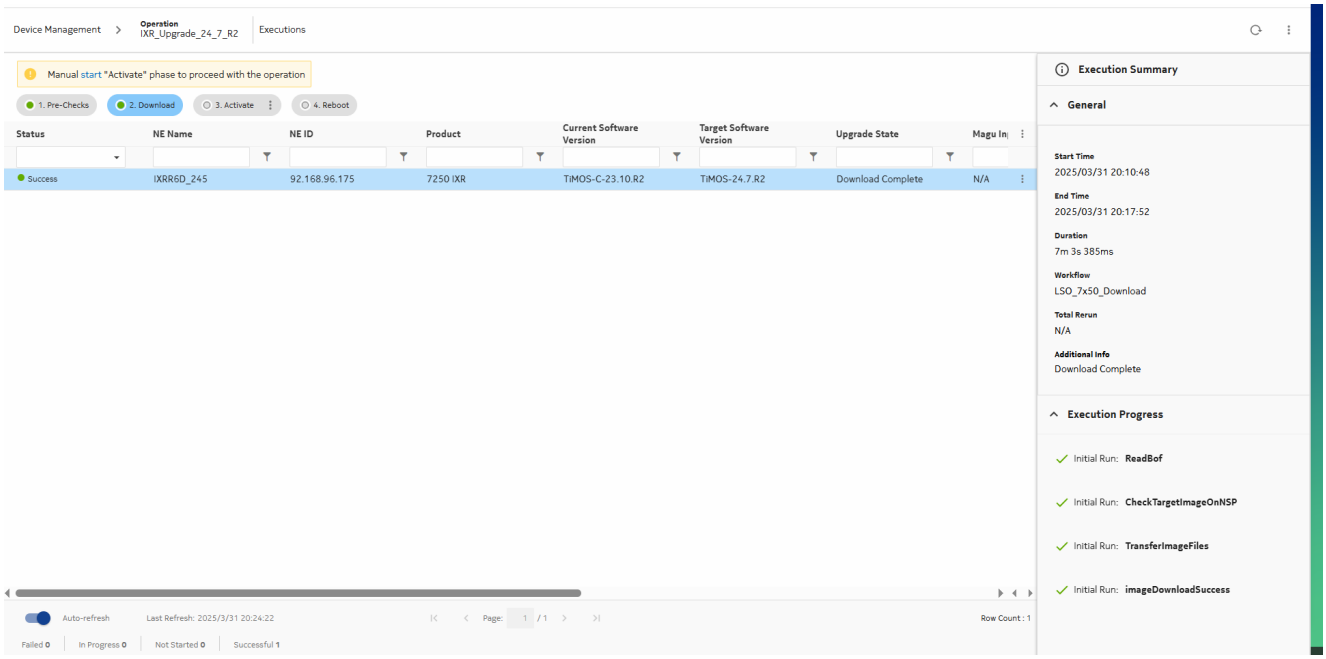
8.8.3 Phase 2: Download

After Pre-check passes, click “Start download”.

In the download phase, the image is downloaded from NSP to the node cf images directory. If the image is already downloaded, it will run the checks and let the user know that the image is already downloaded.

The files will be transferred as shown below if they are not already on the node.

Note: Download can fail for many reasons, such as if there is not enough space on the node and the Auto cleanup was set to False. If this occurs, users can free up space manually and re-run the phase.

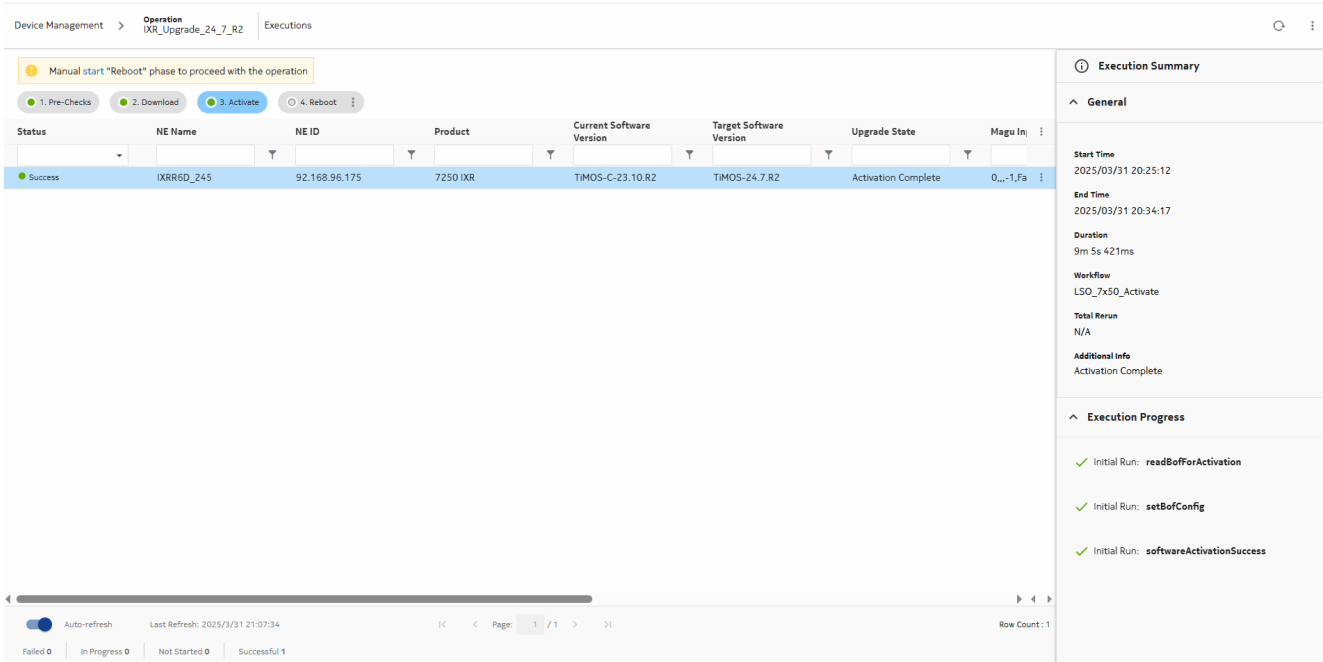


8.8.4 Phase 3: Activate

After Download is successful, users can start the Activate phase.

In the activate phase, the boot image will be copied to cf3, and update bof primary image and boot-env synch command will run on the node (admin redundancy synchronize boot-env).

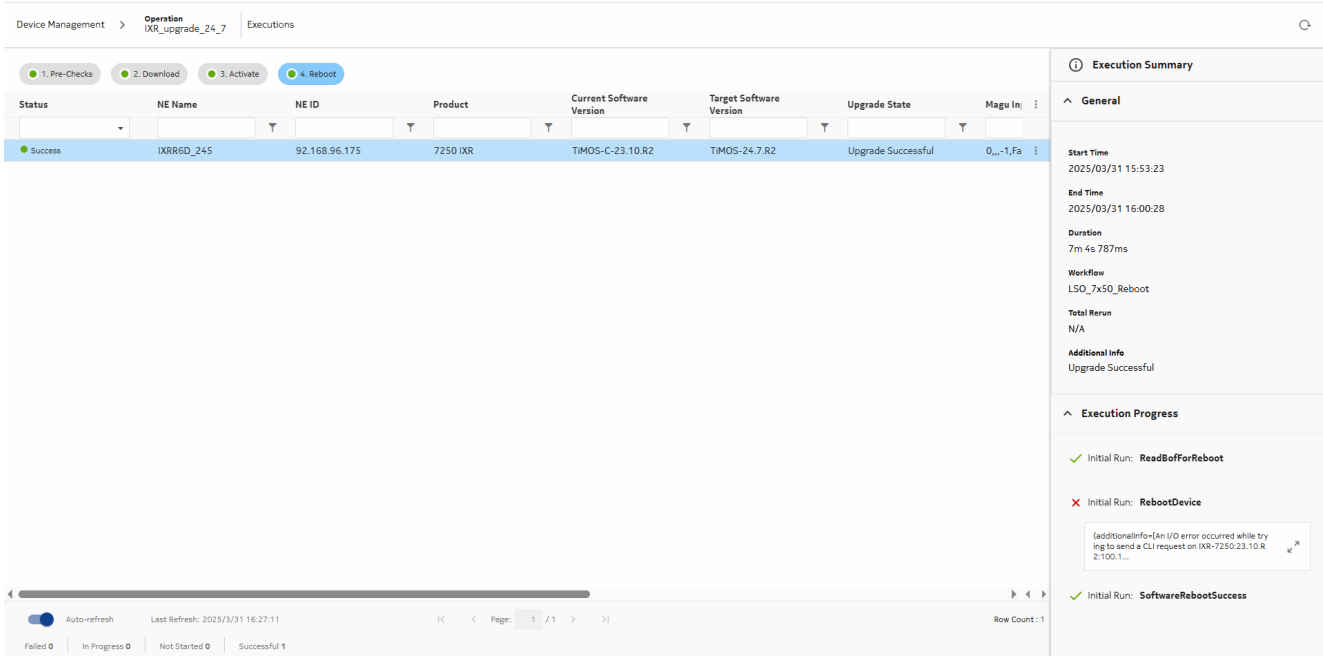
Note: The Activate phase will fail if any of the previous phases fail.



8.8.5 Phase 4: Reboot

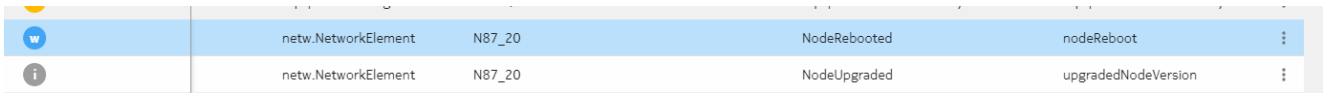
After the Activate phase is successful, users can begin the Reboot phase.

In the reboot phase, the node will either be rebooted or ISSU switchover. 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.



Note: The RebootDevice incorrectly shows that it failed, as connectivity to the node was lost, even though it successfully passed. There is an active PTS to address this issue.

Alarms raised after reboot:



8.8.6 ISSU

See 8.11 “ISSU upgrade” (p. 424) for the steps to perform an ISSU upgrade.

8.9 Single phase upgrade: preparing the upgrade

8.9.1 Steps

Upgrade is completed in one single phase with no pauses. The maintenance window will run before the start of the upgrade until it is complete.

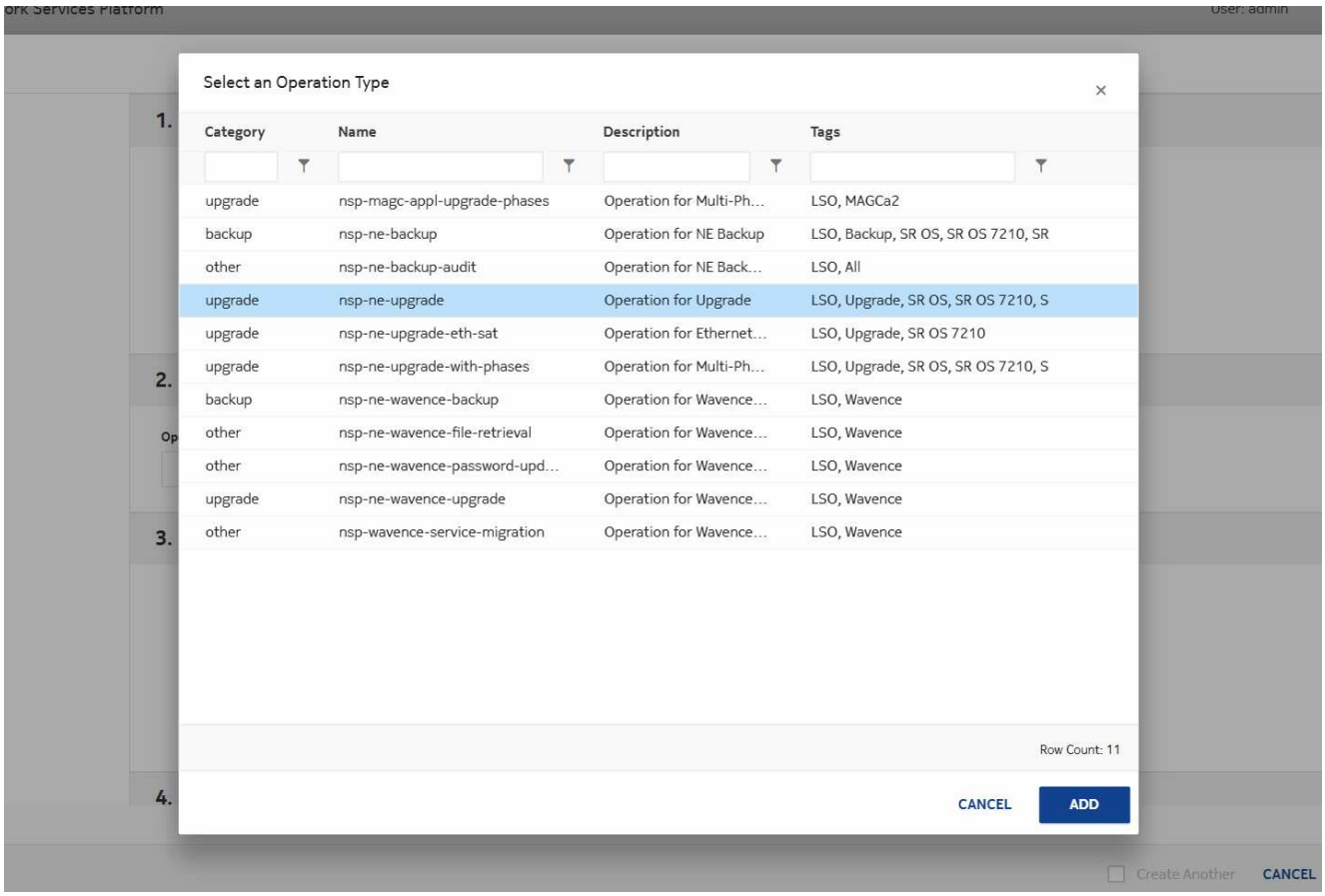
1

Navigate to **Device Management**, **All operations**.

.

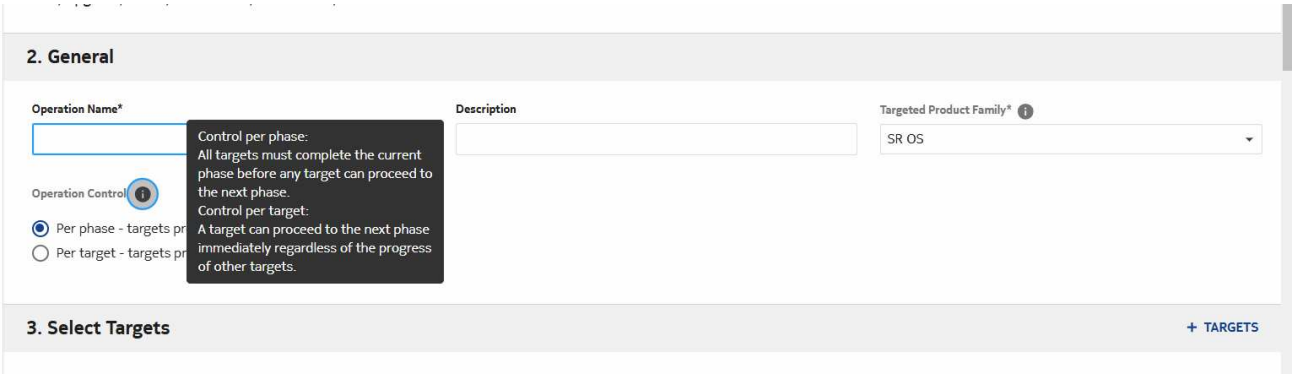
2

Select **Operation**, **Operation Type** and choose "nsp-ne-upgrade" from the list.



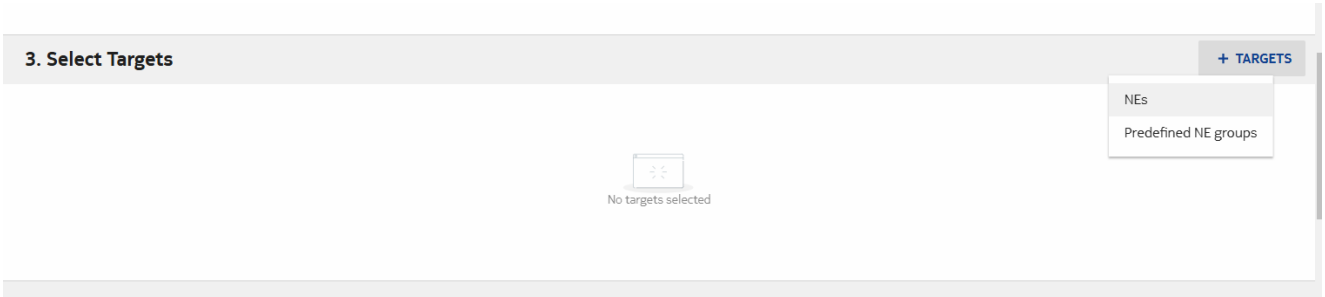
3

Under **General**, fill out the Operation Name and select the Operation Control.



4

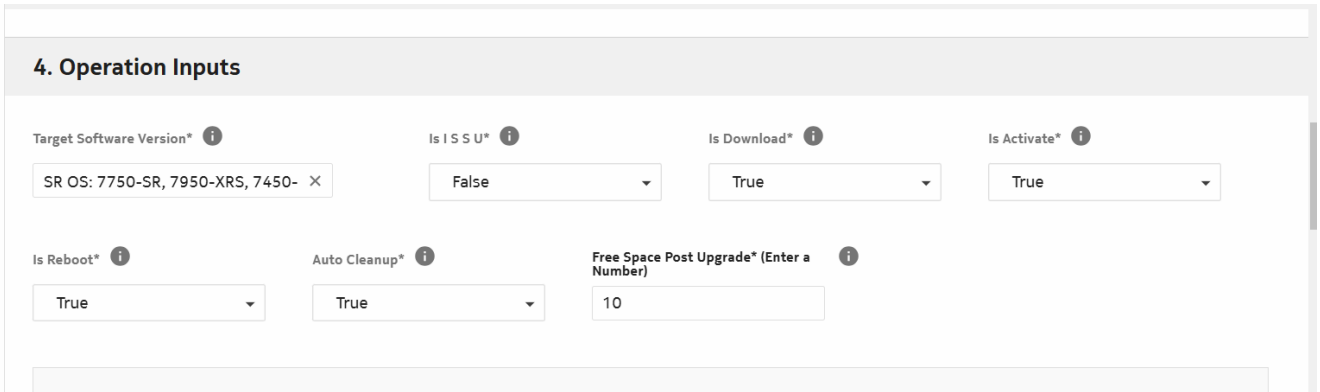
Select **+ TARGETS**, **NEs** or **Predefined NE groups**.



5

Select Operation Inputs:

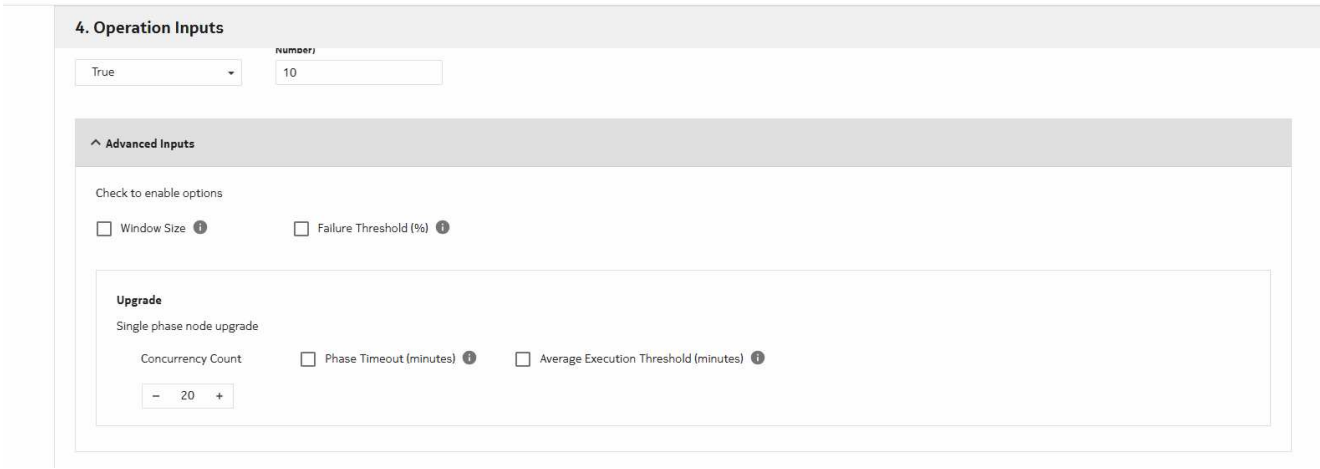
With single phase upgrades, users can select to enable or disable any of the phases. Below are the default options:



Note: Users cannot set both isISSU and isReboot to True.

6

Users can select any of these optional Advanced Inputs for each of the phases:



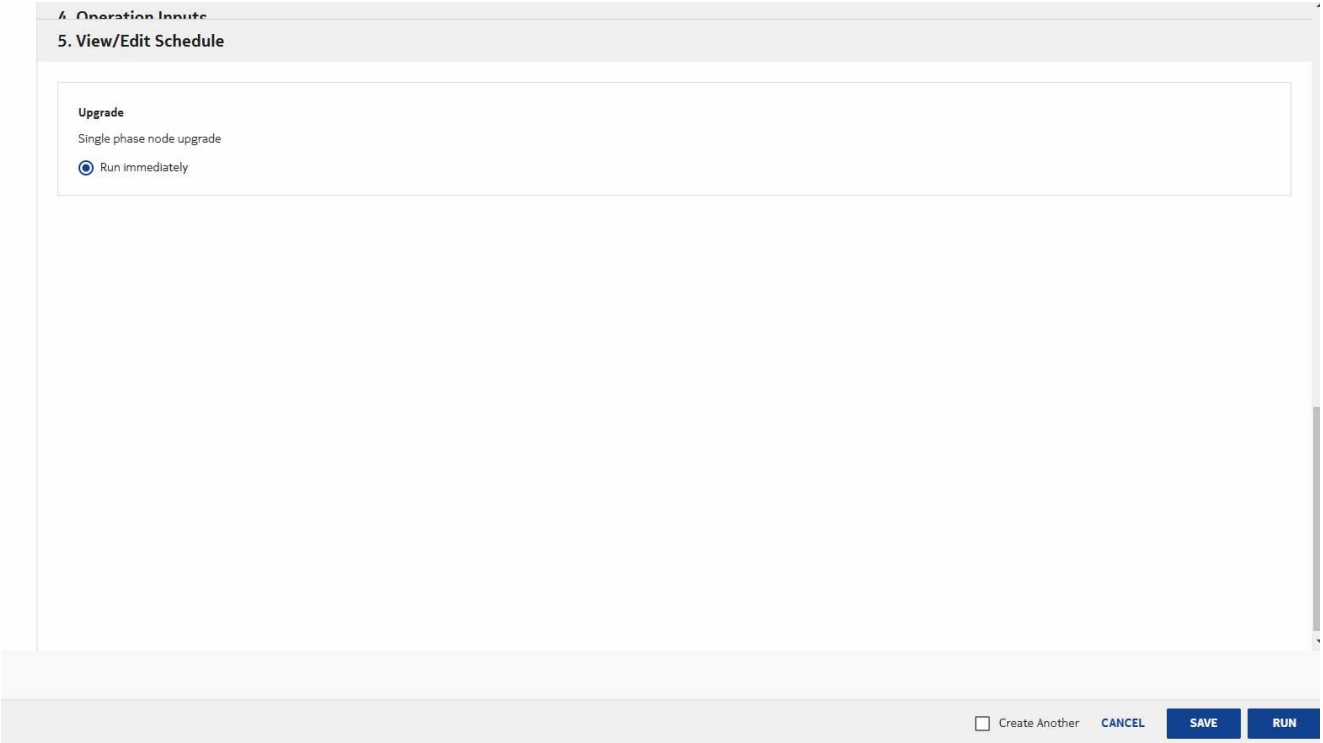
END OF STEPS

8.10 Single phase upgrade: performing the upgrade

8.10.1 Steps

1

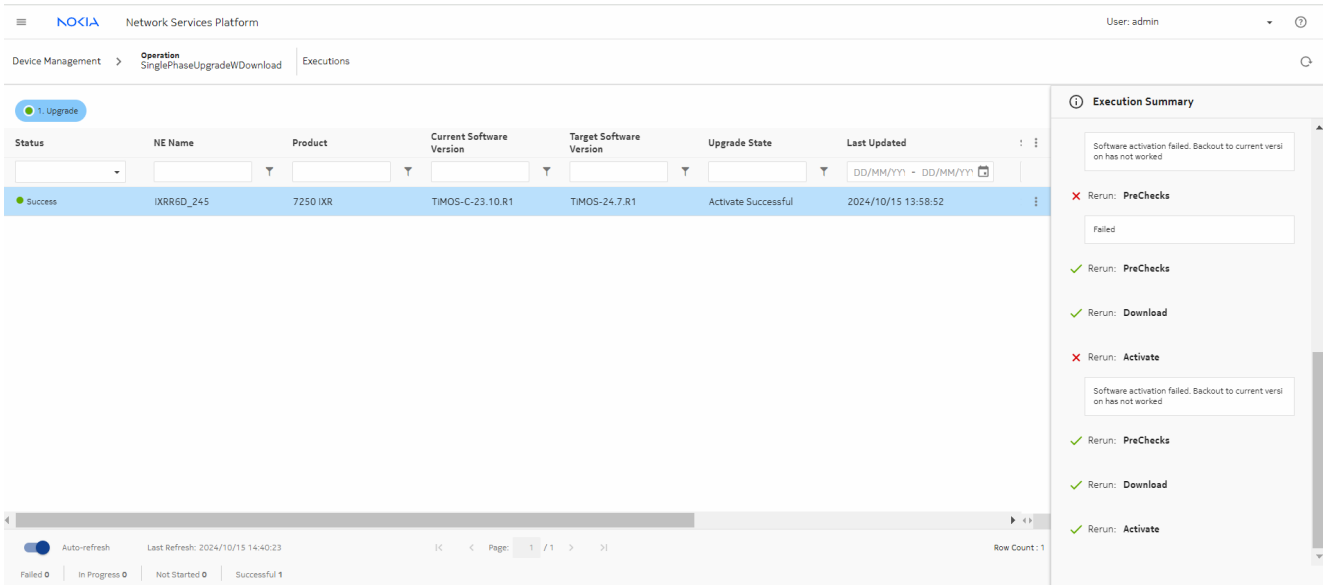
View/Edit Schedule: Choose to Run or Save.



