



NSP

Network Services Platform

Release 23.8

Insights Administrator Application Help

3HE-18975-AAAB-TQZZA
Issue 1
August 2023

© 2023 Nokia.

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

Legal notice

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

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

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

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

No part of this document may be modified.

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

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

© 2023 Nokia.

Contents

- About this document**.....7
- 1 Insights Administrator**9
 - 1.1 What is Insights Administrator?9
 - 1.2 How do I navigate the Insights Administrator application?9
 - 1.3 How do object filters work?10
 - 1.4 Example filters.....13
- 2 Subscriptions**15
 - 2.1 What should I know about telemetry data collection?15
 - 2.2 What is a subscription?15
 - 2.3 How do subscriptions work?16
 - 2.4 How do I create a subscription?17
 - 2.5 How do I edit or delete a subscription?17
- 3 Aggregation**19
 - 3.1 What is aggregation?19
 - 3.2 How do I set the aggregation time zone?.....19
 - 3.3 How do I edit aggregation information?20
 - 3.4 What is an age-out policy?20
 - 3.5 How do I edit an age-out policy?20
- 4 OAM test templates**.....23
 - 4.1 What is an OAM test template?23
 - 4.2 How do test templates work?23
 - 4.3 What is a system template?23
 - 4.4 How do I create an OAM test template?24
 - 4.5 How do I manage OAM test templates?24
- 5 OAM tests**27
 - 5.1 What can I test in Insights Administrator?27
 - 5.2 What is CFM?27
 - 5.3 How do OAM tests work?28
 - 5.4 How do I create an OAM test?30
 - 5.5 How do I execute an OAM test?31
 - 5.6 How do I edit or delete an OAM test?32
 - 5.7 How do I view OAM test results?33

5.8	How can I troubleshoot Twamp-light test issues?	34
6	OAM test suites	37
6.1	What is an OAM test suite?.....	37
6.2	How do I create an OAM test suite?	37
6.3	How do I stop or start an OAM test suite?	38
6.4	How do I edit or delete an OAM test suite?.....	39
6.5	How do I view OAM test suite results?.....	39
7	Config objects	41
7.1	What is a config object?	41
7.2	What config objects are available in Insights Administrator?	41
7.3	How do I create a config object?.....	42
7.4	What can I do with config objects in Insights Administrator?	42
8	Baselines	43
8.1	What are baselines and anomalies?	43
8.2	How do baselines and anomalies work?.....	43
8.3	What should I know about baseline and anomaly detector creation?	47
8.4	How do I create baselines?.....	48
8.5	How do I edit a baseline?.....	49
8.6	How do I delete a baseline?	50
9	Indicators	51
9.1	What is an indicator?.....	51
9.2	How do indicators work?	51
9.3	How do formulas work?.....	54
9.4	What should I know about indicator creation and management?	55
9.5	How do I create an indicator?	56
9.6	How do I edit or delete an indicator?.....	58
10	Indicator templates	61
10.1	What is an indicator template?.....	61
10.2	How do I create an indicator template?.....	61
10.3	How do I edit or delete an indicator template?.....	62

11	Frequently asked questions	65
11.1	Insights Administrator FAQ.....	65
12	Insights Administrator use cases	67
12.1	Setting up statistics and aggregation for Port Throughput on the 7750 SR.....	67
12.2	Creating an OAM test.....	70
12.3	Setting up baselines	75
12.4	Creating a simple indicator.....	80
12.5	Creating a complex indicator using a template	86

About this document

Purpose

The *Insights Administrator Application Help* introduces the Insights Administrator application GUI to operators and administrators by describing application usage and features.

Scope

The help for Insights Administrator covers the full set of application features although some feature sets described in the help require the purchase and configuration of additional feature packages. For example, the Insights Administrator Application Help loads in the Help Center when the Insights Administrator application is deployed. The application is deployed in a containerized NSP by the Platform feature package; however, if the Network Operations Analytics feature package is also included in the deployment, the Baseline Analytics feature set is enabled within Insights Administrator. The application help covers Baseline Analytics features regardless of whether or not the Network Operations Analytics feature package has been enabled.

See the *NSP System Architecture Guide* for more information about feature packages and installation options.

NSP Insights Administrator functions are available for OSS using programmable APIs. For general information about developer support, see the API Documentation page on the [Network Developer Portal](#).

Document support

Customer documentation and product support URLs:

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

How to comment

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

1 Insights Administrator

1.1 What is Insights Administrator?

The Insights Administrator application is used to manage YANG-based telemetry.

Statistics definition and mapping files are included with installation of the NFM-P or, if MDM is in use, with the NE adaptor suite.

1.1.1 Insights Administrator Application help scope

The application help covers managing subscriptions and working with existing aggregation rules in the Insights Administrator application.


For detailed information about the following topics, see the Network and Service Assurance and Network Operations Analytics tutorials on the [Network Developer Portal](#):

- configuring YANG definition files
- configuring device mapping files
- configuring aggregation
- using RESTCONF APIs
- managing notifications in Kafka

1.2 How do I navigate the Insights Administrator application?


The Insights Administrator application consists of the following pages, depending on the feature packages installed. You can navigate from one page to another by choosing from the page selector drop-down list at the top left of the page.

The pages display information in columns. Drag a column header to reorder the columns, drag a column header separator to resize columns, or click on a column header to sort the data in the column. An icon appears when the column is sorted.

Filter the list using the column header filters. To remove a filter, delete information from the filter field or choose **Clear filters** from the  (Table settings & actions) menu in the column header.

You can use wildcards in the filter fields: an underscore character works as a single-character wildcard and a percent character works as a multi-character wildcard. For example:

- 1/_/1 matches “1/1/1” or “1/2/1”. There must be a character: “1//1” will not match.
- 1%/1 matches “1/1/1”, “1/22/1”, “1/abcdefg/1”. Characters are not required: “1//1” will match.

You can click  (Table settings & actions) in the column header on any page to manage the display or export data.

Telemetry

- Subscriptions

The Subscriptions page shows the lists of Telemetry, Baseline, and Indicator subscriptions.

- **Aggregation**
The Aggregation page shows the list of aggregation rules for model-driven telemetry. Aggregation rules are configured on the NSP server.
- **Age-Out Policy**
The Age-Out Policy page displays the retention policies configured for each aggregation rule.

Baseline Analytics

Baseline Analytics is enabled when the Network Operations Analytics feature package is included in the deployment.

- **Baselines**
The Baselines page shows the list of baselines.


NSP Indicators

NSP Indicators is enabled when the Network Infrastructure Management feature package is included in the deployment.

- **Indicator Templates**
The Indicator Templates page shows the list of configured indicator templates.
- **Indicators**
The Indicators page shows the list of configured indicators.

OAM Test

- **Test Templates**
The Test Templates page shows the list of configured OAM test templates. You can filter the list to show proactive or on-demand test templates using the drop-down list at the top of the left column.
- **Tests**
The Tests page shows the list of configured OAM tests.
- **Test Suites**
Insights Administrator provides a read-only list of OAM test suites created in the MD-OAM RESTCONF API.

You can click  (More) at the top right of any page above the column headers to open the corresponding page in the Insights Viewer utility. For example, if you open Insights Viewer from the Baselines page, it opens to the Baselines page in Insights Viewer.

1.3 How do object filters work?

Object filters use XML Path (XPath) expressions against the NSP object YANG model to determine which objects a subscription applies to. The object filter is combined with the telemetry type to create the list of relevant statistics data.

An XPath is composed of a series of XPath elements. Each element represents a step on the YANG model tree from left (root) to right (leaf or container). An element contains a name and a series of optional predicates.

Example: `network-element[ne-id='10.1.0.0']`

1.3.1 Predicates

A predicate is an expression within square brackets that identifies the instance of each XPath element. Keys and attributes of the object (as defined in the NSP model YANG) may be included.

Predicates can contain the following operators:

- =
- >
- <
- >=
- <=
- !=
- and
- or

Subexpressions can be enclosed in parentheses to enforce order of operations.

i **Note:** Comparison operators use string comparators, so “value2” is greater than “value1”.

Examples:

```
[ne-id='10.1.0.0' or ne-id='10.1.1.1']
```

```
[(type='7750 SR-12' and product='7750 SR') and (version='TiMOS-B 19.0.R1'  
or contains('version','15.0'))]
```

1.3.2 Predicate functions

The following functions are supported within a predicate:

- contains('attribute', 'search-text')
searches for all objects where the named attribute contains the search text
- containsIgnoreCase('attribute-name', 'search-text')
same as contains() but conducts a case-insensitive search
- not(<binary-expression>|<function-expression>)
negates the result of the argument expression

Examples:

```
[contains('component-id', 'port=1')]
```

```
[not(contains('component-id', 'port=1'))]
```

```
[contains('component-id', 'port=1') and not(contains('component-id',  
'breakout'))]
```

1.3.3 XPath expressions

An XPath expression is an XPath that can be evaluated to produce a list of XPath identifiers. For the purpose of an object filter, the XPath expression must resolve to a NodeSet of NSP model identifiers.

XPath expressions can be chained together using a union “[|]” operator, which evaluates each subexpression independently into NodeSets and performs a set union operation to combine the NodeSets into a single NodeSet result.

Expressions can be static expressions, which resolve to the same result every time, or wildcard expressions, which can produce different results. The dynamic effect is created by using syntax that does not specifically identify a set of NSP model objects: there is no wildcard character.

Examples:

MDM equipment: `component-id='shelf=1/cardSlot=1/card=1/mdaSlot=1/mda=1/port=1/1/1'`

Classic equipment: `component-id='shelf=1/slot=1/card=1/slot=1/card=1/port=1'`

Example of a static expression:

```
/nsp-equipment:network/network-element[ne-id='10.1.0.0']  
/hardware-component/port[component-id='shelf=1/cardSlot=1/card=1/mdaSlot=1/mda=1/port=1/1/1' or component-id='shelf=1/cardSlot=1/card=1/mdaSlot=1/mda=1/port=1/1/2'] | /nsp-equipment:network/network-element[ne-id='10.1.0.1']/hardware-component/port[component-id='shelf=1/cardSlot=1/card=1/mdaSlot=1/mda=1/port=1/1/3' or component-id='shelf=1/cardSlot=1/card=1/mdaSlot=1/mda=1/port=1/1/4']
```

Examples of wildcard expressions:

Create a wildcard expression by not including all keys in the predicates.

- The following expression chooses all objects of type `port` on NE 1.1.1.1.

```
/nsp-equipment:network/network-element[ne-id='1.1.1.1']  
/hardware-component/port
```

- The following expression chooses all objects of type `port` for all NEs.

```
/nsp-equipment:network/network-element/hardware-component/port
```

- The following expression returns all child objects that can respond to the selected telemetry type and counters.

```
/nsp-equipment:network/network-element[ne-id='10.1.0.0']
```

1.3.4 Filtering models

Paths for MDM-managed NEs are based on the NE YANG models. .

Device model

The NE YANG model used by Modeled Device Configurator is **network-device-mgr**.

- This model uses device model xpath notation—this means that the filter can support all the paths

as implemented by the node. Creating a path using the device model is useful when the object is not supported by, or not defined in, the NSP model.

- The device model provides a view of the device-specific paths. For example, an SR OS NE defines an LSP object using a path similar to `/network-device-mgr:network-devices/network-device[name='10.1.0.0']/root/nokia-state:state/router[router-name='Base']/mpls/statistics/lsp-egress[lsp-name='LSP1']`.

The telemetry mapping file must contain a definition for the device path for telemetry to be collected.

The following is an example of a **network-device-mgr** model filter type for an NFM-P managed device. This filter targets a specific object instance by its FDN:

```
/network-device-mgr:network-devices/network-device[name='10.1.0.0']
/root/nokia-nsp-source:fdn[id='fdn:realm:sam:lsp:from-11.50.150.30-id-2']
```

Equipment model

The **nsp-equipment:network** model is a normalized NSP YANG model that provides a view of the equipment for all network elements, abstracting the device specifics. Using NSP equipment model identifiers is recommended because the models are supported by NSP applications. In addition, filters based on the NSP equipment model can use operators such as AND or CONTAINS.

For example, the following path represents an individual port.`/nsp-equipment:network/network-element[ne-id='10.1.0.0']/hardware-component/port[name='1/1/1']`

Equipment model information can be found using the Network Inventory API; see the Postman collection on the on the [API Documentation page](#).

To assemble a filter, find the relevant model details and add predicates and predicate functions as needed. For example, a `get port` operation provides the path to the port.

See the Network Infrastructure Management tutorial on the [Network Developer Portal](#) for information about using APIs.

1.4 Example filters

You can adapt the following examples to your requirements:

1.4.1 Specific NE

```
/nsp-equipment:network/network-element[ne-id='1.10.1.1'or ne-id='1.10.1.2']
```

i **Note:** Some attributes may have different values for MDM-managed NEs and classically managed NEs. Verify that your filter uses the correct values for the data you need.

1.4.2 Specific card and slot

IOM card equipment

- Classic example

```
IOM slot: /nsp-equipment:network/network-element[ne-id='1.1.1.1']  
/hardware-component/container[component-id='shelf=1/slot=1']  
IOM slot/IOM card:/nsp-equipment:network/network-element[ne-id='1.1.1.1']  
/hardware-component/card[component-id='shelf=1/slot=1/card=1']
```

- **MDM example**

```
IOM card: /nsp-equipment:network/network-element[ne-id='4.4.4.4']  
/hardware-component/  
card[component-id='shelf=1/cardSlot=1/card=1']
```

MDA card equipment

- - **Classic example**
IOM slot/ IOM card/ MDA slot: /nsp-equipment:network/network-element[ne-id='1.1.1.1']/hardware-component/container[component-id='shelf=1/slot=1/card=1/slot=1']
IOM slot/ IOM card/ MDA slot/ MDA card: /nsp-equipment:network/network-element[ne-id='1.1.1.1']/hardware-component/card[component-id='shelf=1/slot=1/card=1/slot=1/card=1']
 - **MDM example**
IOM card/MDA card: /nsp-equipment:network/network-element[ne-id='4.4.4.4']/hardware-component/card[component-id='shelf=1/cardSlot=1/card=1/mdaSlot=1/mda=1']

1.4.3 Specific port

- **Classic example:**
IOM slot/ IOM card/ MDA slot/ MDA card/ port:/nsp-equipment:network/network-element[ne-id='1.1.1.1']/hardware-component/port[component-id='shelf=1/slot=1/card=1/slot=1/card=1/port=1']
- **MDM example:**
IOM card/ MDA card/ port: /nsp-equipment:network/network-element[ne-id='4.4.4.4']/hardware-component/port[component-id='shelf=1/cardSlot=1/card=1/mdaSlot=1/mda=1/port=1/1/1']

1.4.4 Port mode

The following example filters all network mode ports on an NE (NE ID is 2.2.2.2) that are administratively and operationally up:

```
/nsp-equipment:network/network-element[ne-id='2.2.2.2']  
/hardware-component/port[admin-state='unlocked' and  
oper-state='enabled'] [boolean(port-details[port-mode='trunk'])]
```

2 Subscriptions

2.1 What should I know about telemetry data collection?

Insights Administrator has the following prerequisites for telemetry data collection.

- The NEs from which you want to collect data must be discovered, managed, and reachable by the NSP.
- If you want to use a telemetry subscription to manage data from NEs managed by NFM-P, statistics collection must be configured in the NFM-P.
- Mapping and definition files must be installed on the NSP server; see the Telemetry Collection tutorial on the [Network Developer Portal](#).
- If you want to use statistics for Analytics reports with granularity other than raw data, you need aggregation rules for the telemetry types you want to collect; see the Aggregation tutorial on the [Network Developer Portal](#)
- You need to [configure the aggregation time zone](#).
- To collect accounting statistics, an FTP mediation policy must be assigned to the NE. FTP mediation policies are created and assigned using a REST API; see the LSOM Framework and APIs tutorial on the [Network Developer Portal](#).

Subscriptions are automatically created for Baseline Analytics, Indicator Analytics, and OAM testing. To collect statistics for another purpose, [create a subscription](#) and set its state to enabled.

RESTCONF APIs are available for telemetry collection and aggregation; see the Network Assurance API documentation on the [Network Developer Portal](#).

2.1.1 Data storage

You can enable database storage for MDM managed NEs as part of subscription creation. By default, the data collected is stored in Postgres unless there is an auxiliary database enabled, in which case all collected data is stored in the auxiliary database. For NFM-P collected SNMP or accounting statistics, the database parameter in the subscription is ignored.

If gRPC telemetry is enabled on a classic device, known as dual management, the gRPC statistics are stored in the database.

Historical data, that is, data that is stored in a database, is retained according to the age-out policy; see [3.5 “How do I edit an age-out policy?” \(p. 20\)](#).

i **Note:** For statistics to be available to the Analytics application for aggregated reports, they must be stored in the auxiliary database.

The Telemetry data API also provides the functionality to subscribe, stream, and plot historical and real-time data; see Use Case 5 in the Telemetry Collection tutorial on the [Network Developer Portal](#).

2.2 What is a subscription?

A subscription represents a request for statistics information management.

You can configure telemetry subscriptions. Baseline and indicator subscriptions are managed by Baseline Analytics and NSP Indicators respectively, and are read-only in the Subscriptions tab.

Baseline Analytics is available with the Network Operation Analytics feature package, and NSP Indicators is available with the Performance Indicators and Alerts installation option.

