SolarWinds Orion

NetFlow Traffic Analyzer Evaluation Guide

About SolarWinds

SolarWinds, Inc. develops and markets an array of network management, monitoring, and discovery tools to meet the diverse requirements of today's network management and consulting professionals. SolarWinds products continue to set benchmarks for quality and performance and have positioned the company as the leader in network management and discovery technology. The SolarWinds customer base includes over 45 percent of the Fortune 500 and customers from over 90 countries. Our global business partner distributor network exceeds 100 distributors and resellers.

Contacting SolarWinds

You can contact SolarWinds in a number of ways, including the following:

Team	Contact Information
Sales	sales@solarwinds.com www.solarwinds.com 1.866.530.8100 +353.21.5002900
Technical Support	www.solarwinds.com/support
User Forums	thwack.solarwinds.com

Conventions

The documentation uses consistent conventions to help you identify items throughout the printed and online library.

Convention	Specifying
Bold	Window items, including buttons and fields.
Italics	Book and CD titles, variable names, new terms
`Fixed font`	File and directory names, commands and code examples, text typed by you
Straight brackets, as in [*value*]	Optional command parameters
Curly braces, as in {*value*}	Required command parameters
Logical OR, as in *value1*|*value2*	Exclusive command parameters where only one of the options can be specified

Orion NetFlow Traffic Analyzer Documentation Library

The following documents are included in the Orion NetFlow Traffic Analyzer documentation library:

Document	Purpose
Administrator Guide	Provides detailed setup, configuration, and conceptual information.
Evaluation Guide	Provides an introduction to Orion NetFlow Traffic Analyzer features and instructions for installation and initial configuration.
Page Help	Provides help for every window in the Orion NetFlow Traffic Analyzer user interface
Release Notes	Provides late-breaking information, known issues, and updates. The latest Release Notes can be found at www.solarwinds.com.

The following documents supplement the Orion NetFlow Traffic Analyzer documentation library with information about Orion Network Performance Monitor:

Document	Purpose
Orion Network Performance Monitor Administrator Guide	Provides detailed setup, configuration, and conceptual information for Orion Network Performance Monitor.
Orion Network Performance Monitor Evaluation Guide	Provides an introduction to Orion Network Performance Monitor features and instructions for installation and initial configuration.
Page Help	Provides help for every window in the Orion Network Performance Monitor user interface
Release Notes	Provides late-breaking information, known issues, and updates. The latest Release Notes can be found at www.solarwinds.com.

Contents

Chapter 1

Introduction to Orion NetFlow Traffic Analyzer

Orion NetFlow Traffic Analyzer (Orion NTA) provides a simple-to-use, scalable network monitoring solution for IT professionals managing any size NetFlow-, sFlow-, J-Flow-, NetStream-, or Class-based quality of service- (CBQoS)-enabled network.

Why Install Orion NetFlow Traffic Analyzer

As companies and their networks grow, bandwidth needs grow exponentially. All modern connected industries invest significant amounts of time and money to ensure that enough bandwidth is available for business-critical activities and applications. When bandwidth needs exceed currently available capacity or when demand seems to expand beyond the abilities of your network, understanding bandwidth use is no longer a novel interest, but it becomes critical to deciding whether it is necessary to invest in more bandwidth or if stricter usage guidelines are sufficient to regain lost bandwidth.

With the advent of streaming media, voice over IP (VoIP) technologies, online gaming, and other bandwidth-intensive applications, you, as a network engineer, must answer more than the simple question of whether the network is up or down. You must answer why the network is not performing up to expectations.

If you need to know how and by whom your bandwidth is being used, Orion NetFlow Traffic Analyzer provides a simple, integrated 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 Orion NetFlow Traffic Analyzer 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 NetFlow data provided by the Orion NetFlow Traffic Analyzer solution are not purely extrapolated data, but they are based on real information collected about the network by the Orion Network Performance Monitor product that is at the heart of Orion NetFlow Traffic Analyzer.

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

- Bandwidth distribution across traffic types
- Usage patterns over time
- External traffic identification and tracking

- Tight integration with detailed interface performance statistics

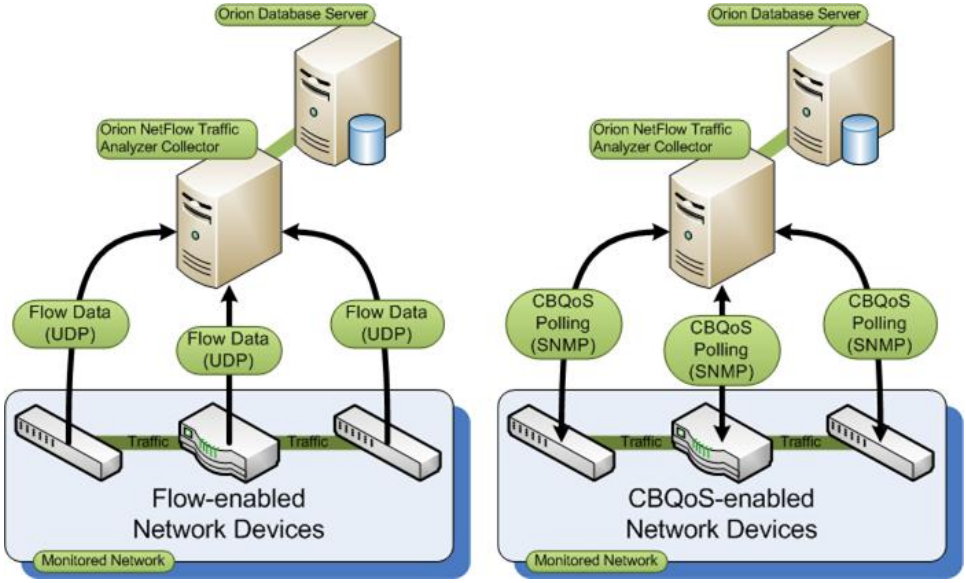
These monitoring capabilities, along with the customizable Orion Network Performance Monitor Web Console and reporting engines, make Orion NetFlow Traffic Analyzer your best option for monitoring your Flow-enabled network.

How Orion NetFlow Traffic Analyzer Works

Flow- and CBQoS-enabled devices can provide a wealth of IP-related traffic information. Orion NTA collects this traffic data, correlates it into a useable format, and then presents it, with detailed network performance data collected by SolarWinds Orion Network Performance Monitor, as easily read graphs and reports on bandwidth use on your network. These reports help you monitor and shape bandwidth usage, track conversations between internal and external endpoints, analyze traffic patterns, and plan bandwidth capacity needs.

The following diagram provides an overview of a simple Orion NTA installation. The diagram shows, generally, how Flow analysis and CBQoS polling functions polling occur simultaneously in NTA. Flow-enabled devices send Flow data to the Orion NTA collector on port 2055, and the Orion NTA collector polls CBQoS-enabled devices for traffic-shaping policies and results on port 161.

Note: The diagram shows CBQoS and Flow monitoring separately to emphasize the difference in collection methods. Network endpoints do not appear in the diagram. Also, a typical Orion NTA installation would not require all CBQoS- and Flow-capable devices be configured to interact directly with the Orion NTA collector. For more information about effectively deploying NetFlow on your network, see NetFlow Basics and Deployment Strategies.



Why Use Orion NetFlow Traffic Analyzer

Orion NetFlow Traffic Analyzer gives you the ability to quickly and easily monitor network resources and usage patterns at a customizable level of detail. The following valuable features represent core Orion NetFlow Traffic Analyzer capabilities:

Enhanced Monitoring and Analytical Planning Capabilities

Orion NTA highlights trends in network traffic, enabling you to intelligently monitor and anticipate changes in bandwidth to areas that are experiencing bottlenecks.

Orion Alerts Integration

Orion NTA automatically adds top talker information to Orion interface utilization alerts. You can navigate directly to NTA interface details from messages in the Orion Events resource.

For more information, see Adding Top Talker Statistics to Orion Alerts.

Customizable Rate-based Charts

Stacked area charts and line charts offer options to include splines showing data trends, and chart data unit options include Rate (Kbps), Percent of interface speed, Percent of total traffic, and Data transferred per interval.

Advanced Port and Application Mapping

Application mappings may be defined based on source and destination IP addresses, in addition to ports and protocols.

Flow Monitoring Support for Cisco Adaptive Security Appliances (ASA)

Orion NTA can report network traffic data provided by NetFlow-enabled Cisco ASA devices.

Filtered Views Including Both Ingress and Egress traffic

Orion NTA provides the ability to select the direction of traffic over any viewed interface. On any monitored interface, you can view traffic data for ingress traffic, egress traffic, or both.

Support for IPFIX-enabled Devices

Internet Protocol Flow Information Export (IPFIX) is a developing standard for formatting and transmitting IP-based network traffic information. As more devices features IPFIX capability, Orion NTA will immediately be able to provide IPFIX Flow monitoring.

Cisco CBQoS Monitoring

Orion NTA provides resources giving you the ability to easily view, chart, and report on the effects of the class-based quality of service policies you have enabled on your CBQoS-capable Cisco devices.

This release enhances CBQoS monitoring with partial support for nested policies and more granular control over polling specific devices.

Improved availability and performance

With Orion NTA, you can more quickly detect, diagnose, and resolve network slowdowns and outages.

This release improves CBQoS polling efficiency, load times for reports, and summary views.

Optimized Network Resource Allocation

Information provided by Orion NTA enables you to identify and reassign areas with excess bandwidth capabilities to areas with limited or stressed connections.

Alignment of IT Resources with Enterprise Business Needs

Because Orion NTA is built on the proven Orion NPM infrastructure, you can assess both the needs of the enterprise network in a high-level overview and the functional details of specific interfaces and nodes.

Increased Network Security

Orion NTA gives you the ability to quickly and precisely pinpoint network traffic and expose curious patterns, unwanted behaviors, and anomalous usage that may indicate possible virus, bot, or spyware infection.

Support for Multiple Flow Ports

The number and types of available Flow-enabled devices has increased, so the number of ports over which Flow data is transmitted has also increased. Orion NTA now supports the designation of multiple ports on which Flow data may be received.

An All-in-One NetFlow, sFlow, J-Flow, NetStream, and IPFIX monitoring solution

Now you can stop switching between network monitoring packages to acquire a complete picture of the usage, performance, and needs of your network, regardless of the type of Flow records provided by your various network devices.

Chapter 2

Installing Orion NetFlow Traffic Analyzer

Orion NTA features a wizard-driven installation procedure. For an enterprise-class product, the requirements are nominal.

Note: NetFlow data is extensive and can consume large amounts of database memory in a relatively short period of time. This is true even for smaller networks. As a result, SolarWinds requires that your SQL Server database and your Orion NPM/NTA installation are maintained on separate physical servers.

SQL Server and SQL Server Express with Orion NTA

Due to the fact that NetFlow data is extensive and can consume large amounts of database memory in a relatively short period of time, SolarWinds does not recommend using SQL Server Express database instances for Orion NTA. Instead, SolarWinds recommends the use of a production version of SQL Server.

Evaluations of Orion NTA are a limited exception. For evaluation purposes, Orion NPM and Orion NTA can support the use of SQL Server Express 2005 database instances. SQL Express allows you to evaluate Orion NTA with a real database, and it is available, free of charge, from Microsoft. However, SolarWinds does not recommend its use with Orion NTA in any production environment for the following reasons:

- SQL Express is unable to manage databases larger than 4GB.
- SQL Express is limited to a single processor.
- SQL Express is unable to utilize more than 1MB RAM.

Note: For production environments, Orion NPM and Orion NTA installations should use a SQL Server database instance installed on a separate server.

Requirements

The server you use to host your NetFlow solution must support both Orion NPM and Orion NTA as Orion NTA is built on and extends Orion NPM. In general, requirements for the current Orion NTA version follow the requirements of an Orion NPM version 3.9 installation, as provided in the Orion NPM Requirements in the *SolarWinds Orion Network Performance Monitor Administrator Guide*.

Note: By default, Orion NTA listens for Flow data on port 2055 (UDP). Ensure that port 2055 is open for UDP communication on any Orion NTA collector.

