NetFlow Traffic Analyzer

Version 4.2.3
© 2017 SolarWinds Worldwide, LLC. All rights reserved.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of SolarWinds. All right, title, and interest in and to the software and documentation are and shall remain the exclusive property of SolarWinds and its respective licensors.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The SolarWinds and other SolarWinds marks, identified on the SolarWinds website, as updated from SolarWinds from time to time and incorporated herein, are registered with the U.S. Patent and Trademark Office and may be registered or pending registration in other countries. All other SolarWinds trademarks may be common law marks or registered or pending registration in the United States or in other countries. All other trademarks or registered trademarks contained and/or mentioned herein are used for identification purposes only and may be trademarks or registered trademarks of their respective companies.
# Table of Contents

**NTA Installation** ........................................................................................................... 19

Installation gotchas ........................................................................................................ 19

SolarWinds NTA licensing .............................................................................................. 19

License Manager for Orion Platform products ............................................................ 20

What does the Web-based License Manager show? ......................................................... 20

What can I do in the Web-based License Manager? ...................................................... 21

Evaluate Orion Platform products ................................................................................ 21

Activate licenses .............................................................................................................. 23

Add or upgrade licenses .................................................................................................. 24

Assign licenses ................................................................................................................ 26

Move licenses: deactivate and re-activate ...................................................................... 26

Synchronize licenses ....................................................................................................... 27

Maintain licenses with the stand-alone Windows License Manager .............................. 27

Stand-alone Windows License Manager requirements .................................................. 27

Install the stand-alone Windows License Manager ......................................................... 28

Activate licenses with the stand-alone Windows License Manager ............................... 29

Deactivate and reactivate licenses ................................................................................ 30

Upgrade and synchronize licenses ................................................................................ 31

Requirements .................................................................................................................. 32

Polling engine requirements .......................................................................................... 32

NTA Flow Storage Database requirements ..................................................................... 33

Recommendations ........................................................................................................... 33

SolarWinds NTA port requirements ................................................................................ 34

Virtual machine requirements ......................................................................................... 37

Orion database server (SQL Server) requirements ........................................................ 37
NTA flow requirements .................................................................41
Required fields ............................................................................42
Sampled flow supported fields ....................................................46
Mandatory fields .........................................................................47
Autonomous system requirements .................................................49
SolarWinds NTA deployment options .........................................50
Install a localized version of SolarWinds NTA .......................50
Install a localized version of SolarWinds NTA .......................50
Upgrade a localized version of SolarWinds NTA .................51
Install SolarWinds NTA and NTA Flow Storage Database locally .................................................................51
Install SolarWinds NTA and a remote NTA Flow Storage Database .................................................................51
Install an additional poller and web console .........................52
Requirements ...........................................................................52
Install an additional poller or web console ..............................52
Install SolarWinds NTA .................................................................53
Deployment options ...................................................................53
Install SolarWinds NTA .................................................................53
Complete the Configuration wizard ........................................53
Install the NTA Flow Storage Database ..................................54
Recommendations and requirements .....................................54
Install the NTA Flow Storage Database ..................................54
Configure a remote NTA Flow Storage Database ..................55
NTA Flow Storage Database recommendations ......................55
Specify the NTA Flow Storage Database destination .............55
Upgrade SolarWinds NTA ...............................................................55
Upgrade paths and compatibility .............................................56
Compatibility table ...................................................................56
Notes ..........................................................................................56
Database migration ........................................................................................................................................... 57
  Migrating flow data from the Orion SQL database ...................................................................................... 57
Uninstall SolarWinds NTA ............................................................................................................................... 57
Get started with SolarWinds NTA .................................................................................................................. 58
  Set up flow monitoring ................................................................................................................................ 58
    Set up network devices to export NetFlow data .......................................................................................... 58
      Requirements for setting up network devices ......................................................................................... 59
    Set up a device to export NetFlow data to SolarWinds NTA ..................................................................... 60
    Exporting both ingress and egress NetFlow traffic data .............................................................................. 61
  Add flow-enabled devices and interfaces to the Orion database ................................................................. 62
    What happens after you add devices and interfaces to the Orion database? ........................................... 62
  Manually add flow sources and CBQoS-enabled devices .......................................................................... 62
    Notes on adding sources and devices ......................................................................................................... 63
    Add flow sources and CBQoS-enabled devices for monitoring ............................................................... 63
    Enable the automatic addition of flow sources ...................................................................................... 63
  Set up NBAR2 on Cisco devices .................................................................................................................. 64
  Create a Flexible NetFlow configuration ...................................................................................................... 64
    Add the flow record .................................................................................................................................... 64
    Add the flow exporter ................................................................................................................................. 64
    Add the flow monitor ................................................................................................................................. 65
    Add the flow monitor to an interface ......................................................................................................... 65
  Diagnostic commands ................................................................................................................................. 65
  Determine the applications your device can recognize .............................................................................. 65
    Check the Protocol Pack version ............................................................................................................... 66
    View a list of the available applications .................................................................................................... 66
  Edit an existing record ................................................................................................................................. 66
    Disable the connection ............................................................................................................................... 66
    Add the application recognition field into the record ............................................................................... 66
Add the application recognition field into the exporter .................................................. 66
Restore the connection ....................................................................................................... 66
NBAR2 Advanced Applications .......................................................................................... 67
NBAR2 requirement for monitoring application IDs ......................................................... 67

**SolarWinds NTA settings** .............................................................................................. 68

SolarWinds NTA settings .................................................................................................. 68
NetFlow management ....................................................................................................... 69
Applications and service ports .......................................................................................... 70
Access the applications and service ports settings ......................................................... 71
Configure data retention for flows on unmonitored ports .............................................. 71
Monitor applications and service ports .......................................................................... 71
Add applications and service ports to NTA .................................................................. 72
Edit applications and service ports ................................................................................. 72
Delete applications and service ports .............................................................................. 73

Autonomous systems ........................................................................................................ 73
Access autonomous systems ......................................................................................... 73
Add autonomous systems ............................................................................................... 73
Edit autonomous systems .............................................................................................. 73
Delete autonomous systems .......................................................................................... 73

IP address groups ............................................................................................................. 74
Add IP address groups ..................................................................................................... 74
Delete IP address groups ................................................................................................. 74
Edit IP address groups ..................................................................................................... 75
Select IP ranges to monitor ............................................................................................. 75

Monitored protocols .......................................................................................................... 75
NetFlow sources and CBQoS polling ................................................................................ 76
Access the management page .......................................................................................... 76
Select interfaces for NetFlow monitoring ........................................................................ 76
IP address processing ....................................................................................................... 85
Database settings ........................................................................................................... 86
Access database settings ............................................................................................... 86
NTA Flow Storage Database settings ........................................................................... 86
  Retention period .......................................................................................................... 87
  Set retention period ..................................................................................................... 87
SolarWinds Orion database maintenance ..................................................................... 87
NTA Flow Storage Database maintenance .................................................................... 87
NTA Flow Storage Database backups .......................................................................... 88
  Best practices for NTA Flow Storage Database backups .......................................... 88
  Schedule regular backups .......................................................................................... 89
  Back up the NTA Flow Storage Database manually .................................................... 89
  Specify a backup folder ............................................................................................... 90
  Restore a backup ......................................................................................................... 90
Remote NTA Flow Storage Database covered by Microsoft Failover Cluster ................... 91
  Failover time ................................................................................................................ 91
  Requirements ............................................................................................................... 92
  Recommendations for the SAN drive ......................................................................... 92
  Set up NTA Flow Storage Database and the Failover Cluster .................................... 92
Cover a local NTA Flow Storage Database by SolarWinds Failover Engine ...................... 93
Move the NTA Flow Storage Database ........................................................................ 93
  Requirements to change the location ......................................................................... 93
  Locate your NTA Flow Storage Database .................................................................... 94
  Move the NTA Flow Storage Database from a remote server to a local disk .............. 94
  Move the NTA Flow Storage Database from a local disk to a remote server .......... 94
  Move the NTA Flow Storage Database to another disk on the same server ............. 95
  Move the NTA Flow Storage Database from an existing remote server to a new remote server ................................................................. 96
High Availability in SolarWinds products .................................................................... 97
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>How does it work?</td>
<td>97</td>
</tr>
<tr>
<td>What is a Virtual IP address?</td>
<td>98</td>
</tr>
<tr>
<td>How do I choose a VIP address?</td>
<td>98</td>
</tr>
<tr>
<td>Which IP address is used as the source?</td>
<td>99</td>
</tr>
<tr>
<td>Examples of matching the binary bits</td>
<td>99</td>
</tr>
<tr>
<td>SolarWinds High Availability requirements</td>
<td>100</td>
</tr>
<tr>
<td>Supported products</td>
<td>100</td>
</tr>
<tr>
<td>Software and Hardware requirements</td>
<td>101</td>
</tr>
<tr>
<td>Port requirements</td>
<td>101</td>
</tr>
<tr>
<td>Networking requirements</td>
<td>102</td>
</tr>
<tr>
<td>High Availability deployment walk-through</td>
<td>102</td>
</tr>
<tr>
<td>Set up the standby server</td>
<td>103</td>
</tr>
<tr>
<td>Activate High Availability pool licenses</td>
<td>104</td>
</tr>
<tr>
<td>Set up an HA pool</td>
<td>104</td>
</tr>
<tr>
<td>Configure High Availability settings</td>
<td>105</td>
</tr>
<tr>
<td>Set up the default High Availability email</td>
<td>106</td>
</tr>
<tr>
<td>Manage HA pools</td>
<td>106</td>
</tr>
<tr>
<td>Disable HA pools</td>
<td>106</td>
</tr>
<tr>
<td>Remove HA pools</td>
<td>107</td>
</tr>
<tr>
<td>Force a manual failover</td>
<td>107</td>
</tr>
<tr>
<td>View the pool member type</td>
<td>107</td>
</tr>
<tr>
<td>How failovers work</td>
<td>108</td>
</tr>
<tr>
<td>Charting and graphing settings</td>
<td>108</td>
</tr>
<tr>
<td>Enable progressive charting</td>
<td>108</td>
</tr>
<tr>
<td>Percentage type for Top XX lists</td>
<td>108</td>
</tr>
<tr>
<td>Top XX list resource percentages</td>
<td>109</td>
</tr>
<tr>
<td>Unit type for area charts</td>
<td>110</td>
</tr>
<tr>
<td>Default time periods for resources</td>
<td>111</td>
</tr>
</tbody>
</table>
Default chart style for resources ................................................................. 111
Default flow direction for resources .......................................................... 111
Enable automatic page refresh ..................................................................... 111
   Automatically refresh resources affected by running updates ..................... 112
Optimize performance in SolarWinds NTA ..................................................... 112
   Configure on demand DNS resolution ....................................................... 112
   Limit flow collections to top talkers .......................................................... 113

View NTA data in the Orion Web Console .................................................... 114
My Dashboards ......................................................................................... 115
   Customize My Dashboards ....................................................................... 116
   Specify My Dashboards and Alerts & Activity items for users .................... 116
   Add items to My Dashboards .................................................................... 117
   Add menu bars ....................................................................................... 118
Change the Orion Web Console logo ............................................................ 118
Edit resources ............................................................................................. 119
Charts ......................................................................................................... 119
   Chart display limitations ........................................................................... 119
   Chart types ............................................................................................... 120
   Chart customization options ....................................................................... 120
   Data granularity shown by default ............................................................ 120
   View flow data for longer time periods with one-minute granularity .......... 120
Pie charts .................................................................................................... 120
   Example .................................................................................................... 121
Area charts .................................................................................................. 121
   Display data for a specific time point ....................................................... 122
   Zoom in to see a specified time period ...................................................... 123
   Hide or show certain items ...................................................................... 124
Customize charts for the current session ....................................................... 124
Customize time and flow direction settings for the current session ........................................ 125
Area charts: zoom and show selected items only ........................................................................ 125
Customize charts for all users ................................................................................................ 125
NTA-specific view customizations .............................................................................................. 127
Enable the NetFlow Traffic Analyzer Summary View ................................................................. 127
Create custom views with the Flow Navigator ........................................................................... 127
Create a custom NetFlow traffic view with the Flow Navigator ................................................ 127
Add NetFlow resources to web console views ............................................................................ 131
Add endpoint-centric resources ............................................................................................. 131
Add an endpoint-centric resource ........................................................................................... 131
Edit time settings for views ..................................................................................................... 132
Change the time period shown by all resources in the view for the current session ............... 132
Edit flow direction in views ..................................................................................................... 132
Change flow direction in a view ............................................................................................... 132
Delete a filtered view .............................................................................................................. 132
Create, delete, modify, or restrict views .................................................................................. 133
Create new views .................................................................................................................... 133
Create views ............................................................................................................................ 134
Add resources and columns to views, and define subviews ..................................................... 134
Add resources to the view ........................................................................................................ 134
Add columns ............................................................................................................................. 135
Change column width ............................................................................................................. 135
Move resources on views ........................................................................................................ 136
Divide content into subviews .................................................................................................. 136
Create custom summary views ............................................................................................... 136
Add external website views ..................................................................................................... 138
Optimize views for TV screens or mobile devices ................................................................... 139
Enable NOC Views .................................................................................................................. 139
Customize NOC Views ................................................................. 139
Exit NOC Views ............................................................................. 139
Manage NOC Views ....................................................................... 139
Display subviews ........................................................................ 140
Move resources in NOC Views ....................................................... 140
Change the NOC view logo ............................................................ 140
Limit objects on a view ................................................................. 140
Use a view as a template ............................................................... 141
Delete views ................................................................................ 141
Specify views for device types ....................................................... 141
Export views to PDF ..................................................................... 141
Monitor traffic flow directions ......................................................... 142
Set flow direction .......................................................................... 143
Change flow direction in a view ...................................................... 143
View CBQoS data .......................................................................... 143
Monitor NBAR2 Applications in SolarWinds NTA ......................... 145
Top XX Applications ..................................................................... 146
View more details about displayed applications ............................. 146
View unmonitored traffic ............................................................... 146
Enable monitoring of unmonitored ports ....................................... 146
Top XX Applications (Endpoint Centric) ......................................... 147
Table legend ................................................................................ 147
Edit the resource .......................................................................... 148
Edit time and flow direction for the view ....................................... 148

Common tasks and user scenarios .................................................... 149
CBQoS policies ............................................................................. 149
Prepare a CBQoS implementation .................................................. 149
Monitor CBQoS dynamically .......................................................... 151
Configure a CBQoS alert ........................................................................................................151
Monitor autonomous systems through BGP ........................................................................152
Prepare to monitor autonomous systems ............................................................................152
Set up a device for monitoring by SolarWinds NTA as part of an autonomous system ....153
Autonomous system requirements .......................................................................................155
NetFlow v5 and compatible flows ......................................................................................156
NetFlow v9, IPFIX, and compatible flows ............................................................................156
Manage autonomous systems .............................................................................................156
Add an autonomous system .................................................................................................156
Edit an autonomous system ...............................................................................................157
Delete an autonomous system ............................................................................................157
Monitor autonomous systems .............................................................................................157
Top XX Autonomous Systems ...........................................................................................157
Top XX Autonomous System Conversations .......................................................................157
IP address groups ................................................................................................................158
Find the cause of high bandwidth utilization .......................................................................158
Track traffic by site ...............................................................................................................159
Perform an immediate hostname lookup ............................................................................160
The thwack user community ...............................................................................................160
User scenarios ......................................................................................................................160
Locate and isolate an infected computer ............................................................................160
Locate and block unwanted use ..........................................................................................161
Recognize and stop a denial-of-service attack ....................................................................161

Users ..................................................................................................................................163
Create users ..........................................................................................................................163
Create users based on existing Active Directory or local domain accounts .................164
Define what users can access and do ..................................................................................165
Restrict user access to network areas by applying limitations ........................................168
<table>
<thead>
<tr>
<th>Change account passwords</th>
<th>168</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patterns for limitations</td>
<td>169</td>
</tr>
<tr>
<td>Limit users to specific network areas</td>
<td>169</td>
</tr>
<tr>
<td>Reports</td>
<td>170</td>
</tr>
<tr>
<td>NetFlow-specific predefined reports</td>
<td>170</td>
</tr>
<tr>
<td>Access NetFlow reports</td>
<td>170</td>
</tr>
<tr>
<td>Historical NetFlow reports</td>
<td>170</td>
</tr>
<tr>
<td>Historical CBQoS reports</td>
<td>172</td>
</tr>
<tr>
<td>Best practices for SolarWinds NTA reports</td>
<td>173</td>
</tr>
<tr>
<td>Execute a SolarWinds NTA report</td>
<td>175</td>
</tr>
<tr>
<td>Create a report</td>
<td>175</td>
</tr>
<tr>
<td>Create a report using SWQL</td>
<td>176</td>
</tr>
<tr>
<td>Edit a SolarWinds NTA report</td>
<td>177</td>
</tr>
<tr>
<td>Change objects that are being reported on</td>
<td>177</td>
</tr>
<tr>
<td>Change the time of the report</td>
<td>178</td>
</tr>
<tr>
<td>Define a customized time period</td>
<td>178</td>
</tr>
<tr>
<td>Change the page layout</td>
<td>178</td>
</tr>
<tr>
<td>Change the logo</td>
<td>179</td>
</tr>
<tr>
<td>Limit access to the report</td>
<td>179</td>
</tr>
<tr>
<td>Specify custom properties</td>
<td>179</td>
</tr>
<tr>
<td>Schedule a report</td>
<td>180</td>
</tr>
<tr>
<td>Create a custom report for IP address groups</td>
<td>180</td>
</tr>
<tr>
<td>Create a custom report for EF type of service</td>
<td>182</td>
</tr>
<tr>
<td>Customize a report to filter multicast data and group UDP data</td>
<td>184</td>
</tr>
<tr>
<td>Customize a historical NetFlow report to include location</td>
<td>186</td>
</tr>
<tr>
<td>Alerts</td>
<td>187</td>
</tr>
<tr>
<td>NetFlow-specific predefined alerts</td>
<td>187</td>
</tr>
<tr>
<td>Where can I find what NTA-specific alerts are enabled?</td>
<td>187</td>
</tr>
</tbody>
</table>
Top talker alerts ................................................................. 187
CBQoS alerts ................................................................. 188
Miscellaneous ................................................................. 189
Configure NTA-specific alerts ........................................ 189
Configure trigger actions for default top talker alerts ....... 189
Change the threshold for Top Talker alerts ...................... 190
Configure a CBQoS alert ................................................... 192
Available alert actions .................................................... 193

**Troubleshooting** ................................................................ 194

NetFlow issues ................................................................. 194
Chart issues ........................................................................ 194
Database connection issues ................................................ 194
CBQoS issues .................................................................... 194
NetFlow Collector Services ................................................ 195
  Edit or add collection ports ............................................. 195
  Delete collectors ............................................................ 195
    Delete a collector permanently .................................... 196
    Delete a collector in the NetFlow Collector Services resource ........................................ 196
  Troubleshoot collector services ...................................... 196
  NetFlow collector services ............................................. 196
NetFlow Sources .................................................................. 197
  Troubleshoot NetFlow sources ..................................... 198
  View more details about displayed objects ...................... 198
  Troubleshoot Long Flow Errors ...................................... 198
Events .............................................................................. 199
  Access Events ................................................................. 199
  What details do events provide? ...................................... 199
  Event colors ................................................................... 199
Filter events and display historical events ......................................................... 200
Filter all events .................................................................................................. 200
Clear events ......................................................................................................... 201
Display resolved events that were cleared .......................................................... 202
Error: NetFlow service inaccessible ..................................................................... 202
Start the NetFlow service .................................................................................... 202
Error: No template received .................................................................................. 202
Resolve the issue .................................................................................................. 202
Required fields ...................................................................................................... 203
Requirements ......................................................................................................... 203
Mandatory fields for the flow template schema ..................................................... 203
Optional fields for the flow template schema ........................................................ 204
Notes ..................................................................................................................... 207
Events list ............................................................................................................... 207
NetFlow receiver service stopped .......................................................................... 207
License limitation .................................................................................................. 207
No valid license ..................................................................................................... 208
No space left on NTA Flow Storage Database ..................................................... 208
Invalid template .................................................................................................... 208
Invalid IPFIX template ......................................................................................... 208
No template received .............................................................................................. 209
NetFlow data export not enabled ........................................................................... 209
NetFlow time difference error ............................................................................... 209
Cannot connect to NTA Flow Storage Database ................................................... 210
Unmanaged NetFlow node ...................................................................................... 210
Unmanaged NetFlow interface ............................................................................... 210
Unmonitored NetFlow interface ............................................................................ 210
Not primary NPM node IP address ........................................................................ 211
Running out of space NTA Flow Storage Database ......................................................... 211
Unmonitored interface automatically added ................................................................. 211
NetFlow time difference warning ................................................................................. 212
NetFlow time difference warning ended ..................................................................... 212
NetFlow receiver service started .................................................................................. 212
NetFlow receiver service settings changed ................................................................. 212
NetFlow event: interface index mapping used for a node ......................................... 212
NetFlow event: removing interface index for a node .................................................... 213
NetFlow database maintenance .................................................................................... 213
Scheduled shrink performed ....................................................................................... 213
Updating data to be used in Top XX aggregated resources ........................................ 213
Windows Firewall is turned on .................................................................................... 217
NetFlow licensing ......................................................................................................... 217
Unable to start listening on port .................................................................................. 217
Port is free listening ...................................................................................................... 218
Notification event status reset .................................................................................... 218
Enough space available On NTA Flow Storage Database ........................................ 218
Connection to NTA Flow Storage Database has been restored .................................... 218
Unmanageable interface speed ..................................................................................... 218
Resolve unknown NetFlow traffic ............................................................................... 219
Resolve unknown traffic events .................................................................................... 220
Test whether the events were resolved ........................................................................ 220
Enable flow monitoring from unmanageable interfaces ............................................. 220
Add an unmanageable interface .................................................................................. 220
Unmanageable interface monitored in SolarWinds NTA ............................................. 221
Set up a NetFlow collection ......................................................................................... 221
Chart issues .................................................................................................................. 221
Duplicate flows ............................................................................................................. 222
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resolving Duplicate Flows</td>
<td>222</td>
</tr>
<tr>
<td>Double rate in Top XX Endpoints and Top XX Domains</td>
<td>222</td>
</tr>
<tr>
<td>Example</td>
<td>222</td>
</tr>
<tr>
<td>No data</td>
<td>223</td>
</tr>
<tr>
<td>Unexpected spikes in CBQoS post-policy charts</td>
<td>223</td>
</tr>
<tr>
<td>Resolve duplicate flows</td>
<td>223</td>
</tr>
<tr>
<td>Things to check</td>
<td>223</td>
</tr>
<tr>
<td>Database connection issues</td>
<td>224</td>
</tr>
<tr>
<td>Troubleshoot the connection to the SolarWinds Orion database</td>
<td>224</td>
</tr>
<tr>
<td>Troubleshoot the connection to a remote NTA Flow Storage Database</td>
<td>224</td>
</tr>
<tr>
<td>Troubleshoot the connection between the two databases</td>
<td>224</td>
</tr>
<tr>
<td>CBQoS issues</td>
<td>225</td>
</tr>
<tr>
<td>Record troubleshooting steps</td>
<td>225</td>
</tr>
<tr>
<td>CBQoS issues list</td>
<td>225</td>
</tr>
<tr>
<td><strong>Device configuration examples</strong></td>
<td>226</td>
</tr>
<tr>
<td>NetFlow device examples</td>
<td>226</td>
</tr>
<tr>
<td>Cisco NetFlow configuration</td>
<td>226</td>
</tr>
<tr>
<td>Cisco Flexible NetFlow configuration</td>
<td>226</td>
</tr>
<tr>
<td>Cisco NGA 3000 series</td>
<td>227</td>
</tr>
<tr>
<td>Cisco WLC 5700 series</td>
<td>228</td>
</tr>
<tr>
<td>sFlow and J-Flow device examples</td>
<td>229</td>
</tr>
<tr>
<td>Brocade (Foundry) sFlow configuration</td>
<td>229</td>
</tr>
<tr>
<td>Extreme sFlow configuration</td>
<td>230</td>
</tr>
<tr>
<td>HP sFlow configuration</td>
<td>230</td>
</tr>
<tr>
<td>Juniper Networks sFlow and J-Flow configurations</td>
<td>230</td>
</tr>
<tr>
<td>Juniper sFlow configuration</td>
<td>230</td>
</tr>
<tr>
<td>Juniper J-Flow configuration</td>
<td>231</td>
</tr>
<tr>
<td>Enable NetFlow and NetFlow data export on Cisco Catalyst switches</td>
<td>232</td>
</tr>
</tbody>
</table>
Requirements to enable NetFlow and NetFlow Data Export .................................................. 232
Cisco Catalyst 4500 Series .................................................................................................................. 233
  Enable NetFlow to work with SolarWinds NTA ................................................................................. 233
  Configure the SolarWinds NTA server as a NetFlow destination ...................................................... 233
  Display the NetFlow configuration for verification ............................................................................ 233
Catalyst 6500 and 7600 series ............................................................................................................. 234
  Enable NetFlow and NDE on the Multilayer Switch Feature Card (MSFC) ........................................ 234
  Enable NetFlow and NDE on the Policy Feature Card (PFC) .............................................................. 235
  Configure the destination for NDE data streams ................................................................................ 235
  Set the aging interval for NDE ........................................................................................................... 235
  Display the NDE address and port configuration for verification .................................................... 235
NTA Installation

Installation gotchas

The SolarWinds NetFlow Traffic Analyzer installation is a simple, wizard-driven process that collects data from any flow-enabled devices monitored by SolarWinds Network Performance Monitor.

- Time zone settings of the Web server (IIS), database, and SolarWinds Information Service must all be the same. 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 to match.
- A single SolarWinds NTA installer contains binaries for the main poller, an additional poller, and additional web interfaces. The installer automatically determines the type of installation needed to match the SolarWinds NPM installation type.
- To complete your installation, you must provide your NetFlow traffic port and confirm that it is enabled and sending flow data.

SolarWinds NTA licensing

Licensing for SolarWinds NTA follows the license level of your underlying SolarWinds NPM installation. For example, if you have an NPM license for SL250, your NTA license must also be SL250.

When you upgrade licenses, the license levels must also match. If you have an NTA license for SL250 and an NPM license for SL250, and you upgrade the NPM license to SL500, you also have to upgrade the NTA license to SL500 or NTA does not work.

The following types of SolarWinds NTA licenses are available:

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

Because your database size increases when you add flow-enabled devices, SolarWinds recommends that you collect NetFlow data on two interfaces for a period of time to learn 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 SolarWinds NTA, the effective capacity of your installation may be lower if the monitored interface throughput is especially high.
License Manager for Orion Platform products

Beginning with SolarWinds Orion Platform products version 2016.2, such as NPM 12.0.1 or SAM 6.3, the Web-based License Manager replaces the stand-alone Windows License Manager.

The Web-based License Manager replaces the stand-alone Windows License Manager in Orion Platform products. If you have upgraded from a previous version of your Orion Platform product, you can still use the stand-alone Windows version. New installs use the web-based License Manager only.

With the Web-based License Manager, you can manage licenses for Orion Platform products, Additional Polling Engines (APE), Additional Web Servers (AWS), and High Availability pools on a single Orion Web Console.

The Web-based License Manager requires the main Orion server to be up. If the Orion server is down for more than 14 days, your licenses may be invalidated.

- Click Settings > All Settings, scroll down, and click License Manager in the Details grouping.

What does the Web-based License Manager show?

The Web-based License Manager reviews and displays the following licenses:

- Full and evaluation licenses for installed Orion Platform products
- Licenses for Additional Polling Engines and Additional Web Servers
- Unassigned licenses
- Orion Scalability Engine Evaluation license for evaluating Additional Polling Engines and Additional Web Servers
- Orion High Availability licenses
All licenses include information about duration and expiration dates, Orion Platform product version, license type and status, and server. Activated licenses display the activation key.

What can I do in the Web-based License Manager?

- **Activate** or **deactivate** licenses.
- **Add or upgrade** licenses.
- **Assign licenses** to a server.
- Sort licenses by Product Name, Product Version, License Type, or Expiration Date.

Evaluate Orion Platform products

If you are evaluating SolarWinds NTA, download a free [30-day evaluation](#). The evaluation version of SolarWinds NTA is a full version of the product, functional for 30 days. After the evaluation period, you can easily convert your evaluation license to a production license by obtaining and applying a license key. If you need assistance with your evaluation, contact sales@solarwinds.com.

When you evaluate High Availability, the evaluation period starts when you activate the evaluation license.

When you activate a full license for a product, the evaluation license expires, and you lose any remaining evaluation days for the product.

The only exception is the Orion Scalability Engine Evaluation License. This evaluation license covers an unlimited number of Additional Polling Engines and Additional Web Servers until the end of the evaluation period.

What happens when an evaluation license expires?

- Additional Web Servers stop working.
- Polling engines stop polling.
- High Availability pools are disabled.
- Orion Web Console only displays historical data.
- The evaluation license in the Web-based License Manager is marked as expired until it is replaced by a full license.

Evaluate the performance improvement achieved by Additional Polling Engines and Additional Web Servers

When you install an Additional Polling Engine (APE) or an Additional Web Server (AWS), the Orion Scalability Engine Evaluation license is in the License Manager on the main polling engine. With this license, each polling engine can poll unlimited number of elements for 30 days.

If you purchase and activate an APE or AWS license during and evaluation period, you can install and use the APE or AWS with the Orion Scalability Engine Evaluation license until the end of the evaluation period.
When the Orion Scalability Engine Evaluation license expires, it is marked as expired in the License Manager. Purchase and activate the appropriate number of APE or AWS licenses.

Can I keep an AWS evaluation if I have commercial licenses for APEs?

Yes. If you purchased an APE license, and want to keep the option to evaluate an AWS in the future, activate the APE license before you install the APE.

1. Click Settings > All Settings > License Manager.
2. Click Activate, provide your activation key for the APE, and complete the activation. The license remains unassigned.
3. Install the APE. During the installation, the activated license is used, and the evaluation period does not start.

When you install an AWS, the evaluation license remains available.

You can also purchase an AWS license, activate the license before you install the AWS, and you can still evaluate APEs.

Evaluate High Availability

**High Availability (HA)** is licensed per pool. To use the HA feature, you need to license HA pools.

With the High Availability Evaluation license, you can create an unlimited number of HA pools and use HA for 30 days. High Availability Evaluation licenses start the 30-day countdown when you add the first HA pool.

How do I evaluate High Availability?

1. Set up high availability servers.
2. Click Settings > All Settings > High Availability Settings > High Availability Deployment Summary, and click Set Up High Availability Pool.
3. Click Set Up HA Licensing in the red banner.
4. Select Evaluate High Availability, and click Next.
5. Complete creating the HA pool.

The 30-day evaluation period starts after you add the first HA pool. The HA evaluation license is activated and assigned to the pool. You can check the number or remaining days next to the license in the web-based License Manager.

What happens when a High Availability evaluation license expires?

HA evaluation licenses expire after the 30-day evaluation period or when you add a full license key. When the evaluation license expires, all pools without a valid license are disabled.

To enable a pool when the evaluation expires, activate a full license and assign it to the pool.
Activate licenses

Activated licenses are automatically assigned to a server. If there are more licenses than installed servers, the extra licenses remain unassigned. You can change the license assignment.

Activate licenses with Internet access

The Web-based License Manager automatically detects whether your Orion server has access to the Internet, or whether it is offline.

1. Click Settings > All Settings.
2. Click License Manager in the Details section.
   Sort the licenses by product name, product version, license type, or expiration date to quickly find a license.

3. Click Activate.
4. Enter the activation key.
   a. Click Customer Portal in the top right corner, and log in using your Customer ID and password, or your individual user account information.
      If you do not know your SolarWinds Customer ID and password or individual profile details, contact Customer Support.
   b. On the menu bar, click License Management > License Management.
   c. Click the plus sign next to the SolarWinds product to display your activation key.
   d. Copy the unregistered activation key, and paste it into the Activation Key field in the License Manager Activate window.
5. Enter the registration details, and click Activate.

The license type, the expiration date, the assigned server, and the license key display in the License Manager.

Activate licenses offline

If you have installed an Orion Platform product on a computer without Internet access, the Web-based License Manager guides you through offline activation.

> In the offline activation mode, you cannot activate a license for a product that is not installed.

1. Click Settings > All Settings > License Manager to open the Web-based License Manager.
2. Select a product, and click Activate.
3. Click Copy to Clipboard to copy the unique machine key.
4. Log in to the Customer Portal, and click License Management > License Management.
5. On the Customer Portal License Management page, expand the product license to activate, and click Activate License Manually.
6. Paste the unique machine ID from clipboard, and click Generate License File. Save the .lic file locally and transfer it to the offline computer.
7. In the License Manager on the offline computer, choose the .lic file, and click Activate.

Your license is now activated, and the license details display in the Web-based License Manager.

Add or upgrade licenses

When you change how your product is licensed, for example when you increase the number of licensed objects, you receive a new activation key. Activate the key to upgrade your license.

If your Orion Web Console is connected to the Internet, you can also add and activate a license for an Orion Platform product before you install it.
1. Click Settings > All Settings, and then click License Manager.
2. In the License Manager, click Add/Upgrade License.
3. Enter the Activation Key and Registration Information, and click Activate.

   Not sure how to get your Activation key? See Activate licenses for more details.

The license is now added to the License Manager and assigned to a server. If no server needs the license, the license remains unassigned.

Update a license

1. Go to the Web-based License Manager, select the license, and click Update.
2. Enter the Activation Key and registration details, and click Activate.

The license key is used for the license, and you can monitor the number of elements covered by the license.
Assign licenses

The License Manager automatically assigns an activated license to a server that needs a license.

**When do I need to manually assign a license?**

- To improve polling capacity (stacking licenses)
- To use the license by a different polling engine
- To change the default polling engine or web server assignment

Stack licenses

Stacking licenses can improve the polling capacity of your polling engines. You can assign up to four polling engine licenses to one server.

Each polling engine can poll a specified number of elements at the default polling interval. After reaching the maximum number, the polling interval is prolonged. To maintain the default polling interval, assign an additional license to the same polling engine. See Scalability Engine Guidelines for your product in the SolarWinds Success Center for more information about extending the monitoring capacity.

Assign licenses to a polling engine

1. Click Settings > All Settings.
2. Click License Manager in the Details section.
3. Select the license to reassign, and click Assign.
4. Select a polling engine and click Assign.

The polling engine is now using the license.

Move licenses: deactivate and re-activate

To move your main polling engine for an Orion Platform product to another server, you need to transfer the licenses to the new server. See the SolarWinds Migration Guide for more information about moving Orion Platform products.

ℹ️ You can only move licenses for product versions that were released during your maintenance period. To get a newer product version, renew your maintenance or re-license your product.

💡 To move an Additional Polling Engine, Additional Web Server, or stackable polling engine license, install the polling engine or web server, and then assign the license to it.

1. Prepare licenses to be moved.
   a. On the Orion server, open the Orion Web Console, and click Settings > All Settings > License Manager.
   b. Copy and paste your activation keys to a text file.
   c. Select the licenses, and click Deactivate.
2. Prepare the main polling engine.
   a. Install the main polling engine on the server.
   b. Add and activate the license keys.

3. Uninstall the old main polling engine.

**Synchronize licenses**

When your Orion server has access to the Internet, the maintenance status of your licenses is synchronized with the Customer Portal daily.

If you want to upgrade your Orion Platform product and your maintenance is expired, extend the maintenance, and then synchronize your license with the Customer Portal. After the license is synchronized, you can upgrade immediately.

1. From the Orion Web Console, click Settings > All Settings > License Manager to start the License Manager.
2. Click Synchronize.

The License Manager synchronizes with the Customer Portal and any updates in the Customer Portal are reflected in the Web-based License Manager.

**Maintain licenses with the stand-alone Windows License Manager**

After you install an Orion Platform product or other products such as DameWare, you are prompted to activate your license. To activate your product, go to the Web-based License Manager.

