SolarWinds Orion

NetFlow Traffic Analyzer Administrator Guide

Copyright© 1995-2007 SolarWinds, all rights reserved worldwide. No part of this document may be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the written consent of SolarWinds All right, title and interest in and to the software and documentation are and shall remain the exclusive property of SolarWinds and its licensors. SolarWinds Orion™, SolarWinds Cirrus™, and SolarWinds Toolset™ are trademarks of SolarWinds and SolarWinds.net® and the SolarWinds logo are registered trademarks of SolarWinds All other trademarks contained in this document and in the Software are the property of their respective owners.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS OR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Microsoft®, Windows 2000 Server®, and Windows 2003 Server® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Graph Layout Toolkit and Graph Editor Toolkit © 1992 - 2001 Tom Sawyer Software, Oakland, California. All Rights Reserved.

Portions Copyright © ComponentOne, LLC 1991-2002. All Rights Reserved.

NetFlow Traffic Analyzer Administrator Guide 10.19.2007 Version 2.2.1

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	1.866.530.8100 www.solarwinds.com
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

Orion NetFlow Traffic Analyzer Documentation Library

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

Document	Purpose
Orion NetFlow Traffic Analyzer Administrator Guide	Provides detailed setup, configuration, and conceptual information.
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.
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

Orion NetFlow Traffic Analyzer provides a simple-to-use, scalable network monitoring solution for IT professionals that are managing any size Cisco NetFlow-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:

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

These monitoring capabilities, along with the customizable Orion Network Performance Monitor Web Console and alerting and reporting engines, make Orion NetFlow Traffic Analyzer the easiest choice you will make involving your NetFlow monitoring needs.

Why Use Orion NetFlow Traffic Analyzer

The following valuable features provided the impetus for the development of Orion NetFlow Traffic Analyzer, and they are the foundation upon which Orion NetFlow Traffic Analyzer is built:

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 and reassign areas with excess bandwidth capabilities to areas with limited or stressed connections.

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 pinpoint inbound network traffic 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.

How Orion NetFlow Traffic Analyzer Works

NetFlow-enabled Cisco devices provide a wealth of IP-related traffic information. Orion NetFlow Traffic Analyzer collects this NetFlow 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 in and to your network. These reports help you monitor bandwidth, track conversations between internal and external endpoints, analyze traffic, and plan bandwidth capacity needs.

Chapter 2

Installing Orion NetFlow Traffic Analyzer

Orion NetFlow Traffic Analyzer provides a simple, wizard-driven installation process for collecting data from any version 5 NetFlow-enabled devices monitored by Orion Network Performance Monitor. For an enterprise-class product, the requirements are rather nominal, even though NetFlow data is extensive and can consume a great deal of database space.

Licensing Orion NetFlow Traffic Analyzer

Licensing for NetFlow Traffic Analyzer follows the licensing levels of your underlying Orion Network Performance Monitor installation. For more information about Orion NPM licensing, see “Licensing Orion Network Performance Monitor” in the *Orion Network Performance Monitor Administrator Guide*.

The following types of NetFlow licenses are currently available.

- Orion NetFlow Traffic Analyzer for Orion SL100
- Orion NetFlow Traffic Analyzer for Orion SL250
- Orion NetFlow Traffic Analyzer for Orion SL500
- Orion NetFlow Traffic Analyzer for Orion SL2000
- Orion NetFlow Traffic Analyzer for Orion SLX

Notes:

- Because the size of your database increases with the addition of more NetFlow interfaces consider first collecting NetFlow data on one or two interfaces for a period of time to understand the memory requirements of your Orion NetFlow Traffic Analyzer. Then, add more interfaces to ensure that your database scales as needed and that your memory needs are understood.
- Though licensing limits the maximum number of interfaces you can monitor with Orion NetFlow Traffic Analyzer, the effective capacity of your installation may be lower if monitored interface throughput is especially high.

Requirements

The server you use to host your NetFlow solution must support both Orion Network Performance Monitor and Orion NetFlow Traffic Analyzer. Orion NetFlow Traffic Analyzer is built on and extends the proven technologies and stable foundation of Orion Network Performance Monitor.

The following requirements are based on a minimum installation of Orion NetFlow Traffic Analyzer with SQL Server on a separate database server. Ensure that your SQL Server has enough memory and available hard drive space to absorb the influx of extensive NetFlow data.

Hardware or Software	Separate SQL Server and Orion: suggestions are for the Orion server unless otherwise stated
CPU	3GHz or faster
RAM	2GB or more
Hard Drive Space	5GB or more. Recommend RAID 0, 1, 0+1, or 1+0 configurations. Other RAID or SAN configurations are not recommended.
Operating System	Windows 2003 Server with IIS installed
.NET Framework	Version 3.0 or later with Orion NPM 8.5
Orion NPM	Orion Network Performance Monitor version 8.5 or later
SQL Server	SQL Server Standard Edition 2000 or SQL Server 2005 on a separate database server with 4-8GB of memory and at least 20GB of available hard drive space. SQL Express and MSDE are not supported, due to their restrictions on database size to 4GB and 2GB, respectively.
Web browser	Internet Explorer version 6 or later for accessing the web console Mozilla Firefox 2.0
NetFlow devices	Cisco devices using NetFlow version 5

Notes:

- Orion NetFlow Traffic Analyzer and SQL Server installations should be maintained on separate servers to optimize database scalability.
- SQL Express and MSDE restrict database size to 4GB and 2GB, respectively. They are not supported for use with Orion NetFlow Traffic Analyzer.
- Windows 2000 Server is no longer supported for Orion NetFlow Traffic Analyzer installations.

Warning: The only RAID configurations that should be used on an Orion NetFlow Traffic Analyzer installation are 0, 1, 0+1, or 1+0. Due to the high speed and large memory requirements of NetFlow data transactions, other RAID or SAN configurations should not be used as they may result in data loss and significantly decrease performance.

For more information about Orion NPM requirements, see “Requirements” in the *Orion Network Performance Monitor Administrator Guide*.

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.

To install Orion NetFlow Traffic Analyzer:

1. Log on to the Orion NPM server that you want to use for NetFlow traffic analysis.

   Notes:

   - SolarWinds generally recommends that you backup your database before performing any upgrade.
   - NetFlow Traffic Analyzer versions 2.2 and higher require Orion NPM version 8.5.

2. ***If you are installing NetFlow Traffic Analyzer on a terminal server,*** perform the following steps before continuing with your installation to ensure that 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**, and then click **Next** in the Install Program From Floppy Disk or CD-ROM window.

3. ***If you downloaded the product from the SolarWinds website,*** navigate to your download location and launch the executable.

4. ***If you received physical media,*** browse to the executable file, and then launch the executable.

