SolarWinds

NetFlow Traffic Analyzer Administrator Guide

solarwinds

Unexpected Simplicity

SolarWinds NetFlow Traffic Analyzer 4.0.3

Document revised: 7/8/2014

Table of Contents

Chapter 1: Introduction **12**
- Why Install NTA 12
- How NTA Works 13
- Why Use NTA 14
- What's new in NTA 4.0 17
  - NTA Flow Storage Database 17
  - More Deployment Options 18
  - Migration 18
  - Host and Domain Names 18
  - Update Operations 19

Chapter 2: Installing SolarWinds NetFlow Traffic Analyzer **22**
- Licensing SolarWinds NetFlow Traffic Analyzer 22
- NTA Requirements 23
  - NTA Polling Engine Requirements 23
  - NTA Flow Storage Database Requirements 24
  - Port Requirements 25
  - Virtual Machine Requirements 26
  - NTA Flow Requirements 26
    - Required Fields 27
    - Sampled Flow Supported Fields 28
    - Autonomous Systems Requirements 29
- NTA 4.0 Deployment Options 30
  - Installing a Localized Version of NTA 31
  - Installing NTA 4.0 and NTA Flow Storage Database Locally 32
  - Installing NTA and Remote NTA Flow Storage Database 33

Installing NTA on a 32-Bit Operating System 34
Installing Additional Pollers and Web Consoles 35
Installing NTA 36
Completing the Configuration Wizard 37
Installing NTA Flow Storage Database 39
Configuring Remote NTA Flow Storage Database 40
Upgrading NTA 41
Upgrade Paths and Compatibility 41
Upgrade Steps 42
Database Migration 45
Moving the NTA Flow Storage Database 47
Uninstalling NTA 50
Chapter 3: Configuring SolarWinds NetFlow Traffic Analyzer 51
Configuring NetFlow Management Settings 51
Adding Flow-Enabled Devices and Interfaces 52
Configuring Flow Sources and CBQoS Devices 53
Enabling the Automatic Addition of Flow Sources 54
Enabling Flow Monitoring from Unmanaged Interfaces 54
CBQoS Polling Settings 56
Adding Flow Sources and CBQoS-Enabled Devices 56
Deleting Flow Sources and CBQoS-Enabled Devices 58
Configuring Monitored Ports and Applications 59
Configuring Data Retention for Flows on Unmonitored Ports 61
Enabling/Disabling Monitoring for Ports or Applications 61
Adding Ports or Applications 63
Editing Ports or Applications 63
Deleting Ports or Applications 64
Selecting IP Address Groups for Monitoring 64
Selecting IP Ranges to Be Monitored 65
Adding a New IP Address or IP Address Group 66
Editing IP Addresses or IP Address Groups 66

Deleting IP Address or IP Address Groups 67
Configuring NetFlow Collector Services Ports 67
Configuring Protocol Monitoring 68
Configuring NetFlow Types of Services 69
Configuring Top Talker Optimization 70
Configuring DNS and NetBIOS Resolution 71
Enabling NetBIOS Resolution 71
DNS Resolution Options in NTA 72
How Does Default DNS Resolution Work in NTA? 73
Configuring DNS Resolution 74
Configuring IP Address Processing 74
Configuring Database Settings 75
Database Maintenance 76
Compression And Aggregation Settings in NTA 78
Configuring NTA Flow Storage Database Backups 79
Best Practices 79
Scheduling Regular Backups 81
Backing up the NTA Flow Storage Database Manually 81
Specifying Backup Folders For NTA Flow Storage Database 82
Restoring Backups 83
Configuring Charting and Graphing Settings 84
Enabling Progressive Charting 84
Configuring Percentage Type for Top XX Lists 85
Top XX List Resource Percentages 85
Configuring Area Charts Display Units 87
Configuring Resource Default Time Periods 88
Configuring the NTA View Refresh Rate 88
Optimizing Performance of NTA 89
Configuring On Demand DNS resolution 90
Limiting Flow Collections To Top Talkers 90
Limiting the Data Retention Period for the Orion SQL Database 91

Setting Retention Period for NTA Flow Storage Database 92
Adjusting Data Aggregation Settings 93
Chapter 4: Viewing NetFlow Traffic Analyzer Data in the Orion Web Console 96
Editing Resources 97
Working with Charts 97
Pie Charts 98
Area Charts 102
Customizing Charts 107
Selecting Classic or Interactive Charts 108
Customizing Resources for the Current Session 110
Customizing Interactive Charts 111
Customizing Classic Charts 113
Customizing Views 115
Enabling the NetFlow Traffic Analysis Summary View 115
Creating New Views 116
Creating Custom Views with the Flow Navigator 117
Adding NetFlow Resources to Web Console Views 123
Adding an Endpoint Centric Resource 124
Configuring View Limitations 125
Editing Views 125
Editing Time Settings for Views 127
Editing Flow Direction in Views 128
Copying Views 128
Deleting Views 129
Deleting a Filtered View 129
Views by Device Type 129
Monitoring Traffic Flow Directions 130
Setting Flow Direction 131
Viewing Class-Based Quality of Service (CBQoS) Data 132
Chapter 5: Working with NTA 136
Implementing and Monitoring CBQoS Policies 136

Using NTA to Prepare a CBQoS Implementation 136
Dynamically Monitoring CBQoS 139
Monitoring Autonomous System Networks (through BGP) 141
Preparing to Monitor Autonomous System Networks 141
Managing Autonomous System Networks 145
Monitoring Autonomous System Networks 147
Top XX Autonomous Systems 147
Top XX Autonomous System Conversations 148
Finding the Cause of High Bandwidth Utilization 148
Tracking Traffic by Site 149
Performing an Immediate Hostname Lookup 154
Interacting with the thwack User Community 154
User Scenarios 154
Locating and Isolating an Infected Computer 155
Locating and Blocking Unwanted Use 156
Recognizing and Thwarting Denial of Service Attacks 157
Chapter 6: Troubleshooting NetFlow Traffic Analyzer 158
NetFlow Collector Services 158
Editing or Adding Collection Ports 159
Deleting Collectors 159
Troubleshooting Collector Services 160
NetFlow Sources 161
NTA Events 162
Filtering Events and Displaying Historical Events 164
Clearing Events 167
NetFlow Events List 168
NetFlow Receiver Service Stopped 168
License Limitation 168
No Valid License 168
No Space Left On NTA Flow Storage Database 168
Invalid Template 169

Invalid IPFIX Template 169
No Template Received 169
Not Enabled NetFlow Data Export 170
NetFlow Time Difference Error 170
Unmanaged NetFlow Node 170
Unmanaged NetFlow Interface 171
Unmonitored NetFlow Interface 171
Not Primary NPM Node IP Address 171
Running Out Of Space NTA Flow Storage Database 172
Unmonitored Interface Automatically Added 172
NetFlow Time Difference Warning 172
NetFlow Time Difference Warning Ended 173
NetFlow Receiver Service Started 173
NetFlow Receiver Service Settings Changed 173
NetFlow Event: Interface Index Mapping Used for A Node 173
NetFlow Event: Removing Interface Index For A Node 173
NetFlow Database Maintenance 173
Scheduled Shrink Performed 174
Updating Data To Be Used In Top XX Aggregated Resources 174
Windows Firewall Is Turned On 174
NetFlow Licensing 174
Unable To Start Listening On Port 175
Port Is Free Listening 175
Notification Event Status Reset 175
Enough Space Available On NTA Flow Storage Database 175
Resolving Unknown Traffic 176
Enabling Flow Monitoring from Unmanageable Interfaces 178
Unmanageable Interface Speed 179
Chapter 7: NetFlow Traffic Analyzer Reports 180
Reports in NTA 4.0 180
Managing Reports 181

Printing Reports 181
Scheduling Reports 181
Using Custom Properties for Creating Reports 182
Report Writer Reports 182
Web-Based Reports 182
Using Customized Report Writer Reports in the Orion Web Console 183
NetFlow-Specific Predefined Reports 184
Historical NetFlow Reports 184
Historical CBQoS Reports 186
Executing Reports 187
Creating Web-Based Reports for NTA 188
Creating Web-Based Reports Using SWQL 190
Editing Web-Based Reports 192
Example: Creating Customized Report Writer Reports as Web-Based 200
Defining the Object to Report On 203
Defining Column Details for the Report 206
Chapter 8: Using NTA Advanced Alerts 210
NetFlow-Specific Predefined Alerts 210
Top Talker Alerts 210
CBQoS Alerts 211
Configuring NetFlow Advanced Alerts 212
Using Orion Advanced Alerts 214
Creating and Configuring Advanced Alerts 215
Creating a New Advanced Alert 216
Naming, Describing, and Enabling an Advanced Alert 217
Setting a Trigger Condition for an Advanced Alert 218
Setting a Reset Condition for an Advanced Alert 221
Setting Suppression for an Advanced Alert 223
Setting the Monitoring Period for an Advanced Alert 224
Setting a Trigger Action for an Advanced Alert 225
Setting a Reset Action for an Advanced Alert 226

Alert Escalation 226
Understanding Condition Groups 227
Using the Advanced Alert Manager 228
Adding Advanced Alert Actions 232
Available Advanced Alert Actions 232
Sending an E-mail/Page 233
Playing a Sound 234
Logging an Advanced Alert to a File 235
Logging an Advanced Alert to the Windows Event Log 237
Logging an Advanced Alert to the NetPerfMon Event Log 238
Sending a Syslog Message 239
Executing an External Program 240
Executing a Visual Basic Script 241
Emailing a Web Page 242
Using Text to Speech Output 243
Sending a Windows Net Message 244
Sending an SNMP Trap 245
Using GET or POST URL Functions 246
Dial Paging or SMS Service 247
Testing Alert Actions 247
Viewing Alerts in the Orion Web Console 249
Acknowledging Advanced Alerts in the Web Console 249
Escalated Advanced Alerts 250
Escalated Alert Example 250
Creating a Series of Escalated Alerts 251
Viewing Alerts from Mobile Devices 254
Appendix A: Managing Software Licenses 255
Activating Your NTA License 255
Activating an NTA Evaluation License 255
Activating an NTA License with Internet Access 256
Activating an NTA License without Internet Access 256

Installing License Manager 258
Requirements 258
Using License Manager 259
Deactivating Currently Installed Licenses 259
Re-Activating Licenses 260
Upgrading Currently Installed Licenses 260
Activating Evaluation Licenses 260
Appendix B: Device Configuration Examples 262
Setting up Network Devices to Export NetFlow Data 262
Configuring NetFlow Devices 265
Cisco NetFlow Configuration 265
Cisco Flexible NetFlow Configuration 266
Cisco NGA 3000 Series 267
Configuring sFlow and J-Flow Devices 268
Brocade (Foundry) sFlow Configuration 269
Extreme sFlow Configuration 269
HP sFlow Configuration 270
Juniper Networks sFlow and J-Flow Configurations 270
Juniper sFlow Configuration 271
Juniper J-Flow Configuration 272
Appendix C: Glossary 273

Chapter 1: Introduction

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

Why Install 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, 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 SolarWinds 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 NTA solution are not purely extrapolated data, but they are based on real information collected about the network by the Network Performance Monitor product that is at the heart of SolarWinds NetFlow Traffic Analyzer.

Out of the box, SolarWinds 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

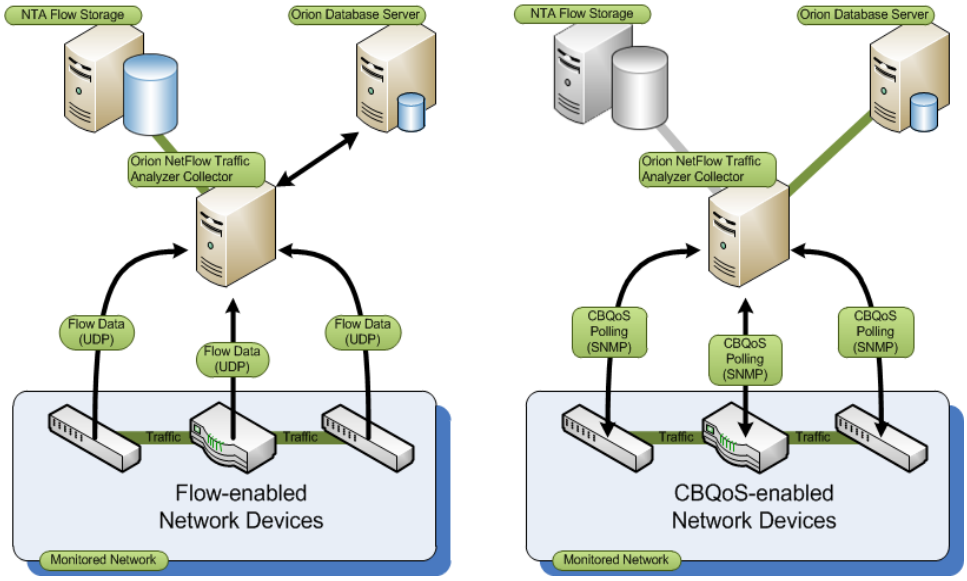
These monitoring capabilities, along with the customizable Orion Web Console and reporting engines, make NTA the easiest choice you will make involving your flow monitoring needs.

How NTA Works

Flow- and CBQoS-enabled devices can provide a wealth of IP-related traffic information. NTA collects this traffic data, correlates it into a useable format, and then presents it, with detailed network performance data collected by SolarWinds 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 NTA installation showing, generally, how flow analysis and CBQoS polling function in NTA. Flow analysis and CBQoS polling occur simultaneously: flow-enabled devices send flow data to the NTA collector on port 2055, and the 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 NTA installation would not require that all CBQoS- and flow-capable devices be configured to interact directly with the NTA collector. For more information about effectively deploying NetFlow on your network, see SolarWinds technical reference "NetFlow Basics and Deployment Strategies".



Why Use NTA

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

Orion Alerts Integration

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 Using NetFlow 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)

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

Filtered views including both ingress and egress traffic

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

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, NTA will immediately be able to provide IPFIX flow monitoring.

Cisco Class-Based Quality of Service (CBQoS) monitoring

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.

NTA also supports CBQoS nested policies.

Improved availability and performance

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

Analytical capacity planning

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

Optimized network resource allocation

Information provided by 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 NTA is built on the proven 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

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 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 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.

NTA also supports sampled NetFlow, taking into account the sample rate set on your devices to display the traffic statistics that match Orion interface utilization charts.

NTA Flow Storage Database

NTA 4.0 on 64-bit operating systems uses a new database for storing your flow data, the NTA Flow Storage Database. The new database brings you the following benefits:

- Increased NTA performance.
- Customizable retention of raw data without aggregation.
- Remote installation on any computer in your network.

Note: NTA 4.0 is also available for 32-bit operating systems, however this version keeps using the Orion SQL database and the above mentioned

benefits do not apply. Please consider upgrading your operating system and installing NTA with the new NTA Flow Storage Database.

What's new in NTA 4.0

This section provides an overview of what's new in NTA 4.0 which is available in two basic versions:

NTA 4.0 on 32-bit operating systems is still based on SQL database only and thus could be compared with NTA 3.11 with all hotfixes and a few minor fixes applied. There are no new features.

NTA 4.0 on 64-bit operating systems introduces a new database for storing flow data with the following updates:

- NTA Flow Storage Database
- More Deployment Options
- Migration Options
- Host and Domain Names
- Update Operations (Updating IP Groups, Applications, and NetFlow Sources)

NTA Flow Storage Database

NTA 4.0 on 64-bit operating systems uses two databases:

- **MS SQL** for storing CBQoS information. NTA further uses data polled and stored in the Orion SQL database by NPM.
- **NTA Flow Storage Database** for storing flow data.

  Warning: There are two databases to backup and maintain. To ensure that NTA data are consistent, execute the backup and restore of both databases (both NTA Flow Storage Database and Orion SQL) at the same time.

NTA Flow Storage is a no-SQL column-oriented database using bitmap indexes. The new NTA Flow Storage Database brings you the following benefits:

- Increased NTA performance – better load times of NTA resources and reports. NTA is also capable of processing more flows per second.

  Note: However, storing more detailed data can affect NTA performance. Loading endpoints, reports, and graphs over longer time periods requires

handling an increased amount of data, and thus can result in slower rendering and processing.

- Storing more information together with the flows which results for example in faster displaying your IP Address groups.
- Customizable retention of raw data without aggregation. NTA Flow Storage Database stores data with one-minute granularity for the whole retention period (30 days by default) thus enabling you to see your flow data in more detail.
- Flexible deployment options – you can use the NTA Flow Storage Database embedded in your NTA server or install NTA Flow Storage Database remotely on any computer in your network.

More Deployment Options

NTA 4.0 provides flexible deployment options to fit your network topology. You can either use NTA 4.0 on 32-bit operating systems with an Orion SQL database or on 64-bit operating systems using either embedded or remote NTA Flow Storage Database. For more information, see NTA 4.0 Deployment Options.

Migration

When upgrading to NTA 4.0 with NTA Flow Storage Database, you can decide whether you want to migrate your historical data from the Orion SQL database immediately or later or whether you do not want to migrate them at all. For more information, see Database Migration.

Host and Domain Names

When flows are received from an IP address, NTA asks a DNS server to resolve the appropriate hostname or domain. This affects the way NTA filters your data, groups items in endpoint-related resources and the way host and domain names are displayed in the Orion Web Console.

For more details, see Configuring DNS and NetBIOS Resolution.

Filtering

In **NTA 4.0 on 32-bit operating systems and older NTA versions**, filtering both by hostnames and IP addresses is based on IP addresses. If you want to filter by a hostname, it is transferred to the IP address that is currently used for it. Per default, hostnames are resolved once every 7 days. If the IP

address changes within this time period, NTA filters will always display only the data connected with the currently resolved hostname.

Example:

Consider having a computer with the hostname *PC*. At first, it has IP address *xxx.xxx.xxx.1*, and within the 7-days-time period, the IP address changes to *xxx.xxx.xxx.2*. During 7 days after the hostname *PC* was resolved for *xxx.xxx.xxx.1*, filtering by the hostname will return only data for *xxx.xxx.xxx.1*, even if *PC* does not use the IP address any more. After 7 days, the hostname is resolved again, and filtering by the hostname *PC* will only display data for *xxx.xxx.xxx.2* for another 7 days.

However, if you use the IP Address for filtering data, you will get data for the currently valid IP address - either *xxx.xxx.xxx.1* or *xxx.xxx.xxx.2*.

In **NTA 4.0 on 64-bit operating systems**, filtering both by host names and IP addresses is based on hostnames. This way, filtering by hostnames returns the same results as filtering via IP addresses.

Endpoint-related resources

In **NTA 4.0 on 32-bit operating systems and in older NTA versions**, items in endpoint-related resources are grouped according to IP addresses.

NTA 4.0 on 64-bit operating systems groups items in endpoint related resources by the hostname.

Host and domain names in NTA resources

NTA does not apply changes of hostname/domain name to your historical data.

Note: If a hostname/domain name changes, you can see flows from the same machine as two items – at first under the old name and after the change under the new name.

In **NTA on 64-bit operating systems**, Top XX resources will thus show data split into more items, based on the appropriate resolved name.

Update Operations

In NTA 4.0 on 64-bit operating systems, updates of IP groups, applications and NetFlow sources are applied to both current and historical data. To make

changes to your IP groups, applications or NetFlow sources, complete the following steps:

1. Go to the appropriate management page (Edit IP Address Groups, Manage Applications, or Manage NetFlow Sources).
2. Make the changes there.
3. Click **Submit** to start the update operation. which applies your changes not only on the newly collected data, but also to historical data already available in your database.

Update operations:

- apply your changes not only to the newly collected data, but also to historical data already available in your database.
- are mutually exclusive and run one-at-a-time. It means that when one update operation is running, you cannot submit further updates until the operation in progress finishes. If you for example click Submit to apply changes to your applications, you cannot apply any other application, IP address groups or NetFlow sources changes until the first update operation is finished.
- run on the background and the data in your Orion Web Console are updated continuously, with most recent data updated first. It means that with each refresh of your Orion Web Console, you can see your updates applied.

Note: Backing up your database also belongs to the mutually exclusive operations. If a backup of your database is running, you cannot simultaneously submit any changes to your IP address groups, application or NetFlow sources.

Displaying IP Groups

In NTA 4.0 on 32-bit operating systems and in older versions, creating IP groups was fast, but displaying IP address groups was a time and performance intensive process.

In NTA 4.0 on 64-bit operating systems, creating groups is more time-consuming than displaying them, because the source and destination IP group details are added into each flow. The currently set view is applied on all records, including historical data.

For more information about configuring IP Groups, see Selecting IP Address Groups for Monitoring.

For more information about configuring Applications, see Configuring Monitored Ports and Applications.

NetFlow Sources

Updating NetFlow sources is also an update and thus belongs to the exclusive one-at-a time operations.

Information about whether a NetFlow source monitoring is enabled or disabled is stored directly in the flow.

For more information about configuring NetFlow Sources, see Adding Flow Sources and CBQoS enabled Devices.

Chapter 2: Installing SolarWinds NetFlow Traffic Analyzer

NTA provides a simple, wizard-driven installation process for collecting data from any flow-enabled devices monitored by SolarWinds Network Performance Monitor.

Notes:

- 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 NTA installer contains binaries for the main poller, an additional poller, and additional web interfaces. The NTA installer determines the type of installation automatically to match already present NPM type.
- To complete your installation, you must provide your NetFlow traffic port and confirm that it is enabled and sending flow data.

Licensing SolarWinds NetFlow Traffic Analyzer

Licensing for NTA follows the license level of your underlying NPM installation. For more information, see Licensing Network Performance Monitor in the *Orion Network Performance Monitor Administrator Guide*.

The following types of NTA licenses are currently available.

- NetFlow Traffic Analyzer for Orion SL100
- NetFlow Traffic Analyzer for Orion SL250
- NetFlow Traffic Analyzer for Orion SL500
- NetFlow Traffic Analyzer for Orion SL2000
- 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 NTA, the effective capacity of your installation may be lower if the monitored interface throughput is especially high.

NTA Requirements

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

NTA Polling Engine Requirements

Hardware and software requirements for the current NTA version are the same as for NPM 10.6. For more information, see Orion Requirements in the *Orion Network Performance Monitor Administrator Guide*.

The following requirements ensure the scalability benefits of NTA 4.0:

64-bit operating system

If you have more than one poller, make sure they are all installed on 64-bit operating systems.

Note: You can also install NTA 4.0 on a 32-bit operating system, however, your flow data will be stored in the Orion SQL database, and you will not be able to enjoy the performance benefits of the NTA Flow Storage Database. The server for NTA 4.0 on 32-bit operating system should comply with the requirements for NPM 10.6. For more information, see Orion Requirements in the *Orion Network Performance Monitor Administrator Guide*.

NPM 10.6

NPM 10.6 has the new web based reporting engine which is required for NTA 4.0.

NTA Flow Storage Database

NTA Flow Storage is the database where NTA stores your flow data. If you decide to store flows on a remote server (recommended for production environments), you need to install the NTA Flow Storage Database there

first. For more information about NTA Flow Storage Database requirements, see NTA Flow Storage Database Requirements.

Orion SQL Database

The connection to Orion SQL database is required, because CBQoS data and some additional low level details are still stored in Orion SQL database. For more information about SQL database requirements, see Requirements for the Orion Database Server in the *Orion Network Performance Monitor Administrator Guide*.

Note: 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 NTA in production environments.

NTA Flow Storage Database Requirements

The following table lists the minimum hardware requirements for the NTA Flow Storage Database which is used for storing flow data in NTA 4.0 on 64-bit operating systems.

Recommendations:

- Install the NTA Flow Storage Database on a different server than the Orion SQL database. This way, the high amount of incoming flows will not affect the performance.
- Do not install the NTA Flow Storage Database on an NTA/NPM polling engine (main or additional) because it might affect performance.
- Use a dedicated disk for storing your flows data.

Hardware/ Software	Requirements
CPU	3GHz or faster Evaluation requires 2 CPUs Production environments require 4 CPUs (4-16 CPUs)
RAM	Evaluation requires 8GB or more Production environments require 16GB or more (16-128GB). To ensure optimal performance, you should increase RAM together with the database size.

Hardware/ Software	Requirements
Hard Drive Space	20GB on 7200 rpm disk or more **Note**: With the default 30-days retention period and default top talker optimization, you should plan at least 8GB of additional storage capacity per sustained 1000 flows per second. However, the required hard drive space strongly depends on your flow traffic, and SolarWinds thus recommends you to provide more space accordingly. NTFS file system required. **Warning**: The only RAID configurations that should be used with NTA are 0 or 1+0. Other RAID or SAN configurations are not recommended, as they can result in data loss and significantly decreased performance.
OS	64-bit Windows Server 2003 SP 2 or newer

Port Requirements

The following table lists ports NetFlow Traffic Analyzer uses for communicating with other devices and servers.

Application Port	Usage
80 (TCP)	port used for web console and any other web servers
161 (TCP)	port used for polling CBQoS-enabled devices
1433 (TCP)	port for communication between the NTA Flow Storage Database and the existing SQL server
2055 (UDP)	port for receiving flows on any NTA collector
17777 (TCP)	port for sending an receiving traffic between NPM and other Orion Modules
device specific	any device specific ports

Virtual Machine Requirements

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

- Each virtual machine needs to meet the NPM requirements for virtual machines. For more information, see Requirements for Virtual Machines and Servers in the *Orion Network Performance Monitor Administrator Guide*.
- Each installation of NPM should have its own, dedicated NIC

Note: NPM uses SNMP to monitor your network. SNMP traffic is generally assigned low priority, and thus you can experience gaps in monitoring data.

NTA Flow Requirements

NTA supports these flow versions:

Flow	Supported Versions	Sampled Flow Support
NetFlow	v5 and 9 **Note**: NetFlow v9 must have an appropriate template with all required fields (see table below).	v5 and v9 **Note**: Some devices using IOS versions export flows without specifying that it is being sampled. NTA processes these flows as un-sampled.
sFlow	n/a	v2, v4 and v5
J-Flow	supported	supported **Note**: Some devices using JunOS versions export flows without specifying that it is being sampled. NTA processes these flows as un-sampled.
IPFIX	supported	
NetStream	v5 and v9	

Required Fields

Most flow-enabled devices use a set of static templates to which exported flows conform.

If flow packets do not include the following field types and appropriate values, NTA ignores the packets.

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 NTA supports flow monitoring for a device, at least one of the templates the device exports satisfies these requirements.
- The NetFlow v9 specification indicates that templates may be configurable on a device-by-device basis. However, most devices have a set of static templates to which exported flows conform. When SolarWinds states that a

device is supported by Orion NTA, SolarWinds has determined that at least one of the templates the device is capable of exporting will satisfy the Orion NTA requirements. For more information, see the Cisco white paper, "NetFlow Version 9 Flow-Record Format".

- Cisco 4500 series switches do not provide information for the TCP_FLAGS field (field type number 6) corresponding to a count of all TCP flags seen in the related flow.
- Cisco Adaptive Security Appliances (ASA) are capable of providing flow data using a limited template based on the NetFlow v5 template.

Sampled Flow Supported Fields

If you are using sampled flows, packets need to contain not only the fields mentioned in the Required Fields section, but also fields supported by NTA for sampled flows. Supported fields depend on the flow version used.

Notes:

- Sampling mode has to be non-zero, otherwise NTA processes flows as non-sampled.
- If some of the required fields are missing on your device or contain unexpected values, please contact your device vendor.

NetFlow v5 and J-Flow v5 Header Format

NTA supports the following bytes in the v5 header format:

Bytes	Contents	Description
22-23	sampling_ interval	First two bits hold the sampling mode; remaining 14 bits hold value of sampling interval.

For more information, consult NetFlow Export Datagram Format on www.cisco.com.

NetFlow v9 and J-Flow v9

Supported fields depend on the template you are using:

- Option template
- Flow template

Option template

Field Type	Field Type Number	Description
FLOW_SAMPLER_ID	48	Identifier shown in "show flow-sampler"
FLOW_SAMPLER_ MODE	49	The type of algorithm used for sampling data: 0x02 random sampling.
FLOW_SAMPLER_ RANDOM_INTERVAL	50	Packet interval at which to sample.

Flow template

Field Type	Field Type Number	Description
SAMPLING_ INTERVAL	34	When using sampled NetFlow, the rate at which packets are sampled, for example, a value of 100 indicates that one of every 100 packets is sampled.
SAMPLING_ ALGORITHM	35	The type of algorithm used for sampled NetFlow: 0x01 Determin-istic Sampling ,0x02 Random Samp-ling

For more information, consult NetFlow Version 9 Flow-Record Format on www.cisco.com.

Autonomous Systems Requirements

If you want to monitor autonomous systems via BGP, the flows have to contain information in appropriate bytes or fields.

Note: NTA does not support extracting BGP information from sFlows.

NetFlow v5 and compatible flows

The flow record has to contain data for the following bytes:

Bytes	Contents	Description
40-41	src_as	Autonomous system number of the source, either origin or peer.
42-43	dst_as	Autonomous system number of the source, either origin or peer.

For more information, consult NetFlow Export Datagram Format on www.cisco.com.

NetFlow v9, IPFIX, and compatible flows

The flow record from autonomous systems has to contain data in the following field types.

Field Type	Value	Length (bytes)	Description
SRC_AS	16	N (default 2)	Source BGP autonomous system number where N could be 2 or 4.
DST_AS	17	N (default 2)	Destination BGP autonomous system number where N could be 2 or 4.

For more information, consult NetFlow Version 9 Flow-Record Format on www.cisco.com.

NTA 4.0 Deployment Options

NTA is a very flexible solution providing you with various deployment options fit for your personal needs.

NTA 4.0 stores collected NetFlow data in one NTA Flow Storage Database. Deploying the NTA Flow Storage Database locally on multiple sites and displaying all the data via one Orion Web Console is not supported.

The following sections introduce the installation process for different deployments:

- Installing a Localized Version of NTA
- Installing NTA and NTA Flow Storage Database on the same server
- Installing NTA and NTA Flow Storage Database on a remote server
- Installing NTA on 32-bit operating systems
- Installing additional pollers and additional web sites
- Changing the Location of NTA Flow Storage Database

Installing a Localized Version of NTA

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

- **Primary Locale** – The locale selected when installing NPM. Once selected, you cannot change the Primary Locale without uninstalling and reinstalling NPM. NTA uses the locale set during the installation of NPM.
- **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.

NTA is available in the following localizations:

- English
- Japanese

To install a localized version of NTA:

1. When installing NPM, select the language you want to use in NTA as the preferred language.

   Note: NTA is not available in German. If you select German as your preferred language during the NPM installation, NTA will install in English.

2. Install NTA. For more details, see NTA 4.0 Deployment Options.

Notes:

- The locale settings (Primary Locale) are specified during the installation and cannot be changed later. Once selected, you cannot change the Primary Locale without uninstalling and reinstalling both NPM and NTA.
- You can change the locale in your browser settings (user locale), however, the database still reflects the primary locale. As a result, resource names, object details, and monitoring events display in the web console under the Primary Locale.

Upgrading Localized NTA Versions

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

To change the language during a NTA Upgrade:

1. Reinstall NPM using the required locale.
2. Reinstall NTA. For more details, see NTA 4.0 Deployment Options.

   Note: Reports and alerts created in older NTA versions with the previously used locale reflect the original locale settings. If you change the locale, you need to reconfigure them to work properly.

Installing NTA 4.0 and NTA Flow Storage Database Locally

NTA 4.0 uses a new database for storing your flows, the NTA Flow Storage Database which allows for a significant improvement in performance.

Notes:

- We recommend using a dedicated server, or at least a dedicated disk or partition for the NTA Flow Storage Database.
- Installing NTA Flow Storage Database on a polling engine (main or additional) server is not recommended. If the server resources are shared by the database and NTA/NPM, the potential performance improvement is not so significant as it could be if the database were on a separate server.

  For more information, see NTA Flow Storage Database Requirements.

