

SolarWinds Orion

NetFlow Traffic Analyzer Administrator Guide



ORION NETFLOW TRAFFIC ANALYZER

Copyright© 1995-2010 SolarWinds, Inc., 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.

SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide, Version 3.6, 02.09.2010

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.
<i>Italics</i>	Book and CD titles, variable names, new terms
Fixed font	File and directory names, commands and code examples, text typed by you
Straight brackets, as in [value]	Optional command parameters
Curly braces, as in {value}	Required command parameters
Logical OR, as in value1 value2	Exclusive command parameters where only one of the options can be specified

Orion NetFlow Traffic Analyzer Documentation Library

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

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

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

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

Contents

<i>About SolarWinds</i>	<i>iii</i>
<i>Contacting SolarWinds</i>	<i>iii</i>
<i>Conventions</i>	<i>iii</i>
<i>Orion NetFlow Traffic Analyzer Documentation Library</i>	<i>iv</i>

Chapter 1

Introduction	1
<i>Why Install Orion NTA</i>	<i>1</i>
<i>How Orion NTA Works</i>	<i>2</i>
<i>Why Use Orion NTA</i>	<i>3</i>

Chapter 2

Installing Orion NetFlow Traffic Analyzer	5
<i>Licensing Orion NetFlow Traffic Analyzer</i>	<i>5</i>
<i>Orion NTA Requirements</i>	<i>5</i>
<i>Hardware Requirements</i>	<i>6</i>
<i>Software Requirements</i>	<i>6</i>
<i>Virtual Machine Requirements</i>	<i>7</i>
<i>NetFlow, IPFIX J-Flow, and sFlow Requirements</i>	<i>7</i>
<i>Installing Orion NTA</i>	<i>8</i>
<i>Activating Your Orion NTA License</i>	<i>9</i>
<i>Activating an Orion NTA Evaluation License</i>	<i>9</i>
<i>Activating an Orion NTA License with Internet Access</i>	<i>9</i>
<i>Activating an Orion NTA License without Internet Access</i>	<i>10</i>
<i>Completing the Configuration Wizard</i>	<i>11</i>

Chapter 3

Configuring Orion NetFlow Traffic Analyzer	13
<i>Adding Flow-enabled Devices and Interfaces</i>	<i>13</i>
<i>Configuring Flow Sources and CBQoS Devices</i>	<i>14</i>
<i>Adding Flow Sources and CBQoS-enabled Devices</i>	<i>14</i>
<i>Deleting Flow Sources and CBQoS-enabled Devices</i>	<i>16</i>

Enabling the NetFlow Traffic Analysis Summary View 17

Data Compression in Orion NTA..... 18

Configuring NetFlow Management Settings 18

Enabling the Automatic Addition of Flow Sources..... 18

Configuring Data Retention for Flows on Unmonitored Ports 19

Enabling Monitoring of Flows from Unmanaged Interfaces..... 19

Configuring Monitored Ports and Applications 20

Selecting IP Address Groups for Monitoring 22

Configuring Protocol Monitoring 24

Managing Flow Sources and CBQoS-enabled Devices..... 24

Configuring NetFlow Collector Services Ports..... 26

Configuring NetFlow Types of Services 27

Configuring the Orion NTA Top Talker Optimization 28

Configuring DNS and NetBIOS Resolution..... 29

Configuring Database Settings 32

Configuring Charting and Graphing Settings 33

Enabling Progressive Charting 33

Configuring Orion NTA Views and Resources 34

Optimizing Orion NTA Performance 37

Configuring Flow Analysis Redundancy 37

Chapter 4

Creating NetFlow Traffic Analyzer Reports..... 39

Using Report Writer with Orion NTA 39

NetFlow-specific Predefined Reports..... 39

Chapter 5

Viewing NetFlow Traffic Analyzer Data in the Orion Web Console 43

Adding NetFlow Resources to Web Console Views 43

Monitoring Traffic Flow Directions..... 44

Creating View Limitations..... 45

Customizing Charts in NetFlow Traffic Analyzer..... 45

Edit Resource Page..... 45

Customize Chart Page..... 46

<i>Customizing Individual Top XX Resources</i>	47
<i>Customizing for All Users (Administrators Only)</i>	47
<i>Customizing for the Current Session (All Users)</i>	48
<i>Using the NetFlow Traffic View Builder</i>	49
<i>Interacting with the thwack User Community</i>	50
<i>Performing an Immediate Hostname Lookup</i>	50
<i>Viewing Class-based Quality of Service (CBQoS) Data</i>	50

Chapter 6

Working with Orion NTA	53
<i>Locating and Isolating an Infected Computer</i>	53
<i>Locating and Blocking Unwanted Use</i>	54
<i>Recognizing and Thwarting a DOS Attack</i>	54

Appendix A

Managing Software Licenses	57
<i>Requirements</i>	57
<i>Installing License Manager</i>	57
<i>Using License Manager</i>	58
<i>Deactivating Currently Installed Licenses</i>	58
<i>Upgrading Currently Installed Licenses</i>	59
<i>Activating Evaluation Licenses</i>	59

Appendix B

Device Configuration Examples	61
<i>Cisco NetFlow Configuration</i>	61
<i>Extreme sFlow Configuration</i>	62
<i>Foundry sFlow Configuration</i>	62
<i>HP sFlow Configuration</i>	63

Index

Index	65
--------------------	-----------

Chapter 1

Introduction

Orion NetFlow Traffic Analyzer (Orion NTA) provides a simple-to-use, scalable network monitoring solution for IT professionals that are managing any size sFlow, J-Flow, IPFIX, or NetFlow-enabled network.

Why Install Orion NTA

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 NTA 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 Flow data presented in Orion NTA 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

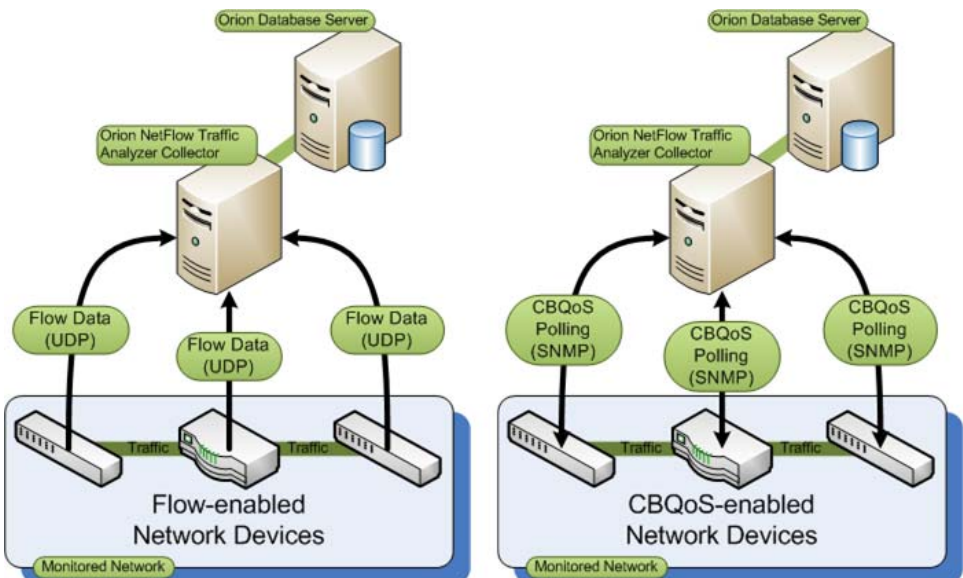
These monitoring capabilities, along with the customizable Orion Web Console and reporting engines, make Orion NTA the easiest choice you will make involving your Flow monitoring needs.

How Orion NTA Works

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

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

Note: CBQoS and Flow monitoring are shown separately to emphasize the difference in collection methods. Network endpoints are not shown, and a typical Orion NTA installation would not require that all CBQoS- and Flow-capable devices be configured to interact directly with the Orion NTA collector. For more information about effectively deploying NetFlow on your network, see “New to Networking Volume 3 – NetFlow Basics and Deployment Strategies”.



Why Use Orion NTA

The following valuable features provided the impetus for the development of current version of Orion NTA, and they are the foundation upon which Orion NTA is built:

Customizable rate-based charts

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

Advanced port and application mapping

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

Flow monitoring support for Cisco Adaptive Security Appliances (ASA)

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

Filtered views including both ingress and egress traffic

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

Support for IPFIX-enabled devices

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

Cisco Class-based quality of service (CBQoS) monitoring

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

Improved availability and performance

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

Analytical capacity planning

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

Alignment of IT resources with enterprise business needs

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

Increased network security

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

Support for multiple Flow ports

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

An all-in-one NetFlow, sFlow, J-Flow, and IPFIX monitoring solution

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

Chapter 2

Installing Orion NetFlow Traffic Analyzer

Orion NTA provides a simple, wizard-driven installation process for collecting data from any Flow-enabled devices monitored by Orion Network Performance Monitor. For an enterprise-class product, the requirements are nominal, even though Flow data is extensive and can use a large amount of database space.

Licensing Orion NetFlow Traffic Analyzer

Licensing for Orion NTA follows the license level of your underlying Orion NPM installation. For more information, 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:

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

Orion NTA Requirements

The server used to host Orion NTA must support both Orion NPM and Orion NTA as Orion NTA is built on and extends Orion NPM. Generally, Orion NTA requirements follow and extend Orion NPM requirements. For more information about Orion NPM requirements, see “Orion NPM Requirements” in the *SolarWinds Orion Network Performance Monitor Administrator Guide*.

