SolarWinds Orion

NetFlow Traffic Analyzer Evaluation Guide

ORION NETFLOW TRAFFIC ANALYZER

Orion NetFlow Traffic Analyzer Evaluation Guide, Version 3.1, 02.03.2009

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	www.thwack.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

SolarWinds Orion NetFlow Traffic Analyzer Documentation Library

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

Document	Purpose
Administrator Guide	Provides detailed setup, configuration, and conceptual information.
Page Help	Provides help for every window in the Orion NetFlow Traffic Analyzer user interface.
Evaluation Guide	Provides an introduction to Orion Network Performance Monitor features and instructions for installation and initial configuration.
Quick Start Guide	Provides installation, setup, and common scenarios for which Orion NetFlow Traffic Analyzer provides a simple, yet powerful, solution.
Release Notes	Provides late-breaking information, known issues, and updates. The latest Release Notes can be found at www.solarwinds.com.

Contents

About SolarWinds iii

Contacting SolarWinds iii

Conventions iii

SolarWinds Orion NetFlow Traffic Analyzer Documentation Library iv

Chapter 1

Introduction to Orion NetFlow Traffic Analyzer **1**

Why Install Orion NetFlow Traffic Analyzer 1

Why Use Orion NetFlow Traffic Analyzer 2

Features of Orion NetFlow Traffic Analyzer 3

How Orion NetFlow Traffic Analyzer Works 4

Chapter 2

Installing Orion NetFlow Traffic Analyzer **5**

Requirements 5

Hardware Requirements 5
Software Requirements 6
Virtual Machine Requirements 7

SQL Server and SQL Server Express with Orion NTA 7

Installing Orion NetFlow Traffic Analyzer 8

Enabling Flow Analysis in Orion NTA 11

Automatically Adding Flow-enabled Devices 11
Adding Devices and Interfaces to the Orion Database 11
Adding NetFlow Sources to NetFlow Traffic Analyzer 17

Chapter 3

Orion NetFlow Traffic Analyzer Quick Tour **19**

Starting Orion NetFlow Traffic Analyzer 19

The NetFlow Traffic Analysis Summary 19

NetFlow Sources 19
Top 10 NetFlow Sources by % Utilization 20
Traffic View Builder 21
Top 5 Applications 21

Top 5 Endpoints 22
Search for NetFlow Endpoints 22
Search for NetFlow Application 24
Top 5 Conversations 25
Last 25 Traffic Analysis Events 26

Orion NetFlow Traffic Analyzer Views 27

NetFlow Application View 27
NetFlow Conversation View 30
NetFlow Endpoint View 31
NetFlow Interface Details View 33
NetFlow Node Details View 34

Chapter 4

Using Orion NetFlow Traffic Analyzer 37

Using the Traffic View Builder 37

Viewing Traffic for a Designated IP Address 37
Viewing Traffic for Specific Ports or Applications 39

Locating and Isolating an Infected Computer 40

Locating and Blocking Unwanted Use 41

Recognizing and Thwarting Denial of Service Attacks 42

Investigating Orion NTA Further 42

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 that are managing any size NetFlow-, sFlow-, or J-Flow-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.

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:

Improved availability and performance

With Orion NetFlow Traffic Analyzer, you can more quickly detect, diagnose, and resolve network slowdowns and outages.

Analytical capacity planning

Orion NetFlow Traffic Analyzer highlights trends in network traffic, enabling you to intelligently anticipate changes in bandwidth to areas that are experiencing bottlenecks.

Optimized network resource allocation

Information provided by Orion NetFlow Traffic Analyzer enables you to identify areas of your network that are experiencing limited or overly stressed connections. You can then redirect existing traffic to other areas of your network that have available bandwidth.

Alignment of IT resources with enterprise business needs

Because Orion NetFlow Traffic Analyzer is built on the proven Orion Network Performance Monitor 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 NetFlow Traffic Analyzer gives you the ability to quickly and precisely examine network traffic and then pinpoint and expose curious patterns, unwanted behaviors, and anomalous usage that may indicate possible virus, bot, or spyware infection.

An all-in-one NetFlow and network performance monitoring application

Now you can stop switching between programs to get a complete picture of the usage, performance, and needs of your network. Everything you need to monitor your Flow-enabled network is found in Orion Network Performance Monitor and Orion NetFlow Traffic Analyzer.

Features of Orion NetFlow Traffic Analyzer

Orion NTA provides the following features to enhance your ability to monitor the Flow-enabled devices on your network.

Automatic Addition of NetFlow Sources

In the event that a Flow-enabled device in the Orion database is sending Flow data to the server hosting Orion NetFlow Traffic Analyzer, Orion NTA now automatically adds the Flow-enabled device as a NetFlow Source. All recognized NetFlow Sources are listed in the NetFlow Sources resource on the NetFlow traffic Analysis Summary view.

Thwack.com: Recent NetFlow Posts Resource

This resource shows the most recent Orion NTA-related posts that have been submitted to Thwack.com, the online SolarWinds user community. Clicking any post title listed in the resource opens the associated post in the NetFlow Traffic Analyzer Thwack.com forum.

Search by IP address range

This version of Orion NTA provides the ability to search for endpoints within a specified IP Address Range (i.e., `10.10.199.1-10.10.199.50`).

Additional flow support is now available

Orion NTA currently supports NetFlow v9, sFlow v5, and J-flow formats for collecting network traffic data.

Customized traffic views

With the Traffic View Builder included in Orion NTA, you can filter collected NetFlow data to create and access customized views. For example, you can build a view that displays traffic to a specific domain generated during standard office hours (8-5p) from a selected IP address.

Top 10 NetFlow Sources by Percent Utilization resource

A new resource on the NetFlow Summary View lists monitored NetFlow sources by percent utilization.

Quality of service (QoS) performance views

Orion NTA allows you to easily view your overall network traffic segmented by Class of Service methods such as Type of Service or DSCP. You can also quantify and visualize the amount of bandwidth consumed by each of your designated QoS levels, including voice and video data.

Full integration of NetFlow resources within Orion views

NetFlow resources can easily be added to Orion views automatically

Port application grouping

Orion NTA now gives you the ability to assign an application that uses several network ports to a group for gauging application performance.

Network-wide Top 5 resources

New network-wide Top 5 traffic resources are now available, listing IP address groups, applications, conversations, countries, endpoints, types of service, transmitters, receivers, and protocols.

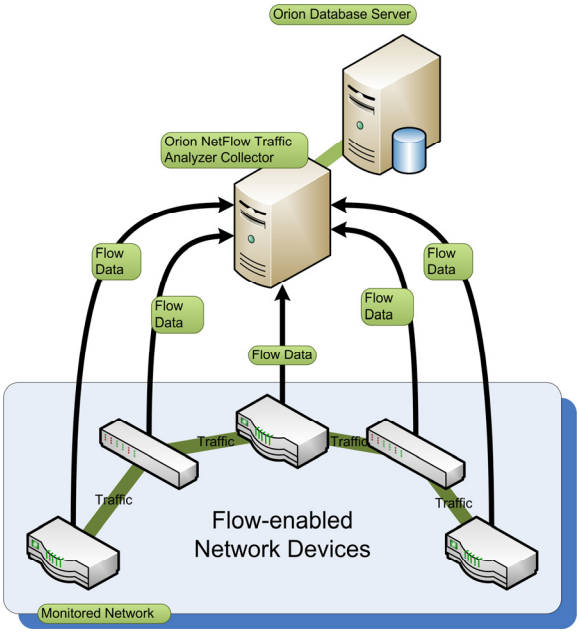
Immediate DNS Lookup feature

Perform manual DNS lookups without waiting for a scheduled DNS update.