To install SolarWinds NetFlow Traffic Analyzer and NTA Flow Storage Database locally:

1. Install NTA and NTA Flow Storage Database:
   Start the Setup Wizard and select the configuration option **NPM/NTA/NTA Flow Storage Database on the same server**. For more details, see Installing NTA.
2. Select one of the available licensing options. For more details, see Activating Your NTA License.
3. Configure your NTA and local NTA Flow Storage Database:

   Define the location for NTA Flow Storage Database by filling in an absolute path to the appropriate folder. For more details, see Completing the Configuration Wizard.

4. Proceed to add your NetFlow devices and interfaces to 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.

Installing NTA and Remote NTA Flow Storage Database

NTA 4.0 allows you to install the database for storing your flows on any computer within your network.

Note: Installing NTA Flow Storage Database on a polling engine (main or additional) server is not recommended. If the server resources are shared by the database and NTA/NPM, the potential performance improvement is not so significant as it could be if the database were on a separate server.

To install NTA using a remote NTA Flow Storage Database:

1. Make sure you have NPM installed on the server where you want to install NTA.

   Note: Please note the credentials for accessing the Orion SQL database used by NPM; you will need them to configure the NTA Flow Storage Database.

2. Log on to your NTA Flow Storage Database server, install and configure the remote NTA Flow Storage Database. For more details, see Installing NTA Flow Storage Database.

3. Log on to the NPM server and install NTA only.
   Start the NTA Setup Wizard, select the installation option **NPM/NTA and NTA Flow Storage Database on two separate servers**, and enter the **NTA Flow Storage Database Server** hostname or IP address. For more details, see Installing NTA.
4. Select one of the available licensing options. For more details, see Activating Your NTA License.
5. Proceed to add your NetFlow devices and interfaces to 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.

Installing NTA on a 32-Bit Operating System

NTA 4.0 can be installed on 32-bit operating systems, too. However, you have to use the MS SQL database for storing your flow data. Please, consider upgrading to a 64-bit operating system.

To install NTA on a 32-bit operating system:

1. Install NTA.
   Launch the NTA installation executable and complete the NTA Setup Wizard. The wizard automatically detects that you are installing NTA on a 32-bit operating system, and will provide only screens relevant for this option. For more details, see Installing NTA.
2. Select one of the available licensing options. For more details, see Activating Your NTA License.
3. Configure your NTA. For more details, see Completing the Configuration Wizard.
4. Proceed to add your NetFlow devices and interfaces to 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.

Installing Additional Pollers and Web Consoles

Installing additional pollers and Web Consoles helps you extend your SolarWinds NTA implementation.

Additional pollers aid you in load balancing, you can increase the monitoring capacity of your installation by enabling multiple pollers that work in parallel across your network.

Additional websites ensure redundant access through more than one web server. The additional web server enables remote access to the Orion Web Console from a location other than your main server. Remote users can view the primary Orion Web Console without deploying an entire Orion installation or excessively taxing the resources of your primary SolarWinds server.

License

Additional pollers and web consoles do not require special licenses; the appropriate licenses are automatically overtaken from Orion.

Requirements:

- NTA additional pollers and websites require that an appropriate additional NPM poller or website is installed on the server.
- Installing additional pollers and websites requires that the main NTA poller is installed.
- If your main NTA poller is installed on a 64-bit server, all additional pollers must also be installed on servers with 64-bit operating systems.
- The NTA version you are installing on an additional poller/website must match the version of NTA you are running on your Orion main poller.

To install an additional poller or website:

1. Log on to the server where you want to install the additional poller or website.
2. Launch the executable for installing NTA.

   Note: The NTA installer will automatically find out that you are installing an additional poller or website, because it detects that NPM additional poller/website available on the server.

3. Complete the installation:

   For more information about installing additional pollers, see Using Additional Polling Engines in the *Orion Network Performance Monitor*

Administrator Guide.

For more information about installing additional web servers, see Using an Additional Web Server in the *Orion Network Performance Monitor Administrator Guide*.

Installing NTA

NTA is provided in a unique installation package which allows you to install the following NTA components, based on the configuration detected on the server:

- NTA Server
- NTA Flow Storage Database
- NTA Additional Poller
- NTA Additional Website

Note: The installation differs according to the selected deployment.

To install NTA, complete the following procedure:

1. Log on to the NPM server that you want to use for flow analysis.
2. Launch the executable in its location (on the physical media or in the folder you have downloaded it to).
3. Review the Welcome information, and then click **Next**.
4. Select the configuration you want to use and click **Next** to continue.
    - **NPM/NTA and NTA Flow Storage Database** on two separate servers (recommended)

      You need to have NTA Flow Storage Database already installed. If it is not the case, log on to the server where you want to install NTA Flow Storage Database and run this installer on the server. For more information, see Installing NTA Flow Storage Database.

      Fill in the **NTA Flow Storage Database Server** hostname or IP address and click **Test Connection**.

      Note: For more information about troubleshooting the connection, see the KB article "Troubleshooting connection to NTA Flow Storage Database server".

- **NPM/NTA/NTA Flow Storage Database** on the same server.

  This option is recommended for evaluations. NTA checks your server configuration and informs you if it does not meet the minimum requirements. If the warning appears, please consider upgrading your server or deploying the NTA Flow Storage Database on a different computer.

Note: If you are installing NTA 4.0 on a 32-bit operating system, the NTA installer detects it and automatically skips this screen.

5. Review the Welcome information and click **Next**.
6. Accept the terms of the license agreement, and then click **Next**.
7. Click **Install**.
8. When the installation completes, click **Finish** to exit the wizard.

Completing the Configuration Wizard

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

To configure your NTA and NTA Flow Storage Database:

1. Review the Configuration Wizard welcome text, and then click **Next**.

   Note: ***If the Configuration Wizard has not started automatically***, start Configuration Wizard in the SolarWinds Orion program folder (SolarWinds Orion > Configuration and Auto-Discovery > Configuration Wizard).

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

   Note: NTA requires the SolarWinds NetFlow Traffic Analyzer Service.

3. ***If you are installing NTA 4.0 on a 64-bit operating system together with the local NTA Flow Storage Database***, define the database location and click **Next**.

   - Fill in an absolute path to the location for storing your flow data into the **NTA Flow Storage Database data file path** field or click **Browse** to navigate to the appropriate location.
   - Define the location for storing database backups:
     Fill in an absolute path to the location for storing your backups into the **Backup NTA Flow Storage Database data file path** or click **Browse** to navigate to the appropriate location.

     Notes:

     - Make sure you save your flow data on a dedicated disk.
     - The folder for NTA Flow Storage Database must be empty or contain the appropriate NTA Flow Storage Database version.
     - The folder path must be a valid uri, and NTA must be able to create a folder there.
     - Make sure your NTA Flow Storage Database and its backups are stored in different folders.
     - Specifying the folder for storing backups is not obligatory now, you can define it later.

   If you have installed NTA Flow Storage Database on a different server, review the information about the NTA Flow Storage Database location and click **Next**.

   If you are installing NTA 4.0 on a 32-bit operating system, this step is skipped.

4. Review the configuration summary, and then click **Next**.
5. Click **Finish** when the Configuration Wizard completes.

Installing NTA Flow Storage Database

Storing your flow data on a server which is different from your NTA and NPM server allows you to fully benefit from the high performance ensured by the NTA Flow Storage Database.

Notes:

- Make sure the NTA Flow Storage Database server complies with the appropriate minimum requirements.
- Make sure the appropriate NPM version is already installed on the NPM/NTA Server. To install NTA Flow Storage Database, you will need the appropriate hostname or IP address of the Orion SQL Database server, the appropriate Orion Database name and credentials.

To install NTA Flow Storage Database:

1. Log on to the server where you want to store your flow data.
2. Launch the executable in its location (on the physical media or in the folder you have downloaded it to).
3. Review the Setup Wizard welcome screen and click **Next**.
4. Select **I would like to install the NTA Flow Storage Database on this server**.
5. NTA needs access to information about nodes and interfaces which is stored in the NPM Orion database. Enter the details for accessing the Orion SQL Database into the blue box:
    a. **Orion Database Server** - type a valid hostname or an IP address of the server where the Orion SQL Database is installed.
    b. **Orion Database Username** and **Password** - enter the SQL database credentials.

    Note: The default Orion Database Username is **SolarWindsOrionDatabaseUser**. You have specified the password with the Configuration Wizard while installing NPM.

c. Select the appropriate database name and click **Test Connection**.
d. After verifying the connection, click **Next** to continue.

Troubleshooting the connection to the Orion SQL Database
If the connection attempt failed, make sure that:

- The username and password are correct and valid.
- You can access the database server.
- No firewall is blocking the connection.
- NPM version is 10.6 or newer.
- When configuring NPM, you have selected Windows Authentication.
- The remote connection option is enabled on the SQL Database.

6. Review the Setup Wizard welcome text, and then click **Next**.
7. Accept the terms of the license agreement, and then click **Next**.
8. Specify the folder for installing NTA Flow Storage Database and click **Next**.
9. Click **Install** to launch the installation.
10. Click **Finish** to close the Setup Wizard.
11. Configure the NTA Flow Storage Database. For more details, see Configuring NTA Flow Storage Database.

Configuring Remote NTA Flow Storage Database

Configuring Remote NTA Flow Storage Database consists of specifying the location for storing your flow data (NTA Flow Storage Database data file path) and the location for your NTA Flow Storage Database backups.

Notes:

- Make sure you save your flow data on a dedicated disk.
- The folder for NTA Flow Storage Database must be empty or contain the appropriate NTA Flow Storage Database version.
- The folder path must be a valid uri, and NTA must be able to create a folder there.

- Make sure your NTA Flow Storage Database and its backups are stored in different folders.
- Specifying the folder for storing backups is not obligatory now, you can define it later.

To specify NTA Flow Storage Database destination:

1. ***If the NTA Flow Storage Configurator does not launch automatically***, start it in the SolarWinds Orion program folder (NetFlow Traffic Analyzer > NTA Flow Storage Configurator).
2. Enter the folder for storing flow data into the **NTA Flow Storage Database data file path** field:
   - Click **Browse** and navigate to the appropriate location; or
   - Fill in an absolute path.
3. If you want to specify the location for storing NTA Flow Storage Database backups now, fill in the folder path for storing backups into the **Backup NTA Flow Storage Database data file path** field.
4. Click **OK**.

Upgrading NTA

You can upgrade NTA from a previous version or upgrade the licensed number of elements you can monitor.

For more information about NTA compatibility and upgrade paths, see the knowledge base article "Compatibility of SolarWinds Orion Products for Installation and Upgrade".

Upgrade Paths and Compatibility

NTA versions are compatible with specific versions of SolarWinds NPM.

To upgrade your NTA to the latest version, use the following upgrade path:

NTA 3.7 ⇒ NTA 3.9 ⇒ NTA 3.11 ⇒ NTA 4.x

NTA-NPM Compatibility Table

	NPM 10.1/ Core 2010.-2	NPM 10.1.1/ Core 2010.2-.1	NPM 10.1.-2/ Core 2011.-1	NPM 10.1.3/ Core 2011.1-.1	NPM 10.2.x/ Core 2011.2-.x	NPM 10.3.x/ Core 2012.1-.x	NPM 10.4.2/ Core 2012.2-.x	NPM 10.5.x/ Core 2013.1-.x	NPM 10.6.x/ Core 2013.2-.x	NPM 10.7.x/ Core 2014.1-.x
NTA 3.7	✓	✓	✓	✓	✓	✓				
NTA 3.8	✓	✓	✓	✓	✓	✓	✓			
NTA 3.9					✓	✓	✓	✓	✓	
NTA 3.10						✓	✓	✓	✓	✓
NTA 3.11							✓	✓	✓	✓
NTA 4.0.x									✓	✓

Notes:

- If a primary poller is running on a 64-bit operating system, all pollers must be 64-bit, too.
- NTA 4.0.x is the last version supporting 32-bit operating systems.
- You cannot upgrade NTA to use a different locale. NTA uses locale settings of the underlying NPM installation. If you want to change the locale settings, you must install NPM using the appropriate locale, and then install NTA.
- 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.

Upgrade Steps

Upgrade steps can differ slightly, according to your current NTA deployment. For more information, see NTA 4.0 Deployment Options.

NTA 4.0 on 64-bit operating systems started storing flows in a new NTA Flow Storage Database.

For more information about frequently asked questions about the new database, see SolarWinds knowledge base article "NTA 4.0 Installation: FAQ".

To upgrade your NTA:

1. Back up your database. For more information about creating database backups, see:

   - Configuring NTA Flow Storage Database Backups if you have been storing flows in the NTA Flow Storage database.
   - "Using SQL Server Management Studio" in the *Orion Network Performance Monitor Administrator Guide* if you have been storing flows in a MS SQL Database.

2. ***If you are using more than one polling engine to collect network information***, shut down all polling engines before continuing.

3. **Upgrade your NTA Flow Storage Database:**

   If you have not been storing flows in NTA Flow Storage Database, skip this step and continue with upgrading your primary poller.

   a. Log in to the NTA Flow Storage Database server and launch the executable.
   b. Install and configure NTA Flow Storage Database. For more information, see Installing NTA Flow Storage Database and Configuring Remote NTA Flow Storage Database.

4. **Upgrade your primary poller:**

   a. Using the local administrator account, log on to your primary poller server.
   b. Launch the executable.
   c. Orion automatically detects the previous installation. When prompted to upgrade the current installation, click **Yes**.

      Note: All customizations, including web console settings, are preserved.

      Re-Indexing of Database Tables

      If you are upgrading from NTA 3.11 to NTA 4.0.2 on a 32-bit operating system using the Orion SQL database, 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, 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 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 10 GB of data in the tables.

d. Confirm your installation type on the Welcome window, and then click **Next**.
e. Accept the terms of the license agreement, and then click **Next**.
f. Confirm the current installation settings, and then click **Next** on the Start Copying Files window.
g. Provide the 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 NTA License.

h. Click **Continue**, and then click **Continue** again when the license is installed.
i. Review the Upgrade Reminder, and then click **Next**.
j. Click **Finish** on the InstallShield Wizard Complete window.
k. Complete the Configuration Wizard and if appropriate, migrate the original database. For more information, see Database Migration.

5. If you are using additional polling engines, log on to the appropriate servers, and upgrade NTA there.
6. If you are using additional websites, log on to the appropriate servers, and upgrade NTA there.

Upgrade Instructions on SolarWinds Customer Portal

Specific instructions for completing an upgrade are also available in the SolarWinds Customer Portal.

To access them, complete the following steps:

- 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.

Database Migration

If you are upgrading to NTA 4.0 and NTA Flow Storage Database, you have the option to migrate your flow data from the SQL database to the new NTA Flow Storage Database.

Note: For upgrading to NTA 4.0 on a 32-bit operating systems, the migration screens are skipped.

The database migration is started within the Configuration Wizard when you are upgrading your NTA.

Migration runs as a background process; however, it might be time-and performance extensive. The speed of your work with NTA might be affected.

Note: You can check the migration progress in the Orion Web Console notification bar at any time.

Free Space Requirement

For migrating your flows data from the SQL Database into the new NTA Flow Storage Database, you will need approximately twice the space occupied by flows data in the SQL Database. The Configuration Wizard will inform you about the precise space requirements.

To perform migration, complete the following steps:

1. ***If the Configuration Wizard has not started automatically after you have installed an NTA update***, start it in the SolarWinds Orion program folder.
2. Select the appropriate migration option:
    - **Migrate historical data from previous installation**.
      Select this option if you want to see historical data in your NTA 4.0.

- **Do not migrate my historical data**.
  Select this option if you do not need to see historical flows data in NTA 4.0, and decide what should happen to your historical flows:
  - Select **Keep flows data in the Orion SQL database** to keep the historical flows in your Orion SQL Database. You can migrate them later, by re-launching the Configuration Wizard and selecting the migration option.
  - Select **Delete flows data from the Orion SQL database** to permanently delete historical flows data in the Orion SQL Database.

3. Make sure you have backed up your database. If you do not back up your database, you might lose your historical data.
   a. Type **YES** in capital letters to confirm that you have backed up your database
   b. Click **Next** to continue.

4. Not Enough Free Space to Migrate

   This screen appears if you want to migrate historical flows, and NTA detects that on NTA Flow Storage Database disk, there is not enough free space for the migration. Select what you want to do:

   - Arrange for more free space on your NTA Flow Storage Database disk. Click **Cancel**, and re-configure NTA to use a larger disk for the NTA Flow Storage Database or free up space on the selected drive.
   - Select the **Start the partial migration** box to start the migration despite the consequences and click **Next**.

     Warning:
     - You will lose your oldest flow data.
     - Your NTA might display only historical data, because the migrated data take up too much space and no more new flows can be stored in the NTA Flow Storage Database.

5. Review the configuration overview and click **Next** to start the migration.
6. Click **Finish**.

Moving the NTA Flow Storage Database

You can have your NTA Flow Storage Database stored locally on a separate disk drive, or on a remote computer. To change the location, use the appropriate workflow:

- Moving remote NTA Flow Storage Database to a local disk
- Moving local NTA Flow Storage Database to a remote disk
- Moving NTA Flow Storage Database to a different disk drive on the same server

Note: Before you start moving your NTA Flow Storage Database, please make sure you back up the database. Otherwise, you will not be able to see your historical data.

To move your NTA Flow Storage Database from a remote server to a local disk:

1. Log on to the server where your NTA Flow Storage Database is currently installed.
2. Stop the SolarWinds NetFlow Storage Service.
3. Locate the NTA Flow Storage Database destination folder.
   How can I find the NTA Flow Storage Database Destination folder?
4. Move the NTA Flow Storage Database folder with its contents to the local server using standard Windows tools (Copy&Paste, shared folder, or FTP).
5. Change the NTA installation on your main polling engine:
   a. Log in to the server where you have your NTA installed.
   b. Run the NTA 4.0 executable.
   c. Click **Next** on the Welcome to the Setup Wizard Screen.
   d. Select the configuration option **NPM/NTA/NTA Flow Storage Database on the same server** and click **Next**.
   e. Review the Welcome information and click **Next**.
   f. Accept the terms of the license agreement, and then click **Next**.
   g. Click **Change**, and complete the Setup Wizard.
   h. Reconfigure your NTA. For more information, see Completing the Configuration Wizard.

i. When prompted to specify the location for storing flow data, fill in the folder where you moved your NTA Flow Storage Database in step 4.

6. Optional: Uninstall the NTA Flow Storage Database from your remote server.

To move your NTA Flow Storage Database from a local disk to a remote server:

1. Log on to the server where your NTA is currently installed.
2. Stop the SolarWinds NetFlow Service.
3. Locate your NTA Flow Storage Database folder.
   How can I find my NTA Flow Storage Database destination folder?
4. Move the NTA Flow Storage Database folder with its contents to the target server using standard Windows tools (Copy&Paste, shared folder, or FTP).
5. Install the NTA Flow Storage Database on the appropriate server. For more information, see Installing NTA Flow Storage Database.
6. Change the NTA installation on your main polling engine:
   a. Log in to the server where you have your NTA installed.
   b. Run the NTA 4.0 executable.
   c. Click **Next** on the Welcome to the Setup Wizard Screen.
   d. Select the configuration option **NPM/NTA/NTA Flow Storage Database on two separate servers** and click **Next**.
   e. Fill in the hostname or IP address of the new NTA Flow Storage Database location and click **Test Connection.**
   f. Review the Welcome information and click **Next**.
   g. Accept the terms of the license agreement, and then click **Next**.
   h. Review the Previous version detected screen and click **Next**.
   i. Click **Change**, and complete the Setup Wizard.
   j. Select the appropriate licensing option.
   k. Reconfigure your NTA. For more information, see Completing the Configuration Wizard.

To move NTA Flow Storage Database to another disk drive within the same server:

1. Stop the SolarWinds NetFlow Service or the SolarWinds NetFlow Storage Service, as appropriate.
2. Launch the command prompt.
3. Locate **SolarWinds.NetFlow.FastBit.DbMove.exe** in the folder where you have installed your NTA Flow Storage Database, such as C:\Program Files (x86)\SolarWinds\Orion\NetFlowTrafficAnalysis.
4. Drag&Drop the **SolarWinds.NetFlow.FastBit.DbMove.exe** file into the command prompt.
5. Define the source and destination folder using the following command:

   ```
   NetFlow.Fastbit.DbMove.exe [source folder]
   [destination folder]
   ```

   Example

   ```
   NetFlow.Fastbit.DbMove.exe D:\OriginalLocation\
   D:\NewLocation\
   ```

   Note: If the path contains folders with blanks in their names, consider renaming the folders or put the path in quotes, such as:

   ```
   Netflow.FastBit.DbMove.exe "D:\Original DB Location
   1\" "D:\New DB Location 2\"
   ```

6. Start the **NTA Flow Storage Configurator** in the SolarWinds Orion > NetFlow Traffic Analysis program folder and fill in the new destination folder for storing your flows data.

To find the current location of your NTA Flow Storage Database:

1. Start the **NTA Flow Storage Configurator** in the SolarWinds Orion > NetFlow Traffic Analysis program folder.
2. The path to the current NTA Flow Storage Database destination folder is available in the appropriate field (**NTA Flow Storage Database data file path**).
3. Click **Cancel** to close the Configurator.

Uninstalling NTA

If you need to uninstall NTA, complete the standard unistallation procedure appropriate for your operating system.

To uninstall NTA on Windows:

1. Launch the **Programs and Features** or **Add or Remove Programs** feature in your Control Panel.

   Note: Accessing the Control Panel might be different on different operating systems. For more details, consult your operating system help.

2. Select **SolarWinds Orion NetFlow Traffic Analyzer** and click **Uninstall** or **Remove**.
3. Complete the Installer Wizard.

Note: You need to uninstall NTA on all poller servers, and on the NTA Flow Storage Database server, too.

Chapter 3: Configuring SolarWinds 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 NTA as NetFlow sources are separate procedures, detailed in separate sections.

Note: If you already have flow-enabled devices on your network, NTA can automatically add them as NetFlow sources if you configure your flow-enabled devices to send their flows to your designated NTA server. For more information, see Device Configuration Examples on page 262.

For NTA to correctly receive and process NetFlow data, you must complete the following tasks:

- Setup your network devices to export flow data.

  For more information about setting up and verifying export of data from your network devices, see Setting up Network Devices to Export Flow Data.

- Add your network devices to NPM as described in Adding Flow-Enabled Devices and Interfaces.
- Define what devices should be monitored by NTA. For more information, see Configuring Flow Sources and CBQoS Devices.

Configuring NetFlow Management Settings

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

- Enabling the Automatic Addition of Flow Sources
- Configuring Data Retention for Flows on Unmonitored Ports
- Enabling Flow Monitoring from Unmanaged Interfaces

- Enabling Flow Monitoring from Unmanageable Interfaces
- Configuring Monitored Ports and Applications
- Selecting IP Address Groups for Monitoring
- Configuring Protocol Monitoring
- Managing Flow Sources and CBQoS-enabled Devices
- Configuring NetFlow Collector Services Ports
- Configuring NetFlow Types of Services

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

For an explanation of individual settings as they are on the NTA Settings view, see NetFlow Traffic Analysis Settings.

Adding Flow-Enabled Devices and Interfaces

For NTA to collect flow data from your network devices you must first specify the NTA server as a target to which each device exports its data. For more information about setting up network devices to export data to NTA, see Setting up Network Devices to Export Flow Data.

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

For 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 NPM. Adding flow-enabled devices and interfaces to NPM and designating the same devices and interfaces as flow sources in NTA are separate actions, and the designation of flow sources does not affect licensing requirements for either NPM or NTA.

Flow-enabled devices must be added to the Orion database using either Network Sonar or Web Node Management in NPM before NTA can initiate flow monitoring. For more information about designating flow sources in NTA, see Adding Flow Sources and CBQoS-enabled Devices.

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

To add your devices and flow-enabled interfaces to NPM:

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

   Note: The current version of NTA requires NPM 10.6 or later.

2. ***If you are adding a large number of nodes***, use Network Sonar Discovery. 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 NPM can be added as NetFlow sources.

   For more information, see Adding Flow Sources and CBQoS-enabled Devices.

After installing NTA, the NPM polling engine establishes a baseline by collecting network status and statistics immediately. Then, 30 seconds later, the NPM polling engine performs another collection. You may notice an increase in your CPU usage during this time. After these initial collections, 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 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.

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 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, consult the following sections:

- Enabling the Automatic Addition of Flow Sources
- Enabling Flow Monitoring from Unmanaged Interfaces
- Enabling CBQoS Polling
- Adding Flow Sources and CBQoS-Enabled Devices for Monitoring in NTA Manually
- Deleting Flow Sources and CBQoS-Enabled Devices for Monitoring in NTA Manually

Enabling the Automatic Addition of Flow Sources

NTA can detect and automatically add flow sources that are monitored by NPM.

To enable the automatic addition of flow sources:

1. Go to the **NetFlow Settings** page:
    a. Start the **Orion Web Console** in the SolarWinds program folder.
    b. Log in using a **User ID** with administrative privileges.
    c. Click **NETFLOW** on the tool bar, and then click **NetFlow Settings** in the top right corner of the NETFLOW view.

    Note: You can also click **Settings** in the top right corner of the Orion Web Console, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
2. Select the **Enable automatic addition of NetFlow sources** box.
3. Click **SAVE**.

Enabling Flow Monitoring from Unmanaged Interfaces

In older versions, NTA discarded any flow record that referred to traffic involving an interface not already managed by NPM. Currently, however, NTA provides the option to retain data for any flow defined with at least one interface monitored by NPM.

It is possible that you may be managing a node in 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 NTA attempt to associate unknown traffic with a non-primary IP address on a currently monitored NPM node.

For more information about managing interfaces in NPM, see Discovering and Adding Network Devices in the *Orion Network Performance Monitor Administrator Guide*. The following procedure enables the option of monitoring traffic on unmanaged interfaces in NTA.

Note: Disabling the option to monitor flows from unmanaged interfaces may significantly decrease the processing load on both your 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. Go to the **NetFlow Settings** page:

    a. Start the **Orion Web Console** in the SolarWinds program folder.

    b. Log in using a **User ID** with administrative privileges.

    c. Click **NETFLOW** on the tool bar, and then click **NetFlow Settings** in the top right corner of the NETFLOW view.

    Note: You can also click **Settings** in the top right corner of the Orion Web Console, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.

2. Select the **Allow monitoring of flows from unmanaged interfaces** box.
3. Select the **Allow matching nodes by another IP Address** box to allow NTA to attempt associating unknown traffic with non-primary IP addresses on a currently monitored NPM node.
4. Click **Save**.

    Note: If there are unknown traffic events, resolve the unknown traffic and add the appropriate devices for monitoring first to NPM, and then to NTA. For more details, see Resolving unknown traffic.

CBQoS Polling Settings

You can enable and disable specific NetFlow Sources in the **Manage NetFlow Sources** resource. However, to be able to poll CBQoS data, you must first enable CBQoS here, in CBQoS Settings.

For more details about Managing NetFlow Sources, see

To enable CBQoS for your NetFlow sources:

1. Go to the **NetFlow Settings** page:
    a. Start the **Orion Web Console** in the SolarWinds program folder.
    b. Log in using a **User ID** with administrative privileges.
    c. Click **NETFLOW** on the tool bar, and then click **NetFlow Settings** in the top right corner of the NETFLOW view.

    Note: You can also click **Settings** in the top right corner of the Orion Web Console, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
2. Scroll down to the **CBQoS Polling** grouping
3. Select the **Enable CBQoS Polling** checkbox.
4. Set the polling interval.
5. Click **Save**.

Adding Flow Sources and CBQoS-Enabled Devices

In NTA, you can either add flow-enabled devices managed by NPM for monitoring in NTA manually, or you can configure that flow-enabled devices are added automatically.

For more information about the automatic addition of flow sources, see Enabling Automatic Adding of Flow Sources.

Notes

- Make sure the devices you want to monitor with NTA are already monitored in NPM.
- If you are using NetFlow version 9, confirm that the template you are using includes all fields included in NetFlow version 5 PDUs.

- Some devices have a default template time-out rate of 30 minutes.If NetFlow v9 flows arrive without a usable template, NTA raises an event every 15 minutes. Therefore, 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 NTA Flow Requirements.
- 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 for monitoring in NTA manually:

1. Open the **Orion Web Console** in the SolarWinds program group.
2. Log in using a **User ID** with administrative privileges.
3. Click **NETFLOW** on the tool bar.
4. Go to the NetFlow Sources resource and click **MANAGE SOURCES**.

   If automatic addition of NetFlow sources is enabled, all flow sources currently monitored by NPM will display in the NetFlow Sources resource. For more information about the automatic addition of flow sources, see the section Enabling Automatic Adding of Flow Sources.

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

5. Click **Settings** in the top right corner of the Web Console.
6. Click **NTA Settings** in the Settings grouping of the Orion Web Console Administration page.
7. Click **NetFlow Sources**.
8. Select the appropriate filter in the **Show** list to display devices where you want to monitor NetFlow or CBQoS data.
   - **Exporters only (last 15 minutes)** - shows all devices in your Orion database that have sent flow data within the last 15 minutes
   - **Cisco devices only** - displays all Cisco devices monitored by NPM.
   - **All** - displays all devices monitored by NPM.
9. Select the appropriate box (**NetFlow** or **CBQoS**) to define what should be monitored for the appropriate device or interface:

- To monitor NetFlow or CBQoS on a device, select the appropriate box for the device.
- To monitor NetFlow on CBQoS all found devices, select the box in the appropriate column header.

  Note: CBQoS monitoring is only available for Cisco devices.
- To monitor NetFlow or CBQoS on all interfaces of a device, select the appropriate box for the device.
- To monitor NetFlow or CBQoS on individual interfaces, click **+** next to the appropriate device, navigate to the interface and select the appropriate box (NetFlow or CBQoS) next to it.

10. Click **SUBMIT** to apply your changes.

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. Go to the **NetFlow Settings** page:
   a. Start the **Orion Web Console** in the SolarWinds program folder.
   b. Log in using a **User ID** with administrative privileges.
   c. Click **NETFLOW** on the tool bar, and then click **NetFlow Settings** in the top right corner of the NETFLOW view.

      Note: You can also click **Settings** in the top right corner of the Orion Web Console, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
2. Click **NetFlow Sources**.
3. Select the type of device to delete from the **Show** menu.
4. Expand the node tree to locate the source you want to delete, and then expand the source you want to delete.
5. 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.

  Note: If you disable NetFlow monitoring for a node or interface, the data stop being collected. However, historical data are kept in the database. Enabling and disabling flow collection can thus result in gaps in NTA graphs.

6. ***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**.

Configuring Monitored Ports and Applications

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.

To change the applications or service ports currently monitored by your NTA:

1. Go to the **Manage Applications and Service Ports** page:
   i. Go to the **NetFlow Settings** page:
      a. Start the **Orion Web Console** in the SolarWinds program folder.
      b. Log in using a **User ID** with administrative privileges.

c. Click **NETFLOW** on the tool bar, and then click **NetFlow Settings** in the top right corner of the NETFLOW view.

Note: You can also click **Settings** in the top right corner of the Orion Web Console, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.

ii. Click **Application and Service Ports**.

2. Make your changes:
   - Enable/Disable monitoring for existing applications/service ports
   - Add new applications/service ports for monitoring
   - Edit existing applications/service ports
   - Delete existing applications/service ports
3. Submit the changes you have made.

Submitting Changes

To apply your changes in the database so that they are reflected in the Orion Web Console, you need to submit them:

a. Click **Submit** to apply your application, port or IP address group updates to the database.

Notes

- Clicking **Submit** launches an update action which might take a while. When an update action is running, the **Submit** button is hidden and you cannot submit any more changes until the first update is finished.
- If you do not submit your changes, a notification about unsubmitted changes displays in red on the top of the page.

b. Confirm the dialog which asks you whether you want to submit your changes.

Note: If you plan to make more changes, we recommend that you click **Cancel** in this dialog, make all appropriate changes and re-submit your changes once you have made all of them.