The following sections provide minimum configuration requirements.

Hardware Requirements

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

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

Notes:

- By default, Orion NTA listens for Flow data on port 2055 (UDP). Ensure that port 2055 is open for UDP communication on any Orion NTA collector.
- Orion NTA requires that TCP port 17777 is opened both to send and to receive traffic between Orion NPM and any other Orion modules.

Hardware	Requirements
CPU	3GHz or faster, dual processors with dual cores
RAM	2GB or more
Hard Drive Space	Orion NTA server: 5GB or more, RAID 0, 1, 0+1, or 1+0. SQL Server: 5GB or more, RAID 0, 1, 0+1, or 1+0 on at least 6 spindles. Other RAID or SAN configurations are not recommended. Warning: Other RAID or SAN configurations are not recommended.
NetFlow Devices	Cisco devices exporting NetFlow version 5 or 9 Note: Orion NTA only recognizes NetFlow version 9 templates that include all fields included in the NetFlow version 5 template.
IPFIX Devices	Network devices exporting IPFIX
J-Flow Devices	Network devices exporting J-Flow
sFlow Devices	Network devices exporting sFlow version 5

For more information about Flows supported by Orion NTA, see “NetFlow, IPFIX J-Flow, and sFlow Requirements” on page 7.

Software Requirements

Operating system and SQL Server requirements for the current Orion NTA version follow the requirements of an Orion NPM version 9.5 SP4 installation, as provided in the section “Orion NPM Requirements” of the *SolarWinds Orion Network Performance Monitor Administrator Guide*, with the following additions:

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

Virtual Machine Requirements

Orion NTA may be installed on VMware Virtual Machines and Microsoft Virtual Servers if the following conditions are met in your virtual environment:

- All hardware requirements listed in the section “Hardware Requirements” on page 6 are met by each virtual machine.
- Each installation of Orion NPM should have its own, dedicated NIC

Note: Since Orion NPM uses SNMP to monitor your network, if you are unable to dedicate a network interface card to your Orion NPM installation, you may experience gaps in monitoring data due to the low priority generally assigned to SNMP traffic.

NetFlow, IPFIX J-Flow, and sFlow Requirements

Most Flow-enabled devices use a set of static templates to which exported flows conform. Any NetFlow, IPFIX, J-Flow, or sFlow packets that do not include the following field types and field values are ignored by Orion NTA:

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

Notes:

- Only one interface index is absolutely required, but both interface indexes (`INPUT_SNMP` and `OUTPUT_SNMP`) should be provided to view accurate statistics for both ingress and egress flows.
- The `SRC_TOS` field type corresponding to the service type of ingress traffic on an interface (field type number 5) is required to view Type of Service information for your traffic through a Flow source. The template used by Cisco Adaptive Security Appliances (ASA) does not provide this field.
- If SolarWinds states that Orion NTA supports Flow monitoring for a device, at least one of the templates the device exports satisfies these requirements.

Installing Orion NTA

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

Note: If you are installing Orion NTA on an Orion Additional Poller, confirm that the version of Orion NTA you are installing on any and all Orion Additional Pollers matches the version of Orion NTA you are running on your primary Orion polling engine.

To install Orion NetFlow Traffic Analyzer:

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

Notes:

- SolarWinds generally recommends that you backup your database before performing any upgrade.
 - Current Orion NTA versions require Orion NPM version 9.5 SP4 or later.
 - If you are upgrading from Orion NTA version 1.0, you must first uninstall Orion NTA version 1.0 before installing the current release.
 - You must upgrade to Orion NTA version 3.1 before upgrading to the current version of Orion NTA.
2. ***If you are installing Orion NTA on a terminal server***, perform the following steps before continuing with your installation:
 - a. Click **Start > Control Panel > Add or Remove Programs**.
 - b. Click **Add New Programs**, and then click **CD or Floppy**.
 - c. 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 then launch the executable.
 4. ***If you received physical media***, navigate to the executable, and then launch it.
 5. ***If this installation is an upgrade of a previous version of Orion NTA***, click **Yes** when you are asked to continue to perform an upgrade of SolarWinds Orion NetFlow Traffic Analyzer.
 6. Confirm your installation type on the Welcome window, and then click **Next**.
 7. 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.

Activating Your Orion NTA License

After installing Orion NTA using the InstallShield Wizard, you are prompted on the Activate Orion NetFlow Traffic Analyzer window to activate your Orion NTA license. The following sections describe the different options for activating your Orion NTA license:

- Activating an Orion NTA Evaluation License
- Activating an Orion NTA License with Internet Access
- Activating an Orion NTA License without Internet Access

Activating an Orion NTA Evaluation License

SolarWinds provides the opportunity to evaluate a fully functional Orion NTA installation for 30 days following initial installation.

To activate an evaluation license:

1. Click **Continue Evaluation** on the Activate Orion NetFlow Traffic Analyzer window.
2. Complete the Orion Configuration Wizard. For more information, see “Completing the Configur” on page 11.

Activating an Orion NTA License with Internet Access

In most cases, Orion NTA is installed on an Orion NPM server that has access to the Internet. When your Orion NPM server is connected to the Internet, license activation is a straightforward process, as detailed in the following procedure.

To activate your license when you have Internet access:

1. Click **Enter Licensing Information** on the Activate Orion NetFlow Traffic Analyzer window.
2. Select **I have internet access and an activation key**.
3. Click the <http://www.solarwinds.com/customerportal/> link to access the customer portal on the SolarWinds web site.
4. Log in to the portal using your SolarWinds **Customer ID** and **Password**.
5. Click **License Management** on the left navigation bar.
6. Navigate to your product, choose an activation key from the **Unregistered Licenses** section, and then copy the activation key.
7. **If you cannot find an activation key in the Unregistered Licenses** section, contact SolarWinds support at <http://www.solarwinds.com/support/>.

8. Return to the Activate Orion NetFlow Traffic Analyzer window, and then paste or enter the activation key in the **Activation Key** field.
9. **If you access Internet web sites through a proxy server**, click **I access the internet through a proxy server**, and enter the proxy address and port.
10. Click **Next**.
11. Enter the requested registration information, including your name, email address and phone number, and then click **Next**.
12. Click **Finish** when your license imports successfully.
13. Complete the Orion Configuration Wizard. For more information, see “Completing the Configur” on page 11.

Activating an Orion NTA License without Internet Access

Even when your Orion NPM server does not have access to the Internet, license activation is a straightforward process, as detailed in the following procedure.

To activate your license when you do not have Internet access:

1. Click **Enter Licensing Information** on the Activate Orion NetFlow Traffic Analyzer window.
2. Select **This server does not have internet access**, and then click **Next**.
3. Click **Copy Unique Machine ID**.
4. Click **OK** to confirm that your Unique machine ID has been copied.
5. Paste the copied data into a text editor document.
6. Transfer the document to a computer with Internet access.
7. On the computer with Internet access, complete the following steps:
8. Browse to <http://www.solarwinds.com/customerportal/>.
9. Log on to the SolarWinds Customer Portal with your SolarWinds Customer ID and Password.
10. Click **License Management** on the left navigation bar.
11. Navigate to your product, and then click **Manually Register License** next to the Activation Key you want to use.
12. **If the Manually Register License option is not available for your product**, contact SolarWinds support at <http://www.solarwinds.com/support/>.
13. Confirm you want to manually generate a license key by clicking **Continue**.
14. Provide your name, email address, phone number, computer name, and the Unique Machine ID copied earlier.

15. Click **Generate License File**.
16. Click the provided link to your generated license file.
Note: A copy of the license file has been sent to your previously supplied email address.
17. Save the license key file to an appropriate location.
18. Transfer the license key file to your Orion server.
19. Return to the Activate Orion NetFlow Traffic Analyzer window, and then click **Browse** to locate the license key file.
Note: Confirm that the extension to your license key file is `.lic`.
20. Click **Next**.
21. *If you are installing Orion NTA 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.
22. Click **Finish** when your license imports successfully.
23. Complete the Orion Configuration Wizard. For more information, see “Completing the Configur” on page 11.

Completing the Configuration Wizard

The Configuration Wizard enables you to configure Orion NTA module to interact with your underlying Orion NPM database, website and services.

To configure Orion NTA:

1. *If the Configuration Wizard has not started automatically*, click **Start > All Programs > SolarWinds Orion > Configuration Wizard**.
2. Review the Orion Configuration Wizard welcome text, and then click **Next**.
3. Confirm that all services you want to install are checked in the Service Settings window, and then click **Next**.
Note: Orion NTA requires the SolarWinds NetFlow Traffic Analyzer Service.
4. Review the configuration summary, and then click **Next**.
5. Click **Finish** when the Orion Configuration Wizard completes.
6. *If you are asked to select a polling engine to manage*, select the Orion server you are using as your NetFlow collector, and then click **Connect to Polling Engine**.
7. Proceed to add your NetFlow devices and interfaces to Orion Network Performance Monitor. For more information about adding NetFlow devices, see “Adding Flow-enabled Devices and Interfaces” on page 13.

Chapter 3

Configuring Orion NetFlow Traffic Analyzer

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.