How Orion NetFlow Traffic Analyzer Works

Flow-enabled devices provide a wealth of IP-related traffic information. Orion NTA collects this Flow 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 into your network, within your network, and from your network. These reports help you monitor bandwidth, track conversations between internal and external endpoints, analyze traffic, and plan bandwidth capacity needs.

The following diagram provides an overview of a simple Orion NetFlow Traffic Analyzer installation to show, generally, how Orion NTA works.



Chapter 2

Installing Orion NetFlow Traffic Analyzer

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.

Requirements

The server used to host your NetFlow solution must support both Orion NPM and Orion NTA. The following sections provide minimum configuration requirements.

Hardware Requirements

The following requirements assume that your Orion NTA evaluation is installed on a server running Orion NPM version 9.0 or later. To evaluate Orion NTA on an earlier version of Orion NPM, contact SolarWinds at sales@solarwinds.com.

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

Warning: Due to the high speed and large memory requirements of NetFlow data transactions, SolarWinds recommends that only RAID configurations 0, 1, 01, or 10 be used for Orion NTA installations Other RAID or SAN configurations may cause data loss and significantly decreased performance.

Hardware	Requirements
CPU	3GHz or faster
RAM	3GB or more
Hard Drive Space	**Orion NTA server:** 20GB or more, RAID 0, 1, 01, or 10. Other RAID or SAN configurations are not recommended. **SQL Server:** 20GB 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 utilized by NetFlow version 5.
J-Flow	Network devices using J-Flow
sFlow devices	sFlow devices using sFlow version 5

Software Requirements

The following software requirements assume that your Orion NTA evaluation is installed on a server running Orion NPM version 9.0 or later. If you want to evaluate Orion NTA on an earlier version of Orion NPM, contact SolarWinds at sales@solarwinds.com.

Notes:

- Except for lmited evaluations, Orion NTA and SQL Server installations are required to be on separate physical servers.
- SQL Express and MSDE restrict database size 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
Operating System	Windows Server 2003 (32-bit or 64-bit) including R2, with IIS installed, running in 32-bit mode. SolarWinds recommends that Orion NPM administrators have local administrator privileges to ensure full functionality of local Orion NPM tools. Users limited to the web console do not require administrator privileges. **Note:** SolarWinds does not support Orion NTA installations on Windows XP in production environments. If you are installing Orion NTA on Windows XP, you must confirm that Shared Memory, Named Pipes, and TCP/IP are enabled on remote databases.
Web Server	Microsoft IIS version 6.0 and later. 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 or later
SNMP Trap Services	Windows operating system management and monitoring tools component
SQL Server	SQL Server 2000 SP4, Standard or Enterprise SQL Server 2005 Standard or Enterprise Database must support mixed-mode or SQL authentication. **Note:** SQL Server Express is unable to manage databases larger than 4GB. It is limited to a single processor, and it will use no more than 1GB RAM. Though it may be used to monitor one or two interfaces, for a very limited time, for evaluation purposes, SolarWinds recommends against its use for larger networks requiring larger databases. If you are evaluating Orion NTA on an installation of Orion NPM that is either installed on the same server as your SQL Server or using a SQL Express database, you must limit your monitored flows to no more than two interfaces.
Web Console Browser	Microsoft Internet Explorer version 6 or later with Active scripting Mozilla Firefox 3.0 or later

Virtual Machine Requirements

Orion NTA installations on VMware Virtual Machines and Microsoft Virtual Servers are fully supported if the following minimum configuration requirements are met for each virtual machine.

Virtual Machine Configuration	Requirements
CPU Speed	3.0 GHz
Allocated Hard Drive Space	20 GB **Note:** RAID 1+0 is recommended; due to intense I/O requirements RAID 5 is not recommended.
Memory	2 GB
Network Interface	Each installation of Orion NPM should have its own, dedicated network interface card. **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 Network Performance Monitor requirements, see “Requirements” in the *SolarWinds Orion Network Performance Monitor Administrator Guide*.

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.

Installing Orion NetFlow Traffic Analyzer

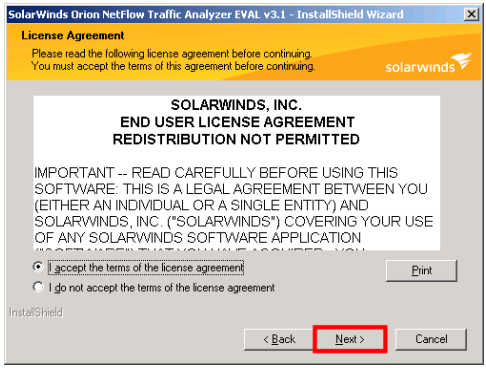
Complete the following procedure to install Orion NetFlow Traffic Analyzer. You must provide your NetFlow traffic port and confirm that it is enabled and sending NetFlow traffic data in order to complete your installation.

Note: The following procedure assumes that you have already installed Orion Network Performance Monitor version 9.0 or later on the server on which you want to install Orion NetFlow Traffic Analyzer. If you would like to evaluate Orion Network Performance Monitor, contact SolarWinds at sales@solarwinds.com.

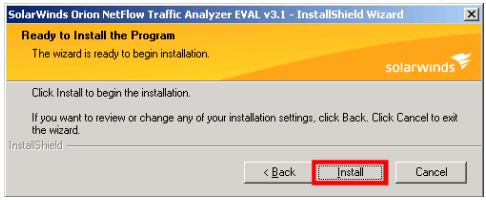
To install Orion NetFlow Traffic Analyzer:

1. Log on to the Orion Network Performance Monitor server that you want to use for NetFlow traffic analysis.
2. ***If you are installing Orion NetFlow Traffic Analyzer on a terminal server,*** perform the following steps before continuing with your installation to ensure that Orion NetFlow Traffic Analyzer is properly installed:
   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,*** complete the following steps:
   a. Navigate to the location of your downloaded `.zip` file.
   b. Extract the evaluation package to an appropriate location.
   c. Launch the SolarWinds Orion NetFlow Traffic Analyzer evaluation executable.
4. ***If you received physical media,*** complete the following steps:
   a. Navigate to the location of your downloaded `.zip` file.
   b. Extract the evaluation package to an appropriate location.
   c. Launch the SolarWinds Orion NetFlow Traffic Analyzer evaluation executable.
5. Review the Welcome text.
6. Click **Next**.

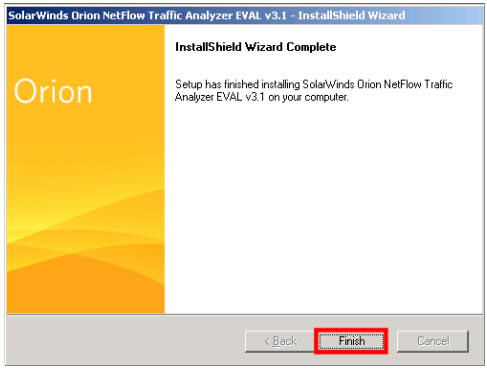
7. Select **I accept the terms of the license agreement**, and then click **Next**.



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



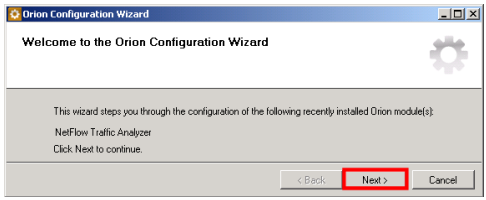
9. When the InstallShield Wizard completes, click **Finish** to exit the wizard.