Orion Platform products with Core 2016.2 and later can use the Web-based License Manager to manage licenses for all polling engines and additional websites from a single Orion Web Console page. Non-Orion Platform products use the stand-alone Windows License Manager.

**What can you do with the Windows License Manager?**

- Deactivate licenses on one computer and activate them on another computer without contacting SolarWinds Customer Service.
- Upgrade production license levels.
- Upgrade from evaluation licenses to production licenses.
- Synchronize licenses with the licensing server.

You cannot activate the license for a product that is released after the end of your maintenance period. You can activate the license for a product released before the end of your maintenance period at any time.

**Stand-alone Windows License Manager requirements**
<table>
<thead>
<tr>
<th>ITEM</th>
<th>REQUIREMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install location</td>
<td>SolarWinds License Manager must be installed on the same computer as your installed products.</td>
</tr>
<tr>
<td><strong>WARNING</strong></td>
<td>You must install License Manager on a computer with the correct time.</td>
</tr>
<tr>
<td>Connectivity</td>
<td>For instant license management, the computer must have internet connectivity. You can also manage licenses using offline activation and deactivation. You must have online access to the SolarWinds Customer Portal from another computer.</td>
</tr>
<tr>
<td>.NET Framework</td>
<td>.NET 4.5</td>
</tr>
</tbody>
</table>
| Operating system     | • Windows Server 2008 R2 SP1  
                        | • Windows Server 2012  
                        | • Windows Server 2012 R2  
                        | For evaluation purposes:                                                                 |
|                      | • Windows 7 SP1  
                        | • Windows 8 (except for Standard edition)  
                        | • Windows 8.1 (except for Standard edition)  
                        | • Windows 10  
                        | Browser                                                                 |
|                      | • Microsoft Internet Explorer 8 or later  
                        | • Microsoft Edge  
                        | • Firefox 44.0 or later  
                        | • Chrome 48.0 or later |

Install the stand-alone Windows License Manager

Install Windows License Manager on the computer with SolarWinds products installed. The License Manager can only license products on that computer.

1. Start the SolarWinds License Manager Setup in the SolarWinds program folder.

   If problems with License Manager occur, or if or the computer does not have access to the Internet, download and install the latest version of License Manager.

2. Click Next to accept the SolarWinds EULA, and click Install.
Activate licenses with the stand-alone Windows License Manager

You can manage licenses for multiple SolarWinds products with the Windows License Manager.

1. Start the License Manager in your SolarWinds program folder.
   - If the License Manager is not installed on the computer, install it.
2. Click Activate next to the SolarWinds product, and complete the Activation wizard.

Activate licenses with Internet access

1. On the Activate Product window, select I Have Internet Access.
2. Enter your activation key in the Activation Key field.
   a. Browse to https://customerportal.solarwinds.com, and then log in using your Customer ID and password, or your individual user account information.
      - If you do not know your SolarWinds Customer ID and password or individual profile details, contact Customer Support.
   b. Under the Licensing Management section, select License Management.
   c. Click the plus sign next to the SolarWinds product to display your activation key.
   d. Copy your unregistered activation key for the SolarWinds product, and paste it into the Activation Key field in the Activate window.
3. If you are using a proxy server to access the Internet, select I Access the Internet Through a Proxy Server, and enter the proxy address and port number.
4. Click Next.
5. Enter your customer data, and complete the Activation wizard.
Activate licenses offline

1. On the Activate Product window, select This Server Does Not Have Internet Access, and click Next.
2. To finalize your registration, click Copy Unique Machine ID.
3. Paste the data into a text editor, and save the text document.
4. Transfer the document to a computer with Internet access. For example, transfer the document to a shared location.
5. Log in to the SolarWinds customer portal and find your activation key:
   a. Browse to https://customerportal.solarwinds.com from a computer with Internet access, and then log in using your Customer ID and password, or your individual user account information.
   
   If you do not know your SolarWinds Customer ID and password or individual profile details, contact Customer Support.

   b. Click License Management.
   c. Browse to the SolarWinds product, such as Network Performance Monitor, and click Manually Register License.
   d. Provide the Unique Machine ID you transferred earlier, and download your license key.
   e. Transfer the license key to a shared location.

6. Return to the offline computer where you have been running the Activation wizard, and browse to the shared License Key File location from the Activate Product window.
7. Click Next to continue, and complete the Activation wizard.

Deactivate and reactivate licenses

To move your SolarWinds product to another server, deactivate the license on the original computer, and reactivate it on the server with the new installation.

You can deactivate and reuse licenses to install product versions that were released during your maintenance period. You cannot deactivate and reuse licenses to install products that were released after your maintenance period expired. To license these products, you must renew your maintenance or re-license your product.

Deactivate, move, and assign licenses online

1. Log in to the computer where the licensed SolarWinds product is installed.
2. Start the License Manager in the SolarWinds program folder.
3. Select the products you want to deactivate on this computer, and click Deactivate.
   You can deactivate multiple products at the same time. When you deactivate a license, it expires.
4. Complete the Deactivation wizard.
5. Log in to the computer on which to install your products, and begin installation.
6. When prompted, specify your license information.
   The license is now assigned to the new installation.

Deactivate, move, and assign licenses offline

1. Log in to the computer where the licensed SolarWinds product is installed.
2. Start the Windows License Manager in the SolarWinds program folder.
3. Select the products you want to deactivate on this computer, and click Deactivate.
   You can deactivate multiple products at the same time. The deactivation file contains information about each product.
5. Log in to the SolarWinds Customer Portal, and navigate to the License Management page.
6. Select your product instance, and click Deactivate License Manually.
7. On the Manage License Deactivation page, locate the deactivation file you created in Windows License Manager, and click Upload.
   The deactivated licenses are now available to activate on a new computer.

   The new License Manager tool allows offline deactivation with a file that can be uploaded to the Customer Portal.

8. Log in to the computer on which to install your products, and begin installation.
9. When prompted, specify your license information.
   The license is now assigned to the new installation.

Upgrade and synchronize licenses

If you have changed how your product is licensed, such as by increasing the number of objects you can monitor, use the Windows License Manager to apply the change to your products.

1. Start the License Manager from 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 complete the upgrade.

Synchronize licenses to the Customer Portal

For most Orion Platform products licenses, you can synchronize the data on your Customer Portal with the data in the Windows License Manager.

Synchronizing can include:

- Updating the maintenance end date
- Registering the license if it was reset
License synchronization takes place automatically once a day. If the automatic synchronization does not occur, or you want to update your licenses immediately, you can synchronize your installed licenses with the SolarWinds Customer Portal:

1. Start the License Manager from the SolarWinds program folder.
2. Select the product, and click Synchronize.
3. Click Synchronize again in the Synchronize Licenses window.

The License Manager synchronizes with the Customer Portal and any updates in the Customer Portal are reflected in the License Manager.

Requirements

SolarWinds NTA requires:

- SolarWinds NPM version hosted on the same server. SolarWinds NTA requirements follow and extend NPM requirements. See Polling engine requirements.
- Microsoft SQL Database. See Orion database server (SQL Server) requirements.
- NTA Flow Storage Database. See NTA Flow Storage Database Requirements. Review the NTA Flow Storage Database settings before you install and configure the NTA Flow Storage Database.

For production environments, SolarWinds recommends that SolarWinds NPM, Microsoft SQL Database, and NTA Flow Storage Database are hosted on separate servers.

SolarWinds NTA requires a 64-bit operating system.

Polling engine requirements

The following requirements ensure the scalability benefits of SolarWinds NTA:

<table>
<thead>
<tr>
<th>TYPE</th>
<th>REQUIREMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>64-bit operating system: Microsoft Windows Server 2012 and later</td>
</tr>
<tr>
<td></td>
<td>If you have more than one poller, make sure they are all installed on 64-bit operating systems.</td>
</tr>
<tr>
<td>SolarWinds NPM</td>
<td>Version 12.2</td>
</tr>
<tr>
<td>Databases</td>
<td>Microsoft SQL Server 2012 and later</td>
</tr>
<tr>
<td></td>
<td>The NTA Flow Storage Database is where SolarWinds NTA stores your flow data. If you decide to store flows on a remote server, which SolarWinds recommends for production environments, you must install the NTA Flow Storage Database there first.</td>
</tr>
</tbody>
</table>
A connection to Orion SQL database is required, because CBQoS data and some additional low level details are still stored in Orion SQL database.

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 SolarWinds NTA.

Recommendations

- Install the NTA Flow Storage Database on a different server than the SolarWinds Orion database, so that incoming flows do not affect performance of the Flow Storage Database.
- In case you want to use SAN storage, please make sure your environment meets the IOPS requirements for the NTA Flow Storage Database server.
- Solid-state drives (SSD) are recommended for all components.
- Do not install the NTA Flow Storage Database on a polling engine, because it might affect performance. Additional polling engine is not supported.
- Use a dedicated disk or LUN for storing your flow data.
- We do not recommend installing the NTA Flow Storage Database on the C:\ drive.
- Do not run anti-virus software or any other file scanning application over data in the NTA Flow Storage Database. File scanning applications affect the database performance and may even prevent the database from running properly.

⚠️ You can also review antivirus exclusions for all Orion products. For more information, see Files and directories to exclude from antivirus scanning.

<table>
<thead>
<tr>
<th>Type</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CPU</strong></td>
<td>3 GHz or faster</td>
</tr>
<tr>
<td></td>
<td>Evaluation requires 2 CPUs</td>
</tr>
<tr>
<td></td>
<td>Production environments require 4 CPUs or more (4 - 16 CPUs)</td>
</tr>
<tr>
<td><strong>RAM</strong></td>
<td>Evaluation requires 8 GB or more</td>
</tr>
<tr>
<td></td>
<td>Production environments require 16 GB or more (16 - 128 GB)</td>
</tr>
<tr>
<td></td>
<td>To ensure optimal performance, you should increase RAM together with the database size.</td>
</tr>
<tr>
<td><strong>Hard drive space</strong></td>
<td>20 GB on 7200 RPM disk or more</td>
</tr>
</tbody>
</table>
|                  | With the default 30-day retention period and default top talker optimization, you should plan at least 8 GB of additional storage capacity per sustained 1000 flows per 33
second. However, the required hard drive space strongly depends on your flow traffic, and SolarWinds recommends you provide more space accordingly.

NTFS file system required

⚠️ The only RAID configurations that should be used with SolarWinds 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.

<table>
<thead>
<tr>
<th>OS</th>
<th>64-bit operating system: Microsoft Windows Server 2012 and later</th>
</tr>
</thead>
<tbody>
<tr>
<td>.NET Framework</td>
<td>4.6.2</td>
</tr>
<tr>
<td></td>
<td>If not already installed, .Net Framework auto-installs with the SolarWinds NTA Flow Storage Database.</td>
</tr>
</tbody>
</table>

### SolarWinds NTA port requirements

The following table lists ports that SolarWinds NetFlow Traffic Analyzer uses to communicate with other devices and servers.

<table>
<thead>
<tr>
<th>APPLICATION PORT</th>
<th>PROTOCOL</th>
<th>SERVICE/PROCESS</th>
<th>DIRECTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>TCP</td>
<td>World Wide Web Publishing Service</td>
<td>Bidirectional</td>
<td>Port used for web console and any other web servers.</td>
</tr>
<tr>
<td>137</td>
<td>UDP</td>
<td>NetBIOS</td>
<td>Outbound</td>
<td>Port for outbound traffic if NetBIOS name resolution is turned on.</td>
</tr>
</tbody>
</table>
When NTA is trying to resolve the NetBIOS names of servers in their conversations, you may find a large amount of outbound UDP 137 traffic from the NTA collector to a number of external addresses. You can confirm the traffic by using the Flow Navigator to match the outbound connections to existing conversations.

- **Port**: 161, **Protocol**: UDP, **Service/Process**: SolarWinds Job Engine v2, **Direction**: Outbound
  - Port used for sending and receiving SNMP information including polling CBQoS-enabled devices.

- **Port**: 1433, **Protocol**: TCP, **Service/Process**: SolarWinds Collector Service, **Direction**: Outbound
  - Port used for communication between the NTA Flow Storage Database and
<table>
<thead>
<tr>
<th>Application Port</th>
<th>Protocol</th>
<th>Service/Process</th>
<th>Direction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2055</td>
<td>UDP</td>
<td>SolarWinds Collector Service</td>
<td>Inbound</td>
<td>Port for receiving flows on any SolarWinds NTA collector.</td>
</tr>
<tr>
<td>5671</td>
<td>TCP</td>
<td>RabbitMQ</td>
<td>Bidirectional</td>
<td>Rabbit MQ messaging</td>
</tr>
<tr>
<td>17777</td>
<td>TCP</td>
<td>SolarWinds Information Service</td>
<td>Bidirectional</td>
<td>Port for sending and receiving traffic between SolarWinds NPM and other Orion Modules. Port used for communication between remote Flow Storage Database and NTA Main Poller.</td>
</tr>
<tr>
<td>17778</td>
<td>HTTPS and TCP</td>
<td>SolarWinds Information Service</td>
<td>Bidirectional</td>
<td>Open to access the SolarWinds Information Service API and agent communication</td>
</tr>
<tr>
<td>17791</td>
<td>TCP</td>
<td>SolarWinds Agent</td>
<td>Bidirectional</td>
<td>Open for agent communication on any SolarWinds Orion server running Windows Server 2008 R2 SP1</td>
</tr>
<tr>
<td>Device-specific</td>
<td></td>
<td></td>
<td></td>
<td>Any port required by a specific device.</td>
</tr>
</tbody>
</table>

For a complete list of the port requirements for the Orion server, see [Port Requirements](#).
Virtual machine requirements

SolarWinds NTA can 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 SolarWinds NPM requirements for virtual machines. For more information, see the SolarWinds Network Performance Monitor Administrator Guide.
- Each installation of NPM should have its own dedicated network interface controller.

<i>SolarWinds NPM uses SNMP to monitor your network. SNMP traffic is generally assigned low priority, and thus you can experience gaps in monitoring data.</i>

Orion database server (SQL Server) requirements

NPM and your SolarWinds Orion database must use separate servers.

<i>Multiple Orion server installations using the same database are not supported.</i>

<i>If you install on a virtual machine, you must maintain your SQL Server database on a separate, physical drive.</i>

The following table lists software and hardware requirements for your SolarWinds Orion database server using SolarWinds NPM license levels.

<table>
<thead>
<tr>
<th>REQUIREMENTS</th>
<th>SL100, SL250, SL500</th>
<th>SL2000</th>
<th>SLX</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Server</td>
<td>SolarWinds supports Express, Standard, or Enterprise versions of the following:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- SQL Server 2012, 2012 SP1, 2012 SP2, or 2012 SP3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- SQL Server 2014 or 2014 SP1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- SQL Server 2016</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- SQL Server 2017</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- &lt;i&gt;SolarWinds strongly recommends using the 64-bit version of SQL Server.&lt;/i&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- &lt;i&gt;The FullWithSQL installer package automatically installs SQL Server 2014 Express. This is recommended for evaluations.&lt;/i&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- &lt;i&gt;SQL Server Compact Edition 3.5 SP2 is only supported for evaluations.&lt;/i&gt;</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Due to latency effects, SolarWinds does not recommend installing your SQL Server and your Orion server or additional polling engine in different locations across a WAN. For more information, see Install SolarWinds software and SolarWinds database (SQL Server) across a WAN.

You can set the database recovery model to Full Recovery if you use Always On Availability. SolarWinds recommends Simple database recovery mode to ensure best performance.

<table>
<thead>
<tr>
<th>SQL Server collation</th>
<th>English with collation setting</th>
<th>German with collation setting</th>
<th>Japanese with collation setting</th>
<th>Simplified Chinese with collation setting</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SQL_Latin1_General_CP1_CI_AS</td>
<td>German_PhoneBook_CI_AS</td>
<td>Japanese_CI_AS</td>
<td>Chinese_PRC_CI_AS</td>
</tr>
</tbody>
</table>

- We support CI database on an CS SQL Server.
- We do not support case-sensitive databases.

<table>
<thead>
<tr>
<th>CPU speed</th>
<th>Quad core processor or better</th>
<th>Dual quad core processor or better</th>
<th>Dual quad core processor or better</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hard drive space</td>
<td>20 GB minimum</td>
<td>50 GB minimum</td>
<td>100 GB minimum</td>
</tr>
<tr>
<td></td>
<td>40 GB recommended</td>
<td>100 GB recommended</td>
<td>400 GB recommended</td>
</tr>
</tbody>
</table>

SolarWinds recommends the following configuration:

- A hardware RAID Controller with a battery backed-up write back cache
- Disk Subsystem 1 Array 1: 2x 146 GB 15K disks RAID 1 (mirroring) for the OS
<table>
<thead>
<tr>
<th>REQUIREMENTS</th>
<th>SL100, SL250, SL500</th>
<th>SL2000</th>
<th>SLX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disc Subsystem 2</td>
<td>Array 2: 2x 146 GB 15K disks RAID 1 (Pagefile + Extra Storage)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk Subsystem 3</td>
<td>Array 3: with 6x 15k 146 GB or 300 GB disks configured in a RAID 1+0 array for your SQL MDF and FILEGROUPS.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk Subsystem 4</td>
<td>Array 4: with 4x 15k 146 GB or 300 GB disks configured in a RAID 1+0 array for your SQL LDF Transaction LOG file</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk Subsystem 5</td>
<td>Array 5: with 4x 15k 146 GB or 300 GB disks configured in a RAID 1+0 array for your tempdb data file</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk Subsystem 6</td>
<td>Array 6: with 4x 15k 146 GB or 300 GB disks configured in a RAID 0 array for your tempdb log file</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Due to intense I/O requirements, a RAID 1+0 drive is strongly recommended for the SolarWinds database, data, and log files with a dedicated drive for the server operating system and tempdb files.
- Other RAID configurations can negatively affect your SQL Server's performance.
### REQUIREMENTS

<table>
<thead>
<tr>
<th>SL100, SL250, SL500</th>
<th>SL2000</th>
<th>SLX</th>
</tr>
</thead>
</table>

- Mirrored drives for the OS and RAID 1+0 for database data files are recommended.
- Solid state drives (SSD) are recommended for all components.

Per Windows standards, some common files may need to be installed on the same drive as your server operating system. You may want to move or expand the Windows or SQL temporary directories.

<table>
<thead>
<tr>
<th>Memory</th>
<th>SL100</th>
<th>SL250 &amp; SL500</th>
<th>SL2000</th>
<th>SLX</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4 GB minimum</td>
<td>8 GB minimum</td>
<td>16 GB minimum</td>
<td>64 GB minimum</td>
</tr>
<tr>
<td></td>
<td>8 GB recommended</td>
<td>16 GB recommended</td>
<td>64 GB recommended</td>
<td>128 GB recommended</td>
</tr>
</tbody>
</table>

- Authentication
  - Both Windows Integrated Authentication and SQL authentication mechanisms are supported.

- Other software
  - If you are managing your SolarWinds Orion database, SolarWinds recommends you install the SQL Server Management Studio component.

  The Installation Wizard installs the following required x86 components if they are not found on your Orion database server:

  - SQL Server System Common Language Runtime (CLR) Types. Orion products use secure SQL CLR stored procedures for selected, non-business data operations to improve overall performance.
  - Microsoft SQL Server Native Client
  - Microsoft SQL Server Management Objects
NTA flow requirements

SolarWinds NTA supports these flow-enabled devices:

<table>
<thead>
<tr>
<th>Flow</th>
<th>Supported Versions</th>
<th>Sampled Flow Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetFlow</td>
<td>v1, v5, and v9</td>
<td>v5 and v9</td>
</tr>
<tr>
<td></td>
<td>NetFlow v9 must have an appropriate template with all required fields.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Some devices using IOS versions export flows without specifying that it is being sampled. SolarWinds NTA processes these flows as unsampled.</td>
</tr>
<tr>
<td>sFlow</td>
<td>v2, v4, and v5</td>
<td>Supported</td>
</tr>
<tr>
<td>J-Flow</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Some devices using JunOS versions export flows without specifying that it is being sampled. SolarWinds NTA processes these flows as unsampled.</td>
</tr>
<tr>
<td>IPFIX</td>
<td>Supports IPFIX generated by ESX 5.1 and later, for IPv4 traffic.</td>
<td>Supported</td>
</tr>
<tr>
<td>NetStream</td>
<td>v5 and v9</td>
<td>Supported</td>
</tr>
<tr>
<td>NetFlow Lite</td>
<td>Supported on the following devices:</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>• Cisco Catalyst 2960-X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cisco Catalyst 2960-XR</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cisco Catalyst 3560-CX</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cisco Catalyst 2960-CX</td>
<td></td>
</tr>
<tr>
<td>Cisco Wireless Controller NetFlow</td>
<td>Supported on the following devices with the ipv4_client_app_flow_record template:</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>• Cisco 2504 WLC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cisco 5508 WLC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cisco 5520 WLC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cisco Flex 7510 WLC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cisco 8510 WLC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cisco 8540 WLC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cisco WiSM2</td>
<td></td>
</tr>
</tbody>
</table>
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, SolarWinds NTA ignores the packets.

Requirements

- The template must include all mandatory fields.
- Where multiple elements are in a group, at least one of them must be included.
- Optional fields are processed into flows if present. If not present, a default value is used.

Mandatory fields for the flow template schema

Mandatory fields are required. If a mandatory field, or at least one field from a group, is not included SolarWinds NTA cannot store flows.

<table>
<thead>
<tr>
<th>Field Type</th>
<th>Field Type Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>4</td>
<td>Layer 4 protocol</td>
</tr>
<tr>
<td>SourceAddress</td>
<td>8</td>
<td>Source IP address</td>
</tr>
<tr>
<td>DestAddress</td>
<td>12</td>
<td>Destination IP address</td>
</tr>
</tbody>
</table>

 Interfaces Group

At least one of the following fields must be included in the template:

<table>
<thead>
<tr>
<th>Field Type</th>
<th>Field Type Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InterfaceRx</td>
<td>10</td>
<td>SNMP ingress interface index</td>
</tr>
<tr>
<td>InterfaceTx</td>
<td>14</td>
<td>SNMP egress interface index</td>
</tr>
</tbody>
</table>

 Bytes Group

At least one of the following fields must be included in the template:

<table>
<thead>
<tr>
<th>Field Type</th>
<th>Field Type Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bytes</td>
<td>1</td>
<td>Delta bytes</td>
</tr>
<tr>
<td>Bytes</td>
<td>85</td>
<td>Total bytes</td>
</tr>
<tr>
<td>OutBytes</td>
<td>23</td>
<td>Out bytes</td>
</tr>
<tr>
<td>InitiatorOctets</td>
<td>231</td>
<td>Initiator bytes</td>
</tr>
<tr>
<td>ResponderOctets</td>
<td>232</td>
<td>Responder bytes</td>
</tr>
</tbody>
</table>

Optional fields for the flow template schema

If the following fields are not included in the template, a default value will be stored. Appropriate resources will thus show *No Data.*
<table>
<thead>
<tr>
<th><strong>FIELD TYPE</strong></th>
<th><strong>FIELD TYPE NUMBER</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>ToS</td>
<td>5</td>
<td>Type of service</td>
</tr>
<tr>
<td>SourceAS</td>
<td>16</td>
<td>Source BGP autonomous system number</td>
</tr>
<tr>
<td>DestAS</td>
<td>17</td>
<td>Destination BGP autonomous system number</td>
</tr>
<tr>
<td>PeerSrcAS</td>
<td>129</td>
<td>Peer source autonomous system number</td>
</tr>
<tr>
<td>PeerDstAS</td>
<td>128</td>
<td>Peer destination autonomous system number</td>
</tr>
<tr>
<td>ApplicationID</td>
<td>95</td>
<td>ID of application detected in NBAR2 flow</td>
</tr>
</tbody>
</table>

**Source Port Group**

At least one of the following fields should be included in the template:

<table>
<thead>
<tr>
<th><strong>FIELD TYPE</strong></th>
<th><strong>FIELD TYPE NUMBER</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>SourcePort</td>
<td>7</td>
<td>Source TCP/UDP port</td>
</tr>
<tr>
<td>UdpSrcPort</td>
<td>180</td>
<td>Source UDP port</td>
</tr>
<tr>
<td>TcpSrcPort</td>
<td>182</td>
<td>Source TPC port</td>
</tr>
</tbody>
</table>

**Destination Port Group**

At least one of the following fields should be included in the template:

<table>
<thead>
<tr>
<th><strong>FIELD TYPE</strong></th>
<th><strong>FIELD TYPE NUMBER</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>DestPort</td>
<td>11</td>
<td>Destination TCP/UDP port</td>
</tr>
<tr>
<td>UdpDstPort</td>
<td>181</td>
<td>Destination UDP port</td>
</tr>
<tr>
<td>TcpDstPort</td>
<td>183</td>
<td>Destination TPC port</td>
</tr>
</tbody>
</table>

**Packets Group**

At least one of the following fields should be included in the template. If no field is included, resources will show 0 in the packets column.

<table>
<thead>
<tr>
<th><strong>FIELD TYPE</strong></th>
<th><strong>FIELD TYPE NUMBER</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets</td>
<td>2</td>
<td>Delta packets</td>
</tr>
<tr>
<td>Packets</td>
<td>86</td>
<td>Total packets</td>
</tr>
<tr>
<td>OutPackets</td>
<td>24</td>
<td>Out packets</td>
</tr>
<tr>
<td>InitiatorPackets</td>
<td>298</td>
<td>Total packets in a flow from the device that triggered the session and remains the same for the life of the session</td>
</tr>
<tr>
<td>ResponderPackets</td>
<td>299</td>
<td>Total packets from the device which</td>
</tr>
<tr>
<td><strong>FIELD TYPE</strong></td>
<td><strong>FIELD TYPE NUMBER</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>replies to the initiator</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Long Flow Detection</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>At least one of the following field pairs should be included in the template for long-flow detection. For example, if including LastSwitched must also include FirstSwitched.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LastSwitched</td>
<td>21</td>
<td>System uptime at which the last packet of this flow was switched</td>
</tr>
<tr>
<td>FirstSwitched</td>
<td>22</td>
<td>System uptime at which the first packet of this flow was switched</td>
</tr>
<tr>
<td>FlowStartSeconds</td>
<td>150</td>
<td>Time in seconds that the flow started</td>
</tr>
<tr>
<td>FlowEndSeconds</td>
<td>151</td>
<td>Time in seconds that the flow ended</td>
</tr>
<tr>
<td>FlowStartMilliseconds</td>
<td>152</td>
<td>Time in milliseconds that the flow started</td>
</tr>
<tr>
<td>FlowEndMilliseconds</td>
<td>153</td>
<td>Time in milliseconds that the flow ended</td>
</tr>
<tr>
<td>FlowStartMicroseconds</td>
<td>154</td>
<td>Time in microseconds that the flow started</td>
</tr>
<tr>
<td>FlowEndMicroseconds</td>
<td>155</td>
<td>Time in microseconds that the flow ended</td>
</tr>
<tr>
<td>FlowStartNanoseconds</td>
<td>156</td>
<td>Time in nanoseconds that the flow started</td>
</tr>
<tr>
<td>FlowEndNanoseconds</td>
<td>157</td>
<td>Time in nanoseconds that the flow ended</td>
</tr>
<tr>
<td>FlowStartDeltaMicroseconds</td>
<td>158</td>
<td>Sets the start delta of the flow</td>
</tr>
<tr>
<td>FlowEndDeltaMicroseconds</td>
<td>159</td>
<td>Sets the end delta of the flow</td>
</tr>
<tr>
<td>FlowDurationMilliseconds</td>
<td>161</td>
<td>Elapsed time in milliseconds of the flow</td>
</tr>
<tr>
<td>FlowDurationMicroseconds</td>
<td>162</td>
<td>Elapsed time in microseconds of the flow</td>
</tr>
</tbody>
</table>

**Cisco WLC Flows**

The following fields must be included for Cisco Wireless devices.

<table>
<thead>
<tr>
<th><strong>FIELD TYPE</strong></th>
<th><strong>FIELD TYPE NUMBER</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Bytes</td>
<td>1</td>
<td>Total bytes</td>
</tr>
<tr>
<td>Packets</td>
<td>2</td>
<td>Total packets</td>
</tr>
<tr>
<td>FlowDirection</td>
<td>61</td>
<td>Direction of the flow defined as Ingress or egress.</td>
</tr>
<tr>
<td>FIELD TYPE</td>
<td>FIELD TYPE NUMBER</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ApplicationID</td>
<td>95</td>
<td>ID of application detected in flow</td>
</tr>
<tr>
<td>PostIPDiffServCodePoint</td>
<td>98</td>
<td>The definition of this Information Element is identical to 'ipDiffServCodePoint', except that it reports a potentially modified value caused by a middlebox function after the packet passed the Observation Point.</td>
</tr>
<tr>
<td>WlanSSID</td>
<td>147</td>
<td>Service Set Identifier or name of the WLAN the wireless device is connected to</td>
</tr>
<tr>
<td>IPDiffServCodePoint</td>
<td>195</td>
<td>Value of a Differentiated Services Code Point (DSCP) encoded in the Differentiated Services field. Differentiated Services field is the most significant six bits of the IPv4 TOS FIELD or the IPv6 Traffic Class field. The value may range from 0 to 63 for this Information Element that encodes only the 6 bits of the Differentiated Services field.</td>
</tr>
<tr>
<td>WirelessStationMacAddress</td>
<td>365</td>
<td>MAC address of a wireless device</td>
</tr>
<tr>
<td>WirelessStationAddressIPv4</td>
<td>366</td>
<td>IPv4 address of a wireless device</td>
</tr>
<tr>
<td>WirelessAPMacAddress</td>
<td>367</td>
<td>MAC address of a wireless access point</td>
</tr>
<tr>
<td>Cisco ASA devices</td>
<td></td>
<td>The following fields must be included for processing flows from Cisco ASA devices.</td>
</tr>
<tr>
<td>FlowID</td>
<td>148</td>
<td>An identifier of a flow that is unique within an observation domain.</td>
</tr>
<tr>
<td>FirewallEvent</td>
<td>233</td>
<td>Indicates a firewall event.</td>
</tr>
</tbody>
</table>
Notes

- If SolarWinds states that SolarWinds NTA supports flow monitoring for a device, at least one of the templates that 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 SolarWinds NTA, SolarWinds has determined that at least one of the templates the device is capable of exporting will satisfy the SolarWinds NTA requirements. For more information, search for NetFlow version 9 flow record format on www.cisco.com.
- 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 Required fields on page 203, but also fields supported by SolarWinds NTA for sampled flows. Supported fields depend on the flow version used.

Sampling mode has to be non-zero, otherwise SolarWinds 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:

<table>
<thead>
<tr>
<th>BYTES</th>
<th>CONTENTS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>22-23</td>
<td>sampling_interval</td>
<td>First two bits hold the sampling mode; remaining 14 bits hold value of sampling interval.</td>
</tr>
</tbody>
</table>


NetFlow v9 and J-Flow v9

Supported fields depend on the template you are using:

- Flow template
- Option template
Flow template

The following fields are optional for the Flow Template Schema. It is enough if the template includes one of the fields in each group.

If at least one from each group is not included in the template, NTA will still be able to store flows. However, a default value will be stored, and appropriate resources will show the "No Data" message.

<table>
<thead>
<tr>
<th>FIELD TYPE</th>
<th>FIELD TYPE NUMBER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sampling Interval Group</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SamplingInterval</td>
<td>34</td>
<td>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.</td>
</tr>
<tr>
<td>SamplerInterval</td>
<td>50</td>
<td>Packet interval at which to sample.</td>
</tr>
<tr>
<td>Sampling Algorithm Group</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SamplingAlgorithm</td>
<td>35</td>
<td>The type of algorithm used for sampled NetFlow: 0x01 Deterministic Sampling, 0x02 Random Sampling</td>
</tr>
<tr>
<td>SamplerMode</td>
<td>49</td>
<td>The type of algorithm used for sampling data: 0x02 random sampling.</td>
</tr>
</tbody>
</table>

Option template

Mandatory fields

If you are using the Option Flow Template, make sure at least one field from each group is included. Otherwise, flow data cannot be stored.

<table>
<thead>
<tr>
<th>FIELD TYPE</th>
<th>FIELD TYPE NUMBER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sampling Interval Group</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SamplingInterval</td>
<td>34</td>
<td>When using sampled NetFlow, the rate at which packets are</td>
</tr>
<tr>
<td>FIELD TYPE</td>
<td>FIELD TYPE NUMBER</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SamplerInterval</td>
<td>34</td>
<td>Packet interval at which to sample.</td>
</tr>
</tbody>
</table>

**Sampling Algorithm Group**

<table>
<thead>
<tr>
<th>SamplingAlgorithm</th>
<th>35</th>
<th>The type of algorithm used for sampled NetFlow: 0x01 Deterministic Sampling, 0x02 Random Sampling.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SamplerMode</td>
<td>35</td>
<td>The type of algorithm used for sampling data: 0x02 random sampling.</td>
</tr>
</tbody>
</table>

**SamplerID**

If the SamplerID isn't included in the options flow template, a default value will be stored, and appropriate resources will display "No Data".
**Field Type** | **Field Type Number** | **Description**
--- | --- | ---
SamplerID | 48 | Identifier shown in *show flow-sampler*.

For more information, search for NetFlow version 9 flow record format.

**Autonomous system requirements**

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

[1] SolarWinds 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:

<table>
<thead>
<tr>
<th>Bytes</th>
<th>Contents</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>40-41</td>
<td>src_as</td>
<td>Autonomous system number</td>
</tr>
<tr>
<td>42-43</td>
<td>dst_as</td>
<td>Autonomous system number</td>
</tr>
</tbody>
</table>

For more information, search for NetFlow export datagram format on [www.cisco.com](http://www.cisco.com).

**NetFlow v9, IPFIX, and compatible flows**

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

<table>
<thead>
<tr>
<th>Field Type</th>
<th>Value</th>
<th>Length (Bytes)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRC_AS</td>
<td>16</td>
<td>N (default 2)</td>
<td>Source BGP autonomous system number where N could be 2 or 4.</td>
</tr>
<tr>
<td>DST_AS</td>
<td>17</td>
<td>N (default 2)</td>
<td>Destination BGP autonomous system number where N could be 2 or 4.</td>
</tr>
<tr>
<td>PeerSrcAS</td>
<td>129</td>
<td>N (default 2)</td>
<td>Peer source autonomous system number</td>
</tr>
<tr>
<td>PeerDstAS</td>
<td>128</td>
<td>N (default 2)</td>
<td>Peer destination autonomous system number</td>
</tr>
</tbody>
</table>

**SolarWinds NTA deployment options**

SolarWinds NTA is a flexible solution providing you with various deployment options that fit with your organization's needs.

SolarWinds NTA 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.

**Install a localized version of SolarWinds NTA**

SolarWinds NTA is available in English and Japanese. When referring to the localized content, SolarWinds documentation uses the following terms:

**Primary Locale**

The locale selected when installing SolarWinds NPM. Once selected, you cannot change the Primary Locale without uninstalled and reinstalling SolarWinds NPM. SolarWinds NTA uses the Primary Locale.

**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.

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.

**Install a localized version of SolarWinds NTA**

1. When installing SolarWinds NPM, select the language you want to use in SolarWinds NTA as the preferred language.
   SolarWinds NTA is not available in German. If you select German as your preferred language during the SolarWinds NPM installation, SolarWinds NTA will install in English.

2. Install SolarWinds NTA.
Upgrade a localized version of SolarWinds NTA

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

1. Reinstall SolarWinds NPM using the required locale.
2. Reinstall SolarWinds NTA.

Reports and alerts created in older SolarWinds 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.

Install SolarWinds NTA and NTA Flow Storage Database locally

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

SolarWinds recommends 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 SolarWinds NTA or SolarWinds NPM, the potential performance improvement is not so significant as it could be if the database were on a separate server.

1. Install SolarWinds NTA and NTA Flow Storage Database.
2. Select a licensing options.
3. Configure your SolarWinds NTA and local NTA Flow Storage Database.
4. Define the location for NTA Flow Storage Database by filling in an absolute path to the appropriate folder.

