

NetFlow Monitoring Foundation Package

A Standard Content Foundation Package
for ESM v5.0 SP2

Version 1.1

September 6, 2011



NetFlow Monitoring Foundation Package

A Standard Content Foundation Package for ESM v5.0 SP2

Copyright © 2011 ArcSight, LLC. All rights reserved.

ArcSight and the ArcSight logo are registered trademarks of ArcSight in the United States and some other countries. Where not registered, these marks and ArcSight Console, ArcSight ESM, ArcSight Express, ArcSight Manager, ArcSightWeb, ArcSight Enterprise View, FlexConnector, ArcSight FraudView, ArcSight Identity View, ArcSight Interactive Discovery, ArcSight Logger, ArcSight NCM, SmartConnector, ArcSight Threat Detector, ArcSight TRM, and ArcSight Viewer, are trademarks of ArcSight, LLC. All other brands, products and company names used herein may be trademarks of their respective owners.

Follow this link to see a complete statement of ArcSight's copyrights, trademarks, and acknowledgements:
<http://www.arcsight.com/copyrightnotice/>

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

This document is ArcSight Confidential.

Revision History

Date	Product Version	Description
08/19/2010	ESM Standard Content Pack for NetFlow Monitoring v1.0	Initial version of the NetFlow Monitoring Foundation Package.
09/06/2011	ESM Standard Content Pack for NetFlow Monitoring v1.1	Updated version of NetFlow Monitoring Foundation Package to support ESM v5.0 SP2

Document template version: 1.0.5

ArcSight Customer Support

Phone	1-866-535-3285 (North America) +44 (0)870 141 7487 (EMEA)
E-mail	support@arcsight.com
Support Web Site	http://www.arcsight.com/supportportal/
Protect 724 Community	https://protect724.arcsight.com

Contents

Chapter 1: About the Netflow Monitoring Foundation Package	1
Supported ArcSight SmartConnectors and Platforms	1
Supported ArcSight SmartConnectors	1
Supported ArcSight Platforms	1
Presentation Resources	2
Data Processing Resources	2
Chapter 2: Installation and Configuration	3
Prepare for Installation	3
Prepare Your Environment	3
Verify Your Environment	4
Install NetFlow Monitoring Foundation Package	4
Installation Troubleshooting	4
Backup and Uninstallation	5
General Configuration	5
Assign User Permissions	5
Adjust Trend Schedules as Needed	5
Configure TotalBytes Variable	7
Background	7
Reconfiguring Resources Affected by the Connector Summation Fields Property	7
Chapter 3: Netflow Monitoring Content	9
Configuration	9
Presentation Resources	9
Dashboards	9
Top NetFlow Bandwidth Usage Monitoring Dashboard	10
NetFlow Bandwidth Usage Overview Dashboard	11
Dashboard Resources	11
Query Viewers	12
Reports	14
Data Processing Resources	15
Data Monitors	15
Filters	16
Queries	16

Trends	19
Test Filters	20
Appendix A: Compare Changes, Back Up, and Uninstall Package	23
Generate a List of Resource Changes	23
Back Up the NetFlow Monitoring Foundation Package	24
Uninstall the NetFlow Monitoring Foundation Package	24
Index	27

About the NetFlow Monitoring Foundation Package

NetFlow is a network protocol developed by Cisco Systems to run on Cisco IOS-enabled equipment for collecting IP traffic information. It is proprietary, but supported by platforms other than Cisco IOS, such as Juniper routers and Linux.

NetFlow provides session-level data. Leveraging this information using your ArcSight SIEM solution can help to monitor network bandwidth usage and correlate it with other security logs (such as firewall, IDS, authentication logs, and so on).

The NetFlow Monitoring Foundation Package provides resources to monitor and report on top bandwidth usage by source, destination and port. The NetFlow Monitoring Foundation Package is available for installation with ArcSight ESM v5.0 SP2.

Supported ArcSight SmartConnectors and Platforms

Supported ArcSight SmartConnectors

The NetFlow Monitoring Foundation Package is triggered by NetFlow events from the following ArcSight SmartConnectors.


SmartConnector	Supports this device version:
ArcSight IP Flow SmartConnector	<ul style="list-style-type: none">• Cisco NetFlow versions 5 and 9• Flexible NetFlow from IOS 15.0• Cisco ASA 8.2, and Juniper Networks J-Flow versions 5 and 9
ArcSight QoSient ARGUS SmartConnector	<ul style="list-style-type: none">• Qosient ARGUS versions 2 and 3


Supported ArcSight Platforms


The NetFlow Monitoring Foundation Package v1.1 runs on the ArcSight platform ArcSight ESM v5.0 SP2 platform.

