SolarWinds Orion

NetFlow Traffic Analyzer
Administrator Guide

solarwinds®

ORION NETFLOW TRAFFIC
ANALYZER

About SolarWinds

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

Contacting SolarWinds

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

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

Conventions

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

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

Orion NetFlow Traffic Analyzer Documentation Library

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

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

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

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

Contents

Chapter 1

Chapter 2

Chapter 3

Chapter 6

Chapter 7

Appendix A

Appendix B

Index

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

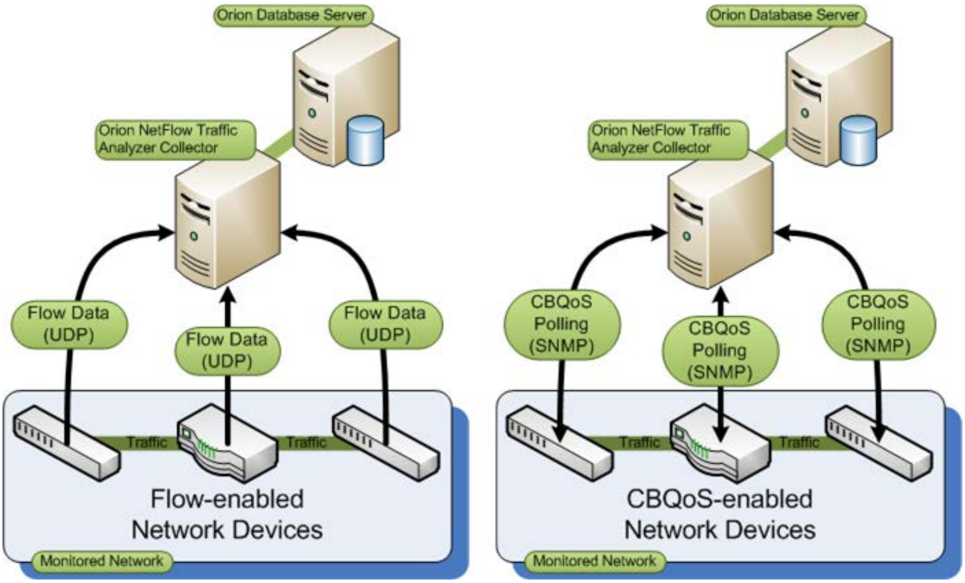
These monitoring capabilities, along with the customizable Orion Web Console and reporting engines, make Orion NTA the easiest choice you will make involving your Flow monitoring needs.

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 [this SolarWinds technical reference](#).



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:

Orion Alerts Integration

Orion NTA automatically adds top talker information to Orion interface utilization alerts. You can navigate directly to NTA interface details from messages in the Orion Events resource. For more information see Configuring NetFlow Advanced Alerts.

Customizable rate-based charts

Stacked area charts and 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.

Global Flow Direction Settings

Orion NTA now provides flow direction settings that pertain to all resources on relevant views. All global settings can be manually over-ridden at the resource level.

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.

This release enhances CBQoS monitoring with three new Orion Advanced Alerts (for Pre-Policy, Post-Policy, Drop thresholds that you set), and seven new historical reports (on Pre-Policy, Post-Policy, and Drop events).

Improved availability and performance

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

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

Analytical capacity planning

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

This release includes reports on Top Conversations with Applications and Top 50 Endpoints; and resources showing Top Traffic Sources and Destinations by Domain, and Top IP Address Group Conversations.

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.

Unknown traffic page as aid in resolving sources

The page includes a list of the last 200 events in which flow traffic was received but was not associated with a NetFlow source.

In creating an item on the list, the Orion NTA software tells you that the NetFlow receiver (node name) to which the flow is coming and the IP address from which it is coming.

Support for Huawei NetStream

The Orion NTA can collect and process NetStream data that meet the requirements of NetFlow v5. Packets can be exported either stream-by-stream as an aggregate. As with NetFlow, NetStream packets are transferred via UDP.

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.

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 Orion NTA 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.

Hardware	Requirements
CPU	3GHz or faster, dual processors with dual cores
RAM	3GB or more
Hard Drive Space	**Orion NTA server:** 5GB or more, RAID 0, 1, 0+1, or 1+0. **SQL Server:** 5GB or more, RAID 0, 1, 0+1, or 1+0 on at least 6 spindles. In terms of data storage capacity, as a guideline, assuming default data retention periods, you should plan to store about 2MB(s) for every flow received. So, for example, for every 1000 flows you intend to collect, you should allocate at least 2GB of storage capacity. 5000 flows would require 10GB of storage capacity; and so on. **Warning:** Other RAID or SAN configurations are not recommended.
NetFlow Devices	Cisco devices exporting NetFlow version 5 or 9 and supporting SNMP **Note:** Orion NTA only recognizes NetFlow version 9 templates that include all fields included in the NetFlow version 5 template.
NetStream Devices	Huawei devices exporting NetStream version 5 or 9 and supporting SNMP **Note:** Orion NTA only recognizes NetStream version 9 templates that include all fields included in NetStream version 5.
IPFIX Devices	Network devices exporting IPFIX and supporting SNMP.
J-Flow Devices	Network devices exporting J-Flow and supporting SNMP.
sFlow Devices	Network devices exporting sFlow versions 2, 4, and 5 and supporting SNMP.

- **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.

For more information about Flows supported by Orion NTA, see NetFlow, IPFIX, J-Flow, NetStream, and sFlow Requirements on page 9.

Software Requirements

Operating system and SQL Server Requirements for the current Orion NTA version are the same as for Orion NPM 10.3, as detailed in the Requirements section of the *SolarWinds Orion Network Performance Monitor Administrator Guide*, with the following additions:

- Orion NTA 3.10.0 can be installed to SQL Server 2012.
- 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 8 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, NetStream, and sFlow Requirements

Orion NTA supports these flow versions: NetFlow versions 5 and 9 (with an appropriate template that includes all required fields); IPFIX; Juniper J-Flow; NetStream versions 5 and 9; sFlow versions 2, 4, and 5.

Most Flow-enabled devices use a set of static templates to which exported flows conform. Any NetFlow, IPFIX, J-Flow, NetStream, 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.

Notes:

- 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.
- Time zone settings of the Web server (IIS), database, and SolarWinds Information Service must all be the same. Therefore, if you change the time zone of the Orion server, you must restart all Orion services, and you must change the time zone on the database server (as needed) to match.

- A single Orion NTA installer contains binaries for the main poller, an additional poller, and additional web interfaces. The Orion NTA installer determines type of installation automatically to match already present Orion NPM type.

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 10.3 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 3.8 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.

   Note: After initial installation and configuration completes, the NetFlow Service re-indexes the NTA NetFlowSummary1, NetFlowSummary2, and NetFlowSummary3 database tables. Do not restart this service during this time. If you cancel the upgrade before the reindexing finishes, your NetFlowSummary tables may become unusable.

   While re-indexing occurs, Orion NTA neither collects nor processes NetFlow data from network devices; and all NetFlow related resources on the Orion web console remain empty of statistics. However, during this time your Orion NPM software and its access to the Orion database function normally.

   The NetFlowService writes an event to the **Last Events** list when it finishes reindexing each NetFlowSummary table.

Time to re-index your database depends on the size of NTA summary tables. As a rule, indexing takes 30 minutes per 10GB of data in the tables.

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 installation completes, click **Finish** to exit the wizard.

Activating Your Orion NTA License

After installing Orion NTA using the 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 Configuration Wizard on page 14.

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 Configuration Wizard on page 14.

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 Configuration Wizard on page 14.

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 Setting up Network Devices to Export NetFlow Data and Adding Flow-enabled Devices and Interfaces.

Upgrading Orion NTA

Complete the following procedure when you are upgrading Orion NTA from a previous version or upgrading the licensed number of elements you can monitor.

Notes:

- SolarWinds does not currently support upgrades from one locale to another. If you want to upgrade your SolarWinds installation to use a new locale, you must complete a clean SolarWinds installation using the new locale.
- SolarWinds recommends that you backup your database before any upgrade. For more information about creating database backups, see Creating Database Backups.
- While it is being upgraded, your Orion polling engine temporarily shuts down which may result in polling data loss. SolarWinds recommends that you perform upgrades during off‑peak hours of network usage to minimize the impact of this temporary polling stoppage.
- Discovery profiles from older Orion NPM versions are not retained through upgrades. If you want to retain a discovery profile, prior to starting your upgrade, externally record the configuration of the profiles you want to retain.

If your currently installed version of Orion NPM is older than version 7.8.5, you must upgrade to Orion NPM 7.8.5.

If you currently have Orion NPM version 7.8.5 through 8.5 installed, you must upgrade to Orion NPM 8.5.1.

If you currently have Orion NPM version 8.5.1, upgrade to version 9.1.

If you currently have Orion NPM version 9.0 through 9.5.1, you must upgrade to version 10.0 before upgrading to the current version.

Specific instructions for completing an upgrade are available in the SolarWinds Customer Portal. For more information about upgrading Orion NTA, particularly if you are upgrading an NTA installation that includes other Orion modules, log in to your SolarWinds Customer Portal at www.solarwinds.com/customerportal/, click License Management, and then click **Upgrade Instructions** under the license listing of any Orion product.

The following procedure completes an NTA upgrade.

To upgrade Orion Network Performance Monitor:

1. ***If you are using more than one polling engine to collect network information***, shut down all polling engines before continuing.
2. Using the local administrator account, log on to the computer on which you want to upgrade Orion NTA.
3. If you downloaded the product from the SolarWinds website, navigate to your download location and then launch the executable.
4. Review the Welcome text, and then click **Next**.
5. Orion automatically detects the previous installation. When prompted to upgrade the current installation, click Next.

   Note: All customizations, including web console settings, are preserved.
6. Accept the terms of the license agreement, and then click **Next**.
7. Confirm the current installation settings, and then click **Next** on the Start Copying Files window.
8. Provide required information on the Install Software License Key window.

   Note: You need your customer ID and password to successfully install the key. For more information, see Activating Your Orion NTA License on page 12.
9. Click **Continue**, and then click Continue again when the license is installed.
10. Review the Upgrade Reminder, and then click **Next**.
11. Click **Finish** on the InstallShield Wizard Complete window.
12. Complete the Configuration Wizard. For more information, see Completing the Orion Configuration Wizard on page 14.

Installing a Localized Version of Orion NTA

Please consider the following when installing a localized Orion NTA 3.10.0 version:

- Direct upgrades from Orion NTA 3.9 and older (English) to Orion NTA 3.10.0 (Japanese) are not supported. If you want to use a Japanese-localized version of Orion NTA, you must perform a completely clean installation of both Orion NPM 10.3 (and above) and Orion NTA 3.10.0. This clean installation should include a completely new database for your localized Japanese installation.
- **Note:** Orion NPM must be installed as a localized installation before you can install a localized version of Orion NTA 3.10.0.
- Alerts and report filters created in older versions of Orion NTA and other SolarWinds products using properties under one locale setting do not function as intended under changed locales. The only resolution at this time is to reconfigure these alerts and report filters after upgrading to Orion NTA.

Terminology

When referring to the Orion NTA 3.10.0 localized content, SolarWinds documentation uses the following terms:

- **Primary Locale** – The locale selected when installing Orion NTA. Once selected, you cannot change the Primary Locale without uninstalling and reinstalling Orion NTA.
- **User Locale** – The locale selected for use in your browser.
- **Operating System (OS) Locale** – The locale configured for your local operating system.
- **Regional Settings** – Settings to configure how times, dates, and numbers are formatted for display.

Notes:

SolarWinds does not currently support the direct upgrade of an Orion NTA installation with one Primary Locale to an Orion NTA 3.10.0 installation with a different Primary Locale:

- The SolarWinds database will remain in English unless you create a new one to use with your installation.
- Though it is possible to configure the User Locale so that it is different from the Primary Locale, data stored in the database, when presented in the web console, will display in accordance with the Primary Locale and not in accordance with the User Locale. As a result, resource names, object details, and monitoring events display in the web console under the Primary Locale.

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.

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 on page 181.

For Orion NTA to correctly receive and process NetFlow data, you must complete these two tasks:

- Setup your network devices to export Flow data.
- See the section “Setting up Network Devices to Export Flow Data“ in the chapter on Key and Critical Tasks for detailed information on setting up and verifying export of data from network devices.
- Add your network devices to those monitored in Orion NPM as described in Adding Flow-enabled Devices and Interfaces.

Adding Flow-enabled Devices and Interfaces

For Orion NTA to collect Flow data from your network devices you must first specify the Orion NTA server as a target to which each device exports its data. See the section “Setting up Network Devices to Export Flow Data“ in Key and Critical Tasks for detailed information on setting up network devices to export data to Orion NTA.

Note: Only SNMP-capable nodes whose interfaces were discovered by Orion NPM can be added as NetFlow sources.

For Orion NTA to analyze network traffic based on collected Flow data, each Flow-enabled network interface regarding 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 21.

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 10.2 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** in the Modules menu bar and view the **NetFlow Sources** resources to confirm the addition of all Flow sources on your network.

   Note: Only SNMP-capable nodes whose interfaces were discovered by Orion NPM can be added as NetFlow sources.

   For more information, see AddingFlowSources and CBQoS-enabled Devices on page 21.

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 30.

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, and the network devices have been configured to export Flow data, the 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 the section Enabling Automatic Addition Flow Sources on page 25.

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.

Notes:

- If you are using NetFlow version 9, confirm that the template you are using includes all fields included in NetFlow version 5 PDUs.
- Since some devices have a default template time-out rate of 30 minutes, and Orion NTA only raises an event every 15 minutes when NetFlow V9 flows arrive without a usable template, you should configure your device to export the appropriate template every 1 minute, so that the version 9 flows show up in NTA without delay.
- For more information, see NetFlow, IPFIX, J-Flow.and sFlow Requirements on page 9.
- Only SNMP nodes—in essence, an interface on the node—can be added as a NetFlow Source.

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 to Orion Web Console,*** click the **NetFlow** tab.
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 24.

   a. Click **Settings** in the top right corner of the Web Console.
   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 the section “Enabling the Automatic Addition of Flow Sources”.
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 **Settings** in the top right corner of the Orion Web Console.
   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 Orion Web Console,*** click **NetFlow Traffic Analyzer** in the Modules toolbar.
3. Click **Settings** in the top right corner of the Web Console, 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 **Settings** in the top right corner of the Web Console.
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** 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 42.

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 a maximum of 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 3 days, 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 NTA 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 **Settings** in the top right corner of the Web Console.
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 for new installations, Orion NTA retains all Flow data provided by NetFlow sources on your network, including Flow data for ports that you are not actively monitoring.

A benefit of having this data is that, should you see a significant percentage of unmonitored traffic in your Top XX Application resource, you can expand the tree to drill down into the interface level; by clicking the **Monitor Port** button, you can begin to track this traffic by port.

However, if you want to save space in your database by disabling this automatic feature and discard data from unmonitored ports, simply clear **Enable data retention for traffic on unmonitored ports**.

For more information about unmonitored ports in Orion NTA, see Configuring Monitored Ports and Applications on page 30.

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 **Settings** in the top right corner of the Web Console.
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 Flow Monitoring 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.

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

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 **Settings** in the top right corner of the Web Console.
4. Click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
5. Check **Allow monitoring of flows from unmanaged interfaces**.

6. Click **Allow matching nodes by another IP Address** to allow Orion NTA to attempt associating unknown traffic with non-primary IP addresses on a currently monitored Orion NPM node.
7. Click **Save**.
8. Click **NETFLOW** on the main toolbar.

   If you currently have unknown traffic events then a link—**Show unknown traffic events**—is posted in the banner area. If there is no such message in the banner area then you currently have no unknown traffic events
9. ***If you see the message Show unknown traffic events*** in the banner area, click that message.

   The Unknown Traffic Events page opens. The list includes the last 200 events in which flow traffic was received but was not associated with a Netflow source.

   In creating an item on the list, the Orion NTA software tells you that the NetFlow receiver (node name) to which the flow is coming and the IP address from which it is coming. The entry looks like this:

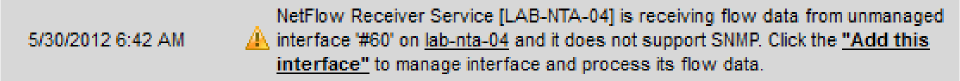
   ```
   NetFlow Receiver Service [LAB-NTA-04] is receiving NetFlow data
   from an unmanaged interface on 10.199.4.3.. The NetFlow data
   will be discarded. Use the "Edit this device" link or Orion
   node management to manage interface '#123' and process its
   NetFlow data.
   ```
10. For each item in the Last 200 Unknown Traffic Events list, click “**Edit this device”**.

    The software navigates into the List Resources screen of the Add Node wizard.
11. Make sure **All Interfaces** is checked and click **Submit**. The software navigates into the Manage Nodes resource.
12. Return to the Last 200 Events screen and repeat steps 9 and 10.
13. When you are finished with items in the Last 200 Events list, click **Refresh Events** to refresh the list, along with the page.

    Note: Unresolved events return to the list if they have not been successfully resolved. This allows you to test your efforts to resolve unresolved traffic items.
14. Go to **NETFLOW** on the main toolbar.You should no longer see a banner indication regarding unknown flow traffic. If you do, click the message and re-examine the Last 200 Unknown Traffic Events list again, repeating the steps in these procedures as needed to associate the flow traffic with the appropriate NPM interface.

Enabling Flow Monitoring from Unmanageable Interfaces

When NTA receives a data flow from an unmanageable interface, the event displays in NTA's Traffic Analyzer pane. The following event is an example of an unmanageable interface.

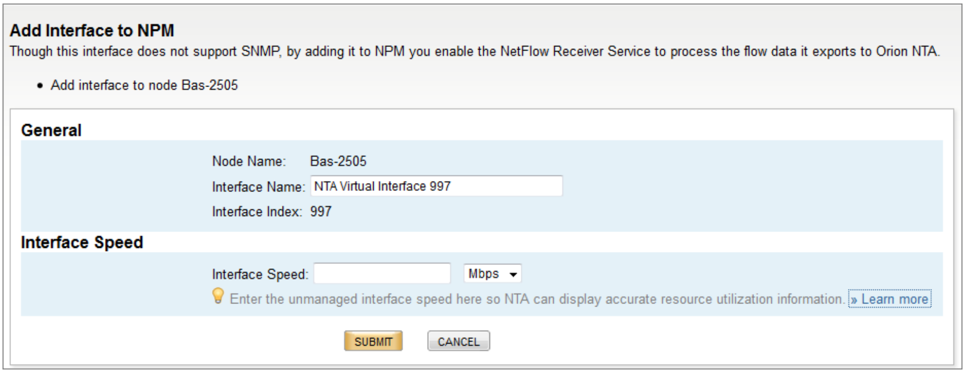


5/30/2012 6:42 AM ⚠ NetFlow Receiver Service [LAB-NTA-04] is receiving flow data from unmanaged interface '#60' on lab-nta-04 and it does not support SNMP. Click the **"Add this interface"** to manage interface and process its flow data.

Though this interface does not support SNMP, by adding it to NPM, you enable the NetFlow Receiver Service to process the flow data it exports to NTA. If you do not add this interface, NTA will drop the data flow.

To add the unmanageable interface:

1. Click **Add this interface** in the unmanaged event. The following dialog displays, with the interface name in the Interface Name field.



Add Interface to NPM

Though this interface does not support SNMP, by adding it to NPM you enable the NetFlow Receiver Service to process the flow data it exports to Orion NTA.

- Add interface to node Bas-2505

General

Node Name: Bas-2505
Interface Name: NTA Virtual Interface 997
Interface Index: 997

Interface Speed

Interface Speed: Mbps
Enter the unmanaged interface speed here so NTA can display accurate resource utilization information. » Learn more

2. ***If you wish to edit the interface name,*** create and enter a name for the interface in the Interface Name field.
3. Refer to your device administration documentation for the correct interface speed, enter the interface speed into the Interface Speed field, select the speed type from the pull-down menu, and then click **SUBMIT**. The interface has been added to Orion NPM and can be viewed in Orion NPM's Node Management page.

After the unmanageable interface has been configured, it looks like any standard interface in Orion NPM and Orion NTA can recognize the interface. Now Orion NTA can manage the unmanageable interface the same as a manageable interface and does one of the following:

- If Orion NTA has been configured to automatically add NetFlow sources, it automatically adds the Netflow source. Orion NTA displays an event that says the source has been automatically added to Orion NTA. The source is visible in Orion NTA in the NetFlow Sources pane.
- If Orion NTA has not been configured to automatically add NetFlow sources, it does not add the Netflow source. Orion NTA displays an event about a flow from an interface not in Netflow sources. The source is not visible in NTA in the NetFlow Sources pane. In this instance, unmanageable interfaces can be added manually to monitor them in Orion NTA.

  Note: Unmanageable interfaces do not have information about interface utilization, because Orion NPM does not poll them. Orion NTA is unable to show these interfaces in Top XX NetFlow Sources by % Utilization pane. These interfaces do not trigger NetFlow alerts based on Utilization for the same reason.

Interface Speed Correction

If you need to correct the interface speed, you can override the interface speed value using Orion NPM's Interface Edit page's Custom Bandwidth feature. For more information on Custom Bandwidth, see Editing Interface Properties in the *SolarWinds Orion Network Performance Monitor Administrator Guide*.

Unmanageable Interface Speed

You must enter the speed for unmanageable interfaces. Unlike managed interfaces that Orion NPM recognizes, Orion NPM cannot get this information from unmanageable interfaces, which it does not recognize. Your device administration guide or your Internet provider can provide you more information on determining an unmanageable interface's speed.

Orion NTA uses the unmanaged interface speed to determine the percentage of resource utilization. Entering an accurate interface speed ensures the correct display of Orion NTA resources. With this information, you can determine the most efficient use of resources. If needed, you can override an interface speed value on Orion NPM's Interface edit page.

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 Settings on page 42.

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 **Settings** in the top right corner of the Orion Web Console.
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 33.

    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 33.

   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 **Settings** in the top right corner of the Web Console, 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 **Settings** in the top right corner of the Web Console.
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 automatically detects the new Flow source. Depending on your Orion NTA configuration, NTA either prompts you to add the detected Flow-enabled device or automatically adds the Flow-enabled device.

Notes:

- For more information about automatically adding Flow sources, see Enabling the Automatic Addition of Flow Sources on page 25.
- 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; also, configure the device to export the template every 1 minute instead of the default, which is often 30 minutes. For more information about required templates, see NetFlow, IPFIX, J-Flow, NetStream, and sFlow Requirements on page 9.
- Because there are different formulas for calculating bitrate in loading CBQoS resources and in generating reports, there is a case in which the numbers on 24-hour views do no correlate. When the device from which the data is being collected has been a CBQoS source node for less than 24 hours, the CBQoS Policy Details resource will show a different number compared to the comparable CBQoS report.
- The following procedure provides instructions for managing Flow sources in Orion NTA.

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 **Settings** in the top right corner of the Web Console.
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:
      - o Check or clear, as appropriate, the **CBQoS** column for individual interfaces
      - o 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, NetStream, and sFlow Requirements on page 9.

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 **Settings** in the top right corner of the Web Console.
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 cannot. **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 use the DSCP to communicate per-hop behaviors (PHBs), including Assured Forwarding (AF) and Expedited Forwarding (EF), to the node services that a given packet encounters. PHBs are configured on individual devices when NetFlow is initially enabled. If a given node is overloaded with NetFlow traffic, node services will keep or drop NetFlow packets in accordance with the configured PHB that matches the DSCP in each NetFlow packet. For more information about Differentiated Services, see 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 **Settings** in the top right corner of the Web Console.
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 cannot share multiple Type of Service Names, and individual Type of Service Names cannot 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 **Settings** in the top right corner of the Web Console, 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 40.

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 **Settings** in the top right corner of the Web Console.
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. NTA does not support internationalized domain names. Internationalized domain names include special characters and symbols and non-English letters, such as Japanese and Chinese letters.

- **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 supports and 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 39.

  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 **Settings** in the top right corner of the Web Console.
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 **Settings** in the top right corner of the Web Console.
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 60 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

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 Running Database Maintenance in the *SolarWinds Orion Network Performance Monitor Administrator Guide*.

The following procedure configures your Orion database maintenance settings.

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 **Settings** in the top right corner of the Web Console.
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. Click **Enable aggregation of Top Talker data** to have Orion NTA to store this data in memory; and select the number of applications, endpoints, and conversations for which Orion NTA should aggregate data.

h. Enter a number of hours for which Orion NTA should save aggregated NetFlow data in cache.

By aggregating data before writing it to the Orion database, Orion NTA software expedites the presentation of summary statistics for three of the most important kinds of information about traffic on your network: Top XX Applications, Top XX Endpoints, and Top XX Conversations.

Aggregating NetFlow data in memory significantly reduces the I/O demands that Orion NTA makes on your Orion database, which can increase the performance of all SolarWinds applications that share the database. In other words, conversely, if its Web Console resources are allowed to work directly against the Orion database in making and presenting their latest calculations, Orion NTA would make big I/O demands on the Orion database, impacting performance of both Orion NTA and Orion NPM.

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 **Settings** in the top right corner of the Web Console, 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 other endpoints (1, 2, 3, and 4). The following table details the two percentage types calculated and displayed for both Top 4 Endpoints and Top 3 Endpoints resources.

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

In the default Interactive view, pie charts are configured to show some, but not all traffic. The **Remaining traffic** row in the legend of Interactive charts show the rest of the data not included in the top XX items.

In Classic pie charts, **Other traffic** is a group of percentages below 3%. The legend below the Classic chart lists all top XX items.

Configuring Percentage Type for Top XX Lists

To configure the percentage type 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 **Settings** in the top right corner of the Web Console, 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 **absolute** or **relative** Percentage Type for Top XX Lists, as appropriate.
5. Click **Save** in the Charting and Graphing Settings section.

Configuring Area Charts Display Units

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.

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 **Settings** in the top right corner of the Web Console, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
4. Under the Charting and Graphing Settings heading, select the appropriate units in the **Units type for area charts** field.

- **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.

5. Click **Save** in the Charting and Graphing Settings section.

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

Configuring Resource Default Time Periods

You can globally set the default time period for all Orion NTA web console resources in the Charting and Graphing Settings section of the NTA Settings view, as described in the following procedure.

Note: The default time period for Orion NTA resources placed on detailed views is Last 15 Minutes, and the default time period for Orion NTA resources placed on summary views is Last 1 Hour(s).

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 **Settings** in the top right corner of the Web Console.
4. Click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
5. Under the Charting and Graphing Settings heading, enter values and select appropriate time units in the **Default time period for…** fields.
6. Click Save in the Charting and Graphing Settings section.

The time period for any Orion NTA resource can also be configured by either by clicking **Edit** in the header of any individual Orion NTA resource,

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 **Settings** in the top right corner of the Web Console.
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.

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 are included with Report Writer. You can modify them or create new reports as necessary.

For more information, see NetFlow-specific Predefined Reports on page 51. 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 NPM 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 NTA 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 NetBIOS and DNS Resolution on page 39.

Historical NetFlow Reports

Top 100 Applications – Last 24 Hours

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

Top 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 100 Conversations Including Applications – Last 24 Hours

Lists the source IP address, the destination IP address, protocol name, port number used, application name, DSCP name, and total traffic for the top 100 most bandwidth-intensive conversations involving applications 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 Endpoints

Lists the FQDN of the host (if available), the IP address of the host (if FQDN is not available), the node name (as assigned through node management), data received by the endpoint (in bytes), data transmitted by the endpoint (in bytes), total data (in bytes).

Top 50 Endpoints by Unique Partners

Lists the FQDN of the host (if available), the IP address of the host (if FQDN is not available), the node name (as assigned through node management), data received by the endpoint (in bytes), data transmitted by the endpoint (in bytes), total data (in bytes).

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.

Historical CBQoS Reports

Top 100 CBQoS Drops – Last 24 Hours

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

Top 100 CBQoS Drops – Last Update

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

Top 100 CBQoS Post-Policy – Last 24 Hours

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

Top 100 CBQoS Post-Policy – Last Update

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

Top 100 CBQoS Pre-Policy – Last 24 Hours

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

Top 100 CBQoS Pre-Policy – Last Update

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

Top 100 CBQoS Stats – Last 24 Hours

Displays each node, interface(s), stats name (Pre-Policy, Post-Policy, Drops), total bytes, and bitrate for traffic during the past 24 hours to which CBQoS policies were applied.

Viewing Reports

All reports, custom or predefined, are available for viewing in both the Orion Web Console and in Report Writer, as shown in the following procedures:

- Viewing Reports in the Orion Web Console
- Viewing Reports in the Orion Report Writer

Note: By default, no report folder is configured for newly created users. If a new user is not seeing reports, you may need to select a **Report Folder** for the new user. For more information, see Configuring an Account Report Folder in the *SolarWinds Orion Network Performance Administrator Guide*.

Viewing Reports in the Orion Web Console

The following procedure opens reports for viewing in the Orion Web Console.

To view reports in the Orion Web Console:

1. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
2. Log in to the Orion Web Console, and then click **Home > Reports**.
3. Select a report group name to expand the report group.
4. Click the title of the report you want to view, and it displays directly in the web console browser.