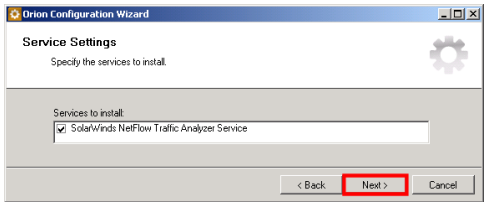
10. ***If you are prompted to reboot your server,*** select from the following options, as appropriate:

    - ***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**.

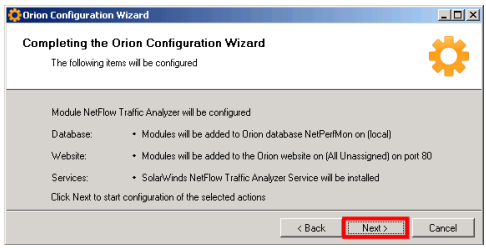
11. ***If the Configuration Wizard does not start automatically,*** click **Start > All Programs > SolarWinds Orion > Configuration Wizard**.
12. Review the Welcome text, and then click **Next**.



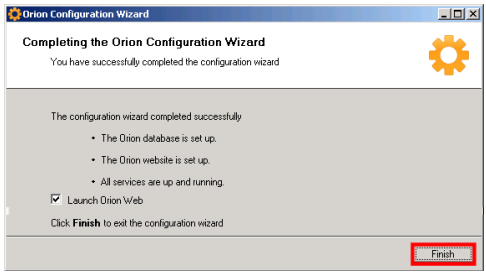
13. Confirm that **SolarWinds NetFlow Traffic Analyzer Service** is checked in the Service Settings window, and then click **Next**.



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



15. After the Configuration Wizard completes, click **Finish**.

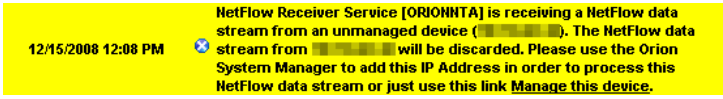


Enabling Flow Analysis in Orion NTA

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.

Automatically Adding Flow-enabled Devices

Orion NTA can automatically add Flow-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 Analysis Events resource.



Click **Manage this device** to add your Flow-enabled device to your Orion database. For more information about managing new network devices, see “Adding Devices and Interfaces to the Orion Database” on page 11. For more information about configuring Flow-enabled devices, see “Device Configuration Examples” in the *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

Adding Devices and Interfaces to the Orion Database

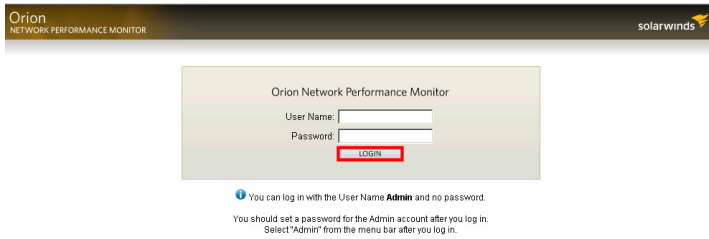
The following procedure adds a device and its interfaces to the Orion database using the Web Node Management feature of the Orion Web Console. If your NetFlow device is already configured to send NetFlow data, Orion NTA will begin to receive NetFlow data as soon as your device is added to the Orion database.

Note: For more information about designating NetFlow sources in Orion NTA, see “Adding NetFlow Sources to NetFlow Traffic Analyzer” on page 17.

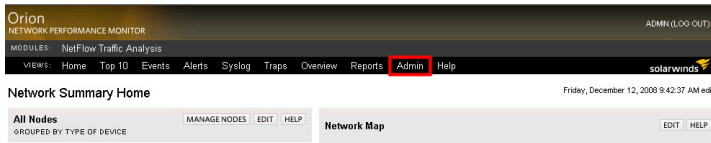
To add Flow-enabled devices and interfaces to the Orion database:

1. Log on to the Orion NPM server that hosts your Orion NTA installation.
2. Click **Start > SolarWinds Orion > Orion Web Console**.
3. Log in to the Orion Web Console as an administrator.

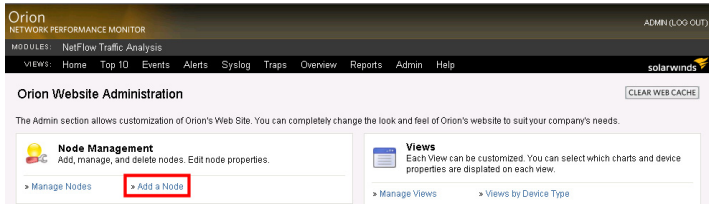
   Note: If you have not already configured another Admin password, you can log in with the **User ID** `Admin` and no password.



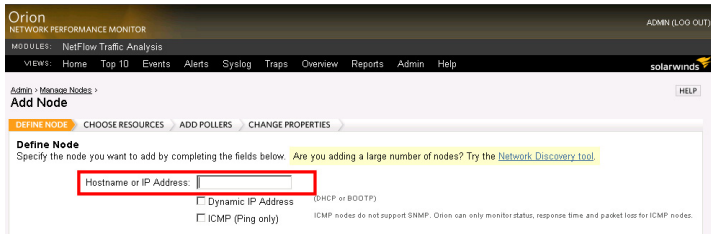
4. Click **Admin** in the Views toolbar.



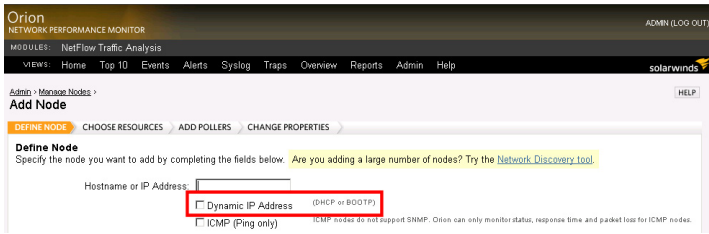
5. Click **Add a Node** in the Node Management grouping.



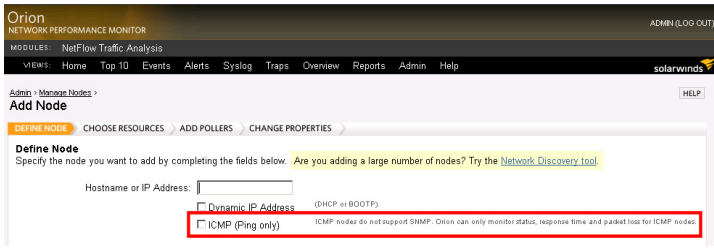
6. Provide the hostname or IP Address of the Flow-enabled device you want to add in the **Hostname or IP Address** field.



7. ***If the IP address of the device you are adding is dynamically allocated (DHCP or BOOTP),*** check **Dynamic IP Address**.

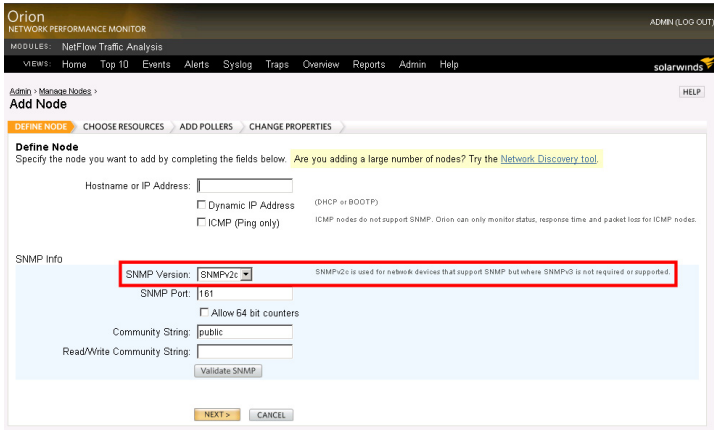


8. Confirm that **ICMP (Ping only)** is not checked.



9. Select the **SNMP Version** for the added node.

   Note: Orion NPM uses **SNMPv2c** by default. If your new device supports or requires the enhanced security features of SNMPv3, select **SNMPv3**.