Note: If you already have Flow-enabled devices on your network, Orion NTA can automatically add them as NetFlow sources if you configure your Flow-enabled devices to send their Flows to your designated Orion NTA server. For more information, see “Device Configuration Examples” in the *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

Adding Flow-enabled Devices and Interfaces

Before Orion NTA can analyze network traffic, the Flow-enabled network interfaces on which you want to monitor traffic must be managed by Orion NPM. Adding Flow-enabled devices and interfaces to Orion NPM and designating the same devices and interfaces as Flow sources in Orion NTA are separate actions, and the designation of Flow sources does not affect licensing requirements for either Orion NPM or Orion NTA.. Flow-enabled devices must be added to the Orion database using either Network Sonar or Web Node Management in Orion NPM before Orion NTA can initiate Flow monitoring. For more information about designating Flow sources in Orion NTA, see “Adding Flow Sources and CBQoS-enabled Devices” on page 14.

The discovery methods in the following procedure add devices and interfaces to Orion NPM. If you have already configured device interfaces to send Flow data, Orion NTA will detect and analyze Flow data, as soon as the device is added.

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

1. Log on to the Orion NPM server that hosts Orion NTA.

Note: The current version of Orion NTA requires Orion NPM 9.5 SP2 or later.

2. ***If you are adding a large number of nodes***, use Orion Network Sonar. For more information, see “Discovering and Adding Network Devices” in the *Orion Network Performance Monitor Administrator Guide*.

Note: Confirm that you add all Flow-enabled interfaces on added devices.

3. **If you are only adding a few nodes**, it may be easier to use Web Node Management in the Orion Web Console. For more information, see “Adding Devices for Monitoring in the Web Console” in the *Orion Network Performance Monitor Administrator Guide*.
4. Click **NetFlow Traffic Analysis** in the Modules menu bar to confirm the addition of all Flow sources on your network. For more information, see “Adding Flow Sources and CBQoS-enabled Devices” on page 14.

After installing Orion NTA, the Orion NPM polling engine establishes a baseline by collecting network status and statistics immediately. Then, 30 seconds later, the Orion NPM polling engine performs another collection. You may notice an increase in your CPU usage during this time. After these initial collections, Orion NPM collects network information every 10 minutes for nodes and every 9 minutes for interfaces. Meaningful Flow analysis data should display in the web console within minutes. Before leaving Orion NTA to gather data, ensure you are collecting Flow data for the correct interface ports and applications. For more information, see “Configuring Monitored Ports and Applications” on page 20.

Configuring Flow Sources and CBQoS Devices

The following sections provide procedures for adding and deleting Flow sources and selecting CBQoS-enabled devices for monitoring.

Note: By default, if they are already monitored by Orion NPM, new Flow sources are detected and added automatically to the NetFlow Sources resource. For more information about the Automatic Addition of Flow Sources option, see “Enabling the Automatic Addition of Flow Sources” on page 18.

Adding Flow Sources and CBQoS-enabled Devices

Depending on your Orion NTA configuration, you will be prompted to add the detected Flow-enabled device or the Flow-enabled device will be automatically added. The following procedure confirms the addition of Flow sources to Orion NTA.

Note: If you are using NetFlow version 9, confirm that the template you are using includes all fields included in NetFlow version 5 PDUs. For more information, see “NetFlow, IPFIX J-Flow, and sFlow Requirements” on page 7.

To add Flow sources and CBQoS-enabled devices to Orion NTA:

1. **If you are not currently logged-in to the Orion Web Console**, click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**, and then log in using a **User ID** with administrative privileges.
2. **If you are currently logged-in the to Orion Web Console**, click **NetFlow Traffic Analyzer** in the Modules toolbar.

3. **If the NetFlow Sources resource is not displayed on the NetFlow Traffic Analysis Summary view**, complete the following steps:

Note: The NetFlow Sources resource is included, by default, in the NetFlow Traffic Analysis Summary View. If the Summary view, including the NetFlow Source resource, is not enabled as the default NetFlow Web Console view, see “Enabling the NetFlow Traffic Analysis Summary View” on page 17.

- a. Click **Admin** in the Views menu bar.
 - b. Click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
 - c. Click **NetFlow Sources**.
4. **If automatic addition of NetFlow sources is enabled**, all Flow sources currently monitored by Orion NPM will display in the NetFlow Sources resource. For more information about the automatic addition of Flow sources, see “Enabling the Automatic Addition of Flow Sources” on page 18.
 5. **If the NetFlow Sources resource is present but a current Flow source is not listed**, confirm that the Flow source is currently monitored by Orion NPM, and then complete the following steps:
 - a. Click **Admin** in the Views menu bar.
 - b. Click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
 - c. Click **NetFlow Sources**.
 6. **If you want to select all available interfaces for Flow monitoring**, complete the following steps:
 - a. Select **All** from the Show menu.
 - b. Check **NetFlow** in the header.
 - c. Click **Submit**.

Note: Exporters only (last 15 minutes) is the default filter. This option shows all devices in your Orion database that have sent Flow data within the last 15 minutes. If you expect other devices to export Flow data in the future, select another option, as described in the following steps.

7. **If you want to select available CBQoS-enabled devices for monitoring**, complete the following steps:
 - a. Select either **All** or **Cisco devices only** from the Show menu.

Note: CBQoS monitoring is only available for Cisco devices.
 - b. Check **CBQoS** in the header.
 - c. Click **Submit**.

8. **If you only want to receive NetFlow data from monitored Cisco devices**, complete the following steps:
 - a. Select **Cisco devices only** from the Show menu.
 - b. Check **NetFlow** in the header.
 - c. Click **Submit**.
9. **If you want to select specific interfaces for monitoring**, use the following procedure:
 - a. Select **All** from the Show menu.
 - b. Click **+** next to the vendor name of your intended Flow source.
 - c. Expand nodes and interfaces, as necessary, to see currently monitored interfaces.
 - d. Select interfaces by any of the following methods:
 - Check the **NetFlow** column for individual interfaces
 - Check the **NetFlow** column for any node to select all interfaces on the selected node
 - Check the **NetFlow** column for any device type to select all devices of the selected types.
 - e. When you have selected all interfaces to monitor, click **Submit**.

Deleting Flow Sources and CBQoS-enabled Devices

To remove a Flow source, complete the following procedure.

To delete either Flow sources or CBQoS-enabled devices:

1. **If you are not currently logged-in to the Orion Web Console**, click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**, and then log in using a **User ID** with administrative privileges.
2. **If you are currently logged-in to the Orion Web Console**, click **NetFlow Traffic Analyzer** in the Modules toolbar.
3. Click **Admin** in the Views menu bar, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
4. Click **NetFlow Sources**.
5. Select the type of device to delete from the **Show** menu.
6. Expand the node tree to locate the source you want to delete, and then expand the source you want to delete.

7. Select Flow sources for deletion using any of the following methods:
 - Clear the **NetFlow** column to delete individual interface sources.
 - Clear the **NetFlow** column for any node to delete all interface sources on the selected node.
 - Clear the **NetFlow** column for any device type to delete all device sources of the selected type.
8. *If you want to stop collecting CBQoS data from a monitored device*, use any of the following methods:
 - Clear the **CBQoS** column to stop monitoring individual CBQoS-enabled interfaces.
 - Clear the **CBQoS** column for any node to stop monitoring all CBQoS-enabled interfaces on the selected node
 - Clear the **CBQoS** column for any device type to stop monitoring all CBQoS-enabled devices of the selected type.
9. Click **Submit**.

Enabling the NetFlow Traffic Analysis Summary View

If the NetFlow 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 **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
2. Log in using a **User ID** with administrative privileges.
3. Click **Admin** in the Views menu bar.
4. Click **Account Manager** in the Accounts grouping of the Orion Website Administration page.
5. Select **Admin**, and then click **Edit**.
6. Under the Default Menu Bar and Views heading, click **+** next to **Admin's NetFlow Traffic Analysis Settings**.
7. In the NetFlow Traffic Analysis View field select **NetFlow Traffic Analysis Summary**.
8. Click **Submit** at the bottom of the page.
9. Click **NetFlow Traffic Analysis** in the Modules menu bar to display the NetFlow Traffic Analysis Summary page.

Data Compression in Orion NTA

Flow-enabled devices can send a large amount of data to your Orion server for processing with Orion NTA. As a result, the Orion database may quickly become unmanageable unless received Flow statistics are compressed. Flow data compression in Orion NTA proceeds as detailed in the following procedure.

Note: For more information about data compression settings and options, see “Configuring Database Settings” on page 32.

1. By default, received Flow data is stored in an uncompressed state for 60 minutes, as designated in the **Keep uncompressed data for** field in the Database Settings grouping on the NetFlow Traffic Analysis Settings view.
Note: This period of time may be extended to 240 minutes (4 hours).
2. As stored Flow data ages beyond the uncompressed data retention period, it is summarized into a single record per 15-minute interval.
3. After a full day, 15-minute interval records are summarized into one-hour interval records.
4. After one week, one-hour interval records are summarized into daily interval records. These daily records are stored for the period indicated in the **Keep compressed data for** field on the NetFlow Settings view.
5. Compressed data that is older than the period designated in the **Keep compressed data for** field is then deleted.

Configuring NetFlow Management Settings

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

Note: The configuration actions in the following sections require administrative access to the Orion Web Console.

Enabling the Automatic Addition of Flow Sources

Orion NTA can detect and automatically add Flow sources that are monitored by Orion NPM. The following procedure enables this option in Orion NTA.

To enable the automatic addition of Flow sources:

1. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
2. Log in using a **User ID** with administrative privileges.
3. Click **Admin** in the Views menu bar.

4. Click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
5. Check **Enable automatic addition of NetFlow sources**.
6. Click **Submit**.