5. ***If this installation is an upgrade of a previous version of Orion NetFlow Traffic Analyzer,*** click **Yes** when you are asked to continue to **perform an upgrade of 'SolarWinds Orion NetFlow Traffic Analyzer'**.

6. Review the Welcome text, and then click **Next**.

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

8. Click **Install**.

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

10. ***If you are installing NetFlow Traffic Analyzer on a terminal server,*** click **No** if the wizard asks you to reboot your server. Otherwise, click **Yes** if the wizard prompts you to reboot your server.

11. ***If this is a new installation of Orion NetFlow Traffic Analyzer,*** provide your information on the Install Software License Key window and click **Continue**.

    Note: You need your SolarWinds customer ID and password to install the key. For more information about Software License Keys, see “Software License Key” on page 41.

12. Click **Continue** when the license is successfully installed.

13. ***If the Configuration Wizard does not start automatically,*** click **Start > SolarWinds Orion > Configuration Wizard**.

14. Confirm that all services that you want to install are checked in the Service Settings window, and then click **Next**.

15. Review the configuration summary.

16. ***If the configuration settings are correct,*** click **Finish**.

17. ***If you are asked to select a polling engine to manage,*** select the Orion server that you are using as your NetFlow collector, and then click **Connect to Polling Engine**.

18. Proceed to add your NetFlow devices and interfaces to Orion Network Performance Monitor. For more information about adding NetFlow devices, see “Adding NetFlow-enabled Devices and Interfaces” on page 9.

Chapter 3

Getting Started

To begin analyzing the available NetFlow data that is produced by devices within your network, you must either add a NetFlow-enabled interface or monitor a previously added interface that is capable of generating NetFlow data.

Adding NetFlow-enabled Devices and Interfaces

Your NetFlow device and the relevant interfaces on which you want to monitor NetFlow traffic must be managed by Orion NPM. Although it is possible to monitor a NetFlow-enabled device or interface in Orion NetFlow Traffic Analyzer without managing it in Orion NPM, your NetFlow-enabled device must be added to Orion NPM first. An arrangement of this kind does not affect licensing requirements for either Orion NPM or Orion NetFlow Traffic Analyzer.

Adding your NetFlow device and interfaces to Orion NPM and adding your NetFlow device and interfaces to Orion NetFlow Traffic Analyzer are separate procedures. NetFlow-enabled devices must be added to the Orion database using System Manager before they can be monitored in Orion NetFlow Traffic Analyzer. For more information about adding your NetFlow device and interfaces to Orion NetFlow Traffic Analyzer, see “Adding NetFlow Sources to NetFlow Traffic Analyzer” on page 11.

The following section walks you through the addition of a device and its interfaces to Orion NPM. If you have already set your NetFlow device to send data, as soon as your device is added, Orion NetFlow Traffic Analyzer will begin to analyze NetFlow traffic.

To add your devices and NetFlow-enabled interfaces to Orion NPM:

1. Log on to the Orion NPM server that hosts Orion NetFlow Traffic Analyzer.

   Note: NetFlow Traffic Analyzer version 2.2 requires Orion NPM version 8.5 or later, and Orion NPM version 8.5 requires NetFlow Traffic Analyzer 2.2.

2. Click **Start > SolarWinds Orion > System Manager**.
3. ***If you want to add a large number of nodes,*** use **Network Discovery**. For more information, see “Using Orion System Manager” in the *Orion Network Performance Monitor Administrator Guide*.
4. Select **Nodes > Add Node**.

5. ***If you know the IP address and community string of the device that you want to add,*** type the hostname or IP address of the node, and then type or select the SNMP community string.

   Note: In most cases, the read-only community string is sufficient.

6. ***If you want to add a node with a dynamic IP address,*** check **Dynamic IP Address (DHCP or BOOTP)**, and the IP address will be determined automatically.

7. ***If you only want to monitor network latency or response time and availability,*** change the node type to **ICMP Only**, and then click **Add Node** to finish adding the device to the database and start polling for ICMP Statistics.

8. ***If you want to monitor a device using SNMPv1 or SNMPv2c,*** complete the following procedure:

   a. In the **Node Type** grouping, select either **SNMPv1** or **SNMPv2c**.

   b. Type the community string or select it from the list, and then click **Next**.

   c. Check or select/deselect the interfaces, volumes, and statistics that you want to monitor, and then click **OK** to add your choices to the database and begin monitoring.

9. ***If you want to monitor a device using SNMPv3,*** perform the following steps:

   a. In the **Node Type** grouping, select **SNMPv3**.

   b. Click **Enter Credentials**, and then provide the appropriate information in the **Select/Edit SNMPv3 Credentials** window or load a credential set by selecting it from the list.

      Note: If the device uses SNMPv3 encryption, you must select a method of authentication before the encryption options are displayed.

   c. ***If you want to save the credentials that you have entered for later use,*** type a name, and then click **Save.**

   d. Click **OK**, and then click **Next** in the Add Node or Interface to Monitor window.

   e. Check or select/deselect the interfaces, volumes, and statistics that you want to monitor, and then click **OK** to add your choices to the database and begin monitoring.

After installing Orion NetFlow Traffic Analyzer, the polling engine establishes a baseline by collecting network status and statistics immediately. Then, 30 seconds later, the polling engine performs another collection. You may notice an increase in your CPU usage during this time. After these initial collections, Orion NetFlow Traffic Analyzer collects network information every 10 minutes for nodes, every 9 minutes for interfaces, and every 15 minutes for volumes. You

should have meaningful data in the NetFlow Traffic Analyzer tab of the web console within 2-3 hours. Before leaving Orion NetFlow Traffic Analyzer to gather data, ensure that you are collecting the correct data. For more information, see “Configuring Monitored Ports and Applications” on page 14.

Adding NetFlow Sources to NetFlow Traffic Analyzer

After your NetFlow-enabled device and its interfaces have been added to Orion NPM, you must designate it for monitoring by Orion NetFlow Traffic Analyzer. The following procedure provides the steps for adding NetFlow sources to Orion NetFlow Traffic Analyzer.

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 > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
3. Log in to the NetFlow Web Console using a **User ID** with administrative privileges.

   Note: Initially, `Admin` is the default administrator **User ID** with a blank **Password**.
4. Click **Admin** in the top menu bar.
5. Click **NTA Settings** in the left pane menu.
6. Click **Settings**.
7. Click **Edit** under the NetFlow Sources heading.