NSP generates predefined OAM-related telemetry subscriptions in systems where MD-OAM is deployed. OAM subscriptions appear in the Telemetry subscriptions list in Insights Administrator and are prefixed with **TestSuiteEx_OAM**. Do not edit predefined OAM subscriptions.

2.3 How do subscriptions work?

When you configure a telemetry subscription, you specify a set of statistics data and notification and storage options for the data. To configure the data set, you select the type of statistics you are interested in, the frequency of collection, and configure filtering by NE and counters as needed.


Statistics collection requirements and behavior depend on the NE management type, as described in the following table.

Management type	Management type definition	Statistics configuration
Classic	Device is discovered and managed exclusively by NFM-P	Statistics collection and database storage must be previously configured in NFM-P before creating a subscription in Insights Administrator. The subscription tells NFM-P to publish any statistics that match subscription requirements to Kafka as they are collected. The interval specified in the subscription request is ignored.
MDM	Device is discovered and managed exclusively by Device Administrator	When the subscription is created, the MDM initiates collection of the Telemetry data from the NE at the specified interval.
Dual managed	Device is discovered and managed in both NFM-P and Device Administrator, that is, both classic and MDM management Dual management enables gRPC telemetry on classic devices. All other management is through NFM-P.	Insights Administrator uses MDM for dual managed NEs. When the subscription is created, the MDM initiates collection of the Telemetry data from the NE at the specified interval. ¹

Notes:

1. If statistics collection is set up in both NFM-P and Insights Administrator, the telemetry framework may receive the same information twice. The duplication could result in incorrect reports or duplicated indicator TCAs. For dual managed NEs, verify that data being used for telemetry, baseline, or indicator subscriptions is only collected once. Disable equivalent MIB based statistics in NFM-P if gRPC telemetry is used.

2.4 How do I create a subscription?

- 1 _____
On the **Subscriptions** page, click **+ SUBSCRIPTION** .
- 2 _____
In the Create Subscription form that opens, configure the General parameters as needed.
Enable database subscriptions as needed to save subscription information to the auxiliary database. For subscription data to be available to Analytics, it must be in the auxiliary database.
- 3 _____
Choose **Enabled** in the **State** field if you want your subscription to start running right away.
- 4 _____
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.
- 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 you need from the list of matches.
- 6 _____
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.
- 7 _____
Click **CREATE**.
The subscription begins collection when it is enabled.


END OF STEPS _____

2.5 How do I edit or delete a subscription?

2.5.1 To edit a subscription

- 1 _____
On the **Subscriptions** page, choose a subscription.

2

Click  (Table row actions), **Edit**.

3

In the form that opens, update the parameters as needed and click **UPDATE**.

END OF STEPS

2.5.2 To delete a subscription

1

On the **Subscriptions** page, choose a subscription.

2

Click  (Table row actions), **Delete**. The subscription is removed immediately.

END OF STEPS

3 Aggregation

3.1 What is aggregation?

Aggregation is the practice of combining measurements for analysis. In the NSP, telemetry data is aggregated based on time period of collection: hourly, daily, weekly, or monthly. When a report is run in Analytics, the granularity parameter in the report determines which aggregated data set is analyzed. For example, if you select hourly granularity, the report shows the hourly aggregated data. Some reports can use raw data, that is, data that is not aggregated, but this is not available for all reports.

3.1.1 What is an aggregation rule?

An aggregation rule defines how the data for a specified telemetry type is aggregated and how long each aggregated data set is retained.

Aggregation rules for model-driven telemetry are configured on the NSP server. They can be [viewed and edited](#) in Insights Administrator.

For aggregation information to be available in Insights Administrator, the auxiliary database must be configured and running.

Use the NFM-P to configure aggregation rules for data collected by the NFM-P; see the *NSP Analytics Report Catalog*.

3.1.2 What is the aggregation time zone?

The aggregation time zone is the time zone that is used to determine the start and end time of data to be aggregated:

- hourly aggregation: from xx:00 to xy:00
- daily aggregation: from midnight to midnight
- weekly aggregation: from midnight Monday to midnight Monday
- monthly: from midnight on the 1st of the month until midnight on the first of the following month

3.2 How do I set the aggregation time zone?

i **Important!** Changing the aggregation time zone changes the start and end times of all future aggregations. The first aggregation following the change may miss data or count data twice due to the difference in time zones.

1

On the **Aggregation** page, click **⋮** (More), **Time zone Setting**.

2

In the form that opens, enter a time zone in the **Aggregation Time Zone** field. You can enter the name of the time zone or the GMT offset, for example, GMT-5:00.

As you type, the list of available time zones is refined to match your input.

3

Choose the time zone from the list.

4

Click **OK** in the confirmation dialog.

5

Click **SAVE**.

END OF STEPS

3.3 How do I edit aggregation information?



Note: For the Aggregation page to be available, the auxiliary database must be configured and running.

1

On the **Aggregation** page, choose an aggregation rule and click (Edit).

2

In the form that opens, edit the parameters as needed and click **UPDATE**.

END OF STEPS

3.4 What is an age-out policy?

An age-out policy is a retention policy for stored data. Data older than the retention period is purged from the database.

Insights Administrator creates a policy for each telemetry type, a policy for baselines, and a policy for indicators.

3.5 How do I edit an age-out policy?

1

On the **Age-Out Policy** page, open the Edit form:

- a. To edit a telemetry policy, choose Telemetry from the drop-down list, choose a policy and click (Edit).
- b. To edit the baseline or indicator policy, choose the policy type from the drop-down list.

2

Edit the retention period and click **UPDATE**.

END OF STEPS

4 OAM test templates

4.1 What is an OAM test template?

An OAM test template is a set of parameters that a user can employ to create or customize a test for a particular use case. You can create a template for each test type, or create separate templates for different use cases. The test template becomes the form used to create and run the test in the future.

On-demand templates are for tests that run a single execution; proactive templates are for tests that execute repeatedly.

4.2 How do test templates work?

A test template includes all the parameters for a test. The template creator can set the parameters or leave them blank and can choose whether the parameter is visible or editable when the template is used.

When a test is created from the template, the parameters are applied as follows.

- If the template creator sets the parameter value in the template and does not set the parameter instance as editable, the test runs with the value set in the template.
- If the template creator sets the parameter instance as editable, the test runs with the value set by the user who creates the test. The template creator can also set the parameter value, creating a template default.
- If the template creator does not set the parameter value and does not set the parameter instance as editable, the test runs with the default value in the YANG model, if applicable.

Test templates can use variable substitution to autopopulate some values, based on entity mapping in the YANG model. The definition of a variable has the following syntax:

```
#{variable-name}
```

For example, "`service:#{service-name}`" is resolved from the current test object after any source/destination entities are resolved.

For more information about variable substitution, see the MD-OAM App tutorial on the [Network Developer Portal](#).

4.3 What is a system template?

System templates are available to NSP applications for test creation.

An operator can create tests in Insights Administrator using any template. However, when an application creates a test, it must use a system template. This requirement includes test suites created using Insights Administrator.

Default system templates are provided with installation of the NSP. You can modify these templates and add additional ones.

4.4 How do I create an OAM test template?

- 1 _____
On the **Test Templates** page, click **+ TEMPLATE**.
- 2 _____
In the Create Test Template form that opens, configure the template settings in the panel on the left.
By default, the settings are not visible or editable at test creation. Enable visibility or editing for each setting as needed. When you enable editing, visibility is automatically enabled.
 - Configure the **Execute type** parameter to configure the template as On-demand or Proactive.
 - Select **System Template** to configure the template as a system template.
- 3 _____
View the test creation form layout in the panel on the right side of the page. Drag the fields to change the order if needed.
- 4 _____
Click **CREATE**.

END OF STEPS _____

4.5 How do I manage OAM test templates?

4.5.1 To edit a template

- 1 _____
On the **Test Templates** page, choose a template and click **⋮** (Table row actions), **Edit**.
Use the **All Templates** drop-down list if required to filter the list to show only on-demand or proactive templates.
- 2 _____
In the form that opens, update the parameters as needed and click **UPDATE**.

END OF STEPS _____

4.5.2 To delete a template

- 1 _____
On the **Test Templates** page, choose a template and click **⋮** (Table row actions), **Delete**.

2

Click **DELETE** to confirm the deletion.

END OF STEPS

5 OAM tests

5.1 What can I test in Insights Administrator?

In Insights Administrator, you can create the following OAM tests:

- CFM DMM
- CFM Linktrace
- CFM LMM
- CFM Loopback
- CFM SLM
- Twamp-light

Tests are created using test templates. Before a test can be created, at least one test template must exist for the test type.

Tests can be created at any time. No additional configuration is required on the tested objects for testing to be performed.

RESTCONF APIs are available for MD-OAM configuration and testing; see the Network and Service Assurance API documentation on the [Network Developer Portal](#).

5.1.1 Data storage for OAM results

By default, OAM test data is stored in Postgres unless there is an auxiliary database enabled, in which case result data is stored in the auxiliary database.

NFM-P SNMP test results are collected from Kafka. Kafka must be enabled in the NFM-P for the NSP to receive the results. Kafka is enabled by default for most test types except NFM-P resynched tests. You must enable Kafka in the NFM-P for NSP to receive the results of these tests.

5.2 What is CFM?

Ethernet Connectivity Fault Management in NSP is implemented based on the IEEE Y.1731 and 802.1ag OAM standards. The standards describe protocols for detecting, isolating, and reporting connectivity faults in an Ethernet network. CFM is a Layer 2 OAM object infrastructure.

You can use Ethernet CFM for the following:

- path discovery
- fault detection
- fault isolation
- fault notification

The following table describes terms relevant to CFM in NSP.

Term	Expansion	Notes
MD	Maintenance domain	MD is the administrative container that defines the scope, reach and boundary for CFM message handling. It is typically the area of ownership and management responsibility. MD levels are in the range of 0 to 7, where the larger the domain, the larger the MD level assigned.
MA	Maintenance association	MA is the construct where the different management entities such as MEPs are contained. An MA is created within an MD. There is also an administrative context where a linkage is made between the domain and the service using the MA bridging-identifier configuration option.
MEG	Maintenance entity group	Typically, a MEG represents one service and consists of a group of MEPs. Only one MEG can be associated with a service, but one service can be associated with multiple MEGs. MDs and MEGs are distributed to NEs using policy distribution.
MEP	Maintenance end point	MEPs are the entities at the edge of a CFM MD and define the boundary for the domain. MEPs are responsible for initiating, processing, and terminating CFM messages. Each MEP with the same MD and MA represent endpoints for a single service.

5.3 How do OAM tests work?

Insights Administrator supports CFM and Twamp-light session tests.

PM session CFM testing is based on Metro Ethernet Forum Specification 35 - Service OAM Performance Monitoring Implementation Agreement, which details a standardized method to test and report network delay and loss using CFM messaging. This testing is performed in Layer 2 networks.

The PM session testing framework can also be used in the IP domain to perform TWAMP IP level monitoring, and runs over IPv4 and IPv6 addresses. TWAMP Light tests target Layer 3 interfaces, providing an option to monitor IP SLA performance as related to KPIs.

5.3.1 CFM DMM

For CFM Delay Measurement Message (DMM) tests, calculations are made to report on three

criteria: frame delay, frame delay range, and interframe delay variation. DMM test frames are issued at regular intervals from a source MEP. Delay measurement information for the forward, backward, and round trip paths is determined from the DMR frames received from the destination MEP.

5.3.2 CFM linktrace

CFM link trace messages that contain a target unicast MAC address are sent to multicast destination MAC addresses. Each MIP at the same MD level replies with a link trace response. Messages are forwarded to the next hop until they reach the destination MAC address.

5.3.3 CFM LMM

The CFM Loss Measurement Message (LMM) single-ended session test is a method of exchanging transmit and receive counters between peer MEPs to determine exact loss on a point-to-point Ethernet virtual circuit.

The following validations are performed:

- The LMM test suite tests can only be created or executed for MEG subgroups with exactly two MEPs.
- The LMM test suite tests can only be executed if the source and target MEPs are not already the source or target MEPs (respectively) of a currently running LMM test.

5.3.4 CFM loopback

CFM loopback messages are sent to a unicast destination MAC address. The MEP at the destination responds to the loopback message with a loopback reply. A MEP or a MIP can reply to a loopback message if the destination MAC address matches the MAC address of the MEP or MIP. CFM loopback tests verify connectivity to a specific MEP or MIP.

You can also perform multicast loopbacks by providing a multicast address (class 1 multicast destination) that aligns with the level that the originating MEP is configured on. Only one multicast test can be run at a time per NE, and results from the previous test are deleted when a new test is started. The stored values include the responding MEP MAC address, the sequence number, and a locally-assigned Rx index (allowing you to detect out-of-order responses).

5.3.5 CFM SLM

The CFM Synthetic Loss Measurement (SLM) session test is an extension of the Y.1731 standard that provides a method of exchanging transmit and receive counters to determine frame loss between a MEP and the destination MAC address or remote MEP ID of another node in the network. This test is used to verify MEP-MEP connectivity in the network and can be used to approximate the frame loss of actual data traffic. CFM SLM session tests measure frame loss using synthetic frames rather than data traffic. Frame loss is measured by calculating the difference between the number of synthetic frames that are sent and received.

5.3.6 Twamp-light

Twamp is a delay/loss measurement protocol that uses both the TCP connection service and the UDP session service.

Twamp-light tests can operate on a base router or on routing instances belonging to L3VPNs. The target, or destination entity, requires configuration of a Twamp-light reflector with a prefix associated

with the Twamp-light test source IP address and a specified UDP listening port in the range specified for the NE type. For example, the 7750 SR Twamp-light reflector destination port range is 864, 64364-64373. A target node requires a configured reflector for the base router instance or for each of the tested L3VPN-based virtual routing instances.

Twamp-light tests require a UDP source port in range undefined or configured in the NE range and a UDP destination port that matches the target device reflector UDP listening port.

Twamp reflectors, Twamp servers, and streaming templates cannot be configured in Insights Administrator. They can be discovered from the router configuration or configured using RESTCONF; see the MD-OAM tutorial on the [Network Developer Portal](#) for RESTCONF information.

See the Config Objects tab in Insights Administrator for the list of configured Twamp reflectors.

Twamp-light test types

You can configure a Twamp-light test to record delay, loss, or delay and loss statistics. Delay tests provide streaming results, accounting-session, and accounting-bin type results; loss tests provide accounting-loss-session type results. Streaming results require configuration of a streaming delay template. The streaming template defines the frequency at which real-time streaming results are received.

Accounting type results require configuration of an accounting policy, a file policy, and associated Twamp-light measurement interval configuration.

5.4 How do I create an OAM test?

1 _____

On the **Tests** page, click **+ TEST**.

2 _____

In the Create OAM Test form that opens, select the Test type and Entity type.

3 _____

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 services that match your input.
2. Click **+** as required to add additional filter criteria.
3. Choose an entity from the list and click **SELECT**.

4 _____

Select an entity reference type if applicable.


5

Click on the Source test entity field.

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 an entity from the list and click **SELECT**.

6

Click on the Destination test entity field.

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 an entity from the list and click **SELECT**.

7

Choose a test template. The test parameters are displayed.

8

Configure the test parameters.

9

Verify the parameters in the Advanced field.

10


Click **CREATE**. The test appears in the list of tests.


END OF STEPS

5.5 How do I execute an OAM test?

1

On the **Tests** page, configure a filter and click **RETRIEVE**. The list of tests is populated, filtered according to your input.

 **Note:** You can sort the list by clicking on a column header; however, the sorting function is not available for all columns.

Click  to open the **Test Details** panel to verify that the test parameters meet your needs. If the **Deployed state** parameter is Deployed, the NSP has received confirmation from the MDM server that mediation was successful.

2


Choose a test and click  (Table row actions), **Execute**. The Execute dialogue opens.

3

Configure the required parameters and click **EXECUTE**.

- The Sync mode parameter specifies whether or not execution requests generate notifications in the GUI. 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 Insights Administrator GUI. If this box is not checked, Insights Administrator does not display results of the test.

4

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

END OF STEPS

5.6 How do I edit or delete an OAM test?

5.6.1 To edit a test


1

On the **Tests** page, configure a filter and click **RETRIEVE**. The list of tests is populated, filtered according to your input.



Note: You can sort the list by clicking on a column header; however, the sorting function is not available for all columns.

2

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

The Editing function is not available for tests that are discovered from the NE.

3


In the form that opens, update the parameters as needed and click **UPDATE**.

END OF STEPS


5.6.2 To delete a test

1

On the **Tests** page, configure a filter and click **RETRIEVE**. The list of tests is populated, filtered according to your input.

 **Note:** You can sort the list by clicking on a column header; however, the sorting function is not available for all columns.

2

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

END OF STEPS


5.7 How do I view OAM test results?

Test results are available in Insights Administrator for tests configured from Insights Administrator or from the RESTCONF API, as long as the original configuration specifies that results are published to the database. Tests created from NE CLI or another network manager are not processed within the NSP.


Twamp-light delay results can also be provided in an accounting file, in the classes `telemetry:/base/oampm-accounting/twl-session-acc-stats` and `telemetry:/base/oampm-accounting/twl-bin-acc-stats`. Twamp-light loss results are available in an accounting file in the class `telemetry:/base/oampm-accounting/twl-session-loss-acc-stats`.

1

On the **Tests** page, configure a filter and click **RETRIEVE**. The list of tests is populated, filtered according to your input.

 **Note:** You can sort the list by clicking on a column header; however, the sorting function is not available for all columns.

2

To view test information, choose a test and click **Test Details** .