Presentation Resources

Presentation resources produce viewable output that provides information about details associated with a particular use case.


Dashboards () display indicators communicating information about the current state of your enterprise by summarizing event information supplied by one or more data monitors.


Reports () evaluate stored events to communicate status based on specific criteria.


Query Viewers () enable you to drill down and investigate anomalies or other interesting events without having to create low-level active channels. Query viewers use events and other resources, such as trends, active lists, session lists, assets, cases, and notifications, as data sources.


Data Processing Resources

Data processing resources evaluate events from devices, and provide the basis of the information displayed in the presentation resources.

Data monitors () define the logic used to process the events displayed in the graphical summaries of dashboards.

Filters () are sets of conditions that focus on particular event attributes. This focus reduces the number of events that are processed by “decision-making” resources that invoke the filter such as rules, active channels, reports, data monitors and other filters.

Queries () gather the event data displayed by reports and used by query viewers and trends. When a report runs, it invokes the associated query against the event data on the ArcSight ESM Manager and returns the event data matching the conditions specified in the query back to the report to display.

Trends () define how and over what time period data will be aggregated and evaluated for prevailing tendencies or currents. A trend executes a specified query on a defined schedule and time duration.

Chapter 2

Installation and Configuration

This chapter describes how to install and configure the NetFlow Monitoring Foundation Package.

[“Prepare for Installation” on page 3](#)

[“Install NetFlow Monitoring Foundation Package” on page 4](#)

Prepare for Installation

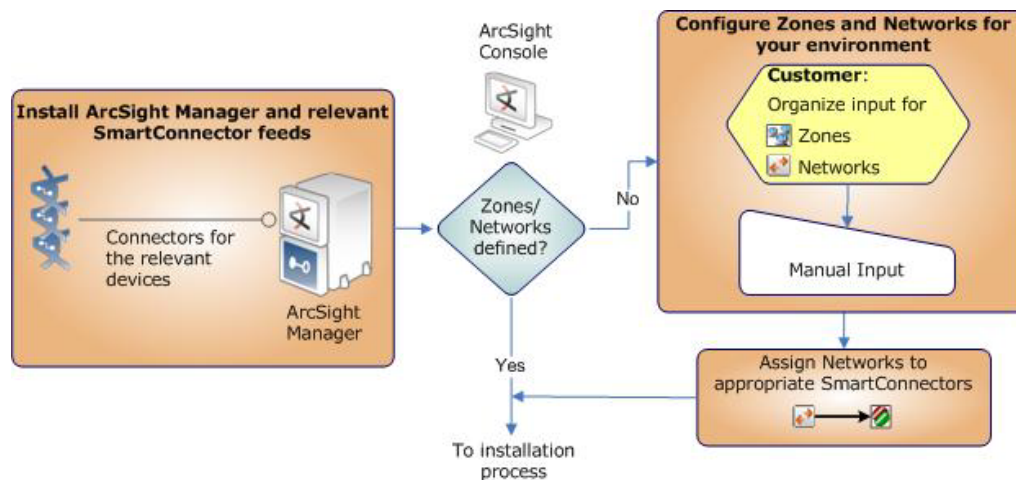
Before installing the NetFlow Monitoring Foundation Package, complete the following preparation tasks:

- 1 [“Prepare Your Environment” on page 3](#)
- 2 [“Verify Your Environment” on page 4](#)

Prepare Your Environment

Before installing, prepare your environment for the NetFlow Monitoring Foundation Package.

- 1 Install and configure the appropriate SmartConnectors for the devices in your environment.
 - ◆ ArcSight IP Flow SmartConnector (NetFlow/J-Flow)
 - ◆ ArcSight QoSient ARGUS SmartConnectorFor details about the supported device versions, see [“Supported ArcSight SmartConnectors” on page 1](#).
- 2 Model your network. Learn more about the ArcSight network modeling process in the *ArcSight ESM 101 Guide*. Find instructions for how to configure zones and networks in the *ArcSight ESM Console Help*.

Figure 2-1 Prepare Your Environment

Verify Your Environment

Before installing the NetFlow Monitoring Foundation Package v1.1, verify that you have ArcSight ESM v5.0 SP2 installed and configured.

If you need to install the NetFlow Monitoring Foundation Package on a previous version of ArcSight ESM, you must install v1.0, which is available as a separate downloadable bundle ([NetFlow_Monitoring_v1.0.arb](#)) from the ArcSight software download site (<https://software.arcsight.com>). For installation and configuration instructions, see the NetFlow Monitoring Foundation Package Guide v.1.0



Content Compatibility

The NetFlow Monitoring Foundation Package relies on the Network Filters package ([/All Packages/ArcSight Foundation/Network Filters](#)) installed by default with ESM as part of the ArcSight Administration Foundation.