   Notes:

   - NetFlow Traffic Analyzer provides a NetFlow Sources resource in the NetFlow Traffic Analysis Summary view. Clicking Edit in the title bar of the NetFlow Sources resource allows you to access the Edit NetFlow Sources page directly from the NetFlow Traffic Analysis Summary view. If you have not enabled the NetFlow Traffic Analysis Summary view, including the NetFlow Source resource, as your default NetFlow Traffic Analysis Web Console view, see “Enabling the NetFlow Traffic Analysis Summary View” on page 12.
   - **Exporters only (last 15 minutes)** is the default filter. This option shows all devices in your Orion database that have sent NetFlow data within the last 15 minutes. If you expect other devices to export NetFlow data in the future, you should select another option, as described in the following steps.

8. ***If you want to select all available interfaces for monitoring,*** select **All…** from the Showing menu, check next to ROUTER and INTERFACE, and then click **Submit**.
9. ***If you want to select specific interfaces for monitoring,*** use the following procedure:
    a. Expand the interface tree through levels of device type and node name to see all available interfaces and select them by any of the following methods:
        - Check individual interfaces
        - Check nodes to select all interfaces on the selected node
        - Check device types to select all nodes and interfaces of the selected device type
    b. When you have selected all the interfaces that you want to monitor, click **Submit**.

Enabling the NetFlow Traffic Analysis Summary View

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

To enable the NetFlow Traffic Analysis Summary view:

1. Click **Admin** in the top menu bar.
2. Click **Account Manager** in the left pane menu.
3. Select **Admin**, and then click **Edit**.
4. Under the Default Menu Bar and Views heading, click **+** next to **Admin's NetFlow Traffic Analysis Settings**.
5. In the NetFlow Traffic Analysis View field select **NetFlow Traffic Analysis Summary**, and then click **Submit** at the bottom of the page.
6. Click the NetFlow Traffic Analyzer tab to see the NetFlow Traffic Analysis Summary page.

Configuring NetFlow Data Compression

Due to the great volume of data that is produced by NetFlow-enabled devices, your database may very quickly become unmanageable unless you choose to compress your NetFlow statistics. Eventually, database memory limitations dictate that older compressed data should be removed from the database. Orion NetFlow Traffic Analyzer compresses NetFlow data records on a configurable schedule. The following procedure presents the steps to enable data compression in Orion NetFlow Traffic Analyzer.

Note: Consider collecting data for a day before adjusting these settings. After a day, you should have a good idea of the volume of data your network produces with NetFlow enabled.

To configure your data compression schedule:

1. Log on to the Orion NPM server that you are using for NetFlow traffic analysis.
2. Click **Start > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
3. Log in to the NetFlow Web Console using a **User ID** with administrative privileges.

   Note: Initially, `Admin` is the default administrator **User ID** with a blank **Password**.
4. Click **Admin** in the top menu bar.
5. Click **NTA Settings** in the left pane menu.
6. Click **Settings**.
7. Click **Edit** under the Global Settings heading.
8. Type a number of minutes in the **Keep uncompressed data for** field.

   Note: The smallest uncompressed period that you can set is 16 minutes. This minimum ensures that at least 15 minutes of realtime data is collected and compressed before any of it is possibly deleted. NetFlow data that is older than this value is compressed and stored.
9. Type a number of days in the **Keep compressed data for** field.

   Note: NetFlow data may be stored in a compressed form for a longer period of time before it is finally deleted from your database. All data older than the value set here is deleted, but it may take up to a few days to fully remove compressed data, especially in large databases, after changing this setting.
10. Click **Submit**.

Configuring Monitored Ports and Applications

Orion NetFlow Traffic Analyzer allows you to directly specify the applications and ports that you want to monitor. Additionally, you can specify protocol types on a per-application basis, giving you the ability to monitor multiple applications on the same port if each application uses a different protocol. You should review this list of ports and applications and check the ports and applications that you want to monitor, adding any that you do not see but need to monitor, as in the following procedure.

To configure monitored applications and ports:

1. Log on to the Orion NPM server that you use for NetFlow traffic analysis.
2. Click **Start > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
3. Log in to the NetFlow Web Console using a **User ID** with administrative privileges.

   Note: Initially, `Admin` is the default administrator **User ID** with a blank **Password**.
4. Click **Admin** in the top menu bar.
5. Click **NTA Settings** in the left pane menu.
6. Click **Settings**.
7. Click **Edit** under Application and Service Ports.
8. Check the applications, protocols, and services that you want to monitor.

   Warning: Port -1 is designated by NetFlow Traffic Analyzer as the default port for all types of unmonitored traffic. This port should not be deleted, and it is recommended that the description not be edited.

   Note: Ensure that the port that is listed for the application that you want to monitor corresponds to the port that you are actually using for that application.
9. ***If you do not know the application port number, but you do know a keyword in the application description,*** type the keyword in the Search Ports field and click **Search Ports** to generate a list of related applications with their port numbers.
10. ***If you do not see a port or application that you want to monitor,*** click **Add New Port**, provide the port and description you need at the top of the displayed list, and then click **Update** to the right of the new port. For example, if you route all your VoIP traffic over 3 specific ports, use **Add New Port** to add these 3 ports.

11. ***If an application that you need to monitor has an incorrect port assignment,*** click **Delete** next to the incorrect port. After deleting the port assignment, use **Add New Port** to reassign the port to the appropriate application, as in the previous step.
12. Click **Submit** at the bottom of the page.

    Note: The number of monitored applications directly affects the amount of NetFlow data stored in the database. The more applications and ports that you monitor, the more data is stored. For more information about solving database size issues, see “Configuring NetFlow Data ” on page 13.

Selecting IP Address Groups for Monitoring

Orion NetFlow Traffic Analyzer allows you to establish IP address groups for selective monitoring of custom categories or segments of your network. The following steps set ranges and descriptions for your network IP addresses so that you can better characterize and assess the NetFlow data that you receive.

To configure IP address group monitoring:

1. Log on to the Orion NPM server that you use for NetFlow traffic analysis.
2. Click **Start > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
3. Log in to the NetFlow Web Console using a **User ID** with administrative privileges.

   Note: Initially, `Admin` is the default administrator **User ID** with a blank **Password**.
4. Click **Admin** in the top menu bar.
5. Click **NTA Settings** in the left pane menu.
6. Click **Settings**.
7. Click **Edit** under the IP Address Groups heading.
8. ***If any one of the pre-existing ranges contains the addresses that you want NetFlow Traffic Analyzer to monitor,*** check the range, and then click **Submit**.

9. ***If none of the pre-existing ranges contains the addresses that you want NetFlow Traffic Analyzer to monitor,*** complete either of the following series of steps to define your IP address group:
    - ***If you want to edit an existing group,*** check the group, click **Edit** to the right of the group description, type the starting and ending IP addresses of the range, edit the description, and then click **Update**.
    - ***If you want to add a new group,*** click **Add New Group,** type the starting and ending IP addresses of the range, type a description, and then click **Update**.
10. ***If you want to delete an existing group,*** check the group range, and then click **Delete** at the end of the IP address group row.
11. ***If you have completed the configuration of your IP address groups,*** click **Submit**.