Configuring Data Retention for Flows on Unmonitored Ports

By default for new installations, 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 NTA, see Enabling Flow Monitoring from Unmanageable Interfaces.

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

To configure data retention for flows on unmonitored ports:

1. Go to the **NetFlow Settings** page:
    a. Start the **Orion Web Console** in the SolarWinds program folder.
    b. Log in using a **User ID** with administrative privileges.
    c. Click **NETFLOW** on the tool bar, and then click **NetFlow Settings** in the top right corner of the NETFLOW view.

    Note: You can also click **Settings** in the top right corner of the Orion Web Console, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
2. Select the **Enable data retention for traffic on unmonitored ports** box.
3. Click **SAVE** to apply your changes.

Enabling/Disabling Monitoring for Ports or Applications

You can decide what ports or applications should be monitored by NTA.

To enable monitoring for a port/application:

1. Go to the Manage Applications and Service Ports page.
2. Locate the application/port you want to monitor and click **Enable** in the **Actions** column.
3. Make further changes or **Submit** your change(s).

To disable monitoring for a port/application:

1. Go to the Manage Applications and Service Ports page.
2. Locate the application/port you want to stop monitoring and click **Disable** in the **Actions** column.
3. Make further changes or **Submit** your change(s).

   If you want to manage all listed ports and applications at once, go to the Manage Applications and Service Ports page and complete the following procedure:

   - If you want to monitor all listed ports and applications, click **Enable All Monitoring** above the application list.
   - If you want to disable monitoring for all listed ports and applications, click **Disable All Monitoring** above the applications and ports list.
   - If you are not sure what ports and applications to monitor, click **Monitor Recommended Ports** to monitor the most typical, high traffic ports.

     Warnings:

     - 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 database and the Orion Web Console. If you are not initially sure what ports and applications you should monitor with 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 all existing custom application and port definitions.
   - Make further changes or **Submit** your change(s).

Adding Ports or Applications

If you do not see a port or application you want to monitor, go to the Manage Applications and Service Ports page and complete the following steps.

To add a new application:

1. Click **Add Application**.
2. Provide a **Description** of the application you want to monitor.
3. 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.

4. 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 NTA, see Selecting IP Address Groups for Monitoring on page 60.

5. Select the appropriate **Protocol** for the new application, and then click **Add Application**.
6. Make further changes or **Submit** your change(s).

Editing Ports or Applications

If you want to edit the properties of a monitored port or application, complete the following steps:

1. Go to the Manage Applications and Service Ports page..
2. Find the application or service port you want to manage:
   a. 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.

   b. 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 number.

3. Click **Edit** in the **Actions** column of the selected port or application.
4. 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
5. If you only want to monitor application traffic to or from a selected Destination or Source IP Address(es), select the appropriate IP address groups.

   For more information about IP address groups in NTA, see Selecting IP Address Groups for Monitoring.
6. Select the appropriate **Protocol** for the selected application.
7. Click **Update Application**.
8. Make further changes or **Submit** your change(s).

Deleting Ports or Applications

If you want to delete a single listed port or application:

1. Go to the Manage Applications and Service Ports page.
2. Click **Delete** in the **Actions** field of the selected application.
3. Click **Delete Application** in the Delete Application dialog.
4. Make further changes or **Submit** your change(s).

Selecting IP Address Groups for Monitoring

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 change the IP address groups currently monitored by your NTA:

1. Go to the **Edit IP Address Groups** page:
    i. Go to the **NetFlow Settings** page:
        a. Start the **Orion Web Console** in the SolarWinds program folder.
        b. Log in using a **User ID** with administrative privileges.
        c. Click **NETFLOW** on the tool bar, and then click **NetFlow Settings** in the top right corner of the NETFLOW view.

        Note: You can also click **Settings** in the top right corner of the Orion Web Console, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
    ii. Click either **IP Address Groups** or **Manage IP Address Groups**.
2. Make your changes:
    - Select IP ranges to be monitored
    - Add new IP Address Groups
    - Edit existing IP Address Groups
    - Delete IP Address Groups
3. Submit the changes you have made. For more information, see Submitting Changes.

Selecting IP Ranges to Be Monitored

1. Go to the Edit IP Address Groups page.
2. ***If any one of the listed, pre-existing ranges contains the addresses you want NTA to monitor***, make sure that the corresponding box in the **Enable** column is selected.
3. Make further changes or **Submit** your change(s).

Adding a New IP Address or IP Address Group

If you want to add a new group, go to the Edit IP Address Groups page and complete the following steps:

1. Click **Add New Group**.
2. Provide a **Description**.
3. ***If you want to define the selected group as a single IP address***, select **IP Address**, and then provide the IP address.
4. ***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.
5. ***If you want to include this defined group, if eligible, in Top XX IP Address Groups resources in the Orion Web Console,*** select the **Enable display in Top XX IP Address Groups resource** box.
6. ***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 ✕ to delete any groups you do not want to maintain.
7. Click **OK** when you have completed your group edits and additions.
8. Make further changes or **Submit** your change(s).

Editing IP Addresses or IP Address Groups

If you want to edit an existing group, go to the Edit IP Address Groups page and complete the following steps:

1. Click **Edit** next to the IP address group which you want to edit.
2. Edit the **Description**, as necessary.
3. ***If you want to define the selected group as a single IP address***, select **IP Address**, and then provide the IP address.
4. ***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.
5. ***If you want to include this defined group, if eligible, in Top XX IP Address Groups resources in the Orion Web Console,*** select the **Enable display in Top XX IP Address Groups resource** box.

6. ***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  to delete any groups you do not want to maintain.

7. Click **OK** when you have completed your group edits and additions.
8. Make further changes or **Submit** your change(s).

Deleting IP Address or IP Address Groups

If you want to delete an existing group:

1. Go to the Edit IP Address Groups page.
2. Click **Delete** at the end of the appropriate IP address group row.
3. Make further changes or **Submit** your change(s).

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 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, 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 NTA Flow Requirements.

To configure NetFlow collector services:

1. Go to the **NetFlow Settings** page:

   a. Start the **Orion Web Console** in the SolarWinds program folder.

   b. Log in using a **User ID** with administrative privileges.

   c. Click **NETFLOW** on the tool bar, and then click **NetFlow Settings** in the top right corner of the NETFLOW view.

Note: You can also click **Settings** in the top right corner of the Orion Web Console, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.

2. Click **NetFlow Collector Services**.
3. ***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.
4. ***If you want to delete a collector,*** click **Delete**.

   Note: If there is the NetFlow service running on the appropriate collector server, the collector together with the default port 2055 will be automatically re-added in 15 minutes. For more information, see Deleting Collectors.
5. Click **Submit** when you finish configuring your NetFlow collectors.

Configuring Protocol Monitoring

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

To specify protocols monitored by NetFlow Traffic Analyzer:

1. Go to the **NetFlow Settings** page:
   a. Start the **Orion Web Console** in the SolarWinds program folder.
   b. Log in using a **User ID** with administrative privileges.
   c. Click **NETFLOW** on the tool bar, and then click **NetFlow Settings** in the top right corner of the NETFLOW view.

Note: You can also click **Settings** in the top right corner of the Orion Web Console, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.

2. Click **Monitored Protocols**.
3. 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.
4. Click **Submit** at the bottom of the Monitored Transport Protocols view.

Configuring NetFlow Types of Services

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 NTA, as shown in the following procedure.

To configure types of services for NetFlow packets:

1. Go to the **NetFlow Settings** page:
    a. Start the **Orion Web Console** in the SolarWinds program folder.
    b. Log in using a **User ID** with administrative privileges.
    c. Click **NETFLOW** on the tool bar, and then click **NetFlow Settings** in the top right corner of the NETFLOW view.

Note: You can also click **Settings** in the top right corner of the Orion Web Console, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.

2. Click **Types of Services**.
3. ***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 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. Top Talker Optimization allows you to configure 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.

By default, on new installations, NTA is configured to capture flows representing the top 95% of total network traffic.

Most users upgrading from previous NTA versions should see an improvement in performance after configuring Top Talker Optimization to capture only those flows representing the top 95% of all network traffic. If you are monitoring a large number of NetFlow 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 if this option is set to 100%. However, the data that is lost corresponds to the least bandwidth-intensive conversations. In most environments, these low bandwidth conversations would not have been displayed in most resources anyway.

To enable the Top Talker Optimization

1. Go to the **NetFlow Settings** page:
    a. Start the **Orion Web Console** in the SolarWinds program folder.
    b. Log in using a **User ID** with administrative privileges.
    c. Click **NETFLOW** on the tool bar, and then click **NetFlow Settings** in the top right corner of the NETFLOW view.

    Note: You can also click **Settings** in the top right corner of the Orion Web Console, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
2. Scroll down to the **Top Talker Optimization** settings grouping.
3. Provide an appropriate percentage in the **Capture flows representing the top XX % of total network traffic** field.
4. Click **Save** in the Top Talker Optimization section.

Configuring DNS and NetBIOS Resolution

To meet varied network requirements, 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
- DNS Resolution Options in NTA
- How Does Default Resolution Work in NTA
- Configuring DNS Resolution

Enabling NetBIOS Resolution

For networks where NetBIOS is the naming convention of preferred use, NTA provides the option to resolve endpoint domain names using NetBIOS.

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.

To enable NetBIOS resolution:

1. Go to the **NetFlow Settings** page:

    a. Start the **Orion Web Console** in the SolarWinds program folder.

    b. Log in using a **User ID** with administrative privileges.

    c. Click **NETFLOW** on the tool bar, and then click **NetFlow Settings** in the top right corner of the NETFLOW view.

    Note: You can also click **Settings** in the top right corner of the Orion Web Console, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.

2. Under the **DNS and NetBIOS Resolution** heading, select the **Enable NetBIOS resolution of endpoints** option.
3. Click **Save** in the DNS and NetBIOS Resolution section.

DNS Resolution Options in NTA

To meet your specific network monitoring needs, 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, 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 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.

- **Disabled** - this option turns DNS resolution off for the endpoints of flows monitored in NTA. This is not generally recommended unless NetBIOS resolution already is enabled. For more information about enabling NetBIOS resolution, see Enabling NetBIOS Resolution.

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

How Does Default DNS Resolution Work in NTA?

In NTA 4.0 on 32-bit operating systems, NTA receives flows from an IP address, and then asks the DNS server to resolve the hostname/domain. Resolved hostnames stay in the database for 7 days.

In NTA 4.0 on 64-bit OS, host or domain names are stored directly in individual flows. NTA receives a flow from an IP address and waits for the DNS server to resolve it:

- **Until the DNS server responds**, flows are stored under the IP address.
- **When the DNS server resolves the hostname**, NTA uses this hostname/domain for flows from this IP address for the next 7 days. Then the query is repeated.
- **When NTA cannot reach the DNS server**, it retries the query again in 1 minute, and keeps repeating the query, until the DNS server responds.
- **If the DNS server cannot find out the host/domain name**, for example if the administrator had not specified it, NTA adds the IP address to the list of unresolved IPs. Flows from this IP address are stored in the database under the appropriate IP address. NTA repeats the query to the DNS server to resolve the hostname in two days.

NTA also allows you to configure the interval between DNS lookups. NTA performs regular DNS lookups on all monitored devices. By default, if the domain of a monitored device resolves successfully, 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.

Configuring DNS Resolution

By default for new installations, 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 configure DNS resolution:

1. Go to the **NetFlow Settings** page:
    a. Start the **Orion Web Console** in the SolarWinds program folder.
    b. Log in using a **User ID** with administrative privileges.
    c. Click **NETFLOW** on the tool bar, and then click **NetFlow Settings** in the top right corner of the NETFLOW view.

    Note: You can also click **Settings** in the top right corner of the Orion Web Console, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.

2. Under the **DNS and NetBIOS Resolution** heading, configure the resolution options in the following procedure.
    a. Select the type of **DNS Resolution** you want 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 NTA makes an attempt to resolve domain names for unresolved endpoints in the Orion database if the persistent DNS resolution option is selected.

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

Configuring IP Address Processing

By default for new installations, 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, 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. Go to the **NetFlow Settings** page:
    a. Start the **Orion Web Console** in the SolarWinds program folder.
    b. Log in using a **User ID** with administrative privileges.
    c. Click **NETFLOW** on the tool bar, and then click **NetFlow Settings** in the top right corner of the NETFLOW view.

    Note: You can also click **Settings** in the top right corner of the Orion Web Console, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
2. Scroll down to the **DNS and NetBIOS Resolution** section.
3. ***If you want to edit the processing time period***, select **Custom number of minutes**, and then provide an appropriate number of minutes.
4. ***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**.

    Note: SolarWinds recommends against removing the time limit for processing expired IP addresses as continuously deleting expired IP addresses may negatively affect NTA performance. By default, 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.
5. 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, NTA gives you the ability to properly manage the size of your 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 NPM, see Running Database Maintenance in the *Orion Network Performance Monitor Administrator Guide*.

Your database settings depend on the database in which your NTA 4.0 stores your flow data:

- In NTA 4.0 on 64-bit operating systems, NTA stores flow data in the NTA Flow Storage Database.
- In NTA 4.0 on 32-bit operating systems and in older NTA versions, NTA continues to store your flows data in the Orion SQL Database.

Database setting options:

- Setting up database maintenance (both Orion SQL Database and NTA Flow Storage Database). For more information, see Database Maintenance.
- Setting up how you want to compress or aggregate flow data in your Orion SQL Database. For more information, see Compression and aggregation settings (NTA 4.0 on 32-bit operating systems).
- Setting up when your flows expire and are deleted from the NTA Flow Storage Database (NTA 4.0 on 64-bit operating systems). For more information, see Setting the retention period for the NTA Flow Storage Database.
- Setting up when your flows expire and are deleted from the Orion SQL Database (NTA 4.0 on 32-bit operating systems). For more details, see Limiting Retention Period for Orion SQL Database.
- Setting up NTA Flow Storage Database Backups. For more information, see Configuring NTA Flow Storage Database Backups.

Database Maintenance

Due to the great volume of data that is produced by flow-enabled devices, your database may very quickly become unmanageable unless you schedule regular database maintenance. Database maintenance includes the deletion of expired flows, meaning flows that have stopped providing current data, and the compression of Orion database and log files.

Note: If you are storing your flow data in the Orion database (NTA 4.0 on 32-bit operating systems or older NTA versions), you can set the period for storing uncompressed data and configure data aggregation. NTA Flow Storage Database used for storing flow data in NTA 4.0 on 64-bit operating systems does not use data aggregation.

The following settings are relevant for both NTA Flow Storage Database and Orion SQL Database.

To configure database settings:

1. Go to the **NetFlow Settings** page:
    a. Start the **Orion Web Console** in the SolarWinds program folder.
    b. Log in using a **User ID** with administrative privileges.
    c. Click **NETFLOW** on the tool bar, and then click **NetFlow Settings** in the top right corner of the NETFLOW view.

    Note: You can also click **Settings** in the top right corner of the Orion Web Console, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
2. Confirm that **Enable Database Maintenance** is checked.
3. Provide a time when **database maintenance is executed**.

    Notes:

    - The database maintenance execution time should be well inside an established off-peak network usage window to minimize any potential disruption of required monitoring.
    - This field accepts times designated in either 24-hour (HH:MM) or standard (H:MM AM/PM or HH:MM AM/PM) formats.
4. Set the time period for keeping data in the database. For more information about setting when data expire, see Setting Retention Period for NTA Flow Storage Database or Limiting Retention Period for Orion SQL Database.
5. Select the frequency with which you want to **Delete expired flow data**. For more information about setting up the time period for expired data, see Setting up the Retention Period for Orion SQL Database or Setting up Retention Period for NTA Flow Storage Database.

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

6. Select the frequency with which you want to shrink the SQL database transaction log file. NTA regularly removes old inactive records from the transaction log, thus freeing some disk space used by the Orion SQL database. Select the frequency for shrinking the log in the **Compress database and log files** list.

   Note: SolarWinds recommends that you compress database and log files once every 10 days.

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

Compression And Aggregation Settings in NTA

Flow-enabled devices can send a large amount of data to your Orion server for processing with NTA. As a result, the database may quickly become unmanageable.

In NTA 4.0 on 64-bit operating systems, NTA introduced the NTA Flow Storage Database, a more powerful database that allows storing your flows data with 1-minute granularity without compression.

In NTA 4.0 on 32-bit operating systems and in older NTA versions, NTA continues to store your flows data in the Orion SQL Database. You can improve NTA performance by:

- Setting up what data should be compressed and when the data should be deleted from the Orion SQL Database. For more information, see Limiting the Retention Period for the Orion SQL Database.
- Setting up what data should be aggregated. For more information, see Adjusting Data Aggregation Settings.

How Does Compression in Orion SQL Database Work?

In NTA 4.0 on 32-bit operating systems and in older NTA versions, the data compression works as follows:

1. By default, received flow data are 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 age beyond the uncompressed data retention period, they are 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 are older than the period designated in the **Keep compressed data for** field are then deleted.

Configuring NTA Flow Storage Database Backups

Backups protect you from data loss caused by hardware failure or other circumstances such as viruses, accidental deletion or natural disasters.

Backing up your data also allows you to maintain your database size and at the same time, if necessary, to be able to recover your data from earlier times.

NTA allows you to specify regular backups or execute immediate backups of your database using the **NTA Flow Storage Backup Scheduler**.

Best Practices

Executing backups, mainly in case of large databases, can be a time-consuming and performance-extensive process.

During the backup, you might experience the following issues:

- Your computer resources might be more utilized.
- ***If you make one of the following changes when a backup is running***, they will be applied in the web console only after the backup finishes:

  Changing the status of applications from monitored to unmonitored and the other way round.

  Creating, updating, removing, enabling or disabling your IP groups.

  Enabling or disabling interfaces.

  Notes:

  - After the backup finishes, NTA applies these updates on the data in the database.

- Updates are stored in a separate file which is updated regularly. When restoring the backup, NTA applies the most recent update settings on the backed-up data. Therefore, when you restore a backup, you will get your data in the same status as they were when you closed your Orion Web Console before the restore.

- ***If there is an update operation running when the backup starts***, the backup will start only after the update finishes.

Optimizing Backups

To minimize the cons and make most of the benefits, consider the following recommendations for scheduling your backups:

1. Execute backups at times when the utilization of your network is low (preferably at night).
2. Set high frequency for your backups. Backups are executed incrementally, only the new data are added to the backup. If you therefore set backups for each day, the backup will be executed more smoothly than if you back up your database once a month.

   Notes

   - The first database backup includes all data and is thus more time-consuming than further regular backups.
   - If you migrate your data from a SQL database to the new NTA Flow Storage Database, the first backup after the migration takes longer, too, because the database already contains the migrated data.
3. Do not use the same physical drive for saving your NTA Flow Storage Database and your backups. If you do:
   - NTA Flow Storage Database performance decreases during the backup.
   - If the hard drive fails, you will not be able to restore your database.
4. Do not schedule backups at the same time as maintenance. Both maintenance and backup are performance-extensive processes and running them at the same time might have a negative impact on your NTA.

Scheduling Regular Backups

Regular backups of your NTA Flow Storage Database protect you to from losing your flows data. To find out more information about best practices for setting up your regular backups, see Optimizing Backups.

To schedule regular backups:

1. Go to the NTA Flow Storage Backup Scheduler.
    a. Log in the Orion Web Console.
    b. Go to **Database Settings** by clicking Settings > NTA Settings > Database Settings.
    c. Click **Backup Scheduler**.
2. Select the **Enable NTA Flow Storage Database backup** box.
3. Define the frequency and time of regular backups:
    - Fill in the frequency in days in the **Execute backup every** field.
    - Specify the time for backups with the **Execute backup at** field. Use either the 24-hour (**HH:MM**) or standard (**HH:MM AM** or **HH:MM PM**) format.

      Note: Make sure you fill in the local time of the NTA Flow Storage Database server.
4. Click **SUBMIT**.

Backing up the NTA Flow Storage Database Manually

If you want to execute a backup, you can do it immediately. Manual backups are convenient before you make any changes to your NTA installation, such as upgrading NTA or changing the location of your NTA Flow Storage Database.

Notes:

- During the backup, flows continue to be collected.
- Initial backups are time-consuming, because they include all data in the database.
- ***If you launch an operation (update or backup) when another operation is running***, the second operation will be executed only after the first one finishes:

- If you launch a backup and an update is in progress, the backup will start only after the update finishes.
- If you start an update and a backup is in progress, the update will be applied only after the backup finishes.

To execute the backup:

1. Go to the NTA Flow Storage Backup Database Scheduler:
   a. Log in the Orion Web Console.
   b. Go to **Database Settings** by clicking Settings > NTA Settings > Database Settings.
   c. Click **Backup Scheduler**.
2. Click **Backup Now**.

Specifying Backup Folders For NTA Flow Storage Database

If you want to back up your NTA Flow Storage Database, you need to define a location for saving the backups. You can define either it in the Configuration Wizard immediately after your NTA installation, or at any time later on, using the NTA Flow Storage Configurator tool.

If you want to find out where your backups are currently stored, go to the NTA Flow Storage Backup Scheduler and check the **Backup destination** read-only field.

To define or change the location for saving your backups:

1. Log on to the server hosting your main poller.
2. Start the **NTA Flow Storage Configurator** in the SolarWinds Orion > NetFlow Traffic Analyzer folder.
3. Define the location for saving backups:
   - Type the absolute path to the backup folder into the **Please enter a folder path for saving the NTA Flow Storage Backups** field, or
   - Click **Browse** and select an appropriate folder.

     Note: Make sure that backups are stored in a different folder than the NTA Flow Storage Database.
4. Click **OK** to save your settings.

Note: If you have the NTA Flow Storage Database installed locally on the main poller, you can also launch the Configuration Wizard and change the backup folder during the configuration.

Restoring Backups

If you want to see historical data after an upgrade from previous NTA versions, you need to backup your database before the upgrade and restore it after you have finished the update. For more information about upgrading NTA, see Upgrading NTA.

To restore NTA Flow Storage Database backups:

1. Log on to the NTA Flow Storage Database server.
2. Make sure the backup file is available on the NTA Flow Storage Database server.
3. Launch the command prompt.
4. Locate the **SolarWinds.NetFlow.FastBit.BackupTool.exe** in the folder where you have installed your NTA Flow Storage Database, such as C:\Program Files (x86)\SolarWinds\Orion\NetFlowTrafficAnalysis.
5. Drag&Drop the **SolarWinds.NetFlow.FastBit.BackupTool.exe** file into the command prompt.
6. Define what should be restored using the following command:

   ```
   NetFlow.Fastbit.BackupTool.exe Restore [source
   folder] [destination folder] [start date] [end date]
   ```

   Example

   ```
   NetFlow.Fastbit.BackupTool.exe Restore D:\FB_Backup\
   D:\FB_Restore\ 2013/06/24 2013/06/27
   ```

   Notes:

   - Start and end dates are obligatory parameters; for setting them, use the format `YYYY/MM/DD`.
   - If you want to restore all data and are not quite sure about the exact dates, use a past date for the start date nd a future date for the end date, such as `1990/1/1 2020/1/1`.

Configuring Charting and Graphing Settings

The Charting and Graphing Settings section of the NTA Settings view gives you the ability to enhance 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 NTA views can become significant. To help this condition, NTA provides a progressive charting option that is enabled by default. The progressive charting option configures 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.

To configure NTA charting and graphing settings:

1. Go to the **NetFlow Settings** page:

    a. Start the **Orion Web Console** in the SolarWinds program folder.

    b. Log in using a **User ID** with administrative privileges.

    c. Click **NETFLOW** on the tool bar, and then click **NetFlow Settings** in the top right corner of the NETFLOW view.

    Note: You can also click **Settings** in the top right corner of the Orion Web Console, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.

2. ***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.

3. ***If you want to enable progressive charting,*** confirm that **Enable Progressive Charting** is checked under Charting and Graphing Settings.
4. Click **Save** in the Charting and Graphing Settings section.

Configuring Percentage Type for Top XX Lists

Percentage Type for Top XX Lists describes how NTA calculates percentages in Top XX resources.

- **Absolute percentages** are calculated for each item based on all monitored items. Items not belonging to the top XX resources, such as items number 6 and more in Top 5 resources, are shown on the chart as Remaining traffic and are included in percentage calculations.
- **Relative percentages** for each item are calculated in terms of the total number of items displayed in the selected resource. Top xx resources thus show only the set number of items, and only the items shown in the chart are included in percentage calculations.

For more information and an example, see Top XX List Resource Percentages.

To configure the percentage type for Top XX list resources:

1. Go to the **NetFlow Settings** page:
    a. Start the **Orion Web Console** in the SolarWinds program folder.
    b. Log in using a **User ID** with administrative privileges.
    c. Click **NETFLOW** on the tool bar, and then click **NetFlow Settings** in the top right corner of the NETFLOW view.

    Note: You can also click **Settings** in the top right corner of the Orion Web Console, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
2. Under the Charting and Graphing Settings heading, select either **absolute** or **relative** Percentage Type for Top XX Lists, as appropriate.
3. Click **Save** in the Charting and Graphing Settings section.

Top XX List Resource Percentages

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 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 NTA area charts.

To globally configure NTA area chart display units:

1. Go to the **NetFlow Settings** page:
    a. Start the **Orion Web Console** in the SolarWinds program folder.
    b. Log in using a **User ID** with administrative privileges.
    c. Click **NETFLOW** on the tool bar, and then click **NetFlow Settings** in the top right corner of the NETFLOW view.

    Note: You can also click **Settings** in the top right corner of the Orion Web Console, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.

2. 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.
3. 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 NTA area chart resource.

Configuring Resource Default Time Periods

You can globally set the default time period for all 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 NTA resources placed on detailed views is Last 15 Minutes, and the default time period for NTA resources placed on summary views is Last 1 Hour(s).

To globally configure the default resource time period:

1. Go to the **NetFlow Settings** page:
    a. Start the **Orion Web Console** in the SolarWinds program folder.
    b. Log in using a **User ID** with administrative privileges.
    c. Click **NETFLOW** on the tool bar, and then click **NetFlow Settings** in the top right corner of the NETFLOW view.

    Note: You can also click **Settings** in the top right corner of the Orion Web Console, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
2. Under the Charting and Graphing Settings heading, enter values and select appropriate time units in the **Default time period for**… fields.
3. Click **Save** in the Charting and Graphing Settings section.

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

Configuring the NTA View Refresh Rate

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

To enable and configure the refresh rate for NTA views:

1. Go to the **NetFlow Settings** page:
    a. Start the **Orion Web Console** in the SolarWinds program folder.
    b. Log in using a **User ID** with administrative privileges.

c. Click **NETFLOW** on the tool bar, and then click **NetFlow Settings** in the top right corner of the NETFLOW view.

   Note: You can also click **Settings** in the top right corner of the Orion Web Console, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.

2. Under the Charting and Graphing Settings heading, check **Enable automatic page refresh every X minutes**.
3. Provide an appropriate refresh interval in minutes.
4. Click **Save** in the Charting and Graphing Settings section.

Optimizing Performance of NTA

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

Maintaining your Orion, SQL and NTA Flow Storage Database servers on separate physical machines is a fundamental requirement in scaling the 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 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. For more details, see Configuring On Demand DNS resolution.
- Capture only the flows required to represent the "top talkers" on your network. For more details, see Limiting Flows Collections To Top Talkers.
- Limit the time period for storing flow data in your database (Orion SQL or NTA Flow Storage Database). For more details, see Limiting Data Retention Period for Orion SQL Database or Setting Data Retention Period for NTA Flow Storage Database.
- If you store your flows data in the Orion SQL Database (NTA 4.0 on 32-bit operating systems and older versions), adjust the data aggregation. For more details, see Adjusting Data Aggregation Settings.
- If you do not need to store traffic data on unmonitored ports, you can disable data retention for unmonitored ports. For more information, see Configuring Data Retention for Flows on Unmonitored Ports.

Configuring On Demand DNS resolution

Enabling On Demand DNS resolution in 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 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. Go to the **NetFlow Settings** page:
    a. Start the **Orion Web Console** in the SolarWinds program folder.
    b. Log in using a **User ID** with administrative privileges.
    c. Click **NETFLOW** on the tool bar, and then click **NetFlow Settings** in the top right corner of the NETFLOW view.

    Note: You can also click **Settings** in the top right corner of the Orion Web Console, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
2. Under **DNS and NetBIOS Resolution**, set DNS Resolution to **On Demand**.
3. 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 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 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 NTA installation.

As a feature of 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. Go to the **NetFlow Settings** page:
    a. Start the **Orion Web Console** in the SolarWinds program folder.
    b. Log in using a **User ID** with administrative privileges.
    c. Click **NETFLOW** on the tool bar, and then click **NetFlow Settings** in the top right corner of the NETFLOW view.

    Note: You can also click **Settings** in the top right corner of the Orion Web Console, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
2. Under **Top Talker Optimization**, in the **Capture flows based on the maximum percentage of traffic** field, set the preferred value.
3. Click **Save**.

Limiting the Data Retention Period for the Orion SQL Database

You can further additionally optimize the performance of your NTA by limiting the period for which your flows data are kept in the database. This time is also called retention period.

Notes:

- CBQoS data are stored in the Orion SQL Database.
- NTA 4.0 on 64-bit operating systems uses the NTA Flow Storage Database where the flows data are not compressed at all, thus enabling you to limit one retention period only. For more information, see Setting Retention Period for NTA Flow Storage Database.
- NTA 4.0 on 32-bit operating systems and older NTA versions store flows data in the Orion SQL Database which allows you to limit the retention period for both compressed and uncompressed data.

To configure the retention period for Orion SQL Database:

1. Go to the **NetFlow Settings** page:

    a. Start the **Orion Web Console** in the SolarWinds program folder.

    b. Log in using a **User ID** with administrative privileges.

    c. Click **NETFLOW** on the tool bar, and then click **NetFlow Settings** in the top right corner of the NETFLOW view.

    Note: You can also click **Settings** in the top right corner of the Orion Web Console, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.

2. Scroll down to the **Database Settings** grouping.
3. Specify how long the data should be kept as uncompressed records in the Orion database. Enter an appropriate number of minutes in the **Keep uncompressed data for** field.

    Notes:

    - You must keep uncompressed data for at least 15 minutes to ensure that at least 15 minutes of data can be collected and compressed before any of it is possibly deleted.
    - Consider collecting data for a day before adjusting these settings. After a day, you should have a good idea of the volume of data your network produces with NetFlow enabled.

4. Specify how long the data are kept in the database until they are finally deleted. Go to the **Keep compressed data for XX days** field and provide a value of 14 or less.
5. Select the frequency with which you want to **Delete expired flow data**.

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

6. Click **Save**.

Setting Retention Period for NTA Flow Storage Database

Retention period specifies the time for which flow data are stored in the database until they expire and are permanently deleted.

To optimize the retention period for your NTA Flow Storage Database, collect data for a few days, and then consider the space taken up by the database when adjusting the retention period.

To set up appropriate retention period for NTA Flow Storage Database:

1. Go to the **NetFlow Settings** page:
    a. Start the **Orion Web Console** in the SolarWinds program folder.
    b. Log in using a **User ID** with administrative privileges.
    c. Click **NETFLOW** on the tool bar, and then click **NetFlow Settings** in the top right corner of the NETFLOW view.

    Note: You can also click **Settings** in the top right corner of the Orion Web Console, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
2. Under **Database Settings**, click the **Refresh NTA Flow Storage Database Info** button. NTA will display the current values in the appropriate fields.
3. Review the current size of the database in the **NTA Flow Storage Database Size** and **Stored days in NTA Flow Storage Database** read-only fields.
4. You can easily find out the average amount of data stored on a daily basis by dividing the NTA Flow Storage Database size by the number of days.
5. Consider the space available on your NTA Flow Storage Database disk, the space required daily and update your **Retention period** accordingly.

    Note: If you need to store the data history for a longer time period than it is possible, please consider upgrading your hardware.
6. Click **Save** in the Database Settings grouping.