Install NetFlow Monitoring Foundation Package

Once you have prepared and verified your environment as described in the previous sections, you can install the NetFlow Monitoring Foundation Package.

The NetFlow Monitoring Foundation Package is available as part of ArcSight ESM v5.0 SP2. For installation instructions, see the *ArcSight Installation Guide*.

Once you have installed the NetFlow Monitoring Foundation package, see ["General Configuration" on page 5](#) for instructions about configuring the package.

Installation Troubleshooting

If the installation was not successful, contact ArcSight technical support:

Resource	Description
Support web site	https://support.arcsight.com . Access to ArcSight incident reporting, knowledge base, software downloads, help, and new customer forum.

Resource	Description
Customer forum	https://protect724.arcsight.com . Offers a place for customers to share ArcSight tips and tricks.

Backup and Uninstallation

If you need to back up or uninstall the NetFlow Monitoring Foundation Package at a later date, see [Appendix A, Compare Changes, Back Up, and Uninstall Package, on page 23](#).

General Configuration

This section describes general configurations to make to the NetFlow Monitoring Foundation Package once it is installed.

Assign User Permissions

By default, users in the [Default](#) user group can view the NetFlow Monitoring Foundation Package content, and users in the [ArcSight Administrators](#) and [Analyzer Administrators](#) user groups have read and write access to the foundation content. Depending on how you have set up user access controls within your organization, you may need to adjust those controls to make sure the new content is accessible to the right users in your organization.

The following procedure assumes that you have user groups set up and users assigned to them. Follow the steps to assign user permissions to each of the following resource types:

- ◆ Dashboards
- ◆ Data Monitors
- ◆ Filters
- ◆ Queries
- ◆ Query Viewers
- ◆ Reports
- ◆ Trends

To assign user permissions:

- 1 Log into the ArcSight ESM Console with an account that has administrative privileges.
- 2 For all the resource types listed above, change the user permissions:
 - a In the Navigator panel, go to the resource type and navigate to [ArcSight Foundations/NetFlow Monitoring](#).
 - b Right-click the **NetFlow Monitoring** group and select **Edit Access Control** to open the ACL editor in the Inspect/Edit panel.
 - c In the ACL editor in the Inspect/Edit panel, select which user groups you want to have permissions to EnterpriseView for Cisco resources and click **OK**.

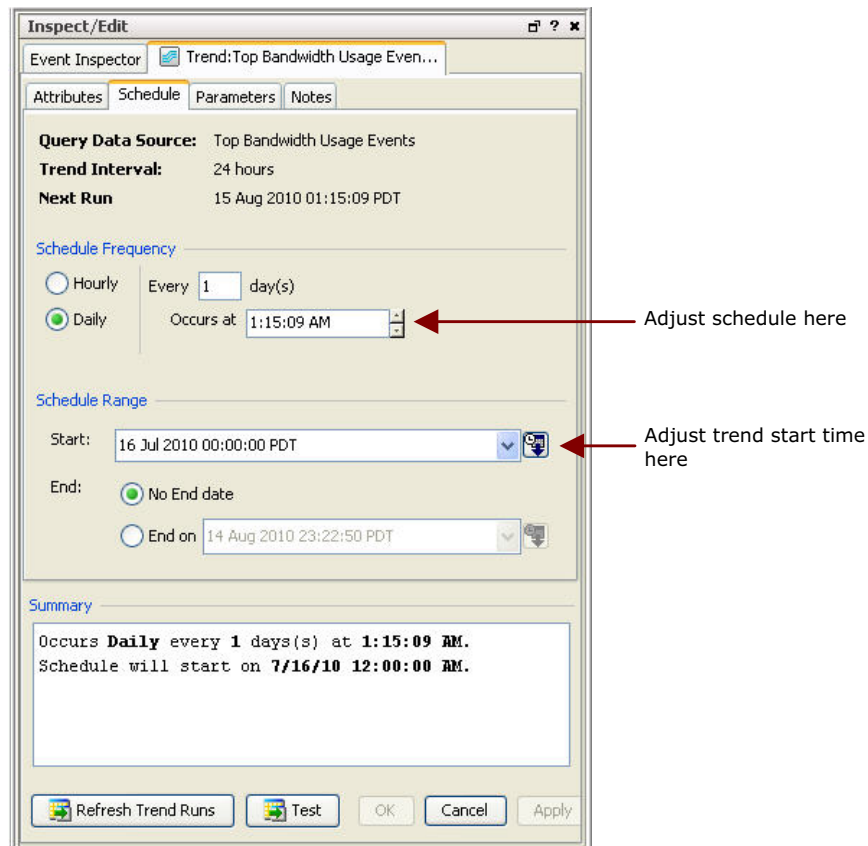
Adjust Trend Schedules as Needed

The NetFlow Monitoring Foundation Package contains five trends. Four of the trends are trend-on-trends, which all collect data from a single base trend ([/All Trends/ArcSight Foundation/NetFlow Monitoring/Top Bandwidth Usage Events](#)). The four trend-on-trends should not be scheduled to run before the base trend