Configuring Protocol Monitoring

The types of transport protocols that Orion NetFlow Traffic Analyzer monitors may be configured from the Edit Transport Protocols to Monitor page. This page allows you to specify precisely which protocols NetFlow Traffic Analyzer monitors. Selectively specifying monitored protocols can reduce the amount of NetFlow traffic that NetFlow Traffic Analyzer processes and improve overall performance. The following procedure enables selective transport protocol monitoring.

To specify protocols monitored by NetFlow Traffic Analyzer:

1. Log on to the Orion NPM server that you use for NetFlow traffic analysis.
2. Click **Start > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
3. Log in to the NetFlow Web Console using a **User ID** with administrative privileges.

    Note: Initially, `Admin` is the default administrator **User ID** with a blank **Password**.
4. Click **Admin** in the top menu bar.
5. Click **NTA Settings** in the left pane menu.
6. Click **Settings**.
7. Click **Edit** under Monitored Protocols.
8. Check the transport protocols you want to monitor and click **Submit**.

Configuring NetFlow Types of Services

Orion NetFlow Traffic Analyzer recognizes the Differentiated Services model of packet delivery prioritization. All NetFlow-enabled devices may be configured to set a Type of Service byte, referred to as the Differentiated Service Code Point (DSCP), on all NetFlow packets that are sent. The DSCP prioritizes NetFlow packet delivery over the NetFlow-enabled devices on your network by assigning each packet both a Differentiated Service class (1, 2, 3, or 4) and a packet-dropping precedence (low, medium, or high). NetFlow packets of the same class are grouped together. Differentiated Services uses the DSCP to communicate per-hop behaviors (PHBs), including Assured Forwarding (AF) and Expedited Forwarding (EF), to the node services that a given packet encounters. PHBs are configured on individual devices when NetFlow is initially enabled. If a given node is overloaded with NetFlow traffic, node services will keep or drop NetFlow packets in accordance with the configured PHB that matches the DSCP in each NetFlow packet. For more information about Differentiated Services, see RFC 2474, RFC 2475, and RFC 3140.

PHBs, corresponding to Types of Services on NetFlow-enabled devices, may be configured with DSCPs within Orion NetFlow Traffic Analyzer, as shown in the following procedure.

To configure types of services for NetFlow packets:

1. Log on to the Orion NPM server that you use for NetFlow traffic analysis.
2. Click **Start > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
3. Log in to the NetFlow Web Console using a **User ID** with administrative privileges.

   Note: Initially, `Admin` is the default administrator **User ID** with a blank **Password**.
4. Click **Admin** in the top menu bar.
5. Click **NTA Settings** in the left pane menu.
6. Click **Settings**.
7. Click **Edit** under the NetFlow Types of Service heading.
8. ***If you want to add a new type of service***, click **Add New Type of Service**, type the new Type of Service Name and DiffServ Code Point in the appropriate fields, and then click **Update**.

9. ***If you want to edit an existing type of service***, click **Edit** next to the Types of Service Name, edit the assigned name or its associated DiffServe Code Point, and then click **Update**.

   Note: Individual DiffServ Code Points can not share multiple Types of Service Names, and individual Types of Service Names can not share multiple DiffServ Code Points.

10. ***If you want to delete a DiffServ Code Point assignment***, click **Delete** next to the DiffServ Code Point that you want to delete.

11. ***If you have finished configuring Types of Service Names***, click **Submit**.

Configuring NetFlow Collector Services

NetFlow Collector Services provides status information about the NetFlow collector that is running Orion NetFlow Traffic Analyzer. In the event that your NetFlow device configuration requires it, the following steps reset the NetFlow collection port on which your NetFlow collector listens for NetFlow data. You can also delete a collector, if necessary.

To configure NetFlow collector services:

1. Log on to the Orion NPM server that you use for NetFlow traffic analysis.
2. Click **Start > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
3. Log in to the NetFlow Web Console using a **User ID** with administrative privileges.

   Note: Initially, `Admin` is the default administrator **User ID** with a blank **Password**.

4. Click **NTA Settings** in the left pane menu.
5. Click **Settings**.
6. Click **Edit** under the NetFlow Collector Services heading.
7. ***If you want to reset a collection port,*** type the new port number in the **Collection Port** field of the collector that you want to edit.

   Note: The **Status Icon** displays your collector status visually. A green icon indicates that the collector can receive NetFlow data, and a red icon indicates that the collector can not receive NetFlow data. **Server Name** provides the network identification of your NetFlow collector, and **Receiver Status** is a verbal statement of collector status.

8. ***If you want to delete a collector,*** click **Delete**.

   Note: If you delete all collectors, you must either run the Configuration Wizard again to restore your initial settings or provide another collector from a different Orion poller.

9. Click **Submit** when you finish configuring your NetFlow collectors.

Chapter 4

Creating NetFlow Traffic Analyzer Reports

Over time, your Orion NetFlow Traffic Analyzer accumulates a great deal of NetFlow information that can be presented in a variety of formats using the Report Writer feature of Orion Network Performance Monitor. SolarWinds has developed Report Writer to provide a quick and easy way for you to extract data from your database, including NetFlow statistics, for presentation in a form that is useful to you.

Several standard NetFlow-specific reports that you can modify are included in the Report Writer distribution, and you can create new reports as necessary. For more information about NetFlow-specific reports, see “NetFlow-specific Predefined Reports” on page 21. In addition, because it is a module of the Orion Network Performance Monitor, NetFlow Traffic Analyzer can also generate any of a number of predefined reports packaged with Orion. For more information about these predefined Orion reports, see “Predefined Reports” in the *SolarWinds Orion Network Performance Monitor Administrator Guide*.

When you have finished editing your reports, you can print them with the click of a button, and you can also view most of them through the Orion NetFlow Traffic Analyzer Web Console by default. For more information, see “Customizing Views” in the *SolarWinds Orion Network Performance Monitor Administrator Guide*.

A report scheduler application is available for download to all customers with a valid maintenance agreement. This tool is used to schedule automatic email reports that can be sent to individual users or groups of users. Simply log in to the customer portion of the SolarWinds website and download the Report Scheduler.

Report Writer capabilities are enhanced when they are used in conjunction with the Custom Property Editor. Once added, properties are available for report sorting and filtering. For more information, see “Creating Custom Properties” in the *Orion Network Performance Monitor Administrator Guide*.

NetFlow-specific Predefined Reports

The following reports are immediately available with your NetFlow Traffic Analyzer installation under the heading Historical NetFlow Reports on the Network Performance Monitor Reports page, accessible by clicking **Reports** in the Views toolbar. These reports may be modified with Report Writer, as necessary, to suit your network performance reporting requirements.