Install SolarWinds NTA and a remote NTA Flow Storage Database

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

1. Make sure you have SolarWinds NPM installed on the server where you want to install SolarWinds NTA.
   Note the credentials for accessing the SolarWinds Orion database used by SolarWinds NPM. You will need them to configure the NTA Flow Storage Database.
2. Log in to your NTA Flow Storage Database server, install, and configure the remote NTA Flow Storage Database.
   a. Log in to the SolarWinds NPM server and install SolarWinds NTA only.
   b. Start the Setup wizard and select the installation option SolarWinds NPM/SolarWinds NTA and NTA Flow Storage Database on Two Separate Servers.
   c. Enter the NTA Flow Storage Database Server hostname or IP address.
3. Select one of the available licensing options.
4. Proceed to add your NetFlow devices and interfaces to SolarWinds NPM.

Install an additional poller and web console

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

Additional pollers help with 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.

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

Requirements

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

Install an additional poller or web console

1. Log in to the server where you want to install the additional poller or website.
2. Launch the SolarWinds NTA installation file.
   - The SolarWinds NTA installer will automatically discover that you are installing an additional poller or website, because it detects that a SolarWinds NPM additional poller or website is available on the server.
3. Complete the installation.
Install SolarWinds NTA

Deployment options

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

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

The installation differs according to the selected deployment.

Install SolarWinds NTA

1. Log in to the SolarWinds NPM server that you want to use for NetFlow traffic analysis.
2. Launch the installation file from the download location.
3. Review the Welcome information, and click Next.
4. Select the configuration, and click Next.
   - 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.
     Fill in the NTA Flow Storage Database Server hostname or IP address, and then click Test Connection.
   - NPM/NTA/NTA Flow Storage Database on the Same Server.
     This option is recommended for evaluations. SolarWinds 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.
5. If you agree, accept the license agreement, and click Next.
6. Click Install.
7. When the installation completes, click Finish.

Complete the Configuration wizard

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

1. If the Configuration wizard does not start automatically, start the Configuration wizard in the Orion Configuration and Auto-Discovery folder.
2. Review the Welcome text, and click Next.
3. Confirm that SolarWinds NetFlow Traffic Analyzer Service is selected in the Service Settings window, and click Next.

4. Enter 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.
   - The path should contain only ASCII characters.
   - The defined folder should be located on a dedicated local NTFS drive, not on the system drive.

5. Enter an absolute path for storing your backups into the Backup NTA Flow Storage Database Data File Path field or click Browse to navigate to the appropriate location.

6. Click Next.

7. Review the configuration summary, and click Next.

8. Click Finish.

Install the NTA Flow Storage Database

Recommendations and requirements

- To maximize performance, SolarWinds recommends storing your flow data on a server which is different from your SolarWinds NTA and SolarWinds NPM server.
- Make sure the NTA Flow Storage Database server complies with the NTA Flow Storage Database requirements.
- Make sure the appropriate SolarWinds NPM version is already installed on the SolarWinds NPM/SolarWinds NTA server. To install NTA Flow Storage Database, you need the appropriate hostname or IP address of the SolarWinds Orion database server, the appropriate SolarWinds Orion database name, and credentials.

Install the NTA Flow Storage Database

1. Log in to the server where you want to store your flow data.
2. Launch the installation file from the download location.
3. Review the Welcome information, and click Next.
4. Select I Would Like to Install the NTA Flow Storage Database on This Server.
5. Enter the details for accessing the SolarWinds Orion 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 user name and password: enter the SQL database credentials.
      - The default Orion database user name is SolarWindsOrionDatabaseUser. You specified the password in the Configuration wizard while installing SolarWinds NPM.
   c. Select the appropriate database, and click Test Connection.
   d. Click Next to continue.
6. If you agree, accept the license agreement, and click Next.
7. Specify the installation folder, and click Next.
8. Click Install.
9. When the installation completes, click Finish.

Configure a remote NTA Flow Storage Database

NTA Flow Storage Database recommendations

- Make sure you save your flow data on a dedicated disk.
- The NTA Flow Storage Database folder must be empty or contain the appropriate NTA Flow Storage Database version.
- The folder path must be a valid URI, and SolarWinds 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 required. You can define it later.

Specify the NTA Flow Storage Database destination

1. If the Configuration wizard does not start automatically, start the Configuration wizard in the Orion Configuration and Auto-Discovery folder.
2. Enter 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.
   - The path should contain only ASCII characters.
   - The defined folder should be located on a dedicated local NTFS drive, not on the system drive.
3. Enter an absolute path for storing your backups into the Backup NTA Flow Storage Database Data File Path field or click Browse to navigate to the appropriate location.
4. Click OK.

Upgrade SolarWinds NTA

You can upgrade SolarWinds NTA from a previous version or upgrade the licensed number of elements you can monitor. If SolarWinds NTA is being upgraded, it cannot display data until the upgrade completes.

For information about upgrading your Orion Platform products see the SolarWinds Upgrade Guide. The guides include all gotchas, preflight and preparation checklists, and installation steps.

- For a single product upgrade, follow the NTA Upgrade Guide.
- For multi-module product upgrades, follow the multiple product upgrade guide.

For details on NTA compatibility, you can review the upgrade and compatibility path information and use the Product Upgrade Advisor to build the upgrade path.
Upgrade paths and compatibility

SolarWinds NTA versions are compatible with specific versions of SolarWinds NPM.

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

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

We recommend using the Product Upgrade Advisor to determine your upgrade path for a single or multi-module environment.

Note that versions 3.7 and 3.9 are no longer supported.

### Compatibility table

<table>
<thead>
<tr>
<th></th>
<th>NPM 10.4.2/Orion Platform 2012.2.x</th>
<th>NPM 10.5.x/Orion Platform 2013.1.x</th>
<th>NPM 10.6.x/Orion Platform 2013.2.x</th>
<th>NPM 10.7.x/Orion Platform 2014.1.x</th>
<th>NPM 11.0.x/Orion Platform 2014.2.x</th>
<th>NPM 11.5.x/Orion Platform 2015.2.x</th>
<th>NPM 12.0.x/Orion Platform 2016.x&gt;</th>
<th>NPM 12.1/Orion Platform 2017.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTA 3.11</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>NTA 4.0.x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTA 4.1</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTA 4.1.1</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTA 4.1.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>NTA 4.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>NTA 4.2.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>NTA 4.2.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

### Notes

- If a primary poller is running on a 64-bit operating system, all pollers must be 64-bit also.
- SolarWinds NTA 4.0.x is the last version supporting 32-bit operating systems.
- You cannot upgrade SolarWinds NTA to use a different locale. SolarWinds NTA uses locale settings of the underlying SolarWinds NPM installation. If you want to change the locale settings, you must install SolarWinds NPM using the appropriate locale, and then install SolarWinds NTA.
- SolarWinds does not currently support upgrades from one locale to another. If you want to upgrade your SolarWinds installation to use a new locale, you must complete a clean SolarWinds installation using the new locale.
- While it is being upgraded, your Orion polling engine temporarily shuts down which may result in polling data loss. SolarWinds recommends that you perform upgrades during off-peak hours of network usage to minimize the impact of this temporary polling stoppage.
Discovery profiles from older SolarWinds NPM versions are not retained through upgrades. If you want to retain a discovery profile, prior to starting your upgrade, externally record the configuration of the profiles you want to retain.

**Database migration**

For migration options, such as moving NTA databases to a new server, see the SolarWinds Migration Guide. We provide guides for migrating the NTA Flow Storage Database (FSDB) using a few different scenarios:

- Migrating to a new remote server from a current remote server or from the local disk
- Migrating from a remote server to the local disk
- Migrating to another disk drive or partition on the same local disk

If you need to migrate the NTA product, you can migrate NTA to a new server using the same or a new IP and hostname.

**Migrating flow data from the Orion SQL database**

If you are upgrading SolarWinds NTA from a previous version that stored flows in the SolarWinds Orion database (NTA 4.0 or earlier), you have the option to migrate your flow data from the SolarWinds Orion database to the NTA Flow Storage Database.

The database migration starts in the Configuration wizard when you upgrade SolarWinds NTA. Migration runs as a background process, but may take time and affect the performance of SolarWinds NTA. You can check the migration progress in the Orion Web Console notification bar at any time.

All FSDB guides includes detailed instructions for the migration of this data.

**Uninstall SolarWinds NTA**

To remove SolarWinds NTA from a server, access the product through the Windows Control Panel:

1. Start Programs and Features in the Windows Control Panel.
3. Uninstall SolarWinds NTA on all poller servers, and on the NTA Flow Storage Database server as well.

For further information and assistance with uninstalling your product, contact Support.
Get started with SolarWinds NTA

If you need to know who is using your bandwidth and how, SolarWinds NTA provides a simple answer. You can quickly trace and monitor the bandwidth use of a specific application or type of traffic. For example, if you see excessive bandwidth use on an interface, you can use SolarWinds NTA to see that the company meeting, that includes streaming video, is consuming 80% of the available bandwidth through a switch. Unlike many other NetFlow analysis products, the network and flow data presented in SolarWinds NTA are not purely extrapolated data, but they are based on real information collected about the network by SolarWinds Network Performance Monitor, on which SolarWinds NTA depends.

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
- Patterns of use over time
- External traffic identification and tracking
- Tight integration with detailed interface performance statistics

SolarWinds NTA is optimized for understanding network use, not auditing every packet. SolarWinds NTA provides an overall traffic summary and how users are using your bandwidth.

Set up flow monitoring

To begin analyzing available flow data produced by devices in your network, install SolarWinds NTA, set up devices to export flow data, add your devices to SolarWinds NPM, and define what devices you want to monitor.

The following list provides the task order in which you need to set up flow monitoring:

1. Set up your network devices to export flow data.
2. Add your network devices to SolarWinds NPM.
3. (Optional) Verify that your collector services are up and listening on the correct port.
5. (Optional) Verify that SolarWinds NTA is monitoring applications, services, ports, and protocols.
6. Allow time for SolarWinds NTA to collect flow or CBQoS data. Collected data are displayed in the SolarWinds NTA resources.

Set up network devices to export NetFlow data

To facilitate traffic analysis on Cisco IOS enabled devices, NetFlow begins polling at the network device. To communicate the traffic-related data about a device, the device must be configured to send, push, or export that data to collection targets.
SolarWinds NTA collects NetFlow data on port 2055 by default, only if a network device is configured to send to it. As a NetFlow collector, SolarWinds NTA can receive exported NetFlow version 5 data and NetFlow version 9 data that includes all fields of the NetFlow version 5 template. After it collects NetFlow traffic data, SolarWinds NTA analyzes device bandwidth usage in terms of the source and destination endpoints of conversations reflected in the traffic.

Requirements for setting up network devices

- Each device must be configured to export NetFlow data to SolarWinds NTA.
- Each device that exports NetFlow data to SolarWinds NTA must be monitored in SolarWinds NPM. Only SNMP-capable nodes whose interfaces were discovered by SolarWinds NPM can be added as NetFlow sources.

> Traffic from a device that is not monitored in SolarWinds NPM is displayed only in aggregate as traffic from unmonitored devices. If the device is setup to export data to SolarWinds NTA, but is unmonitored in SolarWinds NPM, the collector receives the data without being able to analyze it.

- The interface index number for this interface in the SolarWinds Orion database (interface table) must match the index number in the collected flow data.
Set up a device to export NetFlow data to SolarWinds NTA

1. Log in to the network device.
2. Enable NetFlow export on the device using commands. The following example enables NetFlow on a Cisco device:

```
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, search for an appropriate configuration guide on the Cisco website.
- For information on enabling NetFlow for Cisco Catalyst switches, see Enable NetFlow and NetFlow data export on Cisco Catalyst switches.
- For information on enabling NetFlow on Cisco ASA devices, see Cisco ASA NetFlow overview.
- Otherwise, consult these examples:
  - Brocade (Foundry) sFlow configuration
  - HP sFlow configuration
  - Extreme sFlow configuration
  - Juniper sFlow configuration
  - Juniper J-Flow configuration

3. Add the device exporting NetFlow to SolarWinds NPM for monitoring.
   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 SolarWinds 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 Orion Web Console in the SolarWinds Network Performance Monitor Administrator Guide.
Verify that the device is exporting NetFlow data and that the device is monitored in SolarWinds NPM. To verify that data are exported correctly, use a packet capture tool, such as WireShark, to search for packets sent from the network device to the Orion server. The following is an example of a successfully enabled NetFlow device.

If you successfully add a NetFlow enabled device with the IP address 10.199.14.2 to SolarWinds NPM, and the device is actively exporting NetFlow data to the Orion server, you will see in WireShark a packet like the one highlighted below in gray:

As expected, the packet details show that 10.199.14.2 is its source IP address and 10.110.6.113 is the destination, which is the Orion server. This correlates with the node details on the device in Orion (highlighted in yellow).

To verify that the IP address of the exporting interface on the network device is the one being monitored in Orion:

a. Open a command line interface, log in to the network device, and then enter `show run` to see the running configuration of the device.

b. Page down to the lines where the export source interface is defined. In this example, it is `ip flow-export source Ethernet0/0`.

To discover the IP address for this interface, enter `show run int Ethernet0/0`. The IP address of the interface, 10.199.14.2, is monitored by the Orion server.

5. Click My Dashboards > NetFlow > NTA Summary.

Under NetFlow Source, verify the NetFlow-enabled nodes listed with a recent time posted for collected flow.

Exporting both ingress and egress NetFlow traffic data

Flows carrying NetFlow traffic data enter a device through an ingress interface and leave the device through an egress interface. For more information, see Monitor traffic flow directions.

If you export both ingress and egress data for all interfaces, you get the same data twice: once as ingress data entering the device, and once as egress data as the flow leaves the device.

If you configure exporting ingress data on some interfaces and exporting egress data on other interfaces, the data shown by SolarWinds NTA may be inconsistent.

SolarWinds recommends that you configure exporting either ingress or egress data to prevent SolarWinds NTA from showing misleading traffic data.
Add flow-enabled devices and interfaces to the Orion database

SolarWinds NTA collects flow data from your network devices and analyzes network traffic based on collected data.

To collect flow data, you must specify the SolarWinds NTA server as a target to which each device exports data. For more information, see Set up network devices to export NetFlow data.

To analyze flow data, you must add each flow-enabled network interface to the SolarWinds Orion database, so that they can be monitored in SolarWinds NPM.

To initiate flow monitoring, flow-enabled devices in the SolarWinds Orion database must be designated as flow sources. For more information, see Manually add flow sources and CBQoS-enabled devices.

1. Add nodes to SolarWinds NPM.
   - If you are adding a large number of nodes, use Network Sonar Discovery.
   - If you are only adding a few nodes, it may be easier to use Web Node Management in the Orion Web Console.
2. Click My Dashboards > Home > Summary.
3. Under All Nodes, verify that the devices were added.
4. To finish setting up NetFlow monitoring, enable NetFlow monitoring for the selected nodes.

For more information, see Manually add flow sources and CBQoS-enabled devices.

If you have configured device interfaces to send flow data, SolarWinds NTA can detect and analyze flow data after the device is added.

What happens after you add devices and interfaces to the Orion database?

- After installing SolarWinds NTA, the SolarWinds NPM polling engine establishes a baseline by collecting network status and statistics.
- Thirty seconds later, the SolarWinds NPM polling engine performs another collection. You may notice an increase in the CPU usage during this time.
- After these initial collections, SolarWinds NPM collects network information every ten minutes for nodes and every nine minutes for interfaces. Flow analysis data are displayed in the Orion Web Console in minutes.

Before leaving SolarWinds NTA to gather data, ensure you are collecting flow data for the correct interface ports and applications. For more information, see Applications and service ports.

Manually add flow sources and CBQoS-enabled devices

You can add flow-enabled devices managed by SolarWinds NPM for monitoring to SolarWinds NTA.
For more information about the automatic addition of flow sources, see Enable the automatic addition of flow sources.

Notes on adding sources and devices

- Make sure the devices you want to monitor with SolarWinds NTA are monitored in SolarWinds 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 timeout rate of 30 minutes. If NetFlow version 9 flows arrive without a usable template, SolarWinds NTA raises an event every 15 minutes. Configure your device to export a template every one minute, so that the version 9 flows show up in SolarWinds NTA without delay.
- See NTA flow requirements for more information.
- Only an SNMP node can be added as a NetFlow Source.

Add flow sources and CBQoS-enabled devices for monitoring

1. Click My Dashboards > NetFlow > NTA Summary.
2. Under NetFlow Sources, click Manage Sources.
   If you enable automatic addition of NetFlow sources, all flow sources currently monitored by NPM display in the NetFlow Sources resource. For more information about the automatic addition of flow sources, see Enable the automatic addition of flow sources.
3. Select a filter in the Show list to display devices where you want to monitor NetFlow or CBQoS data.
   - Exporters Only (Last 15 Minutes): Displays 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.
4. Locate a device or interface, and then select NetFlow, CBQoS, or both to define what is monitored. CBQoS monitoring is only available for Cisco devices.
   For more information about setting sampling, see Set the sampling rate manually.
5. Click Submit.

Enable the automatic addition of flow sources

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

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
4. Click Save.
Set up NBAR2 on Cisco devices

Network Based Application Recognition (NBAR) is the mechanism used by certain Cisco routers and switches to recognize a dataflow by inspecting some of the packets sent. SolarWinds NTA 4.2.3 supports unknown traffic detection and advanced application recognition through NBAR2.

To analyze NBAR2 data, configure your Cisco devices to send NBAR2 data to SolarWinds NTA. Second, add those devices as nodes in SolarWinds NPM and SolarWinds NTA.

The following are examples used in the commands below:

- NTArecc
- NTAexp
- NTAmone
- GigabitEthernet0/1
- 10.10.10.10

Create a Flexible NetFlow configuration

Add the flow record

This process is similar to creating a standard NetFlow configuration. In this case, you add the collect application name command to enable an AppID to send in each flow.

```bash
flow record NTArecc
  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
  collect application name
exit
```

Add the flow exporter

To send a list of automatically or manually created applications to be NBAR2 classified, use the option application-table command. The option application-attributes command enables the sending of categories for all applications.

```bash
flow exporter NTAexp
  destination 10.10.10.10
  source GigabitEthernet0/1
```
Add the flow monitor

The flow monitor connects the flow recorder and the flow exporter. You can configure multiple recorders, exporters, and monitors at the same time.

```
flow monitor NTAmon
  description NetFlow nbar
  record NTArec
  exporter NTAexp
  cache timeout inactive 30
  cache timeout active 60
exit
```

When you receive long flows, the values may need to be adjusted, see *Troubleshoot Long Flow Errors* for more details. For more information about the timeout values, refer to the Cisco NetFlow Command Reference.

Add the flow monitor to an interface

Assign the Flexible NetFlow configuration to the interface from which to monitor NetFlow.

```
interface GigabitEthernet0/1
  ip flow monitor NTAmon input
  ip flow monitor NTAmon output
exit
```

Diagnostic commands

- `show flow record "recordName"
- `show flow export "exporterName"
- `show flow monitor "monitorName"
- `show flow exporter statistics
- `show flow interface

Determine the applications your device can recognize

The Protocol Pack is a list of applications, definitions, and categories that your device can recognize.
Check the Protocol Pack version

```
show ip nbar version
```

View a list of the available applications

```
show ip nbar protocol-id
```

Edit an existing record

If you edit an existing record that is in use, you receive the following error:

```
% Flow Record: Flow Record is in use. Remove from all clients before editing.
```

To resolve this error, disable the connection between the monitor, record, and interface.

Disable the connection

```
interface GigabitEthernet0/1
  no ip flow monitor NTMon input
  no ip flow monitor NTMon output
exit
```

Add the application recognition field into the record

```
flow record NTAre
collect application name
exit
```

Add the application recognition field into the exporter

```
flow exporter NTAexp
  option application-table timeout 60
  option application-attributes timeout 300
```

Restore the connection