Software Requirements

The following tables list software requirements for the current Orion NTA version.

Notes:

- Due to the high speed and large memory requirements of Flow monitoring transactions, Orion NTA and SQL Server must be installed on separate physical servers.
- SQL Express and MSDE restrict the size of any database to 4GB and 2GB, respectively. For this reason, SolarWinds does not support the use of either SQL Express or MSDE with Orion NTA in production environments.

Software	Requirements
Orion NPM	Version 10.1 or higher
Operating System	Windows 2008 Server and Windows 2008 Server R2 (32-bit or 64-bit, with IIS in 32-bit mode) . Windows 2003 Server R2 (32-bit or 64-bit, with IIS in 32-bit mode) IIS must be installed. SolarWinds recommends that Orion NPM administrators have local administrator privileges to ensure full functionality of local Orion NPM tools. Accounts limited to use of the web console do not require administrator privileges. **Note:** SolarWinds does not support installation of Orion NPM on Windows XP, Windows Vista, and Windows 7 in production environments.
Web Server	Microsoft IIS, version 6.0 and later, in 32-bit mode. DNS specifications require that hostnames be composed of alphanumeric characters (A–Z, 0–9), the minus sign (–), and periods (.). Underscore characters (_) are not allowed. For more information, see *RFC 952*. **Note:** SolarWinds neither recommends nor supports the installation of Orion NTA on the same server or using the same database server as a Research in Motion (RIM) Blackberry server.
.NET Framework	Version 3.5 SP1 or later
SNMP Trap Services	Windows operating system management and monitoring tools component
Web Console Browser	Microsoft Internet Explorer version 6 or later with Active scripting Firefox 3.0 or later

SQL Server Software	Requirements
Operating System	Windows 2008 Server (32- or 64-bit) Windows 2003 Server R2, SP1 and higher (32- or 64-bit)
SQL Server	SQL Server 2005 SP1 Standard or Enterprise SQL Server 2008 Standard, or Enterprise **Note:** Though SQL Express may be used for limited evaluations purposes to monitor one or two interfaces for a very limited time SolarWinds recommends against its use for larger networks.

Hardware Requirements

The following table lists minimum hardware requirements for monitoring a typical network with the current version of Orion NTA.

Note: Orion NTA requires that TCP port 17777 is opened both to send and to receive traffic between Orion NPM and any other Orion modules.

Warning: The only RAID configurations that should be used with Orion NTA are 0, 1, 0+1, or 1+0. Due to the high speed and large memory requirements of NetFlow data transactions, SANs or other RAID configurations should not be used, as they may result in data losses and significantly decreased performance.

Hardware	Requirements
CPU	3GHz or faster, dual processors with dual cores
RAM	3GB or more
Hard Drive Space	**Orion NTA server:** 5GB or more, RAID 0, 1, 01, or 10. Other RAID or SAN configurations are not recommended. **SQL Server:** 5GB or more, RAID 0, 1, 01, or 10 on at least 6 spindles. Other RAID or SAN configurations are not recommended.
NetFlow devices	Cisco devices using NetFlow version 5 or 9 **Note:** Orion NTA only recognizes NetFlow version 9 templates that include all fields included in the NetFlow version 5 template.
IPFIX devices	Network devices using IPFIX
J-Flow devices	Network devices using J-Flow
sFlow devices	Network devices using sFlow version 5
NetStream device	Network devices using NetStream

Note: For more information about supported Flows, see NetFlow, IPIX, J-Flow, sFlow, and NetStream Requirements in the *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

Virtual Machine Requirements

Orion NTA may be installed on VMware Virtual Machines and Microsoft Virtual Servers if the following requirements are met by each virtual server.

Virtual Machine Configuration	Requirements
CPU Speed	3.0 GHz
Allocated Hard Drive Space	**Orion NTA server:** 5GB or more, RAID 0, 1, 01, or 10. Other RAID or SAN configurations are not recommended. **SQL Server:** 5GB or more, RAID 0, 1, 01, or 10 on at least 6 spindles. Other RAID or SAN configurations are not recommended.
Memory	2GB or more
Network Interface	Each installation of Orion NPM should have its own, dedicated NIC **Note:** Since Orion NPM uses SNMP to monitor your network, if you are unable to dedicate a network interface card to your Orion NPM installation, you may experience gaps in monitoring data due to the low priority generally assigned to SNMP traffic.

For more information about Orion NPM requirements, see the *SolarWinds Orion Network Performance Monitor Administrator Guide*.

NetFlow, IPFIX, J-Flow, NetStream, and sFlow Requirements

Any NetFlow, IPFIX, J-Flow, NetStream, or sFlow packets that do not include the following field types and field values may be ignored by Orion NTA:

Field Type	Field Type Number	Description
IN_BYTES	1	Ingress bytes counter
IN_PKTS	2	Ingress packets counter
PROTOCOL	4	Layer 4 protocol
L4_SRC_PORT	7	Source TCP/UDP port
IPV4_SRC_ADDR	8	Source IP address
INPUT_SNMP	10	SNMP ingress interface index
L4_DST_PORT	11	Destination TCP/UDP port
IPV4_DST_ADDR	12	Destination IP address
OUTPUT_SNMP	14	SNMP egress interface index

Notes:

- Only one interface index is absolutely required, but both interface indexes (INPUT_SNMP and OUTPUT_SNMP) should be provided to view accurate statistics for both ingress and egress flows.
- The SRC_TOS field type (field type number 5) is required to view Type of Service data for traffic over a Flow source, but the template used by Cisco Adaptive Security Appliances (ASA) does not provide this field.
- If SolarWinds states that Orion NTA supports Flow monitoring for a device, at least one of the templates the device exports satisfies these requirements.
- Including BGP/AS data in NetFlow packets is optional.

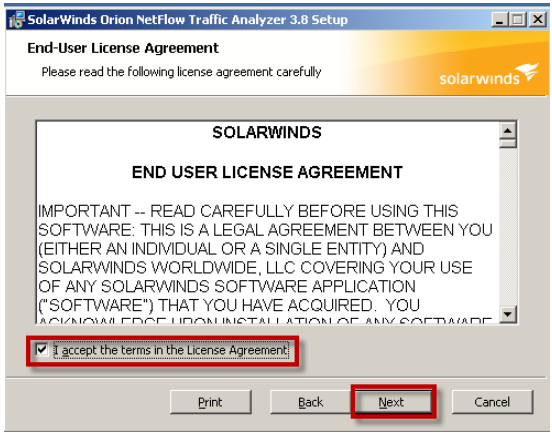
Installing Orion NetFlow Traffic Analyzer

Complete the following procedure to install Orion NTA. You must provide your NetFlow traffic port and confirm that it is enabled and sending NetFlow traffic data in order to complete your installation.

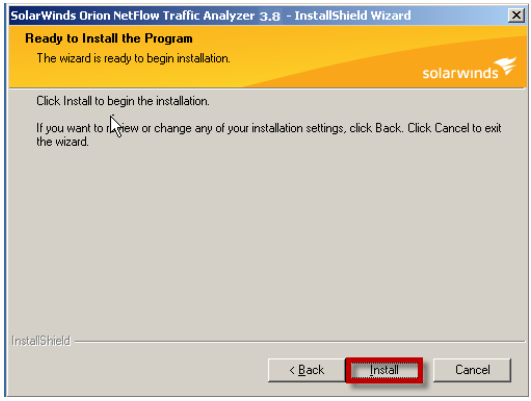
Note: The following procedure assumes Orion NPM version 10.1 or later is already installed on your designated Orion NTA server. If you would like to evaluate Orion NPM, contact SolarWinds at sales@solarwinds.com.

To install Orion NetFlow Traffic Analyzer:

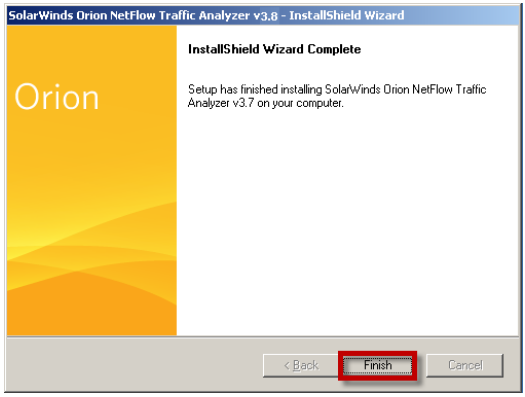
1. Log on to the Orion NPM server you want to use for NetFlow traffic analysis.
2. ***If you are installing Orion NTA on a terminal server,*** complete the following steps before continuing with your Orion NTA installation:
   a. Click **Start > Control Panel > Add or Remove Programs**.
   b. Click **Add New Programs**.
   c. Click **CD or Floppy**.
   d. Click **Next** in the Install Program From Floppy Disk or CD-ROM window.
3. ***If you downloaded Orion NetFlow Traffic Analyzer from the SolarWinds website,*** launch the SolarWinds Orion NTA installer executable from the directory where it is being stored.
4. ***If you received physical media,*** launch the SolarWinds Orion NTA installer executable from you CD drive.
5. Review the Welcome text.
6. Click **Next**.
7. Select **I accept the terms of the license agreement**, and then click **Next**.



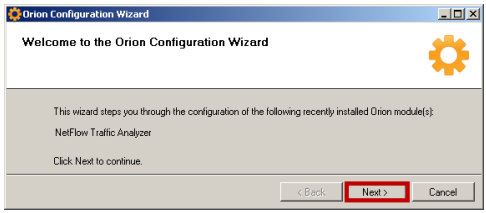
8. Click **Install** on the Ready to Install the Program window.



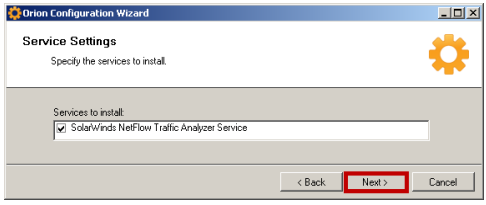
9. When the InstallShield Wizard completes, click **Finish** to exit the wizard.



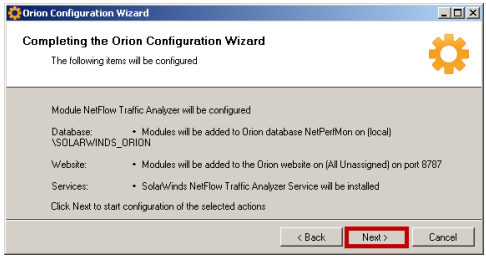
10. Click **Continue Evaluation**.
11. ***If you are prompted to reboot your server,*** select from the following options, as appropriate:
    - ***If you are installing Orion NTA on a terminal server,*** click **No**.
    - ***If you are NOT installing Orion NTA on a terminal server,*** click **Yes**.
12. ***If the Configuration Wizard does not start automatically,*** click **Start > All Programs > SolarWinds Orion > Configuration Wizard**.
13. Review the Welcome text, and then click **Next**.



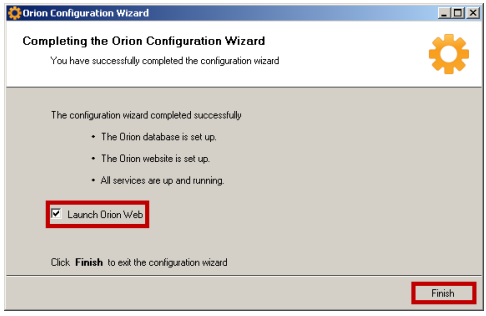
14. Confirm that **SolarWinds NetFlow Traffic Analyzer Service** is checked in the Service Settings window, and then click **Next**.



15. Review the configuration summary, and then click **Next**.



16. After the Configuration Wizard completes, confirm that **Launch Orion Web** is checked, and then click **Finish**.



17. Log in to the Orion Web Console as an administrator.

Note: If you have not already configured another Admin password, you can log in with the **User ID** `Admin` and no password.

18. ***If you are prompted to add NetFlow resources to the Orion website,*** click **Add Resources**.