Historical NetFlow Reports

The following reports are predefined for reporting on the NetFlow-enabled devices on your network.

Top 100 Applications – Last 24 Hours

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

Top 20 Traffic Destinations by Domain – Last 24 Hours

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

Top 20 Traffic Sources by Domain – Last 24 Hours

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

Top 5 Protocols – Last 24 Hours

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

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

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

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

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

Top 50 Receivers – Last 24 Hours

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

Top 50 Transmitters – Last 24 Hours

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

Getting Started with Report Writer

Before you can use Report Writer, you must have collected at least a few minutes worth of data in a database that is populated with the devices that you want to monitor. A variety of reports are included with Report Writer, and icons that precede report names distinguish the different types of reports that are available. The following procedure starts Report Writer.

To start Report Writer:

1. Click **Start > SolarWinds Orion > Report Writer**.
2. Click **File > Settings**.
3. In the General tab of the Report Writer Settings window, select either of the following as a default viewing mode:
   - **Preview** displays the report as it will appear in printed form. For more information, see “Preview Mode” on page 24.
   - **Report Designer** is the report creation and editing interface. For more information, see “Design Mode” on page 24.

   Note: You can toggle between Preview and Report Designer modes at any time by clicking **Preview** or **Design**, respectively, on the toolbar.
4. ***If you want to separate the data for individual network objects with horizontal lines,*** click **Report Style,** and then check **Display horizontal lines between each row.**
5. Click **OK** to exit Report Writer Settings.
6. ***If you want to open a predefined report,*** select one from the list in the left pane of the main window.

   Note: Orion NetFlow Traffic Analyzer supplies the following predefined, NetFlow-specific reports under the heading Historical NetFlow Reports:
   - **Top 100 Applications – Last 7 Days**
   - **Top 20 Traffic Destinations By Domain – Last 7 Days**
   - **Top 20 Traffic Sources By Domain – Last 7 Days**
   - **Top 5 Protocols – Last 7 Days**
   - **Top 5 Traffic Destinations By IP Address Group – Last 7 Days**
   - **Top 5 Traffic Sources By IP Address Group – Last 7 Days**
   - **Top 50 Receivers – Last 7 Days**
   - **Top 50 Transmitters – Last 7 Days**
7. ***If you want to create a new report,*** click **File > New Report**.

Preview Mode

Preview mode shows a report as it will print. When you open a report in Preview mode, or switch to Preview mode from Design mode, Orion NPM runs the query to generate the report and Report Writer displays the results. The toolbar at the top of the Preview window provides the following actions and information:

- Current page number and total number of pages in the report in the form **current# / total#**
- Page navigation buttons: First Page, Page Up, Page Down, and Last Page
- Zoom views

  Note: Double-click on a report preview to zoom in and double-right-click to zoom out.
- Print report.

Design Mode

Use Design mode to create new reports and modify or rename existing reports. The options available for both creating and modifying reports are the same. Design mode options are also dynamic, based upon the type of report, included report data, and report presentation. Available options differ according to the type of report that you are designing, but all reports require that you select the data to include and decide how that data will be sorted, ordered, filtered, and presented.

Creating and Modifying Reports

The following procedure guides you in the modification and creation of reports in Report Writer.

To open a report with Report Writer:

1. ***If you want to modify an existing report,*** select an existing report from the inventory in the left pane of the main Report Writer window.
2. ***If you want to create a new report,*** click **File > New Report**, select the type of report that you would like to create, and then click **OK**.

The following sections describe available options for creating or modifying Historical NetFlow Reports, including directions for options configuration.

Notes:

- The SQL query generated by the report may be viewed in an additional tab. Click **Report > Show SQL** to add a read-only SQL tab to the Design window.
- A preview of your report is available at any time. Click **Preview** to enter Preview Mode. Click **Design** to return to Design Mode.

General Options

The General tab opens by default and shows titling and display options that may be configured as follows.

To configure General options:

1. Specify the following information for your report:
   - **Report Group**
   - **Report Title**
   - **Subtitle**
   - **Description**

   Note: If you use an existing report group name, the new report is added to that existing group in the left pane of the main window.
2. Select the display **Orientation** of your report.
3. ***If you do not want to make this report available on your Orion NPM Web Console,*** clear **Make this Report available from the Orion Web Site.**

   Note: By default, most reports are made available for display in the Orion NPM Web Console. For more information, see “Customizing Views” in the *Orion Network Performance Monitor Administrator Guide*.

Select Fields Options

The Select Fields tab allows you to select the data field that you want either to include in a new report or to modify in an existing report. Data fields are selected and configured as follows.

To select and configure fields:

1. Click Select Fields. In the Select Fields tab, you can choose fields, sort orders, and specify functions.
2. ***If you are creating a new report or adding fields to an existing report,*** click the ellipsis, select **Add a new field,** and then dynamically define each new report field as follows:
   a. Click the asterisk after **Field:** and select the type of information that you want to include in the current report field.
   b. ***If you want to sort the data in the current field,*** click the **sort** asterisk and select a sort order.
   c. ***If you want to perform an operation on the data in the current field,*** click the **function** asterisk and select an operation.

3. ***If you are modifying an existing report,*** click the **Field**, **sort**, or **function** that you want to change, and then select a new value as follows:
   a. Click the asterisk after **Field:** and select the type of information that you want to include in the current report field.
   b. ***If you want to sort the data in the current field,*** click the **sort** asterisk and select a sort order.
   c. ***If you want to perform an operation on the data in the current field,*** click the **function** asterisk and select an operation.
4. ***If you want to test your selections as you assemble your report,*** click **Execute SQL Query** to view the current query results.
5. ***If you want to preview your report,*** click **Preview** to run the query and display the results in Preview mode.

   Note: Click **Design** in the toolbar to return to the Design Mode window.
6. ***If you want to delete a field or rearrange the order of the fields that are listed in your report,*** select a field, click the ellipsis, and select the appropriate action.

   Note: Unchecked fields are not displayed in your report, but their sort and function configurations are retained.

Filter Results Options

The Filter Results tab allows you to generate filter conditions for field data by selecting appropriate descriptors from the linked context menus. Results filters are configured as follows.

To configure results filters:

1. Click the ellipsis, and then select from the following options:
   - Select **Add a new elementary condition** to generate conditions based on direct comparisons of network object data fields.
   - Select **Add a new advanced elementary condition** to generate conditions based on comparisons of network object data fields or values.
   - Select **Add a new complex condition** to define a condition that filters other defined conditions.
   - Select **Delete current condition** to remove a selected condition.
   - Select **Move current condition forward** or **Move current condition backward** to change the order of your conditions accordingly.