Adjusting Data Aggregation Settings

Aggregating NetFlow data in memory significantly reduces the I/O demands that NTA makes on your Orion database, which can increase the performance of all SolarWinds applications that share the database. If Web Console resources are allowed to work directly against the Orion database in making and presenting their latest calculations without aggregation, NTA would make big I/O demands on the Orion database. This would impact performance of both NTA and Orion NPM.

By aggregating data before writing it to the Orion database, 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.

Note: Data aggregation is possible only if you are using NTA 4.0 on a 32-bit operating system together with the Orion database or older NTA versions.

Activating Aggregation

By aggregating data before writing it to the Orion database, 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.

To turn on data aggregation settings:

1. Go to the **NetFlow Settings** page:
    a. Start the **Orion Web Console** in the SolarWinds program folder.
    b. Log in using a **User ID** with administrative privileges.
    c. Click **NETFLOW** on the tool bar, and then click **NetFlow Settings** in the top right corner of the NETFLOW view.

    Note: You can also click **Settings** in the top right corner of the Orion Web Console, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.

2. Scroll down to **Database Settings** and configure the Data Aggregation options as follows:
    a. Check **Enable aggregation of Top Talker Data**.
    b. Enter how many of the following Orion should aggregate NetFlow data for:
        - Top Applications
        - Top Endpoints
        - Top Conversations
    c. Enter the number of hours NTA should save aggregated NetFlow data

in cache.

3. Click **Save**.

Optimizing Aggregation

Optimize aggregation by displaying the items you entered above when you activated aggregation. For example, if you entered 10 Top Conversations for which to aggregate data, you should display up to 10 Top Conversations. Displaying more conversations would require loading more data than is cached and would slow performance.

To set the optimal number of data elements:

1. Click **Edit** from a Top XX Applications, Endpoints, or Conversations pane.
2. On the Edit Resource page, enter the **Maximum Number of Items to Display**. This number should match the number you entered for this resource when you activated data aggregation in the procedure above.
3. Click **Submit**.

Chapter 4: 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 statistics are provided in the Orion Web Console as resources grouped to form individual views.

View is a web page showing information about your network and the traffic going through individual nodes and interfaces. Views consist of resources. You can customize which resources you want to have on a view.

NTA provides two basic types of views:

- **Summary views** show traffic details on all nodes and interfaces managed by your NTA, such as top applications, conversations, and endpoints. You can access your summary views either in the NETFLOW Views menu bar or by clicking an item in another view. For example, clicking on an application in the Top 5 Applications Summary view displays a summary view covering the use of the selected application in all nodes monitored in NTA.
- **Detail views** show traffic information on individual objects in your network, such as interface details, node details, and application details. You can access your detail views by opening a summary view and clicking on the object whose details you want to see.

Resource is a building block of your views, it displays on your views as a box and provides information about different aspects of traffic monitoring, usually in a chart and a table. Some resources are meant to be used on summary views, some are suitable for detail views, and some can be useful on both view types. The information shown pertains to either all devices NTA monitors (if used on a summary view) or to the selected object (if used on a detail view for a node, interface, conversation, application, CBQoS class, or other object).

Note: If you upgraded to NTA 4.0 with the NTA Flow Storage Database from a previous NTA version, you might experience performance issues when trying to display reports and graphs for your endpoints. NTA Flow Storage Database

stores more detailed data, and so viewing the same nodes over the same time period requires handling an increased amount of data, and can thus result in slower rendering or processing.

Editing Resources

Resources in the Orion Web Console are edited on the Edit Resource page. The options available depend on individual resources.

To edit a resource:

1. Click **Edit** in the title bar of the resource.
2. Customize the available options:
    - Title
    - Subtitle
    - Maximum Number of Items to Display
    - Chart customization options. For more information, see Customizing Classic Charts or Customizing Interactive Charts.
3. Click **Submit** to apply your changes.

Working with Charts

NTA's Interactive and Classic charts display NTA pie-chart summaries of resource-related data. 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.

To find out more information about customizing individual charts in general, see Customizing Charts.

Interactive Charts

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.

To find out more information about customizing interactive charts if you have administrator access to the Orion Web Console, see Customizing Interactive Charts.

Classic Charts

Classic charts display information in 2-D pie, 3-D pie, and area charts. 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 find out more information about customizing classic charts if you have administrator access to the Orion Web Console, see Customizing Classic Charts.

The following sections explain the elements of Interactive and Classic charts you may encounter.

Pie Charts

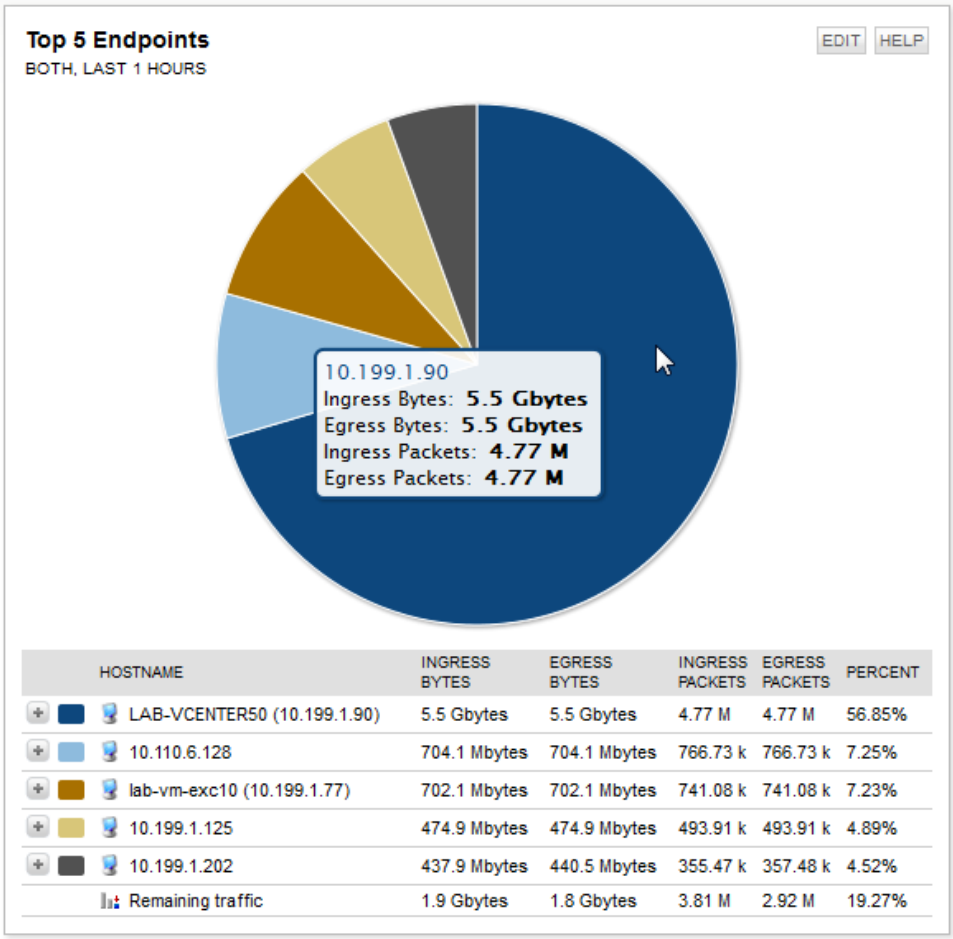
The pie charts in this section show the Top 5 Endpoints. The following charts use absolute percentage calculations. The Interactive charts also show the new feature in Interactive charts, Remaining traffic. For more information on the Remaining traffic feature, see Configuring Charting and Graphing Settings.

Interactive Pie Charts

With Interactive pie charts, NTA gives each resource its own piece of pie, depending on your chart settings. If more resources exist than what is configured to display, 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. NTA labels all other endpoint flow traffic as Remaining traffic, which is 19.27% of the total traffic flow.

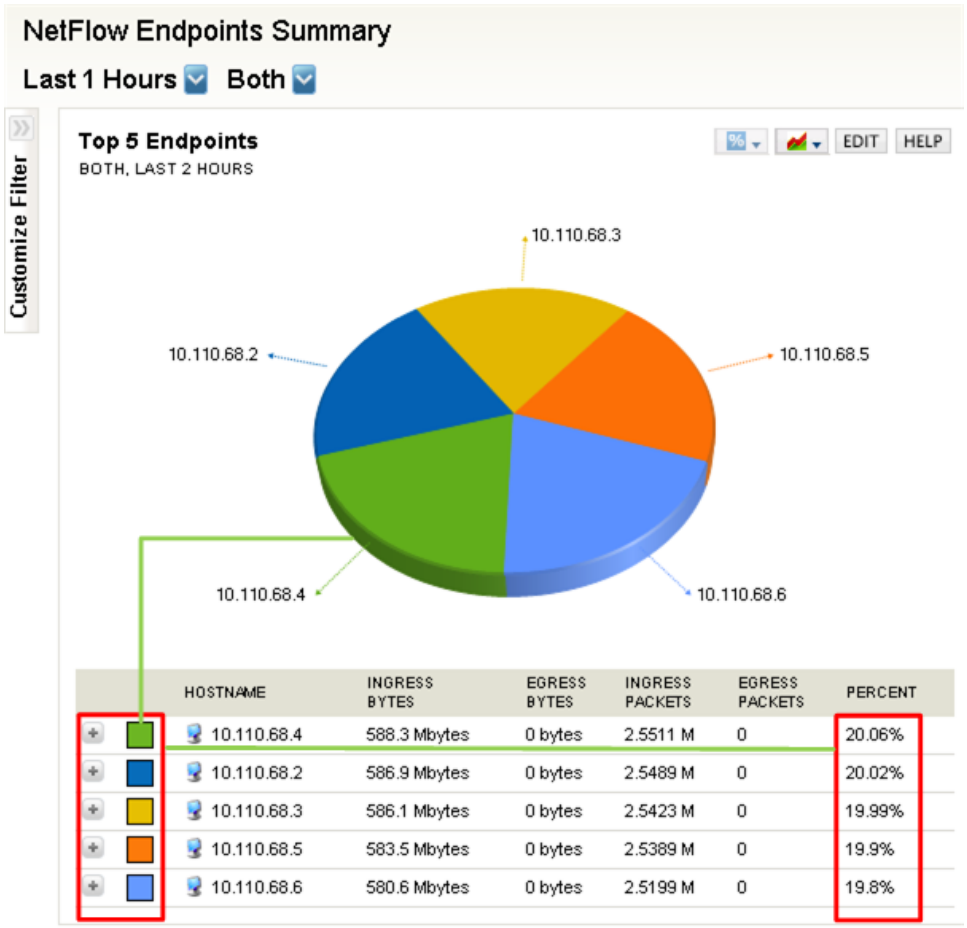


HOSTNAME	INGRESS BYTES	EGRESS BYTES	INGRESS PACKETS	EGRESS PACKETS	PERCENT
LAB-VCENTER50 (10.199.1.90)	5.5 Gbytes	5.5 Gbytes	4.77 M	4.77 M	56.85%
10.110.6.128	704.1 Mbytes	704.1 Mbytes	766.73 k	766.73 k	7.25%
lab-vm-exc10 (10.199.1.77)	702.1 Mbytes	702.1 Mbytes	741.08 k	741.08 k	7.23%
10.199.1.125	474.9 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.

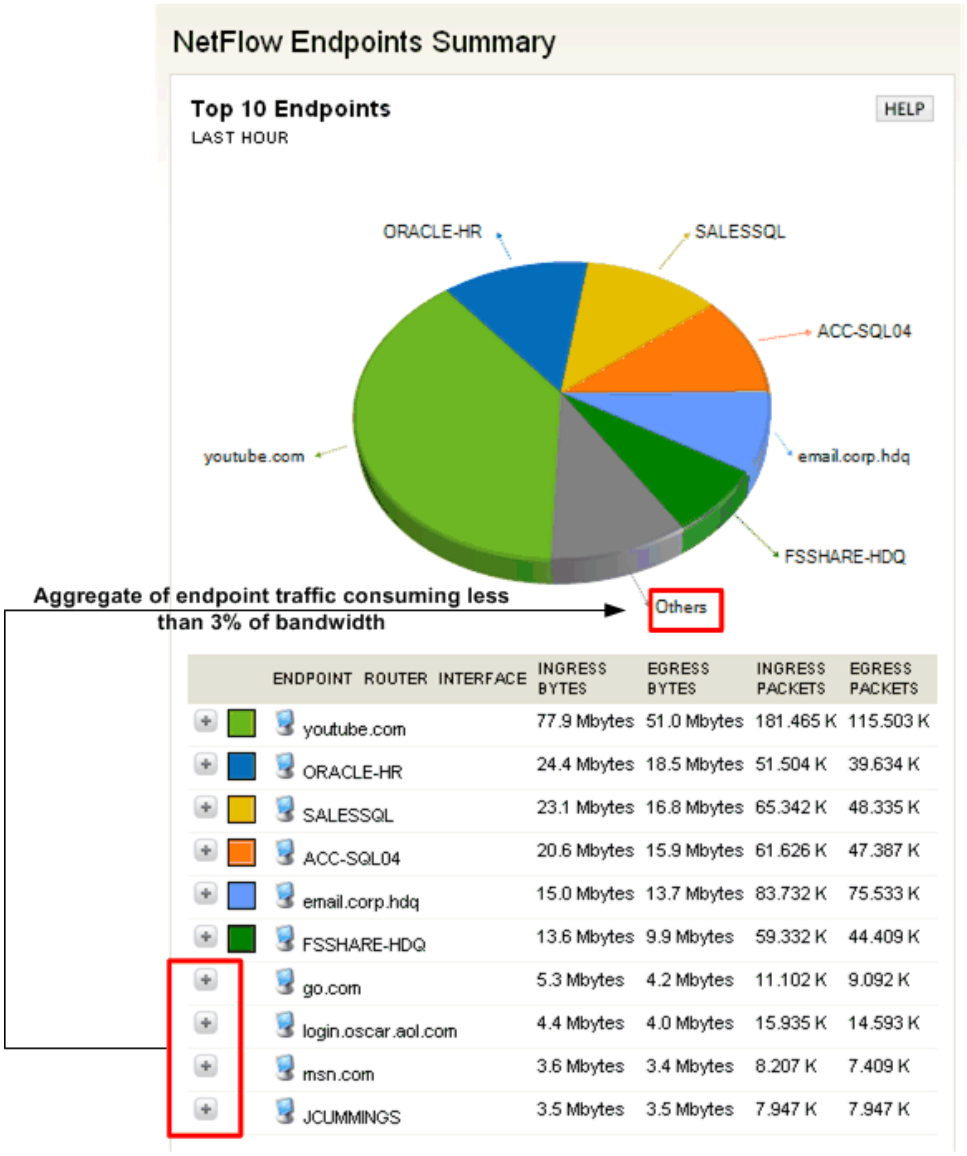


In this chart, which uses absolute percentage calculations, traffic is divided almost evenly at 20% each among the top endpoints.

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.



Area Charts

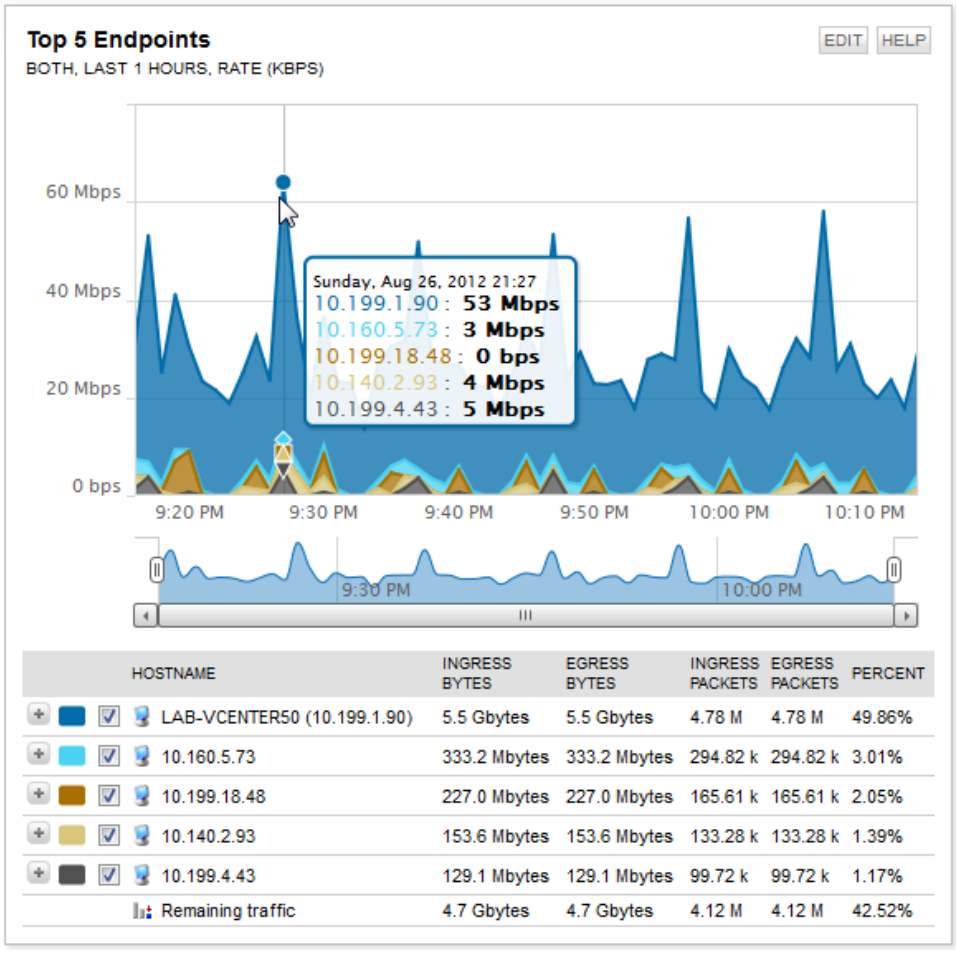
Area charts are the default charts for resource detail pages. They provide a more comprehensive view of traffic and bandwidth usage data than pie charts, so area charts always include a one-to-one relationship of table-to-chart information.

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, 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.

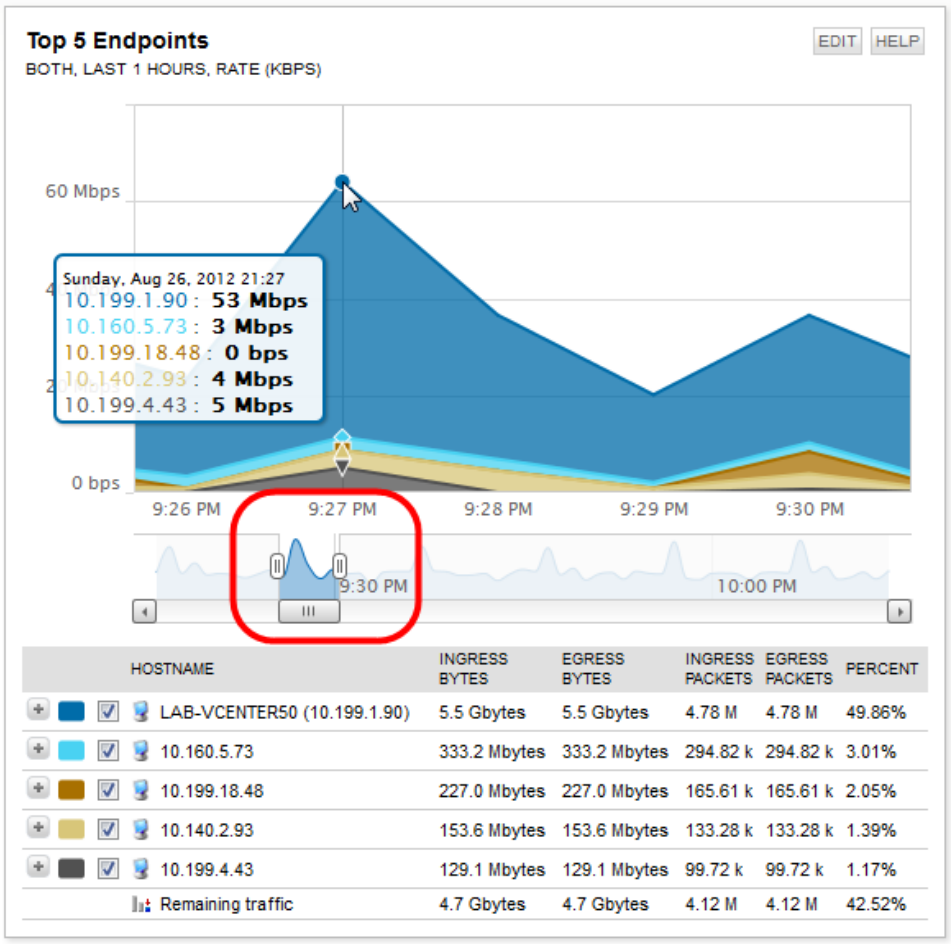
Point your mouse to a specific point on an Interactive area chart, and the chart displays the exact transmission details for that point in time. The detailed information displays within the chart and in a tool tip.



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%

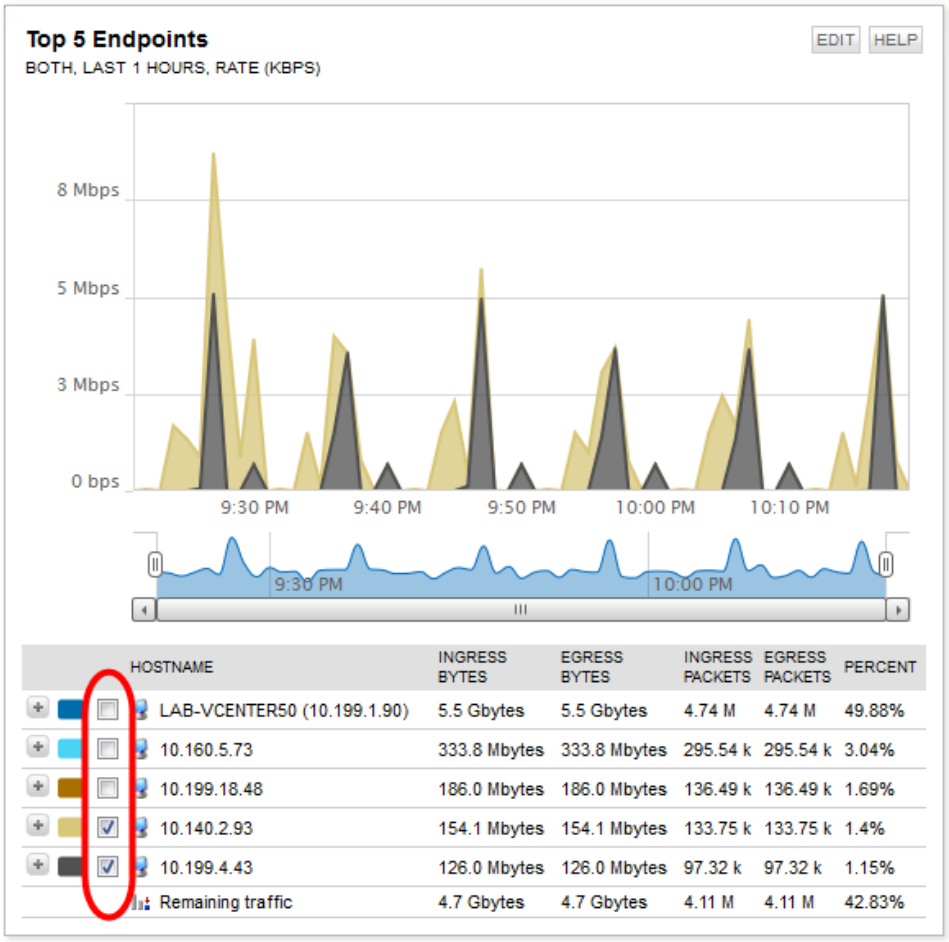
The Top 5 Endpoints data shown the area chart tell us that at their highest traffic points, conversations involving the LAB-VCENTER50 (10.199.1.90) and 10.160.5.73 endpoints not only generated more traffic than the other top 3 endpoints, but they did so consistently across the displayed time intervals.

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.



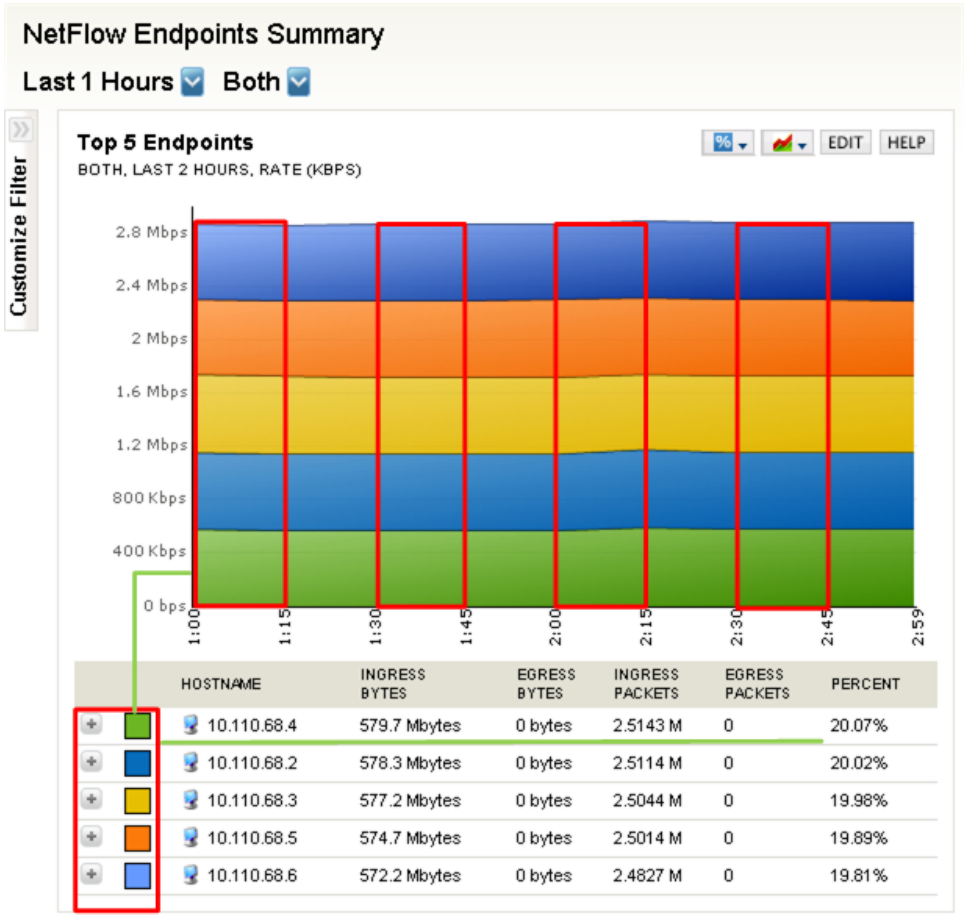
HOSTNAME	INGRESS BYTES	EGRESS BYTES	INGRESS PACKETS	EGRESS PACKETS	PERCENT
LAB-VCENTER50 (10.199.1.90)	5.5 Gbytes	5.5 Gbytes	4.78 M	4.78 M	49.86%
10.160.5.73	333.2 Mbytes	333.2 Mbytes	294.82 k	294.82 k	3.01%
10.199.18.48	227.0 Mbytes	227.0 Mbytes	165.61 k	165.61 k	2.05%
10.140.2.93	153.6 Mbytes	153.6 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.



The top three endpoints 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.

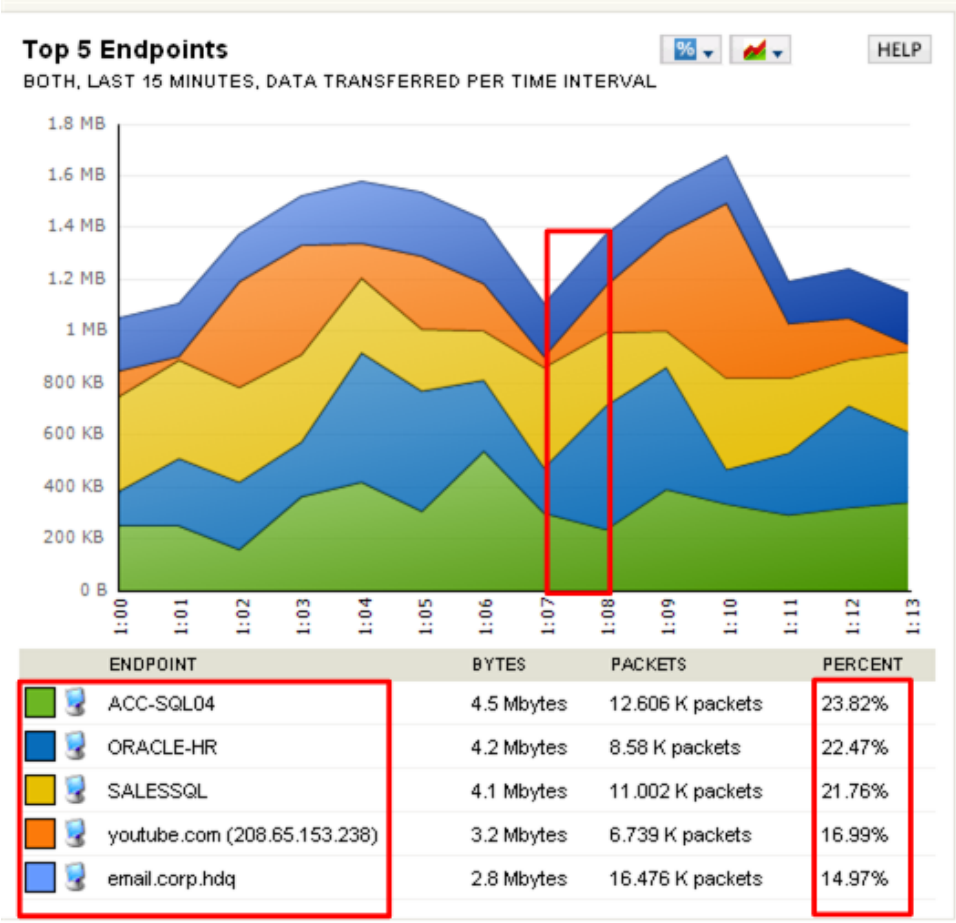
Classic Area Charts



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:



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.

Customizing Charts

NTA 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 based on traffic percentages. Individual 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.

In NTA, there are two chart styles, interactive charts and classic charts.

Interactive charts offer the following types of charts:

- 2-D pie chart
- Area chart (stack area, stack spline area, stack line, line, spline, bar)

Classic charts offer the following types of charts:

- 2-D or 3-D pie chart
- Area chart (stack area, stack spline area, stack line, line, spline, bar)

For information on Classic or Interactive charts' features, see Working With Charts.

For more information about global options for configuring resources, see Configuring Charting and Graphing Settings.

If you have administrator privileges, you can customize resources for all users.For more information, see Customizing Classic Charts or Customizing Interactive Charts.

Non-administrative users may still customize resources for the duration of the current browser session. For more information, see Customizing Resources for the Current Session.

Selecting Classic or Interactive Charts

NTA charts are available as classic and interactive charts. The style of your chart is selected when you add the resource to an appropriate view.

If you want to change the style of a resource that is available on a view, you need to remove the original resource from the view and replace it with the resource of the other style.

To select a chart style:

1. Click **Customize Page**, in the top right corner of any Summary page. The Customization page displays.
2. Click ✚ to add a resource.
3. Select **Feature** in the **Group by** list, and then select **TrafficAnalysis** below the list.

4. Select the appropriate resource(s) which you want to add to your view. Only reports which can be applied on the view are provided. You can select resources from the following categories:
    - **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

    Notes:

    - Resources selected to be added to the view are listed in the **Selected Resources** list.
    - If you do not want to add a resource that is in the Selected Resources list, click **x** next to the resource name.
    - Classic resources are designated by the **Classic Chart Style** label in the **Category** column.
    - On one view, you can use both classic and interactive charts. If you want to see the same resource in both classic and interactive charts, add it twice to the view - once as an interactive and once as the classic style resource.
5. Click **ADD SELECTED RESOURCES**.
6. To review how the chart styles look, click **PREVIEW**. To complete and apply chart style selection, click **DONE**.