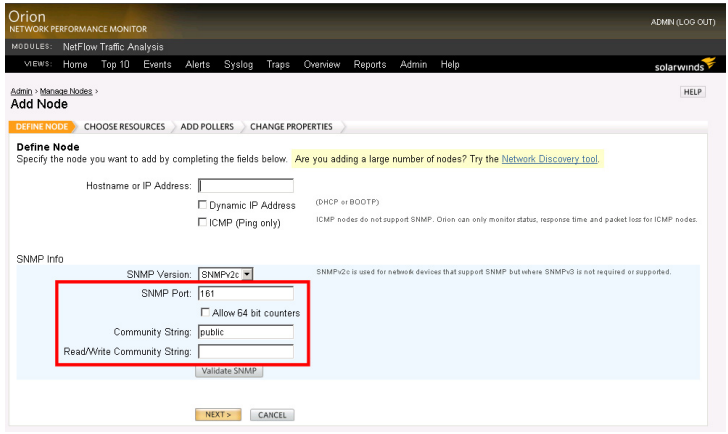
10. ***If you selected* SNMPv2c,** complete the following steps:

    a. ***If the SNMP port on the added node is not the Orion NPM default of 161,*** provide the actual port number in the **SNMP Port** field.

    b. ***If the added node supports 64 bit counters and you want to use them,*** check **Allow 64 bit counters**.

    c. Provide valid community strings for the added node.

    Note: The **Read/Write Community String** is optional, but Orion NPM does require the `public` **Community String**, at minimum.



11. ***If you selected* SNMPv3,** complete the following steps:

    a. ***If the SNMP port on the added node is not the Orion NPM default of 161,*** provide the actual port number in the **SNMP Port** field.

    b. ***If the added node supports 64 bit counters and you want to use them,*** check **Allow 64 bit counters**.

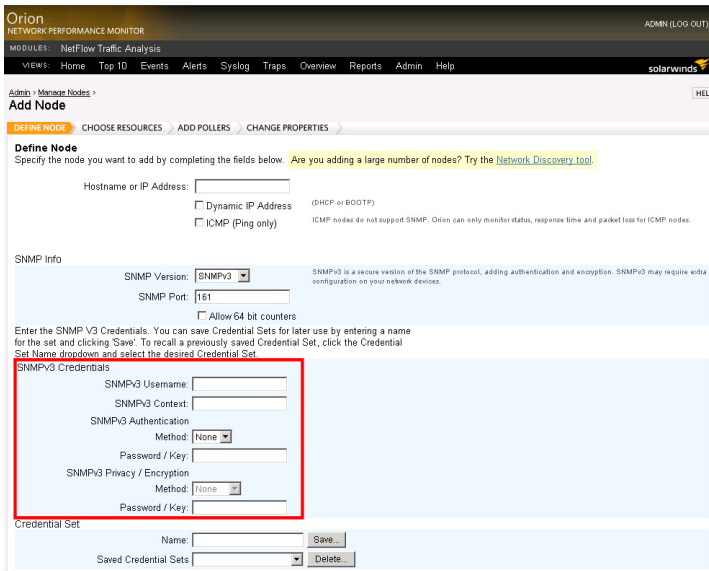
    Note: Orion NPM fully supports the use of 64-bit counters; however, these high capacity counters can exhibit erratic behavior depending on manufacturer implementation. If you notice peculiar results when using these counters, use the Node Details view to disable the use of 64-bit counters for the device and contact the hardware manufacturer.

    c. Provide the following **SNMP Credentials**, **Authentication**, and **Privacy/Encryption** settings:

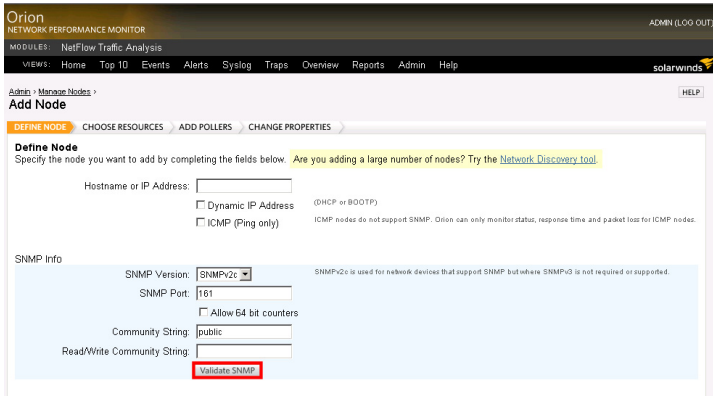
    - **SNMPv3 Username** and **SNMPv3 Context**
    - **SNMPv3 Authentication Method**

- **SNMPv3 Authentication Password/Key**
- **SNMPv3 Privacy/Encryption Method**
- **SNMPv3 Privacy/Encryption Password/Key**

Note: For the purposes of this evaluation, **Read/Write SNMPv3 Credentials** are not required, and it is assumed that you do not already have a saved credential set.



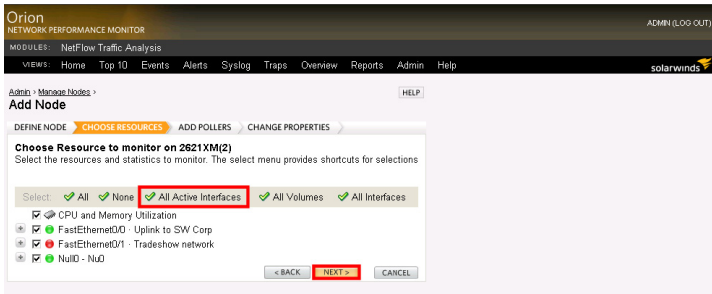
12. Click **Validate SNMP** after entering all required SNMP credentials.



13. After confirming that your SNMP credentials are valid, click **Next**.

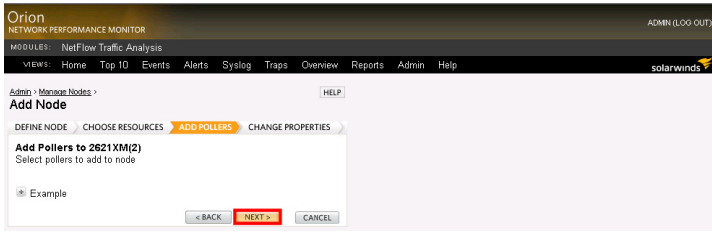
14. Check the interfaces you want Orion NTA to monitor, and then click **Next**.

Note: If you do not know which interfaces are Flow-enabled, click **All Interfaces** to select all interfaces.