It is also possible to include a report within a web console view as a Report from Orion Report Writer resource. For more information about adding the Report from Orion Report Writer resource, see Editing Views on page 84.

Viewing Reports in the Orion NTA Report Writer

The following procedure opens reports for viewing in the Orion NTA Report Writer.

To view reports with Orion NTA Report Writer:

1. Click **Start > All Programs > SolarWinds Orion > Alerting, Reporting, and Mapping > Report Writer**.
2. ***If report groups are not already expanded in the left pane,*** click **+** next to a report group name to expand the group, and then click the title of the report you want to view.
3. Click **Preview**.

Using Report Writer

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

To start Report Writer:

1. Click **Start > All Programs > SolarWinds Orion > Alerting, Reporting, and Mapping > Report Writer**.
2. Click **File > Settings**.
3. In the General tab of the Report Writer Settings window, select either of the following as a default viewing mode:

- **Preview** displays the report as it will appear in printed form. For more information, see Preview Mode on page 56.
- **Report Designer** is the report creation and editing interface. For more information, see Design Mode on page 57.

  Note: You can toggle between Preview and Report Designer modes at any time by clicking **Preview** or **Design**, respectively, on the toolbar.

4. ***If you want to separate the data for individual network objects with horizontal lines,*** click **Report Style,** and then check **Display horizontal lines between each row.**
5. Click **OK** to exit Report Writer Settings.

Preview Mode

Preview mode shows a report as it will print. When you open a report in Preview mode, or switch to Preview mode from Design mode, Orion runs the query to generate the report, and then Report Writer displays the results.

The Preview window toolbar provides the following actions and information:

- Current page number and total number of pages in the report.
- Page navigation buttons: First Page, Page Up, Page Down, and Last Page
- Zoom views

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

Design Mode

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

Creating and Modifying Reports

Use the following procedure to modify or create reports in Report Writer.

To open a report with Report Writer:

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

Each report offers different configuration options, so, depending on the report, some formatting tabs described in the following sections may not be available.

Notes:

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

General Options Tab

The General tab opens by default and shows titling and display options.

To configure General options:

1. Specify the **Report Group**, **Report Title**, **Subtitle**, and **Description**.

   Note: If you use an existing report group name, the new report is added to that existing group in the left pane of the main window.
2. Select the display **Orientation** of your report.

3. ***If you are configuring an historical report and you do not want to group data by days,*** clear **Group historical data by days.**

   Note: By default, data in some availability and historical reports is grouped by days when displayed in the Orion Web Console. Data grouping by days is not viewable in Report Viewer.

4. ***If you do not want to make this report available on your Orion Web Console,*** clear **Make this Report available from the Orion website.**

   Note: By default, most reports are made available for display in the Orion Web Console. For more information, see Customizing Views on page 83.

Select Fields Options Tab

The Select Fields tab allows you to select the data fields in a report.

To select and configure fields:

1. Click Select Fields.
2. ***If you are creating a new report or adding fields to an existing report,*** click the ellipsis, select **Add a new field,** and then dynamically define each new report field as follows:
   a. Click the asterisk after **Field:**, and then select the type of information to include in the current report field.
   b. ***If you want to sort the data in the current field,*** click the **sort** asterisk and select a sort order.
   c. ***If you want to perform an operation on the data in the current field,*** click the **function** asterisk and select an operation.
3. ***If you are modifying an existing report,*** click the **Field**, **sort**, or **function** that you want to change and select a new value as follows.
   a. Click the asterisk after **Field:**.
   b. Select the type of information to include in the current report field.
   c. ***If you want to sort the data in the current field,*** click the **sort** asterisk and select a sort order.
   d. ***If you want to perform an operation on the data in the current field,*** click the **function** asterisk and select an operation.
4. ***If you want to test your selections as you assemble your report,*** click **Execute SQL Query** to view the current query results.

5. ***If you want to delete a field or rearrange the order of the fields that are listed in your report,*** select a field, click **Browse** (**…**), and then select the appropriate action.

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

6. ***If you want to preview your report,*** click **Preview**.

Filter Results Options Tab

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

To configure results filters:

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

   Note: The lists of available linked descriptors are dynamically generated in consideration of all other variables within the same condition. For more information about condition groups and their application, see Understanding Condition Groups on page 119.

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

Top XX Records Options Tab

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

To configure Top XX records:

1. ***If you want to show all records in your report,*** select **Show All Records**.

2. ***If you want to specify a truncated list of eligible items for your report,*** complete the following steps:
    a. Select either **Show only the Top** *`number`* **Records** or **Show the Top** *`percentage`* **% of Records**
    b. Provide appropriate *`number`* or *`percentage`* values.

Time Frame Options Tab

The Time Frame options tab allows you to limit the scope of your report to a specific period of time. To configure Time Frame options, select a **Named**, **Relative**, or **Specific Time Frame**, and then select or provide required values.

Notes:

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

Summarization Options Tab

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

To configure results summarization:

1. ***If you do not want to summarize your results,*** confirm that **Do not Summarize the Results** is selected.
2. ***If you want to summarize your results,*** complete the following steps:
    a. Select **Summarize the Results by Hour, Date, Month, etc**, and then select the summarization period.
    b. Specify the location of the summary field for your report.
    c. Select a location for the **Summary Date/Time** field.

Report Grouping Options Tab

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

To add and edit report groups:

1. ***If you want to add a new report group,*** select a field from the list to define your group, and then click **Add Report Group** to add your selected field to the **Report Groups** list.

   Note: Use up and down arrows to change the grouping order accordingly.

2. ***If you want to edit an existing report group,*** select the field from the Report Groups list, and then click **Edit Report Group**.

3. The following options may be changed as needed:

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

Field Formatting Options Tab

The Field Formatting tab allows you to customize the format of the various results fields in your report. To format results fields, select the field you want to format, and then edit labels and select options as appropriate.

Notes:

- The formatting options available for each field may be different according to the nature of the data contained in that field.
- Check **Hidden Field** to hide any field in your report.
- To view your changes at any time, click **Preview**.

Customizing the Report Header and Footer Image

The image that is displayed at the top and bottom of each report can be changed. To add your company logo as the report header and footer, save your logo as `Header.jpg` in the `SolarWinds\Common\WebResources` folder, typically located in `C:\Program Files\`, and then click **Refresh**.

Note: The image must be in JPEG format with a height of 150 pixels or less.

Exporting Reports

Orion Report Writer gives you the ability to present your created reports in any of the following industry-standard formats:

- Comma-delimited (*.csv, *.cdf)
- Text (*.txt)
- HTML (*.htm, *.html)
- MIME HTML, with embedded images (*.mhtml)
- Excel® spreadsheet (*.xls)
- Adobe® PDF (*.pdf)
- Image (*.gif)

The following procedure presents the steps required to export an open report from Orion Report Writer into any of the previously listed formats.

To export a report from Report Writer:

1. Select a report to export by clicking any of the following:
    - Select a report from the file tree in the left pane
    - **File > Open** to open an existing report
    - **File > New Report** to create a new report.
2. Select **File > Export** and then click the format in which you want to export your report:
3. Check the fields in your open report that you want to export into the selected format, and then click **OK**.
4. Select a location to save your file.
5. Provide a **File name**, and then click **Save**.

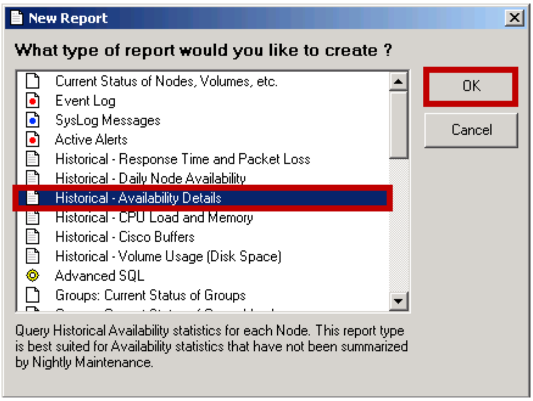
Example Device Availability Report

The following procedure generates an example report of network device availability information over the previous week. The final report is sorted so that the worst errors are viewed first. Down nodes that are still down are at the top with all devices listed in order of increasing availability.

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

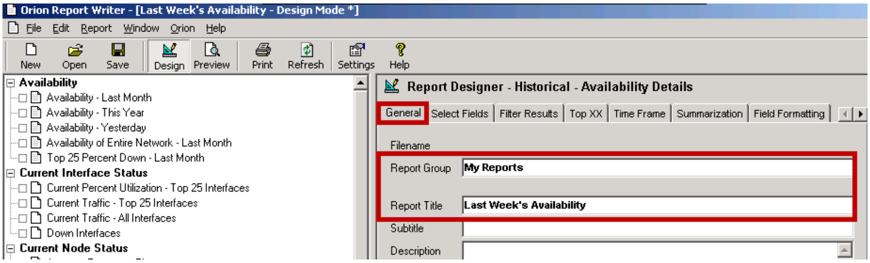
To generates an example report of network device availability information:

1. Click **Start > All Programs > SolarWinds Orion > Alerting, Reporting, and Mapping > Report Writer**.
2. Click **File > New Report**.
3. The example calls for a report on availability over the past week, so select **Historical Availability Details**, and then click **OK**.


New Report
What type of report would you like to create ?
Current Status of Nodes, Volumes, etc.
Event Log
SysLog Messages
Active Alerts
Historical - Response Time and Packet Loss
Historical - Daily Node Availability
Historical - Availability Details
Historical - CPU Load and Memory
Historical - Cisco Buffers
Historical - Volume Usage (Disk Space)
Advanced SQL
Groups: Current Status of Groups
OK
Cancel

Query Historical Availability statistics for each Node. This report type is best suited for Availability statistics that have not been summarized by Nightly Maintenance.

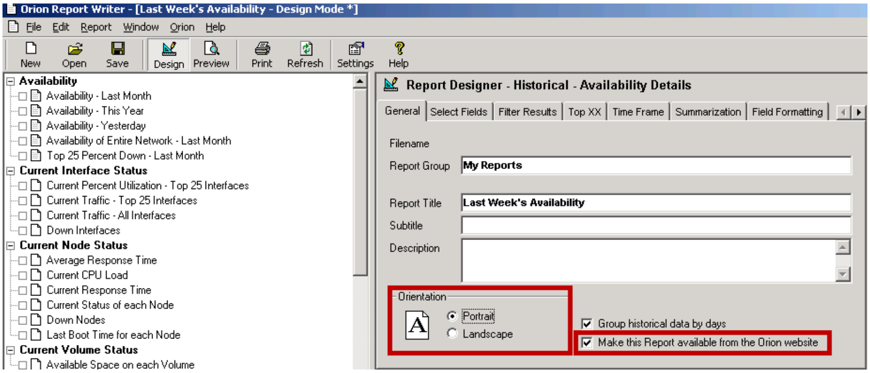
4. Type `My Reports` in the **Report Group** field, and then enter `Last Week's Availability` as the **Report Title**.


Orion Report Writer - [Last Week's Availability - Design Mode *]
File
Edit
Report
Window
Orion
Help
New
Open
Save
Design
Preview
Print
Refresh
Settings
Help
Availability
Availability - Last Month
Availability - This Year
Availability - Yesterday
Availability of Entire Network - Last Month
Top 25 Percent Down - Last Month
Current Interface Status
Current Percent Utilization - Top 25 Interfaces
Current Traffic - Top 25 Interfaces
Current Traffic - All Interfaces
Down Interfaces
Current Node Status
Report Designer - Historical - Availability Details
General
Select Fields
Filter Results
Top XX
Time Frame
Summarization
Field Formatting
Filename
Subtitle
Description

Report Group: My Reports

Report Title: Last Week's Availability

5. Select **Portrait** for the paper orientation, and then confirm that **Make this Report available from the Orion website** is checked.


Orion Report Writer - [Last Week's Availability - Design Mode *]
File Edit Report Window Orion Help
New Open Save Design Preview Print Refresh Settings Help
Availability
Availability - Last Month
Availability - This Year
Availability - Yesterday
Availability of Entire Network - Last Month
Top 25 Percent Down - Last Month
Current Interface Status
Current Percent Utilization - Top 25 Interfaces
Current Traffic - Top 25 Interfaces
Current Traffic - All Interfaces
Down Interfaces
Current Node Status
Average Response Time
Current CPU Load
Current Response Time
Current Status of each Node
Down Nodes
Last Boot Time for each Node
Current Volume Status
Available Space on each Volume
Report Designer - Historical - Availability Details
General Select Fields Filter Results Top XX Time Frame Summarization Field Formatting

Filename

Report Group: My Reports

Report Title: Last Week's Availability

Subtitle

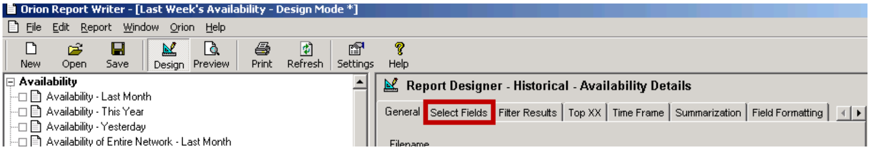
Description

Orientation: ● Portrait ○ Landscape

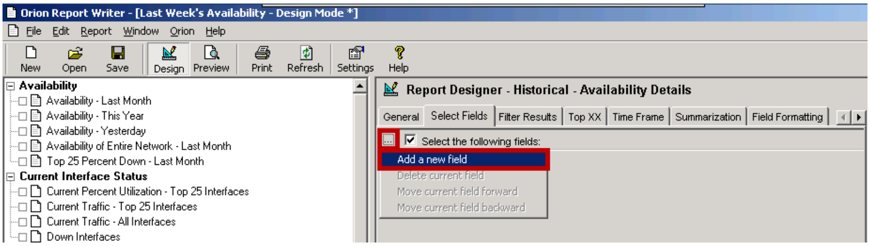
☑ Group historical data by days

☑ Make this Report available from the Orion website

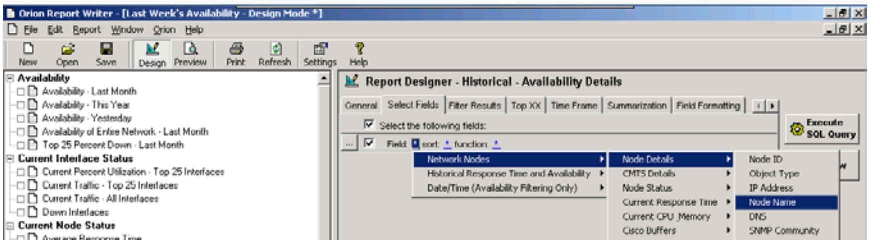
6. Click **Select Fields**.


Orion Report Writer - [Last Week's Availability - Design Mode *]
File Edit Report Window Orion Help
New Open Save Design Preview Print Refresh Settings Help
Availability
Availability - Last Month
Availability - This Year
Availability - Yesterday
Availability of Entire Network - Last Month
Report Designer - Historical - Availability Details
General Select Fields Filter Results Top XX Time Frame Summarization Field Formatting
Filename

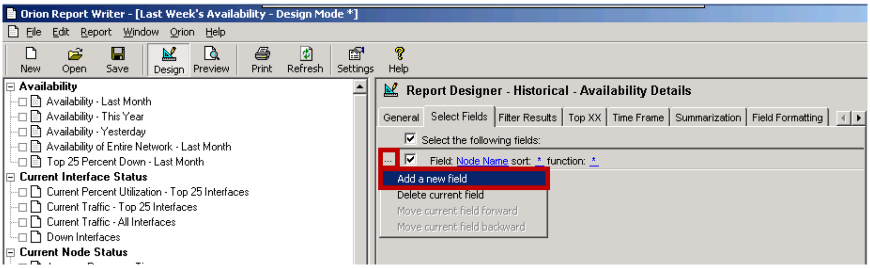
7. Click **Browse** (**…**), and then select **Add a new field**.


Orion Report Writer - [Last Week's Availability - Design Mode *]
File Edit Report Window Orion Help
New Open Save Design Preview Print Refresh Settings Help
Availability
Availability - Last Month
Availability - This Year
Availability - Yesterday
Availability of Entire Network - Last Month
Top 25 Percent Down - Last Month
Current Interface Status
Current Percent Utilization - Top 25 Interfaces
Current Traffic - Top 25 Interfaces
Current Traffic - All Interfaces
Down Interfaces
Report Designer - Historical - Availability Details
General Select Fields Filter Results Top XX Time Frame Summarization Field Formatting
☑ Select the following fields:
Add a new field
Delete current field
Move current field forward
Move current field backward

8. Click the **Field** asterisk, and then select **Network Nodes > Node Details > Node Name**.

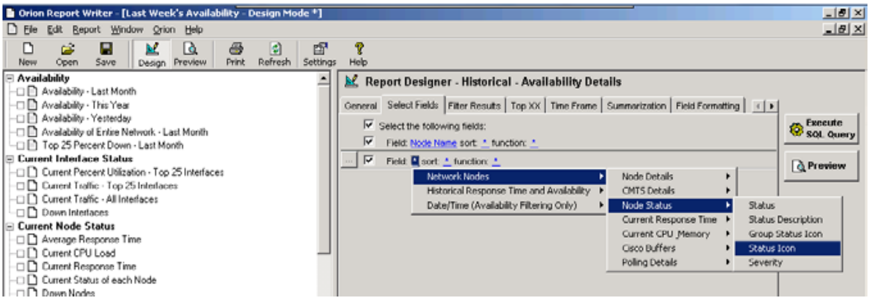

Orion Report Writer - [Last Week's Availability - Design Mode *]
File Edit Report Window Orion Help
New Open Save Design Preview Print Refresh Settings Help
Availability
Availability - Last Month
Availability - This Year
Availability - Yesterday
Availability of Entire Network - Last Month
Top 25 Percent Down - Last Month
Current Interface Status
Current Percent Utilization - Top 25 Interfaces
Current Traffic - Top 25 Interfaces
Current Traffic - All Interfaces
Down Interfaces
Current Node Status
Report Designer - Historical - Availability Details
General Select Fields Filter Results Top XX Time Frame Summarization Field Formatting
Execute SQL Query
☑ Select the following fields:
Field: * sort: * function: *
Network Nodes
Historical Response Time and Availability
Date/Time (Availability Filtering Only)
Node Details
CMTS Details
Node Status
Current Response Time
Current CPU Memory
Cisco Buffers
Node ID
Object Type
IP Address
Node Name
DNS
SNMP Community

9. Click **Browse** (**…**), and then select **Add a new field**.


Orion Report Writer - [Last Week's Availability - Design Mode *]
File Edit Report Window Orion Help
New Open Save Design Preview Print Refresh Settings Help
Availability
Availability - Last Month
Availability - This Year
Availability - Yesterday
Availability of Entire Network - Last Month
Top 25 Percent Down - Last Month
Current Interface Status
Current Percent Utilization - Top 25 Interfaces
Current Traffic - Top 25 Interfaces
Current Traffic - All Interfaces
Down Interfaces
Current Node Status
Report Designer - Historical - Availability Details
General Select Fields Filter Results Top XX Time Frame Summarization Field Formatting
Select the following fields:
Field: Node Name sort: * function: *
Add a new field
Delete current field
Move current field forward
Move current field backward

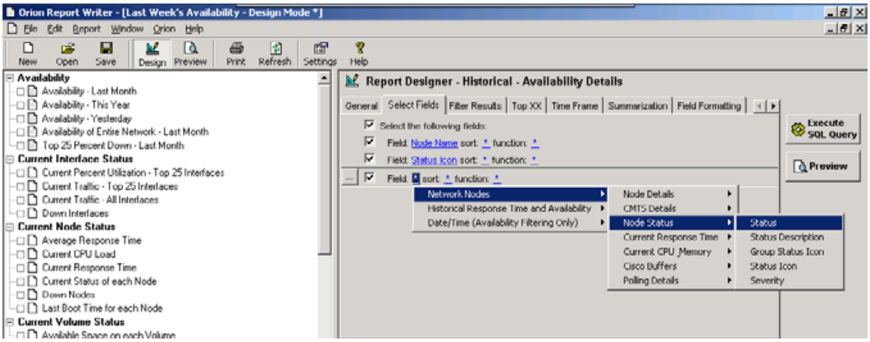
10. Click the **Field** asterisk, and then select **Network Nodes > Node Status > Status Icon**.

    Note: While this field makes a distinct visual difference for a report viewed in color, it will make little or no difference if printed in black and white.


Orion Report Writer - [Last Week's Availability - Design Mode *]
File Edit Report Window Orion Help
New Open Save Design Preview Print Refresh Settings Help
Report Designer - Historical - Availability Details
General Select Fields Filter Results Top XX Time Frame Summarization Field Formatting
Execute SQL Query
Preview
Select the following fields:
Field: Node Name sort: * function: *
Field: sort: * function: *
Network Nodes
Historical Response Time and Availability
Date/Time (Availability Filtering Only)
Node Details
CMTS Details
Node Status
Current Response Time
Current CPU Memory
Cisco Buffers
Polling Details
Status
Status Description
Group Status Icon
Status Icon
Severity

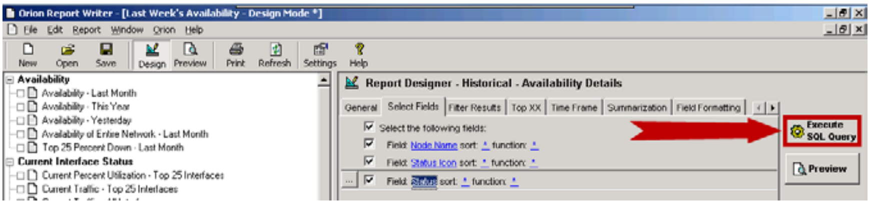
11. Click **Browse** (**…**), and then select **Add a new field**.

12. Click the **Field** asterisk, and then select **Network Nodes > Node Status > Status**.

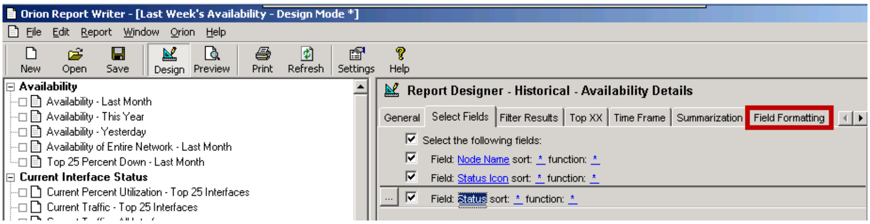

Orion Report Writer - [Last Week's Availability - Design Mode *]
File Edit Report Window Orion Help
New Open Save Design Preview Print Refresh Settings Help
Report Designer - Historical - Availability Details
General Select Fields Filter Results Top XX Time Frame Summarization Field Formatting
Execute SQL Query
Preview
Select the following fields:
Field: Node Name sort: * function: *
Field: Status Icon sort: * function: *
Field: sort: * function: *
Network Nodes
Historical Response Time and Availability
Date/Time (Availability Filtering Only)
Node Details
CMTS Details
Node Status
Current Response Time
Current CPU Memory
Cisco Buffers
Polling Details
Status
Status Description
Group Status Icon
Status Icon
Severity

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

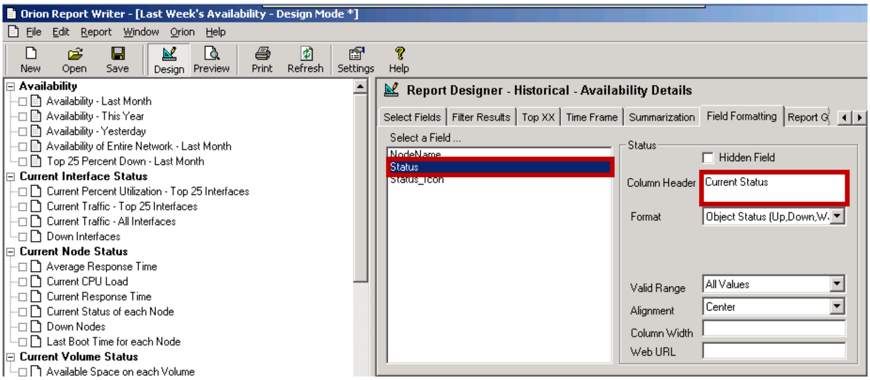
Note: The report preview should show information about both current and historical status. Current status entries must be relabeled to avoid confusion.


Orion Report Writer - [Last Week's Availability - Design Mode *]
File Edit Report Window Orion Help
New Open Save Design Preview Print Refresh Settings Help
Availability
Availability - Last Month
Availability - This Year
Availability - Yesterday
Availability of Entire Network - Last Month
Top 25 Percent Down - Last Month
Current Interface Status
Current Percent Utilization - Top 25 Interfaces
Current Traffic - Top 25 Interfaces
Report Designer - Historical - Availability Details
General Select Fields Filter Results Top XX Time Frame Summarization Field Formatting
Select the following fields:
Field: Node Name sort: * function: *
Field: Status Icon sort: * function: *
Field: Status sort: * function: *
Execute SQL Query
Preview

14. Click **Field Formatting**.


Orion Report Writer - [Last Week's Availability - Design Mode *]
File Edit Report Window Orion Help
New Open Save Design Preview Print Refresh Settings Help
Availability
Availability - Last Month
Availability - This Year
Availability - Yesterday
Availability of Entire Network - Last Month
Top 25 Percent Down - Last Month
Current Interface Status
Current Percent Utilization - Top 25 Interfaces
Current Traffic - Top 25 Interfaces
Report Designer - Historical - Availability Details
General Select Fields Filter Results Top XX Time Frame Summarization Field Formatting
Select the following fields:
Field: Node Name sort: * function: *
Field: Status Icon sort: * function: *
Field: Status sort: * function: *

15. Click **Status** in the Select a Field list, and then change the **Column Header** entry to `Current Status`.


Orion Report Writer - [Last Week's Availability - Design Mode *]
File Edit Report Window Orion Help
New Open Save Design Preview Print Refresh Settings Help
Availability
Availability - Last Month
Availability - This Year
Availability - Yesterday
Availability of Entire Network - Last Month
Top 25 Percent Down - Last Month
Current Interface Status
Current Percent Utilization - Top 25 Interfaces
Current Traffic - Top 25 Interfaces
Current Traffic - All Interfaces
Down Interfaces
Current Node Status
Average Response Time
Current CPU Load
Current Response Time
Current Status of each Node
Down Nodes
Last Boot Time for each Node
Current Volume Status
Available Space on each Volume
Report Designer - Historical - Availability Details
Select Fields Filter Results Top XX Time Frame Summarization Field Formatting Report G
Select a Field ...
NodeName
Status
Status_Icon
Status
Hidden Field

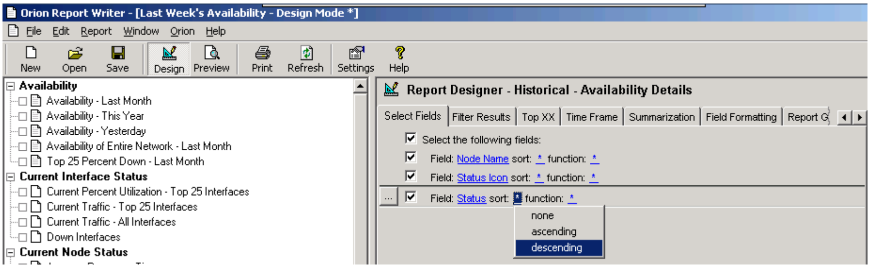
Column Header: Current Status
Format: Object Status (Up,Down,W.
Valid Range: All Values
Alignment: Center
Column Width:
Web URL:

16. Click **Status_Icon** in the Select a Field list, and then change the **Column Header** entry to `Current Status`.
17. Click **Execute SQL Query**.

Note: Column widths are adjustable. To change a column width, place your cursor on the column divider and drag it to a different position.

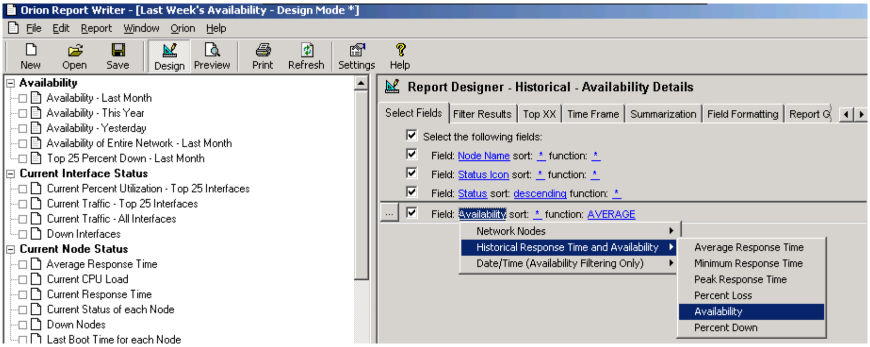
18. Click Select Fields.