If you select “Run immediately” the upgrade will run in one phase and show the status as running.

2

If the upgrade fails, it can be re-run.



3

See 8.11 “ISSU upgrade” (p. 424) for the steps to perform an ISSU upgrade.

END OF STEPS

8.11 ISSU upgrade

8.11.1 Introduction

ISSU (In service software upgrade) is supported on specific chassis types. See “ISSU upgrade procedure” in the *SR OS Software Release Notes* for the specific release you are upgrading to.

8.11.2 Multi-phase ISSU upgrade

Fill out the upgrade operation options. Set the ISSU to “True”. If the ISSU is not supported for the node, the Pre-check will fail.

Figure 8-1 Upgrade operation options

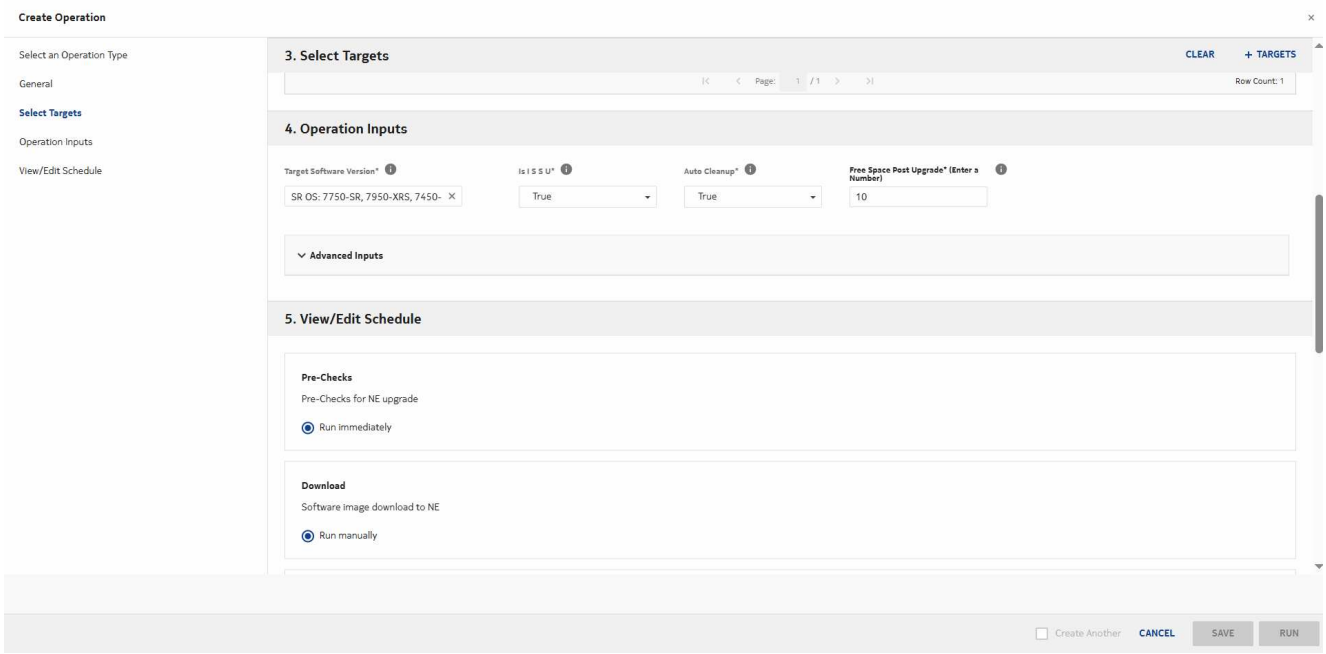
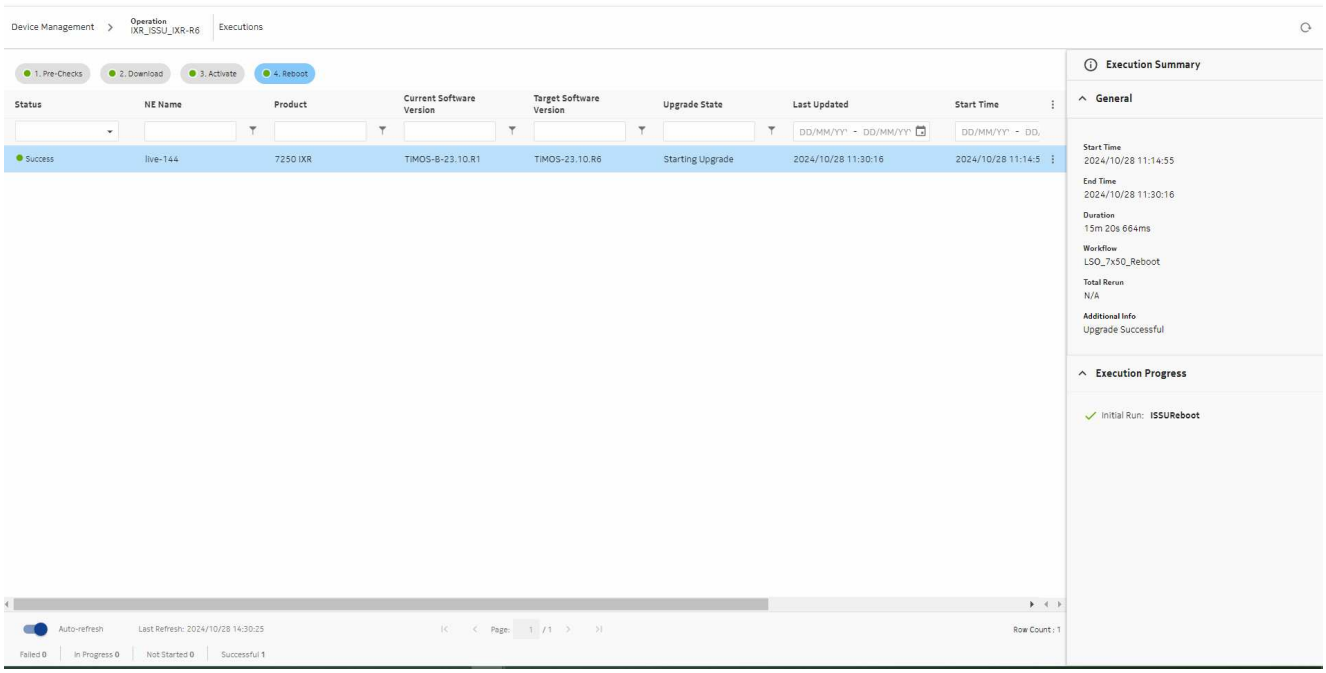
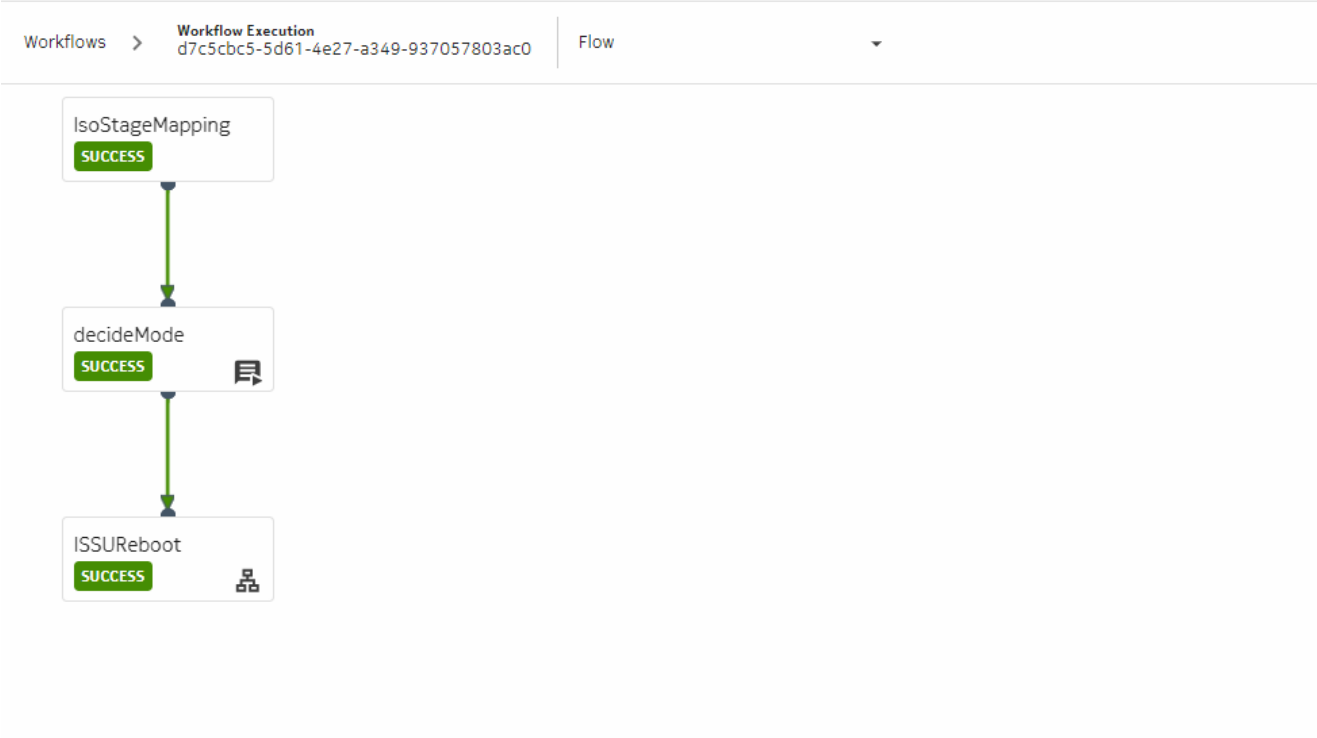


Figure 8-2 Successful ISSU upgrade:





Example IXR node show card command during ISSU upgrade:

Before reboot:

```
A:live-144# show card
===============================================================================

Card Summary
===============================================================================

Slot      Provisioned Type                          Admin Operational
Comments
              Equipped Type (if different)          State State
-------------------------------------------------------------------------------

1         iom-ixr-r6                                up    up
2         iom-ixr-r6                                up    up
A         cpiom-ixr-r6                              up    up/active
B         cpiom-ixr-r6                              up    up/standby
===============================================================================
```

Reboot phase:

```
A:live-144# show card

===============================================================================

Card Summary
===============================================================================

Slot      Provisioned Type                          Admin Operational
Comments
              Equipped Type (if different)          State State
-------------------------------------------------------------------------------

1         iom-ixr-r6                                up    up
2         iom-ixr-r6                                up    provisioned
              (not equipped)
A         cpiom-ixr-r6                              up    up/active
B         cpiom-ixr-r6                              up    down/standby
              (not equipped)
===============================================================================




A:live-144# show card

===============================================================================

Card Summary
===============================================================================

Slot      Provisioned Type                          Admin Operational
Comments
              Equipped Type (if different)          State State
-------------------------------------------------------------------------------

1         iom-ixr-r6                                up    up
2         iom-ixr-r6                                up    booting
A         cpiom-ixr-r6                              up    up/active
B         cpiom-ixr-r6                              up    ISSU/standby
===============================================================================

A:live-144#

B:live-144# show card

===============================================================================
```

```
Card Summary
==============================================================================

Slot      Provisioned Type                          Admin Operational
Comments
              Equipped Type (if different)          State State
------------------------------------------------------------------------------

1         iom-ixr-r6                                up    provisioned
              (not equipped)
2         iom-ixr-r6                                up    up
A         cpiom-ixr-r6                              up    down/standby
              (not equipped)
B         cpiom-ixr-r6                              up    up/active
==============================================================================

B:live-144#


B:live-144# show card

==============================================================================

Card Summary
==============================================================================

Slot      Provisioned Type                          Admin Operational
Comments
              Equipped Type (if different)          State State
------------------------------------------------------------------------------

1         iom-ixr-r6                                up    up
2         iom-ixr-r6                                up    up
A         cpiom-ixr-r6                              up    up/standby
B         cpiom-ixr-r6                              up    up/active
==============================================================================
```

8.11.3 Single phase ISSU upgrade

To complete an ISSU upgrade, users need to set the ISSU to “True” and Reboot to “False”. Both cannot be set to “True” at the same time. The Pre-check will fail if both are set to “True”.

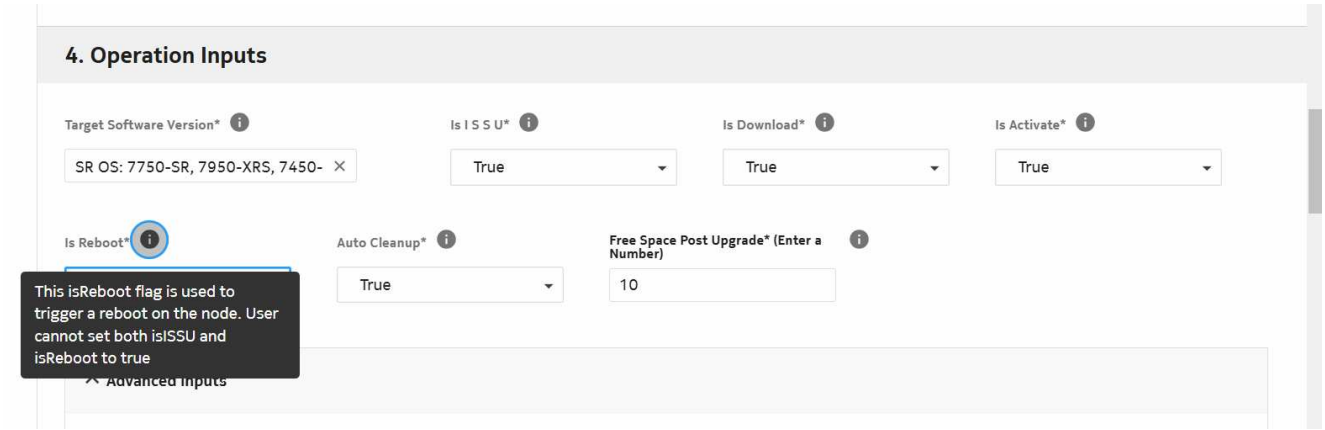
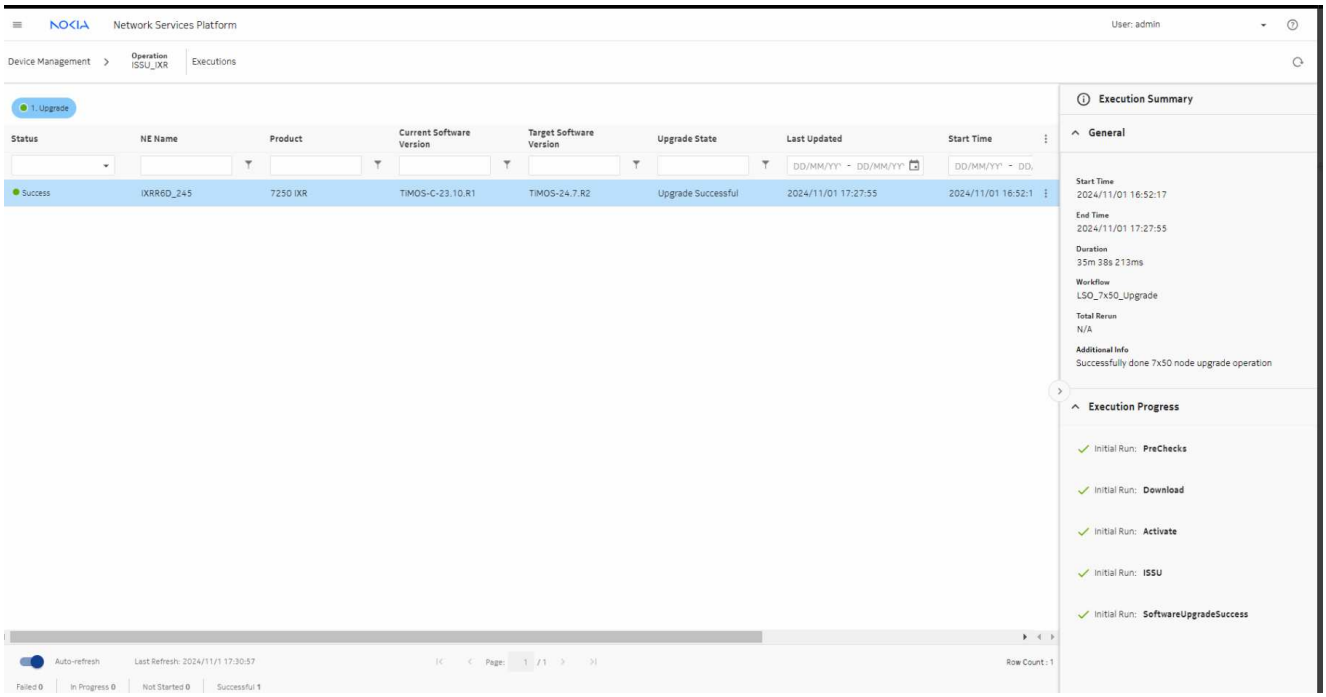


Figure 8-3 Successful single phase ISSU upgrade:



Post-upgrade procedures

8.12 Rollback

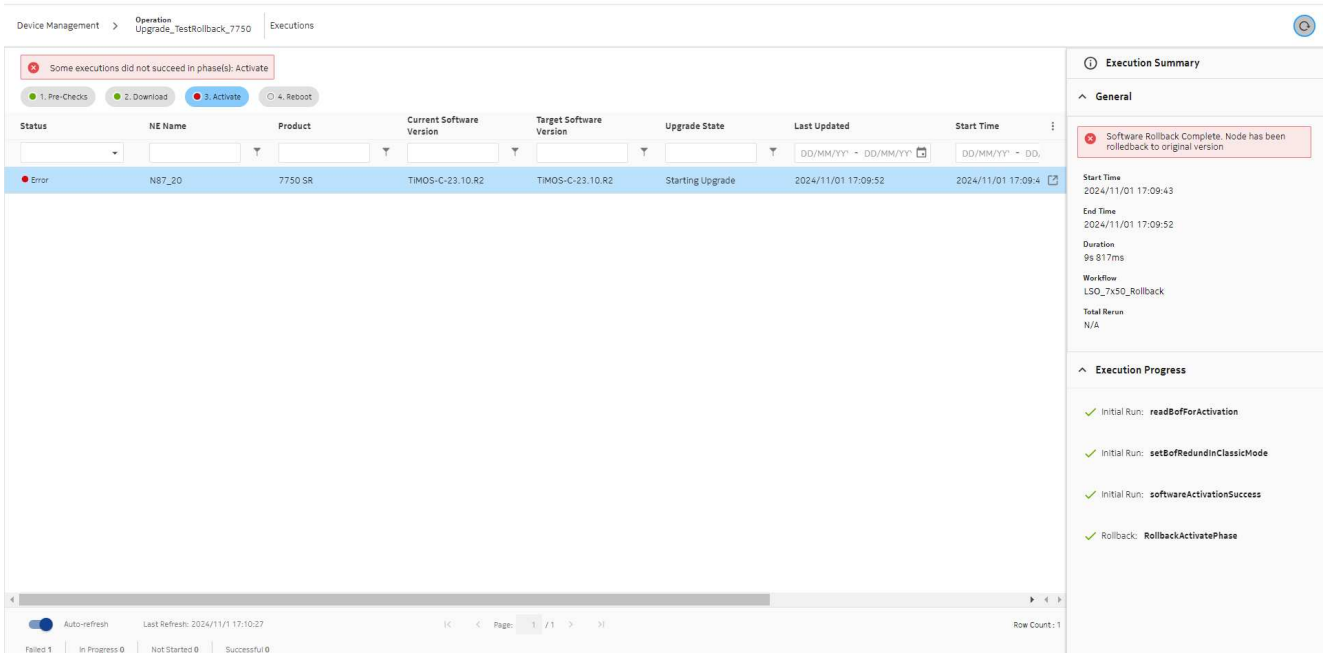
8.12.1 Introduction

Rollback is the process of switching the node version back to its original pre-upgrade version. It is only supported in multi-phase upgrade/upgrade with phases and can be done from the Activate or Reboot state. It is not supported with single phase upgrade or ISSU.

8.12.2 Activate phase

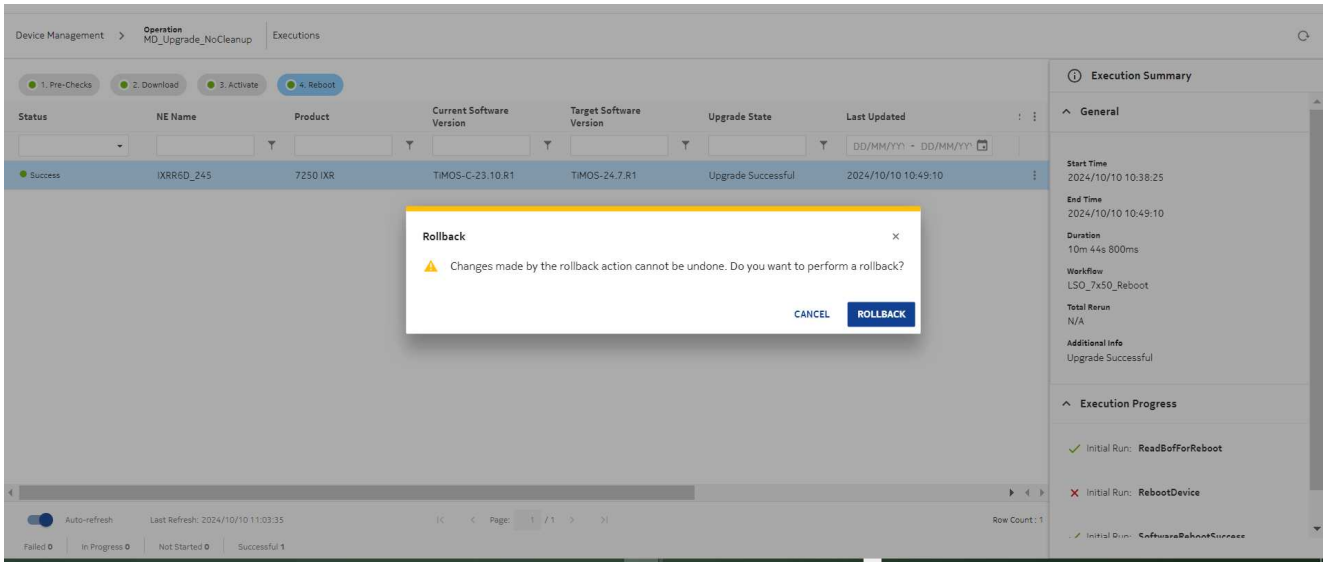
To begin Rollback, click on ⋮ **Rollback**.

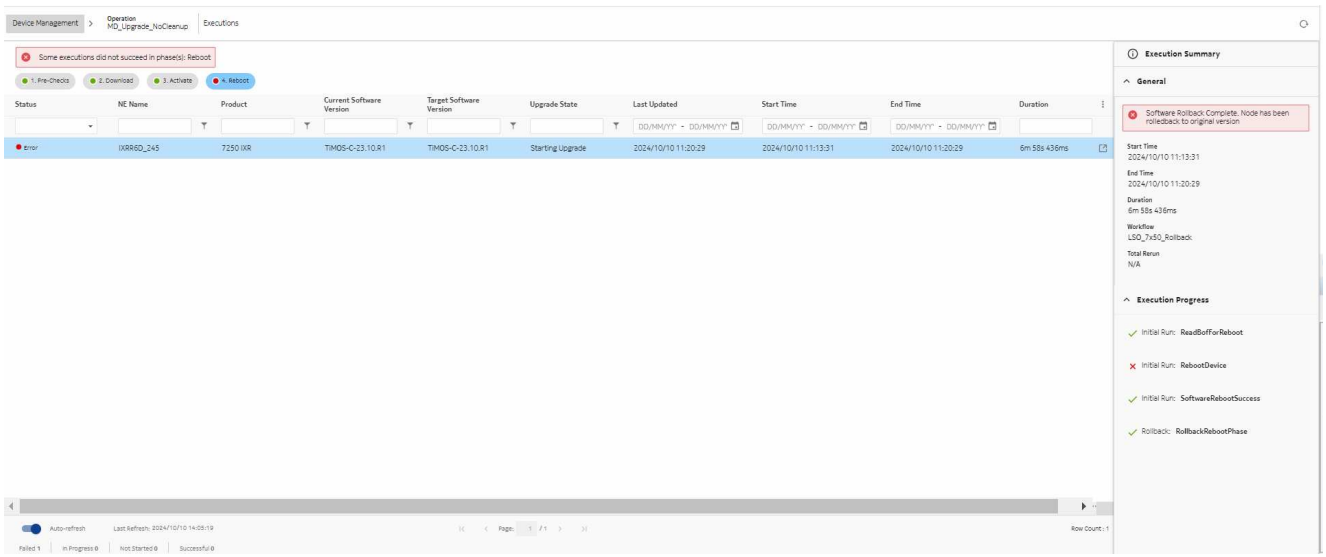
Note: Rollback is an option regardless of if the phase passed or failed. After running the rollback, the phase will be in the failed state. All phases will be complete and cannot be re-run.