```
interface GigabitEthernet0/1
  ip flow monitor NTMon input
  ip flow monitor NTMon output
exit
```
NBAR2 Advanced Applications

SolarWinds NTA monitors Network Based Application Recognition (NBAR2) traffic. NBAR2 is an application classification system that is used with deep packet inspection technologies to provide better visibility into network traffic.

After you have enabled your devices to export NBAR2 flow records, you can view the Top NBAR2 Applications in summary views and reports.

When the netflow data is captured by NTA, the advanced application classification may be unavailable or unknown to NTA. In this case, you see one of the following identifiers for applications that are unidentified.

- **Unknown** — a Cisco application for which there is no classification available from Cisco.
- **Unclassified** — an application that is not supported or recognized by the NBAR engine on Wireless LAN Controller traffic.
- **Unrecognized** — an application that NTA is not able to identify based on information in the current NBAR2 database. This happens when NBAR2 is enabled on a device and it begins sending flows before sending the applications database. This occurrence depends on the interval set in the device settings.
- **Remaining traffic** — this is a standard label used on NTA charts to represent monitored traffic that is not applicable to any category presented on the chart.

You can monitor NBAR2 applications by viewing the Top XX Applications or from the NetFlow Applications Summary view. For more information about monitoring applications, see Monitor NBAR2 Applications in SolarWinds NTA.

NBAR2 requirement for monitoring application IDs

To monitor advanced applications, the following field must be included in the option template for NBAR2 flows.

<table>
<thead>
<tr>
<th><strong>FIELD TYPE</strong></th>
<th><strong>FIELD TYPE NUMBER</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Application ID</td>
<td>95</td>
<td>ID of application detected in NBAR2 flow</td>
</tr>
</tbody>
</table>

You also need to set the Required fields in the template for flow collection.
SolarWinds NTA settings

You can use SolarWinds NTA to customize monitoring flow traffic and CBQoS data on your network to provide the most relevant information.

Use the NetFlow Settings page to configure which flows you want to connect. You can also select which services you want to monitor, including:

- Applications
- Autonomous systems
- IP address groups
- Protocols
- Flow sources
- CBQoS devices
- Collector services

You can also optimize SolarWinds NTA performance by changing your settings for your top talkers, database, or SolarWinds NTA charts.

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.

SolarWinds NTA settings

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

The configuration actions detailed below require administrative access to the Orion Web Console.

NetFlow management

Configure default behavior when flows from SolarWinds NPM devices are received, towards data from ports not monitored in SolarWinds NTA, and unmanaged interfaces. For more information, see the NetFlow Management.

Application and service ports

Configure the ports and applications to monitor in SolarWinds NTA. For more information, see Applications and service ports.

Autonomous systems

Manage autonomous systems monitored in SolarWinds NTA. For more information, see Manage autonomous systems.
**IP address groups**

Manage IP address groups and select IP groups whose traffic you want to monitor in SolarWinds NTA. For more information, see [IP address groups](#).

**Monitored protocols**

Select which protocols you want to monitor in SolarWinds NTA. For more information, see [Monitored protocols](#).

**NetFlow sources**

Select which flow sources and CBQoS devices to monitor in SolarWinds NTA. Change the sample rate for sampled flows or configure NetFlow export on Cisco devices directly from the Orion Web Console. For more information, see [NetFlow sources and CBQoS polling](#).

**NetFlow collector services**

Add or change ports on which the NetFlow service is listening. For more information, see [NetFlow collector services](#).

**Types of services**

Change names used for DiffServ Code Points in SolarWinds NTA. For more information, see [Types of services](#).

**NetFlow management**

The NetFlow Management options detailed below ensure that you are able see all flow data available from flow-enabled devices on your monitored network. On new installations, all the options are enabled by default.

- Due to the volume of data involved in flow monitoring, you may find it necessary to disable the inclusive monitoring options to save database space.
- Only SNMP nodes, which is an interface on the node, can be added as a NetFlow Source.

**Enable automatic addition of NetFlow sources**

All flow-enabled devices in the Orion database sending flow data to the server hosting SolarWinds NTA are automatically added as NetFlow sources. All recognized NetFlow sources are listed under NetFlow Sources on NTA Summary.

**Allow monitoring of flows from unmonitored ports**

SolarWinds 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 under Top XX Applications, you can expand the tree to drill down to the interface level. Click Monitor Port to track this traffic by port.
This option may significantly increase the processing load on both your SolarWinds NTA server and your SolarWinds Orion database server. To save space in your database and discard data from unmonitored ports, clear this option.

**Allow monitoring of flows from unmanaged interfaces**

SolarWinds NTA automatically monitors flow packets even if one of the interfaces is not managed by SolarWinds NPM.

If you want SolarWinds NTA to discard any flow packets where only one of the involved interfaces is managed by SolarWinds NPM, clear this option.

Clearing this option may significantly decrease the processing load on both your SolarWinds NTA server and your SolarWinds Orion database server, but it also decreases the amount of flow data stored in your SolarWinds Orion database.

**Allow matching nodes by another IP address**

SolarWinds NTA automatically associates a flow with a SolarWinds NPM node if the node has multiple IP addresses and is sending flows from a non-primary address.

**Show notification bar for unknown traffic events**

If an unknown traffic event occurs, SolarWinds NTA notifies you in the yellow banner below the main tool bar.

**Show unknown traffic events**

Click this link to navigate to the Last 200 Unknown Traffic Events page. This page provides a list of traffic events involving flow data received from an unmanaged interface. You can use that page to add the relevant interface to NetFlow Sources. For more details, see [Resolving Unknown Traffic](#).

**Applications and service ports**

Use SolarWinds NTA to directly specify the applications and ports you want to monitor. Additionally, you can specify protocol types by application, giving you the ability to monitor multiple applications on the same port if each application uses a different protocol. You should review this list of ports and applications and check the ports and applications you want to monitor, adding any that are not present.

By default, SolarWinds NTA monitors recommended ports and applications that are used most on typical networks.

SolarWinds NTA supports many applications out of the box. However, if you have custom internal applications, remember to assign a port name and number to them so that they are reported and not marked unknown.
Access the applications and service ports settings

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Click Application and Service Ports.

Configure data retention for flows on unmonitored ports

By default, SolarWinds NTA retains all flow data provided by NetFlow sources on your network, including flow data for ports that you are not actively monitoring.

If you see a significant percentage of unmonitored traffic in your Top XX Application resource, expand the tree and drill down to the interface level. Click Monitor Port in the Orion Web Console to track this traffic by port.

For more information about unmonitored ports in SolarWinds NTA, see Enable flow monitoring from unmanageable interfaces.

Enabling this option may significantly increase the processing load on both your SolarWinds NTA server and your SolarWinds Orion database server. Clear the Allow monitoring of flows from unmonitored ports field to save space in your database and discard data from unmonitored ports.

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Select Allow monitoring of flows from unmonitored ports.
4. Click Save.

Monitor applications and service ports

Because of the volume of data from flow-enabled network devices, monitoring all ports and applications may severely affect the performance of both the Orion database and the Orion Web Console.

You can decide what ports or applications should be monitored by SolarWinds NTA. If you are not sure what ports and applications you should monitor, click Monitor Recommended Ports to monitor the most common high traffic ports and applications.

Clicking Monitor Recommended Ports deletes all existing custom application and port definitions.

To enable this option, you need to first access the management page

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Click Application and Service Ports.
Enable monitoring for ports or applications

1. To enable monitoring an application or a port, click Enable in the Actions column.
2. To enable monitoring for all listed applications and ports, click Enable All Monitoring.
3. If you are not sure what ports and applications to monitor, click Monitor Recommended Ports.
4. Click Submit.

Disable monitoring for ports or applications

1. To disable monitoring an application or a port, click Disable in the Actions column.
2. To disable monitoring for all listed applications and ports, click Disable All Monitoring.
3. Click Submit.

Add applications and service ports to NTA

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Click Application and Service Ports.
4. Click Add Application.
5. Enter the application and port information.
6. Click Add Application.
7. Click Submit.

Edit applications and service ports

You can edit the name, port number, source and destination IP addresses, or protocols of an application or service.

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Click Application and Service Ports.
4. Find the application or service port you want to edit:
   - Use the View list to filter the applications and service ports.
   - Applications are listed by ascending port number, with multi-port applications listed first.
   - Use the Search function to filter the list further.
5. Click Edit in the Actions column of the application or port.
6. Edit the application and port information.
7. Click Update Application.
8. Click Submit.
Overlapping ports for multi-port applications

If multi-port applications are configured with overlapping port assignments, traffic is only associated with one of the conflicting applications.

You can remove the port range in conflict, disable a conflicting application, or delete the port or application to avoid overlapping port assignments.

Delete applications and service ports

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Click Application and Service Ports.
4. Click Delete in the Actions column of the application or port.
5. Click Delete Application.
6. Click Submit.

Autonomous systems

To manage autonomous systems in NTA, enter the autonomous systems information in the NTA settings.

For information about NTA requirements for monitoring autonomous systems via BGP, see the Autonomous system requirements.

Access autonomous systems

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Click Autonomous Systems.

Add autonomous systems

1. Click Add Autonomous Systems.
2. Enter the autonomous system information.
3. Click Save.

Edit autonomous systems

1. Click Edit in the Actions column of the autonomous system.
2. Edit the autonomous system information.
3. Click Save.

Delete autonomous systems

1. Click Delete in the Actions column of the autonomous system.
2. Click Delete.
IP address groups

Use SolarWinds NTA to establish IP address groups for selective monitoring of custom categories or segments of your network.

With well-defined IP groups, you can better characterize and assess NetFlow data that you receive.

SolarWinds recommends creating IP Address Groups, for example by location, especially for the benefit of your first level support group, to quickly see IP Address ranges and makes things easier to manage.

Add IP address groups

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Under IP Address Groups, click Manage IP Address Groups.
4. Click Add New Group.
5. Enter a Description.
6. Add the IP address or IP address group:
   - To define the selected group as a single IP address, select IP Address, and enter the IP address.
   - To define the selected group as a range of IP addresses, select IP Range, and provide the starting and ending IP addresses.
   - To include this defined group, if eligible, in Top XX IP Address Groups resources, select the Enable Display in Top XX IP Address Groups Resource.
   - To define another IP Address group, click Add, and repeat the preceding steps.
7. Click OK.
8. Click Submit. For more information, see Submit changes.

Delete IP address groups

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Under IP Address Groups, click Manage IP Address Groups.
4. Click Delete at the end of the an IP address group row.
5. Click Submit. For more information, see Submit changes.
Edit IP address groups

In SolarWinds NTA, you can edit monitored IP addresses and IP address groups. You can also select which groups you want to see in the Top XX IP Address Groups resource.

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Under IP Address Groups, click Manage IP Address Groups.
4. Click Edit next to an IP address group.
5. Edit the Description.
6. Make edits:
   - To define the selected group as a single IP address, select IP Address, and enter the IP address.
   - To define the selected group as a range of IP addresses, select IP Range, and provide the starting and ending IP addresses.
   - To include this defined group, if eligible, in Top XX IP Address Groups resources, select the Enable Display in Top XX IP Address Groups Resource.
   - To define another IP Address group, click Add, and repeat the preceding steps.
7. Click OK.
8. Click Submit. For more information, see Submit changes.

Select IP ranges to monitor

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Under IP Address Groups, click Manage IP Address Groups.
4. If any one of the existing ranges contains the addresses you want SolarWinds NTA to monitor, make sure that the corresponding box in the Enable column is selected.
5. Click Submit. For more information, see Submit changes.

Monitored protocols

Specify which protocols SolarWinds NTA monitors. Selecting specific monitored protocols can reduce the amount of NetFlow traffic that SolarWinds NTA processes and improve performance.

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Click Monitored Protocols.
4. Select or clear the transport protocols you want SolarWinds NTA to monitor.
5. Click Submit.
NetFlow sources and CBQoS polling

This section provides procedures for adding and deleting flow sources and selecting CBQoS-enabled devices for monitoring.

If NPM is monitoring network devices that are configured to export flow data, NTA automatically detects and adds the flow sources under NetFlow Sources.

Access the management page

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Click NetFlow Sources.

The NetFlow Sources page provides a list of active flow- and CBQoS-enabled nodes and interfaces.

If you do not see any NetFlow sources, confirm that the following is true for your configuration:

- NetFlow devices must be configured to send NetFlow data to SolarWinds NPM. Devices and interfaces must be managed by SolarWinds NPM before they can be recognized in SolarWinds NTA.
- Confirm that the SolarWinds NetFlow Service starts in Windows Services.

Select interfaces for NetFlow monitoring

1. Use the Show list to filter the devices to display.
2. Use the Search function to filter the list further.
   
   If you select a node, NetFlow monitors all interfaces for that node.

4. Click Submit.

Enable the automatic addition of flow sources

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

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
4. Click Save.

Enable flow monitoring from unmanaged interfaces

SolarWinds NTA provides the option to retain data for any flow defined with at least one interface monitored by SolarWinds NPM.
It is possible that you may be managing a node in SolarWinds 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 choose to have SolarWinds NTA attempt to associate unknown traffic with a non-primary IP address on a currently monitored SolarWinds NPM node.

For more information about managing interfaces in SolarWinds NPM, see Discovering and Adding Network Devices in the SolarWinds Network Performance Monitor Administrator Guide.

Disabling the option to monitor flows from unmanaged interfaces may significantly decrease the processing load on both your SolarWinds NTA server and your SolarWinds Orion database server, but it will also decrease the amount of flow data stored in your SolarWinds Orion database.

The following procedure enables the option of monitoring traffic on unmanaged interfaces in SolarWinds NTA.

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
4. Select Allow Matching Nodes by Another IP Address to allow SolarWinds NTA to attempt associating unknown traffic with non-primary IP addresses on a monitored SolarWinds NPM node.
5. Click Save.
   If there are unknown traffic events, resolve the unknown traffic and add devices for monitoring first to SolarWinds NPM, and then to SolarWinds NTA. For more details, see Resolve unknown NetFlow traffic.

Set the sampling rate manually

Sampled flows contain information about their sampling rate. SolarWinds NTA uses this information to display sampled flows data.

You can manually specify the sampling rate for flows exported from your nodes when:

- the sampled information is not automatically detected
- the sampled information is not automatically included
- you want to see unsampled flows for a device that exports sampled flows

Manually defined settings override the automatically detected sampling rates.

Manual settings are defined on the node level and are applied on all interfaces monitored for the node.

Access the NetFlow Sources management page

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Click NetFlow Sources.
Edit the sampling rate for flows exported from a node

1. Use the Show list to filter the devices.
2. Select the NetFlow box for the node. Next to the node, you can see the current sampling rate used for flows from the node and from the selected interfaces: either Custom or Auto-Detect.
3. Click Edit to change the current settings.
4. Select Override Auto-Detected Sampling Rate.
5. Enter a value, such as 100.
6. Click Save. The new value is displayed in the NetFlow Sample Rate column.
7. Click Submit.

Process sampling flows as if they were not sampled

1. Use the Show list to filter the devices.
2. Click Edit next to the node whose traffic you want to see as unsampled flows.
3. Select Override Auto-Detected Sampling Rate.
4. Click Save. The change is applied for all monitored interfaces of the node.
5. Click Submit.

Enable CBQoS polling

You can enable and disable NetFlow sources under NTA Settings > NetFlow Sources. To be able to poll CBQoS data, you must first enable CBQoS polling.

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Scroll down to the CBQoS Polling section.
5. Set the polling interval.
6. Click Save.

Delete flow sources and CBQoS-enabled devices

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Click NetFlow Sources.
4. Select a filter from the Show list.
5. Expand the node tree to locate the source you want to delete, and then expand the source you want to delete.
6. 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.

If you disable NetFlow monitoring for a node or interface, the data is not collected. However, historical data are kept in the database. Enabling and disabling flow collection results in gaps in SolarWinds NTA graphs.

7. 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.

**NetFlow collector services**

NetFlow Collector Services provide status information about current flow collectors.

If you employ a firewall on your NetFlow collector, list all ports on which the NetFlow collector listens for flow data as firewall exceptions for UDP communications.

By default, SolarWinds 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](#).

The following procedure resets or adds flow collection ports on which the SolarWinds NTA collector listens for flow data.

**Access the management page**

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.

**Add or reset a collection port**

1. Enter a port number in the Collection Port(s) field of the collector that you want to edit.
   - Separate ports with a single comma, for example, "2055, 9995".
   - A colored icon displays the status of your collector. 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 an explanation of collector status.

2. Click Submit.
Delete a collection port

1. Click Delete next to a collection port.
   - If a NetFlow service is running on the collector server, the collector and port 2055 are added automatically in 15 minutes. For more information, see Delete collectors.
2. Click Submit.

Types of services

SolarWinds NTA recognizes the Differentiated Services model of packet delivery prioritization. All flow-enabled devices can be configured to set a Type of Service byte, referred to as the Differentiated Service Code Point (DSCP), on all sent NetFlow packets. The DSCP prioritizes NetFlow packet delivery over the flow-enabled devices on your network by assigning each packet 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 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 the definition on the Internet Engineering Task Force website.

Configure PHBs with DSCPs

Configure PHBs, corresponding to Types of Services on flow-enabled devices, with DSCPs in SolarWinds NTA.

Access the management page

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Click Types of Services.

Use the Types of Services management page to configure labels for individual types of service. You can also view a list of the types of services available in SolarWinds NTA with DiffServCode Point values.

Undefined types of services are displayed in SolarWinds NTA resources as Unknown.

Edit the name of types of services

1. Click Edit next to a type of service.
2. Edit the name, and click Update on the same line.
   - Individual DiffServ Code Points cannot share multiple Type of Service Names, and individual Type of Service Names cannot share multiple DiffServ Code Points.
3. Click Submit.
Update operations

Changing IP groups, applications, or NetFlow sources are referred to as update operations.

Submit changes

To reflect your changes of applications, service ports, NetFlow sources or IP addresses in the Orion Web Console, you need to submit the changes.

- Update actions might be time-consuming.
- If you do not submit your changes, a notification about unsubmitted changes displays in red on the top of the page.
- You can submit more update operations at the same time, and the Submit button remains active. For more information, see Historical updates.

Historical updates

If you change IP Address Groups, Applications or NetFlow source settings, the changes will also be applied on historical data. The most recent data will be updated first, and then older data stored during the retention period.

As a consequence, two or more users are able to make changes affecting the same applications or IP Address Groups at the same time.

Running updates in NTA resources

If an update is running, all relevant resources will inform you about it. The data in the resource might be inconsistent, because historical data are being updated.

The warning message in the resource includes completion percentage. The shown percentage depends on the time settings in the resource.

For example, say a resource showing the last three hours of data informs you that an update is affecting it, and that 50% is complete. If you change the time frame to the last hour, the percentage of already updated data will rise. However, if you expand the time frame to last month, the completion percentage is much lower.

You can set how often resources should refresh when an update operation is running. Navigate to NTA Settings > Charting and Graphing Settings, select Automatically Refresh Resources Affected by Running Updates, and adjust in minutes.

About change request conflicts

SolarWinds NTA displays a message if you make a change that conflicts with a change by another administrator. Conflicting change requests might cause some of your changes to fail. Possible causes of conflict include:
- Two administrators changing the same application or IP Address Group at the same time.
- An administrator modifying an application while another administrator is changing an IP Address Group relevant for the application.

Resolve a change request conflict

1. Review the conflict message, and submit your changes.
2. Verify that your changes have been submitted successfully.
3. If some changes are not submitted, repeat the changes, and submit them again.

**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 SolarWinds NTA to only record those flows that represent conversations requiring the most bandwidth on your network. Recording only those flows representing the most bandwidth-intensive conversations can significantly improve database performance, reduce page load times, and increase reporting speed.

Most users upgrading from previous SolarWinds 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%.

Enabling this option will result in the intentional loss of some data that may 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.

Setting the Top Talker Optimization to 100% means 40 to 100 times higher storage space requirements, and might affect resource rendering performance. Keeping 100% of flows is suitable only for small installations.

Enable top talker optimization

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Scroll down to the Top Talker Optimization section.
4. Enter a value in Capture Flows Based on This Maximum Percentage of Traffic.
5. Click Save.

**DNS and NetBIOS resolution**

To meet varied network requirements, SolarWinds NTA provides options for both NetBIOS and DNS resolution of endpoint domain names.
DNS resolution options

To meet your specific network monitoring needs, SolarWinds NTA provides the following options for configuring DNS resolution:

Persistent DNS

Persistent DNS resolution continuously resolves domain names for all devices involved in monitored flows. For typically-sized networks, SolarWinds 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. This is the default option for new installations.

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

On Demand DNS 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 SolarWinds 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 SolarWinds NTA waits for domain name resolution.

Disabled

Disabled turns DNS resolution off for the endpoints of flows monitored in SolarWinds NTA. This is not recommended unless NetBIOS resolution already is enabled. For more information, see Enable NetBIOS resolution of endpoints.

How does default DNS resolution work in SolarWinds NTA?

In SolarWinds NTA, host or domain names are stored directly in individual flows. SolarWinds 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, SolarWinds NTA uses this hostname or domain for flows from this IP address for the next seven days. Then the query is repeated.
When SolarWinds NTA cannot reach the DNS server, it retries the query in one minute, and keeps repeating the query until the DNS server responds.

If the DNS server cannot find out the host or domain name, for example if the administrator had not specified it, SolarWinds NTA adds the IP address to the list of unresolved IP addresses. Flows from this IP address are stored in the database under the appropriate IP address. SolarWinds NTA repeats the query to the DNS server to resolve the hostname in two days.

You can also configure the interval between DNS lookups. SolarWinds NTA performs regular DNS lookups on all monitored devices. By default, if the domain of a monitored device resolves successfully, SolarWinds NTA will not attempt another DNS lookup on the same device for seven 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 two days.

Host and domain names

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

For more details, see DNS and NetBIOS resolution.

Filtering

Filtering in SolarWinds NTA is based on hostnames. This way, filtering by hostnames returns the same results as filtering via IP addresses.

Endpoint-related resources

SolarWinds NTA groups items in endpoint-related resources by the hostname.

Host and domain names in SolarWinds NTA resources

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

If a hostname or domain name changes, you can see flows from the same machine as two items: first under the old name and after the change, under the new name. For example, Top XX resources show data split into more items, based on the appropriate resolved name.

Enable NetBIOS resolution of endpoints

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

Enabling NetBIOS resolution does not automatically disable DNS resolution of the same devices. For more information about configuring DNS resolution, see DNS resolution.

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
4. Click Save.
DNS resolution

Persistent

Domain names are resolved continuously for all devices involved in flow monitoring. This is the default for new installations.

If you select Persistent, define:

- Default Number of Days to Wait Until Next DNS Lookup to set the interval on which endpoint domain names are refreshed in the Orion database.
- Default Number of Days to Wait Until Next DNS Lookup for Unresolved IP Addresses to set the interval on which SolarWinds NTA attempts to resolve domain names for unresolved endpoints in the Orion database.

Views may load more quickly because resolved domain names are retained, but database query times may increase as your database is continuously queried.

Top Domains resources and Orion reports that include DNS names require persistent domain name resolution. SolarWinds NTA does not support internationalized domain names which include special characters, symbols, and non-English letters.

On demand

DNS is resolved only when requested from the database.

On Demand DNS 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 SolarWinds Orion database. Database query times may improve as queries are limited, but the load time for some endpoint-related resources may increase as SolarWinds NTA waits for domain name resolution.

 Disabled

DNS resolution is turned off. Not recommended unless NetBIOS resolution is on.

**If DNS Resolution is disabled, all DNS information will be deleted from the database to improve performance.**

IP address processing

By default for new installations, SolarWinds 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.
SolarWinds 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 a reasonable time limit.

1. Under Maximum Time Spent to Process IP Addresses, select one of the following:
   - Custom Number of Minutes, and then enter a value to edit the processing time period.
   - Never Stop Processing Expired IP Addresses to remove the processing limit and delete flow records corresponding to expired IP addresses as they expire.

2. Click Save.

SolarWinds recommends against removing the time limit for processing expired IP addresses, as continuously deleting expired IP addresses may negatively affect performance. By default, SolarWinds 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.

**Database settings**

Due to the great volume of data that is produced by devices on your network, SolarWinds NTA databases may quickly become unmanageable unless you schedule regular maintenance.

The Database Settings grouping allows you to configure maintenance for both databases used by SolarWinds NTA.

**Orion Database**

This database stores CBQoS data and node data relevant for SolarWinds NPM. SolarWinds NTA uses data stored in this database to display appropriate node details and data concerning CBQoS policies defined on your devices.

**NTA Flow Storage Database**

This is a NoSQL database that stores flow data using bitmap indexes. It brings high performance and customizable retention of raw data without aggregation. It stores data with one-minute granularity for the whole retention period (30 days by default) and enables you to see your flow data in more detail.

**Access database settings**

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Scroll down to the Database Settings section.

**NTA Flow Storage Database settings**

Maintaining the NTA Flow Storage Database requires setting an appropriate retention period that corresponds with the amount of data you need to keep and the free space available on the NTA Flow Storage Database disk.
Retention period

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. You should then have an idea of the volume of data your network produces with NetFlow enabled. Consider also the space taken up by the database, and then adjust the retention period accordingly.

Set retention period

1. Note the database Location: hostname and whether the database is installed locally or remotely.
2. Next to Database Size, click Calculate for data to inform your retention period settings.
3. Enter the number of days after which flow data will be deleted in Retention Period.
4. Select a frequency in the Delete Expired Data list.
5. Click Save.

SolarWinds Orion database maintenance

The SolarWinds Orion database stores CBQoS data and node data relevant for SolarWinds NPM. SolarWinds NTA uses data stored in the SolarWinds Orion database to display appropriate node details data and data concerning CBQoS policies defined on your devices.

Because of the growing volume of data produced by your devices, the database may quickly become unmanageable unless you schedule regular maintenance. The SolarWinds Orion database maintenance includes compressing the database and log files.

For more information about the database maintenance application packaged with SolarWinds NPM, see Running database maintenance in the SolarWinds Network Performance Monitor Administrator Guide.

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Scroll down to the Database Settings section.
4. Select Enable Database Maintenance.
5. Provide a time when Maintenance Is Executed.
   - Schedule the database maintenance for an off-peak network usage window to minimize any potential disruption of required monitoring.
6. Select a frequency in the Compress Database and Log Files list.
7. Click Save.

NTA Flow Storage Database maintenance

Maintaining the NTA Flow Storage Database requires setting an appropriate retention period that corresponds with the amount of data you need to keep and the free disk space available on your NTA Flow Storage Database disk.
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. You should then have an idea of the volume of data your network produces with NetFlow enabled. Consider the space taken up by the database, and then adjust the retention period accordingly.

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Scroll down to the Database Settings section.
5. Review the Average Received Flows per Second, Current Size, and Projected Size.
6. Update Retention Period according to the space available on your NTA Flow Storage Database disk, the space required daily, and the estimated maximum size of the NTA Flow Storage Database.
7. Click Save.

NTA Flow Storage Database backups

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

Backups maintain database size and create restoration points for data recovery.

With SolarWinds NTA, you can specify regular backups or execute immediate backups of your database using the NTA Flow Storage Backup Scheduler.

Best practices for NTA Flow Storage Database backups

Considerations when scheduling backups

**Higher utilization of resources**

During the backup, your computer resources may be more utilized.

**Initial backups take longer**

The first database backup includes all data and is more time-consuming than further regular backups.

If you migrate your data from a SQL database to the NTA Flow Storage Database, the first backup after the migration takes longer because the database contains the migrated data.

**Backups and update operations do not run simultaneously**

If you launch an update operation when a backup is in progress, the updates are applied after the backup completes.
Update operations include:

- Changing the status of applications from monitored to unmonitored, or from unmonitored to monitored.
- Creating, updating, removing, enabling, or disabling IP groups.
- Enabling or disabling interfaces.

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

Restoring backups: pick up where you finished last time

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

Optimize your backups

- Execute backups at times when the utilization of your network is low, preferably at night.
- 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.
- Do not use the same physical drive for saving your NTA Flow Storage Database and your backups.
  - NTA Flow Storage Database performance decreases during the backup.
  - If the hard drive fails, you will not be able to restore your database.
- Do not schedule backups at the same time as maintenance. Both maintenance and backup are performance-intensive processes and running them at the same time may have a negatively affect SolarWinds NTA.

Schedule regular backups

1. Under NTA Flow Storage Database Settings, next to Backup, click Backup Scheduler.
2. Select Enable NTA Flow Storage Backup.
3. Define the interval and time for executing backups. Make sure you use the local time of the NTA Flow Storage Database server.
4. Backup Destination displays the folder specified for storing backups.
5. Click Submit.

Back 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 SolarWinds NTA installation, such as an upgrade or changing the location of your NTA Flow Storage Database.

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 update or backup operation when another operation is running, the second operation will be executed after the first one finishes.

Execute the backup

1. Under NTA Flow Storage Database Settings, next to Backup, click Backup Scheduler.
2. Click Backup Now.

Specify a backup folder

Define a backup location to back up your NTA Flow Storage Database. Define the backup location either in the Configuration wizard immediately after the SolarWinds NTA installation, or later using the NTA Flow Storage Configurator tool.

Check the backup location

1. Under NTA Flow Storage Database Settings, next to Backup, click Backup Scheduler.
2. See the location next to Backup Destination.

Change the backup location

1. Log in to the server hosting your main poller.
2. Start the NTA Flow Storage Configurator in the SolarWinds Orion program folder.
3. Enter an absolute path in Backup NTA Flow Storage Database Data File Path, or click Browse to select a folder.
   
   Store backups in a different folder than the NTA Flow Storage Database.
4. Click OK.

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.

Restore a backup

If you want to see historical data after an upgrade from previous SolarWinds NTA versions, back up your database before the upgrade and restore it after the update finishes.

1. Log in 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. Open a File Explorer window.
5. Locate SolarWinds.NetFlow.FastBit.BackupTool.exe in the folder where you installed the NTA Flow Storage Database, such as C:\Program Files (x86) \SolarWinds\Orion\NetFlowTrafficAnalysis.
7. 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\ 2015/08/01 2015/08/15

Date parameters

Start and end dates are mandatory. Use the format YYYY/MM/DD.

If you want to restore all data but you are not sure about the exact dates, use a past date for the start date and a future date for the end date.

For example, 1990/1/1 2020/1/1.

Remote NTA Flow Storage Database covered by Microsoft Failover Cluster

To protect your flow data in a remote NTA Flow Storage Database, you can cover the database by the Microsoft Failover Cluster.

The failover system automatically assumes the primary server functions only in the following cases:

- NTA Flow Storage Database stops
- NTA Flow Storage Database server is down

Failover time

If spare servers in the Failover Cluster are up and running, it takes less than two minutes to failover on most environments. If the cluster needs to start a spare server to become active, you need to additionally count in the starting time of the server.

Some data loss can occur during failover due to service unavailability, when flows are waiting on the NTA receiving service.

On the figure, you can see a full high availability environment. This article deals with setting up the NTA Flow Storage Database to work with the Failover Cluster, which is highlighted in yellow in the picture.
Requirements

- Multiple Windows 2012 servers with similar hardware configuration in the same domain
- SAN drive connected to all servers with:
  - NTFS format
  - Sufficient free space to store all flow data

Recommendations for the SAN drive

- Use RAID 10 to gain performance and fault tolerance.
- Use HA connection to avoid a single point of failure.

Set up NTA Flow Storage Database and the Failover Cluster

1. Install the failover feature to appropriate servers.
2. Set up the failover cluster. For more information, see the Microsoft Failover Cluster help.
3. If you installed the Failover feature using an installer, the SAN disk is automatically taken by the Failover for quorum witness purposes. To use it as your data storage, free it with the Failover Management wizard:
   - Launch the Failover Management wizard, selecting the following items: Failover Management > More Actions > Configure Cluster Quorum Settings > select Quorum > select Shared Folder, and click Finish.
   - If you are using PowerShell for the installation, use the -NoStorage option to keep the SAN disk free.
4. Install NTA Flow Storage Database on all servers.
   a. Install NTA Flow Storage Database on the server where the SAN disk is attached.
   b. In the Flow Storage Configurator, specify the folder for storing flow data to be located on the SAN storage.
   c. Power off the server and SAN disk.
   d. Repeat the previous steps (a-c) on all servers where the disk is attached. Always use the same folder for storing flow data.
5. Power on all servers.
6. Add the NTA Flow Storage Service monitoring using the Failover Management:
   a. Start the failover management and go to Configure role > Generic service.
   b. Select the SolarWinds NetFlow Storage Service from the list.
   c. Provide the access point information. It will be used later when connecting the SolarWinds NTA poller to this NTA Flow Storage Database.
   d. Select the SAN storage you already used for the service during the installation.
   e. Add the following items into the monitored registry:
      - `Software\Wow6432Node\SolarWinds`
      - `Software\Wow6432Node\SolarWinds.net`
   f. Confirm the settings and complete the procedure.

7. Install SolarWinds NTA on the main Orion server and connect it to the access point, using the hostname or IP address, which you created in step 6c.

8. Install additional SolarWinds NTA pollers.

**Cover a local NTA Flow Storage Database by SolarWinds Failover Engine**

1. Deploy the SolarWinds Failover Engine. For more information, see [SolarWinds Failover Engine Administrator Guide](#).
2. In the Failover Manager, click the Data tab > File Filters > Add Inclusion Filter.
3. Enter the path to your NTA Flow Storage Database data folder. The default folder is `C:\ProgramData\SolarWinds\NTA\Data\`.
4. Click the Data tab > Traffic/Queues > Configure.
5. Increase the size of the Differential Queue to 2-4GB.

**Move 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. When you run out of disk space on your NTA Flow Storage Database disk, you can consider moving your NTA Flow Storage Database to a new disk drive, or even to a different remote server.

Before moving the NTA Flow Storage Database, please make sure you [back up the database](#). Otherwise, you will not be able to see your historical data.

**Requirements to change the location**

- NPM 11.5.x
- NPM 12.x
- NTA 4.x

> **If you don’t meet above requirements, this won’t work until you upgrade to NTA 4.x.**
See the Product Upgrade Advisor to find your upgrade path. Before upgrading from NTA 3.11 to 4.1.2, you must have NPM 11.5.x installed. The NTA Flow Storage Database should be installed on a dedicated server, before you upgrade NTA.

Locate your NTA Flow Storage Database

Before you move the database, you need to locate the current file path.

2. The path to the current NTA Flow Storage Database destination folder is available in the appropriate field (please enter a folder path for saving the flow data).
3. Click Cancel to close the Configurator.

Move the NTA Flow Storage Database from a remote server to a local disk

1. Log in to the server where your NTA Flow Storage Database is currently installed.
3. Locate 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, such as a shared folder, FTP, or copy and paste.
5. Change the SolarWinds NTA installation on your main polling engine:
   a. Log in to the server where you have your SolarWinds NTA installed.
   b. Run the SolarWinds NTA executable.
   c. Click Next on the Welcome 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. If you agree, accept the license agreement, and click Next.
   g. Click Change and complete the Setup wizard.
   h. Reconfigure your SolarWinds NTA using the Configuration wizard. For more information, see Complete the Configuration wizard.
   i. When prompted to specify the location for storing flow data, enter 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.

Move the NTA Flow Storage Database from a local disk to a remote server

1. Install the NTA Flow Storage Database on the appropriate server.
2. Log in to the server where your SolarWinds NTA is currently installed.
4. Locate the NTA Flow Storage Database destination folder.
Move the NTA Flow Storage Database folder with its content to the target server using standard Windows tools, such as a shared folder, FTP, or copy and paste.

Change the SolarWinds NTA installation on your main polling engine:

a. Log in to the server where you have your SolarWinds NTA installed.

b. Uninstall NTA on the Control Panel.

c. Cancel the Configuration wizard as it will automatically run after the uninstallation.

d. Run the SolarWinds NTA executable.

This is the Solarwinds-Orion-NTA-v4.x-bxxxx.exe file. The same installer that is used to Install/Upgrade the NTA module on the main polling application server is the same installer used to install the NTA Flow Storage Database application.

e. Click Next on the Welcome to Setup wizard screen.

f. Select the configuration option NPM/NTA/NTA Flow Storage Database on two separate servers, and click Next.

g. Enter the host name or IP address of the new NTA Flow Storage Database location, and click Test Connection.

h. Review the Welcome information, and click Next.

i. If you agree, accept the license agreement, and click Next.

j. Review the Previous version detected screen, and click Next.

k. Click Change, and complete the Setup wizard.

l. Select the appropriate licensing option.

m. The Configuration wizard will run automatically.

n. Select Next and complete the Configuration wizard settings. For more information, see Complete the Configuration wizard.

Move the NTA Flow Storage Database to another disk on the same server

1. Stop the SolarWinds NetFlow Service or the SolarWinds NetFlow Storage Service as appropriate.

2. Launch the command prompt as an administrator.

3. Locate SolarWinds.NetFlow.FastBit.DbMove.exe in the folder where you installed your NTA Flow Storage Database, such as C:\Program Files (x86) \SolarWinds\Orion\NetFlowTrafficAnalysis.

5. Define what should be restored using the following command: `Netflow.Fastbit.DbMove.exe` [source folder] [destination folder].

Example:
`NetFlow.Fastbit.DbMove.exe D:\OldDBLocation\ D:\NewDBLocation\`

Notes:
- 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:\Old DB Location\" "D:\New DB Location\"`.
- In NTA 4.0.3, the source folder is resolved automatically, so that you only specify the destination folder, such as: `Netflow.FastBit.DbMove.exe D:\NewDBLocation\`


7. Enter the new destination folder for storing your flow data.

Move the NTA Flow Storage Database from an existing remote server to a new remote server

1. Install the NTA Flow Storage Database on the appropriate server. For more information, see Install the NTA Flow Storage Database.
2. Log in to the server where your NTA is currently installed.
4. Log in to the server where you installed your NTA Flow Storage Database.
6. Locate the NTA Flow Storage Database destination folder.
7. Move the Flow Storage folder with its contents to the target server using standard Windows tools, such as a shared folder, FTP, or copy and paste.
8. Change the NTA installation on your main polling engine:
   a. Log in to the server where you installed NTA.
   b. Run the NTA executable.
   c. Click Next on the Welcome to Setup wizard screen.
   d. Select the configuration option NPM/NTA/NTA Flow Storage Database on two separate servers, and click Next.
   e. Enter the host name or IP address of the new NTA Flow Storage Database location, and click Test Connection.
   f. Review the Welcome information, and click Next.
   g. If you agree, accept the license agreement, and 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 using the Configuration wizard.

High Availability in SolarWinds products

SolarWinds High Availability (HA) provides failover protection for your Orion server and additional polling engines to reduce data loss. If your primary server fails, the HA feature allows your secondary server to take over all services, such as polling and alerting, with minimal downtime. SolarWinds HA protects your main server, also known as your main polling engine, and additional polling engines. It does not protect your databases or your additional web servers.

SolarWinds supports physical-to-physical, physical-to-virtual, virtual-to-physical, and virtual-to-virtual failover in an IPv4 LAN environment.

How does it work?

When you configure your environment for SolarWinds High Availability, place your secondary server on the same subnet as the primary server. Configure the secondary server to use the same network and database resources as the primary server. In the Orion Web Console, add both servers to an HA pool, which is accessed through a single Virtual IP (VIP) address to route incoming requests and messages to the current, active server.
The SolarWinds HA software monitors the health of both servers in the pool, and both servers keep open communication channels over TCP port 5671 to exchange information. When a critical service goes down, such as the SolarWinds Information Service, the software attempts to restart the service. If the service goes down a second time within a set amount of time, the software initiates a failover to the standby server.

After a failover to the secondary server is complete, the secondary server becomes the active server and continues to act as the active server until another failover event occurs. The secondary server assumes all of the responsibilities of primary server, including receiving syslogs, SNMP traps, and NetFlow information through the VIP. You can manually failover to your primary server to return it to active service.

What is a Virtual IP address?

A Virtual IP (VIP) address is an IP address that is shared by both members of a HA server pool. When a member of the pool goes down, the other pool member takes over the VIP address and responds to requests sent to the VIP. The VIP and each pool member must be part of the same subnet.

SolarWinds High Availability does not support IPv6 addresses.

How do I choose a VIP address?

You have two options when choosing a VIP address.

- Use your original Orion server's IP as your VIP, and add a new IP address to your manually configured network adapter for your Orion server. This allows devices that you have configured for limited access to a set number of IP addresses to continue to send information to the same IP address. This option requires no device configuration change if your devices can only send information to specific IP addresses.
- Use a new IP address as your VIP when you have no device restrictions.

If you lock down the IP addresses you send information to and receive information from, you must make configuration changes to your devices because the HA pool may send polling requests from one of three IP addresses.
You can use SolarWinds Network Configuration Manager to update your router and switch configurations.

Which IP address is used as the source?

Outbound communication from the HA pool, such as WMI or SNMP polling requests, may be sent by the primary or secondary server's IP address or the VIP address. All inbound communication goes through the VIP address.