19. Click the **sort** asterisk on the Status field line, and then select **descending**.


Orion Report Writer - [Last Week's Availability - Design Mode *]
File Edit Report Window Orion Help
New Open Save Design Preview Print Refresh Settings Help
Availability
Availability - Last Month
Availability - This Year
Availability - Yesterday
Availability of Entire Network - Last Month
Top 25 Percent Down - Last Month
Current Interface Status
Current Percent Utilization - Top 25 Interfaces
Current Traffic - Top 25 Interfaces
Current Traffic - All Interfaces
Down Interfaces
Current Node Status
Report Designer - Historical - Availability Details
Select Fields
Filter Results
Top XX
Time Frame
Summarization
Field Formatting
Report G
none
ascending
descending

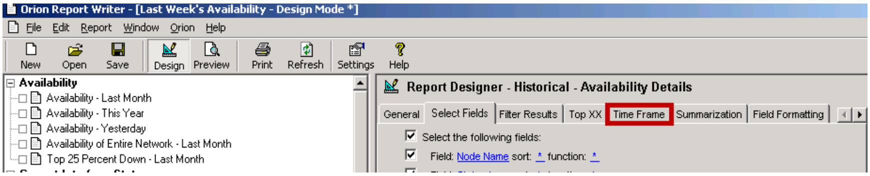
☑ Select the following fields:
☑ Field: Node Name sort: * function: *
☑ Field: Status Icon sort: * function: *
☑ Field: Status sort: * function: *

20. Click **Execute SQL Query** to confirm your choice.
21. Click **Browse** (**…**), and then select **Add a new field**.
22. Click the **Field** asterisk, and then select **Historical Response Time and Availability > Availability**.


Orion Report Writer - [Last Week's Availability - Design Mode *]
File Edit Report Window Orion Help
New Open Save Design Preview Print Refresh Settings Help
Availability
Availability - Last Month
Availability - This Year
Availability - Yesterday
Availability of Entire Network - Last Month
Top 25 Percent Down - Last Month
Current Interface Status
Current Percent Utilization - Top 25 Interfaces
Current Traffic - Top 25 Interfaces
Current Traffic - All Interfaces
Down Interfaces
Current Node Status
Average Response Time
Current CPU Load
Current Response Time
Current Status of each Node
Down Nodes
Last Boot Time for each Node
Report Designer - Historical - Availability Details
Select Fields
Filter Results
Top XX
Time Frame
Summarization
Field Formatting
Report G
Network Nodes
Historical Response Time and Availability
Date/Time (Availability Filtering Only)
Average Response Time
Minimum Response Time
Peak Response Time
Percent Loss
Availability
Percent Down

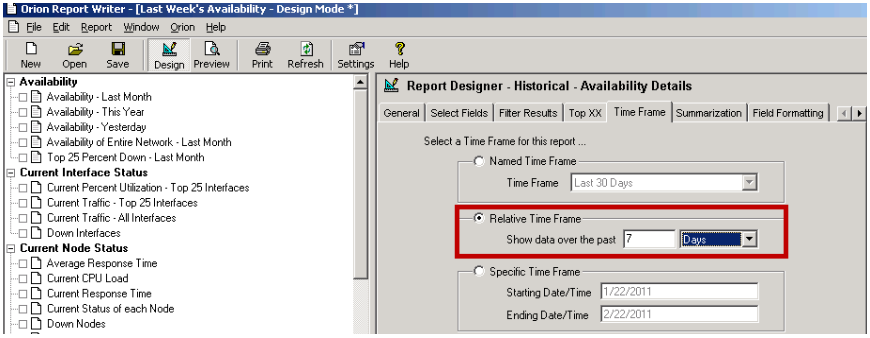
☑ Select the following fields:
☑ Field: Node Name sort: * function: *
☑ Field: Status Icon sort: * function: *
☑ Field: Status sort: descending function: *
☑ Field: Availability sort: * function: AVERAGE

23. Click the **sort** asterisk on the new line, and then select **ascending**.
24. Click **Execute SQL Query** to view the report.
25. Click Time Frame.


Orion Report Writer - [Last Week's Availability - Design Mode *]
File Edit Report Window Orion Help
New Open Save Design Preview Print Refresh Settings Help
Availability
Availability - Last Month
Availability - This Year
Availability - Yesterday
Availability of Entire Network - Last Month
Top 25 Percent Down - Last Month
Report Designer - Historical - Availability Details
General
Select Fields
Filter Results
Top XX
Time Frame
Summarization
Field Formatting

☑ Select the following fields:
☑ Field: Node Name sort: * function: *

26. Select **Relative Time Frame**, type 7 in the text field, and then select **Days** from the list.


Orion Report Writer - [Last Week's Availability - Design Mode *]
File Edit Report Window Orion Help
New Open Save Design Preview Print Refresh Settings Help
Availability
Availability - Last Month
Availability - This Year
Availability - Yesterday
Availability of Entire Network - Last Month
Top 25 Percent Down - Last Month
Current Interface Status
Current Percent Utilization - Top 25 Interfaces
Current Traffic - Top 25 Interfaces
Current Traffic - All Interfaces
Down Interfaces
Current Node Status
Average Response Time
Current CPU Load
Current Response Time
Current Status of each Node
Down Nodes
Report Designer - Historical - Availability Details
General Select Fields Filter Results Top XX Time Frame Summarization Field Formatting

Select a Time Frame for this report ...

○ Named Time Frame

Time Frame: Last 30 Days

● Relative Time Frame

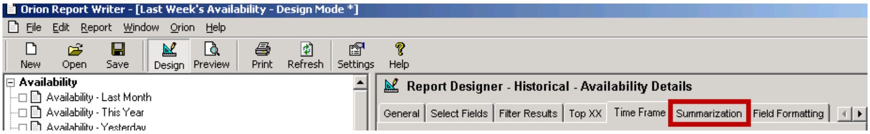
Show data over the past 7 Days

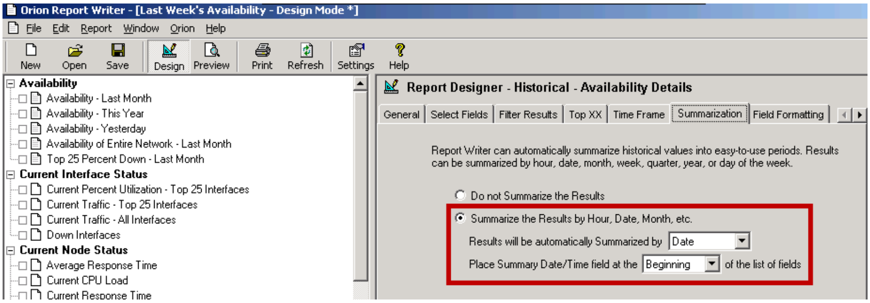
○ Specific Time Frame

Starting Date/Time 1/22/2011

Ending Date/Time 2/22/2011

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


Orion Report Writer - [Last Week's Availability - Design Mode *]
File Edit Report Window Orion Help
New Open Save Design Preview Print Refresh Settings Help
Availability
Availability - Last Month
Availability - This Year
Availability - Yesterday
Report Designer - Historical - Availability Details
General Select Fields Filter Results Top XX Time Frame Summarization Field Formatting


Orion Report Writer - [Last Week's Availability - Design Mode *]
File Edit Report Window Orion Help
New Open Save Design Preview Print Refresh Settings Help
Availability
Availability - Last Month
Availability - This Year
Availability - Yesterday
Availability of Entire Network - Last Month
Top 25 Percent Down - Last Month
Current Interface Status
Current Percent Utilization - Top 25 Interfaces
Current Traffic - Top 25 Interfaces
Current Traffic - All Interfaces
Down Interfaces
Current Node Status
Average Response Time
Current CPU Load
Current Response Time
Report Designer - Historical - Availability Details
General Select Fields Filter Results Top XX Time Frame Summarization Field Formatting

Report Writer can automatically summarize historical values into easy-to-use periods. Results can be summarized by hour, date, month, week, quarter, year, or day of the week.

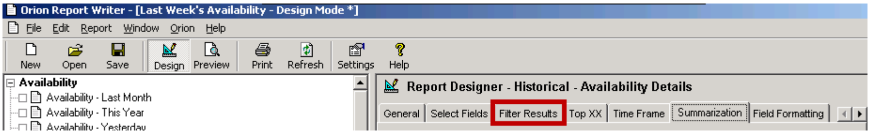
○ Do not Summarize the Results

● Summarize the Results by Hour, Date, Month, etc.

Results will be automatically Summarized by Date

Place Summary Date/Time field at the Beginning of the list of fields

28. ***If you want to filter your report,*** click Filter Results and specify filter rules, as on the Select Fields tab.


Orion Report Writer - [Last Week's Availability - Design Mode *]
File Edit Report Window Orion Help
New Open Save Design Preview Print Refresh Settings Help
Availability
Availability - Last Month
Availability - This Year
Availability - Yesterday
Report Designer - Historical - Availability Details
General Select Fields Filter Results Top XX Time Frame Summarization Field Formatting

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

Chapter 5

Viewing NetFlow Traffic Analyzer Data in the Orion Web Console

Once you have configured and enabled a NetFlow source, you can view the various types of NetFlow statistics that it records in the Orion Web Console.

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 **Settings.**
5. Click **Manage Views** under views.

   The main NTA views are listed in the format NetFlow <view_type>; for example, the NTA application view is NetFlow Application.
6. Select the NetFlow view to which you want to add a NetFlow-specific resource, and then click **Edit**.
7. Click **+** next to the resource column in which you want to display the additional NetFlow resource.
8. Click **+** next to any of the NetFlow resource types 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.

9. 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.

10. ***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.

You can set flow direction globally for all NTA resources in a Charting and Graphing Settings (Settings > NTA Settings).

To set global default for flow direction:

1. Open the Orion Web Console.

2. Click **Settings**, then click **NTA Settings**.

3. Use the flow direction settings under Charting and Graphing Settings to set the defaults for all NTA resources placed in Summary, Node Detail, Interface Detail views.

You call also set global flow direction in NTA Settings for CBQoS resources. Keep in mind that for these resources the global default is applied only if both the view on which the CBQoS resource is placed and the CBQoS resource itself are using their default settings.

4. Click **Save**.

   Note: Manually adjusting flow direction on an NTA resource overrides the global default for that resource only.

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 customized. Depending on 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.

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**.

Selecting Classic or Interactive Charts

Orion NTA resources provide the following chart styles:

- Interactive charts, which offer the following types of charts:
  - 2-D pie chart
  - Area chart (six styles: stack area, stack spline area, stack line, line, spline, bar)
- Classic charts, which offer the following types of charts:
  - 2-D or 3-D pie chart
  - Area chart (six styles: stack area, stack spline area, stack line, line, spline, bar)

For information on Classic or Interactive charts' functionalities, see Working With Charts on page **Error! Bookmark not defined.**

To select a chart style:

1. Click **Customize Page**, in the top right corner of any Summary page. The Customization page displays.
2. To enable either or both the Classic or Interactive chart style:
   a. Click to open one or more of the following options and select the appropriate resource(s):
      - NetFlow Top Resources - Traffic Analyzer Resources suitable for all NetFlow views
      - NetFlow Top Resources (Classic Chart Style) - Traffic Analyzer Resources suitable for all NetFlow views
      - NetFlow EndPoint Centric Resources (Classic Chart Style) - Traffic Analyzer Resources suitable for Node Detail views
      - NetFlow Endpoint Centric Resources (Classic Chart Style) - Traffic Analyzer Resources suitable for Node Detail views
      - NetFlow CBQoS - Traffic Analyzer Resources suitable for Interface Detail views
      - NetFlow CBQoS (Classic Chart Style) - Traffic Analyzer Resources suitable for Interface Detail views

  - NetFlow Traffic Analyzer Summary - Traffic Analyzer Resources suitable mostly for Summary views

  Note: To enable display of resources in both chart styles, open both sets of resources and choose the appropriate individual resources.

3. Click **SUBMIT**.
4. To review how the chart styles look, click **PREVIEW**. To complete and apply chart style selection, click **DONE**.

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 45.

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 74.
- Non-administrative users may still customize any Top XX resource for the duration of the current browser session. For more information, see Customizing forthe Current Session (All Users) on page 77.

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 40.

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. Define a Time Period.
    a. ***If you want the resource to inherit the setting from the view on which it is placed***, select **Use Time Period from current view** (default)
    b. ***If you want to name a time period,*** select **Named Time Period** and then select one of the options (Last 15 Minutes, Last 30 Minutes, Last Hour, Last 2 Hours, Last 24 Hours, or Today).
    c. ***If you want a relative a time period,*** select **Relative Time Period,** enter a number, and select a unit of duration.
    d. ***If you want to name an absolute time period***, select **Absolute Time Period** and set the date and time parameters.
4. Select either **Chart** or **No Chart** as the **Resource Style**.
5. ***If you are working with Classic charts and have selected* Chart *as your Resource Style,*** select from the following **Chart Style** options:
    - **2-D Pie Chart** presents a “flat” view of your data.
    - **3-D Pie Chart**
    - **Area Chart** presents a historical view of your data as represented by areas calculated at past polling times.
6. ***If you are working with Classic charts and have selected the* Area Chart *type,*** 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.
    - **Bar Chart** assigns each data point (for example, an endpoint in top conversations) its own column and plots maximums against the vertical scale.

7. ***If you are working with Interactive charts and have selected* Chart *as your resource style,*** select from the following **Chart Style** options:
    - **Pie Chart** is a 2-D chart that presents a “flat” view of your data
    - **Area Chart** presents a historical view of your data as represented by areas calculated at past polling times.
8. ***If you are working with Interactive charts and have selected the* Area Chart *type,*** 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.
    - **Bar Chart** assigns each data point (for example, an endpoint in top conversations) its own column and plots maximums against the vertical scale.
8. 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.
9. 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:
   - **2-D Pie Chart** presents a “flat” view of your data
   - **3-D Pie Chart**
   - **Area Chart** presents a historical view of your data as represented by areas calculated at past polling times.
2. ***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.
   - **Bar Chart** assigns each data point (for example, an endpoint in top conversations) its own column and plots maximums against the vertical scale.
3. 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.

4. Click **SUBMIT**.
4. ***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.
5. Click **SUBMIT.**

Adding an Endpoint Centric Resource

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

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

You can use **Customize Page** to add an endpoint-centric resource to the Node Details or Interface Details view.

To add an endpoint-centric resource:

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

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

3. Click **Customize Page** on the Node Details view.
4. Click **+** over the column in which you want the new resource to be placed.
5. Click NetFlow Endpoint Centric Resources and check the appropriate resource.
6. Click **Submit**.
7. Use the arrow controls to move the resources listed in the column into the order you want displayed in the Orion Web Console.
8. Click **Done**.

Using the NetFlow Flow Navigator

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

To create a custom NetFlow traffic view with the Flow Navigator:

1. Open the Orion Web Console in the SolarWinds program group.
2. Click **NETFLOW** on the tool bar.
3. Click **Flow Navigator** on the left edge of the summary view. (The Flow Navigator is available on any default NTA view.)
4. Select a view type.
   a. ***If you want a filtered view of your entire network***, click **Summary**.
   b. ***If you want a filtered view of traffic passing through a specific node and interface*****,** click **Detail.**

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

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

- Select **Named Time Period**, and then select a predefined period from the Named Time Period menu.

- Select **Relative Time Period**, and then provide a number appropriate for the selected time units.

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

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

  Note: Format start and end times as `MM/DD/YYYY HH:MM:SS AM/PM`.

6. Select a Flow Direction.

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

7. ***If you want to limit your view to only display network traffic to and from applications, or to exclude traffic to and from them***, a click **+** next to **Applications**, and then complete the following steps:

   a. ***If you want to include traffic from specified applications,*** select **Include**.

   b. ***If you want to exclude traffic from specified applications,*** check **Exclude**.

   c. Enter the name of an appropriate application.

   d. ***If you want to include or exclude another application***, click **Add Filter** and enter the name of an the appropriate application.

8. ***If you want to limit your view to only display network traffic to and from autonomous systems, or to exclude traffic to and from them***, a click **+** next to **Autonomous Systems**, and then complete the following steps:

   a. ***If you want to include traffic from specified autonomous systems,*** select **Include**.

   b. ***If you want to exclude traffic from specified autonomous systems,*** check **Exclude**.

   c. Enter the name of the appropriate automonous system(s).

   d. ***If you want to include or exclude another autonomous system***, click **Add Filter** and enter the name of the appropriate autonomous system.

9. ***If you want to limit your view to only display network traffic to and from autonomous systems, or to exclude traffic to and from them***, a click **+** next to **Autonomous System Conversations**, and then complete the following steps:

   a. ***If you want to include traffic from specified autonomous system conversations,*** select **Include**.

   b. ***If you want to exclude traffic from specified autonomous system conversations,*** check **Exclude**.

   c. Enter the name of an appropriate automonous network.

   d. ***If you want to include or exclude another autonomous system conversation***, click **Add Filter** and enter the name of an the appropriate conversation.

10. ***If you want to limit your view to only display network traffic related to specific conversations, or to exclude traffic to and from them***, a click **+** next to **Conversations**, and then complete the following steps:

    a. ***If you want to include traffic from specified conversations,*** select **Include**.

    b. ***If you want to exclude traffic from specified conversations,*** check **Exclude**.

    c. Enter the endpoints involved in the conversation.

    d. ***If you want to include or exclude another conversation***, click **Add Filter** and enter the names of the appropriate endpoints.

11. ***If you want to limit your view to only display network traffic related to specific countries, or to exclude traffic to and from them***, a click **+** next to **Countries**, and then complete the following steps:

    a. ***If you want to include traffic from specified countries,*** select **Include**.

    b. ***If you want to exclude traffic from specified countries,*** check **Exclude**.

    c. Enter an appropriate country.

    d. ***If you want to include or exclude another country***, click **Add Filter** and enter the name of an appropriate country.

12. ***If you want to limit your view to only display network traffic related to specific domains, or to exclude traffic to and from them***, a click **+** next to **Domains**, and then complete the following steps:

    a. ***If you want to include traffic from specified domains,*** select **Include**.

    b. ***If you want to exclude traffic from specified domains,*** check **Exclude**.

    c. Enter an appropriate domain. .

    d. ***If you want to include or exclude another domain***, click **Add Filter** and enter the name of an appropriate domain.

13. ***If you want to limit your view to only display network traffic related to specific endpoints, or to exclude traffic to and from them***, a click **+** next to **Endpoints**, and then complete the following steps:
    a. ***If you want to include traffic from specified endpoints,*** select **Include**.
    b. ***If you want to exclude traffic from specified endpoints,*** check **Exclude**.
    c. Enter an appropriate endpoint.
    d. ***If you want to include or exclude another endpoint***, click **Add Filter** and enter the name of an appropriate endpoint.
14. ***If you want to limit your view to only display network traffic related to specific endpoints, or to exclude traffic to and from them***, a click **+** next to **IP Address Groups**, and then complete the following steps:
    a. ***If you want to include traffic from specified IP Address Groups,*** select **Include**.
    b. ***If you want to exclude traffic from specified IP Address Groups,*** check **Exclude**.
    c. Enter an appropriate IP Address Group.

       Note: Though an IP Address Group is disabled it may continue to appear in the list. As a workaround, rename the group before disabling it. For example, for an IP Address Group called "PrimaryLan", you might add append "_DISABLED": "PrimaryLAN_DISABLED" would then quickly indicate that the group is currently inactive.
    d. ***If you want to include or exclude another IP Address Group***, click **Add Filter** and enter the name of an appropriate IP Address Group.
15. ***If you want to limit your view to only display network traffic using specific protocols,*** click **+** next to **Protocol**, and then complete the following steps:
    a. ***If you want to include traffic from specified Protocol,*** select **Include**.
    b. ***If you want to exclude traffic from specified Protocol,*** check **Exclude**.
    c. Select an appropriate ***Protocol***.
    d. ***If you want to include or exclude another Protocol***, click **Add Filter** and select an appropriate ***Protocol***.
16. ***If you want to limit your view to only display network traffic using specific service types,*** click **+** next to **Types of Service**, and then complete the following steps:

  a. ***If you want to include traffic from specified type of service,*** select **Include**.
  b. ***If you want to exclude traffic from specified type of service,*** check **Exclude**.
  c. Select an appropriate ***type of service***.
  d. ***If you want to include or exclude another type of service***, click **Add Filter** and select an appropriate ***type of service***.

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

Deleting a Filtered View

If you placed a filtered view on the NTA menu bar but have no further need of it, you can simply delete the view.

To delete a filtered view from the NTA menu:

1. Open the Orion Web Console.
2. Click **Settings**.
3. Click **Customize Menu Bars**.
4. Click **Edit** on the Menu Bar: NTA_TabMenu.
5. Click the **X** beside the custom menu item.
6. Click **Submit**.

Customizing Views

Orion Web Console views are configurable presentations of network information that can include maps, charts, summary lists, reports, events, and links to other resources. Customized views can then be assigned to menu bars.

Note: In environments where security is a priority, SolarWinds recommends against providing a view where users may change their own web console account passwords.

Creating New Views

You can customize the Orion Web Console for individual users by logging in as an administrator and creating new views as shown in the following procedure.

Note: In environments where security is a priority, SolarWinds recommends against providing a view where users may change their own web console account passwords.

To create a new view:

1. Click **Settings** in the top right of the web console.
2. Click **Manage Views** in the Views group.
3. Click **Add**.
4. Enter the **Name of New View**, and then select the **Type of View**.

   Note: The **Type of View** selection affects how the view is made accessible to users, and your choice may not be changed later. For more information, see Views by Device Type on page 86.
5. Click **Submit.**

After you have created a new view, the Customize Your View page opens. For more information, see Editing Views on page 84.

Editing Views

The Orion Web Console allows administrators to configure views for individual users.

The following steps are required to configure an existing view.

To edit an existing view:

1. Click **Settings** in the top right of the web console.
2. Click **Manage Views** in the Views group.
3. Select the view you want to customize from the list, and then click **Edit**.
4. ***If you want to change the column layout of your view,*** complete the

following steps.

   a. Click **Edit** to the right of the column widths.
   b. Select the number of columns under Layout.
   c. Provide the width, in pixels, of each column in the appropriate fields.
   d. Click **Submit**.

5. ***If you want to add a resource,*** repeat the following steps for each resource:
    a. Click **+** next to the column in which you want to add a resource.
    b. Click **+** next to a resource group on the Add Resources page to expand the resource group, displaying available resources.
    c. Check all resources you want to add.
    d. ***If you have completed the addition of resources to the selected view,*** click **Submit**.

    Notes:

- Resources already in your view will not be checked on this page listing all web console resources. It is, therefore, possible to pick duplicates of resources you are already viewing.
- Some resources may require additional configuration. For more information, see Resource Configuration Examples on page 87.
- Several options on the Add Resources page are added to the list of resources for a page, but the actual configuration of a given map, link, or code is not added until the page is previewed.

6. ***If you want to delete a resource from a column,*** select the resource, and then click **X** next to the resource column to delete the selected resource.
7. ***If you want to copy a resource in a column,*** select the resource, and then click ⧉ next to the resource column to delete the selected resource.
8. ***If you want to rearrange the order in which resources appear in your view,*** select resources, and then use the arrow keys to rearrange them.
9. ***If you have finished configuring your view,*** click **Preview**.

    Note: A preview of your custom web console displays in a new window. A message may display in the place of some resources if information for the resource has not been polled yet. For more information, see Resource Configuration Examples on page 87.

10. Close the preview window.
11. ***If you are satisfied with the configuration of your view,*** click **Done**.

    Note: For more information about adding a customized view to menu bars as a custom item, see Customizing Web Console Menu Bars in the SolarWinds Orion Network Performance Administrator Guide. For more information about assigning your customized view as the default view for a user, see Editing User Accounts in that same guide.

Copying Views

When you want to create multiple views based on the same device type, copying views allows you to create one view, and then use that view as a template to create other new views. The following steps copy an existing view.

To copy a view:

1. Click **Settings** in the top right of the web console.
2. Click **Manage Views** in the Views group.
3. Select the view you want to copy, and then click **Copy**.
4. ***If you want to edit a copied view,*** follow the procedure in the Editing Views section on page 84.

Deleting Views

The following steps delete an existing view.

To delete an existing view:

1. Click **Settings** in the top right of the web console.
2. Click **Manage Views** in the Views grouping of the Orion Website Administration page.
3. Select the view you want to delete, and then click **Delete**.

Views by Device Type

There are vast differences among network objects and the statistics they report, but the Orion Web Console can make it easier to view network data by displaying object details by device type, giving you the ability to have a different view for each unique type of device you have on your network, including routers, firewalls, and servers. The following steps assign a view by any available device type.

To assign a view by device type:

1. Click **Settings** in the top right of the web console, and then click **Views by Device Type** in the Views group of the Orion Website Administration page.
2. Select available Web Views for the different types of devices that Orion is currently monitoring or managing on your network.
3. Click **Submit**.

Resource Configuration Examples

Several resources that may be selected from the Add Resources page require additional configuration. Included in this section are examples of these resources and the steps that are required for their proper configuration.

Selecting a Network Map

Network maps created with Orion Network Atlas can give a quick overview of your network, right from the main web console view. For more information about creating maps, see Creating Network Maps in the *SolarWinds Orion Network Performance Administrator Guide*.

Note: Clicking the resource title in the title bar menu displays the resource by itself in a browser window.

The following procedure adds a network map to the Orion Web Console.

To add a network map to the web console:

1. Create a new view or edit an existing view.

   Note: For more information, see Customizing Views on page 83.
2. Select the view to which you want to add the map, and then click **Edit**.
3. Click **+** next to the view column in which you want to display the new map.
4. Click **+** next to **Network Maps**, check **Network Map**, and then click **Submit**.
5. Click **Preview** on the Customize `Your View` page.
6. Click **Edit** in the Network Map resource title bar.
7. ***If you do not want to use the default title provided,*** enter a new **Title** for the title bar of the added map.
8. ***If you want a subtitle,*** enter a new **Subtitle** for the added map.

   Note: Titles and subtitles may be entered as either text or HTML.
9. Select from the list of available maps.
10. Select the **Scale** at which you want to display the map.

    Note: If you leave the **Scale** field blank, the map will display at full scale, based on the size of the column in which the map displays.
11. Click **Submit**.

Displaying a List of Objects on a Network Map

When your web console view includes a network map, it can be helpful to maintain a list of network objects that appear on the map. The following procedure enables a resource listing network map objects.

Note: Clicking the resource title displays the resource in a new browser window.

To display a list of network map objects:

1. Create a new view or edit an existing view.

   Note: For more information, see Customizing Views on page 83.
2. Select the view to display the list of network map objects, and then click **Edit**.
3. Click **+** next to the view column in which you want to display the new list of network map objects.
4. Click **+** next to **Network Maps**, check **List of Objects on Network Map**, and then click **Submit**.
5. Click **Preview** on the Customize `Your View` page.
6. Click **Edit** in the title bar of the List of Objects on Network Map resource.
7. ***If you do not want to use the default title provided,*** enter a new **Title** for the header of the objects list.
8. ***If you want a subtitle,*** enter a new **Subtitle** for the added objects list.

   Note: Titles and subtitles may be entered as either text or HTML.
9. Select from the list of available maps for the objects that you want to populate your list, and then click **Submit**.

Displaying a Custom List of Maps

The web console allows you to populate a custom view with a list of available network maps. Each map in your custom list, when clicked, opens in a new window. The following procedure enables a custom network maps list resource.

Note: Clicking the resource title displays the resource in its own browser window.

To display a custom list of maps:

1. Create a new view or edit an existing view.

   Note: For more information, see Customizing Views on page 83.
2. Select the view to which you want to add the custom list of network maps, and then click **Edit**.
3. Click **+** next to the view column in which you want to display the custom list of network maps.
4. Click **+** next to **Network Maps**.
5. Check **Custom List of Maps**, and then click **Submit**.

6. Click **Preview** on the Customize `Your View` page, and then click **Edit** in the title bar of the Custom List of Maps resource.
7. ***If you do not want to use the default title provided,*** enter a new **Title** for the header of the maps list.
8. ***If you want a subtitle,*** enter a new **Subtitle** for the custom list of maps.

   Note: Titles and subtitles may be entered as either text or HTML.
9. Check the maps you want to include in your maps list.
10. Click **Submit**.

Displaying an Event Summary - Custom Period of Time

You may want your web console view to display an event summary for a specified period of time. The following procedure details the steps to include an event summary in your web console.

Note: Clicking the resource title in the title bar menu displays the resource by itself in a browser window.

To display an event summary:

1. Create a new view or edit an existing view.

   Note: For more information about creating a new view or editing an existing view, see Customizing Views on page 83.
2. Select the view to include the event summary, and then click **Edit**.
3. Click **+** next to the view column that will display the event summary.
4. Click **+** next to **Events**.
5. Check **Event Summary – Custom Time Period**, and then click **Submit**.
6. Click **Preview** on the Customize `Your View` page.
7. Click **Edit** in the title bar of the Event Summary resource.
8. ***If you do not want to use the default title provided,*** enter a new **Title** for the header of the event summary.

   Note: Titles may be entered as either text or HTML.
9. Select the time period for displaying events from **Display Events for the following Time Period**.
10. Click **Submit**.

Specifying User-Defined Links

The User-Defined Links option may be used to create quick access to external websites or customized views. URLs of your customized views can be copied from their preview pages and pasted in a User-Defined Links field. The following steps enable user-defined links from within your web console.