Customizing Resources for the Current Session

All users who can view resources can also customize the charts for the duration of the current session.

You can customize:

- time and flow direction settings for all appropriate resources in a view
- chart style and data units shown by classic area charts
- zoom and display items in interactive area charts

Once you leave the view with the resource, your current settings will be lost and replaced by settings for the resource.

Customizing Time and Flow Direction Settings for the Current Session

You can customize the time and flow direction settings for all appropriate resources on a view.

However, resources with their individual time periods set in their Edit pages are not subject to this time period control.

For more information about customizing time settings, see Editing Time Settings for Views.

For more information about customizing flow direction settings, see Editing Flow Direction Settings for Views.

Classic Area Charts: Customizing Chart Styles and Data Units

To customize classic chart styles and data units:

1. Click the Chart Styles  button in the resource title bar.
2. Select one from the following options:
    - **2-D Pie Chart** presents a “flat” view of your data
    - **3-D Pie Chart** presents a 3-dimensional view of your data
    - **Area Chart** presents a historical view of your data as represented by areas calculated at past polling times.

Note: If you select this option, you will see the Area Chart Style selected in the Edit Resource page. To change it, click **Edit**, select the appropriate **Chart Style** and click **Submit**. The default area chart style will be changed not only for the current session, but for this resource. For more information, see Customizing Classic Charts.

3. ***If you have selected the Area Chart type***, you can further select what data units the chart should display.

   Click the **Data Units** icon and select one of the following data unit types:

   - **Rate (Kbps)** creates a chart displaying historical traffic rate data for selected flow-enabled nodes and interfaces.
   - **% of interface speed** is only available for resources presenting interface traffic data. This option creates a chart showing how bandwidth is allocated across the elements listed in the 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 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.

Interactive Area Charts: Zoom and Show selected items only

Interactive area charts support the following session-related options:

- Beneath interactive area charts, you can see a slider tool. Move the slider to display an in-depth view of the selected part of the chart to get a detailed view of traffic at a certain time.
- Select or clear the boxes in the table below an interactive area chart, to display only the items you want to see at the moment.

Customizing Interactive Charts

To customize interactive charts, complete the following procedure:

1. Click **Edit** in the resource title bar.
2. Now on the Edit Resource page, specify the **Title** and **Subtitle** for the resource.

3. Select the **Chart Style** you want to use:
    - Select **Area Chart** in the **Data** drop down list to use area charts
    - Select **Pie Chart** in the **Data** drop-down list to use pie charts
    - Select **Use chart style default for view** to use the style which is set as default for the resource when used on the appropriate view.
4. Provide the number of items you want to display in the **Maximum number of items to display** field.
5. 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.
6. Select the **Resource Style**:
    - Select **Chart** to display both the chart and the legend in the resource.
    - Select **No Chart** to view only the legend.
7. Select the **Flow Direction** to be displayed in the chart:
    - **Default for view** keeps the flow settings configured in NTA Settings.
    - **Both** displays both ingress and egress traffic.
    - **Ingress** displays ingress traffic only.
    - **Egress** displays egress traffic only.
8. ***If you 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.

9. ***If you have selected the Area Chart type***, 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 resources presenting interface traffic data. This option creates a chart showing how bandwidth is allocated across the elements listed in the 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 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.
10. ***If you want to add a title or subtitle for the chart***, click **+** next to **Advanced** and fill in the appropriate **Chart title** and **Chart subtitle** names.
11. Click **Submit**.

Customizing Classic Charts

To customize classic charts, complete the following procedure:

1. Click **Edit** in the resource title bar.
2. Now on the Edit Resource page, specify the **Title** for the resource.

3. Provide the number of items you want to display in the **Maximum number of items to display** field.
4. 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.
5. Select the **Resource Style**:
    - Select **Chart** to display both the chart and the legend in the resource.
    - Select **No Chart** to view only the legend.
6. Select what Chart Style you want to use:
    - Select **Area Chart** in the **Chart Style** list to use area charts.
    - Select **2D Pie Chart** to display a "flat" view of your data.
    - Select **3D Pie Chart** to display a 3-dimensional view of your data.
    - Select **Use default** to use the style which is set as default for the resource when used on the appropriate view.
7. ***If you have selected Area Chart***, select the appropriate Area Type for use in the 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. ***If you have selected the Area Chart type***, 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 resources presenting interface traffic data. This option creates a chart showing how bandwidth is allocated across the elements listed in the 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 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 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.

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

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 in the *Orion Network Performance Monitor*

Administrator Guide.

5. Click **Submit**.

After you have created a new view, the Customize Your View page opens. For more information, see Editing Views in the *Orion Network Performance Monitor Administrator Guide*.

Creating Custom Views with the Flow Navigator

You can create custom traffic views directly from any NetFlow view, using the Flow Navigator.

These custom filters allow you to view specific statistics about your entire network and its devices without having to navigate through the web console a single device view at a time.

You can configure your custom traffic view to include devices, applications, time periods, and more, all from one configuration pane.

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. Specify the **View type**.
    a. ***If you want a filtered view of your entire network***, click **Summary** and select the appropriate summary view.
    b. ***If you want a filtered view of traffic passing through a specific node and interface***, click **Detail**.

    Select the appropriate **Detail view type**. This displays lists and input fields relevant for the selected view type, such as **Select a Node** or **Select an Interface**,…

    Select or type in the view-related information.
5. Select the **Time Period** over which you want to view traffic data, using any of the following options:
    - Select **Named Time Period**, and then select a predefined period from the Named Time Period menu.

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

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

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

  Note: Use the calendars to set your time or 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. You can further limit the view by including or excluding some of the following items:

   Applications

   If you want to limit your view to only display network traffic to and from applications, or to exclude traffic to and from them, 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 or the appropriate port number.
   d. ***If you want to include or exclude another application***, click **Add Filter** and enter the name of the appropriate application.

   Autonomous Systems

   If you want to limit your view to only display network traffic to and

from autonomous systems, or to exclude traffic to and from certain autonomous systems, 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 ID of an appropriate autonomous network.

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

Autonomous Systems Conversations

If you want to limit your view to only display network traffic related to specific autonomous system conversations, or to exclude traffic to and from them, 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 IDs of autonomous systems involved in conversations that you want to include or exclude.

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

Conversations

If you want to limit your view to only display network traffic related to specific conversations between two endpoints, or to exclude traffic to and from them, 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.

Countries

If you want to limit your view to only display network traffic related to specific countries, or to exclude traffic to and from them, 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.

Domains

If you want to limit your view to only display network traffic related to specific domains, or to exclude traffic to and from them, 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 name.

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

Note: If a domain name is not resolved and saved in NTA, you cannot use it in the Flow Navigator. NTA will inform you about it and ask you to provide a valid name. For more information about resolving domain names, see Host and Domain Names.

Endpoints

If you want to limit your view to only display network traffic related to specific endpoints, or to exclude traffic to and from them, 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 the IP address or hostname of an appropriate endpoint.

d. ***If you want to include or exclude traffic from a specified subnet***, enter the appropriate range of IP addresses.

   Note: You can either type the range in, for example 192.168.1.0-192.168.1.255, or use the CIDR notation, for example 192.168.1.0/24.

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

IP Address Groups

If you want to limit your view to only display network traffic related to specific IP address groups, or to exclude traffic to and from them, 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.

Protocol

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.

Types of Service

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.

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

Adding NetFlow Resources to Web Console Views

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

To add a NetFlow resource to a web console view:

1. Log on to the NPM server that you are using for NetFlow traffic analysis.
2. Start the Orion Web Console in the Orion program folder.
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 Customizing Web Console Menu Bars in the *Orion Network Performance Monitor Administrator Guide*.

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.

Note: If your user account has limitations, you might not see all the expected traffic because of the limitations. For more information, see Creating Account Limitations in the *Orion Network Performance Monitor Administrator Guide*.

To add an endpoint-centric resource:

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

   Note: 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. Locate the endpoint centric resource on the Add Resource page:

   Select **Classic category** in the **Group by** list and then click **NetFlow Endpoint Centric Resources**.

6. Select the appropriate endpoint centric resource and click **Add selected resources**.

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**.

Configuring View Limitations

As a security feature, the web console gives administrators the ability to apply device-based view limitations. NetFlow Traffic Analyzer views thus can be limited to show only information from selected types of NetFlow sources.

To enable view limitations in NetFlow Traffic Analyzer:

1. Log on to the NPM server you are using for NetFlow traffic analysis.
2. Start the **Orion Web Console** in the Orion program folder.
3. Log in to the Orion 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.
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. Provide or check appropriate strings or options to define the device types to include or exclude from the selected view.
11. Click **Submit**.

    Note: The asterisk (*) is a valid wildcard. Pattern limitations restrict views to devices for which the corresponding fields include the provided string.

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. If you have the appropriate view open, click **Customize View**.
   You can also access the view from Orion settings:
   a. Click **Settings** in the top right of the web console.
   b. Click **Manage Views** in the **Views** group.
   c. Select the view you want to customize from the list, and then click **Edit**.
2. ***If you want the view to consist of more subviews***, select **Enable left navigation** and define appropriate subviews, their layout and resources. For more information, see Using and Configuring Subviews in the *Orion Network Performance Monitor Administrator Guide*.
3. ***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**.
4. ***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 in the *Orion Network Performance Monitor Administrator Guide*.

- 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.

5. ***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.
6. ***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.
7. ***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.
8. ***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 in the *Orion Network Performance Monitor Administrator Guide*.

9. Close the preview window.
10. ***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 the Orion Web Console in the *Orion Network Performance Monitor Administrator Guide*. For more information about assigning your customized view as the default view for a user, see Editing Views in that same guide.

Editing Time Settings for Views

You can customize the time shown by all appropriate resources on a view. These settings are limited to the current session. Once you leave the view, all resources will show default time settings.

Note: Resources with their individual time periods set in their Edit pages are not subject to this time period control.

To change the time period shown by all resources in the view for the current session:

1. Click next to the time period setting below the view name.
2. Define the time period in one of the following ways:

- Select **Named Time Period** and select one of the available periods (Last 15 Minutes, Last 30 Minutes, Last Hour, Last 2 Hours, Last 24 Hours, or Today).
- Select **Relative Time Period**, fill in a time value and the appropriate unit (Minutes, Hours, Days, or Months).
- Select **Absolute Time Period** and use the date picker and time selection to define the appropriate time period.

Note:

- The time period shown by resources will always be shifted into the past by 2 minutes compared to the current time settings (**Named Time Period** and **Relative Time Period**). There is a 2-minute delay in loading data into the database.

  Example: If you set **Relative Time Period** to **Last 5 minutes** at 11:02, resources will display data collected from 10:55 to 11:00.

3. Click **SUBMIT**.

Editing Flow Direction in Views

You can customize the flow direction shown by all appropriate resources on a view. These settings are limited to the current session. Once you leave the view, all resources will show default flow direction settings.

To change the flow direction shown by all appropriate resources in the view:

1. Click next to the flow direction setting below the view name.
2. Select the appropriate flow direction (**Ingress**, **Egress** or **Both**).

   Note: The Select Flow direction pop-up provides only the options that can be applied to the current view.

3. Click **SUBMIT**.

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.

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**.

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. Start the **Orion Web Console** in the Orion program folder.
2. Click **Settings**.
3. Click **Customize Menu Bars** in the Customize group.
4. Click **Edit** on the Menu Bar: NTA_TabMenu.
5. Click the **X** beside the custom menu item.
6. Click **SUBMIT**.

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**.

Monitoring Traffic Flow Directions

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 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:

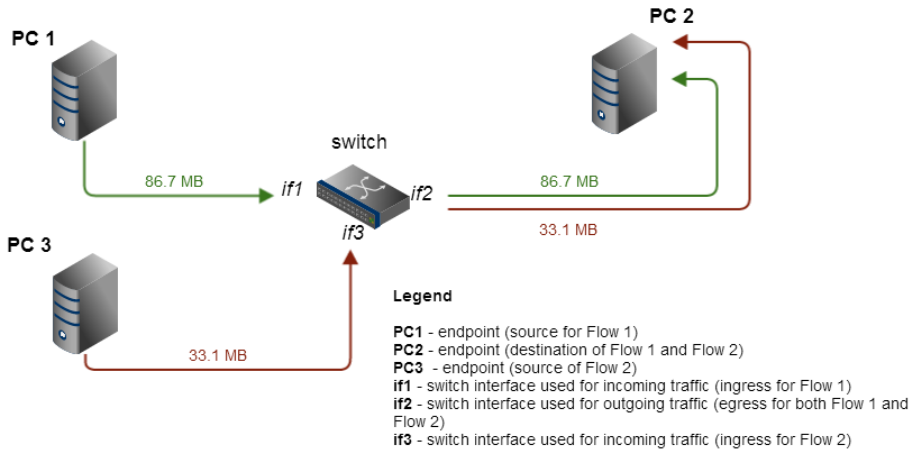
- **Egress** displays only traffic flowing out of the selected node over the selected interface.
- **Ingress** displays only traffic flowing into the selected node over the selected interface.
- **Both** displays a summation of all traffic flowing both in and out of the selected node over the selected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

Note: The size of ingress/egress packets is usually the same. However, it can differ for example if you have CBQoS policies defined for individual interfaces, and these policies define that certain packets are dropped and not delivered to the appropriate endpoint.

Consider the following scenario with two flows:

- Flow F1: PC1 (source) > the traffic of 86.7 MB is coming to the switch through interface if1 (ingress) and leaving the switch via interface if2 (egress) > PC 2 (destination)
- Flow F2: PC3 (source) > the traffic of 33.1 MB is coming to the switch through interface if3 (ingress) and leaving the switch via

interface if2 (egress) > PC 2 (destination)



For PC2, NTA will show us the following interfaces:

- if2 - the interface both flows (F1 and F2) use for leaving the switch (egress: 86.7+33.1=119.8 MB)
- if1 - the interface used by flow F1 for entering the switch (ingress: 86.7 MB)
- if3 - the interface used by flow F2 for entering the switch (ingress: 33.1 MB)

Setting Flow Direction

You can set flow direction either globally for all NTA resources or manually for the current session.

To set global default for flow direction:

1. Start the **Orion Web Console** in the Orion program folder.
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 view overrides the global default for that view only.

To change the flow direction shown by all appropriate resources in the view:

1. Click next to the flow direction setting below the view name.
2. Select the appropriate flow direction (**Ingress**, **Egress** or **Both**).

   Note: The Select Flow direction pop-up provides only the options that can be applied to the current view.

3. Click **SUBMIT**.

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** (also called simply **policies**), 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.

CBQoS policies can be simple or include **nested policies**.

Nested policies are traffic policies applied to a class of an already existing policy. They allow you to set rules for a class-specified type of incoming or outgoing traffic on an interface, thus enabling you to build up a complex approach to different traffic data. Nested policies simplify your job if you need to modify a policy – you just modify it and your changes are automatically applied on all devices using this policy.

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

Note: NTA does not currently provide a CBQoS configuration capability, but any node managed by 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 Configuring Flow Sources and CBQoS-enabled Devices.

For CBQoS-enabled Cisco devices on your network, 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, NPM Interface Details views, and CBQoS Details views:

CBQoS Drops

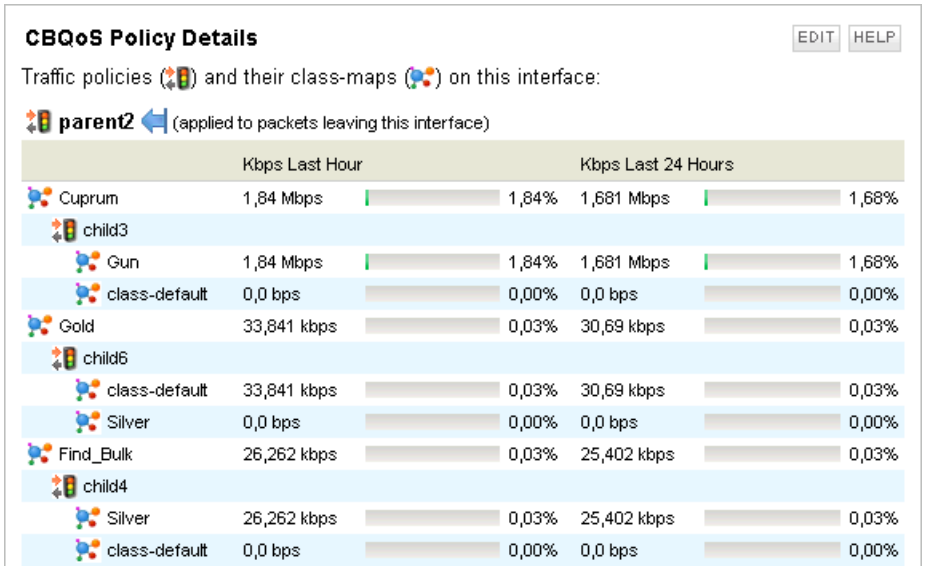
If it is included on a NetFlow Interface Details view, the CBQoS Drops resource provides both a graph and a table reporting each of the defined classes and corresponding amounts of traffic that are filtered out or dropped as a result of policy maps currently enacted on the viewed interface.

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 a table with graphic representations 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. In the header, you can also see whether the policy is applied to incoming packets or to packets leaving the selected interface.

If you have defined nested policies for your interface, you can see a hierarchical tree of classes and policies in this resource. Next to each class, you can see the corresponding traffic in the last hour and last day. For traffic data which do not belong to any defined class, NTA automatically creates a class-default class which displays the remaining traffic.



CBQoS Policy Details EDIT HELP

Traffic policies and their class-maps on this interface:

parent2 (applied to packets leaving this interface)

	Kbps Last Hour		Kbps Last 24 Hours	
Cuprum	1,84 Mbps	1,84%	1,681 Mbps	1,68%
child3				
Gun	1,84 Mbps	1,84%	1,681 Mbps	1,68%
class-default	0,0 bps	0,00%	0,0 bps	0,00%
Gold	33,841 kbps	0,03%	30,69 kbps	0,03%
child6				
class-default	33,841 kbps	0,03%	30,69 kbps	0,03%
Silver	0,0 bps	0,00%	0,0 bps	0,00%
Find_Bulk	26,262 kbps	0,03%	25,402 kbps	0,03%
child4				
Silver	26,262 kbps	0,03%	25,402 kbps	0,03%
class-default	0,0 bps	0,00%	0,0 bps	0,00%

If it is included on the CBQoS Details view, the CBQoS Policy Details resource displays 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.

Note: 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. For more information about different data shown by reports and resources, see the knowledge base article "What is the difference between Ingress Bytes, Egress Bytes, Bytes Through and Total Bytes in NTA?".

Chapter 5: Working with NTA

While NPM can tell you the bandwidth usage on a given interface, SolarWinds 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.

This section guides you through some tasks you might want to accomplish with NTA, and provides use cases illustrating how you can immediately solve your business problems.

Implementing and Monitoring CBQoS Policies

NTA offers flow traffic statistics that can help in determining what CBQoS classes and policies to create and apply. 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.

The following sections explain how to use 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 Cisco devices setup to export flow data—if not, see Adding Flow-Enabled Devices and Interfaces —and 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 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 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. Start the **Orion Web Console** in the Orion program folder.
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 determine the amount of critical data applications typically transfer in the representative time period. You also want to discover the applications that are consuming bandwidth unrelated to the 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 data (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 DNS and NetBIOS Resolution 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, and that devices are all being monitored in NPM and are listed in 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 NTA trigger an alert and take specific actions.

The following Orion Advanced Alerts are available to you:

- Pre-Policy
- Post-Policy
- Drops

For more information about individual alerts, see CBQoS Alerts.

Configuring CBQoS Advanced Alert

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

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

To configure a CBQoS advanced alert:

1. Start the **Advanced Alert Manager** in the Orion Alerting, Reporting, and Mapping folder.
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 to 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, you will need to change the URL the trigger action uses to send out the notification.

For example, if your new credentials were username NTA User with the 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**.

Monitoring Autonomous System Networks (through BGP)

NTA supports monitoring autonomous system networks and autonomous system conversations using the border gateway protocol (BGP). 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

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.

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, 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, 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 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 NTA. For more information about required fields, see Autonomous System Requirements.
- Each device must be configured to include one of the following statistics into the NetFlow exports:
  - `origin-as` command includes the origin AS for the source and destination.
  - `peer-as` command includes the peer AS for the source and destination.

    Note: You cannot include both origin and peer statistics.
- Each device that exports NetFlow data to NTA must be monitored in NPM.

Traffic from a device that is not monitored in NPM appears only in aggregate as part of the traffic from all unmonitored devices. If the device is setup to export data to 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 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 NTA.

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

1. Log in 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 the SolarWinds technical reference "Enabling NetFlow and NetFlow Data Export (NDE) on Cisco Catalyst Switches".

   For information on enabling NetFlow on Cisco ASA devices, consult the KB article "Configuring Cisco ASA devices for use with Orion NTA".

   Otherwise, consult these examples as apply 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 NPM.

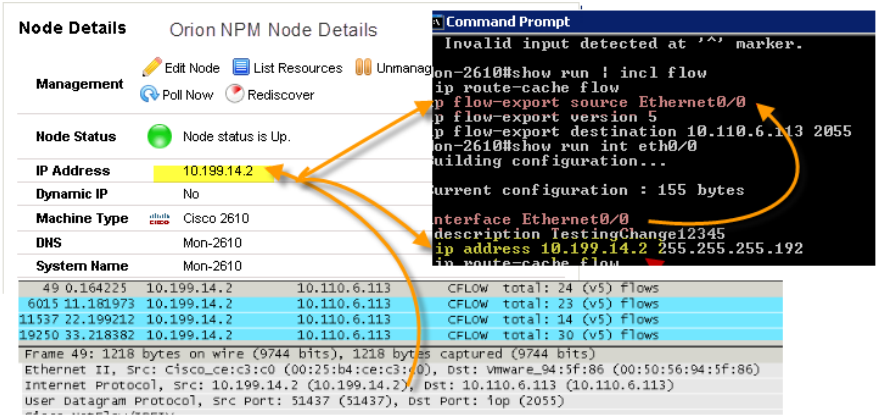
   If you are adding a large number of NetFlow enabled nodes, use Orion Network Sonar. For more information, see Discovering and Adding Network Devices in the *Orion Network Performance Monitor Administrator Guide*.

   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 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:



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 resource 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.

Managing Autonomous System Networks

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

To add an autonomous system network:

1. Go to the **NetFlow Settings** page:

   a. Start the **Orion Web Console** in the SolarWinds program folder.
   b. Log in using a **User ID** with administrative privileges.
   c. Click **NETFLOW** on the tool bar, and then click **NetFlow Settings** in the top right corner of the NETFLOW view.

      Note: You can also click **Settings** in the top right corner of the Orion Web Console, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.

2. Click **Manage Autonomous Systems** under Autonomous Systems.
3. 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
4. Click **Save**.

To edit an autonomous system network:

1. Go to the **NetFlow Settings** page:
    a. Start the **Orion Web Console** in the SolarWinds program folder.
    b. Log in using a **User ID** with administrative privileges.
    c. Click **NETFLOW** on the tool bar, and then click **NetFlow Settings** in the top right corner of the NETFLOW view.

    Note: You can also click **Settings** in the top right corner of the Orion Web Console, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
2. Click **Manage Autonomous Systems** under Autonomous Systems.
3. Click **Edit** beside the relevant autonomous system, 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
4. Click **Save**.

To delete an autonomous system network:

1. Go to the **NetFlow Settings** page:
    a. Start the **Orion Web Console** in the SolarWinds program folder.
    b. Log in using a **User ID** with administrative privileges.
    c. Click **NETFLOW** on the tool bar, and then click **NetFlow Settings** in the top right corner of the NETFLOW view.

Note: You can also click **Settings** in the top right corner of the Orion Web Console, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.

2. Click **Manage Autonomous Systems** under Autonomous Systems.
3. Click **Delete** beside the relevant autonomous system(s).
4. Click **Save**.

Monitoring Autonomous System Networks

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
- Top XX Autonomous System Conversations

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 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 Charts.

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 Customizing Charts.

Finding the Cause of High Bandwidth Utilization

If a node managed in NPM is also a NetFlow Source—meaning that it exports NetFlow data and you are currently monitoring in NTA—you can use 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. Start the **Orion Web Console** in the Orion program folder.
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, 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 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 NTA toolbar.

To keep track of traffic by site:

1. Start the **Orion Web Console** in the Orion program folder and log in.
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 drop-down list 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: Use the calendars to set your time or 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. You can further limit the view by including or excluding some of the following items:

   Autonomous Systems

   If you want to limit your view to only display network traffic to and from autonomous systems, or to exclude traffic to and from certain autonomous systems, 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 ID of an appropriate autonomous network.

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

Autonomous Systems Conversations

If you want to limit your view to only display network traffic related to specific autonomous system conversations, or to exclude traffic to and from them, 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 IDs of autonomous systems involved in conversations that you want to include or exclude.

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

Conversations

If you want to limit your view to only display network traffic related to specific conversations between two endpoints, or to exclude traffic to and from them, 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.

Countries

If you want to limit your view to only display network traffic related

to specific countries, or to exclude traffic to and from them, 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.

Domains

If you want to limit your view to only display network traffic related to specific domains, or to exclude traffic to and from them, 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 name.

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

Note: If a domain name is not resolved and saved in NTA, you cannot use it in the Flow Navigator. NTA will inform you about it and ask you to provide a valid name. For more information about resolving domain names, see Host and Domain Names.

Endpoints

If you want to limit your view to only display network traffic related to specific endpoints, or to exclude traffic to and from them, 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 the IP address or hostname of an appropriate endpoint.

d. ***If you want to include or exclude traffic from a specified subnet***, enter the appropriate range of IP addresses.

Note: You can either type the range in, for example 192.168.1.0-192.168.1.255, or use the CIDR notation, for example 192.168.1.0/24.

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

Protocol

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.

Types of Service

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.

8. When you have completed configuration of your filtered application view, click **SUBMIT**.
9. Click **SAVE FILTERED VIEW TO MENU BAR** to add the filtered view to the menu bar.
10. Name the view.
11. Click **OK**.
12. Repeat steps 3 - 11 for each site you manage.

Performing an Immediate Hostname Lookup

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

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

Interacting with the thwack User Community

By default, NTA provides the thwack Recent NetFlow Posts resource on the NetFlow Traffic Analysis Summary view. This resource shows the most recent 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 NTA forum on thwack.

User Scenarios

The following use cases illustrate the value of SolarWinds 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 SolarWinds 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:

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.

To address this problem, complete the following procedure:

1. Open the Orion Web Console and check that the link to the branch network is up.
2. Consult your **Percent Utilization** chart on the Network Summary home page.
   You can immediately see that the current utilization is 98%, even though normal branch network utilization is 15-25%.
3. Click the NetFlow tab in the Modules toolbar, and then click the name of the branch network link in the **NetFlow Sources** resource to view the flow-enabled router on the branch network.
4. Taking a quick look at the **Top 5 Endpoints** resource, you can 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.

   You know that computers in this IP address range are accessible to customers for personal transactions using the web.

5. Consult the **Top 5 Applications** resource to quickly see that 100% of the last two hours of traffic from the publicly accessible computer has been generated by an IBM MQSeries messaging application.
6. Click the IBM MQSeries messaging application name in the **Top 5 Applications** resource, and you are able to determine that the IBM MQSeries messaging occurs over port 1883.
7. Knowing that you do not 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. Use a configuration management tool, such as SolarWinds Network Configuration Manager, to push a new configuration to your firewall that blocks port 1883.

Locating and Blocking Unwanted Use

With NTA, you can easily chart the increasing usage of your different network uplinks. SolarWinds Network Performance Monitor already allows you to chart utilization, but with the addition of NTA, you can locate specific instances of unwanted use and immediately take corrective action. Consider the following scenario:

Your uplink to the Internet has been slowing progressively over the last 6 months, even though your corporate head count, application use, and dedicated bandwidth have all been stable.

To address this problem, complete the following procedure:

1. Open the Orion Web Console and check in the Orion Summary Home view that the link to the Internet is up at your site.
2. Click the 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. Click the web-facing interface to open the Interface Details view.
4. Customize the **Percent Utilization** chart to show the last 6 months.

   You see that there has been steady growth from 15% to 80% consumption over time. There are even spikes into the high 90s.

5. Click the NetFlow tab in the Modules toolbar, and then click the web-facing interface to open the NetFlow Interface Details view.
6. Looking at the **Top 50 Endpoints** resource, 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. These computers reside in your internal sales IP range.
7. Drill down into each of the offending IP addresses. You find out that each IP you investigate shows Kazaa (port 1214) and World of Warcraft (port 3724) usage in the **Top 5 Applications**.
8. Using a configuration management tool, such as SolarWinds Network Configuration Manager, push a new configuration to your firewall that blocks all traffic on these two ports.

   Within minutes, you see the traffic on the web-facing interface drop back to 25%.

Recognizing and Thwarting Denial of Service Attacks

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

An NPM advanced alert tells you that your web-facing router is having trouble creating and maintaining a stable connection to the Internet.

To address this problem, complete the following procedure:

1. Open the Orion Web Console and search for possible issues.

   All connections are currently up, and bandwidth utilization looks good. But then you notice your CPU utilization on the firewall node. It is holding steady between 99% and 100%.

2. Click the firewall node name to open its Node Details view. You can see that the **Current Percent Utilization of Each Interface** resource shows that your firewall interfaces are receiving abnormally high levels of traffic.
3. Click **NetFlow** in the Modules toolbar to take a quick look at your customized **Top 50 Endpoints** resource.

   The **Top 50 Endpoints** resource shows that the top six computers attempting to access your network are from overseas.

   You realize that you are being port scanned and that your firewall is interactively blocking these attacks.

4. Use a configuration tool, such as SolarWinds Network Configuration Manager, to push a new configuration to your firewall that blocks all traffic over the IP address range of the computers trying to access your network.

   In minutes, your CPU use drops back to normal.

Chapter 6: Troubleshooting NetFlow Traffic Analyzer

For troubleshooting purposes, you can consult the following NTA resources:

NetFlow Collector Services

This resource informs you whether the collector service is up or down. For more details, see NetFlow Collector Services.

NetFlow Sources

This resource lists devices from which your NTA is receiving flows, together with the timestamp of the latest received NetFlow or CBQoS data. You can drill down to individual interfaces to pinpoint the problem. For more information, see NetFlow Sources.

Last 25 Events

This resource provides details about everything that happens in NTA. For more information, see Last 25 Traffic Analysis Events.

Notes:

- For more details about resolving individual events, consult the appropriate item in the Last 25 Traffic Analysis Events resource.
- For more information about troubleshooting NetFlow, see the technical reference Best Practices for Troubleshooting NetFlow.
- For more information about troubleshooting CBQoS, see the knowledge base article "Troubleshooting CBQoS Issues".

NetFlow Collector Services

The NetFlow Collector Services resource provides status information about the servers on which you have installed NetFlow Traffic Analyzer to collect flow and CBQoS information.

The following information about the collectors and the ports on which they are listening for flow and CBQoS data is provided in the table:

Column	Explanation
Status Icon	Displays collector status visually, where a green icon indicates that the collector can actively receive flow and CBQoS data and a red icon indicates that the collector cannot actively receive flow and CBQoS data.
Server Name	The network identification of the NetFlow collector.
Receiver Status	A verbal statement of collector status.
Collection Port	This is the port on which the NetFlow collector is listening for NetFlow data. The collection port is set during the installation and configuration of NetFlow Traffic Analyzer.

Editing or Adding Collection Ports

To add or change the collection port:

1. Click **Edit** to open the Edit NetFlow Collector Services view.
2. Change the collection port or add another collection port into the field appropriate field.

   Note: Separate listed ports with a single comma, as in 2055,9995.