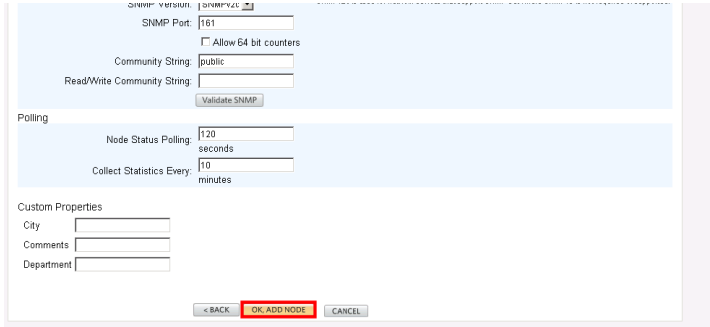
15. For the purposes of this evaluation, click **Next** on the Add Pollers view.

Note: For more information about using or defining pollers, see the *SolarWinds Orion Network Performance Monitor Administrator Guide*.

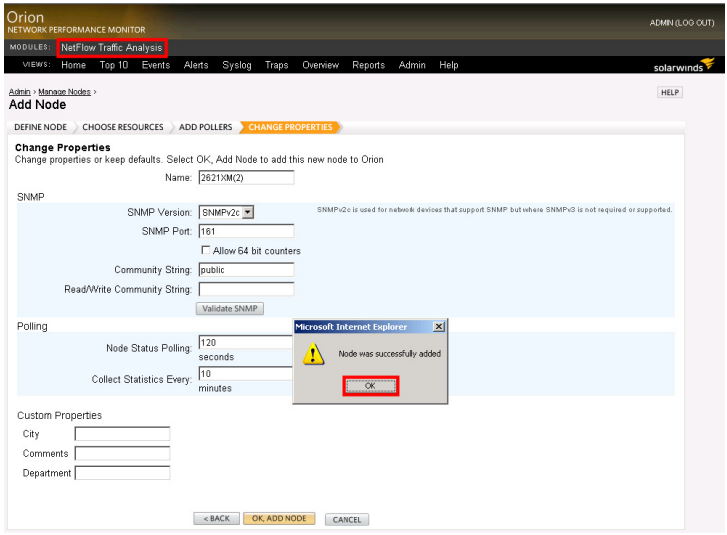


16. Click **OK, Add Node** on the Change Properties view.

Note: On this view, you may choose to provide values for the following default custom properties: **City**, **Comments**, and **Department**. For more information about using custom properties, see “Creating Custom Properties” in the *SolarWinds Orion Network Performance Monitor Administrator Guide*.



17. Click **OK** on the dialog, and then click **NetFlow Traffic Analysis** in the Modules toolbar.



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

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.

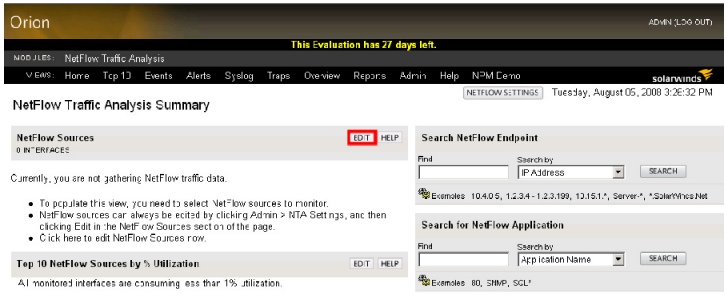
Note: Orion NTA only recognizes NetFlow version 9 templates that include all fields utilized by NetFlow version 5.

To add NetFlow devices and interfaces to NetFlow Traffic Analyzer:

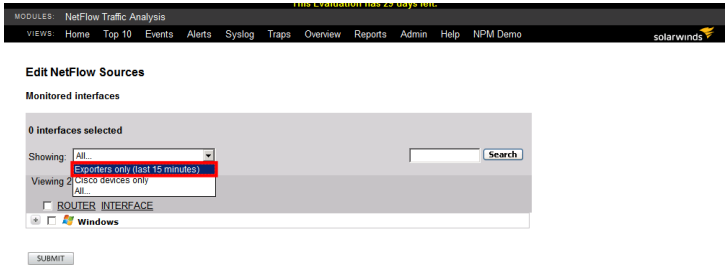
1. Log on to the Orion NPM server that hosts Orion NetFlow Traffic Analyzer.
2. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
3. Log in to the Orion Web Console as an administrator.

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

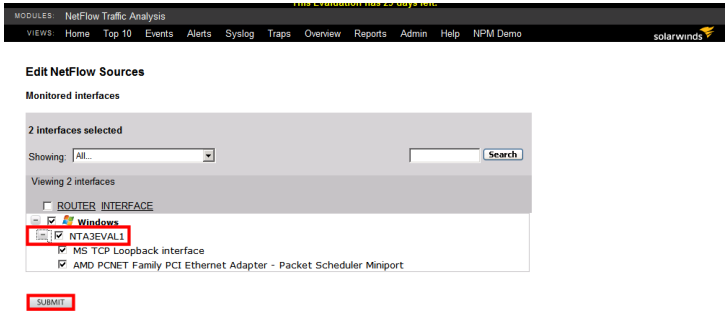
4. Click **Edit** in the header of the NetFlow Sources resource.



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



6. Expand the device list to see all monitored nodes, check the parent nodes of the interfaces you want Orion NTA to monitor, and then click **Submit**.



As a result, Orion NTA should receive meaningful traffic data and display it in the Orion Web Console 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 Analysis 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 Orion NetFlow Traffic Analyzer” on page 37.

Starting Orion NetFlow Traffic Analyzer

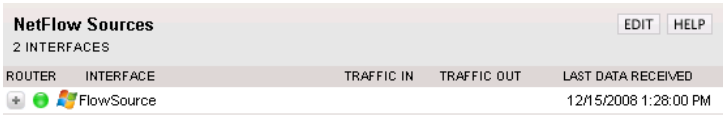
To start Orion NetFlow Traffic Analyzer, click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**. For more information about installing and configuring Orion NTA, see “Installing Orion NetFlow Traffic Analyzer” on page 5.

The NetFlow Traffic Analysis Summary

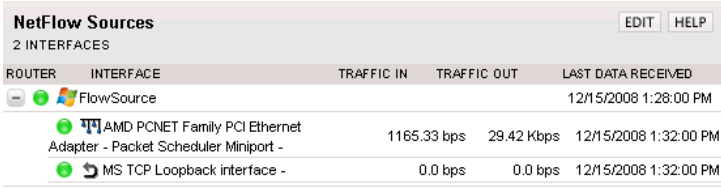
When you launch Orion NetFlow Traffic Analyzer, the NetFlow Traffic Analysis Summary is the first view displayed. This view provides insight into data traffic conditions over your entire network. The following resources are included in the NetFlow Traffic Analysis Summary View by default.

NetFlow Sources

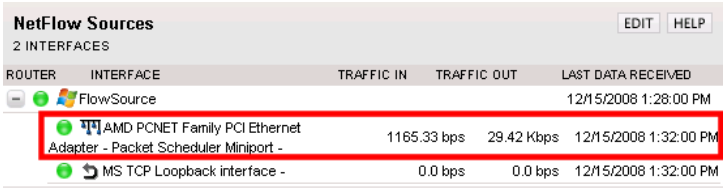
This resource provides a list of all Flow-enabled devices on your network that are currently configured to send NetFlow data to the server hosting your Orion NTA installation. For more information about adding Flow-enabled devices, see “Enabling Flow Analysis” on page 11.



Click **+** next to any router name to display Flow-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 for both incoming and outgoing traffic on each interface.

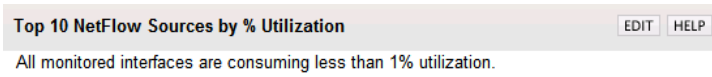


Clicking a router name opens the NetFlow Node Details view, and clicking an interface name opens the NetFlow Interface Details view. For more information about the NetFlow Node Details view, see “NetFlow Node Details View” on page 34. For more information about the NetFlow Interface Details view, see “NetFlow Interface Details View” on page 33.