Note: Clicking the resource title in the title bar menu displays the resource by itself in a browser window.

To enable a user-defined links resource:

1. Create a new view or edit an existing view.

   Note: For more information, see Customizing Views on page 83.
2. Select the view to which you want to add the user-defined links resource.
3. Click **Edit**.
4. Click **+** next to the view column to display the user-defined links resource.
5. Click **+** next to **Miscellaneous**
6. Check **User Defined Links**.
7. Click **Submit**.
8. Click **Preview** on the Customize `Your View` page.
9. Click **Edit** in the title bar of the User Defined Links resource.
10. ***If you do not want to use the default title provided,*** enter a new **Title** for the links list.
11. ***If you want a subtitle,*** enter a new **Subtitle** for the links list.

    Note: Titles and subtitles may be entered as either text or HTML.
12. Enter the following information for each link you want to define:
    - **a.** A link **Name** and the **URL** of your link.
    - **b.** ***If you want your links to open in a new browser window,*** check **Open in New Window.**
13. Click **Submit**.

Specifying Custom HTML or Text

In situations where you have static information that you want to provide in the web console, use the **Custom HTML or Text** option. The **Custom HTML or Text** option may also be used to create quick access to your customized views. The following procedure will create a static content area within your web console for displaying text or HTML content.

Note: Clicking the resource title displays the resource in a new browser window.

To specify custom HTML or text:

1. Create a new view or edit an existing view.

   Note: For more information, see Customizing Views on page 83.
2. Select the view to include the custom HTML or text, and then click **Edit**.
3. Click **+** next to the column to display the custom HTML or text.
4. Click **+** next to **Miscellaneous**, and then check **Custom HTML or Text**.
5. Click **Submit**.
6. Click **Preview** on the Customize `Your View` page.
7. Click **Edit** in the title bar of the Custom HTML or Text resource.
8. ***If you do not want to use the default title provided,*** enter a new **Title** for the specified content area.
9. ***If you want a subtitle,*** enter a new **Subtitle** for the specified content area.

   Note: Titles and subtitles may be entered as either text or HTML.
10. Enter content as either text or HTML into the **Raw HTML** field.
11. Click **Submit**.

Specifying an Orion Report

The web console is able to incorporate reports that you have created in Orion Report Writer into any view. The following procedure will take a report that you have created with Report Writer and include it within a web console view.

Note: Clicking the resource title in the title bar menu displays the resource by itself in a browser window.

To include an Orion report:

1. Create a new view or edit an existing view.

   Note: For more information, see Customizing Views on page 83.
2. Select the view to which you want to add the report.
3. Click **Edit**.
4. Click **+** next to the view column in which you want to display the report.
5. Click **+** next to **Report Writer**.
6. Check **Report from Orion Report Writer**.
7. Click **Submit**.

8. Click **Preview** on the Customize `Your View` page.
9. Click **Edit** in the title bar of the Report from Orion Report Writer resource.
10. ***If you do not want to use the default title provided,*** enter a new **Title** for the included report.
11. ***If you want a subtitle,*** enter a new **Subtitle** for the included report.

    Note: Titles and subtitles may be entered as either text or HTML.
12. **Select a Report** to include.
13. ***If you want to add a filter to the included report,*** enter an appropriate query in the **Filter Nodes** field.

    Note: Filter Nodes is an optional, advanced, web console feature that requires some knowledge of SQL queries. Click **+** next to **Show Filter Examples** to view a few example filters.
14. Click **Submit**.

Displaying a Custom List of Reports

The web console allows you to populate a custom view with a custom reports list. When clicked from the list, each report opens in a new window. The following procedure details the steps required to enable a custom list of network reports.

Note: Clicking the resource title displays the resource in a new browser window.

To display a custom list of reports:

1. Create a new view or edit an existing view. For more information, see Customizing Views on page 83.
2. Select the view to which you want to add the custom list of reports, and then click **Edit**.
3. Click **+** next to the column to display the custom list of reports.
4. Click **+** next to **Report Writer**.
5. Check **Custom List of Reports**, and then click **Submit**.
6. Click **Preview** on the **Customize** `Your View` page, and then click **Edit** in the title bar of the Report from Orion Report Writer resource.
7. ***If you do not want to use the default title provided,*** enter a new **Title** for the header of the reports list.
8. ***If you want a subtitle,*** enter a new **Subtitle** for the custom list of reports.

    Note: Titles and subtitles may be entered as either text or HTML.

9. Check the reports that you want to include in your custom list of reports.

   Note: To allow a user to view a report included in the custom list, you must set the report access for the account. For more information, see Configuring an Account Report Folder in the SolarWinds Orion Network Performance Administrator Guide.

10. Click **Submit**.

Filtering Nodes

Your Orion Web Console can maintain a customizable node list for your network. Node lists may be configured for specific views using SQL query filters. The following steps set up node filtering for node lists included in web console views.

Note: Clicking the resource title displays the resource in a new browser window.

To enable filtering on a node list:

1. Create a new view or edit an existing view.

   Note: For more information, see Customizing Views on page 83.

2. Select the view to which you want to add the node list, and then click **Edit**.
3. Click **+** next to the view column in which you want to display the node list.
4. Click **+** next to **Node Lists**, check **All Nodes – Table**, and then click **Submit**.
5. Click **Preview** on the **Customize** `Your View` page, and then click **Edit** in the title bar of the All Nodes – Table resource.
6. ***If you do not want to use the default title provided,*** enter a new **Title** for the node list.
7. ***If you want a subtitle,*** enter a new **Subtitle** for the node list.

   Note: Titles and subtitles may be entered as either text or HTML.

8. ***If you want to filter your node list by text or IP address range,*** provide the text or IP address range by which you want to filter your node list in the Filter Text field, as shown in the following examples:

- Type `Home` in the Filter Text field to list all nodes with **Home** in the node name or as a location.
- Type `192.168.1.*` in the Filter Text field to list all nodes in the 192.168.1.0-255 IP address range.

9. Select the property that is appropriate to the filter text provided above, as shown in the following examples:

- ***If you typed*** `Home` ***in the Filter Text area,*** select **Node Name** or **Location** to list nodes with “Home” in the node name or as a location.

- ***If you typed*** `192.168.1.*` ***in the Filter Text area,*** select **IP Address** to list only nodes in the 192.168.1.0-255 IP address range.

10. ***If you want to apply a SQL filter to the node list,*** enter an appropriate query in the **Filter Nodes (SQL)** field.

    Notes:

- **Filter Nodes (SQL)** is an optional, advanced, web console feature that requires some knowledge of SQL queries. Click **+** next to **Show Filter Examples** to view a few example filters.
- By default, node list resources are designed to sort nodes alphabetically by node caption. This configuration cannot be overwritten using a SQL filter, so `order by` clauses included in SQL filters are redundant and will result in Custom SQL filter formatting errors.

11. Click **Submit**.

Grouping Nodes

Your Orion Web Console can maintain a customizable node list for your network. Node lists may be configured for specific views with node grouping. The following steps set up node grouping for node lists included in web console views.

Note: Clicking the resource title in the title bar menu displays the resource by itself in a browser window.

To enable grouping on a node list:

1. Create a new view or click **Customize Page** in the top right of an existing web console view.

   Note: For more information, see Customizing Views on page 83.
2. Click **+** next to the view column in which you want to display the node list.
3. Click **+** next to **Node Lists.**
4. Check **All Nodes – Tree (AJAX),** and then click **Submit**.
5. Click **Done**.
6. Click **Edit** in the title bar of the All Nodes – Tree (AJAX) resource.
7. ***If you do not want to use the default title provided,*** enter a new **Title** for the node list.
8. ***If you want a subtitle,*** enter a new **Subtitle** for the node list.

   Note: Titles and subtitles may be entered as either text or HTML.
9. Select up to three criteria, in specified levels, for **Grouping Nodes** within your web console view.

10. ***If you want to apply a SQL filter to the node list,*** enter an appropriate query in the **Filter Nodes** field.

    Notes:

- **Filter Nodes (SQL)** is an optional, advanced, web console feature that requires some knowledge of SQL queries. Click **+** next to **Show Filter Examples** to view a few example filters.
- By default, node list resources are designed to sort nodes alphabetically by node caption. This configuration cannot be overwritten using a SQL filter, so `order by` clauses included in SQL filters are redundant and will result in Custom SQL filter formatting errors.

11. Click **Submit**.

Adding a Service Level Agreement Line to Charts (Orion NPM)

The Orion Web Console can display a service level agreement (SLA) line on any Min/Max/Average bps chart. When you add a customer property named “SLA” and populate the field with your device SLA values, the Orion Web Console will display the appropriate line on your charts.

Notes:

- Interface data is only available in Orion NPM.
- The SLA line may not appear immediately. It may take several minutes for the change to be detected by the Orion web engine.

To add a Service Level Agreement line to Min/Max/Average bps charts:

1. Click **Start > All Programs > SolarWinds Orion > Grouping and Access Control > Custom Property Editor**.
2. Click **Add Custom Property**, and then confirm that **Add Predefined Properties** is selected.
3. Check **SLA** in the list of predefined properties, and then click **OK**.
4. Click **Properties > Edit Interfaces Properties**.
5. Enter the SLA value (in bps) in the **SLA** column for each interface you want to label with SLA values. For example, type `1544000` for a T1 interface (1.544 Mbps) or `225000` for a serial connection running at 225 Kbps.
6. Close the Custom Property Editor.
7. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
8. Browse to the Interface Details view of one of the interfaces you edited. The SLA line displays on any chart showing Min/Max/Average bps.

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 NetBIOS and DNS Resolution on page 39.

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 35.

- Because there are different formulas for calculating bitrate in loading CBQoS resources and in generating reports, there is a case in which the numbers on 24 hour views do no correlate. When the device from which the data is being collected has been a CBQoS source node for less than 24 hours, the CBQoS Policy Details resource will show a different number compared to the comparable CBQoS report.

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 use cases 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 use drops back to normal.

Chapter 7

Using Orion NTA Advanced Alerts

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

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

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

For an excellent overview of alerting in Orion advanced alerts, see Understanding Orion Advanced Alerts. For all specific information on Orion basic and advanced alerts, including detailed instructions for creating and managing them with the Orion Alert Manager, see Chapter 11, Creating and Managing Alerts, in the Orion Performance Manager Administrator’s Guide.

The remaining sections of the chapter discuss more basic topics related to SolarWinds Advanced Alerts, including creating and configuring new advanced alerts, and setting up alert actions.

Configuring NetFlow Advanced Alerts

When you install SolarWinds Orion Network Traffic Analyzer, the software automatically creates top talker and CBQoS alerts in the Orion Alert Manager.

Top Talker Alerts

High Receive Percent Utilization with Top Talkers

> This alert indicates that the traffic received by the relevant interface exceeded the defined bandwidth usage threshold.

High Transmit Percent Utilization with Top Talkers

> This alert indicates that the traffic transmitted by the relevant interface exceeded the defined bandwidth usage threshold.

By default, when triggered, top talker alerts do two things:

- Write the bandwidth utilization event to the SolarWinds event log when the current percent utilization on the transmit side of an interface rises above specified value, and then again when the utilization drops back down below a specified value.
- Initiate a web capture of the most current top talker information and then append and send that information in an email to the configured recipient.

CBQoS Alerts

The following CBQoS alerts can confirm that the CBQoS policies being applied to traffic flowing through your devices are producing the intended results. By effectively setting up alert thresholds, you can get early warning of traffic processing issues and intervene to better shape network traffic.

Pre-Policy

CBQoS Pre-Policy writes to the SolarWinds event log when the amount of Pre-Policy traffic (in bytes) meets the conditions of your alert threshold setting.

Example of alert logged: CBQoS Pre-Policy traffic in class 'class-default (MCQTest)' with policy ‘policy-default (MPQTest)’ on interface 'FastEthernet0/0 · link to core' met the conditions of your alert threshold setting. Total Pre-Policy traffic in the past 15 minutes: 99999 Bytes

By default, this alert writes to the Event Log. This alert also can be configured to send the information in an email to the configured recipient.

Post-Policy

CBQoS Post-Policy writes to the SolarWinds event log when the amount of Post-Policy traffic (in bytes) meets the conditions of your alert threshold setting.

Example of alert logged: CBQoS Post-Policy traffic in class 'class-default (MCQTest)' with policy ‘policy-default (MPQTest)’ on interface 'FastEthernet0/0 · link to core' met the conditions of your alert threshold setting. Total Post-Policy traffic in the past 15 minutes: 99999 Bytes

By default, this alert writes to the Event Log. This alert also can be configured to send the information in an email to the configured recipient.

Drops

CBQoS Drops writes to the SolarWinds event log when, as a result of applying CBQoS policies to traffic on an interface.

Example of alert logged: CBQoS Drops met your alert threshold setting as a result of applying class map 'class-default (MCQTest)' and policy map ‘policy-default (MPQTest)’ on interface 'FastEthernet0/0 · link to core' . Total data dropped in last 15 minutes is: 00333 Bytes

By default, this alert writes to the Event Log. This alert also can be configured to send the information in an email to the configured recipient.

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

For steps on creating an advanced alert see the sections on advanced alerts in Chapter 11, Creating and Managing Alerts, in the Orion Performance Manager Administrator’s Guide.

To configure an NTA advanced alert:

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

      For top talker alerts, the default condition is the interface’s transmit/receive utilization percentage exceeding 75.

      For the CBQoS alerts, the default condition is a match on the relevant **NTA CBQoS Class Map**. For example, for the Drops alert, the dropdown value of NTA CBQoS Class Map is ‘Drops’. The default values for both **Class Name** and **Policy Name** is ‘*’. This does not mean that the alert triggers if there is a match on **any** class name or policy name that has been returned to Orion NTA from polled CBQoS devices; rather, it means that the alert triggers in this default configuration only when the value of Class Name or Policy Name is NULL. These trigger conditions for Class Name and Policy Name, in other words, render the predefined CBQoS alerts inoperable by default.

      To enable these alerts to trigger: you must click value field for Class Name and Policy Name to select a specifically named class or policy from a list that is pre-populated based on CBQoS polling results.

You can adjust the number of seconds for which the match exists, essentially inserting a delay to allow the traffic to fluctuate without triggering the alert.

You can adjust the default trigger conditions as needed or add conditions.

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

For top talker alerts, the default condition is the interface's transmit/receive utilization percentage going below 50. You can adjust this condition or add conditions.

For the CBQoS alerts, the default condition is no match based on the NTA CBQoS Class Map type, Class Name value, and Policy name value. You can adjust the number of seconds for which the match fails to persist, essentially inserting a delay to allow the traffic to fluctuate without canceling the alert.

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

The default condition is no suppression.

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

The default range is 24/7.

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

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

Notes: If there are endpoint-centric resources on the Interface Details page when it is captured for inclusion in top talker alert notification, the links to those resources will be non-functional in the email that the designated recipient receives; essentially, the information provided by default in the alert notification currently is not customizable.

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

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

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

becomes:

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

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

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

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

Using Orion Advanced Alerts

Alerts are generated for network events, and they may be triggered by the simple occurrence of an event or by the crossing of a threshold value for a monitored Interface, Volume, or Node. Alerts can be set to notify different people on different days, different times of the day, different people for different events, or any combination of times, events, and people. Alerts may be configured to notify the people who need to know about the emergent event by several mediums, including:

- Sending an e-mail or page
- Playing a sound on the Orion Network Performance Monitor server
- Logging the alert details to a file
- Logging the alert details to the Windows Event Log
- Logging the alert details to the NetPerfMon Event Log
- Sending a Syslog message
- Executing an external program
- Executing a Visual Basic script
- E-mailing a web page
- Playing text-to-speech output
- Sending a Windows Net Message
- Dialing a paging or SMS service
- Sending an SNMP trap
- GETting or POSTing a URL to a web server

Creating and Configuring Advanced Alerts

Orion NTA allows you to configure advanced alerts with the following features:

- Sustained state trigger and reset conditions
- Multiple condition matching
- Automatic alert escalation
- Separate actions for triggers and resets

Advanced alerts are configured using the Advanced Alert Manager, as shown in the following section.

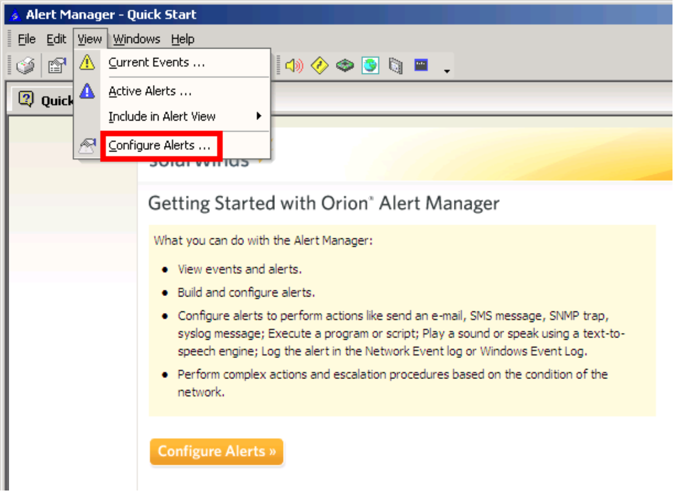
Note: If you want to configure advanced alert features, such as timed alert checking, delayed alert triggering, timed alert resets, or alert suppression, check **Show Advanced Features** at the lower left of any Advanced Alert windows. For the purposes of this document, **Show Advanced Features** is always enabled.

Creating a New Advanced Alert

The following procedure creates a new advanced alert.

To create a new advanced alert:

1. Click **Start > SolarWinds Orion > Alerting, Reporting, and Mapping > Advanced Alert Manager**.
2. Click **View > Configure Alerts**.

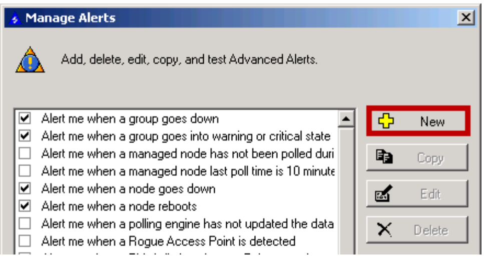


Getting Started with Orion® Alert Manager

What you can do with the Alert Manager:

- View events and alerts.
- Build and configure alerts.
- Configure alerts to perform actions like send an e-mail, SMS message, SNMP trap, syslog message; Execute a program or script; Play a sound or speak using a text-to-speech engine; Log the alert in the Network Event log or Windows Event Log.
- Perform complex actions and escalation procedures based on the condition of the network.

3. Click **New**.



Add, delete, edit, copy, and test Advanced Alerts.

☑ Alert me when a group goes down
☑ Alert me when a group goes into warning or critical state
☐ Alert me when a managed node has not been polled duri
☐ Alert me when a managed node last poll time is 10 minute
☑ Alert me when a node goes down
☑ Alert me when a node reboots
☐ Alert me when a polling engine has not updated the data
☐ Alert me when a Rogue Access Point is detected

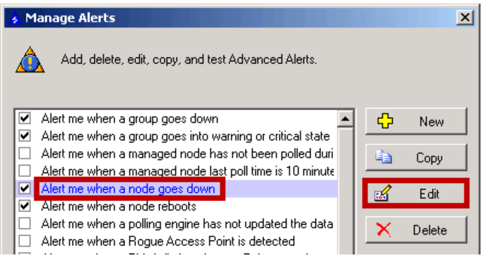
The Edit Alert window displays, providing an array of configurable alerting options, including trigger and reset conditions, suppressions, and date and time limitations. The following sections provide more information about configuring alert options.

Naming, Describing, and Enabling an Advanced Alert

Use the following steps, after clicking **New**, **Copy**, or **Edit** from the Manage Alerts Window, to name and describe an advanced alert.

To name and describe an advanced alert:

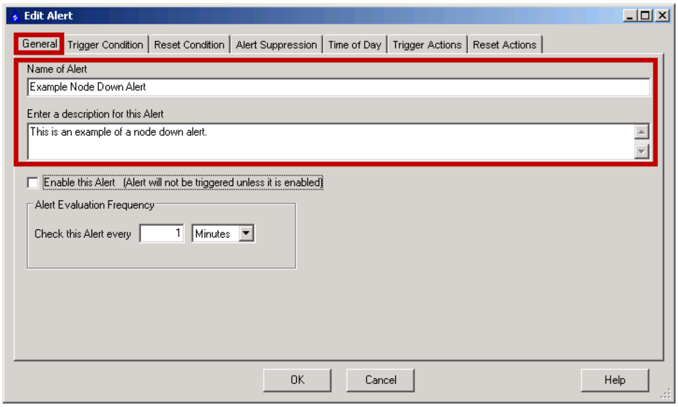
1. Click **Start > SolarWinds Orion > Alerting, Reporting, and Mapping > Advanced Alert Manager**.
2. Click **View > Configure Alerts**.
3. ***If you want to create a new alert,*** click **New.**
4. ***If you want to copy or edit an existing alert,*** select an alert from the list, and then click **Copy** or **Edit**, as appropriate.



Add, delete, edit, copy, and test Advanced Alerts.

☑ Alert me when a group goes down
☑ Alert me when a group goes into warning or critical state
☐ Alert me when a managed node has not been polled duri
☐ Alert me when a managed node last poll time is 10 minute
☑ Alert me when a node goes down
☑ Alert me when a node reboots
☐ Alert me when a polling engine has not updated the data
☐ Alert me when a Rogue Access Point is detected

5. Click **General**, type the name of your alert in the **Name of Alert** field, and then type a description of your alert in the description field.



Name of Alert: Example Node Down Alert

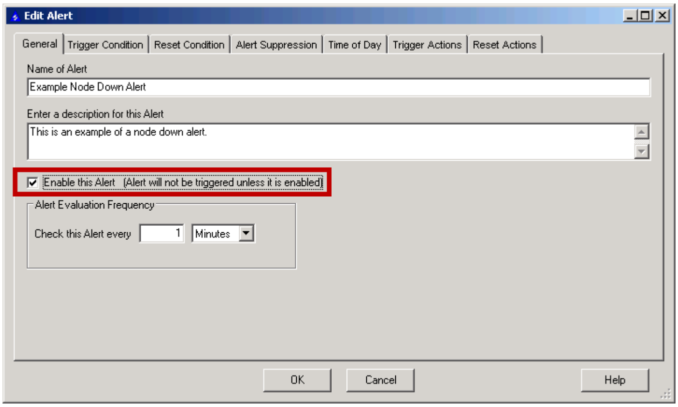
Enter a description for this Alert: This is an example of a node down alert.

☐ Enable this Alert (Alert will not be triggered unless it is enabled)

Alert Evaluation Frequency

Check this Alert every 1 Minutes

6. Check **Enable this Alert**.



Name of Alert: Example Node Down Alert

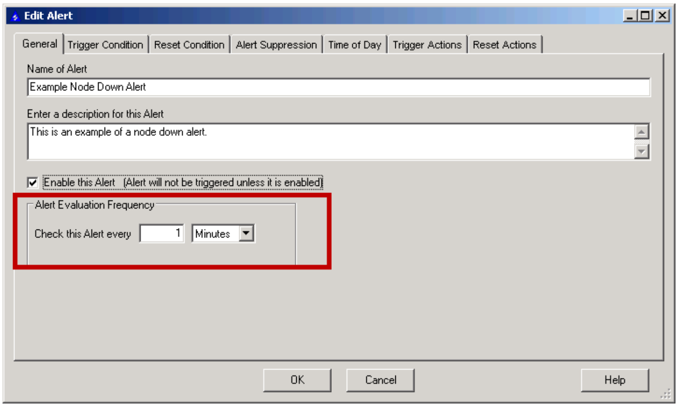
Enter a description for this Alert: This is an example of a node down alert.

☑ Enable this Alert (Alert will not be triggered unless it is enabled)

Alert Evaluation Frequency

Check this Alert every 1 Minutes

7. Type the Alert Evaluation Frequency and select Seconds, Minutes, or Hours from the list to set the checking interval for your alert.



Name of Alert: Example Node Down Alert

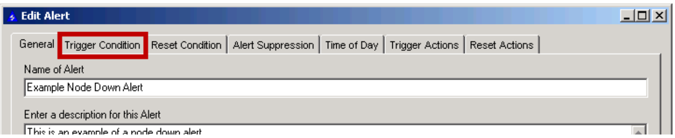
Enter a description for this Alert: This is an example of a node down alert.

☑ Enable this Alert (Alert will not be triggered unless it is enabled)

Alert Evaluation Frequency

Check this Alert every 1 Minutes

8. Click **Trigger Condition** to set the trigger condition for your alert. For more information, see “Setting a Trigger Condition for an Advanced Alert”.



Name of Alert: Example Node Down Alert

Enter a description for this Alert: This is an example of a node down alert

Setting a Trigger Condition for an Advanced Alert

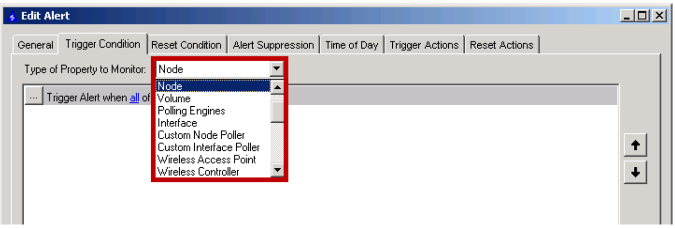
You can set the specific conditions for triggering an advanced alert with the following procedure.

Note: Properly defining alert trigger conditions to address specific network conditions on selected network objects can eliminate the need for alert suppression conditions. SolarWinds recommends the use of appropriately specific trigger conditions to define alerts instead of suppression conditions, if possible. For more information about defining conditions, see “Understanding Condition Groups”.

To set the trigger conditions for an advanced alert:

1. Click **Start > SolarWinds Orion > Alerting, Reporting, and Mapping > Advanced Alert Manager.**
2. Click **View > Configure Alerts**.
3. ***If you want to create a new alert,*** click **New.**
4. ***If you want to copy or edit an existing alert,*** select an alert from the list, and then click **Copy** or **Edit**, as appropriate.
5. Click **Trigger Condition**.
6. Select the **Type of Property to Monitor** from the list.

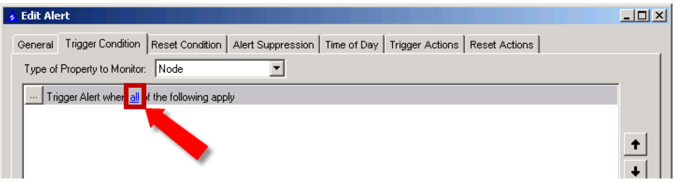
   Note: The following image is a screen capture from an Orion Network Performance Monitor installation. Other modules will look similar, but different objects may be present.



Type of Property to Monitor: Node

Trigger Alert when all of

7. ***If you select* Custom SQL Alert*,*** complete the following steps:
   a. Select the object on which you want to alert in the **Set up your Trigger Query** field.
   b. Provide your custom SQL in the field below the object selection query.
   c. ***If you want to delay the trigger of this alert,*** provide the value and unit of your desired alert trigger delay.
   d. ***If you want to confirm your provided SQL,*** click **Validate SQL**.
8. ***If you select a type of monitored object,*** complete the following steps:
   a. Generate trigger conditions in the text field by selecting appropriate descriptors from the linked context menus and by clicking **Browse** (**…**) on the left of the text field.
   b. Click the linked text to select the number of conditions that you want to apply (**all**, **any**, **none**, **not all**). For more information about linked text conditions, see "Understanding Condition Groups".

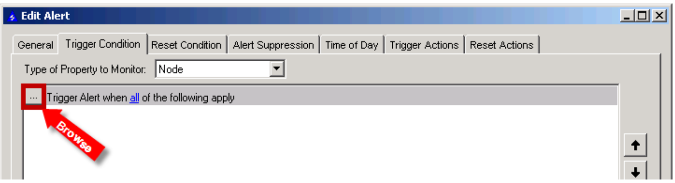


Type of Property to Monitor: Node

Trigger Alert when all of the following apply

   c. Click **Browse** (**…**) to view the following condition options:

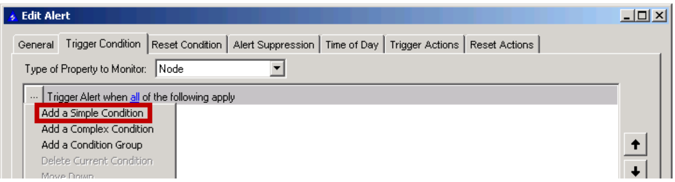
   Note: The **has changed** condition is only valid for the **Last Boot**, **IOS Version**, and **IOS Image Family** device characteristics.



Type of Property to Monitor: Node

Trigger Alert when all of the following apply

- To generate a condition based on a comparison of device states, click **Add a Simple Condition**.