completes its daily query run. By default, the trends are scheduled to run daily at the times indicated below:

Trend Name	Scheduled run time
Top Bandwidth Usage by Destination	3:33:36 AM
Top Bandwidth Usage by Hour	2:40:34 AM
Top Bandwidth Usage by Port	3:15:50 AM
Top Bandwidth Usage by Source	3:07:08 AM
Top Bandwidth Usage Events (base trend)	1:15:09 AM

By default, each trend uses midnight of the date the package was installed as the date and time the trend will start collecting information. To adjust the trend's schedule or start date/time, edit the values in the trend's **Schedule** tab in the Inspect/Edit panel. For example:



Configure TotalBytes Variable



Note

Where this configuration applies

This configuration applies only to ArcSight ESM installations to which the Connector Summation Fields property (`connector.summation.fields=bytesIn,bytesOut`) has been added to the `server.properties` file on the ArcSight ESM Manager.

If your ESM installation **does not** have the Connector Summation Fields property added to the `server.properties` file, then *no additional configuration* is required to the NetFlow Monitoring Foundation Package.

Background

SmartConnectors can be configured to aggregate events and sum the counts in fields, such as `bytesIn` and `bytesOut`. Connectors also set the aggregated event count. By default, ESM interprets the count in fields such as `bytesIn` & `bytesOut` as an average, and if the Connector is configured to sum certain fields, ESM will *multiply* those summed fields by aggregated event count, which creates an inaccurate value.

By default, the NetFlow Monitoring Foundation Package content compensates for this by dividing the `bytesIn` and `bytesOut` fields by aggregated event count using the `TotalBytes` variable.

The **Connector Summation Fields** property is a configuration option with ESM that enables you to tell ESM which fields are sums, so that it can report the correct value without requiring that content compensate by adding a divide-by-aggregated-count function.

For example, the following property added to `server.properties` on the ArcSight ESM Manager tells ESM that the `bytesIn` and `bytesOut` fields coming from the Connector are sums, and thus exempts those fields from being multiplied by aggregated event count:

```
connector.summation.fields=bytesIn,bytesOut
```

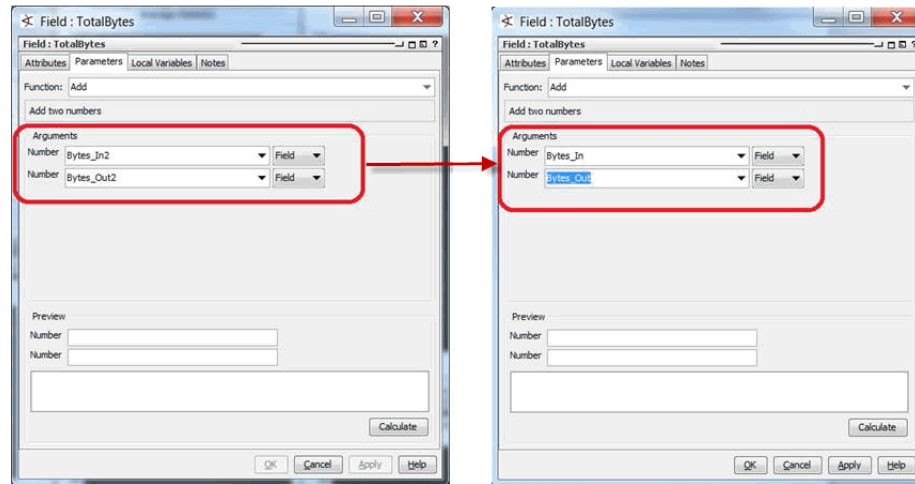
If this property is set in your ESM installation, the content in the NetFlow Monitoring Foundation Package that uses the `TotalBytes` variable must be reconfigured to use a variable that will add the values, not multiply them.