Enabling Flow Analysis

To begin analyzing available Flow data produced by devices within your network, you must either add a Flow-enabled interface to your Orion database or monitor a previously added interface that is capable of generating NetFlow data. Adding your NetFlow devices and interfaces to the Orion database and adding your NetFlow devices and interfaces to Orion NTA as NetFlow sources are separate procedures, detailed in separate sections, as follows.

Preparing to Collect Flow Data

Before you attempt to set up NetFlow Sources in Orion NTA, configure each relevant network device to export Flow data to Orion NTA.

To prepare for flow collections:

1. Configure your network devices to export data regarding each relevant interface.

   Consult vendor documentation on your model. See the *Orion Network Traffic Analyzer Administrator Guide* for examples of Flow configurations for Cisco, Foundry, Extreme, and HP devices.

   For information on enabling NetFlow for Cisco Catalyst switches, consult this SolarWinds technical reference paper.

   For information on enabling NetFlow on Cisco ASA devices, consult this SolarWinds Knowledge Base article.

2. Verify that each interface for which you want to collect and view data is actively being monitored in Orion NPM

   For this task, for any interface that you need to add into Orion NPM, consult Network Discovery Using Sonar Wizard in the *SolarWinds Orion NPM Administrator Guide*.

3. Use a packet capture tool (for example, WireShark) on the relevant interface and port to verify that the device is in fact exporting data as expected.

Adding Devices and Interfaces to the Orion Database

You add nodes and their interfaces to the Orion database using the Web Node Management feature of the Orion Web Console. Nodes must be added as SNMP capable. If nodes are not SNMP capable, add them as ICMP, external, or WMI sources. If your NetFlow device is already configured to send NetFlow data, Orion NTA receives NetFlow data as soon as your device is added to the Orion database.

For step-by-step instructions on adding nodes to the Orion database, see the SolarWinds® Orion®Network Performance Monitor Evaluation Guide.

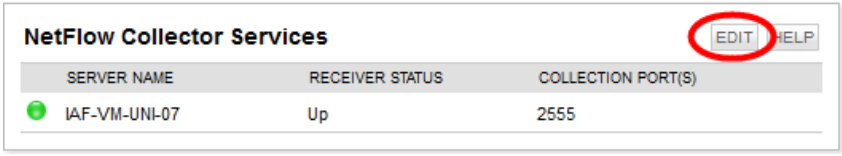
The following sections provides the required steps to start receiving NetFlow data from Flow-enabled devices on your network.

Setting NetFlow Collector Services

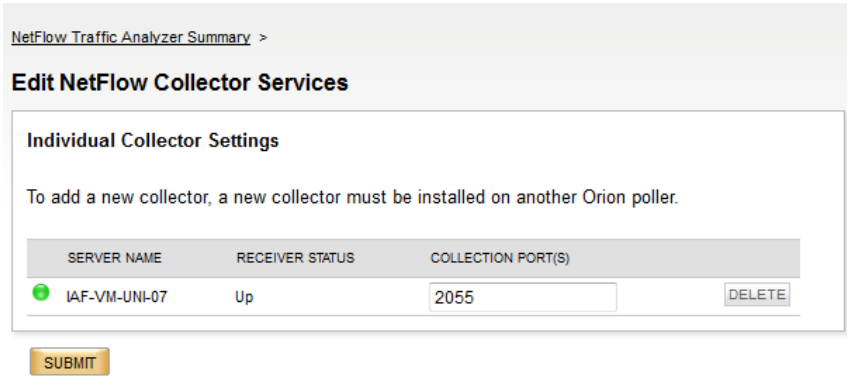
To enable proper collection of NetFlow data, Orion NTA's Netflow Collector Services must be listening on the correct port. NetFlow data defaults to port 2055.

To set NetFlow Collector Services to port 2055:

1. Log on to the Orion NPM server that hosts Orion NetFlow Traffic Analyzer.
2. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
3. Click **EDIT** in the Netflow Collector Service panel in the NetFlow Traffic Analyzer Summary window.



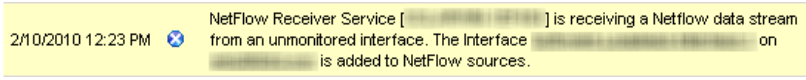
4. Type `2055` in the **COLLECTION PORT(S)** field and then click SUBMIT.



Automatically Adding Flow- and CBQoS-enabled Devices

Orion NTA can automatically add Flow- and CBQoS-enabled devices as NetFlow sources if they are configured to send Flows to your designated Orion NTA server, as shown in the following message from the Last 25 Traffic Analysis Events resource.

Orion NPM also provides the following message in the Last 25 Events resource when a source is detected and added.



By default on new installs, Orion NTA detects Flow-enabled devices on your network as NetFlow sources and automatically and adds them to your network.

For more information about managing new network devices, see Adding Devices and Interfaces to the Orion Database on page 15. For more information about configuring Flow-enabled devices, see Device Configuration Examples in the *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

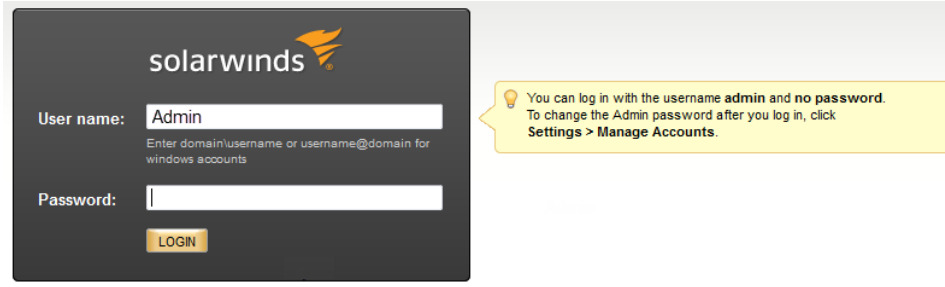
Adding NetFlow Sources to NetFlow Traffic Analyzer

After your Flow-enabled device and its interfaces have been added to Orion NPM, you must designate the device as a NetFlow source. The following procedure provides the steps required to add NetFlow sources to Orion NTA.

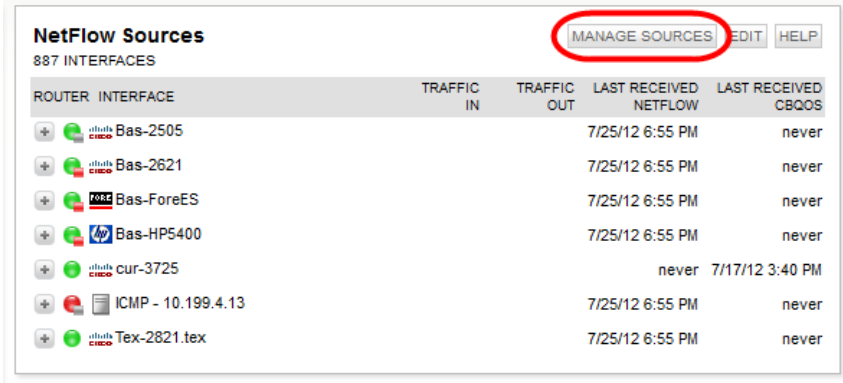
Note: Orion NTA only recognizes NetFlow version 9 templates that include all fields utilized by NetFlow version 5. For more information about the NetFlow templates Orion NTA recognizes, see NetFlow, IPIX, J-Flow, SFlow, and NetStream Requirements in the *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

To add NetFlow devices and interfaces to NetFlow Traffic Analyzer:

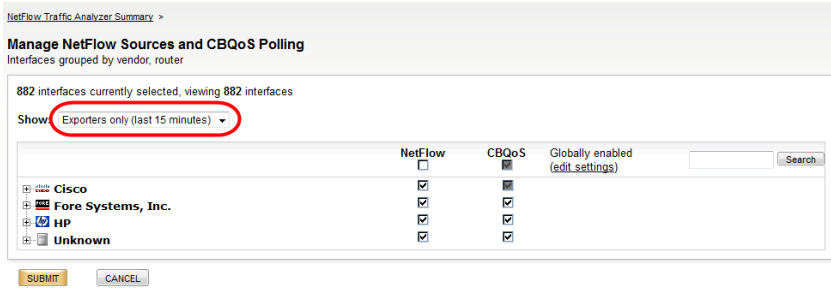
1. Log on to the Orion NPM server that hosts Orion NetFlow Traffic Analyzer.
2. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
3. Log in to the Orion Web Console as an administrator.



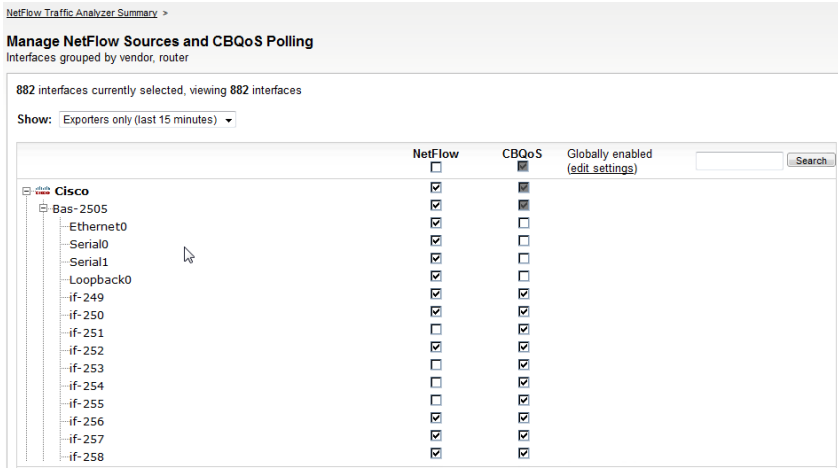
4. Click **Manage Sources** in the header of the NetFlow Sources resource.



5. Select **Exporters Only (last 15 minutes)** from the Showing menu.



6. Expand the device list to see all monitored nodes, check the options (NetFlow and/or CBQoS) for the parent nodes of the interfaces you want Orion NTA to monitor, and then click **Submit**.



Note: For pure CBQoS devices—those that do not export NetFlow—use **Show** to filter for **Cisco only** or **All Devices** and then check the CBQoS box.

Orion NTA should receive traffic data and display it within a few minutes.

Chapter 3

Orion NetFlow Traffic Analyzer Quick Tour

The features and flexibility provided by Orion NetFlow Traffic Analyzer give highly detailed insight into the quantity and the quality of traffic on your network. The sections of this chapter build on each other sequentially to show you the key features of Orion NetFlow Traffic Analyzer. This chapter is most useful when it is read and followed from start to finish; the chapter begins with an overview of the resources immediately available on the NetFlow Traffic Analyzer Summary view, and it continues through summaries of the most often used Orion NTA views.

Note: Extensive use cases, including scenarios incorporating other SolarWinds tools, are available in the final chapter of this Evaluation Guide. For more information, see Using NetFlow Traffic Analyzer on page 41.

Starting Orion NetFlow Traffic Analyzer

To start Orion NetFlow Traffic Analyzer, click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**. For more information about installing and configuring Orion NTA, see Installing Orion NetFlow Traffic Analyzer on page 7.

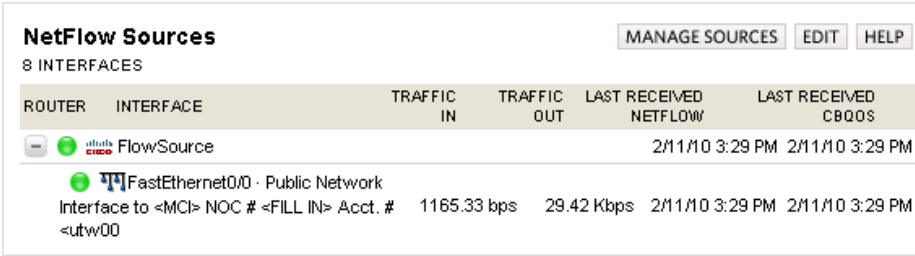
The NetFlow Traffic Analyzer Summary

When you launch Orion NetFlow Traffic Analyzer, the NetFlow Traffic Analyzer Summary is the first view displayed. This view provides insight into data traffic conditions over your entire network. The following resources are included in the NetFlow Traffic Analyzer Summary View by default.