8.12.3 Reboot Rollback

Following the completion of the Rollback procedure, reboot the Rollback.





8.13 LSO reporting

8.13.1 Reports

Reports are not published as out of the box with NSP, but LSO framework does support a way to generate and publish reports as part of the upgrade operation. The content of the report can be customized to include running config/show commands.

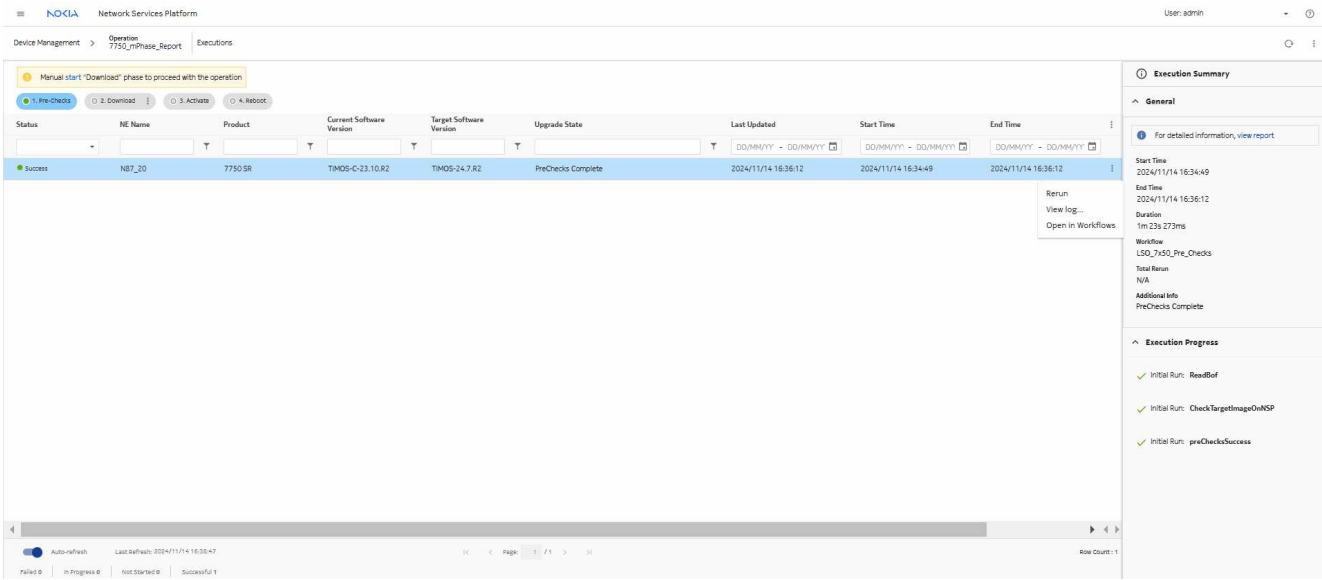
Note: There is a limitation on the size of the generated file: 15Mb.

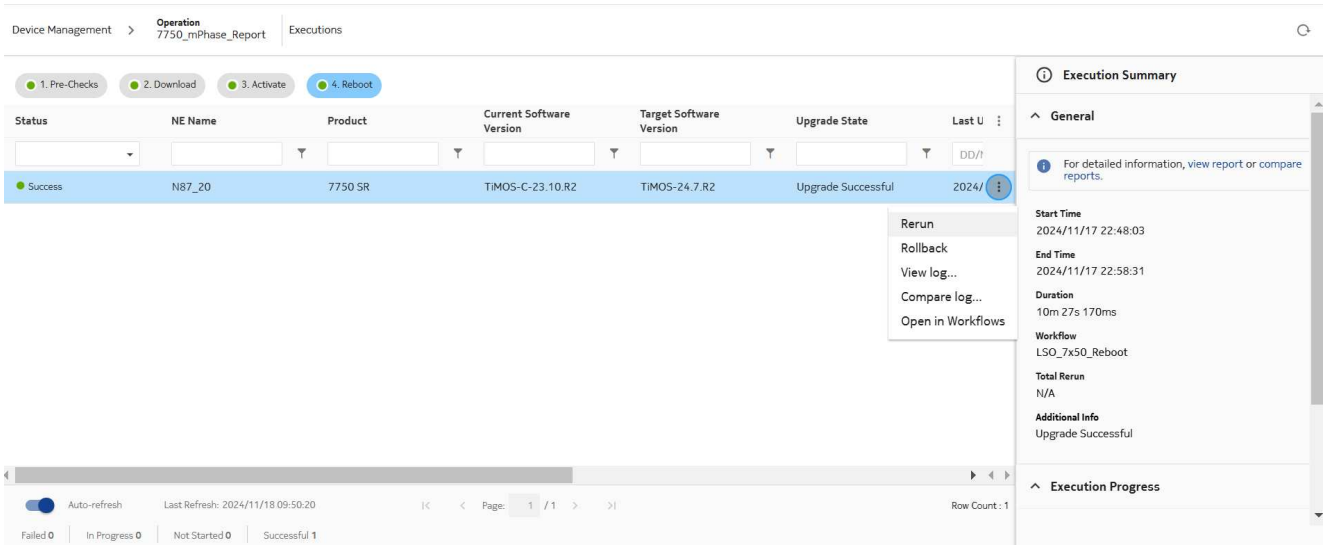
This needs to be requested and customized per customer need. Please contact the Nokia support team for more information.

For this use case, the Pre-check and Reboot workflows are customized to enable report generation and collect the following show commands pre and post-upgrade:

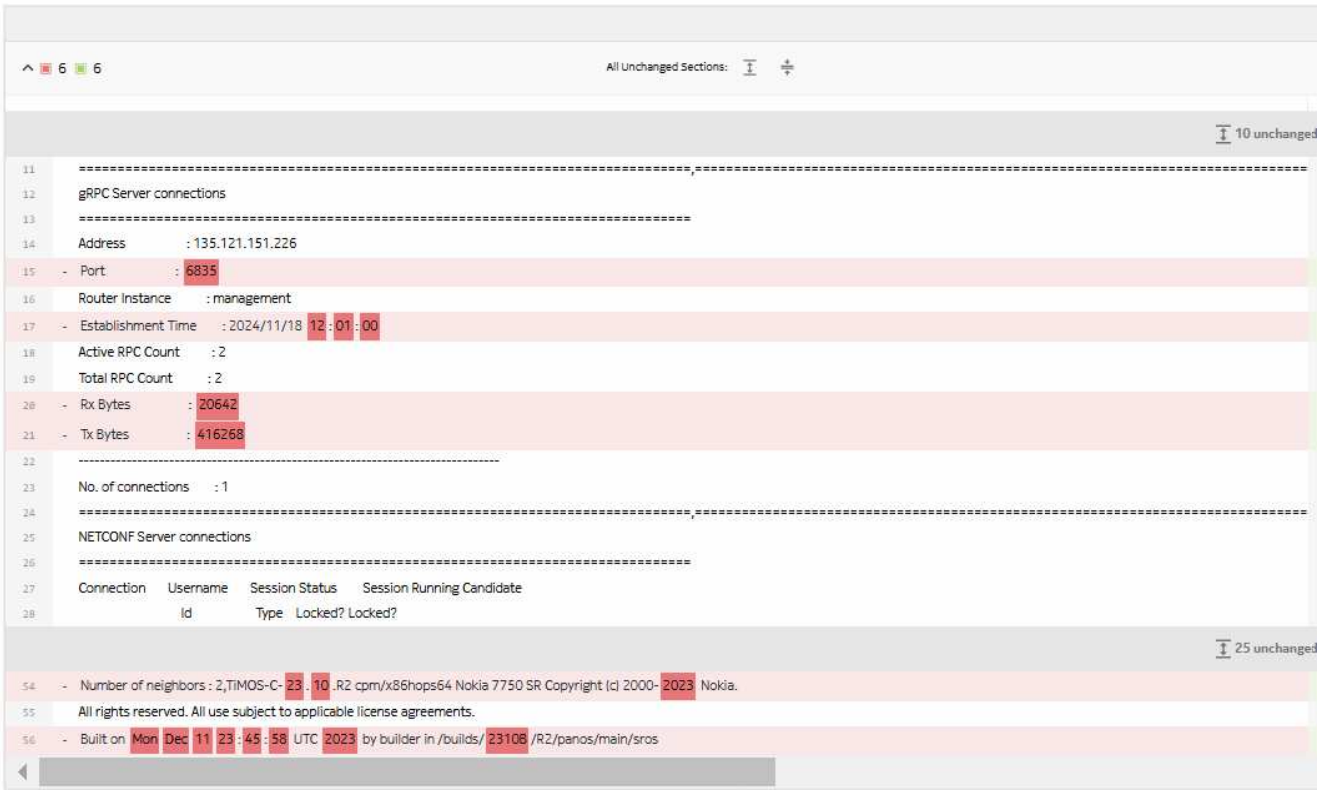
```
cmds:
        - show card
        - show system grpc connection
        - show system netconf connection
        - show router interface
        - show system lldp neighbor
        - show version
```

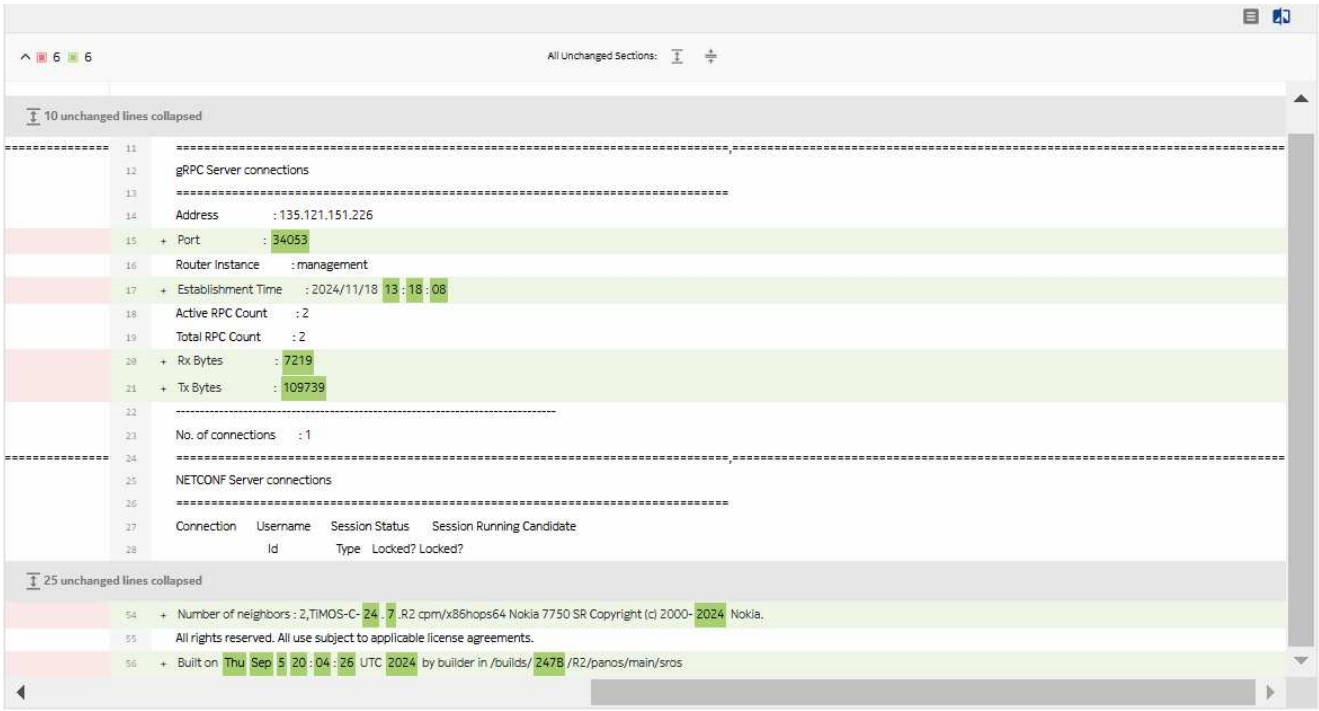
After enabling reporting for Pre-check and Reboot phases, users will see the new option “For detailed information, **view report**” in the info panel for these phases when they select ⋮ "View log". Users can pick any supported file format in the workflow: csv, yaml, json, txt.





Compare the reports:





8.14 Post-upgrade checks

8.14.1 Checks

For this use case, post-upgrade checks, show commands, and node configs are run on the nodes and compared to pre-upgrade.

NSP post-upgrade checks:

- Node version in Device Management is updated to the new version
- Network Health View, Network Map View, and Inventory View are updated as expected

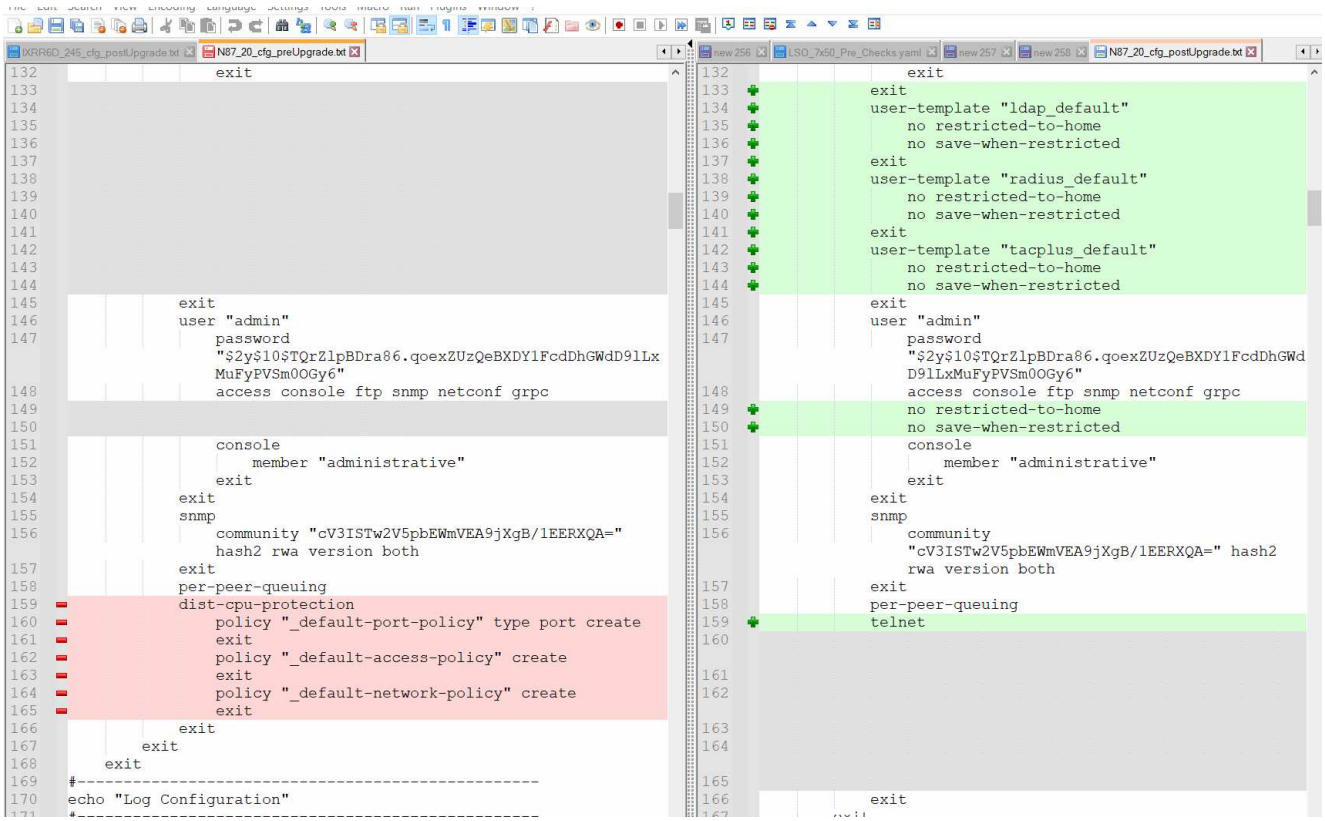
Additional NSP checks depend on NSP-enabled features. Some possible checks include:

- Service Management - all services are in the same state pre-upgrade
- Configuration Deployments (ICM) - deployment status is the same pre-upgrade
- Telemetry - stats collection works as expected post-upgrade
- OAM tests continue to pass post-node upgrade

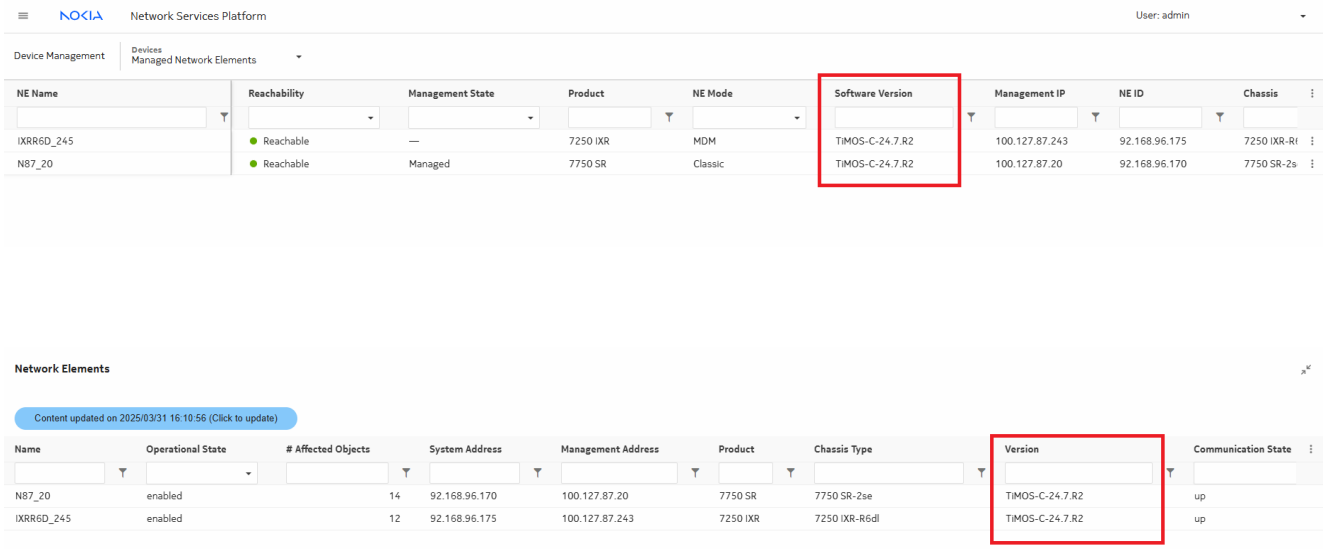
The following are examples of commands run during Pre-check. Run the commands again, then save the output to a file and compare it to the pre-upgrade output.

```
show card
show chassis
show mda
show version
show bof
show service service-using
show service sdp-using
show oam-pm tests
show system lldp neighbor
show router interface
show router rsvp neighbor
show router ospf neighbor
show system netconf connection
show system grpc connection
show port
show system information
```

The following 7750 SR example shows some default config changes occurred when upgrading from 23.10 R2 to 24.7 R2:



Users can check that the software version is successfully updated in Device Management and in the Network Elements dashboard:

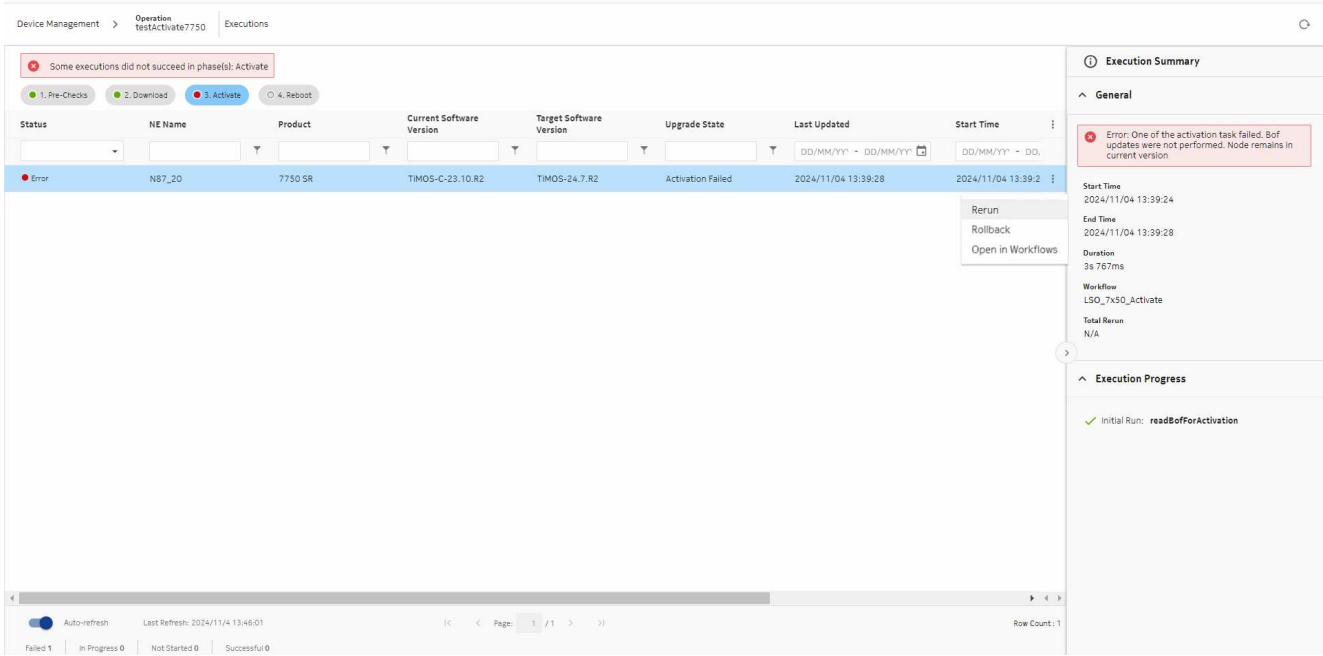


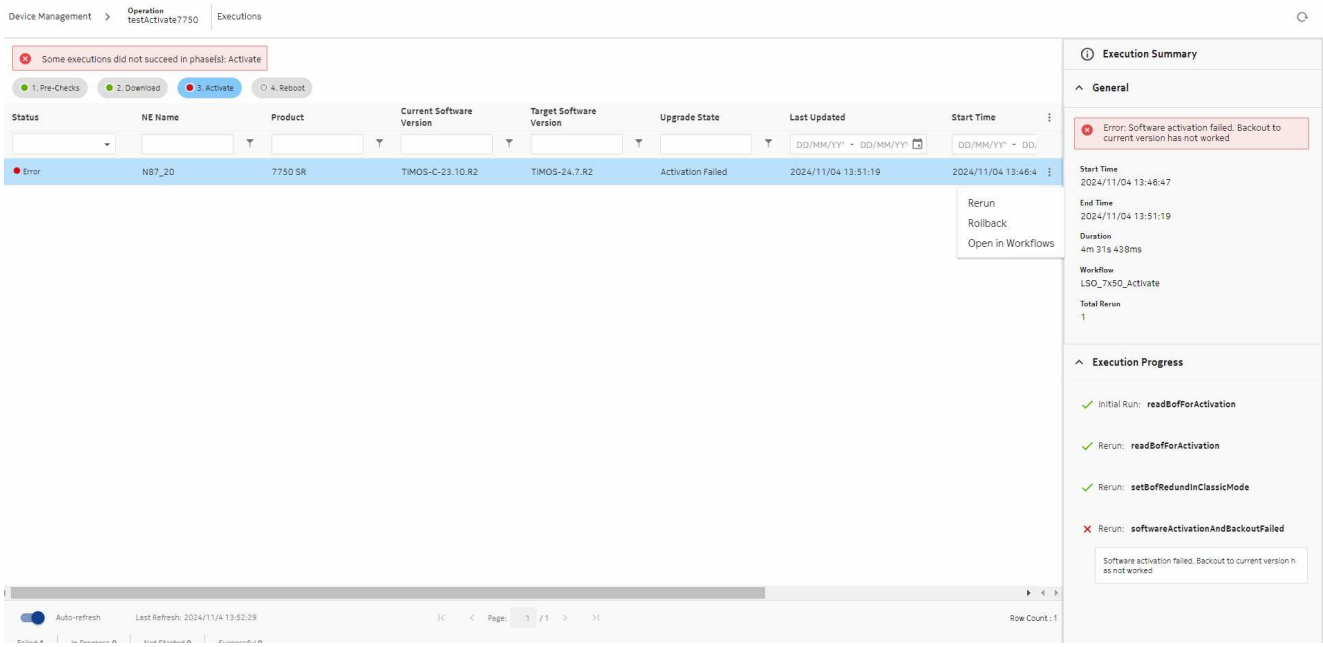
8.15 Troubleshooting upgrades

8.15.1 Fail scenarios

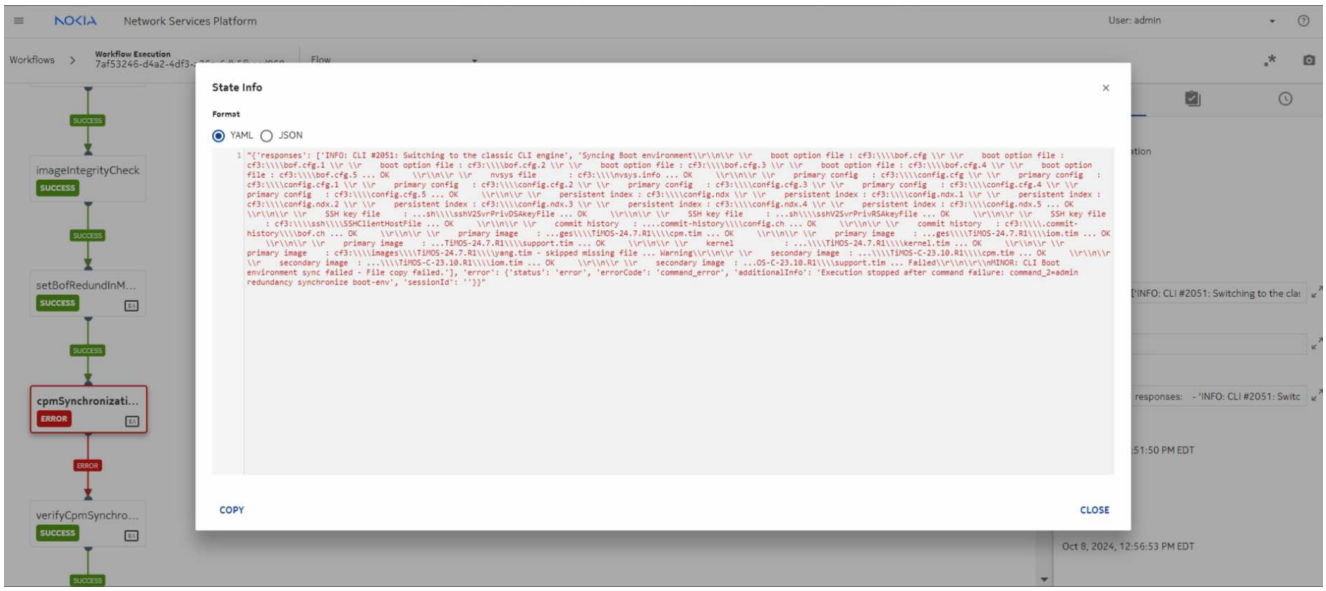
When an upgrade operation fails, users can click on the failed operation and select **Open in Workflows**. A new window will open.