The active pool member has a minimum of two IP addresses available: the IP address of the server and the VIP address for the pool.

Because there are multiple IP addresses bound to a single NIC, Windows chooses which IP address is used as the originating IP address. The IP address with the most high order bits that match the destination of the next hop is used as the source IP address for all outbound polling activity.

You can determine the source IP address by doing the following:

1. Convert the IP addresses to binary.
2. From left to right, compare how many bits in the IP addresses match the default gateway's IP address.

The IP address with the most consecutive, matching bits is used for the HA pool's source IP address.

Choose an IP address close to the default gateway's IP address so outbound communication comes from the VIP address. You can also modify the converted bits to be the IP address with the longest match and convert it back to an IP address.

Examples of matching the binary bits

The following is an example where the VIP is used as the outbound IP address.

<table>
<thead>
<tr>
<th>IP ADDRESS</th>
<th>IP ADDRESS CONVERTED TO BINARY</th>
<th># OF MATCHING BITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Gateway (first hop)</td>
<td>10.199.15.1</td>
<td>00001010-11000111-00001111-00000001</td>
</tr>
<tr>
<td>VIP</td>
<td>10.199.15.20</td>
<td>00001010-11000111-00001111-00010100</td>
</tr>
<tr>
<td>Primary pool member</td>
<td>10.199.15.61</td>
<td>00001010-11000111-00001111-00111011</td>
</tr>
<tr>
<td>Secondary pool member</td>
<td>10.199.15.62</td>
<td>00001010-11000111-00001111-00111110</td>
</tr>
</tbody>
</table>
The longest match in the example above is the VIP. It has 27 consecutive matching high order bits to the default gateway.

The following is an example where pool members' IP addresses are used as the outbound IP address.

<table>
<thead>
<tr>
<th>IP ADDRESS</th>
<th>IP ADDRESS CONVERTED TO BINARY</th>
<th># OF MATCHING BITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Gateway (first hop)</td>
<td>10.199.15.1</td>
<td>00001010-11000111-00001111-00000001</td>
</tr>
<tr>
<td>VIP</td>
<td>10.199.15.82</td>
<td>00001010-11000111-00001111-01010010</td>
</tr>
<tr>
<td>Primary pool member</td>
<td>10.199.15.61</td>
<td>00001010-11000111-00001111-00111101</td>
</tr>
<tr>
<td>Secondary pool member</td>
<td>10.199.15.62</td>
<td>00001010-11000111-00001111-00111110</td>
</tr>
</tbody>
</table>

In this example, the longest match is the pool members' IP addresses. When a failover occurs, the IP address of the active Orion server is used as the source IP for all polling requests. The VIP address is only used for inbound traffic, such as syslog, SNMP traps, NetFlow, and accessing the Orion Web Console.

SolarWinds High Availability requirements

High Availability is provided for SolarWinds products released on Orion Platform products version 2016.2 and later. You cannot enable an HA pool for a server that includes non-supported products.

Visit SolarWinds KB MT6886 to build an upgrade path.

Supported products

- Network Performance Monitor 12.0.1 and later
- Server & Application Monitor 6.3 and later
- NetFlow Traffic Analyzer 4.2.1 and later
- Network Configuration Manager 7.5.1 and later
- IP Address Manager 4.3.2 and later
- User Device Tracker 3.2.4 and later
- VoIP & Network Quality Manager 4.2.4 and later
- Storage Resource Monitor 6.3 and later
- Web Performance Monitor 2.2.1 and later

The following products can be integrated with your Orion Platform-based product. The integration module between products is supported under SolarWinds High Availability, but the stand-alone product is not supported.
- Storage Manager 6.2.3
- Virtualization Manager 6.3.2 and later
- Firewall Security Manager 6.6.8
- Engineers Toolset 11.0.3 and later
- Database Performance Analyzer on Orion 10.2 and later
- Patch Manager 2.1.3 and later

Software and Hardware requirements

SolarWinds strongly recommends that the hardware and software of the standby server matches the primary server. Using matching system specifications and installed software ensures the same performance in the event of a failover.

- Both servers must be installed on Windows Server 2008 R2 or later.
- Both servers must also meet or closely match the minimum hardware and software requirements for the products you have installed on the primary server.
- Both servers must be able to connect to your SolarWinds Orion database.
- If protecting an NTA environment, both servers must be able to connect to the separate NTA Flow Storage database.

SolarWinds does not provide failover support for any database.
- Some SNMP trap, syslog message, and flow data is lost while waiting for the secondary server to become active.

Port requirements

<table>
<thead>
<tr>
<th>PORT</th>
<th>PROTOCOL</th>
<th>SERVICE/PROCESS</th>
<th>DIRECTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>4369</td>
<td>TCP</td>
<td>RabbitMQ</td>
<td>bidirectional</td>
<td>TCP ports 4369 and 25672 must be open between the main and secondary servers to allow RabbitMQ clustering between the two servers. These ports exchange EPMD and Erlang distribution protocol messages for RabbitMQ. They do not need to be open in additional polling engine pools.</td>
</tr>
<tr>
<td>5671</td>
<td>TCP</td>
<td>SolarWinds High Availability</td>
<td>bidirectional</td>
<td>Port 5671 must be open into the HA pool with the main Orion server from all Orion servers.</td>
</tr>
<tr>
<td>25672</td>
<td>TCP</td>
<td>RabbitMQ</td>
<td>bidirectional</td>
<td>TCP ports 4369 and 25672 must be open between the main and secondary servers to allow RabbitMQ clustering between the two servers. These ports</td>
</tr>
</tbody>
</table>
Networking requirements

⚠️ SolarWinds High Availability does not support IPv6 addresses.

- Both your primary and secondary servers must be on the same subnet.
- Both pool members must have static IPv4 addresses set on the network adapter. You do not need dedicated NICs.
- All pool members must be able to resolve the host names of all additional pollers, additional websites, and the main Orion server. Pool members must also be able to resolve the host names of members in the same pool.
- A virtual IP address must be available on the same subnet as the primary and secondary servers.
- Devices must be able to accept inbound connections from the source IP and VIP addresses.
- Devices sending sylogs, SNMP traps, and NetFlow information to your Orion server must be configured to send the information to the VIP address and receive requests from the pool.

ℹ️ You may need to modify firewall rules to allow traffic from pool members and to the VIP address. For example, you may need to modify the NetFlow firewall rules to allow incoming TCP traffic on port 2055 to go to the VIP address.

Depending on your network, you may have additional requirements. Up to three IP addresses per pool may be in use among the VIP, primary, and secondary servers because of how Windows calculates the source IP address from the HA pool. You can modify your devices to receive requests from all IP addresses or determine which IP address is used as the source IP address.

High Availability deployment walk-through

The following provides a high-level walk-through of how to set up high availability protection on your main server or additional polling engines.

Before you begin, review the requirements and how to choose a VIP address.

1. Reserve an available IP address to use as the Virtual IP (VIP) address on the same subnet as the primary and standby servers.
2. Build a standby server on the same subnet as the server you want to protect.
3. Open port 5671 (TCP) on the primary (incoming) and standby (outgoing) servers.
4. Open ports 4369 and 25672 (TCP) on the main Orion server and its standby server. These ports are not required when protecting additional polling engines.
5. Download and install the secondary server software.
6. Activate your HA pool licenses.
7. Create your HA pool.

Optional deployment steps

Depending on your network and device configuration, you may need to perform some or all of the following steps:

- Modify your DNS to point your Orion Web Console's host name to the VIP.
- Modify the firewall settings to all communication to the VIP address and from the primary and secondary servers.
- Modify devices that send syslog messages, SNMP traps, or NetFlow data to your Orion server to use the VIP instead.

Depending on your network setup, you may be able to change your primary server's IP address to another address in the subnet and use the already established SolarWinds IP address as the VIP address. See What is a Virtual IP address? for more information.

- Modify devices' SNMP settings to accept requests from the VIP address and the primary and secondary IP addresses.

Set up the standby server

Your secondary, or backup, server takes over all tasks in case of a failover. Download or move the backup server installer on the secondary server. The installer uses the information on the main server or polling engine to install the correct products and product versions.

If you upgrade an HA pool member, the products installed on the secondary server must match your primary server, including the version numbers.

You can open the main server's Orion Web Console while logged in to the secondary server to download the server software instead of moving the installer to the secondary server.

Before you begin, you need the credentials for your SolarWinds Orion SQL database.

1. Open the Orion Web Console.
2. Click Settings > All Settings > High Availability Deployment Summary.
3. Click Setup a new HA server.

High Availability Deployment Summary

The diagram below shows the deployment of your polling engines

,set up a new HA server,
4. On the dialog, click Get started setting up a server.
5. **Activate** your HA pool license.
6. On the Setup a High Availability Server dialog, click Download installer now.
7. Move the downloaded installer to your secondary server and run it.
   - Select which type of backup server you want to install under High Availability.
   - Enter your SQL credentials for your Orion SQL database when prompted.

You can now [add the backup server to a pool](#) with your main server or additional polling engine.

### Activate High Availability pool licenses

High Availability is licensed per pool, which is an internal grouping of a primary and secondary server. You receive a 30-day evaluation license for an unlimited number of HA pools.

You do not need to purchase a second additional polling engine license or additional product licenses for the secondary servers and polling engines in your HA pools.

If you are setting up multiple pools, activate all of your HA pool licenses. When you set up your HA pools, each pool automatically consumes one HA pool license until no more licenses are available.

1. Click Settings > All Settings > License Manager.
2. Select a license.
3. Click activate.
4. Enter your license information.

Licenses are automatically assigned to the pool with the Main poller and then to pools without licenses.

### Set up an HA pool

An HA pool is a group of two servers that have access to the same network and database resources. The pool includes one main server or additional polling engine and one secondary server or polling engine. Each server is called a pool member and can take over all responsibilities of the other server.

When a pool member is sending and receiving data, it is the active member. When a pool member is waiting to take over, it is the standby member.

Because of the web-based License Manager, the main Orion server must stay up. If the main server is down for more than 14 days, your licenses may be invalidated. The main Orion server does not require Internet access.

Before you begin, you need the following:
A VIP address
The secondary HA server
An available HA pool license

1. In the Orion Web Console, click Settings > All Settings > High Availability Deployment Summary.
2. Click Setup High Availability pool next to your standby server. If a HA pool license is not available, you are prompted to activate an HA pool license.
3. Enter the pool name and the virtual IP (VIP) address. The VIP must be unassigned and on the same subnet as the primary and secondary servers.
4. Click Create Pool to complete the pool setup.

Your main server or additional polling engine is now highly available and can failover to the standby server. A failover audit event is logged when you create the pool.

When the pool is created, the High Availability Deployment Summary displays the active and standby servers grouped under the pool name. Failover events will be logged and you can receive email notifications.

<i>You may need to refresh the page to see the correct pool and server status.</i>

SolarWinds recommends that you perform a manual failover after you create your pool and observe the data collected to ensure that all network and device changes are correct.

Configure High Availability settings

Click Settings > All Settings > High Availability Settings to access these options.

By default, High Availability is enabled and an email is sent when a failover occurs. You can change the default interval and modify your default email settings.

**Default interval to consider a member as down in a pool**

Define how long the active pool member can be down before a failover occurs. Provide the interval in seconds.

**Email me when server status is changed**

Choose to receive email messages when a failover occurs. This is enabled by default and uses the default email settings to send notifications. High Availability notifications do not depend on the SolarWinds alerting service or the Orion database so you receive High Availability alerts when the service or database is down.

**Email me when facility status is changed**

Receive email messages when the status of a low-level component changes, such as the percent used of the CPU or RAM. Facilities are used to gauge the health of the system and may trigger a failover condition. For example, the computer may restart and failover if the CPU stays over 100% for a significant amount of time.
**Email me when resource status is changed**

Receive email messages when a SolarWinds Orion component changes, such as the polling or job engines. Resources are generally SolarWinds specific processes or services that are monitored by the High Availability software that can trigger a failover condition. For example, if the job engine is down and does not restart successfully, the active server fails over to the standby server.

**SolarWinds recommends disabling this setting due to a potentially large message volume.**

---

**Set up the default High Availability email**

The information you provide in the default email action is used to send email messages when there is a status change in an HA pool member, facility, or resource. This is also used as the default information for the Send an Email/Page alert action.

While the information in the default email action is used by default for all SolarWinds email notifications, High Availability-specific notifications are sent independent of the SolarWinds alerting service. When the SolarWinds alerting service or the database is down, you can still receive email notifications for failover events as long there is a network connection available and your SMTP server is up.

**i** Separate email addresses with a semicolon.

1. Click Settings > All Settings in the menu bar.
2. Click Configure Default Send Email Action.
3. Under the Default Recipients heading, provide the email addresses of all default recipients for any email alert action. For example:
   email@company.com; email2@company.com; distrolist@company.com
4. Provide the default sender and reply address.
5. Enter the default SMTP server information.

**Selecting SSL encryption automatically changes the SMTP port number to 465.**

---

**Manage HA pools**

Use the High Availability Deployment Summary page to view and manage your pools and to view the pool member type.

**Disable HA pools**

During an upgrade or maintenance procedures on your HA pool members, you must disable your pool. HA pools can also be disabled when you no longer have sufficient HA pool licenses for the number of enabled pools.
1. In the Orion Web Console, click Settings > All Settings > High Availability Deployment Summary.
2. Select the pool you want to disable.
3. Toggle High Availability to Off.

You can also disable the entire feature on the [High Availability Settings](#) page.

### Remove HA pools

You may need to delete one or more HA pools to free an HA pool license or to change pool members. When you remove a pool, the VIP is still reserved in the database and is not recycled so you can re-establish the pool without modifying your network or device settings.

1. In the Orion Web Console, click Settings > All Settings > High Availability Deployment Summary.
2. Select the pool you want to delete.
3. Click Commands on the Pool Details section.
4. Click Remove Pool.

A failover audit event is logged when you remove a pool.

### Force a manual failover

When testing SolarWinds High Availability and network configuration changes or when upgrading, you can failover to the standby pool member manually.

> **Tip:** Failover can only occur when both pool members are up, the pool is enabled, and High Availability is enabled.

1. In the Orion Web Console, click Settings > All Settings > High Availability Deployment Summary.
2. Select the pool you want to failover manually.
3. Click Commands on the pool details section of the pool you want to failover.
4. Click Force Failover.

The pool fails over to the secondary server and a failover audit event is logged that records who forced the failover and when it occurred.

### View the pool member type

In addition to polling metrics, individual pool members list a Server Type and an HA Run Type. Select a pool member to view the pool member type and other polling information.

- The Server Type displays the type of Orion server, such as Additional or Main Polling Engine.
- The HA Run Type indicates if the server is currently the active or standby server.
How failovers work

After High Availability is enabled and you have set up a pool, each pool monitors itself for failover conditions such as:

- Inability to connect to the network
- Stopped SolarWinds services
  - Stopped Agent services is not a failover condition.
- Power loss
- Network connection loss to the primary server

When a monitored service is down, the Orion server tries to allow the service to recover before failing over to the secondary server. If the same service fails within the default self-recovery period, a failover occurs.

When a failover condition is met and failover occurs in a pool, a failover event is logged and can be viewed in the Event Summary resource or the Events view. An email is also sent to your default recipients.

For example, if the job engine service is down, the High Availability software attempts to restart it. If the job engine fails again within 1 hour, then a failover occurs and the event is logged. If the job engine fails within 61 minutes, a failover does not occur.

Charting and graphing settings

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

Enable 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 SolarWinds NTA views can become significant. To help this condition, SolarWinds NTA provides a progressive charting option that is enabled by default.

- Disabling progressive charting may significantly increase the amount of time it takes to load data into charts and graphs in web console views.

The progressive charting option configures SolarWinds NTA to draw charts incrementally, spreading the chart generation load over multiple database queries. For SolarWinds NTA installations monitoring and processing numerous data flows, progressive charting can minimize the amount of time you have to wait before actually seeing charted data.

Percentage type for Top XX lists

Percentage Type for Top XX lists describes how SolarWinds NTA calculates percentages in Top XX resources.
**Absolute**

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**

For each item, relative percentages are calculated in terms of the total number of items displayed in the selected resource. Top XX resources show only the set number of items, and only the items shown in the chart are included in percentage calculations.

**Top XX list resource percentages**

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.

By default, pie charts are configured to show some, but not all traffic. You can see the rest of the data not included in the top XX items in the Remaining Traffic row in the legend.

**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.

<table>
<thead>
<tr>
<th>ENDPOINT</th>
<th>ACTUAL AMOUNT OF TRAFFIC</th>
<th>% OF TOTAL ACTUAL TRAFFIC</th>
<th>ABSOLUTE PERCENTAGE</th>
<th>RELATIVE PERCENTAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>TOP 4</td>
<td>TOP 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Top 4</td>
<td>Top 3</td>
</tr>
<tr>
<td>Hostname 1</td>
<td>4 MB</td>
<td>40%</td>
<td>40 %</td>
<td>40 %</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4/8.5 MB = 47%</td>
<td>4/8 MB = 50%</td>
</tr>
<tr>
<td>Hostname 2</td>
<td>3 MB</td>
<td>30%</td>
<td>30 %</td>
<td>30 %</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3/8.5 MB = 35.3%</td>
<td>3/8 MB = 37.5%</td>
</tr>
<tr>
<td>Hostname 3</td>
<td>1 MB</td>
<td>10%</td>
<td>10 %</td>
<td>10 %</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1/8.5 MB = 11.7%</td>
<td>1/8 MB = 12.5%</td>
</tr>
<tr>
<td>Hostname 4</td>
<td>.5 MB</td>
<td>5%</td>
<td>5%</td>
<td>Not Shown</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.5/8.5 MB = 5.9%</td>
<td>Not Shown</td>
</tr>
<tr>
<td>ENDPOINT</td>
<td>ACTUAL AMOUNT OF TRAFFIC</td>
<td>% OF TOTAL ACTUAL TRAFFIC</td>
<td>ABSOLUTE PERCENTAGE</td>
<td>RELATIVE PERCENTAGE</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------</td>
<td>---------------------------</td>
<td>---------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Remaining Traffic in MB and %</td>
<td>1.5 MB</td>
<td>15%</td>
<td>15%</td>
<td>Not Shown (Remaining Traffic shown only in Absolute values.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>20%</td>
<td>Not Shown (Remaining Traffic shown only in Absolute values.)</td>
</tr>
<tr>
<td>Total Traffic Shown in Resource (in MB and %)</td>
<td>10 MB</td>
<td>100%</td>
<td>100% (10MB includes remaining traffic)</td>
<td>100% (10MB includes remaining traffic)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>100% (8.5MB includes just top 4 entries)</td>
<td>100% (8MB includes just top 3 entries)</td>
</tr>
</tbody>
</table>

**Unit type for area charts**

Settings configured on the NTA Settings view apply globally to all SolarWinds NTA area charts.

**Rate (kbps)**

Provides the actual rate of data transfer, in kilobytes per second, corresponding to items displayed in a Top XX resource.

**% of interface speed**

Displays the resource data as a percentage of the nominal total bandwidth of the selected interface. 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 time interval**

Displays the amount of data corresponding to listed items transferred over a designated period of time.

**% of class utilization**

Creates a chart displaying what percentage of the limit set for the appropriate class is used up by the interface or node. Selecting this option sets the chart style to line chart.
This option requires that you have set limits for individual classes on appropriate devices and is available only for the following CBQoS resources on Interface Details Views:

- CBQoS Pre-Policy Class Map
- CBQoS Post-Policy Class Map
- CBQoS Drops

For example, you have allocated a 10 Mbps bandwidth for a class on a device. This option displays a real percentage how the bandwidth is used.

Area chart units can also be configured on a per 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 SolarWinds NTA area chart resource.

**Default time periods for resources**

You can globally set the default time period for all Orion Web Console resources in the Charting and Graphing Settings section of NTA Settings.

- The default time period for SolarWinds NTA resources placed on Detail views is Last 15 Minutes.
- The default time period for SolarWinds NTA resources placed on Summary views is Last 1 Hour(s).
- The default time period for SolarWinds NTA search is Last 15 Minutes.

High default resource time periods may significantly affect load times for SolarWinds NTA views.

You can also configure the time period for any SolarWinds NTA resource by clicking Edit in the header of the resource.

**Default chart style for resources**

By default, all resources in detail views present chart data in an area chart and Orion summary views present chart data in a pie chart.

You can configure the chart style for any resource individually.

Pie charts present a flat view of your data. Area charts present a historical view of your data as represented by areas calculated at past polling times.

**Default flow direction for resources**

By default, all resources in node detail views and interface detail views present data for ingress flows and Orion summary views present data for both flow directions.

You can configure the flow direction for any resource individually.

**Enable automatic page refresh**

The refresh rate for SolarWinds NTA views is configurable. Select this option, and then provide the refresh interval in minutes.
Automatically refresh resources affected by running updates

Define how often update progress should be refreshed. Once the update is completed, appropriate resources are refreshed.

By default, the progress message is refreshed every one minute.

**Optimize performance in SolarWinds NTA**

Due to the volume of data it collects and processes, SolarWinds 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 SolarWinds 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 SolarWinds 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 information, see [Configure on demand DNS resolution](#).

- Capture only the flows required to represent the top talkers on your network. For more information, see [Limit flow collections to top talkers](#).

- Limit the time period for storing flow data in your database. For more information, see [NTA Flow Storage Database maintenance](#).

- If you store your flows data in the SolarWinds Orion database, and you are running SolarWinds NTA 4.0 and older on a 32-bit operating system, adjust the data aggregation. For more information, 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 [Configure data retention for flows on unmonitored ports](#).

**Configure on demand DNS resolution**

Enabling On Demand DNS resolution in SolarWinds NTA decreases the amount of database memory used to store DNS information and the read and 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 SolarWinds 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.
1. Click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
4. Click Save.

Limit flow collections to top talkers

Up to 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 SolarWinds 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 large amount of unnecessary data. As a result, your database may be unnecessarily large and the load times for SolarWinds 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 SolarWinds NTA.

The Top Talker Optimization setting, by default, captures only those flows representing the top 95% of total network traffic. By changing this setting you are permanently limiting the amount of data that is available for a historical analysis of traffic flows.

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Under Top Talker Optimization, edit Capture Flows Based on This Maximum Percentage of Traffic.
4. Click Save.
View NTA 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 as resources grouped to form individual views.

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

SolarWinds NTA provides two basic types of views:

**Summary views**

Display traffic details on all nodes and interfaces managed by SolarWinds NTA, such as top applications, conversations, and endpoints. You can access your summary views either in the My Dashboards > NetFlow views 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 SolarWinds NTA.

**Detail views**

Display 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 then clicking on the object whose details you want to see.

A resource is a building block of a view. A resource displays on a view as a box and provides information about different aspects of traffic monitoring, usually in a chart or 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 SolarWinds NTA monitors, if used on a summary view.
- To the selected object, if used on a detail view for a node, interface, conversation, application, CBQoS class, or other object.

SolarWinds NTA resources provide data in tables, and most resources also display data graphically using charts.

If you upgraded to SolarWinds NTA with the NTA Flow Storage Database, 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 may result in slower rendering or processing.
My Dashboards

My Dashboards provide menu bars with shortcuts to Orion Web Console views. The default menu bars include Home, and a menu bar for each installed Orion Platform product.

Click My Dashboards to show the default menus.

You can customize views and labels offered in default menus for individual users.

If you do not need to see all items in menu bars, and prefer navigating to display items in a menu bar, click My Dashboards > Collapse.
Customize My Dashboards

Menu bars available in My Dashboards depend on both the settings in your user account and the products you have installed.

1. **Find out** which menu bar is assigned to Home, Network, or other product-specific tab for your user.
2. **Add an Orion Web Console view or an external web page to the menu bar.** The change will concern all users who access the menu bar from My Dashboards.

   ![To add a link to a details view for an important device, go to the view, copy the URL, and add it as an extra item to the view.]

3. To provide access to a specific set of links for specific users, create a menu bar, add the links and assign the menu bar as the Home tab for the users.

Specify My Dashboards and Alerts & Activity items for users

The items users see in My Dashboards and in Alerts & Activity are specified in their user accounts.

![Improve performance by setting the Home Page View to a view with a limited number of resources on it.](image)

1. Click Settings > All Settings in the menu bar.
2. In the User Accounts grouping, click Manage Accounts.
3. Select a user, and click Edit.
4. Scroll down to Default Menu Bars and Views, and select top menu bars from the lists.

   ![DEFAULT MENU BAR AND VIEWS](image)

5. Select Yes for the items the user will see in the Alerts & Activity menu bar.

![Show Alerts Menu](image)

   ![Show Events Menu](image)

   ![Show Syslog Menu](image)

   ![Show Traps Menu](image)

   ![Show Message Center Menu](image)
6. Select an item and use the arrows to change the order of menu bars. Select an item from the list to specify the default Home page view.

![Tabs ordering]

7. Click Submit.

The user can now use the specified links in My Dashboards and Alerts & Activity menu bars.

Add items to My Dashboards

What users see in My Dashboards depends on menu bars assigned to them in their user account. To add an item to My Dashboards for all users who can see a menu bar, add the item to the menu bar.

1. Click My Dashboards > Configure.
2. Click Edit.

![Menu Bar: New York]

3. Drag available items from the left-hand column to Selected Items on the right.

![Available items and Selected items]

- Hover over any view title to read the description.
  To change the order of menu items, drag and drop items in the Selected column.

4. Click Submit to save your changes.
You can also add links to node details views for specific nodes, or to external Internet pages as a menu item.

- Click Add below the Available items list, provide a name, URL and description for the menu item, and click add.
- Drag the new item to the Selected items column.

Users who can see the menu bar in My Dashboards will see the added items.

Add menu bars

When you have a list of items you want users to access from My Dashboards, create a menu bar.

1. Click My Dashboards > Configure.
2. Scroll to the bottom of the page, and click New Menu Bar.
3. Name the menu bar.
4. Drag views from the Available items column into Selected items.

5. Click Submit.

The new menu bar is created. You can now assign it to users who will see the items in My Dashboards.

Change the Orion Web Console logo

1. Create a graphic to replace the SolarWinds logo.
   - The recommended logo size is 250 x 50 pixels. The maximum allowed size is 900 x 500 pixels.

2. Place your graphic in the images directory.
   - The default location of the directory is C:\Inetpub\SolarWinds\NetPerfMon\.
3. Click Settings > All Settings in the menu bar.
4. In the Product Specific Settings grouping, click Web Console Settings.
5. Ensure the Site Logo box is selected, and click Browse to navigate to your logo.

6. Click Submit.

---

**Edit resources**

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

1. Click Edit in the header of the resource.
2. Customize the available options:
   - Title
   - Subtitle
   - Maximum Number of Items to Display
   - Chart customization options. For more information, see [Customize charts for all users](#).
3. Click Submit.

**Charts**

SolarWinds NTA charts display pie chart or area chart summaries of resource-related data, enabling a more detailed view of resources. You can create different types of area charts, including stack area, stack spline area, stack line, line, spline, and bar.

Charts offer tooltips with current values, as well as the ability to disable data series and to zoom in on data. They also have features you can click offering detailed resource information and editing capabilities.

**Chart display limitations**

- Orion views can display up to 100 resources.
- Pie charts can display up to 100 items.
- Area charts can display up to 10 items, with the rest of the series visible in the legend.
Chart types

- Pie charts
- Area charts

Chart customization options

- Global settings defining how displayed data are calculated and setting default options. For more information, see Charting and graphing settings.
- Customize charts for the current session
- Customize charts for all users

Data granularity shown by default

NTA Flow Storage Database supports saving flow data without compression and with one-minute granularity. However, charts display data in such detail only for time periods up to five hours.

Data are summarized in the following way:

- For time periods up to five hours, charts display data with one-minute granularity. Data are not summarized.
- For time periods of five hours up to 48 hours, charts display data with 15-minute granularity.
- For time periods of 48 hours up to seven days, charts display data with one-hour granularity.
- For time periods longer than seven days, charts display data with six-hour granularity.

View flow data for longer time periods with one-minute granularity

To see flow data with one-minute granularity, set the time period displayed by the view to up to five hours, focusing on the period you are interested in most.

For more information about setting time period for views, see Edit time settings for views.

Pie charts

The pie charts in this section show the Top 5 Endpoints resource, and use absolute percentage calculations. For more information about chart settings, see Charting and graphing settings.

SolarWinds NTA gives each item its own piece of pie, depending on your chart settings. If more items exist than what is configured to display, SolarWinds NTA creates a category in the legend of the pie chart called Remaining traffic, which is not displayed in chart. If fewer items exist than what the chart is configured to display, the chart shows only those resources that exist.
Example

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. SolarWinds NTA labels all other endpoint flow traffic as Remaining traffic, which is 19.27% of the total traffic flow.

Pointing to 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).

Area charts

Area charts are the default charts for all detail views. They display resources within a defined traffic level and time frame. 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.

Like pie charts, if more items exist than what is configured to display, SolarWinds NTA creates a category in the legend of the area chart called Remaining traffic. If fewer items exist than what the chart is configured to display, the chart shows only those resources that exist.
Display data for a specific time point

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

The Top 5 Endpoints data shown the area chart tell us that conversations involving the LAB-VCENTER50 (10.199.1.90) endpoint generated substantially more traffic than the other top 4 endpoints.
Zoom in to see a specified time period

For a more detailed look at resource use, locate the slider tool beneath the area chart. Move it 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.
Hide or show certain items

To display only certain endpoints out of those already selected for review, for example, the bottom two out of the top five, clear the boxes for 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.

Customize charts for the current session

All users who can view resources can also customize the charts for the duration of the current session, directly in the appropriate view or resource.

For the current session, you can customize:

- Time and flow direction settings for all appropriate resources in a view
- Zoom and displayed items in area charts

Once you leave the view with the resource, your current settings will be lost and replaced by settings for the resource.
Customize 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 Edit time settings for views.
For more information about customizing flow direction settings, see Edit flow direction in views.

Area charts: zoom and show selected items only

Area charts support the following session-related options:

- Beneath 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 the traffic at a certain time point.
- 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.

Customize charts for all users

1. Click Edit in the header of the resource.
2. On the Edit Resource page, specify the Title and Subtitle.
3. Select the Chart Style you want to use: Area Chart or Pie Chart.
4. 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.
5. Edit the Maximum Number of Items to Display.
6. Define a Time Period.
   - If you want the resource to inherit the setting from the view on which it is placed, select Use Time Period from Current View. This is the default.
   - If you want to name a time period, select Named Time Period, and select a time period.
   - If you want a relative time period, select Relative Time Period, enter a number, and select a unit of duration.
   - If you want to name an absolute time period, select Absolute Time Period, and set the date and time parameters.
7. 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.
8. Select the Flow Direction.
9. If selected the Area Chart, select an Area Type:
   - 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 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 its own column and plots maximums against the vertical scale.

10. If selected the Area Chart, select a Data Unit:
    - 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.
    - % of Class Utilization creates a chart displaying what percentage of the limit set for the appropriate class is used up by the interface or node. This option requires that you have set limits for individual classes on appropriate devices and is available only for the following CBQoS resources on Interface Details Views:
      - CBQoS Pre-Policy Class Map
      - CBQoS Post-Policy Class Map
      - CBQoS Drops
      - Selecting this option sets the chart style to line chart.

11. If you want to add a title or subtitle for the chart, expand Advanced and enter a Chart Title and Chart Subtitle.

12. Click Submit.
NTA-specific view customizations

Enable the NetFlow Traffic Analyzer Summary View

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

1. Click Settings > All Settings.
2. Under User Accounts, click Manage Accounts.
3. Select Admin, and then click Edit.
5. Select NTA_TabMenu.
6. Click Submit at the bottom of the page.
7. Click My Dashboards > NetFlow to display the NetFlow Traffic Analyzer Summary view.

Create custom views with the Flow Navigator

Using the Flow Navigator, you can create custom traffic views directly from any NetFlow view.

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

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

Create a custom NetFlow traffic view with the Flow Navigator

1. Click My Dashboards > NetFlow > NTA Summary.
2. Click Flow Navigator on the left edge of the summary view. The Flow Navigator is available on any default NTA view.
3. Specify the View Type.
   a. If you want a filtered view of your entire network, click Summary, and select a summary view.
   b. If you want a filtered view of traffic passing through a specific node and interface, click Detail, and select a Detail View Type.
4. Select the Time Period over which you want to view traffic data:
   - Select Named Time Period, and select a time period.
   - Select Relative Time Period, and provide a number appropriate for the selected time units. The relative time period is measured with respect to the time at which the configured view is loaded.
   - Select Absolute Time Period, and provide the start and end time periods.
5. Select a Flow Direction.
   - Select Both to include ingress and egress traffic in the calculations SolarWinds NTA makes.
   - Select Ingress to include only ingress traffic in the calculations SolarWinds NTA makes.
   - Select Egress to include only egress traffic in the calculations SolarWinds NTA makes.
6. 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, expand 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, select 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 then enter the name of the appropriate application.

**Autonomous Systems**
To only display network traffic to and from autonomous systems, or to exclude traffic to and from certain autonomous systems, expand Autonomous Systems, and enter the ID of an appropriate autonomous network. Click Add Filter.

**Autonomous Systems Conversations**
To only display network traffic related to specific autonomous system conversations, or to exclude traffic to and from them, expand Autonomous System Conversations, and enter IDs of autonomous systems involved in conversations. Click Add Filter.

**Conversations**
To only display network traffic related to specific conversations between two endpoints, or to exclude traffic to and from them, expand Conversations and enter the endpoints involved in the conversation. Click Add Filter.

**Countries**
To only display network traffic related to specific countries, or to exclude traffic to and from them, expand Countries, and select a country to Include or Exclude.
To select multiple countries, select each one and click Add Filter to apply each selection.

**Domains**
To only display network traffic related to specific domains, or to exclude traffic to and from them, expand Domains, and enter the domain name you want to Include or Exclude.
   - To add multiple domains, enter a name and then click Add Filter to apply your selection after each entry.
   - If a domain name is not resolved and saved in NTA, you cannot use it in the Flow Navigator. In this case, NTA will prompt you for a valid name. For more information about resolving domain names, see [Host and domain names](#).
Endpoints
To only display network traffic related to specific endpoints, or to exclude traffic to and from them, expand Endpoints:

a. Enter the IP address or hostname of an appropriate endpoint to Include or Exclude.

b. If you want to include or exclude traffic from a specified subnet, enter the appropriate range of IP addresses.
   You can either type in the range, for example 192.168.1.0-192.168.1.255, or use the CIDR notation, for example 192.168.1.0/24.

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

IP Address Groups
To only display network traffic related to specific IP address groups, or to exclude traffic to and from them, expand IP Address Groups, and then complete the following steps:

a. Enter an appropriate IP address group.
   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 _DISABLED to the end. An entry called PrimaryLANDISABLED indicates that the group is inactive.

b. If you want to include or exclude another IP address group, click Add Filter, and then enter the name of an appropriate IP address group.

IP Address Group Conversations
To only display network traffic related to conversations between specified IP address groups, or to exclude traffic to and from them, expand IP Address Group Conversations:

a. Select the IP address groups involved in conversations that you want to include or exclude.

b. If you want to include or exclude another IP address group conversation, click Add Filter, and then enter the appropriate conversation IP address groups.

Protocols
To only display network traffic using specific protocols, expand Protocols and select the protocol to Include or Exclude.
If you want to include or exclude another protocol, click Add Filter, and then select another protocol.

Types of Service
To only display network traffic using specific service types, expand Types of Service and select an appropriate type of service to Include or Exclude.
If you want to include or exclude another type of service, click Add Filter, and then select another type of service.

7. Click Submit.
8. If you want to save your custom filtered view for future reference, click Save Filtered View to Menu Bar.
Add NetFlow resources to web console views

1. Click Settings > All Settings.
2. Under Views, click Manage Views.
3. In the list of views, scroll down to the NetFlow entries.
4. Select a NetFlow view to which you want to add a NetFlow-specific resource, and click Edit.
5. Click + next to the column in which you want the new resource to be placed.
6. In the Group By list, select Classic Category.
7. Select a NetFlow entry in the list.
8. Select one or more resources, and then click Add Selected Resources.
9. Use the arrow buttons to move the resources listed in the column into the order you want displayed in the Orion Web Console.
10. Click Done.

For more information about using your customized view as a default view assigned to a user, see Editing User Accounts in the SolarWinds 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 SolarWinds Network Performance Monitor Administrator Guide.

Add endpoint-centric resources

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 or interface originated or terminated.

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 SolarWinds Network Performance Monitor Administrator Guide.

Add an endpoint-centric resource

1. Click My Dashboards > Home > Summary.
2. Under All Nodes, click a node. If nodes on are grouped, drill down to the relevant group.
3. Click Customize Page.
4. Click + next to the column in which you want the new resource to be placed.
5. In the Group By list, select Classic Category.
6. Select NetFlow Endpoint-Centric Resources in the list.
7. Select one or more resources, and then click Add Selected Resources.
8. Use the arrow buttons to move the resources listed in the column into the order you want displayed in the Orion Web Console.
9. Click Done.

Edit 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.

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

The time period shown by resources will always be shifted into the past by two minutes compared to the current time settings. There is a two-minute delay in loading data into the database. For example, if you set Relative Time Period to Last 5 Minutes at 11:02, resources display data collected from 10:55 to 11:00.

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 then select a time period.
   - Select Relative Time Period, and then enter a time value and the appropriate unit.
   - Select Absolute Time Period, and then use the date picker and time selector to define a time period.
3. Click Submit.

Edit 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.

Change flow direction in a view

1. Click ▼ next to the flow direction setting below the view name.
2. Select a flow direction: Both, Ingress, or Egress. The Select Flow Direction menu only provides the options that can be applied to the current view.
3. Click Submit.

Delete a filtered view

1. Click Settings > All Settings.
4. Click the trash icon next to the custom menu item.
5. Click Submit.

Create, delete, modify, or restrict 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 be assigned to menu bars. With NOC View Mode enabled, views may be optimized for display in Network Operations Centers.

To make views and graphs larger for larger screens, resize the columns dynamically (drag the division bars) and use your browser zoom controls, such as <Ctrl>+<+> in Chrome.

Create new views

You can customize the Orion Web Console for individual users by creating views.

You need Administrator Rights for creating views.

Plan what should be on a view before you create it.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify objects to see on the view.</td>
<td>Select the appropriate object type, such as nodes, interfaces, groups, applications, and so on.</td>
</tr>
<tr>
<td>View information for all objects of the selected object type.</td>
<td>Select a Summary view.</td>
</tr>
<tr>
<td>View details for a selected object.</td>
<td>Select a Details view.</td>
</tr>
<tr>
<td>Select information about the objects you want to see.</td>
<td>Select resources.</td>
</tr>
<tr>
<td>Divide the information into several tabs.</td>
<td>Enable Left Navigation.</td>
</tr>
<tr>
<td>Optimize the view for large screens or mobile devices.</td>
<td>Create a Network Operations Center (NOC) view.</td>
</tr>
<tr>
<td>Limit what devices should be displayed on the view.</td>
<td>Add a limitation.</td>
</tr>
<tr>
<td>Access the view from the Menu Bar.</td>
<td>Add the view into the menu bar.</td>
</tr>
</tbody>
</table>
Create views

Check out this video on creating a new view.

1. Log in to the Orion Web Console, and click Settings > All Settings.
2. Click Add New View in the Views grouping.
3. Name the view, and select the view type.

![Add New View]

4. Click Submit.

You have now created an empty view. The Customize view page opens automatically. Add resources that contain the information you want to see.

The Type of View affects how the view is made accessible to users, and your choice may not be changed later. For more information, see Specify views for device types.

After you have created a new view, the Customize page opens.

Add resources and columns to views, and define subviews

Administrators can edit views on the Customize page for the view. Click Customize Page on the view, or access the page through Manage Views.

1. Click Settings > All Settings in the menu bar.
2. In the Views grouping, click Manage Views.
3. Select the view, and click Edit.

Add resources to the view

Check out this video on adding and customizing resources.

1. On the Customize page, click + next to the column that you want to add the resources.

![Column 1 and Column 2]

To open the Customize view page, click Settings > All Settings > Manage Views. Select the view, and click Edit.
2. Select resources in the middle pane, and click Add Selected Resources.

   You can limit offered resources by criteria in the Group by list, or search for a resource in the Search box.

3. Use the arrow icons next to the columns to move resources between columns.

4. Click Done.

   The view should now be populated with the resources you selected.

- Resources already in your view are not marked in the list. You can add a resource on a view more than once.
- Some resources may require additional configuration.
- 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.

Add columns

Resources on views are divided into columns.

On the Customize Page, click Add New Column.

   You do not have to add resources here. You can click Done, and drag resources between the columns on the view.

Change column width

To change a column width, position the cursor between the columns and drag the column border to achieve the appropriate width.
Move resources on views

To move resources within a column or between columns on a subview, drag the handle at the top of the resource to the new location.

![Top 10 Nodes by Current Response Time](image)

Divide content into subviews

If there is too much information on the view, group and divide resources into subviews.

1. On the Customize view, select Enable Left Navigation.
   - To open the Customize view page, click Settings > All Settings > Manage Views. Select the view, and click Edit.

2. Click Add Tab.
3. Type a name for the new tab, and click Update.
4. Select an icon, and add resources.
5. Click Done.

   ![Node Details](image)

   To save space on the views, click the double arrow button to minimize subviews.

When you are done with your changes, click Preview, and then click Submit.

Create custom summary views

The Custom Summary view enables you to create a fully customized object-based view.
1. Click My Dashboards > Home > Custom Summary.
2. Click Edit in any Custom Object Resource.
3. Provide a Title and Subtitle for the resource.
4. Select an object type from the Choose Object Type drop-down.