The Test Details panel shows the test attributes, and the Tested Entities panel shows the list of entities. Information provided depends on the test type.

3


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. Use the drop-down lists to filter by time frame and telemetry type as needed.


i **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 _____
Select a different time range for the test executions, if required. Choose a range from the drop down list, or configure a customized time range.

5 _____
If required, choose a telemetry type from the drop-down list.

6 _____
To see additional information columns on the Test executions page, click  (Table row actions), **Manage Columns**. Select or de-select columns to suit your information needs.

i **Note:** The sorting function is not available for columns on the Test executions page. By default, executions are sorted by Time Captured.

7 _____
For more detailed information about a specific test, choose an execution and click **Test result details** .
Information provided depends on the test type.

END OF STEPS _____

5.8 How can I troubleshoot Twamp-light test issues?

The following guidelines apply to Twamp-light tests, but may also be useful for other test types. Contact support if you need further assistance.

- The test doesn't start.
Usually, errors on test execution occur when there is a difference in state between the NSP and the NE or if test attributes are outside the accepted range of the NE. In this case, follow guidance from the error or warning message returned when the test is started. Executing the test in sync-mode "sync-execute" ensures that the most complete error and warning messages are shown in Insights Administrator.
- The test starts and results are received, but the packet counts and delay values are all zero.
 - Confirm that the destination address is reachable from the NE executing the test.
 - Confirm that the Twamp-light reflector is enabled, that the test dst-udp-port parameter matches the reflector listening port, and that the Twamp-light reflector has a matching prefix for the test src IP address parameter.
- The test starts but no results are observed.
 - Check the execution status from Insights Administrator to confirm that the test is executing.
 - Confirm the test type and the expected result classes. Verify from the results class (streaming

or accounting) the expected delay until the first result should arrive. Confirm that the correct class of result is selected, and click **Refresh Results** to trigger result retrieval from results stored to the database.

- Confirm that the configuration is correct and complete: the deployment state is “deployed”, the streaming template is defined (for intended streaming delay results), the bulk result is true (for intended accounting results), and properties (IP addresses, UDP ports, measurement interval) are correct.
- If streaming test results are intended, validate the configuration and status of the streaming delay template (especially the admin state and sample window period).
- Validate telemetry subscriptions for the test classes: telemetry subscriptions are created automatically for tests created in the NSP. 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`.
- Validate the Twamp-light reflector configuration:
 - Does the target node have a deployed, enabled reflector?
 - Does the UDP port match those of configured tests?
 - Is the reflector on the correct routing instance (router- or service-based)? Twamp-light reflector prefixes can be viewed from the RESTCONF API.
- Validate the bin group information for accounting type results: confirm that the bin group configured in the test is configured on the node and that admin state is enabled. Details of bin groups may be configured or retrieved using RESTCONF API or discovered from node configuration.


6 OAM test suites

6.1 What is an OAM test suite?

A test suite is 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.

Insights Administrator provides a read-only list of test suites created in the MD-OAM RESTCONF API and in Insights Administrator.

See the MD-OAM App tutorial on the [Network Developer Portal](#) for information about using the API.

 **Note:** On-demand test suites can be created and executed for LMM and SLM tests, but results may not be available to be shown.

6.2 How do I create an OAM test suite?

1

On the **Test Suites** page, click **+ SUITE**.

2

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.

3

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.


4

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.

5

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**.

6

Configure the test parameters as needed.

7

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

After the test suite is successfully created, Insights Administrator automatically navigates to the GENERATION LOG tab of the **View Test Suite Details** screen for the generated test suite. The generation log automatically refreshes every few seconds to show the test generation process.

As soon as the test suite is executed, a new row in the AGGREGATED RESULTS tab appears, corresponding to that execution. If a test suite execution has produced any results, the results corresponding to that execution are visible in the INDIVIDUAL RESULTS tab.


6.3 How do I stop or start an OAM test suite?

1


On the **Test Suites** page, choose a test suite and click  (Table row actions), **Execute**.

2

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.

3

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

END OF STEPS


6.4 How do I edit or delete an OAM test suite?

Test suites can only be modified using the MD-OAM RESTCONF API.


To delete a test suite, choose a test suite and click  (Table row actions), **Delete**.

Deleting a test suite deletes all associated tests.





6.5 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.

1

On the **Test Suites** page, choose a test suite and click  (Table row actions), **View Details**.

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

Tab	Notes
AGGREGATED RESULTS	<p>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.</p> <p>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 .</p>
INDIVIDUAL RESULTS	<p>The page displays the results of each test executed.</p> <p>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 .</p> <p>For more detailed information about a specific test, choose an execution and click View Results .</p> <p>Note: If a test suite was created from the Insights Administrator application, 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.</p> <p>See the TESTS tab for a list of tests in the suite.</p>
GENERATION LOG	<p>The page displays log information from the generation of the suite and tests.</p>
TESTS	<p>The page lists the test identifiers included in the suite.</p> <p>If the test suite is an on-demand suite, the TESTS tab shows the included tests grouped by stage.</p> <p>Stages are executed sequentially, but tests within each stage will be executed either sequentially or in parallel depending on how the stage is configured.</p> <p>For more detailed information about a specific test, double click on an execution or choose an execution and click View Results .</p>

END OF STEPS

7 Config objects

7.1 What is a config object?

A config object in Insights Administrator represents an OAM configuration object that is used for testing, other than the test object itself.

Insights Administrator provides a list of configuration objects. Click on the object type drop-down list to switch to the list for a different object type.

7.2 What config objects are available in Insights Administrator?

The following table describes the available configuration objects.

Configuration object type	Description	Notes
Bin Group	A bin group is a template of Performance Measurement histogram measurement bin definitions. Bin groups contain measurement bins, which count instances of frame delay (FD), frame delay range (FDR), or interframe delay variation (IFDV) metrics within a defined range of lower to upper threshold values. Bin group definitions may also include definitions for delay-event thresholds and calculation of average FD, FDR, and IFDV values.	Bin groups define a service level agreement quality quantitatively. Service offerings with differentiated service level agreements may be measured using different bin groups.
CFM Domain	CFM Maintenance Domain (level 0 to 7)	Each MD can include multiple MAs.
CFM Association	CFM maintenance associations.	Insights Administrator supports auto-configuration of MAs when creating CFM based tests
CFM MEP	CFM maintenance entity point. A MEP is an end point in an MA, on which CFM tests can be performed. Each MEP with the same MD and MA represents endpoints for a single service.	Insights Administrator supports auto-configuration of MEPs when creating CFM based tests. Service MEPs, such as SAPs, and facility MEPs, such as LAGs, are supported.
Streaming Delay Template	A template that defines real-time measurement of FD and IFDV from delay-based Performance Management tests. Average values are calculated over 10-to-60 second intervals and stream in real-time.	NSP supports delay streaming using gNMI, for 7750 SR NEs.

Configuration object type	Description	Notes
Twamp Server	<p>TWAMP is a delay/loss measurement protocol that uses both the TCP connection service and the UDP session service. A TWAMP server may be configured to accept TCP control connections from a specified range of IP networks and TCP ports; also, it will accept requests for clients to initiate UDP test sessions for specific IP address or UDP port pairs on the service router.</p>	—
Twamp-light Reflector (Router)	<p>A Twamp-light reflector controls the set of IP network and UDP ports where the service router replies to TWAMP-light test messages. TWAMP light reflectors may be configured for both base and service routing instances.</p>	<p>Insights Administrator supports auto-create/update of TWAMP-light reflectors when starting TWL based tests.</p>
Twamp-light Reflector (Service)		

7.3 How do I create a config object?

Config objects are created using RESTCONF, using classic IP mediation, or, for CFM objects in particular, can be auto-generated when CFM tests are created.

7.4 What can I do with config objects in Insights Administrator?

You can sort or filter the lists or click  (Delete) to delete a config object.

Any other actions must be done using RESTCONF or classic IP mediation, depending on how the object was created.


8 Baselines


8.1 What are baselines and anomalies?

Baselines and anomaly detection are included with NSP Baseline Analytics.

A baseline detects a historical trend and generates expected values based on the trend.

An anomaly is a value that deviates enough from the expected value to be flagged for attention. You can configure anomaly thresholds as part of baseline creation.

Baseline and anomaly charts and the list of anomalies are available in the Insights Viewer utility. To open Insights Viewer, click  (More), **Insights Viewer** at the top of any page in Insights Administrator. Insights Viewer opens to the Baseline Charts page.

To open Insights Viewer for a baseline, choose the baseline and click  (Table row actions), **Open in Insights Viewer**. Insights Viewer opens to a New Chart form with the baseline selected.


RESTCONF APIs are available for Baseline Analytics; see the Network Infrastructure Management API documentation on the [Network Developer Portal](#).

8.2 How do baselines and anomalies work?

A baseline provides the logic for the collection of baseline statistics, and for the detection of anomalies.

When you create baselines, you specify a resource or group of resources to collect a set of statistics over a defined time window. Information collected during that window is used to calculate a data point for the baseline. You also define a season, which is the length of time statistics need to be measured to assess trends. For example, to assess network traffic, you could set up a 15-minute window with a one-week season, which provides values calculated every 15 minutes over a one-week period.

Creation of a baseline creates a baseline subscription to collect the required data.

 **Note:** Baseline subscriptions and telemetry subscriptions are separate. A baseline cannot be generated from data collected by a telemetry subscription.

On-demand NFM-P statistics cannot be used to create baselines.

A baseline consists of the following components. The components appear in the Create and Edit forms.

- [General parameters](#)
- [Filter & Counters](#)
- [Anomaly Detectors](#)

Baselines are created on a per-resource basis. A resource is an entity that can collect the desired statistics. In the Create Baselines form, you configure the required parameters and choose the resources to collect the statistics.

If the NE is managed using MDM, configuration of a baseline initiates statistics collection. If the NE is managed by NFM-P, statistics collection must be configured on the NFM-P and the resource must already be collecting the desired statistics for a baseline to be created.

 **Note:** Baseline Analytics is different from the NSP Analytics application.

Baseline Analytics provides near-real-time baseline and anomaly detection from telemetry counters, for example, received octets for the `/telemetry:base/interfaces/interface` telemetry type.

The Analytics application computes a baseline for data configured for reporting, for example, utilization and throughput for a port in a Port LAG Details report, or bandwidth and data for an application group in a Router Level Usage Summary report with Baseline. See the *Analytics Report Catalog* and the *NSP User Guide* for more information about Analytics.

8.2.1 Baseline Analytics data storage

Baseline data is stored in Postgres, unless there is an auxiliary database enabled, in which case all collected data goes in the auxiliary database.

The following data is stored:

- statistics data collected during the configured window; see [General parameters](#)
- the calculated baseline for the window
- anomalies

By default, data is stored in Postgres for 35 days and in the auxiliary database for 90 days. These values can be changed using the RESTCONF API.

8.2.2 General

The general parameters include the following:

- **Description**
Add an optional description for filtering on the Baselines page.
- **Collection interval**
For MDM managed NEs, this represents the interval at which to collect the statistics, for example, every 30 seconds. For NEs managed by the NFM-P, this value is ignored and statistics are collected according to the settings configured in the NFM-P.
- **Season**
A season is the length of time statistics must be collected for a pattern to be seen. For example, for network traffic you can expect the data pattern to repeat on a weekly basis.
- **Window duration**
Window duration is the size of the data bucket for telemetry calculation. For example, a counter calculates the change between the first and last values taken during the window. The calculation used depends on the counter type parameter in the Filters & Counters panel.
- **Admin State and Training Status**
These parameters are enabled by default when a baseline is created. They can be changed in the Edit form.
 - **Admin State**

If the Admin State of a baseline is Enabled, Insights Administrator is monitoring the statistics.

– **Training Status**

If the Training Status is Active, Insights Administrator is incorporating new information into the baseline's model. If the Training Status is paused, future anomalies will be detected against the expected values that are already calculated.

If you are monitoring for error counters, such as packet loss, you can pause learning after a season with no errors, which sets the expected number of errors to zero, while continuing to monitor.

For example, if you create a baseline and set the Collection Interval to 30, the Season to 1 week, and the Window Duration to 15 minutes, the baseline subscription collects the statistics values every 30 seconds, calculates a baseline data point every 15 minutes, and assesses trends based on one week of data.

8.2.3 Filter & Counters

The Filter & Counters parameters declare the telemetry values to be collected, the counter types, and the resources of interest.

When a telemetry type is selected, the **Add Counters** button becomes available.

You can configure one of the following counter types:

- **Counter:** a counter takes input counter values and calculates the change in value over the window. For example, if the counter represents the number of transmitted octets and windows are 15 minutes, a counter baseline value is the number of octets transmitted over 15 minutes.
- **Gauge:** a gauge takes input values and calculates the mean value over the window. For example, if the input value is octets per second over a 30 second period and windows are 15 minutes, a gauge baseline value is the mean octets per second over 15 minutes.
An example of a gauge is CPU usage: it is a bounded value between 1 and 100%.
- **Sampled:** a sampled baseline takes sampled values and calculates the sample mean value over the window. Sampled values represent the value at the exact time the sample was taken, not the value since the last sample was taken. For example, if CPU % is sampled every 2 minutes and windows are 15 minutes, a sampled baseline value is the sampled mean over the samples collected in the 15 minutes.
An example of a sampled value is latency.

Configure an object filter as needed to filter the available resources; see [1.3 “How do object filters work?”](#) (p. 10).

When at least one counter is added, the **Verify Resources** button becomes available.

8.2.4 Detectors

A detector defines the rules for anomaly detection. The detector rule provides an acceptable range of expected values. If a detected value exceeds the range, it is marked anomalous.

Anomaly detection is optional.

A detector rule is composed of the following:

- **algorithm** — the formula to use to compare the expected and measured values

- comparison — greater than or less than
- evaluate what — value, rate, or bandwidth

The measured values may be converted to a rate or bandwidth to perform the evaluation:

- rate — $\text{value} / \text{window}$
- bandwidth — $(\text{value} * 8) / \text{window}$

- threshold — the end of the acceptable range

The comparison and threshold parameters define the range of acceptable values. For example, a rule could state that a value with an absolute Z-score greater than 2 is an anomaly.

Algorithms

You can define a rule based on an algorithm.

The following algorithms are suitable for most purposes:

- **Z-score**

This refers to the Z-score (number of standard deviations) of the measured value against the expected values. In this case, the expected value is the mean.

Formula: $(\text{measured} - \text{expected}) / \text{stddev}$

- **Z-score absolute**

This refers to the absolute value of the Z-score of the measured value against the expected values. In this case, the expected value is the mean.

Formula: $|(\text{measured} - \text{expected}) / \text{stddev} |$

The Z-score algorithms are useful because they incorporate the standard deviation: in addition to recording how far the current value is from the mean, the algorithm also factors in the variability of the values. This can be very important when deciding if a value is anomalous. If your values are highly variable, that is, the standard deviation is high, it is important to choose a Z-score algorithm.

You can also use one of the following:

- **relative difference mean**

This is the relative difference using the absolute value of the arithmetic mean of the measured and expected values.

Formula: $| \text{measured} - \text{expected} | / (| \text{measured} + \text{expected} | * 0.5)$

This algorithm could be suitable if the standard deviation is very small, that is, if there is very little variation in the values.

- **relative change signed**

This is the relative change (including the positive or negative sign) between the measured and expected values.

Formula: $(\text{measured} - \text{expected}) / | \text{expected} |$

- **relative change**

This is the relative change (with no sign) between the measured and expected values.

Formula: $| \text{measured} - \text{expected} | / | \text{expected} |$

- **change over mean**

This is the change of the measured and expected values over the absolute value of the arithmetic mean.

Formula: $(\text{measured} - \text{expected}) / (|\text{measured} + \text{expected}| * 0.5)$

- **change max score**

This is a score that becomes more sensitive as the measured or expected value approaches +/-100. This detector algorithm works well with percentages although it may have use with other types of values.

Formula: $(\text{sign}(\text{measured} - \text{expected}) * (|\text{measured} - \text{expected}| + \text{max}(\text{measured}, \text{expected}))) / 200$

8.3 What should I know about baseline and anomaly detector creation?

When baselines are configured, Insights Administrator creates a baseline with the parameter values for each resource selected. For example, if you want to collect baseline values for 20 ports with the same telemetry type, configure the Create Baselines parameters and Insights Administrator will create 20 baselines.

Bulk creation of baselines can take significant time and resources to complete. If the bulk creation process is interrupted by a network disruption or user action, it results in failed or partial creation.

If a baseline creation process has been interrupted by a network problem or user action (such as a page refresh), incorrect entries may exist in the database. Contact Nokia support.

Keep these suggestions in mind:

- Use object filters in the Create Baselines form to target the resources you need.
- Avoid unfiltered baseline creation requests unless the network is limited in size.
- If you configure the Convert to Bitrate parameter for a baseline counter and want to detect anomalies, set the Evaluate What parameter in the detector rule to Bandwidth. Using a different evaluation setting results in a mismatch between the Anomalies list in Insights Viewer and the baseline and anomaly chart generated for the baseline.
- Current Baseline and Indicator support for OAM telemetry is limited to the following:
telemetry type: `telemetry:/base/oam-pm/twamp-light-delay-streaming`
counter: `delay`
Other telemetry types and counters are not certified by Nokia.
- Ensure that you have enough time to wait for the creation operation to complete before configuring baseline creation.

The following table shows some average time frames for bulk baseline creation.