Note: If auto cleanup is set to False, and there is not enough space on the node, the Activate will fail but will not show the accurate reason.





```
A:N87_20# show bof
===============================================================================

BOF (Memory)
===============================================================================

    primary-image     cf3:\images\TiMOS-24.7.R2
    primary-config    cf3:\7750SR2SE.cfg
    secondary-image   cf3:\images\TiMOS-SR-23.10.R2
    address           100.127.87.20/24 active
    address           100.127.87.21/24 standby
    primary-dns       138.120.252.56
    dns-domain        labs.ca.alcatel-lucent.com
    static-route      10.0.0.0/8 next-hop 100.127.87.1
    static-route      100.127.0.0/16 next-hop 100.127.87.1
    static-route      135.0.0.0/8 next-hop 100.127.87.1
    static-route      138.0.0.0/8 next-hop 100.127.87.1
    autonegotiate
    duplex            full
    speed             100
    wait              3
    persist           on
    no li-local-save
    no li-separate
===============================================================================

A:N87_20#
```



```
A:N87_20# show redundancy synchronization

===============================================================================
Synchronization Information
===============================================================================
Standby Status          : standby ready
Last Standby Failure    : N/A
Standby Up Time         : 2024/09/30 10:03:42
Standby Version         : TiMOS-C-23.10.R2 cpm/x86hops64 Nokia 7750 SR
                  Copyright (c) 2000-2023 Nokia.
                  All rights reserved. All use subject to
                  applicable license agreements.
                  Built on Mon Dec 11 23:45:58 UTC 2023 by
                  builder in /builds/2310B/R2/panos/main/sros
Failover Time           : N/A
Failover Reason         : N/A
Boot/Config Sync Mode   : Configuration
Boot/Config Sync Status : Boot environment synchronize failed
Last Config File Sync Time : 10/08/2024 10:13:10
Last Boot Env Sync Time : Never
Rollback Sync Mode      : None
Rollback Sync Status    : No Rollback synchronization
Last Rollback Sync Time : Never
Certificate Sync        : Enabled
Cert Sync Status        : unknown
Last Cert Sync Time     : Never
===============================================================================
A:N87_20#
```

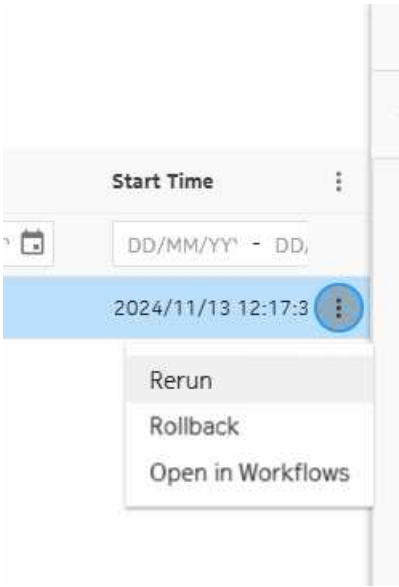
admin redundancy synchronize boot-env on the node manually

```
A:N87_20# admin redundancy synchronize boot-env
Syncing Boot environment
   boot option file : cf3:\bof.cfg.1 ... OK
   nvsys file       : cf3:\nvsys.info ... OK
   primary config   : cf3:\7750SR2SE.cfg.2 ... OK
   persistent index : cf3:\7750SR2SE.ndx.2 ... OK
   primary image    : ...ges\TiMOS-24.7.R2\cpm.tim ... Failed
```

MINOR: CLI Boot environment sync failed - Compact flash full or has no capacity on standby.

8.15.2 Solution

Delete some old files on the node and re-run the Activate phase.



8.15.3 Some useful node commands:

```
A:admin@IXRR6D_245# show redundancy synchronization
admin redundancy synchronize boot-env
show card B detail | match expression cf3 post-lines 10
show card A detail | match expression cf3 post-lines 10
```

```
A:N87_20# file version cf3-a:\boot.ldr
TiMOS-L-24.7.R2
Thu Sep 5 20:04:26 UTC 2024 by builder in /builds/247B/R2/panos/main/sros

A:N87_20# file version cf3-b:\boot.ldr
TiMOS-L-24.7.R2
Thu Sep 5 20:04:26 UTC 2024 by builder in /builds/247B/R2/panos/main/sros

A:N87_20#
```

9 UCC-33: LSP Enhanced Path Control

9.1 Overview

9.1.1 Purpose

This chapter describes the process required to configure LSP Enhanced Path Control on SR OS NEs using NSP. Two options for telemetry-based optimization, also called enhanced optimization, are presented.

Configuration examples in this chapter show NSP Release 24.4, SR OS 23.7.R2 NEs, and a VSR-NRC 24.3.R3 NE.

The following artifact bundles were used to test this use case:

- nsp-icm-intents-23.11.0-cam-bundle.zip
- nsp-telemetry-cr-va-sros-2.0.0-rel.8

See the NSP and NE documentation for more information.

9.1.2 Contents

Preparation

9.2 Prerequisites

9.2.1 Network configuration prerequisites

Before enhanced path control can be configured in NSP, the network configuration prerequisites must be met. The following table describes the requirements that can apply to similar use cases, and indicates whether each prerequisite is required for this use case.

Where an NSP intent type is not available, CLI or MD-CLI must be used to perform configuration on the device.

Prerequisite	Documentation reference	Notes
Mandatory for LSP Enhanced Path Control		
GRPC configuration 1. Generate security certificates 2. Configure security and enable GRPC on all devices 3. Apply security certificates on all devices	See SR TLS information here in the SR OS 24.3 R1 documentation: TLS	—
Netconf/SNMP provisioning: enable NETCONF and SNMP protocols on all devices	For more information about SNMP and NETCONF with SR OS, see SNMP and NETCONF in the *SR OS 24.3 R1 System Management Guide*.	—
NSP installation	Pathway for NSP system installation in the *NSP Installation and Upgrade Guide* How do I enable TLS for telemetry and gNMI on_change support? in the *NSP System Administrator Guide*.	Include the following in your deployment: • Feature packs: - platform-baseServices - platform-pluggableNetworkAdaptation - platform-loggingMonitoring - networkInfrastructureManagement-basicManagement - networkInfrastructureManagement-deviceConfig - enhancedOptimization • Adaptor suites: - sros-common - sros-oc-logical-inventory - sros-23-7-r1 • Additional required components: - VSR-NRC NE

Prerequisite	Documentation reference	Notes
Download the required artifact bundles from the NSP software delivery site: • NSP predefined set for ICM (device configuration) • vendor agnostic custom resources to support telemetry collection.	How do I install an artifact bundle? in the *NSP Network Automation Guide*	The vendor agnostic custom resources bundle is found on the NSP software delivery site, in the Adaptors folder along with your NE adaptor suite, for example, NSP → 23.11 → Adaptors → Nokia_SROS. Choose the zip file with va and cr in the filename, for example, `nsp-telemetry-cr-va-sros-1.0.0-rel.10.zip`.
Device discovery	Pathway for device discovery in the *NSP Classic Management User Guide* How do I discover devices? in the *NSP Device Management Guide* Nokia Developer Portal for information about FTP mediation policy creation using API.	—
Cards and MDAs provisioning	ICM process in the *NSP Device Management Guide* for more information about using the Device Configuration views, and the other procedures in the *NSP Device Management Guide* for further detail. See the NSP ICM Intent Type Catalog for information about this and other device configuration intent types developed by Nokia.	The intent type required for this configuration is icm-equipment-card-mda.
Connectors and Ports provisioning		The intent types required for this configuration are: • icm-equipment-port-connector • icm-equipment-port-ethernet
OSPF/ISIS	CLI Reference Guides for SR OS	—
LDPs, MPLS and RSVP configuration	CLI Reference Guides for SR OS	For LDP to be operational, the IPv4 and IPv6 bindings must be configured manually using CLI.
Interfaces Provisioning	How do I create a physical configuration deployment? in the *NSP Device Management Guide*.	The intent type required for this configuration is icm-router-network-interface
PCEP configuration	CLI Reference Guides for VSR-NRC	Most of the connections required for PCEP are established during previous configuration steps. For this use case, the VSR-NRC component must be correctly integrated with the setup. PCEP sessions between the routers in the network and the VSR-NRC component (VSR-I NE) must be established.
Optional		

Prerequisite	Documentation reference	Notes
Optional items to include in your NSP deployment	Pathway for NSP system installation in the *NSP Installation and Upgrade Guide* SR OS *Router Configuration Guide* for information about configuring Cflowd sampling on NEs.	• Optional feature packs: - An AuxDB - serviceActivationAndConfiguration-intentBasedServiceFulfillment To force incoming traffic to use a particular LSP path, the easiest way is to configure a service between the edge routers. The service can be provisioned using CLI, but if the user wishes to use NSP, the serviceActivationAndConfiguration-intentBasedServiceFulfillment feature pack must be included. The service fulfillment artifact bundle is also required for this option. If you choose to provision a service via NSP, a customer will also have to be provisioned via NSP's Device Management, Device Configuration views. • A Flow Collector (FC) and Flow Collector Controller (FCC) FC and FCC components are required if the older generation of 7250 IXRs are part of the Nokia SR OS network. For such devices, there is no gNMI telemetry support for collecting LSP/path statistics. Therefore, Cflowd sampling was used to collect interface/MPLS statistics. Cflowd sampling can be used for other NE types if preferred, however, this document assumes that gNMI telemetry will be used whenever possible. Older generation 7250 IXRs: - 7250 IXR-S - 7250 IXR-6 - 7250 IXR-R6 - 7250 IXR-10 - 7250 IXR-e • An NFM-P instance NFM-P is required if classically managed NEs are part of the network
Download the following artifact bundle from the NSP software delivery site: • NSP product artifact bundle for Service Fulfillment	How do I install an artifact bundle? in the *NSP Network Automation Guide*	—
BGP/EVPN	How do I create a logical configuration deployment? in the *NSP Device Management Guide*.	The intent type required for this configuration is icm-router-bgp_group

Prerequisite	Documentation reference	Notes
Segment Routing	CLI Reference Guides for SR OS	The examples in this use case use RSVP/MPLS LSPs. If SR-TE LSPs are used instead, segment routing configuration is mandatory.
Scheduler QoS Policies Network QoS Policies configuration	How do I create a logical configuration deployment? in the *NSP Device Management Guide*.	The intent types required for this configuration are: • icm-qos-schedulerpolicy-srqos • icm-qos-network-srqos • icm-qos-sapingress-srqos • icm-qos-sapegress-srqos
LAGs and MC-LAG creation	How do I create a logical configuration deployment? in the *NSP Device Management Guide*.	The intent types required for this configuration are: • icm-logical-lag-access • icm-logical-mc_lag-access

9.3 Install the required artifact bundles

9.3.1 Purpose

Use this procedure to make the required artifacts, intent types and telemetry files, available to NSP. This procedure is based on the procedure for installing an artifact bundle in the *NSP Network Automation Guide*.

For example, the reference procedure in NSP 24.4 is How do I install an artifact bundle?.

9.3.2 Steps

Download the required intent types

1

Download the ICM and CN telemetry artifact bundles from the NSP software delivery site.

Navigate through the hierarchy to the folder of artifacts that can be imported using the Artifacts views, for example: NSP → 24.4 → Artifacts → Artifact_Admin_Import.

See the description to verify which bundles to download.

Install an artifact bundle in NSP

2

Log in to the NSP.

3

Open **Artifacts**, **Artifact Bundles**.

4

Click **IMPORT & INSTALL**.

5

In the form that opens, drag and drop the zip files, or click **Browse** and navigate to the files on your system.

6

To install the artifact bundles immediately, click **IMPORT & INSTALL**. To import without installing, click **IMPORT**.

The chosen operation is triggered immediately. The artifact bundle status is updated to Imported or Installed when NSP has confirmed the status of all artifacts in the artifact bundle.

7

To install a bundle in Imported status, choose **Install bundle** from the ⋮ (Table row actions) menu.

END OF STEPS

MPLS LSP provisioning

9.4 Provision MPLS LSPs using Device Configuration

9.4.1 Purpose

Use this procedure to configure MPLS LSPs using the Device Management views. This procedure is based on the overall device configuration procedure in the *NSP Device Management Guide*.

For example, the reference procedure in NSP Release 24.4 is ICM Process

The intent type required is `icm-te-tunnel`.

9.4.2 Prerequisites

Intent types must be installed and imported to NSP; see 9.3 “Install the required artifact bundles” (p. 448).

For this use case, the following parameters must be configured:

- `egress-statistics` must be enabled on the LSPs of the NE. This parameter may be enabled by default upon provisioning, depending on the NE type.
- `pce-report` - this parameter must be enabled for the LSP to appear in Path Control in NSP. This attribute is enabled by default upon provisioning.

9.4.3 Steps

Import the intent type

1

Log in the NSP.

2

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

3

Click + **IMPORT**

4

Choose the `icm-te-tunnel` intent type from the list and click **IMPORT**.

Create a configuration template

5

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

6

Click **+ TEMPLATE**

7

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

Note: Template names cannot start or end with a space, or contain special characters other than spaces, underscores, or hyphens.

8

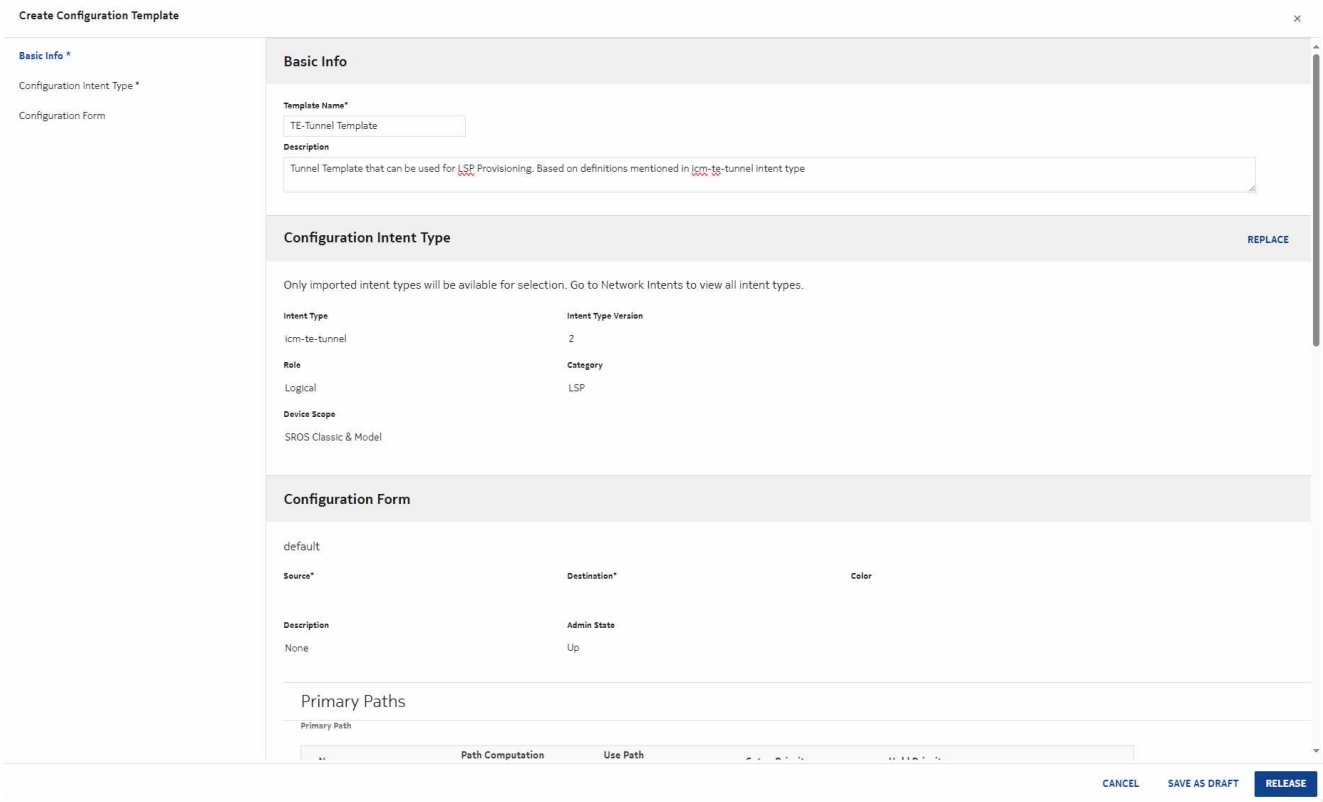
Click **+ INTENT TYPE** and choose the `icm-te-tunnel` intent type.

9

Choose a configuration form from the drop-down list.

10

Click **RELEASE** to create the template in released state.



The configuration template is added to the list.

Deploy the configuration

11

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

b. From the list, choose a template you created in the previous steps and click ⋮ (More actions) **Deploy to Network**.

The form opens with the template already selected.

12

Choose the target NE:

1. Click + **TARGET** and choose **NEs** from the drop-down list.
2. Choose an NE from the list to add to the Bin.
3. Verify that the correct NE is shown in the Bin and click **ADD**.

13

1. Click **VIEW/EDIT TEMPLATE CONFIG**.
2. In the form that opens, configure the template parameters. The following parameters are required:
   - A primary path must be added:
     Use Path Computation must be enabled
     path-computation-method must be **path-locally-computed**
   - **Signaling Type** must be **RSVP**.
   - An association object must be created, with the path profile associated to the LSP.
     The path profile is created in Path Control; see 9.6 “Create a bandwidth-based path profile” (p. 455) and 9.12 “Create a latency-based path profile” (p. 467)
     It is not necessary to create path profiles before performing this procedure.
3. Click **UPDATE**.

In this example, no secondary path is provisioned.

14

Identifier fields appear in the form for each selected template. Enter information in each field.

Attention: Your input can’t contain the hash symbol (#).

15

Click **DEPLOY** to apply the configuration to the targets.

Audit the configuration

16

Perform an audit to verify that the configuration has deployed correctly:

1. Open **Device Management**, **Configuration Deployments**.
2. Choose a deployment.
3. Click ⓘ if needed to open the **Deployment Details** panel.
4. Click **AUDIT CONFIG**. The audit results and alignment status information are updated.

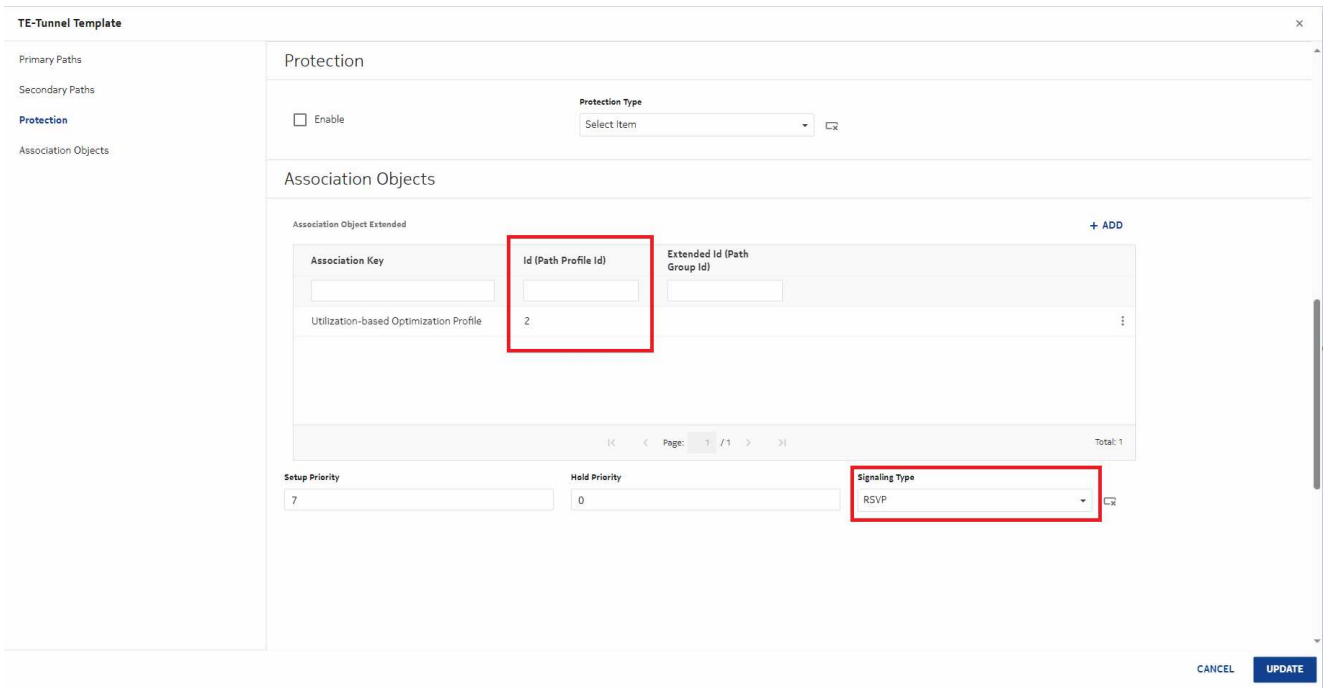
Repeat to deploy other LSPs

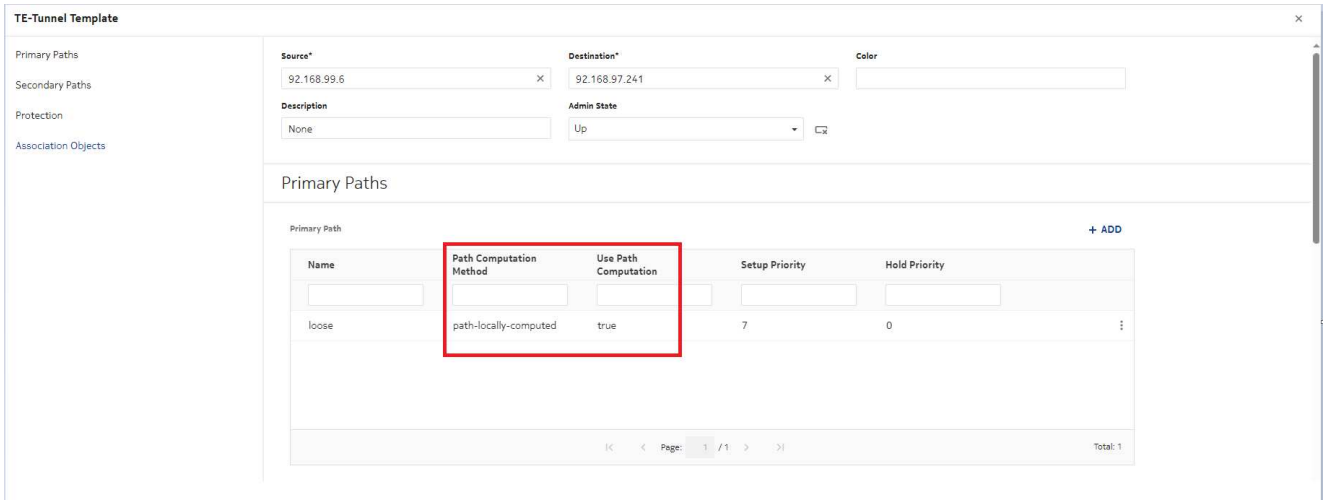
17

Repeat this procedure to deploy all other LSPs. Ensure that the correct path profile is assigned to each LSP.