Configuring Data Retention for Flows on Unmonitored Ports

By default, Orion NTA retains data for traffic on unmonitored ports, but some significant savings in terms of database storage space and server processing loads may be realized by disabling this option. For more information about unmonitored ports in Orion NTA, see “Configuring Monitored Ports and Applications” on page 20.

The following procedure configures the option of retaining data for traffic on unmonitored ports in Orion NTA.

Note: Enabling this option may significantly increase the processing load on both your Orion NTA server and your Orion database server.

To configure data retention for flows on unmonitored ports:

1. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
2. Log in using a **User ID** with administrative privileges.
3. Click **Admin** in the Views menu bar.
4. Click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
5. Check **Enable data retention for traffic on unmonitored ports**, and then click **Submit**.

Enabling Monitoring of Flows from Unmanaged Interfaces

In older versions, Orion NTA discarded any Flow record that referred to traffic involving an interface not already managed by Orion NPM. Currently, however, Orion NTA provides the option to retain data for any Flow defined with at least one interface monitored by Orion NPM. For more information about managing interfaces in Orion NPM, see “Discovering and Adding Network Devices” in the *SolarWinds Orion Network Performance Monitor Administrator Guide*. The following procedure enables the option of monitoring traffic on unmanaged interfaces in Orion NTA.

Note: Disabling the option to monitor flows from unmanaged interfaces may significantly decrease the processing load on both your Orion NTA server and

your Orion database server, but it will also decrease the amount of Flow data stored in your Orion database.

To enable the automatic addition of Flow sources:

1. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
2. Log in using a **User ID** with administrative privileges.
3. Click **Admin** in the Views menu bar.
4. Click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
5. Check **Allow monitoring of flows from unmanaged interfaces**, and then click **Submit**.

Configuring Monitored Ports and Applications

Orion NTA allows you to directly specify the applications and ports 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 select the ports and applications you want to monitor, adding any that you do not see but need to monitor, as in the following procedure.

Note: The number of monitored applications directly affects the amount of NetFlow data stored in the database. The more applications and ports you monitor, the more data is stored. For more information about solving database size issues, see “Configuring Database ” on page 32.

To configure monitored applications and ports:

1. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
2. Log in using a **User ID** with administrative privileges.
3. Click **Admin** in the Views menu bar.
4. Click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
5. Click **Application and Service Ports**.
6. Group the viewed applications and service ports by selecting the appropriate view type from the View menu on the left of the Manage Applications and Service Ports view.

Note: By default, applications are listed by increasing associated port number, with multi-port applications listed first.

7. **If you do not know the port number or application name you want to monitor, but you do know a keyword in the application description**, type the keyword in the **Search applications & ports** field, and then click **Search** to generate a list of related applications with their port numbers.
8. **If you want to monitor all listed ports and applications**, click **Enable All Monitoring** above the application list.

Notes:

- Due to the potential volume of data from Flow-enabled network devices, Monitoring all ports and applications may severely affect the performance of both the Orion database and the Orion Web Console. If you are not initially sure what ports and applications you should monitor with Orion NTA, click **Monitor Recommended Ports** above the applications and ports list to monitor the most typical, high-traffic ports and applications.
 - Clicking **Monitor Recommended Ports** will delete any and all existing custom application and port definitions.
9. **If you want to disable monitoring for all listed ports and applications**, click **Disable All Monitoring** above the applications and ports list.

Notes:

- If you are not sure what ports and applications to monitor, click **Monitor Recommended Ports** to monitor the most typical, high-traffic ports.
 - Clicking **Monitor Recommended Ports** will delete any and all existing custom application and port definitions.
10. **If you do not see a port or application you want to monitor**, complete the following steps to add a new application:
 - a. Click **Add Application**,
 - b. Provide a **Description** of the application you want to monitor.
 - c. Provide the **Port(s)** assigned to the application you want to add.

Note: *If you want to add a new multi-port application*, enter port ranges or multiple ports, separated by commas, in the **Port(s)** field.
 - d. **If you only want to monitor application traffic to or from selected Destination or Source IP Address(es)**, select corresponding IP address groups.

Note: For more information about IP address groups in Orion NTA, see “Selecting IP Address Groups for Monitoring” on page 22.
 - e. Select the appropriate **Protocol** for the new application, and then click **Add Application**.

11. **If you want to disable monitoring for a single listed port or application**, click **Disable** in the **Actions** field of the selected application.
12. **If you want to delete a single listed port or application**, click **Delete** in the **Actions** field of the selected application, and then click **Delete Application** in the Delete Application dialog.
13. **If you want to edit the properties of a monitored port or application**, complete the following steps:
 - a. Click **Edit** in the **Actions** column of the selected port or application.
 - b. Edit the **Description** and **Port(s)** information for the selected application.

Notes:

- **If you want to edit a multi-port application**, enter port ranges or multiple ports, separated by commas, in the **Port(s)** field.
 - Some default multi-port applications may be configured with overlapping port assignments. Traffic will only be associated with one of the conflicting applications. To avoid this conflict, remove the port range in conflict, disable a conflicting application, or delete the port or application entirely.
- c. **If you only want to monitor application traffic to or from selected Destination or Source IP Address(es)**, select corresponding IP address groups.

Note: For more information about IP address groups in Orion NTA, see “Selecting IP Address Groups for Monitoring” on page 22.
 - d. Select the appropriate **Protocol** for the selected application.
 - e. Click **Update Application**.

Selecting IP Address Groups for Monitoring

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

To configure IP address group monitoring:

1. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
2. Log in using a **User ID** with administrative privileges.
3. Click **Admin** in the Views menu bar, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.

4. Click either **IP Address Groups** or **Manage IP Address Groups**.
5. *If any one of the listed, pre-existing ranges contains the addresses you want Orion NTA to monitor*, confirm that the range is checked.
6. *If you want to edit an existing group*, complete the following steps:
 - a. Check the IP address group to edit.
 - b. Click **Edit**.
 - c. Edit the Description, as necessary.
 - d. *If you want to define the selected group as a single IP address*, select **IP Address**, and then provide the IP address.
 - e. *If you want to define the selected group as a range of IP addresses*, select **IP Range**, and then provide the starting and ending IP addresses of the range.
 - f. *If you want to include this defined group, if eligible, in Top XX IP Address Groups resources in the Orion Web Console*, check **Enable display** in Top XX IP Address Groups resource.
 - g. *If you want to define another IP Address group*, click **Add**, and then repeat the preceding steps for each additional IP address group.

Note: Click **X** to delete any groups you do not want to maintain.
7. *If you want to add a new group*, complete the following steps:
 - a. Click **Add New Group**.
 - b. Provide a Description.
 - c. *If you want to define the selected group as a single IP address*, select **IP Address**, and then provide the IP address.
 - d. *If you want to define the selected group as a range of IP addresses*, select **IP Range**, and then provide the starting and ending IP addresses of the range.
 - e. *If you want to include this defined group, if eligible, in Top XX IP Address Groups resources in the Orion Web Console*, check **Enable display** in Top XX IP Address Groups resource.
 - f. *If you want to define another IP Address group*, click **Add**, and then repeat the preceding steps for each additional IP address group.

Note: Click **X** to delete any groups you do not want to maintain.
8. Click **OK** when you have completed your group edits and additions.
9. *If you want to delete an existing group*, click **Delete** at the end of the IP address group row.

Configuring Protocol Monitoring

The types of transport protocols that Orion NTA monitors may be configured from the Monitored Transport Protocols page. This page allows you to specify precisely which protocols Orion NTA monitors. Selectively specifying monitored protocols can reduce the amount of Flow traffic Orion NTA has to process, improving overall performance. The following procedure enables selective transport protocol monitoring.

To specify protocols monitored by NetFlow Traffic Analyzer:

1. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
2. Log in using a **User ID** with administrative privileges.
3. Click **Admin** in the Views menu bar.
4. Click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
5. Click **Monitored Protocols**.
6. Confirm that any and all protocols you do not want to monitor are cleared, and then confirm that all the protocols you do want to monitor are checked.
7. Click **Submit** at the bottom of the Monitored Transport Protocols view.

Managing Flow Sources and CBQoS-enabled Devices

After devices with either Flow-enabled or CBQoS-enabled interfaces have been added to Orion NPM, Orion NTA must recognize the new devices for monitoring as Flow sources. By default, if a Flow-enabled device is already properly configured and sending Flow data to the Orion server, Orion NTA will automatically detect the new Flow source. Depending on your Orion NTA configuration, either you will be prompted to add the detected Flow-enabled device or the Flow-enabled device will be added automatically. The following procedure provides instructions for managing Flow sources in Orion NTA.

Notes:

- For more information about automatically adding Flow sources, see “Enabling the Automatic Addition of Flow Sources” on page 18.
- If you are using NetFlow version 9 you must confirm that the template you are using includes all fields included in NetFlow version 5 PDUs. For more information about required templates, see “NetFlow, IPFIX J-Flow, and sFlow Requirements” on page 7.

To manage Flow sources and CBQoS-enabled devices in Orion NTA:

1. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
2. Click **Admin** in the Views menu bar.
3. Click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
4. Click **NetFlow Sources**.
5. *If you want to select all available interfaces to either start or stop Flow monitoring*, select **All** from the Show menu, check or clear **NetFlow** in the header, as appropriate, and then click **Submit**.

Note: **Exporters only (last 15 minutes)** is the default filter. This option shows all devices in your Orion database that have sent Flow data within the last 15 minutes. If you expect other devices to export Flow data in the future, select another option, as described in the following steps.