Top 10 NetFlow Sources by % Utilization

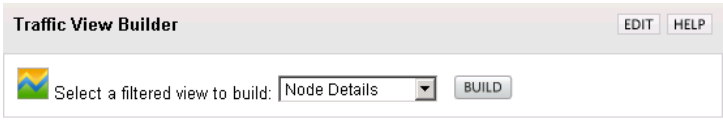
This resource provides a list of the NetFlow sources on your network that are currently routing enough traffic to significantly tax their system resources.

Note: Sources are only listed if they experience utilization in excess of 1%.



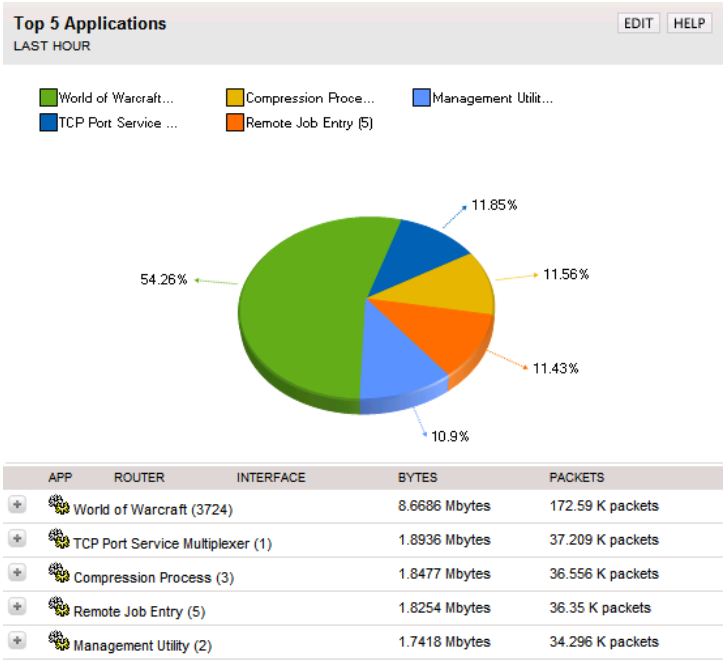
Traffic View Builder

The Traffic View Builder application allows you to create your own custom Orion NTA views. Because Orion NTA is a web-based module, you can then 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 the Traffic View Builder, see “Using the Traffic View Builder” on page 37.



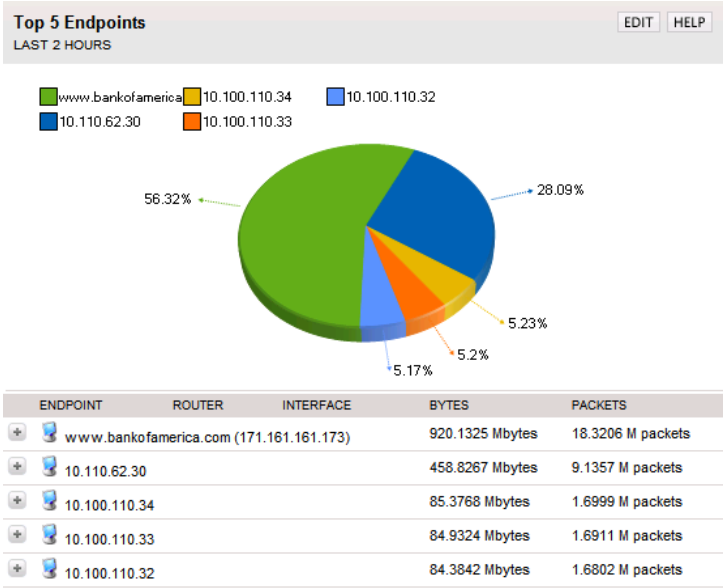
Top 5 Applications

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.



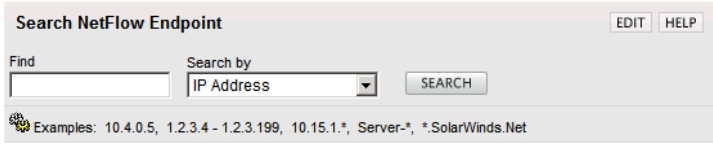
Top 5 Endpoints

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 for NetFlow Endpoints

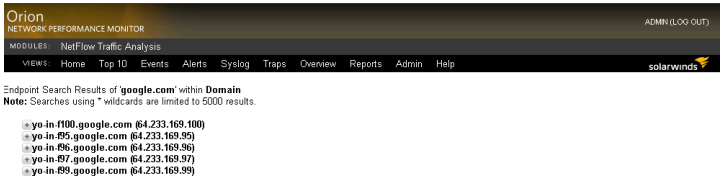
Using this resource, you can quickly locate any endpoint communicating with any devices on your network.



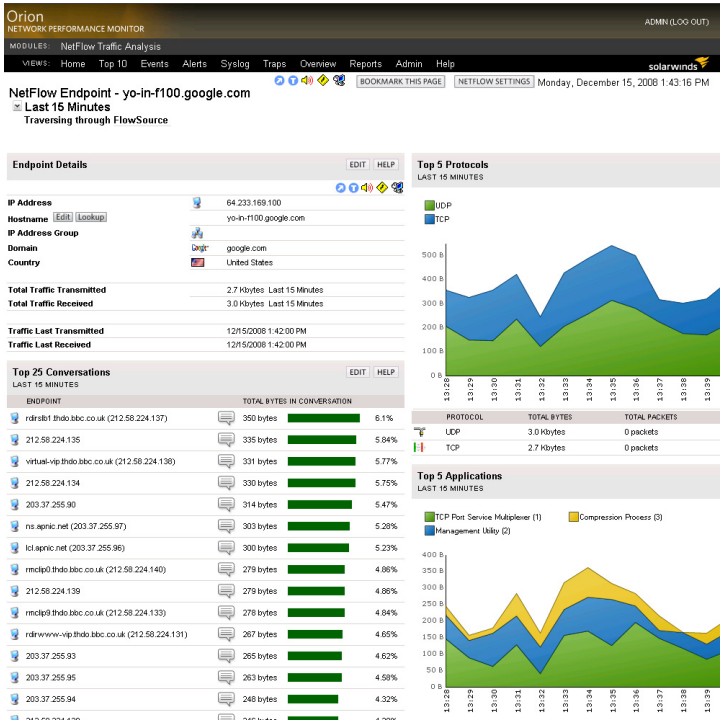
Simply search for endpoints by using any of the criteria in the following table:

Search NetFlow Endpoint Criteria		
Country	Domain	Hostname
IP Address	IP Address Group Name	

Provide an appropriate search term, and then click **Search**. Your search results provide an expandable list of the devices on your network that are routing traffic either to or from endpoints matching your search criteria.

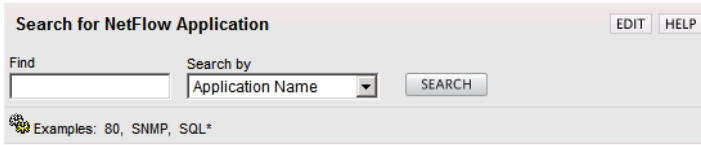


Clicking any result, followed by clicking the name of any of your network devices opens the NetFlow Endpoint View for all endpoint traffic through the selected device. For more information about the NetFlow Endpoint View, see “NetFlow Endpoint View” on page 31.