END OF STEPS

9.4.4 LSP creation example, template parameters





Use case 1: Utilization/Bandwidth optimization

9.5 Bandwidth optimization

9.5.1 Overview

This use case demonstrates NSP's Path Control Bandwidth optimization. With bandwidth optimization, optimization is triggered when link utilization exceeds a configured threshold.

To perform bandwidth optimization, create a path profile to optimize on Cost, with Telemetry as the bandwidth strategy.

9.6 Create a bandwidth-based path profile

9.6.1 Purpose

Use this procedure to configure a path profile for bandwidth optimization, using the Path Control view.

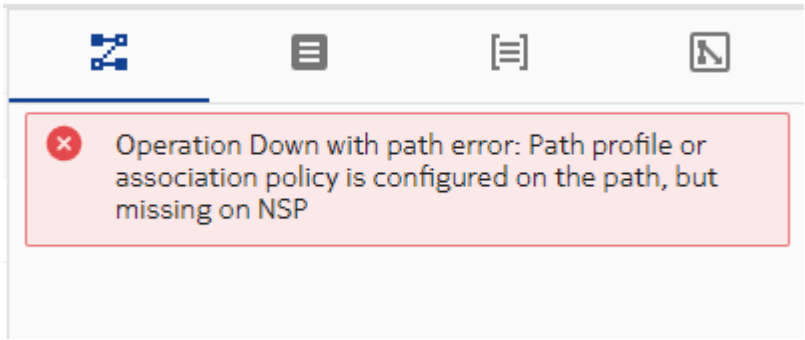
This procedure is based on the following:

- the procedure to configure a path profile policy in the *NSP Path Control and Simulation Guide*
- an API call using the NSP Path Control API

For example, the reference procedures in NSP Release 24.4 are:

- How do I create a path profile policy?
- Swagger documentation for the NSP Path Control API on the Nokia Developer Portal

Note: If LSPs were created with path profile IDs before the creation of path profiles, an error message is displayed showing that a path profile or association policy is configured on the path but missing on NSP. This is expected and will resolve when the profiles are created.



9.6.2 Steps

Create a path profile policy

1

Log in to the NSP.

2

From the **Path Control, Path Profiles** view, click **Create Policy** ⊕. The Create Path Profile policy form opens.

3

Configure the required parameters:

- the Profile ID parameter must match the profile ID number configured for the LSPs in Step 13 of 9.4 “Provision MPLS LSPs using Device Configuration” (p. 450).
- Optimize on (Objective) must be Cost
- Bandwidth Strategy must be Telemetry

4

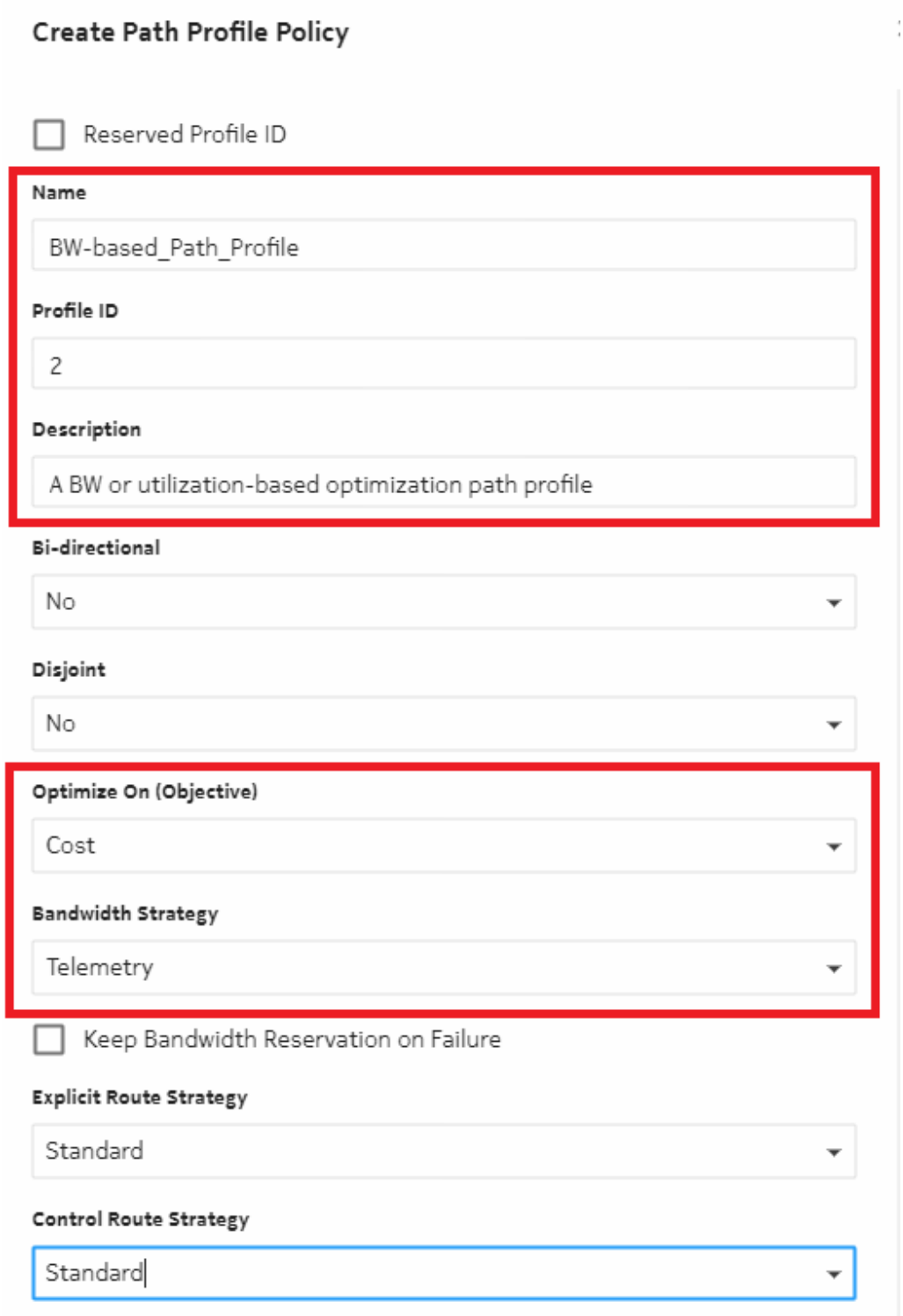
As required, Exclude Route Objects by adding the IP address(es) of the object(s) to be excluded.

5

As required, Include Route Objects by adding the IP address(es) of the object(s) to be included. You must also specify Hop Type.

6

Click **CREATE**. The Path Profile policy is created.



Re-signal LSPs

7

Now that the path profile policy is in place, the LSPs assigned to the profile can be brought up:

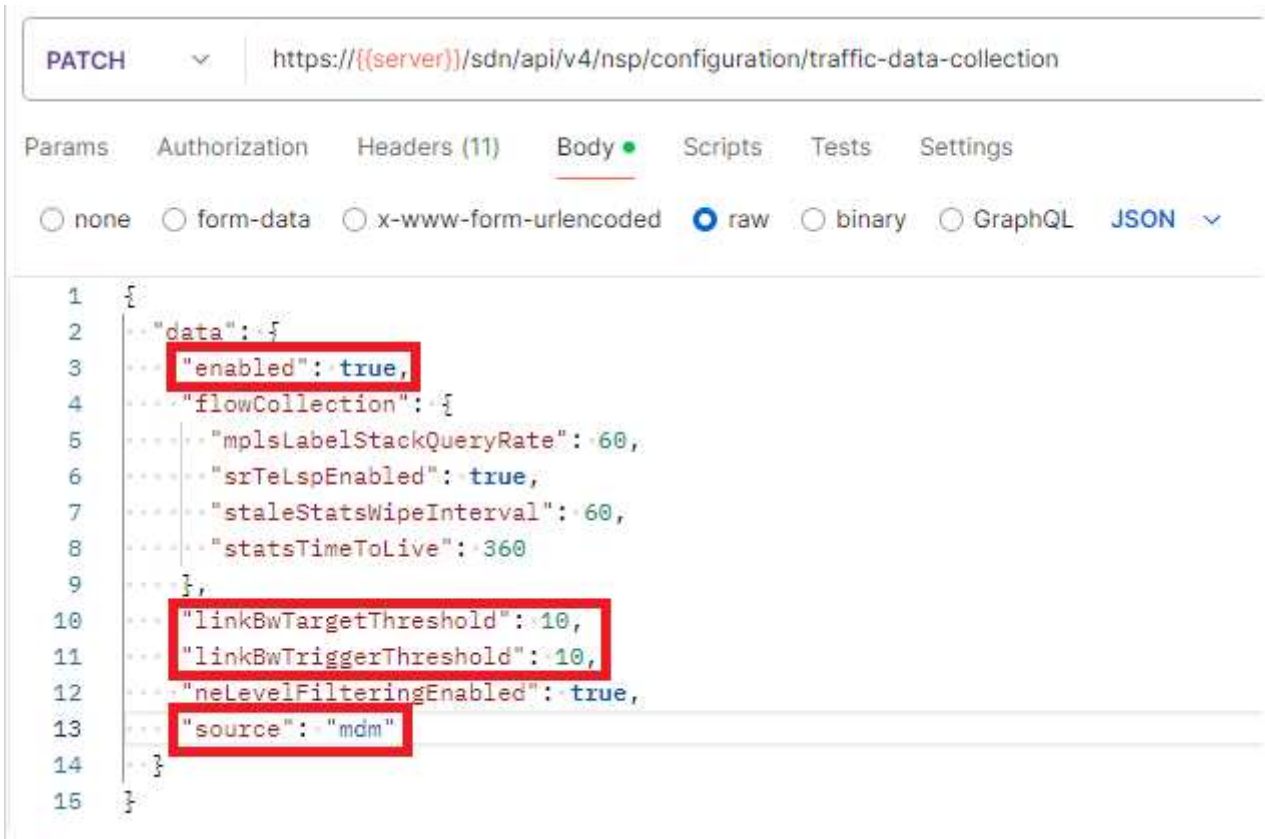
1. Open the **Path Control, LSPs** view.
2. Select an LSP and click ⋮ (Table row actions), **Resignal**.

END OF STEPS

9.7 Enable traffic collection parameters using an API

9.7.1 Allow Path Control to receive the bandwidth measurements from the network

The next step is to configure specific parameters and subscriptions to enable collection and set thresholds. There is no UI support for this: the pre-requisites can be configured via a specific NSP Path Control API call. See the following example:

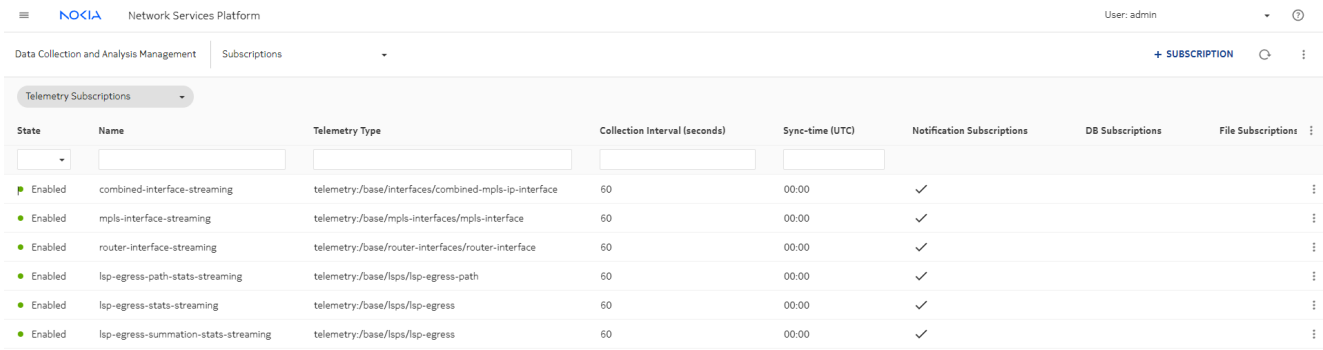


In this example, the BW link threshold values were set to 10, which means 10%. Therefore, if a particular link has a utilization value exceeding 10%, NSP's Path Control module will attempt to re-

route one or more LSPs, avoiding that link. It is important to note that for this use case to work, the 'source' value must also be set to 'mdm'.

When the call is successful, real-time BW measurements in Path Control for both LSP and link objects are displayed. The measurements are updated approximately every minute.

Following the API call, streaming telemetry subscriptions for reporting link and LSP bandwidth are automatically created, as shown in the following figure.



9.8 Monitor bandwidth

9.8.1 Monitoring links in Path Control

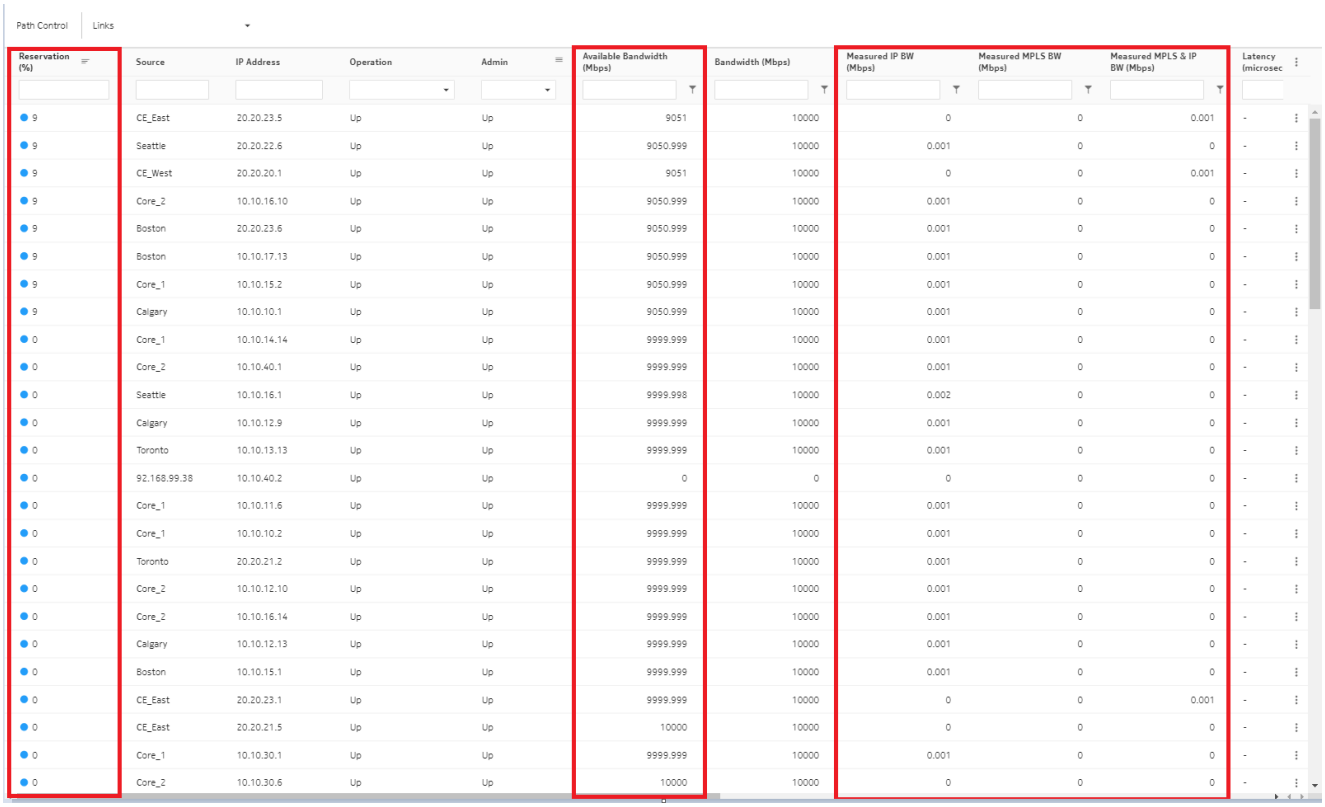
Open the **Path Control**, **Links** view and select a link.

You can click **LSPS** in the Info panel to see LSPs on the selected link.

The following columns show bandwidth data:

- Utilization/Reservation (%)
- Available Bandwidth

  Note: Available Bandwidth is Total Link Bandwidth — Consumed Bandwidth. Bandwidth can be reserved for another LSP using the same link.
- Bandwidth
- Measured IP BW: pure IP traffic on the link
- Measured MPLS BW: MPLS traffic over the link (the sum of all LSPs using the link)
- Measured MPLS & IP BW: this value is only used for 7250 IXR NEs. These NEs do not split MPLS and IP traffic.

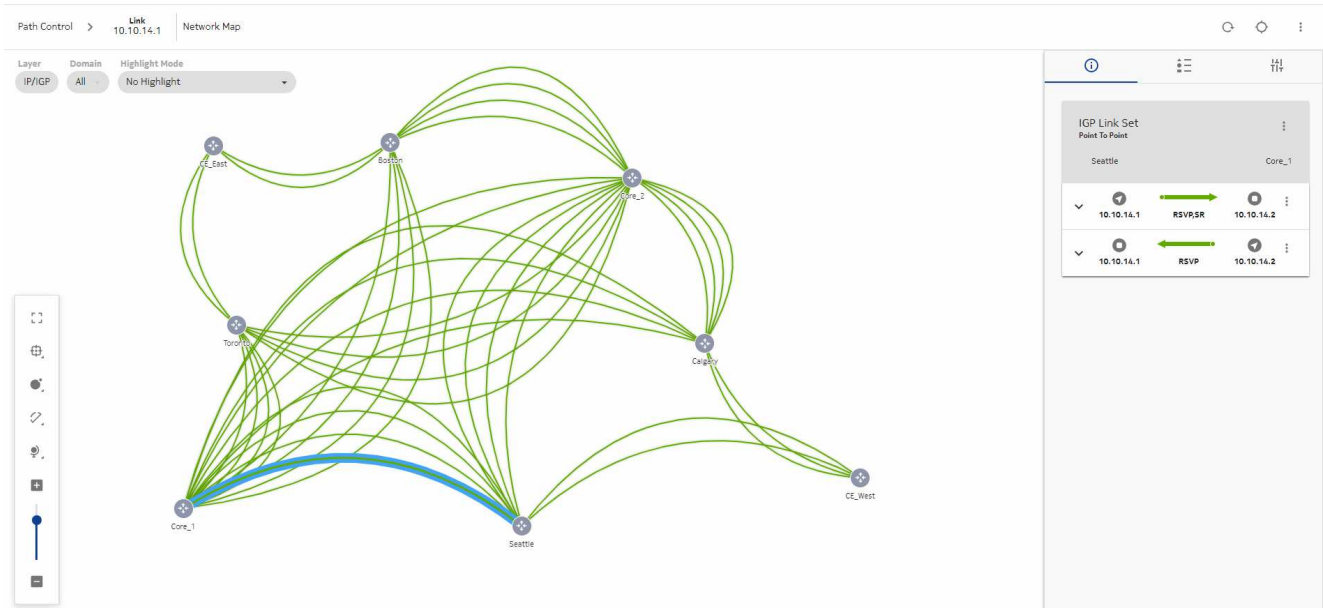


Path Control | Links

Reservation (%)	Source	IP Address	Operation	Admin	Available Bandwidth (Mbps)	Bandwidth (Mbps)	Measured IP BW (Mbps)	Measured MPLS BW (Mbps)	Measured MPLS & IP BW (Mbps)	Latency (microsec
9	CE_East	20.20.23.5	Up	Up	9051	10000	0	0	0.001	-
9	Seattle	20.20.22.6	Up	Up	9050.999	10000	0.001	0	0	-
9	CE_West	20.20.20.1	Up	Up	9051	10000	0	0	0.001	-
9	Core_2	10.10.16.10	Up	Up	9050.999	10000	0.001	0	0	-
9	Boston	20.20.23.6	Up	Up	9050.999	10000	0.001	0	0	-
9	Boston	10.10.17.13	Up	Up	9050.999	10000	0.001	0	0	-
9	Core_1	10.10.15.2	Up	Up	9050.999	10000	0.001	0	0	-
9	Calgary	10.10.10.1	Up	Up	9050.999	10000	0.001	0	0	-
0	Core_1	10.10.14.14	Up	Up	9999.999	10000	0.001	0	0	-
0	Core_2	10.10.40.1	Up	Up	9999.999	10000	0.001	0	0	-
0	Seattle	10.10.16.1	Up	Up	9999.998	10000	0.002	0	0	-
0	Calgary	10.10.12.9	Up	Up	9999.999	10000	0.001	0	0	-
0	Toronto	10.10.13.13	Up	Up	9999.999	10000	0.001	0	0	-
0	92.168.99.38	10.10.40.2	Up	Up	0	0	0	0	0	-
0	Core_1	10.10.11.6	Up	Up	9999.999	10000	0.001	0	0	-
0	Core_1	10.10.10.2	Up	Up	9999.999	10000	0.001	0	0	-
0	Toronto	20.20.21.2	Up	Up	9999.999	10000	0.001	0	0	-
0	Core_2	10.10.12.10	Up	Up	9999.999	10000	0.001	0	0	-
0	Core_2	10.10.16.14	Up	Up	9999.999	10000	0.001	0	0	-
0	Calgary	10.10.12.13	Up	Up	9999.999	10000	0.001	0	0	-
0	Boston	10.10.15.1	Up	Up	9999.999	10000	0.001	0	0	-
0	CE_East	20.20.23.1	Up	Up	9999.999	10000	0	0	0.001	-
0	CE_East	20.20.21.5	Up	Up	10000	10000	0	0	0	-
0	Core_1	10.10.30.1	Up	Up	9999.999	10000	0.001	0	0	-
0	Core_2	10.10.30.6	Up	Up	10000	10000	0	0	0	-

Click ⋮ (Table row actions), **Show on map** to display the link in a network map format.

Click on the highlighted link to display link information in the Info panel.

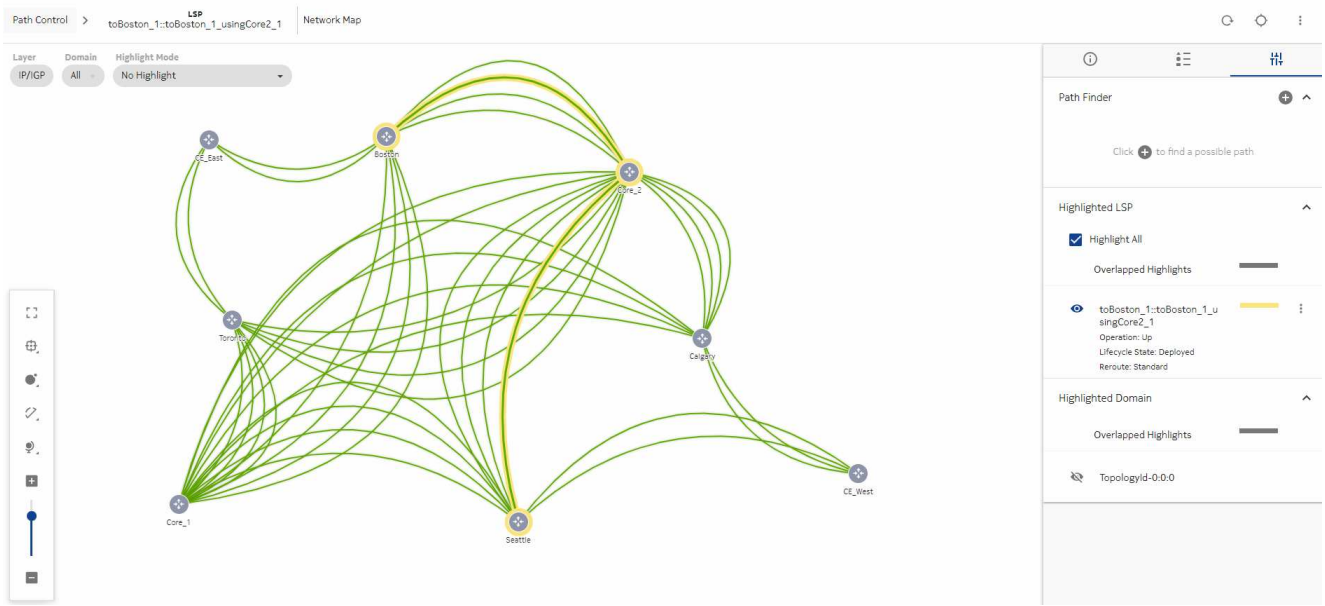


9.8.2 Monitoring LSPs in Path Control

Open the **Path Control**, **LSPs** and select an LSP.

- The Hops panel in the Info panel shows the LSP paths.
- The following columns show bandwidth data:
  - Bandwidth
  - Telemetry Measured BW

Click ⋮ (Table row actions), **Show on map** to display the LSP in a network map format.



Click on a link to display link information in the Info panel.