6. *If you want to select all available CBQoS-enabled nodes to either start or stop CBQoS monitoring*, select **All** from the Show menu, check or clear **CBQoS** in the header, as appropriate, and then click **Submit**.

Note: CBQoS is a Cisco technology. SNMP polls of the MIB for non-Cisco devices will be unsuccessful for CBQoS OIDs, and CBQoS resources for these devices are automatically hidden as they have no data to display.
7. *If you only want to either start or stop receiving NetFlow data from all monitored Cisco devices*, select **Cisco devices only** from the Show menu, check or clear **NetFlow** in the header, as appropriate, and then click **Submit**.
8. *If you only want to either start or stop polling from all monitored CBQoS-enabled Cisco devices*, select **Cisco devices only** from the Show menu, check or clear **CBQoS** in the header, and then click **Submit**.
9. *If you want to select specific interfaces to either start or stop Flow monitoring*, use the following procedure:

- a. Select **All** from the Show menu, and then click **+** next to the vendor name of your intended Flow source.
- b. Expand nodes, as necessary, to see currently monitored interfaces.
- c. Check or clear the **NetFlow** column to select interfaces as Flow sources by any of the following methods, and then click **Submit**.:
 - for individual interfaces
 - for any node to check or clear all interfaces on the selected node
 - for any device type to check or clear all devices of the selected types.

10. If you want to select specific CBQoS-enabled nodes to either start or stop CBQoS polling, use the following procedure:

- a. Select **All** from the Show menu.
- b. Click **+** next to the vendor name of your intended CBQoS-enabled device.
- c. Expand nodes and interfaces, as necessary, to see currently monitored interfaces, and then select interfaces by any of the following methods:
 - Check or clear, as appropriate, the **CBQoS** column for individual interfaces
 - Check or clear, as appropriate, the **CBQoS** column for any node to check or clear all interfaces on the selected node
 - Check or clear, as appropriate, the **CBQoS** column for any device type to check or clear all devices of the selected types.
- d. When you have checked or cleared all devices to poll, click **Submit**.

Configuring NetFlow Collector Services Ports

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

Notes:

- If you are employing a firewall on your NetFlow collector, all ports on which the NetFlow collector listens for Flow data should be listed as firewall exceptions for UDP communications.
- By default, Orion NTA listens for Flow data on port 2055, but some Flow-enabled devices, including some Nortel IPFIX-enabled devices, send Flow data on port 9995. For more information about requirements for IPFIX-enabled devices, see “NetFlow, IPFIX J-Flow, and sFlow Requirements” on page 7.

To configure NetFlow collector services:

1. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
2. Log in using a **User ID** with administrative privileges.
3. Click **Admin** in the Views menu bar.
4. Click **NTA Settings** in the Settings grouping of the Orion Website Administration page.

5. Click **NetFlow Collector Services**.
6. *If you want to add or reset a collection port*, type the new port number in the **Collection Port(s)** field of the collector that you want to edit.

Notes:

- Separate listed ports with a single comma, as in 2055,9995.
- A colored icon displays your collector status visually. Green indicates that the collector can receive Flow data, and red indicates that it can not. **Server Name** provides the network identification of your collector, and **Receiver Status** is a verbal statement of collector status.

7. *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.

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

Configuring NetFlow Types of Services

Orion NTA recognizes the Differentiated Services model of packet delivery prioritization. All Flow-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 Flow-enabled devices on your network by assigning each packet both a Differentiated Service class (1, 2, 3, or 4) and a packet-dropping precedence (low, medium, or high). NetFlow packets of the same class are grouped together. Differentiated Services 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 Flow-enabled devices, may be configured with DSCPs within Orion NTA, as shown in the following procedure.

To configure types of services for NetFlow packets:

1. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
2. Log in using a **User ID** with administrative privileges.
3. Click **Admin** in the Views menu bar.

4. Click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
5. Click **Types of Services**.
6. *If you want to edit an existing type of service*, click **Edit** at the end of each Type of Service Name listing, edit the assigned name, and then click **Update** on the same line.

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

Configuring the Orion NTA Top Talker Optimization

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

Most users should see an improvement in performance after configuring the Top Talker Optimization to capture only those Flows representing the top 95% of all network traffic. If you are monitoring a large number of Flow sources or interfaces, you may see more improved performance by setting this value lower than 95%.

Note: Enabling this option will result in the intentional loss of some data that might otherwise be recorded were this option set to 100%. However, the data that is lost corresponds to the least bandwidth-intensive conversations, and, in most environments, these low bandwidth conversations would not have been displayed in most Orion NTA resources anyway.

To configure the Orion NTA Top Talker Optimization:

1. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
2. Log in using a **User ID** with administrative privileges.
3. Click **Admin** in the Views menu bar, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
4. Under the Top Talker Optimization heading, provide an appropriate percentage value in the **Capture Flows representing the top XX % of total network traffic** field.
5. Click **Save** in the Top Talker Optimization section.

Configuring DNS and NetBIOS Resolution

To meet varied network requirements, Orion NTA provides options for both NetBIOS and DNS resolution of endpoint domain names. The following sections provide more information about each available type of domain name resolution.

Enabling NetBIOS Resolution

For networks where NetBIOS is the naming convention of preferred use, Orion NTA provides the option to resolve endpoint domain names using NetBIOS. The following procedure enables NetBIOS resolution in Orion NTA.

Note: Enabling NetBIOS resolution does not automatically disable DNS resolution of the same devices. For more information about configuring DNS resolution, see “Configuring DNS Resolution” on page 29.

To enable NetBIOS resolution:

1. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
2. Log in using a **User ID** with administrative privileges.
3. Click **Admin** in the Views menu bar.
4. Click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
5. Under the DNS and NetBIOS Resolution heading, check **Enable NetBIOS resolution of endpoints**.
6. Click **Save** in the DNS and NetBIOS Resolution section.

Configuring DNS Resolution

By default for new installations, Orion NTA resolves the domain names of all endpoints referenced in monitored Flows on demand. For most users, on demand DNS resolution optimizes overall performance. To meet your specific network monitoring needs, Orion NTA provides the following options for configuring DNS resolution:

- **Persistent** DNS resolution continuously resolves domain names for all devices involved in monitored Flows. For typically-sized networks, Orion NTA views may load more quickly as resolved domain names are retained, but database query times may increase as your Orion database is continuously queried.

Note: Top Domains resources and Orion reports that include DNS names require persistent domain name resolution.

- **On Demand** DNS resolution is the default option for new installations, and it is intended to assist users with larger networks. With this option, an endpoint domain name is only resolved when information about it is actually requested from the Orion database. Database query times may be improved with this option as queries are limited, but the load time for some endpoint-related resources may increase as Orion NTA waits for domain name resolution.

Warning: Top Domains resources and Orion reports that include DNS names require persistent domain name resolution, so they will not display DNS names if On Demand DNS resolution is enabled.

- Selecting **Disabled** turns DNS resolution off for the endpoints of flows monitored in Orion NTA. This is not generally recommended unless NetBIOS resolution already is enabled. For more information about enabling NetBIOS resolution, see “Enabling NetBIOS Resolution” on page 29.

Warning: If DNS resolution is disabled, all DNS information will be deleted from the database to improve database performance,

Orion NTA also allows you to configure the interval between DNS lookups. Orion NTA performs regular DNS lookups on all monitored devices. By default, if the domain of a monitored device resolves successfully, Orion NTA will not attempt another DNS lookup on the same device for 7 days. If the domain name of a monitored device does not resolve successfully, by default, Orion will attempt to resolve the same device again in 2 days.

The following procedure configures all DNS resolution options in Orion NTA.

To configure DNS resolution:

1. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
2. Log in using a **User ID** with administrative privileges.
3. Click **Admin** in the Views menu bar.
4. Click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
5. Under the DNS and NetBIOS Resolution heading, configure the resolution options in the following procedure.
 - a. Select the type of **DNS Resolution** you want Orion NTA to use.
 - b. Provide the **Default number of days to wait until next DNS lookup**.

Note: This value sets the interval on which endpoint domain names are refreshed in the Orion database if the persistent DNS resolution option is selected.

- c. Provide the **Default number of days to wait until next DNS lookup for unresolved IP addresses**.

Note: This value sets the interval on which Orion NTA makes an attempt to resolve domain names for unresolved endpoints in the Orion database if the persistent DNS resolution option is selected.

6. Click **Save** in the DNS and NetBIOS Resolution section.

Configuring IP Address Processing

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

Note: By default on new installations, Orion NTA is configured to spend no more than 15 minutes attempting to process any expired IP addresses. To conserve your processing and database resources, SolarWinds recommends that you maintain some reasonable time limit.

To configure IP address processing:

1. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
2. Log in using a **User ID** with administrative privileges.
3. Click **Admin** in the Views menu bar.
4. Click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
5. **If you want to edit the processing time period**, select **Custom number of minutes** under the DNS and NetBIOS Resolution heading, and then provide an appropriate number of minutes.
6. **If you want to delete flow records corresponding to expired IP addresses as assigned IP addresses expire**, remove the processing time limit by selecting **Never stop processing expired IP addresses** under the DNS and NetBIOS Resolution heading,

Note: SolarWinds recommends against removing the time limit for processing expired IP addresses as continuously deleting expired IP addresses may negatively affect Orion NTA performance. By default, Orion NTA sets a maximum period of 15 minutes for processing expired IP addresses to ensure that excessive processing resources are not drawn away from monitoring your network.