3. Click **Submit** to apply the changes.

Deleting Collectors

If you have stale records in your database, for example if a poller breaks down, or you replace a poller with another one, the information about collectors can be inaccurate. Delete unused collectors.

If the NetFlow service is still running on the appropriate server, deleting the collector in this resource is temporary. In 15 minutes, the collector will be automatically added again, together with the default port 2055. If you had more or non-default ports defined for the collector, you will need to adjust the default setting.

To permanently delete a collector:

1. Log on to the appropriate server.
2. Uninstall NTA.
3. Delete the collector in the NetFlow Collector Services resource.

To delete a collector in the NetFlow Collector Services resource:

1. Click the **Delete** button next to the collector.
2. Click **Submit** to apply your changes.

For more information about configuring your collectors, see Configuring NetFlow Collector Services Ports in the *SolarWinds NetFlow Traffic Analyzer Administrator Guide*.

Troubleshooting Collector Services

Obvious problems with the NetFlow service are reflected in the Collector Services resource. If your collector service status is down or unknown, you can troubleshoot it using for example the Orion Service Manager.

To troubleshoot a collector service:

1. Start the **Orion Service Manager** in your **SolarWinds Orion > Advanced Features** program folder.
2. Check that the SolarWinds NetFlow Service has the status **Started**.
3. If the SolarWinds NetFlow Service is not started, select it, and click **Start**.

   Note: You can also start the service in the Windows Task Manager or in the Windows Services tool.

4. If the SolarWinds NetFlow Service starts and stops again, there is an underlying reason causing it to fail, such as an issue with the connection to the database (NTA Flow Storage Database or Orion SQL Database). Make sure the connection is working, and that the appropriate database server has sufficient CPU and memory available. For more details see Troubleshooting Remote NTA Flow Storage Installation and the Managing Orion Performance technical reference.
5. As a final attempt to reconcile the SolarWinds NetFlow Service, start the Configuration Wizard in your SolarWinds Orion program folder, select all three components (Database, Website, and Services), and complete the wizard. If it fails, open a ticket with SolarWinds Support.

NetFlow Sources

The NetFlow Sources resource provides a list of flow- and CBQoS-enabled nodes and interfaces that are currently monitored by Orion NPM. For each listed device, the NetFlow Sources resource provides the following details:

- A color-coded device status icon
- An icon indicating the device type or manufacturer
- For each listed source interface, both the incoming and outgoing traffic volumes are reported.
- For all listed flow-enabled devices, a date-time stamp of the last flow packet received by the NTA collector.
- For all listed CBQoS-enabled devices, a date-time stamp of the last CBQoS poll completed by the NTA collector.

Troubleshooting NetFlow Sources

Devices not listed in the resource

If you are not seeing expected flow- or CBQoS-enabled devices in the NetFlow Sources resource, confirm that the following is true for your flow- and CBQoS-enabled devices:

- Confirm that the automatic addition of NetFlow sources option is enabled on the NetFlow Traffic Analysis Settings view. For more information, see Enabling the Automatic Addition of Flow Sources.
- Flow-enabled nodes and interfaces must be monitored by Orion NPM before they can be recognized in as flow sources in NTA. For more information about adding devices for monitoring by Orion NPM, see Adding flow-enabled Devices and Interfaces.
- Flow-enabled devices must be configured to send flow data to the Orion NPM server on which you have installed NTA. For more information about configuring devices to send flows to NTA, see Device Configuration Examples.
- Confirm that the SolarWinds NetFlow Service has been started in the Windows Services listing. To view a list of services, log on to your NTA server as an administrator, and then click **Start> Administrative Tools> Services**.

Time stamp "never" or not up to date

If the time stamp of the last received NetFlow or CBQoS data is not as expected, click **Manage Sources** to confirm that flow monitoring is enabled for the appropriate device and interfaces. For more information, see Configuring Flow Sources and CBQoS Devices.

Editing the Resource

Click **Manage Sources** to go to the Manage NetFlow Sources page where you can select available flow sources and CBQoS-enabled devices. For more information, see Configuring Flow Sources and CBQoS Devices.

To edit the resource:

1. Click **Edit** to go to the Edit Resource page.
2. Change its title in the **Title** field.
3. Select **Show NetFlow sources** to display NetFlow sources in the resource
4. Select **Show CBQoS sources** to display CBQoS sources in the resource.
5. Click **Submit** to apply your edits in the resource.

NTA Events

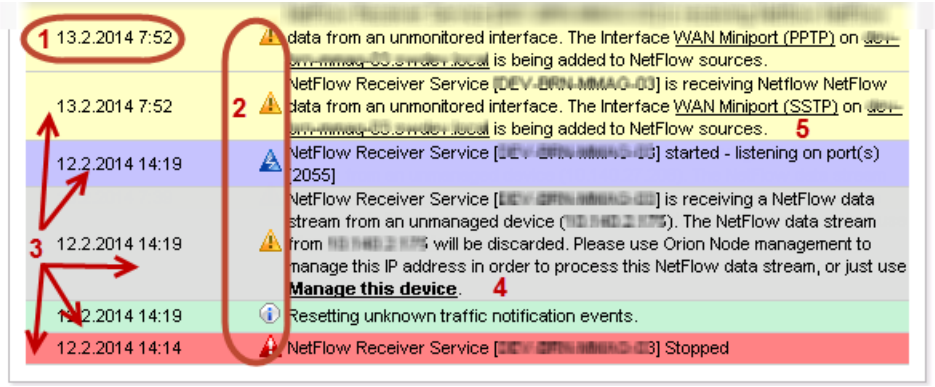
Events are a simple troubleshooting tool giving you an overview of everything important that happens in NTA. If you feel NTA is not showing expected results, consult the **Last 25 Traffic Analyzer Events** and pay attention especially to red and grey events. For more details, see NTA Events List.

What Details Events Provide

Event messages provide the following details:

- The time stamp informs you when the event occurred (**1**).
- Event icons help you distinguish whether it is just an information, warning or an error message (**2**).
- The event color informs you about how serious the event is (**3**).
- The event description includes links that help you solve the situation (**4**), provide troubleshooting information or give more details about objects

relevant for the event (5).



Event Colors

Red events indicate errors that need your immediate attention.

Green events inform you that NTA has successfully completed a task.

Blue events provide system information.

Grey events inform you about a situation that requires an action (unmanaged nodes, interfaces, ...)

Yellow events are informative, you do not need to take any action.

Event Icons

Icon	Message
	Error: this icon informs you that NTA is not working at all and you need to troubleshoot the mentioned issue immediately.
	Warning: NTA warns you about an existing issue which requires an action.
	Information: NTA informs you about an issue that might require assistance, however NTA will continue working even if you disregard this message.
	System information: NTA provides information about system processes, such as database maintenance or NetFlow Receiver Service status changes.
	SolarWinds Licensing: NTA informs you that your NTA has not been licensed yet.

Filtering Events and Displaying Historical Events

You can view your events in the **Last 25 Traffic Analyzer Events** resource which is available on all NetFlow summary views.

If you want to see more than last 25 events or want to display only certain events, you can do so on the Events view.

Note: If you want to see only unknown traffic events, click **NetFlow Settings** on the NetFlow tab, and click **Show unknown traffic events** in the NetFlow Management grouping. For more information about unknown traffic, see Resolving Unknown Traffic.

To filter all events:

1. Open the **Orion Web Console** in the SolarWinds program group.
2. Click **Home > Events**.
3. You can further filter events by:
    a. **Device or a device type:**

        If you want to display only events concerning a certain device or device type, select the device or device type in the appropriate the drop-down list.

    b. **Event type**:

        Select the event type you want to view. If you want to see all events, keep the default All Types option.

        The following table provides event types relevant for NTA events, and the corresponding NTA events.

Event Type	NTA Events
NetFlow Receiver Service Started	NetFlow Receiver Service Started NetFlow Receiver Service settings changed
NetFlow Receiver Service Stopped	NetFlow Receiver Service Stopped License limitation

Event Type	NTA Events
	No valid license
Unmanaged NetFlow Node	Unmanaged NetFlow Node
Unmonitored NetFlow Interface Automatically Added	Unmonitored NetFlow Interface Automatically added
NetFlow Event	NetFlow Event Interface index mapping is being used for node NetFlow Event: Removing interface index mapping for node NetFlow database maintenance Scheduled shrink performed Updating data to be used in Top xx aggregated resources Windows Firewall is turned on
Unmanaged NetFlow Interface	Unmanaged NetFlow interface
Unmonitored NetFlow Interface	Unmonitored NetFlow interface
Invalid Template	Invalid template Invalid IPFIX template
No Template Received	No template received
Not Enabled NetFlow Data Export	Not enabled NetFlow data export
Not Primary NPM Node	Not Primary NPM Node IP Address

Event Type	NTA Events
IP Address	
Notification Reset	Notification Event Status Reset Enough disk space available on NTA Flow Storage disk.
NetFlow Licensing	NetFlow Licensing
Informational	Unable to start listening on port Port is free, listening You are running out of free space on NTA Flow Storage disk.
NetFlow service time difference warning	NetFlow service time difference warning NetFlow service time difference warning ended
NetFlow service time difference error	NetFlow Service time difference error
NetFlow Critical	No space left on NTA Flow Storage disk.

c. **Time period**
   Define the time period when the events were generated.

4. If you want to see even cleared events, select the **Show cleared events** box.
5. If you want to limit the number of items displayed, enter the appropriate number into the box.
6. Click **Refresh**. Events according to your settings will be displayed in the table.

For more information about the Events view, see Viewing Event Details in the Orion Web Console.

Clearing Events

If there are too many events on your Last 200 Unknown Traffic Events view and you have resolved the relevant ones, you can clear the events. Clearing events helps you find out which events have been resolved successfully.

To clear events:

1. Go to the Last 200 Unknown Traffic Events view (**NetFlow Settings > Show unknown traffic events** in the **NetFlow Management** grouping).
2. Click **Clear Notifications**.

   Notes: This will clear events from this view and from the Events view. However, the Last 25 Traffic Analyzer Events resources will still show the last 25 items and will include the following event:

   Notification Event Status Reset

   ```
   "Resetting unknown traffic notifications events."
   ```

3. Click **Refresh Events**. Unresolved events will appear in the Last 200 Unknown Events view again.

   Notes:

   - It might take a few minutes until unresolved events return to the list.
   - Unresolved events return also return to the list if you refresh the page.

Displaying Cleared Events

If you clear your events and later on decide that you would like to consult the cleared events, you can do so in the NPM Events view.

To display resolved events that have been cleared:

1. Go to the **Events** view (**HOME > Events**).
2. Define what events you want to see. For more details, see Filtering Events and Displaying Historical Events.
3. Make sure you have the **Show Cleared Events** box selected.
4. Click **Refresh**.

NetFlow Events List

The following sections list events you can encounter in NTA. Each event is briefly described and provided with steps that help you resolve it or with links leading to more details about the situation triggering the event.

NetFlow Receiver Service Stopped

NTA informs you that SolarWinds NetFlow Service stopped.

```
"NetFlow Receiver Service [service name] Stopped."
```

To resolve the issue, restart the SolarWinds NetFlow Service:

1. Start the **Orion Service Manager** in your SolarWinds Orion > Advanced Features folder.
2. Check the status of the SolarWinds NetFlow Service.
3. If it is stopped, select it and click **Start**.

License Limitation

NTA informs you that your NTA license does not match your NPM license, and NTA thus cannot monitor your flow traffic.

```
"License limitation doesn't fit Orion license!"
```

To resolve this event, make sure your NTA license matches your NPM license. For more information, see Licensing SolarWinds NTA.

No Valid License

NTA informs you that your NTA license is expired.

```
"License status check failed: no valid license were found for
[license key not in brackets]"
```

To resolve this event, log in to the SolarWinds customer portal, and procure an appropriate NTA license.

No Space Left On NTA Flow Storage Database

Triggered when there is less than 1MB free on your NTA Flow Storage Database disk. NTA cannot store flows any more.

```
No space left on your NTA Flow Storage Database disk. You cannot
store flow data any more. » Help
Disk size: xx GB; available space: xx GB.
```

To resolve the issue, consider options provided in the KB article "How to provide more disk space on your NTA Flow Storage Database drive".

Invalid Template

NTA informs you that incoming NetFlow v9 flows have a wrong or invalid template.

```
"NetFlow Receiver Service [xy] received an invalid v9 template with
ID xx from device x.x.x.x. See knowledge base for more
information."
```

To resolve the issue:

1. Log on to the appropriate device and check the template.
2. Make sure the device exports an appropriate template in 1-minute intervals.
3. Make sure the template includes all required details. For more details, see Required fields.

Invalid IPFIX Template

NTA informs you that the IPFIX template does not include required fields.

```
"NetFlow Receiver Service [xy] received an invalid IPFIX template
with ID XX from device x.x.x.x. "
```

To resolve the issue:

1. Log on to the appropriate device and check the template.
2. Make sure the device exports an appropriate template in 1-minute intervals.
3. Make sure the template includes all required details. For more details, see Required fields.

No Template Received

NTA informs you that there is no NetFlow v9 template received for incoming NetFlow v9 traffic.

```
"NetFlow Receiver Service [xy] received NetFlow v9 flows without
any template for decoding them. Configure the device x.x.x.x to
export an appropriate NetFlow v9 template at 1-minute intervals.
See help for details."
```

To resolve the issue:

1. Log on to the appropriate device and check the template.
2. Make sure the device exports an appropriate template in 1-minute intervals.

3. Make sure the template includes all required details. For more details, see Required fields.

Not Enabled NetFlow Data Export

NTA is receiving NetFlow traffic from a wrong interface (restricted or unsupported)

```
"You have not enabled NetFlow data export on the x.x.x.x device.
For more information, see "Enabling NetFlow and NetFlow Data Export
(NDE) on Cisco Catalyst Switches" in the Support-Product
Documentation area of www.solarwinds.com."
```

To resolve the issue, make sure the interface is being managed in NPM and monitored by NTA. For more information, see the technical reference Enabling NetFlow and NetFlow Data Export on Cisco Catalyst Switches.

NetFlow Time Difference Error

This event informs you that the time difference between your servers (Orion SQL Database server, NTA Flow Storage Database, and the NTA Service server) is above the critical threshold. The critical threshold is hard-coded to 300s.

```
"Time on NetFlow Receiver Service [xy] is: xxx. DB server time is
xx. The difference is: 719 s. Which is above critical threshold.
The data won't be correct. Synchronize the clocks and restart the
service."
```

To resolve the issue, synchronize time settings on all servers (Orion SQL Database, NTA polling engine(s), and NTA Flow Storage Database server).

Unmanaged NetFlow Node

This event informs the user that NTA is receiving NetFlow traffic from a node which is not managed in NPM.

```
"NetFlow Receiver Service [xy] is receiving NetFlow data stream
from an unmanaged device (x.x.x.x). The NetFlow data stream from
x.x.x.x will be discarded. Please use Orion Node management to
manage this IP address in order to process this NetFlow data
stream, or just use Manage this device."
```

To resolve the issue, click **Manage this device** and complete the Add node wizard to add the node in NPM. For more information, see Adding Devices for Monitoring in the Web Console in the *Orion Network Performance Monitor Administrator Guide*.

Unmanaged NetFlow Interface

This event informs you that NTA is receiving traffic from an interface which is not managed in NPM. However, the corresponding node is managed in NPM. Click Add this interface or Edit this interface to add the object to NPM for monitoring.

```
"NetFlow Receiver Service [xy] is receiving NetFlow data from an
unmanaged interface 'interface1name To interface2name'. Click Add
this interface or Edit this interface to manage interface and
process its flow data."
```

To resolve the event, click **Add this interface** or **Edit this interface** and add the interface to NPM for monitoring. For more information, see Adding Devices for Monitoring in the Web Console in the *Orion Network Performance Monitor Administrator Guide*.

Unmonitored NetFlow Interface

NTA informs you that NTA is receiving flow traffic from an interface, which is managed in NPM, but not monitored in NTA. This happens if the **Enable automatic addition of NetFlow sources** in NTA Settings is disabled.

```
"NetFlow Receiver Service [xy] is receiving NetFlow data from
unmonitored interface if name on node. Click Monitor NetFlow source
or enable the "Automatic addition of NetFlow sources" option on the
Netflow Settings page to process future NetFlow data from this
interface."
```

To resolve the issue:

- Click **Monitor NetFlow Source** and enable monitoring for the interface. For more details, see Adding Flow Sources and CBQoS-Enabled Devices.
- Click **Automatic addition of NetFlow sources** and make sure the **Enable automatic addition of NetFlow sources** option is selected. For more information, see Enabling Automatic Addition of Flow Sources.

Not Primary NPM Node IP Address

This event informs you that the mentioned node has more IP addresses and that the IP address through which flow data are coming is not used for polling purposes.

```
NetFlow Receiver Service [xy] is receiving NetFlow data from an NPM
device name (device IP address) through an IP address that is not
its primary IP address. The NetFlow data will be discarded. Enable
```

```
the Match NetFlow devices also by not primary IP Address option to
process NetFlow data from this device.
```

To resolve the issue, follow the link to NetFlow Settings and make sure the **Allow matching nodes by another IP Address** option is selected. For more information, see Enabling Flow Monitoring from Unmanaged Interfaces.

Running Out Of Space NTA Flow Storage Database

Triggered when there is less than 5% free space on your NTA Flow Storage Database disk.

```
You are running out of disk space on your NTA Flow Storage Database
disk. » Help
Disk size: xx GB; available space: xx GB.
```

To resolve the issue, provide more free space, or optimize the amount of flows stored in the NTA Flow Storage Database.

For more information about providing more free space for your NTA Flow Storage Database, see "How to provide more disk space on your NTA Flow Storage Database drive".

For more information about optimizing the amount of flows stored in the database, see Setting Retention Period for NTA Flow Storage Database.

Unmonitored Interface Automatically Added

NTA informs you that an unmonitored interface has been added into NTA sources automatically. This happens if you enabled the **Enable automatic addition of NetFlow sources** option in the NTA Settings. For more details, see Enabling the Automatic Addition of Flow Sources.

```
"NetFlow Receiver Service [xy] is receiving NetFlow data from an
unmonitored interface. The interface if name on service is being
added to NetFlow sources."
```

NetFlow Time Difference Warning

This event informs you that there is a time difference between your database and NTA servers, but it does not exceed the critical threshold.

```
"Time on NetFlow Receiver Service [xy] is: xxx. DB server time is
xx. The difference is: xxx s. Which is above threshold. Fetched
data could be unreliable."
```

To prevent corrupt data, synchronize time settings on all servers (Orion SQL Database, NTA polling engine(s), and NTA Flow Storage Database server).

NetFlow Time Difference Warning Ended

This event informs you that the time difference between the database server and NTA server has been resolved and the server times have been synchronized.

```
"Time on NetFlow Receiver Service [xy] is: xx, DB server time is:
xx. The difference is: 0s. Which is under warning threshold"
```

NetFlow Receiver Service Started

NTA informs you that the NTA service has been started. This event is triggered when the SolarWinds NetFlow Service starts.

```
"NetFlow Receiver Service [service name] started - listening on
port(s) [port number(s)]."
```

NetFlow Receiver Service Settings Changed

NTA informs you if the port it is listening on has changed, or if a new port has been added. For more information, see NetFlow Collector Services.

```
"NetFlow Receiver Service [service name] setting was changed -
listening on port(s) [port number(s)]."
```

NetFlow Event: Interface Index Mapping Used for A Node

NTA informs you that a new device using interface index mapping has been added for monitoring in NTA.

```
Interface index mapping is being used for node [node name].
```

SNMP index is a value identifying a specific interface. Flows coming from this device are using different values than SNMP interface indexes and NTA thus needs to establish a relation between the interface index and the values included in these flows.

NetFlow Event: Removing Interface Index For A Node

NTA informs you that interface index mapping has been removed for a node.

```
Removing interface index mapping for node [node name].
```

For more information, see NetFlow Event Interface Index Mapping Used for a Node.

NetFlow Database Maintenance

NTA informs you that the database maintenance has been completed.

```
NetFlow Database Maintenance: Deleted x expired endpoints in x.xx
seconds.
```

For more information, see Database Maintenance.

Scheduled Shrink Performed

NTA informs you that the database has been compressed.

`Scheduled shrink performed. DB size before shrink xMB, DB size after shrink xMB, released space xMB.` For more information, see Database Maintenance.

Updating Data To Be Used In Top XX Aggregated Resources

NTA informs you that data aggregation settings for Top XX applications, Top XX Conversations or Top XX Endpoints has been changed.

`Updating data to be used in showing Top [x] [Conversations, Applications, or Endpoints].`

Note: This event only occurs in NTA 4.0 using SQL for storing flows and in newer NTA versions. For more information, see Adjusting Data Aggregation Settings.

Windows Firewall Is Turned On

NTA informs you that the NTA service has started or restarted and it is blocked by a firewall.

`"Windows FireWall is turned on and its current exceptions do not allow the NetFlow Service to receive packets. Run the Configuration Wizard for Services to remedy."`

To resolve the issue, complete the Configuration Wizard for Services:

1. Start the **Configuration Wizard** in your SolarWinds Orion > Configuration and Auto-Discovery program folder.
2. Select Services and complete the wizard. For more information, see Completing the Configuration Wizard.

You can also consider adding an exception to your firewall settings.

NetFlow Licensing

NTA informs you that you are running an evaluation version of NTA, which has not been licensed yet.

`Your SolarWinds NetFlow Receiver Service Evaluation [receiver name] will expire in x days. Please contact SolarWinds support to purchase a licensed version. Thank you.`

To resolve the issue, purchase a license and activate it. For more information, see Managing Software Licenses.

Unable To Start Listening On Port

NTA informs you that the port NTA is listening at is being used by another listener. NTA cannot collect flows.

```
Unable to start listening on port x. Waiting until the port is
free.
```

To resolve the issue:

1. Log on to the device and check what applications use the port NTA is using (port 2055 by default).
2. If the port is being used by another application, switch the application off.
3. If the port is being used only by the SolarWinds NetFlow Service, restart the service:
    a. Start the **Orion Service Manager** in your SolarWinds Orion > Advanced Features folder.
    b. Check the status of the SolarWinds NetFlow Service.
    c. If it is stopped, select it and click **Start**.

Port Is Free Listening

NTA informs you that the port NTA is listening at is free again, and that the issue has been resolved.

```
Port x is free, listening.
```

Notification Event Status Reset

NTA informs you that you have reset the Last 200 Events view by clicking the **Clear Notification** button.

```
"Resetting unknown traffic notifications events."
```

For more information about seeing cleared events, see Filtering Events and Displaying Historical Events.

Enough Space Available On NTA Flow Storage Database

This event is triggered after the lack of free space on your NTA Flow Storage Database is resolved.

```
You have enough free space available on your NTA Flow Storage
Database disk now.
Disk size: xx GB; available space: xx GB.
```

Resolving Unknown Traffic

If your devices export flows to the NTA receiver, but are not managed in NPM, or are not configured for monitoring in NTA, NTA cannot process the exported information. NTA informs you that it is receiving **unknown traffic** by displaying a message in the yellow information banner at the top of your NTA views.

Unknown traffic can be viewed either as individual events within the Last 25 Traffic Analysis Events resource or on the Last 200 Unknown Traffic Events view.

Unknown traffic can include traffic from unmanaged devices, unmonitored or unmanageable interfaces. The following sections introduce different unknown traffic types:

Traffic from unmanaged nodes or interfaces

Unmanaged objects are nodes or interfaces that are not managed in NPM. The devices export flows, but NTA cannot access the necessary data stored in the Orion SQL Database. You need to add these nodes and interfaces to NPM first. For more information, see Adding Flow-Enabled Devices and Interfaces.

Traffic from unmonitored interfaces

Unmonitored interfaces are interfaces managed in NPM, but not monitored by NTA. Traffic data from them are collected, but you cannot see them in NTA until you enable monitoring for them. For more information about monitoring flow- and CBQoS-sources in NTA, see Configuring Flow Sources and CBQoS Devices.

Traffic from unmonitored interfaces appears in NTA mainly if flow sources are not being added to NTA automatically. For more details, see Enabling the Automatic Addition of Flow Sources.

Traffic from unmanageable interfaces

Unmanageable interfaces cannot be monitored using SNMP. However, we can receive traffic from these interfaces. NPM does not poll data for these nodes via SNMP, the nodes are only "registered" there and flows from these can be processed by NTA. However, to monitor these data in NTA, you have to add the interface for monitoring to NTA, and provide the interface speed. For more information, see Enabling Flow Monitoring from Unmanageable Interfaces.

Note: If you cannot see an unknown traffic event concerning a device which should be exporting NetFlow, log on to the device and check the configuration. Make sure the device sends data to the appropriate port (default 2055).

To resolve unknown traffic events:

1. Go to the Last 200 Unknown Traffic Events view:
   a. Open the **Orion Web Console** in the SolarWinds program group.
   b. Log in using a **User ID** with administrative privileges.
   c. Click **NETFLOW** on the tool bar.
   d. Check the yellow banner area below the tool bar. If there are unknown traffic events, go to the Last 200 Unknown Traffic Events view:

      If you see the message Show unknown traffic events there, click that message.

      If there is no such message, then you currently have no unknown traffic events.

      Note: If you cannot see the banner area, click **NetFlow Settings** and click **Show unknown traffic events** in the NetFlow Management area.

2. The Last 200 Unknown Traffic Events page opens. The page lists last 200 NTA-related events, including those in which flow traffic was received but was not associated with a NetFlow source.

3. Resolve individual events. For more information, see instructions for appropriate events:

   Unmanaged NetFlow Node

   Unmanaged NetFlow Interface

   Unmonitored NetFlow Interface Automatically added

   Unmonitored NetFlow Interface

   Not Primary NPM Node IP Address

To test whether the events have been resolved successfully:

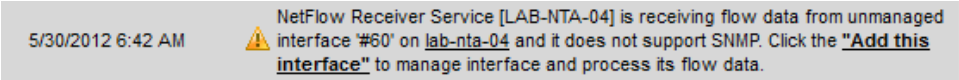
1. Go to the Last 200 Unknown Traffic Events view.
2. Click **CLEAR NOTIFICATIONS** to clear the list, and then click **REFRESH EVENTS**.

New events will be added to the list, and unknown traffic events will return to the list if they have not been successfully resolved.

Note: You can also test resolving unknown traffic events by clicking **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 to resolve unknown traffic.

Enabling Flow Monitoring from Unmanageable Interfaces

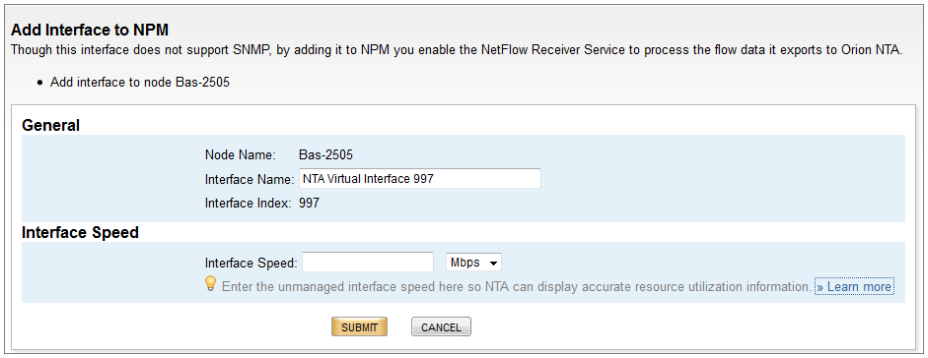
When NTA receives a data flow from an unmanageable interface, it displays an event in NTA Traffic Analyzer pane, such as on the following image.



Though this interface does not support SNMP, you can "register" it to NPM, and thus enable the NetFlow Receiver Service to process the flow data it exports to NTA. If the interface is not in NPM, 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.



2. ***If you wish to edit the interface name***, edit the name for the interface in the **Interface Name** field.
3. Define the **Interface Speed**:
    a. Refer to your device administration documentation for the correct interface speed, and enter it into the appropriate field.

b. Select the speed type from the pull-down menu.

4. Click **SUBMIT**. The interface has been added to NPM and can be viewed in NPM's Node Management page.

Unamanageable Interface Monitored in NTA

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

- ***If NTA has been configured to automatically add NetFlow sources***, it automatically adds the NetFlow source. NTA displays an event that says the source has been automatically added to NTA. You can see the source in the NetFlow Sources view now.
- ***If NTA has not been configured to automatically add NetFlow sources***, it does not add the NetFlow source. 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. If you want to monitor this interface, you need to manually enable its monitoring in NTA. For more information, see Configuring Flow Sources and CBQoS Devices.

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

Unmanageable Interface Speed

You must enter the speed for unmanageable interfaces. Unlike managed interfaces that NPM recognizes, 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.

NTA uses the unmanaged interface speed to determine the percentage of resource utilization, as seen below.

Entering an accurate interface speed ensures the correct display of NTA resources. With this information, you can determine the most efficient use of resources.

Chapter 7: NetFlow Traffic Analyzer Reports

In NTA 4.0 on 64-bit operating systems, flow data are stored in the NTA Flow Storage Database and CBQoS data are stored in the Orion SQL Database. Over time, both databases accumulate a great deal of information. SolarWinds offers both a broad array of predefined reports and user interfaces that enable you to create your own custom reports.

The reports interfaces include powerful tools to help you format your information and easily preview your reports before you display them. When you have finished editing your reports, you can view and then print them with the click of a button.

The following sections provide detailed information related to creating, viewing, and managing SolarWinds reports:

- Reports in NTA 4.0
- NetFlow-Specific Predefined Reports
- Executing Reports
- Creating Web-Based NTA Reports
- Creating Web-Based NTA Reports using SWQL
- Editing Web-Based Reports
- Example: Top 5 destinations, sources, protocols and ports for a specific conversation in past 7 days (creating an obsolete Report Writer report as a web-based report)

Reports in NTA 4.0

There are two report types – web-based reports and Report Writer reports. NTA is transitioning from the old Report Writer reports to the new, web-based reporting system. In one of the future versions, NTA will be using web-based reports only.

You can find and execute all reports in the Orion Web Console. The way you can create, edit, and delete your reports depends on the type of individual reports:

- Report Writer Reports
- Web-Based Reports

Note: SQL views, such as **dbo.NetFlowApplicationSummary**, used for pulling information on applications, conversations, or endpoints are not supported any more. To get a report showing the information, edit an appropriate historical NetFlow report - Top 100 Applications, Top 100 Conversations, or Top 50 Endpoints. For more information, see Historical NetFlow Reports and Creating Web-Based Reports for NTA.

Managing Reports

- If you want to manage **Report Writer reports**, see Using Report Writer in the *Orion Network Performance Monitor Administrator Guide*.
- If you want to create web-based reports, see Creating reports in the *Orion Network Performance Monitor Administrator Guide*.
- If you want to create web-based reports for NTA, see Creating Web-Based NTA Reports.

  Note: You cannot use NTA resources to provide data for your web-based reports.

- If you want to edit an NTA web-based report, see Editing Web-Based NTA Reports.
- If you want to edit a Report Writer NTA report in the Orion Web Console, see Using Customized Report Writer Reports in the Orion Web Console.

Printing Reports

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 *Orion Network Performance Monitor Administrator Guide*.

Scheduling Reports

To schedule automatic email reports for individual users or groups of users, start the Orion Report Scheduler in the Orion program folder. For more information, see

Using Orion Report Scheduler in the *Orion Network Performance Monitor Administrator Guide*.

Using Custom Properties for Creating Reports

NetFlow and NPM reporting 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*.

Report Writer Reports

Originally, all activities related to creating, editing or deleting reports were done in the special SolarWinds tool designed for reports management, in the Report Writer. It provides features allowing you to flexibly design almost any report you might need.

However, the Report Writer was designed to work with data stored in the Orion SQL Database, and thus cannot be used to display flow data from the NTA Flow Storage Database.

To find out more about creating, editing or deleting Report Writer reports, see Using Report Writer in the *Orion Network Performance Monitor Administrator Guide*.