The path for the global variable `TotalBytes` is

```
/All Fields/ArcSight Foundation/Variables Library/TotalBytes
```

Reconfiguring Resources Affected by the Connector Summation Fields Property

In the `TotalBytes` Field dialog box, click the Parameters tab, and change the arguments in the `TotalBytes` global variable from `BytesIn_2` and `BytesOut_2` to `Bytes_In` and `Bytes_Out`, as shown in the following figure.



For instructions about how to find and modify the `server.properties` file on the Manager, see the topic “Managing and Changing Properties File Settings” in the Configuration chapter of the *ArcSight ESM Administrator's Guide*.

For instructions about how to configure a SmartConnector to aggregate and sum on fields, such as `bytesIn` and `bytesOut` and `targetPort`, see the topic “Filter Aggregation” in the Configuring SmartConnectors chapter of the *ArcSight SmartConnector User's Guide*.

Chapter 3

Netflow Monitoring Content

The NetFlow Monitoring Foundation Package provides a series of coordinated resources that:

- Monitor, investigate, and report on bandwidth usage by source, destination, and port
- Monitor bandwidth moving average and identify top bandwidth usage by source, destination, and port
- Report on bandwidth usage in daily or weekly increments using trends, and by source, destination, and port

You can use this information to build correlation content, such as a rule that correlates NetFlow events with other security logs, such as firewall or IDS logs.

Configuration

There are no specific configurations required to resources in the NetFlow Monitoring Foundation Package. Any configuration you may need to do depends on your installation environment:

- If you have installed the NetFlow Monitoring Foundation Package that has the **Connector Summation Fields** property (`connector.summation.fields=bytesIn,bytesOut`) added to the `server.properties` file on the ArcSight ESM Manager, perform the configurations outlined in [“Configure TotalBytes Variable” on page 7](#).
- If the default trend schedule and start dates do not work for your environment, configure them as outlined in [“Adjust Trend Schedules as Needed” on page 5](#).
- If you have NetFlow events that you want to add to the NetFlow Monitoring Foundation Package from additional devices, review the guidelines in the section [“Test Filters” on page 20](#).

Presentation Resources

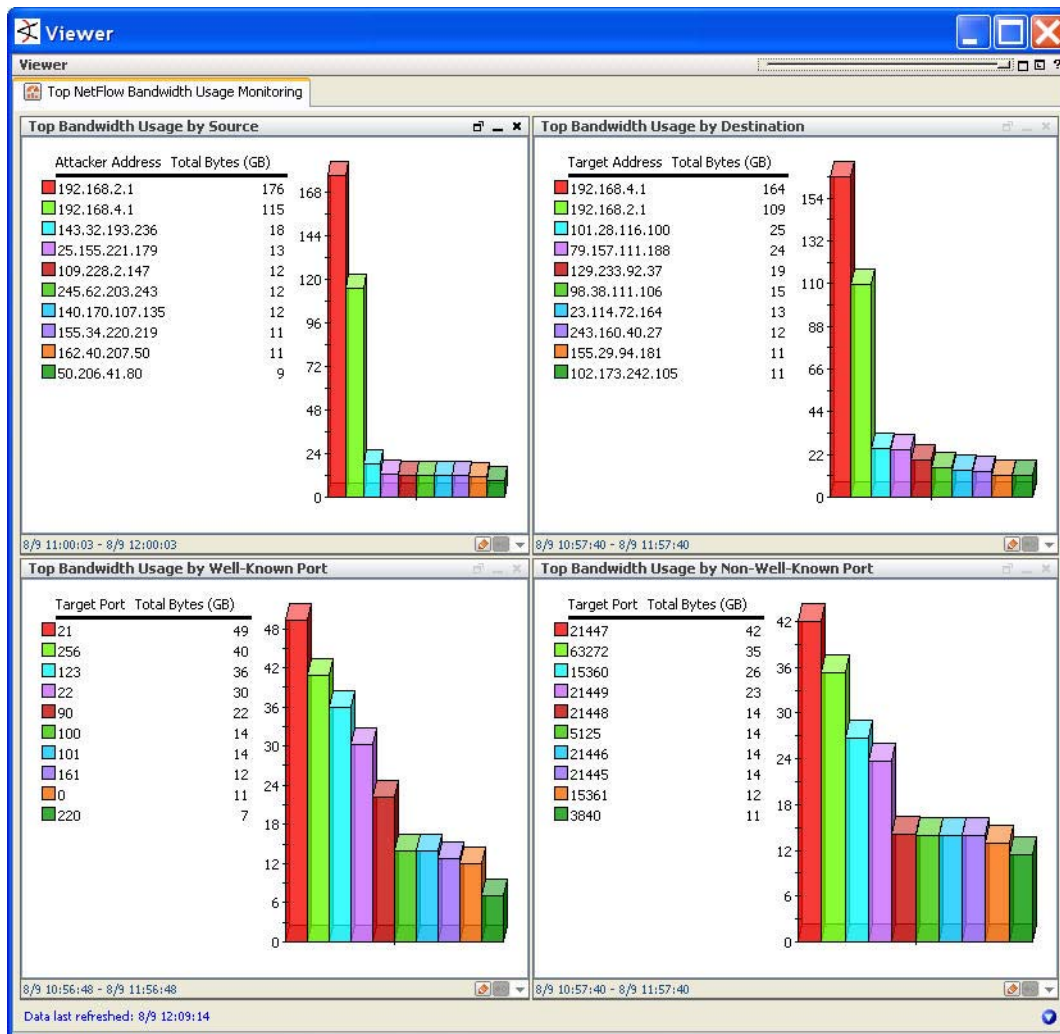
The NetFlow Monitoring Foundation Package provides a series of dashboards for monitoring and drill-down investigation of bandwidth usage, and a series of reports for analyzing bandwidth usage from multiple viewpoints.