7. Click **Save** in the DNS and NetBIOS Resolution section.

Configuring Database Settings

Flow-enabled network devices are capable of generating very large amounts of traffic data in a relatively short period of time, overwhelming even a large database very quickly if you do not enact scheduled database maintenance. With its scheduled database maintenance features, Orion NTA gives you the ability to properly manage the size of your Orion database. The following procedure configures your Orion database maintenance settings.

Notes:

- Collect data for a day before adjusting these settings. You should then have an idea of the volume of data your network produces with NetFlow enabled.
- For more information about the Database Maintenance application that is packaged with Orion NPM, see “Database Maintenance” in the *SolarWinds Orion Network Performance Monitor Administrator Guide*.

To configure database maintenance and compression in Orion NTA:

1. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
2. Log in using a **User ID** with administrative privileges.
3. Click **Admin** in the Views menu bar.
4. Click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
5. Under the Database Settings heading, configure the database maintenance and compression options in the following procedure.

- a. Check **Enable Database Maintenance**.

Note: Due to the high volume of data provided by Flow-enabled devices, some level of database maintenance is generally recommended.

- b. Provide a time in the **Database maintenance is executed at** field.

Notes:

- This time should be within an established off-peak network usage window to minimize any potential disruption of required monitoring.
- This field can accept times entered in either 24-hour (HH:MM) or standard (H:MM AM/PM or HH:MM AM/PM) formats.

- c. Select a number of minutes in the **Keep uncompressed data for** field.

Note: The smallest uncompressed period that you can set is 15 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.

- d. 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.

- e. Select the frequency with which you want to **Delete expired flow data**.

Note: SolarWinds recommends deleting expired flow data **Once a day**.

- f. Select an interval on which you want to **Compress database and log files**.

Note: SolarWinds recommends that you compress database and log files once every ten days.

- g. *If you regularly search by endpoint*, you may consider checking the **Enable Accelerated Search by Endpoint** option to improve the speed with which search results are returned.

Note: Enabling this feature may significantly impact overall Orion NTA performance. Although search results may be provided more quickly, both database access and web console performance may decrease considerably as a result of enabling this option.

6. Click **Save** in the Database Settings section.

Configuring Charting and Graphing Settings

The Charting and Graphing Settings section of the NTA Settings view gives you the ability to enhance Orion NTA performance by enabling progressive charting and to configure options regarding the presentation of historical information in web console views and resources.

Enabling Progressive Charting

Due to the large amount of data that can be required to complete all charts on any web console view, the load times of some Orion NTA views can become significant. To help this condition, Orion NTA provides a progressive charting option that is enabled by default. The progressive charting option configures Orion NTA to draw charts incrementally, spreading the chart generation load over multiple database queries. For NetFlow installations monitoring and processing numerous data flows, progressive charting can minimize the amount of time you have to wait before actually seeing charted data. The following procedure opens

the Edit Charting and Graphing Settings page, where progressive charting may be enabled or disabled, as necessary.

To configure Orion NTA charting and graphing settings:

1. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
2. Log in using a **User ID** with administrative privileges.
3. Click **Admin** in the Views menu bar, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
4. **If you want to disable progressive charting**, clear **Enable progressive charting** under the Charting and Graphing Settings heading.

Note: Disabling progressive charting may significantly increase the amount of time it takes to load data into charts and graphs in web console views.
5. **If you want to enable progressive charting**, confirm that **Enable Progressive Charting** is checked under Charting and Graphing Settings.
6. Click **Save** in the Charting and Graphing Settings section.

Configuring Orion NTA Views and Resources

Orion NTA provides global options for both resource time periods and the type of percentages used in Top XX resources, as described in the following sections:

Configuring Top XX List Resource Percentages

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

For example, a given node (HOME) is communicating with 4 other endpoints (1, 2, 3, and 4). The following table details the two percentage types 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	Top 3
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 %

To configure the percentage type used for Top XX list resources:

1. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
2. Log in using a **User ID** with administrative privileges.
3. Click **Admin** in the Views menu bar, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
4. Under the Charting and Graphing Settings heading, select either **Calculate Absolute Percentages for Top XX Lists Percentages** or **Calculate Relative Percentages for Top XX Lists Percentages**, as appropriate.
5. Click **Save** in the Charting and Graphing Settings section.

Configuring Area Charts Display Units

The following options are available for displaying data in Orion NTA area charts:

- **Rate (Kbps)** provides the actual rate of data transfer, in kilobytes per second, corresponding to items displayed in a Top XX resource.
- **% of interface speed** displays the resource data as a percentage of the nominal total bandwidth of the selected interface.
Note: This option only displays when you are viewing ingress and egress data through a selected interface.
- **% of total traffic** displays the resource data as a percentage of the total traffic measured through the selected device.
- **Data transferred per interval** displays the amount of data corresponding to listed items transferred over a designated period of time.

Note: The default time period for Orion NTA resources is Last 15 Minutes.

The following procedure globally configures area chart display units from the NTA Settings view. Settings configured on the NTA Settings view apply globally to all Orion NTA area charts.

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

To globally configure Orion NTA area chart display units:

1. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
2. Log in using a **User ID** with administrative privileges.

3. Click **Admin** in the Views menu bar, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
4. Under the Charting and Graphing Settings heading, select appropriate units, as defined above, in the **Calculate *Display Units* for area charts** field.
5. Click **Save** in the Charting and Graphing Settings section.

Configuring Resource Default Time Periods

By default, all Orion NTA web console resources are configured to display data for the most recent 15 minutes. The time period for any Orion NTA resource may be configured either by clicking **Edit** in the header of any individual Orion NTA resource, or by globally setting the default time period for all Orion NTA web console resources in the Charting and Graphing Settings section of the NTA Settings view, as shown in the following procedure.

To globally configure the default resource time period:

1. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
2. Log in using a **User ID** with administrative privileges.
3. Click **Admin** in the Views menu bar.
4. Click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
5. Under the Charting and Graphing Settings heading, provide a value and appropriate time units in the **Default resource time period is** fields.
6. Click **Save** in the Charting and Graphing Settings section.

Configuring the Orion NTA View Refresh Rate

The refresh rate for Orion NTA views is configurable on the NTA Settings view, as shown in the following procedure.

To enable and configure the refresh rate for Orion NTA views:

1. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
2. Log in using a **User ID** with administrative privileges.
3. Click **Admin** in the Views menu bar.
4. Click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
5. Under the Charting and Graphing Settings heading, check **Enable automatic page refresh every X minutes**.

6. Provide an appropriate refresh interval in minutes.
7. Click **Save** in the Charting and Graphing Settings section.

Optimizing Orion NTA Performance

Even when you maintain your Orion and SQL servers on separate physical machines, in an otherwise standard Flow-monitoring environment, the volume of data generated by Flow-enabled devices can quickly overwhelm both the processing ability of your Orion server and the read/write capacity of your SQL Server. To guard against this possibility, SolarWinds recommends enabling both the Orion NTA Top Talker Optimization and On Demand DNS Resolution.

Note: Due to differences in network environments, results of these optimizations will vary from installation to installation.

For more information about the Top Talker Optimization, see “Configuring the Orion NTA Top Talker Optimization” on page 28. For more information about On Demand DNS Resolution, see “Configuring DNS Resolution” on page 29.

Configuring Flow Analysis Redundancy

If you have Orion NTA installed on an Orion Hot Standby server and your Flow-enabled device allows you to define two or more export targets, you can configure your environment to manually enable redundant flow analysis, as shown in the following procedure.

To configure basic failover for Orion NTA:

1. Either use SolarWinds Orion Network Configuration Manager (Orion NCM) or connect to the console of your device to configure your Flow-enabled device to send exported Flow data to both your Orion Hot Standby server and the primary Orion server.

Note: Not all devices support the ability to define two or more export targets. For more information, see your device documentation.

2. Configure an alert to notify you when your primary Orion NPM server is no longer responding. For more information, see “Creating and Configuring Advanced Alerts” in the *SolarWinds Orion Network Performance Monitor Administrator Guide*.
3. Confirm that Flow analysis is enabled on your Orion Hot Standby server by completing the following procedure.
 - a. Log on to your Orion Hot Standby server using an account with administrative privileges.
 - b. Click **Start > Administrative Tools > Services**.

Chapter 4

Creating NetFlow Traffic Analyzer Reports

Your Orion database can accumulate a great deal of Flow information that can be presented in a variety of formats using the Report Writer feature of Orion NPM. SolarWinds has developed Orion Report Writer to help you quickly and easily extract viewable data, including Flow statistics, from your Orion database.

Using Report Writer with Orion NTA

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, see “NetFlow-specific Predefined Reports” on page 39. In addition, as an Orion module, Orion NTA can also generate any of the predefined reports packaged with Orion NPM. For more information, see “Predefined Reports” in the *SolarWinds Orion Network Performance Monitor Administrator Guide*. For more information about Report Writer, see “Creating 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. You can also view most reports in the Orion Web Console by default. For more information, see “Customizing Views” in the *SolarWinds Orion Network Performance Monitor Administrator Guide*. To schedule automatic email reports for individual users or groups of users, open the Orion Report Scheduler by clicking **Start > All Programs > SolarWinds Orion > Alerting, reporting, and Mapping > Orion 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. The following reports are predefined for your Flow-enabled network devices.

Note: All reports with domain information require persistent DNS resolution. For more information, see “Configuring DNS and NetBIOS Resolution” on page 29.

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 100 Conversations – Last 24 Hours

Lists the endpoints, Flow source, and total traffic generated by each of the 100 most bandwidth-intensive conversations 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

Lists the 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 on your monitored network in the last 24 hours.