2. Set filter conditions by clicking the dynamically generated descriptor links.

   Note: Available linked descriptors are dynamically generated in keeping with all other variables in the same condition. For more information about conditions and condition groups, see “Understanding Condition Groups” in the *Orion Network Performance Monitor Administrator Guide*.

3. Check or clear individual filter conditions to enable or disable their application, respectively, to your report.

Top XX Records Options

The Top XX tab allows you to limit the number of records that are shown in your report to either a top *number* or a top *percentage* of all results. Top XX options are configured as follows.

To configure Top XX records:

1. ***If you want to show all records in your report,*** select **Show All Records**.
2. ***If you want to specify a truncated list of eligible items for your report,*** select one of the following options with *number* or *percentage* values as appropriate:
   - **Show only the Top *number* Records**
   - **Show the Top *percentage* % of Records**

Time Frame Options

The Time Frame tab allows you to limit the scope of your report to a specific period of time. Time Frame options are configured as follows.

To configure Time Frame options:

1. Select one of the following Time Frame options:
   - **Named Time Frame**
   - **Relative Time Frame**
   - **Specific Time Frame**
2. Select or type required values.

   Notes:

   - If you receive a SQL Timeout error message, edit the timeout setting in the SWNetPerfMon.db file. By default, this file is located in the `C:\Program Files\SolarWinds\Orion` directory
   - Since the **Relative Time Frame** is continuously variable, reports may show different results, even if they are run close together in time.

Summarization Options

The Summarization tab allows you to generate summaries of your results over specific periods of time. Summarization options are configured as follows.

To configure results summarization:

1. Select **Summarize the Results by Hour, Date, Month, etc**.
2. Select the summarization period and then specify where to locate the summary field in your report.

Field Formatting Options

The Field Formatting tab allows you to customize the format of the various results fields in your report. Field formatting options are configured as follows.

To format results fields:

1. Select the field that you want to format.
2. Edit labels and select options as appropriate.

   Note: The formatting options available for each field may be different according to the nature of the data contained in that field.
3. ***If you want to hide any field,*** check **Hidden Field**.
4. ***If you want to view your changes at any time,*** click **Preview**.

Report Grouping Options

The Report Grouping tab allows you to group results by field descriptor within your report. Add, edit, and delete report groups to organize the data in your report. Establish and edit report groups as follows.

To add and edit report groups:

1. ***If you want to add a new report group,*** use the following procedure for both new and pre-existing reports.
   a. Select a group from the list to serve as the basis of your new group.
   b. Click **Add Report Group** to add your selected base group to the **Report Groups** list.
   c. If you want to change the grouping order, use the up and down arrows to change the grouping order accordingly.
2. ***If you want to edit an existing report group,*** use the following procedure for both new and pre-existing reports.
   a. Select the field from the Report Groups list.
   b. Click **Edit Report Group**.

3. The following options may be changed as needed:
   - The **Group Header** is the text that designates groups on your report.
   - The **Web URL** is the dynamic location of your published report with respect to your Orion NPM Web Console.
   - **Font** size, face, color, and background may all be modified by clicking associated ellipses.
   - **Alignment** may be left, center, or right.
   - Check **Transparent Background** for better results when publishing your report to the Web.
   - If you want to change the grouping order, use the up and down arrows to change the grouping order accordingly.

Example Report

The following procedure generates an example report of the top 15 sources of network traffic, listed by domain, from the previous 30 days. The final report is sorted so that the greatest sources of traffic are viewed first with the rest following in descending order of traffic volume.

Note: At any point during the creation of a report (or perhaps at many points), you may save what you've done by clicking **File > Save**. The first time you save, you must give your report a filename, or accept the default, which will be the report title that you assign in the following procedure.

1. Click **File > New Report**.
2. The example calls for a report of the top 15 sources of network traffic, listed by domain, from the previous 30 days, so select **Historical Interface Traffic**, and then click **OK**.
3. Type `My Reports` in the **Report Group** field.
4. Type `Top 10 Sources of Network Traffic` as the **Report Title**.
5. Type `Listed by Domain, from the Previous 30 Days` as the **Subtitle**.
6. Select **Portrait** for the paper orientation.
7. Click Select Fields.
8. Click the ellipsis, and then select **Add a new field**.
9. Click the **Field** asterisk, and then select **Network Nodes > Node Details > DNS**.
10. Click the ellipsis, and then select **Add a new field**.
11. Click the **Field** asterisk, and then select **Historical Interface Traffic > Transmit+Receive Data Combined > Total Bytes Recv+Xmit**.

12. Click the **sort** asterisk on the **Total Bytes Recv+Xmit** line, and then select **descending**.

    Note: Some fields require predefined functions, as in the case of the Total Bytes Recv+Xmit field, which requires a SUM function.

13. Click **Execute SQL Query** to view the report data in the preview window.

    Notes:

    - Click **Execute SQL Query** at any time to view the results of your report design, and click **Preview** to see how the final report will appear.
    - Column widths in the preview window are adjustable. To resize columns, grab the column dividers in the title bar and reposition them as required.

14. Click Top XX.

15. Select **Show only the Top** *number* **Records**, and then type `15` as the number of records that you want to view.

16. Click Time Frame.

17. Select **Named Time Frame**, and then select **Last 30 Days** in the **Time Frame** field.

18. ***If you want to break down the report day-by-day,*** click Summarization and specify your choices.

19. ***If you want to filter your report,*** click Filter Results and specify filter rules.

20. Click **File > Save** to save your work.

Chapter 5

Viewing NetFlow Traffic Analyzer Data in the Orion Web Console

Once you have configured and enabled a NetFlow source, you can view the various types of NetFlow statistics that it records in the Orion NPM Web Console. Available NetFlow-specific resources are listed in the following table.

NetFlow-specific Resources for Web Console Views	
NetFlow Traffic Analysis Summary	NetFlow Endpoints
NetFlow Protocols	NetFlow Applications
NetFlow IP Address Group	NetFlow Conversation
NetFlow Country	NetFlow Domain
NetFlow Traffic Analysis	NetFlow Types of Service

The following procedure configures your Orion NPM Web Console to show NetFlow Traffic Analyzer resources.

Adding NetFlow Resources to Web Console Views

The following procedure adds a NetFlow-specific resource to any Orion NPM Web Console view.

To add a NetFlow resource to a web console view:

1. Log on to the Orion NPM server that you are using for NetFlow traffic analysis.
2. Click **Start > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
3. Log in to the NetFlow Web Console using a **User ID** with administrative privileges.