Dashboards

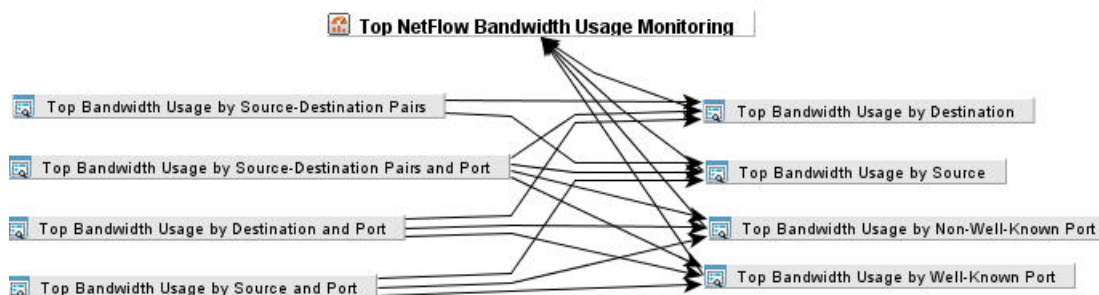
The NetFlow Monitoring Foundation Package provides two dashboards supported by data monitors and query viewers for drill-down investigation of bandwidth usage during monitoring.

Top NetFlow Bandwidth Usage Monitoring Dashboard

This dashboard provides a comprehensive overview of the NetFlow bandwidth usage in your environment by source, destination, well-known port, and non-well-known port.