Type of Property to Monitor: Node

Trigger Alert when all of the following apply

- To generate a condition based on a comparison of device fields and values, click **Add a Complex Condition**.
- To define more conditions, click **Add a Condition Group**.
- To remove a selected condition, click **Delete Current Condition**.
- To change the order of your conditions, click **Move Down** or **Move Up**, as appropriate.

d. ***If you need an additional condition,*** click **Browse** (**…**), and then click **Add** *ConditionType*, as appropriate for the condition you want to add.

e. ***If you need to delete a condition,*** click **Browse** (**…**), next to the condition you want to delete, and then click **Delete Current Condition.**

Notes:

- Conditions may be exported for use with other alerts by clicking **Export Conditions** and saving as appropriate.
- Click **Import Conditions** to import existing conditions from other alerts. Imported trigger conditions automatically overwrite any existing trigger conditions.

f. ***If you want to specify a time duration for the condition to be valid,*** type the interval and select Seconds, Minutes, or Hours from the list.

Note: You may need to delay alert trigger actions until a condition has been sustained for a certain amount of time. For example, an alert based on CPU load would not trigger unless the CPU Load of a node has been over 80% for more than 10 minutes. To set up a sustained-state trigger condition, at the bottom of the Trigger Condition tab, provide an appropriate amount of time the alert engine should wait before any actions are performed. By default, the alert triggers immediately, if the trigger condition exists. The maximum alert action delay is eight hours after the trigger condition is met.

g. ***If you are finished configuring your advanced alert,*** click **OK**.

Setting a Reset Condition for an Advanced Alert

Set specific conditions for resetting an advanced alert using the following steps.

To set the conditions for resetting an advanced alert:

1. Click **Start > SolarWinds Orion > Alerting, Reporting, and Mapping > Advanced Alert Manager.**

2. Click **View > Configure Alerts**, and then click **New** or select an alert from the list and click **Copy** or **Edit**.
3. Click **Reset Condition**.
4. ***If you want a simple alert reset when trigger conditions no longer exist,*** select **Reset when trigger conditions are no longer true**.
5. ***If you want a conditional alert reset,*** select **Reset this alert when the following conditions are met**.

   Notes: Generate reset conditions in the text field by selecting appropriate descriptors from the linked context menus and by clicking **Browse** (**…**).
6. ***If you want to copy the condition used on the Trigger Condition tab,*** click **Copy From Trigger**.
7. Click the linked text to select the number of conditions to apply. For more information, see “Understanding Condition Groups”.
8. Click **Browse** (**…**) to view the following condition options:

- To generate a condition based on a comparison of device states, click **Add a Simple Condition**.
- To generate a condition based on a comparison of device fields and values, click **Add a Complex Condition**.
- To further define condition application, click **Add a Condition Group**.
- To remove a selected condition, click **Delete Current Condition**.
- To change the order of your conditions, click **Move Down** or **Move Up**.

9. ***If you need an additional condition,*** click **Add**, and then select the type of condition you want to add.
10. ***If you need to delete a condition,*** select the condition from the condition list, and then click **Delete**.

    Notes:

- Conditions may be exported for use with other alerts by clicking **Export Conditions** and saving as appropriate.
- Conditions from other alerts may be imported to the current alert by clicking **Import Conditions**.

  > **Warning:** Imported trigger conditions automatically overwrite any existing trigger conditions.
- Because there are many situations where the reset conditions are the opposite of, or are very similar to, the trigger conditions, SolarWinds has provided a function that copies the trigger conditions to the reset conditions. Click **Copy From Trigger** to add the trigger condition.

11. ***If you want to specify a time duration for the condition to be valid,*** type the time interval and select Seconds, Minutes, or Hours from the list.

    Note: It is often appropriate to delay alert reset actions until a condition has been sustained for a certain amount of time. For example, an alert based on node status would not reset until the node has been up for more than five minutes. To establish a sustained-state reset condition, provide an appropriate interval at the bottom of the Reset Condition tab for the amount of time that the alert engine should wait before any actions are performed. The default setting is to reset the alert immediately, once the reset condition exists. The maximum interval between when the trigger condition first exists and when the corresponding alert action is performed is eight hours.

12. ***If you are finished configuring your advanced alert,*** click **OK**.

Setting a Suppression for an Advanced Alert

You can set the specific conditions for suppressing an advanced alert using the following procedure.

Notes:

- Alert Suppression is only available if you have checked **Show Advanced Features** in the lower left of the Edit Advanced Alert window.
- In many cases, because suppression conditions are checked against all monitored objects on your network, properly defining alert trigger conditions may eliminate the need for alert suppression. For more information about defining alert trigger conditions, see “Setting a Trigger Condition for an Advanced Alert” and “Understanding Condition Groups”.

To set conditions for advanced alert suppression:

1. Click **Start > All Programs > SolarWinds Orion > Alerting, Reporting, and Mapping > Advanced Alert Manager.**
2. Click **View > Configure Alerts**.
3. Click **New** or select an alert from the list.
4. Click **Copy** or **Edit**, as appropriate.
5. Click **Alert Suppression**.

   Note: Generate suppression conditions in the text field by selecting appropriate descriptors from the linked context menus and by clicking **Browse** (**…**) on the left of the text field.

6. ***If you want to copy the condition used on the Trigger Condition tab,*** click **Copy From Trigger**.

7. Click the linked text to select the number of conditions that you want to apply (**all**, **any**, **none**, **not all**). For more information about linked text conditions, see “Understanding Condition Groups”.
8. Click **Browse** (**…**) to view the following condition options:

- To generate a condition based on a comparison of device states, click **Add a Simple Condition**.
- To generate a condition based on a comparison of device fields and values, click **Add a Complex Condition**.
- To further define the application of your conditions, click **Add a Condition Group**.
- To remove a selected condition, click **Delete Current Condition**.
- To change the order of your conditions, click **Move Down** or **Move Up**.

9. ***If you need an additional condition,*** click **Add** and then select the type of condition you want to add.
10. ***If you need to delete a condition,*** select the condition from the condition list, and then click **Delete**.

    Note: Conditions may be exported for use with other alerts by clicking **Export Conditions** and saving as appropriate. Conditions from other alerts may be imported to the current alert by clicking **Import Conditions**.

    Warning: Imported conditions automatically overwrite existing conditions.
11. ***If you are finished configuring your advanced alert,*** click **OK**.

Setting the Monitoring Period for an Advanced Alert

You can select the specific time periods and days that your advanced alert will monitor your network objects with the following procedure.

To set the monitoring time period and days for an advanced alert:

1. Click **Start > All Programs > SolarWinds Orion > Alerting, Reporting, and Mapping > Advanced Alert Manager.**
2. Click **View > Configure Alerts**.
3. Click **New** or select an alert from the list.
4. Click **Copy** or **Edit**.
5. Click **Time of Day**.

6. Enter the time period over which you want to monitor your network.

   Note: Alerts only trigger if the trigger condition is met within this time period.

7. Select the days on which you want to monitor your network.

   Note: Alerts will only trigger if your trigger condition is met on the days selected.

8. ***If you are finished configuring your advanced alert,*** click **OK**.

Setting a Trigger Action for an Advanced Alert

Select actions that will occur when your advanced alert is triggered as follows.

To set a trigger action for an advanced alert:

1. Click **Start > SolarWinds Orion > Alerting, Reporting, and Mapping > Advanced Alert Manager.**
2. Click **View > Configure Alerts**.
3. Click **New** or select an alert from the list, and then click **Copy** or **Edit**, as appropriate.
4. Click **Trigger Actions**.
5. ***If you are adding a new advanced alert action,*** click **Add New Action**, and then select the actions you want to occur when the alert triggers.
6. ***If you are editing an existing advanced alert action,*** select the existing alert action, and then click **Edit Selected Action**.
7. Follow the instructions to configure each action.

   Note: Depending on the type of action selected, different options will be displayed to configure the alert action. For more information about individual alert actions, see “Available Advanced Alert Actions”.

8. ***If you need to delete an action,*** select the action and then click **Delete Selected Action**.
9. ***If you are finished configuring your advanced alert,*** click **OK**.

Setting a Reset Action for an Advanced Alert

Select actions that will occur when your advanced alert is reset with the following procedure.

To set a reset action for an advanced alert:

1. Click **Start > SolarWinds Orion > Alerting, Reporting, and Mapping > Advanced Alert Manager.**
2. Click **View > Configure Alerts**.
3. Click **New Alert**, **Copy Alert**, or **Edit Alert**, as appropriate.
4. Click **Reset Actions**.
5. ***If you are adding a new advanced alert action,*** click **Add New Action**, and then select the actions you want to occur when the alert triggers.
6. ***If you are editing an existing advanced alert action,*** select the existing alert action, and then click **Edit Selected Action**.
7. Follow the instructions to configure each action.

   Note: Depending on the type of action selected, different options display configuring the alert action. For more information about individual alert actions, see “Available Advanced Alert Actions”.
8. ***If you need to delete a selected action,*** click **Delete Selected Action**.
9. ***If you are finished configuring your advanced alert,*** click **OK**.

Alert Escalation

When editing any trigger or reset action, use the Alert Escalation tab, if it is available, to define additional alert action options. Depending on the alert action being configured, any or all of the following options may be available on the Alert Escalation tab:

- To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
- To execute the action repeatedly as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.
- To delay the execution of the alert action, check **Delay the execution of this Action** and then provide an appropriate interval that the alert engine should wait after the alert condition is met before the alert action is executed.

For more information, see Escalated Advanced Alerts.

Understanding Condition Groups

A condition group is a set of user-defined rules governing alert triggers and resets. By default, the condition group `Trigger Alert when all of the following apply` is added when new alert triggers or reset conditions are created. Four different logical descriptors are used to create conditions: `all`, `any`, `none`, and `not all`, and clicking the word `all` and enables you to select different values. The following sections describe these logical descriptors.

All Condition Group

`Trigger Alert when` *`all`* `of the following apply` means that every condition in the group must be true before the alert is triggered.

In the following example, there are three conditions within the condition group:

- Node Status is equal to Up.
- Percent Loss is greater than or equal to 75.
- CPU Load is greater than or equal to 85.

This alert will not trigger unless the Node is Up, packet loss is greater than or equal to 75%, and CPU load is greater than or equal to 85%.

When setting the condition group to *`all`*, picture every condition as being separated by an *and* statement. So, in this example, the alert trigger would read:

```
Alert when: (Node Status = Up) and (Percent Loss >= 75) and (CPU
Load >= 85)
```

Any Condition Group

Changing the condition group to `Trigger Alert when` *`any`* `of the following apply` changes the logic to *`or`* statements. In this example, changing the condition group to *`any`* would change the alert trigger to:

```
Alert when: (Node Status = Up) or (Percent Loss >= 75) or (CPU
Load >= 85)
```

In this situation, if **any** of the three conditions become true, the alert will trigger.

None Condition Group

Changing the condition group to `Trigger Alert when` *`none`* `of the following apply` means that all conditions in the group must be false before the alert is triggered.

In this example the alert trigger would read:

```
Alert when: (Node Status = Down) and (Percent Loss <= 75) and
(CPU Load <= 85)
```

Each condition is separated by an *and* statement just like the *`all`* condition group; however, the conditions have been inverted (`Node Status = Down` instead of `Node Status = Up`).

Not All Condition Group

Changing the condition group to `Trigger Alert when` *`not all`* `of the following apply` means that any condition in the group must be false before the alert is triggered. So, in this example the alert trigger would read:

```
Alert when: (Node Status = Down) or (Percent Loss <= 75) or (CPU
Load <= 85)
```

Each condition is separated by an *or* statement just like the *any* condition group; however, the conditions have been inverted (`Node Status = Down` instead of `Node Status = Up`).

Using the Advanced Alert Manager

The Advanced Alert Manager is an interface used to view network events and alerts. You can also use Advanced Alert Manager to create and manage advanced alerts. The following procedures introduce the main features of the Advanced Alert Manager showing how to configure and view advanced alerts.

Current Events Window

The Current Events window of the Advanced Alert Manager shows the most recent network events with their descriptions and other information from the events log.

To use the Current Events window to view network events:

1. Click **Start > All Programs > SolarWinds Orion > Alerting, Reporting, and Mapping > Advanced Alert Manager**.
2. Click **View > Current Events**.
3. Select an appropriate **Group By:** criterion for grouping events.

4. ***If you want to change the viewable category columns in the Current Events window,*** click **Include**, and then complete the following procedure:
    a. Click the Event View Columns tab, and then select column IDs from the **All Columns** field.
    b. Click the right arrow to move your column IDs into the **Selected Columns** field.
    c. ***If there are any column IDs in the*** **Selected Columns** ***field that you do not want to view,*** select them, and then click the left arrow to move your selected column IDs to the **All Columns** field.
    d. Click the up or down arrows to change the order of your selected columns accordingly.
    e. Position the slider to set the Event View refresh rate.
    f. Type the number of events that you want to be able to review in the **Display a maximum of** XXXX **events in the Event View** field.
    g. ***If you are finished configuring your Current Events View,*** click **OK**.
5. Click **Refresh** to update the Current Events window with the latest events and column IDs.
6. ***If you want to acknowledge a network event,*** click **X** next to the event.

Active Alerts Window

The Active Alerts window of the Advanced Alert Manager shows network alerts with their descriptions and other information from the alerts log.

To use the Active Alerts window to view active network alerts:

1. Click **Start > All Programs > SolarWinds Orion > Alerting, Reporting, and Mapping > Advanced Alert Manager**.
2. Click **View > Active Alerts**.
3. Select an appropriate **Group By:** criterion for grouping alerts.
4. Click **Include**, and then check the types of alerts that you want to view: **Acknowledged**, **Trigger Pending**, **Triggered**, or **Reset Pending**.
5. ***If you want to change the viewable category columns in the Current Events window,*** click **Include > Select Alert Columns**, and then complete the following procedure:
    a. Select column IDs from the **All Columns** field.
    b. Click the right arrow to move your column IDs into the **Selected Columns** field.

   c. ***If there are any column IDs in the* Selected Columns *field that you do not want to view,*** select them, and then click the left arrow to move your selected column IDs to the **All Columns** field.
   d. Click the up or down arrows to change the order of your selected columns accordingly.
   e. Position the slider to set the Alert View refresh rate.
   f. ***If you are finished configuring your Active Alerts View,*** click **OK**.
6. Click **Refresh** to update the Active Alerts window with the latest alerts and column IDs.
7. Click **Configure Alerts** to change the settings for individual alerts.
8. ***If you want to acknowledge an active alert,*** check the alert in the **Acknowledged** column.

   Note: As soon as the alert is acknowledged, the user information and date/time is recorded in the database.

Alert Viewer Settings

Alert views in the Orion Advanced Alert Manager are configured in the Alert Viewer Settings window, as presented in the following procedure.

To configure alert views in the Advanced Alert Manager:

1. Click **Start > All Programs > SolarWinds Orion > Alerting, Reporting, and Mapping > Advanced Alert Manager**.
2. Click **File > Settings**.

   Note: The Configure Alerts tab of the Alert Viewer Settings window displays all available network alerts, and from this window you can create, copy, edit, and delete alerts. For more information, see “Creating and Configuring Advanced Alerts”.
3. Click **Alert View Columns**.
4. Select the information titles that you want to see about your alerts from the **All Columns** list.
5. Click the right arrow to transfer them to the **Selected Columns** list.

   Note: The Selected Columns list provides a list of all the information that the Alert Viewer will show for each active alert.
6. ***If you want to remove titles from the Selected Columns list,*** select titles that you want to remove from the active view in the **Selected Columns** list, and then click the left arrow.

7. ***If you want to rearrange the order in which the different pieces of alert information are presented in the Alert Viewer,*** select titles from the **Selected Columns** list and use the up and down arrows to arrange the titles accordingly.
8. Position the slider at the bottom of the tab to set the Alert View refresh rate.
9. Click **Event View Columns**.
10. Select the information titles that you want to see about events from the **All Columns** list.
11. Click the right arrow to transfer them to the **Selected Columns** list.

    Note: The Selected Columns list provides a list of all the information that the Alert Viewer will show for each recorded event.
12. ***If you want to remove titles from the Selected Columns list,*** select titles that you want to remove from the active view in the **Selected Columns** list, and then click the left arrow.
13. ***If you want to rearrange the order in which the different pieces of event information are presented in the Alert Viewer,*** select titles from the **Selected Columns** list and use the up and down arrows to arrange the titles accordingly.
14. Position the slider at the bottom of the tab to set the Event View refresh rate.
15. Enter the number of events that you want to see in the Event View.

Adding Alert Actions

SolarWinds provides a variety of actions to signal an alert condition on your network. These alert actions are available for both basic and advanced alerts, and the following procedure assigns actions to the alert conditions that you have defined for your network.

To add an alert action:

1. Click **Start > All Programs > SolarWinds Orion > Network Performance monitor > System Manager**.
2. Click **Alerts > Active Alerts**, and then click either **Configure Basic Alerts** or **Configure Advanced Alerts**, as appropriate.
3. Check the alert to trigger your action, and then click **Edit Alert**.
4. Click **Actions**, and then select the action you want to edit.
5. Click **Add Alert Action**, and then click the action to add to your chosen alert.

For more information about individual alert actions, see Available Advanced Alert Actions.

Available Advanced Alert Actions

The following sections detail the configuration of available alert actions:

- Sending an E-mail/Page
- Playing a Sound
- Logging an Advanced Alert to a File
- Logging an Advanced Alert to the Windows Event Log
- Logging an Advanced Alert to the NetPerfMon Event Log
- Sending a Syslog Message
- Executing an External Program
- Executing a Visual Basic Script
- Emailing a Web Page
- Using Text to Speech Output
- Sending a Windows Net Message
- Sending an SNMP Trap
- Using GET or POST URL Functions
- Dial Paging or SMS Service

Sending an E-mail/Page

The following procedure configures an e-mail/page action for an advanced alert.

Notes:

- Confirm that the polling engine you have configured to trigger your alert has access to your SMTP server.
- Emails and pages are sent in plain text.

To configure an email/page action for an advanced alert:

1. Click **E-mail/Pager Addresses**, and then complete the **To**, **CC**, **BCC**, **Name**, and **Reply Address** fields.

   Note: You must provide at least one email address in the **To** field, and multiple addresses must be separated with commas. Some pager systems require a valid reply address to complete the page.

2. Click **Message**, and then select your email format (**Plain text** or **HTML**).

3. Type the **Subject** and **Message** of your alert trigger email/page.

   Note: Messaging is disabled if both **Subject** and **Message** fields are empty.

4. ***If you want to insert a variable into the Subject or Message field,*** click the location of the new variable, and then complete the following procedure:
   a. Click **Insert Variable**.
   b. Select a **Variable Category**, and then select the variable to add.
   c. ***If you want to change the parser,*** check **Change Parser**, and then select the parser you want to use.
   d. ***If you want to define the SQL variable to copy to the clipboard,*** check **Define SQL Variable**, and then click **Insert Variable From Above List**.
   e. Click **Build Selected Variable**.

      Note: For more information on the use of variables, see “Orion Variables and Examples”. For more information about messages that use variables, see “Example Messages Using Variables”.

5. Click **SMTP Server**.

6. Type the **Hostname or IP Address of your SMTP Server** and the designated **SMTP Port Number**.

   Note: The SMTP server hostname or IP address field is required. You cannot send an email/page alert without identifying the SMTP server.

7. ***If you want to use SSL/TLS encryption for your alert email,*** check **Enable SSL**.

8. ***If your SMTP server requires authentication,*** check **This SMTP Server requires Authentication**.

9. Click **Time of Day**.

10. Enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.

11. ***If you want to enable alert escalation,*** click the Alert Escalation tab, and then check any of the following options, as appropriate for your alert:

- To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
- To execute the action repeatedly as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.

- To delay alert action execution, check **Delay the execution of this Action**, and then provide an appropriate interval the alert engine should wait after the alert condition is met before the alert action is executed.

12. ***If you are finished configuring your email/page alert action,*** click **OK**.

Playing a Sound

The following procedure configures a sound to play for an advanced alert.

Note: Due to restrictions on Windows service applications, the Play a Sound action is not available to Orion installations on either Windows 7 or Windows Server 2008 and higher.

To configure a play sound action for an advanced alert:

1. Click **Play Sound**.
2. Specify a sound file for the alert trigger by doing either of the following in the **Sound file to play** field:

- Type the complete directory path and file name.
- Click **Browse** (**…**) to navigate your file system and select the target file.

3. Click the musical note button to the right of either text field to test the sound file you have specified.
4. Click **Time of Day**.
5. Enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.
6. ***If you want to enable alert escalation,*** click **Alert Escalation**, and then check any of the following options, as appropriate for your alert:

- To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
- To execute the action repeatedly as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.
- To delay alert action execution, check **Delay the execution of this Action**, and then provide an appropriate interval the alert engine should wait after the alert condition is met before the alert action is executed.

7. ***If you are finished configuring your play a sound alert action,*** click **OK**.

Logging an Advanced Alert to a File

Orion can be configured to log alerts to a designated file. The following procedure logs an advanced alert to a designated file

To configure an alert log file for an advanced alert:

1. Click **Event Log**, and then specify an alert log file by doing either of the following in the **Alert Log Filename** field:

   Note: If the file specified does not exist, it will be created with the first alert occurrence.

- Type the complete path and name of the target file.
- Click **Browse (…)** to navigate your file system and select the target file.

2. Type the message you want to log to your alert log file in the **Message** field.
3. ***If you want to insert a variable into the Message field,*** complete the following procedure:
   a. Click **Insert Variable**, and then select a **Variable Category**.
   b. Select the variable you want to add.
   c. ***If you want to change the parser,*** check **Change Parser**, and then select the parser you want to use.
   d. ***If you want to define the SQL variable to copy to the clipboard,*** check **Define SQL Variable**, and then click **Insert Variable From Above List**.
   e. Click **Build Selected Variable**.

      Note: For more information on the use of variables, see “Orion Variables and Examples” .
4. Click **Time of Day**.
5. Enter the time period over which you want to activate your alert action.
6. Select the days on which you want to activate your alert action.
7. ***If you want to enable alert escalation,*** click the Alert Escalation tab, and then check any of the following options, as appropriate for your alert:

- To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
- To execute the action repeatedly as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.

- To delay alert action execution, check **Delay the execution of this Action**, and then provide an appropriate interval the alert engine should wait after the alert condition is met before the alert action is executed.

8. ***If you are finished configuring your alert log file,*** click **OK**.

Logging an Advanced Alert to the Windows Event Log

You may specify that an alert be logged to the Windows Event Log either on the Orion server or on a remote server. The following procedure logs an advanced alert to the Windows Event Log on a designated server.

To configure advanced alert logging to the Windows Event Log:

1. Click **Windows Event Log**.
2. ***If you want your alert to write to the Windows Event Log on your Orion server,*** select **Use Event Log Message on Network Performance Monitor Server**.
3. ***If you want your alert to write to the Windows Event Log on a remote server,*** select **Use Event Log Message on a Remote Server**, and then provide the **Remote Server Name or IP Address**.
4. Type the message you want to log to the Windows Event Log in the **Message to send to Windows Event Log** field.
5. ***If you want to insert a variable into the Message field,*** complete the following procedure:
   a. Click **Insert Variable**.
   b. Select a **Variable Category**.
   c. Select the variable you want to add.
   d. ***If you want to change the parser,*** check **Change Parser**, and then select the parser you want to use.
   e. ***If you want to define the SQL variable to copy to the clipboard,*** check **Define SQL Variable**, and then click **Insert Variable From Above List**.
   f. Click **Build Selected Variable**.

      Note: For more information on the use of variables, see “Orion Variables and Examples”.
6. Click **Time of Day**.
7. Enter the time period and select the days over which you want to activate your alert action.

8. ***If you want to enable alert escalation,*** click **Alert Escalation**, and then check any of the following options, as appropriate for your alert:

- To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
- To execute the action repeatedly as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.
- To delay alert action execution, check **Delay the execution of this Action**, and then provide an appropriate interval the alert engine should wait after the alert condition is met before the alert action is executed.

9. ***If you are finished configuring your alert log file,*** click **OK**.

Logging an Advanced Alert to the NetPerfMon Event Log

You may specify that an alert be logged to the NetPerfMon Event Log either on the Orion server or on a remote server. The following procedure logs an advanced alert to the NetPerfMon Event Log on a designated server.

To configure advanced alert logging to the NetPerfMon Event Log:

1. Click **NPM Event Log**.
2. Type the message you want to log to the NetPerfMon Event Log in the **Message to send to Network Performance Monitor Event Log** field.
3. ***If you want to insert a variable into the Message field,*** complete the following procedure:
   a. Click **Insert Variable**.
   b. Select a **Variable Category**.
   c. Select the variable you want to add.
   d. ***If you want to change the parser,*** check **Change Parser**, and then select the parser you want to use.
   e. ***If you want to define the SQL variable to copy to the clipboard,*** check **Define SQL Variable**, and then click **Insert Variable From Above List**.
   f. Click **Build Selected Variable**.

   Note: For more information on the use of variables, see “Orion Variables and Examples”.
4. Click **Time of Day**.
5. Enter the time period and select the days over which you want to activate your alert action.

6. ***If you want to enable alert escalation,*** click **Alert Escalation**, and then check any of the following options, as appropriate for your alert:

- To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
- To execute the action repeatedly as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.
- To delay alert action execution, check **Delay the execution of this Action**, and then provide an appropriate interval the alert engine should wait after the alert condition is met before the alert action is executed.

7. ***If you are finished configuring your alert log file,*** click **OK**.

Sending a Syslog Message

Orion can log received alerts to the Syslog of a designated machine. The following procedure configures an advanced alert to send a message to a designated Syslog server.

To configure an advanced alert to send a Syslog message:

1. Click **Syslog Message**.
2. Type the **Hostname or IP Address of the Syslog Server** to which you want to send Syslog messages.
3. Select the **Severity** of your alert Syslog message.
4. Select **Facility** of your alert Syslog message.
5. Type the **Syslog Message** you want to send.
6. ***If you want to insert a variable into the Message field,*** complete the following procedure:
   a. Click **Insert Variable**.
   b. Select a **Variable Category**.
   c. Select the variable you want to add.
   d. ***If you want to change the parser,*** check **Change Parser**, and then select the parser you want to use.
   e. ***If you want to define the SQL variable to copy to the clipboard,*** check **Define SQL Variable**, and then click **Insert Variable From Above List**.

   f. Click **Build Selected Variable**.

      Note: For more information on the use of variables, see “Orion Variables and Examples”.

7. Click **Time of Day**.
8. Enter the time period over which you want to activate your alert action.
9. Select the days on which you want to activate your alert action.
10. ***If you want to enable alert escalation,*** click **Alert Escalation**, and then check any of the following options, as appropriate for your alert:

- To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
- To execute the action repeatedly as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.
- To delay alert action execution, check **Delay the execution of this Action**, and then provide an appropriate interval the alert engine should wait after the alert condition is met before the alert action is executed.

11. ***If you are finished with the configuration of your send Syslog message action,*** click **OK**.

Executing an External Program

There are several circumstances where you may want to execute a program when a specific network event occurs. Use the Edit Execute Program Action window to specify the executable that should be started when the specified alert is triggered or reset, as shown in the following procedure.

Note: External programs selected for this action must be executable using a batch file called from the command line.

To configure an advanced alert to execute an external program:

1. Click **Execute Program**.
2. Specify the batch file to execute, either by typing the complete path and name of the target file into the **Program to execute** field or by clicking **Browse** (**…**), to browse your folder structure and select the target executable.
3. Click **Time of Day**, and then enter the time period when you want to execute the external program.
4. Select the days on which you want to execute the external program.

5. Click **Alert Escalation**, and then check any of the following options, as appropriate for your alert:

- To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
- To execute the action repeatedly, while the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered**, and then provide an action execution interval.
- To delay alert action execution, check **Delay the execution of this Action**, and then provide the interval the alert engine should wait.

6. ***If you are finished configuring your external program execution action,*** click **OK**.

Executing a Visual Basic Script

In some situations you may want to execute a Visual Basic (VB) script when a network event occurs. The Edit Execute VB Script Action window is used to specify the name and complete path of the file that shall be executed when the specified alert is triggered or reset.

To configure alerts to execute a Visual Basic (VB) script:

1. Click **VB Script**.
2. Select an available **VB Script Interpreter**.
3. Specify a VB script to execute either by typing the complete path and name of the VB script into the **VB Script to execute** field or by clicking **Browse (…)** to browse your folder structure and select the script.
4. Click **Time of Day**, and then enter the time period and select the days on which you want to execute the selected VB script.
5. Click **Alert Escalation**, and then check any of the following options, as appropriate for your alert:

- To disable the script when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
- To execute the script repeatedly as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.
- To delay script execution, check **Delay the execution of this Action**, and then provide an appropriate interval the alert engine should wait after the alert condition is met before the script executes.

6. ***If you are finished configuring your VB script execution action,*** click **OK**.

Emailing a Web Page

The Edit E-mail Web Page Action window includes several tabs for configuration. The following procedure configures an e-mail URL action for an advanced alert.

Note: Emails are sent in plain text.

To configure an email web page action for an advanced alert:

1. Click **E-mail a Web Page**, and then click **OK**.
2. Complete the **To**, **CC**, **BCC**, **Name**, and **Reply Address** fields.

   Note: You must provide at least one address in the **To** field. When entering multiple addresses, you may only separate addresses with a comma. Some pager systems require a valid reply address to complete the page.
3. Click **SMTP Server**.
4. Type the **Hostname or IP Address of your SMTP Server** and the designated **SMTP Port Number**.