```
Title: Average Response Time
Subtitle: Custom object resource
Choose Object Type: Nodes
Select object: SELECT OBJECT
```
5. Click Select Object.
6. On the Select Objects window, use the Group by selection field to filter the list of monitored objects.
7. Select one or more objects on which to base the selected resource, click the green arrow to move objects into the Selected Objects pane and click Submit to add the objects.
8. Specify what information about the selected object(s) you want to see in the resource, and click Submit.

```
Select a Chart: Average Response Time
Select object:  
Limit Series:  
Show Sum in Data Series:  
Time Period:  
Sample Interval:  
Auto-Hide Resource:  
```

137
The fields displayed and information required depend upon the object type selected.

Add external website views

You can select any external website and add it to the Orion Web Console as a view.

You need Administrator Rights.

1. Log in to the Orion Web Console and click Settings > All Settings in the menu bar.
2. In the Customize Navigation & Look grouping, click External Websites.
3. Click Add.
4. Provide a Menu Title. This will be used for the website in the My Dashboards menu bar.
5. If you want to include a heading for the view, provide an optional Page Title.
6. Provide the URL of the external website, in the following format:
   http://domain_name
7. Select the Menu Bar to which you want to add the website link.
   If you select Admin as the menu bar, the website will be available from My Dashboards > Home for administrators.
8. Click OK.
9. Click Preview to see the external website in the Orion Web Console.
Optimize views for TV screens or mobile devices

A Network Operations Center (NOC) view provides a single page view of critical statistics that can fit on a TV screen or a mobile device. If you define multiple subviews, they rotate automatically on the screen, each subview available as a separate slide.

Headers and footers are compressed in NOC views, increasing the available space to display resources.

Enable NOC Views

You can configure any Orion Web Console view to appear in the NOC view form.

1. Log in to the Orion Web Console as an administrator.
2. Open a view, and click Customize Page in the top right corner of the view.
3. Select Enable NOC view mode.
4. If the view contains several subviews, select the rotation interval for the subview.
   To get a direct link to a NOC view, use the Link to NOC View link.
5. Click Done & Go to NOC View.
   You have created a NOC version of your view with a compressed header and footer, and without the left navigation area.

Customize NOC Views

To add resources, remove resources, or add subviews on a NOC view, click the top-right icon, and select Customize Page.

Exit NOC Views

Click the NOC Settings icon, and select Exit NOC Mode.

You will return to the default view with the full header, footer and left navigation.

Manage NOC Views

You can display a list of all NOC views defined in your Orion to get a better understanding of your NOC views. From the NOC views list, you can easily add, edit or manage your NOC views.

1. Click Settings > All Settings.
2. In the Views grouping, click Created NOC views.
   You can view NOC views from any view. Click Customize Page, and click List of created NOC views in the NOC view section.
3. Manage the NOC views:
   - To add a new view, click Add New View.
   - To edit a NOC view, select the view, and click Edit.
   - To disable a NOC view and maintain the default view, select the view and click Disable NOC.
Display subviews

If more subviews are defined for the view, you can see white circles in the top right corner. The currently active tab is displayed in orange.

To display a subview, click the circle.

Move resources in NOC Views

If you want to move resources within a NOC view, you turn on the drag&drop mode.

1. Click the Settings icon in the top right corner of the NOC view, and select Enable Drag&Drop / Pause.
2. Drag and drop resources within the selected pane.
3. When you have finished repositioning the resources, click the Settings icon again, and select Disable Drag&Drop / Resume.

Change the NOC view logo

You can hide the default SolarWinds logo on the NOC view, or use a customized image in the top left corner of your NOC views.

**Logo requirements:**

- Supported image formats: .png, .jpg
- Maximum resolution: 900x200 px

To use a customized logo on your NOC views:

1. If you already are in a NOC view, click the NOC Settings icon and select Customize NOC View Logo.
2. To hide the logo, clear the NOC View Logo option.
3. To change the logo:
   a. Make sure that NOC View Logo is selected.
   b. Click the Browse button for NOC View Logo and navigate to the appropriate logo image. By default, the SolarWinds logo is used on NOC views. It is available as SW_NOClogo.png in /NetPerfMon/images on your Orion server.
4. Click Submit to apply your changes in the view.

Limit objects on a view

As a security feature, administrators can limit which devices are displayed on a view.

1. Click Settings > All Settings in the menu bar, and click Manage Views in the Views grouping.
2. Select a view, and click Edit.
3. On the Customize View page, click Edit in the View Limitation area.
4. Select the type of view limitation you want to apply, and click Continue.
5. Provide or select strings or options to define the device types that you want to include or exclude from the selected view, and click Submit.

Use a view as a template

When you want to create multiple views, create one view, and use it as a template to create other new views.

If you copy a view with a view limitation applied, that view limitation is carried over to the copied view and any change you make applies to both views. You can delete the view limitation to remove it from all views, and then create a view limitation for each view.

Specify views for device types

In the Orion Web Console, you can specify views displayed for each type of device you have on your network, such as routers, firewalls, or servers.

Export views to PDF

Many views in the Orion Web Console can be exported to portable document format (PDF).
1. Open a view, and click Export to PDF in the top right corner of the view.
2. If you are prompted to save the PDF file, click Save.
3. Navigate to a location, provide a file name, and click Save.

Monitor traffic flow directions

SolarWinds NTAmonitor 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 SolarWinds 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:

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

The size of ingress and 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, SolarWinds NTA shows 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)
Set flow direction

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

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Under Charting and Graphing Settings, use the Default Flow Direction settings to set the defaults for all SolarWinds NTA resources placed in Summary, Node Detail, Interface Detail views.
4. You can also set global Default Flow Direction for CBQoS 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.
5. Click Save.

> Manually adjusting flow direction on an SolarWinds NTA view overrides the global default for that view only.

Change flow direction in a view

1. Click ⬅️ next to the flow direction setting below the view name.
2. Select a flow direction: Both, Ingress, or Egress. The Select Flow Direction menu only provides the options that can be applied to the current view.
3. Click Submit.

View CBQoS data

Class-Based Quality of Service (CBQoS) is an SNMP-based, proprietary Cisco technology available on selected Cisco devices that gives you the ability to prioritize and manage traffic on your network. Using policy maps, also known as policies, the different types of traffic on your network are categorized, and then given a priority. Based on 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% 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 the policy 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](http://www.cisco.com).
SolarWinds NTA does not currently provide a CBQoS configuration capability, but any node managed by SolarWinds NPM can 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 NetFlow sources and CBQoS polling.

For CBQoS-enabled Cisco devices on your network, SolarWinds 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, SolarWinds NTA automatically creates a class-default class which displays the remaining traffic.
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.

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.

**Monitor NBAR2 Applications in SolarWinds NTA**

After you have configured your devices to send NBAR2 data and added the devices for monitoring in NTA, you can identify the top applications and top categories and subcategories of applications consuming bandwidth on your network.

1. To access the Applications Summary view, in the Dashboard, select NetFlow > Apps.
2. In the top of the Top XX Applications resource, select NBAR2 for the type.

NTA populates the chart with the top NBAR2 applications identified by name.

> You can also run reports to view the top categories and subcategories for NBAR2 flows.

> If you see "NO DATA" in the Top XX Applications resource, see this article. Make sure you have completed the NBAR2 requirement for monitoring application IDs.
Top XX Applications

This resource provides a view of the top XX applications responsible for monitored traffic on your network, ranked in order of traffic volume.

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

This resource shows only applications whose monitoring has been enabled on the Manage Applications and Service Ports view. Data for ports and applications whose monitoring is not enabled are collected, aggregated, and shown in the Top XX Applications resource as Unmonitored Traffic. For more information about monitored ports and applications, see Configuring Monitored Ports and Applications.

If you are seeing no data in the Top XX Applications view, make sure you are receiving data for the flow type selected in the top right of the Top Applications panel. If monitoring advanced applications for which you are not seeing a name identified for the application, see NBAR2 Advanced Applications for an explanation of how these applications are classified in NTA.

View more details about displayed applications

- Click a listed application to open the NetFlow Applications Summary view that presents statistics for the selected application.
- Click + to expand a listed application and display the list of nodes and their respective interfaces over which the selected application traffic is currently flowing.
- Click a node or interface to display the NetFlow Application detail view showing statistics for the selected application traffic traversing through the appropriate node or interface.

View unmonitored traffic

If there are applications whose monitoring is not enabled in the Manage Applications and Service Ports page, the Top XX Applications resource on a summary view displays the Unmonitored Traffic item. This item aggregates traffic coming from ports or applications whose monitoring is not enabled at the moment.

1. Click the Unmonitored Traffic item to go the NetFlow Applications Summary view filtered by unmonitored traffic.
2. Consult the Top XX Applications resource. The resource will list unmonitored applications, and allow you to monitor appropriate ports.

Enable monitoring of unmonitored ports

If you are viewing the Top XX Applications resource on an Unmonitored Traffic view, you can enable monitoring of unmonitored ports:
1. In the list of unmonitored applications, click Monitor Port to enable monitoring of the port.
2. On the Monitor Application window, select the port(s) to monitor.
3. Select the Source and Destination IP Address and the protocol to monitor.
4. Enter a Description, and then click Add Application to enable monitoring.

You can also enable monitoring for these applications and ports on the Manage Applications and Service Ports page. For more details, see Configuring Monitored Ports and Applications.

Top XX Applications (Endpoint Centric)

You can customize an endpoint-centric version of this resource and place it on the NetFlow Node Details or Interface Details view.

The endpoint-centric Top XX Applications resource provides a ranked list of applications responsible for traffic passing through the specified node or interface.

For more information about adding endpoint-centric resources, see Add endpoint-centric resources.

Table legend

The table below the chart provides the following information:

<table>
<thead>
<tr>
<th>COLUMN TITLE</th>
<th>CONTENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>The application name with its assigned port number in parentheses.</td>
</tr>
<tr>
<td>Ingress Bytes, Egress Bytes, Ingress Packets, Egress Packets</td>
<td>Displays the amount of data (in bytes and packets) flowing to the selected application through the viewed node or interface. The columns displayed depend on the flow direction set in the top left corner of the view (either only Ingress Bytes, or only Egress Bytes, or both columns).</td>
</tr>
<tr>
<td>Percent (Utilization)</td>
<td>Displays the percentage of all traffic through the viewed object attributed to use of the listed application.</td>
</tr>
<tr>
<td></td>
<td>The first value describes the percentage of the appropriate item based on items shown by the chart. Individual items in the legend add up 100%.</td>
</tr>
<tr>
<td></td>
<td>This percentage can be absolute or relative. For more information, see Percentage type for Top XX lists.</td>
</tr>
<tr>
<td></td>
<td>A value in parentheses is available only for interfaces. It describes how the appropriate item utilizes the interface bandwidth in percentage.</td>
</tr>
<tr>
<td></td>
<td>If the utilization is approximately twice as high as it should be, for example 150% instead of 75%, it might be caused by flow duplication. For more information, see Resolve duplicate flows.</td>
</tr>
</tbody>
</table>
Edit the resource

If you are logged in using a User ID with administrative privileges, you can change the way this resource is displayed for all users:

1. Click Edit to load the Customize/Edit Resource page.
2. Make changes.
3. Click Submit.

Edit time and flow direction for the view

You can also change the time period and flows direction shown by all resources in the view:

1. Directly below the view name, click ☑ next to the appropriate setting and define the appropriate settings.
2. Change the Relative Time Period, by default set to 1 hour prior to the current time, or specify a specific time period.

The time and flow direction settings are limited to the current session only. After you leave the view, your changes will be lost and default settings are re-applied.
Common tasks and user scenarios

While SolarWinds NPM reports the bandwidth usage on a given interface, SolarWinds NTA provides information about the actual user of that bandwidth and the applications the user is running.

This section guides you through tasks you may want to accomplish with SolarWinds NTA, and provides user scenarios illustrating how you can solve business problems.

CBQoS policies

SolarWinds NTA offers flow traffic statistics that can help in determining what CBQoS classes and policies to create and apply. SolarWinds 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. SolarWinds NTA provides information for tuning the CBQoS implementation.

The following sections explain how to use SolarWinds 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, see the Cisco documentation.

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 set up to export flow data and SolarWinds NTA is showing the devices under NetFlow Sources on the NetFlow Traffic Analyzer Summary view, begin by examining each node for traffic statistics and useful traffic information. For more information about setting Cisco devices, see Add flow-enabled devices and interfaces to the Orion database.

The following steps cover the basic process for using SolarWinds NTA to analyze flow data in preparation to defining a CBQoS strategy. These steps are meant to give general guidance on how to use SolarWinds NTA in analyzing your current traffic as it pertains to determining CBQoS needs.

1. Click My Dashboards > NetFlow > NTA Summary.
2. Under NetFlow Sources, expand a node, and then click an interface for which you want to analyze the traffic. This brings up an Interface Details view for the interface.
3. Click next to Time Period and 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.
4. Click Submit.
5. Click next to Flow Direction and set the flow direction for which you want to review the traffic.
6. Click Submit.
7. Use a combination of Top XX resources on the Interface Details to analyze how traffic data is flowing through the interface. For example:
   Use 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 YouTube streaming. You probably need to follow up on what you see in Top XX Applications by viewing Top XX Conversations or by using another tool, like 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 may only list the application as HTTP. By cross-referencing 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 involved in generating the real bandwidth-intensive data. Use Top XX Conversations to view the endpoints involved in the highest bandwidth-consuming conversations, and to determine 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. You also want to discover the uses of bandwidth that are not related to the primary purposes of your organization, so that you can lower the priority of this traffic when you put it in a CBQoS class.
   In this case, since the conversation gives you endpoints, you can use DNS, with a tool like nslookup, to discover where 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 www.youtube.com tells you that audio or video data is being transferred.
   Use Top XX Traffic Sources or 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. For information on using persistent instead of On Demand DNS, see DNS and NetBIOS resolution.
   When viewing traffic history in this way, you probably will observe obvious top priorities for shaping the use of bandwidth on the interface.
8. Repeat steps 3 through 9 for each flow-enabled Cisco device for which you might need to create CBQoS policies.
9. 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.
10. 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 usage, if traffic exceeds bandwidth, shaping occurs based on the desired priority.
Monitor CBQoS dynamically

This section assumes that you set up your CBQoS policies and applied them to interfaces on your devices, and that devices are all being monitored in SolarWinds NPM and are listed in SolarWinds NTA as NetFlow Sources.

For more information on discovering network devices, see Discovering and Adding Network Devices in the SolarWinds Network Performance Monitor Administrator Guide.

For more information on setting up on NetFlow collections, see Set 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 SolarWinds 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.

Configure a CBQoS alert

1. Click Alerts & Activity > Alerts.
2. Use the Group By list to filter alerts.
3. Select the relevant CBQoS alert.
4. Click Edit Alert Definition.
   a. On Properties, click Enabled to turn the alert on, and then select an Evaluation Frequency of Alert.
   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 Time of Day, define the days and times during which the software actively evaluates the database for trigger conditions. The default is Always Enabled.
e. 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 a contact.

On the URL tab, if you changed the default Orion login from Admin with a blank password, change the URL the trigger action uses to send the notification.

For example, if your new credentials are user name My User with the password Bravo, adjust the default URL as follows:

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

becomes:

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

f. On Reset Actions, define actions to execute when the software resets the alert.

5. Click Next, and click Submit.

**Monitor autonomous systems through BGP**

SolarWinds NTAsupports monitoring autonomous system networks and autonomous system conversations using the border gateway protocol (BGP). You set up network devices within autonomous systems.

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

### Prepare to monitor autonomous systems

SolarWinds NTAcollects and stores information regarding autonomous systems that network devices send in the NetFlow packets they export. You set up a network device for exporting autonomous system information as part of setting up the device to export NetFlow.

> Since in sFlow BGP/AS information is provided in a special and extended header, SolarWinds NTA does not collect and process BGP/AS data for sFlow.

SolarWinds 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, SolarWinds 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, SolarWinds 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 SolarWinds 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 SolarWinds 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.
  
    You cannot include both origin and peer statistics.

- Each device that exports NetFlow data to SolarWinds NTA must be monitored in SolarWinds NPM.

Traffic from a device that is not monitored in SolarWinds NPM appears only in aggregate as part of the traffic from all unmonitored devices. If the device is setup to export data to SolarWinds NTA, but is unmonitored in SolarWinds NPM, the collector may receive the data without being able to analyze it meaningfully.

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

Set up a device for monitoring by SolarWinds NTA as part of an autonomous system

1. Log in to the network device.
2. Based on the documentation of the device, 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, search for an appropriate configuration guide on the [Cisco website](https://www.cisco.com).
   - For information on enabling NetFlow for Cisco Catalyst switches, see [Enable NetFlow and NetFlow data export on Cisco Catalyst switches](https://www.cisco.com).
   - For information on enabling NetFlow on Cisco ASA devices, see [Cisco ASA NetFlow overview](https://www.cisco.com).
   - Otherwise, consult these examples:
     - [Brocade (Foundry) sFlow configuration](https://www.brocade.com)
     - [HP sFlow configuration](https://www.hp.com)
     - [Extreme sFlow configuration](https://www.extreme.com)
     - [Juniper sFlow configuration](https://www.juniper.net)
     - [Juniper J-Flow configuration](https://www.juniper.net)

4. Add the device exporting NetFlow to SolarWinds NPM for monitoring.
   If you are adding a large number of NetFlow enabled nodes, use Orion Network Sonar. For more information, see [Discovering and Adding Network Devices](https://www.solarwinds.com) in the SolarWinds 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 Orion Web Console](https://www.solarwinds.com) in the SolarWinds Network Performance Monitor Administrator Guide.
5. Verify that the device is exporting NetFlow data and that the device is monitored in SolarWinds NPM. To verify that data are exported correctly, use a packet capture tool, such as WireShark, to search for packets sent from the network device to the Orion server. The following is an example of a successfully enabled NetFlow device. If you successfully add a NetFlow enabled device with the IP address 10.199.14.2 to SolarWinds NPM, and the device is actively exporting NetFlow data to the Orion server, you will see in WireShark a packet like the one (49) highlighted below in gray:

As expected, the packet details show that 10.199.14.2 is its source IP address and 10.110.6.113 is the destination, which is the Orion server. This correlates with the node details on the device in Orion (highlighted in yellow).

To verify that the IP address of the exporting interface on the network device is the one being monitored in Orion:

a. Open a command line interface, log in to the network device, and then enter `show run` to see the running configuration of the device.

b. Page down to the lines where the export source interface is defined. In this example, it is `ip flow-export source Ethernet0/0`.

To discover the IP address for this interface, enter `show run int Ethernet0/0`. The IP address of the interface, 10.199.14.2, is monitored by the Orion server.

Under NetFlow Source, verify the NetFlow-enabled nodes listed with a recent time posted for collected flow.

7. Click My Dashboards > NetFlow > BGP. You should see chart statistics in the Top XX Autonomous Systems and Top XX Autonomous Systems Conversations resources.

**Autonomous system requirements**

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

> SolarWinds 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:

<table>
<thead>
<tr>
<th>BYTES</th>
<th>CONTENTS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>40-41</td>
<td>src_as</td>
<td>Autonomous system number</td>
</tr>
<tr>
<td>42-43</td>
<td>dst_as</td>
<td>Autonomous system number</td>
</tr>
</tbody>
</table>


NetFlow v9, IPFIX, and compatible flows

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

<table>
<thead>
<tr>
<th>FIELD TYPE</th>
<th>VALUE</th>
<th>LENGTH (BYTES)</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRC_AS</td>
<td>16</td>
<td>N (default 2)</td>
<td>Source BGP autonomous system number where N could be 2 or 4.</td>
</tr>
<tr>
<td>DST_AS</td>
<td>17</td>
<td>N (default 2)</td>
<td>Destination BGP autonomous system number where N could be 2 or 4.</td>
</tr>
<tr>
<td>PeerSrcAS</td>
<td>129</td>
<td>N (default 2)</td>
<td>Peer source autonomous system number</td>
</tr>
<tr>
<td>PeerDstAS</td>
<td>128</td>
<td>N (default 2)</td>
<td>Peer destination autonomous system number</td>
</tr>
</tbody>
</table>


Manage autonomous systems

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.

Add an autonomous system

1. Click Add Autonomous System.
2. Enter values for the new autonomous system.
3. Click Save.
Edit an autonomous system

1. Under the Actions column, click Edit next to an autonomous system.
2. Modify values for the autonomous system.
3. Click Save.

Delete an autonomous system

1. Under the Actions column, click Delete next to an autonomous system.
2. Click Save.

Monitor autonomous systems

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

Top XX Autonomous Systems

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

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

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

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.

IP address groups

SolarWinds 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.

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
3. Under IP Address Groups, click Manage IP Address Groups.
4. Make your changes:
   - Select IP ranges to monitor
   - Add IP address groups
   - Edit IP address groups
   - Delete IP address groups
5. Click Submit. For more information, see Submit changes.

Find the cause of high bandwidth utilization

If a node managed in SolarWinds NPM is also a NetFlow source, it exports NetFlow data that you are currently monitoring in SolarWinds NTA. You can use SolarWinds NTA to analyze interface bandwidth utilization on the node whenever your workflow requires.

This procedure assumes that you have created an Orion 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.

1. Click My Dashboards > NetFlow > NTA Summary.
2. Under NetFlow Sources, locate and expand the relevant node.
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, SolarWinds 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.

**Track 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 SolarWinds NTA is to set up 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 SolarWinds NTA toolbar.

1. Click My Dashboards > NetFlow > NTA Summary.
2. Click Flow Navigator on the left edge of the summary view. The Flow Navigator is available on any default SolarWinds NTA view.
3. Under View Type, select Detail.
   a. Select the IP Address Group View Type.
   b. Select the node that corresponds to the main network device for the site, through which all or most traffic passes.
   c. Use the private address range in the View Filter list that encompasses the specific site.
4. Select the Time Period over which you want to view network traffic by country of origin or destination.
5. Select a Flow Direction.
6. You can further limit the view by including or excluding the following items: Applications, Autonomous Systems, Autonomous System Conversations, Conversations, Domains, Endpoints, IP Address Group Conversations, Protocols, and Types of Service.
   a. Select Include or Exclude traffic.
   b. Enter the appropriate value(s).
   c. Click Add Filter.
   - Under Domains, if a domain name is not resolved and saved in SolarWinds NTA, you cannot use it in the Flow Navigator. SolarWinds 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](#).
   - Under Endpoints, you can either type the range, for example 192.168.1.0-192.168.1.255, or use the CIDR notation, for example 192.168.1.0/24.
7. Click Submit.
8. Click Save Filtered View to Menu Bar, and enter a name.
9. Click OK.

Perform 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.

The hostname is also retrieved on a scheduled basis. For more information, see DNS and NetBIOS resolution.

The thwack user community

By default, SolarWinds NTA provides the thwack Recent NetFlow Posts resource on the NetFlow Traffic Analyzer Summary view. This resource shows the most recent posts related to SolarWinds NTA that have been submitted to thwack, the online SolarWinds user community. Click a post title to open it in the SolarWinds NTA forum on thwack.

User scenarios

The following user scenarios illustrate the value of SolarWinds NTA and how it can immediately offer you a return on your investment.

Locate and isolate an infected computer

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.

Use SolarWinds NTA to quickly pinpoint and respond to the wide variety of viruses that can attack your network.

1. Check that the link to the branch network is up.
2. Click My Dashboards > Network > NPM Summary.
3. Consult the Percent Utilization chart. You see that the current utilization is 98%, even though normal branch network utilization is 15-25%.
5. Under NetFlow Sources, click the name of the branch network to view its flow-enabled router.
6. Under Top 10 Endpoints, 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.
7. Under Top 10 Applications, you see that 100% of the last two hours of traffic from the publicly accessible computer has been generated by an IBM MQSeries messaging application. Click the application name to determine that the IBM MQSeries messaging occurs over port 1883.

8. You do not have any devices using IBM MQSeries messaging in the customer accessible location, nor any other services or protocols that require port 1883. You recognize that this is a virus exploit.

9. Use a configuration management tool, such as SolarWinds Network Configuration Manager, to push a new configuration to your firewall that blocks port 1883.

Locate and block unwanted use

Consider the following scenario:

*Your uplink to the Internet has been slowing progressively over the last six months, even though your number of employees, application use, and dedicated bandwidth have all been stable.*

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

1. Click My Dashboards > Home > Summary. Check that the link to the Internet is up at your site.
2. Under Nodes with Problems, click the specific uplink.
3. Under Current Percent Utilization of Each Interface, you see that the current utilization of your web-facing interface is 80%.
4. Click the web-facing interface to open the Interface Details view.
5. Customize the Percent Utilization chart to show the last six months. You see that there has been steady growth from 15% to 80% consumption over time. There are even spikes into the high nineties.
7. Under NetFlow Sources, click the web-facing interface to open the NetFlow Interface Details view.
8. Under Top 5 Endpoints, you see that a group of computers in the 10.10.12.0-10.10.12.255 IP range is consuming most of the bandwidth. These computers reside in your internal sales IP range.
9. 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.
10. Use a configuration management tool, such as SolarWinds Network Configuration Manager, to push a new configuration to your firewall that blocks all traffic on these two ports.
11. Within minutes, you see the traffic on the web-facing interface drop back to 25%.

Recognize and stop a denial-of-service attack

Consider the following scenario:

*A SolarWinds NPM advanced alert tells you that your web-facing router is having trouble creating and maintaining a stable connection to the Internet.*
SolarWinds NTA helps you easily characterize both outgoing and incoming traffic. This ability becomes ever more important as corporate networks are exposed to malicious denial of service attacks.

1. Click My Dashboards > Home > Summary.
2. Under Top 10 Nodes by Average CPU Load, you notice the CPU load on the firewall node is holding steady between 99% and 100%.
3. Click the firewall node name to open its Node Details view. Under Current Percent Utilization of Each Interface, you see that your firewall interfaces are receiving abnormally high levels of traffic.
5. Under Top 10 Endpoints, you see that the top six computers attempting to access your network are overseas. You realize that you are being port scanned and that your firewall is interactively blocking these attacks.
6. 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.
7. In minutes, your CPU usage drops back to normal.
Users

Users need an Orion Web Console account to perform actions in your SolarWinds product, such as acknowledging alerts. Default account views and privileges are assigned in the account manager.

- Create users
- Define what users can access and do
- Restrict user access to network areas by applying limitations

For more information, see sections on users in the SolarWinds Orion Platform online help.

Create users

Before you begin, consider what tasks the user must perform, and what views and menu bars are most suitable.

Users created using default settings can log in to the Orion Web Console and see information available in views, resources, and reports. For administration and customization tasks, users need extra rights.

1. Log in to the Orion Web Console, and click Settings > All Settings.
2. Click Manage Accounts in the User Accounts grouping, and click Add New Account on the Individual Accounts tab.

3. Select Orion individual account, and click Next.
4. Provide the account credentials, and click Next.
5. On Define Settings, provide rights so that the user can perform assigned tasks, select default views and menu bars, and then click Submit.

The user account is listed in the Individual Accounts tab.

Create users based on existing Active Directory or local domain accounts

Users can use their existing Active Directory credentials to log in to the Orion Web Console, so you do not need to manage an extra user account.

> You must enable Windows Account Login in the Orion Web Console.
  1. Click Settings > All Settings, and in Product Specific Settings, click Web Console Settings.
  2. In Windows Account Login, select Enable automatic login, and click Submit.
> To maintain administrative privileges, individual and group Windows user accounts must be defined in the same domain as the SolarWinds server they can access.
> Only Security AD groups are supported. Distribution Groups are not supported.

1. Log in to Orion Web Console, and click Settings > All Settings.
2. Click Manage Accounts in the User Accounts grouping, and click Add New Account.
3. Select Windows individual account or Windows group account, and click Next.

4. Provide the credentials for an account with administrative access to the Active Directory or local domain, and click Next.
5. If a system account is available, you can use it. Select Use [Account Name] account to access Active Directory or Local Domain, and click Test Active Directory.

   You may need to specify the credentials manually.

6. To specify the credentials manually, select Specify credentials to access the Active Directory or Local Domain, and provide the credentials.

7. Search for the Active Directory or local domain account.

   To search for all users or groups in the domain, enter domain name\* and click Search.

8. Select the appropriate users in the Add Users area, and click Next.

9. On Define Settings, provide rights so that the user can perform assigned tasks, select default views and menu bars, and then click Submit.

Users can now log in to the Orion Web Console using their local domain or Active Directory credentials.

If you use Active Directory, users can also automatically login with their Windows credentials.

Define what users can access and do

Each user or group account can have different privileges applied to it, such as the ability to modify alert definitions or delete nodes.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. Click Manage Accounts in the User Accounts grouping.
4. Select an account, and click Edit.
5. Specify the login options.

<table>
<thead>
<tr>
<th>LOGIN OPTION</th>
<th>SETTING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Should the user be able to log in immediately?</td>
<td>Set Account Enabled to Yes. Disabling an account does not delete it. Account definitions and details are stored in the SolarWinds Orion database and can be enabled later.</td>
</tr>
<tr>
<td>Should the user be able to log in only temporarily?</td>
<td>Specify the expiration date.</td>
</tr>
<tr>
<td>Should the user be logged in indefinitely even if the browser is closed?</td>
<td>Select Yes for the Disable Session Timeout option. Session timeouts are global and set in Web Console Settings. By default, new user accounts are configured to timeout automatically.</td>
</tr>
</tbody>
</table>
6. Specify what tasks the user should be able to do.

<table>
<thead>
<tr>
<th>Task</th>
<th>Access (Select Yes for this option or do as instructed)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add and edit user accounts and reset passwords.</td>
<td>Allow Administrator Rights</td>
</tr>
<tr>
<td>SolarWinds recommends that you do not allow users to change their own Orion Web Console account passwords.</td>
<td>Granting administrator rights does not assign the Admin menu bar to a user.</td>
</tr>
<tr>
<td>Add, edit, and delete nodes.</td>
<td>Allow Node Management Rights</td>
</tr>
<tr>
<td>Create, edit, and delete maps in the Network Atlas.</td>
<td>Allow Map Management Rights</td>
</tr>
<tr>
<td>Add, edit, schedule, and delete reports.</td>
<td>Allow Report Management Rights</td>
</tr>
<tr>
<td>Add, edit, and delete alerts.</td>
<td>Allow Alert Management Rights</td>
</tr>
<tr>
<td>Customize views.</td>
<td>Allow Account to Customize Views</td>
</tr>
<tr>
<td>Enable/disable monitoring elements.</td>
<td>Allow Account to Unmanage Objects</td>
</tr>
<tr>
<td>Acknowledge and clear events, advanced alerts, and Syslogs.</td>
<td>Allow Account to Clear Events, Acknowledge Alerts and Syslogs.</td>
</tr>
</tbody>
</table>

7. If you want the user to use additional browser functions, such as right-click menu options, set Allow Browser Integration to Yes.

   Right-click menu options also depend on installing the SolarWinds Desktop Toolset and running the Toolset Integration Tray application on each client computer.

8. Provide the maximum Number of Items in the Breadcrumb List.

   To show all available items in breadcrumb drop-downs, set this option to 0.
9. Click Submit.

New account settings are applied when a user next logs in.

**Restrict user access to network areas by applying limitations**

Account limitations restrict user access to specific network areas or withhold certain types of information from designated users.

To limit user access, apply a limitation on the user account, and specify the network area the user can access. Depending on the limitation, you can use [logical operators and wildcards](#).

Pattern limitations can have a negative impact on performance and are error prone.

If the default limitations are not enough, you can create limitations based on custom properties, and apply them on user accounts.

- Group limitations are not applied until after the group availability is calculated.
- Because SolarWinds NetFlow Traffic Analyzer (NTA) initially caches account limitations, it may take up to a minute for account limitations to take effect in SolarWinds NTA.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the User Accounts grouping, click Manage Accounts.
4. Edit an individual or group account.
   a. Click Add Limitation in the Account Limitations section.
   b. Select the type of limitation to apply, and click Continue.
   c. Define the limitation, and click Submit.
      The limitation will be added to the Edit Account page.
5. Click Submit.

When the user logs back in, the account respects the limitations applied to it.

**Change account passwords**

When you log in to the Orion Web Console for the first time, SolarWinds recommends that you change the password for the Admin account.
Only users with administrator rights can change the password.

1. Log in to the Orion Web Console, and click Settings > All Settings.
2. Click Manage Accounts in the User Accounts grouping.
3. Select a user, and click Change Password.

4. Enter and confirm the new password, and click Change Password.

## Patterns for limitations

When restricting user access to network areas, you can specify the limitation with patterns using OR, AND, EXCEPT, and NOT operators with _ and * as wildcards if the limitation allows pattern matching.

> Patterns are not case sensitive.

You may also group operators using parentheses, as in the following example.

\[(*)foo*\ EXCEPT \(*b*)\ AND \(*all* \ OR \ *sea*)\] matches seafood and footfall, but not football or Bigfoot.

## Limit users to specific network areas

Account limitations ensure that Orion Web Console users only view the network objects that are relevant to their job duties.

You can use account limitations in the following ways:

- Limit customer views to specific network nodes
- Limit views by department or functional area
- Limit views by device type or device role
- Limit views based on the geographic location of devices

Predefined account limitations use built-in SolarWinds Orion properties to limit user access. For greater flexibility, you can create your own account limitations in the Account Limitation Builder, based on custom properties.
Reports

In SolarWinds NTA, flow data are stored in the NTA Flow Storage Database and CBQoS data are stored in the SolarWinds Orion database. Over time, both databases accumulate a large amount of information. SolarWinds offers both a broad array of predefined reports and user interfaces that enable you to create your own custom reports.

You can find and execute all reports in the Orion Web Console. See Create and view reports in the NPM online documentation for more information.

SolarWinds NTA offers several NetFlow-specific predefined reports.

NetFlow-specific predefined reports

Several standard NetFlow-specific reports are available with SolarWinds NetFlow Traffic Analyzer. You can modify the predefined reports or create new reports.

Access NetFlow reports

1. Click Reports > All Reports.
2. Under Group By, select Report Category. NetFlow-specific reports are grouped into the following categories:
   - Historical NetFlow reports
   - Historical CBQoS reports

![i] All reports with domain information require persistent DNS resolution. For more information, see DNS and NetBIOS resolution.

Historical NetFlow reports

Top 100 Applications – Last 24 Hours

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

Top 50 Cisco WLC Applications- Last 24 Hours

Displays the name and byte count of the top advanced applications in monitored Cisco WLC flows in the last 24 hour period. The table lists the name, number of Ingress and egress bytes, and number of ingress and egress packets.

Top 100 CBQoS Drops - Last 24 Hours

Top 100 CBQoS Post-Policy

Top 100 CBQoS Pre-Policy
Top 100 CBQoS Stats - 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 NBAR2 Application Categories - Last 24 Hours**

Displays the top NBAR2 applications by category and byte count in NBAR2 monitored flows in the last 24 hour period.
Top 50 NBAR2 Application Subcategories - Last 24 Hours

Displays the top NBAR2 applications by subcategory and byte count in NBAR2 monitored flows in the last 24 hour period.

Top 50 NBAR2 Applications - Last 24 Hours

Displays the application name and byte count of the top advanced applications in NBAR2 monitored flows in the last 24 hour period.

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

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.

Best practices for SolarWinds NTA reports
To solve performance issues caused by custom reports, consider the following recommendations. If appropriate, a SWQL code example is attached.

- To optimize the speed of executing reports and to optimize the performance, add the ID columns for all appropriate objects to the report. If you do not want to see these columns in the report, hide them.

The recommendations are valid for SolarWinds NTA 4.1 and newer with SolarWinds NPM 11.5 and newer.
- Do not query all data from NTA Flow Storage Database, use the Top XX Results to cover the most significant traffic. Every filter that limits data speeds up the report.

**SWQL Example: Data limitation**
The following query limits the report to show top 10 nodes only:

```sql
SELECT TOP 10 [T1].[NodeID], SUM([T1].[TotalBytes]) AS TotalBytes
FROM Orion.NetFlow.Flows AS T1
ORDER BY TotalBytes DESC
```

- Limit the data by time. If a query in SWQL does not use a time limit, all available data are queried. To query only the last hour, use the value 0.04167, which is calculated as 1 day/24 hours.

**SWQL Example: Time condition in SWQL**
The following query limits the report to show top 100 nodes during the last day:

```sql
SELECT TOP 100 [T1].[NodeID], [T1].[InterfaceIDTx], [T1].[InterfaceIDRx], SUM([T1].[TotalBytes]) AS TotalBytes
FROM Orion.NetFlow.Flows AS T1
WHERE ([T1].[TimeStamp] >= (GetUTCDate() - 0.04167))
GROUP BY [T1].[NodeID], [T1].[InterfaceIDTx], [T1].[InterfaceIDRx]
ORDER BY TotalBytes DESC
```

- Test out a new report using a short time period. If a report with a short time period works out, and a longer time period causes the report to crash, there might be an issue with provided time periods.

**SWQL Example: Time condition in SWQL**

```sql
SELECT [T1].[ToSID], IngressBytes
FROM Orion.NetFlow.Flows AS T1
WHERE ([T1].[TimeStamp] >= (GetUTCDate() - 0.005))
```
Use aggregation functions.

**SWQL Example: Aggregation**

When you use aggregation in a SWQL query, all 'other' columns must be grouped. Reports created via the user interface group these columns automatically.