NetFlow Sources

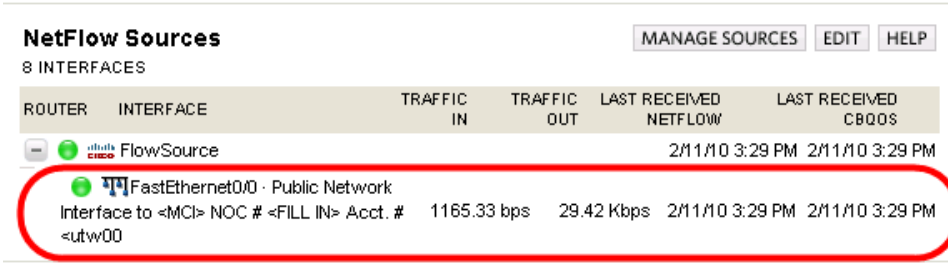
This resource provides a list of all Flow- and CBQoS-enabled devices on your network that are currently configured to send NetFlow data to the server hosting your Orion NTA installation. For more information about adding Flow-enabled devices, see Enabling Flow Analysis on page 14.

Click **+** next to any router name to display Flow- and CBQoS-enabled interfaces on the selected router.



Interfaces are also listed with both a status icon and a timestamp indicating when Orion NTA last received NetFlow data from the selected interface. Additionally, the NetFlow Sources resource provides reported values (as polled by Orion NPM) for both incoming and outgoing traffic on each interface.

Note: Since NetFlow Sources display values as polled by Orion NPM, these numbers may differ from those displayed in NTA charts.

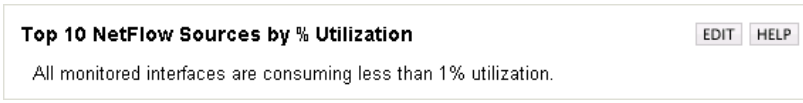


Clicking a router name opens the NetFlow Node Details view, and clicking an interface name opens the NetFlow Interface Details view. For more information about the NetFlow Node Details view, see NetFlow Node Details View on page 38. For more information about the NetFlow Interface Details view, see NetFlow Interface Details View on page 35.

Top 10 NetFlow Sources by % Utilization

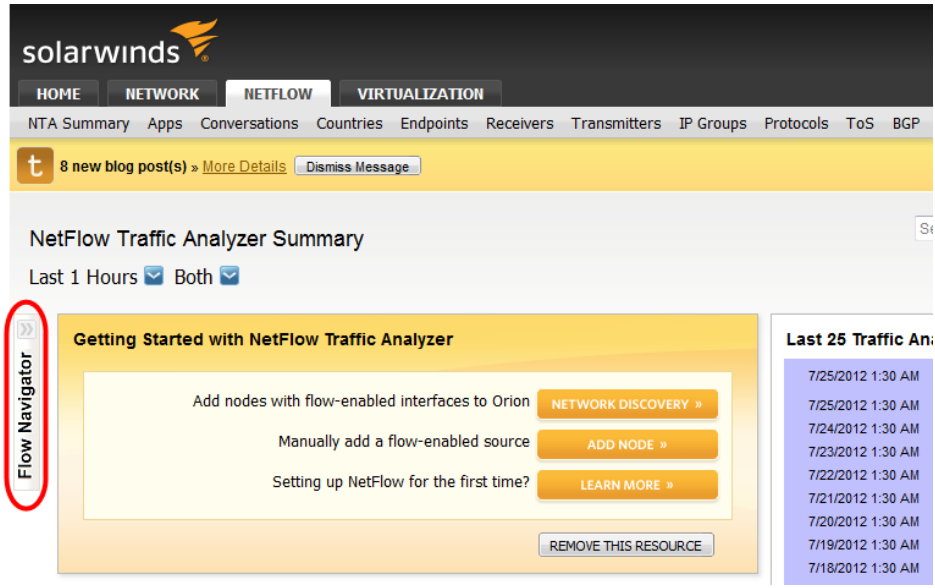
This resource provides a list of the NetFlow sources on your network that are currently routing enough traffic to significantly tax their system resources.

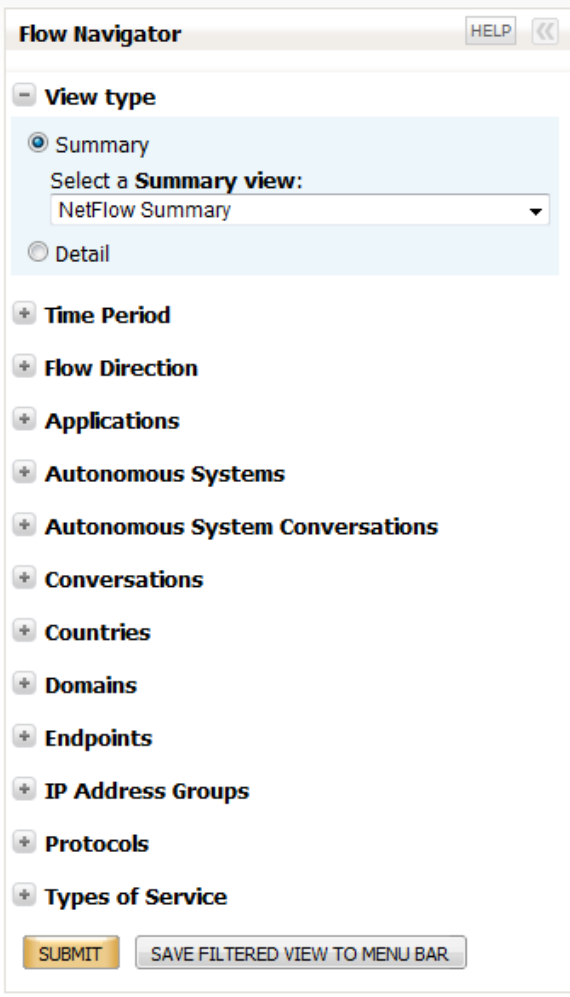
Note: Sources are only listed if they experience utilization in excess of 1%. Clicking on displayed interface open NetFlow Interface Details.



Flow Navigator

The Flow Navigator application allows you to filter your Orion NTA views and add them directly to the Views toolbar. Also, because Orion NTA is a web-based module, you can create browser bookmarks for any Orion NTA view to easily check the status of potential trouble spots at a later date. For more information about using the Flow Navigator to create custom views, see Using Flow Navigator Using Flow Navigator.





Top 5 Applications

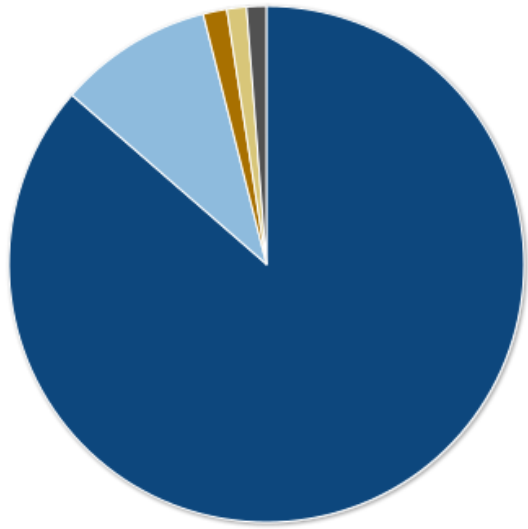
The Top 5 Applications resource provides a quick view of the applications and ports that are most in use by the devices on your network.

By clicking **+**, you can expand each application to see the network devices routing traffic for each application.

Top 5 Applications

BOTH, LAST 1 HOURS

EDIT HELP

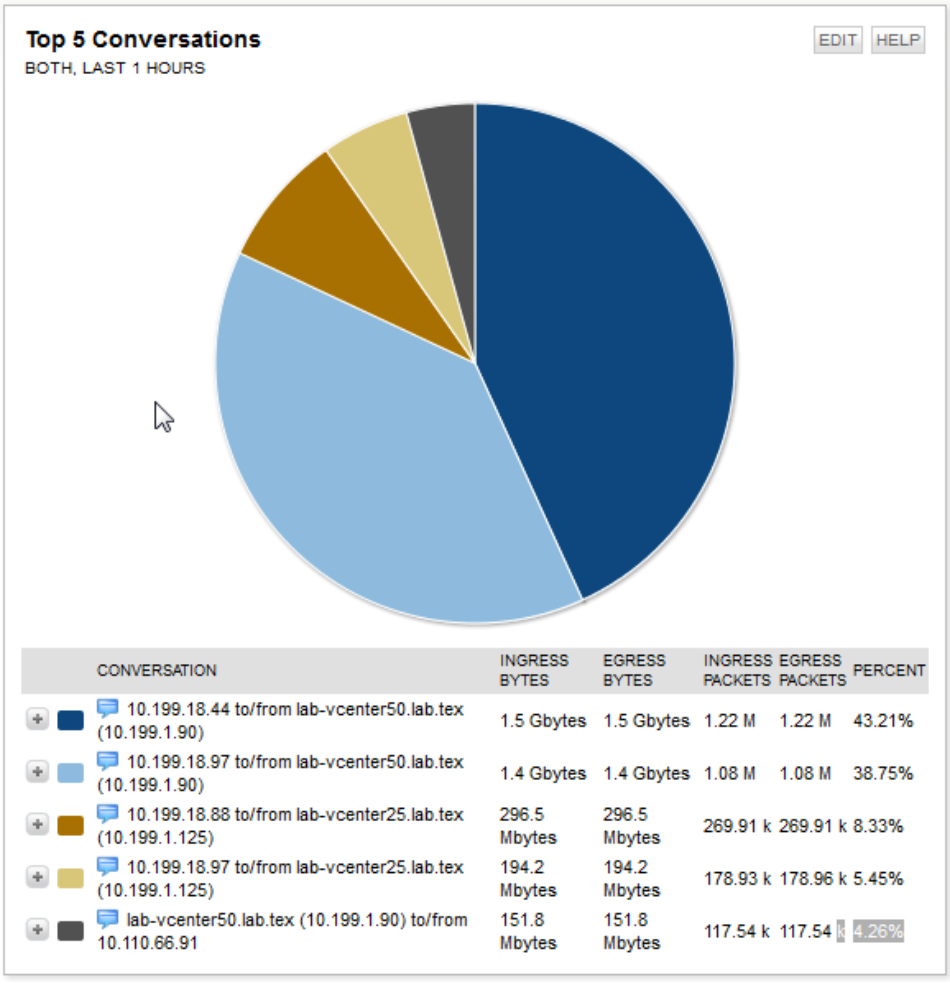


APPLICATION	INGRESS BYTES	EGRESS BYTES	INGRESS PACKETS	EGRESS PACKETS	PERCENT
http protocol over TLS/SSL (443)	11.4 Gbytes	11.4 Gbytes	9.58 M	9.58 M	86.37%
Microsoft-DS (445)	1.3 Gbytes	1.3 Gbytes	1.4 M	1.4 M	9.68%
SNMP (161)	196.6 Mbytes	196.1 Mbytes	920.26 k	914.15 k	1.49%
Port 49154 (TCP)	162.8 Mbytes	162.8 Mbytes	601.92 k	601.92 k	1.24%
Unmonitored traffic	162.0 Mbytes	161.8 Mbytes	566.02 k	560.95 k	1.23%

Top 5 Conversations

This resource provides view of the conversations using the most bandwidth on your network. Each color in the chart corresponds to a single continuing conversation between two specific endpoints. The table below the chart lists the endpoints involved in each conversation, with the bandwidth consumed by each conversation, in both bytes and packets.

Click **+** to expand the conversation description to see all devices on your network through which the selected conversation is conducted. The first level of expansion shows the network nodes through which conversation traffic is routed. The next level of expansion shows the interfaces that are passing traffic for the selected conversation.