Number of baselines	Average maximum time required
100	30 s
1000	3 min
5000	15 min
10 000	30 min

i **Note:** The baseline subscriptions are created last, therefore no statistics are collected for any baseline in the group until the bulk creation is completed.

8.4 How do I create baselines?

i **Important!** If you are creating multiple baselines, the create operation may take a long time and cannot be stopped. Ensure that you are able to wait for the operation to complete before proceeding. For example, average maximum time required for creation of 100 baselines is 30 s; average maximum time required for creation of 10 000 baselines is 30 min.

1 _____

On the **Baselines** page, click **+ BASELINES**.

2 _____

In the Create Baselines form that opens, configure the General parameters as needed.

3 _____

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.

4 _____

Click **+ COUNTERS** .

5 _____

In the **Add Counters** form that opens, choose the required counters and click **ADD**.

6 _____

Configure the Counter parameters as needed.

7 _____

Click **+ COUNTERS** to add additional counters.

8 _____

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.

9 _____

Click **VERIFY RESOURCES**.

Insights Administrator searches for resources that are collecting statistics to match the telemetry type and object filter.



Note: NFM-P resources appear in the list after the NFM-P collects the statistics. Therefore, you need to wait for the current collection interval to end before the NFM-P resource appears in the list.

If needed, you can click **STOP VERIFICATION** at any time and **Edit Filters & Counters** to update the configuration and restart the verification process.

10

When the resources you need appear in the resources list, click **STOP VERIFICATION**.

11

Select the resources you need in the resources list.

12

In the Detectors panel, add a rule for each counter as needed:

1. Click **+ RULE**.
2. Configure the rule parameters.

Repeat steps 1 and 2 to add detector rules for other counters.

13

Click **CREATE**.

END OF STEPS

8.5 How do I edit a baseline?

1

On the **Baselines** page, choose a baseline and click (Table row actions), **Edit**.

2

To stop or restart monitoring, change the **Admin State** parameter.

If the admin state is Disabled, Insights Administrator stops monitoring the statistics.

3

To stop or restart training, change the training status parameter.

If the training status is Paused, new data will no longer affect the calculated baseline.

4

To reset training:


1. If the Admin State is Enabled, select Disabled from the drop-down list and click **UPDATE**.
2. Click **RESET BASELINE WINDOWS** and click **APPLY** to confirm.
3. Wait a minimum of 15 min.

You can close the form while you are waiting, if needed.

4. Click **RESET BASELINE WINDOWS** again and click **APPLY** to confirm.
5. Set the Admin State to Enabled and click **UPDATE**.

5

To edit detectors:

1. Click  (Delete) to remove the existing detector.
2. Click **+ RULE**.
3. In the Detector Rule form that opens, configure the new parameters.
4. Click **TEST** to preview how your changes will impact the range of expected values.
5. Click **ADD**.

6



Click **UPDATE**.

END OF STEPS


8.6 How do I delete a baseline?

1

On the **Baselines** page:

- To delete one baseline, select the baseline and click  (Table row actions), **Delete**.
- To delete multiple baselines, use the Control or Shift key to select two or more baselines and click  (Delete) at the top of the page.

2

From the Subscriptions page, select a baseline subscription and click  (Table row actions), **Delete**.

Deleting the subscription also deletes all associated baselines.

3

In the form that opens, confirm the deletion.

END OF STEPS

9 Indicators

9.1 What is an indicator?


An indicator is a subscription to a customized metric. Indicators allow you to define and track KPIs using a combination of telemetry data, arithmetic operators, and aggregation functions. Thresholds can also be included in the indicator, with actions that are triggered by threshold violations.



For example, you can create an indicator to track the average utilization of a three-node ring: utilization counters on the selected ports and LAGs in the ring are tracked and aggregated. Thresholds are set for rising and falling average utilization at specified values, generating alarms when the average utilization is outside the preferred range.

Creation of an indicator creates an indicator subscription to collect the required data.

i **Note:** Indicator subscriptions and telemetry subscriptions are separate. An indicator cannot be generated from data collected by a telemetry subscription.

On-demand NFM-P statistics cannot be used to create indicators.

Indicator charts and a list of threshold crossing events are available in the Insights Viewer utility. To open Insights Viewer, click  (More), **Insights Viewer** at the top of the page. Insights Viewer opens to the Indicator Charts page.

To open Insights Viewer for a selected indicator, choose the indicator and click  (Table row actions), **Open in Insights Viewer**. If the indicator has multiple outputs, choose the resources in the form that opens and click  **OPEN IN INSIGHTS VIEWER**. Insights Viewer opens to a New Chart form with the indicator resources selected.

RESTCONF APIs are available for NSP Indicators; see the Network Infrastructure Management API documentation on the [Network Developer Portal](#).

9.2 How do indicators work?

An indicator consists of the following components:

- [General parameters](#)
- [Filter & Counters](#)
- [Thresholds](#)

The components appear in the Create and Edit forms.

9.2.1 Sample indicator

An example indicator tracks average utilization for a three-node ring, sampling from four ports and a LAG in the ring. Alarms are generated if average utilization is increasing above 50% or decreasing below 5%.

9.2.2 General

The general parameters include the following:

- unique name and optional description

- **collection interval**

For NEs managed by MDM, this represents the interval for collecting the statistics (for example, every 30 s), while for NEs managed by the NFM-P, this value is ignored and statistics are collected according to the settings configured in the NFM-P.

- **window duration**

Window duration is the size of the data bucket for telemetry calculation.

i **Note:** For simple indicators, that is, indicators with only one counter and no formula, there is no data bucket. The window duration is ignored; KPI values are calculated at the collection interval.

9.2.3 Counters & Formula

The Counters & Formula parameters declare the telemetry values to be collected and the operations and aggregation functions to apply. An object filter ensures that the data is collected on the resources of interest.

- **counters**

When a telemetry type is selected, the **+ ADD COUNTERS** button becomes available.

For the sample indicator, selecting the `/telemetry:base/interfaces/utilization` telemetry type allows collection of the input-utilization counter.

- **formula**

A formula applies arithmetic operators and aggregation functions to the counters. The following can be applied:

- arithmetic operators: addition, subtraction, multiplication, division, absolute value
- aggregation functions: minimum, maximum, sum, average

For the sample indicator, the formula is configured to provide an average of the counter value data.

See [9.3 “How do formulas work?” \(p. 54\)](#) for details.

Object filter

Configure an object filter as needed to filter the available resources; see [1.3 “How do object filters work?” \(p. 10\)](#).

When at least one counter has been selected, the **VERIFY RESOURCES** button becomes available. Check the contents of the resource list to ensure that your object filter is retrieving the correct objects.

For the sample indicator, the object filter determines the ports and LAGs to collect information from.


9.2.4 Thresholds

Thresholds define the preferred range of data values for the indicator. Thresholds are optional: you can create zero, one, or multiple thresholds, for increasing or decreasing values.

When the indicator is plotted in Insights Viewer, thresholds appear on the plot and threshold crossing events are indicated.

Each threshold can be configured to trigger one or more actions:

- **raise a threshold crossing alarm (TCA)**
The TCA is raised in Fault Management.
- **generate email**
An email can be generated for each threshold crossing event or aggregated by time period or number of events.
Email server settings must be configured in NSP Settings in the NSP Launchpad by an administrator.
- **output a message to a Kafka topic**
The Kafka topic must already be created. The default topic is **nsp-act-action-event**.

 **Note:** Indicator alarms may still be raised shortly after a resource (for example, an NE) is unmanaged in NSP if statistics messages are already in the system waiting to be processed.

For the sample indicator, you can configure an example threshold, with:

- an increasing threshold for a value of 50
- an alarm action with major severity
- a falling threshold for a value of 5 with a Kafka message showing low utilization

This configuration allows for high and low utilization to be handled differently according to differing levels of urgency. If needed, another increasing threshold could be set at 40, for example, with warning severity, to tell operators that the ring may need attention.

Threshold crossing alarms

Indicator TCAs appear in Fault Management as alarms with Source System “fdn:app:nsp-indicator” and Alarmed Object Type “nsp-indicator:rta-indicator-rules/rule”. The Alarmed Object ID contains the indicator rule name and the Additional Text contains the threshold violation details.

The Object Full Name field contains the indicator name and the specific object instance. For aggregate TCAs, where the aggregation functions such as avg() or sum() are used, the threshold violation may be based on statistics from multiple objects, and therefore cannot be attributed to a single object instance. In this case, the Object Full Name field contains the name of the indicator rule.

Visibility of TCAs depends on user access control settings in User Management.

- Aggregate TCAs do not contain a Site ID or Site name, and are considered system level alarms. To view these alarms, the user must either have the Administrator role, or have both **Access to all Equipment** and **Access to all Services** enabled.
- If the user has access to certain NEs only, the user sees Indicator TCAs for those NEs, but no aggregate TCAs.

9.2.5 Simple and complex indicators

Simple indicators use a single counter and no formula. A simple indicator is evaluated every collection interval, for every resource returned by the object filter.

Complex indicators use one or more counters and a formula. A complex indicator uses counter statistics received during each window duration to aggregate each incoming counter from each resource into a counter function. This output is then, depending on the formula, used in arithmetic or aggregation operations, or both, to calculate the KPI.

9.2.6 Indicator data storage

Indicator data is stored in Postgres unless there is an auxiliary database enabled, in which case all collected data is stored in the auxiliary database.

By default, data is stored in Postgres for 35 days, and in the auxiliary database for 90 days. These values can be changed using the RESTCONF API.

9.3 How do formulas work?

An indicator formula defines the calculation of a KPI value. A formula is optional if only one counter is configured.

Formulas are composed of the following components, combined as needed.

Component	Definition	Notes
Counter functions	<p>Aggregation functions performed on a per-counter basis with one value output per counter for each resource. The output of the counter function is then used in the rest of the formula calculation.</p> <p>Counter functions are expressed as <i>counter_function</i>, for example, <i>input-utilization_avg</i>.</p>	<p>The following function types are available on a counter:</p> <ul style="list-style-type: none"> • sum: adds up all samples received for the counter during the window duration. Sum is used for counted statistics such as octets or packets. • avg: the average of all samples received for the counter during the window duration. Avg is used for rate or value statistics such as percentage or temperature. • min/max: the minimum or maximum value of all samples received for the counter during the window duration.
Arithmetic operations	<p>Simple arithmetic operations using one or more counters received from each unique resource. These operations produce <i>n</i> KPI outputs (one per resource), per window period. Operations can include counter functions and numbers. Negative numbers must be in parentheses.</p> <p>An example of an arithmetic expression is: $({received-octets-periodic_sum} - {transmitted-octets-periodic_sum}) * 8 / 60$</p>	<p>The following arithmetic operations can be performed:</p> <ul style="list-style-type: none"> • addition (+) • subtraction (—) • multiplication (*) • division (/) • absolute value ()

Component	Definition	Notes
Aggregation functions	<p>A formula can perform aggregations on one or more counters received from every resource. This aggregation produces a single indicator output (one KPI value for all resources) per window period.</p> <p>An aggregation operation can perform multiple aggregation operations and can include arithmetic operations. For example, a formula for average utilization in the sample indicator is: <code>avg({input-utilization_avg})</code></p>	<p>The following aggregation operations are available:</p> <ul style="list-style-type: none"> • min • max • sum • avg

An example formula combining the components is: `max(({transmitted-octets-periodic_sum}+{received-octets-periodic_sum})*8/60)/sum({speed_avg})*100`

This formula creates a single mixed-expression-operator that has two aggregation operations: the first outputs the port with the maximum value of `((tx+rx)*8/60)`, the second sums the speed of all ports. These two outputs are then divided and the result multiplied by 100.

9.4 What should I know about indicator creation and management?

Keep the following notes in mind when creating and managing indicators:

- Consider the following when you set the collection interval and window duration:
 - The collection interval configured in Insights Administrator is ignored by resources that are managed by NFM-P. Instead, the collection interval of resources managed by NFM-P is determined by the corresponding NFM-P MIB entry policy.
 - When configuring an indicator with a formula for resources managed by NFMP, the window duration must be at least twice as long as, and be a multiple of, the NFM-P MIB policy. An example is a 5 min MIB policy and a 15 min window duration.
 - When configuring an indicator with a formula for resources managed by MDM, the window duration must be at least twice as long as, and be a multiple of, the collection interval.
- Avoid divide-by-zero scenarios when constructing formulas. Arithmetic operations that are divided by zero produce no output, while aggregation operations output zero from the operation that is divided by zero.
- Before completing indicator creation, it is the best practice to verify resources to ensure you see a reasonable value for each counter.

Certain counters may not be fully supported in an NE managed by NFM-P and they default to zero, which causes an unexpected calculated KPI value. Other counters may have an actual value of zero. For example, a value of zero for a speed counter can indicate a down port—that is, an actual value of zero speed—or a counter that does not appear in the relevant mapping file.
- Clicking **VERIFY RESOURCES** in an indicator shows the network device identifiers for the resources that respond to the object filter. The network device identifier is the unique identifier included by the NE in the telemetry messages.

The network device indicator is also the NE identifier used for indicator charting and threshold events in Insights Viewer.
- If an indicator configuration is updated, the indicator restarts, causing an expected gap in data until it can start collecting data with the new window duration.
- Indicator data points are normalized to the start of the window duration. For example, for an

indicator with a window duration of 15 min, the data point or threshold event at 16:15 on the chart represents the window from 16:15 to 16:30.

- Data points for simple indicators are output immediately after the window duration ends.

- Output from Indicators with formulas:

The data required by the formula must be received and processed after the window duration ends before generating the Indicator value.

Example: Indicators with a 5-minute collection interval and 15-minute window duration. The 15-minute collection window starts at midnight (00:00 to 00:15).

After the window closes, the indicator waits for the next set of messages to be received before proceeding to calculate the indicator value for the previous window. When a message is received with a time stamp after 00:15, it confirms that all messages from the 00:00 to 00:15 window have been received and the value can be calculated.

- Indicators with arithmetic operations require one additional collection interval.
- Indicators with aggregation operations require one additional collection interval and one window duration.
- Output from an indicator with an arithmetic formula requires an additional 5 minutes (the collection interval).

For example, consider formula: {received-octets-periodic_sum}+{transmitted-octets-periodic_sum}

The data point for the 00:00 to 00:15 collection window is processed at 00:20. The sum can be calculated when the next collection occurs and a value for after 00:15 is received.

- Output from an indicator with an aggregate formula requires an additional 20 minutes (the collection interval, plus the window duration).

For example, consider formula: sum({received-octets-periodic_sum}+{transmitted-octets-periodic_sum})

The data point for the 00:00 to 00:15 window is processed at 00:35.

The example formula is a sum of values which are collected at an interval. Each of these values is confirmed when the next interval starts, at 00:20. After the values are confirmed, the sum can be calculated. The sum is confirmed when another aggregated message from after 00:15 is received, at 00:35.

9.5 How do I create an indicator?

1 _____

On the **Indicators** page, click **+ INDICATOR**.

2 _____

In the Create Indicator form that opens, enter a unique name for the indicator.

3 _____

Configure the collection interval and window duration parameters.

4

If needed, click **APPLY TEMPLATE** at the top right of the window, select a template from the list, and click **APPLY**.

The parameters configured in the template appear in the Create Indicator form. These parameters can be changed.

5

Configure the counters and formula as needed:

1. 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.
2. Click **+ COUNTERS**.
3. If you have chosen more than one counter, a formula is required; see [9.3 "How do formulas work?"](#) (p. 54).
Enter information in the Formula field. As you type, the field identifies incorrect syntax.

6

In the **Object Filter** field, enter filtering information as needed to filter the collected data; see [1.3 "How do object filters work?"](#) (p. 10).

As you type, the field provides suggestions for available filters to match your input and identifies incorrect syntax.

7

Click **VERIFY RESOURCES** to ensure that the resources found by the object filter are correct for your requirements and that counter values are returned.

8

Configure thresholds as needed:

1. Click **+ THRESHOLD**.
2. In the Add Threshold window that opens, enter a threshold value in the Threshold field.
3. Choose a direction from the drop-down list.
4. Click **ADD**.
5. Add additional thresholds as needed.

9

Configure threshold actions as needed:

1. Click on a threshold you created in [Step 8](#).
2. Click **+ ACTION** and choose **Alarm**, **Email**, or **Kafka** from the drop-down list.
 - To configure an alarm, choose the severity from the drop-down list.

- To configure an email action, enter recipient email addresses, separated with commas, and enter boilerplate information in the Subject and Content fields.
To aggregate emails, enable the Aggregation toggle and configure the parameters. For example, the default value of 5 in the Period and Number of Events fields will send an email every five min, and for every five threshold crossing events, whichever comes sooner.
- To configure a Kafka message, enter an existing topic name and enter the message information in the Content field.

3. Add additional actions for each threshold as needed.
4. Click **SAVE**.

10

Click **CREATE**.



Note: If your formula does not include all the counters you selected, the **CREATE** button is dimmed. If you cannot create the indicator, check the Formula field to ensure all counters you selected are part of the formula and spelled correctly.

END OF STEPS

9.6 How do I edit or delete an indicator?



Attention: When an indicator is changed, the current data window becomes invalid and a new data bucket is created starting from the next interval. Depending on the timing, up to two window periods of data could be missed.

9.6.1 To edit an indicator

1

On the **Indicators** page, choose an indicator.

2

Click (Table row actions), **Edit**.

3

In the form that opens, update the parameters as needed and click **UPDATE**.


END OF STEPS

9.6.2 To delete an indicator

1

On the **Indicators** page, choose an indicator.

2

Click  (Table row actions), **Delete**.