CBQoS Reports

Reports displaying CBQoS data are created, edited or deleted in the Report Writer. CBQoS data are stored in the Orion SQL Database, for which the Report Writer was implemented.

NetFlow Reports in NTA 4.0 on 32-bit operating systems

NTA 4.0 on 32-bit operating systems does not support web-based reporting, and all reports are available as Report Writer reports only. Please consider transferring your NTA 4.0 to a 64-bit operating system.

Web-Based Reports

NPM 10.6 has introduced the new reporting – a way of doing all reports-related tasks directly in the Orion Web Console. NTA transferred all reports displaying NetFlow data from the new NTA Flow Storage Database to the web interface.

NetFlow Reports

In NTA 4.0 with NTA Flow Storage Database, reports displaying NetFlow data are available only as **web-based reports**. NetFlow data are stored in

the NTA Flow Storage Database which cannot communicate with the Report Writer.

If you want to manage web-based reports, you need to do so directly in the Orion Web Console:

Click **Manage Reports** on the All Reports page to access the Manage Reports page where you can create new web-based reports, and edit or delete existing web-based reports. For more information, see Creating and Viewing Reports - Core in the *Orion Network Performance Monitor Administrator Guide*.

Using Customized Report Writer Reports in the Orion Web Console

If you had customized your NetFlow reports in your previous installation and want to use them as web-based reports in NTA 4.0, you need to re-create them manually.

To re-create Report Writer Reports as web-based reports:

1. Go to the **All Reports** page in the Orion Web Console (HOME > Reports).
2. Select **Report Category** in the **Group by** list.
3. Click **Historical NetFlow Reports** (Obsolete, please re-create).

   Note: This category is available only if you have upgraded to NTA from an older NTA version.

4. Open obsolete reports as a reference so that you can re-create the appropriate web-based report:
   a. Start the **Report Writer** in the SolarWinds Orion program folder.
   b. Open the customized report you want to re-create for web-based reporting to see the report settings.
5. Go back to reports in your Orion Web Console and create a new web-based report using the same settings as the original Report Writer report.

   For more information about creating web-based reports, see Creating Reports in the Web Console in the *Orion Network Performance Monitor Administrator Guide*.

   For more information about working with the Report Writer, see Using Report Writer in the *Orion Network Performance Monitor Administrator Guide*.

For an example workflow how to recreate a report showing top 5 sources, destinations, protocols and ports for a specified conversation, see Creating Report Writer Reports as Web-Based.

NetFlow-Specific Predefined Reports

Several standard NetFlow-specific reports are immediately available with your NetFlow Traffic Analyzer installation. You can modify them or create new reports as necessary.

In addition, as an Orion module, NTA can also generate any of the predefined reports packaged with NPM. For more information, see Predefined Orion Reports in the *Orion Network Performance Monitor Administrator Guide*.

To access NTA-specific predefined reports:

1. Log on into your Orion Web Console and click **Home > Reports**.
2. Select **Report Category** in the **Group by** list and select an appropriate Report Category. NetFlow-specific reports are grouped into following categories:
    - Historical NetFlow Reports
    - Historical CBQoS Reports

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

Historical NetFlow Reports

These reports are web-based; you can view and edit them directly in your Orion Web Console. For more information about creating and modifying web-based reports, see Creating Reports in the Web Console in the *Orion Network Performance Monitor Administrator Guide*.

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 destination, 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 endpoints, flow source and destination, protocol name, port number used, application name, ToS 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, 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, 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, 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, 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, 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, the node name, 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, the node name, data received by the endpoint (in bytes and packets), data transmitted by the endpoint (in bytes and packets), total data (in bytes and packets).

Top 50 Receivers – Last 24 Hours

Displays the full hostname, if available, IP address, 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, 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

You can display these reports directly in the Orion Web Console. If you want to modify them, you need to go to the Orion Report Writer. For more information, see Using Report Writer in the *Orion Network Performance Monitor Administrator Guide*.

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 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 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 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.

Executing Reports

You can view all your reports, both Report Writer and web-based reports, in the Orion Web Console. You can execute the reports there and export them to a .pdf file.

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 *Orion Network Performance Monitor Administrator Guide*.

To execute a report:

1. Log on to your **Orion Web Console**.
2. Click **HOME > Reports**.
3. Find the appropriate NTA Report:
    - Select the appropriate grouping criteria in the **Group by** list.

      Note: To find Historical NetFlow web-based reports, select **Product > Custom**, or **Report Category > Historical NetFlow Report**,

      or

- Type the report name or a string included in it into the **Search**.

4. Click the report to execute it.

   Note: You can also export the displayed report to PDF. To do so, click **Export to PDF** in the top right corner of the report.

Creating Web-Based Reports for NTA

Before you start defining a brand new web-based report, take a look at predefined reports. Consider whether you could not use an already available report, only adjusting some properties or time frame used.

To create a NTA web-based report:

1. Log in to your Orion Web Console.
2. Go to **HOME > Reports** and click **Manage Reports**.
3. Click **Create New Report**.

   Note: If you intend to adjust an existing report, select it and click **Duplicate & Edit**. For more information, see "Creating Reports in the Web Console" in the SolarWinds technical reference Web-Based Reports.
4. Select the form. For NTA, only **Custom Table** is supported.
5. Define the object to report on. For NTA, use one of the following objects.

   NTA Relevant objects

   - NetFlow Flow History
   - NetFlow Flow by Autonomous System History
   - NetFlow Flow by Conversation History
   - NetFlow Flow by Country Code History
   - NetFlow Flow by Domain History
   - NetFlow Flow by Hostname History
   - NetFlow Flow by IP History

For more details about the other selection methods, see Adding a Custom Table to a Web-Based Report Column in the *Orion Network Performance Monitor Administrator Guide*.

6. Define what the custom table should show in the resulting report, select properties and sorting of items:
    a. Add appropriate columns.
    b. To edit information provided by individual columns, click **Advanced** in the appropriate column. You can define display settings, data aggregation and alignment for individual columns here.
    c. Define sorting of items in the report (**Sort results by**).
    d. If necessary, define grouping of data (**Group results by**).
    e. If you want to limit the number of items on the report, go to the **Filter results** section and select the appropriate option (all, limit items by number or percent).

       Note: The **Time-based settings** area allows you to change the **Sample Interval** used for filtering or summarizing data by time period. The defined table must contain at least one column with historical data so that you can filter the data. This is why the **Timestamp** column is automatically added; by default, the column is hidden, as demonstrated by the icon.

    f. Click PREVIEW RESOURCE, review the preview, and click **OK** to close the pop-up preview.
    g. If you are contented with the preview, click **SUBMIT** to continue with the report definition in the Add Report Wizard.
7. Complete the Add Report Wizard.
    a. Define the layout (report header, content, page layout, and footer) and time period shown by the report.
    b. Preview the report.
    c. Fill in the report properties (description, report category, custom properties,or limit the access to the report). For more information, see Creating Custom Properties or Setting Account Limitations in the *Orion Core Administrator Guide.*

d. Schedule the report if necessary. For more information, see "Scheduling a Web-Based Report" in the Orion Common Components Guide.

e. Click **SUBMIT** to add the report into the Manage Reports list.

For more information about creating web-based reports, see the SolarWinds Orion Web-Based Reports technical reference or Creating a New Web-Based Report in the Network Performance Monitor webhelp.

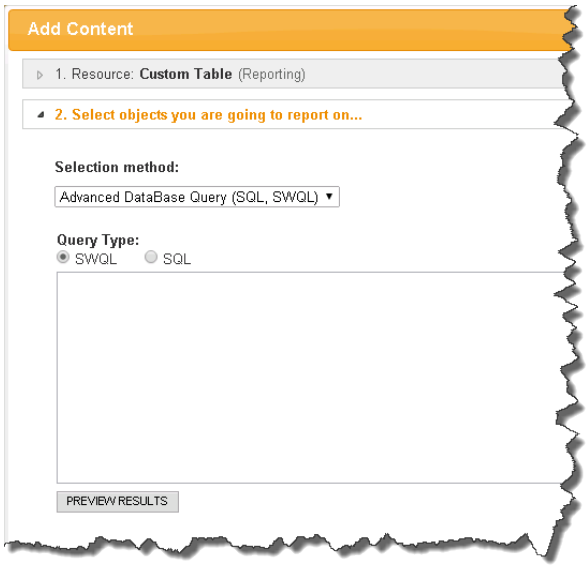
Creating Web-Based Reports Using SWQL

Web-Based reports provide you with the option to define the objects you want to report on using the semantic web query language.

Semantic Web Query Language (SWQL) is a proprietary, read-only subset of SQL. Similar to SQL, you can use SWQL to query your SolarWinds database for specific network information.

1. Log in to your Orion Web Console.
2. Go to **HOME > Reports** and click **Manage Reports**.
3. Click **Create New Report**.
4. Select **Custom Table** and click **SELECT AND CONTINUE**.
5. Define what objects you want to query:

    a. Now in the Select objects you want to report on, go to the **Selection method** drop-down list and select **Advanced DataBase Query (SQL, SWQL)**.



b. Select **SWQL** as the **Query Type** and enter the code.

   For more information about the SWQL supported by Orion, see the SolarWinds KB article How to use SWQL or consult the section "Using SWQL" in the SolarWinds Network Performance Monitor webhelp.

   If you need to find out table and fields names in your database, you can use the Orion Software Development Kit (SDK) API, available in the Orion SDK forum on thwack.com.

Logging in Orion SDK

- Download and install SDK on the same server as you run your NTA. For more information about downloading and beginning to use the Orion SDK, see the post, "Orion SDK Information" in the Orion SDK forum on thwack.com.
- Start the **SWQL Studio** in your program folder.
- Fill in details necessary for connecting to the SolarWinds Information Service:

  Server Name: localhost

  Server Type: Orion (v3)

  User Name and **Password**: Use the same credentials that you use for logging in NTA.

6. Define columns that will present the data gathered by your SWQL query, and click **SUBMIT**.
7. Add the report to your reports.
   a. Define the report layout, preview the report, and define the report properties.
   b. Click **SUBMIT** to add the report.

For more information about creating web-based reports, see the SolarWinds Orion Web-Based Reports technical reference.

Editing Web-Based Reports

This section provides details on the most usual edits in reports:

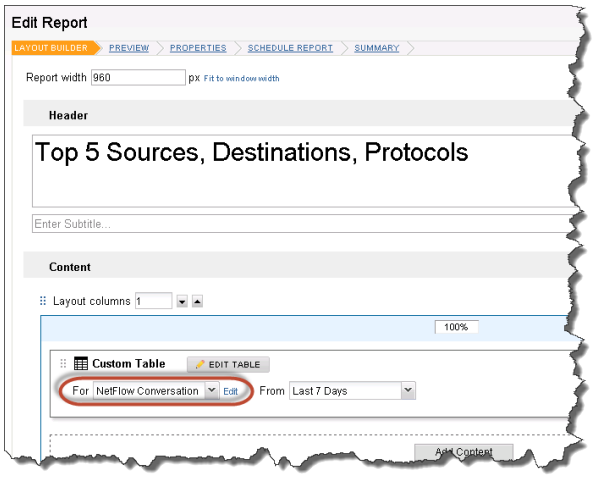
Changing Objects That Are Being Reported On

You might need to change some of the conditions used to define objects for your reports, such as an IP address, or add a protocol you want to report on.

To change the object of a report:

1. Go to the **Manage Reports** page.
   a. Select **Home > Reports** in the Menu Bar.
   b. Click **Manage Reports**.

2. Select the appropriate report and click **Edit** or **Duplicate&Edit** if you want to edit a copy of the report and retain the original.
   Note: To find historical NetFlow reports, select **Product > Custom**, or **Report Category > Historical NetFlow Reports** in the **Group by** list.
3. Now on the Edit Report view in the Layout Builder tab, click **Edit** next to the **For** drop down list.



4. Change the objects for the report on the Add content popup window and click **ADD TO LAYOUT**. For more information, see "Selecting Monitored Objects for Custom Chart and Table Resources" in the SolarWinds Technical Reference Orion Web-Based Reports.
5. Complete the wizard.

   Note: You can either use the **NEXT** buttons or click the Summary tab to switch directly to the last Wizard screen. Click **SUBMIT** to apply your changes.

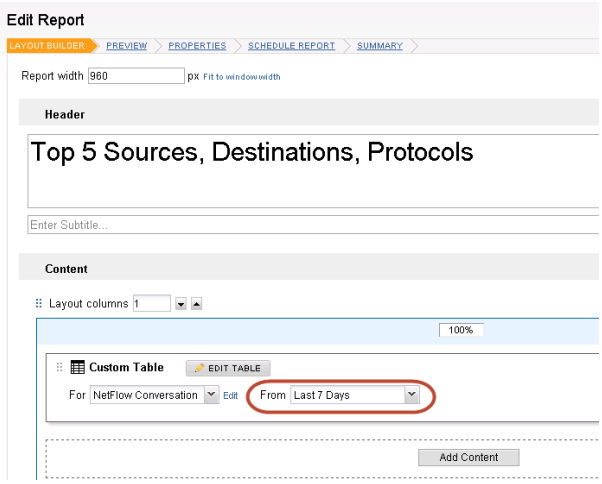
Changing Time of the Report

You might need to extend or shorten the time interval you want to report on.

To change the time period:

1. Go to the **Manage Reports** page.
   a. Select **Home > Reports** in the Menu Bar.
   b. Click **Manage Reports**.

2. Select the appropriate report and click **Edit** or **Duplicate&Edit** if you want to edit a copy of the report and retain the original.
   Note: To find historical NetFlow reports, select **Product > Custom**, or **Report Category > Historical NetFlow Reports** in the **Group by** list.
3. Now on the Edit Report view in the Layout Builder tab, select the appropriate time period in the **From** drop down list.



   Note: You can either use a predefined time period, such as past hour, last 24 hours, last 30 days, or define a customized time period for your report (see the following question).

4. Complete the wizard.

   Note: You can either use the **NEXT** buttons or click the Summary tab to switch directly to the last Wizard screen. Click **SUBMIT** to apply your changes.

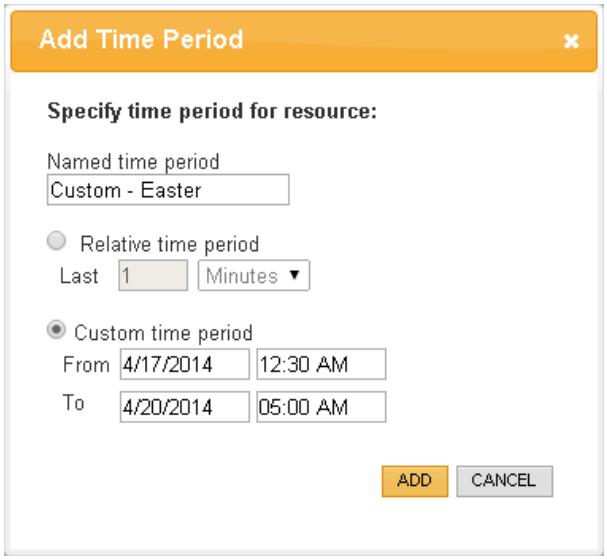
Defining Customized Time for Reports

If you have not found the appropriate time period you want to report on among predefined items, you can customize it yourself.

Note: Web-based reports only support uninterrupted time intervals, it is thus not possible to report on repeated time periods, such as the peak hours traffic in a specified week, or report on all working days in a month.

To define customized time:

1. Go to the **Manage Reports** page.
    a. Select **Home > Reports** in the Menu Bar.
    b. Click **Manage Reports**.
2. Select the appropriate report and click **Edit** or **Duplicate&Edit** if you want to edit a copy of the report and retain the original.
   Note: To find historical NetFlow reports, select **Product > Custom**, or **Report Category > Historical NetFlow Reports** in the **Group by** list.
3. Now on the Edit Report view in the Layout Builder tab, go to the **From** drop down list.
4. Scroll down in the list and select the **Custom**... item.



5. Now in the Add Time Period pop-up window, provide a name for the customized time period in the **Named time period** field. This name will be used in the **For** list.
6. Specify the time period:
    a. If you want to add a specified historical period from past to now, select **Relative time period**.
        - Provide a value and units (minutes, hours, days, weeks, months, or years) to define how far into past you want to go.

b. If you want to add a limited time in the past, not related to present, select **Custom time period**.
   - Specify the start date and time in the **From** boxes.
   - Specify the end date and time in the **To** boxes.

7. Click **ADD** to add the defined time period to the **For** list.
8. Select the new customized time period in the **From** list.
9. Complete the wizard.

   Note: You can either use the **NEXT** buttons or click the Summary tab to switch directly to the last Wizard screen. Click **SUBMIT** to apply your changes.

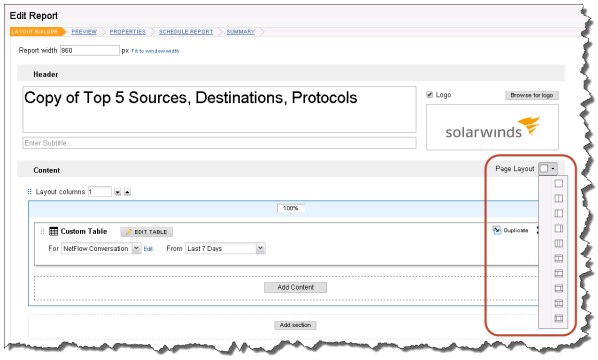
Changing Page Layout

You can change a report layout so that you have two or more data sources next to each other to simplify comparing the values.

To change page layout:

1. Go to the **Manage Reports** page.
   a. Select **Home > Reports** in the Menu Bar.
   b. Click **Manage Reports**.
2. Select the appropriate report and click **Edit** or **Duplicate&Edit** if you want to edit a copy of the report and retain the original.
   Note: To find historical NetFlow reports, select **Product > Custom**, or **Report Category > Historical NetFlow Reports** in the **Group by** list.
3. Now on the Edit Report view in the Layout Builder tab, click the **Page**

Layout button and select the appropriate layout in the list.



4. Complete the wizard.

   Note: You can either use the **NEXT** buttons or click the Summary tab to switch directly to the last Wizard screen. Click **SUBMIT** to apply your changes.

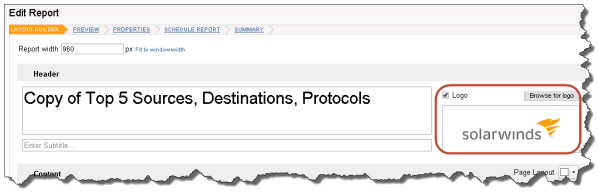
Changing Logo on a Report

You might need to replace the default SolarWinds logo with your company's logo.

Note: The provided space allows for maximum height of 103px and maximum width of 238px. Larger images will be adjusted accordingly to fit in the space.

To change the logo:

1. Go to the **Manage Reports** page.
   a. Select **Home > Reports** in the Menu Bar.
   b. Click **Manage Reports**.
2. Select the appropriate report and click **Edit** or **Duplicate&Edit** if you want to edit a copy of the report and retain the original.
   Note: To find historical NetFlow reports, select **Product > Custom**, or **Report Category > Historical NetFlow Reports** in the **Group by** list.
3. Now on the Edit Report view in the Layout Builder tab, make sure the **Logo** box is selected.



4. Click **Browse for logo**, navigate to the requested logo and select it.
5. Complete the wizard.

   Note: You can either use the **NEXT** buttons or click the Summary tab to switch directly to the last Wizard screen. Click **SUBMIT** to apply your changes.

Limiting Access to a Report

You can specify a group of users who can access individual reports.

To limit the access to a report:

1. Go to the **Manage Reports** page.
   a. Select **Home > Reports** in the Menu Bar.
   b. Click **Manage Reports**.
2. Select the appropriate report and click **Edit** or **Duplicate&Edit** if you want to edit a copy of the report and retain the original.
   Note: To find historical NetFlow reports, select **Product > Custom**, or **Report Category > Historical NetFlow Reports** in the **Group by** list.
3. Click Next on the Layout Builder tab.
4. Click Next on the Preview tab.
5. Now on the Properties tab of the Edit Report Wizard, click **Report limitation** and select an appropriate report in the list. For more information, see Setting Account Limitations in the *Orion Core Administrator Guide.*
6. Complete the wizard.

   Note: You can either use the **NEXT** buttons or click the Summary tab to switch directly to the last Wizard screen. Click **SUBMIT** to apply your changes.

Specifying Custom Properties for a Report

You can assign custom properties to your reports to help you manage your reports. For example, you can have a custom property "department" and provide the information for which department is the report used.

To specify custom properties:

1. Go to the **Manage Reports** page.
    a. Select **Home > Reports** in the Menu Bar.
    b. Click **Manage Reports**.
2. Select the appropriate report and click **Edit** or **Duplicate&Edit** if you want to edit a copy of the report and retain the original.
   Note: To find historical NetFlow reports, select **Product > Custom**, or **Report Category > Historical NetFlow Reports** in the **Group by** list.
3. Click on the Properties tab.
4. Fill in values for all required custom properties. For more information, see Creating Custom Properties in the *Orion Core Administrator Guide.*
5. Complete the wizard.

   Note: You can either use the **NEXT** buttons or click the Summary tab to switch directly to the last Wizard screen. Click **SUBMIT** to apply your changes.

Scheduling a Report

You can set the report to run automatically, according to a defined schedule. Generated reports can further be sent to a defined email address.

Note: This procedure expects that you are using SolarWinds NPM 10.7. If you are running an older NPM version, you might notice minor differences while scheduling the report.

To schedule a report:

1. Go to the **Manage Reports** page.
    a. Select **Home > Reports** in the Menu Bar.
    b. Click **Manage Reports**.

2. Select the appropriate report and click **Edit** or **Duplicate&Edit** if you want to edit a copy of the report and retain the original.
   Note: To find historical NetFlow reports, select **Product > Custom**, or **Report Category > Historical NetFlow Reports** in the **Group by** list.
3. Click the Schedule Report tab.
4. Select **Schedule this report to run regularly**.
5. Select the appropriate schedule in the list and click **Assign Schedule**. For more information, see "Scheduling a Web-Based Report" in the Orion Common Components Guide.
6. Complete the wizard.

   Note: You can either use the **NEXT** buttons or click the Summary tab to switch directly to the last Wizard screen. Click **SUBMIT** to apply your changes.

Example: Creating Customized Report Writer Reports as Web-Based

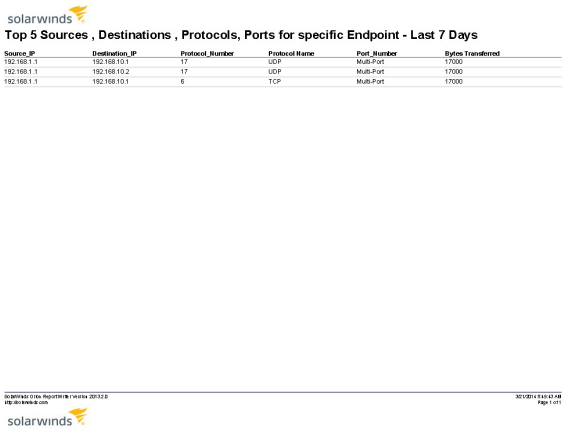
Starting with NTA 4.0, the provided flow reports are web-based only. If you have customized flow reports, you need to create them manually according to appropriate obsolete Report Writer reports.

This section provides instructions how to create a customized Report Writer report showing top 5 sources, destinations, protocols and ports for a specific conversation over the last 7 days as a web-based report.

Notes:

- This procedure expects that you are using SolarWinds NPM 10.7. If you are running an older NPM version, you might notice minor differences while creating the report.
- Take the appropriate obsolete Report Writer report to help you define the

report as web-based, see the image below.



To create an obsolete Report Writer report as web-based:

1. Log in to your Orion Web Console.
2. Go to **HOME > Reports** and click **Manage Reports**.
3. Click **Create New Report**.
4. Open the report which you want to re-create in the Report Writer.
    a. Start the Orion Report Writer in your **SolarWinds Orion > Alerting, Reporting and Mapping** program folder.
    b. Click **Open** and navigate to the appropriate Report Writer report.
5. Define the form used for displaying data in the report: Select **Custom Table** and click **SELECT AND CONTINUE**.
6. Define the object on which you want to report.
7. Define columns for the report table.
8. Add the report to your Orion reports:
    a. Define the report layout:
        - Fill in an appropriate **Report Title** and **Subtitle**.

          Note: You can also change the logo, change the page layout, or define the footer here.
        - Define the time period for including data into the report. To see bytes connected with your IP groups in the past 24 hours, select

Last 24 hours in the **From** list.

Note: To check time settings of the obsolete report, consult an archived version of it or the Time Frame tab in the Report Writer.

- Click **Next** to proceed to the Report preview.

b. Check the preview and click **Next** to continue.

If you are not satisfied with the report layout, click **Back** and adjust the table settings.

c. Define the report properties and click **NEXT**.

- If you want to have the report on the top of your report lists, select **My Favorite Reports**.
- If necessary, update the **Report description**.
- Select the appropriate category for the report in the **Report category** list.
- You can also define custom properties for the report, or add limitations. For more information, see Creating Custom Properties or Setting Account Limitations in the *Orion Core Administrator Guide.*

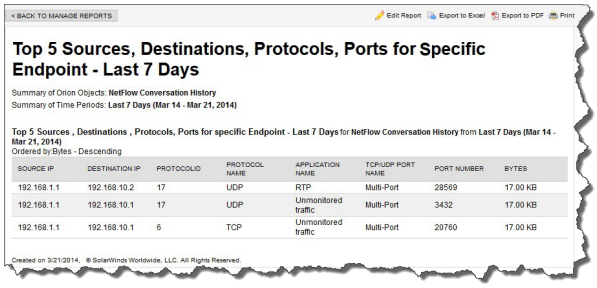
d. If you want to create the report regularly, schedule the report, and click **NEXT**.

To schedule the report, select **Schedule this report to run regularly**, and select an existing schedule in the list. For more information, see "Scheduling a Web-Based Report" in the Orion Common Components Guide.

e. Review the report summary and click **SUBMIT**.

If you want to the report name, properties, time period,or scheduling, click the appropriate **Edit** link. You will return to the appropriate place in the Add Report Wizard.

The resulting report should look as follows:



< BACK TO MANAGE REPORTS

Edit Report Export to Excel Export to PDF Print

Top 5 Sources, Destinations, Protocols, Ports for Specific Endpoint - Last 7 Days

Summary of Orion Objects: **NetFlow Conversation History**
Summary of Time Periods: **Last 7 Days (Mar 14 - Mar 21, 2014)**

Top 5 Sources , Destinations , Protocols, Ports for specific Endpoint - Last 7 Days for **NetFlow Conversation History** from **Last 7 Days (Mar 14 - Mar 21, 2014)**
Ordered by:Bytes - Descending

SOURCE IP	DESTINATION IP	PROTOCOLID	PROTOCOL NAME	APPLICATION NAME	TCP/UDP PORT NAME	PORT NUMBER	BYTES
192.168.1.1	192.168.10.2	17	UDP	RTP	Multi-Port	28569	17.00 KB
192.168.1.1	192.168.10.1	17	UDP	Unmonitored traffic	Multi-Port	3432	17.00 KB
192.168.1.1	192.168.10.1	6	TCP	Unmonitored traffic	Multi-Port	20760	17.00 KB

Created on 3/21/2014, © SolarWinds Worldwide, LLC. All Rights Reserved.

For more information about creating web-based reports, see the SolarWinds Orion Web-Based Reports technical reference or Creating a New Web-Based Report in the Network Performance Monitor webhelp.

Defining the Object to Report On

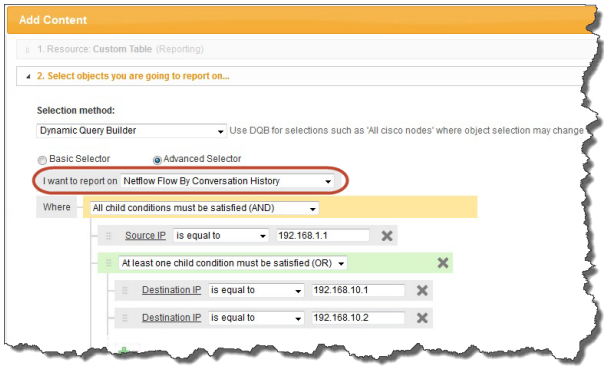
We want to report on top 5 traffic sources, destinations, protocols and ports used by a specified endpoint. We are therefore interested in the endpoint's conversations, and need to specify the endpoint and protocols we are interested in.

To define objects for the report:

1. Select the **Dynamic Query Builder** selection method.
2. Details shown on the report will change over time, so we need to select the objects for the report dynamically. For more details about the other selection methods, see Adding a Custom Table to a Web-Based Report Column in the *Orion Network Performance Monitor Administrator Guide*.
3. Select **Advanced Selector**.
    - **Advanced selector** provides a list of associated objects and allows you to define objects for the report by their properties in a defined relation. You can also create blocks of conditions. We need to define that we want to see all NetFlow Flow By Conversation History objects, specify the appropriate source and destination IP addresses, and protocols we are interested in. We thus need to use the **Advanced selector**. For more details, see the SolarWinds technical reference "Orion Web-Based Reports".
    - **Basic Selector** allows you to create simple conditions. The **Select field** list provides properties of the selected object, and allows you to

select a property, the appropriate relation and a value the resulting objects should or should not have, according to the selected relation.

4. Select **NetFlow Flow By Conversation History** as the object to report on.



5. Define the appropriate source IP address:

   a. Click **Select field**. The Add Column dialog opens.

   b. Make sure **Netflow Flow By Conversation History** is selected in the Orion Object list.

   c. Below this item, select **Netflow Flow By Conversation History**.

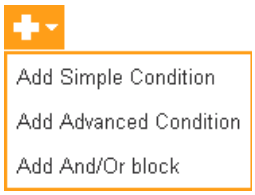
   d. In the Database column name list, select **Source IP**, and click **ADD COLUMN**.

   e. Back in the Add Content screen, go to the **Source IP** property list, select **is equal to**, and enter the appropriate source IP address.

6. Define possible destination IP addresses.

   We want to specify two possible destination IP addresses and that we want to report on conversations whose destination IP is one of those IP addresses.

   a. Click the  icon and select **Add And/Or block**.



   b. Click **Select field**.

c. Now in the **Add Column** screen, make sure you have selected **Netflow Flow By Conversation History** in both the drop-down list and below it.

d. Select **Destination IP** and click **ADD COLUMN**.

e. Back in the Add Content screen, go to the **Destination IP** property list, select **is equal to** and provide an appropriate IP address.

f. Click the  icon and select **Add Simple Condition**.

g. Repeat steps b-e to add the other Destination IP address.

h. Go to the parent drop-down list and select **At least one child condition must be specified (OR)**.

7. Define protocols you want to follow.

   We are interested in application traffic, and we will thus specify that we want to report on traffic connected with UDP and TCP protocols. These protocols are used by applications.

   a. Click the  icon connected with the protocol specification and select **Add And/Or Block**.

   b. Click **Select field**.

   c. Now in the **Add Column** screen, make sure you have selected Netflow Flow By Conversation History the drop-down list.

   d. Select **Netflow Protocol** below the drop-down list.

   e. Select **Protocol Name** and click **ADD COLUMN**.

   f. Back in the **Add Content** screen, go to the **Protocol Name** property list, select **is equal to** and enter **UDT**.

   g. Click the  icon and select **Add Simple Condition**.