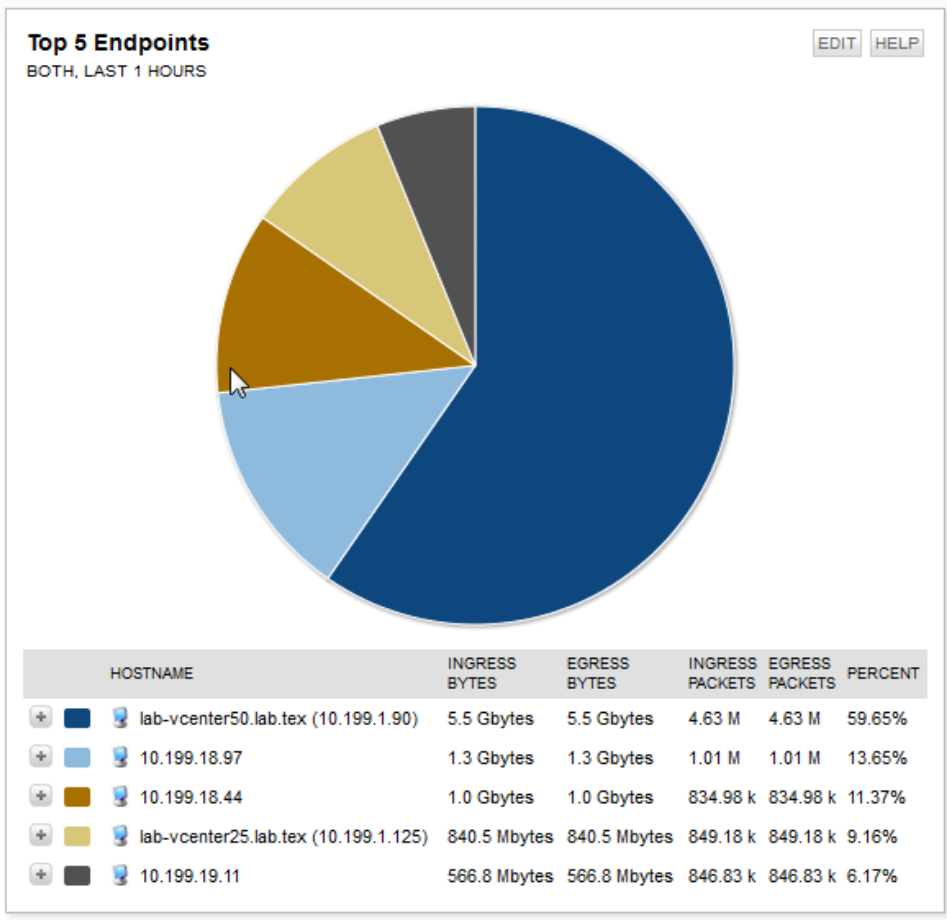
CONVERSATION	INGRESS BYTES	EGRESS BYTES	INGRESS PACKETS	EGRESS PACKETS	PERCENT
10.199.18.44 to/from lab-vcenter50.lab.tex (10.199.1.90)	1.5 Gbytes	1.5 Gbytes	1.22 M	1.22 M	43.21%
10.199.18.97 to/from lab-vcenter50.lab.tex (10.199.1.90)	1.4 Gbytes	1.4 Gbytes	1.08 M	1.08 M	38.75%
10.199.18.88 to/from lab-vcenter25.lab.tex (10.199.1.125)	296.5 Mbytes	296.5 Mbytes	269.91 k	269.91 k	8.33%
10.199.18.97 to/from lab-vcenter25.lab.tex (10.199.1.125)	194.2 Mbytes	194.2 Mbytes	178.93 k	178.96 k	5.45%
lab-vcenter50.lab.tex (10.199.1.90) to/from 10.110.66.91	151.8 Mbytes	151.8 Mbytes	117.54 k	117.54 k	4.26%

At both the node and interface levels, respective shares of the total bandwidth consumed by the selected conversation are listed in both bytes and packets. For any node, the conversation traffic on the node is equal to the sum of the conversation traffic on all the interfaces on that node.

For more information, see NetFlow Conversations View on page 32.

Top 5 Endpoints

The Top 5 Endpoints resource gives an at-a-glance view of the endpoints that are the sources or targets of the most network traffic. By clicking **+** to expand each endpoint, you can see the network devices routing traffic for each endpoint.



Search by Endpoint or Application/Port

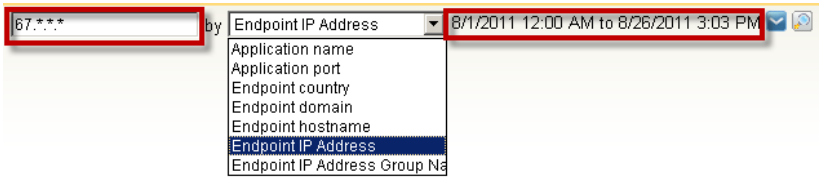
Using this resource, you can quickly locate any endpoint communicating with any devices or using a specific application on your network.

Search results provide an expandable list matching your search criteria. Clicking any result, followed by clicking the name of any of your network devices, opens the appropriate view—NetFlow Endpoint View or NetFlow Application View—for all traffic passing through the selected device.

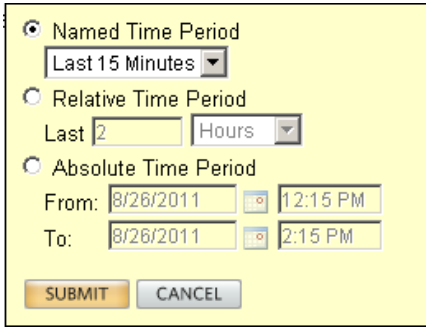
For more information about the NetFlow Endpoint View, see NetFlow Endpoint View on page 33. For more information about the NetFlow Application View, see NetFlow Application View on page 30.

To search for an endpoint:

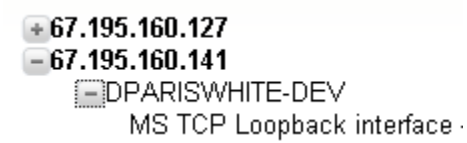
1. Select the appropriate endpoint filter in the list.



2. Select a time period.

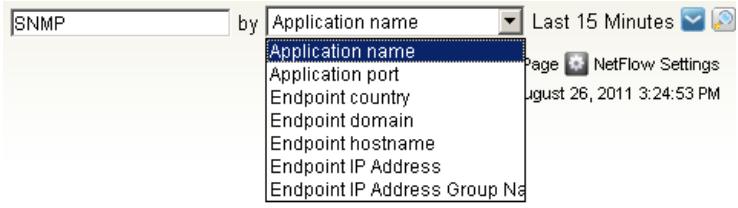


3. Enter the endpoint's IP address and then push **Enter.**

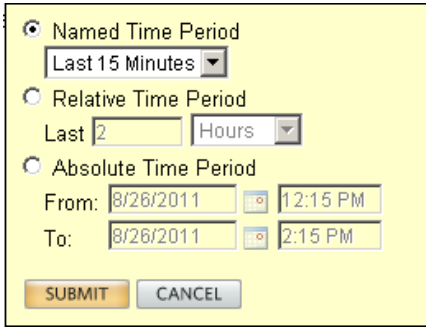


To search for an application/port:

1. Select the appropriate application filter in the list.



2. Select a time period.



3. Enter the relevant application information and then push **Enter.**

Last 25 Traffic Analysis Events

This resource lists the last 25 NetFlow-specific events that have occurred to devices on your monitored network. Typically, this resource lists the dates and times when the NetFlow Receiver Service stops and starts, but it is also used to communicate updates for database upgrades and to provide notification of newly discovered Flow sources.

Orion NetFlow Traffic Analyzer Views

The following sections detail the types of information that are available by default on selected Orion NTA views.

Notes:

- The following are a few of the Orion NTA views that are used in most typical installations. These listed views are linked directly from default resources on the NetFlow Traffic Analyzer Summary view. Additional resources available on the NetFlow Traffic Analyzer Summary view and on subsequent Orion NTA views link to additional views. For more information about Orion NTA views and resources, see Viewing NetFlow Traffic Analyzer Data in the Orion Web Console in the *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.
- Some resources may not be present in the default configuration of a selected view. To see all available resources, you must edit the view with the Customize Page options. For more information, see Viewing NetFlow Traffic Analyzer Data in the Orion Web Console in the *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

NetFlow Application View

The following sections offer brief descriptions of the resources on the NetFlow Application view. More information about each resource, including configuration details, is available by clicking **Help** in the resource title bar.

Application Details

The Application Details resource provides a table that contains the relevant application name, port used by the application, total amount of traffic data within the selected period of time, and the total number of packets sent within the selected period of time.

Top 5 Protocols

The Top 5 Protocols resource provides a view of the traffic protocols the selected application uses most. The table below the chart provides the protocol type, the amount of data, the total number of packets, and the percentage of all traffic that has been using each listed protocol.

Top 5 Types of Service

The Top 5 Types of Service resource provides a view of the most active services employed by the selected application. The table below the chart provides the type of service, the amount of traffic handled by the service, the number of packets handled by the service, and the percentage of all serviced traffic to the selected application that is handled by the selected type of service

Total Bytes Transferred

The Total Bytes Transferred resource displays a chart that details the total number of bytes that are transferred by the selected application over a specified period of time.

Unique Visitors

The Unique Visitors resource provides a chart that details the number of unique IP addresses that have used the selected application over a specified period of time.

Total Packets Transferred

The Total Packets Transferred resource displays a chart that details the total number of packets transferred by the selected application over a specified period of time.

Top 5 Transmitters

The Top 5 Transmitters resource provides a view of the most active transmitting endpoints using the selected application. The table below the chart provides the name or IP address of the endpoint, the amount of traffic that is transmitted by the endpoint, and the percentage of all transmitted traffic that is traceable to the endpoint.

You can click each listed endpoint to open the NetFlow Endpoint view that presents similar statistics for each transmitting endpoint. For more information, see NetFlow Endpoint View on page 33.

Top 5 Receivers

The Top 5 Receivers resource provides a view of the most active receiving endpoints using the selected application. The table below the chart provides the name or IP address of the endpoint, the amount of traffic that is received by the endpoint, and the percentage of all received traffic that is traceable to the endpoint.

You can click each listed endpoint to open the NetFlow Endpoint view that presents similar statistics for each receiving endpoint. For more information, see NetFlow Endpoint View on page 33.

Top 5 Traffic Sources by Country

The Top 5 Traffic Sources by Country resource provides a view of the countries where traffic on the selected application originates, ranked by percentage of total application traffic. The table below the chart provides the name of the country, the amount of traffic that is sourced in the country, and the percentage of all traffic that is traceable to the country.

Top 5 Traffic Destinations by Country

The Top 5 Traffic Destinations by Country resource provides a view of the countries that serve as destinations of traffic on the selected application, ranked by percentage of total application traffic. The table below the chart provides the name of the country, the amount of application traffic that is routed to endpoints in the country, and the percentage of all application traffic traceable to endpoints in the country

Top 5 Conversations

The Top 5 Conversations resource provides a list of the most bandwidth-heavy conversations routed through the selected device, using the selected application. Conversations are listed with the amount of data transferred in the conversation, in both bytes and packets, and the percentage of total application traffic generated by the conversation. Clicking a conversation opens the NetFlow Conversation view for the selected conversation. For more information, see NetFlow Conversations View below.

NetFlow Conversations View

The following sections offer brief descriptions of the resources on the NetFlow Conversation view. More information about each resource, including configuration details, is available by clicking **Help** in the resource title bar.

Total Bytes Transferred

The Total Bytes Transferred resource displays a chart detailing the total number of bytes transferred, over a specified period of time, between the two nodes, IP addresses, or domains indicated in the view title.

Conversation Traffic History

The Conversation Traffic History resource provides a table displaying the date/time stamp of the exchange, the protocol used for the exchange, the application and port used for the exchange, the direction of the traffic flow, the amount of traffic communicated in bytes, and the equivalent number of packets communicated.

NetFlow Endpoint View

The following sections offer brief descriptions of the resources on the NetFlow Endpoint view. More information about each resource, including configuration details, is available by clicking **Help** in the resource title bar.