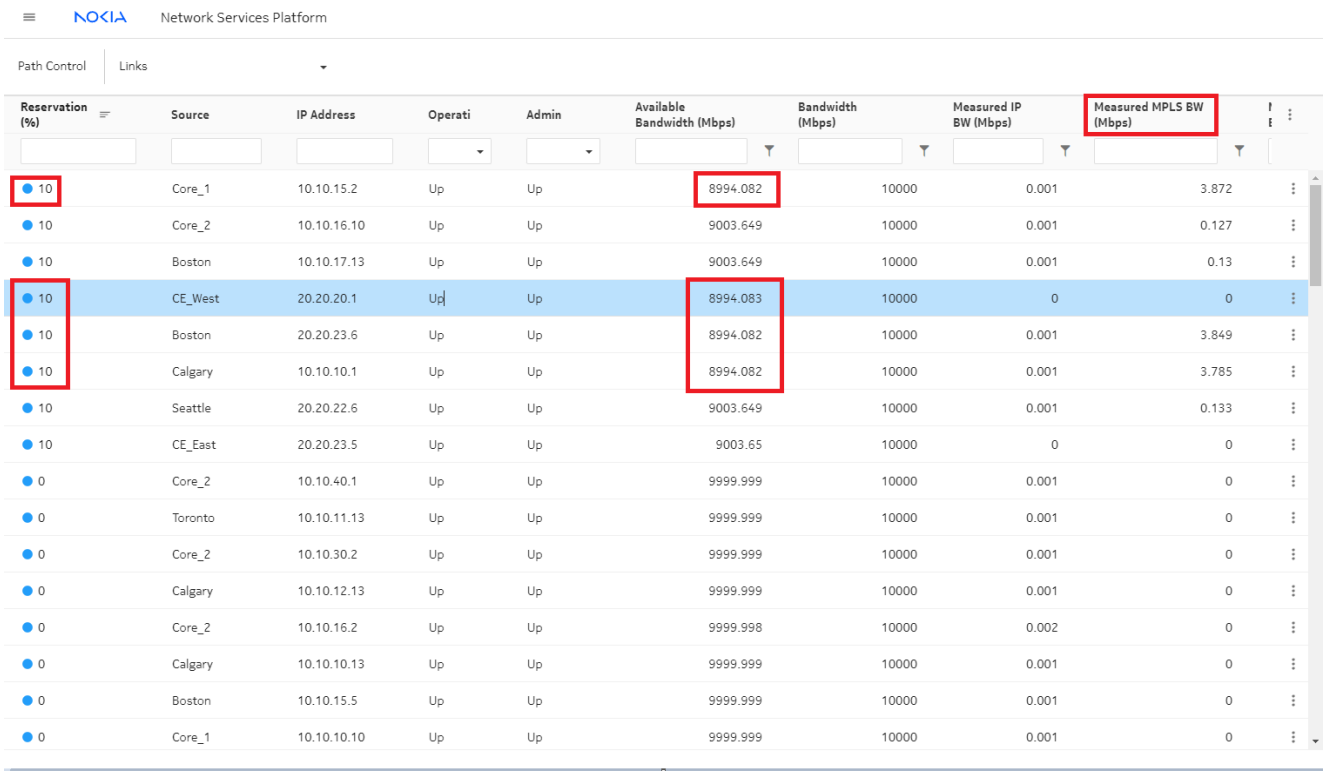
9.9 Bandwidth optimization

9.9.1 Link rerouting

After injecting some traffic, we can check the Path Control, Links view to see that at least one LSP has been rerouted to bypass links where utilization exceeds the configured threshold value of 10%.

Note: To demonstrate this particular use case, the iPerf3 tool was used to inject traffic (i.e. to simulate real-live traffic).

Example, before optimization:

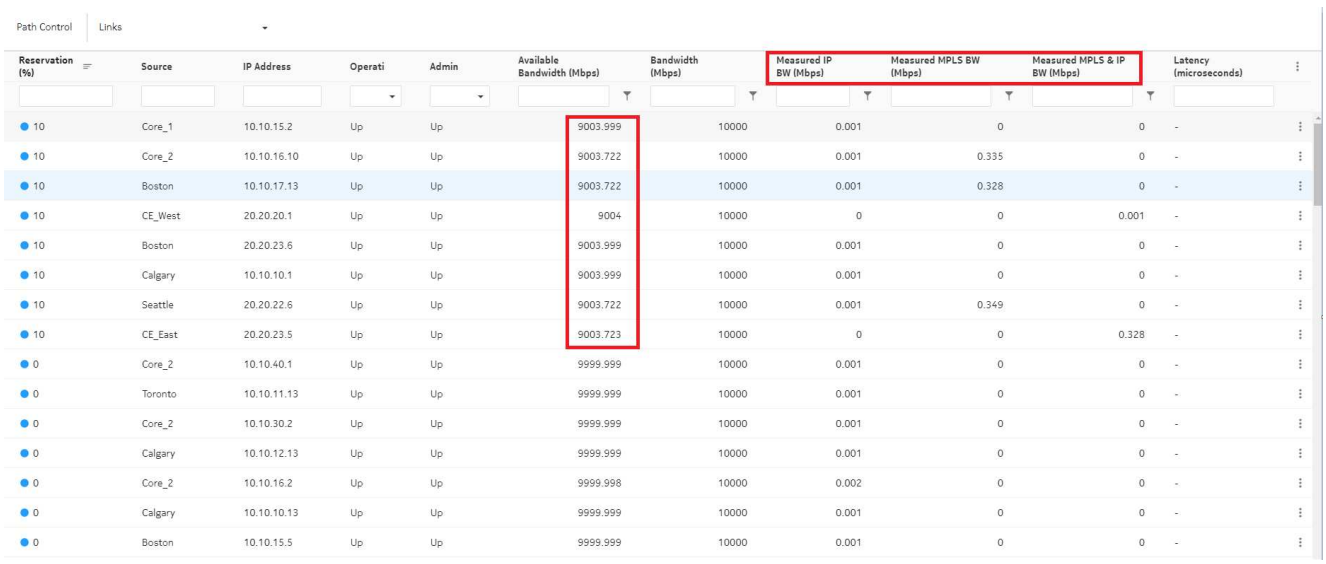


Network Services Platform

Path Control | Links

Reservation (%)	Source	IP Address	Operati	Admin	Available Bandwidth (Mbps)	Bandwidth (Mbps)	Measured IP BW (Mbps)	Measured MPLS BW (Mbps)
10	Core_1	10.10.15.2	Up	Up	8994.082	10000	0.001	3.872
10	Core_2	10.10.16.10	Up	Up	9003.649	10000	0.001	0.127
10	Boston	10.10.17.13	Up	Up	9003.649	10000	0.001	0.13
10	CE_West	20.20.20.1	Up	Up	8994.083	10000	0	0
10	Boston	20.20.23.6	Up	Up	8994.082	10000	0.001	3.849
10	Calgary	10.10.10.1	Up	Up	8994.082	10000	0.001	3.785
10	Seattle	20.20.22.6	Up	Up	9003.649	10000	0.001	0.133
10	CE_East	20.20.23.5	Up	Up	9003.65	10000	0	0
0	Core_2	10.10.40.1	Up	Up	9999.999	10000	0.001	0
0	Toronto	10.10.11.13	Up	Up	9999.999	10000	0.001	0
0	Core_2	10.10.30.2	Up	Up	9999.999	10000	0.001	0
0	Calgary	10.10.12.13	Up	Up	9999.999	10000	0.001	0
0	Core_2	10.10.16.2	Up	Up	9999.998	10000	0.002	0
0	Calgary	10.10.10.13	Up	Up	9999.999	10000	0.001	0
0	Boston	10.10.15.5	Up	Up	9999.999	10000	0.001	0
0	Core_1	10.10.10.10	Up	Up	9999.999	10000	0.001	0

Example, after optimization:



Path Control | Links

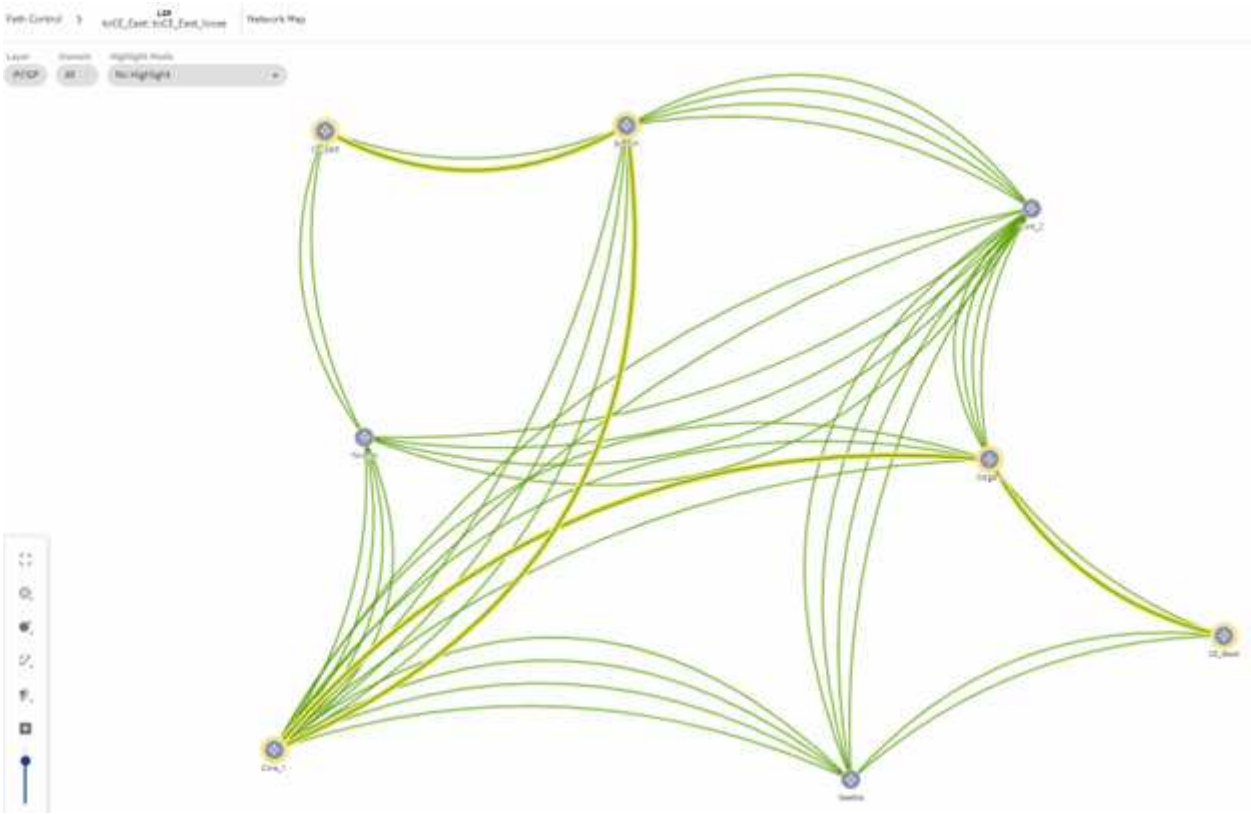
Reservation (%)	Source	IP Address	Operati	Admin	Available Bandwidth (Mbps)	Bandwidth (Mbps)	Measured IP BW (Mbps)	Measured MPLS BW (Mbps)	Measured MPLS & IP BW (Mbps)	Latency (microseconds)
10	Core_1	10.10.15.2	Up	Up	9003.999	10000	0.001	0	0	-
10	Core_2	10.10.16.10	Up	Up	9003.722	10000	0.001	0.335	0	-
10	Boston	10.10.17.13	Up	Up	9003.722	10000	0.001	0.328	0	-
10	CE_West	20.20.20.1	Up	Up	9004	10000	0	0	0.001	-
10	Boston	20.20.23.6	Up	Up	9003.999	10000	0.001	0	0	-
10	Calgary	10.10.10.1	Up	Up	9003.999	10000	0.001	0	0	-
10	Seattle	20.20.22.6	Up	Up	9003.722	10000	0.001	0.349	0	-
10	CE_East	20.20.23.5	Up	Up	9003.723	10000	0	0	0.328	-
0	Core_2	10.10.40.1	Up	Up	9999.999	10000	0.001	0	0	-
0	Toronto	10.10.11.13	Up	Up	9999.999	10000	0.001	0	0	-
0	Core_2	10.10.30.2	Up	Up	9999.999	10000	0.001	0	0	-
0	Calgary	10.10.12.13	Up	Up	9999.999	10000	0.001	0	0	-
0	Core_2	10.10.16.2	Up	Up	9999.998	10000	0.002	0	0	-
0	Calgary	10.10.10.13	Up	Up	9999.999	10000	0.001	0	0	-
0	Boston	10.10.15.5	Up	Up	9999.999	10000	0.001	0	0	-

None of the links has available bandwidth lower than 9 000 Mbps. The network has optimized itself; redirecting LSPs to other links.

9.9.2 Network map views

The change to the path is clear in the network map.

Network map example, before optimization:



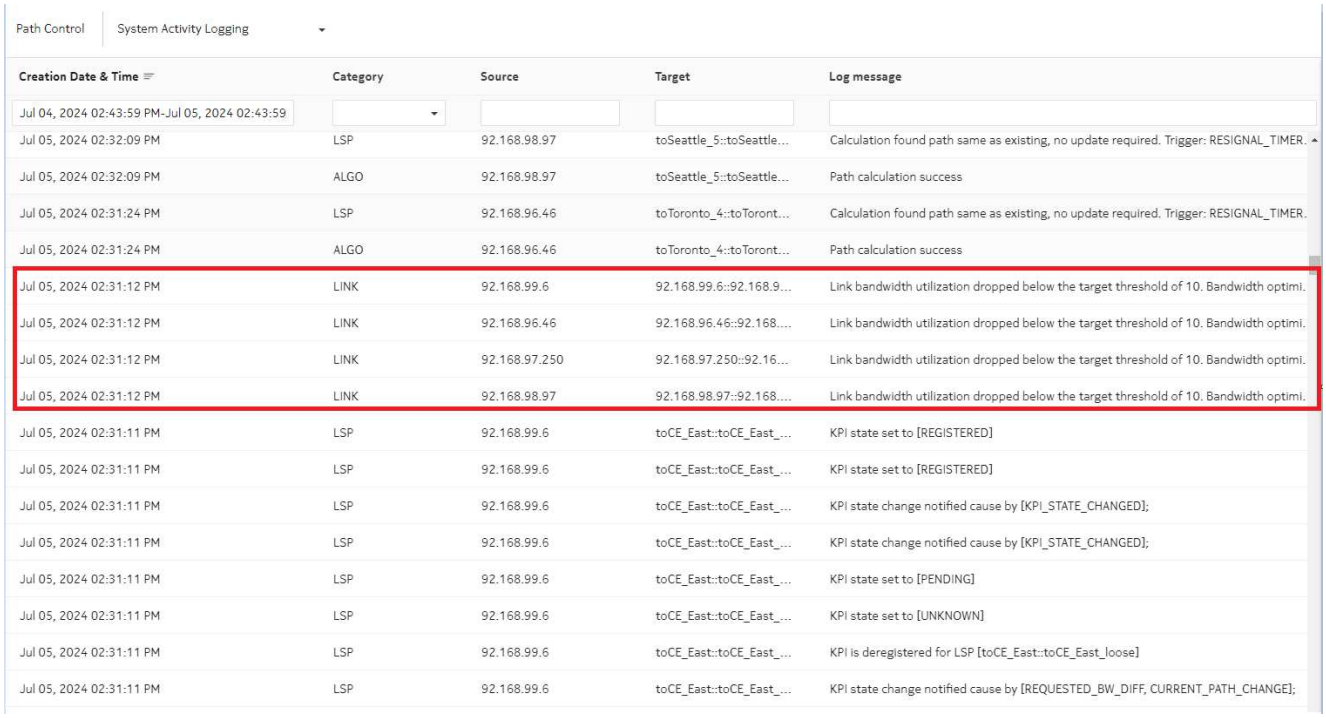
Network map example, after optimization:

9.10 System activity logging after bandwidth optimization

9.10.1 Monitor events in real time

To view system event logs, open the **Path Control**, **System Activity Logging** view.

The logs show the bandwidth optimization operation on the links, as seen in the following example:



Use case 2: Latency-based optimization

9.11 Latency optimization

9.11.1 Overview

This use case demonstrates NSP's Path Control latency-based optimization. With latency-based optimization, optimization is triggered when latency exceeds a configured threshold.

To perform latency-based optimization, create a path profile to optimize on Latency, with Telemetry as the bandwidth strategy.

9.12 Create a latency-based path profile

9.12.1 Purpose

Use this procedure to configure a path profile for latency-based optimization, using the Path Control view.

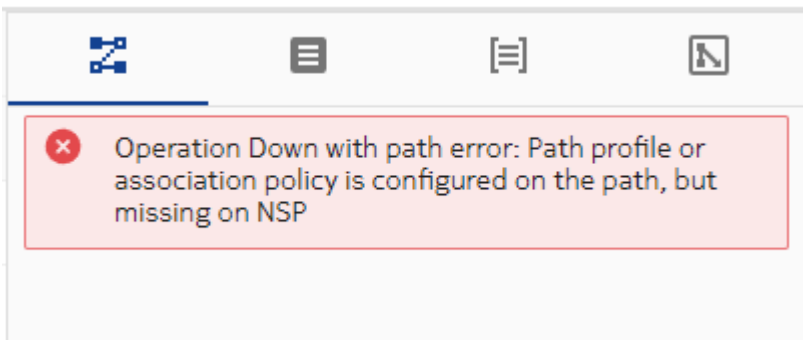
This procedure is based on the following:

- the procedure to configure a path profile policy in the *NSP Path Control and Simulation Guide*

For example, the reference procedures in NSP Release 24.4 are:

- How do I create a path profile policy?
- Swagger documentation for the NSP Path Control API on the Nokia Developer Portal

Note: If LSPs were created with path profile IDs before the creation of path profiles, an error message is displayed showing that a path profile or association policy is configured on the path but missing on NSP. This is expected and will resolve when the profiles are created.



9.12.2 Steps

1

Log in to the NSP.

2

From the **Path Control, Path Profiles** view, click **Create Policy** ⊕. The Create Path Profile policy form opens.

3

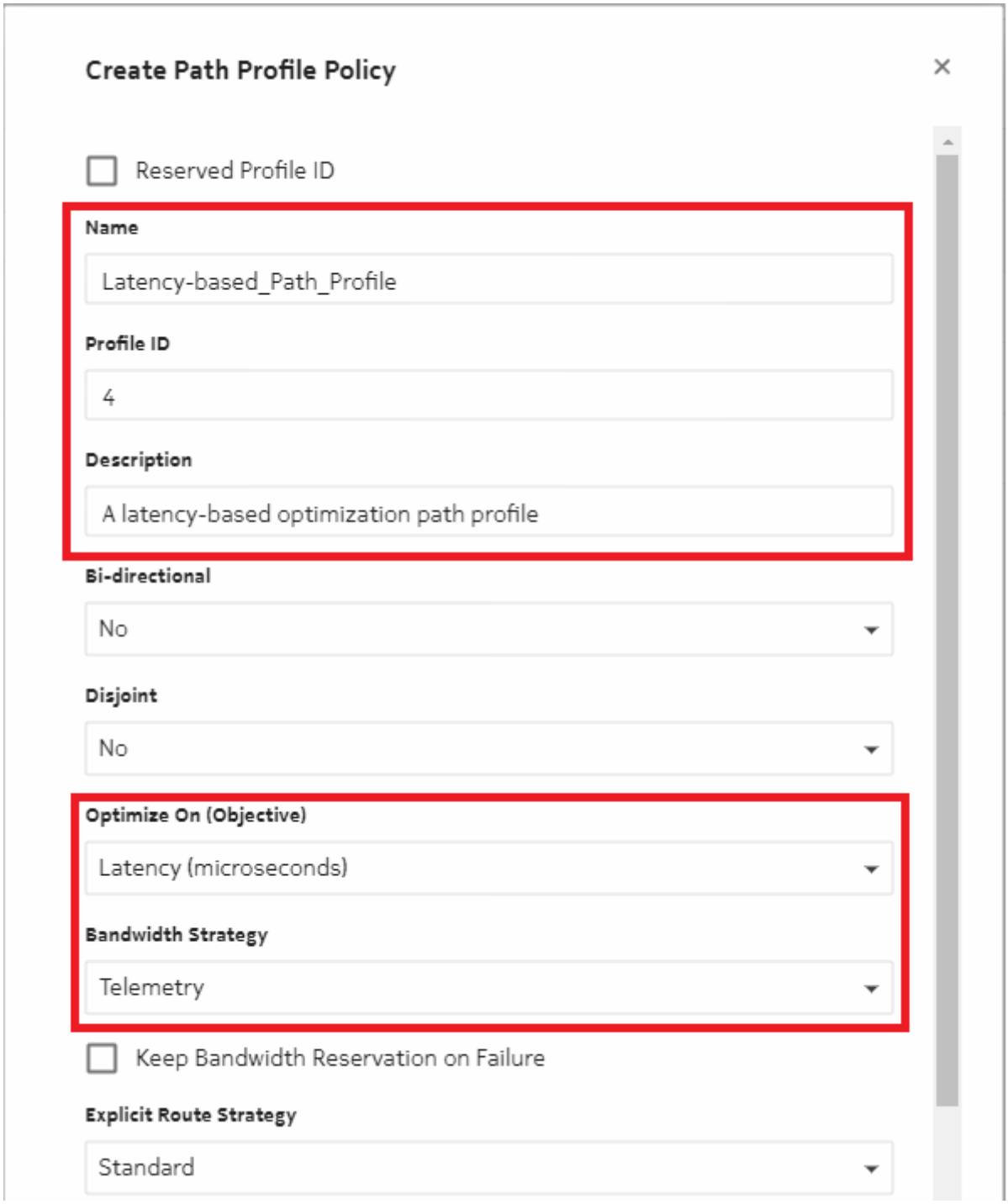
Configure the required parameters:

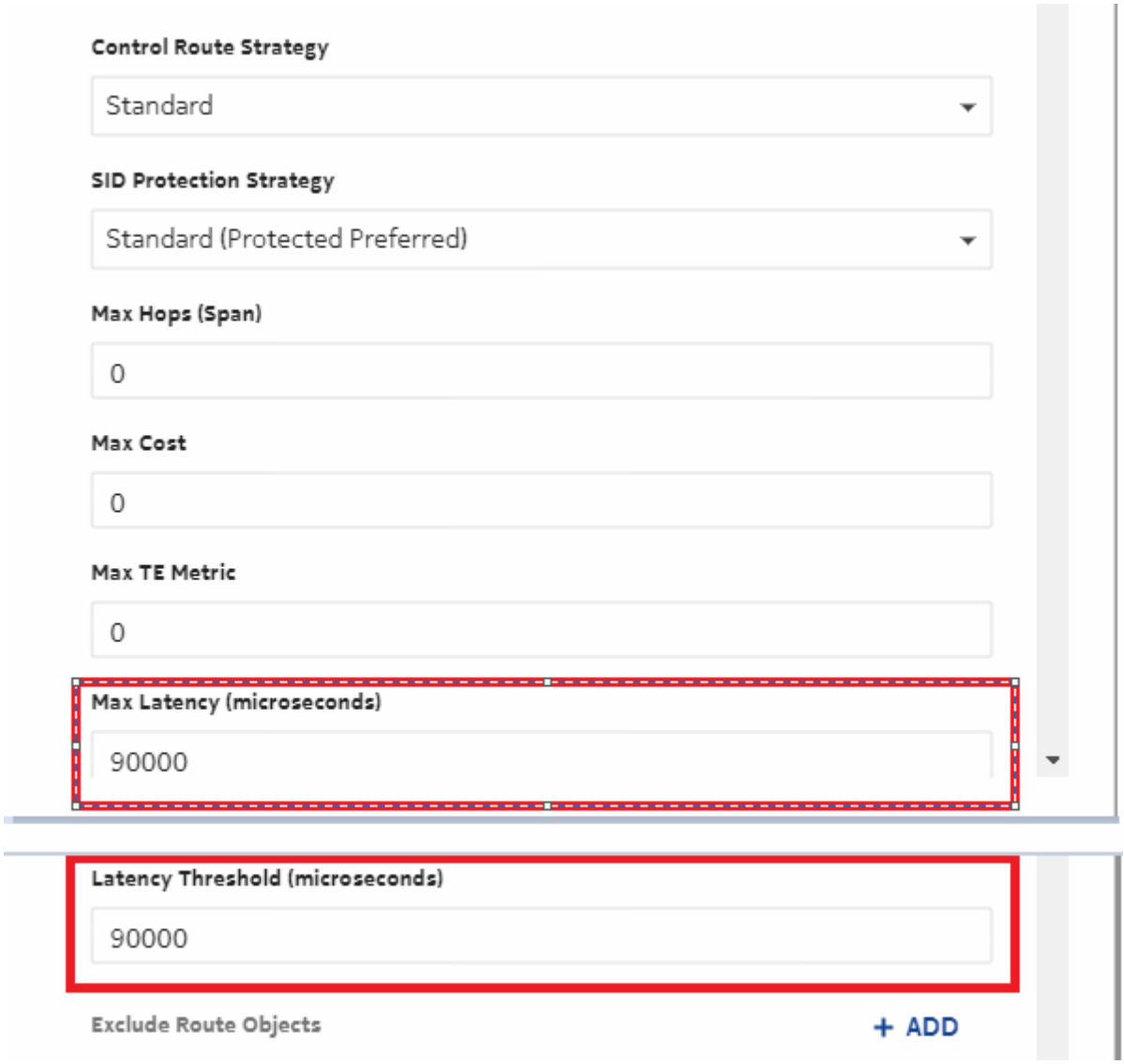
- the Profile ID parameter must match the profile ID number configured for the LSPs in Step 13 of 9.4 “Provision MPLS LSPs using Device Configuration” (p. 450).
- Optimize on (Objective) must be Latency
- Bandwidth Strategy must be Telemetry
- the Max Latency and Latency Threshold parameters must be configured.