   Note: Initially, `Admin` is the default administrator **User ID** with a blank **Password**.
4. Click **Admin** on the Views menu bar, and then click **Manage Views** in the Admin menu on the left.
5. Select the view to which you want to add a NetFlow-specific resource, and then click **Edit**.
6. Click **+** next to the resource column in which you want to display the additional NetFlow resource.

7. Click **+** next to any of the NetFlow resource types listed in the previous table to expand the resource tree and display all available resources for the group.

   Note: Resources that are already listed in your view will not be checked on this page, as it is a view of all available resources. Therefore, it is possible to pick duplicates of resources that you are already displaying.

8. Check the resources that you want to add, and then click **Submit**.

   Note: You are returned to the **Customize View** page, where you may arrange the display of resources using the arrow buttons provided next to each resource column.

9. ***If you still want to change aspects of your view,*** repeat the preceding steps as needed.

   Notes:

   - For more information about using your customized view as a default view assigned to a user, see “Editing User Accounts” in the *Orion Network Performance Monitor Administrator Guide*.
   - To add your customized view to a menu bar as a custom item, see “Adding a Custom Menu Item” in the *Orion Network Performance Monitor Administrator Guide*.

Creating View Limitations

NetFlow Traffic Analyzer views may also be limited to show NetFlow information from selected types of NetFlow sources. The procedure for setting view limitations is as follows.

To create view limitations in NetFlow Traffic Analyzer:

1. Log on to the Orion NPM server that you are using for NetFlow traffic analysis.
2. Click **Start > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
3. Log in to the NetFlow Web Console using a **User ID** with administrative privileges.

   Note: Initially, `Admin` is the default administrator **User ID** with a blank **Password**.

4. Click **Admin** on the Views menu bar, and then click **Manage Views** in the Admin menu on the left.
5. Select the view that you want to limit, and then click **Edit**.
6. Click **Edit** below the View Limitation heading.

7. Select the type of limitation that you want to apply, and the click **Continue**.
8. Select the appropriate limitations, and then click **Submit**.

Customizing Charts in NetFlow Traffic Analyzer

Charts produced within the Orion Network Performance Monitor Web Console are easily customizable. Depending upon the resource, charts are customized either on an Edit *Resource* page or from a Customize Charts page. The following sections describe the available options in either case.

Edit *Resource* Page

Click **Edit** in the title bar of any chart resource to access customizable chart options, including the Maximum Number of Items to Display (for Top XX charts) and the Resource Style. The following Chart Styles are also available:

- 2D Pie Chart
- 3D Pie Chart
- Area Chart

Customize Chart Page

The following sections describe options that are available on the Customize Chart page to modify the presentation of a selected chart.

Note: Click **Refresh** at any time to review changes that you have made.

Chart Titles

Chart Titles are displayed at the top center of a generated chart. The Chart Titles area allows you to modify the Title and Subtitles of your generated chart.

Note: Orion Network Performance Monitor may provide default chart titles and subtitles. If you edit any of the **Chart Titles** fields on the Custom Chart page, you can restore the default titles and subtitles by clearing the respective fields, and then clicking **Submit**.

Time Periods

Predefined and custom time periods are available for generated charts. You may designate the time period for your chart by either of the following methods:

- Select a predefined time period from the **Adjust Time Period for Chart** menu.
- Provide custom Beginning and Ending Dates/Times in the appropriate fields in the **Enter Date / Time Period** area.

Adjust Sample Interval

The sample interval dictates the precision of your generated chart. A single point or bar is plotted for each sample interval. If a sample interval spans multiple polls, polled data is automatically summarized and plotted as a single point or bar on the chart.

Note: Due to limits of memory allocation, some combinations of time periods and sample intervals may require too many system resources to display, due to the large number of polled data points. As a result, charts may not display if the time period is too long or if the sample interval is too small.

Chart Size

Chart Size options configure the width and height, in pixels, of the chart. You can maintain the same width/height aspect ratio, or scale the chart in size, by typing a width in the **Width** field and then typing `0` for the **Height**.

Data Tables

The **Data Table Below Chart** option, if selected, displays a table of the charted data points below the chart.

Note: You may not be able to read individual data points if you select a small Sample Interval. Increase the Sample Interval to make data points easier to read.

Font Size

Font sizes for generated charts are variable. The **Font Size** option allows you to select a **Small**, **Medium**, or **Large** size font for your chart labels and text.

Note: Font Size selections are maintained in the printable version of your chart.

Printing Options

To print your customized chart, click **Printable Version** and a printable version of your customized chart displays in the browser.

Data Export Options

Exportable chart data is available as Microsoft Excel-compatible **Raw Data** or as HTML-formatted **Chart Data**, as shown in the following steps.

To export chart data:

1. ***If you want to view your chart data as Microsoft Excel-compatible Raw Data,*** click **Raw Data** in the Display Data from Chart area, and then follow the prompts, if provided, to open or save the resulting raw data file.
2. ***If you want to view your chart as HTML-formatted data,*** click **Chart Data** in the Display Data from Chart area and the data for your chart displays in a new browser window.

Customizing Top XX Resources

Top *XX* resources provide charts and data that characterize the types of traffic on your network. Traffic is reported both visually, with customizable charts and numerically, in terms of percentages. The following procedure presents the available custom options for presenting data in Top XX resources.

To customize Top *XX* resource titles and chart types:

1. Click **Edit** in the Top *XX* resource title bar.
2. Type the number of items that you want to display in the Maximum Number of Items to Display field.
3. Select from the following Resource Style options:
   - **Chart with Legend**
   - **Chart with No Legend**
   - **No Chart**.
4. Select from the following Chart Style options:
   - **2D Pie Chart** presents a “flat” view of your data
   - **3D Pie Chart**
   - **Area Chart** presents a historical view of your data as represented by areas calculated at past polling times

Items are displayed in Top *XX* resources based on traffic percentages. Individual Top *XX* resources may be configured to show any number of items. Absolute percentages are calculated for each item based on all monitored items. Relative percentages for each item are calculated in terms of the total number of items displayed in the selected resource.

For example, a given node (HOME) is communicating with 4 other endpoints (1, 2, 3, and 4). The following table shows the difference between the types of percentages that are calculated and displayed for both Top 3 Endpoints and Top 4 Endpoints resources.

Endpoint	Traffic	Percentage of Total Actual Traffic	Absolute Percentage		Relative Percentage	
			Top 4	Top 3	Top 4	Top3
1	4 MB	40 %	40 %	40 %	40 %	44.4%
2	3 MB	30 %	30 %	30 %	30 %	33.3%
3	2 MB	20 %	20 %	20 %	20 %	22.2
4	1 MB	10 %	10 %	Not Shown	10 %	Not Shown
TOTAL	10 MB	100 %	100 %	90 %	100 %	100 %

The following procedure presents the steps required to configure the display of traffic percentages in Top *XX* resources.