Endpoint Details

The Endpoint Details resource provides the following information about a selected endpoint:

- IP address
- Hostname
- IP address group
- Domain
- Country
- Total traffic transmitted
- Total traffic received

Top 25 Conversation Endpoints

This resource provides a list of the endpoints with which the currently viewed endpoint has transferred the most data. For each conversation, this resource reports the amount of data transferred in the conversation and the percentage the listed conversation represents of the total data transferred by the viewed endpoint. Clicking an endpoint opens the NetFlow Endpoint view for the selected endpoint. All other links for a listed endpoint open the NetFlow Conversation view for the conversation between the viewed and selected endpoints. For more information, see NetFlow Conversations View on page 32.

Total Packets Transferred

The Total Packets Transferred resource displays a chart displaying the total number of packets both transmitted from the viewed endpoint and received by the viewed endpoint over a specified period of time.

Total Bytes Transferred

The Total Bytes Transferred resource displays a chart detailing the total number of bytes both transmitted from the viewed endpoint and received by the viewed endpoint, over a specified period of time.

Top 5 Protocols

The Top 5 Protocols resource provides an at-a-glance view of the traffic protocols that the selected endpoint uses most. The table below the chart

provides the protocol type, the amount of data, the total number of packets, and the percentage of all traffic that has been using each listed protocol.

Top 5 Applications

The Top 5 Applications resource provides a quick view of the applications used most by the selected endpoint. The table below the chart provides the application name, the amount of data that is flowing, the equivalent total number of packets, and the percentage of all traffic that is traceable to use of the listed application by the selected endpoint. Clicking an application opens the NetFlow Application view. For more information, see NetFlow Application View on page 30.

Top 5 Traffic Sources by Country

The Top 5 Traffic Sources by Country resource provides an at-a-glance view, in the form of a chart, of the countries where traffic to the selected endpoint originates, ranked by percentage of total traffic to the selected endpoint. The table below the chart provides the name of the country sourcing traffic to the viewed endpoint, the amount of traffic routed to the endpoint from the listed country, and the percentage of all traffic routed to the viewed endpoint that is traceable to the listed country.

Top 5 Traffic Destinations by Country

The Top 5 Traffic Destinations by Country resource provides a chart and table of the countries hosting destinations of traffic from the selected endpoint, ranked by percentage of total traffic from the selected endpoint. The table below the chart provides the name of the country to which traffic is routed, the amount of traffic routed to servers in the listed country, and the percentage of all routed traffic from the viewed endpoint that is routed to servers in the listed country.

Unique Visitors

The Unique Visitors resource provides a chart of unique IP addresses that have communicated with the viewed endpoint over a specified period of time.

Top 5 Traffic Destinations by Domain

The Top 5 Traffic Destinations by Domain resource provides a chart and table of the domains hosting destinations of traffic from the selected endpoint, ranked by percentage of total traffic from the selected endpoint. The table below the chart provides the name of the domain to which traffic is routed, the amount of traffic routed to servers in the listed domain, and the percentage of all routed traffic from the viewed endpoint that is routed to servers in the listed domain.

Top 5 Traffic Sources by Domain

The Top 5 Traffic Sources by Domain resource provides a chart and table of the domains hosting sources of traffic from the selected endpoint, ranked by percentage of total traffic from the selected endpoint. The table below the chart

provides the name of the domain to which traffic is routed, the amount of traffic routed to servers in the listed domain, and the percentage of all routed traffic from the viewed endpoint that is routed to servers in the listed domain.

Top 5 IP Group Conversations

The Top 5 IP Groups Conversations resource provides a chart and table of the conversations generating traffic from the selected endpoint, ranked by percentage of total traffic. The table below the chart provides the name of the IP Group to which traffic is routed, the amount of traffic routed to servers in the listed IP Group, and the percentage of all routed traffic from the viewed endpoint that is routed to servers in the listed IP Group.

Top 5 Types of Service

The Top 5 Types of Service resource provides a quick view of the services most actively employed by the selected endpoint. The table below the chart provides the type of service, the amount of traffic in bytes and packets that is handled by the service, and the percentage of all serviced traffic to the selected endpoint that is handled by the selected type of service.

For more information about service type monitoring in Orion NTA, see Configuring NetFlow Types of Service in the *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

NetFlow Interface Details View

The following sections offer brief descriptions of the resources on the default NetFlow Interface Details view. More information about each resource, including configuration details, is available by clicking **Help** in the resource title bar.

Note: For the NetFlow Node Details View, and the NetFlow Interface Detailed View, and for any managed Orion device, you can add endpoint-centric resources that filter information regarding the node in terms of all standard Orion NTA filters, giving you relevant traffic initiation and termination information. For information on adding such resources, see Adding an Endpoint Centric Resource.

Top 5 Protocols

The Top 5 Protocols resource provides a view of the traffic protocols the viewed interface sees most. The table below the chart provides the protocol type, the amount of data, the total number of packets, and the percentage of all traffic over the viewed interface using each listed protocol.

Top 5 Applications

The Top 5 Applications resource provides a quick view of the applications used most by the viewed interface. The table below the chart provides the application

name, the amount of data that is flowing, the equivalent total number of packets, and the percentage of all traffic that is traceable to use of the listed application by the viewed interface. Clicking an application opens the NetFlow Application view. For more information, see NetFlow Application View on page 30.

Top 5 Conversations

This resource provides a list of conversations creating the most traffic over the viewed interface. For each conversation, this resource reports the amount of data transferred in the conversation and the percentage the listed conversation represents of the total data transferred over the viewed interface. Clicking a conversation opens the NetFlow Conversation view for the selected conversation. For more information, see NetFlow Conversations View on page 32.

CBQoS Pre-Policy Class Map

If you are viewing a CBQoS-enabled interface to which a CBQoS policy is currently applied, this resource displays the classes of traffic traversing the viewed interface. For each class of defined traffic, the table below the chart reports the average and most recently polled interface utilization values as a percentage of total defined interface bandwidth as measured before any traffic-shaping CBQoS policy is applied on the viewed interface.

CBQoS Post-Policy Class Map

If you are viewing a CBQoS-enabled interface to which a CBQoS policy is currently applied, this resource displays the classes of traffic traversing the viewed interface. For each class of defined traffic, the table below the chart reports the average and most recently polled interface utilization values as a percentage of total defined interface bandwidth as measured after any traffic-shaping CBQoS policy is applied on the viewed interface.

CBQoS Policy Details

If you are viewing a CBQoS-enabled interface to which a CBQoS policy is currently applied, this resource displays the applied traffic policies and corresponding defined traffic classes on the viewed interface. For each defined traffic class, this resource provides the amount of traffic and corresponding percentage of total defined interface bandwidth over both the last hour and the last 24 hours.

CBQoS Drops

If you are viewing a CBQoS-enabled interface to which a CBQoS policy is currently applied, this resource displays the amount of traffic traversing the viewed interface that is dropped as a result of CBQoS policy application. For each class of defined traffic, the table below the chart reports the average and most recently polled interface utilization values as a percentage of total defined

interface bandwidth corresponding to the amount of traffic that is dropped as a result of CBQoS policy application.

Top 5 Endpoints

The Top 5 Endpoints resource provides a view of the endpoints producing the most traffic over the selected interface. The table below the chart provides the name or IP address of each listed endpoint, the amount of traffic from each listed endpoint, in both bytes and packets, and the percentage of all traffic over the viewed interface that is traceable to each listed endpoint. Clicking an endpoint opens the NetFlow Endpoint view for the selected endpoint. For more information, see NetFlow Endpoint View on page 33.

Top 5 Traffic Destinations by Domain

The Top 5 Traffic Destinations by Domain resource provides a chart and table of the domains hosting destinations of traffic from the selected interface, ranked by percentage of total traffic. The table below the chart provides the name of the domain to which traffic is routed, the amount of traffic routed to servers in the listed domain, and the percentage of all routed traffic from the viewed interface that is routed to servers in the listed domain.

Top 5 Traffic Sources by Domain

The Top 5 Traffic Sources by Domain resource provides a chart and table of the domains hosting sources of traffic from the selected interface, ranked by percentage of total traffic from the selected interface. The table below the chart provides the name of the domain to which traffic is routed, the amount of traffic routed to servers in the listed domain, and the percentage of all routed traffic from the viewed interface that is routed to servers in the listed domain.

Top 5 IP Group Conversations

The Top 5 IP Groups Conversations resource provides a chart and table of the conversations generating traffic from the selected interface, ranked by percentage of total traffic. The table below the chart provides the name of the IP Group to which traffic is routed, the amount of traffic routed to servers in the listed IP Group, and the percentage of all routed traffic from the viewed interface that is routed to servers in the listed IP Group.

Top 5 Domains

This resource provides a view of the domains producing the most traffic on the selected interface. The table below the chart provides the domain name, the amount of traffic in bytes, the total number of packets communicated, and the percentage of all traffic on the selected interface that is traceable to each domain.

Note: This resource is only available if persistent DNS resolution is enabled. On evaluation installations, DNS resolution is set to persistent by default. For more information, see Configuring DNS and NetBIOS Resolution in the *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

Top 5 Types of Service

The Top 5 Types of Service resource provides a quick view of the services most actively employed by the viewed interface. The table below the chart provides the type of service, the amount of traffic in bytes and packets that is handled by the service over the viewed interface, and the percentage of all serviced traffic over the viewed interface that is handled by the selected type of service.

For more information about service type monitoring in Orion NTA, see in the *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

NetFlow Node Details View

The following sections offer brief descriptions of the resources on the default NetFlow Node Details view. More information about each resource, including configuration details, is available by clicking **Help** in the resource title bar.

Note: For the NetFlow Node Details View, and the NetFlow Interface Detailed View, and for any managed Orion device, you can add endpoint-centric resources that filter information regarding the node in terms of all standard Orion NTA filters, giving you relevant traffic initiation and termination information. For information on adding such resources, see Adding an Endpoint Centric Resource.

Top 5 Protocols

The Top 5 Protocols resource provides a view of the traffic protocols the viewed node uses most. The table below the chart provides the protocol type, the amount of data, the total number of packets, and the percentage of all traffic on the viewed node using each listed protocol.

Top 5 Applications

The Top 5 Applications resource provides a quick view of the applications used most by the viewed node. The table below the chart provides the application name, the amount of data that is flowing, the equivalent total number of packets, and the percentage of all traffic that is traceable to use of the listed application by the viewed node. Clicking an application opens the NetFlow Application view. For more information, see NetFlow Application View on page 30.

Top 5 Conversations

This resource provides a list of conversations that are creating the most traffic over the viewed node. For each conversation, this resource reports the amount of data transferred in the conversation and the percentage the listed conversation represents of the total data transferred over the viewed node. Clicking a conversation opens the NetFlow Conversation view for the selected conversation. For more information, see NetFlow Conversations View on page 32.

Top 5 Endpoints

The Top 5 Endpoints resource provides both a chart and a table view of the endpoints producing the most traffic over the viewed node. The table below the chart provides the name or IP address of each listed endpoint, the amount of traffic from each listed endpoint, in both bytes and packets, and the percentage of all traffic over the viewed node that is traceable to each listed endpoint. Clicking an endpoint opens the NetFlow Endpoint view for the selected endpoint. For more information, see NetFlow Endpoint View NetFlow Endpoint View on page 33.

Top 5 Domains

This resource provides an at-a-glance view of the domains that are producing the most traffic on the viewed node. The table below the chart provides the domain name, the amount of traffic in bytes, the total number of packets communicated, and the percentage of all traffic on the viewed node traceable to each domain.

Note: This resource is only available if persistent DNS resolution is enabled. By default on evaluation installations, DNS resolution is configured to occur on demand only. For more information, see Configuring DNS and NetBIOS Resolution in the *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

Node Interfaces

This resource provides a list of all monitored interfaces on the viewed node. For each interface, both incoming and outgoing traffic are reported. Clicking an interface opens the NetFlow Interface Details view for the selected interface. For more information, see NetFlow Interface Details View on page 35.

Chapter 4

Using Orion NetFlow Traffic Analyzer

While Orion Network Performance Monitor can tell you the bandwidth usage on an interface, Orion NTA takes this ability one step further, by providing information about the actual user of that bandwidth and the applications they are using. The scenarios presented in this chapter illustrate the value of Orion NTA and how it can immediately offer you a significant return on your investment.