Top 50 Receivers by Unique Partners – Last 24 Hours

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

Top 50 Transmitters – Last 24 Hours

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

Top 50 Transmitter by Unique Partners – Last 24 Hours

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

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 Summary	Search
NetFlow Traffic Analysis Summary	Events
NetFlow Traffic Analysis Summary	Sources by % Utilization
NetFlow Traffic Analysis Summary	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 > All Programs > 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*.

Monitoring Traffic Flow Directions

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

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

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 you are using for NetFlow traffic analysis.
2. Click **Start > All Programs > 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.
5. Click **Manage Views** in the Admin menu on the left.
6. Select the view that you want to limit, and then click **Edit**.
7. Click **Edit** below the View Limitation heading.
8. Select the type of limitation that you want to apply.
9. Click **Continue**.
10. Select the appropriate limitations.
11. 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:

- 2-D or 3-D 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.

Notes:

- Click **Refresh** at any time to review changes that you have made.
- Depending on the type of chart displayed, some resources may not provide all of the options described in the following sections.

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**.

Customizing Individual 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 listed in resource tables. 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, and relative percentages for each item are calculated in terms of the total number of items displayed in the selected resource. For more information about global options for configuring Top XX resources, see “Configuring Top XX List Resource Percentages” on page 34.

Depending on the access rights granted to the user viewing a Top XX resource, Orion NTA also provides the following options:

- Administrators may customize a selected Top XX resource for all web console users. For more information, see “Customizing for All Users (Administrators Only)” on page 47.
- Non-administrative users may still customize any Top XX resource for the duration of the current browser session. For more information, see “Customizing for the Current Session (All Users)” on page 48.

Customizing for All Users (Administrators Only)

The following procedure presents the custom options available to administrators for configuring Top XX resources for all web console users.

Note: Top XX Domains resources are not available if On Demand DNS resolution is enabled. Only users with administrative privileges may configure this setting. For more information, see “Configuring DNS Resolution” on page 29.

To administratively customize Top XX resource titles and chart types:

1. Click **Edit** in the Top XX resource title bar.
2. Provide the number of items you want to display in the **Maximum number of items to display** field.
3. Select either **Chart** or **No Chart** as the **Resource Style**.
4. **If you have selected Chart as your Resource Style**, 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.

5. **If you have selected the Area Chart style**, select one of the following types of area charts for use in the selected resource
 - **Stack Area** is an area chart where multiple series of data are stacked vertically. If there is only one series in your chart, the stacked area chart displays the same as an area chart.
 - **Stack Spline Area** is an area chart that stacks multiple series of data vertically and plots a fitted curve through all data points in the series.
 - **Stack Line** is simply a Stack Area chart that does not fill the areas defined by each stacked series. Data series are stacked at each point of measurement marked on the x-axis.
 - **Line Chart** is a chart created using lines to connect series data points. All series use the x-axis as a common baseline
 - **Spline** plots a fitted curve through all series data points in a line chart.
6. Select one of the **Data Units** types to use, as available:
 - **Rate (Kbps)** creates a chart displaying historical traffic rate data for selected Flow-enabled nodes and interfaces.
 - **% of interface speed** is only available for Top XX resources presenting interface traffic data. This option creates a chart showing how bandwidth is allocated across the elements listed in the Top XX resource.
 - **% of total traffic** creates a chart showing how the total traffic over the selected node or interface is distributed across the elements listed in the Top XX resource. This is the default data unit type.
 - **Data transferred per time interval** creates a chart displaying the actual amount of data transferred over the selected node or interface. Data volume is measured over successive time intervals.
7. Click **Submit**.

Customizing for the Current Session (All Users)

All users capable of viewing Top XX resources in the web console can customize individual Top XX resources for the duration of the current session, as shown in the following procedure.

To customize a Top XX resource for the current session:

1. Click **Chart Styles** in the Top XX resource title bar, and then select from the following options:
 - **Area Chart** presents a historical view of your data as represented by areas calculated at past polling times.

- **2D Pie Chart** presents a “flat” view of your data
 - **3D Pie Chart**
2. **If you have selected the Area Chart type**, click **Data Units** to select one of the following data unit types for use in the selected resource
- **Rate (Kbps)** creates a chart displaying historical traffic rate data for selected Flow-enabled nodes and interfaces.
 - **% of interface speed** is only available for Top XX resources presenting interface traffic data. This option creates a chart showing how bandwidth is allocated across the elements listed in the Top XX resource.
 - **% of total traffic** creates a chart showing how the total traffic over the selected node or interface is distributed across the elements listed in the Top XX resource. This is the default data unit type.
 - **Data transferred per interval** creates a chart displaying the actual amount of data transferred over the selected node or interface. Data volume is measured over successive time intervals.

Using the NetFlow Traffic View Builder

You can create custom traffic views directly from the NetFlow Traffic Analysis Summary view, using the Traffic View Builder resource. These custom filters allow you to view specific statistics about your entire network and its devices without having to navigate through the web console a single device view at a time. You can configure your custom traffic view to include devices, applications, time periods, and more, all from one configuration page, as shown in the following procedure.

To create a custom NetFlow traffic view with the Traffic View Builder:

1. Log in to the Orion Web Console as an administrator.
2. Click **NetFlow Traffic Analysis** in the Modules menu bar.
3. In the Traffic View Builder resource, select the type of custom, filtered view you want to create, and then click **Build**.

Note: The Traffic View Builder resource is available on the NetFlow Traffic Analysis Summary view, but it is also available for inclusion on any other Orion Web Console view. For more information, see “Customizing Views” in the *SolarWinds Orion Network Performance Monitor Administrator Guide*.

4. Select the appropriate network characteristics and the time period for which you want to view filtered data.

- 5. If filter options are provided**, complete the following steps to filter your custom traffic view:

Note: Repeat the following procedure for each filter type you want to use to define your custom traffic view.

- Click **+** next to any filter type you want to apply.
- If you want to select items to exclude from your view**, check **Exclude selected items**.
- Select an item to define your filter appropriately, and then click **Add**.
Note: Repeat this step until you have completely defined your filter type.
- If you want to delete a selected item**, click **X** next to the item to delete.

- Click **Submit**.

- If you want to save your custom view for future reference**, click **Bookmark This Page** at the top of your new view.

Note: Bookmarked views are only saved locally to the browser on the computer on which you are viewing the web console.

Interacting with the thwack User Community

By default, Orion NTA provides the thwack Recent NetFlow Posts resource on the NetFlow Traffic Analysis Summary view. This resource shows the most recent Orion NTA-related posts that have been submitted to thwack, the online SolarWinds user community. Clicking any post title listed in the resource opens the associated post in the Orion NTA forum on thwack.

Performing an Immediate Hostname Lookup

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

Note: The hostname is also retrieved on a scheduled basis. For more information, see “Configuring DNS and NetBIOS Resolution” on page 29.

Viewing Class-based Quality of Service (CBQoS) Data

CBQoS is a proprietary, SNMP-based, Cisco technology available on selected Cisco devices that gives you the ability to prioritize and manage traffic on your network. Using policy maps, the different types of traffic on your network are categorized and then given a priority. Based on respectively assigned priorities, only specified amounts of selected traffic types are allowed through designated, CBQoS-enabled devices. For example, you could define a policy map in which only 5 percent of the total traffic over a selected interface may be attributed to

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

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

Note: Orion NTA does not currently provide a CBQoS configuration capability, but any node that managed by Orion NPM may be polled for CBQoS information. If SNMP polls of the MIB for monitored devices are unsuccessful for CBQoS OIDs, CBQoS resources are automatically hidden because they are empty. For more information about enabling CBQoS polling for monitored devices, see “Managing Flow Sources and CBQoS-enabled Devices” on page 24.

CBQoS Drops

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

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

CBQoS Policy Details

If it is included on a NetFlow Interface Details view, the CBQoS Policy Details resource provides both a graph and a table reporting the amount of traffic corresponding to defined classes that has passed over the viewed interface in both the hour and the 24 hours prior to the currently viewed time period.

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

CBQoS Post-Policy Class Map

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

If it is included on the CBQoS Details view, the CBQoS Post-Policy Class Map resource provides both a graph and a table detailing both the average

and the most recently polled amount of traffic corresponding to the selected CBQoS policy class passing through the viewed interface resulting from the application of policy maps on the viewed interface.

CBQoS Pre-Policy Class Map

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

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

Chapter 6

Working with Orion NTA

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 applications 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

Managing Software Licenses

SolarWinds License Manager provides you with the following capabilities:

- Easily migrate licenses from one computer to another without contacting SolarWinds Customer Service.
- Upgrade from one license level to another, including from an evaluation-level license to a production-level license.

Requirements

The following requirements must be satisfied to successfully install and run SolarWinds License Manager.

	Need
Install Location	SolarWinds License Manager must be installed on the same computer as the products to be migrated.
Connectivity	Computer must have access to the internet.
.net Framework	3.0 or later, links to the framework are included in the installation
Operating System	Windows Server 2008 (32-bit & 64-bit) Windows Server 2003 SP1 and higher, including R2 (32-bit & 64-bit) Windows 2000 SP4 with Update Rollup 1 or later Windows XP Windows Vista Note: If the machine time is off 24 hours in either direction from the Greenwich Mean Time, you will be unable to reset licenses. Time zone settings do not affect and do not cause this issue.
Browser	Internet Explorer 6 or later Firefox 2.0 or later

Installing License Manager

Install License Manager on the computer from which you are uninstalling currently licensed products.