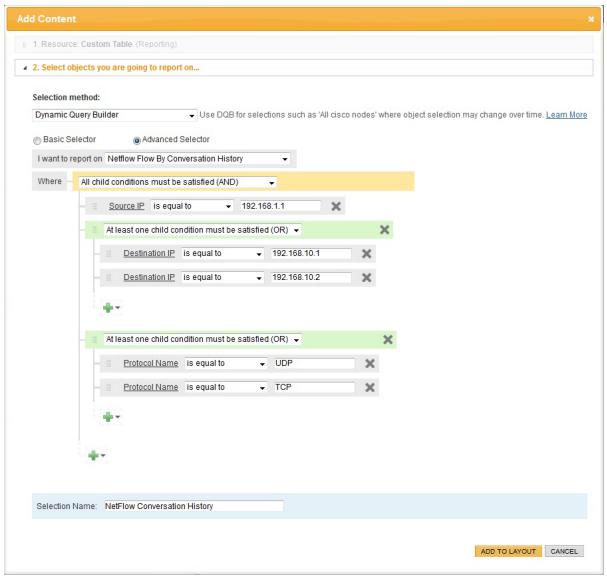
   h. Repeat steps b-e to add the **TCP** Protocol.

   i. Go to the parent drop-down list and select **At least one child condition must be specified (OR)**.

8. Provide a name for the selection in the **Selection Name** field. Selection names are useful when editing reports that consist of more tables or charts.

9. Click **ADD TO LAYOUT**.

   The definition should look like this:



Defining Column Details for the Report

Originally, our report table included six columns: Source IP, Destination IP, Protocol Number, Protocol Name, Port Number, and Bytes Transferred.

To define columns for your customized report:

1. Click **Add column**.

   To find out what columns you used, take a look at your Report Writer report output or go to the Report Writer and activate the Select Fields tab.

2. Add **Source IP**, **Destination IP**, **Protocol ID**, **Port Number** and **Bytes** columns.

   Note: To find out what columns you used, consult an archived Report Writer report or go to the Report Writer and activate the Select Fields tab.

   a. Make sure you have **Netflow Flow By Conversation History** selected both in the drop-down list and below it.

   b. Select **Source IP** in the Database column name area.

   c. Select **Destination IP** in the Database column name area.

d. Select **ProtocolID** in the Database column name area.

e. Select **Bytes** in the Database column name area.

3. Add **Application Name** and **TCP/UDP Port Name** columns.

   a. Make sure **Netflow Flow By Conversation History** is selected in the drop-down list and below it, select **Netflow Application**.

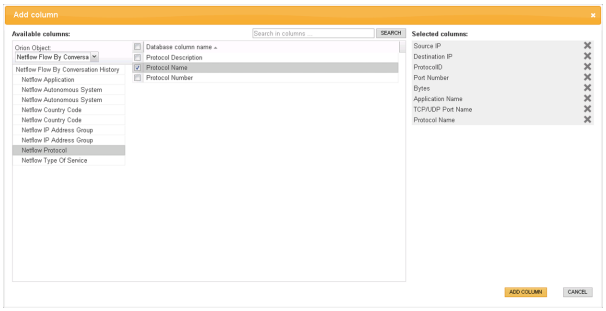
   b. Select **Application Name** and **TCP/UDP Port Name** in the Database column name area.

4. Add the **Protocol Name** column.

   a. Make sure **Netflow Flow By Conversation History** is selected in the drop-down list and below it, select **Netflow Protocol**.

   b. Select **Protocol Name** in the Database column name area.

   The Add column screen with all required columns looks like this:



5. Click **ADD COLUMN** to add selected columns.
6. Drag and Drop the columns to achieve the requested order.
7. Specify units and aggregation of bytes.

   Note: To check aggregation settings in the obsolete report, consult the Select Fields tab in the Report Writer.

   a. Click **Advanced** in the **Bytes** column .

   b. Select **Data Unit** in the **Add display settings** list.

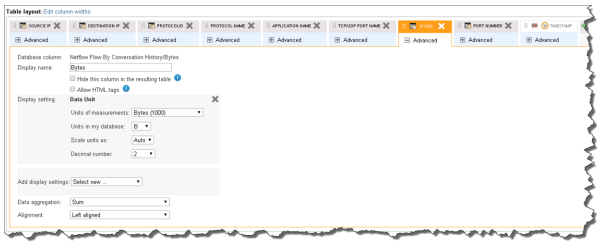
   c. In the **Units of measurements**, select **Bytes (1000)**. This defines the units shown on the report.

   d. In the **Units in my database** list, select **B**.

      Note: Make sure you select correct units used in your database.

Selection of incorrect units results in incorrect data displayed in the report.

e. In the **Data aggregation** list, select **Sum**.



8. If you want to edit the look of a column for the report, click the **Advanced** button next to it. You can adjust for example the column title (Display name), hide the column in the resulting report or add further display settings (icons, units, etc.).

   To find out these details in the Report Writer, activate the Field Formatting tab and review the information provided for individual fields.

9. Define how items should be sorted in the report:

   We would like to have items in the resulting report sorted by the bytes column, the lowest value being first and the highest value being last.

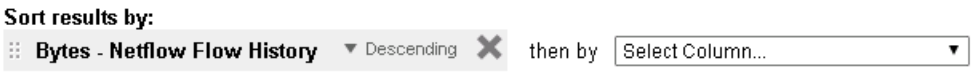
   Note: If you want to check the aggregation settings in the original Report Writer report, go to the Report Writer and consult the Select Fields tab.

   a. Go to the **Sort results by** area.

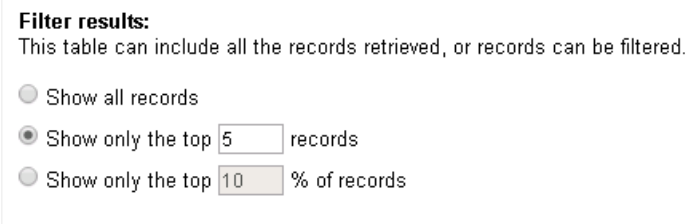
   b. Select the column according to which results should be sorted. For our report, select **Bytes - NetFlow Flow by Conversation History**.

   c. Define the sorting direction. Select **Descending** here.
   Sorting directions:

   - **Ascending**: smallest values are shown first, and the sorting proceeds to highest values.
   - **Descending**: highest values are shown first, and the sorting proceeds to smallest values.



10. Define how many items you want to see in the table.
    a. Go to the **Filter results** area.
    b. Select the **Show only the top** option.
    c. Enter the value **5**.



Note: In the Report Writer, you can find this information in the Top XX tab.

11. Click **PREVIEW REPORT**.

    If there are any columns that you do not want to see in the report, remove them by clicking the appropriate X in the header or hide them:

    a. Click **Advanced** for the appropriate column.
    b. Select the **Hide this column in the resulting table** option.

12. Click **SUBMIT**.

Chapter 8: Using 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 Creating and Managing Alerts in the *Orion Network Performance Monitor Administrator 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.

NetFlow-Specific Predefined Alerts

When you install SolarWinds NetFlow 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 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.

Configuring NetFlow Advanced Alerts

This section describes how you can configure an advanced alert for NTA based on a predefined top talker or CBQoS alert.

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

For steps on creating an advanced alert see the sections on advanced alerts in Creating and Managing Alerts in the *Orion Network Performance Monitor Administrator 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 for the software to launch 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 drop-down 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 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 for the software to reset 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 for the software to suppress the alert.

   The default condition is no suppression.

e. On Time of Day, define the days and times when 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.

   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 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

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

Note: If you want to configure advanced alert features, such as timed alert checking, delayed alert triggering, timed alert resets, or alert suppression, select

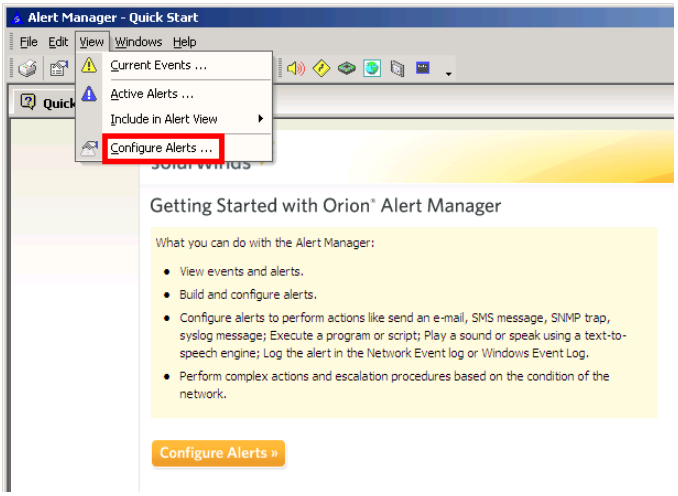
Show Advanced Features at the lower left of any Advanced Alert windows. For the purposes of this document, **Show Advanced Features** is always enabled.

Creating a New Advanced Alert

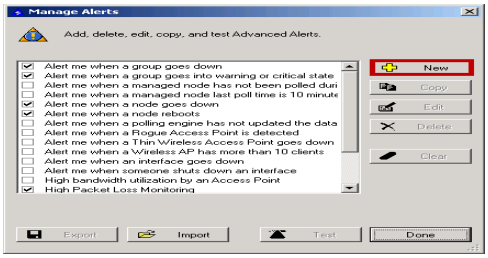
The following procedure creates a new advanced alert.

To create a new advanced alert:

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



3. Click **New**.



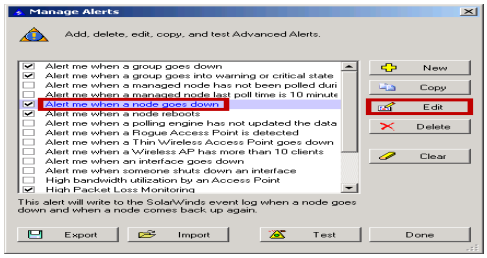
The **Edit Alert** window displays, providing an array of configurable alerting options, including trigger and reset conditions, suppressions, and date and time limitations. The following sections provide more information about configuring alert options.

Naming, Describing, and Enabling an Advanced Alert

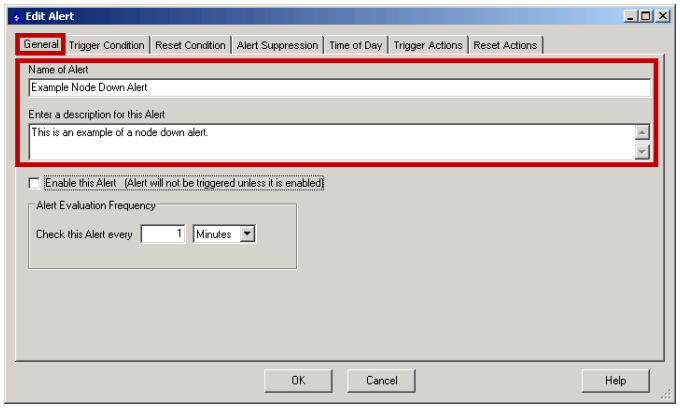
Use the following steps, after clicking New, Copy, or Edit from the Manage Alerts Window, to name and describe an advanced alert.

To name and describe an advanced alert:

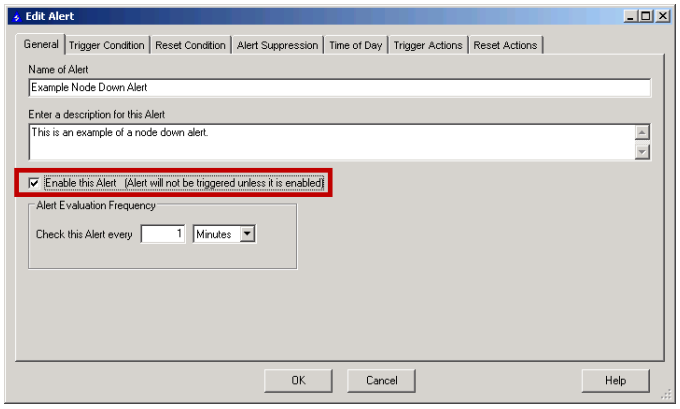
1. Start the **Advanced Alert Manager** in the Orion Alerting, Reporting, and Mapping folder.
2. Click **View > Configure Alerts**.
3. ***If you want to create a new alert***, click **New**.
4. ***If you want to copy or edit an existing alert***, select an alert from the list, and then click **Copy**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



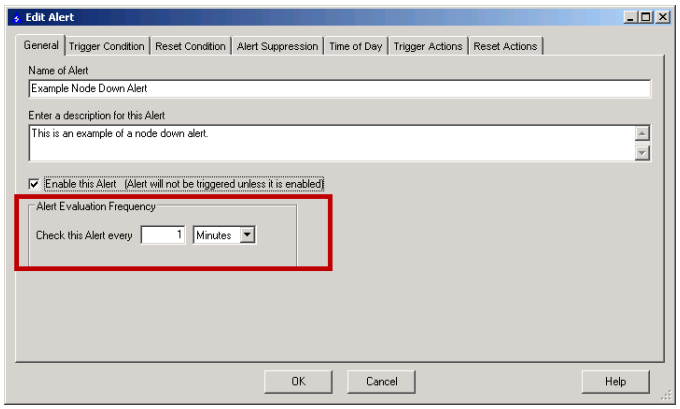
5. Click General, type the name of your alert in the Name of Alert field, and then type a description of your alert in the description field.



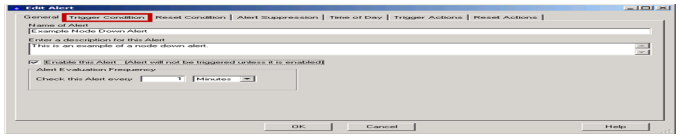
6. Select **Enable this Alert**.



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



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



Setting a Trigger Condition for an Advanced Alert

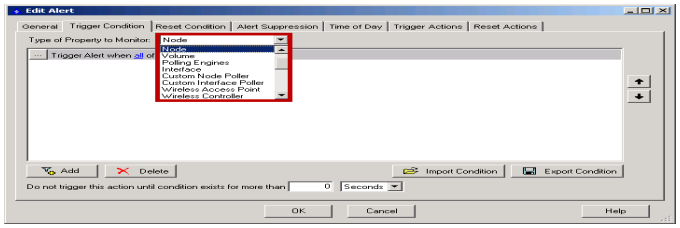
You can set the specific conditions for triggering an advanced alert with the following procedure.

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. Start the **Advanced Alert Manager** in the Orion Alerting, Reporting, and Mapping folder.
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 a Network Performance Monitor installation. Other modules will look similar, but different objects may be present.



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.

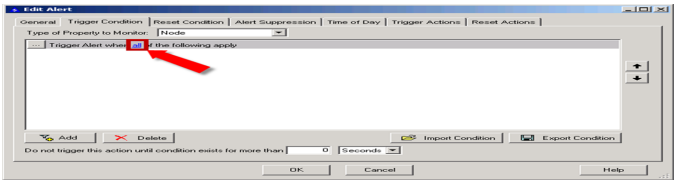
   c. ***If you want to delay the trigger of this alert,*** provide the value and unit of your desired alert trigger delay.

   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:

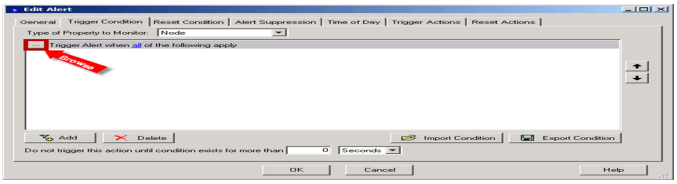
a. Generate trigger conditions in the text field by selecting appropriate descriptors from the linked context menus and by clicking **Browse** (…) on the left of the text field.

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.

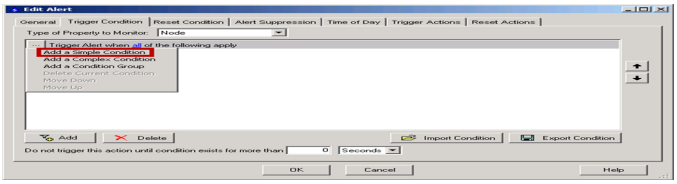


c. Click **Browse** (…) to view the following condition options:

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



- 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.

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

9. ***If you need an additional condition,*** click **Browse** (…), and then click **Add ConditionType**, as appropriate for the condition you want to add.
10. ***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.
11. ***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.
12. ***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. Start the **Advanced Alert Manager** in the Orion Alerting, Reporting, and Mapping folder.
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.

   Note: 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 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. Start the **Advanced Alert Manager** in the Orion Alerting, Reporting, and Mapping folder.
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. Start the **Advanced Alert Manager** in the Orion Alerting, Reporting, and Mapping folder.
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. Start the **Advanced Alert Manager** in the Orion Alerting, Reporting, and Mapping folder.
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. Start the **Advanced Alert Manager** in the Orion Alerting, Reporting, and Mapping folder.
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. Start the **Advanced Alert Manager** in the Orion Alerting, Reporting, and Mapping folder.

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. Start the **Advanced Alert Manager** in the **Orion Alerting, Reporting, and Mapping** folder.
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. Start the **Advanced Alert Manager** in the Orion Alerting, Reporting, and Mapping folder.
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 Advanced 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. Start the **Advanced Alert Manager** in the Orion Alerting, Reporting, and Mapping folder.
2. Click **View > Configure Alerts**.
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**.

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:

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

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

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**.
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 NPM Variables and Examples in the *Orion Network Performance Monitor Administrator Guide*.
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 I**nsert Variable From Above List**.

    f. Click **Build Selected Variable**.

    Note: For more information on the use of variables, see NPM Variables and Examples in the *Orion Network Performance Monitor Administrator Guide*.

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 NPM Variables and Examples in the *Orion Network Performance Monitor Administrator Guide*.

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 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.
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 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.
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**.
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 the alert engine should wait after the alert condition is met before the alert action is executed.
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 the alert engine should wait after the alert condition is met before the alert action is executed.
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.

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 NPM Variables and Examples in the *Orion Network Performance Monitor Administrator Guide*.

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 the alert engine should wait after the alert condition is met before the alert action is executed.
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.

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 the alert engine should wait after the alert condition is met before the alert action is executed.
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 the alert engine should wait after the alert condition is met before the alert action is executed.
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. Start the **Advanced Alert Manager** in the Orion Alerting, Reporting, and Mapping folder.
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 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. Start the **Orion Web Console** in the Orion program folder.
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 S**how Acknowledged Alerts**.
8. Click **Refresh** to complete your Alerts view configuration.

Acknowledging Advanced Alerts in the Web Console

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 in the *SolarWinds Orion Network Performance Monitor Administrator Guide*.

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 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, 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 NTA recognizes an alert condition, 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, 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. Start the **Advanced Alert Manager** in the Orion Alerting, Reporting, and Mapping folder.
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

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 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, 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

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.

Appendix A: Managing Software Licenses

Your SolarWinds licenses can be activated directly during the installation process. However, SolarWinds also provides a powerful License Manager which allows you not only to activate your licenses, but also deactivate a license on a certain machine and re-activate it elsewhere.

The following sections provide more details about:

- Activating your NTA license during the installation
- Installing License Manager
- Using License Manager

Activating Your NTA License

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

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

Activating an NTA Evaluation License

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

To activate an evaluation license:

1. Click **Continue Evaluation** on the Activate NetFlow Traffic Analyzer window.
2. Complete the Configuration Wizard. For more information, see Completing the Configuration Wizard.

Activating an NTA License with Internet Access

In most cases, NTA is installed on an NPM server that has access to the Internet. When your 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 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 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 Configuration Wizard. For more information, see Completing the Configuration Wizard.

Activating an NTA License without Internet Access

Even when your 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 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 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 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 Configuration Wizard. For more information, see Completing the Configuration Wizard.

Installing License Manager

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

For more information about installation requirements, see License Manager Requirements.

To install SolarWinds License Manager:

1. Start the SolarWinds License Manager Setup in the SolarWinds program folder.
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**.

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.

	Need
.net Framework	3.0 or later, links to the framework are included in the installation.
Operating System	Windows Server 2003 SP1 and higher, including R2 Windows Server 2008 and higher, including R2 Windows Server 2012 Windows XP Windows Vista Windows 7 Windows 8
Browser	Internet Explorer 6 or later Firefox 2.0 or later Chrome 27 or later

Note: License Manager must be installed on a computer with the correct time. If the time on the computer is off 24 hours in either direction from the Greenwich Mean Time clock, you will be unable to reset licenses. Time zone settings do not affect and do not cause this issue.

Using License Manager

License Manager must be running on the computer where the currently licensed SolarWinds product is installed.

Deactivating Currently Installed Licenses

The following procedure deactivates a currently installed license.

To deactivate currently installed licenses:

1. Start the **SolarWinds License Manager** in the SolarWinds program folder.
2. Check the products you want to deactivate on this computer.
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.

Re-Activating Licenses

When you have successfully deactivated your products, you can re-activate the license you have de-activated.

To re-activate your license:

1. Log on to the computer on which you want to install your products.
2. Launch the executable to install NTA.
3. When asked to specify your licenses, provide the appropriate information:
   a. Log on to the Customer Portal at https://customerportal.solarwinds.com/.
   b. Select **Licensing&Maintenance > License Management**.
   c. Select NetFlow Traffic Analyzer.
   d. Copy the activation key and use it during the installation.
4. 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 currently installed licenses:

1. Start **the SolarWinds License Manager** in the SolarWinds program folder.
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. Start the **SolarWinds License Manager** in the SolarWinds program folder.
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 sections can be used to help you configure your devices to send flow data to SolarWinds NetFlow Traffic Analyzer.

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.

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, 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, 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 NTA to correctly process NetFlow data and process relevant traffic statistics:

- Each device must be configured to export NetFlow data to NTA.
- Each device that exports NetFlow data to NTA must be monitored in NPM. Only SNMP capable nodes whose interfaces were discovered by NPM can be added as NetFlow sources.
- Traffic from a device that is not monitored in NPM appears only in aggregate as traffic from unmonitored devices. If the device is setup to export data to 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 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 NTA.

To setup a device to export NetFlow data to NTA:

1. Log in 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 on configuring NetFlow on Cisco devices, see Enabling NetFlow for Cisco IOS.

   For information on enabling NetFlow for Cisco Catalyst switches, consult the SolarWinds technical reference "Enabling NetFlow and NetFlow Data Export (NDE) on Cisco Catalyst Switches".

   For information on enabling NetFlow on Cisco ASA devices, consult the KB article "Configuring Cisco ASA devices for use with Orion NTA".

   Otherwise, consult these examples as apply 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.

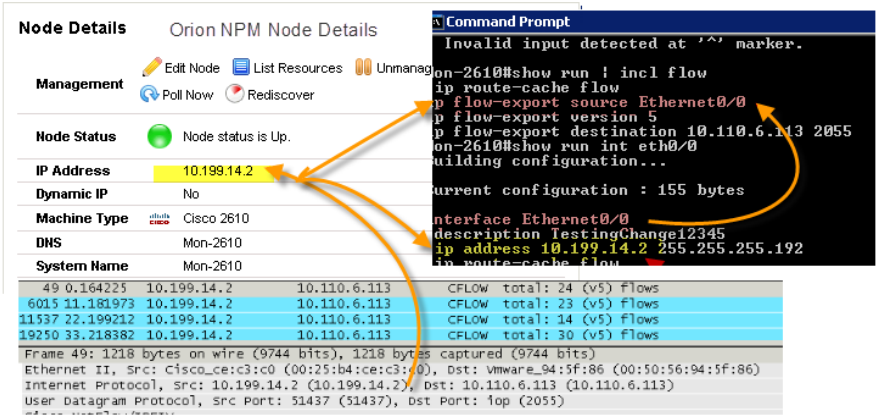
3. Verify that your device and its NetFlow exporting interface are being monitored in Orion NPM.

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 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:



   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 resource 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.

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

Configuring NetFlow Devices

The following sections cover configuration examples for:

- Cisco NetFlow Devices
- Cisco Flexible NetFlow Devices
- Cisco NGA 3000

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 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. SolarWinds 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 NPM server.

SolarWinds 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.

Cisco NGA 3000 Series

This configuration example exports flows from Cisco NetFlow Generation Appliances of 3000 series:

```
flow record IPv4 OrionNetFlow
match ip tos
match ip protocol
match source
match destination
match transport source-port
match transport destination-port
match input-interface
match output-interface
collect counter bytes
collect counter packets
exit
!
!
flow collector Orion
address 10.10.10.30
```

```
dscp 0
transport udp destination-port 2055
exit
!
flow exporter Netflow-to-Orion
version v9
template-period 1
option-period 1
policy multi-destination
destination Orion
exit
!
flow monitor NetFlow-Monitor
exporter Netflow-to-Orion
record OrionNetFlow
dataport 1,2,3,4
tunnel inner
cache size 25
cache type standard
cache timeout active 60
cache timeout inactive 30
cache timeout session disable
exit
!
flow monitor NetFlow-Monitor enable
```

Configuring sFlow and J-Flow Devices

The following sections provide sFlow and J-Flow configuration examples for individual vendors:

- Foundry sFlow Configuration
- HP sFlow Configuration
- Extreme sFlow Configuration

- Juniper sFlow Configuration
- Juniper J-Flow Configuration

Brocade (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 NPM server. This value also contains the port number (`2055`) that is required in this step.

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 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 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 Technical Documentation website,the Juniper Networks Knowledge Center Search, or the Juniper Networks page on Configuring Flow-Based Statistics Collection.

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;
             }
         }
     }
}
```

Appendix C: Glossary

A

additional poller
A server where an additional polling engine is installed to balance the load on the primary polling engine. Enabling multiple polling engines that work in parallel across your network can increase the monitoring capacity of your installation.

additional website
Orion Web Console installed on other than your main server enabling remote access to your NTA and Orion data. Remote users can view the primary Orion Web Console without deploying an entire Orion installation or excessively taxing the resources of the primary Orion server.

B

BGP
See border gateway protocol.

border gateway protocol (BGP)
Border Gateway Protocol is a routing protocol used to exchange routing and reachability details between autonomous systems on the Internet.

C

CBQoS
See class based quality of service.

class based quality of service (CBQoS)
Class Based Quality of Service is a proprietary, SNMP-based Cisco technology allowing you to manage traffic on your network by assigning different priorities for different traffic types.

collector
The server responsible for receiving flows where NetFlow service is running. In NTA context, this term is the same as receiver. See also receiver.

D

destination endpoint
A target endpoint where the traffic is heading.

E

egress interface
An interface used for outgoing traffic.

endpoint
A point where the data conversation beings/stops, such as an FTP server, or a Windows computer. However, it is not where traffic ends but one of the IPs in the data conversation (Source or Destination).

F

flow
A sequence of packets from a particular source to a destination. The source being a computer, and the destination can be another host, a multicast group or a broadcast domain. Flow is used as a superordinate term covering packets sent using different protocols - NetFlow, jFlow, sFlow, IPFIX.

I

ingress interface
An interface used for incoming traffic.

inserts per second / database writes per second (IPS)
The amount of records/rows being inserted into the NTA Flow Storage Database in one second. This value is typically lower than received flows per second because of top talker optimization and received flow aggregation. This value is relevant for HW requirements. However, it can significantly differ from the FPS value, and without the investigation of real

data from a customer, it is very difficult to predict the appropriate IPS. NTA 4.0 stores flows into a single NTA Flow Storage Database, and thus the load of IPS cannot be spread among multiple servers.

interface index

A value identifying a specific interface. Some devices use different indexes than SNMP interface indexes used by NTA, and thus the values must be mapped. See interface index mapping.

interface index mapping

Establishing a relation between a device interface index and SNMP interface index, if they have different values. See also interface index.

M

main poller

Primary polling engine; the main server where your NTA is installed. The primary server retrieving monitored data from flow- and CBQoS-enabled devices.

module

A product based on the Orion Core platform that can be included into the Orion Web Console as an independent tab.

N

NetFlow

Network protocol by Cisco designed to collect and monitor traffic flow data generated by NetFlow-enabled routers and switches.

node

A monitored device (node, switch, server).

NTA Flow Storage Database

A no-SQL column-oriented database using bitmap indexes, which is used for storing flow data in NTA 4.0 on 64-bit operating systems and in newer NTA versions.

O

object
A generic term used for anything that is monitored (node, interface, volume,...)

Orion
The platform, on which SolarWinds base some of its products, such as NPM, or SAM. These products (also called modules) share a common core that ensures that you can add any module you might need for your network monitoring and include it in the Orion Web Console.

Orion SQL Database
SQL database used for storing object relevant data, CBQoS data, and until NTA 4.0 on 64-bit operating systems also for storing flow data. Since NTA 4.0, flow data are stored in the NTA Flow Storage Database.

Orion Web Console
The Orion website providing access to your NTA, NPM or other modules' data.

P

peak flows per second
The received flows per second value that can be processed and saved by NTA in a peak with a duration not longer than 1 minute.

poller (NPM)
In the NPM context of Device Kit Studio, poller is an object that holds information about what property we want to monitor on a device, specification of how to get to the current value of the property and where and how to display the data retrieved.

poller (NTA)
In NTA, poller is used as a synonymum for "polling engine". In this sense, a poller is a device which retrieves monitored data from devices. See also main poller, additional pollers.

R

received flow aggregation (RFA)

Received and processed flows (not dropped, see received flows per second) are held in the NTA Service memory for at most one minute, and then saved to the NTA Flow Storage Database. During this time, NTA aggregates all identical flows (flows with the same IP address, port, protocol, tos, ...) into one flow, sums up bytes and packets, and then saves these identical flows into the NTA Flow Storage Database as a single record. Aggregation strongly affects the HW requirements. The ratio of received flows per second to aggregated flows is not predictable, it strongly depends on the customer's environment and network's traffic.

received flows per second (RFPS)

The amount of flows per second received by the NTA receiver service. Some of these flows could be dropped and thus not processed because of unsupported flow format, top talker optimization, or insufficient performance.

receiver (I)

NTA term meaning the server responsible for receiving flows where the NetFlow Service is running. See also collector.

receiver (II)

An endpoint receiving traffic, such as an IP address downloading a file from the Internet.

resource

A widget on views showing different aspects of traffic monitoring, usually in a chart and a table.

retention period

Retention period specifies the time for which flow data are stored in the database until they expire and are permanently deleted.

S

SolarWinds NetFlow Service
A SolarWinds program that is running in the background ensuring that NTA is operating properly.

SolarWinds NetFlow Storage Service
A SolarWinds program that is running in the background ensuring that the remote NTA Flow Storage Database is operating properly.

source endpoint
An endpoint where the traffic originates.

sustained received flows per second
RFPS that can be processed and saved by NTA for an entire retention period. The default retention period is 30 days.

T

threshold
A defined level whose crossing results in triggering a notification or an alert. For example, setting a warning threshold of 80% for disk usage means that when your disk usage reaches 80%, Orion Web Console will notify you about it.

thwack
SolarWinds online community; a space for users to find out product news, get help with their issues, or share content.

Top Talker
Flows representing the most bandwidth-intensive conversations on your network.

top talker optimization
Decreasing the percentage of flows captured by NTA to improve database performance, reduce page load times, and increase reporting speed. Top talker flows are flows representing the most bandwidth-intensive conversations on your network. By default, NTA captures flows representing

the top 95% of total network traffic. Please note that decreasing the percentage will also decrease the accuracy of data.

transmitted flows per second (TFPS)

Rate at which flows are sent by the router or switch to NTA. Each Orion poller has one NTA Receiver/Service. You can use multiple NTA receivers to relieve the performance load on individual servers hosting the NTA receivers. The TFPS rate is often used to determine storage, RAM, and CPU requirements for the receiver.

transmitter

An endpoint sending out traffic, such as an IP address sending out a file.

U

unknown traffic

Flows exported to the NTA receiver by devices that are either not managed in NPM, or not configured for monitoring in NTA. NTA thus cannot process the exported information, unless you add the exporter nodes to NPM and/or enable monitoring for appropriate interfaces.

unmanageable interface

Unmanageable interfaces cannot be monitored using SNMP. NPM only "registers" these nodes. To process the traffic data from them in NTA, you need to add the interface for monitoring to NTA, and provide the interface speed.

unmanaged nodes or interfaces

Nodes or interfaces not managed in NPM. The devices export flows, but NTA cannot access the necessary data stored in Orion SQL Database.

unmonitored interface

Interfaces managed in NPM, but not monitored by NTA. Traffic data from them are collected, but you cannot see them in NTA until you enable monitoring for them.

V

view
A web page containing resources that display information about your network and the traffic going through individual nodes and interfaces.