END OF STEPS

10 Indicator templates

10.1 What is an indicator template?

An indicator template is a set of parameters that a user can optionally employ to create an indicator.

When a template is applied, the configuration information in the template is copied to the indicator configuration. The indicator parameters provide the object filter, collection interval, and window. That is, the KPI is defined in the template and the KPI object and collection details are defined in the indicator. Thresholds are optional and can be configured in the template or the indicator.

For example, a template can be created for average port utilization. An indicator created from the template specifies the port and configures the data collection.

10.2 How do I create an indicator template?

1

On the **Indicator Templates** page, click **+ TEMPLATE**.

2

In the Create Indicator Template form that opens, enter a name for the template.
The name must be unique.

3

Enter a description and units as needed.

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 from the list of matches.

5

Click **+ COUNTERS**.

6

If you have chosen more than one counter, a formula is required; see [9.3 "How do formulas work?"](#) (p. 54).

Enter information in the Formula field. As you type, the field identifies incorrect syntax.

7

Configure thresholds as needed:

1. Click **+ THRESHOLD**.
2. In the Add Threshold window that opens, enter a threshold value in the Threshold field.
3. Choose a direction from the drop-down list.
4. Click **ADD**.
5. Add additional thresholds as needed.


8

Configure threshold actions as needed:

1. Click on a threshold you created in [Step 7](#).
2. Click **+ ACTION** and choose Alarm, Email, or Kafka from the drop-down list.
 - To configure an alarm, choose the severity from the drop-down list.
 - To configure an email action, enter recipient email addresses, separated with commas, and enter boilerplate information in the Subject and Content fields.
To aggregate emails, enable the Aggregation toggle and configure the parameters. For example, the default value of 5 in the Period and Number of Events fields sends an email every 5 min and for every five threshold crossing events, whichever comes sooner.
 - To configure a Kafka message, enter an existing topic name and enter the message information in the Content field.
3. Add additional actions for each threshold as needed.
4. Click **SAVE**.

9

Click **CREATE**.

 **Note:** If your formula does not include all the counters you selected, the **CREATE** button is dimmed. If you cannot create the template, check the Formula field to ensure all counters you selected are part of the formula and spelled correctly.

END OF STEPS

10.3 How do I edit or delete an indicator template?

10.3.1 To edit an indicator template

1

On the **Indicator Templates** page, choose a template.

2

Click  (Table row actions), **Edit**.

3

In the form that opens, update the parameters as needed and click **UPDATE**.


END OF STEPS

10.3.2 To delete an indicator template

1

On the **Indicator Templates** page, choose a template.

2

Click  (Table row actions), **Delete**.

END OF STEPS

11 Frequently asked questions

11.1 Insights Administrator FAQ

11.1.1 Do I need to create separate telemetry subscriptions or baselines for NEs managed by NFM-P and MDM?

No.

For an NE managed by NFM-P, the statistics you need must be collected by the NFM-P.

11.1.2 My Analytics reports don't look like I expect. How can I troubleshoot?

- Verify that subscriptions are in place for the telemetry types you need and that database storage is enabled where appropriate.
OAM subscriptions do not use database storage.
- Verify that an aggregation rule is present for each telemetry type you are reporting.
- Verify that the Report Time Zone for the Analytics browser matches the aggregation time zone. If the aggregation time zone has been changed, aggregated data from before the change reflects the old time zone.
- Check the aggregation rule to verify that the retention periods meet your requirements and that there has been a successful collection for the time period you need.

For example, if there has not yet been a successful daily aggregation, you can't run a daily report.

12 Insights Administrator use cases

12.1 Setting up statistics and aggregation for Port Throughput on the 7750 SR

This use case shows how to use Insights Administrator to set up the data collection and aggregation required to run a Port Throughput report in Analytics for 7750 SR NEs managed using MDM.

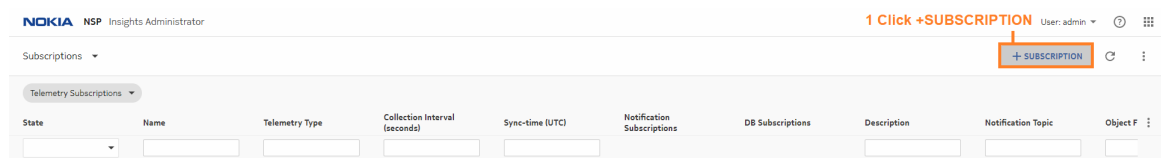
i **Note:** The images in this article show the NSP 20.6 release of the Insights Administrator.

The following prerequisites must be completed.

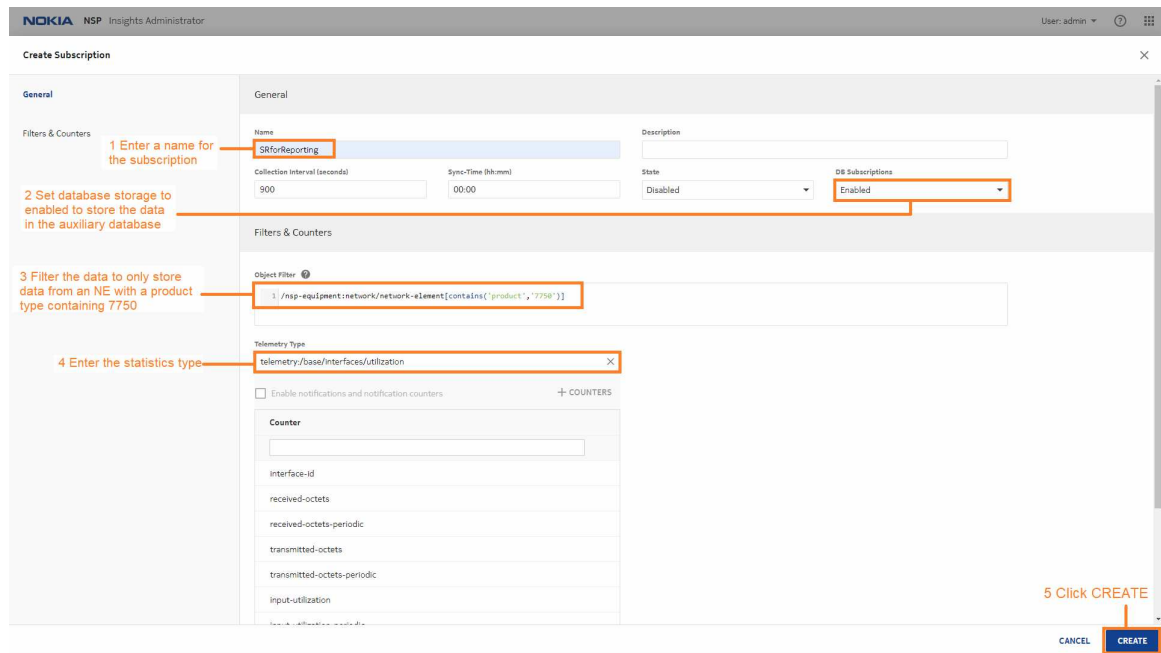
- At least one 7750 SR NE has been discovered in the network and is reachable.
- Aggregation rules have been deployed.

12.1.1 Let's go

From the Subscriptions view, we'll create a subscription.

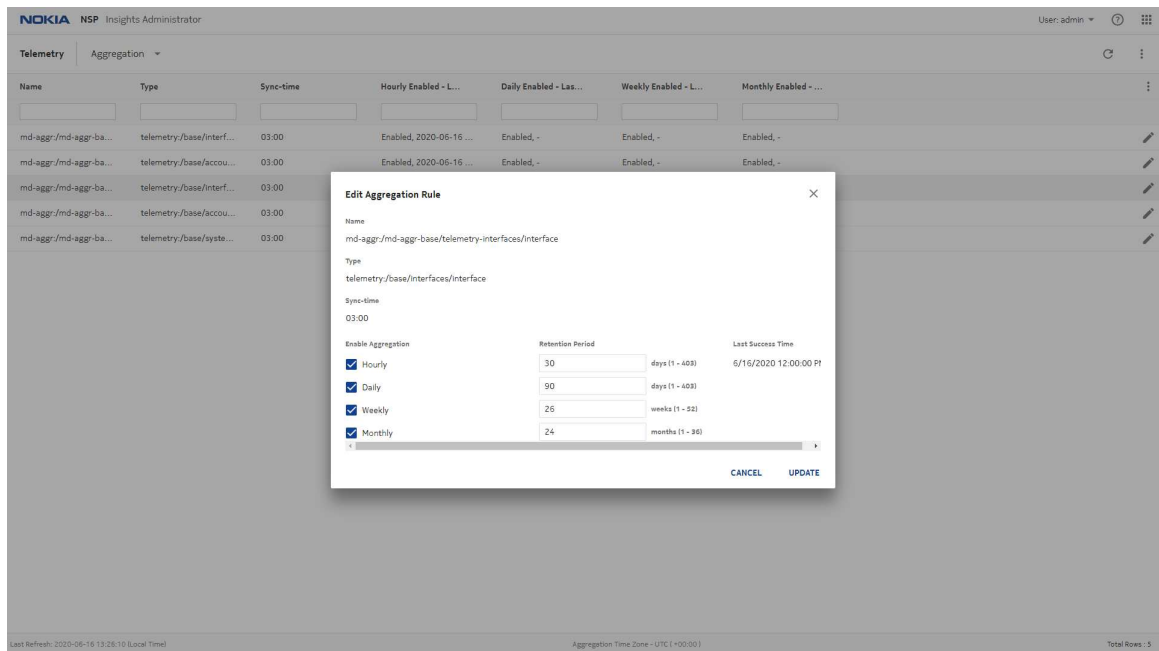


We need interface utilization statistics for 7750 SR NEs. An object filter that contains “7750” ensures that we receive data whether the NE type says “7750 SR” or “7750 SR-12”.

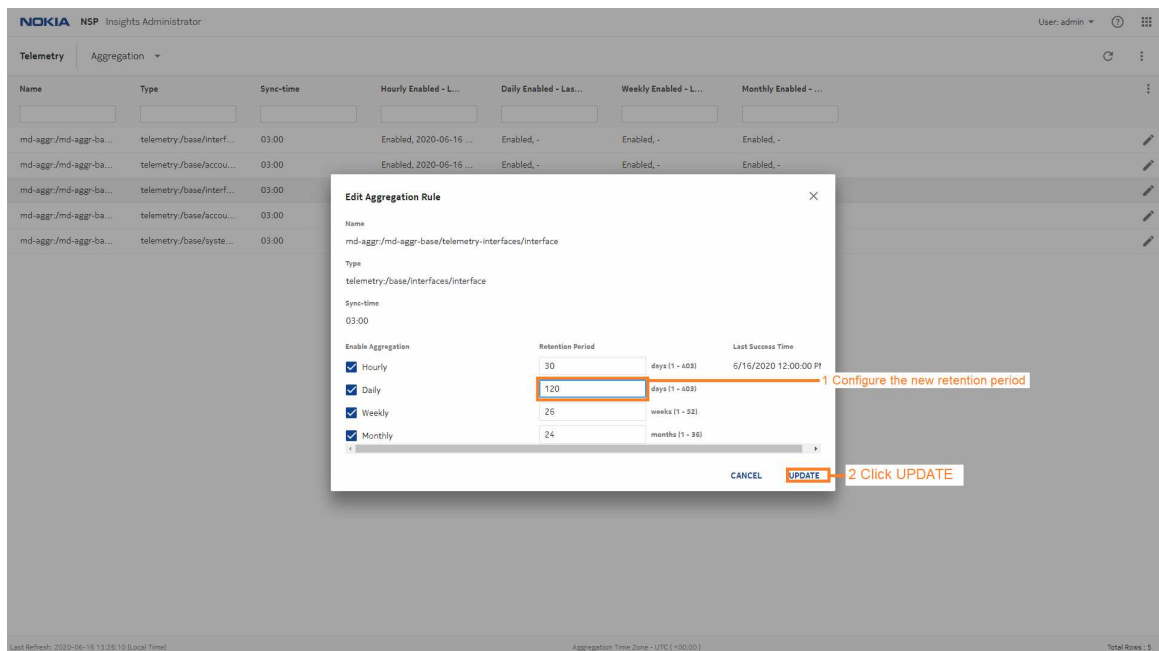


Let's look at the aggregation rule for interface data. From the Aggregation view, choose the aggregation rule and click **Edit Aggregation Rule** to see the details.

The **Retention Period** fields show how long aggregated data is stored in the auxiliary database. The default retention period for daily aggregation is 90 days. That means that daily granularity is available in Analytics for up to 90 days of data.



Changing the retention period to 120 days makes daily granularity available for a longer time. Change the retention time and click **UPDATE**.



12.1.2 We're done

We've set up a subscription for interface utilization data, and aggregation is deployed. When data has been successfully collected and aggregated, we'll be able to run a Port Throughput Summary (NSP) report in the Analytics application.

12.2 Creating an OAM test

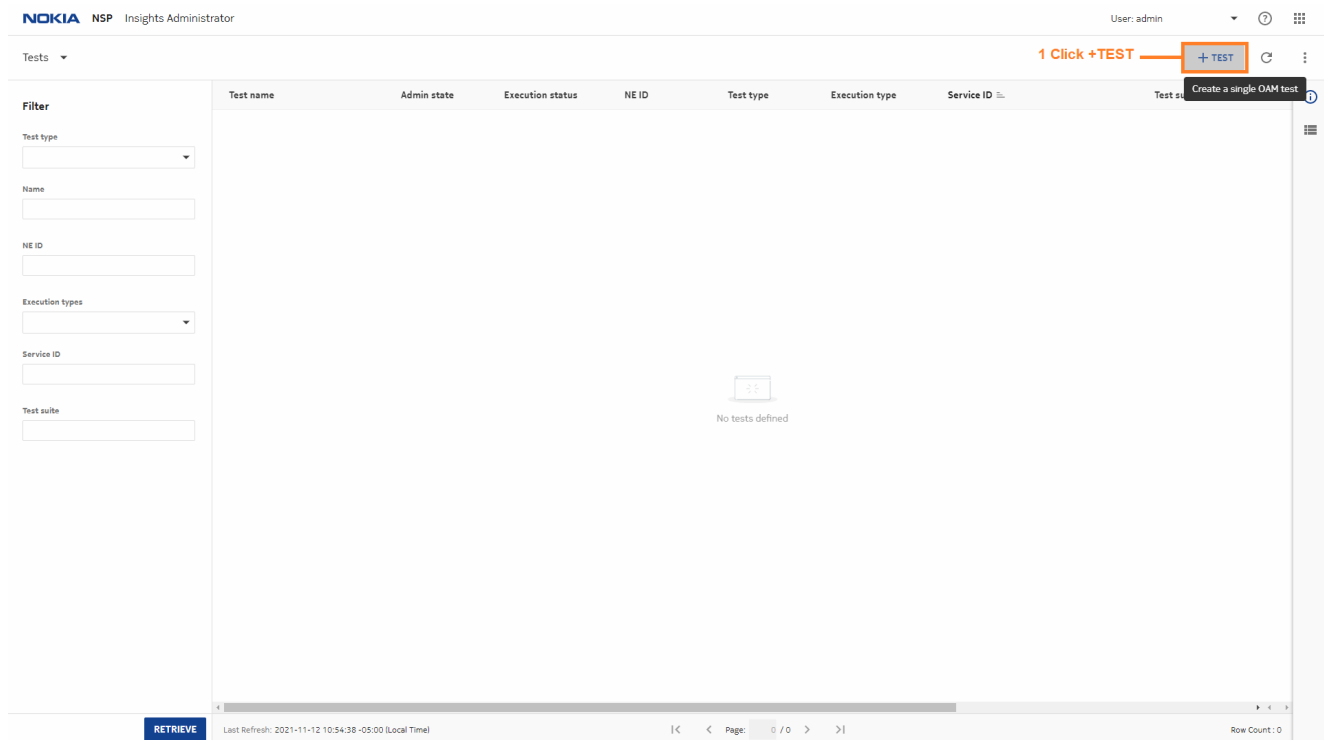
This use case shows how to use Insights Administrator to create and execute an OAM test.

The following prerequisites must be completed.

- The service we need to monitor has been configured.
- A test template for the test type and execute type is available.

12.2.1 Let's go

From the Tests view, we'll create a test.



In the Create Test form, choose a test type and entities to test.

When you choose a template, the template parameters appear. Configure the parameters and click **CREATE**.

NOKIA NSP Insights Administrator User: admin

Create OAM Test demo

Test type
CFM Loopback

Entity type
ELINE Endpoint

Source test entity
/nsp-service/services/service-laye

Destination test entity
/nsp-service/services/service-laye

Template
Quick Validate (on-demand)

Name*
demo

Test ID
0

The selected template does not have any configurable settings.

Advanced

CANCEL CREATE

1 Choose the test type, entity type, and entities to test

2 Choose a template. The template parameters appear.

3 Configure the parameters

4 Click CREATE

The test is added to the list of tests, in Stopped status.