To install License Manager:

1. Click **Start > All Programs > SolarWinds > SolarWinds License Manager Setup**.
2. **If the SolarWinds License Manager Setup application is not available**, complete the following procedure to install License Manager.
 - a. Navigate to <ftp://ftp.solarwinds.net/LicenseManager/LicenseManager.zip>.
 - b. Save LicenseManager.zip to an appropriate location.

- c. Extract LicenseManager.zip.
 - d. Open the extracted License Manager folder, and then launch the License Manager installer, LicenseManager.exe.
3. Click **I Accept** to accept the terms of and End User License Agreement.
4. *If you are prompted to install SolarWinds License Manager*, click **Install**.

Using License Manager

License Manager must be running on the computer where the currently licensed SolarWinds product is installed. The following sections provide instructions for managing SolarWinds licenses:

- Deactivating Currently Installed Licenses
- Upgrading Currently Installed Licenses
- Activating Evaluation Licenses

Deactivating Currently Installed Licenses

The following procedure deactivates a currently installed license.

To deactivate currently installed licenses:

1. Click **Start > All Programs > SolarWinds > SolarWinds License Manager**.
2. Check the products you want to deactivate on this computer, and then
3. Click **Deactivate**.
4. Confirm deactivation of the selected application by clicking **Deactivate** again.
5. Click **Close** to complete license deactivation.

Note: Deactivated licenses are now available for activation on a new computer.

When you have successfully deactivated your products, log on to the computer on which you want to install your products and begin the installation procedure. When asked to specify your licenses, provide the appropriate information. The license you have deactivated is available for assignment to the new installation.

Upgrading Currently Installed Licenses

The following procedure upgrades a currently installed license.

To upgrade a currently installed licenses:

1. Click **Start > All Programs > SolarWinds > SolarWinds License Manager**.
2. Click Upgrade in the Action column next to the products for which you want to upgrade the license on this computer.
3. Complete the Activation wizard to upgrade your license.

Activating Evaluation Licenses

The following procedure upgrades the license of an evaluation installation to an activated production license.

To activate a currently installed evaluation and license the product:

1. Click **Start > All Programs > SolarWinds > SolarWinds License Manager**.
2. Click Activate in the Action column next to the products you want to register as licensed products on this computer.
3. Complete the Activation wizard to upgrade your license.

Appendix B

Device Configuration Examples

The following examples of device configurations can be used to help configure your devices to send flow data to Orion NetFlow Traffic Analyzer.

Cisco NetFlow Configuration

The port used for NetFlow traffic is specified in the configuration of your Flow-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 2055  
!
```

The `ip flow-export destination` value must reflect the IP address of your Orion NPM server. This value also contains the port number (2055) 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 and version 9. For more information about NetFlow version 5 or 9, 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.

Extreme sFlow Configuration

To support Extreme devices, you must configure the device using the following configuration template.

```
enable sflow

configure sflow config agent 10.199.5.10

configure sflow collector 192.168.72.67 port 2055

configure sflow sample-rate 128

configure sflow poll-interval 30

configure sflow backoff-threshold 50

enable sflow backoff-threshold

enable sflow ports all
```

The `sFlow collector` value must reflect the IP address of your Orion NPM server. This value also contains the port number (2055) that is required in this step.

Foundry sFlow Configuration

To support Foundry devices, you must configure the device using the following configuration template.

Note: Ensure your Foundry device supports sFlow version 5.

```
config> int e 1/1 to 4/48

interface> sflow forwarding

config> sflow destination 10.199.1.199 2055

config> sflow sample 128

config> sflow polling-interval 30

config> sflow enable
```

The `sFlow destination` value must reflect the IP address of your Orion NPM server. This value also contains the port number (2055) that is required in this step.

HP sFlow Configuration

To support HP devices, you must configure the device using the following configuration template.

Note: This will not show up in the command line interface. Because of this it will not return if the switch is reset.

```
setmib sFlowRcvrAddress.1 -o 0AC70199
setmib sFlowRcvrPort.1 -i 6343
setmib sFlowRcvrOwner.1 -D net sFlowRcvrTimeout.1 -i 100000000
setmib 1.3.6.1.4.1.14706.1.1.5.1.4.11.1.3.6.1.2.1.2.2.1.1.1.1 -i 37
setmib 1.3.6.1.4.1.14706.1.1.5.1.3.11.1.3.6.1.2.1.2.2.1.1.1.1 -i 1
setmib 1.3.6.1.4.1.14706.1.1.6.1.4.11.1.3.6.1.2.1.2.2.1.1.53.1 -i 8
setmib 1.3.6.1.4.1.14706.1.1.6.1.3.11.1.3.6.1.2.1.2.2.1.1.53.1 -i 1
```

Where 0AC70199 is the IP address of your Orion NPM server in hex format. Line 4 sets the sample rate. Line 5 enables sFlow. Line 6 sets the polling interval, and line 7 enables polling.

Index

Index

A

- absolute percentages 47
- Accelerated Search 37
- additional poller
 - installing Orion NTA 8
- applications
 - configuration 20
- automatic source addition 18

C

- CBQoS 50
 - Drops 51
 - Policy Details 51
 - Post-Policy Class Map 51
 - Pre-Policy Class Map 52
 - resources 50

charts

- configuration 33
- customizing 46
- editing 45
- sample intervals 46
- size 46
- time periods 46
- titles 46

collection ports 26

- collector services
 - configuration 26

compression

- configuration 32
- description 18

configuration

- device examples 61
- Custom Property Editor 39
- custom views 49

D

- data collection
 - intervals 14
- data compression
 - configuration 32
 - description 18

deleting

- Flow source 16

devices

- adding to NetFlow Traffic Analyzer 14, 24
- adding to Orion 13
- configuration examples 61
- data collection intervals 14
- differentiated service code point
 - configuration 27
- DNS resolution
 - configuration 29
 - on demand 29
 - persistent 29
- documentation iv
- DSCP See differentiated service code point

E

- egress 44
- examples 53

F

- failover
 - configuration 37

features 3

Flow sources

- automatic addition 18

Flows

- from unmanaged interfaces 19
- unmonitored ports 19

G

- getting started 13
- graphs
 - configuration 33

H

- hostname lookup 50

- I**
 - ingress 44
 - installing 5
 - on additional pollers 8
 - procedure 8
 - requirements 5
 - interfaces
 - adding to NetFlow Traffic Analyzer 14, 24
 - adding to Orion 13
 - data collection intervals 14
 - unmanaged 19
 - IP address groups
 - selection 22
 - IPFIX
 - requirements 7
- J**
 - J-Flow
 - requirements 7
- L**
 - License Manager 57
 - activating evaluation licenses 59
 - deactivating licenses 58
 - installation 57
 - requirements 57
 - upgrading licenses 59
 - using 58
 - licensing 5
 - activating evaluation licenses 59
 - deactivating licenses 58
 - evaluation 9
 - managing licenses 57
 - software license key 9
 - upgrading licenses 59
- lookup 50
- M**
 - monitored ports
 - configuration 20
 - monitoring
 - IP address groups 22
 - protocols 24
- N**
 - NetBIOS resolution
 - configuration 29
 - NetFlow
 - requirements 7
 - NetFlow Collector Services *See* collector services
 - NetFlow source
 - deleting 16
 - nodes *See* devices
- O**
 - optimization
 - top talkers 28
- Orion
 - Custom Property Editor *See* Custom Property Editor
 - documentation iv
 - Report Writer *See* Report Writer
- Orion NTA
 - features 3
 - introduction 1
 - why install? 1
- P**
 - pages
 - refresh rate 36
 - per hop behavior
 - configuration 27
 - percentages
 - absolute 47
 - relative 47
 - Top XX resources 47
 - performance optimization 37
 - PHB *See* per hop behavior
 - policy maps 50
 - polling engine
 - baseline 14
 - port
 - 1 20
 - unmonitored traffic 20
 - ports
 - collection 26
 - unmonitored 19
 - ports, monitored
 - configuration 20
 - ports, NetFlow traffic
 - Cisco configuration 61

- ports, sFlow traffic
 - Extreme configuration 62
 - Foundry configuration 62
 - HP configuration 63
- progressive charting 33
- protocols
 - configuration 20
 - monitoring 24
- Q**
- QoS
 - class-based 50
- R**
- refresh rate 36
- relative percentages 47
- Report Scheduler 39
- Report Writer
 - creating reports 39
 - using custom properties 39
- reports *See also* Report Writer
 - creating 39
 - Flow 39
 - using custom properties 39
- requirements 5
 - Flow sources 7
 - hardware 6
 - software 6
 - virtual machine 7
- resources
 - configuration 34
 - percentage calculation 34
 - time period 34
 - Top XX 47
- S**
- sFlow
 - requirements 7
- software license key
 - activation 9
 - activation with Internet access 9
 - activation without Internet access 10
 - evaluation 9
- SolarWinds
 - contacting iii
- sources
 - automatic addition 18
- T**
- thwack 50
- time period
 - resource default 34
- top talker optimization 28
- top XX lists
 - percentage calculation 34
- traffic
 - unmonitored port 20
- Traffic View Builder 49
- types of service
 - configuration 27
- U**
- unmonitored traffic 20
- use cases 53
- V**
- views
 - adding resources 43
 - available resources 43
 - creating limitations 45
 - custom 49
 - customizing 43
 - NetFlow Traffic Analysis
 - Summary 17
 - refresh rate 36
 - setting default 17
 - traffic flow directions 44
- volumes
 - data collection intervals 14