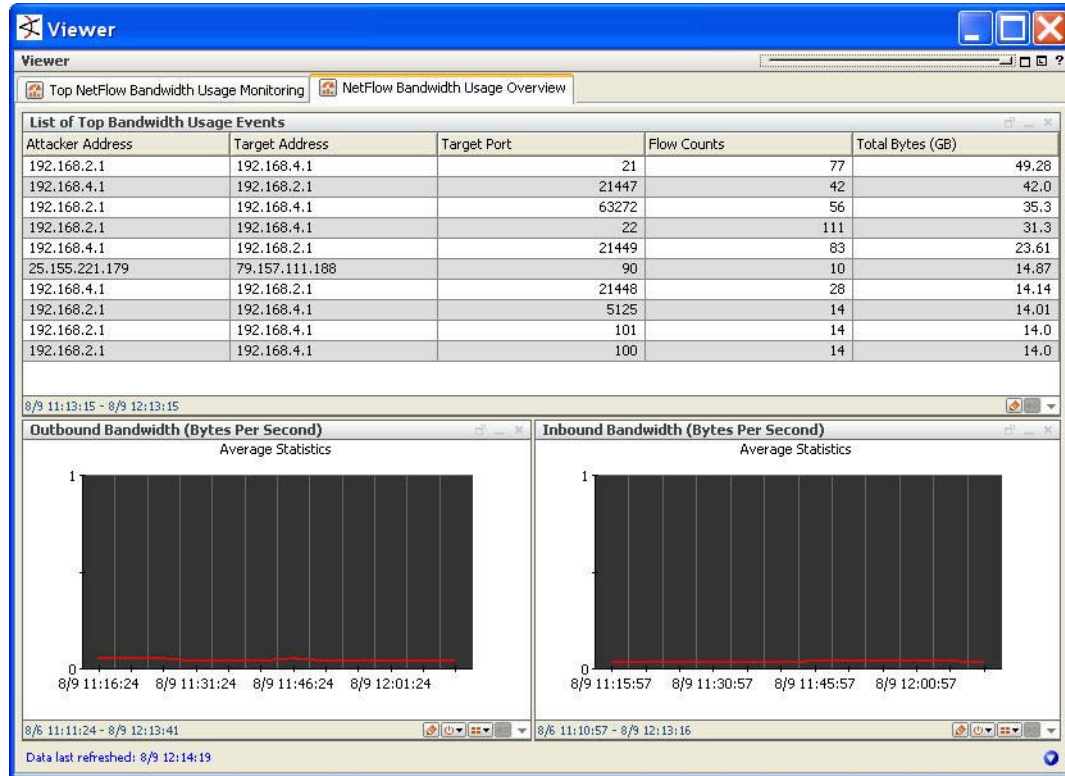


Each view in the dashboard is powered by [Query Viewers](#), as shown below, which enables drill-down investigation of any node in the dashboard.

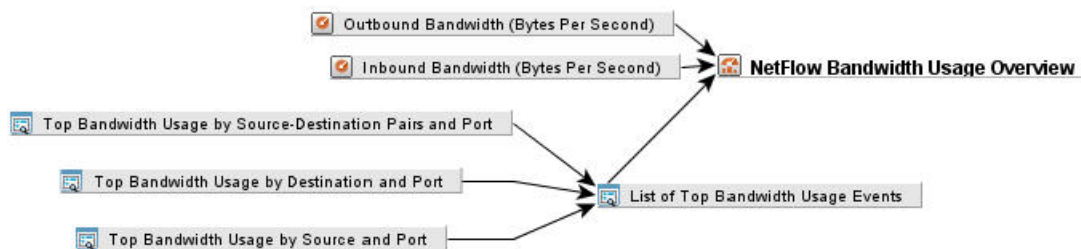


NetFlow Bandwidth Usage Overview Dashboard

The NetFlow Bandwidth Usage Overview dashboard provides an breakdown of the top bandwidth usage events, as well as the average inbound and outbound bandwidth usage.



These views are powered by the List of Top Bandwidth Usage Events query viewer and its supporting drill-down [Query Viewers](#), and two moving average [Data Monitors](#).



Dashboard Resources

The NetFlow Monitoring Foundation Package dashboards are described below.

Resource	Description	Type	URI
NetFlow Bandwidth Usage Overview	This dashboard shows an overview of bandwidth usage reported by NetFlow events, showing top bandwidth usage events, inbound and outbound bandwidth moving average.	Dashboard	/All Dashboards/ArcSight Foundation/NetFlow Monitoring/

Resource	Description	Type	URI
Top NetFlow Bandwidth Usage Monitoring	This dashboard shows the top bandwidth usage as reported by NetFlow events, showing top bandwidth usage by source, destination, well known port and non well known Port.	Dashboard	/All Dashboards/ArcSight Foundation/NetFlow Monitoring/

Query Viewers

The query viewers that support the NetFlow Monitoring Foundation Package dashboards are described below.

Resource	Description	Type	URI
List of Top Bandwidth Usage Events	<p>This query viewer displays top 10 bandwidth usage events.</p> <p>This query viewer contains 4 Drilldowns for investigation:</p> <ul style="list-style-type: none"> • Passing source address and Port to Top Bandwidth Usage Events • Passing source address to Top Bandwidth Usage by Source and Port • Passing destination address and Port to Top Bandwidth Usage Events • Passing destination address to Top Bandwidth Usage by Destination and Port 	Query Viewer	/All Query Viewers/ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Destination	<p>This query viewer displays top 10 destination addresses, and total bytes from the NetFlow events, sorted by bytes.</p> <p>This query viewer contains 3 Drilldowns for investigation:</p> <ul style="list-style-type: none"> • Passing destination address to Top Bandwidth Usage by Source-Destination Pairs • Passing destination address to Top Bandwidth Usage Events • Passing destination address to Top Bandwidth Usage by Destination and Port 	Query Viewer	/All Query Viewers/ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Destination and Port	This query viewer displays top 10 destination addresses, destination ports, flow counts, and total bytes from the NetFlow events, sorted by bytes.	Query Viewer	/All Query Viewers/ArcSight Foundation/NetFlow Monitoring/