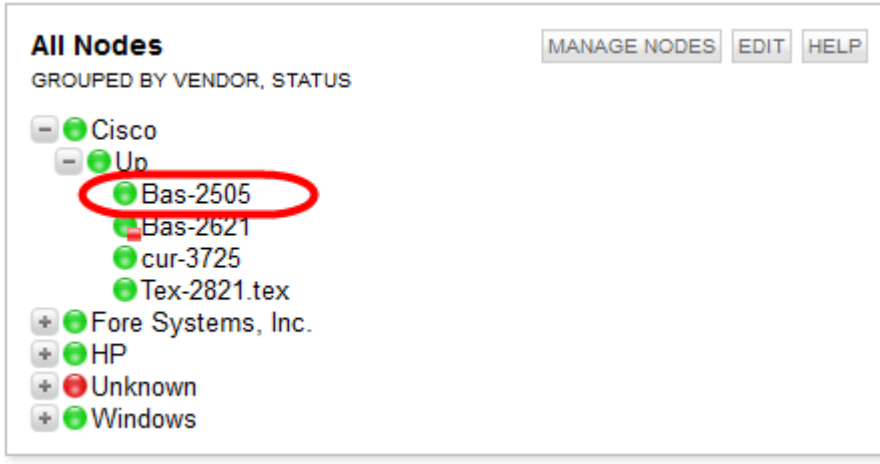
Adding Endpoint Centric Resources to Orion Nodes

Using **Customize Page,** you can add an endpoint-centric resource to the Node Details or Interface Details view on any node in Orion Network Performance Manager.

Note: An endpoint centric resource displays information related to a concrete node, which is also an endpoint.

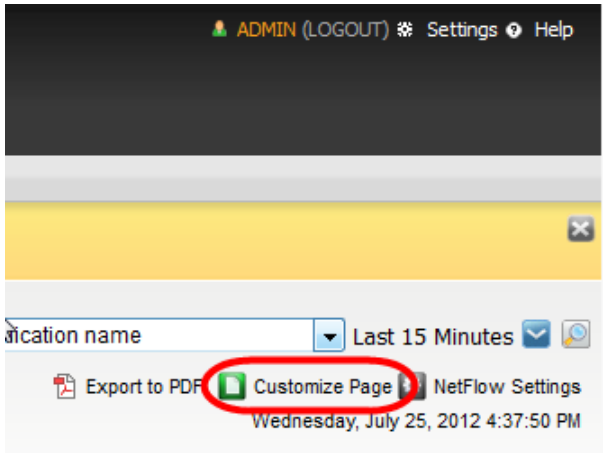
To add an endpoint-centric resource:

1. Open the Orion Web Console.
2. Click the relevant node in All Nodes on the HOME page.

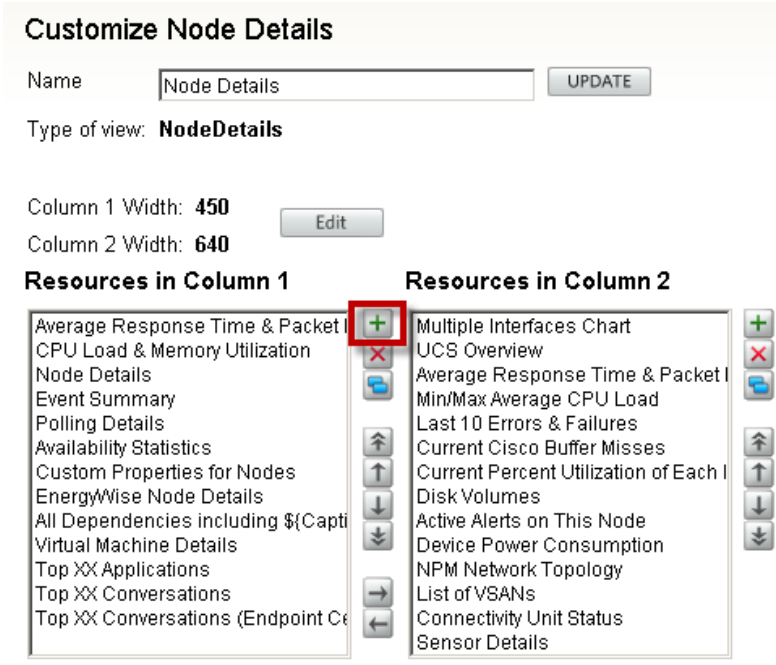


   If nodes on All Nodes are grouped, drill down as needed into the relevant group.

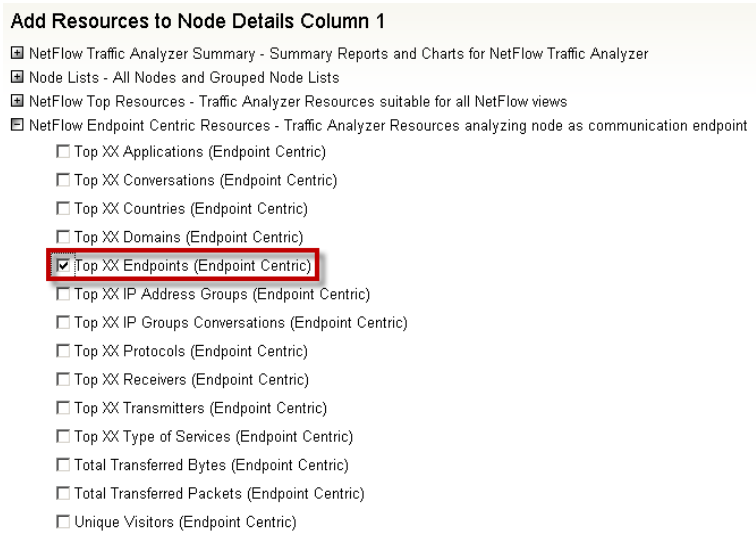
3. Click **Customize Page** on the Node Details view.



4. Click **+** over the column in which you want the new resource to be placed.

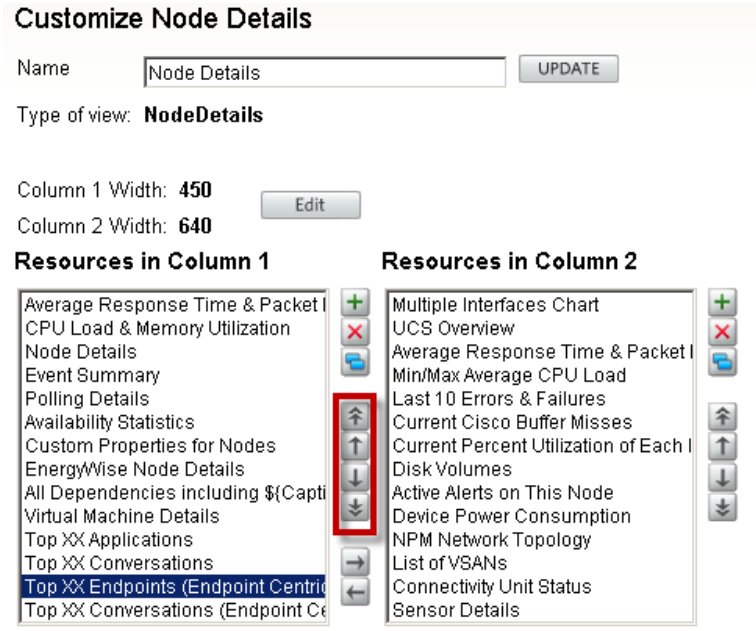


5. Click **NetFlow Endpoint Centric Resources** and check the appropriate resource.



6. Click **Submit**.

7. Use the arrow controls to move the resources listed in the column into the order you want displayed in the Orion Web Console.



8. Click **Done**.

Adding Top Talker Statistics to Orion Alerts

Orion alerting software can alert on polled, syslog, and trap data. Alerts are defined in terms of thresholds related to data in the Orion database. Scans in the form of SQL queries at set intervals detect recorded values that exceed thresholds, triggering an alert if relevant conditions pertain.

When an Orion alert is triggered, the software evaluates suppression criteria. If an alert is not qualified to be suppressed, the software executes a defined action. If no action is defined, the software merely displays the alert on the web console.

Throughout this workflow timers are used to allow the software to do its work at each step and to ensure that the alerting workflow had appropriate redundancy for timely reporting of alerts.

For an excellent overview of alerting in Orion advanced alerts, see Understanding Orion Advanced Alerts. For all specific information on Orion basic and advanced alerts, including detailed instructions for creating and managing them with the Orion Alert Manager, see Creating and Managing Alerts, in the *Orion Network Performance Monitor Administrator's Guide*.

Top Talker Advanced Alerts

When you install SolarWinds Orion Network Traffic Analyzer, the software automatically creates in the Orion Alert Manager two predefined alerts called "High Receive Percent Utilization with Top Talkers" and "High Transmit Percent Utilization with Top Talkers."

The primary purpose of these alerts is to help in understanding what specific network traffic contributed most to reaching the set interface bandwidth utilization threshold, triggering the utilization threshold alert.

By default, these advanced alerts, when triggered, do two things: 1) write the bandwidth utilization event to the SolarWinds event log when the current percent utilization on the transmit side of an interface rises above specified value, and then again when the utilization drops back down below a specified value. 2) Initiate a web capture of the most current top talker information and then append and send that information in an email to the configured recipient.

The instructions in this section assume you are familiar with the Orion Alert Manager and already know how to setup an advanced alert.

For steps on creating an advanced alert see the sections on advanced alerts in Creating and Managing Alerts in the *Orion Network Performance Monitor Administrator's Guide*.

To use the default NetFlow "High Transmit Percent Utilization with Top Talkers" alert:

1. Open the Orion Alert Manager in the Orion program group.
2. Navigate to the Manage Alerts resource resource (View > Configure Alerts).
3. Select the relevant top talker alert.
4. Click Edit.
   a. On General, check Enable this Alert and select an appropriate Alert Evalutation Frequency.
   b. On Trigger Condition, define the conditions in which the software launches the alert.

      The default condition is the interface's transmit utilitization percentage exceeding 75. You can adjust this condition or add conditions.

   c. On Reset Condition, define the conditions in which the software resets the alert.

      The default condition is the interface's transmit utilitization percentage going below 50. You can adjust this condition or add conditions.

   d. On Alert Suppression, define the conditions in which the software suppresses the alert.

      The default condition is no suppression.

   e. On Time of Day, define the days and times during which the software actively evaluates the database for trigger conditions.

      The default range is 24/7.

   f. On Trigger Actions, create actions to execute when the software triggers the alert.

      As discussed, the default action writes to the SolarWinds event log, initiates a web capture of current top talkers transmitting on the overutilized interface, and then append and send the information in email to an appropriate contact.

      Note: On the **URL** tab, if you changed the default Orion login from 'Admin' with a blank password, then accordingly you will need to change the URL that the trigger action uses to send out the notification.

      For example, if your new credentials were username **NTA User** with password **Bravo**, you would adjust the default URL so that:

${SQL:SELECT REPLACE(REPLACE(Macro, **'$$Password$$', ''),'$$User$$', 'Admin'**) FROM NetFlowAlertMacros WHERE ID='InWebMailInterfaceDetailsLink'}

becomes:

${SQL:SELECT REPLACE(REPLACE(Macro, **'$$Password$$', 'Bravo'),'$$User$$', 'NTA User'**) FROM NetFlowAlertMacros WHERE ID='InWebMailInterfaceDetailsLink'}

g. On Reset Conditions, define actions to execute when the software resets the alert. .

As discussed, the default reset action writes to the SolarWinds event log.

5. Click **OK** and then click **Done**.

To use the default NetFlow "High Receive Percent Utilization with Top Talkers" alert:

1. Open the Orion Alert Manager in the Orion program group.

2. Navigate to the Manage Alerts resource (**View > Configure Alerts**).

3. Select the relevant top talker alert.

4. Click **Edit**.

a. On General, check Enable this Alert and select an appropriate Alert Evalutation Frequency.

b. On Trigger Condition, define the conditions in which the software launches the alert.

The default condition is the interface's transmit utilitization percentage exceeding 75. You can adjust this condition or add conditions.

c. On Reset Condition, define the conditions in which the software resets the alert.