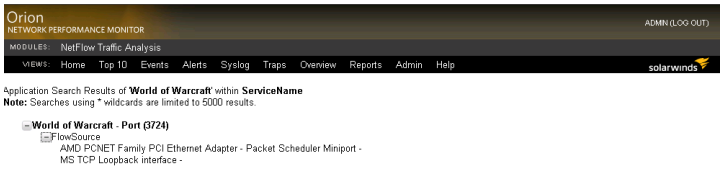


Search for NetFlow Application

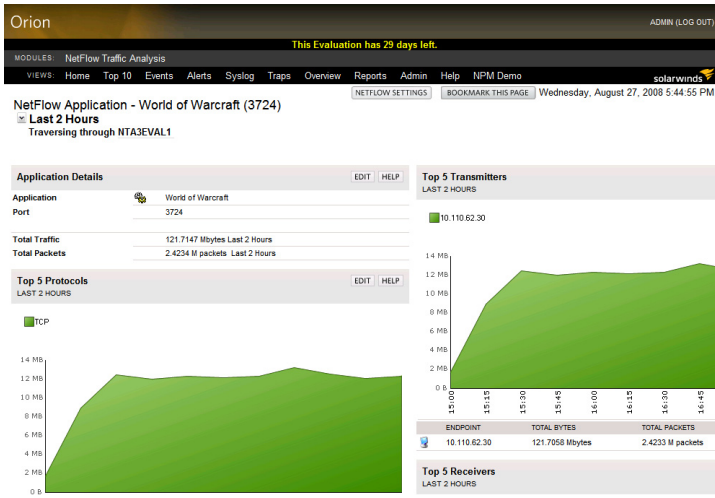
With the Search for NetFlow Application resource, you can quickly see which devices on your network are using a specific application or port at any time. Simply choose to search by Application Name or Port, provide an appropriate application name or port number, and then click **Search**.



Your search results provide an expandable list of the devices on your network that are routing traffic either for the selected application or over the selected port.

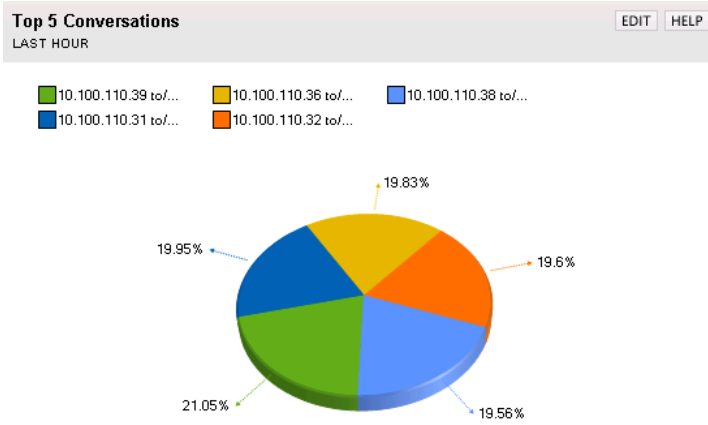


Clicking the name of a device on your network opens the NetFlow Application View for all traffic through the selected device that is either intended for the searched application or routed through the searched port. For more information about the NetFlow Application View, see “NetFlow Application View” on page 27.



Top 5 Conversations

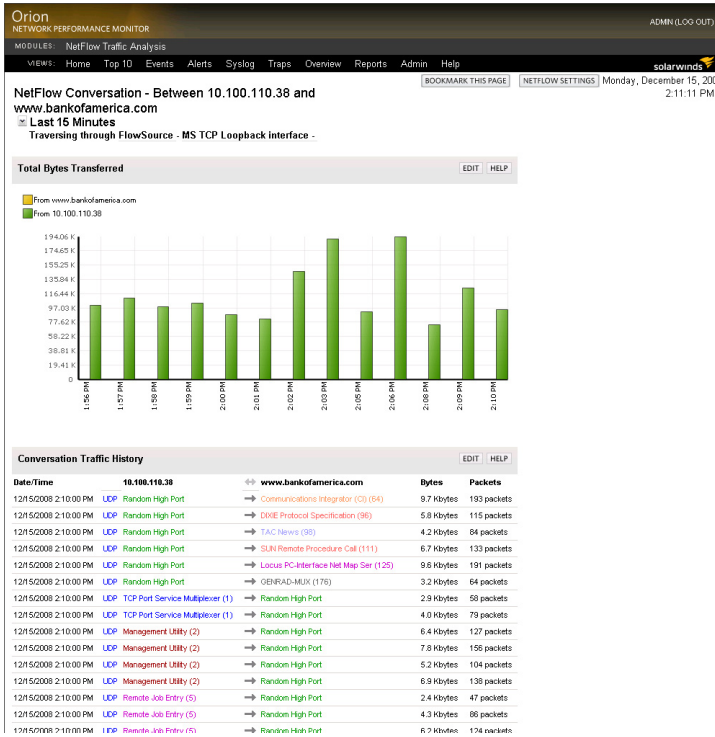
This resource provides view of the conversations using the most bandwidth on your network. Each color in the chart corresponds to a single continuing conversation between two specific endpoints. The table below the chart lists the endpoints involved in each conversation, with the bandwidth consumed by 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 ROUTER INTERFACE	BYTES	PACKETS
Between 10.100.110.39 and www.bankofamerica.com	3.3 Mbytes	66.153 K packets
Between 10.100.110.31 and www.bankofamerica.com	3.1 Mbytes	62.692 K packets
Between 10.100.110.36 and www.bankofamerica.com	3.1 Mbytes	62.29 K packets
Between 10.100.110.32 and www.bankofamerica.com	3.1 Mbytes	61.58 K packets
Between 10.100.110.38 and www.bankofamerica.com	3.1 Mbytes	61.445 K packets
FlowSource	3.1 Mbytes	61.445 K packets
FlowSource - MS TCP Loopback interface	1.5 Mbytes	29.032 K packets
FlowSource - AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport	1.6 Mbytes	32.413 K packets

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.

Clicking the name of any network device opens the NetFlow Conversation View for all traffic between the two endpoints conversing through the selected network device. For more information, see “NetFlow Conversation View” on page 30.



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 most used Orion NTA views. They are linked directly from default resources on the NetFlow Traffic Analysis Summary view. Additional resources link to additional views. For more information, 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 from the Admin view of the Orion NPM Web Console. 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 default 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 following information about the application and port that you are currently viewing:

- Application name
- Port used by the application
- Total amount of traffic data within the selected period of time
- 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 following information for each service type:

- The type of service
- The amount of traffic handled by the service
- The number of packets handled by the service
- 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. A wide array of custom charts is available to print or export for recordkeeping. Clicking the chart opens the Customize Chart page for the selected chart. For more information about customizing charts, see “Customizing Charts in NetFlow Traffic Analyzer” in the *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

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. A wide array of custom charts is available to print or export for recordkeeping. Clicking the chart opens the Customize Chart page for the selected chart. For more information about customizing charts, see “Customizing Charts in NetFlow Traffic Analyzer” in the *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

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. A wide array of custom charts is available to print or export for recordkeeping. Clicking the chart opens the Customize Chart page for the selected chart. For more information about customizing charts, see “Customizing Charts in NetFlow Traffic Analyzer” in the *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

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 following information for each endpoint:

- The name or IP address of the endpoint
- The amount of traffic that is transmitted by the endpoint
- 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 31.

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 following information for each endpoint:

- The name or IP address of the endpoint
- The amount of traffic that is received by the endpoint
- 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 31.