In this example, the latency threshold value is set to 90,000 microseconds (90 milliseconds). Therefore, if a particular link latency exceeds this value (i.e. 90,000 microseconds, NSP's Path Control will attempt to re-route the LSPs which are using the link.

4

Click **CREATE**. The Path Profile policy is created.





END OF STEPS

9.13 Associate the latency-based path profile to LSPs in Device Management

9.13.1 Purpose

Use this procedure to assign the newly created latency-based path profile to the LSPs. Perform this procedure for each LSP.

To perform this procedure, the LSPs must be configured using Device Configuration; see 9.4 “Provision MPLS LSPs using Device Configuration” (p. 450).

This procedure is based on the procedure to edit a deployment in the *NSP Device Management Guide*.

For example, the reference procedure in NSP Release 24.4 is How do I edit a deployment?.

9.13.2 Steps

1

Log in to the NSP.

2

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

3

Choose an LSP deployment and click ⋮ (Table row actions), **View/Edit**.

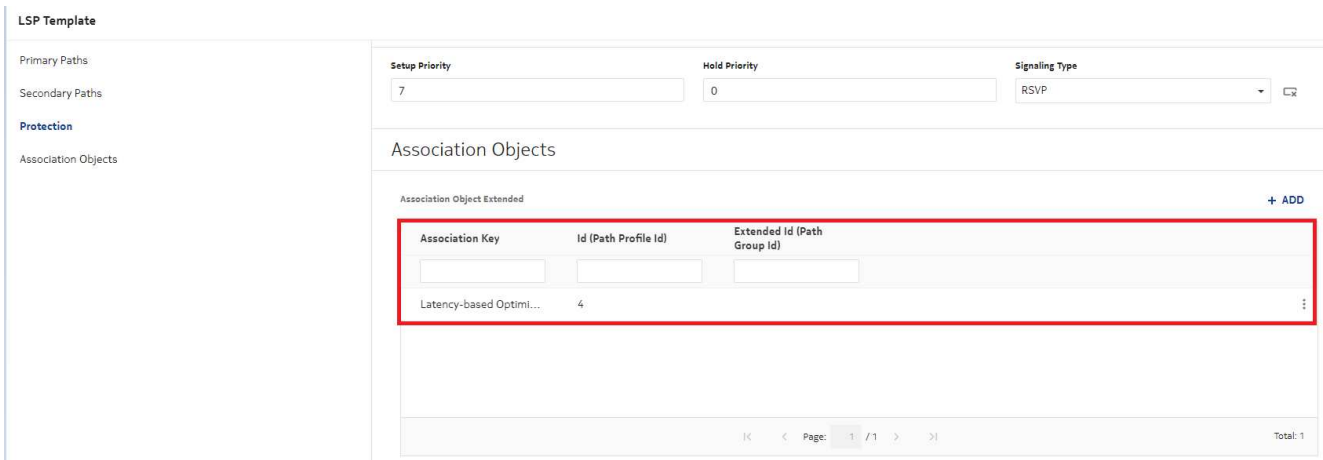
4

In the **Deploy Logical Configuration** form, click **VIEW/EDIT TEMPLATE CONFIG** to change the parameters.

5

In the Association Objects panel, click + **ADD**.

Enter an association key to describe the path profile, and the path profile ID. The path profile ID must match the ID provided in 9.12 “Create a latency-based path profile” (p. 467).



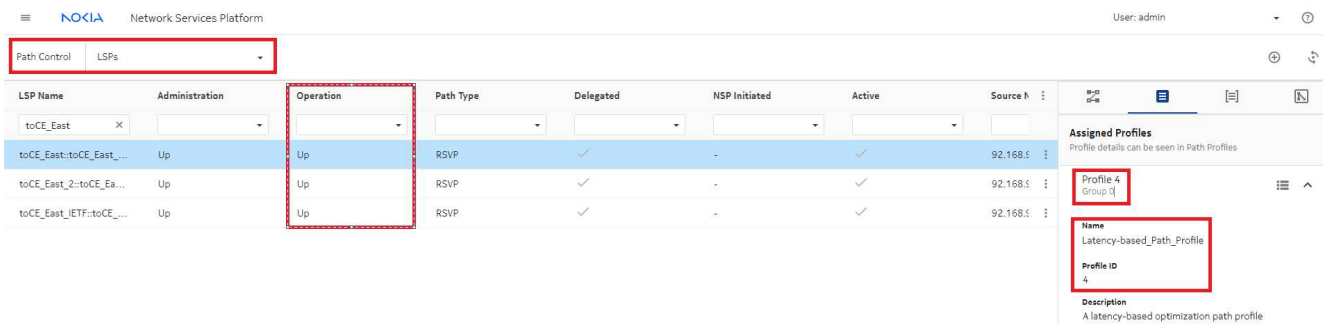
6

Click **DEPLOY**.

7

Verify that the path profile has been assigned:

1. Open the **Path Control**, **LSPs** view.
2. Select the LSP and view the Association Groups and Profiles panel.
3. Verify the profile ID.



END OF STEPS

9.14 Configure OAM configuration objects using an API

9.14.1 Purpose

Use this procedure to create configuration objects that are required prerequisites for TWAMP Light session tests. There is no UI support for this: the pre-requisites can be configured via NSP OAM configuration API calls.

See the Swagger documentation for the NSP OAM configuration API on the Nokia Developer Portal for more information.

9.14.2 Steps

1

Configure an OAM-PM bin group for each NE. Note the `bin-group-id` attribute.

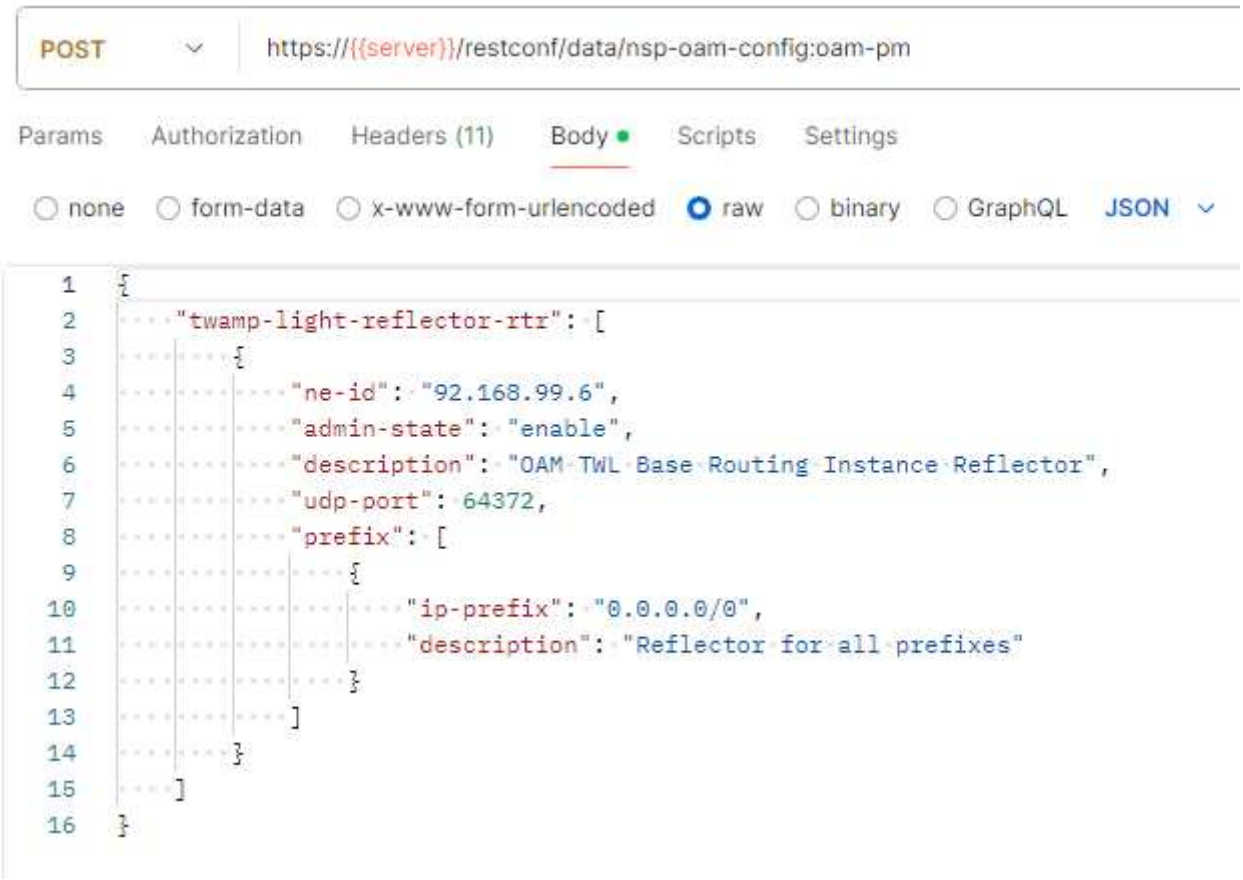
Example API call

Repeat this step for all NEs, updating the ne-id attribute.

2

Configure a TWAMP-Light reflector for each NE. Note the `udp-port` attribute.

Example API call



Repeat this step for all NEs, updating the ne-id attribute.

END OF STEPS

9.15 Create a TWAMP Light test session

9.15.1 Purpose

Use this procedure to provision TWAMP Light tests for each link in the network, where the source of the latency information is OAM.

This procedure is based on the procedure to configure an OAM test in the *NSP Data Collection and Analysis Guide*.

For example, the reference procedure in NSP Release 24.4 is How do I create an OAM test?.

9.15.2 Steps

1

Log in to the NSP.

2

Open **Data Collection and Analysis Management**, **Tests**.

3

Click **+ TEST**.

4

In the Create OAM Test form that opens, select Twamp-light in the Test type field.

Enter the link details in the entity identification parameters.

5

Choose a the Delay Streaming (proactive) test template. The test parameters are displayed.

6

Configure the required test parameters:

- The **Destination UDP port** must match the UDP port used when the TWAMP Light reflector was created in Step 2 of 9.14 “Configure OAM configuration objects using an API” (p. 472).
- The **Bin group** must match the bin group ID created in Step 1 of 9.14 “Configure OAM configuration objects using an API” (p. 472).
- The **Execute type** parameter must be Proactive.
- The **Record stats** parameter must be Delay.

Note: If the required parameters are not visible or configurable in the form on the UI, you can edit the proactive system template to customize the test creation form; see How do I edit an OAM test template?

7

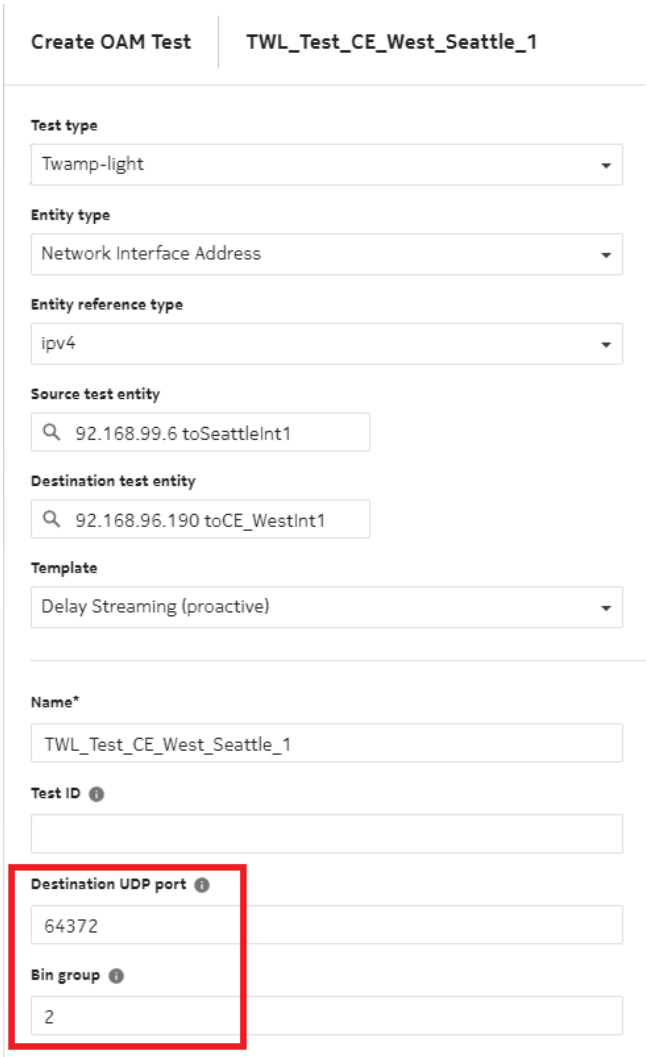
Click **CREATE**. The test appears in the list of tests.

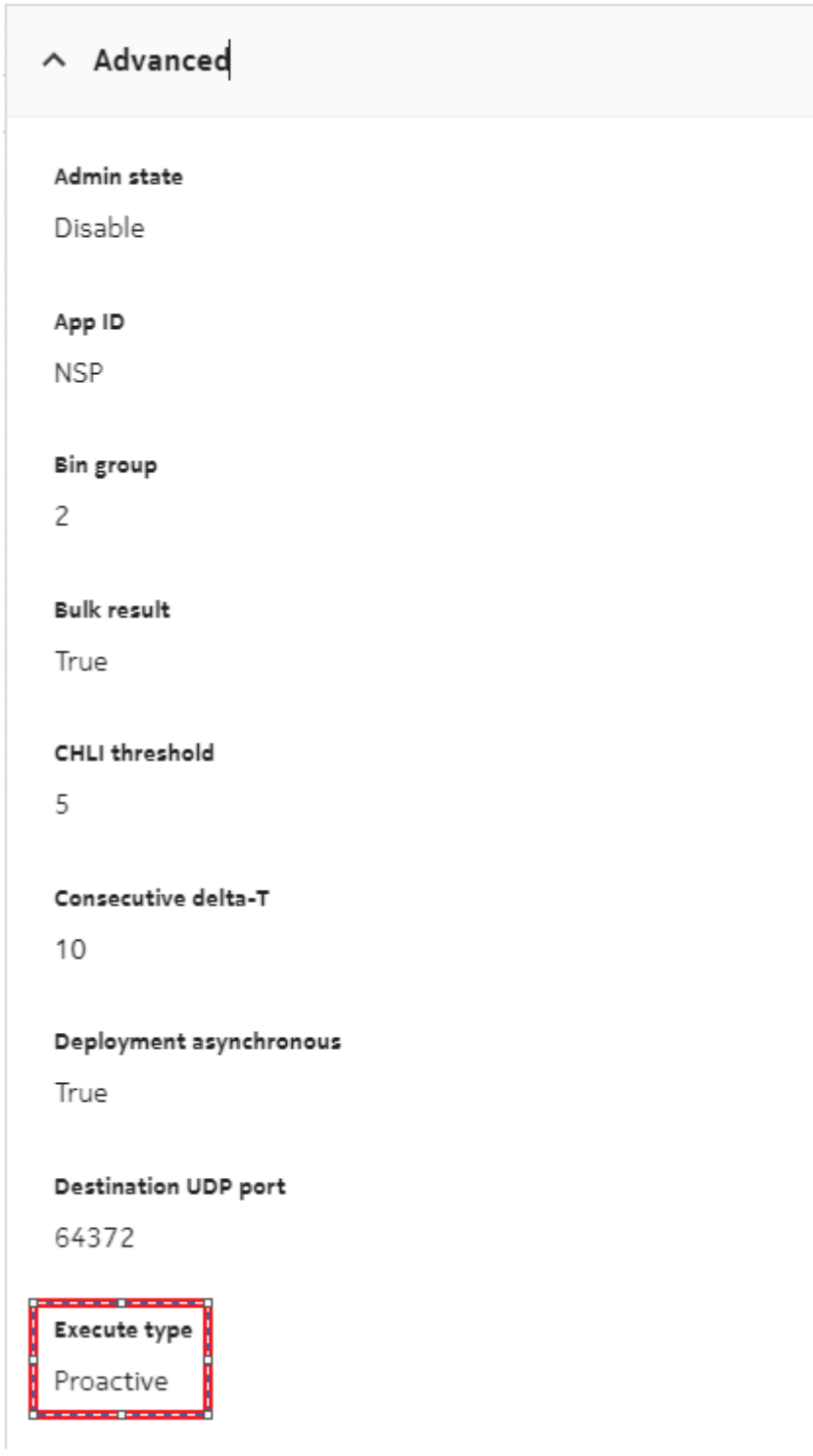
8

Repeat this procedure to create additional TWAMP Light session tests for other links in the network.

END OF STEPS

Example test configuration





FLR threshold

50

Frames per delta-T

1

Interval

1000

Measurement interval

5

Name

TWL_Test_CE_West_Seattle_1

Notify target NE

Never

Record stats

Delay

Router instance

Base

Sample window

60

Streaming template

default

9.16 Execute TWAMP Light session tests

9.16.1 Purpose

Use this procedure to execute the TWAMP Light tests created in 9.15 “Create a TWAMP Light test session ” (p. 474).

This procedure is based on the procedures to execute an OAM test and view results of an OAM test, in the *NSP Data Collection and Analysis Guide*.

For example, the reference procedures in NSP Release 24.4 are:

- How do I execute an OAM test?
- How do I view OAM test results?

Note: The execution of a test auto-generates telemetry subscriptions. Auto-generated subscriptions can be identified in the **Data Collection and Analysis Management**, **Subscriptions** view by their names. The subscription name format is `TestSuiteEx_OAM-PM-`*`test_type-statistic-type`*; for example, the subscription for Twamp-light delay streaming statistics would be named `TestSuiteEx_OAM-PM-TWAMP-streaming`.
Do not edit or delete these subscriptions.

9.16.2 Steps

1

Log in to the NSP.

2

Open **Data Collection and Analysis Management**, **Tests**.

3

In the **Filter** column at the left of the view, select Twamp-Light in the Test type field and click **RETRIEVE**. The list of TWAMP-Light tests is populated.

4

Choose a test and click ⋮ (Table row actions), **Execute**. The Execute dialogue opens.

5

Configure the required parameters and click **EXECUTE**.

- The Sync mode parameter specifies whether or not execution requests generate notifications in the UI. The **Sync-execute** option (default) provides a notification if the execution fails.
- The Result Classifier parameter specifies the name of the result classifier used to determine test success or failure. Result classifiers are configurable using a REST API.
  Check the **Perform result classification** check box to apply the classifications.
- The **Publish results** check box publishes results to Kafka.

- The **Save results to database** check box makes results available to the NSP UI. If this box is not checked, the UI does not display results of the test.

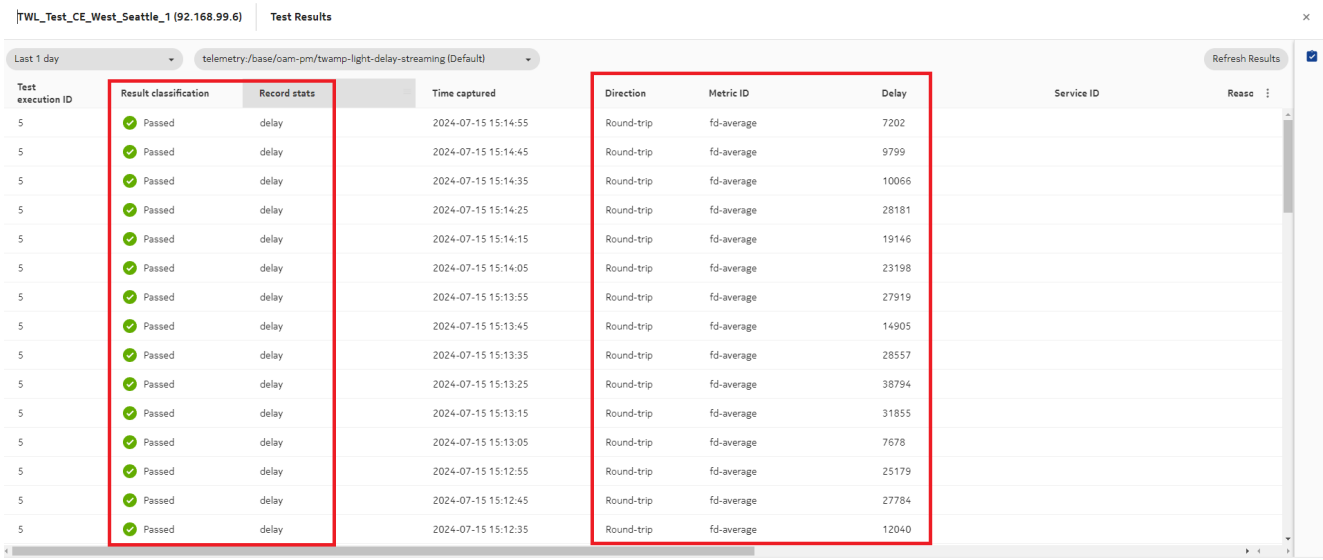
6

To view results of a test, select the test and click ⋮ (Table row actions), **View Results**.

The Test executions page opens, showing the executions and their results.

Note: After a test has executed, there is a brief processing delay before results are available. For tests that have just finished running, Nokia recommends that you wait a minimum of 5 s before viewing results.

Results example



Test execution ID	Result classification	Record stats	Time captured	Direction	Metric ID	Delay	Service ID	Reasc
5	Passed	delay	2024-07-15 15:14:55	Round-trip	fd-average	7202		
5	Passed	delay	2024-07-15 15:14:45	Round-trip	fd-average	9799		
5	Passed	delay	2024-07-15 15:14:35	Round-trip	fd-average	10066		
5	Passed	delay	2024-07-15 15:14:25	Round-trip	fd-average	28181		
5	Passed	delay	2024-07-15 15:14:15	Round-trip	fd-average	19146		
5	Passed	delay	2024-07-15 15:14:05	Round-trip	fd-average	23198		
5	Passed	delay	2024-07-15 15:13:55	Round-trip	fd-average	27919		
5	Passed	delay	2024-07-15 15:13:45	Round-trip	fd-average	14905		
5	Passed	delay	2024-07-15 15:13:35	Round-trip	fd-average	28557		
5	Passed	delay	2024-07-15 15:13:25	Round-trip	fd-average	38794		
5	Passed	delay	2024-07-15 15:13:15	Round-trip	fd-average	31855		
5	Passed	delay	2024-07-15 15:13:05	Round-trip	fd-average	7678		
5	Passed	delay	2024-07-15 15:12:55	Round-trip	fd-average	25179		
5	Passed	delay	2024-07-15 15:12:45	Round-trip	fd-average	27784		
5	Passed	delay	2024-07-15 15:12:35	Round-trip	fd-average	12040		

END OF STEPS

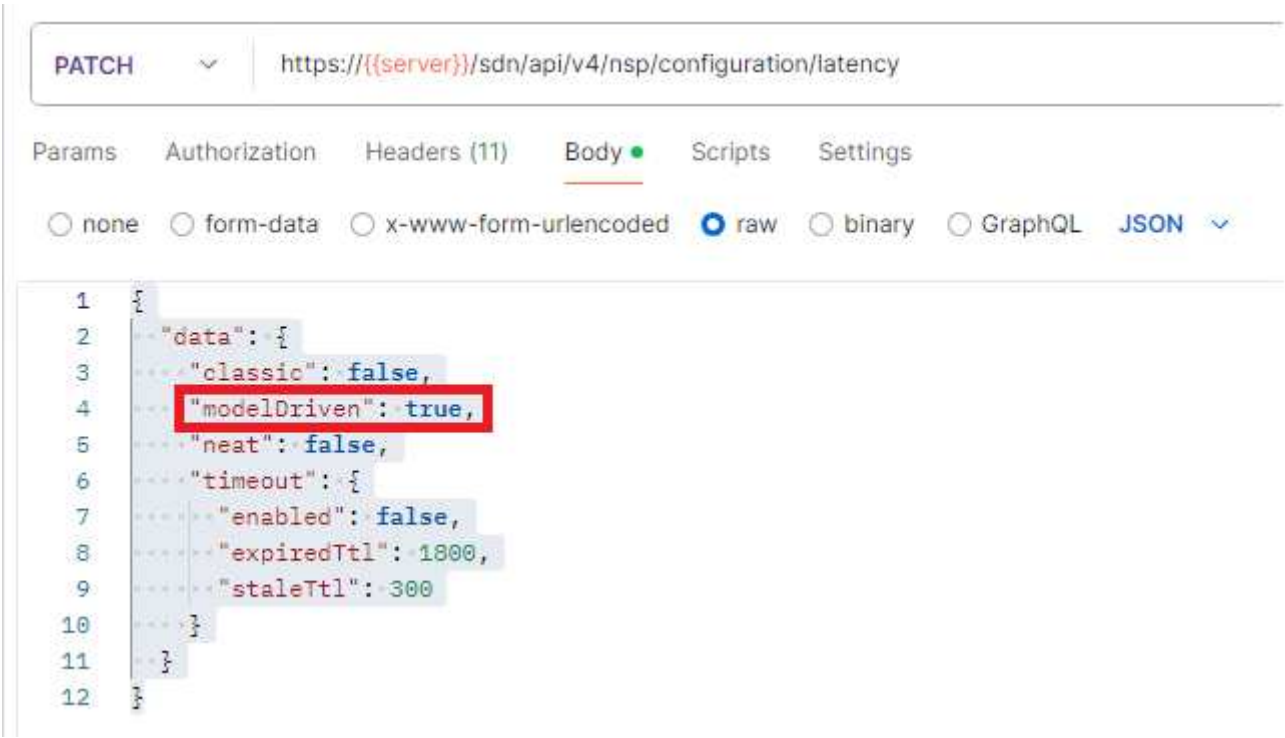
9.17 Enable latency parameters using an API

9.17.1 Allow Path Control to receive the bandwidth measurements from the network

Now that the tests are running, the next step is to allow latency collection in NSP's Path Control module. By default, Path Control's latency configuration is displayed. To enable latency collection in Path Control, a specific NSP Path Control API call is used.