   Note: The SMTP server hostname or IP address field is required. You cannot email a web page without identifying the SMTP server.
5. Click **URL**, and then type the **Subject** of your alert email.

   Note: Messaging is disabled if both **Subject** and **URL** fields are empty.
6. ***If you want to insert a variable into the Subject field,*** click the location of the new variable, and then complete the following procedure:
   a. Click **Insert Variable**, select a **Variable Category**, and then select the variable to add.
   b. ***If you want to change the parser,*** check **Change Parser**, and then select the parser you want to use.
   c. ***If you want to define the SQL variable to copy to the clipboard,*** check **Define SQL Variable**, and then click **Insert Variable From Above List**.
   d. Click **Build Selected Variable**.

      Note: For more information on the use of variables, see “Orion Variables and Examples”. For more information about messages that use variables, see “Example Messages Using Variables”.
7. Provide the **URL** of your alert email.

Note: Messaging is disabled if both **Subject** and **URL** fields are empty.

8. ***If the web server of the URL you want to email requires user access authentication,*** provide both the **Web Server UserID** and the **Web Server Password** in the Optional Web Server Authentication area.
9. Click **Time of Day**, and then enter the time period and select the days when you want to activate your alert action.
10. ***If you want to enable alert escalation,*** click **Alert Escalation**, and then check any of the following options, as appropriate for your alert:

- To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
- To execute the action repeatedly, as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.
- To delay alert action execution, check **Delay the execution of this Action**, and then provide an appropriate interval for the alert engine to wait after the alert condition is met before executing the alert action.

11. ***If you are finished configuring your URL email alert action,*** click **OK**.

Using Text to Speech Output

You may specify a phrase that will be spoken upon alert trigger and a separate phrase for the alert reset. Orion uses Microsoft Speech Synthesis Engine version 5.0, as included with Windows 2003 and XP Professional. If you have Orion maintenance, you may also install and use other text-to-speech engines by visiting the SolarWinds website. The following procedure configures text-to-speech output for an advanced alert trigger or reset.

Note: Due to restrictions on Windows service applications, the Text to Speech action is not available to Orion installations on either Windows 7 or Windows Server 2008 and higher.

To configure a text-to-speech output action for an advanced alert:

1. Click **Text to Speech output**, and then click **OK**.
2. On the General tab, Select a Speech Engine, and then use the sliders to set the required **Speed**, **Pitch** and **Volume**.
3. On the Phrase tab, type the text you want to output as speech in the **Phrase to speak** field.

Note: Click **Speak** to hear the text, as provided, with the options configured as set on the General tab.

4. On the Time of Day tab enter the time period and select the days on which you want to activate your alert action.
5. ***If you want to enable alert escalation,*** open the Alert Escalation tab, and then check any of the following options, as appropriate for your alert:

- To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
- To execute the action repeatedly, as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.
- To delay alert action execution, check **Delay the execution of this Action**, and then provide an appropriate interval for the alert engine to wait after the alert condition is met before executing the alert action.

6. ***If you are finished configuring your text-to-speech alert action,*** click **OK**.

Sending a Windows Net Message

Alerts can be configured to display a pop-up Windows Net Message either on a specific computer or on all computers in a selected domain or workgroup. The following steps configure Windows Net messaging for triggered or reset alerts.

Note: The only operating systems supporting Windows Net Messaging on which SolarWinds supports Orion installations are Windows Server 2003 and Windows XP. SolarWinds only supports evaluation installations of Orion on Windows XP.

To configure Orion to send a Windows Net message upon alert:

1. Click **Send a Windows Net Message**, and then click **OK**.
2. On the Net Message tab, enter the **Computer Name or IP Address** of the machine where you want to send a Windows Net message upon an alert trigger or reset.
3. ***If you want to send the message to all computers in the domain or workgroup of your target computer,*** check **Send to all Computers in the Domain or Workgroup**.
4. Enter the Windows Net message you want to send in the **Message to send** field.

   Note: You may use variables in this message. For more information on the use of variables, see “Orion Variables and Examples”.
5. On the Time of Day tab enter the time period and select the days on which you want to activate your alert action.

6. ***If you want to enable alert escalation,*** open the Alert Escalation tab, and then check any of the following options, as appropriate for your alert:

- To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
- To execute the action repeatedly, as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.
- To delay alert action execution, check **Delay the execution of this Action**, and then provide an appropriate interval for the alert engine to wait after the alert condition is met before executing the alert action.

7. ***If you are finished configuring your text-to-speech alert action,*** click **OK**.

Sending an SNMP Trap

The following steps configure an alert to send an SNMP trap on trigger or reset.

To configure Orion to send an SNMP trap upon alert:

1. Click **Send an SNMP Trap**, and then click **OK**.
2. On the SNMP Trap tab, in the **SNMP Trap Destinations** field, enter the IP addresses of the servers to which you want to send your generated SNMP traps.

   Note: Use commas to separate multiple destination IP addresses.
3. Select the type of trap to send on alert trigger from the **Trap Template** list.

   Note: Some trap templates may use an alert message. You may change any provided text, if you want, but it is important that you understand the use of variables beforehand. For more information about using variables, see “Orion Variables and Examples”.
4. Enter the **SNMP Community String** for your network in the designated field.
5. On the Time of Day tab enter the time period and select the days on which you want to activate your alert action.
6. ***If you want to enable alert escalation,*** open the Alert Escalation tab, and then check any of the following options, as appropriate for your alert:

- To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
- To execute the action repeatedly, as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.

- To delay alert action execution, check **Delay the execution of this Action**, and then provide an appropriate interval for the alert engine to wait after the alert condition is met before executing the alert action.

7. ***If you are finished configuring your SNMP trap alert action,*** click **OK**.

Using GET or POST URL Functions

Orion can be configured to communicate alerts using HTTP GET or POST functions. As an example, a URL may be used as an interface into a trouble ticket system, and, by correctly formatting the GET function, new trouble tickets may be created automatically. The following procedure configures Orion to use GET or POST HTTP functions to communicate alert information.

To configure Orion to use GET or POST URL functions with alerts:

1. Click **Get or Post a URL to a Web Server**, and then click **OK**.
2. Select either **Use HTTP GET** or **Use HTTP POST** to set the function that you want to use to communicate alert information.
3. ***If you selected Use HTTP GET,*** enter the **URL** you want to GET.
4. ***If you selected Use HTTP POST,*** enter the **URL** you want to POST, and then enter the **Body to POST**.
5. On the Time of Day tab enter the time period and select the days on which you want to activate your alert action.
6. ***If you want to enable alert escalation,*** open the Alert Escalation tab, and then check any of the following options, as appropriate for your alert:

- To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
- To execute the action repeatedly, as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.
- To delay alert action execution, check **Delay the execution of this Action**, and then provide an appropriate interval for the alert engine to wait after the alert condition is met before executing the alert action.

7. ***If you are finished with the configuration of Orion to use HTTP GET or POST URL functions,*** click **OK**.

Dial Paging or SMS Service

If NotePager Pro is installed Orion can be configured to communicate alerts using paging and SMS services. For more information about installation and configuration, see “SolarWinds Orion Network Performance Monitor Integration” at www.notepage.net.

Testing Alert Actions

The Advanced Alert Manager provides an alert action test feature so you can confirm the desired function for actions you have configured to fire when Orion detects an alert condition on your network. Complete the following procedure to test an alert action.

To test an alert action:

1. Click **Start > All Programs > SolarWinds Orion > Alerting, Reporting, and Mapping > Advanced Alert Manager**.
2. Click **Configure Alerts**.
3. Click the alert for which the action you want to test is configured.
4. Click **Test**.
5. ***If the alert is configured to fire on a node condition,*** select **Alert on Network Node**, and then select the node against which you want to test the action.
6. ***If the alert is configured to fire on an interface condition,*** complete the following steps:

   Note: Testing alert actions against interfaces is only available if Orion Network Performance Monitor is installed and monitoring interfaces on your network. For more information, see the *SolarWinds Orion Network Performance Monitor Administrator Guide*.

   a. Select **Alert on Network Node**, and then select the parent node of the interface against which you want to test the action.
   b. Select **Select Interface on** *ParentNode*, and then select the interface against which you want to test the action.
7. ***If the alert is configured to fire on a volume condition,*** complete the following steps:
   a. Select **Alert on Network Node**, and then select the parent node of the volume against which you want to test the action.
   b. Select **Select Volume on** *ParentNode*, and then select the volume against which you want to test the action.

8. ***If you are testing an alert trigger action,*** click **Test Alert Trigger**.
9. ***If you are testing an alert reset action,*** click **Test Alert Reset**.
10. When the test completes, as indicated by the test log, click **Done**.

Confirm that the expected action occurred as a result of the selected alert trigger or reset.

Viewing Alerts in the Orion Web Console

The Triggered Alerts for All Network Devices page provides a table view of your alerts log. You can customize the list view by using the following procedure to select your preferred alert grouping criteria.

To view alerts in the Web Console:

1. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
2. Click **Alerts** in the Views toolbar.
3. ***If you want to filter your alerts table view by device,*** select the device to which you want to limit your alerts view in the **Network Object** field.
4. ***If you want to filter your alerts table by type of device,*** select the device type to which you want to limit your alerts view in the **Type of Device** field.
5. ***If you want to limit your alerts table to show a specific type of alert,*** select the alert type in the **Alert Name** field.
6. In the **Show Alerts** field, provide the number of alerts you want to view.
7. ***If you want to show all alerts, even if they have already been cleared or acknowledged,*** check **Show Acknowledged Alerts**.
8. Click **Refresh** to complete your Alerts view configuration.

Acknowledging Advanced Alerts in the Web Console

Orion NTA allows you to acknowledge advanced alerts in the Orion Web Console, allowing you to eliminate time lost either when multiple users attempt to resolve the same issue or when a user tries to address an issue that has already been resolved.

To acknowledge advanced alerts using the Orion Web Console:

1. Log in to the Orion Web Console using an account that has been granted alert acknowledgement privileges.

   Note: For more information about access privileges for Orion Web Console users, see “User Account Access Settings”.
2. Click **Alerts** on the Views toolbar.

3. ***If you want to limit the list of alerts to only those dealing with a single device,*** select the specific device from the **Network Object** list.

   Note: This option is only available if alerts fire on multiple network devices.

4. ***If you want to limit the list of alerts to only those dealing with a single type of device,*** select the device type from the **Type of Device** list.

   Note: This option is only available if Orion is monitoring multiple types of network devices.

5. ***If you want to limit the list of alerts to only those of a single type,*** select the specific alert type from the **Alert Name** list.

   Note: This option is only available when multiple types of Orion NTA alerts have been triggered.

6. Confirm the number of alerts displayed in the **Show Alerts** field.
7. ***If you want acknowledged alerts to remain in the Alerts view, even after they have been acknowledged,*** check **Show Acknowledged Alerts**.
8. Click **Refresh** to update the alerts list with your new settings.
9. Check **Acknowledged** next to the alerts you want to acknowledge.
10. Click **Acknowledge Alerts**.

Escalated Advanced Alerts

By creating an escalated alert, Orion NTA enables you to customize a series of alerts to trigger successive actions as an alert condition persists. The following sections provide a scenario where an escalated alert may be useful and the steps required to create a series of escalated alerts using the Orion Advanced Alert Manager.

Escalated Alert Example

WidgetCo is a business with a small IT staff, consisting of two technicians and an IT manager. To ensure that issues are addressed appropriately, the IT manager has created multiple escalated alerts for a range of potential network events, including device failures and excessive disk space or bandwidth usage. Typically, the escalated alerts configured by the WidgetCo IT manager proceed as follows:

1. Immediately, as soon as Orion NTA recognizes an alert condition, Orion NTA generates both an email and a page that are sent to one of the two technicians. An entry is also recorded in the Orion events log.
2. If the alert is not acknowledged in the Orion Web Console within 20 minutes, a second alert is fired, generating another email and another page, both sent to both technicians. An entry is also recorded in the Orion events log.

3. If the second alert is not acknowledged within 20 minutes, Orion NTA fires a third alert that sends both an email and a page to both technicians and to the IT manager. An entry is also recorded in the Orion events log.

Escalated alerts ensure that everyone on the WidgetCo IT staff is notified of any significant network alert conditions within 45 minutes without burdening the IT manager with excessive alert notifications. The following section provides a procedure to create a similar escalated alert scheme.

Creating a Series of Escalated Alerts

The following procedure creates a series of escalated alerts similar to the scheme described in the preceding example.

Note: Repeat these steps to create a separate alert for each notification level. The example provided in the previous section uses a three-level escalated alert, The following procedure should be completed three times, once for each alert, to replicate the escalated alert of the previous section.

To create an escalated alert:

1. Click **Start > All Programs > SolarWinds Orion > Alerting, Reporting, and Mapping > Advanced Alert Manager**.
2. Click **Configure Alerts**.
3. Click **New**, and then click **General.**
4. Type `Level` *`X`* , where *X* is the level corresponding to the currently configured alert, as the name of your escalated alert in the **Name of Alert** field.

   Note: The example provided in the previous section uses a three-level escalated alert.
5. Type a description of your first level escalated alert in the description field, and then check **Enable this Alert**.
6. Type the Alert Evaluation Frequency and select Seconds, Minutes, or Hours from the list to set the checking interval for your alert.
7. Click **Trigger Condition.**

   Note: For more information about configuring trigger conditions, see "Setting a Trigger Condition for an Advanced Alert".
8. Select **Node** as the Type of Property to Monitor.
9. Confirm that the linked text in the alert definition field displays **all**.

Note: Click the linked text to select the number of conditions that you want to apply (**all**, **any**, **none**, **not all**). For more information about linked text conditions, see “Understanding Condition Groups”.

10. Click **Browse** (**…**), and then click **Add a Simple Condition**.
11. Click the first asterisk (*****), and then select **Network Nodes > Node Details > Node Name**.
12. Confirm that **is equal to** is the linked condition text in the trigger definition.

    Note: Click the linked text to select the condition you want to apply (**equal**, **greater**, **less**, **…**). For more information about linked text conditions, see “Understanding Condition Groups”.
13. Click the second asterisk (*****), and then select your production web server from the list of monitored nodes.
14. Click **Add**, and then click **Simple Condition**.
15. Click the first asterisk (*****) in the second condition, and then select **Network Nodes > Node Status > Node Status**.
16. Confirm that **is equal to** is the linked condition text in the second trigger definition.

    Note: Click the linked text condition to select the condition you want to apply (**equal**, **greater**, **less**, **…**). For more information about linked text conditions, see “Understanding Condition Groups”.
17. Click the second asterisk (*****) in the second condition, and then select **Down**.
18. ***If you want to apply any reset conditions to your escalated alert,*** click **Reset Condition**, and then provide appropriate conditions. For more information, see “Setting a Reset Condition for an Advanced Alert”.
19. ***If you want to apply any alert suppressions to your escalated alert,*** click **Alert Suppression**, and then provide appropriate suppression conditions. For more information, see “Setting a Suppression for an Advanced Alert”.
20. ***If you want to restrict when your escalated alert is valid,*** click **Time of Day**, designate the Valid Time of Day for your escalated alert, and then select the Days of the Week on which your escalated alert is valid. For more information, see “Setting the Monitoring Period for an Advanced Alert”.

    Note: By default, your escalated alert is always valid.
21. Click **Trigger Actions**, and then click **Add New Action**.
22. Select **Send an E-mail / Page**, and then click **OK**.

23. Click **E-mail/Pager Addresses**, and then complete the **To**, **CC**, **BCC**, **Name**, and **Reply Address** fields for your Level 1 contact.

    Note: You must provide at least one email address in the **To** field. When entering multiple addresses in a field, y separate addresses with a comma.

24. Click **Message**, and then type the **Subject** and **Message** of your escalated alert email.

    Notes:

- Messaging is disabled if both **Subject** and **Message** fields are empty.
- For more information about variables in email subjects and messages, see "Sending an E-mail / Page".

25. Click **SMTP Server**, and then provide the **Hostname or IP Address of your SMTP Server** and the designated **SMTP Port Number**.

    Note: The SMTP server hostname or IP address field is required. You cannot send an email/page alert without identifying the SMTP server.

26. ***If your SMTP server requires authentication,*** check **This SMTP Server requires Authentication**.
27. ***If you want to restrict when your escalated alert is valid,*** check **Execute this Action only between specific hours**, and then configure the appropriate settings.

    Note: By default, your escalated alert is always valid. For more information, see "Setting the Monitoring Period for an Advanced Alert".

28. Click **Alert Escalation**.
29. Check **Do not execute this Action if the Alert has been Acknowledged**.
30. ***If you want to execute the action repeatedly as long as the trigger condition exists,*** check **Execute this Action repeatedly while the Alert is Triggered**, and then provide an appropriate action execution interval.
31. ***If you want to delay alert action execution,*** check **Delay the execution of this Action**, and then provide an appropriate interval the alert engine should wait after the alert condition is met before the alert action is executed.

    Note: Typically, if you are configuring the first level alert, you should leave this option unchecked. If you are configuring the second level alert, check this option and provide the desired delay between the first and second notifications. If you are configuring the third level alert, check this option and provide the desired delay between the first and third notifications.

32. Click **OK**.

33. ***If you want your escalated alert to perform any actions upon reset,*** click the Reset Action tab, and then configure appropriate actions. For more information, see “Setting a Reset Action for an Advanced Alert”.
34. ***If you are finished configuring your escalated alert,*** click **OK**.

Viewing Alerts from Mobile Devices

Orion NTA is capable of detecting when you are accessing the Orion Web Console from a mobile device. This mobile alerts view allows you to view and acknowledge existing active alerts.

To view and acknowledge alerts from a mobile device:

1. Using a browser on your mobile device, log in to your Orion Web Console as a user with alert management rights.
2. Click **Alerts** in the Views toolbar.

   Note: If you want to view the mobile alerts view from a desktop or server browser, add `?IsMobileView=true` to the URL of the Alerts view in your Orion Web Console.
3. Check alerts you want to acknowledge, and then click **Acknowledge**.

Clickable links in alert messages provide more information about triggered alerts.

Chapter 8

Monitoring Autonomous System Networks (through BGP)

Orion NTA supports monitoring autonomous system networks and autonomous system conversations. You setup network devices within autonomous systems

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

Preparing to Monitor Autonomous System Networks

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

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

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

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

- Each device must be configured as part of an autonomous system network, with specified connections to all neighbors within the system.
- Each device must be configured to export NetFlow data to Orion NTA.
- Each device that exports NetFlow data to Orion NTA must be monitored in Orion NPM.
- Traffic from a device that is not monitored in Orion NPM appears only in aggregate as part of the traffic from all unmonitored devices. If the device is setup to export data to Orion NTA, but is unmonitored in NPM, the collector may receive the data without being able to meaningfully analyze it.

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

Follow the procedures in this section to setup each autonomous system network device; and to verify that each device correctly exports NetFlow data to Orion NTA.

To setup a device for monitoring by Orion NTA as part of an autonomous system network:

1. Login to the network device.
2. Based on your vendor's documentation, you would minimally do these things, adding the appropriate commands to the configuration file:
   a. Enable a BGP routing process, which places you in router configuration mode.
   b. Flag a network as local to this autonomous system and enter it to the BGP table.

      Enter as many networks as needed.

   c. Specify BGP neighbors.

      Enter as many neighbors as needed.

   For example, for detailed information on BGP configuration for Cisco devices, see this Cisco documentation.

3. Enable NetFlow export from your device.

   For detailed information on configuring NetFlow on Cisco devices, see Enabling NetFlow for Cisco IOS.

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

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

   Otherwise, consult these examples as relevant to your device:

   Foundry sFlow Configuration

   HP sFlow Configuration

   Extreme sFlow Configuration

   Juniper sFlow Configuration

   Juniper J-Flow Configuration

If your network device is of a different vendor, consult that vendor's documentation.

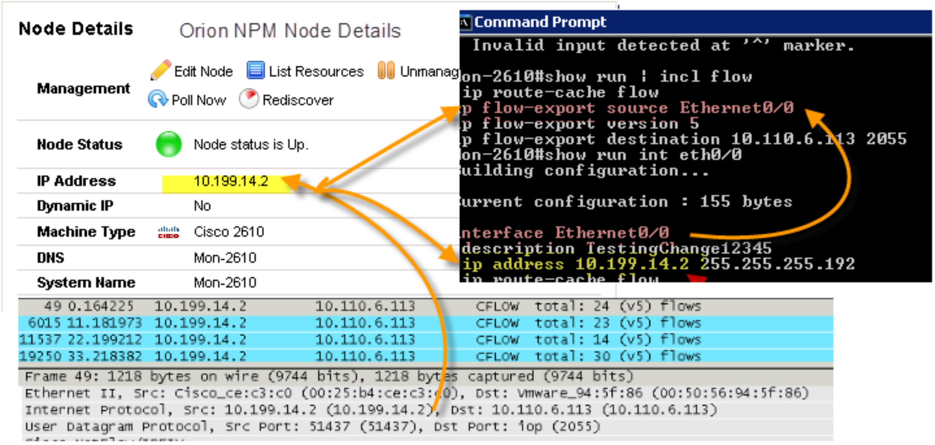
4. Verify that your device and its NetFlow exporting interface are being monitored in Orion NMP.

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

   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*

5. To verify that a device is exporting data as expected, use a packet capture tool (for example, Wireshark) to search for packets sent from the network device to the Orion server.

   As an example, if you successfully added a NetFlow enabled device with IP address 10.199.14.2 to Orion NPM, and the device were actively exporting NetFlow data to the Orion server, you would see in Wireshark a packet like the one (49) highlighted below in gray:



Node Status: Node status is Up.
IP Address: 10.199.14.2
Dynamic IP: No
Machine Type: Cisco 2610
DNS: Mon-2610
System Name: Mon-2610

```
 Invalid input detected at '^' marker.

on-2610#show run | incl flow
ip route-cache flow
p flow-export source Ethernet0/0
p flow-export version 5
p flow-export destination 10.110.6.113 2055
on-2610#show run int eth0/0
uilding configuration...

urrent configuration : 155 bytes

nterface Ethernet0/0
description TestingChange12345
ip address 10.199.14.2 255.255.255.192
```

```
   49 0.164225   10.199.14.2        10.110.6.113        CFLOW  total: 24 (v5) flows
 6015 11.181973  10.199.14.2        10.110.6.113        CFLOW  total: 23 (v5) flows
11537 22.199212  10.199.14.2        10.110.6.113        CFLOW  total: 14 (v5) flows
19250 33.218382  10.199.14.2        10.110.6.113        CFLOW  total: 30 (v5) flows
 Frame 49: 1218 bytes on wire (9744 bits), 1218 bytes captured (9744 bits)
 Ethernet II, Src: Cisco_ce:c3:c0 (00:25:b4:ce:c3:c0), Dst: Vmware_94:5f:86 (00:50:56:94:5f:86)
 Internet Protocol, Src: 10.199.14.2 (10.199.14.2), Dst: 10.110.6.113 (10.110.6.113)
 User Datagram Protocol, Src Port: 51437 (51437), Dst Port: iop (2055)
```

As indicated and expected, we see in the packet details that 10.199.14.2 is its source IP address and 10.110.6.113 (i.e., the Orion server) the destination. This correlates with the node details on the device in Orion, as highlighted in yellow.

To verify that the IP address of the exporting interface on the network device is the one being monitored in Orion, open a CLI, log into the network device, and type ‘show run’ to see the device’s running configuration. Page down to the lines where the export source interface is defined; in this case, we see *ip flow-export source Ethernet0/0.* To discover the IP address for this interface, type ‘show run int *Ethernet0/0’*. We see that the interface’s IP address (10.199.14.2) is in fact being monitored in the Orion server.

6. In the Orion Web Console click NETFLOW in the modules toolbar.

   You should see NetFlow enabled nodes listed in the NetFlow Sources resources with a recent time posted for collected flow.

   To add relevant devices as NetFlow Sources, if they are not already in the list, refer to Adding Flow Sources and CBQoS-enabled Devices.

7. Click the **BGP** view on the NETFLOW views toolbar.

   You should see chart statistics in the Top XX Autonomous Systems and Top XX Autonomous Systems Conversations resources.

Monitoring Autonomous System Networks

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

Top XX Autonomous Systems

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

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

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

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

For more information, see “Customizing Individual Top *XX* Resources”.

Top XX Autonomous System Conversations

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

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

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

OrionNetFlowPHASView

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

For more information, see Customizing Individual Top XX Resources Customizing Individual Top XX Resources on page 74.

Managing Autonomous System Networks

You and add, edit, and delete an autonomous system network to and from those Orion NTA monitors.

To add an autonomous system network:

1. Click **NETFLOW** on the toolbar.
2. Click NTA Settings.
3. Click **Manage Autonomous Systems** under Autonomous Systems.
4. Click **Add Autonomous Systems** and enter appropriate values for these parameters:
    - Unique Autonomous System ID
    - Name of the Autonomous System

  - Country code
  - Organization
  - Date of Registration
  - Date of Last Update

5. Click **Save**.

To edit an autonomous system network:

1. Click **NETFLOW** on the toolbar.
2. Click NTA Settings.
3. Click **Manage Autonomous Systems** under Autonomous Systems.
4. Click **Add Autonomous Systems** and modify values as needed for these parameters:
   - Unique Autonomous System ID
   - Name of the Autonomous System
   - Country code
   - Organization
   - Date of Registration
   - Date of Last Update
5. Click **Save**.

To delete an autonomous system network:

1. Click **NETFLOW** on the toolbar.
2. Click NTA Settings.
3. Click **Manage Autonomous Systems** under Autonomous Systems.
4. Click **Delete** beside the relevant autonomous system(s).
5. Click **Save**.

Chapter 9

Key and Critical Tasks

These sections cover common but critical tasks to perform in setting up and managing your Orion NTA implementation. .

Setting up Network Devices to Export NetFlow Data

As a feature to facilitate traffic analysis on Cisco IOS enabled devices, NetFlow begins its work at the network device itself. And any device that is NetFlow enabled, in order to communicate the traffic related data it is holding about that device, must be configured to send, push, or export that data to specific collection targets.

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

All of these things need to be done for Orion NTA to correctly process NetFlow data and process relevant traffic statistics:

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

Follow the procedures in this section to setup each NetFlow-enabled device; and to verify that each device correctly exports NetFlow data to Orion NTA.

To setup a device to export NetFlow data to Orion NTA:

1. Login to the network device.

2. To enable NetFlow on a Cisco device, for example, you would use these commands:

```
ip flow-export source <netflow_export_interface><interface_num>

ip flow-export version 5

ip flow-export destination <Orion_Server_IP_address> 2055

    ip flow-cache timeout active 1

    ip flow-cache timeout inactive 15

    snmp-server ifindex persist
```

For detailed information see Enabling NetFlow for Cisco IOS.

> For information on enabling NetFlow for Cisco Catalyst switches, consult this SolarWinds technical reference paper.
>
> For information on enabling NetFlow on Cisco ASA devices, consult this SolarWinds Knowledge Base article.

Otherwise, consult these examples as relevant to your device:

Foundry sFlow Configuration

HP sFlow Configuration

Extreme sFlow Configuration

Juniper sFlow Configuration

Juniper J-Flow Configuration

If your network device is of a different vendor, consult that vendor's documentation.

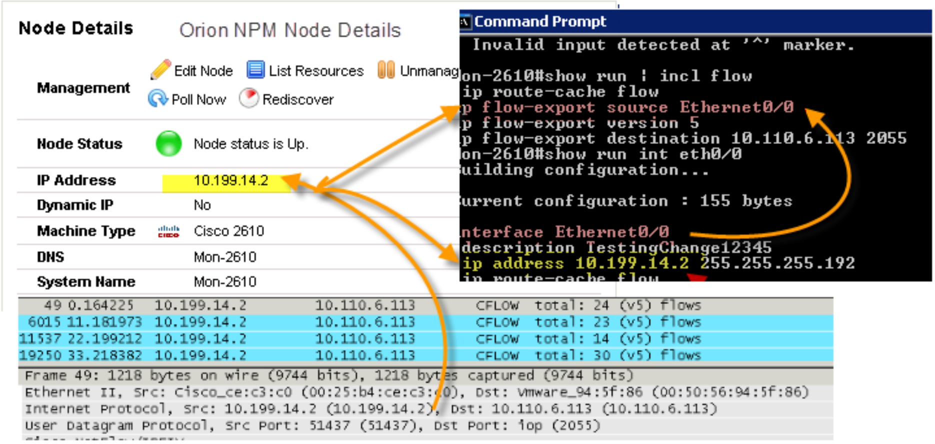
3. Verify that your device and its NetFlow exporting interface are being monitored in Orion NMP.

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

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. To verify that a device is exporting data as expected, use a packet capture tool (for example, WireShark) to search for packets sent from the network device to the Orion server.