```sql
SELECT SourceIP, DestinationIP, Port, Protocol, MAX(IngressBytes) AS IngressMaximum, MIN(IngressBytes) AS IngressMinimum
GROUP BY SourceIP, DestinationIP, Port, Protocol
```

Comments in SWQL

If you are adding comments in SWQL, start the comment on a separate line and add an extra line after the comment. Generally, you can place comments anywhere. Comments are started by a double dash sign (--); a comment is everything on one line which comes after the -- sign, up to the end of the line.

**Execute a SolarWinds NTA report**

1. Click Reports > All Reports.
2. Under Group By, select Product.
3. Click NTA Reports.
4. Select the report you want to run and click View Report.
5. Click Export to PDF or Printable Version to save the report.

For helpful information about running NTA reports, see [Best practices for SolarWinds NTA reports](#).

**Create a report**

Before creating a new report, look at the predefined reports. Consider whether you can use a predefined report, adjusting certain properties or the time frame.

For detailed information about creating reports in the Orion Web Console, see [Create and view reports](#) in the NPM online documentation for more information.

1. Click Reports > All Reports.
2. Click Manage Reports.
3. Decide whether to copy and edit a predefined report, or create a new report.
   - To adjust an existing report, select the report, and click Duplicate & Edit.
   - To create a new report, click Create New Report.
4. Click Custom Table. SolarWinds NTA does not support Custom Chart.
5. Click Select and Continue.
6. Select a NetFlow object to report on.
7. Click Add to Layout.
8. Define what the custom table should show in the resulting report. Select properties and sorting of items:
   a. Add columns.
   b. To edit information provided by individual columns, click Advanced in the column.
   c. Define sorting of items in the report with Sort Results By.
   d. Define grouping of data with Group Results By.
   e. To limit the number of items on the report, use the Filter Number of Results section.
   f. Time-Based Settings 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. The column is hidden by default, as indicated by the icon.
   g. Click Preview Resource, review the preview, and click OK.
   h. Click Submit.
9. Complete the Add Report wizard, clicking Next between each step.
   a. Define the layout: header, content, and footer.
   b. Preview the report.
   c. Enter report properties: description, category, custom properties, or limitation.
   d. Schedule the report, if desired.
   e. Click Submit.

Create a report using SWQL

You can define the objects you want to report on using the Semantic Web query language (SWQL).

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. Click Reports > All Reports.
2. Click Manage Reports.
4. Click Custom Table, and then click Select and Continue.
5. Define the objects to query:
   a. Under Selection Method, select Advanced Database Query (SQL, SWQL).
   b. Click SWQL as the Query Type and enter the code. For more information about the SWQL supported by Orion, see [Using SWQL](#).
   To discover table and field names in your database, use the Orion SDK API, available in the [Orion SDK forum](#) on thwack.com.

**Log in to the Orion SDK**
- Download and install the Orion SDK on the same server as you run SolarWinds NTA. For more information about downloading and using the Orion SDK, see [Orion SDK Information](#).
- Start the SWQL Studio in your program folder.
- Enter information to connect to the SolarWinds Information Service:
  - Server Name: localhost
  - Server Type: Orion (v3)
  - User Name and Password: Use the same credentials that you use to log on to the Orion Web Console.

6. Define columns that will present the data gathered by your SWQL query, and click Submit.
7. Add the report.
   a. Define the report layout, preview the report, and define the report properties.
   b. Click Submit.

### Edit a SolarWinds NTA report

This section provides details on the most usual edits in reports:

#### Change objects that are being reported on

1. Click Reports > All Reports.
2. Click Manage Reports.
3. Select a report and click Edit Report or Duplicate & Edit if you want to edit a copy of the report and retain the original. To find historical NetFlow reports, under Group By select Report Category, and click Historical NetFlow Reports.
4. On the Edit Report view, under Content, click Edit next to the For list.
5. Change the objects for the report on the Add Content menu, and click Add to Layout.
6. Complete the wizard.
   You can either use the Next buttons or click the Summary tab to switch directly to the last screen. Click Submit.
Change the time of the report

1. Click Reports > All Reports.
2. Click Manage Reports.
3. Select a report and click Edit Report or Duplicate & Edit if you want to edit a copy of the report and retain the original. To find historical NetFlow reports, under Group By select Report Category, and click Historical NetFlow Reports.
4. On the Edit Report view, under Content, select a time period in the From list.
5. Complete the wizard.
   You can either use the Next buttons or click the Summary tab to switch directly to the last screen. Click Submit.

Define a customized time period

Reports only support uninterrupted time intervals. It is 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.

1. Click Reports > All Reports.
2. Click Manage Reports.
3. Select a report and click Edit Report or Duplicate & Edit if you want to edit a copy of the report and retain the original. To find historical NetFlow reports, under Group By select Report Category, and click Historical NetFlow Reports.
4. On the Edit Report view, under Content, select Custom in the From list.
5. In the Add Time Period menu, enter a Named Time Period. This name is used in the For list.
6. Specify the time period: relative or custom.
7. Click Add.
8. Select the new custom time period in the From list.
9. Complete the wizard.
   You can either use the Next buttons or click the Summary tab to switch directly to the last screen. Click Submit.

Change the page layout

You can change a report layout so that you have two or more data sources next to each other to compare the values.

1. Click Reports > All Reports.
2. Click Manage Reports.
3. Select a report and click Edit Report or Duplicate & Edit if you want to edit a copy of the report and retain the original. To find historical NetFlow reports, under Group By select Report Category, and click Historical NetFlow Reports.
4. On the Edit Report view, under Content, select a layout from the Page Layout list.
5. Complete the wizard.
   You can either use the Next buttons or click the Summary tab to switch directly to the last screen.
   Click Submit.

Change the logo

You may need to replace the default SolarWinds logo with your company's logo. The provided space allows for maximum height of 103 pixels and a maximum width of 238 pixels. Larger images are scaled to fit the space.

1. Click Reports > All Reports.
2. Click Manage Reports.
3. Select a report and click Edit Report or Duplicate & Edit if you want to edit a copy of the report and retain the original. To find historical NetFlow reports, under Group By select Report Category, and click Historical NetFlow Reports.
5. Click Browse for Logo, navigate to the file, and then select it.
6. Complete the wizard.
   You can either use the Next buttons or click the Summary tab to switch directly to the last screen.
   Click Submit.

Limit access to the report

You can specify a group of users who can access individual reports.

1. Click Reports > All Reports.
2. Click Manage Reports.
3. Select a report and click Edit Report or Duplicate & Edit if you want to edit a copy of the report and retain the original. To find historical NetFlow reports, under Group By select Report Category, and click Historical NetFlow Reports.
4. Click the Properties tab at the top of the screen.
5. Expand Report Limitation, and then select a report under Report Limitation Category.
6. Complete the wizard.
   You can either use the Next buttons or click the Summary tab to switch directly to the last screen.
   Click Submit.

Specify custom properties

You can assign custom properties to your reports to help you manage your reports. For example, you can have a custom property called Department, and provide the information for which department the report is used.
1. Click Reports > All Reports.
2. Click Manage Reports.
3. Select a report and click Edit Report or Duplicate & Edit if you want to edit a copy of the report and retain the original. To find historical NetFlow reports, under Group By select Report Category, and click Historical NetFlow Reports.
4. Click the Properties tab at the top of the screen.
5. Enter values for all required custom properties.
6. Complete the wizard.
   You can either use the Next buttons or click the Summary tab to switch directly to the last screen.
   Click Submit.

**Schedule a report**

You can set the report to run according to a defined schedule. Generated reports can be sent to an email address. SolarWinds NPM 10.7 or newer is required.

1. Click Reports > All Reports.
2. Click Manage Reports.
3. Select a report and click Edit Report or Duplicate & Edit if you want to edit a copy of the report and retain the original. To find historical NetFlow reports, under Group By select Report Category, and click Historical NetFlow Reports.
4. Click the Schedule Report tab at the top of the screen.
5. Click Schedule This Report to Run Regularly.
6. Assign an existing schedule or create a new one.
7. Complete the wizard.
   You can either use the Next buttons or click the Summary tab to switch directly to the last screen.
   Click Submit.

**Create a custom report for IP address groups**

SolarWinds NPM 10.7 or newer is required.

1. Click Reports > All Reports.
2. Click Manage Reports.
4. Click Custom Table, and then click Select and Continue.
5. Define what objects should be in the report. We want to report on collected traffic connected with IP address groups. IP addresses included in a group have a property that gives the IP address group.
   b. Click Advanced Selector.
   d. Click Select Field.
   f. Under Database Column name, click IP Address Group Name.
   g. Click Add Column.
   h. On the Add Content menu, go to the IP Address Group name property list and select Is Not Empty.
   i. Enter a Selection Name.
   j. Click Add to Layout.

6. Define what columns you want to see in the report, how the items should be sorted, how many items you want to see, how the items should be grouped, and details for individual columns:
   a. Click Add Column.
   b. Add appropriate columns.
      - Add the IP Address Group Name column:
        i. Select NetFlow Flow by IP History in the Orion Object list.
        iii. Under Database Column Name, select IP Address Group Name.
      - Add the Bytes column:
        i. Select NetFlow Flow by IP History in the Orion Object list.
        iii. Under Database Column Name, select Bytes.
      - Add the Node Name column:
        i. Select Node in the Orion Object list.
        ii. Under Available Columns, click Node.
        iii. Under Database Column Name, select Node Name.
      - Click Add Column.
   c. Define table sorting.
      i. Under Sort Results By, select Bytes - NetFlow Flow by IP History.
      ii. Define the sorting direction as Ascending.
d. Specify units and aggregation of bytes.
   i. Under the Bytes column, click Advanced.
   ii. In the Add Display Settings list, select Data Unit.
   iii. In the Units of Measurements list, select Bytes (1000). This defines the units shown on the report.
   iv. In the Units in My Database list, select B.
   v. In the Data Aggregation list, select Sum.

e. Use the Filter Number of Results section to limit the number of items shown by the report.

f. Use the Group Results By list to set how individual items are grouped in the report.

g. Click Preview Resource, and then click OK.

h. Click Submit.

7. Add the report to your Orion reports:
   a. Define the report layout:
      i. Enter a Title and Subtitle. You can also change the logo, page layout, and footer.
      ii. Under Content, in the From list, select Last 24 Hours.
      iii. Click Next.

b. Check the preview, and click Next.

c. Define the report properties, and click Next.

d. If you want to create the report regularly, schedule the report, and click Next.

e. Review the summary, and click Submit.

Create a custom report for EF type of service

SolarWinds NPM 10.7 or newer is required.

1. Click Reports > All Reports.

2. Click Manage Reports.


4. Click Custom Table, and then click Select and Continue.
5. Define what objects should be in the report. We want to report on traffic using a specified type of service, so we need to specify that we are interested in NetFlow History objects whose type of service is EF.
   b. Click Advanced Selector.
   d. Click Select Field.
   e. On the Add Column menu, under Available Columns, click NetFlow Type of Service.
   f. Under Database Column Name, click ToS Name.
   g. Click Add Column.
   h. On the Add Content menu, go to the ToS Name property list and select Is Equal To.
   i. Type EF in the last field on that line.
   j. Enter a Selection Name.
   k. Click Add to Layout.

6. Define what columns you want to see in the report, how the items should be sorted, how many items you want to see, how the items should be grouped, or details for individual columns:
   a. Click Add Column.
   b. Add appropriate columns.
      - Add the Node Name column:
        i. Select Node in the Orion Object list.
        ii. Under Available Columns, click Node.
        iii. Under Database Column Name, select Node Name.
      - Add the Ingress Interface Name column:
        i. Select Interface in the Orion Object list.
        ii. Under Available Columns, click Ingress Interface.
        iii. Under Database Column Name, select Interface Name.
      - Add the ToS Name column:
        i. Select NetFlow Flow History in the Orion Object list.
        ii. Under Available Columns, click NetFlow Type of Service.
        iii. Under Database Column Name, select ToS Name.
      - Add the Bytes column:
        i. Select NetFlow Flow History in the Orion Object list.
        iii. Under Database Column Name, select Bytes.
   c. Click Add Column.
c. Define table sorting.
   i. Under Sort Results By, select Bytes - NetFlow Flow History.
   ii. Define the sorting direction as Descending.

d. Specify units and aggregation for bytes.
   i. Under the Bytes column, click Advanced.
   ii. In the Add Display Settings list, select Data Unit.
   iii. In the Units of Measurements list, select Bytes (1000). This defines the units shown on the report.
   iv. In the Units in My Database list, select B.
   v. In the Data Aggregation list, select Sum.

e. Use the Filter Number of Results section to limit the number of items shown by the report.

f. Use the Group Results By list to set how individual items are grouped in the report.

g. Click Preview Resource, and then click OK.

h. Click Submit.

7. Add the report to your Orion reports:
   a. Define the report layout:
      i. Enter a Title and Subtitle. You can also change the logo, page layout, and footer.
      ii. Under Content, in the From list, select Last 24 Hours.
      iii. Click Next.
   b. Check the preview, and click Next.
   c. Define the report properties, and click Next.
   d. If you want to create the report regularly, schedule the report, and click Next.
   e. Review the summary, and click Submit.

Customize a report to filter multicast data and group UDP data

1. Create an IP Address Group for multicast traffic:
   a. Click Settings > All Settings.
   b. Under Product Specific Settings, click NTA Settings.
   c. Under IP Address Groups, click Manage IP Address Groups.
   d. Click Add New Group.
   e. Add a Description.
   f. Select IP Range, and type 224.0.0.0 and 239.255.255.255.

   If you want to display the new IP address group in the Top XX Address Group resource, select
Enable Display in Top XX Address Group Resource.

g. Click OK.
h. Click Submit.

Click Reports > All Reports.
Click Manage Reports.

2. Find and edit the report you want to modify:
   a. In the Group By list, select Report Category, and then select Historical NetFlow Reports in the list below.
   b. Select the Top 50 Endpoints box in the main reports list, and click Duplicate & Edit.

3. Adjust the object you want to report on. Add conditions stipulating that you are only interested in the multicast traffic through the UDP port.
   a. Click Edit next to the For list.
   b. On the Add Content menu, click Advanced Selector.
   c. Add the condition defining the port for the monitored traffic.
      i. Click Add Condition to display a new branch below the Where list.
      ii. Click Select Field.
      iii. On the Add Column menu, under Database Column Name, select Port Number, and click Add Column.
      iv. Type the port number in the last field next to Port Number.
   d. Add the condition defining that you are only interested in the traffic via IP addresses in the multicast IP address group.
      i. Click , and then Add Simple Condition.
      ii. Click Select Field.
      iii. In the Available Columns list, click NetFlow IP Address Group.
      iv. Under Database Column Name, select IP Address Group Name, and then click Add Column.
      v. Type the name of the multicast IP address group, which you created in step 1, in the last field next to IP Address Group Name.
   e. Click Add to Layout.
4. Edit the output table for the report:
   a. Under Content, click Edit Table.
   b. Add the Protocol column.
      i. Click ▶ to add a new column.
      iii. Under Database Column Name, select Protocol Name.
      iv. Click Add Column.
   c. Add interface-relevant columns that you want to see in the report.
      i. Click ▶ to add a new column.
      ii. In the Orion Object list, select Interface.
      iii. Select Egress Interface if you are interested in traffic leaving the node via interfaces, or
         Ingress Interface if you are interested in traffic coming into the node.
      iv. Under Database Column Name, select appropriate columns, and then click Add Column.
   d. Define how you want to sort results. Select the column according to which you want to sort
      results in the Sort By list, and the direction.
   e. Under Group Results By, select Protocol Name - NetFlow Protocol.
   f. Click Submit.
5. Complete the Edit Report wizard.
6. On the Summary tab, click Submit.

Customize a historical NetFlow report to include location

1. Click Reports > All Reports.
2. Click Manage Reports.
3. In the Group By list, select Report Category, and then select Historical NetFlow Reports in the list
   below.
4. Select a report, and click Duplicate & Edit.
5. Under Content, click Edit Table.
6. Click ▶ to add a new column.
7. On the Add Column menu, in the Orion Object list, select Node.
8. Under Database Column Name, select Location.
9. Click Add Column.
10. Click Submit.
12. On the Summary tab, click Submit.
Alerts

An alert is an automated notification that a network event has occurred, such as a server becoming unresponsive. The network event that triggers an alert is determined by conditions you set up when you configure your alert. You can schedule alerts to monitor your network during a specific time period, and create alerts that notify different people based on how long the alert has been triggered. Available notifications include for example sending a web page in an email.

The types of events for which you can create alerts vary, depending on the Orion Platform products you have installed. For example, you can create an alert to notify you if a node in a specific location goes down or if the network response time is too slow when you have NPM. See NetFlow-specific predefined alerts for a list of out-of-the box alerts delivered with NTA.

For more information about alerts, see Use alerts to monitor your environment in the NPM Administrator Guide.

NetFlow-specific predefined alerts

Alerts must be enabled to trigger when the defined condition occurs. Not all out-of-the box alerts are enabled by default.

- You need Alert Management Rights to enable, create, edit, delete alerts, or to view a list of available alerts.

Where can I find what NTA-specific alerts are enabled?

1. Click Alerts & Activity > Alerts, and click Manage Alerts in the upper right.
2. In the Alert Manager, filter the alerts to display NTA-only items. Type netflow or CBQoS into the search box.
3. Make sure the alerts are on.

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:

- When the percent utilization of an interface rises above the specified value, the alert writes the bandwidth utilization event to the SolarWinds event log. When the utilization drops back below a specified value, the alert writes another event to the log.
- Initiate a web capture of the most current top talker information and email the information to the configured recipient.

CBQoS alerts

The CBQoS alerts can help you confirm that the CBQoS policies applied to traffic flowing through your devices are producing the intended results. For example, the default Drops alert can notify you when packets dropped as a result of a policy exceed the 1GB threshold. Specify a policy and set up alert thresholds to get an early warning about traffic processing issues and intervene to better shape network traffic.

CBQoS out-of-the-box alerts are not enabled by default because you need to specify the policy and class path to complete the trigger definition.

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.
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.

Miscellaneous

Flow storage backup failed

This alert emails you when the NTA Flow Storage Database backup fails.

Configure NTA-specific alerts

You can use the out-of-the-box alerts as templates for customized alerts. Configure an alert for SolarWinds NTA based on a predefined top talker or CBQoS alert.

For out-of-the box alerts, you have limited edit options. You can enable or disable the alerts, add trigger and reset actions, or adjust Time of Day settings. To make more substantial changes, such as changing the conditions, select the alert and click Duplicate & Edit.

Configure trigger actions for default top talker alerts

Default top talker alerts notify you when current percent utilization of an interface (receive or transmit side) rises above a specified threshold (75%). The alert writes an entry into the SolarWinds event log and sends a web page to specified recipients.

To make the top talker work, configure credentials used for accessing and sending the Orion Web Console page and specify the email address that will receive the notification.

Default top talker alerts use the default Admin account and no password for sending the Orion web page. When you change the default account credentials, top talker alerts stop working. Provide valid credentials into the trigger action macro.

1. Click Alerts & Activity > Alerts.
2. Click Manage Alerts.
3. Select a top talker alert.
   To find top talker alerts, type top talker into the search box to filter the alerts.
4. Select a Top Talker alert, and click Edit.
5. Go to Trigger Actions.
6. Click Edit for the E-Mail a Web page action.
7. Enter an Email address for receiving the web page. You can specify the sender and a reply address.
8. Expand Message.
9. In the Enter or Paste the Web macro, specify the credentials used for sending the Orion Web Console page. Enter the password into the single brackets after $$Password$$, and replace Admin with the user name.

```sql
${SQL:SELECT REPLACE(REPLACE(Macro, '$$Password$$', 'qwerty123'), '$$User$$', 'test')} FROM NetFlowAlertMacros WHERE ID='OutWebMailInterfaceDetailsLink'}
```

For example, if you use `test` as the user name and `qwerty123` as the password, the macro will look as follows:

```sql
${SQL:SELECT REPLACE(REPLACE(Macro, '$$Password$$', 'qwerty123'), '$$User$$', 'test')} FROM NetFlowAlertMacros WHERE ID='OutWebMailInterfaceDetailsLink'}
```

Tips:

- If you have a DirectLink account, you can use the DirectLink credentials. Make sure the DirectLink rights do not allow the webpage recipient to make any changes in your Orion Platform installation.
- Use User currently logged-in as the Optional Web Server Authentication. The other options are not optimized for NTA.

10. Complete the Edit Alert wizard.

When an interface utilization reaches the specified threshold, the specified recipient will receive an email with the Orion Web Console page. See Emailing a Web Page in the Orion Platform online help for more details.

Change the threshold for Top Talker alerts

1. Click Alerts & Activity > Alerts.
2. Click Manage Alerts.
3. Select a top talker alert.
4. Click Duplicate & Edit to create a copy of the alert and keep the original intact.
5. Adjust the alert properties if necessary. Under Enabled, turn the alert On and select how often the trigger condition should be checked.

6. On Trigger Condition, define the conditions that trigger the alert. Default top talker alerts trigger when the transmitted or received utilization of the interface exceeds 75%.

7. On Reset Condition, define the conditions for resetting the alert. Default top talker alerts are reset when the transmitted or received utilization of the interface drops below 50%. You can adjust this condition or add conditions.

8. On Time of Day, schedule when to run the alert. To run the alert always, select Alert Is Always Enabled, No Schedule Needed.

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

   If there are endpoint-centric resources on the Interface Details page when it is captured for a top talker alert notification, the links to those resources will be non-functional in the email. The information in the alert notification is not customizable.

10. On Reset Actions, define specific tasks to be performed when an alert is no longer active, such as writing to the log that the issue has been acknowledged.

11. Review the Summary, and click Submit.
Configure a CBQoS alert

Specify the policy and class path for default CBQoS alerts. If you only enable a default CBQoS alert without configuring the trigger condition, the alert will never trigger.

1. Click Alerts & Activity > Alerts.
2. Click Manage Alerts.
3. Select a CBQoS alert, and click Duplicate & Edit.
4. Adjust the alert properties if necessary. Under Enabled, turn the alert On and select how often the trigger condition should be evaluated.

![Enabled (On/Off)
ON](image)

**Evaluation Frequency of Alert**
Evaluate the trigger condition every 1 minutes

5. On Trigger Condition, define the conditions that trigger the alert.
   Go to the fourth field in the Policy and Class Path line, press the down key, and select a policy.

![All child conditions must be satisfied (AND)](image)

6. To allow traffic to fluctuate and delay triggering the alert, select Condition must exist for... and adjust the number of seconds for which the condition exists.

![Aggregated data must occur within the last 15 minutes](image)

![Condition must exist for more than 10 minutes](image)

---

**Tips**

- If the class name is unique, select "includes" in the third box for Policy and Class Path, and type a unique part of the class name into the last box.
- To be alerted on all policies (Drops, Pre-Policy, or Post-Policy, based on the selection in the CBQoS Stats Name line) that exceed the specified sum of bytes, delete the Policy and Class Path line from the trigger condition.
- To be alerted on policies on a node, add a simple condition defining the node name. Select Node as the Orion Object in the first field, and Node Name as the Database column. See Define the conditions that must exist to trigger an alert in the Orion Platform online help.
7. On Reset Condition, define the conditions for resetting the alert.

8. On Time of Day, define the days and times when the software actively evaluates the database for trigger conditions.
   To run the alert always, select Alert Is Always Enabled, No Schedule Needed.

9. On Trigger Actions, create actions to execute when the software triggers the alert.
   The default action for all alerts is to write to the SolarWinds event log.

10. On Reset Actions, you can define actions to execute when the software resets the alert.

11. Review the Summary, and click Submit.

**Available alert actions**

Orion Platform products provide a variety of actions to signal an alert condition on your network, such as emailing a web page.

See Available alert actions in the Orion platform online documentation for a list of available actions.
Troubleshooting

In SolarWinds NTA, you can encounter various issues, such as NetFlow issues, chart issues, database connection issues, or CBQoS issues.

NetFlow issues

For troubleshooting NetFlow issues, you can consult the following SolarWinds NTA resources:

- **NetFlow collector services**
  
  This resource informs you whether the collector service is up or down. For more information, see [NetFlow Collector Services](#).

- **NetFlow sources**
  
  This resource lists devices from which SolarWinds 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 SolarWinds NTA. For more information, see [Last 25 Traffic Analysis Events](#).

For more information about troubleshooting NetFlow, see the technical reference [Best Practices for Troubleshooting NetFlow](#).

Chart issues

For more information about resolving chart issues, such as charts displaying duplicate traffic, see [Chart issues](#).

Database connection issues

For more information about troubleshooting the connection to the Orion Database, or to the NTA Flow Storage Database, see [Database connection issues](#).

CBQoS issues

For more information about troubleshooting CBQoS, see [CBQoS issues](#).
NetFlow Collector Services

The NetFlow Collector Services resource provides status information about the servers on which you have installed SolarWinds 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:

<table>
<thead>
<tr>
<th>COLUMN</th>
<th>EXPLANATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status Icon</td>
<td>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.</td>
</tr>
<tr>
<td>Server Name</td>
<td>The network identification of the NetFlow collector.</td>
</tr>
<tr>
<td>Receiver Status</td>
<td>A verbal statement of collector status.</td>
</tr>
<tr>
<td>Collection Port</td>
<td>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.</td>
</tr>
</tbody>
</table>

Edit or add collection ports

You can change the port SolarWinds NTA is listening for flow packets at, or add an additional port on the Edit NetFlow Collector Services page.

1. Click Edit on the NetFlow Collector Services resource.
2. Change the collection port, or add another collection port by separating listed ports with a single comma. For example: 2055, 9995.
3. Click Submit.

Delete collectors

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

If the NetFlow service is still running on the server, deleting the collector in this resource is temporary. In 15 minutes, the collector will be added again 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.
Delete a collector permanently

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

Delete a collector in the NetFlow Collector Services resource

1. Click Delete next to the collector.
2. Click Submit.

For more information about configuring your collectors, see [NetFlow collector services](#) in the SolarWinds NetFlow Traffic Analyzer Administrator Guide.

Troubleshoot collector services

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 the Orion Service Manager.

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 then click Start. 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. Make sure the connection is working, and that the appropriate database server has sufficient CPU and memory available.
5. As a final attempt to reconcile the SolarWinds NetFlow Service, start the Configuration wizard in the 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 collector services

The Edit NetFlow Collector Services page provides status information about the NetFlow collectors that are running NetFlow Traffic Analyzer. The following information about the collectors and the ports on which they are listening for NetFlow data is provided in the table:

**Status Icon**

Displays collector status visually, where a green icon indicates that the collector can actively receive NetFlow data and a red icon indicates that the collector cannot actively receive NetFlow data.

**Server Name**

The network identification of the NetFlow collector.

**Receiver Status**

A verbal statement of the 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. Designate additional collection ports by listing port numbers separated by commas.

Clicking Delete to the right of any listed collector ends traffic analysis on the selected collector.

For more information about configuring collector services, see NetFlow collector services on page 79.

NetFlow Sources

The NetFlow Sources resource provides a list of flow- and CBQoS-enabled nodes and interfaces that are currently monitored by SolarWinds NTA. 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 volume
- For all listed flow-enabled devices, the date and time of the last flow packet received by the SolarWinds NTA collector
- For all listed CBQoS-enabled devices, the date and time of the last CBQoS poll completed by the SolarWinds NTA collector

Device status icons are color-coded as indicated in the following table.

<table>
<thead>
<tr>
<th>ICON COLOR</th>
<th>DEVICE STATUS INDICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>The selected source is either able to actively send flow data or it is currently able to provide CBQoS information.</td>
</tr>
<tr>
<td>Yellow</td>
<td>Device status is unknown, flow data has not been received, or CBQoS information cannot be polled from the selected device. This color may be displayed for interfaces on a Down node, as it is impossible to determine interface status when the parent node is down.</td>
</tr>
<tr>
<td>Red</td>
<td>The selected device is unable to actively provide flow or CBQoS data.</td>
</tr>
</tbody>
</table>
Troubleshoot NetFlow sources

In the NetFlow Sources resource, you can encounter various issues.

**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 [Enable the automatic addition of flow sources](#).
- Flow-enabled nodes and interfaces must be monitored by SolarWinds NPM before they can be recognized in as flow sources in SolarWinds NTA. For more information about adding devices for monitoring by SolarWinds NPM, see [Add flow-enabled devices and interfaces to the Orion database](#).
- Flow-enabled devices must be configured to send flow data to the SolarWinds NPM server on which you have installed SolarWinds NTA. For more information about configuring devices to send flows to SolarWinds 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 SolarWinds NTA server as an administrator, and then open Control Panel > 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 [NetFlow sources and CBQoS polling](#).

**View more details about displayed objects**

Clicking + next to a listed node expands the list of interfaces on the selected parent node.

Clicking a node name opens the NetFlow Node Details view for the selected node.

Clicking an interface name opens the NetFlow Interface Details view for the selected interface.

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 [NetFlow sources and CBQoS polling](#).

1. Click Edit in the Resource header.
2. Edit the Title.
3. Select or clear Show NetFlow Sources and Show CBQoS Sources.
4. Click Submit.

**Troubleshoot Long Flow Errors**

Invalid flow errors recorded in the NetFlow Analyzer may result when a flow duration exceeds the cache timeout values. This condition displays the following event in the Traffic Analyzer Events monitor:
NetFlow Receiver Service [Poller] detected long flow with duration 90s on [link]Node[/link]

To resolve this error, the following lines must appear in the Flow Monitor section of the Configuration file for Flow Records on Cisco devices:

```
cache timeout inact 10
```
```
cache timeout act 5
```

For additional information, see Configuring Devices for Flow Collection in the online help.

Events

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

Access Events

Click Alerts & Activity > Events.

What details do events provide?

- 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 SolarWinds 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.

Filter events and display 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.

If you want to see only unknown traffic events, click NetFlow Settings in any NetFlow view, and Under NetFlow Management click Show Unknown Traffic Events. For more information about unknown traffic, see Resolve unknown NetFlow traffic.

Filter all events

1. Click Alerts & Activity > Events.
2. You can further filter events by:
   a. Network Object or Type of Device
   b. Event Type
      The table below provides event types relevant for SolarWinds NTA events, and the corresponding events.
   c. Time Period
3. If you want to see cleared events, select Show Cleared Events.
4. If desired, edit the Number of Displayed Events.
5. Click Refresh.

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetFlow Receiver Service Started</td>
<td>NetFlow receiver service started</td>
</tr>
<tr>
<td></td>
<td>NetFlow receiver service settings changed</td>
</tr>
<tr>
<td>NetFlow Receiver Service Stopped</td>
<td>NetFlow receiver service stopped</td>
</tr>
<tr>
<td></td>
<td>License limitation</td>
</tr>
<tr>
<td></td>
<td>No valid license</td>
</tr>
<tr>
<td>Unmanaged NetFlow Node</td>
<td>Unmanaged NetFlow node</td>
</tr>
<tr>
<td>Unmonitored NetFlow Interface</td>
<td>Unmonitored interface automatically added</td>
</tr>
<tr>
<td>Automatically Added</td>
<td></td>
</tr>
<tr>
<td>NetFlow Event</td>
<td>NetFlow event: interface index mapping used for a node</td>
</tr>
<tr>
<td></td>
<td>NetFlow event: removing interface index for a node</td>
</tr>
<tr>
<td>Event Type</td>
<td>Events</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>NetFlow database maintenance</td>
<td>Scheduled shrink performed</td>
</tr>
<tr>
<td></td>
<td>Updating data to be used in Top XX aggregated resources</td>
</tr>
<tr>
<td></td>
<td>Windows Firewall is turned on</td>
</tr>
<tr>
<td>Unmanaged NetFlow Interface</td>
<td>Unmanaged NetFlow interface</td>
</tr>
<tr>
<td>Unmonitored NetFlow Interface</td>
<td>Unmonitored NetFlow interface</td>
</tr>
<tr>
<td>Invalid Template</td>
<td>Invalid template</td>
</tr>
<tr>
<td></td>
<td>Invalid IPFIX template</td>
</tr>
<tr>
<td>No Template Received</td>
<td>No template received</td>
</tr>
<tr>
<td>Not Enabled NetFlow Data Export</td>
<td>NetFlow data export not enabled</td>
</tr>
<tr>
<td>Not Primary NPM Node IP Address</td>
<td>Not primary NPM node IP address</td>
</tr>
<tr>
<td>Notification Reset</td>
<td>Notification event status reset</td>
</tr>
<tr>
<td></td>
<td>Enough space available On NTA Flow Storage Database</td>
</tr>
<tr>
<td>NetFlow Licensing</td>
<td>NetFlow licensing</td>
</tr>
<tr>
<td>Informational</td>
<td>Unable to start listening on port</td>
</tr>
<tr>
<td></td>
<td>Port is free listening</td>
</tr>
<tr>
<td></td>
<td>Running out of space NTA Flow Storage Database</td>
</tr>
<tr>
<td>NetFlow service time difference</td>
<td>NetFlow time difference warningN</td>
</tr>
<tr>
<td>warning</td>
<td>NetFlow time difference warning ended</td>
</tr>
<tr>
<td>NetFlow service time difference</td>
<td>NetFlow time difference error</td>
</tr>
<tr>
<td>error</td>
<td>NetFlow Critical</td>
</tr>
<tr>
<td></td>
<td>No space left on NTA Flow Storage Database</td>
</tr>
</tbody>
</table>

**Clear 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.

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NTA Settings.
4. Click Clear Notifications. This will clear events from this view and from the Events view. However, the Last 25 Traffic Analyzer Events resources still show the last 25 items and include the following event:

   | Notification Event Status Reset
   | "Resetting unknown traffic notifications events."

5. Click Refresh Events. Unresolved events will appear in the Last 200 Unknown Events view again. It might take a few minutes until unresolved events return to the list. Unresolved events return to the list if you refresh the page.

Display resolved events that were cleared

1. Click Alerts & Activity > Events.
2. Define what events you want to see. For more details, see Filter events and display historical events.
3. Select Show Cleared Events.
4. Click Refresh.

Error: NetFlow service inaccessible

This error informs you that the SolarWinds NetFlow Service is not running.

This error might be triggered by various causes, such as a licensing error. You can usually resolve the issue by restarting the NetFlow Service.

Make sure your SolarWinds NTA license is valid and has been activated. See Web-based License Manager in the NPM online help.

Start the NetFlow service

1. Start the Orion Service Manager in the SolarWinds Orion program folder.
2. Click Start Everything to start all stopped services.

Error: No template received

If you are receiving NetFlow v9 flows from a device without an appropriate template for longer than 15 minutes, SolarWinds NTA displays this error: "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."

Resolve the issue

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

For more information about appropriate commands, see documentation of the device.
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, SolarWinds NTA ignores the packets.

Requirements

- The template must include all mandatory fields.
- Where multiple elements are in a group, at least one of them must be included.
- Optional fields are processed into flows if present. If not present, a default value is used.

Mandatory fields for the flow template schema

Mandatory fields are required. If a mandatory field, or at least one field from a group, is not included SolarWinds NTA cannot store flows.

<table>
<thead>
<tr>
<th>Field Type</th>
<th>Field Type Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>4</td>
<td>Layer 4 protocol</td>
</tr>
<tr>
<td>SourceAddress</td>
<td>8</td>
<td>Source IP address</td>
</tr>
<tr>
<td>DestAddress</td>
<td>12</td>
<td>Destination IP address</td>
</tr>
</tbody>
</table>

**Interfaces Group**

At least one of the following fields must be included in the template:

<table>
<thead>
<tr>
<th>Field Type</th>
<th>Field Type Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InterfaceRx</td>
<td>10</td>
<td>SNMP ingress interface index</td>
</tr>
<tr>
<td>InterfaceTx</td>
<td>14</td>
<td>SNMP egress interface index</td>
</tr>
</tbody>
</table>

**Bytes Group**

At least one of the following fields must be included in the template:

<table>
<thead>
<tr>
<th>Field Type</th>
<th>Field Type Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bytes</td>
<td>1</td>
<td>Delta bytes</td>
</tr>
<tr>
<td>Bytes</td>
<td>85</td>
<td>Total bytes</td>
</tr>
<tr>
<td>OutBytes</td>
<td>23</td>
<td>Out bytes</td>
</tr>
<tr>
<td>InitiatorOctets</td>
<td>231</td>
<td>Initiator bytes</td>
</tr>
<tr>
<td>ResponderOctets</td>
<td>232</td>
<td>Responder bytes</td>
</tr>
</tbody>
</table>
Optional fields for the flow template schema

If the following fields are not included in the template, a default value will be stored. Appropriate resources will thus show *No Data.*

<table>
<thead>
<tr>
<th><strong>FIELD TYPE</strong></th>
<th><strong>FIELD TYPE NUMBER</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>ToS</td>
<td>5</td>
<td>Type of service</td>
</tr>
<tr>
<td>SourceAS</td>
<td>16</td>
<td>Source BGP autonomous system number</td>
</tr>
<tr>
<td>DestAS</td>
<td>17</td>
<td>Destination BGP autonomous system number</td>
</tr>
<tr>
<td>PeerSrcAS</td>
<td>129</td>
<td>Peer source autonomous system number</td>
</tr>
<tr>
<td>PeerDstAS</td>
<td>128</td>
<td>Peer destination autonomous system number</td>
</tr>
<tr>
<td>ApplicationID</td>
<td>95</td>
<td>ID of application detected in NBAR2 flow</td>
</tr>
</tbody>
</table>

**Source Port Group**

At least one of the following fields should be included in the template:

<table>
<thead>
<tr>
<th><strong>FIELD TYPE</strong></th>
<th><strong>FIELD TYPE NUMBER</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>SourcePort</td>
<td>7</td>
<td>Source TCP/UDP port</td>
</tr>
<tr>
<td>UdpSrcPort</td>
<td>180</td>
<td>Source UDP port</td>
</tr>
<tr>
<td>TcpSrcPort</td>
<td>182</td>
<td>Source TPC port</td>
</tr>
</tbody>
</table>

**Destination Port Group**

At least one of the following fields should be included in the template:

<table>
<thead>
<tr>
<th><strong>FIELD TYPE</strong></th>
<th><strong>FIELD TYPE NUMBER</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>DestPort</td>
<td>11</td>
<td>Destination TCP/UDP port</td>
</tr>
<tr>
<td>UdpDstPort</td>
<td>181</td>
<td>Destination UDP port</td>
</tr>
<tr>
<td>TcpDstPort</td>
<td>183</td>
<td>Destination TPC port</td>
</tr>
</tbody>
</table>

**Packets Group**

At least one of the following fields should be included in the template. If no field is included, resources will show 0 in the packets column.

<table>
<thead>
<tr>
<th><strong>FIELD TYPE</strong></th>
<th><strong>FIELD TYPE NUMBER</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets</td>
<td>2</td>
<td>Delta packets</td>
</tr>
<tr>
<td>Packets</td>
<td>86</td>
<td>Total packets</td>
</tr>
<tr>
<td>OutPackets</td>
<td>24</td>
<td>Out packets</td>
</tr>
<tr>
<td>Field Type</td>
<td>Field Type Number</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>InitiatorPackets</td>
<td>298</td>
<td>Total packets in a flow from the device that triggered the session and remains the same for the life of the session</td>
</tr>
<tr>
<td>ResponderPackets</td>
<td>299</td>
<td>Total packets from the device which replies to the initiator</td>
</tr>
</tbody>
</table>

**Long Flow Detection**

At least one of the following field pairs should be included in the template for long-flow detection. For example, if including LastSwitched must also include FirstSwitched.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LastSwitched</td>
<td>21</td>
<td>System uptime at which the last packet of this flow was switched</td>
</tr>
<tr>
<td>FirstSwitched</td>
<td>22</td>
<td>System uptime at which the first packet of this flow was switched</td>
</tr>
<tr>
<td>FlowStartSeconds</td>
<td>150</td>
<td>Time in seconds that the flow started</td>
</tr>
<tr>
<td>FlowEndSeconds</td>
<td>151</td>
<td>Time in seconds that the flow ended</td>
</tr>
<tr>
<td>FlowStartMilliseconds</td>
<td>152</td>
<td>Time in milliseconds that the flow started</td>
</tr>
<tr>
<td>FlowEndMilliseconds</td>
<td>153</td>
<td>Time in milliseconds that the flow ended</td>
</tr>
<tr>
<td>FlowStartMicroseconds</td>
<td>154</td>
<td>Time in microseconds that the flow started</td>
</tr>
<tr>
<td>FlowEndMicroseconds</td>
<td>155</td>
<td>Time in microseconds that the flow ended</td>
</tr>
<tr>
<td>FlowStartNanoseconds</td>
<td>156</td>
<td>Time in nanoseconds that the flow started</td>
</tr>
<tr>
<td>FlowEndNanoseconds</td>
<td>157</td>
<td>Time in nanoseconds that the flow ended</td>
</tr>
<tr>
<td>FlowStartDeltaMicroseconds</td>
<td>158</td>
<td>Sets the start delta of the flow</td>
</tr>
<tr>
<td>FlowEndDeltaMicroseconds</td>
<td>159</td>
<td>Sets the end delta of the flow</td>
</tr>
<tr>
<td>FlowDurationMilliseconds</td>
<td>161</td>
<td>Elapsed time in milliseconds of the flow</td>
</tr>
<tr>
<td>FlowDurationMicroseconds</td>
<td>162</td>
<td>Elapsed time in microseconds of the flow</td>
</tr>
</tbody>
</table>

**Cisco WLC Flows**

The following fields must be included for Cisco Wireless devices.
<table>
<thead>
<tr>
<th>FIELD TYPE</th>
<th>FIELD TYPE NUMBER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bytes</td>
<td>1</td>
<td>Total bytes</td>
</tr>
<tr>
<td>Packets</td>
<td>2</td>
<td>Total packets</td>
</tr>
<tr>
<td>FlowDirection</td>
<td>61</td>
<td>Direction of the flow defined as Ingress or egress.</td>
</tr>
<tr>
<td>ApplicationID</td>
<td>95</td>
<td>ID of application detected in flow</td>
</tr>
<tr>
<td>PostIPDiffServCodePoint</td>
<td>98</td>
<td>The definition of this Information Element is identical to 'ipDiffServCodePoint', except that it reports a potentially modified value caused by a middlebox function after the packet passed the Observation Point.</td>
</tr>
<tr>
<td>WlanSSID</td>
<td>147</td>
<td>Service Set Identifier or name of the WLAN the wireless device is connected to</td>
</tr>
<tr>
<td>IPDiffServCodePoint</td>
<td>195</td>
<td>Value of a Differentiated Services Code Point (DSCP) encoded in the Differentiated Services field. Differentiated Services field is the most significant six bits of the IPv4 TOS FIELD or the IPv6 Traffic Class field. The value may range from 0 to 63 for this Information Element that encodes only the 6 bits of the Differentiated Services field.</td>
</tr>
<tr>
<td>WirelessStationMacAddress</td>
<td>365</td>
<td>MAC address of a wireless device</td>
</tr>
<tr>
<td>WirelessStationAddressIPv4</td>
<td>366</td>
<td>IPv4 address of a wireless device</td>
</tr>
<tr>
<td>WirelessAPMacAddress</td>
<td>367</td>
<td>MAC address of a wireless access point</td>
</tr>
<tr>
<td>Cisco ASA devices</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The following fields must be included for processing flows from Cisco ASA devices.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FlowID</td>
<td>148</td>
<td>An identifier of a flow that is unique within an observation domain.</td>
</tr>
<tr>
<td>FirewallEvent</td>
<td>233</td>
<td>Indicates a firewall event.</td>
</tr>
</tbody>
</table>
Notes

- If SolarWinds states that SolarWinds NTA supports flow monitoring for a device, at least one of the templates that 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 SolarWinds NTA, SolarWinds has determined that at least one of the templates the device is capable of exporting will satisfy the SolarWinds NTA requirements. For more information, search for NetFlow version 9 flow record format on www.cisco.com.
- 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.

Events list

The following sections list events you can encounter in SolarWinds 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

SolarWinds 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 the SolarWinds Orion > Advanced Features program folder.
2. Check the status of the SolarWinds NetFlow Service.
3. If it is stopped, select it, and then click Start.

⚠️ License limitation

SolarWinds NTA informs you that your SolarWinds NTA license does not match your SolarWinds NPM license, and SolarWinds NTA thus cannot monitor your flow traffic.
"License limitation doesn't fit Orion license!"

To resolve this event, make sure your SolarWinds NTA license matches your SolarWinds NPM license. Both NPM and NTA must be at the same license level. For more information, see SolarWinds NTA licensing.
No valid license

SolarWinds NTA informs you that your 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 SolarWinds 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. SolarWinds 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 the following options:

- Move your NTA Flow Storage Database to a larger disk. For more information, see Move the NTA Flow Storage Database.
- Set a lower retention period for saving your flow data. For more information, see NTA Flow Storage Database maintenance. The default retention period is set to 30 days. Consider the size of your NTA Flow Storage Database disk and the number of flows you need to collect. If you need help with calculating the retention period suitable for your environment, contact SolarWinds support.
- Make some space on your disk by deleting old or unwanted files.
- If you are using virtual machines, allocate more space to the machine hosting your NTA Flow Storage Database.

Invalid template

SolarWinds 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."

Resolve the issue

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

Invalid IPFIX template

SolarWinds 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. "

208
Resolve the issue

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

⚠️ No template received

SolarWinds 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."

Resolve the issue

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

⚠️ NetFlow data export not enabled

SolarWinds NTA is receiving NetFlow traffic from a wrong interface (restricted or unsupported)
"NetFlow data export on device x.x.x.x is not enabled. If you cannot see NetFlow data from the device in SolarWinds NTA, make sure the device is configured to export NetFlow. » Learn more."

The event is generated when both indexes are 0. This can happen in two cases:

- Incorrectly configured device. For more information about configuring the device, see Set up network devices to export NetFlow data.
- If data from the node are visible in SolarWinds NTA, it is safe to ignore this event. In this case, this event only makes you aware of internal node configuration.

⚠️ NetFlow time difference error

This event informs you that the time difference between your servers (SolarWinds Orion database server, NTA Flow Storage Database, and the SolarWinds 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 (SolarWinds Orion database, SolarWinds NTA polling engine(s), and NTA Flow Storage Database server).
Cannot connect to NTA Flow Storage Database

This event informs you that NTA Flow Storage Database is currently unavailable. "Cannot connect to NTA Flow Storage Database. SolarWinds NTA cannot save any flows now."

To resolve the issue, make sure that the server is running, port 17777 is open, and no firewall is blocking the connection.

Unmanaged NetFlow node

This event informs the user that SolarWinds NTA is receiving NetFlow traffic from a node which is not managed in SolarWinds 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 SolarWinds NPM. For more information, see Adding Devices for Monitoring in the Web Console in the SolarWinds Network Performance Monitor Administrator Guide.

Unmanaged NetFlow interface

This event informs you that SolarWinds NTA is receiving traffic from an interface which is not managed in SolarWinds NPM. However, the corresponding node is managed in SolarWinds NPM. Click Add this interface or Edit this interface to add the object to SolarWinds 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 SolarWinds NPM for monitoring. For more information, see Adding Devices for Monitoring in the Web Console in the SolarWinds Network Performance Monitor Administrator Guide.

Unmonitored NetFlow interface

SolarWinds NTA informs you that it is receiving flow traffic from an interface, which is managed in SolarWinds NPM, but not monitored in SolarWinds NTA. This happens if the Enable Automatic Addition of NetFlow Sources in SolarWinds 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:
1. Click Monitor NetFlow Source and enable monitoring for the interface. For more details, see Manually add flow sources and CBQoS-enabled devices.

2. Click Automatic Addition of NetFlow Sources and make sure the Enable Automatic Addition of NetFlow Sources option is selected. For more information, see Enable flow monitoring from unmanaged interfaces.

⚠️ 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 Enable 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 NTA Flow Storage Database maintenance.

⚠️ Unmonitored interface automatically added

SolarWinds NTA informs you that an unmonitored interface has been added into NetFlow sources automatically. This happens if you enabled the Enable Automatic Addition of NetFlow Sources option in the NTA Settings. For more information, see Enable 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 SolarWinds 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:

- SolarWinds Orion database
- SolarWinds NTA polling engine(s)
- NTA Flow Storage Database server

⚠️ NetFlow time difference warning ended

This event informs you that the time difference between the database server and SolarWinds 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

SolarWinds NTA informs you that the NetFlow 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

SolarWinds 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

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

SolarWinds 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

SolarWinds 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 SolarWinds Orion database maintenance.

Scheduled shrink performed

SolarWinds NTA informs you that the SolarWinds Orion database has been compressed. Scheduled shrink performed. DB size before shrink xMB, DB size after shrink xMB, released space xMB. For more information, see SolarWinds Orion database maintenance.

Updating data to be used in Top XX aggregated resources

SolarWinds 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]. This event only occurs in SolarWinds NTA 4.0 using SQL for storing flows and in older SolarWinds NTA versions.

Adjust data aggregation settings

Aggregating NetFlow data in memory significantly reduces the I/O demands that SolarWinds 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, SolarWinds NPM would make big I/O demands on the Orion database. This would impact performance of both SolarWinds NTA and SolarWinds NPM.

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

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

By aggregating data before writing it to the SolarWinds Orion database, SolarWinds NTA 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 NetFlow Settings:
   a. Click My Dashboards > NetFlow > NTA Summary.
   b. Click NetFlow Settings in the top right corner.
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 SolarWinds NTA should save aggregated NetFlow data in cache.
3. Click Save.

Optimize 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.

Top XX Applications

This resource provides a view of the top XX applications responsible for monitored traffic on your network, ranked in order of traffic volume.

When placed on the Node Details or Interface Details view, this resource provides a view of the applications responsible for the most traffic passing through the viewed node or interface over the selected period of time.
This resource shows only applications whose monitoring has been enabled on the Manage Applications and Service Ports view. Data for ports and applications whose monitoring is not enabled there are collected, aggregated, and shown in the Top XX Applications resource as Unmonitored Traffic. For more information about monitored ports and applications, see Configuring Monitored Ports and Applications.

If you are seeing no data in the Top XX Applications view, make sure you are receiving data for the flow type selected in the top right of the Top Applications panel. If monitoring advanced applications for which you are not seeing a name identified for the application, see NBAR2 Advanced Applications for an explanation of how these applications are classified in NTA.

View more details about displayed applications

- Click a listed application to open the NetFlow Applications Summary view that presents statistics for the selected application.
- Click + to expand a listed application and display the list of nodes and their respective interfaces over which the selected application traffic is currently flowing.
- Click a node or interface to display the NetFlow Application detail view showing statistics for the selected application traffic traversing through the appropriate node or interface.

View unmonitored traffic

If there are applications whose monitoring is not enabled in the Manage Applications and Service Ports page, the Top XX Applications resource on a summary view displays the Unmonitored Traffic item. This item aggregates traffic coming from ports or applications whose monitoring is not enabled at the moment.

1. Click the Unmonitored Traffic item to go the NetFlow Applications Summary view filtered by unmonitored traffic.
2. Consult the Top XX Applications resource. The resource will list unmonitored applications, and allow you to monitor appropriate ports.

Enable monitoring of unmonitored ports

If you are viewing the Top XX Applications resource on an Unmonitored Traffic view, you can enable monitoring of unmonitored ports:

1. In the list of unmonitored applications, click Monitor Port to enable monitoring of the port.
2. On the Monitor Application window, select the port(s) to monitor.
3. Select the Source and Destination IP Address and the protocol to monitor.
4. Enter a Description, and then click Add Application to enable monitoring.
   You can also enable monitoring for these applications and ports on the Manage Applications and Service Ports page. For more details, see Configuring Monitored Ports and Applications.

Top XX Applications (Endpoint Centric)

You can customize an endpoint-centric version of this resource and place it on the NetFlow Node Details or Interface Details view.
The endpoint-centric Top XX Applications resource provides a ranked list of applications responsible for traffic passing through the specified node or interface.

For more information about adding endpoint-centric resources, see Add endpoint-centric resources.

Table legend

The table below the chart provides the following information:

<table>
<thead>
<tr>
<th>COLUMN TITLE</th>
<th>CONTENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>The application name with its assigned port number in parentheses.</td>
</tr>
<tr>
<td>Ingress Bytes,</td>
<td>Displays the amount of data (in bytes and packets) flowing to the selected</td>
</tr>
<tr>
<td>Egress Bytes</td>
<td>application through the viewed node or interface.</td>
</tr>
<tr>
<td>Ingress Packets,</td>
<td>The columns displayed depend on the flow direction set in the top left</td>
</tr>
<tr>
<td>Egress Packets</td>
<td>corner of the view (either only Ingress Bytes, or only Egress Bytes, or</td>
</tr>
<tr>
<td></td>
<td>both columns).</td>
</tr>
<tr>
<td>Percent (Utilization)</td>
<td>Displays the percentage of all traffic through the viewed object</td>
</tr>
<tr>
<td></td>
<td>attributed to use of the listed application.</td>
</tr>
<tr>
<td></td>
<td>The first value describes the percentage of the appropriate item based on</td>
</tr>
<tr>
<td></td>
<td>items shown by the chart. Individual items in the legend add up 100%.</td>
</tr>
<tr>
<td></td>
<td>This percentage can be absolute or relative. For more information, see</td>
</tr>
<tr>
<td></td>
<td>Percentage type for Top XX lists.</td>
</tr>
<tr>
<td></td>
<td>A value in parentheses is available only for interfaces. It describes how</td>
</tr>
<tr>
<td></td>
<td>the appropriate item utilizes the interface bandwidth in percentage.</td>
</tr>
<tr>
<td></td>
<td>If the utilization is approximately twice as high as it should be, for</td>
</tr>
<tr>
<td></td>
<td>example 150% instead of 75%, it might be caused by flow duplication. For</td>
</tr>
<tr>
<td></td>
<td>more information, see Resolve duplicate flows.</td>
</tr>
</tbody>
</table>

Edit the resource

If you are logged in using a User ID with administrative privileges, you can change the way this resource is displayed for all users:

1. Click Edit to load the Customize/Edit Resource page.
2. Make changes.
3. Click Submit.

Edit time and flow direction for the view

You can also change the time period and flows direction shown by all resources in the view:
1. Directly below the view name, click next to the appropriate setting and define the appropriate settings.

2. Change the Relative Time Period, by default set to 1 hour prior to the current time, or specify a specific time period.

The time and flow direction settings are limited to the current session only. After you leave the view, your changes will be lost and default settings are re-applied.

Windows Firewall is turned on

SolarWinds NTA informs you that the NetFlow 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 the SolarWinds Orion > Configuration and Auto-Discovery program folder.
2. Select Services and complete the wizard. For more information, see Complete the Configuration wizard.

You can also add an exception to your firewall settings.

NetFlow licensing

SolarWinds NTA informs you that you are running an evaluation version, 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. 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.

Unable to start listening on port

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

Unable to start listening on port x. Waiting until the port is free.
To resolve the issue:

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

Port is free listening

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

Notification event status reset

SolarWinds NTA informs you that you have reset the Last 200 Events view by clicking Clear Notification.
"Resetting unknown traffic notifications events."

For more information about seeing cleared events, see Filter events and display 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.

Connection to NTA Flow Storage Database has been restored

This event is triggered when the connection to NTA Flow Storage Database is restored.

Unmanageable interface speed

You must enter the speed for unmanageable interfaces. Unlike managed interfaces that SolarWinds NPM recognizes, SolarWinds NPM cannot get this information from unmanageable interfaces which it does not recognize. The documentation of your device or your Internet service provider can give more information on determining the speed of an unmanageable interface.

SolarWinds NTA uses the unmanaged interface speed to determine the percentage of resource utilization. Entering an accurate interface speed ensures the correct display of SolarWinds NTA resources. With this information, you can determine the most efficient use of resources.
Resolve unknown NetFlow traffic

If your devices export flows to the SolarWinds NTA receiver, but are not managed in SolarWinds NPM, or are not configured for monitoring in SolarWinds NTA, SolarWinds NTA cannot process the exported information. SolarWinds NTA informs you that it is receiving unknown traffic by displaying a message in the yellow information banner at the top of your SolarWinds 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 and 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 SolarWinds NPM. The devices export flows, but SolarWinds NTA cannot access the necessary data stored in the Orion SQL Database. You need to add these nodes and interfaces to SolarWinds NPM first. For more information, see Add flow-enabled devices and interfaces to the Orion database.

Traffic from unmonitored interfaces

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

Traffic from unmanageable interfaces

Unmanageable interfaces cannot be monitored using SNMP. However, SolarWinds NTA can receive traffic from these interfaces. SolarWinds NPM does not poll data for these nodes via SNMP, the nodes are only registered there and flows can be processed by SolarWinds NTA. However, to monitor this data in SolarWinds NTA, you must add the interface for monitoring to SolarWinds NTA, and provide the interface speed. For more information, see Enable flow monitoring from unmanageable interfaces.

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, which is 2055 by default.
Resolve unknown traffic events

1. Click My Dashboards > NetFlow > NTA Summary.
2. Check the yellow banner area below the tool bar.
3. If there are unknown traffic events, click Show Unknown Traffic Events in the banner. If you cannot see the banner, click NetFlow Settings, and then click Show Unknown Traffic Events under NetFlow Management.
4. The Last 200 Unknown Traffic Events view lists the last 200 events related to SolarWinds NTA, including those in which flow traffic was received but was not associated with a NetFlow source.
5. Resolve individual events.

Test whether the events were resolved

2. Click Refresh Events. New events are added to the list, and unknown traffic events return to the list if they have not been resolved.
3. You can also test resolving unknown traffic events by clicking My Dashboards > NetFlow > NTA Summary. You should no longer see a banner 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.

Enable flow monitoring from unmanageable interfaces

When SolarWinds NetFlow Traffic Analyzer receives a data flow from an unmanageable interface, it displays an event in the SolarWinds NTA Events, such as on the following image.

![NetFlow Receiver Service](image)

Though this interface does not support SNMP, you can register it to SolarWinds NPM, and enable the NetFlow Receiver Service to process the flow data it exports to SolarWinds NTA. If the interface is not in SolarWinds NPM, SolarWinds NTA drops the data flow.

Add an unmanageable interface

1. Click Add This Interface in the unmanaged event.
2. On the Add Interface to NPM menu, edit the Interface Name field if desired.
3. Define the Interface Speed:
   a. See the documentation of the device for the correct interface speed.
   b. Select the speed type from the list.
4. Click Submit. The interface is added to SolarWinds NPM and can be viewed on the Node Management page.
Unmanageable interface monitored in SolarWinds NTA

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

- If SolarWinds NTA is configured to automatically add NetFlow sources, it adds the source. An event informs you that the source was automatically added to SolarWinds NTA. You can see the source in the NetFlow Sources view.
- If SolarWinds NTA is not configured to automatically add NetFlow sources, it does not add the source. An event informs you about a flow from an interface not in NetFlow sources. The source is not visible in SolarWinds NTA in the NetFlow Sources view. If you want to monitor this interface, enable monitoring for the interface in SolarWinds NTA. For more information, see NetFlow sources and CBQoS polling.

Unmanageable interfaces do not have information about interface utilization, because SolarWinds NPM does not poll them. SolarWinds NTA cannot show these interfaces in the Top XX NetFlow Sources by % Utilization resource. These interfaces do not trigger NetFlow alerts based on utilization for the same reason.

Set up a NetFlow collection

If you see a network device in your NetFlow Sources and you do not intend to collect NetFlow data from it, you can eliminate unnecessary traffic by turning off the export of data at the device.

1. Configure your network devices to export NetFlow data for each interface for which you want to collect the data. For more information, see Device Configuration Examples.
   For information on enabling NetFlow for Cisco Catalyst switches, see the SolarWinds technical reference Enabling NetFlow and NetFlow Data Export (NDE) on Cisco Catalyst Switches. For information on enabling NetFlow on Cisco ASA devices, see the SolarWinds technical reference Understanding Cisco ASA NetFlow.
   If your network device is of a different vendor, see the documentation of the vendor.
2. Verify that each interface for which you want to collect and view data is actively being monitored in SolarWinds NPM.
   For any interface that you need to add to SolarWinds NPM, see Network Discovery Using the Network Sonar wizard.
   Use a packet capture tool, such as WireShark, on the relevant interface and port to verify that the device is hexporting data as expected.

Chart issues

Below are the most common issues encountered on SolarWinds NTA charts.
Duplicate flows

If your devices are configured to export NetFlow on both ingress and egress interfaces, you might see duplicate traffic in your resources.

Duplicate flows can occur in the following cases:

- You have both ip flow ingress and ip flow egress applied for all interfaces on a device.
- You have set ip flow ingress on some interfaces and ip flow egress on other interfaces.
- On your serial interfaces with subinterfaces, you have NetFlow export enabled on both the physical and logical interfaces.

Resolving Duplicate Flows

- If your device configuration contains both ip flow ingress and ip flow egress commands, make sure NetFlow is enabled only for ingress interfaces.
- If you have NetFlow enabled for both physical and logical subinterfaces, remove the NetFlow export commands from the physical serial interfaces and only have the subinterfaces enabled for the export.

Double rate in Top XX Endpoints and Top XX Domains

The Top XX Endpoints and Top XX Domains resources display double data by design. Each flow has two distinct endpoints. To display statistics for top endpoints, SolarWinds NTA disregards that one endpoint is the source and the other endpoint is the target of flows, and treats both as endpoints only. This effectively doubles the total amount of data displayed by the Top XX Endpoints resource.

Example

Let us take two flows and look at what you see in most resources and in the Top XX Endpoints resource.

Most Resources

<table>
<thead>
<tr>
<th>FLOW</th>
<th>SOURCE IP</th>
<th>DESTINATION IP</th>
<th>PROTOCOL</th>
<th>BYTES TRANSFERRED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow 1</td>
<td>IP1</td>
<td>IP2</td>
<td>TCP</td>
<td>50</td>
</tr>
<tr>
<td>Flow 2</td>
<td>IP2</td>
<td>IP3</td>
<td>TCP</td>
<td>40</td>
</tr>
<tr>
<td>Total bytes transferred:</td>
<td></td>
<td></td>
<td></td>
<td>50+40=90</td>
</tr>
</tbody>
</table>

Top XX Endpoints resource

<table>
<thead>
<tr>
<th>ENDPOINT</th>
<th>BYTES TRANSFERRED</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP1</td>
<td>50</td>
</tr>
<tr>
<td>IP2</td>
<td>50+40=90</td>
</tr>
</tbody>
</table>
### ENDPOINT | Bytes Transferred
--- | ---
IP3 | 40
Total: | 50+90+40=180

**No data**

If your resources show the "no data" message, it can be caused by one of the following:

**No data to be displayed**

There are no data to be displayed for the current time and flow direction settings.

To resolve the issue, check the time settings for both the resource and the view.

**Too long time period selected for the view**

If SolarWinds NTA needs more than one hour to process data that you want to see in the resources, the query times out and the resources show the "no data" message.

To resolve the issue, define a shorter time period for both the view and the resource.

**Devices**

**Unexpected spikes in CBQoS post-policy charts**

If you remove a shaping policy from a class, post-policy charts with the chart type set to % of Class Utilization may display unexpected spikes.

This is normal behavior, because devices affected by the policy change temporarily report huge amounts of data, which is reflected by the post-policy spike.

**Resolve duplicate flows**

If your devices are configured to export NetFlow on both ingress and egress interfaces, you might see duplicate traffic in your resources.

Duplicate flows can occur in the following cases:

- You have both `ip flow ingress` and `ip flow egress` applied for all interfaces on a device.
- You have set `ip flow ingress` on some interfaces and `ip flow egress` on other interfaces.
- On your serial interfaces with subinterfaces, you have NetFlow export enabled on both the physical and logical interfaces.

**Things to check**

- If your device configuration contains both `ip flow ingress` and `ip flow egress` commands, make sure NetFlow is enabled only for ingress interfaces. Go to appropriate devices and make sure the configuration contains only the `ip flow ingress` command.
If you have NetFlow enabled for both physical and logical subinterfaces, remove the NetFlow export commands from the physical serial interfaces and only have the subinterfaces enabled for the export.

**Database connection issues**

SolarWinds NTA uses two databases: the SolarWinds Orion database and the NTA Flow Storage Database.

**Troubleshoot the connection to the SolarWinds Orion database**

When installing NTA Flow Storage Database on a remote computer, you need the connection to the SolarWinds Orion database used by SolarWinds NTA.

If the connection fails, make sure that:

- The user name and password are correct.
- You can access the database server.
- No firewall is blocking the connection.
- Use the appropriate SolarWinds NPM version. For more information, see Upgrade paths and compatibility.
- SolarWinds NPM is configured for Windows Authentication.
- The remote connection option is enabled on the SolarWinds Orion database.

**Troubleshoot the connection to a remote NTA Flow Storage Database**

When installing SolarWinds NTA with a remote NTA Flow Storage Database, you need to successfully test the connection to the remote database.

The connection to NTA Flow Storage Database may be interrupted while monitoring. SolarWinds NTA triggers an appropriate event.

If the connection fails, make sure that:

- The NTA Flow Storage Database server is installed and configured, and check that the SolarWinds NetFlow Storage Service is running.
- The hostname or IP address is correct and you can access it. Use the ping command to test this.
- The software and hardware firewall settings between the NTA Flow Storage Database server and the Orion server are correct. If necessary, turn the firewall off until the installation finishes.
- Port 17777 is open.
- Anti-virus software is not blocking the connection to the NTA Flow Storage Database server.

**Troubleshoot the connection between the two databases**

In SolarWinds NTA 4.1.1 and later, you may see the following events in the Last 10 Traffic Analysis Events resource:
NetFlow Receiver Service [serverName] stopped.
The connection between NTA Flow Storage Database and Orion SQL Database has been lost. NTA cannot save any flows now.

If you are upgrading or using the Configuration wizard, these messages are normal and can be ignored. The service will start and the connection will be restored when you are finished.

If you are not performing a special task, see the troubleshooting tips in the previous sections.

**CBQoS issues**

**Record troubleshooting steps**

Record detailed results as you perform your troubleshooting steps. It will help expedite a resolution if you need to contact SolarWinds Support about your CBQoS issue.

Use packet capture on the relevant interface of the Orion server to verify SNMP communication, on port 161, with relevant device(s).

**CBQoS issues list**

**CBQoS not running on the device**

Use SolarWinds MIB Viewer to check the status of CBQoS on your device.

Support is determined by cbQosConfigIndex="1.3.6.1.4.1.9.9.166.1.5.1.1.2"

If you see any value in your MIB viewer for this OID, then CBQoS data is being successfully pulled.

**SolarWinds services not running**

Make sure all SolarWinds services are running:

1. Start the Orion Service Manager in the SolarWinds Orion program folder.
2. If some SolarWinds services are not running, click Start Everything.

In particular, the SolarWinds Orion Module Engine service enables polling of CBQoS. The SolarWinds NetFlow service takes the data the Orion poller obtains from the device through SNMP and writes it into the NetFlow database table. If this service is not working, polled CBQoS data sits in a queue and eventually gets dropped.
Device configuration examples

The following sections can be used to help you configure your devices to send flow data to SolarWinds NetFlow Traffic Analyzer.

NetFlow device examples

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 and transport udp values must reflect the IP address and port (2055) of your SolarWinds NPM server.

SolarWinds NTA 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

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

Cisco WLC 5700 series

! Create a Record

configure terminal
flow record NTA-record
description record-for-NTA-ipv4flow
match ipv4 tos
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
end

show flow record record-for-NTA-ipv4flow
!copy running-config startup-config
! Create a Flow Exporter

configure terminal
flow exporter NetFlow-to-NTA
description export-to-NTA
destination 10.10.10.10
source gigabitEthernet1/0/1
transport udp 2055
! export protocol can be left on default
!export-protocol netflow-v5
end

show flow exporter NetFlow-to-NTA
!copy running-config startup-config

! Create a Flow Monitor

configure terminal
flow monitor NTA-Monitor
description monitor-for-NTA-ipv4
record NTA-record
exporter NetFlow-to-NTA
cache timeout inactive 10
cache timeout active 5
end

show flow monitor name NTA-Monitor
!copy running-config startup-config! Creating record

sFlow and J-Flow device examples

Brocade (Foundry) sFlow configuration

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

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 SolarWinds 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.

```bash
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 SolarWinds 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.

```bash
This configuration will not show up in the command line interface. If you reset the switch, you will lose the configuration.

setmib sFlowRcvrAddress.1 -o 1414140a
setmib sFlowRcvrPort.1 -i 2055
setmib sFlowRcvrOwner.1 -D sFlowtool sFlowRcvrTimeout.1 -i 100000000
```

1414140a is the IP address of your SolarWinds NPM server in hex format.

2055 is the default port NTA listens on. If you changed the default port, replace 2055 with your port.

Add the following lines for each interface. Replace ‘10’ with the interface number.

```bash
setmib sFlowFsReceiver.11.1.3.6.1.2.1.2.1.1.10.1 -i 1
setmib sFlowFsPacketSamplingRate.11.1.3.6.1.2.1.2.1.1.10.1 -i 512
setmib sFlowFsMaximumHeaderSize.11.1.3.6.1.2.1.2.1.1.10.1 -i 128
setmib sFlowCpReceiver.11.1.3.6.1.2.1.2.1.1.10.1 -i 128
setmib sFlowCpInterval.11.1.3.6.1.2.1.2.1.1.10.1 -i 30
```

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.

Juniper sFlow configuration

You can perform Juniper switch sFlow configuration using the following sample configuration:
Juniper J-Flow configuration

Configure Juniper J-Flow devices using a configuration template such as the following:

```bash
#show interfaces ge-0/0/0
unit 0 {
    family inet {
        sampling {
            input
            output;
        }
        address 1.1.1.1/30;
    }
}
```
Enable NetFlow and NetFlow data export on Cisco Catalyst switches


Unless stated otherwise, this document refers to Cisco Internetwork Operating System (IOS) Releases 12.2 (18)SXD and higher. The contents of this technical reference are adapted from original Cisco documentation. This document is not intended as a substitute or replacement for your original Cisco documentation or the advice of your Cisco technical support representative.

Due to significant differences in the availability of the commands required to enable NetFlow and NetFlow Data Export, SolarWinds does not support the use of Cisco IOS versions older than 12.2(18) SXD.

Requirements to enable NetFlow and NetFlow Data Export

- NetFlow-capable devices
- Cisco Internetwork Operating System (IOS) Release 12.2(18)SXD and higher
- SolarWinds NPM and SolarWinds NTA installed
- SolarWinds NTA supports NetFlow versions 5 and 9

```bash
#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;
            }
        }
    }
}
```
Cisco Catalyst 4500 Series

The following sections provide the procedures required to enable NetFlow and NetFlow export to Orion NetFlow Traffic Analyzer from the Catalyst 4500 Series.

Enable NetFlow to work with SolarWinds NTA

The Catalyst 4500 platform requires a NetFlow Services Card installed to enable NetFlow.

1. Configure your switch for IP routing.
2. Log in to the switch, and then enter global configuration mode.
3. Enter `ip flow ingress infer-fields` to enable NetFlow for IP routing with inferred input/output interfaces and source/destination border gateway protocol (BGP) as information. You must enable the `infer-fields` option to determine any autonomous system information.

Configure the SolarWinds NTA server as a NetFlow destination

1. Log in to the switch and enter global configuration mode.
2. Type `ip flow-export destination {hostname | ip-address} udp-port` to direct exported NetFlow data to SolarWinds NTA, as in this example, where SolarWinds NTA is hosted on TAHost:
   ```
ip flow-export destination TAHost 2055
   ```
   If you need to send data to more than one destination, you can specify up to two different destinations using successive calls of this command.
3. Type `ip flow-export version 5|9 {origin-as | peer-as}` to set the NetFlow version for use with SolarWinds NTA.
   - Select `origin-as` to direct NetFlow to determine the origin BGP autonomous system of both the source and the destination hosts of the flow, as in:
     ```
     ip flow-export version 5|9 origin-as
     ```
   - Select `peer-as` to direct NetFlow to determine the peer BGP autonomous system of both the input and output interfaces of the flow, as in:
     ```
     ip flow-export version 5|9 peer-as
     ```
4. Type `ip flow-export source interface` to specify the interface that provides the source IP address in the IP header of the NDE packet. The default is the NDE output interface.

Display the NetFlow configuration for verification

1. Enter privileged EXEC mode on your switch.
2. Type `show ip flow export` to display statistics and cache contents for your NetFlow configuration.
Catalyst 6500 and 7600 series

The following sections provide the procedures required to enable NetFlow and NetFlow Data Export (NDE) on Catalyst 6500 Series switches and the 7600 Series.

- You must enable NetFlow on every monitored Multilayer Switch Feature Card (MSFC) Layer 3 interface to support NetFlow Data Export from both the Policy Feature Card (PFC) and the MSFC.
- You must enable NDE on the MSFC to support NDE on the PFC.

This information is provided as a guide for enabling NetFlow to work with SolarWinds NTA. Consult your Cisco product documentation for details about configuring NetFlow and Netflow export on Cisco Catalyst 6500 and 7600 Series devices.

Enable NetFlow and NDE on the Multilayer Switch Feature Card (MSFC)

The MSFC maintains a table of NetFlow data representing software-routed data flows through the device. The following procedure for enabling NetFlow and NDE on the MSFC should be performed on every monitored Layer 3 interface.

1. Log in to the device, and enter global configuration mode.
2. Type `interface {vlan vlan_ID} | {type slot/port} | {port-channel port_channel_number}` to select a Layer 3 interface to configure.
   - `type` can be any of the following: `ethernet`, `fastethernet`, `gigabitethernet`, `tengigabitethernet`
   - `type` can also be any of the following, if the device is running Supervisor Engine 2: `ge-wan`, `pos`, `atm`
3. Type `ip flow ingress` to enable NetFlow.
4. Type `exit` to exit interface configuration mode and return to global configuration mode.
5. Type `ip flow-export source {{vlan vlan_ID} | {type slot/port} | {port-channel port_channel_number} | {loopback number}}` to configure the interface used as the source of the NDE packets containing statistics from the MSFC.
6. Repeat this procedure for each additional interface on which you want to enable NetFlow and NDE.
7. Type `end` to exit global configuration mode and return to privileged EXEC mode.
8. Type `ip flow-export source {{vlan vlan_ID} | {type slot/port} | {port-channel port_channel_number} | {loopback number}}` to configure the interface used as the source of the NDE packets containing statistics from the MSFC.

You must select an interface configured with an IP address.
Enable NetFlow and NDE on the Policy Feature Card (PFC)

1. Log in to the device, and enter global configuration mode.
2. Enter `mls netflow` to enable NetFlow on the PFC.
3. Enter `mls nde sender version 5|9` to enable NDE from the PFC and configure the NDE version.
   - SolarWinds NTA accepts data in NetFlow version 5 and version 9 formats.
   - NDE from the PFC uses the source interface configured for the MSFC.

Configure the destination for NDE data streams

Provide the IP address and UDP port number you have or plan to specify when you install SolarWinds NTA. Export redundancy is available with the NetFlow Multiple Export Destinations feature. This feature allows for the designation of multiple destinations for NDE data streams by successively calling the following function for different destinations. Multiple destinations establishes backup for all NDE streams.

1. Log in to the device, and enter global configuration mode.
2. Type `ip flow-export destination ip_address udp_port_number` with the appropriate IP address and UDP port for the installation of SolarWinds NTA. For example:
   - `ip flow-export destination 12.36.43.7 2055`
     - NetFlow Multiple Export Destinations: To configure redundant NDE data streams, you can enter the `ip flow-export destination` command twice and configure a different destination in each command.
     - Configuring two destinations increases the RP CPU utilization, as you are exporting the data records twice.
     - The destination address and UDP port number are saved in NVRAM and are preserved if NDE is disabled and re-enabled or if the device is power cycled.

Set the aging interval for NDE

The aging interval determines the cutoff point at which the device exports current NetFlow data.

1. Log in to the device, and enter global configuration mode.
2. Type `mls aging normal 64` to export data every 64 seconds. The default value is five minutes.
3. Type `mls aging long 64` to export data approximately every two minutes. The default value is 32 minutes.

Display the NDE address and port configuration for verification

1. Enter privileged EXEC mode on your device.
2. Type `show mls nde` to display the NDE configuration.
3. Type `show ip flow export` to display the NDE source interface configuration.