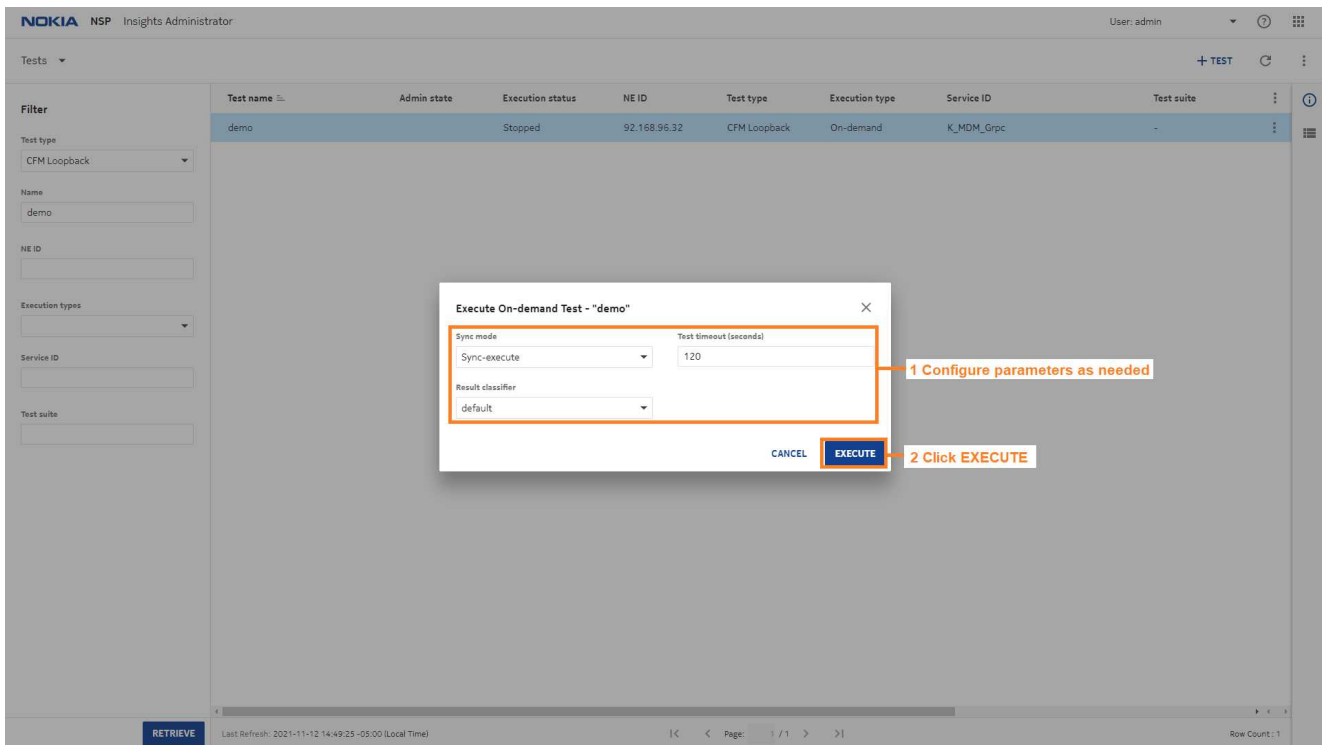
Enter details in the Filter panel to find the test.

The screenshot shows the 'Insights Administrator' interface for 'NSP'. The top navigation bar includes the Nokia logo, 'NSP Insights Administrator', and a user profile 'User: admin'. Below the navigation bar, there is a 'Tests' dropdown menu and a '+ TEST' button. The main content area is divided into a 'Filter' sidebar on the left and a table of test configurations. The table has columns for 'Test name', 'Admin state', 'Execution status', 'NE ID', 'Test type', 'Execution type', 'Service ID', and 'Test suite'. A single row is visible with the following values: 'demo', 'Admin state', 'Stopped', '92.168.96.32', 'CFM Loopback', 'On-demand', 'K_MDM_Grpc', and '-'. The 'Execution status' cell 'Stopped' is highlighted with an orange box. The 'Test type' dropdown in the filter sidebar is also highlighted with an orange box. At the bottom of the filter sidebar, there is a 'RETRIEVE' button highlighted with an orange box. Three orange annotations with arrows point to these elements: '1 Choose the test type and enter filter information' points to the 'Test type' dropdown; '2 Click RETRIEVE' points to the 'RETRIEVE' button; and '3 The test is displayed. Note the execution status.' points to the 'Stopped' status in the table. The footer of the interface shows 'Last Refresh: 2021-11-12 14:36:45 -05:00 (Local Time)', 'Page: 1 / 1', and 'Row Count: 1'.

Choose Execute from the Table row actions menu to run the test.


The screenshot shows the Nokia NSP Insights Administrator interface. At the top left, it says "NOKIA NSP Insights Administrator" and "User: admin" is shown at the top right. Below the header, there is a "Tests" section with a "+ TEST" button. On the left, there is a "Filter" panel with fields for "Test type" (set to "CFM Loopback"), "Name" (set to "demo"), "NE ID", "Execution types", "Service ID", and "Test suite". The main area is a table with columns: "Test name", "Admin state", "Execution status", "NE ID", "Test type", "Execution type", "Service ID", and "Test suite". A single row is visible with the following values: "demo", "Admin state", "Stopped", "92.168.96.32", "CFM Loopback", "On-demand", "K_MDM_Grpc", and "-". A context menu is open over this row, with options: "View Results", "Edit", "Execute..." (highlighted with an orange box), and "Delete". At the bottom of the interface, there is a "RETRIEVE" button, a refresh timestamp "Last Refresh: 2021-11-12 14:38:00 -05:00 (Local Time)", a page indicator "Page: 1 / 1", and a "Row Count: 1" label.

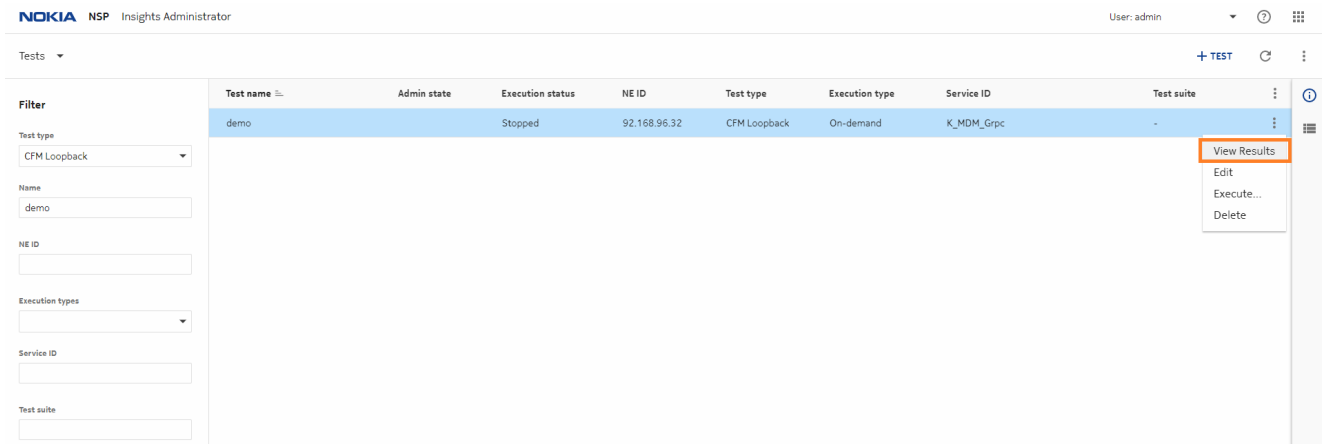
Configure the execution parameters and click **EXECUTE**.



12.2.2 We're done

After the test executes, choose **View Results** from the Table row actions menu to see results.

 **Note:** Wait at least 5 s for results to be available.



Execution ID	Result classification	Result status	Time captured	Probes sent	Probes received	Probes lost	Loss ratio
61	Success	success	2021-11-12 11:09:49 -05:00	5	5	0	0.00

12.3 Setting up baselines

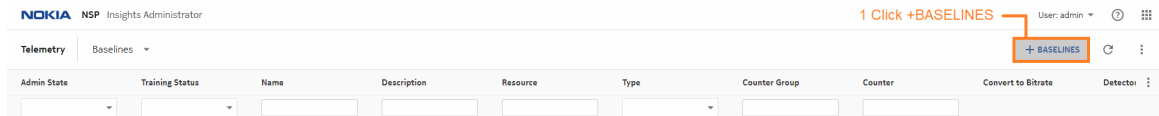
This use case shows how to use Insights Administrator to create baselines to monitor transmitted and received octets on a network port. These baselines can be used to detect anomalies and to create baseline and anomaly charts in Insights Viewer.

The following prerequisites must be completed.

- The NE we need to monitor has been discovered in the network and is reachable.
- If the NE we need to monitor is managed by NFM-P, statistics collection has been configured and started in the NFM-P.

12.3.1 Let's go

From the Baselines view, we'll create baselines.



Creating an object filter to specify the NE and port makes finding the resources easier.

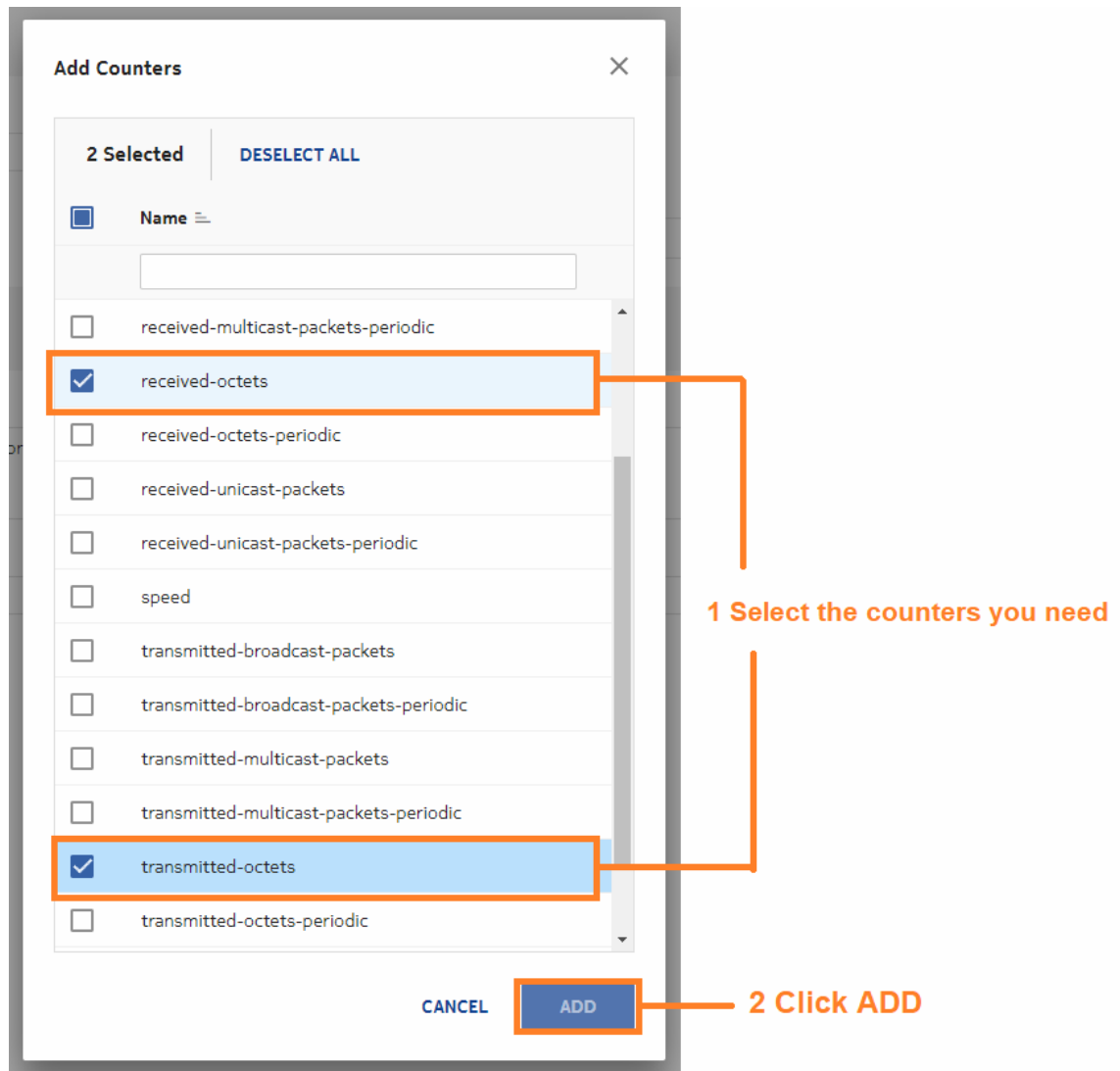
1 Configure the collection and learning parameters. These baselines will collect statistics every 30 seconds, calculate counters based on a 15 minute window, and learn trends based on one week of tracking.

2 Filter the data to collect statistics from a specific port

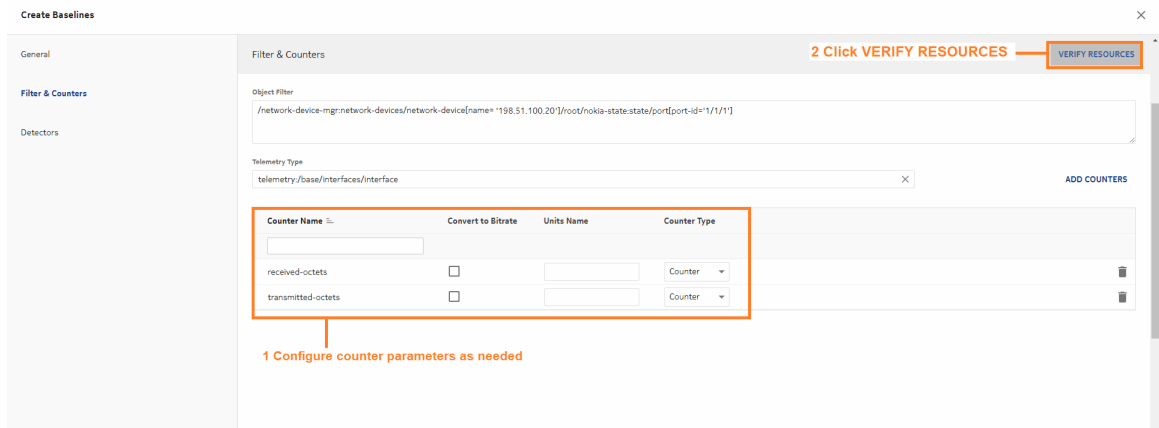
3 Enter the telemetry type

4 Click +COUNTERS

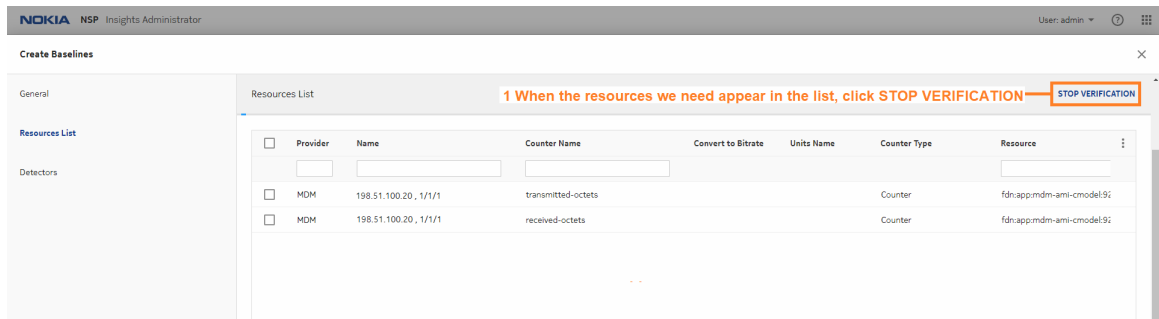
A form opens, showing the available counters. We'll choose transmitted and received octets. Select the counters and click **ADD**.



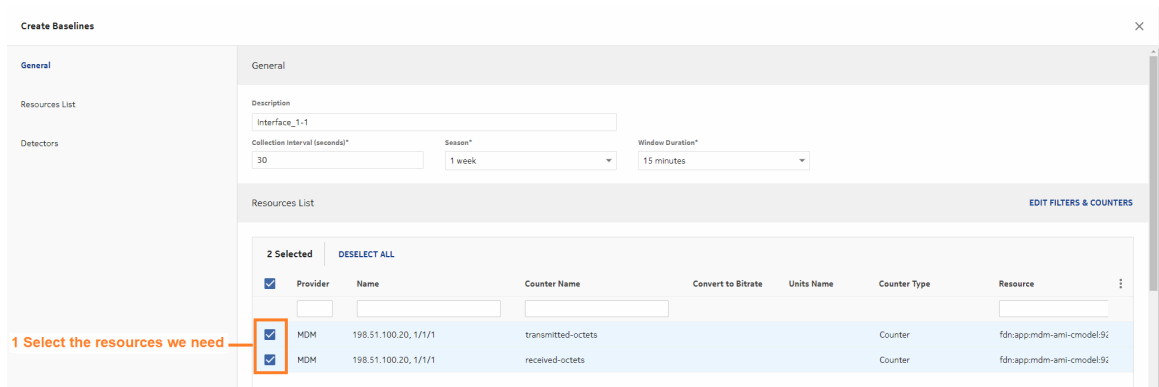
We can configure the counter type or conversion to bitrate if needed. We'll use the defaults for these baselines.