As an example, if you successfully added a NetFlow enabled device with IP address 10.199.14.2 to Orion NPM, and the device were actively exporting NetFlow data to the Orion server, you would see in Wireshark a packet like the one (49) highlighted below in gray:



Node Status	Node status is Up.
IP Address	10.199.14.2
Dynamic IP	No
Machine Type	Cisco 2610
DNS	Mon-2610
System Name	Mon-2610

```
 Invalid input detected at '^' marker.

on-2610#show run | incl flow
ip route-cache flow
p flow-export source Ethernet0/0
p flow-export version 5
p flow-export destination 10.110.6.113 2055
on-2610#show run int eth0/0
uilding configuration...

urrent configuration : 155 bytes

nterface Ethernet0/0
description TestingChange12345
ip address 10.199.14.2 255.255.255.192
ip route-cache flow
```

```
   49 0.164225   10.199.14.2        10.110.6.113       CFLOW  total: 24 (v5) flows
 6015 11.181973  10.199.14.2        10.110.6.113       CFLOW  total: 23 (v5) flows
11537 22.199212  10.199.14.2        10.110.6.113       CFLOW  total: 14 (v5) flows
19250 33.218382  10.199.14.2        10.110.6.113       CFLOW  total: 30 (v5) flows
Frame 49: 1218 bytes on wire (9744 bits), 1218 bytes captured (9744 bits)
Ethernet II, Src: Cisco_ce:c3:c0 (00:25:b4:ce:c3:c0), Dst: Vmware_94:5f:86 (00:50:56:94:5f:86)
Internet Protocol, Src: 10.199.14.2 (10.199.14.2), Dst: 10.110.6.113 (10.110.6.113)
User Datagram Protocol, Src Port: 51437 (51437), Dst Port: iop (2055)
```

As indicated and expected, we see in the packet details that 10.199.14.2 is its source IP address and 10.110.6.113 (i.e., the Orion server) the destination. This correlates with the node details on the device in Orion, as highlighted in yellow.

To verify that the IP address of the exporting interface on the network device is the one being monitored in Orion, open a CLI, log into the network device, and type ‘show run’ to see the device’s running configuration. Page down to the lines where the export source interface is defined; in this case, we see ‘ip flow-export source Ethernet0/0’. To discover the IP address for this interface, type ‘show run int *Ethernet0/0’*. We see that the interface’s IP address (10.199.14.2) is in fact being monitored in the Orion server.

5. In the Orion Web Console click NetFlow in the modules toolbar.

   You should see NetFlow enabled nodes listed in the NetFlow Sources resources.

   To add relevant devices as NetFlow Sources, if they are not already in the list, refer to Adding Flow Sources and CBQoS-enabled Devices.

   Note: Only SNMP capable nodes whose interfaces were discovered by Orion NPM can be added as NetFlow sources.

Optimizing Performance of Orion NTA

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

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

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

- Configure DNS resolution to occur on demand instead of persistently.
- Capture only the Flows required to represent the "top talkers" on your network.
- Limit the compressed data retention period.
- Aggregate Top Talk flow data.

Configuring On Demand DNS resolution

Enabling On Demand DNS resolution in Orion NTA decreases the amount of database memory used to store DNS information and the read/write load on your SQL Server associated with domain name resolution.

With On Demand DNS resolution enabled, domain names are only resolved for device IP addresses that are actually displayed in Orion NTA resources. Since they require persistent DNS resolution to calculate statistics, Top XX Domains, Top XX Traffic Destinations by Domain (report), and Top XX Traffic Sources by Domain (report) become unavailable with this setting.

To configure On Demand DNS resolution:

1. Log on to the Orion server hosting your Orion NTA installation using an account with administrative privileges.
2. Click **Settings** in the right corner.
3. Click **NTA Settings** in the Settings grouping.
4. Under **DNS and NetBIOS Resolution**, set DNS Resolution to **On Demand**.
5. Click **Save** to enable On Demand DNS resolution.

Limiting Flow Collections To Top Talkers

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

As a feature of Orion NTA, the Top Talker Optimization, by default, captures only those Flows representing the top 95% of total network traffic. Keep in mind that by enabling this option you are permanently limiting the amount of data that is available for a historical analysis of traffic flows.

To limit flow captures to top talkers:

1. Log on to the Orion server hosting your Orion NTA installation.
2. Click **Settings** in the right corner.
3. Click **NTA Settings** in the Settings grouping.
4. Under Top Talker Optimization, in the Capture Flows based on the maximum percentage of traffic field, set the preferred value.
5. Click **Save**.

Limiting the Compressed Data Retention Period

Besides restricting collected data to top talkers, configuring Orion NTA to keep compressed data for 14 or fewer days can additionally optimize how the software processes and manages flow data.

Allowing Orion NTA to run in this mode for a couple of weeks, or at least longer than the number of days provided, will ensure that all old, unnecessary compressed Flow data you collected prior to enabling the "top talker" percentage optimization is flushed from your Orion database. After the old compressed Flow data is deleted from your database, you should see noticeable performance improvements in Orion NTA resource load times.

To configure the compressed data retention period:

1. Log in to your Orion Web Console as an administrator.
2. Click **Settings** in the right corner.

3. Click **NTA Settings** in the Settings grouping.
4. Under Database Settings, in the Keep compressed data for XX days field, provide a value of 14 or less.
5. Click **Save.**

Aggregating Top Talker Flow Data

Aggregating NetFlow data in memory significantly reduces the I/O demands that Orion NTA makes on your Orion database, which can increase the performance of all SolarWinds applications that share the database. In other words, conversely, if its Web Console resources are allowed to work directly against the Orion database in making and presenting their latest calculations, Orion NTA would make big I/O demands on the Orion database, impacting performance of both Orion NTA and Orion NPM.

By aggregating data before writing it to the Orion database, Orion NTA software expedites the presentation of summary statistics for three of the most important kinds of information about traffic on your network: Top XX Applications, Top XX Endpoints, Top XX Conversations.

To aggregate data for use in updating Top XX Application, Top XX Endpoints, and Top XX Conversations resources:

1. Log in to your Orion Web Console as an administrator.
2. Click **Settings** in the right corner.
3. Click **NTA Settings** in the Settings grouping.
4. Under Database Settings, click the checkbox to Enable aggregation of top talker data.
5. For the Top XX Applications, Endpoints, and Conversations statistics, select how many of each you want Orion NTA to use as the basis for aggregating the NetFlow data it receives from your network devices.
6. Enter a number of hours for which Orion NTA should save aggregated NetFlow data in cache.
7. Click **Save**.

Implementing and Monitoring CBQoS Policies

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

These sections explain how to use Orion NTA in preparing CBQoS policies and how to monitor the implementation. They do not cover the details of defining class and policy maps and applying them to interfaces; for that you need to consult Cisco documentation.

Using NTA to Prepare a CBQoS Implementation

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

Assuming you have all Cisco devices setup to export flow data—if not, see “Adding Flow-enabled Devices and Interfaces”—and Orion NTA is showing the devices in the NetFlow Sources resource (NETFLOW on the main toolbar), begin by examining each node for traffic statistics useful traffic information.

The following steps cover the basic process for using Orion NTA to analyze flow data in preparation to defining a CBQoS strategy. These steps mainly are meant to give general guidance on how to use Orion NTA in analyzing your current traffic as pertains to determining CBQoS needs. Improvising your analysis will most likely be necessary to gain the right level of knowledge and insight into the way your network is handling traffic, so that using CBQoS, instead of simply increasing bandwidth, can be a workable solution for you.

To gather traffic information for an interface:

1. Open **Orion Web Console**.
2. Click **NETFLOW** in the toolbar.
3. Click a relevant node in the list of NetFlow Sources.
4. Click an interface for which you want to analyze the traffic.

   This brings up an Interface Details view for the interface.
5. Set the time frame for which you want to examine traffic statistics.

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

   Note: Based on what you observe with this data slice you would decide if you need to look at other slices for comparison.
6. Click **Submit**.
7. Set the flow direction for which you want to review the traffic.
8. Click **Submit**.

9. Use a combination of Top XX resources on the Interface Details to analyze how traffic data is flowing through the interface. For example:

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

  The goal is to figure out what amount of data applications critical to the purpose of your business or organization typically transfer in the representative time period. You also want to discover the applications that are consuming bandwidth unrelated to the primary purposes of your organization, such as recreational YouTube streaming.

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

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

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

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

- Use Top XX Traffic Sources/Destinations by Countries to view the countries whose traffic is most serviced through the interface.
- If you are using Persistent DNS instead of On Demand DNS, you can view the domains responsible for the highest levels of data transfer through the interface and correlate those levels with statistics in the other Top XX resources. See Configuring NetBIOS and DNS Resolution on page 39 for information on using persistent instead of on-demand DNS.

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

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

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

Dynamically Monitoring CBQoS

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

For more information on discovering network devices, see Discovering and Adding Network Devices in the *Orion Network Performance Monitor Administrator Guide*. For more information on setting up on NetFlow collections, see Setting up Network Devices to Export NetFlow Data.

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

These three Orion Advanced Alerts are available to you:

Pre-Policy

CBQoS Pre-Policy writes to the SolarWinds event log when the amount of Pre-Policy traffic (in bytes) meets the conditions of your alert threshold setting.

Example of alert logged: CBQoS Pre-Policy traffic in class 'class-default (MCQTest)' with policy ‘policy-default (MPQTest)’ on interface 'FastEthernet0/0 · link to core' met the conditions of your alert threshold setting. Total Pre-Policy traffic in the past 15 minutes: 99999 Bytes

By default, this alert writes to the Event Log. This alert also can be configured to send the information in an email to the configured recipient.

Post-Policy

CBQoS Post-Policy writes to the SolarWinds event log when the amount of Post-Policy traffic (in bytes) meets the conditions of your alert threshold setting.

Example of alert logged: CBQoS Post-Policy traffic in class 'class-default (MCQTest)' with policy ‘policy-default (MPQTest)’ on interface 'FastEthernet0/0 · link to core' met the conditions of your alert threshold setting. Total Post-Policy traffic in the past 15 minutes: 99999 Bytes

By default, this alert writes to the Event Log. This alert also can be configured to send the information in an email to the configured recipient.

Drops

CBQoS Drops writes to the SolarWinds event log when, as a result of applying CBQoS policies to traffic on an interface.

Example of alert logged: CBQoS Drops met your alert threshold setting as a result of applying class map 'class-default (MCQTest)' and policy map ‘policy-default (MPQTest)’ on interface 'FastEthernet0/0 · link to core' . Total data dropped in last 15 minutes is: 00333 Bytes

By default, this alert writes to the Event Log; and also can be configured to send the information in an email to the configured recipient.

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

For steps on creating an advanced alert see the sections on advanced alerts in Chapter 11, “Creating and Managing Alerts,” in the Orion Performance Manager Administrator’s Guide.

To configure a CBQoS advanced alert:

1. Open the Orion Alert Manager in the Orion program group.
2. Navigate to the Manage Alerts resource (View > Configure Alerts).
3. Select the relevant CBQoS alert.

4. Click **Edit**.

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

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

For the CBQoS alerts, the default condition is a match on the SQL query. You can adjust the number of seconds for which the match exists, essentially inserting a delay to allow the traffic to fluctuate without triggering the alert.

You can adjust this condition or add conditions.

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

For the CBQoS alerts, the default condition is no match on the SQL query. You can adjust the number of seconds for which the match fails to persist, essentially inserting a delay to allow the traffic to fluctuate without canceling the alert.

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

The default condition is no suppression.

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

The default range is 24/7.

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

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

For CBQoS alerts the default actions include write the same event message into an email and send it to an appropriate contact.

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

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

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

becomes:

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

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

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

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

Finding the Cause of High Bandwidth Utilization

If a node managed in Orion NPM is also a NetFlow Source—meaning that it exports NetFlow data and you are currently monitoring in Orion NTA—you can use Orion NTA to analyze interface bandwidth utilization either in response to an Orion Advanced Alert that you configure or whenever your workflow requires. For information on creating an Orion Advanced Alert, see “Creating and Configuring Advanced Alerts”.

These procedures assume that you have created an Orion Advanced alert on bandwidth utilization for a specific interface, and that the alert has been triggered based on your threshold setting. For example, you may have set the trigger threshold at 80% of interface bandwidth and you now see an alert-related event.

To find the cause of bandwidth utilization:

1. Open the Orion Web Console.

2. Click NETFLOW, then locate and expand **(+)** the relevant node in NetFlow Sources.

3. Click the interface for which you received the bandwidth utilization alert.

4. View the Top XX Endpoints for the interface.

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

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

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

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

Tracking Traffic by Site

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

To keep track of traffic by site:

1. Login on the Orion Web Console.
2. Click **NETFLOW**.
3. Click **Flow Navigator** on the left edge of the summary view. (The Flow Navigator is available on any default NTA view.)
4. Select the **Detailed** view type.
    a. Select the node that corresponds to the main network device for the site (through which all or most traffic passes).
    b. Select an IP Address Group view filter.

       Use the private address range in the dropdown that encompasses this specific site.
5. Select the **Time Period** over which you want to view network traffic by country of origin or destination, using any of the following options:

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

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

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

Note: Format start and end times as `MM/DD/YYYY HH:MM:SS AM/PM`.

6. Select a Flow Direction.

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

7. ***If you want to limit your view to only display network traffic to and from autonomous systems, or to exclude traffic to and from them***, a click **+** next to **Autonomous Systems**, and then complete the following steps:
    a. ***If you want to include traffic from specified autonomous systems,*** select **Include**.
    b. ***If you want to exclude traffic from specified autonomous systems,*** check **Exclude**.
    c. Enter the name of an appropriate automonous network.
    d. ***If you want to include or exclude another autonomous system***, click **Add Filter** and enter the name of an the appropriate autonomous system.
8. ***If you want to limit your view to only display network traffic related to specific countries, or to exclude traffic to and from them***, a click **+** next to **Autonomous System Conversations**, and then complete the following steps:
    a. ***If you want to include traffic from specified autonomous system conversations,*** select **Include**.
    b. ***If you want to exclude traffic from specified autonomous system conversations,*** check **Exclude**.
    c. Enter an appropriate country.
    d. ***If you want to include or exclude another autonomous system conversation***, click **Add Filter** and enter the name of an appropriate country.
9. ***If you want to limit your view to only display network traffic related to specific conversations, or to exclude traffic to and from them***, a click **+** next to **Conversations**, and then complete the following steps:
    a. ***If you want to include traffic from specified conversations,*** select **Include**.
    b. ***If you want to exclude traffic from specified conversations,*** check **Exclude**.

   c. Enter the endpoints involved in the conversation.
   d. ***If you want to include or exclude another conversation***, click **Add Filter** and enter the names of the appropriate endpoints.

10. ***If you want to limit your view to only display network traffic related to specific countries, or to exclude traffic to and from them***, a click **+** next to **Countries**, and then complete the following steps:
    a. ***If you want to include traffic from specified countries,*** select **Include**.
    b. ***If you want to exclude traffic from specified countries,*** check **Exclude**.
    c. Select an appropriate country.
    d. ***If you want to include or exclude another country***, click **Add Filter** and select the name of an appropriate country.
11. ***If you want to limit your view to only display network traffic related to specific domains, or to exclude traffic to and from them***, a click **+** next to **Domains**, and then complete the following steps:
    a. ***If you want to include traffic from specified domains,*** select **Include**.
    b. ***If you want to exclude traffic from specified domains,*** check **Exclude**.
    c. Enter an appropriate domain.
    d. ***If you want to include or exclude another domain***, click **Add Filter** and enter the name of an appropriate domain.
12. ***If you want to limit your view to only display network traffic related to specific endpoints, or to exclude traffic to and from them***, a click **+** next to **Endpoints**, and then complete the following steps:
    a. ***If you want to include traffic from specified Endpoints,*** select **Include**.
    b. ***If you want to exclude traffic from specified Endpoints,*** check **Exclude**.
    c. Enter an appropriate endpoint.
    d. ***If you want to include or exclude another endpoint***, click **Add Filter** and enter the name of an appropriate endpoint.
13. ***If you want to limit your view to only display network traffic using specific protocols,*** click **+** next to **Protocol**, and then complete the following steps:

   a. ***If you want to include traffic from specified Protocol,*** select **Include**.
   b. ***If you want to exclude traffic from specified Protocol,*** check **Exclude**.
   c. Select an appropriate ***Protocol***.
   d. ***If you want to include or exclude another Protocol***, click **Add Filter** and select an appropriate ***Protocol***.

14. ***If you want to limit your view to only display network traffic using specific service types,*** click **+** next to **Types of Service**, and then complete the following steps:
    a. ***If you want to include traffic from specified type of service,*** select **Include**.
    b. ***If you want to exclude traffic from specified type of service,*** check **Exclude**.
    c. Select an appropriate ***type of service***.
    d. ***If you want to include or exclude another type of service***, click **Add Filter** and select an appropriate ***type of service***.
15. When you have completed configuration of your filtered application view, click **SUBMIT.**
16. Click to save click **SAVE FILTERED VIEW TO MENU BAR**.
17. Name the view.
18. Click **OK**.
19. Repeat steps 3 through 18 for each site you manage.

Managing Unmonitored NetFlow Traffic

Two kinds of unmonitored flow data comes into Orion NTA; data sent to ports other than 2055, where NetFlow is setup to listen; and data sent from an IP address that is not currently associated with a node monitored in Orion.

By default for new installations, Orion NTA retains all flow data provided by NetFlow sources on your network, including Flow data for ports that you are not actively monitoring. For more information on data received on unmonitored ports, see Configuring Data Retention Flows on Unmonitored Ports on page 26.

This section explains how to resolve events related to unmonitored flow traffic.

To resolve unknown traffic events:

1. Open the Orion Web Console.
2. Click **NETFLOW** on the main toolbar.

If you currently have unknown traffic events then a link—**Show unknown traffic events**—is posted in the banner area. If there is no such message in the banner area then you currently have no unknown traffic events

3. ***If you see the message Show unknown traffic events*** in the banner area, click that message.

   The Unknown Traffic Events page opens. The list includes the last 200 events in which flow traffic was received but was not associated with a Netflow source.

   In creating an item on the list, the Orion NTA software tells you that the NetFlow receiver (node name) to which the flow is coming and the IP address from which it is coming. The entry looks like this:

   ```
   NetFlow Receiver Service [LAB-NTA-04] is receiving NetFlow data
   from an unmanaged interface on 10.199.4.3.. The NetFlow data
   will be discarded. Use the "Edit this device" link or Orion
   node management to manage interface '#123' and process its
   NetFlow data.
   ```

4. For each item in the Last 200 Unknown Traffic Events list, click **Edit this device**.

   The software navigates into the List Resources screen of the Add Node wizard.

5. Make sure that **All Interfaces** is checked and click **Submit**.

   The software navigates into the Manage Nodes resource.

6. Return to the Last 200 Events screen and repeat steps 9 and 10.

7. When you are finished with items in the Last 200 Events list, click Refresh Events to refresh the list along with the page.

   Unresolved events return to the list if they have not been successfully resolved. This allows you to test your efforts to resolve unresolved traffic items.

8. Go to NETFLOW on the main toolbar.

   You should no longer see a banner indication regarding unknown flow traffic. If you do, click the message and re-examine the Last 200 Unknown Traffic Events list again, repeating the steps in these procedures as needed to associate the flow traffic with the appropriate NPM interface.

Working with Charts

Orion NTA’s Interactive and Classic charts display NTA pie-chart summaries of resource-related data. Orion NTA area charts enable a more detailed view of resources in both Interactive and Classic views. You can create different types of area charts, including stack area, stack spline area, stack line, line, spline, and bar.

Interactive charts are the default charts for new NTA installations and upgrades. Software upgrades to NTA 3.10.0 and beyond automatically change Classic charts to Interactive charts after the upgrade finishes.

Interactive charts offer tooltips with current values, as well as the ability to disable data series and to zoom in on data. Interactive charts also have clickable features offering detailed resource information and editing capabilities.

The number of displayed resources is limited to 100 for Interactive pie and area charts. The number of data series shown in Interactive pie charts is a whole 100 items. Area charts, however, are limited to showing 10 items in the chart, with the rest of the series visible in the legend.

Note: Unlike Classic charts, Interactive charts do not support the fast-switch buttons and Cancel/Cancel all buttons displayed during progressive loading.

Classic charts display information in 2-D pie, 3-D pie, and area charts. Orion NTA’s default Interactive charts have clickable features offering detailed resource information, tooltips with current values, as well as the ability to disable data series and overview charts for zooming and editing capabilities through area charts and 2-D pie charts

Note: Interactive and Classic charts can be placed on views together. However, there is no way how to change all charts globally back to Classic or Interactive charts. The only way how to do this is to add Classic charts and remove Interactive charts after installation or upgrade through the Customize page or Manage views option.

To customize individual Top XX resources, consult Customizing Individual Top *XX* Resources. To customize Top XX resources for all users, if you have administrator access to the Orion Web Console, consult the section Customizing for All Users (Administrators Only).

The following sections explain the elements of Interactive and Classic charts you may encounter.

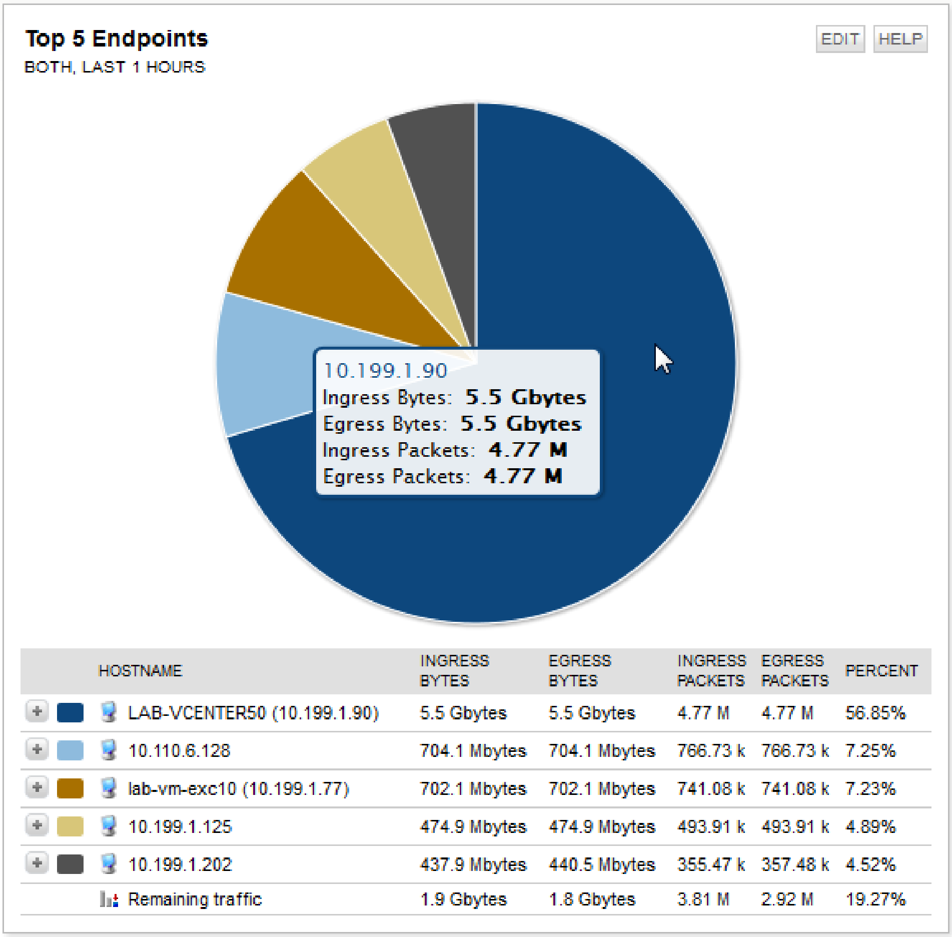
Pie Charts

The pie charts in this section show the Top 5 Endpoints. The following charts use absolute percentage calculations. The Interactive charts also show the new feature in Interactive charts, **Remaining traffic**. For more information on the Remaining traffic feature, see Configuring Orion NTA Views and Resources on page 45.

Interactive Pie Charts

With Interactive pie charts, Orion NTA gives each resource its own piece of pie, depending on your chart settings. If more resources exist than what is configured to display, Orion NTA creates a category in the pie chart's legend called **Remaining traffic**, which is not displayed in chart. If fewer resources exist than what the chart is configured to display, the chart shows only those resources that exist.

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



Top 5 Endpoints

BOTH, LAST 1 HOURS

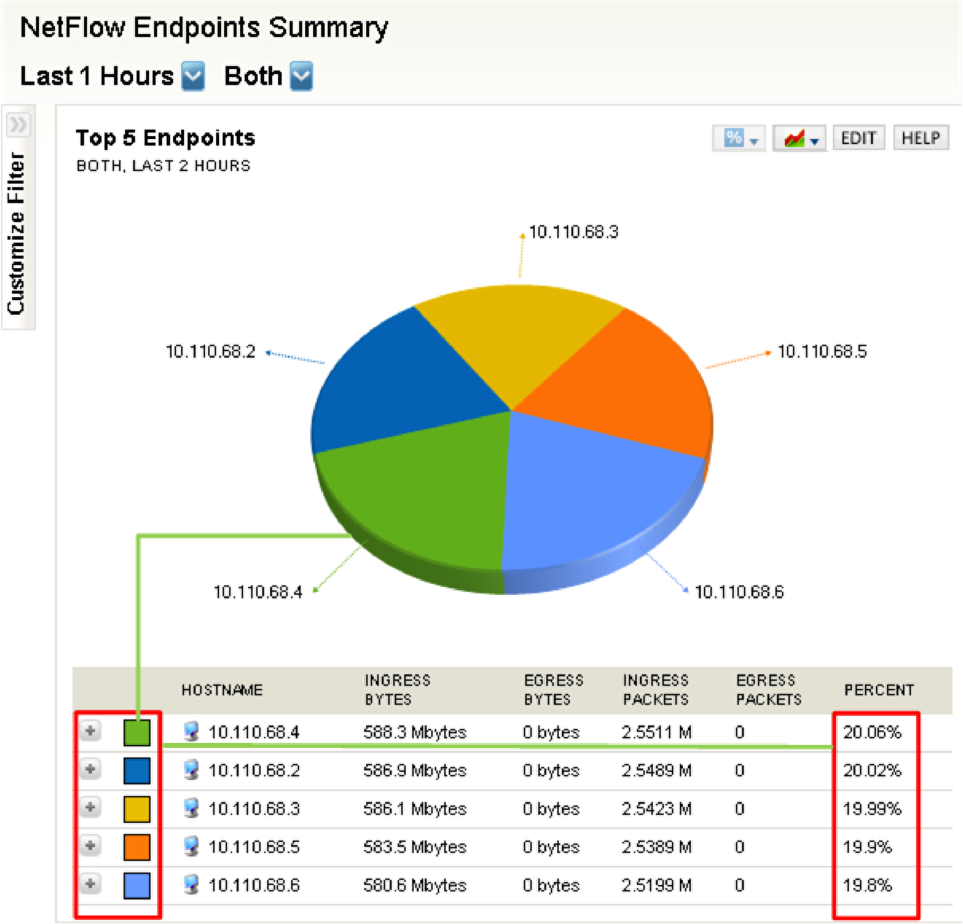
10.199.1.90
Ingress Bytes: **5.5 Gbytes**
Egress Bytes: **5.5 Gbytes**
Ingress Packets: **4.77 M**
Egress Packets: **4.77 M**

		HOSTNAME	INGRESS BYTES	EGRESS BYTES	INGRESS PACKETS	EGRESS PACKETS	PERCENT
+	🟦	LAB-VCENTER50 (10.199.1.90)	5.5 Gbytes	5.5 Gbytes	4.77 M	4.77 M	56.85%
+	🟦	10.110.6.128	704.1 Mbytes	704.1 Mbytes	766.73 k	766.73 k	7.25%
+	🟫	lab-vm-exc10 (10.199.1.77)	702.1 Mbytes	702.1 Mbytes	741.08 k	741.08 k	7.23%
+	🟨	10.199.1.125	474.9 Mbytes	474.9 Mbytes	493.91 k	493.91 k	4.89%
+	⬛	10.199.1.202	437.9 Mbytes	440.5 Mbytes	355.47 k	357.48 k	4.52%
		Remaining traffic	1.9 Gbytes	1.8 Gbytes	3.81 M	2.92 M	19.27%

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

Classic Pie Charts

2-D and 3-D pie charts present the same information. The Classic chart examples in this section use 3-D charts.