To configure Top *XX* resource percentages:

1. Log in to the NetFlow Web Console using a **User ID** with administrative privileges.

   Note: Initially, `Admin` is the default administrator **User ID** with a blank **Password**.
2. Click **Admin** in the top menu bar.
3. Click **NTA Settings** in the left pane menu.
4. Click **Settings**.
5. Click **Edit** under Global Settings.
6. Select either of the following, as appropriate:
   - Calculate Absolute Percentages for Top *XX* Lists
   - Calculate Relative Percentages for Top *XX* Lists

Chapter 6

Working with Orion NetFlow Traffic Analyzer

While Orion NPM can tell you the bandwidth usage on a given interface, Orion NetFlow Traffic Analyzer takes this capability one step further, providing you with more information about the actual user of that bandwidth and the application that they are using.

The following scenarios illustrate the value of Orion NetFlow Traffic Analyzer and how it can immediately offer you a significant return on your investment.

Locating and Isolating an Infected Computer

You can use your currently installed Orion instance, with the addition of Orion NetFlow Traffic Analyzer, 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 banking network that handles all of your credit card transactions complains of an extremely sluggish network, causing frequent timeouts during sensitive data transfers.
2. You open the Orion NPM Web Console to see that the link to the network is up at the branch site. You consult your Percent Utilization chart and immediately see that, though your normal utilization is 15-25%, current utilization is 98%.
3. You click the NetFlow Traffic Analyzer tab, and then click the link to the branch site.
4. Taking a quick look at the Top 5 Endpoints, you see that a single computer in the `10.10.10.0-10.10.10.255` IP range is generating 80% of the load on the branch link.
5. You know that this computer resides in a part of the branch that is accessible to customers for personal transactions using the web.
6. You quickly see that 100% of the last two hours of traffic generated by this computer has been over port 1883.
7. 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 1883, you recognize that this is a virus exploit.
8. You quickly use your configuration management tool, for example Cirrus Configuration Manager, to push a new configuration to your firewall that blocks port 1883.

Locating and Blocking Unwanted Use

Within your network, you can easily chart the increasing usage of your different uplinks. With the addition of Orion NetFlow Traffic Analyzer, you are able to chart utilization as you can with a basic Orion NPM installation, and you can locate specific instances of unwanted use and take corrective action. Consider the following scenario:

1. Your uplink to the internet has been slowing progressively over the last 6 months, even though your head count, application use, and dedicated bandwidth have all been stable.
2. You open the Orion NPM Web Console to see that the link to the net is up at your site. You click your specific uplink and consult your Current Percent Utilization of each Interface chart. You can see that the current utilization of your web-facing interface is 80%.
3. You click this specific interface. Using the Percent Utilization chart and customizing the 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.
4. You click the NetFlow Traffic Analyzer tab, and then click the uplink at that site. Taking a quick look at the top 50 Endpoints, you see that a group of computers in the `10.10.12.0-10.10.12.255` IP range is consuming most of the bandwidth.
5. These computers reside in your internal sales IP range. You begin to drill into each of the offending IP addresses.
6. Each IP you investigate shows Kazaa (port 1214) and World of Warcraft (port 3724) usage in the Top 5 applications.
7. You push a new configuration to your firewall using Cirrus Configuration Manager that blocks all traffic on these two ports.
8. Within minutes, you see the traffic on your interface drop back to 25%.

Recognizing and Thwarting a DOS Attack

Orion NetFlow Traffic Analyzer helps you easily identify both outgoing and incoming traffic. This capability becomes ever more important as corporate networks are exposed to increasingly malicious DOS attacks. Consider the following scenario:

1. You receive a page from Orion NPM. Your router is having trouble linking out to the internet and maintaining a stable connection.
2. You open the Orion NPM Web Console and begin sifting through the possible issues. Your connections are currently up; bandwidth utilization looks good, and then you notice your CPU utilization on the firewall. It is steady between 99% and 100%.
3. You open the firewall node and begin to drill into the interfaces.
4. On the NetFlow Traffic Analyzer tab, you take a quick look at the top 50 Endpoints.
5. The top six computers attempting to access your network are from overseas.
6. You realize that you are being port scanned and that your firewall is interactively blocking these attacks.
7. You push a new configuration to your firewall using Cirrus Configuration Manager that blocks all traffic over the IP range that is attempting to access your network.
8. In minutes, your CPU drops back to normal.

Appendix A

Software License Key

During installation, you may be prompted with the Install Software License Key window requesting that you supply your name, e-mail address, phone number, customer ID, and password. If this is the case, follow the instructions below to enable a software license key.

To enable a software license key:

1. ***If the computer on which you are installing Orion NetFlow Traffic Analyzer is connected to the Internet,*** type the requested information on the Install Software License Key window, and then click **Continue**.

   Note: The SolarWinds license registration server will immediately issue a license key that will allow NetFlow Traffic Analyzer to operate.

2. ***If the computer on which you are installing Orion NetFlow Traffic Analyzer is not connected to the Internet,*** your server cannot authenticate to the SolarWinds license registration server, so you must complete the following procedure.

   a. Click **Skip This and Enter Software License Key Now** on the Install Software License Key window.

   b. Using another computer that is connected to the Internet, log in to the customer area of the SolarWinds website at `www.solarwinds.com/keys`.

   c. Click **Software Keys** from the Customer Area menu.

   d. Select the product for which you need a key, and follow the instructions on the page to obtain a key.

   e. Type the key in the **Enter Software License Key** text box.

3. Click **Continue** to complete your Software License Key installation.

Appendix B

NetFlow Port Configuration

The port used for NetFlow traffic is specified in the configuration of your NetFlow-enabled Cisco appliance. The following excerpts from a Cisco router configuration file offer an example of where to look to enable NetFlow traffic on a Cisco router:

```
!

interface GigabitEthernet0/1

description link to PIX

ip address 10.3.1.2 255.255.255.252

ip route-cache flow

!

ip flow-export source GigabitEthernet0/1

ip flow-export version 5

ip flow-export destination 1.2.0.12 9090

!
```

The `ip flow-export destination` value must reflect the IP address of your NetFlow-enabled Orion NPM server. This value also contains the port number (`9090`) that is required in this step. The `ip route-cache flow`, `ip flow export source`, and `ip flow-export version` values are required to enable NetFlow traffic. Orion NetFlow Traffic Analyzer supports NetFlow version 5. For more information about NetFlow version 5, see your Cisco router documentation or the Cisco website at `www.cisco.com`. For more information on enabling NetFlow traffic on Cisco switches, see the “Enabling NetFlow and NetFlow Data Export on Cisco Catalyst Switches” technical reference on the SolarWinds website or your Cisco documentation.

Index