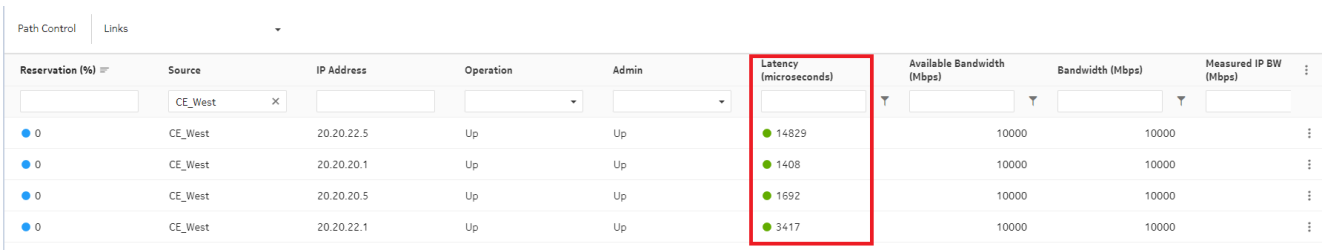
For more information about the API, see the Swagger documentation for the NSP Path Control API on the Nokia Developer Portal.

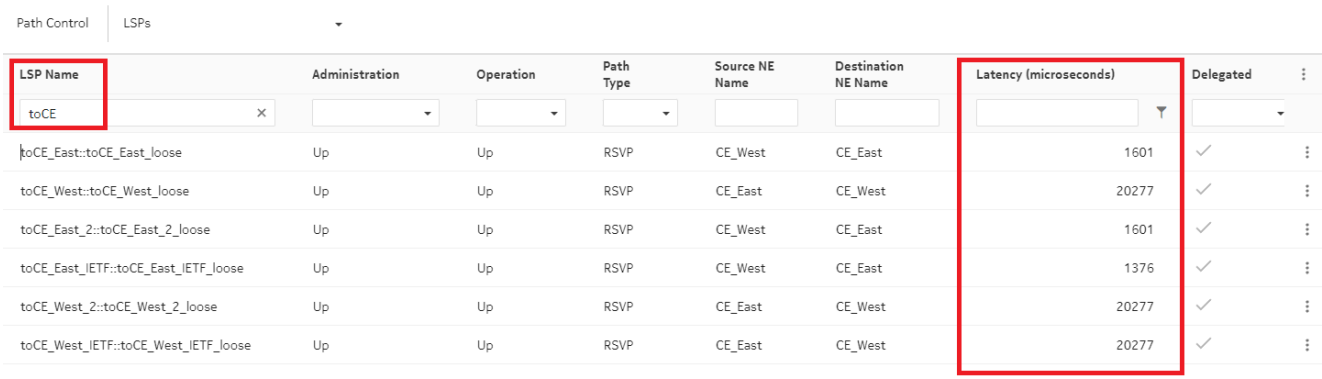
See the following example:



In this example, the "modelDriven" parameter is the parameter to be enabled. That is because we need Path Control to report link latency based on the measurements coming from Data Collection and Analysis Management.

When the call is successful, real-time latency measurements in Path Control for both LSP and link objects are displayed. The measurements are updated approximately every minute.





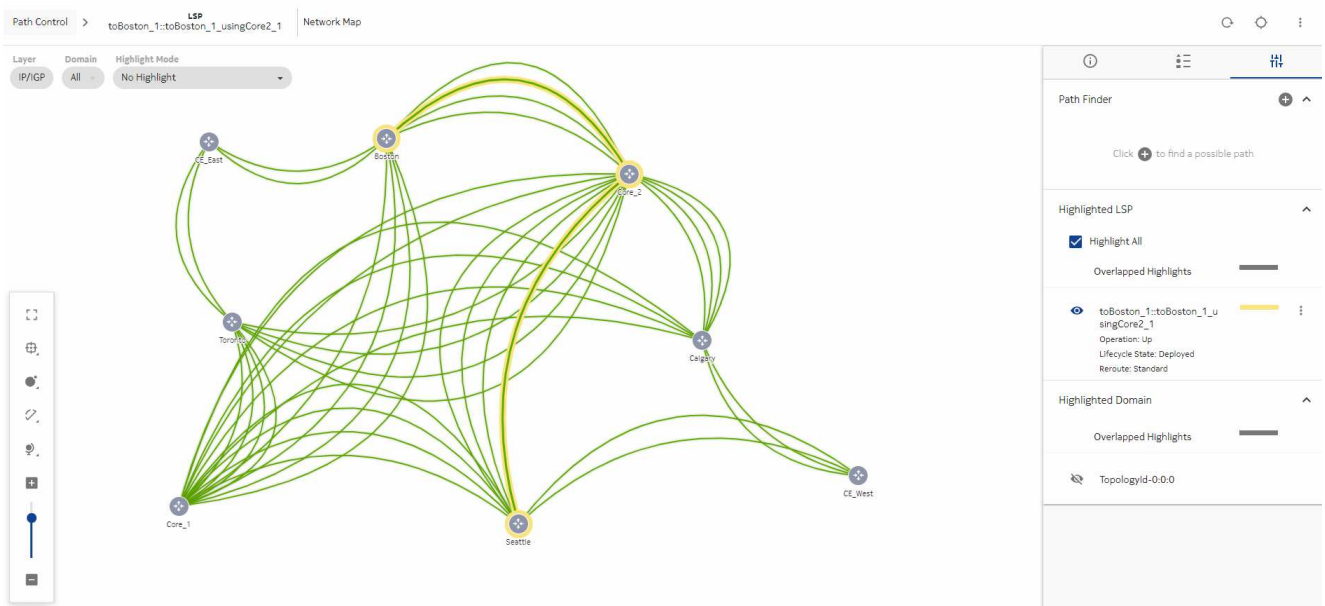
9.18 Monitor latency

9.18.1 Monitoring LSPs in Path Control

Open the **Path Control**, **LSPs** and select an LSP.

- The Hops panel in the Info panel shows the LSP paths. Pay close attention to the current path the LSPs of interest are taking to reach the destination.
- The Latency column shows the measured latency in microseconds.

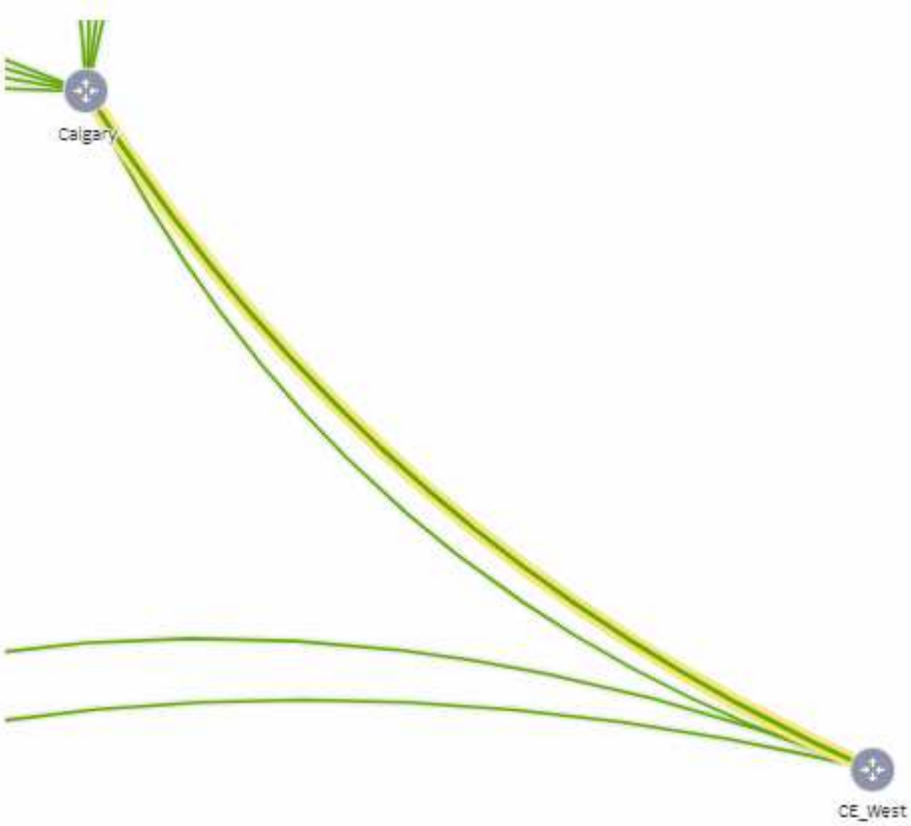
Click ⋮ (Table row actions), **Show on map** to display the LSP in a network map format.

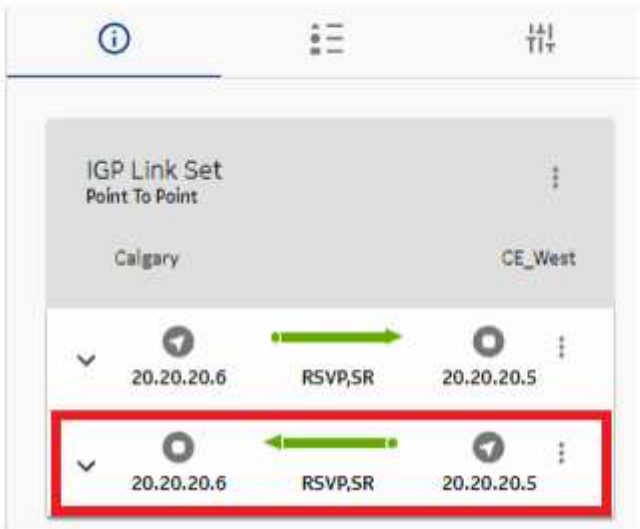


Click on a link to display link information in the Info panel.

9.18.2 Monitoring links in Path Control

From the network map view of the LSP, click on a highlighted link to display link information in the Info panel.

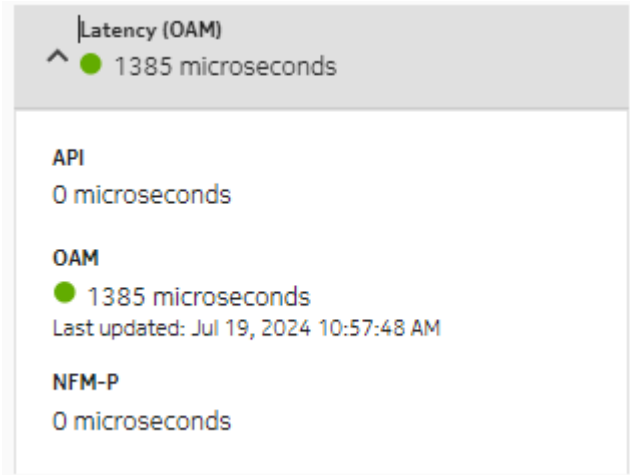




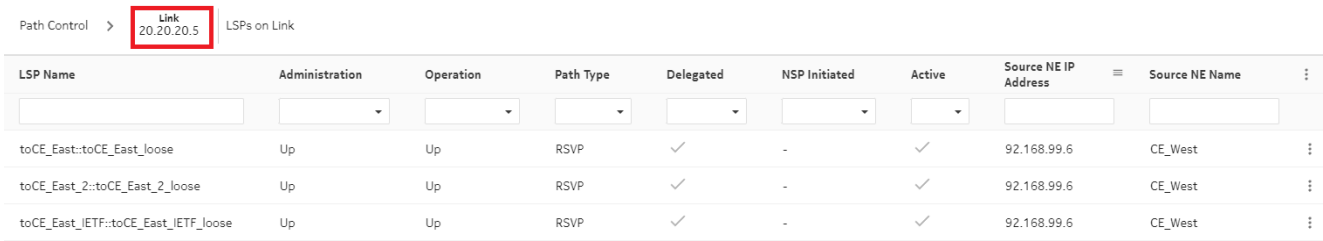
Open the **Path Control**, **Links** view and select a link.

The Latency column shows the measured latency in microseconds. The Latency information in the Info panel provides further details about recorded latency measurements. Path Control considers three possible sources (API, OAM, and NFM-P). The measurements shown in this example are coming from MD-OAM, as expected.

Furthermore, as shown here, latency values can be configured manually via APIs. If latency values are coming from both API and OAM/NFM-P sources, latency values or measurements from API calls will take precedence over OAM and NFM-P.



From the selected link, click ⋮ (Table row actions), **LSPs on Link** to see the list of LSPs on the selected link.



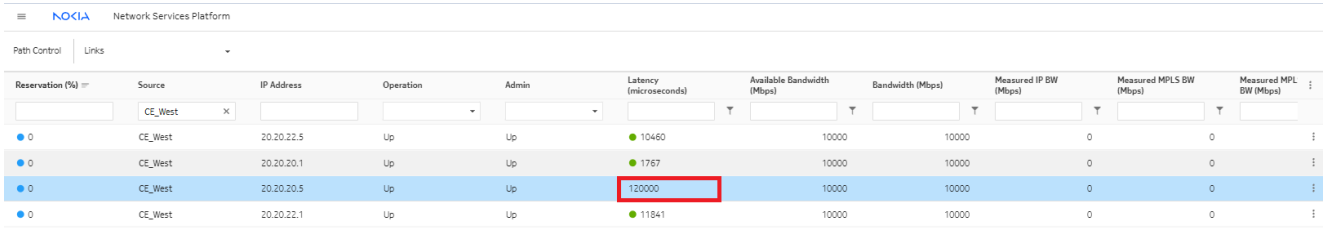
9.19 Latency-based optimization

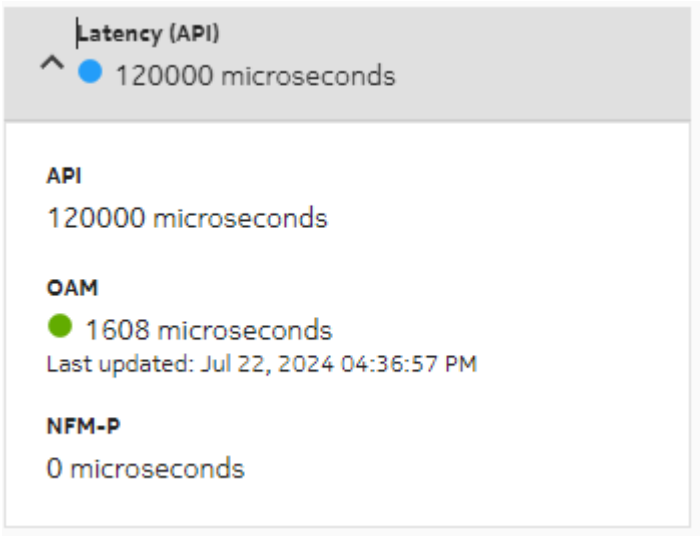
9.19.1 Link rerouting

After injecting latency on a particular link beyond the configured threshold (i.e. 90,000 microseconds in this example), we can see that the LSPs that were using the link have been re-routed, bypassing the link with the high latency value.

Note: To demonstrate this particular use case on a lab setup, the link latency was manually configured on a link via API, overriding the value obtained from the OAM tests. In a real network, if there is congestion or network-related performance problems, the latency measurements coming from the OAM source are expected to fluctuate, sometimes exceeding the configured link threshold values.

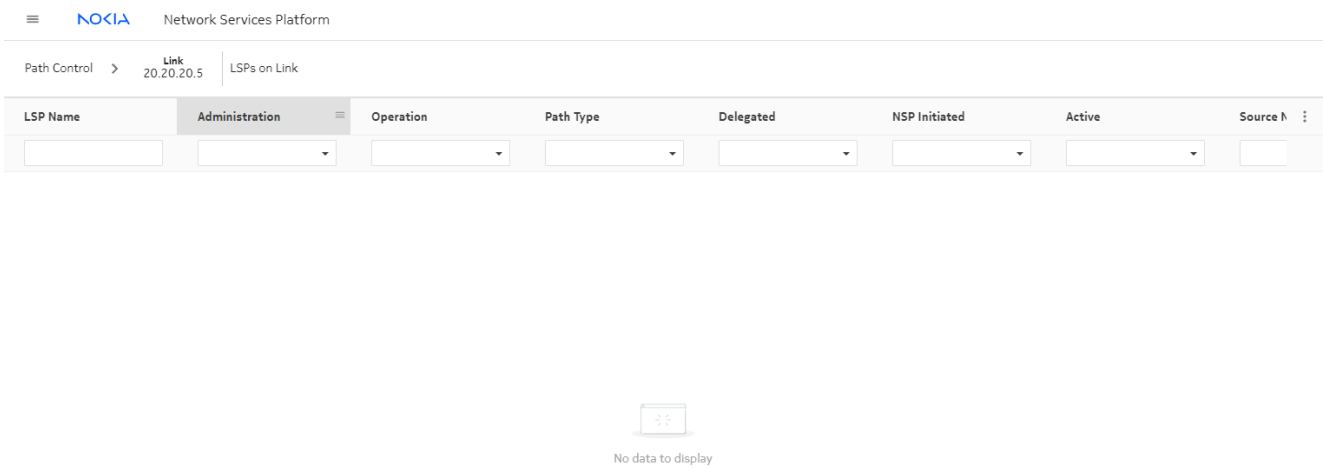
Example, before optimization:





The latency measurement from the API, 120000 microseconds, is taking precedence over the OAM measurement of 1608 microseconds.

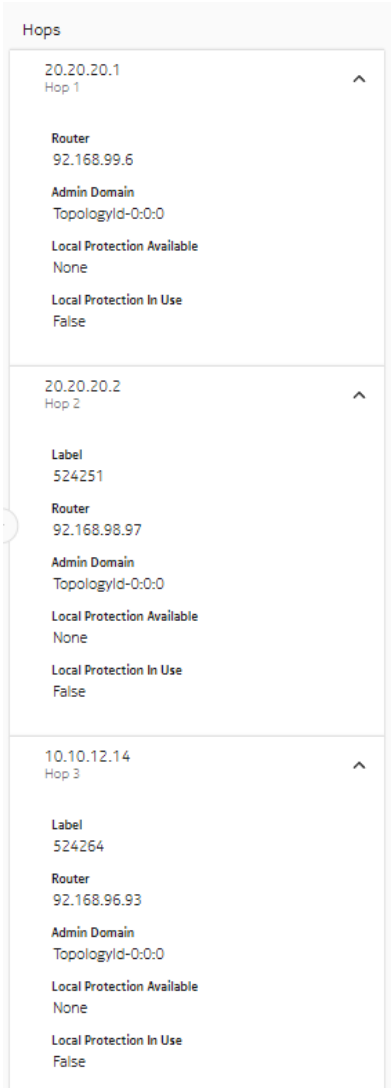
Example, after optimization:

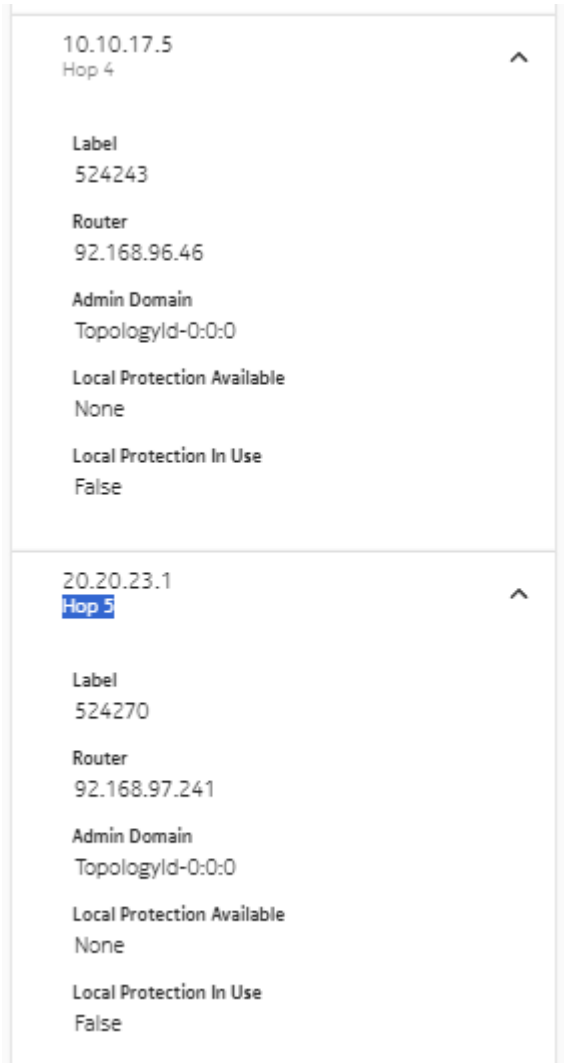


The LSPs are no longer using this link to reach the destination.

View the LSP in the **Path Control**, **LSPs** view to see the new set of hops. For reference, the previous hops were:

- Hop 1: 20.20.20.5
- Hop 2: 20.20.20.6
- Hop 3: 10.10.12.2
- Hop 4: 10.10.17.5
- Hop 5: 20.20.23.1

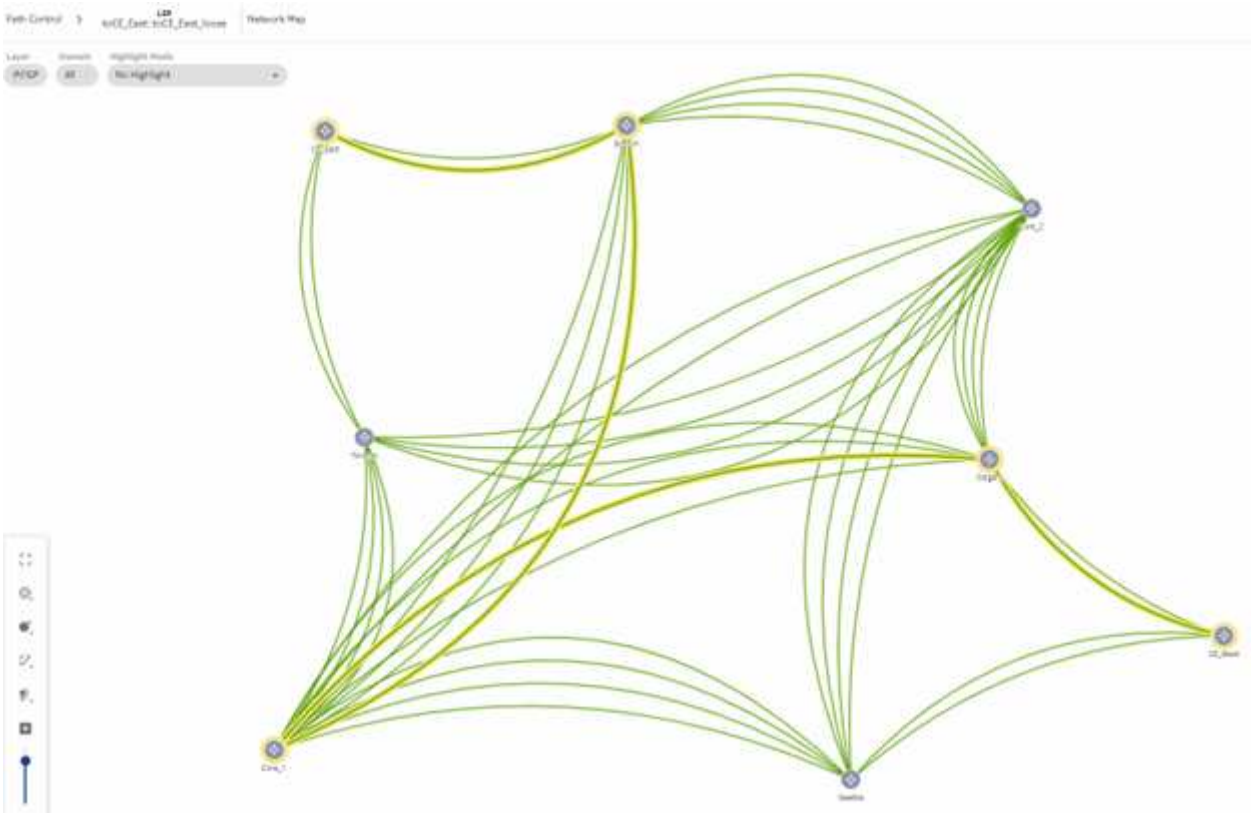




9.19.2 Network map views

The change to the path is clear in the network map.

Network map example, before optimization:



Network map example, after optimization:

9.20 System activity logging after latency optimization

9.20.1 Monitor events in real time

To view system event logs, open the **Path Control**, **System Activity Logging** view.

The logs show the latency optimization operation on the links, as seen in the following example: