



ADMINISTRATOR GUIDE

NetFlow Traffic Analyzer

Version 2024.4

© 2024 SolarWinds Worldwide, LLC. All rights reserved.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of SolarWinds. All right, title, and interest in and to the software, services, and documentation are and shall remain the exclusive property of SolarWinds, its affiliates, and/or its respective licensors.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS, OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION NONINFRINGEMENT, ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION CONTAINED HEREIN. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY, EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The SolarWinds, SolarWinds & Design, Orion, and THWACK trademarks are the exclusive property of SolarWinds Worldwide, LLC or its affiliates, are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other SolarWinds trademarks, service marks, and logos may be common law marks or are registered or pending registration. All other trademarks mentioned herein are used for identification purposes only and are trademarks of (and may be registered trademarks) of their respective companies.

Table of Contents

NTA licensing	6
Get started with NTA	7
Local NetFlow Source	7
Set up flow monitoring	11
Difference between a polling engine and a collector in NTA	17
NTA flow requirements	18
Set up NBAR2 on Cisco devices	19
VMware support in NTA	23
Process flow data from Meraki devices in NTA	26
Configure NTA	28
NTA Settings	28
Top talker optimization in NTA	62
DNS and NetBIOS resolution in NTA	63
Database settings in NTA	66
Charting and graphing settings in NTA	69
Optimize performance in NTA	72
View NTA data in the SolarWinds Platform Web Console	75
Views	75
Widgets	75
Edit widgets in NTA	76
Charts in NTA	76
Enable the NetFlow Traffic Analyzer Summary view	84
Create custom views with the Flow Navigator	84
Add NetFlow widgets to web console views	88
Add endpoint-centric widgets to NTA views	89
Edit time settings for NTA views	89
Edit flow direction in NTA views	90
Delete an NTA filtered view	90
View Palo Alto Security Policies in the Top XX Conversations on Policy widget	91

Monitor traffic flow directions	93
View CBQoS data in NTA	94
Monitor NBAR2 Applications in NTA	97
Common tasks and user scenarios	98
CBQoS policies in NTA	98
Monitor autonomous systems through BGP in NTA	101
Use NTA to find the cause of high bandwidth utilization	107
Track traffic by site using NTA	108
Perform an immediate hostname lookup with NTA	109
NTA and the THWACK user community	109
User scenarios for NTA	110
Reports in NTA	113
NetFlow-specific predefined reports	113
Flows per Second statistics	116
Best practices for NTA reports	117
Execute a report in NTA	119
Create a report in NTA	119
Create a report using SWQL in NTA	120
Edit an NTA report	121
Create a custom report for IP address groups in NTA	125
Create a custom report for EF type of service in NTA	127
Customize a report to filter multicast data and group UDP data in NTA	129
Customize a historical NetFlow report to include location	131
Alerts in NTA	133
NetFlow-specific predefined alerts	133
Configure NTA-specific alerts	136
Configure Flow alerts	141
Troubleshoot with NTA	151
NetFlow issues	151
Chart issues	151
CBQoS issues	151
NetFlow Collector Services	151

Flow and CBQoS Sources	154
Troubleshoot Long Flow Errors in NTA	156
Events in NTA	156
Resolve unknown NetFlow traffic	189
Set up a NetFlow collection	191
NTA chart issues	191
CBQoS issues in NTA	194
Device configuration examples for NTA	195

NTA licensing

Licensing for NTA follows the license level of your NPM installation. For example, if you have an NPM license for SL250, your SolarWinds NTA license is also SL250. For more information on NPM licenses, see [NPM licensing model](#).

When upgrading licenses, the license levels **must** match. For example, when you upgrade an NPM SL250 license to SL500, you must upgrade your SolarWinds NTA license to SL500.

The following types of NTA licenses are available:

License	Number of monitored elements
SL100	Up to 100 nodes and 100 interfaces.
SL250	Up to 250 nodes and 250 interfaces.
SL500	Up to 500 nodes and 500 interfaces.
SL2000	Up to 2000 nodes and 2000 interfaces.
SLX	Virtually unlimited number of elements. With the default polling interval, one polling engine can monitor a maximum of 12,000 elements. To monitor over 12,000 elements, use additional polling engines (APEs) . Each APE requires a license.

- **Nodes:** any devices being monitored, such as routers, switches, virtual and physical servers, access points, and modems.
- **Interfaces:** any single points of network traffic, such as switch ports, physical interfaces, virtual interfaces, sub-interfaces, and VLANs.

For more information on checking your SolarWinds NTA licenses, see [How to check licenses in the SolarWinds Platform Web Console](#).

For more information on licensing, see [License SolarWinds Platform products in the SolarWinds Platform Web Console](#).

Get started with NTA

If you need to know how and by whom your bandwidth is being used, NTA provides a simple answer. You can quickly trace and monitor the bandwidth usage of a particular application or type of traffic. For example, if you see excessive bandwidth use on a particular interface, you can use NTA to see that the company meeting, consisting of streaming video, is consuming 80% of the available bandwidth through a particular switch. Unlike many other NetFlow analysis products, the network and flow data presented in NTA are not purely extrapolated data, but they are based on real information collected about the network by Network Performance Monitor, on which NTA depends.

Out of the box, NetFlow Traffic Analyzer offers broad monitoring and charting capabilities, coupled with detail-driven statistics, including the following:

- Distribution of bandwidth across traffic types
- Usage patterns over time
- External traffic identification and tracking
- Tight integration with detailed interface performance statistics





These monitoring capabilities, along with the customizable SolarWinds Platform Web Console and reporting engines, make NTA the easiest choice you will make involving your flow monitoring needs.

i NTA is optimized for understanding network usage, not auditing every packet. NTA provides an overall traffic summary and how users are using your bandwidth.


Local NetFlow Source

The Local NetFlow Source in SolarWinds NetFlow Traffic Analyzer (NTA) presents real flow data. It allows you to use all standard SolarWinds NTA features, such as navigation, drill-down, filters, reporting, and more, without any prior configuration and discovery.

The Local NetFlow Source presents live NetFlow traffic data sourced from, and destined to, the Main Polling Engine server, providing basic insight into traffic on the Main Polling Engine. All traffic for any network interface on the Main Polling Engine is captured and transformed into NetFlow flows.

NetFlow Sources		MANAGE SOURCES EDIT HELP		
1 INTERFACES				
ROUTER INTERFACE	TRAFFIC IN	TRAFFIC OUT	LAST RECEIVED NETFLOW	LAST RECEIVED CBQOS
   WIN-2019-08-08			4/2/19 3:28 PM	never
 Local Netflow Source	N/A	N/A	4/2/19 3:29 PM	never


When installing NTA, the Local NetFlow Source is enabled by default. If you are upgrading from a previous version of NTA, you have to [manually enable it](#).

- 
 • The Local NetFlow Source works **only** on the Main Polling Engine. After an upgrade, the Local NetFlow Source installs only when there is an existing node for the Main Polling Engine.
- When you install the latest version of NTA or upgrade to version 2020.2.6 and later, an interface is created for the Local NetFlow Source. This interface consumes an NPM license. Unmanaging the interface does not release the NPM license. You need to remove the Local NetFlow Source interface in order to release the NPM license. Removing the Local NetFlow Source interface is a permanent operation. If you wish to use the Local NetFlow Source again, contact [Technical Support](#).
- After an upgrade, if there is a free license, the local NetFlow Source will consume it immediately. Otherwise, it keeps checking for free licenses every one minute. When you release a license, the Local NetFlow Source will consume it.

Install the Local NetFlow Source

The Local NetFlow Source is automatically installed on the Main Polling Engine during the installation or upgrade of SolarWinds NTA. The process is different for installations and upgrades:

- During fresh installations of SolarWinds NTA, the Local NetFlow Source and the interface are automatically created and added to the Main Polling Engine nodes. The Local NetFlow Source is automatically enabled and starts capturing traffic on the Main Polling Engine.
- When upgrading SolarWinds NTA, the Local NetFlow Source and the SolarWinds Platform interface are automatically created and added to the Main Polling Engine nodes. The Local NetFlow Source and traffic capturing are disabled by default and you need to enable it in the [Flow Sources Management page](#).


 Both above scenarios create a new NetFlow Source and SolarWinds Platform Interface that consume the customer license. You can manually delete the interface if needed.


Manage the Local NetFlow Source

You can manage the Local NetFlow Source through the following standard operations within the SolarWinds Platform Web Console.

When installing NTA, the Local NetFlow Source is enabled by default. If you are upgrading from a previous version of NTA, you have to manually enable it.

Enable/disable the Local NetFlow Source

Follow the steps below to enable or disable the Local NetFlow Source.

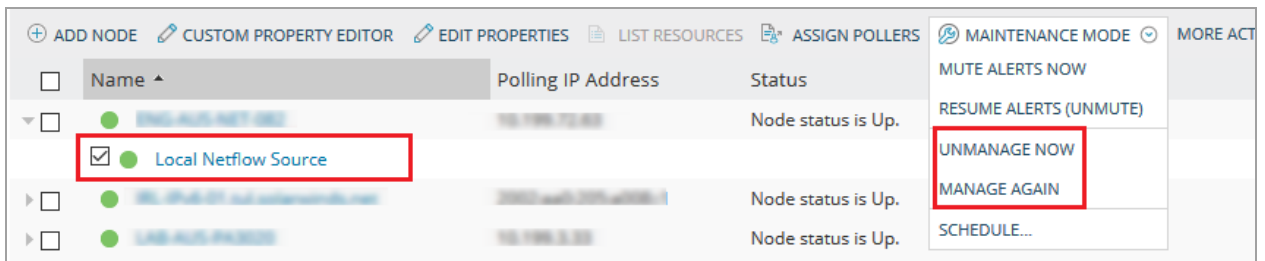
 Disabling the Local NetFlow Source stops local traffic collection, and historical flow data for the source are not visible in widgets.

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Click NTA Settings > Flow Sources Management.
3. To enable the Local NetFlow Source, select the check box in the NetFlow column.
4. Click Submit.

Manage the interface of the Local NetFlow Source

Follow the steps below to manage the Local NetFlow Source interface.

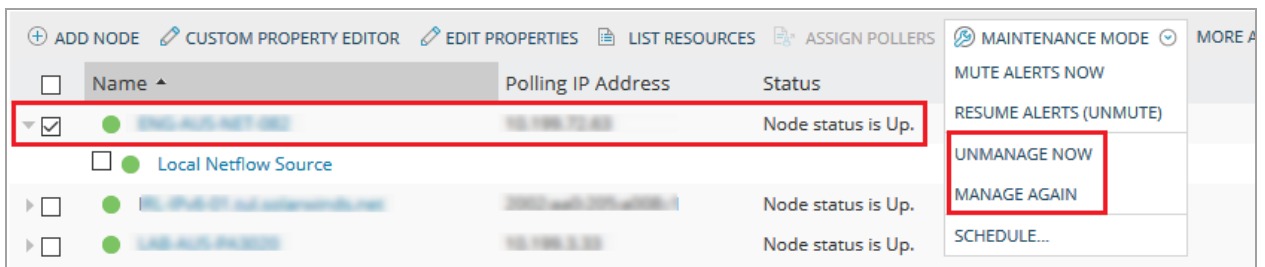
1. In the SolarWinds Platform Web Console, click Settings > Manage Nodes.
2. Select the Local NetFlow Source interface and click Maintenance mode.
3. Select one of the following options:
 - Unmanage Now to disable the node.
Disabling the Local NetFlow Source stops traffic collection, but historical flow data for the Source stay visible.
 - Manage Again to enable the node.



Manage the Main Polling Engine node with the Local NetFlow Source interface


Follow the steps below to enable or disable the Main Polling Engine node with the Local NetFlow Source interface.

1. In SolarWinds Platform Web Console, click Settings > Manage Nodes.
2. Select the Local NetFlow Source and click Maintenance mode.
3. Select one of the following options:
 - Unmanage Now to disable the node.
Disabling the Local NetFlow Source stops traffic collection, but historical flow data for the Source stay visible.
 - Manage Again to enable the node.



Delete the interface of the Local NetFlow Source


Follow the steps below to delete the Local NetFlow Source interface.

 This operation is permanent. You cannot recreate the local NetFlow Source.

1. In the SolarWinds Platform Web Console, click Settings > Manage Nodes.
2. Select the Local NetFlow Source interface, and click Delete in the top-right corner.
This action permanently removes the Local NetFlow Source. You will not see historical flow data for the Source.

Delete the Main Polling Engine node with the Local NetFlow Source interface

Follow the steps below to delete the node with the Local NetFlow Source interface on the Main Polling Engine.

 This operation is permanent. You cannot recreate the local NetFlow Source.

1. In the SolarWinds Platform Web Console, click Settings > Manage Nodes.

2. Select the Main Polling Engine node with the Local NetFlow Source interface, and click Delete in the top-right corner.
This action permanently removes the Local NetFlow Source. You will not see historical flow data for the Source.

Set up flow monitoring

To begin analyzing available flow data produced by devices in your network, install NTA, set up devices to export flow data, add your devices to NPM, and define what devices you want to monitor.

1. Set up your network devices to export flow data.
2. [Add your network devices to SolarWinds NPM.](#)
3. (Optional) Verify that your collector services are up and listening on the correct port.
4. Define what devices should be monitored by NTA.
5. (Optional) Verify that NTA is monitoring appropriate applications, services, ports, and protocols.
6. Wait a few minutes for NTA to collect flow or CBQoS data.

Collected data is displayed in [NTA widgets](#).

Set up network devices to export NetFlow data

You must configure your device to send flow data to SolarWinds NTA.

NTA collects NetFlow data, on port 2055 by default, only if a network device is specifically configured to send data to NTA. As a NetFlow collector, NTA can receive exported NetFlow version 5 data and NetFlow version 9 data that includes all fields of the NetFlow version 5 template. Once it collects NetFlow traffic data, NTA analyzes device bandwidth usage in terms of the source and destination endpoints of conversations reflected in the traffic.

Requirements

- Each device must be configured to export NetFlow data to NTA.
- Each device that exports NetFlow data to NTA must be monitored in NPM. Only nodes whose interfaces were discovered by NPM can be added as NetFlow sources.
- Traffic from a device that is not monitored in NPM appears only in aggregate as traffic from unmonitored devices. If the device is setup to export data to NTA, but is unmonitored in NPM, the collector may receive the data without being able to meaningfully analyze it.
- The specific interface through which a device exports NetFlow data must be monitored in NPM. The interface index number for this interface in the SolarWinds Platform database (interface table) must match the index number in the collected flow data.

Set up a device to export NetFlow data to NTA

1. Log in to the network device.
2. Enable NetFlow export on the device using appropriate commands. The following example enables NetFlow on a Cisco 6500 Series device:

```
ip flow-export source <netflow_export_interface><interface_num>
ip flow-export version 5
ip flow-export destination <Orion_Server_IP_address> 2055
ip flow-cache timeout active 1
ip flow-cache timeout inactive 15
snmp-server ifindex persist
```

- For detailed information on configuring NetFlow on Cisco devices, search for the appropriate configuration in the [Cisco NetFlow Configuration guide](#) (© 2021 Cisco, available at <https://www.cisco.com/>, obtained on May 6th, 2021).
 - For information on enabling NetFlow for Cisco Catalyst switches, see [Enable NetFlow and NetFlow data export on Cisco Catalyst switches](#).
 - For information on enabling NetFlow on Cisco ASA devices, see [Cisco ASA NetFlow overview](#).
 - Otherwise, consult these examples as apply to your device:
 - [Brocade \(Foundry\) sFlow configuration](#)
 - [HP sFlow configuration](#)
 - [Extreme sFlow configuration](#)
 - [Juniper sFlow configuration](#)
 - [Juniper J-Flow configuration](#)
 - The documentation of your network device
3. Add the device exporting NetFlow to NPM for monitoring.

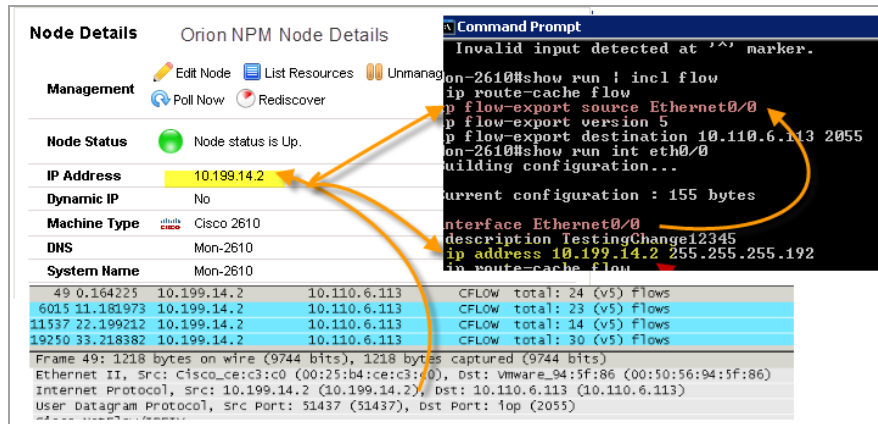
If you are adding a large number of NetFlow enabled nodes, use SolarWinds Platform Network Sonar. For more information, see [Discovering and Adding Network Devices](#).

If you are only adding a few nodes, it may be easier to use Web Node Management in the SolarWinds Platform Web Console. For more information, see [Adding Devices for Monitoring in the SolarWinds Platform Web Console](#).
 4. Verify that the device is exporting NetFlow data as expected and that the device is monitored in NPM.

To verify that data are exported correctly, use a packet capture tool, such as WireShark, to search for packets sent from the network device to the SolarWinds Platform server.

Example

If you successfully add a NetFlow enabled device with IP address 10.199.14.2 to NPM, and the device is actively exporting NetFlow data to the SolarWinds Platform server, you will see in WireShark a packet like the one (49) highlighted below in gray:



As expected, we see in the packet details that 10.199.14.2 is its source IP address and 10.110.6.113 is the destination, which is the SolarWinds Platform server. This correlates with the node details on the device in the SolarWinds Platform, as highlighted in yellow.

To verify that the IP address of the exporting interface on the network device is the one being monitored in SolarWinds Platform:

- a. Open a command line interface, log into the network device, and then type `show run` to see the running configuration of the device.
- b. Page down to the lines where the export source interface is defined. In this case, we see `ip flow-export source Ethernet0/0`.

To discover the IP address for this interface, type `show run int Ethernet0/0`. The IP address of the interface, 10.199.14.2, is being monitored by the SolarWinds Platform server.

5. Click My Dashboards > NetFlow > NTA Summary.

Under NetFlow Source, verify the NetFlow-enabled nodes listed with a recent time posted for collected flow.

Reasons not to export both ingress and egress NetFlow traffic data

Flows carrying NetFlow traffic data enter a device through an ingress interface and leave the device through an egress interface. For more information, see [Monitor Traffic Flow Directions](#).

If you export both ingress and egress data for all interfaces, you will get the same data twice: once as ingress data entering the device, and once as egress data as the flow leaves the device.

If you configure exporting ingress data on some interfaces and exporting egress data on other interfaces, the data shown by NTA may be inconsistent.

SolarWinds recommends that you configure exporting either ingress or egress data to prevent NTA from showing misleading traffic data.

Add flow-enabled devices and interfaces to the SolarWinds Platform database

NTA collects flow data from your network devices and analyzes network traffic based on collected data.

To collect flow data, you must specify the NTA server as a target to which each device exports data. For more information, see [Set up network devices to export NetFlow data](#).

Only nodes whose interfaces were discovered by NPM can be added as Flow sources.

To analyze flow data, you must add each flow-enabled network interface to the SolarWinds Platform database, so that they can be monitored in NPM.

To initiate flow monitoring, flow-enabled devices in the SolarWinds Platform database must be designated as flow sources. For more information, see [Add flow sources and CBQoS-enabled devices](#).

i Adding flow-enabled devices and interfaces to NPM and designating the same devices and interfaces as flow sources in NTA are separate actions. The designation of flow sources does not affect licensing requirements for either NPM or NTA.

1. Add the appropriate nodes to NPM.

- If you are adding a large number of nodes, use Network Sonar Discovery.

Click Settings > Network Discovery.

Confirm that you add all flow-enabled interfaces on added devices.

For more information, see [Discovering and adding network devices](#).

- If you are only adding a few nodes, it may be easier to use Web Node Management in the SolarWinds Platform Web Console.

Click Settings > Manage Nodes > Add Node.

For more information, see [Adding Devices for Monitoring in the SolarWinds Platform Web Console](#).

2. Click My Dashboards > Home > Summary.
3. Under All Nodes, verify that the devices were added.
4. Click My Dashboards > NetFlow > Flow Sources.
5. To finish setting up NetFlow monitoring, enable NetFlow monitoring for the selected nodes. For more information, see [Add Flow Sources and CBQoS-enabled Devices](#).

If you have already configured device interfaces to send flow data, NTA can detect and analyze flow data after the device is added.

What happens after you add devices and interfaces to the SolarWinds Platform database?

- After installing NTA, the NPM polling engine establishes a baseline by collecting network status and statistics.
- Thirty seconds later, the NPM polling engine performs another collection. You may notice an increase in the CPU usage during this time.
- After these initial collections, NPM collects network information every ten minutes for nodes and every nine minutes for interfaces. Flow analysis data displays in the SolarWinds Platform Web Console in minutes.

Before leaving NTA to gather data, ensure you are collecting flow data for the correct interface ports and applications. For more information, see [Applications and service ports in NTA](#).

Add flow sources and CBQoS-enabled devices

You can either add flow-enabled devices managed by NPM for monitoring to NTA manually, or you can configure that flow-enabled devices are added automatically.

For more information about the automatic addition of flow sources, see [Enable the Automatic Addition of Flow Sources](#).

Notes on adding sources and devices

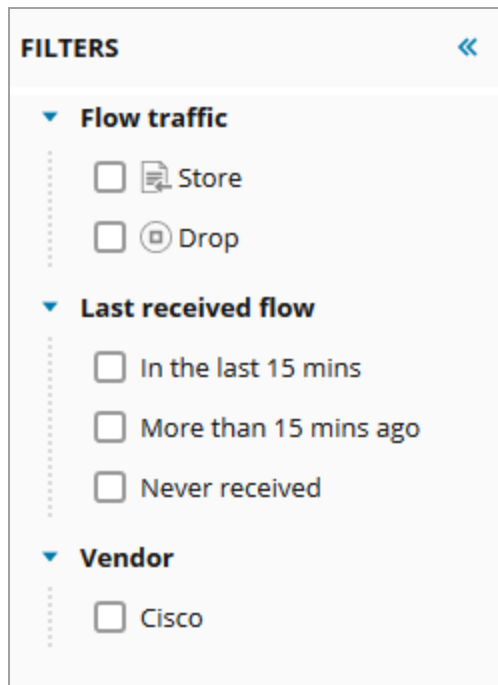
- Make sure the devices you want to monitor with NTA are already monitored in NPM.
- If you are using NetFlow version 9, confirm that the template you are using includes all fields included in NetFlow version 5 PDUs.
- Some devices have a default template timeout rate of 30 minutes. If NetFlow v9 flows arrive without a usable template, NTA raises an event every 15 minutes. Configure your device to export the appropriate template every one minute, so that the version 9 flows show up in NTA without delay.
- For more information about flow requirements, see [NTA flow requirements](#).

Add flow sources for monitoring

If automatic addition of NetFlow sources is enabled, all flow sources currently monitored by NPM will display in the Flow and CBQoS Sources widget. For more information about the automatic addition of flow sources, see [Enable the automatic addition of flow sources](#).

i The settings are available for anyone with user limitation applied, but only users with Manage nodes privileges can change the settings.

1. Click My Dashboards > NetFlow > Flow Sources.
2. Select the appropriate filters in the Filters list to display devices where you want to monitor NetFlow data.

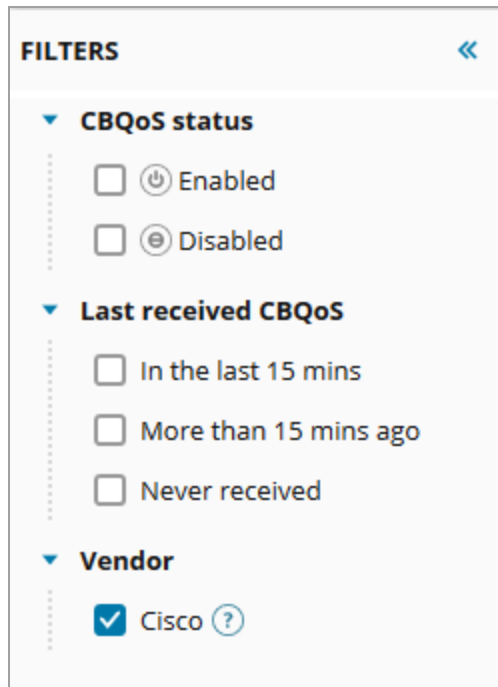


3. Select a device or interface, and then click Store traffic to enable receiving of flow data.

The sampling rate can be changed only per node. For more information about setting sampling, see [Set the sampling rate manually](#).

Add CBQoS-enabled devices for monitoring

1. Click My Dashboards > NetFlow > CBQoS Polling.
2. Select the appropriate filters in the Filters list to display devices where you want to monitor CBQoS data.



CBQoS monitoring is only available for Cisco devices. The Vendor filter is selected by default.

3. Select a device or interface, and click Enable to monitor CBQoS traffic.

Difference between a polling engine and a collector in NTA


To understand the way SolarWinds NTA processes flow data, you first need to understand the methods of capturing these data.

What is a flow collector?

Devices with flow enabled generate and export flow records. These records are collected using the flow collector. The flow collector then processes and analyzes the data. Flow collectors can be either hardware based, such as probes, or software based, such as the SolarWinds NTA collector. After processing and analyzing data, the NTA collector presents these data in the web-based user interface of the SolarWinds Platform Web Console.

What is a polling engine?

A polling engine is also used for monitoring and collecting data. While a collector gathers data that are being sent to it by the particular device, a polling engine pings the device and requests the data to be sent.

 NTA is a collector, not a polling engine. You must set up your devices, such as routers or firewalls, to send flow data to the collector.

NTA flow requirements

NTA supports these flow protocols:

Flow	Supported Versions	Sampled Flow Support
NetFlow	v1, v5, and v9 NetFlow v9 must have an appropriate template with all required fields.	v5 and v9 Some devices using IOS versions export flows without specifying that it is being sampled. NTA processes these flows as unsampled.
sFlow	v2, v4, and v5	Supported
J-Flow	Supported	Supported Some devices using JunOS versions export flows without specifying that it is being sampled. NTA processes these flows as unsampled.
IPFIX	Supports IPFIX generated by ESX 5.1 and later, for IPv4 traffic. Supports IPFIX generated by VMware vSwitch.	Supported
NetStream	v5 and v9	Supported
NetFlow Lite	Supported on the following devices: <ul style="list-style-type: none"> • Cisco Catalyst 2960-X • Cisco Catalyst 2960-XR • Cisco Catalyst 3560-CX • Cisco Catalyst 2960-CX 	Supported

Flow	Supported Versions	Sampled Flow Support
Cisco Wireless Controller NetFlow	Supported on the following devices with the <code>ipv4_client_app_flow_record</code> template: <ul style="list-style-type: none"> • Cisco 2504 WLC • Cisco 3504 WLC • Cisco 5508 WLC • Cisco 5520 WLC • Cisco Flex 7510 WLC • Cisco 8510 WLC • Cisco 8540 WLC • Cisco WiSM2 	Not supported

Set up NBAR2 on Cisco devices

Network Based Application Recognition (NBAR) is the mechanism used by certain Cisco routers and switches to recognize a dataflow by inspecting some of the packets sent. NTA 2024.4 supports unknown traffic detection and advanced application recognition through NBAR2.

First, configure your Cisco devices to send NBAR2 data to NTA. Second, add those devices as nodes in NPM and NTA.

The following values are examples used in the commands below:

- NTAreC
- NTAexp
- NTAmom
- GigabitEthernet0/1
- 10.10.10.10

Create a new Flexible NetFlow configuration

Add the flow record

This process is similar to creating a standard NetFlow configuration. In this case, you add the `collect application name` command to enable the sending of AppID in each flow.

```
flow record NTAreC
  match ipv4 tos
```

```

match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match interface input
collect interface output
collect counter bytes
collect counter packets
collect application name
exit

```

Add the flow exporter

The option `application-table` command enables the sending of a list of applications that can be classified using NBAR2, including applications that were manually created. The option `application-attributes` command enables the sending of categories for all applications.

```

flow exporter NTAexp
  destination 10.10.10.10
  source GigabitEthernet0/1
  transport udp 2055
  export-protocol netflow-v9
  template data timeout 60
  option application-table timeout 60
  option application-attributes timeout 300
exit

```


Add the flow monitor

The flow monitor connects the flow recorder and the flow exporter. You can configure multiple recorders, exporters, and monitors at once.

```

flow monitor NTAMon
  description NetFlow nbar
  record NTArec
  exporter NTAexp
  cache timeout inactive 30
  cache timeout active 60
exit

```

 When receiving long flows, these values may need to be adjusted, see [Troubleshoot Long Flow Errors in NTA](#) for more details. For more information about the timeout values, refer to the Cisco NetFlow Command Reference.

Apply the monitor to an interface

Assign the Flexible NetFlow configuration to the interface from which to monitor NetFlow.

```
interface GigabitEthernet0/1
    ip flow monitor NTAMon input
    ip flow monitor NTAMon output
exit
```

Diagnostic commands

```
show flow record "recordName"
show flow export "exporterName"
show flow monitor "monitorName"
show flow exporter statistics
show flow interface
```

Determine the applications your device can recognize

The Protocol Pack is a list of applications, definitions, and categories that your device can recognize.

Check the Protocol Pack version


```
show ip nbar version
```

View a list of the available applications

```
show ip nbar protocol-id
```

Edit an existing record

If you edit an existing record that is in use, you receive the following error:

 % Flow Record: Flow Record is in use. Remove from all clients before editing.

To resolve this error, remove the connection between the monitor, record, and interface.

Disable the connection

```
interface GigabitEthernet0/1
    no ip flow monitor NTAMon input
    no ip flow monitor NTAMon output
exit
```

Add the application recognition field into the record

```
flow record NTArec
    collect application name
exit
```

Add the application recognition field into the exporter

```
flow exporter NTAexp
    option application-table timeout 60
    option application-attributes timeout 300
```

Restore the connection

```
interface GigabitEthernet0/1
    ip flow monitor NTAMon input
    ip flow monitor NTAMon output
exit
```

NBAR2 Applications

NTA monitors Network Based Application Recognition (NBAR2) traffic. NBAR2 is an application classification system that is used with deep packet inspection technologies to provide better visibility into network traffic.

After you have enabled your devices to export NBAR2 flow records, you can view the Top NBAR2 Applications in summary views and reports.

When the netflow data is captured by NTA, the NBAR2 application classification may be unavailable or unknown to NTA. In this case, you may see one of the following identifiers for applications that are unidentified.

- **Unknown** – a Cisco application for which there is no classification available from Cisco.
- **Unclassified**– an application that is not supported or recognized by the NBAR engine on Wireless LAN Controller traffic and is captured as unclassified.
- **Unrecognized** – an application that NTA is not able to identify based on information in the current NBAR2 database. This will mostly likely happen when NBAR2 is first enabled on a device and it begins sending flows before sending the applications database. This occurrence depends on the interval set in the device settings.
- **Remaining traffic** – this is a standard label used on NTA charts to represent monitored traffic that is not applicable to any category presented on the chart.

You can monitor NBAR2 applications by switching the view type in the top-right corner of the [Top XX Applications](#) widget or from the NetFlow Applications Summary view. For more information about monitoring applications, see [Monitor NBAR2 Applications in NTA](#).

NBAR2 requirements for application ID

To monitor NBAR2 applications, the following field must be included in the option template for NBAR2 flows.

Field Type	Field Type Number	Description
Application ID	95	ID of application detected in NBAR2 flow

You also need to set the [Required fields](#) in the template for flow collection.

VMware support in NTA

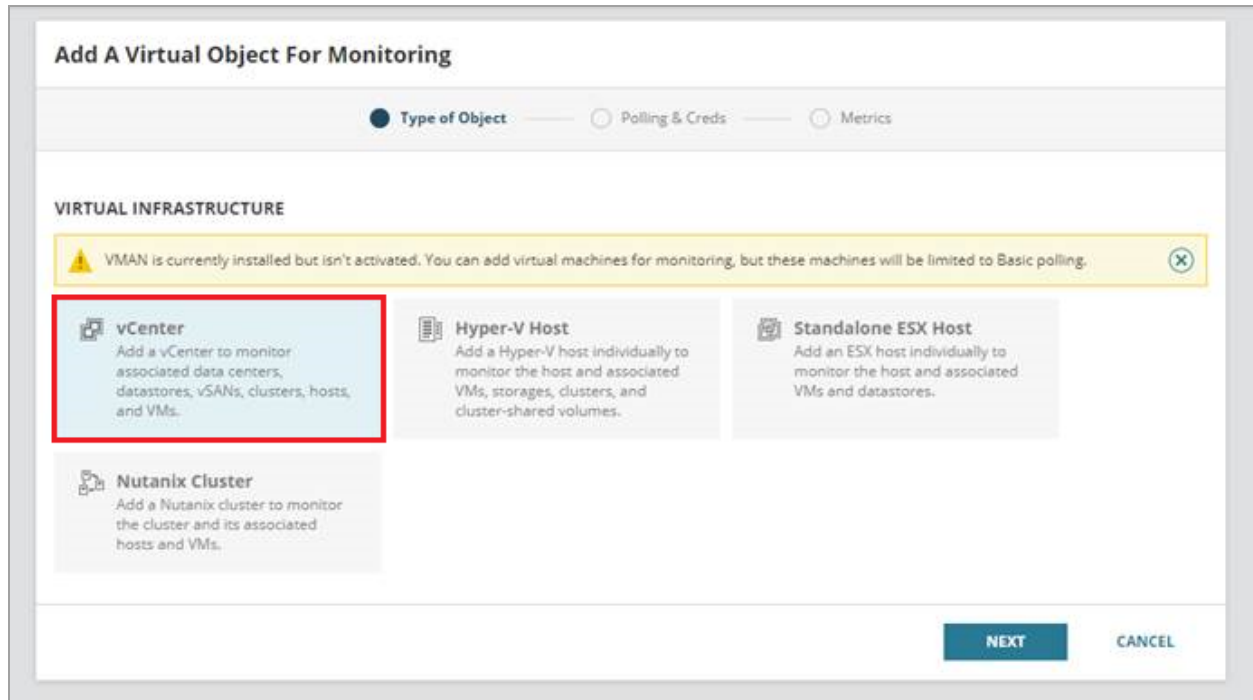
With NTA, you can view flow data from a VMware infrastructure.

Before you begin

- You must add vCenter to the SolarWinds Platform, choosing VMware/vCenter as the polling method.
- Make sure vCenter is added to the SolarWinds Platform in advance. After approximately 10 minutes, you can enable IPFIX export from the vCenter. This time is needed to correctly poll the data and identify hosts. If NTA receives any data beforehand, the data might be incorrectly handled and NTA will fire events about unknown traffic.
- SolarWinds recommends enabling the Automatic Addition of Flow Sources. All incoming flows will be automatically assigned and stored.

Discover a vCenter

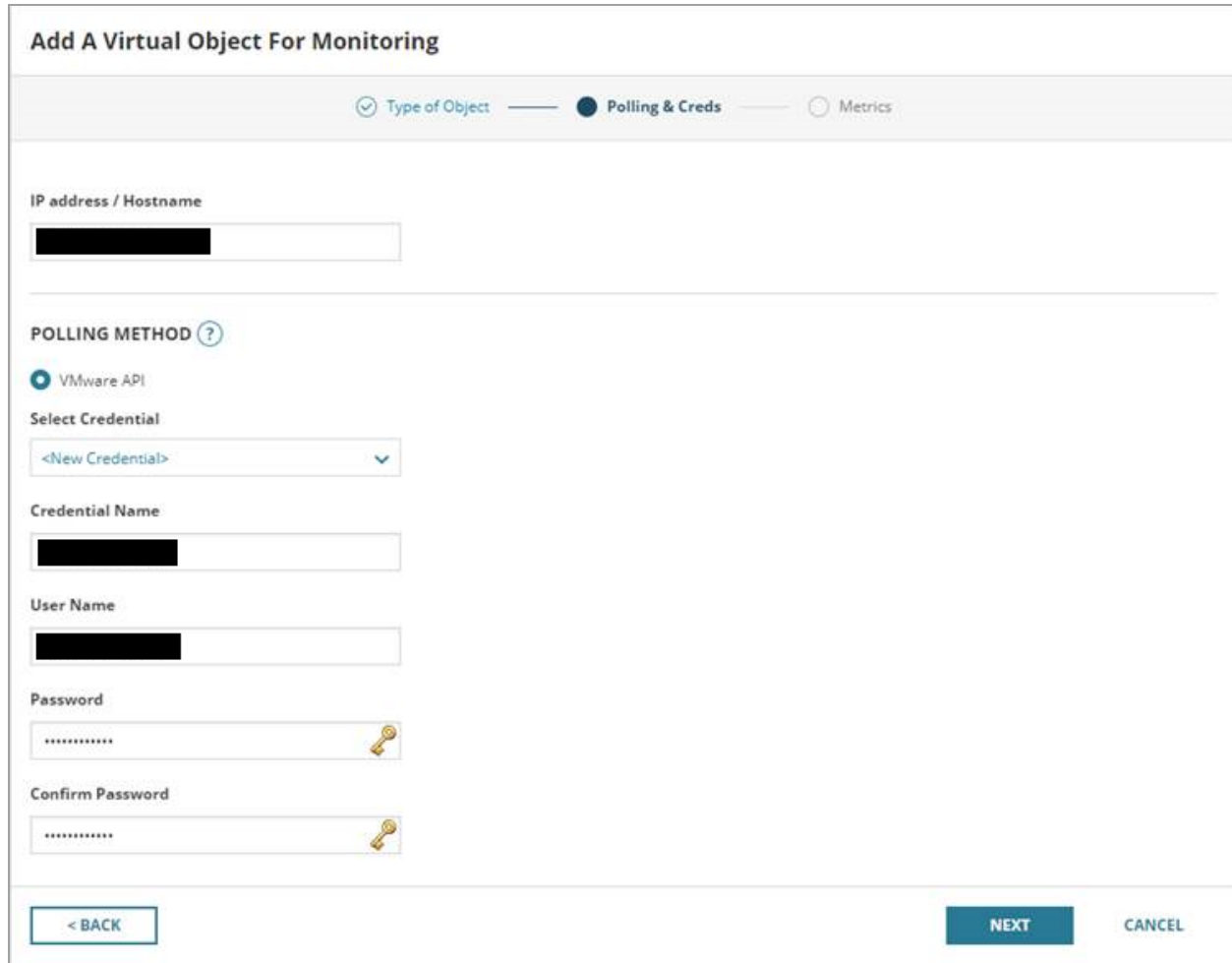
1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Getting Started with Orion, click Add VMware, Hyper-V or Nutanix entities.
3. On the Type of Object tab, select vCenter, and click Next.



4. On the Polling & Creds tab, enter the IP Address / Hostname, vCenter Credential name, vCenter User name, Password, and confirm the password.

For information on required permissions, see the [VMAN documentation](#).

5. Click Next.



Add A Virtual Object For Monitoring

Type of Object
 Polling & Creds
 Metrics

IP address / Hostname

POLLING METHOD ?

VMware API

Select Credential

Credential Name

User Name

Password

Confirm Password

6. On the Metrics tab, review the metrics and click Finish or Finish and add another.

For information on enabling the switch to export IPFIX records, see [Introducing the NTA 2020-2 Release-Candidate - VMware VDS Support](#) on THWACK.

How to monitor flow from a distributed vSwitch

You can manage VMware devices only on the node level. On the [Flow Sources Management page](#), select Node to see your VMware devices:

1. In the SolarWinds Platform Web Console, click My Dashboards > NetFlow > Flow Sources.

You can also access the Flow Sources Management page by clicking Settings > All Settings > Under Product Specific Settings, click NTA Settings > Flow Sources Management.

2. In the drop-down menu in the upper left of the page, click Node.

Your VMware devices will appear in the list. If you've assigned an IP address to your distributed vSwitch, you'll see all of your traffic sourced from one node - the address you assigned the switch. If you did not assign an IP address to the vSwitch, you'll see traffic sourced from your ESXi hosts.

Troubleshooting

I get unknown flow source events on an IP address associated with my VMware host.

This is normal behavior if you just added your VMware nodes. There is approximately a 10 to 20-minute interval before the devices are correctly polled, including IP address information.

Check that the node is managed and if you have disabled automatic addition of flow sources, add the node as a flow source manually.

I get unknown interface index events on VMware nodes.

This is normal behavior if you just added your VMware nodes. There is approximately a 10 to 20-minute interval before the devices are correctly polled.

I created virtual interfaces based on the event, but I don't see data for these interfaces.

This is normal behavior. You can delete the created interfaces so that they don't take up your NPM license limit.

I do not see flow data widgets on the details pages of my VMware devices.

Check that there are data visible for this device on the NTA pages and that they are correctly associated to the requested node.

Check that widgets are added to Node Details page (they are added by default, and hidden only if the node never received any flows).

Process flow data from Meraki devices in NTA

You can view flow data from Cisco Meraki MX devices. The data are associated with SNMP-managed interfaces from NPM. Certain devices use different Interface IDs when polled by SNMP and different Interface IDs in NetFlow. Due to this discrepancy, traffic cannot be correctly bound to the interface. This issue is solved by mapping between Flow Interface ID and SNMP Interface ID.

- You must have Meraki firmware version MX 14.7 or later to get the correct bytes values. SolarWinds NTA supports flow processing for earlier versions and it will not block outdated firmware, but NTA will display incorrect traffic volumes for the bytes counter.
- You must have Meraki firmware version 15.13 or later to get correct packet values. Earlier versions of Meraki MX show an incorrect packet number, as the counter is not providing increments but total values with each flow.
- For Huawei and Alcatel devices, the flow must be processed on the same polling engine where SNMP data are polled.
- After changing the polling engine, mapping is generated for the new polling engine but kept on the old one. The mapping for the node is removed from all polling engines on cleanup (by default, every 60 minutes) when you disable the node through NetFlow Sources.
- Starting with Meraki MX 15.14 or later, the interface mapping is corrected and the feature will be disabled automatically on the NTA side, or you can disable it manually through NTA Settings.

To start monitoring data from Cisco Meraki MX devices, you must [add the device to SolarWinds NPM](#) and [configure it to export flows](#) to the Main or Additional Polling Engine. The mapping is generated automatically when NTA receives the first flow traffic from the relevant Meraki device. Mapping is kept in the SolarWinds Platform database in separate tables for each polling engine. Mapping is valid until you manage the node, enable flow processing, and the NetFlow Service receives flow data.

Enable or disable the Meraki MX mapping feature

You can enable the Meraki mapping feature through NTA Settings in the SolarWinds Platform Web Console. If you are monitoring devices running Meraki firmware version MX 15.14 or later, you can disable the mapping feature completely.

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Under NetFlow Management, select Process flow data from Meraki MX 15.13 and earlier to enable the feature, and clear the option to disable it.

- SolarWinds NTA uses autodetection per device for new Meraki firmware. Processing therefore works correctly with Meraki firmware 15.14 or later and this option enabled.
- If you disable this option through NTA Settings, the changes are global for all devices.
- If you have devices with Meraki firmware MX 15.13 or later, you see data on the wrong interfaces.

Configure NTA

You can use NTA to customize monitoring flow traffic and CBQoS data on your network to provide the most relevant information.

Use the NetFlow Settings page to configure which flows you want to collect. You can also select which services you want to monitor, including:

- Applications
- Autonomous systems
- IP address groups
- Protocols
- Flow sources
- CBQoS devices
- Collector services

You can also optimize NTA performance by setting top talker optimization, making database-relevant settings, or setting defaults for NTA charts.

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.


NTA Settings

Each of the following sections provides instructions for configuring NTA and customizing it to meet your network analysis requirements.

Access the NetFlow Traffic Analyzer Settings page

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.

Available settings

 The configuration actions described in the following sections require administrative access to the SolarWinds Platform Web Console.

- **NetFlow management:** Configure default behavior when flows from NPM devices are received, towards data from ports not monitored in NTA, and unmanaged interfaces.
- **Application and service ports:** Configure the ports and applications that should be monitored in NTA.
- **Autonomous systems:** Manage autonomous systems monitored in NTA.
- **IP address groups:** Manage IP address groups and select IP groups whose traffic should be monitored in NTA.
- **Monitored protocols:** Select what protocols you want to monitor in NTA.
- **Flow sources and CBQoS polling management:** Select what flow sources and which CBQoS-enabled devices you want to monitor with NTA.
- **NetFlow collector services:** Add or change ports on which the NetFlow service is listening.
- **Types of services:** Change names used for DiffServ Code Points in NTA.

NetFlow management

NetFlow Management options ensure that you are able see all flow data available from flow-enabled devices on your monitored network. On new installations, all the options are enabled by default.

Due to the volume of data involved in flow monitoring, you may find it necessary to disable the inclusive monitoring options to save database space.

Access the NetFlow Management options

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.

Options for NetFlow Management are available on top of the NetFlow Traffic Analyzer Settings page.

3. Click Save after modifying any options.

Available options

Enable automatic addition of NetFlow sources

If selected, all flow-enabled devices in the SolarWinds Platform database sending flow data to the server hosting NTA are automatically added as NetFlow sources. All recognized NetFlow sources are listed under NetFlow Sources on NTA Summary.

Allow monitoring of flows from unmonitored ports

If selected, NTA retains all flow data provided by NetFlow sources on your network, including flow data for ports that you are not actively monitoring.

A benefit of having this data is that, should you see a significant percentage of unmonitored traffic under Top XX Applications, you can expand the tree to drill down to the interface level. Click Monitor Port to track this traffic by port.

To save space in your database and discard data from unmonitored ports, clear this option.

This option may significantly increase the processing load on both your NTA server and your SolarWinds Platform database server.

Allow monitoring of flows from unmanaged interfaces

If selected, NTA automatically monitors flow packets even if one of the involved interfaces is not managed by NPM.

If you want NTA to discard any flow packets where only one of the involved interfaces is managed by NPM, clear this option.

Clearing this option may significantly decrease the processing load on both your NTA server and your SolarWinds Platform database server, but it will also decrease the amount of flow data stored in your SolarWinds Platform database.

Allow matching nodes by another IP address

If selected, NTA automatically associates a flow with an appropriate NPM node if the node has multiple IP addresses and is sending flows from a non-primary address.

Show notification bar for unknown traffic events

If this option is selected and an unknown traffic event occurs, NTA notifies you about it in the yellow banner below the main tool bar.

Show interfaces for Wireless Controllers

Enable this option for SolarWinds NTA to monitor interfaces for Wireless Controller nodes on the NetFlow sources widget and on the Manage sources page.

Process IPv6 flow data

This option is enabled by default. Disable this option if you do not want to process and store IPv6 flow data. For more information, see [IPv6 traffic processing in NTA](#).

Process flow data from Meraki MX 15.13 and earlier

This option must be enabled for Meraki MX firmware version 15.13 and earlier. Clear this option if you upgraded your devices to MX firmware 15.14 or later.

NAT Stitching

With NAT Stitching, you can observe conversations that traverse through Network Address Translation (NAT) devices, such as routers, security gateways, firewalls, and load balancers. For more information, see [NAT Stitching](#).

Show unknown traffic events

Click this link to navigate to the Last 200 Unknown Traffic Events page. This page provides a list of traffic events involving flow data received from an unmanaged interface. You can use that page to add the relevant interface to NetFlow Sources. For more details, see [Resolve Unknown Traffic](#).

NAT Stitching

Enable NAT Stitching to monitor and report on the full path of your network traffic, ensuring that you have a comprehensive view of the conversations between your internal network and external entities. With NAT Stitching, you can observe conversations that traverse through Network Address Translation (NAT) devices, such as routers, security gateways, firewalls, and load balancers.

When you enable NAT Stitching, you have the possibility to not only store public IP addresses of devices, but also link the communication to private IP addresses on your network. If NTA detects Post-NAT fields in flow data, the IP addresses are automatically switched during processing.

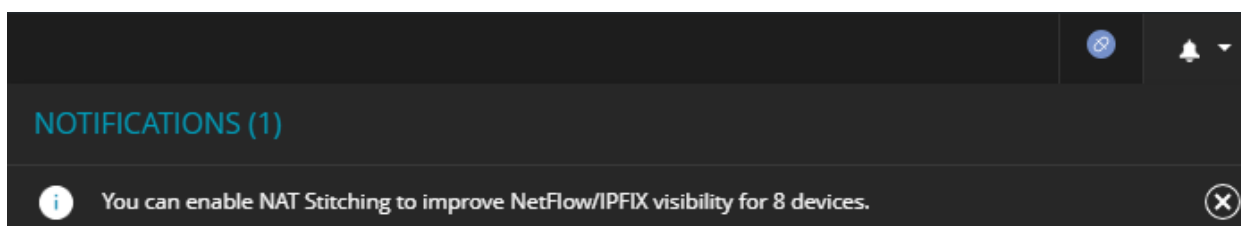
Enable NAT Stitching

In fresh installations, the feature is enabled by default. If you have upgraded from an earlier version, NAT Stitching is disabled. To enable the feature:

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product specific settings, click NTA Settings.
3. Under NetFlow Management, select Enable NAT Stitching.

NAT events



If the feature is disabled, you receive a one-time notification and an event message.



You can either click dismiss to remove the notification from the notification bar, or click the notification to access the Events page and review related events.


When the feature is disabled, the service tries to detect NAT-capable devices. If devices are found, an event message of NetFlow Device Capability type is displayed in the SolarWinds Platform Web Console. Detection is based on NetFlow/IPFIX data templates. If the templates contain Post-NAT fields for a particular device and if the device is sending data, the device is considered NAT-capable.

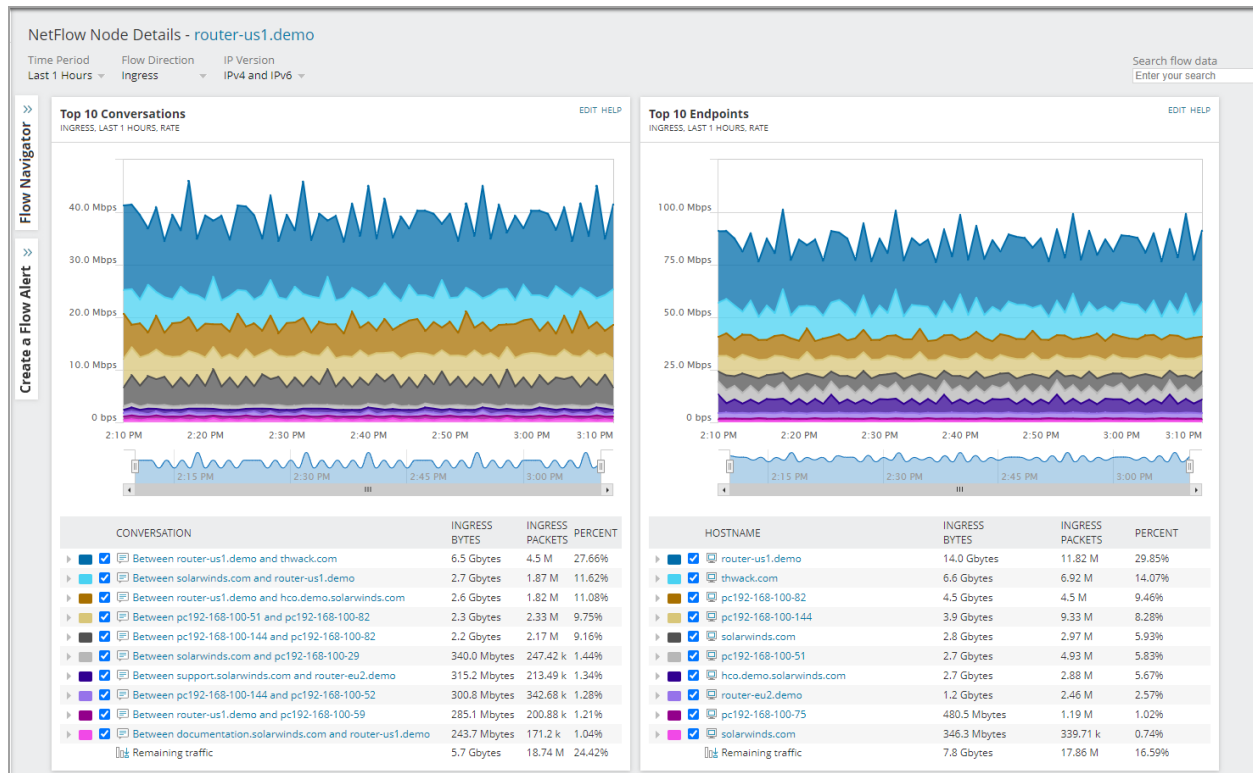
When NAT-capable devices are detected while the feature is disabled, you receive an events message with a list of the detected devices. Click NTA Settings in the events message to access NetFlow Management settings and enable NAT Stitching.

TIME OF EVENT	MESSAGE
<input type="checkbox"/> 7/11/2024 11:58 AM	 To get better visibility of NAT traffic for gw-b479.demo , router-us1.demo , router-us2.demo , router-eu2.demo , gw-b478.demo , and 3 additional devices, enable NAT Stitching in NTA settings . For more information, see NAT Stitching .
<input type="checkbox"/> 7/10/2024 10:32 AM	 To get better visibility of NAT traffic for gw-b479.demo , router-us1.demo , router-us2.demo , router-eu2.demo , gw-b478.demo , and 3 additional devices, enable NAT Stitching in NTA settings . For more information, see NAT Stitching .

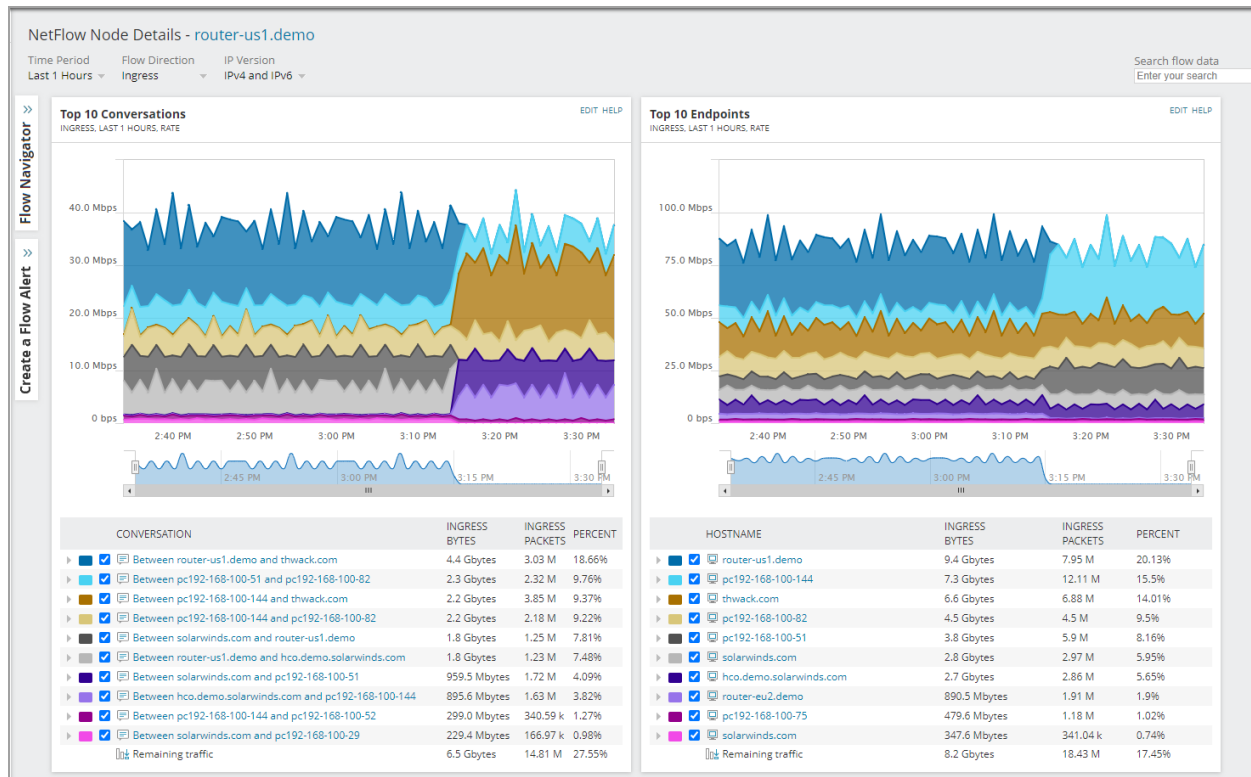
Review how NAT stitching affects you data

1. Select a device with NAT configured and navigate to the NetFlow Node Details page for the device.
2. Observe the Top 10 Endpoints widget. You should see large amount of traffic reported under the hostname/IP address of the router or edge device. In the image below, that would be the device `router-us1.demo`.
3. Observe the Top 10 Conversations widget and check what conversations are reported. You may want to change to Absolute Time Period, confirming the prefilled time range, to persist the actual charts and to compare with charts after the settings change.

 If you don't have the Top 10 Endpoints and Top 10 Conversations widgets on the NetFlow Node Details page, add them.



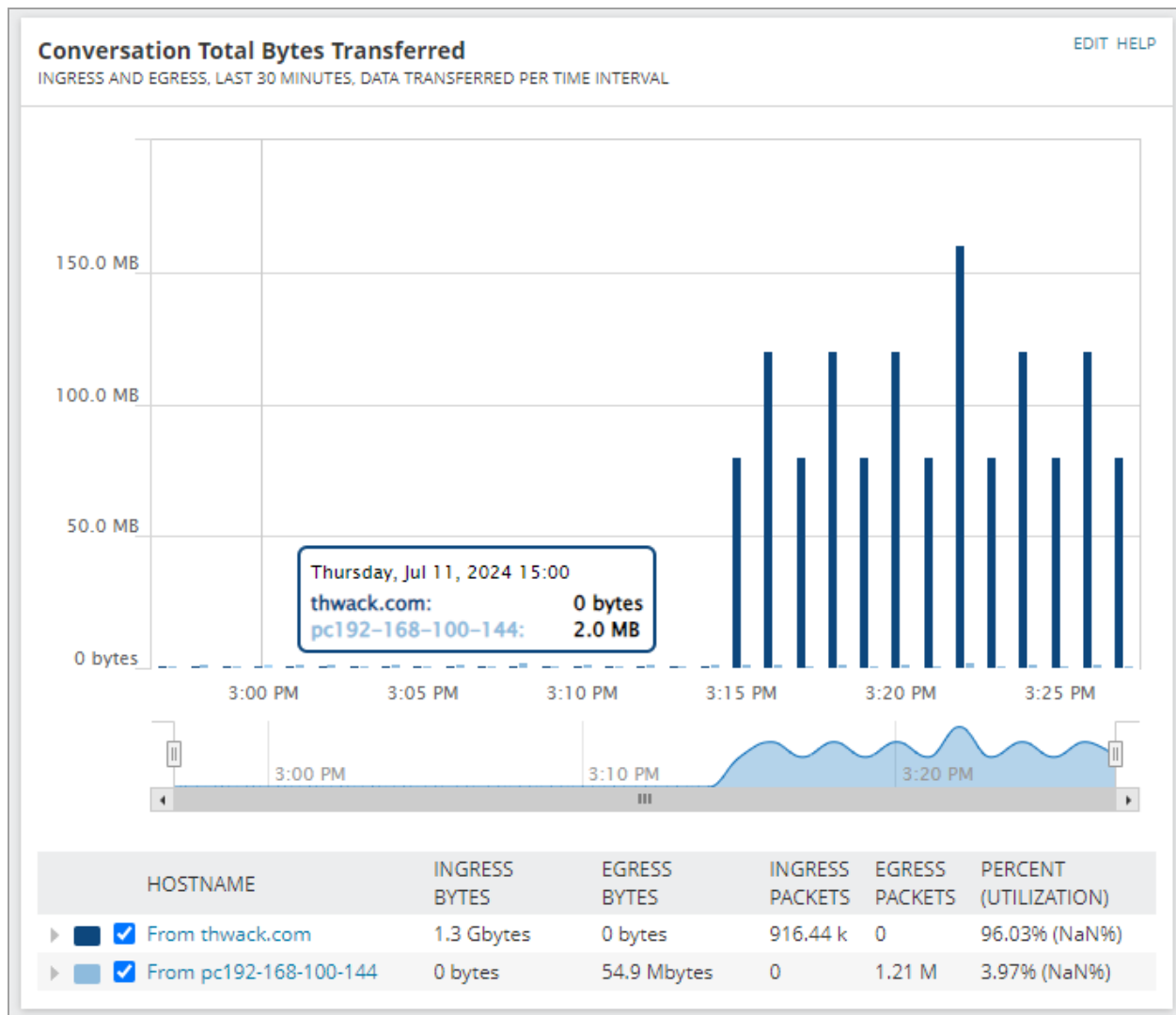
4. [Enable](#) NAT Stitching.
5. Go back to the NetFlow Node Details page and set the default time interval to Last 1 hour. After 5 - 10 minutes refresh the page to see if and how the data changed.
6. In the Top 10 Endpoints widget, you should see that the amount of data reported under the router hostname or IP address reduces significantly and traffic load is now reported under hostnames or IP addresses from the internal network. In the below example, that would be pc192-168-100-144.



- In the Top 10 Conversations widget, you should see a different list of conversation. Less conversation with routers or edge devices (for example, between `router-us1.demo` and `thwack.com`), more between private and public endpoints, for example, between `pc192-168-100-144` and `thwack.com`, or between `solarwinds.com` and `pc192-168-100-51`.

If there is no significant difference, you may try a different device for investigation. If you still don't see any significant difference, the device may be capable of reporting Post-NAT data, but there is no NAT traffic or no significant amount of NAT traffic visible in widgets.

- Additionally, you can investigate one of the conversations between an endpoint in a private network and a public endpoint. In the scenario below, conversation between `pc192-168-100-144` and `thwack.com` was investigated by expanding the legend under the charts to the interface level and clicking an interface, for example `eth16`.
- When you open the NetFlow Conversation page, switch the flow direction to ingress and egress to see both requests and responses. Observe the Conversation Total Bytes Transferred to check if only one direction was reported before the settings change. If both directions are reported before and after the settings change, NAT stitching does not affect you and it does not matter if you keep it enabled or disabled.



- You can also investigate the Conversation Traffic History widget to see the traffic directions. Without NAT stitching you should see only one direction of the traffic.


Conversation Traffic History							EDIT HELP
LAST 50 CONVERSATIONS							
DATE/TIME	PC192-168-100-144	↔	THWACK.COM	BYTES	PACKETS		
7/11/2024 3:17:00 PM	TCP	Random High Port	→	http protocol over TLS/SSL (443)	2.0 Mbytes	44.859K Packets	
7/11/2024 3:17:00 PM	TCP	Random High Port	←	http protocol over TLS/SSL (443)	120.5 Mbytes	83.313K Packets	
7/11/2024 3:16:00 PM	TCP	Random High Port	→	http protocol over TLS/SSL (443)	1.4 Mbytes	29.906K Packets	
7/11/2024 3:16:00 PM	TCP	Random High Port	←	http protocol over TLS/SSL (443)	80.4 Mbytes	55.542K Packets	
7/11/2024 3:15:00 PM	TCP	Random High Port	→	http protocol over TLS/SSL (443)	2.0 Mbytes	44.859K Packets	
7/11/2024 3:15:00 PM	TCP	Random High Port	←	http protocol over TLS/SSL (443)	120.5 Mbytes	83.313K Packets	
7/11/2024 3:14:00 PM	TCP	Random High Port	→	http protocol over TLS/SSL (443)	2.0 Mbytes	44.859K Packets	
7/11/2024 3:14:00 PM	TCP	Random High Port	←	http protocol over TLS/SSL (443)	80.4 Mbytes	55.542K Packets	
7/11/2024 3:13:00 PM	TCP	Random High Port	→	http protocol over TLS/SSL (443)	2.0 Mbytes	44.859K Packets	
7/11/2024 3:12:00 PM	TCP	Random High Port	→	http protocol over TLS/SSL (443)	1.4 Mbytes	29.906K Packets	
7/11/2024 3:11:00 PM	TCP	Random High Port	→	http protocol over TLS/SSL (443)	2.0 Mbytes	44.859K Packets	
7/11/2024 3:10:00 PM	TCP	Random High Port	→	http protocol over TLS/SSL (443)	1.4 Mbytes	29.906K Packets	
7/11/2024 3:09:00 PM	TCP	Random High Port	→	http protocol over TLS/SSL (443)	2.0 Mbytes	44.859K Packets	
7/11/2024 3:08:00 PM	TCP	Random High Port	→	http protocol over TLS/SSL (443)	1.4 Mbytes	29.906K Packets	
7/11/2024 3:07:00 PM	TCP	Random High Port	→	http protocol over TLS/SSL (443)	2.7 Mbytes	59.812K Packets	
7/11/2024 3:06:00 PM	TCP	Random High Port	→	http protocol over TLS/SSL (443)	1.4 Mbytes	29.906K Packets	
7/11/2024 3:05:00 PM	TCP	Random High Port	→	http protocol over TLS/SSL (443)	2.0 Mbytes	44.859K Packets	
7/11/2024 3:04:00 PM	TCP	Random High Port	→	http protocol over TLS/SSL (443)	1.4 Mbytes	29.906K Packets	
7/11/2024 3:03:00 PM	TCP	Random High Port	→	http protocol over TLS/SSL (443)	2.0 Mbytes	44.859K Packets	
7/11/2024 3:02:00 PM	TCP	Random High Port	→	http protocol over TLS/SSL (443)	1.4 Mbytes	29.906K Packets	

IPv6 traffic processing in NTA

NTA listens for packets on IPv6 addresses. NTA is also able to extract IPv6 traffic details from Protocol Data Units (PDUs).

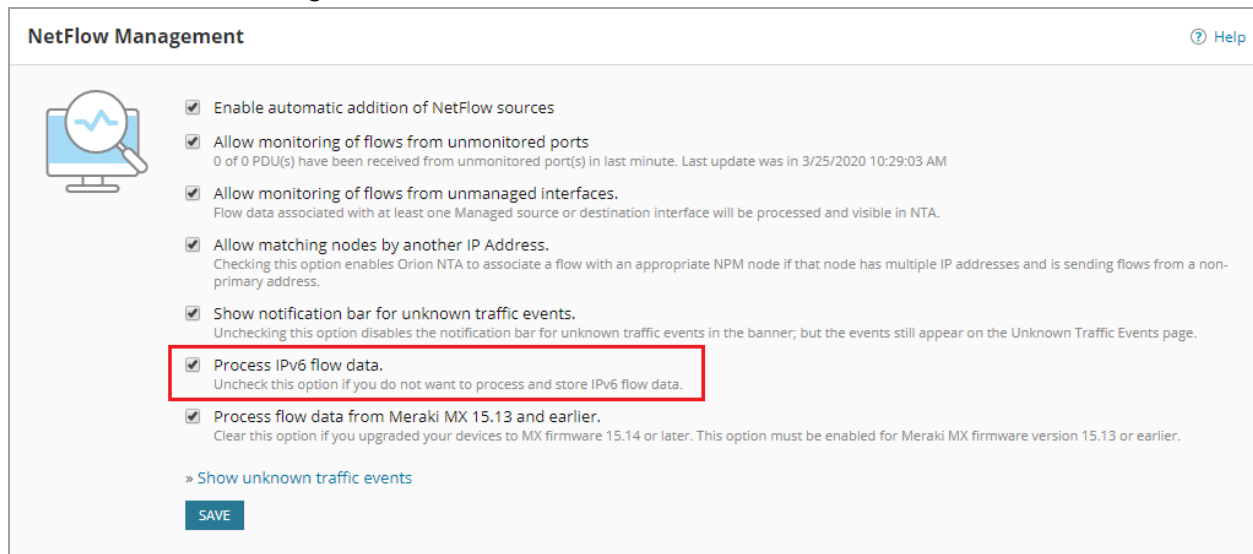
When you enable IPv6 traffic processing, [reports](#) and widgets automatically display available IPv6 data.

Enable processing of IPv6 traffic

 In case of fresh installations and upgrades, IPv6 traffic processing is **enabled by default**.

You can enable or disable IPv6 traffic processing through NTA Settings in the SolarWinds Platform Web Console:

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Under NetFlow Management, select Process IPv6 flow data.

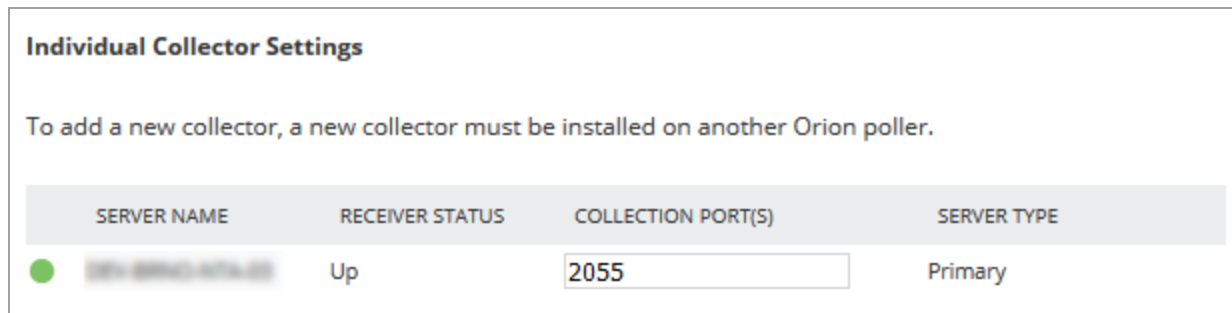


When you enable this option, the port defined as NetFlow Collector automatically binds to all available IP addresses on the polling engine, including IPv6 endpoints.

Verify the collector settings

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Click NetFlow Collector Services.

The Edit NetFlow Collector Services page provides status information about the NetFlow collectors and the ports on which they are listening for NetFlow data. For more information, see [NetFlow Collector Services](#).




You can also use the new filters within the Flow Navigator feature. For more information, see [Create custom views with the Flow Navigator](#).

Applications and service ports in NTA


Use NTA to directly specify the applications and ports you want to monitor. Additionally, you can specify protocol types by application, giving you the ability to monitor multiple applications on the same port if each application uses a different protocol. You should review this list of ports and applications and check the ports and applications you want to monitor, adding any that are not present.

By default, NTA monitors recommended ports and applications that are used most on typical networks.

 NTA supports many applications out of the box. However, if you have custom internal applications, remember to assign a port name and number to them so that they are reported correctly and not marked unknown.

Access the applications and service ports settings

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Click Application and Service Ports.

 To monitor ports on a server, you first need to create an IP address Group and then two applications:

Let's assume you have a server with an IP address 1.1.1.1 and you want to monitor ports 80 and 443 on that server.

1. Add an IP address group with the IP address 1.1.1.1. For more information, see [IP address groups in SolarWinds NTA](#).
2. Create an application called Application1 with ports 80 and 443, and select your new IP address group as the Source IP Address.
3. Create an application called Application2 with ports 80 and 443, and select your new IP address group as the Destination IP Address.



You cannot create a single application when monitoring ports on a server.

Learn more

Add applications and service ports

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Click Application and Service Ports.
4. Click Add Application.
5. Enter the application and port information.
6. Click Add Application.
7. Click Submit.


Edit applications and service ports

You can edit the name of an application or service, ports it uses, source and destination IP addresses, or protocols connected with the application.

Some multi-port applications may be configured with overlapping port assignments. Traffic will only be associated with one of the conflicting applications.

To avoid this conflict, remove the port range in conflict, disable a conflicting application, or delete the port or application entirely.

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Click Application and Service Ports.
4. Find the application or service port you want to edit:
 - Use the View list to filter the applications and service ports.
 - Applications are listed by ascending port number, with multi-port applications listed first.
 - Use the Search function to filter the list further.
5. Click Edit in the Actions column of the application or port.
6. Edit the application and port information.
7. Click Update Application.
8. Click Submit.

 Submitting these changes does not update historical data.

Monitor applications and service ports

Because of the volume of data from flow-enabled network devices, monitoring all ports and applications may severely affect the performance of both the SolarWinds Platform database and the SolarWinds Platform Web Console.

You can decide what ports or applications should be monitored by NTA. If you are not sure what ports and applications you should monitor, click Monitor Recommended Ports to monitor the most common high traffic ports and applications.



Clicking Monitor Recommended Ports deletes all existing custom application and port definitions.

Enable monitoring for ports or applications

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Click Application and Service Ports.
4. To enable monitoring an application or a port, click Enable in the Actions column.
5. To enable monitoring for all listed applications and ports, click Enable All Monitoring.
6. If you are not sure what ports and applications to monitor, click Monitor Recommended Ports.
7. Click Submit.

Disable monitoring for ports or applications

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Click Application and Service Ports.
4. To disable monitoring an application or a port, click Disable in the Actions column.
5. To disable monitoring for all listed applications and ports, click Disable All Monitoring.
6. Click Submit.

Configure data retention for flows on unmonitored ports

By default, NTA retains all flow data provided by NetFlow sources on your network, including flow data for ports that you are not actively monitoring.

If you see a significant percentage of unmonitored traffic in your Top XX Application widget, expand the tree and drill down to the interface level. Click Monitor Port in the SolarWinds Platform Web Console to track this traffic by port.

i Enabling this option may significantly increase the processing load on both your NTA server and your SolarWinds Platform database server. Clear the Allow monitoring of flows from unmonitored ports option to save space in your database and discard data from unmonitored ports.

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Select Allow monitoring of flows from unmonitored ports.
4. Click Save.

Delete applications and service ports

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Click Application and Service Ports.
4. Click Delete in the Actions column of the application or port.
5. Click Delete Application.
6. Click Submit.

Autonomous systems in NTA

To manage autonomous systems in NTA, enter the autonomous systems information in the NTA settings.

For information about NTA requirements for monitoring autonomous systems via BGP, see the [Autonomous system requirements](#).

Access autonomous systems

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Click Autonomous Systems.

Add autonomous systems

1. Click Add Autonomous Systems.
2. Enter the autonomous system information.
3. Click Save.

Edit autonomous systems

1. Click Edit in the Actions column of the autonomous system.
2. Edit the autonomous system information.
3. Click Save.

Delete autonomous systems

1. Click Delete in the Actions column of the autonomous system.
2. Click Delete.

IP address groups in NTA

NTA allows you to establish IP address groups for selective monitoring of custom categories or segments of your network.

With well-defined IP groups, you can better characterize and assess NetFlow data that you receive.

i SolarWinds recommends creating IP Address Groups, for example by location, especially for the benefit of your first level support group, to quickly see IP Address ranges and makes things easier to manage.

IP Address Groups Management page

You can manage your IP address groups through a completely reimplemented IP Address Groups Management page.

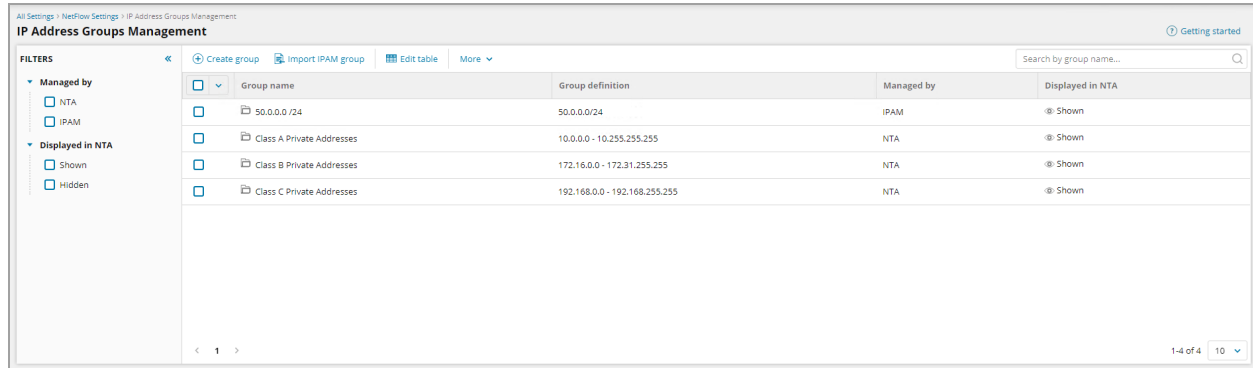
You can [unify IP address groups with SolarWinds IPAM](#), define the IP Range with CIDR notation, filter IP address groups with predefined filters, or search IP address groups by their name and customize visible information. Changes on the IP Address Groups Management page are automatically confirmed, unlike in earlier versions of NTA where you had to click the Confirm button to apply the change.

i All IP address groups features from previous versions of NTA are still available on the new management page, except for the explicit Printable version.

- [Adding new IP address groups](#) with ranges.
- [Deleting IP address groups](#).
- [Editing IP address groups](#) and their ranges.
- Importing and exporting IP address groups from or to XML files.
- Enabling or disabling visibility of IP address groups in NTA widgets.

Access the IP Address Groups Management page

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Under IP Address Groups, click Manage IP Address Groups.



Available actions

All IP address groups features from older versions of NTA are still available on the new management page, except for the explicit Printable version.

[Adding new IP address groups with ranges](#)

IP address group with ranges is created immediately after you click on the Create button. You can use CIDR notation to identify the IP address group range.

[Deleting IP address groups](#)

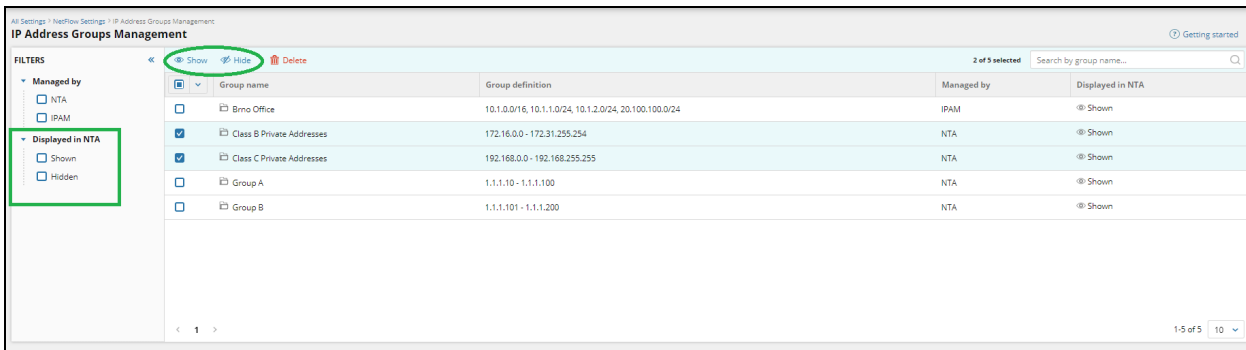
After selecting an IP address group, you can click Delete to remove IP address groups. You can bulk-delete by selecting multiple IP address groups. You must confirm the operation in another window what also provides and option for canceling.

[Editing IP address groups and their ranges](#)

After selecting an IP address group, you can edit the IP address groups. Changes are applied immediately after you click on Save. You can edit only one IP address group at a time. You cannot edit IP address groups managed by IPAM. You can use CIDR notation for IP ranges.

Show or Hide IP address groups

After selecting an IP address group, you can click Show for NTA to display IP address groups in widgets, or Hide in order to hide them. You can filter out the IP address groups that are either shown or hidden in the sidebar on the IP Address Groups Management page.

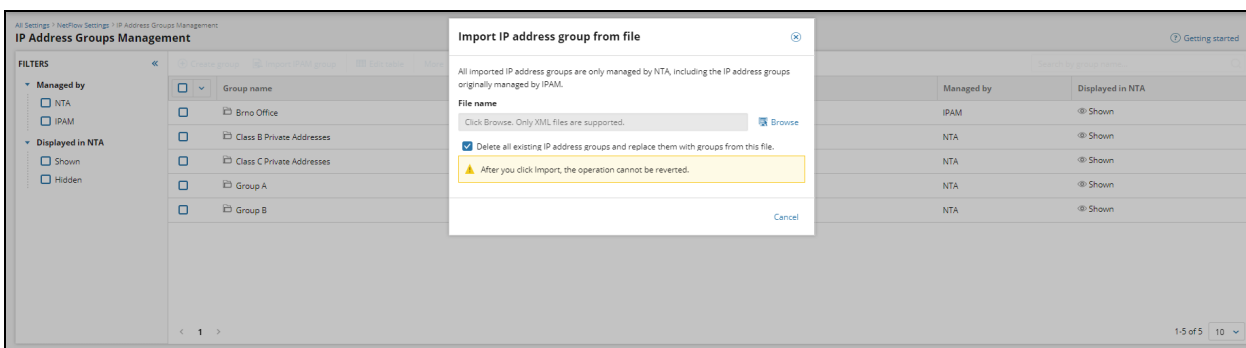
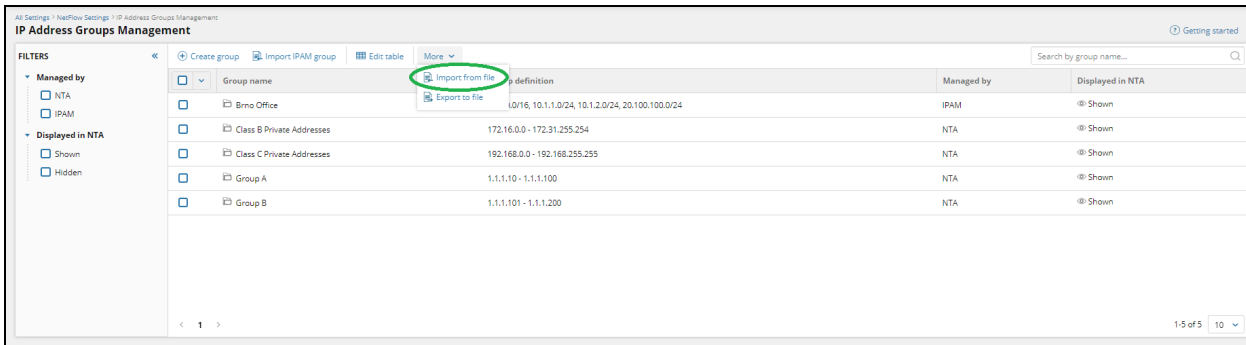


Import IPAM IP address groups

You can import IP address Groups managed by SolarWinds IPAM. For more information, see [IP address groups unification with IPAM](#).

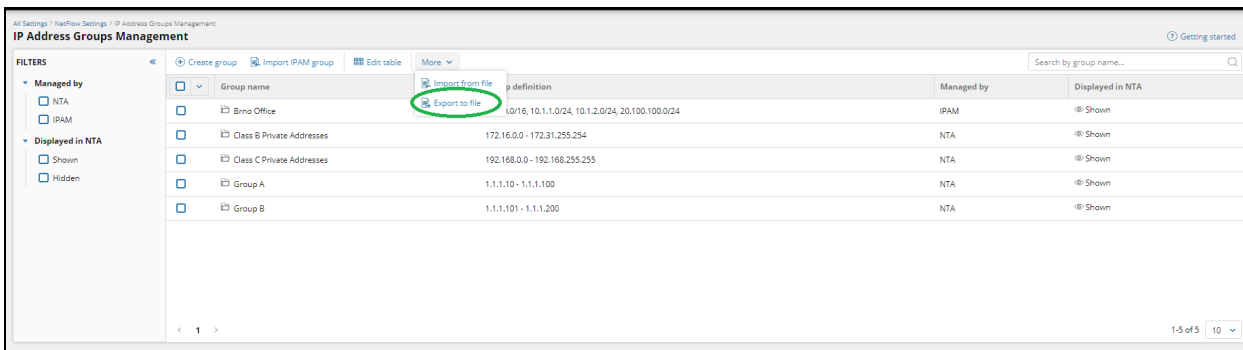
Import IP address groups from a file

You can add IP address groups to existing groups or delete all existing groups by import new ones. If you choose to delete the existing IP address groups and replace them with imported ones, NTA check if the IP address groups are used by any NTA application. The operation is canceled if such an application is found. These application conflicts can be resolved automatically or manually. You can use CIDR notation when importing XML files. All IP address groups are imported as standard IP address groups managed by NTA, even when you export IP address groups previously imported from IPAM.



Export IP address groups to a file

You can export the IP address groups in your SolarWinds Platform Web Console through the IP Address Groups Management page, clicking More > Export to file.



Standard features of the filtered list

You can use standard features for the filtered list, such as filtering Shown or Hidden IP address groups or which product they are managed by, searching by IP address group name, or customizing the layout of the page and order of the columns.

Troubleshooting IP address groups

In NTA you can have IP address groups with overlapping ranges. Unlike IP address groups, applications cannot have groups with overlapped ranges in the same direction. If you have applications linked to a group (source, destination) and you edit or delete that group, you can create application collisions. These are overlaps in source or destination IP address groups. Application collisions are caused by editing or deleting an IP address group, or importing IP address groups from a file, deleting existing ones and replacing them with the new import. When a collision is detected, the operation is stopped and NTA will display a pop-up window with the collisions listed in a table, such as in the example below.

Edit IP address group ✕

⚠ Application conflict. Modifying this IP address group to the defined range will cause a conflict because the range is already being used by other IP address group for the following applications. [Learn more](#) ↗

Affected applications

Name ▲	Port	Protocol	IP address group
✕ App A	50000	Both	Group A
✓ App B	50000	Both	Group B

Automatically resolve the conflict by clicking **Save & Delete**. This will **delete** all marked applications and **cannot be reverted**.

Cancel
Back
Save & Delete

You can resolve the collision manually through the NTA Applications Management page or automatically by clicking Save & Delete in the pop-up window.

💡 Application collisions are automatically resolved by deleting one of the applications in the collision. The applications with ✕ icon will be deleted. Applications with ✓ will remain in the list.

Troubleshooting FAQs

Why is my NTA Application missing or why was it deleted?

Automatically resolving application conflicts during an IP address group synchronization can delete applications. If you do not want to delete any NTA applications, do not use IP address groups imported from IPAM for application definition.

Why are data in IP address group charts invalid or seem to be incorrect?

When you update IP ranges including IP segments, historical data are not valid and widgets can show mismatched data. This situation is temporary. Changing an IP group range in IPAM can cause this behavior, too.

Why is the window with application collisions displayed again with different application when I've already automatically resolved application conflicts?

It is possible that someone else is editing IP address groups at the same time, or IP address group synchronization is running on the background. In such a case, conflicts are automatically resolved, but the other updates make change in IP address groups causing new conflicts. You have to resolve the conflicts again. This situation should be rare.

I've exported all of my IP address groups into the XML file. Then I've imported them again. Why are all IP address groups managed by IPAM are now standard IP Groups managed by NTA?

This is the expected behavior. All IP Groups are imported as IP Groups managed by NTA. Also, there is no possibility of how to "link" those IP Groups to existing IPAM groups. User has to delete those groups and import them again from IPAM.

Can I use IPAM IP address groups with applications in NTA without my applications being deleted by application collisions auto-resolving?

SolarWinds cannot guarantee that while the applications are still managed by IPAM. In the current implementation, you cannot have synchronized groups managed by IPAM used in applications without the risk of deleting the applications during synchronization with IPAM. You can use IP groups managed by IPAM without this risk if you don't use them as a source or destination IP address group for applications. The only safe workaround is to:

1. Import IP address groups from IPAM as IP address groups managed by IPAM.
2. Export all IP address groups.
3. Import IP address groups as IP address groups managed by NTA, deleting the existing groups.



The synchronization will not delete any application because there is no group to synchronize. But changes in IPAM will not be propagated into NTA anymore.

I've edited or deleted an IP address group and the Applications Conflicts window pops up. I want to resolve the conflicts manually because auto-resolve options are not suitable for me. What can I do?

Go to the NTA Application Management page. Find the applications listed in the Application Conflicts window and edit them to remove conflicts. The specific resolution depends on your needs and possibilities you have to modify your applications.

Applications are usually conflicted in the following properties:

- Protocol (TCP, UDP, or both)
- Port number or port numbers for multiport applications,
- Source and destination IP address group.

The following options are available for resolving such conflicts:

- Delete one of the conflicting applications. This is how auto-resolve works, but you have a chance to choose the application to be deleted.
- Remove overlapping IP address group or IP address groups from the application. This IP address group still exists, but NTA will not use it as a source or destination IP address group of the application. You can create new IP address groups without overlaps by removing overlapping parts of the range and use these groups for edited applications. These steps can create a new application collision, but the Application Management page will inform you about it. This step can be used if you cannot edit the range of the original IP Group used for the application.
- Manually edit ranges of the colliding IP address groups to eliminate overlaps.
- If you have an Application with only one IP address group (source or destination, not both) in conflict, you can resolve the conflict by configuring the second IP address group, making this application more specific. This application will not be in collision anymore because more specific applications are preferred in processing.
- For multiport applications, you can remove the overlapping port.
- For applications with both protocols, you can set the protocol to TCP or UDP, so the protocol does not overlap with other applications.

Add IP address groups to NTA

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Under IP Address Groups, click Manage IP Address Groups.
4. Click Create group.
5. Enter a Description.
6. Add a new IP address or IP address group:
 - To define the selected group as a single IP address, select IP Address, and enter the IP address.
 - To define the selected group as a range of IP addresses, select IP Range, and provide the starting and ending IP addresses.
 - To include this defined group, if eligible, in Top XX IP Address Groups widgets, select the Enable Display in Top XX IP Address Groups Widget.
 - To define another IP Address group, click Add, and repeat the preceding steps.
7. Click OK.
8. Click Submit.

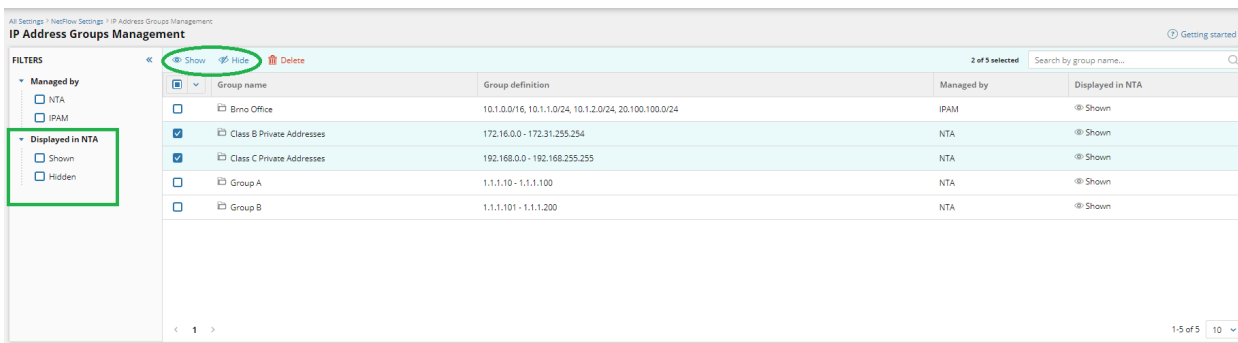
9. Define the parameters of the new IP address or IP address group:

- To define the selected group as a range of IP addresses, select IPv4 range, and provide the starting and ending IP addresses.
- To define the selected group as a single IP address, select IPv4 address, and enter the IP address.
- To define the selected group range using CIDR, select IPv4 CIDR, and enter the CIDR notation.

10. Click Create.

The IP address group will be displayed on the IP Address Management page.

To include this defined group, if eligible, in Top XX IP Address Groups widgets, select the group and click Show. You can also filter the IP address groups that are shown or hidden in NTA widgets.



To define another IP Address group, click Create group, and repeat the preceding steps.

Edit IP address groups in NTA

In NTA, you can edit monitored IP addresses and IP address groups. You can also decide, whether you want to see selected groups in the Top XX IP Address Groups widget.


1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Under IP Address Groups, click Manage IP Address Groups.
4. Click Edit next to an IP address group.
5. Edit the Description.

6. Make the edits:

- To define the selected group as a single IP address, select IP Address, and enter the IP address.
- To define the selected group as a range of IP addresses, select IP Range, and provide the starting and ending IP addresses.
- To include this defined group, if eligible, in Top XX IP Address Groups widgets, select the Enable Display in Top XX IP Address Groups Widget.
- To define another IP Address group, click Add, and repeat the preceding steps.

7. Click OK.

8. Click Submit.


 Submitting these changes does not update historical data.

9. Select the IP address group and click Edit.

10. Make the appropriate edits:


- To define the selected group as a range of IP addresses, select IPv4 range, and provide the starting and ending IP addresses.
- To define the selected group as a single IP address, select IPv4 address, and enter the IP address.
- To define the selected group range using CIDR, select IPv4 CIDR, and enter the CIDR notation.

11. Click Save.

 Editing IP address groups can cause application collisions. For more information, see [IP address groups in SolarWinds NTA](#).

Delete IP address groups from NTA

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Under IP Address Groups, click Manage IP Address Groups.
4. Click Delete at the end of an IP address group row.
5. Click Submit.
6. Select an IP address group and click Delete.
7. Confirm the operation in the pop-up window.

 Deleting IP address groups can cause application collisions. For more information, see [IP address groups in SolarWinds NTA](#).


Select IP ranges to monitor in NTA

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Under IP Address Groups, click Manage IP Address Groups.
4. If any one of the existing ranges contains the addresses you want NTA to monitor, make sure that the corresponding box in the Enable column is selected.
5. Click Submit.

IP address groups unification with IPAM

You can unify IP address groups with SolarWinds IPAM. With the new [IP Address Groups Management page](#), you can import IPAM IP address groups and use them the same way as standard NTA IP address groups:

- See IP address groups in [NTA widgets](#).
- Create [reports](#) on IP address groups.
- Use the IP address groups in [Flow Navigator](#) or NTA search.
- Use the IP address groups as a Source and Destination IP Address Group for Applications.

 Imported IPAM groups cannot be edited in NTA, only in IPAM. Any change in IPAM is automatically reflected in NTA.

The new IP Address Group Management page also allows you to define IP ranges with CIDR notation or filter IP address groups with predefined filters, search IP address groups by their names and customize the visible information, such as columns in the table.

Using IPAM IP address groups in NTA

You must install SolarWinds NTA 2020.2.6 or later together with SolarWinds IPAM 2020.2.6 or later to be able to import and use IPAM IP address groups in NTA.

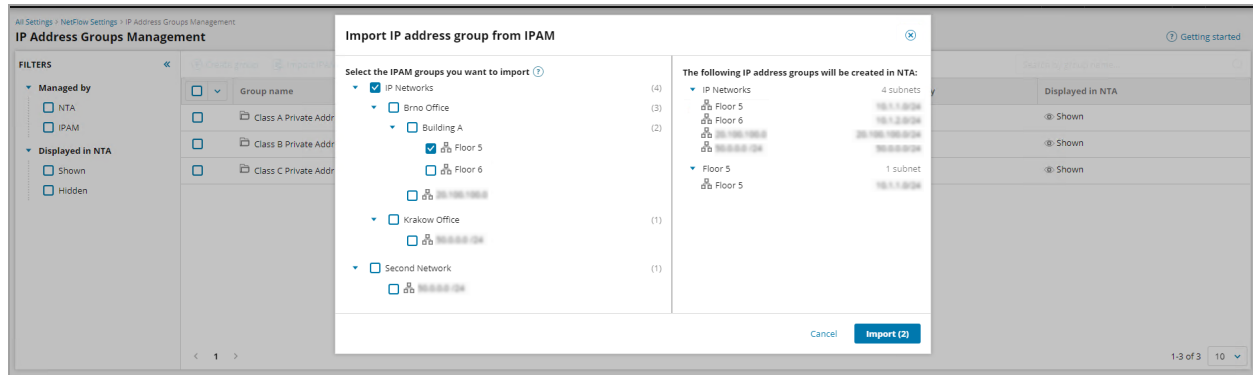
1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Under IP Address Groups, click Manage IP Address Groups.

4. Click Import IPAM group.

A list of IPAM IP address groups is displayed.

5. Select the IPAM IP address groups you wish to import.

Every checked item creates a new NTA IP address group with ranges from IPAM subnets under the directly-linked IPAM IP address group. If you explicitly select IPAM IP address groups in a hierarchy, you can create overlapped IP address groups.



The IPAM IP address group must have at least one child subnet to be displayed in the Import IP address group from IPAM window. Otherwise, this group will not be visible in the list.

6. Click Import.

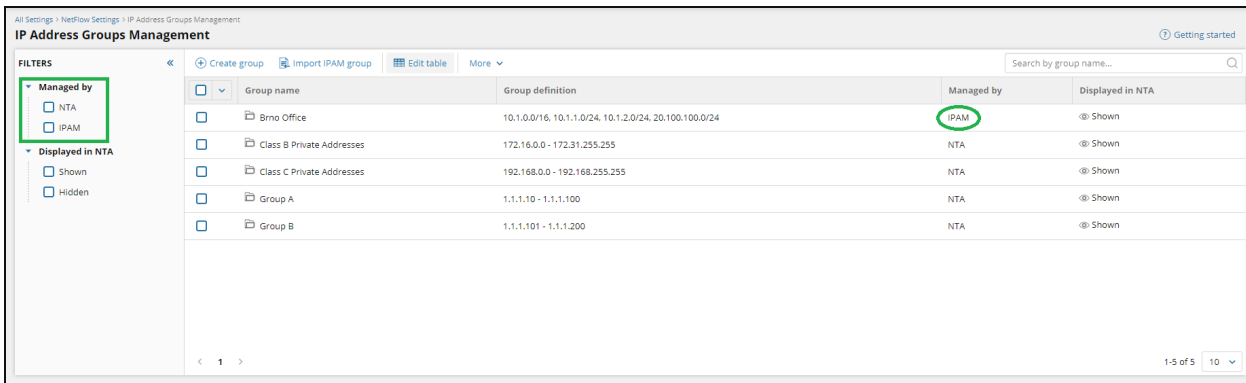
Groups are imported according to the displayed mapping.

Management options for IP address groups imported from IPAM

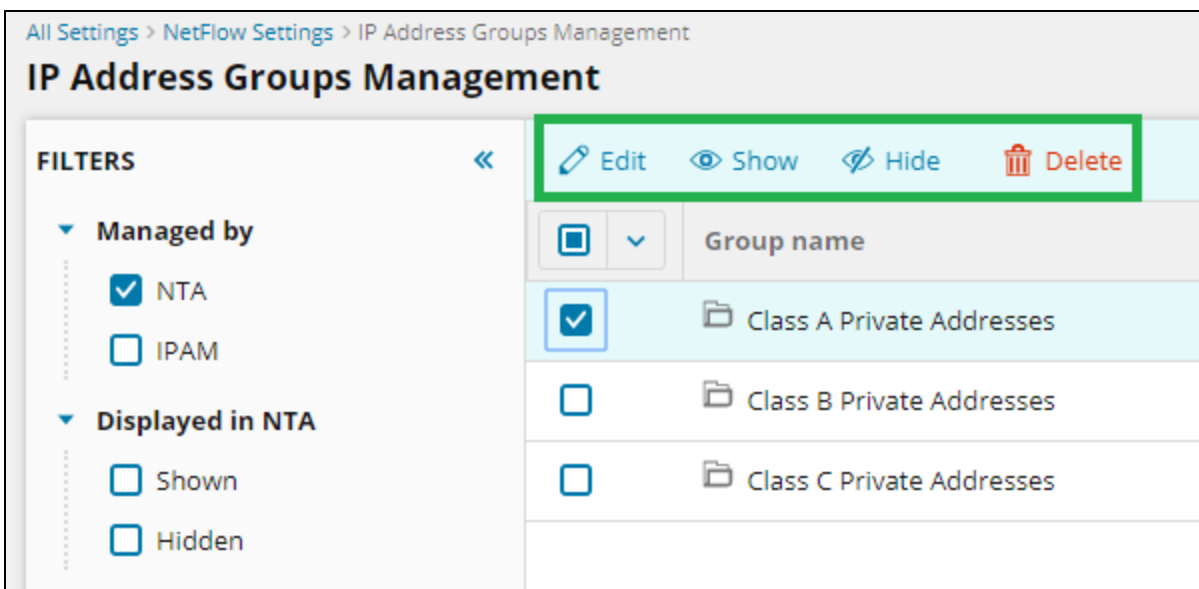
The imported IP address groups will show `IPAM` in the Managed by column. You **cannot edit IP address groups managed by IPAM through NTA**, only through IPAM. All changes in IPAM are automatically reflected in NTA after a delay which can take from 1 minute to 30 minutes, depending on the number of changes made in IPAM.

i IP address groups managed by IPAM can be deleted in NTA, but this operation deletes only the NTA IP address groups imported from IPAM. The original IPAM groups are not affected.

You can filter the IP address groups to view only groups Managed by IPAM or groups Managed by NTA. You can also filter the IP address groups that are set as Hidden or Shown in NTA widgets. The filter options are available in the sidebar on the left of the [IP Address Groups Management page](#).



Selecting the IP address group provides the options to Edit, Show, Hide, or Delete the IP address group. For more information, see [Managing IP address groups](#).



Protocols monitored with NTA

Specify which protocols NTA monitors. Selecting specific monitored protocols can reduce the amount of NetFlow traffic that NTA processes and improve performance.

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Click Monitored Protocols.
4. Select or clear the transport protocols you want NTA to monitor.
5. Click Submit.

Flow sources and CBQoS polling

This section provides procedures for adding and deleting flow sources and selecting CBQoS-enabled devices for monitoring.

If NPM is monitoring network devices that are configured to export flow data, and if automatic addition of flow sources is enabled in NTA Settings, NTA automatically detects and adds the flow sources under NetFlow Sources.

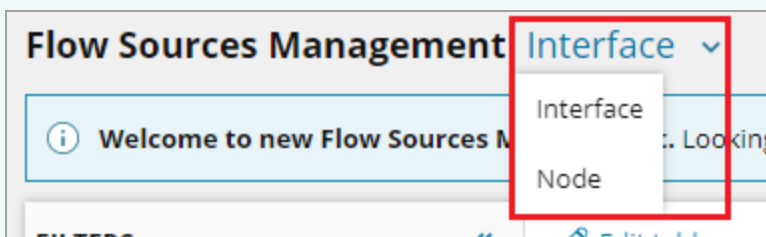
Access the Flow Sources Management page and select interfaces for NetFlow monitoring

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Under Flow Sources Management, click Manually manage flow sources.

i You can also access the Flow sources management page by clicking My Dashboards > NetFlow > Flow Sources.

This page provides a list of flow-enabled nodes and interfaces.

i You can manage flow sources on the level of node or on the level of interface. Selecting Interface in the drop-down next to the Flow Sources Management page title displays the list of interfaces. Selecting Node displays the list of nodes.




If you do not see any Flow sources, confirm that the following is true for your configuration:

- NetFlow devices must be configured to send NetFlow data to the NTA collector. Devices and interfaces must be managed by NPM before they can be recognized in NTA.
- Confirm that the SolarWinds NetFlow Service starts in Windows Services.

4. Use the Filters to find the devices to display.
5. Use the Search function to filter the list further.
6. Select nodes and interfaces for NetFlow monitoring.
7. Click Store traffic.

Access the CBQoS polling management page and select interfaces for CBQoS monitoring

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Under CBQoS polling Management, click Manually manage CBQoS polling.

 You can also access the CBQoS polling management page by clicking My Dashboards > NetFlow > CBQoS Polling.

This page provides a list of all nodes and interfaces in SolarWinds NPM.

CBQoS-enabled devices must be configured to allow CBQoS polling. Devices and interfaces must be managed by NPM before they can be recognized in NTA.

4. Use the Filters to find the devices to display.
5. Use the Search function to filter the list further.
6. Select nodes and interfaces for CBQoS monitoring.
7. Click Enable.

Learn more

Enable the automatic addition of flow sources

NTA can detect and automatically add flow sources that are monitored by NPM.

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Under NetFlow Management, select Enable Automatic Addition of NetFlow Sources if it's not already selected.
4. Click Save.

Enable flow monitoring from unmanaged interfaces

SolarWinds NTA provides the option to retain data for any flow defined with at least one interface monitored by SolarWinds NPM.

It is possible that you may be managing a node in NPM by one interface and IP address, but NetFlow data is coming from a different interface and IP address on that node. In such cases, you can choose to have NTA attempt to associate unknown traffic with a non-primary IP address on a currently monitored NPM node.

For more information about managing interfaces in NPM, see [Discovering and Adding Network Devices](#).

i Disabling the option to monitor flows from unmanaged interfaces may significantly decrease the processing load on both your NTA server and your SolarWinds Platform database server, but it will also decrease the amount of flow data stored in your SolarWinds Platform database.

The following procedure enables the option of monitoring traffic on unmanaged interfaces in NTA.

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Under NetFlow Management, select Allow Monitoring of Flows from Unmanaged Interfaces.
4. Select Allow Matching Nodes by Another IP Address to allow NTA to attempt associating unknown traffic with non-primary IP addresses on a currently monitored NPM node.
5. Click Save.

If there are unknown traffic events, resolve the unknown traffic and add the appropriate devices for monitoring first to NPM, and then to NTA. For more details, see [Resolve unknown NetFlow traffic](#).

Set the sampling rate manually

Sampled flows contain information about their sampling rate. NTA uses this information to correctly display sampled flows data.

You can also manually specify the sampling rate for flows exported from your nodes. This allows you to resolve issues where the appropriate sampling information is not correctly included in the flows, it is not automatically detected, or when you want to see unsampled flows for a device which exports sampled flows.

Manually defined settings override the automatically detected sampling rates.


Manual settings are defined on the node level and are applied on all interfaces monitored for the node.

Edit the sampling rate for flows exported from a node

i The Sampling rate is set on the whole node and can be changed only per node.

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.

3. Under Flow Sources Management, click Manually manage flow sources.

 You can also access the Flow sources management page by clicking My Dashboards > NetFlow > Flow Sources.

4. In the drop-down next to the Flow sources management page title, select Node.
5. Use the Filters to find the devices to display.
6. Select the node, and click Edit sampling rate.
7. Click Edit to change the current settings.
8. Select Override sampling rates.
9. Enter a value, such as 100.
10. Click Apply.

Your setting displays in the Sampling rate column.


The change is applied for all monitored interfaces of the node.

Enable CBQoS polling

You can enable and disable specific CBQoS sources under NTA Settings > CBQoS Polling Management. To be able to poll CBQoS data, you must first enable CBQoS polling.

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Under CBQoS Polling Management, click Manually manage CBQoS polling.

This will take you to the [CBQoS polling management](#) page.

 You can also access the CBQoS polling management page by clicking My Dashboards > NetFlow > CBQoS Polling.

4. Select the nodes and click Enable.

Reconcile flow collection across multiple interfaces of a node

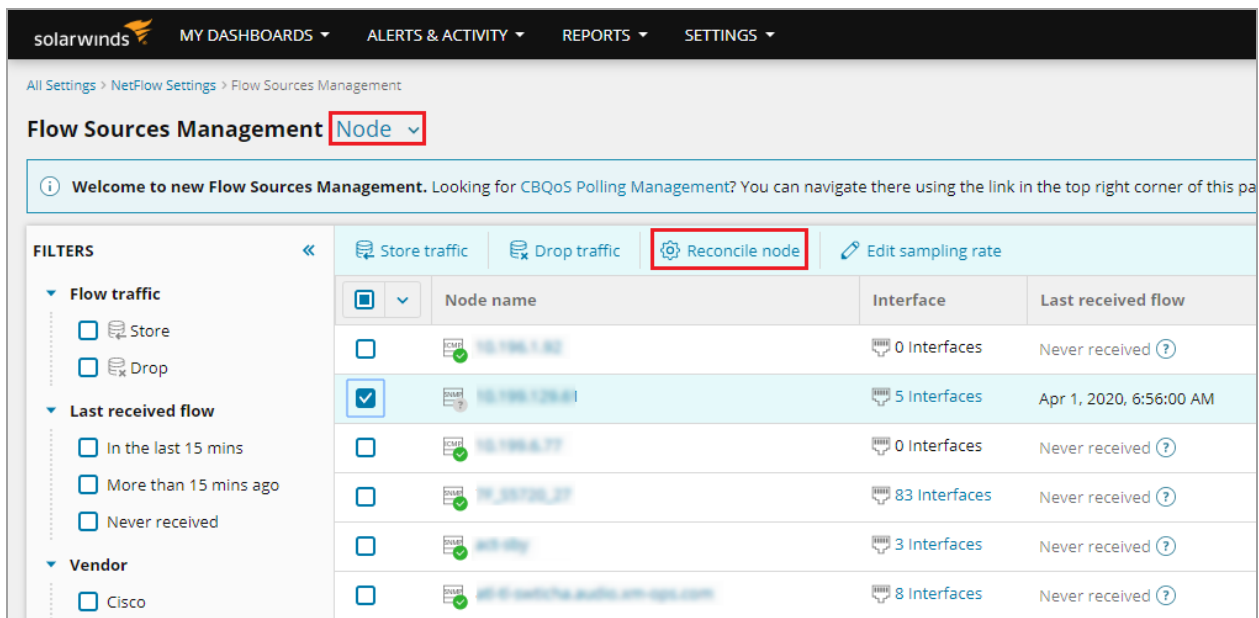
Flow collection is often configured inconsistently across the interfaces of a node. This results in double counted traffic. With NTA, you can reconcile the traffic volumes across multiple interfaces to accurately represent the traffic flowing through a node.

Configure flow collection

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Under Flow Sources Management, click Manually manage flow sources.

i You can also access the Flow Sources Management page by clicking My Dashboards > NetFlow > Flow Sources.

4. In the drop-down menu in the upper left of the page, click Node.
5. Select the node you want to configure, and click Reconcile node.



6. In the pop-up, define the Direction for each interface.

7. Click Apply.

Reconcile node [Redacted] ✕

Search...

Interface name	Traffic last received	Direction
if-1	Apr 1, 2020, 6:56:00 AM	None ▼
if-2	Apr 1, 2020, 6:56:00 AM	Egress Only ▼
if-3	Apr 1, 2020, 6:56:00 AM	Unknown ▼
if-4	Apr 1, 2020, 6:56:00 AM	Both egress & ingress ▼
if-5	Apr 1, 2020, 6:56:00 AM	Ingress Only ▼

Cancel
Apply

You can reconcile only interfaces with InterfaceIndex polled by SolarWinds NPM.

Reconcile node 7F_S5720_27 ✕

Search...

Data not available. Only NPM-managed interfaces with received flow data will be displayed.

Cancel
Apply


Disable flow sources and CBQoS-enabled devices

You can disable NetFlow and CBQoS monitoring through the NTA Settings in the SolarWinds Platform Web Console.


Disable flow sources

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.

3. Click Flow Sources Management.


 You can also access the Flow sources management page by clicking My Dashboards > NetFlow > Flow Sources.

4. Use the Filters to find the devices to display.
5. Locate the interface you want to delete.
6. Select flow sources, and click Drop traffic.

 If you disable NetFlow monitoring for a node or interface, the data stop being collected. However, historical data are kept in the database. Enabling and disabling flow collection can thus result in gaps in NTA graphs.

Disable CBQoS-enabled devices

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Under CBQoS Polling Management, click Manually manage CBQoS polling.

 You can also access the CBQoS polling management page by clicking My Dashboards > NetFlow > CBQoS Polling.

4. Use the Filters to find the devices to display.
5. Locate the interface you want to disable.
6. Select CBQoS sources, and click Disable.

NetFlow collector services

NetFlow Collector Services provide status information about current flow collectors. In case your flow-enabled device configuration requires it, the following procedure resets or adds flow collection ports on which the NTA collector listens for flow data. You can also delete a collector, if necessary.

If you are employing a firewall on your NetFlow collector, all ports on which the NetFlow collector listens for flow data should be listed as firewall exceptions for UDP communications.

By default, NTA listens for flow data on port 2055, but some flow-enabled devices, including some Nortel IPFIX-enabled devices, send flow data on port 9995. For more information about requirements for IPFIX-enabled devices, see [Flow Requirements](#).

Access the management page

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Click NetFlow Collector Services.

Add or reset a collection port

1. Type the new port number in the Collection Port(s) field of the collector that you want to edit.
 - Separate listed ports with a single comma, as in 2055, 9995.
 - A colored icon displays your collector status. Green indicates that the collector can receive flow data, and red indicates that it cannot. Server Name provides the network identification of your collector, and Receiver Status is a verbal statement of collector status.
2. Click Submit.

Delete a collection port

1. Click Delete next to a collection port.
 - If there is the NetFlow service running on the appropriate collector server, the collector together with the default port 2055 will be automatically added again in 15 minutes. For more information, see [Delete collectors in NTA](#).
2. Click Submit.

Types of services in NTA

NTA recognizes the Differentiated Services model of packet delivery prioritization. All flow-enabled devices can be configured to set a Type of Service byte, referred to as the Differentiated Service Code Point (DSCP), on all NetFlow packets that are sent. The DSCP prioritizes NetFlow packet delivery over the flow-enabled devices on your network by assigning each packet both a Differentiated Service class (1, 2, 3, or 4) and a packet-dropping precedence (low, medium, or high). NetFlow packets of the same class are grouped together.

Differentiated Services use the DSCP to communicate per-hop behaviors (PHBs), including Assured Forwarding (AF) and Expedited Forwarding (EF), to the node services that a given packet encounters. PHBs are configured on individual devices when NetFlow is initially enabled. If a given node is overloaded with NetFlow traffic, node services will keep or drop NetFlow packets in accordance with the configured PHB that matches the DSCP in each NetFlow packet. For more information about Differentiated Services, see the appropriate definition on the [Internet Engineering Task Force website](#).

PHBs, corresponding to Types of Services on flow-enabled devices, can be configured with DSCPs in NTA, as shown in the following procedure.

Access the management page

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Under Types of Services, click Configure labels for Types of Service.

This page allows you to configure labels for individual types of service. It provides a list of types of service available in NTA together with the appropriate DiffServCode Point values.

Types of service that are not defined in this list are displayed in NTA widgets as Unknown.

Edit the types of services


1. Click Edit next to a type of service.
2. Edit the name, and click Update on the same line.
 - Individual DiffServ Code Points cannot share multiple Type of Service Names, and individual Type of Service Names cannot share multiple DiffServ Code Points.
3. Click Submit.

Top talker optimization in NTA

In many environments, a majority of network traffic may be attributed to conversations represented by a percentage of all possible monitored flows. Top Talker Optimization allows you to configure NTA to only record those flows that represent conversations requiring the most bandwidth on your network. Recording only those flows representing the most bandwidth-intensive conversations can significantly improve database performance, reduce page load times, and increase reporting speed.

If you are monitoring a large number of NetFlow sources or interfaces, you may see more improved performance by setting this value lower than 95%.

Enabling this option will result in the intentional loss of some data that may otherwise be recorded if this option is set to 100%. However, the data that is lost corresponds to the least bandwidth-intensive conversations. In most environments, these low bandwidth conversations would not have been displayed in most widgets.

 Setting the Top Talker Optimization to 100% means 40 to 100 times higher storage space requirements, and might affect widget rendering performance. Keeping 100% of flows is suitable only for small installations.

Manage top talker optimization

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Scroll down to the Top Talker Optimization section.
4. Enter a value in Capture Flows Based on This Maximum Percentage of Traffic.
5. Click Save.

DNS and NetBIOS resolution in NTA

To meet varied network requirements, NTA provides options for both NetBIOS and DNS resolution of endpoint domain names.

To access the DNS and NetBIOS Resolution settings page, follow the steps below:

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Scroll down to the DNS and NetBIOS Resolution section.

DNS resolution options in NTA

To meet your specific network monitoring needs, NTA provides the following options for configuring DNS resolution:

Resolve and store IPv4 hostnames immediately when a flow record is received

This option continuously resolves domain names for all devices involved in monitored flows. For typically-sized networks, NTA views may load more quickly as resolved domain names are retained, but database query times may increase as your SolarWinds Platform database is continuously queried. This is the default option for new installations.

Top Domains widgets and SolarWinds Platform reports that include DNS names require resolving and storing IPv4 hostnames immediately when a flow record is received.

Resolve IPv4 and IPv6 addresses to DNS hostnames

Resolving IPv4 and IPv6 addresses to DNS hostnames is intended to assist users with recognizing endpoints in internal networks. With this option, an endpoint domain name is only resolved when information about it is actually requested from the SolarWinds Platform database. Database query times may be improved with this option as queries are limited, but the load time for some endpoint-related widgets may increase as NTA waits for domain name resolution.

i Top Domains widgets and SolarWinds Platform reports that include DNS names require immediate resolving and storing of IPv4 hostnames, so they will not display DNS names if you enable the option Resolve IPv4 and IPv6 addresses to DNS hostnames.

How does default DNS resolution work in NTA?

In NTA, host or domain names are stored directly in individual flows. NTA receives a flow from an IP address and waits for the DNS server to resolve it:

- Until the DNS server responds, flows are stored under the IP address.
- When the DNS server resolves the hostname, NTA uses this hostname or domain for flows from this IP address for the next seven days. Then the query is repeated.
- When NTA cannot reach the DNS server, it retries the query in one minute, and keeps repeating the query until the DNS server responds.
- If the DNS server cannot find out the host or domain name, for example if the administrator had not specified it, NTA adds the IP address to the list of unresolved IP addresses. Flows from this IP address are stored in the database under the appropriate IP address. NTA repeats the query to the DNS server to resolve the hostname in two days.

You can also configure the interval between DNS lookups. NTA performs regular DNS lookups on all monitored devices. By default, if the domain of a monitored device resolves successfully, NTA will not attempt another DNS lookup on the same device for seven days. If the domain name of a monitored device does not resolve successfully, by default, the SolarWinds Platform will attempt to resolve the same device again in two days.

Host and domain names in SolarWinds NTA

When flows are received from an IP address, NTA asks a DNS server to resolve the appropriate hostname or domain. This affects the way NTA filters your data, groups items in endpoint-related widgets, and displays host and domain names in the SolarWinds Platform Web Console.

For more details, see [DNS and NetBIOS resolution in NTA](#).

Filtering

Filtering in NTA is based on hostnames. This way, filtering by hostnames returns the same results as filtering via IP addresses.

Endpoint-related widgets

NTA groups items in endpoint-related widgets by the hostname.

Host and domain names in NTA widgets

NTA does not apply changes of hostname or domain name to your historical data.

If a hostname or domain name changes, you can see flows from the same machine as two items: first under the old name and after the change, under the new name. For example, Top XX widgets show data split into more items, based on the appropriate resolved name.

Enable NetBIOS resolution of endpoints in NTA

For networks where NetBIOS is the preferred naming convention, NTA provides the option to resolve endpoint domain names using NetBIOS.

Enabling NetBIOS resolution does not automatically disable DNS resolution of the same devices. For more information about configuring DNS resolution, see [DNS resolution in NTA](#).

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Under DNS and NetBIOS Resolution, select Enable NetBIOS Resolution of Endpoints.
4. Click Save.

DNS resolution in NTA

DNS resolution is done on the main polling engine. SolarWinds NTA does not support resolving DNS on additional polling engines.

Resolve and store IPv4 hostnames immediately when a flow record is received

Domain names are resolved continuously for all devices involved in flow monitoring. This is the default for new installations.

If you select Resolve and store IPv4 hostnames immediately when a flow record is received, define:

- Default Number of Days to Wait Until Next DNS Lookup to set the interval on which endpoint domain names are refreshed in the SolarWinds Platform database.
- Default Number of Days to Wait Until Next DNS Lookup for Unresolved IP Addresses to set the interval on which NTA attempts to resolve domain names for unresolved endpoints in the SolarWinds Platform database.

Views may load more quickly because resolved domain names are retained, but database query times may increase as your database is continuously queried.

Top Domains widgets and SolarWinds Platform reports that include DNS names require resolving and storing IPv4 hostnames immediately when a flow record is received. NTA does not support internationalized domain names which include special characters, symbols, and non-English letters.

Resolve IPv4 and IPv6 addresses to DNS hostnames

DNS is resolved only when requested from the database.

Resolving IPv4 and IPv6 addresses to DNS hostnames is intended to assist users with larger networks. With this option, an endpoint domain name is only resolved when information about it is actually requested from the SolarWinds Platform database. Database query times may improve as queries are limited, but the load time for some endpoint-related widgets may increase as NTA waits for domain name resolution.

i Top Domains widgets and SolarWinds Platform reports that include DNS names require immediate resolving and storing of IPv4 hostnames. They will not display DNS names if Resolve IPv4 and IPv6 addresses to DNS hostnames is selected.

IP address processing

By default for new installations, NTA conserves your processing and database resources by limiting the amount of time spent attempting to process the expired IP addresses of endpoints in monitored flow conversations.

NTA is configured to spend no more than 15 minutes attempting to process any expired IP addresses. To conserve your processing and database resources, SolarWinds recommends that you maintain a reasonable time limit.

1. Under Maximum Time Spent to Process IP Addresses, select one of the following:
 - Custom Number of Minutes, and then enter a value to edit the processing time period.
 - Never Stop Processing Expired IP Addresses to remove the processing limit and delete flow records corresponding to expired IP addresses as they expire.
2. Click Save.

SolarWinds recommends against removing the time limit for processing expired IP addresses, as continuously deleting expired IP addresses may negatively affect performance. By default, NTA sets a maximum period of 60 minutes for processing expired IP addresses to ensure that excessive processing resources are not drawn away from monitoring your network.

Database settings in NTA

Due to the great volume of data that is produced by devices on your network, NTA databases may quickly become unmanageable unless you schedule regular maintenance.

The Database Settings grouping allows you to configure maintenance for both databases used by NTA.

SolarWinds Platform database

This database stores CBQoS data and node data relevant for NPM. NTA uses data stored in this database to display appropriate node details and data concerning CBQoS policies defined on your devices.

NTA SQL Flow Storage database

This is a SQL database that stores flow data using columnstore indexes. It brings high performance and customizable retention of raw data without aggregation. It stores data with one-minute granularity for the whole retention period (30 days by default) and enables you to see your flow data in more detail.

Access database settings


1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Scroll down to the Database Settings section.

NTA Flow Storage database settings

Maintaining the NTA Flow Storage database requires setting a retention period that corresponds with the amount of data you need to keep and the free space available on the NTA Flow Storage database disk.


Retention period

Retention period specifies the time for which flow data are stored in the database until they expire and are permanently deleted.

 The minimum retention period is three days. The default retention period is 30 days.

Set retention period

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. In Retention Period, enter the number of days after which flow data will be deleted.

 Minimum retention period is 3 days.

4. Select a frequency in the Delete Expired Data list.
5. Click Save.


SolarWinds Platform database maintenance

The SolarWinds Platform database stores CBQoS data and node data relevant for NPM. NTA uses data stored in the SolarWinds Platform database to display appropriate node details data and data concerning CBQoS policies defined on your devices.

Because of the growing volume of data produced by your devices, the database may quickly become unmanageable unless you schedule regular maintenance. The SolarWinds Platform database maintenance includes compressing the database and log files.

For more information about the database maintenance application packaged with NPM, see [Running database maintenance](#).

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Scroll down to the Database Settings section.
4. Select Enable Database Maintenance.
5. Provide a time when Maintenance Is Executed.

 Schedule the database maintenance for an off-peak network usage window to minimize any potential disruption of required monitoring.

6. Select a frequency in the Compress Database and Log Files list.
7. Click Save.

NTA Flow Storage database maintenance

Retention period

Maintaining the NTA Flow Storage database requires setting a retention period that corresponds with the amount of data you need to keep and the free disk space available on your NTA Flow Storage database disk.

Retention Period specifies the time for which flow data are stored in the database until they expire and are permanently deleted.

To optimize the retention period for your NTA Flow Storage database, collect data for a few days. You should then have an idea of the volume of data your network produces with NetFlow enabled. Consider the space taken up by the database, and then adjust the retention period accordingly.

NTA SQL Flow Storage database backups

Backups protect you from data loss caused by hardware failure, viruses, accidental deletion, or natural disasters.

Backups maintain database size and create restoration points for data recovery.

With NTA, you can create and restore backups of your database. For more information on backing up the NTA SQL Flow Storage database, see [Back up and restore the database for SolarWinds Platform products](#).

Charting and graphing settings in NTA

The Charting and Graphing Settings section of the NTA Settings view gives you the ability to configure NTA options regarding the presentation of historical information in web console views and widgets.

Percentage type for Top XX lists

Percentage type for Top XX lists describes how NTA calculates percentages in Top XX widgets.

Top XX list widget percentages in NTA

Top XX list widgets may be configured to show any number of items, listed in either absolute or relative terms of overall traffic percentage. Absolute percentages are calculated for each item based on all monitored items. Relative percentages for each item are calculated in terms of the total number of items displayed in the selected widget.

By default, pie charts are configured to show some, but not all traffic. You can see the rest of the data not included in the top XX items in the Remaining Traffic row in the legend.

Example

A given node, HOME, is communicating with other endpoints: 1, 2, 3, and 4. The following table details the two percentage types calculated and displayed for both Top 4 Endpoints and Top 3 Endpoints widgets.

Endpoint	Actual Amount of Traffic	% of Total Actual Traffic	Absolute Percentage		Relative Percentage	
			Top 4	Top 3	Top 4	Top 3
Hostname 1	4 MB	40%	40 %	40 %	4/8.5 MB = 47%	4/8 MB = 50%
Hostname 2	3 MB	30%	30 %	30 %	3/8.5 MB = 35.3%	3/8 MB = 37.5%
Hostname 3	1 MB	10%	10 %	10 %	1/8.5 MB = 11.7%	1/8 MB = 12.5%
Hostname 4	.5 MB	5%	5%	Not Shown	0.5/8.5 MB = 5.9%	Not Shown
Remaining traffic (in MB and %)	1.5 MB	15%	15%	20%	Not Shown (Remaining Traffic shown only in Absolute values.)	Not Shown (Remaining Traffic shown only in Absolute values.)
Total traffic shown in widget (in MB and %)	10 MB	100%	100% (10 MB includes remaining traffic)	100% (10 MB includes remaining traffic)	100% (8.5 MB includes just top 4 entries)	100% (8 MB includes just top 3 entries)

Set the Unit type for area charts in NTA

Settings configured on the NTA Settings view apply globally to all NTA area charts.

Rate (kbps)

Provides the actual rate of data transfer, in kilobytes per second, corresponding to items displayed in a Top XX widget.

% of interface speed

Displays the widget data as a percentage of the nominal total bandwidth of the selected interface. This option only displays when you are viewing ingress and egress data through a selected interface.

% of total traffic

Displays the widget data as a percentage of the total traffic measured through the selected device.

Data transferred per time interval

Displays the amount of data corresponding to listed items transferred over a designated period of time.

% of class utilization

Creates a chart displaying what percentage of the limit set for the appropriate class is used up by the interface or node. Selecting this option sets the chart style to line chart.

This option requires that you have set limits for individual classes on appropriate devices and is available only for the following CBQoS widgets on Interface Details Views:

- CBQoS Pre-Policy Class Map
- CBQoS Post-Policy Class Map
- CBQoS Drops

For example, you have allocated a 10 Mbps bandwidth for a class on a device. This option displays a real percentage how the bandwidth is used.


Area chart units can also be configured on a per widget basis by clicking Edit in the widget header and selecting the appropriate data units. Additionally, area chart display units may be configured for the duration of the current web console user session by selecting appropriate data units from the Data Units menu in the header of any NTA area chart widget.

Default time periods for widgets in NTA

You can globally set the default time period for all SolarWinds Platform Web Console widgets in the Charting and Graphing Settings section of NTA Settings.

- The default time period for NTA widgets placed on Detail views is Last 15 Minutes.
- The default time period for NTA widgets placed on Summary views is Last 1 Hour(s).
- The default time period for NTA search is Last 15 Minutes.

High default widget time periods may significantly affect load times for NTA views.

 You can also configure the time period for any NTA widget by clicking Edit in the header of the widget.

Default chart style for widgets in NTA

By default, all widgets in detail views present chart data in an area chart and SolarWinds Platform summary views present chart data in a pie chart.

You can configure the chart style for any widget individually.

Pie charts present a flat view of your data. Area charts present a historical view of your data as represented by areas calculated at past polling times.

Default flow direction for widgets in NTA

By default, all widgets in node detail views and interface detail views present data for ingress flows and SolarWinds Platform summary views present data for both flow directions.

You can configure the flow direction for any widget individually.

Enable automatic page refresh in NTA

The refresh rate for NTA views is configurable. Select this option, and then provide the refresh interval in minutes.

Automatically refresh widgets affected by running updates

Define how often update progress should be refreshed. Once the update is completed, appropriate widgets are refreshed.

By default, the progress message is refreshed every one minute.

Optimize performance in NTA

Due to the volume of data it collects and processes, NTA constantly makes demands on the widgets of both the SolarWinds Platform server and its database.

Maintaining your SolarWinds Platform, SQL and NTA Flow Storage database servers on separate physical machines is a fundamental requirement in scaling the NTA implementation. However, even with this setup, the volume of collected and processed NetFlow data calls for other performance optimizing steps.

Follow the recommendations and steps in these sections to optimize performance of your NTA implementation. Due to differences in network environments, results of these optimizations will vary from installation to installation:

- Configure DNS resolution to resolve IPv4 and IPv6 addresses to DNS hostnames instead of immediately. For more information, see [Configure resolving IPv4 and IPv6 addresses to DNS hostnames in NTA](#).
- Capture only the flows required to represent the top talkers on your network. For more information, see [Limit flow collections to top talkers](#).
- Limit the time period for storing flow data in your database. For more information, see [NTA Flow Storage database maintenance](#).
- If you do not need to store traffic data on unmonitored ports, you can disable data retention for unmonitored ports. For more information, see [Configure data retention for flows on unmonitored ports](#).

Configure resolving IPv4 and IPv6 addresses to DNS hostnames in NTA

Disabling the option `Resolve and store IPv4 hostnames immediately when a flow record is received` when the option `Resolve IPv4 and IPv6 addresses to DNS hostnames` is enabled decreases the amount of database memory used to store DNS information and the read and write load on your SQL server associated with domain name resolution.

With the option `Resolve IPv4 and IPv6 addresses to DNS hostnames` enabled and the option `Resolve and store IPv4 hostnames immediately when a flow record is received` disabled, domain names are only resolved for device IP addresses that are actually displayed in SolarWinds NTA widgets. Since they require DNS resolution with storing to calculate statistics, Top XX IPv4 Domains, Top XX IPv4 Traffic Destinations by Domain (report), and Top XX IPv4 Traffic Sources by Domain (report) become unavailable with this setting.

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Scroll to the DNS and NetBIOS Resolution section.
4. Make sure the option `Resolve and store IPv4 hostnames immediately when a flow record is received` is unselected.
5. Make sure the option `Resolve IPv4 and IPv6 addresses to DNS hostnames` is selected.
6. Click Save.

Limit flow collections to top talkers

Up to 95% of all traffic on many networks can be captured with as little as 4% of the total amount of flow data received from monitored flow sources. If you are primarily using NTA to determine the top talkers on your network and you are currently storing 100% of the data received from monitored flow sources, you are probably storing a large amount of unnecessary data. As a result, your database may be unnecessarily large and the load times for NTA widgets and reports may be unnecessarily long. In this case, restricting flow data storage to only those flows required to represent the top bandwidth users on your network can significantly improve the performance of NTA.

The Top Talker Optimization setting, by default, captures only those flows representing the top 95% of total network traffic. By changing this setting you are permanently limiting the amount of data that is available for a historical analysis of traffic flows.

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Under Top Talker Optimization, edit Capture Flows Based on This Maximum Percentage of Traffic.
4. Click Save.

View NTA data in the SolarWinds Platform Web Console

Once you have configured and enabled a NetFlow source, you can view the various types of NetFlow statistics that it records in the SolarWinds Platform Web Console. The statistics are provided as widgets grouped to form individual views.

Views

A view is a web page showing information about your network and the traffic going through individual nodes and interfaces. A view consists of widgets. You can customize which widgets you want to have on a view.

NTA provides two basic types of views:

Summary views

Display traffic details on all nodes and interfaces managed by NTA, such as top applications, conversations, and endpoints. You can access your summary views either in the My Dashboards > NetFlow views or by clicking an item in another view. For example, clicking on an application in the Top 5 Applications Summary view displays a summary view covering the use of the selected application in all nodes monitored in NTA.

Detail views

Display traffic information on individual objects in your network, such as interface details, node details, and application details. You can access your detail views by opening a summary view, and then clicking on the object whose details you want to see.

Widgets

A widget is a building block of your views. It displays on your views as a box and provides information about different aspects of traffic monitoring, usually in a chart and a table. Some widgets are meant to be used on summary views, some are suitable for detail views, and some can be useful on both view types. The information shown pertains to either all devices NTA monitors (if used on a summary view) or to the selected object (if used on a detail view for a node, interface, conversation, application, CBQoS class, or other object).

Edit widgets in NTA

Widgets in the SolarWinds Platform Web Console are edited on the Edit Resource page. The options available depend on individual widgets.

1. Click Edit in the header of the widget.
2. Customize the available options:
 - Title
 - Subtitle
 - Maximum Number of Items to Display
 - Chart customization options. For more information, see [Customize charts for all users in NTA](#).
3. Click Submit.

Charts in NTA

NTA charts display pie chart or area chart summaries of widget-related data, enabling a more detailed view of widget. You can create different types of area charts, including stack area, stack spline area, stack line, line, spline, and bar.

Charts offer tooltips with current values, as well as the ability to disable data series and to zoom in on data. They also have features you can click offering detailed widget information and editing capabilities.

Chart display limitations

- SolarWinds Platform views can display up to 100 widgets.
- Pie charts can display up to 100 items.
- Area charts can display up to 10 items, with the rest of the series visible in the legend.

Chart types

- [Pie charts in NTA](#)
- [Area charts in NTA](#)

Chart customization options

- Global settings defining how displayed data are calculated and setting default options. For more information, see [Charting and graphing settings in NTA](#).

- [Customize charts for the current session in NTA](#)
- [Customize charts for all users in NTA](#)

Data granularity shown by default

NTA Flow Storage database supports saving flow data without compression and with one-minute granularity. However, charts display data in such detail only for time periods up to five hours.

Data are summarized in the following way:

- For time periods up to five hours, charts display data with one-minute granularity. Data are not summarized.
- For time periods of five hours up to 48 hours, charts display data with 15-minute granularity.
- For time periods of 48 hours up to seven days, charts display data with one-hour granularity.
- For time periods longer than seven days, charts display data with six-hour granularity.

View flow data for longer time periods with one-minute granularity

To see flow data with one-minute granularity, set the time period displayed by the view to up to five hours, focusing on the period you are interested in most.

For more information about setting time period for views, see [Edit time settings for NTA views](#).

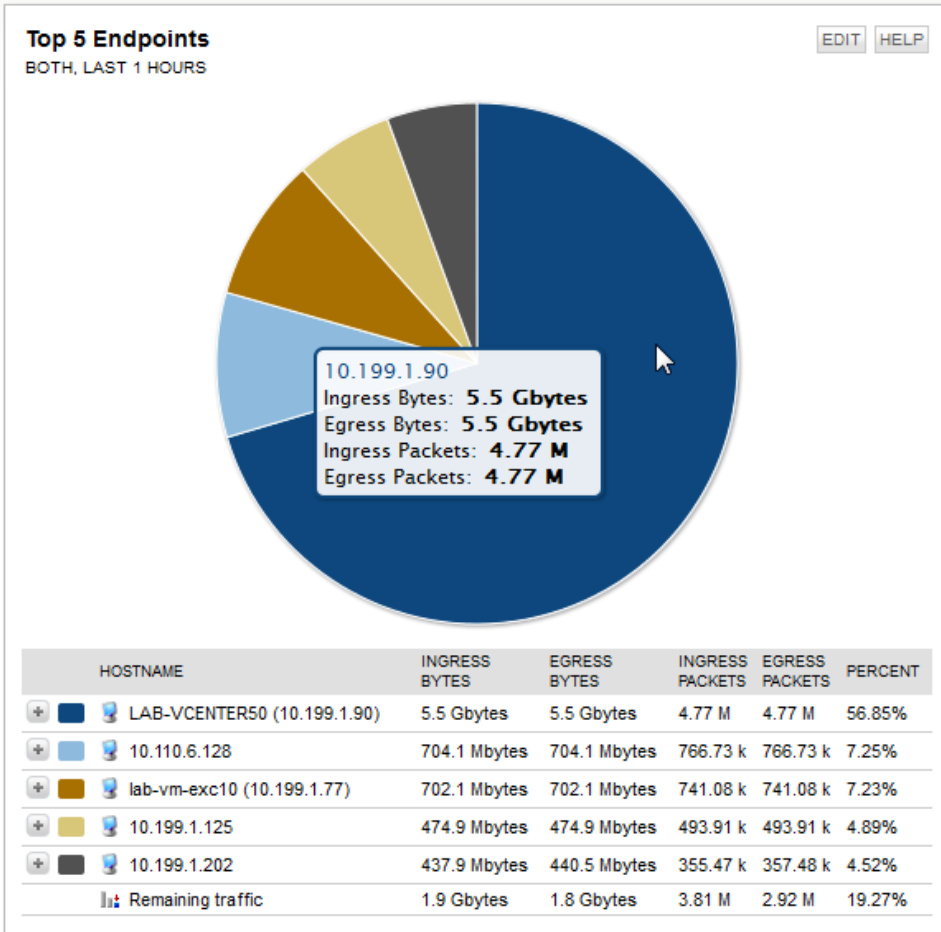
Pie charts in NTA

The pie charts in this section show the Top 5 Endpoints widget, and use absolute percentage calculations. For more information about chart settings, see [Charting and graphing settings in NTA](#).

NTA gives each item its own piece of pie, depending on your chart settings. If more items exist than what is configured to display, NTA creates a category in the legend of the pie chart called Remaining traffic, which is not displayed in chart. If fewer items exist than what the chart is configured to display, the chart shows only those widgets that exist.

Example

The following chart divides traffic among the top five top endpoints. The largest traffic flow is from LAB VCENTER50 (10.199.1.90) and is 56.85% of the total traffic flow. The next four highest endpoints' traffic flows are 7.25%, 7.23%, 4.89%, and 4.52% of the total traffic flow. NTA labels all other endpoint flow traffic as Remaining traffic, which is 19.27% of the total traffic flow.



Pointing to the chart provides tool tips on the details for that portion of the chart. For example, the pie chart above shows tool tip details for LAB VCENTER50 (10.199.1.90).

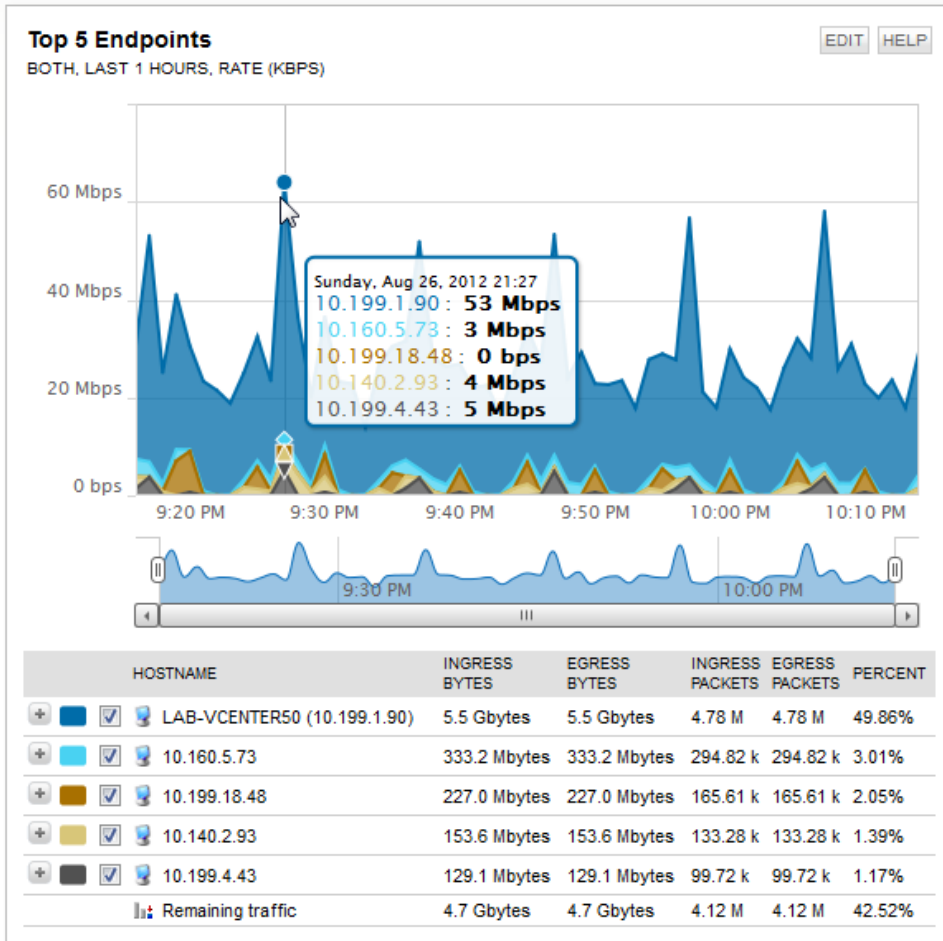
Area charts in NTA

Area charts are the default charts for all detail views. They display resources within a defined traffic level and time frame. They provide a more comprehensive view of traffic and bandwidth usage data than pie charts, so area charts always include a one-to-one relationship of table-to-chart information.

Like pie charts, if more items exist than what is configured to display, NTA creates a category in the legend of the area chart called Remaining traffic. If fewer items exist than what the chart is configured to display, the chart shows only those resources that exist.

Display data for a specific time point

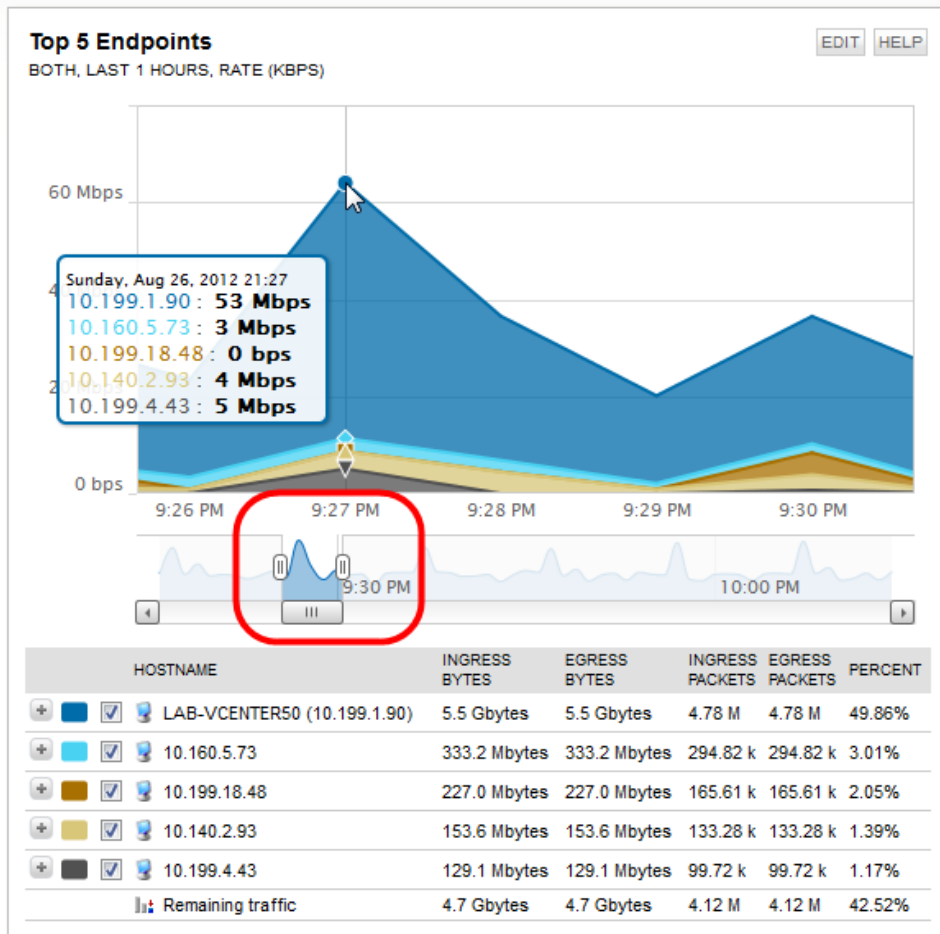
To display exact transmission details for a specific point in the time, point your mouse to a specific point on an area chart. The detailed information displays within the chart and in a tool tip.



The Top 5 Endpoints data shown the area chart tell us that conversations involving the LAB-VCENTER50 (10.199.1.90) endpoint generated substantially more traffic than the other top 4 endpoints.

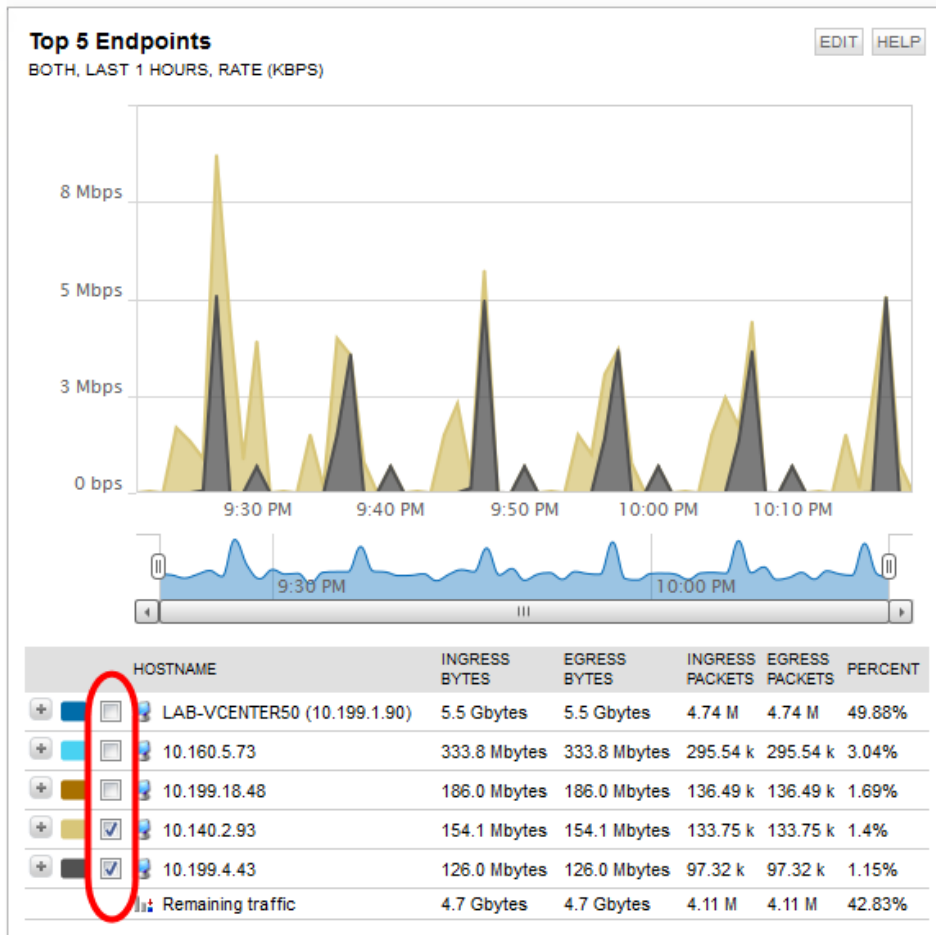
Zoom in to see a specified time period

For a more detailed look at resource use, locate the slider tool beneath the area chart. Move it right or left to display an in-depth view of a selected portion of the area chart. This feature allows you to visually pinpoint and compare endpoint traffic flow data using an exact time.



Hide or show certain items

To display only certain endpoints out of those already selected for review, for example, the bottom two out of the top five, clear the boxes for top three endpoints.



The top three endpoints still display in the legend, but do not display in the table, making for easy comparisons between the bottom two endpoints. You can also use the slider below the graph for a more detailed view of the endpoints, in the same way as described above.

Customize charts for the current session in NTA

All users who can view widgets can also customize the charts for the duration of the current session, directly in the appropriate view or widget.

For the current session, you can customize:

- Time and flow direction settings for all appropriate widgets in a view
- Zoom and displayed items in area charts

Once you leave the view with the widget, your current settings will be lost and replaced by settings for the widget.

Customize time and flow direction settings for the current session

You can customize the time and flow direction settings for all appropriate widgets on a view.

However, widgets with their individual time periods set in their Edit pages are not subject to this time period control.

For more information about customizing time settings, see [Edit time settings for NTA views](#).

For more information about customizing flow direction settings, see [Edit flow direction in NTA views](#).

Area charts: zoom and show selected items only

Area charts support the following session-related options:

- Beneath area charts, you can see a slider tool. Move the slider to display an in-depth view of the selected part of the chart to get a detailed view of the traffic at a certain time point.
- Select or clear the boxes in the table below an interactive area chart, to display only the items you want to see at the moment.

For more information on customizing SolarWinds Platform views, see [Add widgets to SolarWinds Platform views, or classic dashboards](#).

Customize charts for all users in NTA

1. Click Edit in the header of the widget.
2. On the Edit Resource page, specify the Title and Subtitle.
3. Select the Chart Style you want to use: Area Chart or Pie Chart.
4. Select Use Chart Style Default for View to use the style which is set as default for the widget when used on the appropriate view.
5. Edit the Maximum Number of Items to Display.
6. Define a Time Period.
 - If you want the widget to inherit the setting from the view on which it is placed, select Use Time Period from Current View. This is the default.
 - If you want to name a time period, select Named Time Period, and select a time period.
 - If you want a relative time period, select Relative Time Period, enter a number, and select a

unit of duration.

- If you want to name an absolute time period, select Absolute Time Period, and set the date and time parameters.

7. Select the widget style:

- Select Chart to display both the chart and the legend in the widget.
- Select No Chart to view only the legend.

8. Select the Flow Direction.

9. If selected the Area Chart, select an Area Type:

- Stack Area is an area chart where multiple series of data are stacked vertically. If there is only one series in your chart, the stacked area chart displays the same as an area chart.
- Stack Spline Area is an area chart that stacks multiple series of data vertically and plots a fitted curve through all data points in the series.
- Stack Line is a Stack Area chart that does not fill the areas defined by each stacked series. Data series are stacked at each point of measurement marked on the x-axis.
- Line Chart is a chart created using lines to connect series data points. All series use the x-axis as a common baseline .
- Spline plots a fitted curve through all series data points in a line chart.
- Bar Chart assigns each data point its own column and plots maximums against the vertical scale.

10. If selected the Area Chart, select a Data Unit:

- Rate (Kbps) creates a chart displaying historical traffic rate data for selected flow-enabled nodes and interfaces.
- % of Interface Speed is only available for widgets presenting interface traffic data. This option creates a chart showing how bandwidth is allocated across the elements listed in the widget.
- % of Total Traffic creates a chart showing how the total traffic over the selected node or interface is distributed across the elements listed in the widget. This is the default data unit type.
- Data Transferred Per Time Interval creates a chart displaying the actual amount of data transferred over the selected node or interface. Data volume is measured over successive time intervals.
- % of Class Utilization creates a chart displaying what percentage of the limit set for the appropriate class is used up by the interface or node. This option requires that you have set limits for individual classes on appropriate devices and is available only for the following CBQoS widgets on Interface Details Views:

- CBQoS Pre-Policy Class Map
- CBQoS Post-Policy Class Map
- CBQoS Drops

Selecting this option sets the chart style to line chart.

11. If you want to add a title or subtitle for the chart, expand Advanced and enter a Chart Title and Chart Subtitle.
12. Click Submit.

Enable the NetFlow Traffic Analyzer Summary view

If the NetFlow Web Console does not display the NetFlow Traffic Analyzer Summary view by default, use the following steps to enable it:

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under User Accounts, click Manage Accounts.
3. Select Admin, and then click Edit.
4. Under Default Menu Bar and Views, locate NetFlow Tab Menu Bar.
5. Select NTA_TabMenu.
6. Click Submit at the bottom of the page.
7. Click My Dashboards > NetFlow to display the NetFlow Traffic Analyzer Summary view.

Create custom views with the Flow Navigator

Using the Flow Navigator, you can create custom traffic views directly from any NetFlow view.

These custom filters allow you to view specific statistics about your entire network and its devices without having to navigate through the web console by single-device views.

You can configure your custom traffic view to include devices, applications, time periods, and more from one configuration pane.

Create a custom NetFlow traffic view with the Flow Navigator

1. Click My Dashboards > NetFlow > NTA Summary.
2. Click Flow Navigator on the left edge of the summary view. The Flow Navigator is available on any default NTA view.

3. Specify the View Type.
 - a. If you want a filtered view of your entire network, click Summary, and select a summary view.
 - b. If you want a filtered view of traffic passing through a specific node and interface, click Detail, and select a Detail View Type.
4. Select the Time Period over which you want to view traffic data:
 - Select Named Time Period, and select a time period.
 - Select Relative Time Period, and provide a number appropriate for the selected time units. The relative time period is measured with respect to the time at which the configured view is loaded.
 - Select Absolute Time Period, and provide the start and end time periods.
5. Select a Flow Direction.
 - Select Both to include ingress and egress traffic in the calculations NTA makes.
 - Select Ingress to include only ingress traffic in the calculations NTA makes.
 - Select Egress to include only egress traffic in the calculations NTA makes.
6. You can further limit the view by including or excluding some of the following items:

IP Version

To only display network traffic related to IPv4 or IPv6 data, or to display data for both IPv4 and IPv6 traffic, expand IP Version, and select the appropriate filter. Click Add Filter.

Applications

If you want to limit your view to only display network traffic to and from applications, or to exclude traffic to and from them, expand Applications, and then complete the following steps:

- a. If you want to include traffic from specified applications, select Include.
- b. If you want to exclude traffic from specified applications, select Exclude.
- c. Enter the name of an appropriate application or the appropriate port number.
- d. If you want to include or exclude another application, click Add Filter, and then enter the name of the appropriate application.

Autonomous Systems

To only display network traffic to and from autonomous systems, or to exclude traffic to and from certain autonomous systems, expand Autonomous Systems, and enter the ID of an appropriate autonomous network. Click Add Filter.

Autonomous Systems Conversations

To only display network traffic related to specific autonomous system conversations, or to exclude traffic to and from them, expand Autonomous System Conversations, and enter IDs of autonomous systems involved in conversations. Click Add Filter.

Conversations

To only display network traffic related to specific conversations between two endpoints, or to exclude traffic to and from them, expand Conversations and enter the endpoints involved in the conversation. Click Add Filter.

Countries

To only display network traffic related to specific countries, or to exclude traffic to and from them, expand Countries, and select a country to Include or Exclude.

To select multiple countries, select each one and click Add Filter to apply each selection.

Domains

To only display network traffic related to specific domains, or to exclude traffic to and from them, expand Domains, and enter the domain name you want to Include or Exclude.

- To add multiple domains, enter a name and then click Add Filter to apply your selection after each entry.
- If a domain name is not resolved and saved in NTA, you cannot use it in the Flow Navigator. In this case, NTA will prompt you for a valid name. For more information about resolving domain names, see [Host and domain names in SolarWinds NTA](#)

Endpoints

To only display network traffic related to specific endpoints, or to exclude traffic to and from them, expand Endpoints:

- a. Enter the IP address or hostname of an appropriate endpoint to Include or Exclude.
- b. If you want to include or exclude traffic from a specified subnet, enter the appropriate range of IP addresses.

You can either type in the range, for example `192.168.1.0-192.168.1.255`, or use the CIDR notation, for example `192.168.1.0/24`.

- c. If you want to include or exclude another endpoint, click Add Filter, and then enter the name of an appropriate endpoint.

IP Address Groups

To only display network traffic related to specific IP address groups, or to exclude traffic to and from them, expand IP Address Groups, and then complete the following steps:

- a. Enter an appropriate IP address group.

Though an IP Address Group is disabled, it may continue to appear in the list. As a workaround, rename the group before disabling it. For example, for an IP Address Group called `PrimaryLAN`, you might add `_DISABLED` to the end. An entry called `PrimaryLAN_DISABLED` indicates that the group is inactive.

- b. If you want to include or exclude another IP address group, click Add Filter, and then enter the name of an appropriate IP address group.

IP Address Group Conversations

To only display network traffic related to conversations between specified IP address groups, or to exclude traffic to and from them, expand IP Address Group Conversations:

- a. Select the IP address groups involved in conversations that you want to include or exclude.
- b. If you want to include or exclude another IP address group conversation, click Add Filter, and then enter the appropriate conversation IP address groups.

Protocols

To only display network traffic using specific protocols, expand Protocols and select the protocol to Include or Exclude.

If you want to include or exclude another protocol, click Add Filter, and then select another protocol.

Types of Service

To only display network traffic using specific service types, expand Types of Service and select an appropriate type of service to Include or Exclude.

If you want to include or exclude another type of service, click Add Filter, and then select another type of service.

7. Click Submit.
8. If you want to save your custom filtered view for future reference, click Save Filtered View to Menu Bar.

Add NetFlow widgets to web console views

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Views, click Manage Dashboards/Views.
3. In the list of views, select a NetFlow view to which you want to add a NetFlow-specific widget, and click Edit.
4. Click + next to the column in which you want the new widget to be placed.
5. In the Group By list, select Classic category.
6. Select a NetFlow entry in the list.
7. Select one or more widgets, and then click Add Selected Resources.
8. Use the arrow buttons to move the widgets listed in the column into the order you want displayed in the SolarWinds Platform Web Console.
9. Click Done.

For more information about using your customized view as a default view assigned to a user, see [Editing User Accounts](#) in the SolarWinds Network Performance Monitor Administrator Guide .

To add your customized view to a menu bar as a custom item, see [Customizing Web Console Menu Bars](#) in the SolarWinds Network Performance Monitor Administrator Guide.

Add endpoint-centric widgets to NTA views

An endpoint-centric widget is a special type of Top XX widget that you can place on either Node Details or Interface Details views.

To understand the difference between a Top XX widget and its endpoint-centric variant, consider this example: If you place Top XX Conversations on either the Node Details or Interface Details view, you will see data on conversations responsible for the most traffic passing through the selected node or interface over the set period of time. However, if you place Top XX Conversations (Endpoint Centric) on either of those views, you will see data on the conversations the selected node or interface originated or terminated.

If your user account has limitations, you might not see all the expected traffic because of the limitations. For more information, see [Creating Account Limitations](#) in the SolarWinds Network Performance Monitor Administrator Guide.

Add an endpoint-centric widget

1. Click My Dashboards > Home > Summary.
2. Under All Nodes, click a node. If nodes are grouped, drill down to the relevant group.
3. Click Customize Page > Add tab.
4. Click + next to the column in which you want the new widget to be placed.
5. In the Group By list, select Classic category.
6. Select NetFlow Endpoint-Centric Resources in the list.
7. Select one or more widgets, and then click Add Selected Resources.
8. Use the arrow buttons to move the widgets listed in the column into the order you want displayed in the SolarWinds Platform Web Console.
9. Click Done.

Edit time settings for NTA views

You can customize the time shown by all appropriate widgets on a view. These settings are limited to the current session. Once you leave the view, all widgets will show default time settings.

Widgets with their individual time periods set in their Edit pages are not subject to this time period control.

The time period shown by widgets will always be shifted into the past by two minutes compared to the current time settings. There is a two-minute delay in loading data into the database. For example, if you set Relative Time Period to Last 5 Minutes at 11:02, widgets display data collected from 10:55 to 11:00.

Change the time period shown by all widgets in the view for the current session

1. Click next to the time period setting below the view name.
2. Define the time period in one of the following ways:
 - Select Named Time Period, and then select a time period.
 - Select Relative Time Period, and then enter a time value and the appropriate unit.
 - Select Absolute Time Period, and then use the date picker and time selector to define a time period.
3. Click Submit.

Edit flow direction in NTA views

You can customize the flow direction shown by all appropriate widgets on a view. These settings are limited to the current session. Once you leave the view, all widgets will show default flow direction settings.

Change flow direction in a view

1. Click next to the flow direction setting below the view name.
2. Select a flow direction: Both, Ingress, or Egress. The Select Flow Direction menu only provides the options that can be applied to the current view.
3. Click Submit.

Delete an NTA filtered view

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Customize Navigation & Look, click Customize Menu Bars.
3. Under Menu Bar: NTA_TabMenu, click Edit.
4. Click the trash icon next to the custom menu item.
5. Click Submit.

View Palo Alto Security Policies in the Top XX Conversations on Policy widget

NTA extends visibility of the NCM Palo Alto Security Policy Details page with NTA conversation traffic.

If you install SolarWinds Network Configuration Manager (NCM) together with SolarWinds NetFlow Traffic Analyzer (NTA), the Top XX Conversations on Policy widget displays traffic conversations that are affected by the selected policy. When a policy changes, use this widget to see how the change affects network traffic.

View the Top XX Conversations on Policy widget

1. In the SolarWinds Platform Web Console, click My Dashboards > Network Configuration > Config Summary.

2. In the NCM Node List, click a Palo Alto device.

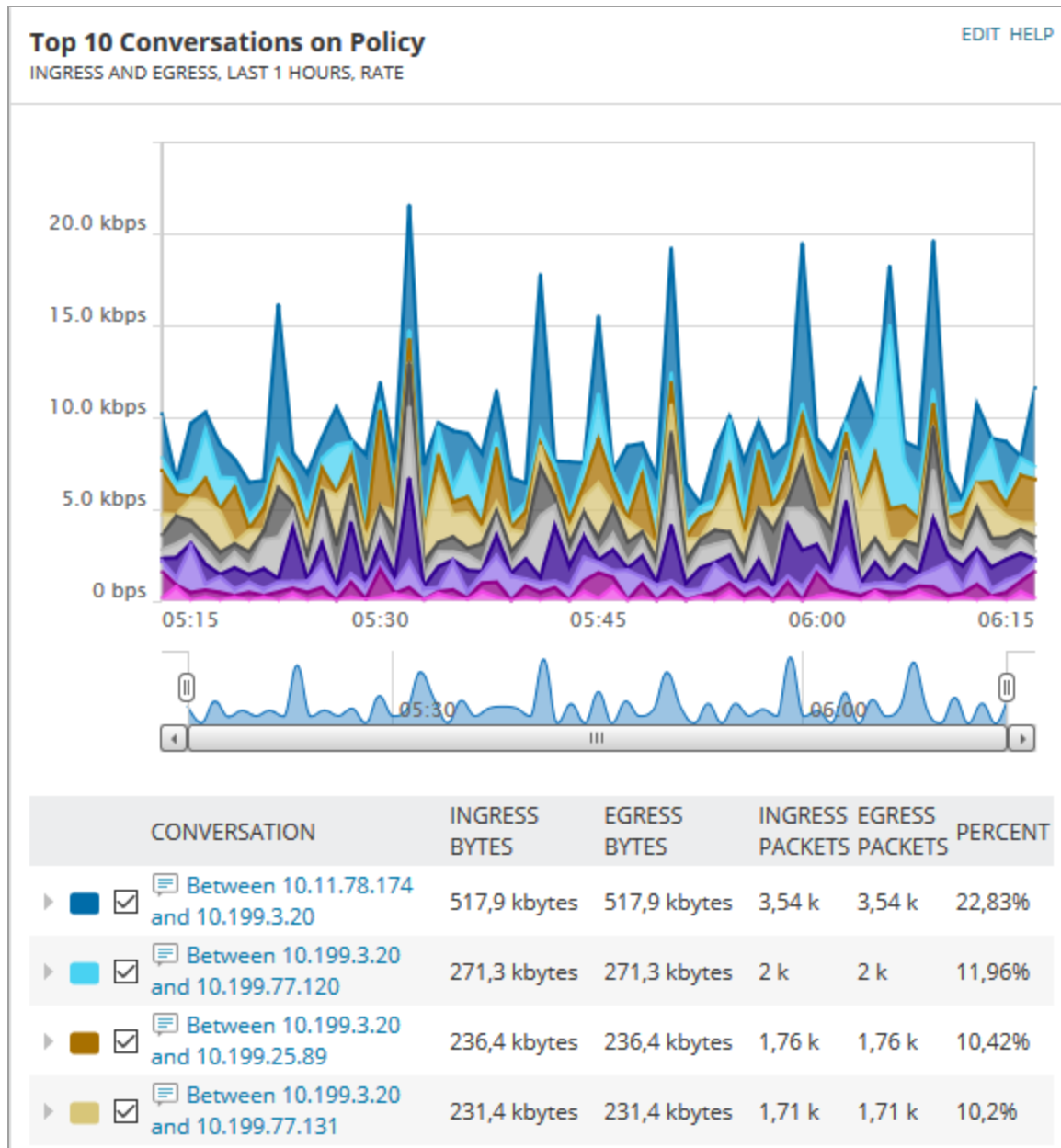
The Node Details page displays information about the selected device.

3. In the menu on the left, click Policies.

The Policy view displays a summary of each policy, including the name, source zones, and destination zones.

4. Use filters or search to locate the policy that you're interested in, and click the policy name.

- The Policy Details page displays information about the policy definition, as well as other information, such as the Top XX Conversations on Policy widget.



For more information, see [View Palo Alto Policies](#) in the NCM Administrator Guide.

Monitor traffic flow directions

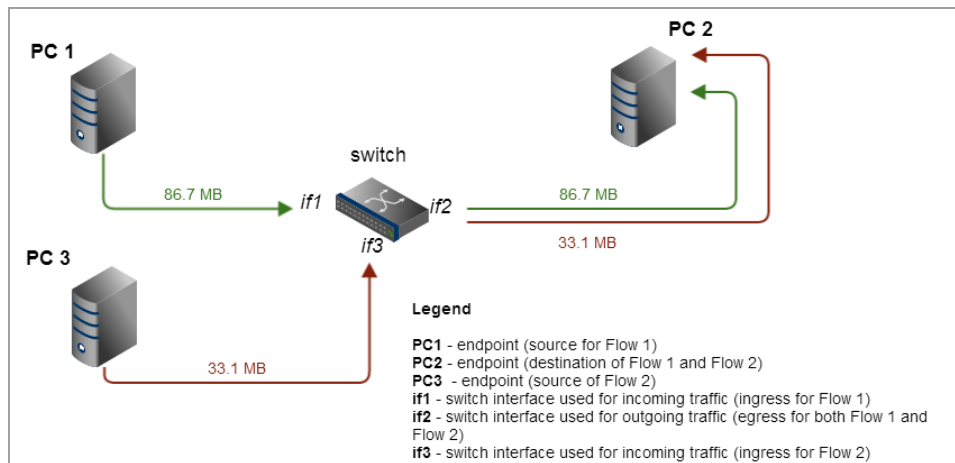
NTA monitors traffic flow over interfaces on your network devices. On any selected device interface, network traffic can flow both into the device (ingress) and out from the device (egress). The header of any NTA view showing interface-level traffic provides a control that gives you the ability to choose the traffic direction you want to monitor. The traffic direction control gives you the following options for traffic flow monitoring:

- Both displays a summation of all traffic flowing both in and out of the selected node over the selected interface.
- Ingress displays only traffic flowing into the selected node over the selected interface.
- Egress displays only traffic flowing out of the selected node over the selected interface.

The size of ingress and egress packets is usually the same. However, it can differ for example if you have CBQoS policies defined for individual interfaces, and these policies define that certain packets are dropped and not delivered to the appropriate endpoint.

Consider the following scenario with two flows:

- **Flow F1:** PC1 (source) > the traffic of 86.7 MB is coming to the switch through interface if1 (ingress) and leaving the switch via interface if2 (egress) > PC 2 (destination)
- **Flow F2:** PC3 (source) > the traffic of 33.1 MB is coming to the switch through interface if3 (ingress) and leaving the switch via interface if2 (egress) > PC 2 (destination)




For PC2, NTA shows the following interfaces:

- if2 - the interface both flows (F1 and F2) use for leaving the switch (egress: 86.7+33.1=119.8 MB)
- if1 - the interface used by flow F1 for entering the switch (ingress: 86.7 MB)
- if3 - the interface used by flow F2 for entering the switch (ingress: 33.1 MB)

Set flow direction in NTA

You can set flow direction either globally for all NTA widgets or manually for the current session.

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Under Charting and Graphing Settings, use the Default Flow Direction settings to set the defaults for all NTA widgets placed in Summary, Node Detail, Interface Detail views.
4. You can also set global Default Flow Direction for CBQoS widgets. The global default is applied only if both the view on which the CBQoS widget is placed and the CBQoS widget itself are using their default settings.
5. Click Save.

 Manually adjusting flow direction on an NTA view overrides the global default for that view only.

Change flow direction in a view

1. Click next to the flow direction setting below the view name.
2. Select a flow direction: Both, Ingress, or Egress. The Select Flow Direction menu only provides the options that can be applied to the current view.
3. Click Submit.

View CBQoS data in NTA

Class-Based Quality of Service (CBQoS) is an SNMP-based, proprietary Cisco technology available on selected Cisco devices that gives you the ability to prioritize and manage traffic on your network. Using policy maps, also known as policies, the different types of traffic on your network are categorized, and then given a priority. Based on assigned priorities, only specified amounts of selected traffic types are allowed through designated, CBQoS-enabled devices.

For example, you could define a policy map in which only 5% of the total traffic over a selected interface may be attributed to YouTube.

CBQoS policies can be simple or include nested policies.

Nested policies are traffic policies applied to a class of an already existing policy. They allow you to set rules for a class-specified type of incoming or outgoing traffic on an interface, thus enabling you to build up a complex approach to different traffic data. Nested policies simplify your job if you need to modify a policy. You just modify the policy and your changes are automatically applied on all devices using this policy.

For more information about configuring class maps for your CBQoS-enabled network devices, search CBQoS at www.cisco.com.

NTA does not currently provide a CBQoS configuration capability, but any node managed by NPM can be polled for CBQoS information. If SNMP polls of the MIB for monitored devices are unsuccessful for CBQoS OIDs, CBQoS widgets are automatically hidden because they are empty. For more information about enabling CBQoS polling for monitored devices, see [Flow sources and CBQoS polling](#).

For CBQoS-enabled Cisco devices on your network, NTA can provide immediate insight into the effect of your currently enacted policy maps. The following CBQoS widgets are available for inclusion on NetFlow Interface Details views, NPM Interface Details views, and CBQoS Details views:

CBQoS drops

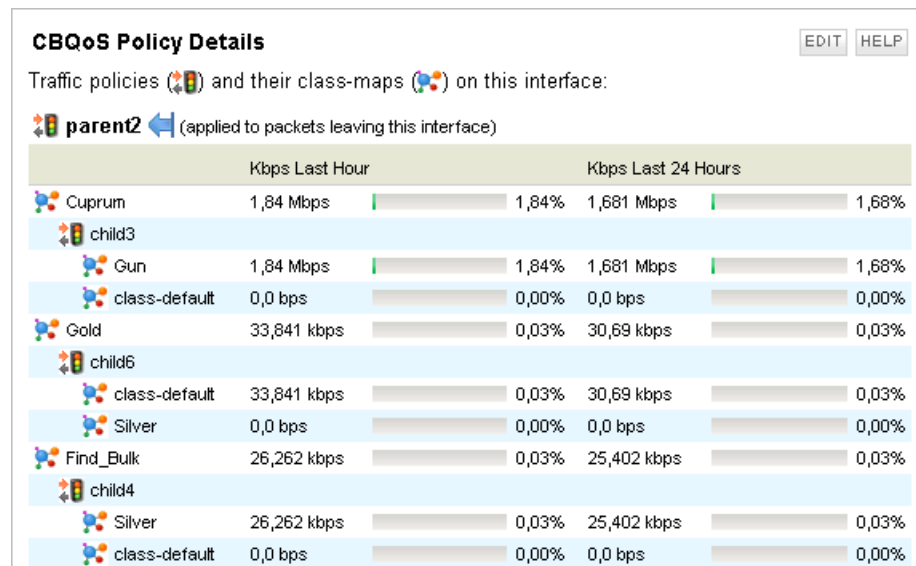
If it is included on a NetFlow Interface Details view, the CBQoS Drops widget provides both a graph and a table reporting each of the defined classes and corresponding amounts of traffic that are filtered out or dropped as a result of policy maps currently enacted on the viewed interface.

If it is included on the CBQoS Details view, the CBQoS Drops widget provides both a graph and a table reporting the amount of traffic corresponding to the selected CBQoS policy class that is filtered out or dropped as a result of policy maps currently enacted on the viewed interface.

CBQoS policy details

If it is included on a NetFlow Interface Details view, the CBQoS Policy Details widget provides a table with graphic representations of traffic corresponding to defined classes that has passed over the viewed interface in both the hour and the 24 hours prior to the currently viewed time period. In the header, you can also see whether the policy is applied to incoming packets or to packets leaving the selected interface.

If you have defined nested policies for your interface, you can see a hierarchical tree of classes and policies in this widget. Next to each class, you can see the corresponding traffic in the last hour and last day. For traffic data which do not belong to any defined class, NTA automatically creates a class-default class which displays the remaining traffic.



If it is included on the CBQoS Details view, the CBQoS Policy Details widget displays the amount of traffic corresponding to the selected CBQoS policy class that has passed over the viewed interface in both the hour and the 24 hours prior to the currently viewed time period.

CBQoS post-policy class map

On a NetFlow Interface Details view, the CBQoS Post-Policy Class Map widget provides a graph and a table detailing the average and the most recently polled amount of traffic corresponding to defined classes passing over the viewed interface as a result of the application of policy maps.

If it is included on the CBQoS Details view, the CBQoS Post-Policy Class Map widget provides both a graph and a table detailing both the average and the most recently polled amount of traffic corresponding to the selected CBQoS policy class passing through the viewed interface resulting from the application of policy maps on the viewed interface.

CBQoS pre-policy class map


If it is included on a NetFlow Interface Details view, the CBQoS Pre-Policy Class Map widget provides both a graph and a table detailing both the average and the most recently polled amount of traffic corresponding to defined classes passing through the viewed interface prior to the application of any policy maps.

If it is included on the CBQoS Details view, the CBQoS Pre-Policy Class Map widget provides both a graph and a table detailing both the average and the most recently polled amount of traffic corresponding to the selected CBQoS policy class passing through the viewed interface prior to the application of any policy maps.

Because there are different formulas for calculating bitrate in loading CBQoS widgets and in generating reports, there is a case in which the numbers on 24 hour views do not correlate. When the device from which the data is being collected has been a CBQoS source node for less than 24 hours, the CBQoS Policy Details widget will show a different number compared to the comparable CBQoS report.


Monitor NBAR2 Applications in NTA

After you have configured your devices to send NBAR2 data and added the devices for monitoring in NTA, you can identify the top applications and top categories and subcategories of applications consuming bandwidth on your network.

 You can also run [reports](#) to view the top categories and subcategories for NBAR2 flows.

1. To access the Applications Summary view, in the Dashboard, click NetFlow > Apps.
2. In the top-right corner of the Top XX Applications widget, select NBAR2 from the drop-down.

NTA populates the chart with the top NBAR2 applications identified by name.

 If you deployed [SolarWinds Observability Self-Hosted](#) 2022.2, NBAR2 applications are identified by name and application vendor icon. Hover over the icon of the application vendor to see the name of the vendor.

 If NTA displays "NO DATA" in the Top XX Applications widget, make sure you have completed the [NBAR2 requirements for application ID](#).

Common tasks and user scenarios

While NPM reports the bandwidth usage on a given interface, NTA provides information about the actual user of that bandwidth and the applications the user is running.

This section guides you through tasks you may want to accomplish with NTA, and provides user scenarios illustrating how you can solve business problems.

CBQoS policies in NTA

NTA offers flow traffic statistics that can help in determining what CBQoS classes and policies to create and apply. NTA also includes configurable alerts to help you verify the expected effects of the policy maps you apply to interfaces on your relevant Cisco devices. NTA provides information for tuning the CBQoS implementation.

The following sections explain how to use NTA in preparing CBQoS policies and how to monitor the implementation. They do not cover the details of defining class and policy maps and applying them to interfaces. For that, see the Cisco documentation.

Prepare a CBQoS implementation in NTA

Since CBQoS pertains to the use of bandwidth on the interfaces of your Cisco devices, the best way to define your objectives for CBQoS class and policy creation is to establish the trend of bandwidth use on your network at the interface level.

Assuming you have Cisco devices set up to export flow data and NTA is showing the devices under NetFlow Sources on the NetFlow Traffic Analyzer Summary view, begin by examining each node for traffic statistics and useful traffic information. For more information about setting Cisco devices, see [Add flow-enabled devices and interfaces to the SolarWinds Platform database](#).

The following steps cover the basic process for using NTA to analyze flow data in preparation to defining a CBQoS strategy. These steps are meant to give general guidance on how to use NTA in analyzing your current traffic as it pertains to determining CBQoS needs.

1. Click My Dashboards > NetFlow > NTA Summary.
2. Under NetFlow Sources, expand a node, and then click an interface for which you want to analyze the traffic. This brings up an Interface Details view for the interface.

3. Click next to Time Period and set the time frame for which you want to examine traffic statistics.

For example, with the intention of understanding what happens with traffic in a representative month, you might set an Absolute Time Period that includes the first and last day of the most recently concluded month.

4. Click Submit.
5. Click next to Flow Direction and set the flow direction for which you want to review the traffic.
6. Click Submit.
7. Use a combination of Top XX widgets on the Interface Details to analyze how traffic data is flowing through the interface. For example:

Use Top XX Applications to view the applications that were used to send the most traffic through the interface.

The goal is to determine the amount of critical data applications typically transfer in the representative time period. You also want to discover the applications that are consuming bandwidth unrelated to the purposes of your organization, such as YouTube streaming.

You probably need to follow up on what you see in Top XX Applications by viewing Top XX Conversations or by using another tool, like a packet sniffer (WireShark) or Cisco Network Based Application Recognition (NBAR), to discover the exact identity of the bandwidth-consuming applications. For example, based on available layer 3 and 4 information that it has, Top XX Applications may only list the application as HTTP. By cross-referencing with Top XX Conversations, or by digging deeper with other tools, you can often discover other data (ports, IP addresses) that lead you to the actual applications involved in generating the real bandwidth-intensive data.

Use Top XX Conversations to view the endpoints involved in the highest bandwidth-consuming conversations, and to determine if there is a pattern to when the conversations took place and which endpoints were involved.

The goal is to discover predictable recurrent uses of bandwidth related the purpose of your business or organization. You also want to discover the uses of bandwidth that are not related to the primary purposes of your organization, so that you can lower the priority of this traffic when you put it in a CBQoS class.

In this case, since the conversation gives you endpoints, you can use DNS, with a tool like nslookup, to discover where each endpoint is operating. Knowing the domain often helps identify the type of data involved. For example, finding out that one of the endpoints is operating within `www.youtube.com` tells you that audio or video data is being transferred.

Use Top XX Traffic Sources or Destinations by Countries to view the countries whose traffic is most serviced through the interface.

If you are using Persistent DNS instead of On Demand DNS, you can view the domains responsible for the highest levels of data transfer through the interface and correlate those levels with statistics in the other Top XX widgets. For information on using persistent instead of On Demand DNS, see [DNS and NetBIOS resolution in NTA](#).

When viewing traffic history in this way, you probably will observe obvious top priorities for shaping the use of bandwidth on the interface.

8. Repeat steps 3 through 9 for each flow-enabled Cisco device for which you might need to create CBQoS policies.
9. Based on what your traffic analysis reveals, for each interface, rank and group the types of data you discovered according to their importance to your organization, or to the experience of those who use the critical applications for which the type of data is passed over the network.
10. Translate the groups of data types into CBQoS class maps and work to define policy maps that would result in an allocation of interface bandwidth that match your rankings.

The goal is to have traffic flowing through the interface so that in cases of peak usage, if traffic exceeds bandwidth, shaping occurs based on the desired priority.

Monitor CBQoS dynamically in NTA

This section assumes that you set up your CBQoS policies and applied them to interfaces on your devices, and that devices are all being monitored in NPM and are listed in NTA as CBQoS Sources.

For more information on discovering network devices, see [Discovering and Adding Network Devices](#).

For more information on setting up on NetFlow collections, see [Set up network devices to export NetFlow data](#).

Should data matched for CBQoS processing violate your expectations as expressed in the form of alert threshold settings, you can have NTA trigger an alert and take specific actions.

The following SolarWinds Platform Advanced Alerts are available to you:

- Pre-Policy
- Post-Policy
- Drops

For more information about individual alerts, see [CBQoS Alerts](#).

Configure a CBQoS alert

1. Click Alerts & Activity > Alerts.
2. Use the Group By list to filter alerts.
3. Select the relevant CBQoS alert.
4. Click Edit Alert Definition.
 - a. On Properties, click Enabled to turn the alert on, and then select an Evaluation Frequency of Alert.
 - b. On Trigger Condition, define the conditions in which the software launches the alert.

For the CBQoS alerts, the default condition is a match on the SQL query. You can adjust the number of seconds for which the match exists, essentially inserting a delay to allow the traffic to fluctuate without triggering the alert. You can adjust this condition or add conditions.
 - c. On Reset Condition, define the conditions in which the software resets the alert.

For the CBQoS alerts, the default condition is no match on the SQL query. You can adjust the number of seconds for which the match fails to persist, essentially inserting a delay to allow the traffic to fluctuate without canceling the alert.
 - d. On Time of Day, define the days and times during which the software actively evaluates the database for trigger conditions.

The default is Always Enabled.
 - e. On Trigger Actions, create actions to execute when the software triggers the alert.

As discussed, the default action for all alerts is to write to the SolarWinds event log.

For CBQoS alerts, the default actions include write the same event message into an email and send it to a contact.
 - f. On Reset Actions, define actions to execute when the software resets the alert.
5. Click Next, and click Submit.

Monitor autonomous systems through BGP in NTA

NTA supports monitoring autonomous system networks and autonomous system conversations using the border gateway protocol (BGP). You set up network devices within autonomous systems.

The following sections cover how to prepare to monitor autonomous system networks and the options available for managing them.

Prepare to monitor autonomous systems in NTA

NTA collects and stores information regarding autonomous systems that network devices send in the NetFlow packets they export. You set up a network device for exporting autonomous system information as part of setting up the device to export NetFlow.

i Since in sFlow BGP/AS information is provided in a special and extended header, NTA does not collect and process BGP/AS data for sFlow.

NTA collects NetFlow data, by default on port 2055, only if a network device is specifically configured to send to it. As a NetFlow collector, NTA can receive exported NetFlow version 5 data and NetFlow version 9 data that includes all fields of the NetFlow version 5 template. Once it collects NetFlow traffic data, NTA analyzes device bandwidth usage in terms of the source and destination endpoints of conversations reflected in the traffic.

All of these things need to be done for NTA to correctly monitor autonomous system networks through BGP:

- Each device must be configured as part of an autonomous system network, with specified connections to all neighbors within the system.
- Each device must be configured to export NetFlow data to NTA. For more information about required fields, see [Autonomous system requirements for NTA](#).
- Each device must be configured to include one of the following statistics into the NetFlow exports:
 - `origin-as` command includes the origin AS for the source and destination.
 - `peer-as` command includes the peer AS for the source and destination.

i You cannot include both origin and peer statistics.

- Each device that exports NetFlow data to NTA must be monitored in NPM.

Traffic from a device that is not monitored in NPM appears only in aggregate as part of the traffic from all unmonitored devices. If the device is setup to export data to NTA, but is unmonitored in NPM, the collector may receive the data without being able to analyze it meaningfully.

The specific interface through which a device exports NetFlow data must be monitored in NPM, and the interface index number for this interface in the SolarWinds Platform database (interface table) must match the index number in the collected flow data.

Set up a device for monitoring by NTA as part of an autonomous system

1. Log in to the network device.
2. Based on the documentation of the device, you would minimally do these things, adding the appropriate commands to the configuration file:

- a. Enable a BGP routing process, which places you in router configuration mode.
- b. Flag a network as local to this autonomous system and enter it to the BGP table. Enter as many networks as needed.
- c. Specify BGP neighbors. Enter as many neighbors as needed.

For example, for detailed information on BGP configuration for Cisco devices, see this [Cisco documentation](#).

3. Enable NetFlow export from your device.

- For detailed information on configuring NetFlow on Cisco devices, search for the appropriate configuration in the [Cisco NetFlow Configuration guide](#) (© 2021 Cisco, available at <https://www.cisco.com/>, obtained on May 6th, 2021).
- For information on enabling NetFlow for Cisco Catalyst switches, see [Enable NetFlow and NetFlow data export on Cisco Catalyst switches](#).
- For information on enabling NetFlow on Cisco ASA devices, see [Cisco ASA NetFlow overview](#).
- Otherwise, consult these examples as apply to your device:
 - [Brocade \(Foundry\) sFlow configuration](#)
 - [HP sFlow configuration](#)
 - [Extreme sFlow configuration](#)
 - [Juniper sFlow configuration](#)
 - [Juniper J-Flow configuration](#)
 - The documentation of your network device

4. Add the device exporting NetFlow to NPM for monitoring.

If you are adding a large number of NetFlow enabled nodes, use SolarWinds Platform Network Sonar. For more information, see [Discovering and Adding Network Devices](#).

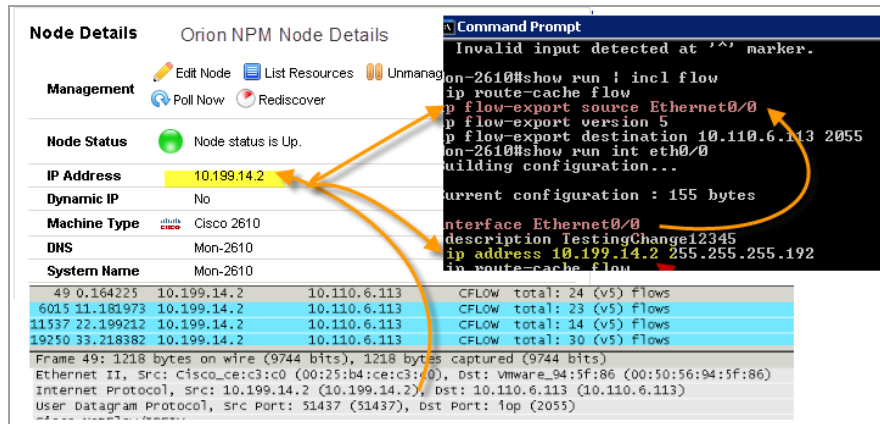
If you are only adding a few nodes, it may be easier to use Web Node Management in the SolarWinds Platform Web Console. For more information, see [Adding Devices for Monitoring in the SolarWinds Platform Web Console](#).

5. Verify that the device is exporting NetFlow data as expected and that the device is monitored in NPM.

To verify that data are exported correctly, use a packet capture tool, such as WireShark, to search for packets sent from the network device to the SolarWinds Platform server.

Example

If you successfully add a NetFlow enabled device with IP address 10.199.14.2 to NPM, and the device is actively exporting NetFlow data to the SolarWinds Platform server, you will see in WireShark a packet like the one (49) highlighted below in gray:



As expected, we see in the packet details that 10.199.14.2 is its source IP address and 10.110.6.113 is the destination, which is the SolarWinds Platform server. This correlates with the node details on the device in the SolarWinds Platform, as highlighted in yellow.

To verify that the IP address of the exporting interface on the network device is the one being monitored in SolarWinds Platform:

- a. Open a command line interface, log into the network device, and then type `show run` to see the running configuration of the device.
- b. Page down to the lines where the export source interface is defined. In this case, we see `ip flow-export source Ethernet0/0`.

To discover the IP address for this interface, type `show run int Ethernet0/0`. The IP address of the interface, 10.199.14.2, is being monitored by the SolarWinds Platform server.

6. Click My Dashboards > NetFlow > NTA Summary.

Under NetFlow Source, verify the NetFlow-enabled nodes listed with a recent time posted for collected flow.

7. Click My Dashboards > NetFlow > BGP. You should see chart statistics in the Top XX Autonomous Systems and Top XX Autonomous Systems Conversations widgets.

Autonomous system requirements for NTA

If you want to monitor autonomous systems via BGP, the flows have to contain information in appropriate bytes or fields.

i NTA does not support extracting BGP information from sFlows.

NetFlow v5 and compatible flows

The flow record has to contain data for the following bytes:

Bytes	Contents	Description
40-41	src_as	Autonomous system number
42-43	dst_as	Autonomous system number

For more information, search for NetFlow export datagram format on www.cisco.com.

NetFlow v9, IPFIX, and compatible flows

The flow record from autonomous systems has to contain data in the following field types.

Field Type	Value	Length (bytes)	Description
SRC_AS	16	N (default 2)	Source BGP autonomous system number where N could be 2 or 4.
DST_AS	17	N (default 2)	Destination BGP autonomous system number where N could be 2 or 4.
PeerSrcAS	129	N (default 2)	Peer source autonomous system number
PeerDstAS	128	N (default 2)	Peer destination autonomous system number

For more information, search for NetFlow version 9 flow record format on www.cisco.com.

Manage autonomous systems in NTA

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Under Autonomous Systems, click Manage Autonomous Systems.

Add an autonomous system

1. Click Add Autonomous System.
2. Enter values for the new autonomous system.
3. Click Save.

Edit an autonomous system

1. Under the Actions column, click Edit next to an autonomous system.
2. Modify values for the autonomous system.
3. Click Save.

Delete an autonomous system

1. Under the Actions column, click Delete next to an autonomous system.
2. Click Save.

Monitor autonomous systems in NTA

NTA collects and stores information regarding autonomous systems that network devices send in the NetFlow packets they export. Two widgets provide graphical views of the data collected during a specified period of time.

Top XX Autonomous Systems

This widget provides a list of the most bandwidth-intensive autonomous systems. Autonomous systems are listed with the amount of data (kbps) transferred, in both bytes and packets, and the percentage of all traffic generated by the autonomous system over the specified time period.

When placed on the Node Details or Interface Details view, this widget provides a view of the autonomous systems responsible for the most traffic passing through the viewed node or interface over the selected period of time.

Clicking a listed autonomous system or drilling down to relevant nodes and interfaces opens the NetFlow Autonomous Systems Summary for the selected autonomous system. The NetFlow Autonomous System Summary provides both a chart of Total Bytes Transferred by the autonomous system and the conversation and a Conversation Traffic History.

The control under the view title designates the time period that is applied to all default view widgets. However, widgets that are added to customize a view may not be subject to this time period control.

Top XX Autonomous System Conversations

This widget provides a list of the most bandwidth-intensive autonomous systems conversations. Autonomous systems conversations are listed with the amount of data (kbps) transferred, in both bytes and packets, and the percentage of all traffic generated by the autonomous system over the specified time period.

When placed on the Node Details or Interface Details view, this widget provides a view of the autonomous systems conversations responsible for the most traffic passing through the viewed node or interface over the selected period of time.

Clicking a listed autonomous systems conversations or drilling down to relevant nodes and interfaces opens the NetFlow Autonomous Systems Conversations Summary for the selected conversation. The NetFlow Autonomous Systems Conversations Summary provides both a chart of Total Bytes Transferred in the conversation and a Conversation Traffic History.

IP address groups in NTA

NTA allows you to establish IP address groups for selective monitoring of custom categories or segments of your network. The following procedure sets ranges and descriptions for your network IP addresses so you can better characterize and assess the flow data you receive.

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Under IP Address Groups, click Manage IP Address Groups.
4. Make your changes:
 - [Select IP ranges to monitor in NTA](#)
 - [Add IP address groups to NTA](#)
 - [Edit IP address groups in NTA](#)
 - [Delete IP address groups from NTA](#)
5. Click Submit.

Use NTA to find the cause of high bandwidth utilization

If a node managed in NPM is also a NetFlow source, it exports NetFlow data that you are currently monitoring in NTA. You can use NTA to analyze interface bandwidth utilization on the node whenever your workflow requires.

This procedure assumes that you have created an SolarWinds Platform alert on bandwidth utilization for a specific interface, and that the alert has been triggered based on your threshold setting. For example, you may have set the trigger threshold at 80% of interface bandwidth and you now see an alert-related event.

1. Click My Dashboards > NetFlow > NTA Summary.
2. Under NetFlow Sources, locate and expand the relevant node.
3. Click the interface for which you received the bandwidth utilization alert.
4. View the Top XX Endpoints for the interface.

Each endpoint in the list has a utilization percentage associated with it. You should quickly see here the endpoint(s) responsible for the utilization alert. And you should see the domain associated with the endpoint. Even in On Demand DNS mode, NTA resolves hostnames in loading the Top XX Endpoints widget.

5. View the Top XX Conversations to correlate the relevant items from the Top XX Endpoints list.

The endpoints in these conversations should allow you to infer if the traffic involved in these bandwidth-consuming conversations qualifies as critical to your organization. If not, you can take steps to block the offending domain or investigate for a virus attack.

If the bandwidth consumption reflected in these conversations does meet the criteria for organizational propriety or importance, then you probably need to consider this as a capacity planning or traffic management problem. If you cannot easily increase provision more bandwidth then you might consider managing the traffic on the interface with CBQoS priorities.

Track traffic by site using NTA

For capacity planning or other purposes, you may need to monitor bandwidth usage across sites within your network. An effective way to do that with NTA is to set up an IP Address Group for each site, create a custom filter for monitoring traffic within and between those groups, and place the new filtered view on the NTA toolbar.

1. Click My Dashboards > NetFlow > NTA Summary.
2. Click Flow Navigator on the left edge of the summary view. The Flow Navigator is available on any default NTA view.
3. Under View Type, select Detail.
 - a. Select the IP Address Group View Type.
 - b. Select the node that corresponds to the main network device for the site, through which all

or most traffic passes.

- c. Use the private address range in the View Filter list that encompasses the specific site.
4. Select the Time Period over which you want to view network traffic by country of origin or destination.
5. Select a Flow Direction.
6. You can further limit the view by including or excluding the following items: Applications, Autonomous Systems, Autonomous System Conversations, Conversations, Domains, Endpoints, IP Address Group Conversations, Protocols, and Types of Service.
 - a. Select Include or Exclude traffic.
 - b. Enter the appropriate value(s).
 - c. Click Add Filter.
 - Under Domains, if a domain name is not resolved and saved in NTA, you cannot use it in the Flow Navigator. NTA will inform you about it and ask you to provide a valid name. For more information about resolving domain names, see [Host and domain names in SolarWinds NTA](#).
 - Under Endpoints, you can either type the range, for example 192.168.1.0-192.168.1.255, or use the CIDR notation, for example 192.168.1.0/24.
7. Click Submit.
8. Click Save Filtered View to Menu Bar, and enter a name.
9. Click OK.

Perform an immediate hostname lookup with NTA

From any NetFlow Endpoint view, you can resolve the hostname of the viewed endpoint using immediate hostname lookup. To perform a lookup, browse to an Endpoint Details widget, and then click Lookup in the Hostname field.

The hostname is also retrieved on a scheduled basis. For more information, see [DNS and NetBIOS resolution in NTA](#).

NTA and the THWACK user community

By default, NTA provides the THWACK Recent NetFlow Posts widget on the NetFlow Traffic Analyzer Summary view. This widget shows the most recent posts related to NTA that have been submitted to THWACK, the online SolarWinds user community. Click a post title to open it in the NTA forum on THWACK.

User scenarios for NTA

The following user scenarios illustrate the value of NTA and how it can immediately offer you a return on your investment.

Locate and isolate an infected computer with NTA

Consider the following scenario:

A local branch of your banking network that handles all of your credit card transactions complains of an extremely sluggish network, causing frequent timeouts during sensitive data transfers.

Use NTA to quickly pinpoint and respond to the wide variety of viruses that can attack your network.

1. Check that the link to the branch network is up.
2. Click My Dashboards > Network > NPM Summary.
3. Consult the Percent Utilization chart. You see that the current utilization is 98%, even though normal branch network utilization is 15-25%.
4. Click My Dashboards > NetFlow > NTA Summary.
5. Under NetFlow Sources, click the name of the branch network to view its flow-enabled router.
6. Under Top 10 Endpoints, you can see that a single computer in the 10.10.10.0–10.10.10.255 IP range is generating 80% of the load on the branch link. You know that computers in this IP address range are accessible to customers for personal transactions using the web.
7. Under Top 10 Applications, you see that 100% of the last two hours of traffic from the publicly accessible computer has been generated by an IBM MQSeries messaging application. Click the application name to determine that the IBM MQSeries messaging occurs over port 1883.
8. You do not have any devices using IBM MQSeries messaging in the customer accessible location, nor any other services or protocols that require port 1883. You recognize that this is a virus exploit.
9. Use a configuration management tool, such as SolarWinds Network Configuration Manager, to push a new configuration to your firewall that blocks port 1883.

Locate and block unwanted use with NTA

Consider the following scenario:

Your uplink to the Internet has been slowing progressively over the last six months, even though your number of employees, application use, and dedicated bandwidth have all been stable.

With NTA, you can easily chart the increasing usage of your different network uplinks. NPM already allows you to chart utilization, but with the addition of NTA, you can locate specific instances of unwanted use and immediately take corrective action.

1. Click My Dashboards > Home > Summary. Check that the link to the Internet is up at your site.
2. Under Nodes with Problems, click the specific uplink.
3. Under Current Percent Utilization of Each Interface, you see that the current utilization of your web-facing interface is 80%.
4. Click the web-facing interface to open the Interface Details view.
5. Customize the Percent Utilization chart to show the last six months. You see that there has been steady growth from 15% to 80% consumption over time. There are even spikes into the high nineties.
6. Click My Dashboards > NetFlow > NTA Summary.
7. Under NetFlow Sources, click the web-facing interface to open the NetFlow Interface Details view.
8. Under Top 5 Endpoints, you see that a group of computers in the 10.10.12.0-10.10.12.255 IP range is consuming most of the bandwidth. These computers reside in your internal sales IP range.
9. Drill down into each of the offending IP addresses. You find out that each IP you investigate shows Kazaa (port 1214) and World of Warcraft (port 3724) usage.
10. Use a configuration management tool, such as SolarWinds Network Configuration Manager, to push a new configuration to your firewall that blocks all traffic on these two ports.
11. Within minutes, you see the traffic on the web-facing interface drop back to 25%.

Recognize and stop a denial-of-service attack with NTA

Consider the following scenario:

A NPM advanced alert tells you that your web-facing router is having trouble creating and maintaining a stable connection to the Internet.

NTA helps you easily characterize both outgoing and incoming traffic. This ability becomes ever more important as corporate networks are exposed to malicious denial of service attacks.

1. Click My Dashboards > Home > Summary.
2. Under Top 10 Nodes by Average CPU Load, you notice the CPU load on the firewall node is holding steady between 99% and 100%.

3. Click the firewall node name to open its Node Details view. Under Current Percent Utilization of Each Interface, you see that your firewall interfaces are receiving abnormally high levels of traffic.
4. Click My Dashboards > NetFlow > NTA Summary.
5. Under Top 10 Endpoints, you see that the top six computers attempting to access your network are overseas. You realize that you are being port scanned and that your firewall is interactively blocking these attacks.
6. Use a configuration tool, such as SolarWinds Network Configuration Manager, to push a new configuration to your firewall that blocks all traffic over the IP address range of the computers trying to access your network.
7. In minutes, your CPU usage drops back to normal.

Reports in NTA

In NTA, flow data are stored in the NTA Flow Storage database and CBQoS data are stored in the SolarWinds Platform database. Over time, both databases accumulate a large amount of information. SolarWinds offers both a broad array of predefined reports and user interfaces that enable you to create your own custom reports.

You can find and execute all reports in the SolarWinds Platform Web Console. See [Create and view reports](#) in the NPM online documentation for more information.

NTA offers several [NetFlow-specific predefined reports](#).

NetFlow-specific predefined reports

Several standard NetFlow-specific reports are available with NetFlow Traffic Analyzer. You can modify the predefined reports or create new reports. Some reports are IPv4 only. These reports have IPv4 in their name. Other reports automatically display available IPv6 traffic.

Access NetFlow reports

1. Click Reports > All Reports.
2. Under Group By, select Report Category. NetFlow-specific reports are grouped into the following categories:
 - [Historical NetFlow reports](#)
 - [Historical CBQoS reports](#)

i All reports with domain information require resolving and storing IPv4 hostnames immediately when a flow record is received. For more information, see [DNS and NetBIOS resolution in NTA](#).

Historical NetFlow reports

Top 100 Applications – Last 24 Hours

Displays the application name, port number used, user node, and bytes processed for the top 100 applications used by monitored devices on your network in the last 24 hours.

Top 50 Cisco WLC Applications- Last 24 Hours

Displays the name and byte count of the top advanced applications in monitored Cisco WLC flows in the last 24 hour period. The table lists the name, number of Ingress and egress bytes, and number of ingress and egress packets.

Top 100 CBQoS Drops - Last 24 Hours

Top 100 CBQoS Post-Policy

Top 100 CBQoS Pre-Policy

Top 100 CBQoS Stats - Last 24 Hours

Top 100 Conversations – Last 24 Hours

Lists the endpoints, flow source and destination, and total traffic generated by each of the 100 most bandwidth-intensive conversations on your network in the last 24 hours.

Top 100 Conversations Including Applications – Last 24 Hours

Lists the endpoints, flow source and destination, protocol name, port number used, application name, ToS name, and total traffic for the top 100 most bandwidth-intensive conversations involving applications on your network in the last 24 hours.

Top 20 IPv4 Traffic Destinations by Domain – Last 24 Hours

Displays the destination domain name, node, and bytes transferred for the top 20 destinations of traffic from monitored devices on your network in the last 24 hours.

Top 20 IPv4 Traffic Sources by Domain – Last 24 Hours

Lists the domain name, node, and bytes transferred for the top 20 sources of traffic to monitored devices on your network in the last 24 hours.

Top 5 Protocols – Last 24 Hours

Displays the protocol name and description, node, and bytes transferred for the top 5 protocols used by monitored devices on your network in the last 24 hours.

Top 5 Traffic Destinations by IP Address Group – Last 24 Hours

Displays the destination IP address group, node, and bytes transferred for the top 5 destinations of traffic, by IP address group, from monitored devices on your network in the last 24 hours.

Top 5 Traffic Sources by IP Address Group – Last 24 Hours

Displays the source IP address group, node, and bytes transferred for the top 5 sources of traffic, by IP address group, to monitored devices on your network in the last 24 hours.

Top 50 Endpoints

Lists the FQDN of the host (if available), the IP address of the host, the node name, data received by the endpoint (in bytes), data transmitted by the endpoint (in bytes), total data (in bytes).

Top 50 IPv4 Endpoints by Unique Partners

Lists the FQDN of the host (if available), the IP address of the host, the node name, data received by the endpoint (in bytes and packets), data transmitted by the endpoint (in bytes and packets), total data (in bytes and packets).

Top 50 NBAR2 Application Categories - Last 24 Hours

Displays the top NBAR2 applications by category and byte count in NBAR2 monitored flows in the last 24 hour period.

Top 50 NBAR2 Application Subcategories - Last 24 Hours

Displays the top NBAR2 applications by subcategory and byte count in NBAR2 monitored flows in the last 24 hour period.

Top 50 NBAR2 Applications - Last 24 Hours

Displays the application name and byte count of the top advanced applications in NBAR2 monitored flows in the last 24 hour period.

Top 50 Receivers – Last 24 Hours

Displays the full hostname, if available, IP address, node, and bytes transferred for the top 50 receivers of traffic on your monitored network in the last 24 hours.

Top 50 IPv4 Receivers by Unique Partners – Last 24 Hours

Displays the full hostname, if available, IP address, number of unique conversation partners, and data volume, in bytes and packets, transferred for the top 50 receivers of traffic on your monitored network in the last 24 hours.

Top 50 Transmitters – Last 24 Hours

Displays the full hostname, if available, IP address, node, and bytes transferred for the top 50 transmitters of traffic to monitored devices on your network in the last 24 hours.

Top 50 IPv4 Transmitter by Unique Partners – Last 24 Hours

Displays the full hostname, if available, IP address, number of unique conversation partners, and data volume, in bytes and packets, transferred for the top 50 transmitters of traffic on your monitored network in the last 24 hours.

Historical CBQoS reports

Top 100 CBQoS Drops – Last 24 Hours

Displays each node, interface(s), policy name, class name, flow direction, total bytes, and bitrate related to drops during the past 24 hours resulting from processing of applied CBQoS policies to traffic flows.

Top 100 CBQoS Drops – Last Update

Displays each node, interface(s), policy name, class name, flow direction, and last update time stamp related to drops resulting from processing of applied CBQoS policies to traffic flows.

Top 100 CBQoS Post-Policy – Last 24 Hours

Displays each node, interface(s), policy name, class name, flow direction, total bytes, and bitrate for Post-Policy traffic during the past 24 hours resulting from processing traffic with applied CBQoS policies.

Top 100 CBQoS Post-Policy – Last Update

Displays each node, interface(s), policy name, class name, flow direction, and last update time stamp for Post-Policy traffic resulting from processing traffic with applied CBQoS policies.

Top 100 CBQoS Pre-Policy – Last 24 Hours

Displays each node, interface(s), policy name, class name, flow direction, total bytes, and bitrate for Pre-Policy traffic during the past 24 hours related to traffic to which CBQoS policies were applied.

Top 100 CBQoS Pre-Policy – Last Update

Displays each node, interface(s), policy name, class name, flow direction, and last update time stamp for Pre-Policy traffic related to traffic to which CBQoS policies were applied.

Flows per Second statistics

With NTA, you can view Flows Per Second statistics for nodes. The feature is available only through the SolarWinds Information Service (SWIS). You can create reports for the Flows per Second statistics [using SWQL studio](#) or through the entity NetFlow Node Sources in the SolarWinds Platform Web Console:

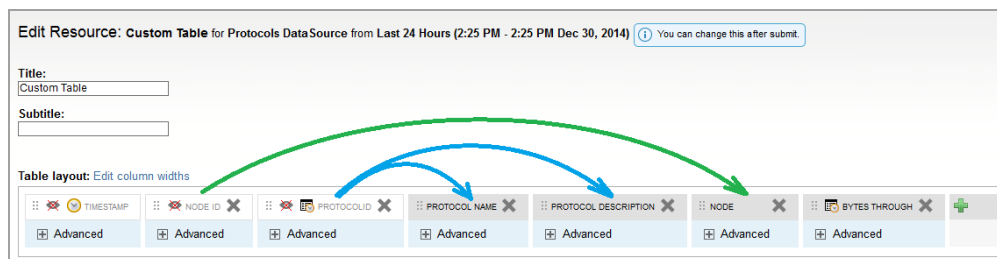
1. In the SolarWinds Platform Web Console, click Reports > All reports.
2. In the Group by drop-down, select Product > click NTA Reports > click NetFlow Sources.
3. Click Edit report.

4. On the Edit Report page (Layout builder tab), under Content, click Edit table.
5. On the Edit Resource page, under Table layout, click + to add a new column.
6. Click NetFlow Node Statistic, and select one or more of the following:
 - Flows Per Second Last 24 Hours: Displays the Flows per Second statistics for nodes for the last 24 hours.
 - Flows Per Second Last 3 Days: Displays the Flows per Second statistics for nodes for the last three days.
 - Flows Per Second Last 5 Minutes: Displays the Flows per Second statistics for nodes for the last five minutes.

Best practices for NTA reports

To solve performance issues caused by custom reports, consider the following recommendations. If appropriate, a SWQL code example is attached.

- To optimize the speed of executing reports and to optimize the performance, add the ID columns for all appropriate objects to the report. If you do not want to see these columns in the report, hide them.



- Do not query all data from NTA Flow Storage database, use the Top XX Results to cover the most significant traffic. Every filter that limits data speeds up the report.

SWQL Example: Data limitation

The following query limits the report to show top 10 nodes only:

```
SELECT TOP 10 [T1].[NodeID], SUM([T1].[TotalBytes]) AS TotalBytes

FROM Orion.NetFlow.Flows AS T1

ORDER BY TotalBytes DESC
```

- Limit the data by time. If a query in SWQL does not use a time limit, all available data are queried. To query only the last hour, use the value 0.04167, which is calculated as 1 day/24 hours.

SWQL Example: Time condition in SWQL

The following query limits the report to show top 100 nodes during the last day:

```
SELECT TOP 100 [T1].[NodeID], [T1].[InterfaceIDTx], [T1].[InterfaceIDRx],
SUM([T1].[TotalBytes]) AS TotalBytes FROM Orion.NetFlow.Flows AS T1

WHERE ([T1].[TimeStamp] >= (GetUTCDate() - 0.04167))

GROUP BY [T1].[NodeID], [T1].[InterfaceIDTx], [T1].[InterfaceIDRx]

ORDER BY TotalBytes DESC
```

- Test out a new report using a short time period. If a report with a short time period works out, and a longer time period causes the report to crash, there might be an issue with provided time periods.

SWQL Example: Time condition in SWQL

```
SELECT [T1].[ToSID], IngressBytes
FROM Orion.NetFlow.Flows AS T1
WHERE ([T1].[TimeStamp] >= (GetUTCDate() - 0.005))
```

- Use aggregation functions.

SWQL Example: Aggregation

When you use aggregation in a SWQL query, all 'other' columns must be grouped. Reports created via the user interface group these columns automatically.

```
SELECT SourceIP, DestinationIP, Port, Protocol, MAX(IngressBytes) AS
IngressMaximum, MIN(IngressBytes) AS IngressMinimum
FROM Orion.NetFlow.Flows
GROUP BY SourceIP, DestinationIP, Port, Protocol
```

- Comments in SWQL

If you are adding comments in SWQL, start the comment on a separate line and add an extra line after the comment.

Generally, you can place comments anywhere. Comments are started by a double dash sign (--); a comment is everything on one line which comes after the -- sign, up to the end of the line.


Execute a report in NTA

1. Click Reports > All Reports.
2. Under Group By, select Product.
3. Click NTA Reports.
4. Select the report you want to run and click View Report.
5. Click Export to PDF or Printable Version to save the report.


For helpful information about running NTA reports, see [Best practices for NTA reports](#).

Create a report in NTA

Before creating a new report, look at the predefined reports. Consider whether you can use a predefined report, adjusting certain properties or the time frame.

 For detailed information about creating reports in the SolarWinds Platform Web Console, see [Create and view reports](#) in the NPM online documentation for more information.

1. Click Reports > All Reports.
2. Click Manage Reports.
3. Decide whether to copy and edit a predefined report, or create a new report.
 - To adjust an existing report, select the report, and click Duplicate & Edit.
 - To create a new report, click Create New Report.
4. Click Custom Table. NTA does not support Custom Chart.
5. Click Select and Continue.
6. Select a NetFlow object to report on.
7. Click Add to Layout.

8. Define what the custom table should show in the resulting report. Select properties and sorting of items:
 - a. Add columns.
 - b. To edit information provided by individual columns, click Advanced in the column.
 - c. Define sorting of items in the report with Sort Results By.
 - d. Define grouping of data with Group Results By.
 - e. To limit the number of items on the report, use the Filter Number of Results section.
 - f. Time-Based Settings allows you to change the Sample Interval used for filtering or summarizing data by time period. The defined table must contain at least one column with historical data so that you can filter the data. This is why the Timestamp column is automatically added. The column is hidden by default, as indicated by the  icon.
 - g. Click Preview Resource, review the preview, and click OK.
 - h. Click Submit.
9. Complete the Add Report wizard, clicking Next between each step.
 - a. Define the layout: header, content, and footer.
 - b. Preview the report.
 - c. Enter report properties: description, category, custom properties, or limitation.
 - d. Schedule the report, if desired.
 - e. Click Submit.

Create a report using SWQL in NTA

You can define the objects you want to report on using the SolarWinds Query Language (SWQL).

SWQL is a proprietary, read-only subset of SQL. Similar to SQL, you can use SWQL to query your SolarWinds database for specific network information.

1. Click Reports > All Reports.
2. Click Manage Reports.
3. Click Create New Report.
4. Click Custom Table, and then click Select and Continue.

5. Define the objects to query:
 - a. Under Selection Method, select Advanced Database Query (SQL, SWQL).
 - b. Click SWQL as the Query Type and enter the code.

For more information about the SWQL supported by the SolarWinds Platform, see [Using SWQL](#).

To discover table and field names in your database, use the Orion SDK API, available in the [Orion SDK forum](#) on thwack.com.

Log in to the Orion SDK

- Download and install the Orion SDK on the same server as you run NTA. For more information about downloading and using the Orion SDK, see [Orion SDK Information](#).
- Start the SWQL Studio in your program folder.
- Enter information to connect to the SolarWinds Information Service:
 - Server Name: localhost
 - Server Type: Orion (v3)
 - User Name and Password: Use the same credentials that you use to log on to the SolarWinds Platform Web Console.

6. Define columns that will present the data gathered by your SWQL query, and click Submit.
7. Add the report.
 - a. Define the report layout, preview the report, and define the report properties.
 - b. Click Submit.

Edit an NTA report

This section provides details on the most usual edits in reports:

Change objects that are being reported on

1. Click Reports > All Reports.
2. Click Manage Reports.
3. Select a report and click Edit Report or Duplicate & Edit if you want to edit a copy of the report and retain the original. To find historical NetFlow reports, under Group By select Report Category, and click Historical NetFlow Reports.
4. On the Edit Report view, under Content, click Edit next to the For list.
5. Change the objects for the report on the Add Content menu, and click Add to Layout.

6. Complete the wizard.

You can either use the Next buttons or click the Summary tab to switch directly to the last screen. Click Submit.

Change the time of the report

1. Click Reports > All Reports.
2. Click Manage Reports.
3. Select a report and click Edit Report or Duplicate & Edit if you want to edit a copy of the report and retain the original. To find historical NetFlow reports, under Group By select Report Category, and click Historical NetFlow Reports.
4. On the Edit Report view, under Content, select a time period in the From list.
5. Complete the wizard.

You can either use the Next buttons or click the Summary tab to switch directly to the last screen. Click Submit.

Define a customized time period

Reports only support uninterrupted time intervals. It is not possible to report on repeated time periods, such as the peak hours traffic in a specified week, or report on all working days in a month.

1. Click Reports > All Reports.
2. Click Manage Reports.
3. Select a report and click Edit Report or Duplicate & Edit if you want to edit a copy of the report and retain the original. To find historical NetFlow reports, under Group By select Report Category, and click Historical NetFlow Reports.
4. On the Edit Report view, under Content, select Custom in the From list.
5. In the Add Time Period menu, enter a Named Time Period. This name is used in the For list.
6. Specify the time period: relative or custom.
7. Click Add.
8. Select the new custom time period in the From list.
9. Complete the wizard.

You can either use the Next buttons or click the Summary tab to switch directly to the last screen. Click Submit.

Change the page layout

You can change a report layout so that you have two or more data sources next to each other to compare the values.

1. Click Reports > All Reports.
2. Click Manage Reports.
3. Select a report and click Edit Report or Duplicate & Edit if you want to edit a copy of the report and retain the original. To find historical NetFlow reports, under Group By select Report Category, and click Historical NetFlow Reports.
4. On the Edit Report view, under Content, select a layout from the Page Layout list.
5. Complete the wizard.

You can either use the Next buttons or click the Summary tab to switch directly to the last screen. Click Submit.

Change the logo

You may need to replace the default SolarWinds logo with your company's logo. The provided space allows for maximum height of 103 pixels and a maximum width of 238 pixels. Larger images are scaled to fit the space.

1. Click Reports > All Reports.
2. Click Manage Reports.
3. Select a report and click Edit Report or Duplicate & Edit if you want to edit a copy of the report and retain the original. To find historical NetFlow reports, under Group By select Report Category, and click Historical NetFlow Reports.
4. On the Edit Report view, under Content, select Logo.
5. Click Browse for Logo, navigate to the file, and then select it.
6. Complete the wizard.

You can either use the Next buttons or click the Summary tab to switch directly to the last screen. Click Submit.

Limit access to the report

You can specify a group of users who can access individual reports.

1. Click Reports > All Reports.
2. Click Manage Reports.
3. Select a report and click Edit Report or Duplicate & Edit if you want to edit a copy of the report and retain the original. To find historical NetFlow reports, under Group By select Report Category, and click Historical NetFlow Reports.
4. Click the Properties tab at the top of the screen.
5. Expand Report Limitation, and then select a report under Report Limitation Category.
6. Complete the wizard.

You can either use the Next buttons or click the Summary tab to switch directly to the last screen. Click Submit.

Specify custom properties

You can assign custom properties to your reports to help you manage your reports. For example, you can have a custom property called Department, and provide the information for which department the report is used.

1. Click Reports > All Reports.
2. Click Manage Reports.
3. Select a report and click Edit Report or Duplicate & Edit if you want to edit a copy of the report and retain the original. To find historical NetFlow reports, under Group By select Report Category, and click Historical NetFlow Reports.
4. Click the Properties tab at the top of the screen.
5. Enter values for all required custom properties.
6. Complete the wizard.

You can either use the Next buttons or click the Summary tab to switch directly to the last screen. Click Submit.

Schedule a report

You can set the report to run according to a defined schedule. Generated reports can be sent to an email address. SolarWinds NPM 10.7 or newer is required.

1. Click Reports > All Reports.
2. Click Manage Reports.

3. Select a report and click Edit Report or Duplicate & Edit if you want to edit a copy of the report and retain the original. To find historical NetFlow reports, under Group By select Report Category, and click Historical NetFlow Reports.
4. Click the Schedule Report tab at the top of the screen.
5. Click Schedule This Report to Run Regularly.
6. Assign an existing schedule or create a new one.
7. Complete the wizard.

You can either use the Next buttons or click the Summary tab to switch directly to the last screen. Click Submit.

Create a custom report for IP address groups in NTA

1. Click Reports > All Reports.
2. Click Manage Reports.
3. Click Create New Report.
4. Click Custom Table, and then click Select and Continue.
5. Define what objects should be in the report. We want to report on collected traffic connected with IP address groups. IP addresses included in a group have a property that gives the IP address group.
 - a. Under Selection Method, select Dynamic Query Builder.
 - b. Click Advanced Selector.
 - c. In the I Want to Report On list, select NetFlow Flow by IP History.
 - d. Click Select Field.
 - e. On the Add Column menu, under Available Columns, click NetFlow IP Address Group.
 - f. Under Database Column name, click IP Address Group Name.
 - g. Click Add Column.
 - h. On the Add Content menu, go to the IP Address Group name property list and select Is Not Empty.
 - i. Enter a Selection Name.
 - j. Click Add to Layout.

6. Define what columns you want to see in the report, how the items should be sorted, how many items you want to see, how the items should be grouped, and details for individual columns:
 - a. Click Add Column.
 - b. Add appropriate columns.
 - Add the IP Address Group Name column:
 - i. Select NetFlow Flow by IP History in the Orion Object list.
 - ii. Under Available Columns, click NetFlow IP Address Group.
 - iii. Under Database Column Name, select IP Address Group Name.
 - Add the Bytes column:
 - i. Select NetFlow Flow by IP History in the Orion Object list.
 - ii. Under Available Columns, click NetFlow Flows by IP History.
 - iii. Under Database Column Name, select Bytes.
 - Add the Node Name column:
 - i. Select Node in the Orion Object list.
 - ii. Under Available Columns, click Node.
 - iii. Under Database Column Name, select Node Name.
 - Click Add Column.
 - c. Define table sorting.
 - i. Under Sort Results By, select Bytes - NetFlow Flow by IP History.
 - ii. Define the sorting direction as Ascending.
 - d. Specify units and aggregation of bytes.
 - i. Under the Bytes column, click Advanced.
 - ii. In the Add Display Settings list, select Data Unit.
 - iii. In the Units of Measurements list, select Bytes (1000). This defines the units shown on the report.
 - iv. In the Units in My Database list, select B.
 - v. In the Data Aggregation list, select Sum.
 - e. Use the Filter Number of Results section to limit the number of items shown by the report.

- f. Use the Group Results By list to set how individual items are grouped in the report.
 - g. Click Preview Resource, and then click OK.
 - h. Click Submit.
7. Add the report to your SolarWinds Platform reports:
- a. Define the report layout:
 - i. Enter a Title and Subtitle. You can also change the logo, page layout, and footer.
 - ii. Under Content, in the From list, select Last 24 Hours.
 - iii. Click Next.
 - b. Check the preview, and click Next.
 - c. Define the report properties, and click Next.
 - d. If you want to create the report regularly, schedule the report, and click Next.
 - e. Review the summary, and click Submit.

Create a custom report for EF type of service in NTA

SolarWinds NPM 10.7 or later is required.

1. Click Reports > All Reports.
2. Click Manage Reports.
3. Click Create New Report.
4. Click Custom Table, and then click Select and Continue.
5. Define what objects should be in the report. We want to report on traffic using a specified type of service, so we need to specify that we are interested in NetFlow History objects whose type of service is EF.
 - a. Under Selection Method, select Dynamic Query Builder.
 - b. Click Advanced Selector.
 - c. In the I Want to Report On list, select NetFlow Flow History.
 - d. Click Select Field.
 - e. On the Add Column menu, under Available Columns, click NetFlow Type of Service.
 - f. Under Database Column Name, click ToS Name.

- g. Click Add Column.
 - h. On the Add Content menu, go to the ToS Name property list and select Is Equal To.
 - i. Type EF in the last field on that line.
 - j. Enter a Selection Name.
 - k. Click Add to Layout.
6. Define what columns you want to see in the report, how the items should be sorted, how many items you want to see, how the items should be grouped, or details for individual columns:
- a. Click Add Column.
 - b. Add appropriate columns.
 - Add the Node Name column:
 - i. Select Node in the Orion Object list.
 - ii. Under Available Columns, click Node.
 - iii. Under Database Column Name, select Node Name.
 - Add the Ingress Interface Name column:
 - i. Select Interface in the Orion Object list.
 - ii. Under Available Columns, click Ingress Interface.
 - iii. Under Database Column Name, select Interface Name.
 - Add the ToS Name column:
 - i. Select NetFlow Flow History in the Orion Object list.
 - ii. Under Available Columns, click NetFlow Type of Service.
 - iii. Under Database Column Name, select ToS Name.
 - Add the Bytes column:
 - i. Select NetFlow Flow History in the Orion Object list.
 - ii. Under Available Columns, click NetFlow Flows History.
 - iii. Under Database Column Name, select Bytes.
 - Click Add Column.
 - c. Define table sorting.

- i. Under Sort Results By, select Bytes - NetFlow Flow History.
 - ii. Define the sorting direction as Descending.
 - d. Specify units and aggregation for bytes.
 - i. Under the Bytes column, click Advanced.
 - ii. In the Add Display Settings list, select Data Unit.
 - iii. In the Units of Measurements list, select Bytes (1000). This defines the units shown on the report.
 - iv. In the Units in My Database list, select B.
 - v. In the Data Aggregation list, select Sum.
 - e. Use the Filter Number of Results section to limit the number of items shown by the report.
 - f. Use the Group Results By list to set how individual items are grouped in the report.
 - g. Click Preview Resource, and then click OK.
 - h. Click Submit.
7. Add the report to your SolarWinds Platform reports:
 - a. Define the report layout:
 - i. Enter a Title and Subtitle. You can also change the logo, page layout, and footer.
 - ii. Under Content, in the From list, select Last 24 Hours.
 - iii. Click Next.
 - b. Check the preview, and click Next.
 - c. Define the report properties, and click Next.
 - d. If you want to create the report regularly, schedule the report, and click Next.
 - e. Review the summary, and click Submit.

Customize a report to filter multicast data and group UDP data in NTA



1. Create an IP Address Group for multicast traffic:
 - a. In the SolarWinds Platform Web Console, click Settings > All Settings.
 - b. Under Product Specific Settings, click NTA Settings.



- c. Under IP Address Groups, click Manage IP Address Groups.
- d. Click Add New Group.
- e. Add a Description.
- f. Select IP Range, and type 224.0.0.0 and 239.255.255.255.

If you want to display the new IP address group in the Top XX Address Group widget, select Enable Display in Top XX Address Group Resource.

- g. Click OK.
- h. Click Submit.


Click Reports > All Reports.
Click Manage Reports.

2. Find and edit the report you want to modify:
 - a. In the Group By list, select Report Category, and then select Historical NetFlow Reports in the list below.
 - b. Select the Top 50 Endpoints box in the main reports list, and click Duplicate & Edit.
3. Adjust the object you want to report on. Add conditions stipulating that you are only interested in the multicast traffic through the UDP port.
 - a. Click Edit next to the For list.
 - b. On the Add Content menu, click Advanced Selector.
 - c. Add the condition defining the port for the monitored traffic.
 - i. Click  Add Condition to display a new branch below the Where list.
 - ii. Click Select Field.
 - iii. On the Add Column menu, under Database Column Name, select Port Number, and click Add Column.
 - iv. Type the port number in the last field next to Port Number.
 - d. Add the condition defining that you are only interested in the traffic via IP addresses in the multicast IP address group.
 - i. Click , and then Add Simple Condition.
 - ii. Click Select Field.
 - iii. In the Available Columns list, click NetFlow IP Address Group.

- iv. Under Database Column Name, select IP Address Group Name, and then click Add Column.
 - v. Type the name of the multicast IP address group, which you created in step 1, in the last field next to IP Address Group Name.
 - e. Click Add to Layout.
4. Edit the output table for the report:
 - a. Under Content, click Edit Table.
 - b. Add the Protocol column.
 - i. Click  to add a new column.
 - ii. In the Available Columns list, select NetFlow Protocol.
 - iii. Under Database Column Name, select Protocol Name.
 - iv. Click Add Column.
 - c. Add interface-relevant columns that you want to see in the report.
 - i. Click  to add a new column.
 - ii. In the Orion Object list, select Interface.
 - iii. Select Egress Interface if you are interested in traffic leaving the node via interfaces, or Ingress Interface if you are interested in traffic coming into the node.
 - iv. Under Database Column Name, select appropriate columns, and then click Add Column.
 - d. Define how you want to sort results. Select the column according to which you want to sort results in the Sort By list, and the direction.
 - e. Under Group Results By, select Protocol Name - NetFlow Protocol.
 - f. Click Submit.
5. Complete the Edit Report wizard.
6. On the Summary tab, click Submit.

Customize a historical NetFlow report to include location

1. Click Reports > All Reports.
2. Click Manage Reports.

3. In the Group By list, select Report Category, and then select Historical NetFlow Reports in the list below.
4. Select a report, and click Duplicate & Edit.
5. Under Content, click Edit Table.
6. Click  to add a new column.
7. On the Add Column menu, in the Orion Object list, select Node.
8. Under Database Column Name, select Location.
9. Click Add Column.
10. Click Submit.
11. Complete the Edit Report wizard.
12. On the Summary tab, click Submit.

Alerts in NTA


An alert is an automated notification that a network event has occurred, such as a server becoming unresponsive. The network event that triggers an alert is determined by conditions you set up when you configure your alert. You can schedule alerts to monitor your network during a specific time period, and create alerts that notify different people based on how long the alert has been triggered. Available notifications include for example [sending a web page in an email](#).

The types of events for which you can create alerts vary, depending on the SolarWinds Platform products you have installed. For example, you can create an alert to notify you if a node in a specific location goes down or if the network response time is too slow when you have NPM. See [NetFlow-specific predefined alerts](#) for a list of out-of-the box alerts delivered with NTA.

For more information about alerts, see [Use alerts to monitor your environment](#).

NetFlow-specific predefined alerts

Alerts must be enabled to trigger when the defined condition occurs. Not all out-of-the box alerts are enabled by default.

 You need Alert Management Rights to enable, create, edit, delete alerts, or to view a list of available alerts.

Where can I find what NTA-specific alerts are enabled?

1. Click Alerts & Activity > Alerts, and click Manage Alerts in the upper right.
2. In the Alert Manager, filter the alerts to display NTA-only items. Type netflow or CBQoS into the search box

3. Make sure the alerts are on.

Alert Name	Enabled (On/Off)	Alert Description	Property to N
<input type="checkbox"/> Flow storage backup failed	ON <input type="checkbox"/>	This alert will send an email if Flow Storage backup fails.	Orion.NetFlo
<input type="checkbox"/> High Receive Percent Utilization with Top Talkers	ON <input type="checkbox"/>	This alert writes to the SolarWinds event log when the curr...	Interface
<input type="checkbox"/> High Transmit Percent Utilization with Top Talkers	ON <input type="checkbox"/>	This alert writes to the SolarWinds event log when the curr...	Interface
<input type="checkbox"/> NTA Alert on EAST-2821-WAN - Egress Exceeded on SQL	ON <input type="checkbox"/>	NTA: Application traffic exceeds threshold	Interface
<input type="checkbox"/> NTA Alert on EAST-2821-WAN - Ingress Exceeded on SQL	ON <input type="checkbox"/>	NTA: Application traffic exceeds threshold	Interface
<input type="checkbox"/> NTA Alert on EAST-2821-WAN - MySQL Overflow	ON <input type="checkbox"/>	NTA: Application present in Top Applications	Interface
<input type="checkbox"/> NTA Alert on EAST-2821-WAN - SQL Data Not Present	ON <input type="checkbox"/>	NTA: Application not present in Top Applications	Interface
<input type="checkbox"/> NTA Alert on LOSA-2821-WAN - Egress on Exchange Lost	ON <input type="checkbox"/>	NTA: Application not present in Top Applications	Interface
<input type="checkbox"/> NTA Alert on LOSA-2821-WAN - Ingress on Exchange Lost	ON <input type="checkbox"/>	NTA: Application not present in Top Applications	Interface
<input type="checkbox"/> NTA Alert on NEWY-EX2200-45thFI - No Flow Data Found	ON <input type="checkbox"/>	NTA: Flow no longer being received	Interface
<input type="checkbox"/> NTA Alert on vSwitch - IPIFIX - No Flow Data Found	ON <input type="checkbox"/>	NTA: Flow no longer being received	Interface
<input type="checkbox"/> NTA Alert on WEST-2821-WAN - Egress Exceeded on SQL	ON <input type="checkbox"/>	NTA: Application traffic exceeds threshold	Interface
<input type="checkbox"/> NTA Alert on WEST-2821-WAN - Ingress Exceeded on SQL	ON <input type="checkbox"/>	NTA: Application traffic exceeds threshold	Interface
<input type="checkbox"/> NTA Alert on WEST-2821-WAN - SQL Data Not Present	ON <input type="checkbox"/>	NTA: Application not present in Top Applications	Interface
<input type="checkbox"/> NTA: CBQoS Drops	OFF <input type="checkbox"/>	CBQoS Drops writes to the SolarWinds event log when, as ...	NetFlow CBC
<input type="checkbox"/> NTA: CBQoS Post-Policy	OFF <input type="checkbox"/>	CBQoS Post-Policy writes to the SolarWinds event log when...	NetFlow CBC
<input type="checkbox"/> NTA: CBQoS Pre-Policy	OFF <input type="checkbox"/>	CBQoS Pre-Policy writes to the SolarWinds event log when ...	NetFlow CBC

Flow alerts

You can create alerts on recently processed flows to quickly identify and solve quality issues. The Create a Flow Alert panel creates a standard SolarWinds Platform alert based on Custom SWQL query. If you want to change settings such as the Trigger Action, you must either do so in the Advanced Alert Editor, or delete the existing alert and create a new one using the Create a Flow Alert panel. The default values in the Create a Flow Alert panel are based on the standard Advanced Alert Editor functionality. See [Configure Flow alerts](#) for more information.

Application Threshold

This alert notifies you that a NetFlow-reporting node reports traffic for an application or NBAR2 application over or under a certain threshold. After you create an alert for the NBAR2 application and the threshold for a particular node, the alert is triggered when the traffic exceeds the threshold.

The alert can be created across multiple applications and NBAR2 applications. It is also possible to combine the applications and NBAR2 applications. This means that the alert will be triggered when the combined threshold of all selected applications is reached.

Application present in Top Applications / Application not present in Top Applications

This alert notifies you that an application or NBAR2 application is or is not present in Top XX Applications or NBAR2 Applications lists. After you create an alert for a specific application of NBAR2 application for a node or interface, the alert is triggered when the application or NBAR2 application is missing in the Top XX Applications or NBAR2 applications widgets.

Flow no longer being received

This alert notifies you that a device (node or interface) is not sending data over a defined time period.

Top talker alerts

High Receive Percent Utilization with Top Talkers

This alert indicates that the traffic received by the relevant interface exceeded the defined bandwidth usage threshold.

High Transmit Percent Utilization with Top Talkers

This alert indicates that the traffic transmitted by the relevant interface exceeded the defined bandwidth usage threshold.

By default, when triggered, top talker alerts do two things:

- When the percent utilization of an interface rises above the specified value, the alert writes the bandwidth utilization event to the SolarWinds event log. When the utilization drops back below a specified value, the alert writes another event to the log.
- Initiate a web capture of the most current top talker information and email the information to the configured recipient.

CBQoS alerts

The CBQoS alerts can help you confirm that the CBQoS policies applied to traffic flowing through your devices are producing the intended results. For example, the default Drops alert can notify you when packets dropped as a result of a policy exceed the 1GB threshold. Specify a policy and set up alert thresholds to get an early warning about traffic processing issues and intervene to better shape network traffic.

CBQoS out-of-the-box alerts are not enabled by default because you need to [specify the policy and class path](#) to complete the trigger definition.

Pre-Policy

CBQoS Pre-Policy writes to the SolarWinds event log when the amount of Pre-Policy traffic (in bytes) meets the conditions of your alert threshold setting.

Example of alert logged: CBQoS Pre-Policy traffic in class 'class-default (MCQTest)' with policy 'policy-default (MPQTest)' on interface 'FastEthernet0/0 link to core' met the conditions of your alert threshold setting. Total Pre-Policy traffic in the past 15 minutes: 99999 Bytes.

By default, this alert writes to the Event Log. This alert also can be configured to send the information in an email to the configured recipient.

Post-Policy

CBQoS Post-Policy writes to the SolarWinds event log when the amount of Post-Policy traffic (in bytes) meets the conditions of your alert threshold setting.

Example of alert logged: CBQoS Post-Policy traffic in class 'class-default (MCQTest)' with policy 'policy-default (MPQTest)' on interface 'FastEthernet0/0 · link to core' met the conditions of your alert threshold setting. Total Post-Policy traffic in the past 15 minutes: 99999 Bytes.

By default, this alert writes to the Event Log. This alert also can be configured to send the information in an email to the configured recipient.

Drops


CBQoS Drops writes to the SolarWinds event log when applying CBQoS policies to traffic on an interface.

Example of alert logged: CBQoS Drops met your alert threshold setting as a result of applying class map 'class-default (MCQTest)' and policy map 'policy-default (MPQTest)' on interface 'FastEthernet0/0 · link to core' . Total data dropped in last 15 minutes is: 00333 Bytes.

By default, this alert writes to the Event Log. This alert also can be configured to send the information in an email to the configured recipient.

Configure NTA-specific alerts

You can use the out-of-the-box alerts as templates for customized alerts. Configure an alert for NTA based on a predefined top talker or CBQoS alert.

 For out-of-the-box alerts, you have limited edit options. You can enable or disable the alerts, add trigger and reset actions, or adjust Time of Day settings. To make more substantial changes, such as changing the conditions, select the alert and click Duplicate & Edit.

Configure trigger actions for default top talker alerts

Default top talker alerts notify you when current percent utilization of an interface (receive or transmit side) rises above a specified threshold (75%). The alert writes an entry into the SolarWinds event log and sends a web page to specified recipients.

To make the top talker work, configure credentials used for accessing and sending the SolarWinds Platform Web Console page and specify the email address that will receive the notification.

i Default top talker alerts use the default Admin account and no password for sending the SolarWinds Platform Web Console page. When you change the default account credentials, top talker alerts stop working. Provide valid credentials into the trigger action macro.

1. Click Alerts & Activity > Alerts.
2. Click Manage Alerts.
3. Select a top talker alert.

 To find top talker alerts, type top talker into the search box to filter the alerts.

4. Select a Top Talker alert, and click Edit.
5. Go to Trigger Actions.
6. Click Edit for the E-Mail a Web page action.
7. Enter an Email address for receiving the web page. You can specify the sender and a reply address.
8. Expand Message.
9. In the Enter or Paste the Web macro, enter the macro:
 - For incoming traffic: `${N=NTA.Alerting;M=NTA.InInterfaceDetailsLink}`
 - For outgoing traffic: `${N=NTA.Alerting;M=NTA.OutInterfaceDetailsLink}`

Enter or Paste the Web Page URL

`${N=NTA.Alerting;M=NTA.InInterfaceDetailsWebMailUrl}`

[How can I create a dynamic URL](#) PREVIEW URL

Optional Web Server Authentication

User currently logged-in (admin)

Another user

No user defined

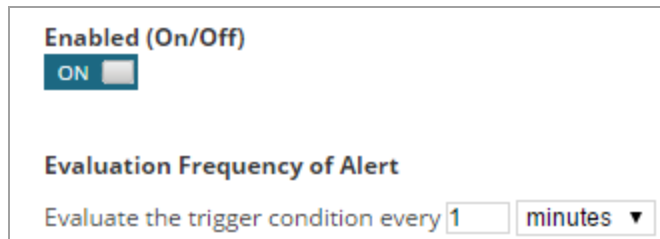
Importance: Normal v

10. Complete the Edit Alert wizard.

When an interface utilization reaches the specified threshold, the specified recipient will receive an email with the SolarWinds Platform Web Console page. See [Emailing a Web Page](#) in the SolarWinds Platform online help for more details.

Change the threshold for Top Talker alerts

1. Click Alerts & Activity > Alerts.
2. Click Manage Alerts.
3. Select a top talker alert.
4. Click Duplicate & Edit to create a copy of the alert and keep the original intact.
5. Adjust the alert properties if necessary. Under Enabled, turn the alert On and select how often the trigger condition should be checked.

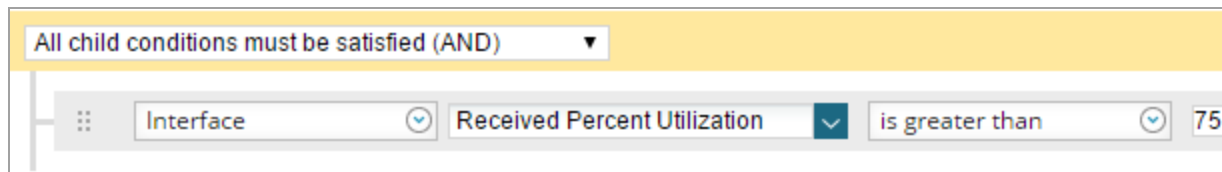


Enabled (On/Off)
 ON

Evaluation Frequency of Alert
 Evaluate the trigger condition every minutes

6. On Trigger Condition, define the conditions that trigger the alert.

Default top talker alerts trigger when the transmitted or received utilization of the interface exceeds 75%.

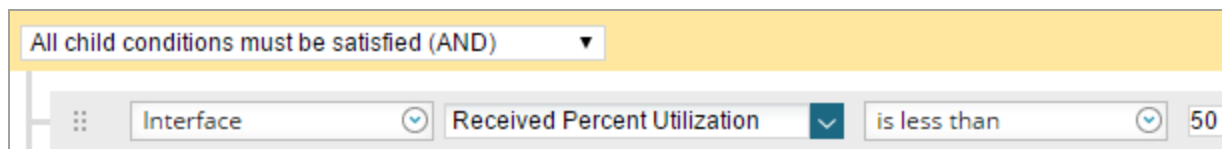


All child conditions must be satisfied (AND)

Interface Received Percent Utilization is greater than 75

7. On Reset Condition, define the conditions for resetting the alert.

Default top talker alerts are reset when the transmitted or received utilization of the interface drops below 50%. You can adjust this condition or add conditions.



All child conditions must be satisfied (AND)

Interface Received Percent Utilization is less than 50

8. On Time of Day, schedule when to run the alert.

To run the alert always, select Alert Is Always Enabled, No Schedule Needed.

9. On Trigger Actions, create actions to execute when the alert triggers.

i If there are endpoint-centric widgets on the Interface Details page when it is captured for a top talker alert notification, the links to those widgets will be non-functional in the email. The information in the alert notification is not customizable.

Trigger Actions:

Escalation Level 1 (When the alert is triggered, all actions in this level fire.)

ACTION TITLE
⋮ Copy of E-Mail a Web page (High Receive Percent Utilization is \${Interface.InPercentUtil}%)
⋮ Copy of NetPerfMon Event Log : Interface \${NetObjectName} on \${NodeName} received at \${I

10. On Reset Actions, define specific tasks to be performed when an alert is no longer active, such as writing to the log that the issue has been acknowledged.

11. Review the Summary, and click Submit.

Configure a CBQoS alert

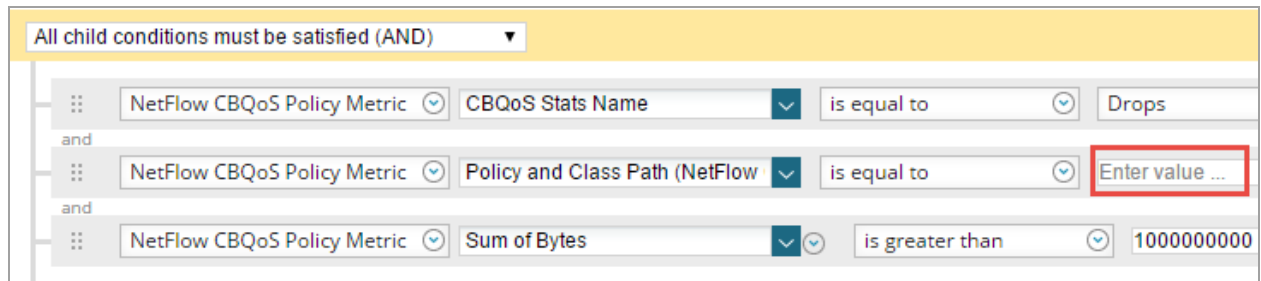
Specify the policy and class path for default CBQoS alerts. If you only enable a default CBQoS alert without configuring the trigger condition, the alert will never trigger.

1. Click Alerts & Activity > Alerts.
2. Click Manage Alerts.
3. Select a CBQoS alert, and click Duplicate & Edit.
4. Adjust the alert properties if necessary. Under Enabled, turn the alert On and select how often the trigger condition should be evaluated.

Enabled (On/Off)
 ON

Evaluation Frequency of Alert
 Evaluate the trigger condition every minutes ▼

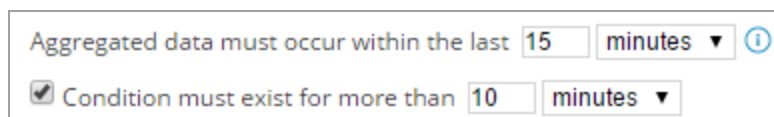
- On Trigger Condition, define the conditions that trigger the alert.
Go to the fourth field in the Policy and Class Path line, press the down key, and select a policy.



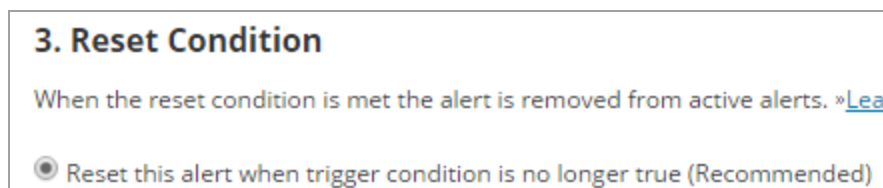
Tips

- If the class name is unique, select "includes" in the third box for Policy and Class Path, and type a unique part of the class name into the last box.
- To be alerted on all policies (Drops, Pre-Policy, or Post-Policy, based on the selection in the CBQoS Stats Name line) that exceed the specified sum of bytes, delete the Policy and Class Path line from the trigger condition.
- To be alerted on policies on a node, add a simple condition defining the node name. Select Node as the Orion Object in the first field, and Node Name as the Database column. See [Define the conditions that must exist to trigger an alert](#) in the SolarWinds Platform online help.

- To allow traffic to fluctuate and delay triggering the alert, select Condition must exist for... and adjust the number of seconds for which the condition exists.



- On Reset Condition, define the conditions for resetting the alert.



- On Time of Day, define the days and times when the software actively evaluates the database for trigger conditions.



To run the alert always, select Alert Is Always Enabled, No Schedule Needed.

9. On Trigger Actions, create actions to execute when the software triggers the alert.

The default action for all alerts is to write to the SolarWinds event log.

Trigger Actions:

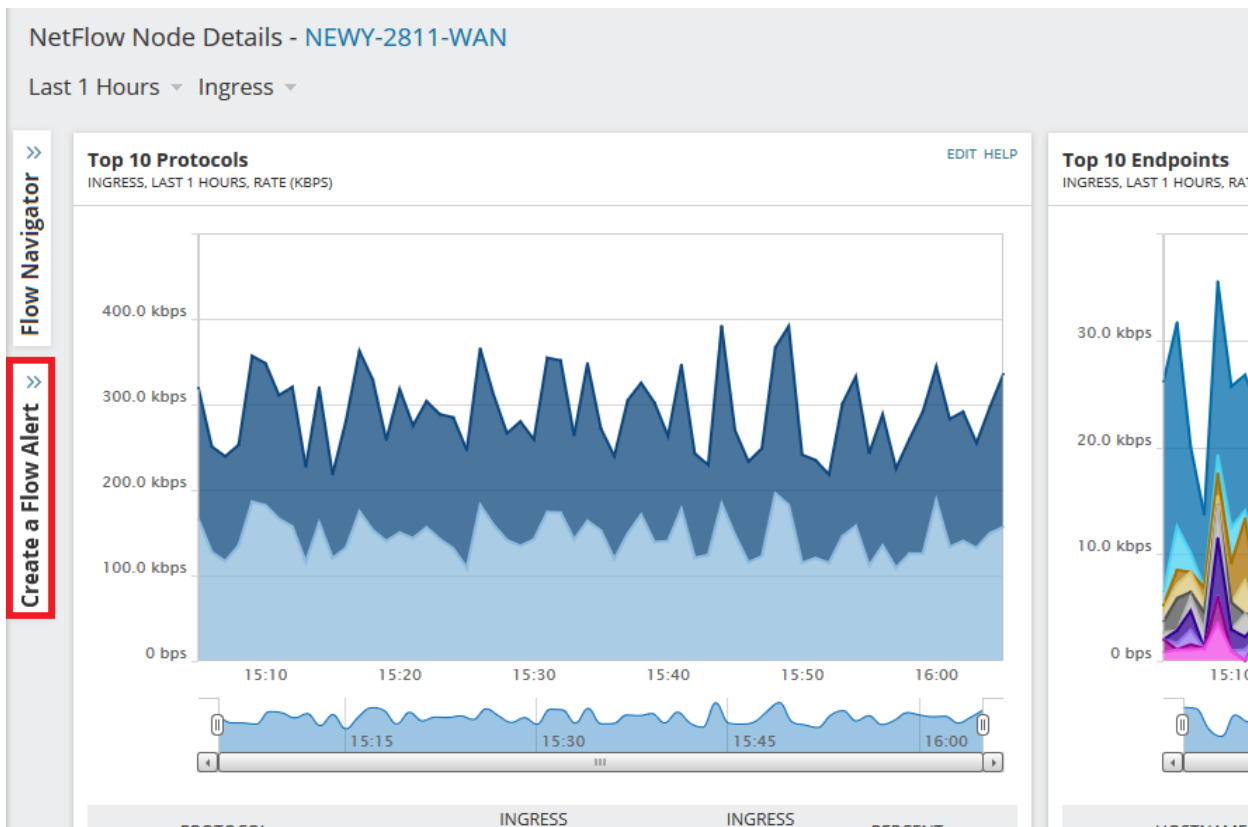
Escalation Level 1 (When the alert is triggered, all actions in this level fire.)

ACTION TITLE
<div style="font-family: monospace; font-size: 0.9em;"> ::  Copy of NetPerfMon Event Log : CBQoS <code>{N=SwisEntity;M=StatisticsDescription.StatisticsName}</code> met your alert threshold setting as a result of applying class map '<code>{N=SwisEntity;M=Policy.PolicyFullPathName}</code>' to traffic on interface '<code>{N=SwisEntity;M=Policy.Interface.Caption}</code>'. Total data dropped in the past 15 minutes: <code>{N=SWQL;M=SELECT SUM(m.Statistics.Bytes) as Bytes FROM Orion.Netflow.CBQoSPolicyMetric m WHERE m.MetricId = {N=SwisEntity;M=MetricID} AND m.Statistics.Timestamp > AddMinute(-15, GetUtcDate());F=Bytes}</code>  </div>

10. On Reset Actions, you can define actions to execute when the software resets the alert.
11. Review the Summary, and click Submit.

Configure Flow alerts

Unlike Top Talker or CBQoS alerts, Flow alerts are configured in the Create a Flow alert panel. The panel creates a standard SolarWinds Platform alert based on Custom SWQL query. If you want to change settings such as the Trigger Action, you must do so in the Advanced Alert Editor. The default values in the Create a Flow Alert panel are based on the standard Advanced Alert Editor functionality.




Configure the alert Application Threshold

The Application Threshold alert notifies you that a NetFlow-reporting node reports traffic for an application or NBAR2 application over or under a certain threshold.

- The alert can be created across multiple applications and NBAR2 applications.
- It is possible to combine applications and NBAR2 applications. The alert will be triggered when you reach the combined threshold of all selected applications.
- The threshold is compared to the average bits per second value over X minutes of flow data being checked.

1. In the SolarWinds Platform Web Console, navigate to a NetFlow Node Details or Interface Details view.

2. Open the Flow Navigator panel, click Applications or NBAR2 Applications, and set Include filters for the desired application or NBAR2 application:
 - a. In the drop-down menu, click Include.
Only Include filters are valid for this type of alert.
 - b. Select the application from the Select application drop-down menu.
The selected application filter must be set for an application that is stored through NTA Applications as an application. Filtering by port is not supported for this type of alert.
 - c. Click Add filter.
3. Click the Create a Flow Alert panel located under the Flow Navigator.
4. Verify that the filter you've set in the Flow Navigator is visible in the Create a Flow Alert panel.
5. Fill in the name of the alert in the Name field.
6. Select the severity from the Severity drop-down.
7. Under the Trigger Condition section, fill in the following fields:
 - a. In the first drop-down menu, select Trigger when application traffic exceeds a certain threshold.
 - b. Select either ingress or egress traffic.
 - c. Select the proper inequality symbol.
 - d. Insert a numeric value representing the threshold.
 - e. Select the units of bps.
8. Set the flow alert time interval.
This is the number of minutes which are supposed to be queried into the past.
9. If you want to set other options, such as the Trigger Actions, select Open this alert in Alert wizard before saving.

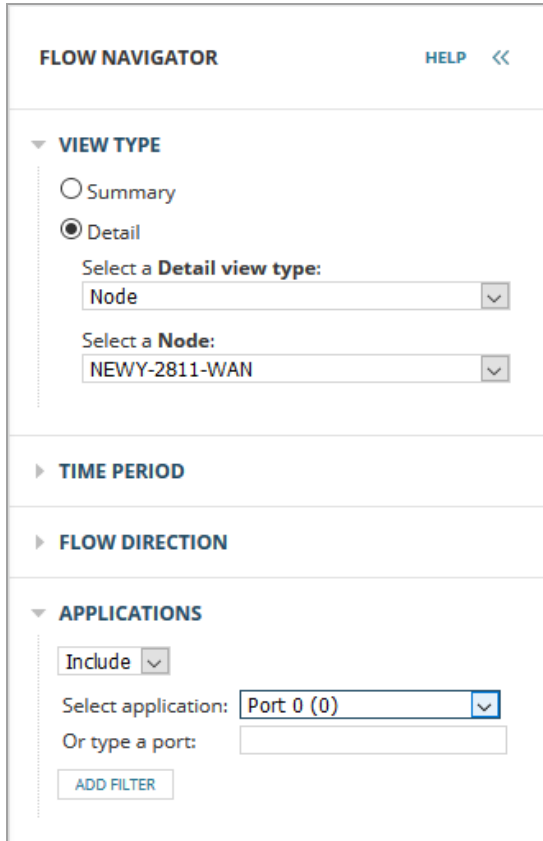
 By default, flow alerts have no trigger action, only an alert message displayed in the widgets. The alert message can be copied and pasted into a Send an Email trigger action.

10. Click Create alert.

Alert example

The below scenario assumes you are configuring an alert to notify you if ingress traffic for application Port 0 on node NEWY-2811-WAN exceeds the value of 1 Kbps in 10 minutes.

1. In the SolarWinds Platform Web Console, navigate to the NetFlow Node Details view for node NEWY-2811-WAN.
2. Open the Flow Navigator.
3. Click Applications > select Port 0 in the Select application drop-down.



FLOW NAVIGATOR HELP <<

▼ **VIEW TYPE**

Summary

Detail

Select a **Detail view type**:

Node

Select a **Node**:

NEWY-2811-WAN

▶ **TIME PERIOD**

▶ **FLOW DIRECTION**

▼ **APPLICATIONS**

Include

Select application: Port 0 (0)

Or type a port:

ADD FILTER

4. Click Add filter.
5. Open the Create a Flow Alert panel.

Note that node NEWY-2811-WAN is already selected.
6. Fill in the name of the alert in the Name field.
7. Select the severity from the Severity drop-down.
8. Under Trigger Condition, select Application traffic exceeds threshold from the drop-down.
9. Select Ingress Traffic from the drop-down.
10. Select the ">" inequality symbol from the drop-down.
11. In the following field, insert "1".
12. Select Kbps from the units drop-down.

13. Set the flow alert time interval to 10.

CREATE A FLOW ALERT HELP <<

Netflow Source

The alert will trigger on flow data received from Node **NEWY-2811-WAN**.

Alert Name

NTA Alert on NEWY-2811-WAN

Severity

Warning

Trigger Condition

Application traffic exceeds threshold

Ingress Traffic > 1 Kbps

The alert will check the last 10 minutes of Flow data.

14. Verify that you have Port 0 in the filters list.

Trigger Condition

Application traffic exceeds threshold

Ingress Traffic > 1 Kbps

The alert will check the last 10 minutes of Flow data.

For traffic matching the current Flow Navigator filters:

Included Application: **Port 0 (0)**

15. Click Create alert.

Configure the alert Application present in Top Applications / Application not present in Top Applications

This alert notifies you that an application or NBAR2 application is or is not present in Top Applications or NBAR2 Applications lists. After you create an alert for a specific application or NBAR2 application for a node or interface, the alert is triggered when the application or NBAR2 application is missing in the Top Applications or NBAR2 applications widgets.



- The alert can be created either for an application or for an NBAR2 application.
- It is **not possible** to combine applications and NBAR2 applications.
- Applications and NBAR2 applications in Top Applications are sorted by bytes.

1. In the SolarWinds Platform Web Console, navigate to a NetFlow Node Details or Interface Details view.
2. In the Flow Navigator, click Applications and select the desired application from the Select application drop-down menu.

The selected application filter must be set for an application that is stored through NTA Applications as an application. Filtering by port is not supported for this type of alert.

Only Include filters are valid for this type of alert. The options is selected by default.

3. Click Add filter.
4. Open the Create a Flow Alert panel.
5. Fill in the name of the alert in the Name field.
6. Select the severity from the Severity drop-down.
7. Under Trigger Condition, select one of the following options, depending on what you want to be alerted on:
 - Application present in Top Applications.
 - Application not present in Top Applications.
8. Select if you want to monitor ingress or egress traffic.
9. Enter the number of applications you want to be alerted on.
10. Set the flow alert time interval.

This is the number of minutes which are supposed to be queried into the past.

11. If you want to set other options, such as the Trigger Actions, select Open this alert in Alert wizard before saving.

i By default, flow alerts have no trigger action, only an alert message displayed in the widgets. The alert message can be copied and pasted into a Send an Email trigger action.

12. Click Create alert.

Alert example

The below scenario assumes you are configuring an alert to notify you that the application World Wide Web HTTP 80 on interface Gig0/0.204 of node NEWY-2811-WAN is present in Top Applications.

1. In the SolarWinds Platform Web Console, navigate to the NetFlow Interface Details view for Interface Gig0/0.204 of node NEWY-2811-WAN.
2. Open the Flow Navigator.
3. Click Applications > select World Wide Web HTTP 80 in the Select application drop-down.

FLOW NAVIGATOR
HELP <<

VIEW TYPE

Summary

Detail

Select a **Detail view type**:

Interface ▼

Select a **Detail view**:

NetFlow Interface Details ▼

Select a **Node**:

NEWY-2811-WAN ▼

Select an **Interface**:

Gig0/0.204 ▼

TIME PERIOD

FLOW DIRECTION

APPLICATIONS

Include ▼

Select application: World Wide Web HTTP ▼

Or type a port:

[ADD FILTER](#)

4. Click Add filter.

5. Open the Create a Flow Alert panel.
Note that node NEWY-2811-WAN and Interface Gig0/0.204 (if-4) are already selected.
6. Fill in the name of the alert in the Name field.
7. Select the severity from the Severity drop-down.
8. Under Trigger Condition, select Application present in Top Applications from the drop-down.
9. Select Ingress Traffic from the next drop-down.
10. Insert the number 5 into the field Number of top Applications.
11. You can leave the time interval as it is.
12. Verify that you have World Wide Web HTTP 80 in the filters list.

CREATE A FLOW ALERT
HELP <<

Netflow Source

The alert will trigger on flow data received from Node **NEWY-2811-WAN** Interface **if-4**.

Alert Name

Severity

Trigger Condition

Ingress Traffic Applications

The alert will check the last minutes of Flow data.

For traffic matching the current Flow Navigator filters:

Included Application: **World Wide Web HTTP (80)**

13. Click Create alert.

Configure the alert NetFlow source not receiving any data

This alert notifies you that a device (node or interface) is not sending data over a defined time period. The alert is created on a monitored node or interface. In case the alert is triggered on a node, none of the monitored interfaces is sending flow data. This means that if the node includes an interface that does send NetFlow data, the alert is not triggered.

- In case the node or interface is Unmanaged during the monitored period, the alert is not triggered.
- In case the NetFlow Service was down during the monitored period, the alert is not triggered.

1. In the SolarWinds Platform Web Console, navigate to a NetFlow Node Details or Interface Details page.
2. Open the Create a Flow alert panel.
3. Fill in the name of the alert in the Name field.
4. Select the severity from the Severity drop-down.
5. Select Flow no longer being received from the Trigger Condition drop-down.
6. Set the flow alert time interval.

This is the number of minutes which are supposed to be queried into the past.

7. If you want to set other options, such as the Trigger Actions, select Open this alert in Alert wizard before saving.

i By default, flow alerts have no trigger action, only an alert message displayed in the widgets. The alert message can be copied and pasted into a Send an Email trigger action.

8. Click Create alert.

Alert Example

The below scenario assumes you are configuring an alert to notify you that the node NEWY-2811-WAN is not sending flow data to SolarWinds NTA.

1. In the SolarWinds Platform Web Console, navigate to the NetFlow Node Details view for node NEWY-2811-WAN.
2. Open the Create a Flow Alert panel
3. Fill in the name of the alert in the Name field.
4. Select the severity from the Severity drop-down.

5. Under Trigger Condition, select Flow no longer being received from the drop-down.
6. You can leave the time interval as it is.

CREATE A FLOW ALERT
HELP <<

Netflow Source

The alert will trigger on flow data received from Node **NEWY-2811-WAN**.

Alert Name

Severity

Trigger Condition

The alert will check the last minutes of Flow data.

i **There are more options available.** Open this alert in Alert wizard to configure email sending, time frames, and more.

Open this alert in Alert wizard before saving.

7. Click Create alert.

Troubleshoot with NTA

In NTA, you can encounter various issues, such as NetFlow issues, chart issues, database connection issues, or CBQoS issues.

NetFlow issues

For troubleshooting NetFlow issues, you can consult the following NTA widgets:

NetFlow collector services

This widget informs you whether the collector service is up or down. For more information, see [NetFlow Collector Services](#).

Flow and CBQoS sources

This widget lists devices from which NTA is receiving flows, together with the time stamp of the latest received NetFlow or CBQoS data. You can drill down to individual interfaces to pinpoint the problem. For more information, see [Flow and CBQoS Sources](#).

Last xx events

This widget provides details about everything that happens in NTA. For more information, see [Last XX Traffic Analysis Events](#).

Chart issues

For more information about resolving chart issues, such as charts displaying duplicate traffic, see [NTA chart issues](#).

CBQoS issues

For more information about troubleshooting CBQoS, see [CBQoS issues in NTA](#).

NetFlow Collector Services

The NetFlow Collector Services widget provides status information about the servers on which you have installed NetFlow Traffic Analyzer to collect flow and CBQoS information.

The following information about the collectors and the ports on which they are listening for flow and CBQoS data is provided in the table:

Column	Explanation
Status Icon	Displays collector status visually, where a green icon indicates that the collector can actively receive flow and CBQoS data and a red icon indicates that the collector cannot actively receive flow and CBQoS data.
Server Name	The network identification of the NetFlow collector.
Receiver Status	A verbal statement of collector status.
Collection Port	This is the port on which the NetFlow collector is listening for NetFlow data. The collection port is set during the installation and configuration of NetFlow Traffic Analyzer.

Edit or add collection ports in NTA

You can change the port NTA is listening for flow packets at, or add an additional port on the Edit NetFlow Collector Services page.

1. Click Edit on the NetFlow Collector Services widget.
2. Change the collection port, or add another collection port by separating listed ports with a single comma. For example: 2055,9995.
3. Click Submit.

Delete collectors in NTA

If you have stale records in your database, for example if a poller breaks down, or if you replace a poller, the information about collectors may be inaccurate. Delete unused collectors.

If the NetFlow service is still running on the server, deleting the collector in this widget is temporary. In 15 minutes, the collector will be added again with the default port 2055. If you had more or non-default ports defined for the collector, you will need to adjust the default setting.

Delete a collector permanently

1. Log in to the appropriate server.
2. Uninstall NTA.
3. Delete the collector in the NetFlow Collector Services widget.

Delete a collector in the NetFlow Collector Services widget

1. Click Delete next to the collector.
2. Click Submit.

For more information about configuring your collectors, see [NetFlow collector services](#).

Troubleshoot collector services in NTA

Problems with the NetFlow service are reflected in the Collector Services widget. If your collector service status is down or unknown, you can troubleshoot it using the SolarWinds Platform Service Manager.

1. Start the SolarWinds Platform Service Manager through Start > SolarWinds Orion > Orion Service Manager.
2. Check that the SolarWinds NetFlow Service has the status Started.
3. If the SolarWinds NetFlow Service is not started, select it, and then click Start. You can also start the service in the Windows Task Manager or in the Windows Services tool.
4. If the SolarWinds NetFlow Service starts and stops again, there is an underlying reason causing it to fail, such as an issue with the connection to the database. Make sure the connection is working, and that the appropriate database server has sufficient CPU and memory available.
5. As a final attempt to reconcile the SolarWinds NetFlow Service, start the Configuration wizard in the SolarWinds Platform program folder, select all three components (Database, Website, and Services), and complete the wizard. If it fails, open a ticket with [SolarWinds Support](#).

NetFlow collector services

The **Edit NetFlow Collector Services** page provides status information about the NetFlow collectors that are running NetFlow Traffic Analyzer. The following information about the collectors and the ports on which they are listening for NetFlow data is provided in the table:

Status Icon

Displays collector status visually, where a green icon indicates that the collector can actively receive NetFlow data and a red icon indicates that the collector cannot actively receive NetFlow data.

Server Name

The network identification of the NetFlow collector.

Receiver Status

A verbal statement of the collector status.

Collection Port

This is the port on which the NetFlow collector is listening for NetFlow data. The collection port is set during the installation and configuration of NetFlow Traffic Analyzer. Designate additional collection ports by listing port numbers separated by commas.

Clicking Delete to the right of any listed collector ends traffic analysis on the selected collector.

For more information about configuring collector services, see [NetFlow collector services](#).

Flow and CBQoS Sources

The Flow and CBQoS Sources widget provides a list of flow- and CBQoS-enabled nodes and interfaces that are currently monitored by NTA. For each listed device, the Flow and CBQoS Sources widget provides the following details:

- A color-coded device status icon
- An icon indicating the device type or manufacturer
- For each listed source interface, both the incoming and outgoing traffic volume
- For all listed flow-enabled devices, the date and time of the last flow packet received by the NTA collector
- For all listed CBQoS-enabled devices, the date and time of the last CBQoS poll completed by the NTA collector

Status icon colors

Device status icons are color-coded as indicated in the following table.

Icon Color	Device Status Indication
Green	The selected source is either able to actively send flow data or it is currently able to provide CBQoS information.
Yellow	Device status is unknown, flow data has not been received, or CBQoS information cannot be polled from the selected device. This color may be displayed for interfaces on a Down node, as it is impossible to determine interface status when the parent node is down.
Red	The selected device is unable to actively provide flow or CBQoS data.

Troubleshoot Flow and CBQoS Sources

In the Flow and CBQoS Sources widget, you can encounter various issues.

Devices not listed in the widget

If you are not seeing expected flow- or CBQoS-enabled devices in the Flow and CBQoS Sources widget, confirm that the following is true for your flow- and CBQoS-enabled devices:

- Confirm that the automatic addition of NetFlow sources option is enabled on the NetFlow Traffic Analysis Settings view. For more information, see [Enable the automatic addition of flow sources](#).
- Flow-enabled nodes and interfaces must be monitored by NPM before they can be recognized in as flow sources in NTA. For more information about adding devices for monitoring by NPM, see [Add flow-enabled devices and interfaces to the SolarWinds Platform database](#).
- Flow-enabled devices must be configured to send flow data to the NPM server on which you have installed NTA. For more information about configuring devices to send flows to NTA, see [Device configuration examples for NTA](#).
- Confirm that the SolarWinds NetFlow Service has been started in the Windows Services listing. To view a list of services, log on to your NTA server as an administrator, and then open Control Panel > Administrative Tools > Services.

Time stamp "never" or not up to date

If the time stamp of the last received NetFlow or CBQoS data is not as expected, click Manage Flow Sources to confirm that flow monitoring is enabled for the appropriate device and interfaces. For more information, see [Flow sources and CBQoS polling](#).

View more details about displayed objects

Clicking + next to a listed node expands the list of interfaces on the selected parent node.

Clicking a node name opens the NetFlow Node Details view for the selected node. For more information, see [NetFlow Node Details View](#).

Clicking an interface name opens the NetFlow Interface Details view for the selected interface. For more information, see [NetFlow Interface Details View](#).

Edit the widget

Click Manage Flow Sources to go to the Flow Sources management page where you can select available flow sources and CBQoS-enabled devices. For more information, see [Flow sources and CBQoS polling](#).

1. Click Edit in the widget header.
2. Edit the Title.
3. Select or clear Show Flow Sources and Show CBQoS Sources.
4. Click Submit.

Troubleshoot Long Flow Errors in NTA

Invalid flow errors recorded in the NetFlow Traffic Analyzer may result when a flow duration exceeds the cache timeout values. This condition displays the following event in the Last XX Traffic Analyzer Events widget:



To resolve this error, the following lines must appear in the Flow Monitor section of the Configuration file for Flow Records on Cisco devices:

```
cache timeout inact 10
```

```
cache timeout act 5
```

For additional information, see [Configuring Devices for Flow Collection](#) in the online help.

Events in NTA

Events is a simple troubleshooting tool that gives an overview of everything important that happens in NTA. If you feel NTA is not showing expected results, consult the Last XX Traffic Analyzer Events and pay attention to red and grey events. For more details, see the [Last XX Traffic Analysis Events](#) widget.







Access Events

Click Alerts & Activity > Events.

What details do events provide?

- The time stamp informs you when the event occurred (1).
- Event icons help you distinguish whether it is just an information, warning, or an error message. The background color of the event icon informs you about how serious the event is (2).

- The event description provides details about objects relevant for the event (3).

TIME OF EVENT ¹	MESSAGE ³
<input type="checkbox"/> 10/7/2021 1:30 AM	 NetFlow Database Maintenance : Deleted 0 expired endpoints in 0.04 seconds. ²
<input type="checkbox"/> 10/6/2021 1:30 AM	 NetFlow Database Maintenance : Deleted 0 expired endpoints in 0.01 seconds.
<input type="checkbox"/> 10/5/2021 1:30 AM	 NetFlow Database Maintenance : Deleted 0 expired endpoints in 0.04 seconds.
<input type="checkbox"/> 10/4/2021 1:30 AM	 NetFlow Database Maintenance : Deleted 0 expired endpoints in 0.01 seconds.
<input type="checkbox"/> 10/3/2021 1:30 AM	 NetFlow Database Maintenance : Deleted 0 expired endpoints in 0.01 seconds.
<input type="checkbox"/> 10/2/2021 1:30 AM	 NetFlow Database Maintenance : Deleted 0 expired endpoints in 0.01 seconds.

Event colors

Red events indicate errors that need your immediate attention.

Green events inform you that a task has been successfully completed.

Blue events provide system information.

Grey events inform you about a situation that requires an action (unmanaged nodes, interfaces,)

Yellow events are informative, you do not need to take any action.

Last XX Traffic Analyzer Events

This widget provides a list of the last NTA events. These events can include but are not limited to stopping or starting the NetFlow Receiver service and the reception of NetFlow data on an unmonitored interface.

For more information about events, see [Events in NTA](#).

Depending on the type of event, clicking a link in a listed event may open an NPM view.

Edit the widget

1. Click Edit in the widget header.
2. In Maximum number of items to display, enter the number of events shown in the widget.
3. Click Submit.

Errors



NetFlow Receiver Service Stopped

NTA informs you that SolarWinds NetFlow Service stopped.

"NetFlow Receiver Service [service name] Stopped."

To resolve the issue, restart the SolarWinds NetFlow Service:

1. Start the SolarWinds Platform Service Manager in the SolarWinds Orion > Advanced Features program folder.
2. Check the status of the SolarWinds NetFlow Service.
3. If it is stopped, select it, and then click Start.

License limitation

NTA informs you that your NTA license does not match your NPM license, and NTA thus cannot monitor your flow traffic.

```
"License limitation doesn't fit Orion license!"
```

To resolve this event, make sure your NTA license matches your NPM license. Both NPM and NTA must be at the same license level. For more information, see [Licensing SolarWinds](#).

No valid license

NTA informs you that your license is expired.

```
"License status check failed: no valid license were found for [license key not in brackets]"
```

To resolve this event, log in to the SolarWinds customer portal, and procure an appropriate NTA license.

Invalid template

NTA informs you that incoming NetFlow v9 flows have a wrong or invalid template.

```
"NetFlow Receiver Service [xy] received an invalid v9 template with ID xx from device x.x.x.x. See knowledge base for more information."
```

Resolve the issue

1. Log in to the appropriate device and check the template.
2. Make sure the device exports an appropriate template in one-minute intervals. For more information, see [Device configuration examples](#).
3. Make sure the template includes all required details. For more details, see [Required Fields](#).

Invalid IPFIX template

NTA informs you that the IPFIX template does not include required fields.

```
"NetFlow Receiver Service [xy] received an invalid IPFIX template with ID XX from device x.x.x.x. "
```

Resolve the issue

1. Log in to the appropriate device and check the template.
2. Make sure the device exports an appropriate template in one-minute intervals. For more information, see [Device configuration examples](#).
3. Make sure the template includes all required details. For more details, see [Required Fields](#).

NetFlow time difference error

This event informs you that the time difference between your servers (SolarWinds Platform database server, NTA Flow Storage database, and the NTA Service server) is above the critical threshold. The critical threshold is hard-coded to 300s.

```
"Time on NetFlow Receiver Service [xy] is: xxx. DB server time is xx. The difference is: 719 s. Which is above critical threshold. The data won't be correct. Synchronize the clocks and restart the service."
```

To resolve the issue, synchronize time settings on all servers (SolarWinds Platform database, NTA polling engine(s), and NTA Flow Storage database server).

Cannot connect to NTA Flow Storage database.

This event informs you that NTA Flow Storage database is currently unavailable.

```
"Cannot connect to NTA Flow Storage database. NTA cannot save any flows now."
```

Resolve the issue

Make sure that the NTA SQL Flow Storage database server is running and online. For tips on troubleshooting issues with the SQL database, see [Best practices and troubleshooting for the SolarWinds Platform database](#) in the SolarWinds Platform documentation.

Warnings

Unmanaged NetFlow Node

This event informs the user that NTA is receiving NetFlow traffic from a node which is not managed in NPM.

```
"NetFlow Receiver Service [xy] is receiving NetFlow data stream from an unmanaged device (x.x.x.x). The NetFlow data stream from x.x.x.x will be discarded. Please use Orion Node management to manage this IP address in order to process this NetFlow data stream, or just use Manage this device."
```

Resolve the issue

Click **Manage This Device** and complete the **Add Node** wizard to add the node in NPM. For more information, see [Adding Devices for Monitoring in the Web Console](#) in the SolarWinds Network Performance Monitor Administrator Guide.



Unmanaged NetFlow Interface

This event informs you that NTA is receiving traffic from an interface which is not managed in NPM. However, the corresponding node is managed in NPM. Click **Add this interface** or **Edit this interface** to add the object to NPM for monitoring.

"NetFlow Receiver Service [xy] is receiving NetFlow data from an unmanaged interface 'interface1name To interface2name'. Click [Add this interface](#) or [Edit this interface](#) to manage interface and process its flow data."

Resolve the issue

Click **Add This Interface** or **Edit This Interface**, and add the interface to NPM for monitoring. For more information, see [Adding Devices for Monitoring in the Web Console](#) in the SolarWinds Network Performance Monitor Administrator Guide.



Unmonitored NetFlow Interface

NTA informs you that it is receiving flow traffic from an interface, which is managed in NPM, but not monitored in NTA. This happens if the **Enable Automatic Addition of NetFlow Sources** in NTA Settings is disabled.

"NetFlow Receiver Service [xy] is receiving NetFlow data from unmonitored interface if name on node. Click [Monitor NetFlow source](#) or enable the ["Automatic addition of NetFlow sources"](#) option on the Netflow Settings page to process future NetFlow data from this interface."

Resolve the issue

1. Click **Monitor NetFlow Source** and enable monitoring for the interface. For more details, see [Add flow sources and CBQoS-enabled devices](#).
2. Click **Automatic Addition of NetFlow Sources** and make sure the **Enable Automatic Addition of NetFlow Sources** option is selected. For more information, see [Enable flow monitoring from unmanaged interfaces](#).

Not Primary NPM Node IP Address

This event informs you that the mentioned node has more IP addresses and that the IP address through which flow data are coming is not used for polling purposes.

NetFlow Receiver Service [xy] is receiving NetFlow data from an NPM device name (device IP address) through an IP address that is not its primary IP address. The NetFlow data will be discarded. Enable the Match NetFlow devices also by not primary IP Address option to process NetFlow data from this device.

Resolve the issue

Follow the link to NetFlow Settings and make sure the Allow Matching Nodes by Another IP Address option is selected. For more information, see [Enable flow monitoring from unmanaged interfaces](#).

Unmonitored NetFlow Interface Automatically Added

NTA informs you that an unmonitored interface has been added into NetFlow sources automatically. This happens if you enabled the Enable Automatic Addition of NetFlow Sources option in the NTA Settings. For more information, see [Enable the automatic addition of flow sources](#).

"NetFlow Receiver Service [xy] is receiving NetFlow data from an unmonitored interface. The interface if name on service is being added to NetFlow sources."

NetFlow time difference warning

This event informs you that there is a time difference between your database and NTA servers, but it does not exceed the critical threshold.

"Time on NetFlow Receiver Service [xy] is: xxx. DB server time is xx. The difference is: xxx s. Which is above threshold. Fetched data could be unreliable."

To prevent corrupt data, synchronize time settings on all servers:

- SolarWinds Platform database
- NTA polling engine(s)
- NTA Flow Storage database server

NetFlow time difference warning ended

This event informs you that the time difference between the database server and NTA server has been resolved and the server times have been synchronized.

"Time on NetFlow Receiver Service [xy] is: xx, DB server time is: xx. The difference is: 0s. Which is under warning threshold"

System information

NetFlow Receiver Service Started

NTA informs you that the NetFlow service has been started. This event is triggered when the SolarWinds NetFlow Service starts.

```
"NetFlow Receiver Service [service name] started - listening on port(s) [port number(s)]."
```

NetFlow Receiver Service settings changed

NTA informs you if the port it is listening on has changed, or if a new port has been added. For more information, see [NetFlow Collector Services](#).

```
"NetFlow Receiver Service [service name] setting was changed - listening on port (s) [port number(s)]."
```

NetFlow Event: Interface index mapping is being used for node.

NTA informs you that a new device using interface index mapping has been added for monitoring in NTA.

```
Interface index mapping is being used for node [node name].
```

SNMP index is a value identifying a specific interface. Flows coming from this device are using different values than SNMP interface indexes and NTA thus needs to establish a relation between the interface index and the values included in these flows.

NetFlow Event: Removing interface index mapping for node.

NTA informs you that interface index mapping has been removed for a node.

```
Removing interface index mapping for node [node name].
```

For more information, see [NetFlow event: interface index mapping used for a node](#).

NetFlow database maintenance

NTA informs you that the database maintenance has been completed.

```
NetFlow Database Maintenance: Deleted x expired endpoints in x.xx seconds. For more information, see SolarWinds Platform database maintenance.
```

Scheduled shrink performed

NTA informs you that the SolarWinds Platform database has been compressed.

```
Scheduled shrink performed. DB size before shrink xMB, DB size after shrink xMB, released space xMB. For more information, see SolarWinds Platform database maintenance.
```

Updating data to be used in Top XX Aggregated widgets

NTA informs you that data aggregation settings for Top XX applications, Top XX Conversations or Top XX Endpoints has been changed.

Updating data to be used in showing Top [x] [Conversations, Applications, or Endpoints].

This event only occurs in NTA 4.0 using SQL for storing flows and in older NTA versions.

Windows Firewall is turned on

NTA informs you that the NetFlow service has started or restarted and it is blocked by a firewall.

"Windows FireWall is turned on and its current exceptions do not allow the NetFlow Service to receive packets. Run the Configuration wizard for Services to remedy."

Resolve the issue

Complete the Configuration wizard for Services:

1. Start the Configuration wizard in the SolarWinds Orion > Configuration and Auto-Discovery program folder.
2. Select Services and complete the wizard.

Information

NetFlow Licensing

NTA informs you that you are running an evaluation version, which has not been licensed yet.

Your SolarWinds NetFlow Receiver Service Evaluation [receiver name] will expire in x days. Please contact SolarWinds support to purchase a licensed version.

Thank you.

To resolve the issue, purchase a license and activate it. Your SolarWinds licenses can be activated directly during the installation process. However, SolarWinds also provides a powerful License Manager which allows you not only to activate your licenses, but also deactivate a license on a certain machine and re-activate it elsewhere.

Unable to start listening on port

NTA informs you that the port NTA is listening at is being used by another listener. NTA thus cannot collect flows.

Unable to start listening on port x. Waiting until the port is free.

Resolve the issue

1. Log in to the device and check what applications use the port NTA is using. Port 2055 is the default.
2. If the port is being used by another application, close the application.
3. If the port is being used only by the SolarWinds NetFlow Service, restart the service:
 - a. Start the SolarWinds Platform Service Manager in the SolarWinds Orion > Advanced Features program folder.
 - b. Check the status of the SolarWinds NetFlow Service.
 - c. If it is stopped, select it, and click Start.

Port is free, listening

NTA informs you that the port it is listening at is free again, and that the issue has been resolved.
`Port x is free, listening.`

Notification Event Status Reset

NTA informs you that you have reset the Last 200 Events view by clicking Clear Notification.
`"Resetting unknown traffic notifications events."`

For more information about seeing cleared events, see [Filter events and display historical events in NTA](#).

Connection to NTA Flow Storage database has been restored.

This event is triggered when the connection to NTA Flow Storage database is restored.

Filter events and display historical events in NTA

You can view your events in the Last XX Traffic Analyzer Events widget which is available on all NetFlow summary views.

If you want to adjust the number of events to display or want to display only certain events, you can do so on the Events view.

If you want to see only unknown traffic events, click NetFlow Settings in any NetFlow view, and Under NetFlow Management click Show Unknown Traffic Events. For more information about unknown traffic, see [Resolve unknown NetFlow traffic](#).

Filter all events

1. Click Alerts & Activity > Events.
2. You can further filter events by:
 - a. Network Object or Type of Device
 - b. Event Type

The table below provides event types relevant for NTA events, and the corresponding events.
 - c. Time Period
3. If you want to see cleared events, select Show Cleared Events.
4. If desired, edit the Number of Displayed Events.
5. Click Refresh.

Event Type	Events
NetFlow Receiver Service Started	NetFlow Receiver Service Started NetFlow Receiver Service Settings Changed
NetFlow Receiver Service Stopped	NetFlow Receiver Service Stopped License Limitation No Valid License
Unmanaged NetFlow Node	Unmanaged NetFlow Node
Unmonitored NetFlow Interface Automatically Added	Unmonitored NetFlow Interface Automatically Added
NetFlow Event	NetFlow Event Interface Index Mapping Is Being Used for Node NetFlow Event: Removing Interface Index Mapping for Node NetFlow Database Maintenance Scheduled Shrink Performed Updating Data to Be Used in Top XX Aggregated widgets Windows Firewall Is Turned on

Event Type	Events
Unmanaged NetFlow Interface	Unmanaged NetFlow Interface
Unmonitored NetFlow Interface	Unmonitored NetFlow Interface
Invalid Template	Invalid Template
	Invalid IPFIX Template
No Template Received	No Template Received
Unsupported Incoming Flow	Unsupported Incoming Flow
Not Enabled NetFlow Data Export	Not Enabled NetFlow Data Export
ICMP NetFlow Node	ICMP NetFlow Node
Not Primary NPM Node IP Address	Not Primary NPM Node IP Address
Notification Reset	Notification Event Status Reset
NetFlow Licensing	NetFlow Licensing
Informational	Unable to Start Listening on Port
	Port Is Free, Listening
NetFlow service time difference warning	NetFlow service time difference warning
	NetFlow service time difference warning ended
NetFlow service time difference error	NetFlow Service time difference error

Clear events in NTA

If there are too many events on your Last 200 Unknown Traffic Events view and you have resolved the relevant ones, you can clear the events. Clearing events helps you find out which events have been resolved successfully.

1. In the SolarWinds Platform Web Console, click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Under NetFlow Management, click Show Unknown Traffic Events.
4. Click Clear Notifications.

This will clear events from this view and from the Events view. However, the Last XX Traffic Analyzer Events widgets still show the last items and include the following event:



Notification Event Status Reset

"Resetting unknown traffic notifications events."

5. Click Refresh Events. Unresolved events will appear in the Last 200 Unknown Events view again.

It might take a few minutes until unresolved events return to the list.

Unresolved events return to the list if you refresh the page.

Display resolved events that were cleared

1. Click Alerts & Activity > Events.
2. Define what events you want to see. For more details, see [Filter events and display historical events in NTA](#).
3. Select Show Cleared Events.
4. Click Refresh.

Error: NetFlow service inaccessible

This error informs you that the SolarWinds NetFlow Service is not running.

This error might be triggered by various causes, such as a licensing error. You can usually resolve the issue by restarting the NetFlow Service.

Make sure your NTA license is valid and has been activated. See [License SolarWinds Platform products in the SolarWinds Platform Web Console](#).

Start the NetFlow service

1. Start the SolarWinds Platform Service Manager in the SolarWinds Platform program folder.
2. Click Start Everything to start all stopped services.

Error: No template received

If you are receiving NetFlow v9 flows from a device without an appropriate template for longer than 15 minutes, NTA displays this error:

```
"NetFlow Receiver Service [xy] received NetFlow v9 flows without any template for decoding them. Configure the device x.x.x.x to export an appropriate NetFlow v9 template at 1-minute intervals. See help for details."
```

Resolve the issue

1. Log in to the appropriate device and check the template.
2. Make sure the device exports an appropriate template in one-minute intervals. For more information, see [Device configuration examples](#).
3. Make sure the template includes all required details. For more details, see [Required Fields](#).

For more information about appropriate commands, see documentation of the device.

Required fields in SolarWinds NTA

Most flow-enabled devices use a set of static templates to which exported flows conform.

If flow packets do not include the following field types and appropriate values, NTA ignores the packets.

Requirements

- The template must include all mandatory fields.
- Where multiple elements are in a group, at least one of them must be included.
- Optional fields are processed into flows if present. If not present, a default value is used.

For more information about fields required for sampled flows, see [Sampled flow supported fields](#).

Mandatory fields for the flow template schema

Mandatory fields are required. If a mandatory field, or at least one field from a group, is not included NTA cannot store flows.

Field Type	Field Type Number	Description
Protocol	4	Layer 4 protocol
SourceAddress	8, 27	Source IP address or source IPv6 address
DestAddress	12, 28	Destination IP address or destination IPv6 address
Interfaces Group		
At least one of the following fields must be included in the template.		
InterfaceRx	10	SNMP ingress interface index
InterfaceTx	14	SNMP egress interface index

Field Type	Field Type Number	Description
------------	-------------------	-------------

Bytes Group

At least one of the following fields must be included in the template.

Bytes	1	Delta bytes
Bytes	85	Total bytes
OutBytes	23	Out bytes
InitiatorOctets	231	Initiator bytes
ResponderOctets	232	Responder bytes

Optional fields for the flow template schema

If the following fields are not included in the template, a default value will be stored. Appropriate widgets will thus show *No Data*.

Field Type	Field Type Number	Description
ToS	5	Type of service
SourceAS	16	Source BGP autonomous system number
DestAS	17	Destination BGP autonomous system number
PeerSrcAS	129	Peer source autonomous system number
PeerDstAS	128	Peer destination autonomous system number
ApplicationID	95	ID of application detected in NBAR2 flow

Source Port Group

At least one of the following fields should be included in the template.

SourcePort	7	Source TCP/UDP port
UdpSrcPort	180	Source UDP port
TcpSrcPort	182	Source TPC port

Field Type	Field Type Number	Description
------------	-------------------	-------------

Destination Port Group

At least one of the following fields should be included in the template.

DestPort	11	Destination TCP/UDP port
UdpDstPort	181	Destination UDP port
TcpDstPort	183	Destination TPC port

Packets Group

At least one of the following fields should be included in the template. If no field is included, widgets will show 0 in the packets column.



Packets	2	Delta packets
Packets	86	Total packets
OutPackets	24	Out packets
InitiatorPackets	298	Total packets in a flow from the device that triggered the session and remains the same for the life of the session
ResponderPackets	299	Total packets from the device which replies to the initiator

Long Flow Detection

At least one of the following field pairs should be included in the template for long-flow detection. For example, if including LastSwitched must also include FirstSwitched.

LastSwitched	21	System uptime at which the last packet of this flow was switched
FirstSwitched	22	System uptime at which the first packet of this flow was switched
FlowStartSeconds	150	Time in seconds that the flow started
FlowEndSeconds	151	Time in seconds that the flow ended
FlowStartMilliseconds	152	Time in milliseconds that the flow started
FlowEndMilliseconds	153	Time in milliseconds that the flow ended

Field Type	Field Type Number	Description
FlowStartMicroseconds	154	Time in microseconds that the flow started
FlowEndMicroseconds	155	Time in microseconds that the flow ended
FlowStartNanoseconds	156	Time in nanoseconds that the flow started
FlowEndNanoseconds	157	Time in nanoseconds that the flow ended
FlowStartDeltaMicroseconds	158	Sets the start delta of the flow
FlowEndDeltaMicroseconds	159	Sets the end delta of the flow
FlowDurationMilliseconds	161	Elapsed time in milliseconds of the flow
FlowDurationMicroseconds	162	Elapsed time in microseconds of the flow
Cisco WLC Flows		
The following fields must be included for Cisco Wireless devices.		
Bytes	1	Total bytes
Packets	2	Total packets
FlowDirection	61	Direction of the flow defined as Ingress or egress.
ApplicationID	95	ID of application detected in flow
WlanSSID	147	Service Set Identifier or name of the WLAN the wireless device is connected to
WirelessStationMacAddress	365	MAC address of a wireless device
WirelessAPMacAddress	367	MAC address of a wireless access point

Field Type	Field Type Number	Description
PostIPDiffServCodePoint	98	The definition of this Information Element is identical to <code>ipDiffServCodePoint</code> , except that it reports a potentially modified value caused by a middlebox function after the packet passed the Observation Point.
 As of NTA 2023.1, this field is optional.		
IPDiffServCodePoint	195	Value of a Differentiated Services Code Point (DSCP) encoded in the Differentiated Services field. Differentiated Services field is the most significant six bits of the IPv4 TOS FIELD or the IPv6 Traffic Class field. The value may range from 0 to 63 for this Information Element that encodes only the 6 bits of the Differentiated Services field.
 As of NTA 2023.1, this field is optional.		
Cisco WLC Flows		
At least one of the following fields should be included in the template.		
WirelessStationAddressIPv4	366	IPv4 address of a wireless device
IPv4SourceAddress	8	Source IPv4 address
IPv4DestinationAddress	12	Destination IPv4 address
Cisco ASA devices		
The following fields must be included for processing flows from Cisco ASA devices.		
FlowID	148	An identifier of a flow that is unique within an observation domain.
FirewallEvent	233	Indicates a firewall event.
NAT Group		
The following fields must be included for NAT stitching		
Post-NAT Source IPv4	225	Source IP address for Network Address Translation (NAT).

Field Type	Field Type Number	Description
Post-NAT Destination IPv4	226	Destination IP address for Network Address Translation (NAT).
Post-NAT Source Port	227	Source port for Network Address Translation (NAT).
Post-NAT Destination Port	228	Destination port for Network Address Translation (NAT).

Notes

- If SolarWinds states that NTA supports flow monitoring for a device, at least one of the templates that the device exports satisfies these requirements.
- The NetFlow v9 specification indicates that templates may be configurable on a device-by-device basis. However, most devices have a set of static templates to which exported flows conform. When SolarWinds states that a device is supported by NTA, SolarWinds has determined that at least one of the templates the device is capable of exporting will satisfy the NTA requirements. For more information, search for NetFlow version 9 flow record format on www.cisco.com.
- Cisco 4500 series switches do not provide information for the TCP_FLAGS field (field type number 6) corresponding to a count of all TCP flags seen in the related flow.
- Cisco Adaptive Security Appliances (ASA) are capable of providing flow data using a limited template based on the NetFlow v5 template.

Sampled flow supported fields

If you are using sampled flows, packets need to contain not only the fields mentioned in [Required fields in SolarWinds NTA](#), but also fields supported by NTA for sampled flows. Supported fields depend on the flow version used.

Sampling mode has to be non-zero, otherwise NTA processes flows as non-sampled.

If some of the required fields are missing on your device or contain unexpected values, please contact your device vendor.

NetFlow v5 and J-Flow v5 header format

NTA supports the following bytes in the v5 header format:

Bytes	Contents	Description
22-23	sampling_interval	First two bits hold the sampling mode; remaining 14 bits hold value of sampling interval.

For more information, search for NetFlow export datagram format on www.cisco.com.

NetFlow v9 and J-Flow v9

Supported fields depend on the template you are using:

- Flow template
- Option template

Flow template

The following fields are optional for the Flow Template Schema. It is enough if the template includes one of the fields in each group.

If at least one from each group is not included in the template, NTA will still be able to store flows. However, a default value will be stored, and appropriate widgets will show the "No Data" message.

Field Type	Field Type Number	Description
Sampling Interval Group		
SamplingInterval	34	When using sampled NetFlow, the rate at which packets are sampled, for example, a value of 100 indicates that one of every 100 packets is sampled.
SamplerInterval	50	Packet interval at which to sample.
Sampling Algorithm Group		
SamplingAlgorithm	35	The type of algorithm used for sampled NetFlow: 0x01 Deterministic Sampling, 0x02 Random Sampling
SamplerMode	49	The type of algorithm used for sampling data: 0x02 random sampling.

Option template

Mandatory fields

If you are using the Option Flow Template, make sure at least one field from each group is included. Otherwise, flow data cannot be stored.

Field Type	Field Type Number	Description
Sampling Interval Group		
SamplingInterval	34	When using sampled NetFlow, the rate at which packets are sampled, for example, a value of 100 indicates that one of every 100 packets is sampled.
SamplerInterval	34	Packet interval at which to sample.
Sampling Algorithm Group		
SamplingAlgorithm	35	The type of algorithm used for sampled NetFlow: 0x01 Deterministic Sampling, 0x02 Random Sampling.

Field Type	Field Type Number	Description
SamplerMode	35	The type of algorithm used for sampling data: 0x02 random sampling.

SamplerID

If the SamplerID isn't included in the options flow template, a default value will be stored, and appropriate widgets will display "No Data".

SamplerID	48	Identifier shown in <i>show flow-sampler</i> .
-----------	----	--

For more information, search for NetFlow version 9 flow record format.

Events list

The following sections list events you can encounter in NTA. Each event is briefly described and provided with steps that help you resolve it or with links leading to more details about the situation triggering the event.

NetFlow receiver service stopped

NTA informs you that SolarWinds NetFlow Service stopped.

```
"NetFlow Receiver Service [service name] Stopped."
```

To resolve the issue, restart the SolarWinds NetFlow Service:

1. Start the SolarWinds Platform Service Manager in the SolarWinds Orion > Advanced Features program folder.
2. Check the status of the SolarWinds NetFlow Service.
3. If it is stopped, select it, and then click Start.

License limitation

NTA informs you that your NTA license does not match your NPM license, and NTA thus cannot monitor your flow traffic.

```
"License limitation doesn't fit Orion license!"
```


To resolve this event, make sure your NTA license matches your NPM license. Both NPM and NTA must be at the same license level. For more information, see [Licensing SolarWinds](#).

No valid license

NTA informs you that your license is expired.

```
"License status check failed: no valid license were found for [license key not in brackets]"
```

To resolve this event, log in to the SolarWinds customer portal, and procure an appropriate NTA license.

Invalid template

NTA informs you that incoming NetFlow v9 flows have a wrong or invalid template.

```
"NetFlow Receiver Service [xy] received an invalid v9 template with ID xx from device x.x.x.x. See knowledge base for more information."
```

Resolve the issue

1. Log in to the appropriate device and check the template.
2. Make sure the device exports an appropriate template in one-minute intervals. For more information, see [Device configuration examples](#).
3. Make sure the template includes all required details. For more details, see [Required Fields](#).

Invalid IPFIX template

NTA informs you that the IPFIX template does not include required fields.

```
"NetFlow Receiver Service [xy] received an invalid IPFIX template with ID XX from device x.x.x.x. "
```

Resolve the issue

1. Log in to the appropriate device and check the template.
2. Make sure the device exports an appropriate template in one-minute intervals. For more information, see [Device configuration examples](#).
3. Make sure the template includes all required details. For more details, see [Required Fields](#).

No template received

NTA informs you that there is no NetFlow v9 template received for incoming NetFlow v9 traffic. "NetFlow Receiver Service [xy] received NetFlow v9 flows without any template for decoding them. Configure the device x.x.x.x to export an appropriate NetFlow v9 template at 1-minute intervals. See help for details."

Resolve the issue

1. Log in to the appropriate device and check the template.
2. Make sure the device exports an appropriate template in one-minute intervals. For more information, see [Device configuration examples](#).
3. Make sure the template includes all required details. For more details, see [Required Fields](#).

NetFlow data export not enabled

NTA is receiving NetFlow traffic from a wrong interface (restricted or unsupported) "NetFlow data export on device x.x.x.x is not enabled. If you cannot see NetFlow data from the device in NTA, make sure the device is configured to export NetFlow. » [Learn more](#)."

The event is generated when both indexes are 0. This can happen in two cases:

- Incorrectly configured device. For more information about configuring the device, see [Set up network devices to export NetFlow data](#).
- If data from the node are visible in NTA, it is safe to ignore this event. In this case, this event only makes you aware of internal node configuration.

NetFlow time difference error

This event informs you that the time difference between your servers (SolarWinds Platform database server, NTA Flow Storage database, and the NTA Service server) is above the critical threshold. The critical threshold is hard-coded to 300s.

"Time on NetFlow Receiver Service [xy] is: xxx. DB server time is xx. The difference is: 719 s. Which is above critical threshold. The data won't be correct. Synchronize the clocks and restart the service."

To resolve the issue, synchronize time settings on all servers (SolarWinds Platform database, NTA polling engine(s), and NTA Flow Storage database server).

 **Cannot connect to NTA Flow Storage database**

This event informs you that NTA Flow Storage database is currently unavailable.

"Cannot connect to NTA Flow Storage database. NTA cannot save any flows now."

To resolve the issue, make sure that the server is running, port 17777 is open, and no firewall is blocking the connection.

 **Unmanaged NetFlow node**

This event informs the user that NTA is receiving NetFlow traffic from a node which is not managed in NPM.

"NetFlow Receiver Service [xy] is receiving NetFlow data stream from an unmanaged device (x.x.x.x). The NetFlow data stream from x.x.x.x will be discarded. Please use Orion Node management to manage this IP address in order to process this NetFlow data stream, or just use [Manage this device](#)."

Resolve the issue

Click [Manage This Device](#) and complete the Add Node wizard to add the node in NPM. For more information, see [Adding Devices for Monitoring in the Web Console](#) in the SolarWinds Network Performance Monitor Administrator Guide.

 **Unmanaged NetFlow interface**

This event informs you that NTA is receiving traffic from an interface which is not managed in NPM. However, the corresponding node is managed in NPM. Click [Add this interface](#) or [Edit this interface](#) to add the object to NPM for monitoring.

"NetFlow Receiver Service [xy] is receiving NetFlow data from an unmanaged interface 'interface1name To interface2name'. Click [Add this interface](#) or [Edit this interface](#) to manage interface and process its flow data."

Resolve the issue

Click [Add This Interface](#) or [Edit This Interface](#), and add the interface to NPM for monitoring. For more information, see [Adding Devices for Monitoring in the Web Console](#) in the SolarWinds Network Performance Monitor Administrator Guide.

Unmonitored NetFlow interface

NTA informs you that it is receiving flow traffic from an interface, which is managed in NPM, but not monitored in NTA. This happens if the Enable Automatic Addition of NetFlow Sources in NTA Settings is disabled.

```
"NetFlow Receiver Service [xy] is receiving NetFlow data from unmonitored interface if name on node. Click Monitor NetFlow source or enable the "Automatic addition of NetFlow sources" option on the Netflow Settings page to process future NetFlow data from this interface."
```

Resolve the issue

1. Click Monitor NetFlow Source and enable monitoring for the interface. For more details, see [Add flow sources and CBQoS-enabled devices](#).
2. Click Automatic Addition of NetFlow Sources and make sure the Enable Automatic Addition of NetFlow Sources option is selected. For more information, see [Enable flow monitoring from unmanaged interfaces](#).

Not primary NPM node IP address

This event informs you that the mentioned node has more IP addresses and that the IP address through which flow data are coming is not used for polling purposes.

```
NetFlow Receiver Service [xy] is receiving NetFlow data from an NPM device name (device IP address) through an IP address that is not its primary IP address. The NetFlow data will be discarded. Enable the Match NetFlow devices also by not primary IP Address option to process NetFlow data from this device.
```

Resolve the issue

Follow the link to NetFlow Settings and make sure the Allow Matching Nodes by Another IP Address option is selected. For more information, see [Enable flow monitoring from unmanaged interfaces](#).

Unmonitored interface automatically added

NTA informs you that an unmonitored interface has been added into NetFlow sources automatically. This happens if you enabled the Enable Automatic Addition of NetFlow Sources option in the NTA Settings. For more information, see [Enable the automatic addition of flow sources](#).

```
"NetFlow Receiver Service [xy] is receiving NetFlow data from an unmonitored interface. The interface if name on service is being added to NetFlow sources."
```

NetFlow time difference warning

This event informs you that there is a time difference between your database and NTA servers, but it does not exceed the critical threshold.

```
"Time on NetFlow Receiver Service [xy] is: xxx. DB server time is xx. The difference is: xxx s. Which is above threshold. Fetched data could be unreliable."
```

To prevent corrupt data, synchronize time settings on all servers:

- SolarWinds Platform database
- NTA polling engine(s)
- NTA Flow Storage database server

NetFlow time difference warning ended

This event informs you that the time difference between the database server and NTA server has been resolved and the server times have been synchronized.

```
"Time on NetFlow Receiver Service [xy] is: xx, DB server time is: xx. The difference is: 0s. Which is under warning threshold"
```

NetFlow receiver service started

NTA informs you that the NetFlow service has been started. This event is triggered when the SolarWinds NetFlow Service starts.

```
"NetFlow Receiver Service [service name] started - listening on port(s) [port number(s)]."
```

NetFlow receiver service settings changed

NTA informs you if the port it is listening on has changed, or if a new port has been added. For more information, see [NetFlow Collector Services](#).

```
"NetFlow Receiver Service [service name] setting was changed - listening on port(s) [port number(s)]."
```

NetFlow event: interface index mapping used for a node

NTA informs you that a new device using interface index mapping has been added for monitoring in NTA.

```
Interface index mapping is being used for node [node name].
```

SNMP index is a value identifying a specific interface. Flows coming from this device are using different values than SNMP interface indexes and NTA thus needs to establish a relation between the interface index and the values included in these flows.

NetFlow event: removing interface index for a node

NTA informs you that interface index mapping has been removed for a node.

Removing interface index mapping for node [node name].

For more information, see [NetFlow event: interface index mapping used for a node](#).

NetFlow database maintenance

NTA informs you that the database maintenance has been completed.

NetFlow Database Maintenance: Deleted x expired endpoints in x.xx seconds.

For more information, see [SolarWinds Platform database maintenance](#).

Scheduled shrink performed

NTA informs you that the SolarWinds Platform database has been compressed.

Scheduled shrink performed. DB size before shrink xMB, DB size after shrink xMB, released space xMB. For more information, see [SolarWinds Platform database maintenance](#).

Updating data to be used in Top XX aggregated widgets

NTA informs you that data aggregation settings for Top XX applications, Top XX Conversations or Top XX Endpoints has been changed.

Updating data to be used in showing Top [x] [Conversations, Applications, or Endpoints].

This event only occurs in NTA 4.0 using SQL for storing flows and in older NTA versions.

Adjust data aggregation settings

Aggregating NetFlow data in memory significantly reduces the I/O demands that NTA makes on your SolarWinds Platform database, which can increase the performance of all SolarWinds applications that share the database. If SolarWinds Platform Web Console widgets are allowed to work directly against the SolarWinds Platform database in making and presenting their latest calculations without aggregation, NPM would make big I/O demands on the SolarWinds Platform database. This would impact performance of both NTA and NPM.

By aggregating data before writing it to the SolarWinds Platform database, NTA software expedites the presentation of summary statistics for three of the most important kinds of information about traffic on your network: Top XX Applications, Top XX Endpoints, and Top XX Conversations.

Activate aggregation

By aggregating data before writing it to the SolarWinds Platform database, NTA expedites the presentation of summary statistics for three of the most important kinds of information about traffic on your network: Top XX Applications, Top XX Endpoints, and Top XX Conversations.

To turn on data aggregation settings:

1. Go to NetFlow Settings:
 - a. Click My Dashboards > NetFlow > NTA Summary.
 - b. Click NetFlow Settings in the top right corner.
2. Scroll down to Database Settings and configure the Data Aggregation options as follows:
 - a. Check Enable Aggregation of Top Talker Data.
 - b. Enter how many of the following SolarWinds Platform should aggregate NetFlow data for:
 - Top Applications
 - Top Endpoints
 - Top Conversations
 - c. Enter the number of hours NTA should save aggregated NetFlow data in cache.
3. Click Save.

Optimize aggregation

Optimize aggregation by displaying the items you entered above when you activated aggregation. For example, if you entered 10 Top Conversations for which to aggregate data, you should display up to 10 Top Conversations. Displaying more conversations would require loading more data than is cached and would slow performance.

To set the optimal number of data elements:


1. Click Edit from a Top XX Applications, Endpoints, or Conversations pane.
2. On the Edit Resource page, enter the Maximum Number of Items to Display. This number should match the number you entered for this widget when you activated data aggregation in the procedure above.
3. Click Submit.

Top XX Applications

This widget provides a view of the top XX applications responsible for monitored traffic on your network, ranked in order of traffic volume.

When placed on the Node Details or Interface Details view, this widget provides a view of the applications responsible for the most traffic passing through the viewed node or interface over the selected period of time.

This widget shows only applications whose monitoring has been enabled on the Manage Applications and Service Ports view. Data for ports and applications whose monitoring is not enabled are collected, aggregated, and shown in the Top XX Applications widget as Unmonitored Traffic. For more information about monitored ports and applications, see [Configuring Monitored Ports and Applications](#).


 If you are seeing no data in the Top XX Applications view, make sure you are receiving data for the flow type selected in the top right of the Top Applications panel. If monitoring NBAR2 applications for which you are not seeing a name identified for the application, see [NBAR2 Applications](#) for an explanation of how these applications are classified in NTA.

View more details about displayed applications

- Click a listed application to open the NetFlow Applications Summary view that presents statistics for the selected application.
- Click + to expand a listed application and display the list of nodes and their respective interfaces over which the selected application traffic is currently flowing.
- Click a node or interface to display the NetFlow Application detail view showing statistics for the selected application traffic traversing through the appropriate node or interface.

View details about NBAR2 applications

If you select NBAR2 in the drop-down in the top-right corner of the Top XX Applications widget, NTA populates the chart with the top [NBAR2 applications](#) identified by name.

 If you deployed [SolarWinds Observability Self-Hosted](#) 2022.2, NBAR2 applications are identified by name and application vendor icon. Hover over the icon of the application vendor to see the name of the vendor.

- Click a listed application to open the NetFlow Applications Summary view that presents statistics for the selected application.
- Click + to expand a listed application and display the list of nodes and their respective interfaces over which the selected application traffic is currently flowing.
- Click a node or interface to display the NetFlow Advanced Application detail view showing statistics for the selected application traffic traversing through the appropriate node or interface.

View unmonitored traffic

If there are applications whose monitoring is not enabled in the Manage Applications and Service Ports page, the Top XX Applications widget on a summary view displays the Unmonitored Traffic item. This item aggregates traffic coming from ports or applications whose monitoring is not enabled at the moment.

1. Click the Unmonitored Traffic item to go to the NetFlow Applications Summary view filtered by unmonitored traffic.
2. Consult the Top XX Applications widget. The widget will list unmonitored applications, and allow you to monitor appropriate ports.

Enable monitoring of unmonitored ports

If you are viewing the Top XX Applications widget on an Unmonitored Traffic view, you can enable monitoring of unmonitored ports:

1. In the list of unmonitored applications, click Monitor Port to enable monitoring of the port.
2. On the Monitor Application window, select the port(s) to monitor.
3. Select the Source and Destination IP Address and the protocol to monitor.
4. Enter a Description, and then click Add Application to enable monitoring.

You can also enable monitoring for these applications and ports on the Manage Applications and Service Ports page. For more details, see [Configuring Monitored Ports and Applications](#).

Top XX Applications (Endpoint Centric)

You can customize an endpoint-centric version of this widget and place it on the NetFlow Node Details or Interface Details view.

The endpoint-centric Top XX Applications widget provides a ranked list of applications responsible for traffic passing through the specified node or interface.

For more information about adding endpoint-centric widgets, see [Add endpoint-centric widgets to NTA views](#).

Table legend

The table below the chart provides the following information:

Column Title	Contents
Application	The application name with its assigned port number in parentheses.

Column Title	Contents
Ingress Bytes, Egress Bytes Ingress Packets, Egress Packets	Displays the amount of data (in bytes and packets) flowing to the selected application through the viewed node or interface. The columns displayed depend on the flow direction set in the top left corner of the view (either only Ingress Bytes, or only Egress Bytes, or both columns).
Percent (Utilization)	<p>Displays the percentage of all traffic through the viewed object attributed to use of the listed application.</p> <p>The first value describes the percentage of the appropriate item based on items shown by the chart. Individual items in the legend add up 100%. This percentage can be absolute or relative. For more information, see Percentage type for Top XX lists.</p> <p>A value in parentheses is available only for interfaces. It describes how the appropriate item utilizes the interface bandwidth in percentage.</p> <p>If the utilization is approximately twice as high as it should be, for example 150% instead of 75%, it might be caused by flow duplication. For more information, see Resolve duplicate flows.</p>

Edit the widget

If you are logged in using a User ID with administrative privileges, you can change the way this widget is displayed for all users:

1. Click Edit to load the Edit Resource page.
2. Make changes.
3. Click Submit.

Edit time and flow direction for the view

You can also change the time period and flows direction shown by all widgets in the view:

1. Directly below the view name, click next to the appropriate setting and define the appropriate settings.
2. Change the Relative Time Period, by default set to 1 hour prior to the current time, or specify a specific time period.

The time and flow direction settings are limited to the current session only. After you leave the view, your changes will be lost and default settings are re-applied.

 **Windows Firewall is turned on**

NTA informs you that the NetFlow service has started or restarted and it is blocked by a firewall.

"Windows FireWall is turned on and its current exceptions do not allow the NetFlow Service to receive packets. Run the Configuration wizard for Services to remedy."

Resolve the issue

Complete the Configuration wizard for Services:

1. Start the Configuration wizard in the SolarWinds Orion > Configuration and Auto-Discovery program folder.
2. Select Services and complete the wizard.

 **NetFlow licensing**

NTA informs you that you are running an evaluation version, which has not been licensed yet.

Your SolarWinds NetFlow Receiver Service Evaluation [receiver name] will expire in x days. Please contact SolarWinds support to purchase a licensed version.

Thank you.

To resolve the issue, purchase a license and activate it. Your SolarWinds licenses can be activated directly during the installation process. However, SolarWinds also provides a powerful License Manager which allows you not only to activate your licenses, but also deactivate a license on a certain machine and re-activate it elsewhere.

 **Unable to start listening on port**

NTA informs you that the port NTA is listening at is being used by another listener. NTA thus cannot collect flows.

Unable to start listening on port x. Waiting until the port is free.

Resolve the issue

1. Log in to the device and check what applications use the port NTA is using. Port 2055 is the default.
2. If the port is being used by another application, close the application.
3. If the port is being used only by the SolarWinds NetFlow Service, restart the service:
 - a. Start the SolarWinds Platform Service Manager in the SolarWinds Orion > Advanced Features program folder.
 - b. Check the status of the SolarWinds NetFlow Service.
 - c. If it is stopped, select it, and click Start.

Port is free, listening

NTA informs you that the port it is listening at is free again, and that the issue has been resolved.

```
Port x is free, listening.
```

Notification event status reset

NTA informs you that you have reset the Last 200 Events view by clicking Clear Notification.

```
"Resetting unknown traffic notifications events."
```

For more information about seeing cleared events, see [Filter events and display historical events in NTA](#).

Connection to NTA Flow Storage database has been restored

This event is triggered when the connection to NTA Flow Storage database is restored.

Interface speed on unmanaged interfaces

You must enter the speed for unmanaged interfaces. Unlike managed interfaces that NPM recognizes, NPM cannot get this information from unmanaged interfaces which it does not recognize. The documentation of your device or your Internet service provider can give more information on determining the speed of an unmanaged interface.

NTA uses the unmanaged interface speed to determine the percentage of widget utilization. Entering an accurate interface speed ensures the correct display of NTA widgets. With this information, you can determine the most efficient use of widgets.

Resolve unknown NetFlow traffic

If your devices export flows to the NTA receiver, but are not managed in NPM, or are not configured for monitoring in NTA, NTA cannot process the exported information. NTA informs you that it is receiving unknown traffic by displaying a message in the yellow information banner at the top of your NTA views.

Unknown traffic can be viewed either as individual events within the [Last XX Traffic Analysis Events](#) widget or on the Last 200 Unknown Traffic Events view.

Unknown traffic can include traffic from unmanaged devices and unmonitored or unmanaged interfaces. The following sections introduce different unknown traffic types:

Traffic from unmanaged nodes or interfaces

Unmanaged objects are nodes or interfaces that are not managed in NPM. The devices export flows, but NTA cannot access the necessary data stored in the SolarWinds Platform database. You need to add these nodes and interfaces to NPM first. For more information, see [Add flow-enabled devices and interfaces to the SolarWinds Platform database](#).

Traffic from unmonitored interfaces

Unmonitored interfaces are interfaces managed in NPM, but not monitored by NTA. Traffic data from them are collected, but you cannot see them in NTA until you enable monitoring for them. For more information about monitoring flow and CBQoS sources in NTA, see [Flow sources and CBQoS polling](#).

Traffic from unmonitored interfaces appears in NTA mainly if flow sources are not being added to NTA automatically. For more details, see [Enable the automatic addition of flow sources](#).

Traffic from unmanaged interfaces

Unmanaged interfaces cannot be monitored using SNMP. However, NTA can receive traffic from these interfaces. NPM does not poll data for these nodes via SNMP, the nodes are only registered there and flows can be processed by NTA. However, to monitor this data in NTA, you must add the interface for monitoring to NTA, and provide the interface speed. For more information, see [Enable flow monitoring from unmanaged interfaces](#).

If you cannot see an unknown traffic event concerning a device which should be exporting NetFlow, log on to the device and check the configuration. Make sure the device sends data to the appropriate port, which is 2055 by default.

Resolve unknown traffic events

1. Click My Dashboards > NetFlow > NTA Summary.
2. Check the yellow banner area below the tool bar.

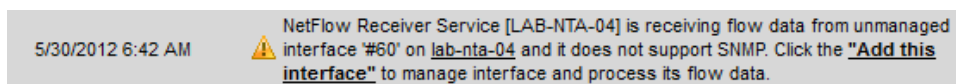
3. If there are unknown traffic events, click Show Unknown Traffic Events in the banner.
If you cannot see the banner, click NetFlow Settings, and then click Show Unknown Traffic Events under NetFlow Management.
4. The Last 200 Unknown Traffic Events view lists the last 200 events related to NTA, including those in which flow traffic was received but was not associated with a NetFlow source.
5. Resolve individual events.

Test whether the events were resolved

1. On the Last 200 Unknown Traffic Events view, click Clear Notifications.
2. Click Refresh Events. New events are added to the list, and unknown traffic events return to the list if they have not been resolved.
3. You can also test resolving unknown traffic events by clicking My Dashboards > NetFlow > NTA Summary. You should no longer see a banner regarding unknown flow traffic. If you do, click the message and re-examine the Last 200 Unknown Traffic Events list again, repeating the steps in these procedures to resolve unknown traffic.

Enable flow monitoring from unmanaged interfaces

When NetFlow Traffic Analyzer receives a data flow from an unmanaged interface, it displays an event in the NTA Events, such as on the following image.



Though this interface does not support SNMP, you can register it to NPM, and enable the NetFlow Receiver Service to process the flow data it exports to NTA. If the interface is not in NPM, NTA drops the data flow.

Add an unmanaged interface

1. Click Add This Interface in the unmanaged event.
2. On the Add Interface to NPM menu, edit the Interface Name field if desired.
3. Define the Interface Speed:
 - a. See the documentation of the device for the correct interface speed.
 - b. Select the speed type from the list.
4. Click Submit. The interface is added to NPM and can be viewed on the Node Management page.

Unmanaged interface monitored in NTA

After the unmanaged interface is configured, it looks like any standard interface in NPM, and NTA can recognize the interface. Now NTA can manage the unmanaged interface the same as a managed interface and does one of the following:

- If NTA is configured to automatically add NetFlow sources, it adds the source. An event informs you that the source was automatically added to NTA. You can see the source in the Flow and CBQoS Sources widget.
- If NTA is not configured to automatically add NetFlow sources, it does not add the source. An event informs you about a flow from an interface not in NetFlow sources. The source is not visible in NTA in the Flow and CBQoS Sources widget. If you want to monitor this interface, enable monitoring for the interface in NTA. For more information, see [Flow sources and CBQoS polling](#).

Unmanaged interfaces do not have information about interface utilization, because NPM does not poll them. NTA cannot show these interfaces in the Top XX NetFlow Sources by % Utilization widget. These interfaces do not trigger NetFlow alerts based on utilization for the same reason.

Set up a NetFlow collection

If you see a network device in your NetFlow Sources and you do not intend to collect NetFlow data from it, you can eliminate unnecessary traffic by turning off the export of data at the device.

1. Configure your network devices to export NetFlow data for each interface for which you want to collect the data. For more information, see [Device Configuration Examples](#).

For information on enabling NetFlow for Cisco Catalyst switches, see [Enabling NetFlow and NetFlow Data Export \(NDE\) on Cisco Catalyst Switches](#).

For information on enabling NetFlow on Cisco ASA devices, see [Cisco ASA NetFlow overview](#).

If your network device is of a different vendor, see the documentation of the vendor.

2. Verify that each interface for which you want to collect and view data is actively being monitored in NPM.

For any interface that you need to add to NPM, see [Network Discovery Using the Network Sonar wizard](#).

Use a packet capture tool, such as WireShark, on the relevant interface and port to verify that the device is exporting data as expected.

NTA chart issues

Below are the most common issues encountered on NTA charts.

Duplicate flows

If your devices are configured to export NetFlow on both ingress and egress interfaces, you might see duplicate traffic in your widgets.

Duplicate flows can occur in the following cases:

- You have both ip flow ingress and ip flow egress applied for all interfaces on a device.
- You have set ip flow ingress on some interfaces and ip flow egress on other interfaces.
- On your serial interfaces with subinterfaces, you have NetFlow export enabled on both the physical and logical interfaces.

Resolving Duplicate Flows

- If your device configuration contains both `ip flow ingress` and `ip flow egress` commands, make sure NetFlow is enabled only for ingress interfaces.
- If you have NetFlow enabled for both physical and logical subinterfaces, remove the NetFlow export commands from the physical serial interfaces and only have the subinterfaces enabled for the export.

Double rate in Top XX Endpoints and Top XX IPv4 Domains

The Top XX Endpoints and Top XX IPv4 Domains widgets display double data by design. Each flow has two distinct endpoints. To display statistics for top endpoints, NTA disregards that one endpoint is the source and the other endpoint is the target of flows, and treats both as endpoints only. This effectively doubles the total amount of data displayed by the Top XX Endpoints widget.

Example

Let us take two flows and look at what you see in most widgets and in the Top XX Endpoints widget.

Most widgets

Flow	Source IP	Destination IP	Protocol	Bytes Transferred
Flow 1	IP1	IP2	TCP	50
Flow 2	IP2	IP3	TCP	40
Total bytes transferred:				50+40=90

Top XX Endpoints widget

Endpoint	Bytes Transferred
IP1	50

Endpoint	Bytes Transferred
IP2	50+40=90
IP3	40
Total:	50+90+40=180

No data

If your widgets show the "no data" message, it can be caused by one of the following:

No data to be displayed

There are no data to be displayed for the current time and flow direction settings.

To resolve the issue, check the time settings for both the widget and the view.

Too long time period selected for the view

If NTA needs more than one hour to process data that you want to see in the widgets, the query times out and the widgets show the "no data" message.

To resolve the issue, define a shorter time period for both the view and the widget.

Unexpected spikes in CBQoS post-policy charts

If you remove a shaping policy from a class, post-policy charts with the chart type set to % of Class Utilization may display unexpected spikes.

This is normal behavior, because devices affected by the policy change temporarily report huge amounts of data, which is reflected by the post-policy spike.

Resolve duplicate flows

If your devices are configured to export NetFlow on both ingress and egress interfaces, you might see duplicate traffic in your widgets.

Duplicate flows can occur in the following cases:

- You have both `ip flow ingress` and `ip flow egress` applied for all interfaces on a device.
- You have set `ip flow ingress` on some interfaces and `ip flow egress` on other interfaces.
- On your serial interfaces with subinterfaces, you have NetFlow export enabled on both the physical and logical interfaces.

Things to check

- If your device configuration contains both `ip flow ingress` and `ip flow egress` commands, make sure NetFlow is enabled only for ingress interfaces. Go to appropriate devices and make sure the configuration contains only the `ip flow ingress` command.
- If you have NetFlow enabled for both physical and logical subinterfaces, remove the NetFlow export commands from the physical serial interfaces and only have the subinterfaces enabled for the export.

CBQoS issues in NTA

Record troubleshooting steps

Record detailed results as you perform your troubleshooting steps. It will help expedite a resolution if you need to contact SolarWinds Support about your CBQoS issue.

Use packet capture on the relevant interface of the SolarWinds Platform server to verify SNMP communication, on port 161, with relevant device(s).

CBQoS issues list

CBQoS not running on the device

Use SolarWinds MIB Viewer to check the status of CBQoS on your device.

Support is determined by `cbQosConfigIndex="1.3.6.1.4.1.9.9.166.1.5.1.1.2"`

If you see any value in your MIB viewer for this OID, then CBQoS data is being successfully pulled.

SolarWinds services not running

Make sure all SolarWinds services are running:

1. Start the SolarWinds Platform Service Manager in the SolarWinds Platform program folder.
2. If some SolarWinds services are not running, click Start Everything.

In particular, the SolarWinds Platform Module Engine service enables polling of CBQoS. The SolarWinds NetFlow service takes the data the SolarWinds Platform poller obtains from the device through SNMP and writes it into the NetFlow database table. If this service is not working, polled CBQoS data sits in a queue and eventually gets dropped.

Device configuration examples for NTA

The following sections can be used to help you configure your devices to send flow data to NetFlow Traffic Analyzer.

- NetFlow device examples
 - [Cisco NetFlow configuration](#)
 - [Cisco Flexible NetFlow configuration](#)
 - [Cisco NGA 3000 series configuration](#)
 - [Cisco WLC 5700 series configuration](#)
- sFlow and J-Flow device examples
 - [Brocade \(Foundry\) sFlow configuration](#)
 - [Extreme sFlow configuration](#)
 - [HP sFlow configuration](#)
 - Juniper Networks sFlow and J-Flow configurations
 - [Juniper sFlow configuration](#)
 - [Juniper J-Flow configuration](#)
- [Enable NetFlow and NetFlow data export on Cisco Catalyst switches](#)
 - [Requirements to enable NetFlow and NetFlow Data Export](#)
 - [Enable NetFlow on Cisco Catalyst 4500 Series](#)
 - [Enable NetFlow on Catalyst 6500 and 7600 series](#)
- [Cisco ASA NetFlow overview](#)