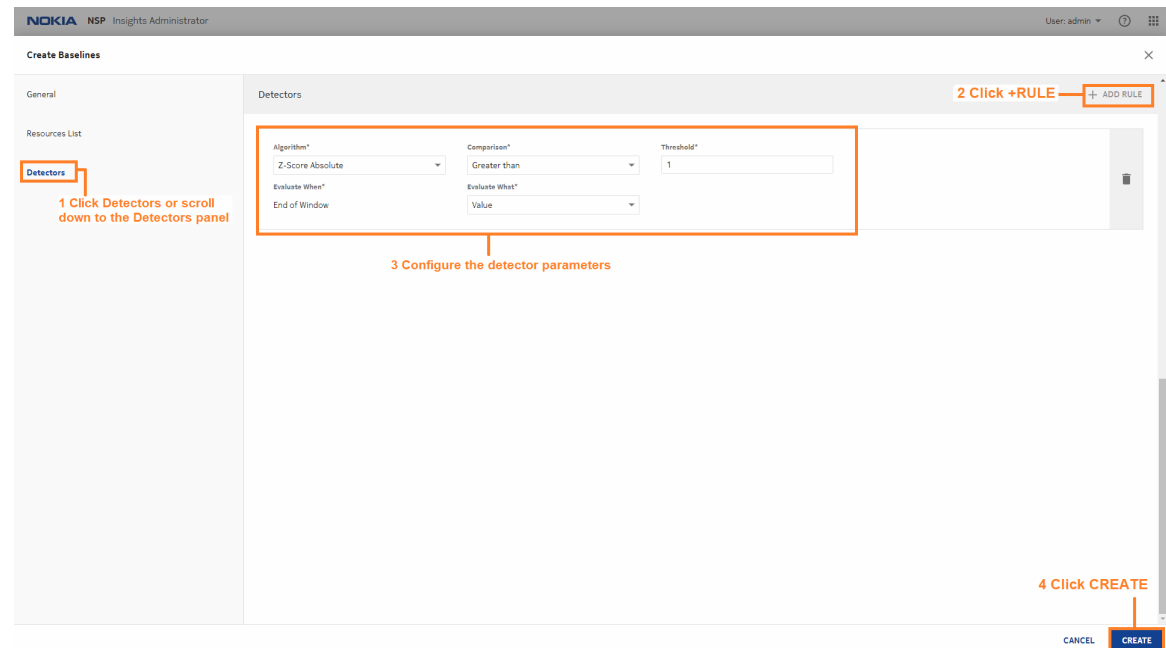
Insights Administrator checks for resources corresponding to the filters and counters specified. When the resources we need appear in the resources list, click **STOP VERIFICATION**. The verification does not stop on its own.



Select the resources in the resources list.



The final step is configuring anomaly detection. Then we can click **CREATE**.



12.3.2 We're done

Insights Administrator creates a baseline for each resource. When complete, they appear in the list in the Baselines page.

Admin State	Training Status	Name	Description	Resource	Type	Counter Group	Counter	Convert to Bitrate	Detector
Enabled	Active	198.51.100.20_1/1/1	Interface_1-1	fdn-app.mdm-ami-cm...	Counter	telemetry/base/interf...	received-octets		✓
Enabled	Active	198.51.100.20_1/1/1	Interface_1-1	fdn-app.mdm-ami-cm...	Counter	telemetry/base/interf...	transmitted-octets		✓

12.4 Creating a simple indicator

This use case shows how to use Insights Administrator to create an indicator with a single counter and no formula. This indicator outputs the input utilization of each port on NE 4.4.4.4.

The following prerequisites must be completed:

- The NE we need to monitor has been discovered in the network and is reachable.
- If the NE we need to monitor is managed by NFM-P, statistics collection has been configured and started in the NFM-P.

12.4.1 Let's go

From the Indicators view, we'll create an indicator.

Admin State	Name	Description	Telemetry Type	Counters	Units	Thresholds	Actions	Multiple Output	Collectic (second)

Enter a name for the indicator, and configure the collection interval and window duration.

General

Name* NE 4 input util Description Input Utilization Indicator

Collection Interval (seconds)* 900 Window Duration* 15 minutes

1 Configure the name and collection parameters. This indicator will collect statistics every 900 seconds (15 minutes). The window duration is ignored for simple indicators.

Configuration

Units

Counters & Formula

Telemetry Type* Type to find telemetry type... + COUNTERS

Selected Counter(s)* No Counters Added

Formula

Object Filter 1

Resource List

CANCEL CREATE

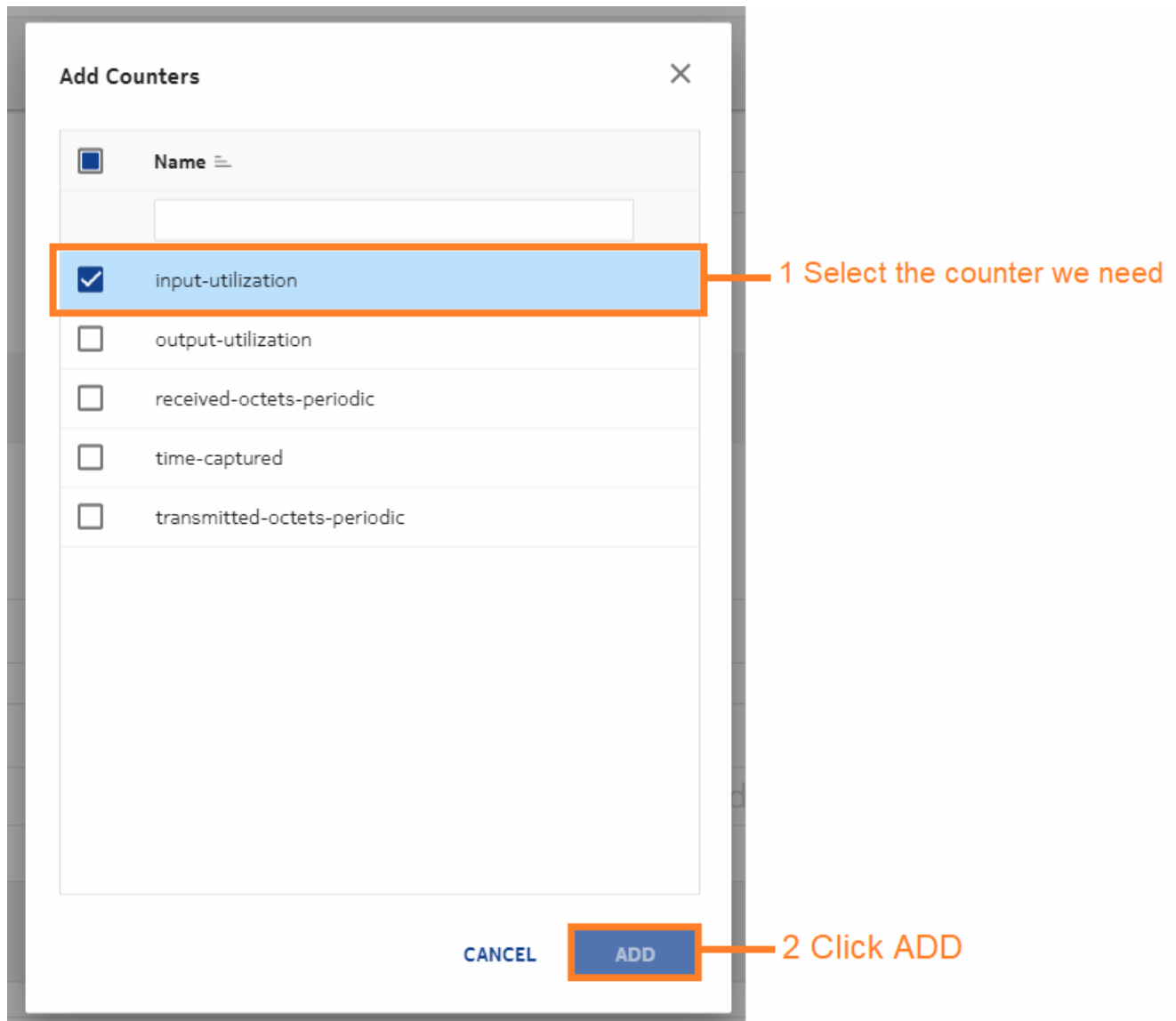
Configure the telemetry type.

1 Enter the units to display the values

2 Enter the telemetry type

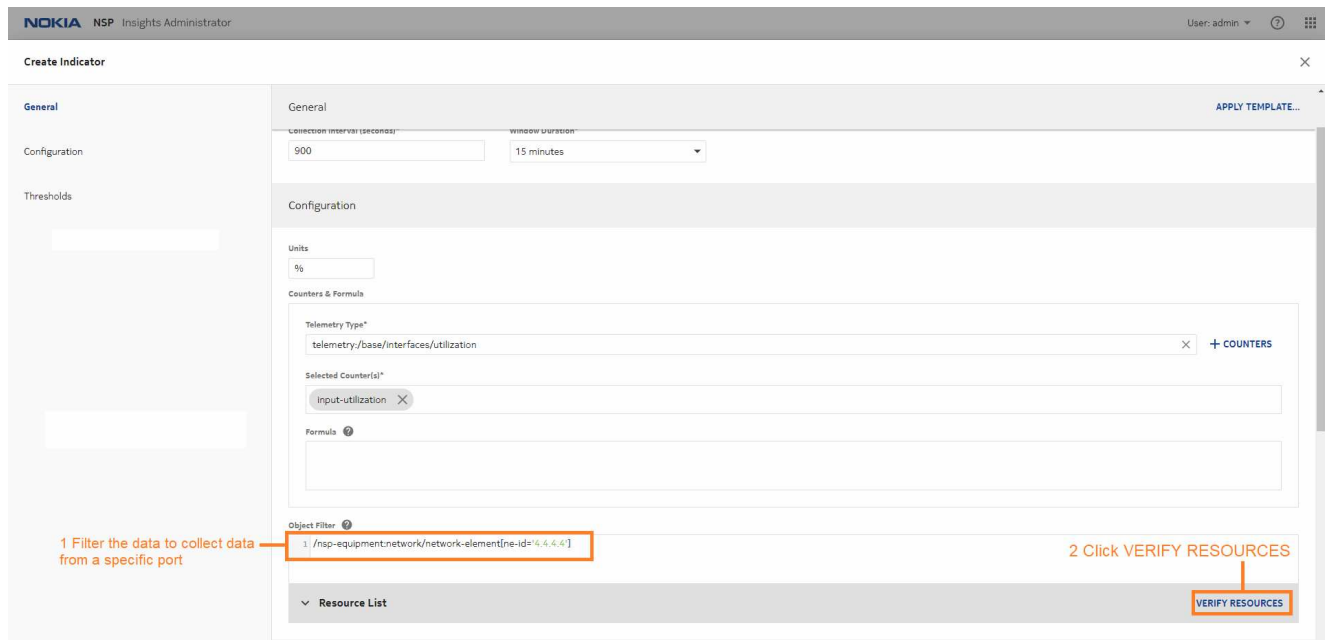
3 Click +COUNTERS

A form opens showing the available counters. We'll choose input utilization.



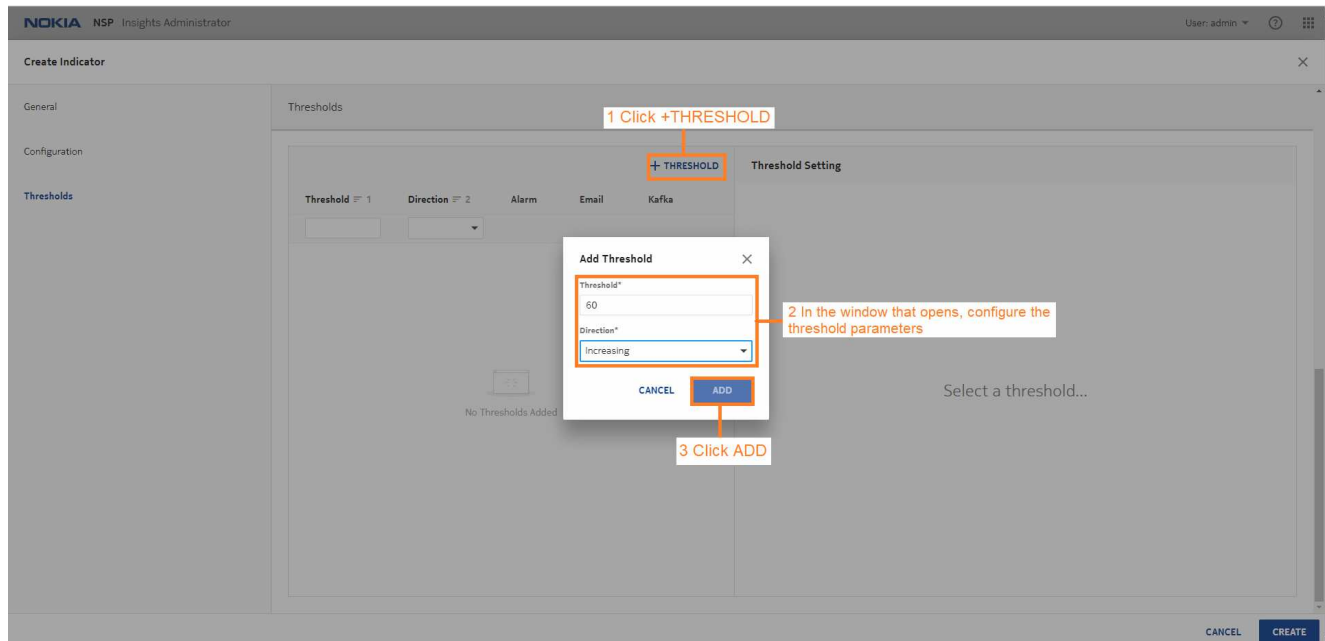
The screenshot shows a dialog box titled "Add Counters" with a close button (X) in the top right corner. Inside the dialog, there is a search bar with a "Name" label and a list of counter options. The "input-utilization" option is selected, indicated by a checked checkbox and a blue highlight. An orange arrow points to this option with the text "1 Select the counter we need". At the bottom of the dialog, there are two buttons: "CANCEL" and "ADD". The "ADD" button is highlighted with an orange box, and an orange arrow points to it with the text "2 Click ADD".

Configure an object filter to collect statistics from a specific port, and click **VERIFY RESOURCES** to make sure the filter is correct.

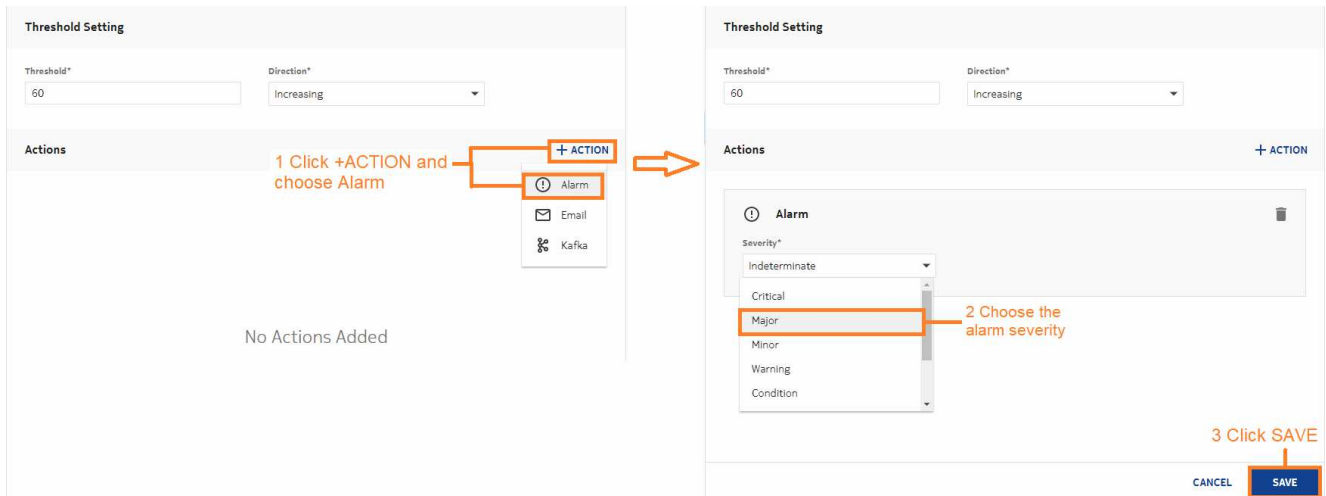


When the resources we need appear in the resources list, click **STOP VERIFICATION**. The verification does not stop on its own.