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 following information for each country:

- The name of the country
- The amount of traffic that is sourced in the country
- 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 following information for each country:

- The name of the country
- The amount of application traffic that is routed to endpoints in the country
- 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 Conversation View” on page 30.

NetFlow Conversation View

The following sections offer brief descriptions of the resources on the default 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 following information for each listed conversation exchange:

- 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
- the equivalent number of packets communicated

NetFlow Endpoint View

The following sections offer brief descriptions of the resources on the default 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 and received
- Date-time stamps of last transmitted and last received data

Top 5 Conversations

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 Conversation View” on page 30.

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 27.

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 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 following information for each service type:

- The type of service
- The amount of traffic, in bytes and packets, that is handled by the service
- 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 Services" 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.

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 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 31.

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 27.

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.

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 following information for each service type:

- The type of service
- The amount of traffic, in bytes and packets, that is handled by the service over the viewed interface
- 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 "Configuring NetFlow Types of Services" in the *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

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 Conversation View" on page 30.

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.

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 27.

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 Conversation View” on page 30.

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” on page 31.

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.

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 33.

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.

Using the Traffic View Builder

Using the Traffic View Builder resource, you can quickly generate your own custom views for any Flow-enabled device. Traffic View Builder allows you to create your own versions of any of the views in the following table.

Traffic View Builder View Types		
Application	Country	Domain
Endpoint	Interface	IP Address Group
Protocol	Router	Type of Service

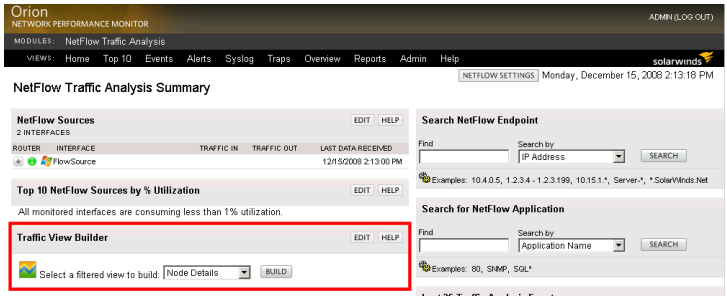
The following sections present scenarios showing how the Orion NTA Traffic View Builder resource enables you to create your own views.

Viewing Traffic for a Designated IP Address

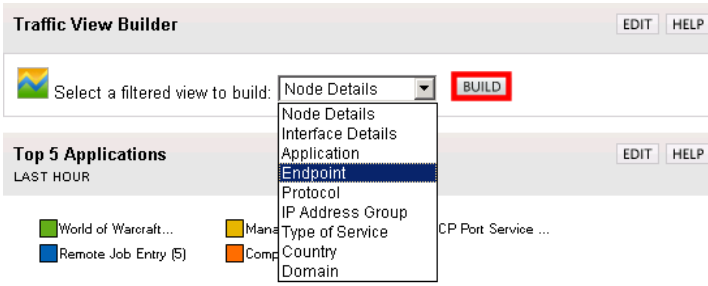
The following procedure creates a custom Orion NTA view showing both incoming and outgoing network traffic from a designated IP address.

To create a view for a specific IP address:

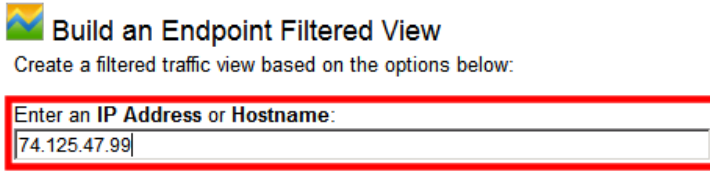
1. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console** to use the Traffic View Builder resource.



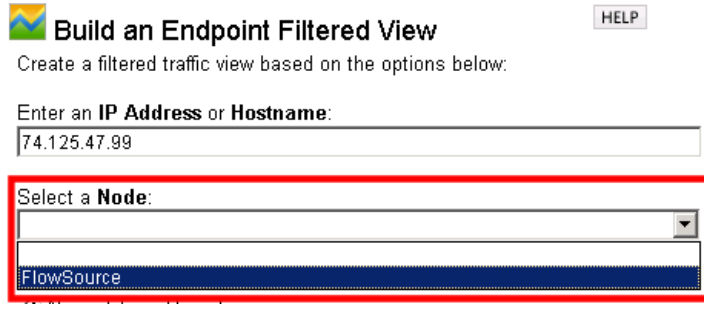
2. Select **Endpoint**, and then click **Build**.



3. Enter the **IP address** you want to monitor.



4. Select the **Node** that is sending traffic to your selected IP address.



5. Select **All Interfaces** when the Select an Interface menu displays.

   Note: You can further customize your view to show only traffic over a specific interface on the router, but, for the purposes of this evaluation, select **All Interfaces** to view all traffic through the selected router.

6. Click **Submit**, and then your custom NetFlow Endpoint view displays.

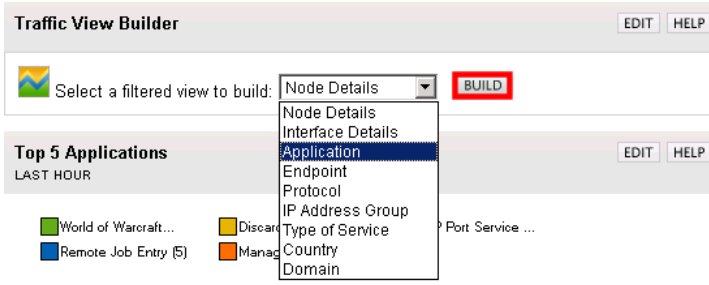
   Note: For more information about the NetFlow Endpoint view and its default resources, see “NetFlow Endpoint View” on page 31.

Viewing Traffic for Specific Ports or Applications

The following procedure creates a custom Orion NTA view showing network traffic through specified ports or to designated applications.

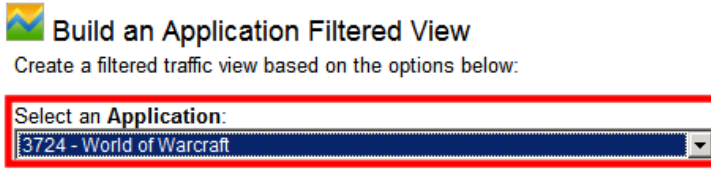
To create a view for specific ports or applications:

1. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**, and then locate the Traffic View Builder resource.
2. Select **Application**, and then click **Build**.

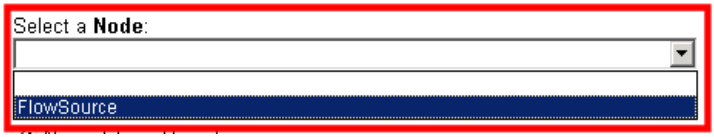


3. Select the **Application** or Port you want to monitor.

   Note: Applications are listed by associated port numbers. To determine application port number associations, use the Search for NetFlow Application resource on the NetFlow Traffic Analysis Summary view. For more information, see “Search for NetFlow Application” on page 24.



4. Select the Flow-enabled **Node** that is routing your application traffic.



5. Select **All Interfaces** when the Select an Interface menu displays.

   Note: You can further customize your view to show only application traffic over a specific interface on the router, but, for the purposes of this evaluation, select **All Interfaces** to view all traffic through the selected router.

6. Click **Submit**, and then your custom NetFlow Application view displays.

Note: For more information about the NetFlow Application view and its default resources, see “NetFlow Application View” on page 27.

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 Traffic Analysis** 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. Using a configuration management tool, such as Cirrus 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 Cirrus 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 Traffic Analysis** 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 Cirrus 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.