The default condition is the interface's receive utilitization percentage going below 50. You can adjust this condition or add conditions.

d. On Alert Suppression, define the conditions in which the software suppresses the alert.

The default condition is no suppression.

e. On Time of Day, define the days and times during which the software actively evaluates the database for trigger conditions.

The default range is **24/7**.

f. On Trigger Actions, create actions to execute when the software triggers the alert.

As discussed, the default action writes to the SolarWinds event log, initiates a web capture of current top talkers receiving on the over-utilized interface, and then append and send the information in email to an appropriate contact.

Note: On the **URL** tab, if you changed the default Orion login from 'Admin' with a blank password, then accordingly you will need to change the URL that the trigger action uses to send out the notification.

For example, if your new credentials were username 'NTA User' with password 'Bravo,' you would adjust the default URL so that:

${SQL:SELECT REPLACE(REPLACE(Macro, **'$$Password$$', ''),'$$User$$', 'Admin'**) FROM NetFlowAlertMacros WHERE ID='InWebMailInterfaceDetailsLink'}

becomes:

${SQL:SELECT REPLACE(REPLACE(Macro, **'$$Password$$', 'Bravo'),'$$User$$', 'NTA User'**) FROM NetFlowAlertMacros WHERE ID='InWebMailInterfaceDetailsLink'}

g. On Reset Conditions, define actions to execute when the software resets the alert. .

As discussed, the default reset action writes to the SolarWinds event log.

5. Click **OK** and then click **Done**.

Using the Flow Navigator

You can create custom traffic views directly from any NetFlow view, using the Flow Navigator. These custom filters allow you to view specific statistics about your entire network and its devices without having to navigate through the web console a single device view at a time. You can configure your custom traffic view to include devices, applications, time periods, and more, all from one configuration pane, as shown in the following procedures.

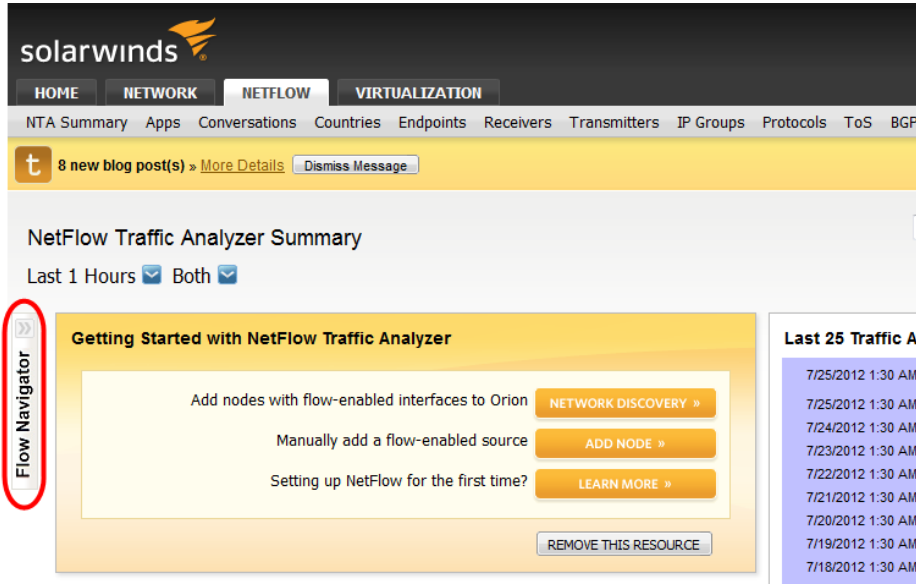
Viewing Traffic for a Designated IP Address

The following procedure filters the current Orion NTA view by showing both incoming and outgoing network traffic from a designated IP address.

To filter a NetFlow traffic view with the Flow Navigator:

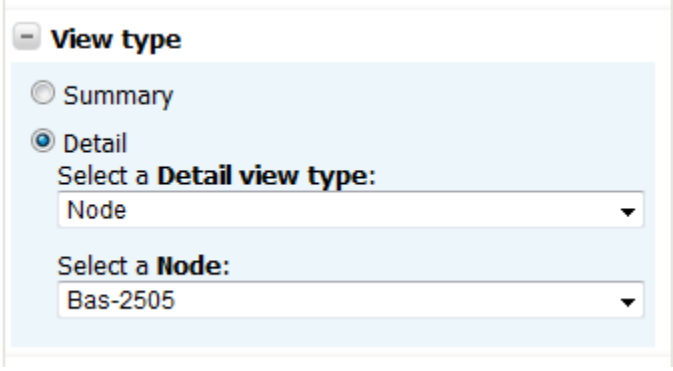
1. Open the NetFlow Web Console in the SolarWinds program group.

2. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.



3. Click **Flow Navigator** on the left edge of the summary view. (The Flow Navigator is available on any default NTA view.)

4. Select a view type.

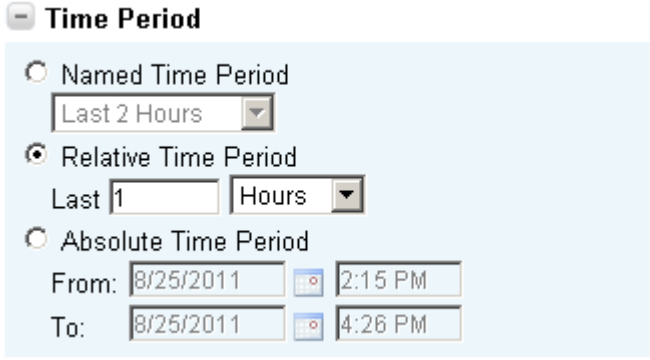


a. ***If you want a filtered view of your entire network***, click **Summary**.

b. ***If you want a filtered view of traffic passing through a specific node and interface*****,** click **Detail.**

- Select the **Node** for which you want to monitor network traffic attributed to the selected view type.
- Select the **Interface** for which you want to monitor network traffic attributed to the selected view type.
- Select or type in the view-related information.

5. Select the **Time Period** from which you want to view traffic data, using any of the following options:



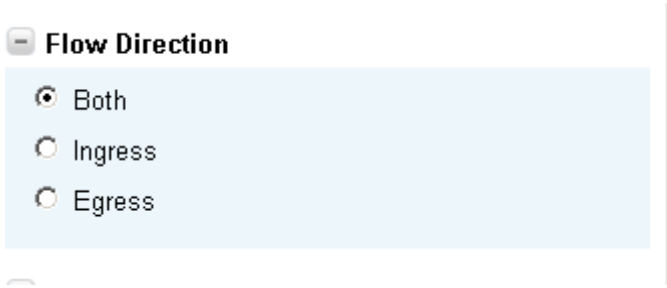
- Select **Named Time Period**, and then select a predefined period from the Named Time Period menu.
- Select **Relative Time Period**, and then provide a number appropriate for the selected time units.

  Note: The relative time period is measured with respect to the time at which the configured view is loaded.

- Select **Absolute Time Period**, and then provide both the start time and the end time for the period over which you want to view monitoring data.

  Note: Use the calendars to set your time.

6. Select a **Flow Direction**.



- Select **Both** to include ingress and egress traffic in the calculations NTA makes.

  Note: For the Node Details view, this selection is automatically converted to Ingress.
- Select **Ingress** to include only ingress traffic in the calculations NTA makes.
- Select **Egress** to include only egress traffic in the calculations NTA makes.

7. Select **Endpoints**.

8. When you have completed configuration of your filtered application view, click **SUBMIT.**
9. ***If you want to save your custom view for future reference,*** click **SAVE FILTERED VIEW TO MENU BAR**.

Note: You can also use an IP Groups filter for endpoints.

Locating and Isolating an Infected Computer

You can use your currently installed Orion NPM instance, with the addition of Orion NTA, to quickly pinpoint and respond to the wide variety of self-propagating viruses that can attack your network. Consider the following scenario:

1. A local branch of your bank network that handles all credit card transactions complains of an extremely sluggish network, causing frequent timeouts during sensitive data transfers.
2. The Orion Web Console shows that the link to the branch network is up.
3. Orion NPM Percent Utilization charts on the Network Summary home page show that current utilization is 98%, even though normal branch network utilization is 15-25%.
4. You click **NetFlow** in the Modules toolbar, and then click the name of the branch network link in the NetFlow Sources resource to view the Flow-enabled router on the branch network.
5. Taking a quick look at the Top 5 Endpoints resource, you see that a single computer in the `10.10.10.0-10.10.10.255` IP address range is generating 80% of the load on the branch link.
6. You know that computers in this IP address range are accessible to customers for personal transactions using the web.
7. By viewing the Top 5 Applications resource, you quickly see that 100% of the last two hours of traffic from a publicly accessible computer has been generated by an IBM MQSeries messaging application.
8. By clicking the IBM MQSeries messaging application name in the Top 5 Applications resource, you are able to determine that IBM MQSeries messaging occurs over port 1883.
9. Knowing that you don't 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.
10. To address the problem discovered (in step 5), using a configuration management tool, such as Orion Network Configuration Manager, you push a new configuration to your firewall that blocks port 1883.

Locating and Blocking Unwanted Use

With Orion NTA, you can easily chart increasing usage on any of your different network uplinks. Orion NPM already allows you to chart utilization, but, with the addition of Orion NTA, you can locate specific instances of unwanted use, immediately allowing you to take corrective action, as in the following scenario:

1. Your uplink to the internet has been slowing progressively over the last 6 months, even though your corporate head count, application use, and dedicated bandwidth have all been stable.
2. When you open the Orion Web Console, the Network Summary Home view shows that your site link to the internet is up, but, when you click your specific uplink and consult the Current Percent Utilization of each Interface chart, you see that the current utilization of your web-facing interface is 80%.
3. You click your web-facing interface to open the Interface Details view.
4. Customizing the Percent Utilization chart to show the last 6 months, you see that there has been steady growth from 15% to 80% consumption over time. There are even spikes into the high 90s.
5. You click the NetFlow Traffic Analysis tab, and then click the web-facing interface to open the NetFlow Interface Details view.
6. Looking at the top 50 Endpoints, you see that a group of computers in the `10.10.12.0-10.10.12.255` IP address range is consuming most of the bandwidth. These computers reside in your internal sales IP address range.
7. You begin to drill into each of the offending IP addresses, and each IP address you investigate shows Kazaa (port 1214) and World of Warcraft (port 3724) usage in the Top 5 applications.
8. Using a configuration management tool, such as Orion Network Configuration Manager, you push a new configuration to your firewall that blocks ports 1214 and 3724.
9. Within minutes, you see the traffic on your interface drop back to 25%.

Recognizing and Thwarting Denial of Service Attacks

Orion NTA enables you to easily characterize both outgoing and incoming traffic. This ability becomes ever more important as corporate networks are exposed to increasingly malicious denial of service attacks. Consider the following scenario:

1. An Orion NPM advanced alert tells you that your web-facing router is having trouble creating and maintaining a stable connection to the internet.
2. You open the Orion Web Console to search for possible issues. All connections are currently up, and bandwidth utilization looks good. But then you notice your CPU utilization on the firewall node. It is holding steady between 99% and 100%.

3. Clicking the firewall node name opens its Node Details page where the Current Percent Utilization of Each Interface resource shows that your firewall interfaces are receiving abnormally high levels of traffic.
4. You click **NetFlow** in the Modules toolbar to take a quick look at your customized Top 50 Endpoints resource.
5. The Top 50 Endpoints resource shows that the top six computers attempting to access your network are from overseas.
6. You realize that your ports are being scanned and that your firewall is interactively blocking these attacks.
7. Using a configuration management tool, such as Orion Network Configuration Manager, you push a new configuration to your firewall that blocks all traffic over the IP address range of the computers trying to access your network.
8. In minutes, CPU utilization on your web-facing router returns to normal.

Investigating Orion NTA Further

While this concludes the guided tour of Orion NetFlow Traffic Analyzer, this *Evaluation Guide* has in no way fully covered the wealth of Flow-enabled network monitoring features available with Orion NTA. Please explore the *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*, available on the SolarWinds website, at http://www.solarwinds.com/support/documentation.aspx, to learn even more about the power and convenience of Orion NetFlow Traffic Analyzer.