NetFlow Endpoints Summary

Last 1 Hours Both

Top 5 Endpoints

BOTH, LAST 2 HOURS

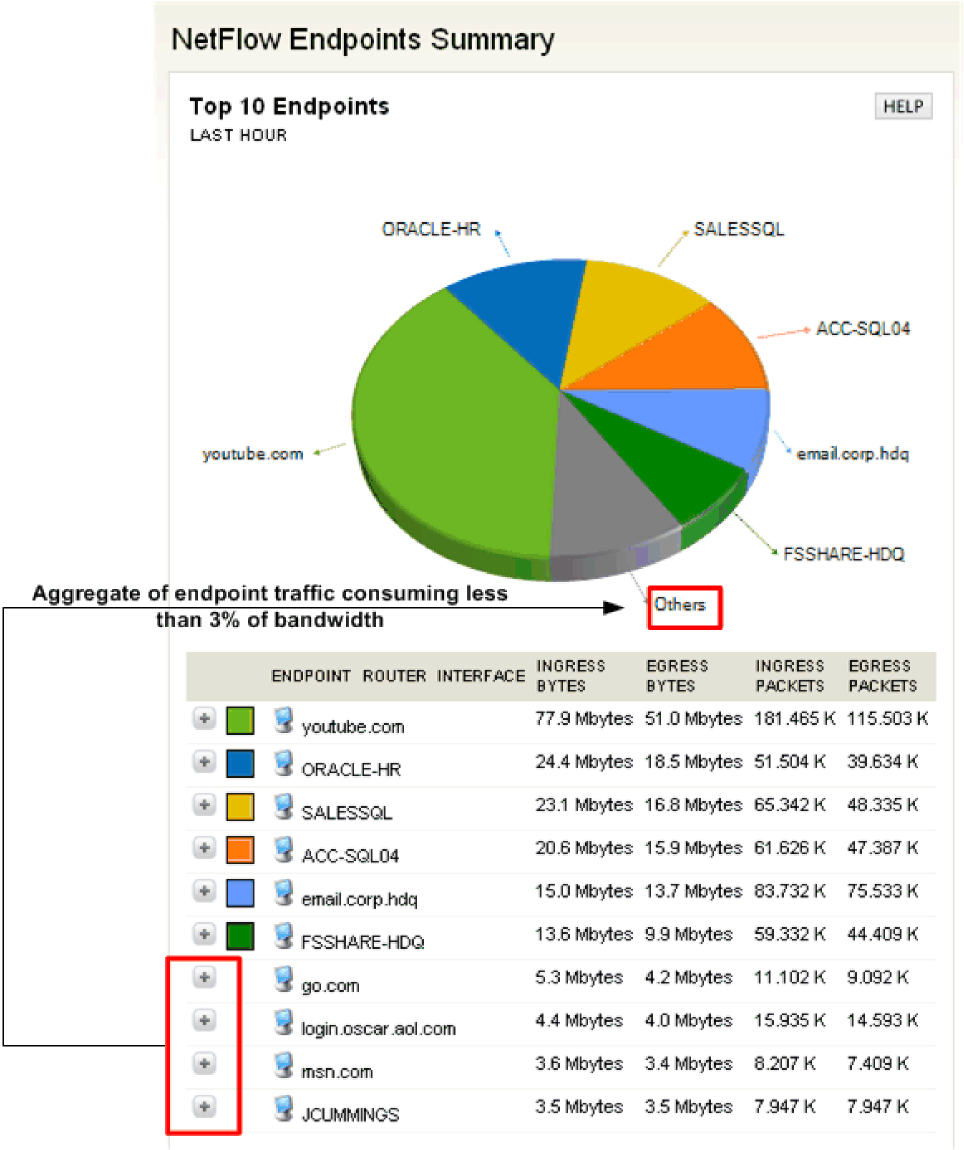
		HOSTNAME	INGRESS BYTES	EGRESS BYTES	INGRESS PACKETS	EGRESS PACKETS	PERCENT
+	🟩	10.110.68.4	588.3 Mbytes	0 bytes	2.5511 M	0	20.06%
+	🟦	10.110.68.2	586.9 Mbytes	0 bytes	2.5489 M	0	20.02%
+	🟨	10.110.68.3	586.1 Mbytes	0 bytes	2.5423 M	0	19.99%
+	🟧	10.110.68.5	583.5 Mbytes	0 bytes	2.5389 M	0	19.9%
+	🟦	10.110.68.6	580.6 Mbytes	0 bytes	2.5199 M	0	19.8%

In this chart, which uses absolute percentage calculations, traffic is divided almost evenly at 20% each among the top endpoints.

There are of course many cases in which traffic generation is very uneven. In preparing the data for display in the Top XX Endpoints pie chart, the NTA software gives each endpoint consuming at least 3% of interface bandwidth its own slice in the pie. For all endpoints in the Top XX set, if they consume less than 3% (of interface bandwidth or total traffic, depending on your chart settings), the NTA software creates a remaining slice of the pie called 'Other,' with a total percentage made from the smaller slices.

As a result of how NTA software calculates Top XX for charting, it's possible to have a chart for Top 10 Endpoints that shows just 6 slices, one of which would be **Other** — in which 4 of the endpoints would be contained.

For example, this chart shows Top 10 Endpoints based on interface bandwidth usage.



Aggregate of endpoint traffic consuming less than 3% of bandwidth

		ENDPOINT	ROUTER	INTERFACE	INGRESS BYTES	EGRESS BYTES	INGRESS PACKETS	EGRESS PACKETS
+	🟩	youtube.com			77.9 Mbytes	51.0 Mbytes	181.465 K	115.503 K
+	🟦	ORACLE-HR			24.4 Mbytes	18.5 Mbytes	51.504 K	39.634 K
+	🟨	SALESSQL			23.1 Mbytes	16.8 Mbytes	65.342 K	48.335 K
+	🟧	ACC-SQL04			20.6 Mbytes	15.9 Mbytes	61.626 K	47.387 K
+	🟦	email.corp.hdq			15.0 Mbytes	13.7 Mbytes	83.732 K	75.533 K
+	🟩	FSSHARE-HDQ			13.6 Mbytes	9.9 Mbytes	59.332 K	44.409 K
+		go.com			5.3 Mbytes	4.2 Mbytes	11.102 K	9.092 K
+		login.oscar.aol.com			4.4 Mbytes	4.0 Mbytes	15.935 K	14.593 K
+		msn.com			3.6 Mbytes	3.4 Mbytes	8.207 K	7.409 K
+		JCUMMINGS			3.5 Mbytes	3.5 Mbytes	7.947 K	7.947 K

Area Charts

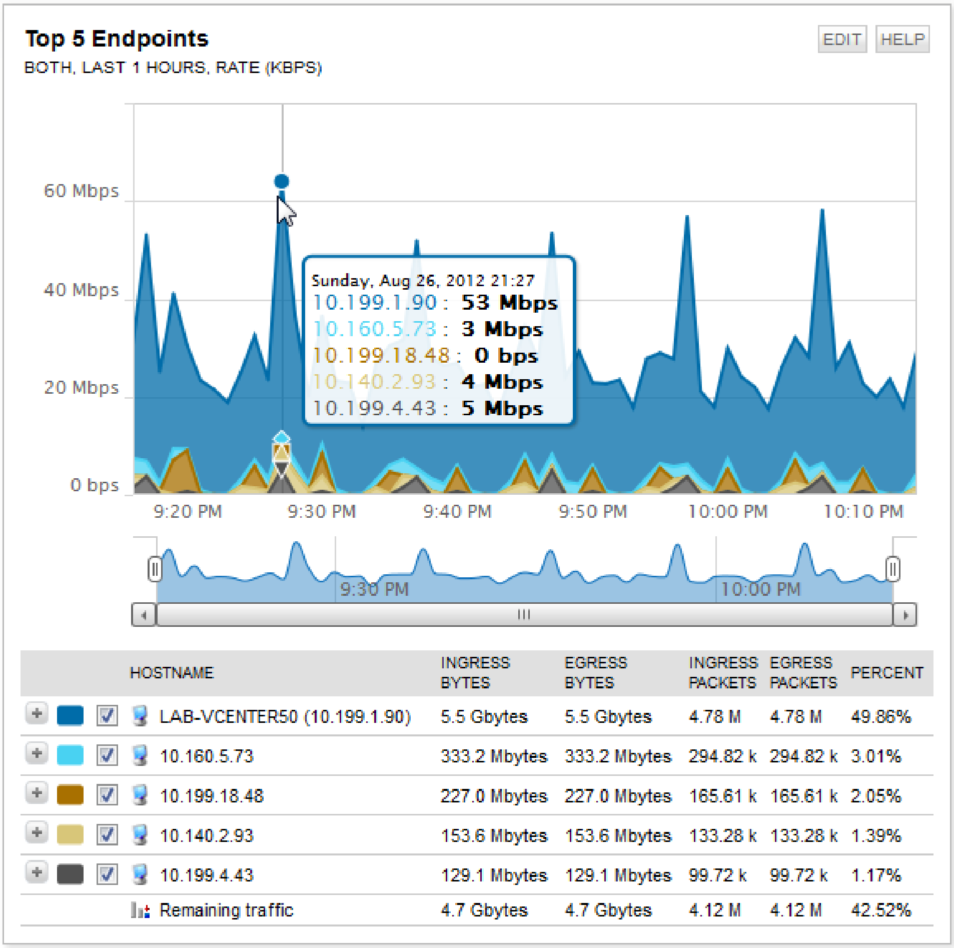
Area charts are the default charts for resource detail pages. They provide a more comprehensive view of traffic and bandwidth usage data than pie charts, so area charts always include a one-to-one relationship of table-to-chart information.

Interactive Area Charts

Interactive area charts are the default charts for all detail views and display resources within a defined traffic level and timeframe.

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

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



Top 5 Endpoints

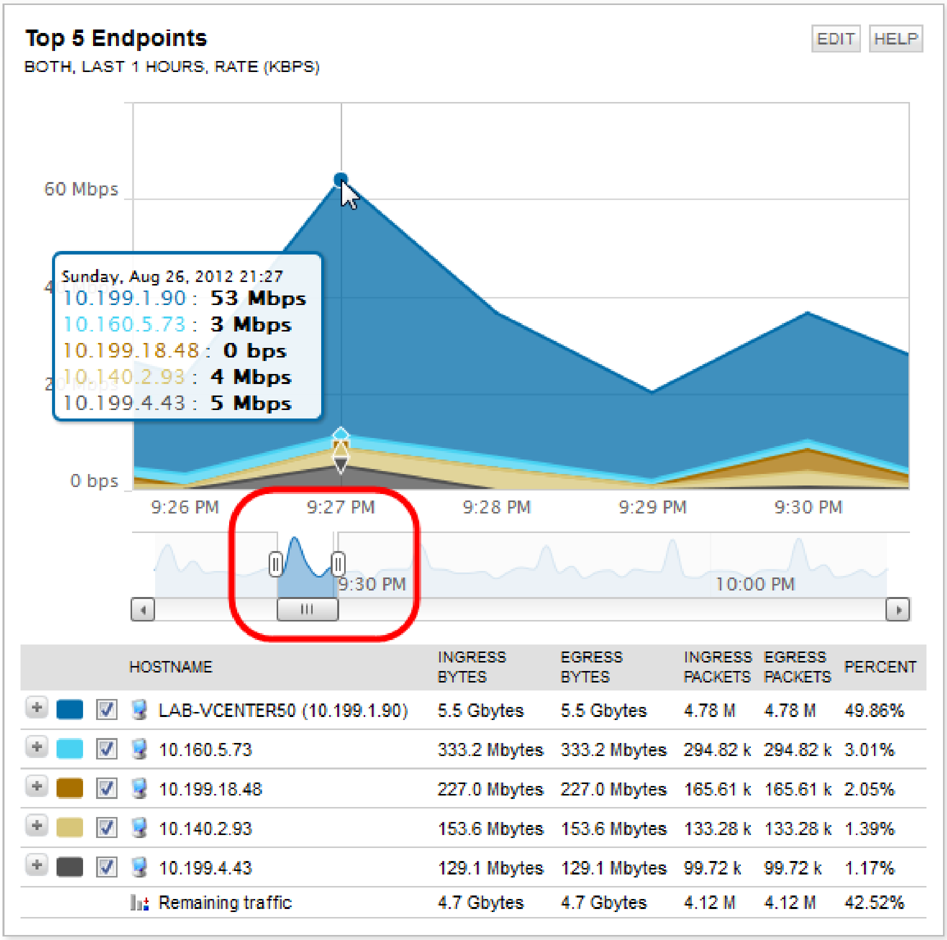
BOTH, LAST 1 HOURS, RATE (KBPS)

Sunday, Aug 26, 2012 21:27
10.199.1.90 : **53 Mbps**
10.160.5.73 : **3 Mbps**
10.199.18.48 : **0 bps**
10.140.2.93 : **4 Mbps**
10.199.4.43 : **5 Mbps**

			HOSTNAME	INGRESS BYTES	EGRESS BYTES	INGRESS PACKETS	EGRESS PACKETS	PERCENT
+	🟦	☑	LAB-VCENTER50 (10.199.1.90)	5.5 Gbytes	5.5 Gbytes	4.78 M	4.78 M	49.86%
+	🟦	☑	10.160.5.73	333.2 Mbytes	333.2 Mbytes	294.82 k	294.82 k	3.01%
+	🟫	☑	10.199.18.48	227.0 Mbytes	227.0 Mbytes	165.61 k	165.61 k	2.05%
+	🟨	☑	10.140.2.93	153.6 Mbytes	153.6 Mbytes	133.28 k	133.28 k	1.39%
+	⬛	☑	10.199.4.43	129.1 Mbytes	129.1 Mbytes	99.72 k	99.72 k	1.17%
			Remaining traffic	4.7 Gbytes	4.7 Gbytes	4.12 M	4.12 M	42.52%

The Top 5 Endpoints s data shown the area chart tell us that at their highest traffic points, conversations involving the LAB-VCENTER50 (10.199.1.90) and 10.160.5.73 endpoints not only generated more traffic than the other top 3 endpoints, but they did so consistently across the displayed time intervals.

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



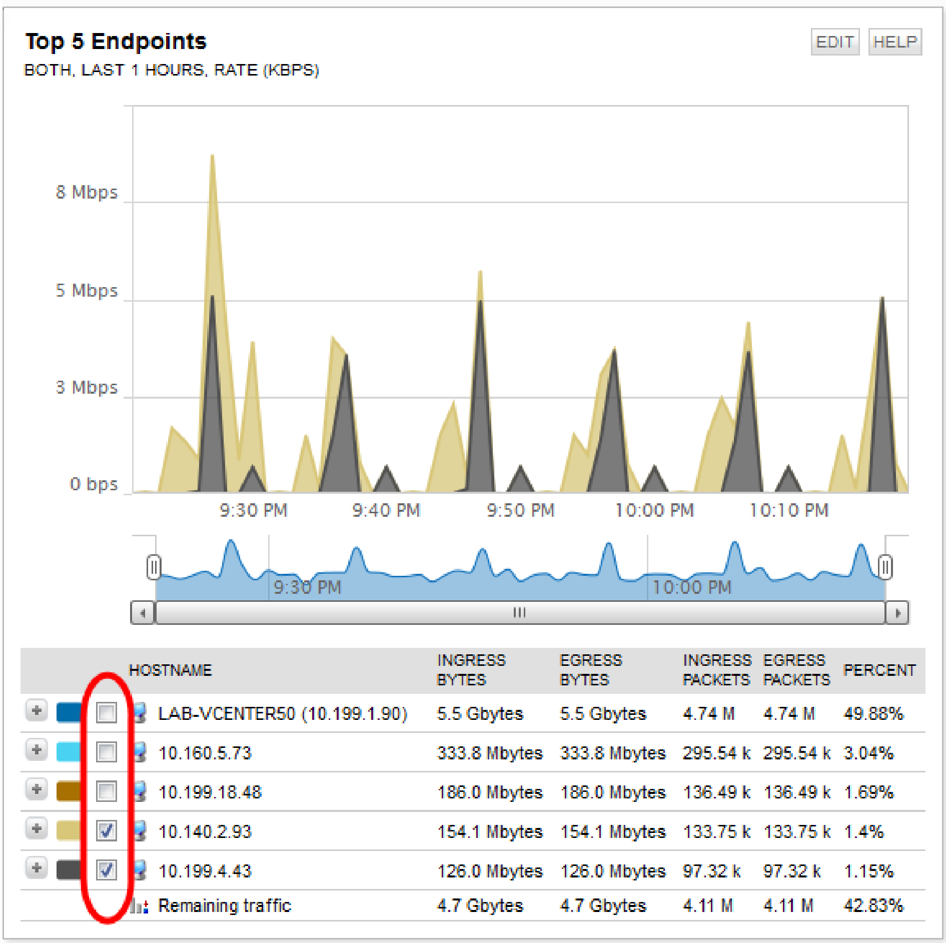
Top 5 Endpoints

BOTH, LAST 1 HOURS, RATE (KBPS)

Sunday, Aug 26, 2012 21:27
10.199.1.90 : **53 Mbps**
10.160.5.73 : **3 Mbps**
10.199.18.48 : **0 bps**
10.140.2.93 : **4 Mbps**
10.199.4.43 : **5 Mbps**

	HOSTNAME	INGRESS BYTES	EGRESS BYTES	INGRESS PACKETS	EGRESS PACKETS	PERCENT
+ 🟦 ☑	LAB-VCENTER50 (10.199.1.90)	5.5 Gbytes	5.5 Gbytes	4.78 M	4.78 M	49.86%
+ 🟦 ☑	10.160.5.73	333.2 Mbytes	333.2 Mbytes	294.82 k	294.82 k	3.01%
+ 🟫 ☑	10.199.18.48	227.0 Mbytes	227.0 Mbytes	165.61 k	165.61 k	2.05%
+ 🟨 ☑	10.140.2.93	153.6 Mbytes	153.6 Mbytes	133.28 k	133.28 k	1.39%
+ ⬛ ☑	10.199.4.43	129.1 Mbytes	129.1 Mbytes	99.72 k	99.72 k	1.17%
	Remaining traffic	4.7 Gbytes	4.7 Gbytes	4.12 M	4.12 M	42.52%

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



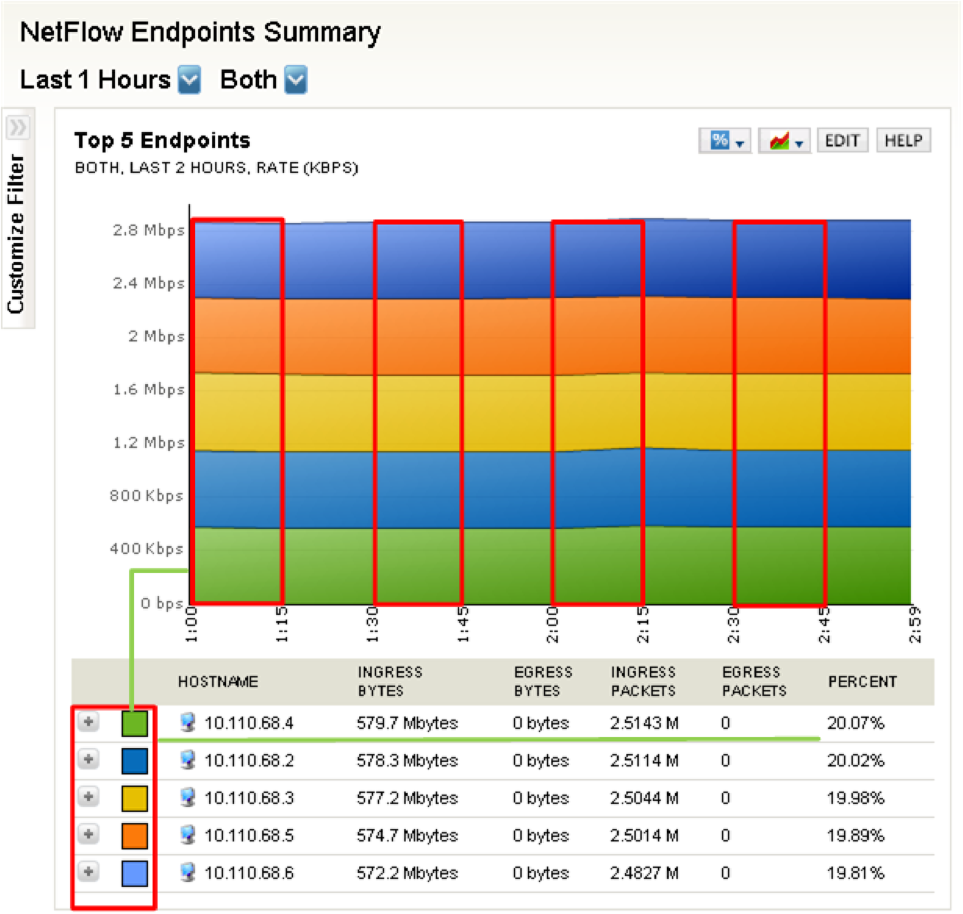
Top 5 Endpoints

BOTH, LAST 1 HOURS, RATE (KBPS)

			HOSTNAME	INGRESS BYTES	EGRESS BYTES	INGRESS PACKETS	EGRESS PACKETS	PERCENT
+	🟦	☐	LAB-VCENTER50 (10.199.1.90)	5.5 Gbytes	5.5 Gbytes	4.74 M	4.74 M	49.88%
+	🟦	☐	10.160.5.73	333.8 Mbytes	333.8 Mbytes	295.54 k	295.54 k	3.04%
+	🟫	☐	10.199.18.48	186.0 Mbytes	186.0 Mbytes	136.49 k	136.49 k	1.69%
+	🟨	☑	10.140.2.93	154.1 Mbytes	154.1 Mbytes	133.75 k	133.75 k	1.4%
+	⬛	☑	10.199.4.43	126.0 Mbytes	126.0 Mbytes	97.32 k	97.32 k	1.15%
			Remaining traffic	4.7 Gbytes	4.7 Gbytes	4.11 M	4.11 M	42.83%

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

Classic Area Charts



NetFlow Endpoints Summary

Last 1 Hours Both

Top 5 Endpoints

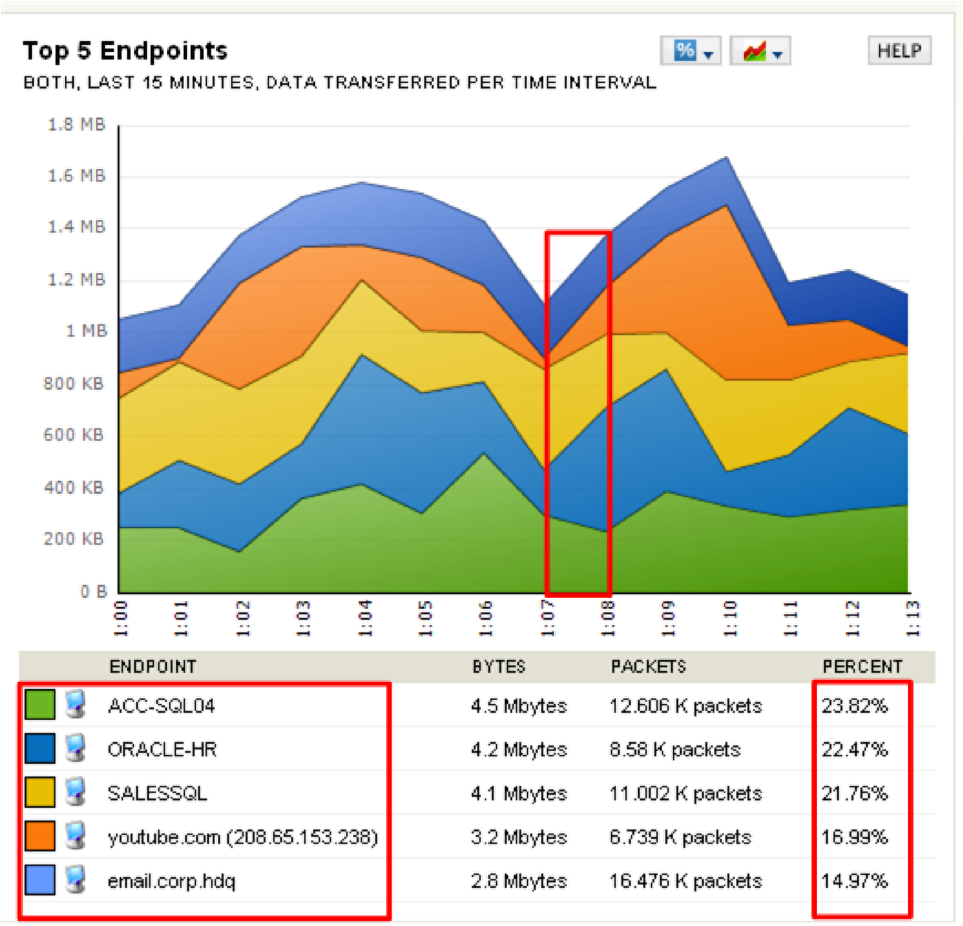
BOTH, LAST 2 HOURS, RATE (KBPS)

		HOSTNAME	INGRESS BYTES	EGRESS BYTES	INGRESS PACKETS	EGRESS PACKETS	PERCENT
+	🟩	10.110.68.4	579.7 Mbytes	0 bytes	2.5143 M	0	20.07%
+	🟦	10.110.68.2	578.3 Mbytes	0 bytes	2.5114 M	0	20.02%
+	🟨	10.110.68.3	577.2 Mbytes	0 bytes	2.5044 M	0	19.98%
+	🟧	10.110.68.5	574.7 Mbytes	0 bytes	2.5014 M	0	19.89%
+	🟦	10.110.68.6	572.2 Mbytes	0 bytes	2.4827 M	0	19.81%

This is the same Top 5 Endpoints data initially shown in the Classic pie chart. Shown here in an area chart, the data tell us that not only did the top endpoints generate equal percentages of traffic but they did so consistently across all intervals.

A glance at any interval tells us each endpoint generated traffic at a rate of about 500 Kbps for each minute of the 2 hours reported.

This next example shows an area chart of less evenly distributed traffic:



Top 5 Endpoints

BOTH, LAST 15 MINUTES, DATA TRANSFERRED PER TIME INTERVAL

	ENDPOINT	BYTES	PACKETS	PERCENT
🟩	ACC-SQL04	4.5 Mbytes	12.606 K packets	23.82%
🟦	ORACLE-HR	4.2 Mbytes	8.58 K packets	22.47%
🟨	SALESSQL	4.1 Mbytes	11.002 K packets	21.76%
🟧	youtube.com (208.65.153.238)	3.2 Mbytes	6.739 K packets	16.99%
🟦	email.corp.hdq	2.8 Mbytes	16.476 K packets	14.97%

The overall percentage numbers tells us that ACC-SQL04 generated the most traffic. However, if you look the minute between 1:07 and 1:08, you can see at a glance that for that particular interval the endpoints SALESSQL and ORACL-HR were the high traffic generators.

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

ip flow-cache timeout active 1

ip flow-cache timeout inactive 15

snmp-server ifindex persist
!
```

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.

Cisco Flexible NetFlow Configuration

Exporting flows on some Cisco devices (for example, the 4500 series, with Supervisor 7) requires using Flexible NetFlow. This configuration example successfully exports flows from a Cisco 4507 with Supervisor 7:

```
flow record ipv4
! match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
  match interface input
 collect interface output
 collect counter bytes
 collect counter packets

flow exporter NetFlow-to-Orion
 destination 10.10.10.10
 source vlan254
 transport udp 2055
export-protocol netflow-v5
flow monitor NetFlow-Monitor
 description Original Netflow captures
 record ipv4
 exporter NetFlow-to-Orion
cache timeout inact 10
cache timeout act 5
vlan configuration 666
ip flow monitor NetFlow-Monitor input
```

The `flow exporter destination` value `transport udp` values must reflect the IP address and port (2055) of your Orion NPM server.

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`.

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.

Juniper Networks sFlow and J-Flow Configurations

Juniper Network switches run both HP's sFlow flow sampling technology and J-Flow, Juniper Networks' own flow sampling technology. Following are two examples of sFlow and J-Flow configurations on Juniper products. For more sFlow and J-Flow configuration examples, see the Juniper Networks website at http://www.juniper.net/techpubs/ and http://kb.juniper.net/InfoCenter/index?page=home.

Juniper sFlow Configuration

You can perform Juniper switch sFlow configuration using the following sample configuration:

```
sflow {
   polling-interval 30;
   sample-rate 128;
   collector 10.1.2.5 {
   udp-port 6343;
   }
   interfaces ge-0/0/0.0;
   interfaces ge-0/0/1.0;
   interfaces ge-0/0/2.0;
   interfaces ge-0/0/3.0;
   interfaces ge-0/0/4.0;
   interfaces ge-0/0/5.0;
   interfaces ge-0/0/6.0;
   interfaces ge-0/0/7.0;
   interfaces ge-0/0/8.0;
   interfaces ge-0/0/9.0;
   interfaces ge-0/0/10.0;
   interfaces ge-0/0/11.0;
   interfaces ge-0/0/12.0;
   interfaces ge-0/0/13.0;
   interfaces ge-0/0/14.0;
   interfaces ge-0/0/15.0;
   interfaces ge-0/0/16.0;
   interfaces ge-0/0/17.0;
   interfaces ge-0/0/18.0;
   interfaces ge-0/0/19.0;
   interfaces ge-0/0/20.0;
   interfaces ge-0/0/21.0;
   interfaces ge-0/0/22.0;
   interfaces ge-0/0/23.0 {
       polling-interval 30;
       sample-rate 128;
   }
}
```

Juniper J-Flow Configuration

Configure Juniper J-Flow devices using a configuration template such as the following:

```
#show interfaces ge-0/0/0
unit 0 {
    family inet {
        sampling {
            input;
            output;
        }
       address 1.1.1.1/30;
    }
}

#show forwarding-options
sampling {
     input {
         rate 100;
     }
     family inet {
         output {
             flow-server 2.2.2.2 {
                 port <JFlow port number e.g. 2055,2056>;
                 version 5;
             }
        }
     }
}
```

Index