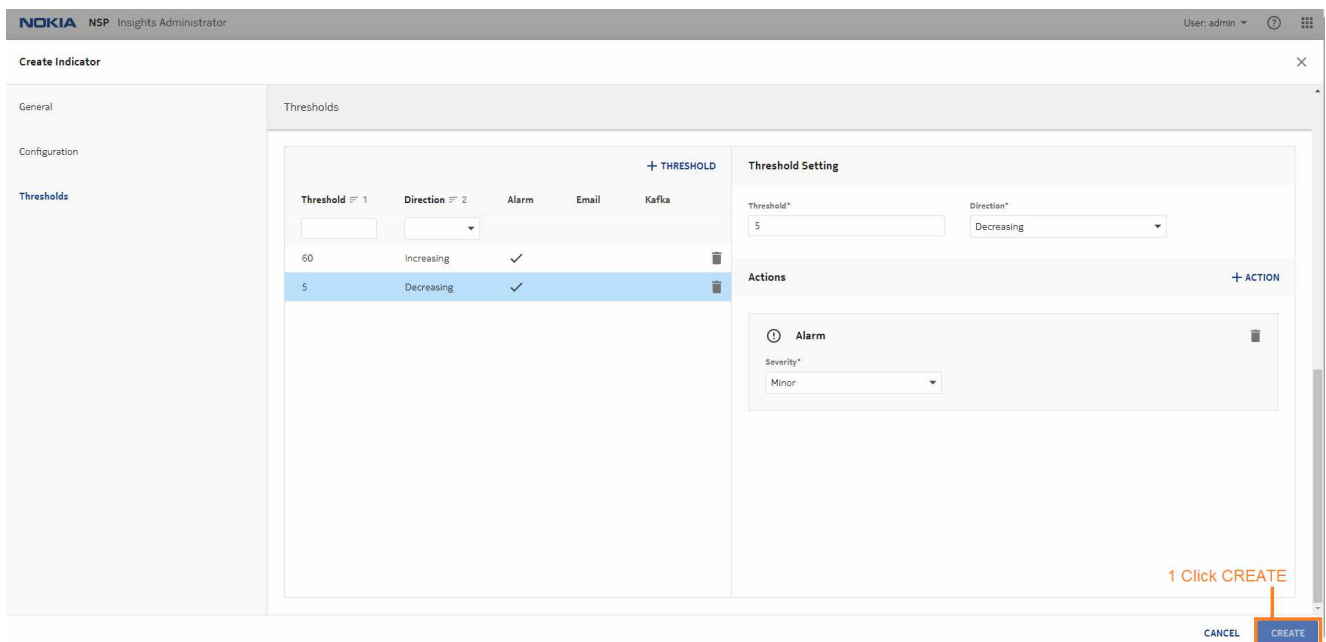
Create thresholds as needed. We'll create thresholds for utilization increasing past 60% and for decreasing below 5%.



Configure threshold actions. We'll configure a Threshold Crossing Alarm alarm to be generated for each threshold. The alarm for the increasing threshold has Major severity, and the alarm for the decreasing threshold has Minor severity.



When both thresholds are configured, we can click **CREATE** to create the indicator.



12.4.2 We're done

The indicator appears in the list in Insights Administrator.

Admin State	Name	Description	Telemetry Type	Counters	Units	Thresholds	Actions	Multiple Output	Collectic (seconds)
Enabled	NE 4 input util	Input Utilization Indica...	telemetry-/base/interf...	input-utilization	%	✓	✓	✓	900

12.5 Creating a complex indicator using a template

This article shows how to use Insights Administrator to create an indicator template with a formula and apply the template to an indicator.

12.5.1 Let's go

From the Indicator Templates view, we'll create a template.

Name	Description	Telemetry Type	Counters	Units	Thresholds	Actions
------	-------------	----------------	----------	-------	------------	---------

Configure the telemetry type and click **+ COUNTERS**.

NOKIA NSP Insights Administrator User: admin

Create Indicator Template

General

Name* Ring Utilization Description

Configuration

Units %

Telemetry Type* telemetry:/base/interfaces/utilization + COUNTERS

Selected Counter(s)* No Counters Added

Formula

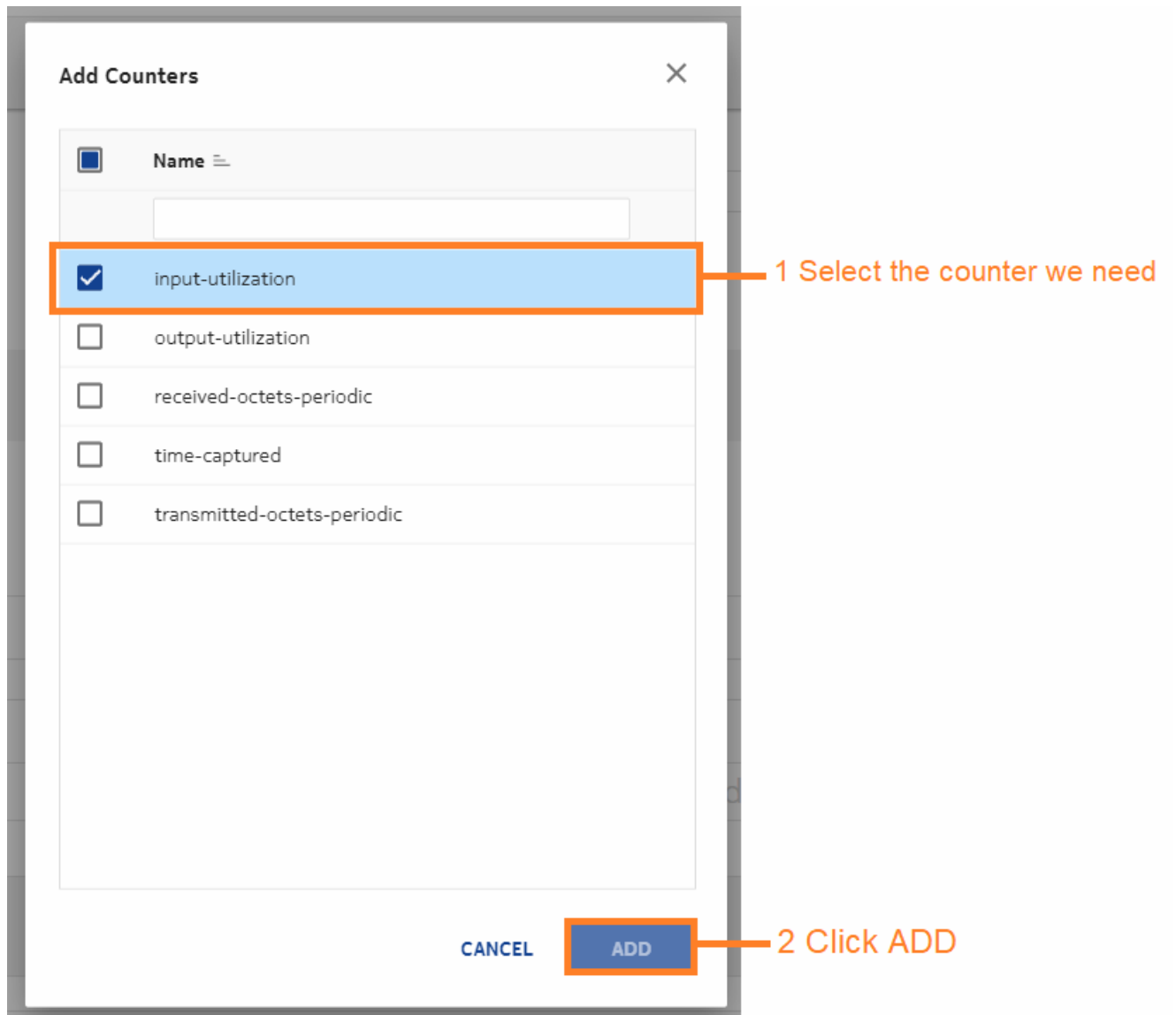
1 Configure a name for the template

2 Enter the units to display

3 Enter the telemetry type

4 Click +COUNTERS

A form opens showing the available counters. We'll choose input utilization.



Enter a formula for the indicator to use to calculate KPI values. Our formula calculates average input utilization.

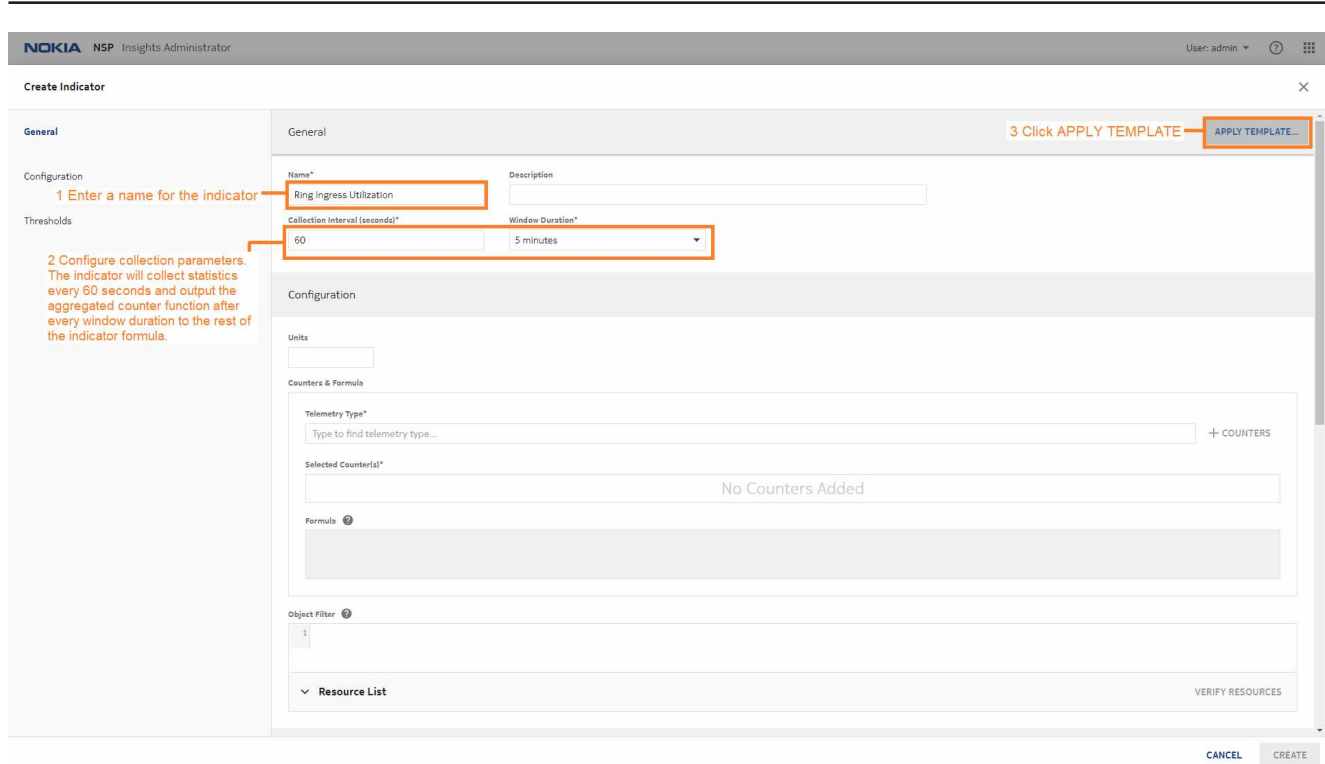
Click **CREATE** to create the template.

1 Enter a formula to calculate average input utilization

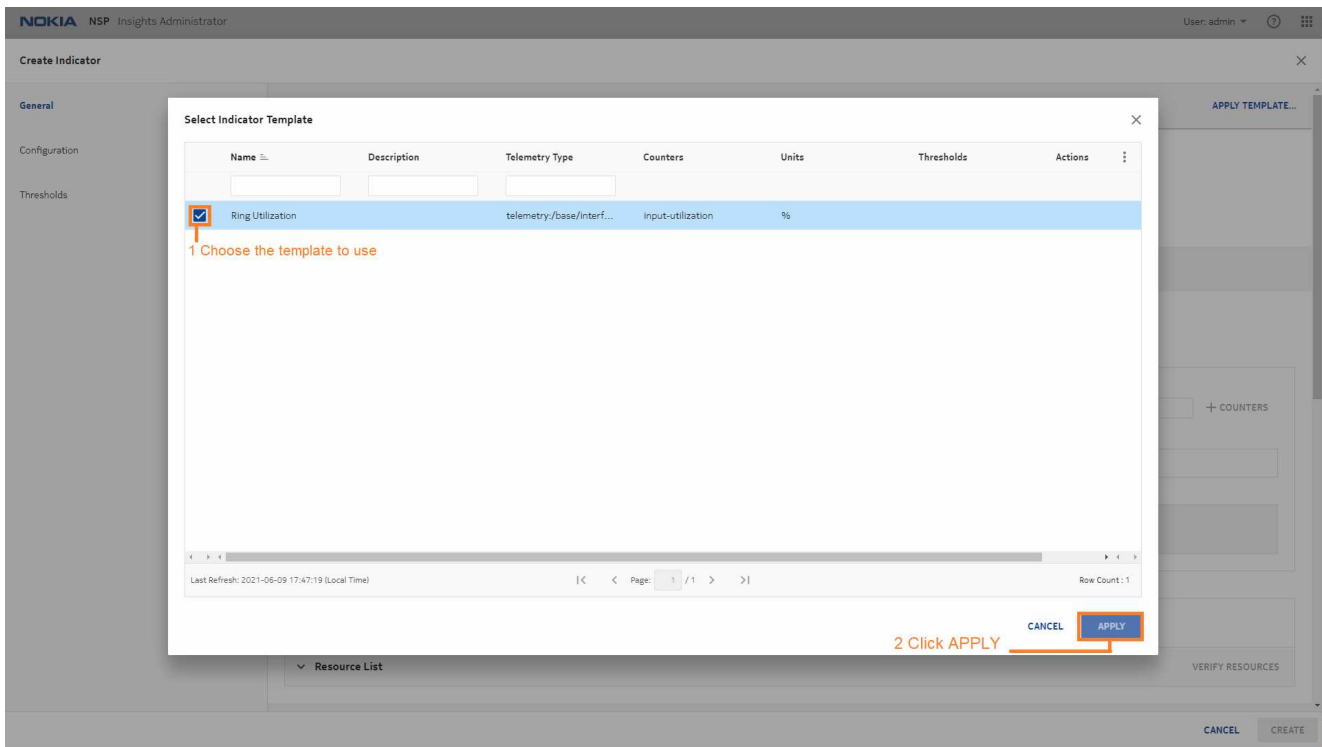
2 Click Create

Now we can create the indicator. From the Indicators view, click **+ INDICATOR**. Enter a name for the indicator and configure the collection settings.

Click **APPLY TEMPLATE**.

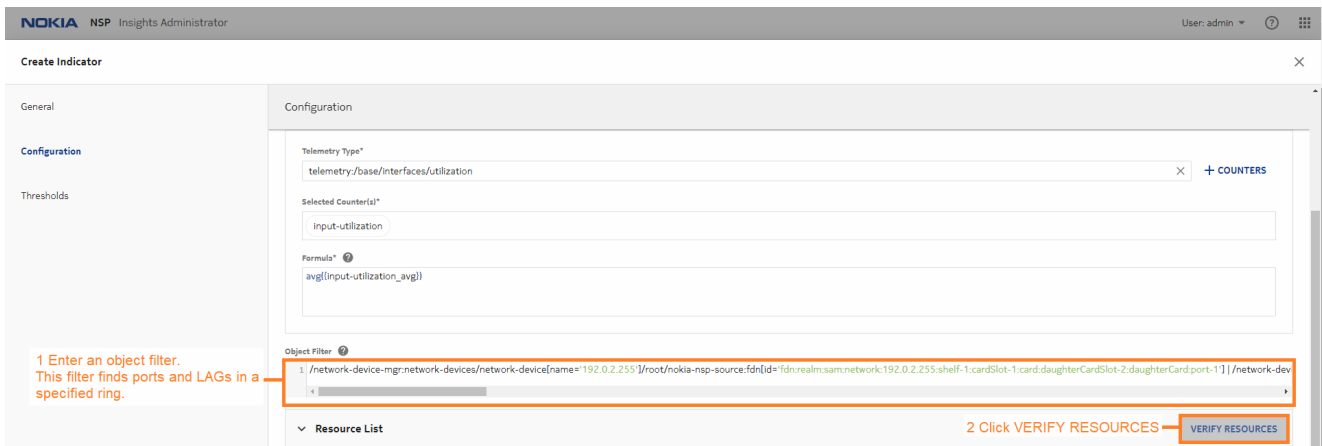


In the window that opens, choose the template and click **APPLY**.



The template has provided most of the parameters for the indicator, including defining how we want to calculate ring utilization. Next we can apply an object filter to define the resources to monitor.

Click **VERIFY RESOURCES** to show the resources found by the filter and ensure that they are returning values.



When the resources of interest appear in the resources list, click **STOP VERIFICATION**. The verification does not stop on its own.

1 Verify that the correct resources are found and that they are returning data

2 Click STOP VERIFICATION

Provider	Name	input-utilization	Resource
NFM-P	(198.51.100.0), Port 1/2/3	0	/network-device-mgr:network-devices/network-device[name='198.51.100.0']/root/nokia-nsp-source:fdn[id='fdn:realms...
NFM-P	(198.51.100.0), Port 1/2/7	0	/network-device-mgr:network-devices/network-device[name='198.51.100.0']/root/nokia-nsp-source:fdn[id='fdn:realms...
NFM-P	(198.51.100.0), Port 1/2/8	0	/network-device-mgr:network-devices/network-device[name='198.51.100.0']/root/nokia-nsp-source:fdn[id='fdn:realms...
NFM-P	(192.0.2.255), Port 1/2/1	0	/network-device-mgr:network-devices/network-device[name='192.0.2.255']/root/nokia-nsp-source:fdn[id='fdn:realms...
NFM-P	(192.0.2.255), Port 1/2/9	0	/network-device-mgr:network-devices/network-device[name='192.0.2.255']/root/nokia-nsp-source:fdn[id='fdn:realms...
NFM-P	(192.0.2.255), Port 1/2/13	0	/network-device-mgr:network-devices/network-device[name='192.0.2.255']/root/nokia-nsp-source:fdn[id='fdn:realms...

Add thresholds if needed and click **CREATE**. See 12.4 “Creating a simple indicator” (p. 80) for steps to create a threshold.

12.5.2 We’re done

The indicator appears in the list in Insights Administrator.

Admin State	Name	Description	Telemetry Type	Counters	Units	Thresholds	Actions	Multiple Output	Collect (seconds)
Enabled	Ring Ingress Util	avg input util on ingres...	telemetry:/base/interf...	input-utilization	%	✓	✓		60