Resource	Description	Type	URI
Top Bandwidth Usage by Non-Well-Known Port	<p>This query viewer displays top 10 non-well-known destination ports, and total bytes from the NetFlow events, sorted by bytes.</p> <p>This query viewer contains 3 Drilldowns for investigation:</p> <ul style="list-style-type: none"> • Passing destination port to Top Bandwidth Usage by Destination and Port • Passing destination port to Top Bandwidth Usage Events • Passing destination port to Top Bandwidth Usage by Source and Port 	Query Viewer	/All Query Viewers/ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Source	<p>This query viewer displays top 10 source addresses and total bytes from the NetFlow events, sorted by bytes.</p> <p>This query viewer contains 3 Drilldowns for investigation:</p> <ul style="list-style-type: none"> • Passing source address to Top Bandwidth Usage by Source-Destination Pairs • Passing source address to Top Bandwidth Usage Events • Passing source address to Top Bandwidth Usage by Source and Port 	Query Viewer	/All Query Viewers/ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Source and Port	<p>This query viewer displays top 10 source address, destination port, flow counts, and total bytes from the NetFlow events, sorted by bytes.</p>	Query Viewer	/All Query Viewers/ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Source-Destination Pairs	<p>This query viewer displays top 10 source address, destination address, and total bytes from the NetFlow events, sorted by bytes.</p>	Query Viewer	/All Query Viewers/ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Source-Destination Pairs and Port	<p>This query viewer displays top 10 source address, destination address, destination port, counts and total bytes from the NetFlow events, sorted by bytes.</p>	Query Viewer	/All Query Viewers/ArcSight Foundation/NetFlow Monitoring/

Resource	Description	Type	URI
Top Bandwidth Usage by Well-Known Port	<p>This query viewer displays Top 10 well-known destination ports, and total bytes from the NetFlow events, sorted by bytes.</p> <p>This query viewer contains 3 Drilldowns for investigation:</p> <ul style="list-style-type: none"> • Passing destination port to Top Bandwidth Usage by Destination and Port • Passing destination port to Top Bandwidth Usage Events • Passing destination port to Top Bandwidth Usage by Source and Port 	Query Viewer	/All Query Viewers/ArcSight Foundation/NetFlow Monitoring/

Reports

The NetFlow Monitoring Foundation Package contains a series of reports that analyze daily and weekly NetFlow bandwidth usage, as well as by source, destination, and port.

Resource	Description	Type	URI
Top Bandwidth Usage Daily Report	This report displays an hourly chart showing the bandwidth usage, a chart showing the top bandwidth usage by source, a chart showing the top bandwidth usage by destination and a chart showing the top bandwidth usage by port. The default time range for this report is yesterday.	Report	/All Reports/ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage Weekly Report	This report displays a daily chart showing the bandwidth usage, a chart showing the top bandwidth usage by source, a chart showing the top bandwidth usage by destination and a chart showing the top bandwidth usage by port. The default time range for this report is the past 7 days.	Report	/All Reports/ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Destination	This report displays a chart and a table showing top bandwidth usage by destination. The default time range for this report is yesterday.	Report	/All Reports/ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Destination Port	This report displays a chart and a table showing top bandwidth usage by destination port. The default time range for this report is yesterday.	Report	/All Reports/ArcSight Foundation/NetFlow Monitoring/

Resource	Description	Type	URI
Top Bandwidth Usage by Source	This report displays a chart and a table showing top bandwidth usage by source. The default time range for this report is yesterday.	Report	/All Reports/ArcSight Foundation/NetFlow Monitoring/

Data Processing Resources

The NetFlow Monitoring Foundation Package presentation resources are supported by the following data processing resources.

Data Monitors

Resource	Description	Type	URI
Inbound Bandwidth (Bytes Per Second)	This moving average data monitor shows the average inbound bandwidth (bytes/sec) for the last hour. The values are updated every 5 minutes.	Data Monitor	/All Data Monitors/ArcSight Foundation/NetFlow Monitoring/
Outbound Bandwidth (Bytes Per Second)	This moving average data monitor shows the average outbound bandwidth (bytes/sec) for the last hour. The values are updated every 5 minutes.	Data Monitor	/All Data Monitors/ArcSight Foundation/NetFlow Monitoring/

Filters

Resource	Description	Type	URI
Inbound NetFlow Traffic	This filter looks for NetFlow events coming from external sources targeting the internal network.	Filter	/All Filters/ArcSight Foundation/NetFlow Monitoring/
NetFlow Traffic Reporting Devices	This filter is used to select the NetFlow traffic reporting devices. By default, it contains QoSient Argus events, NetFlow V5 events, and NetFlow V9 events.	Filter	/All Filters/ArcSight Foundation/NetFlow Monitoring/
NetFlow V5 Events	This filter looks for NetFlow Version 5 events.	Filter	/All Filters/ArcSight Foundation/NetFlow Monitoring/
NetFlow V9 Events	This filter looks for NetFlow Version 9 events.	Filter	/All Filters/ArcSight Foundation/NetFlow Monitoring/
Non-Well-Known Ports	This filter selects events in which the Target Port is not NULL, and is greater than 1024.	Filter	/All Filters/ArcSight Foundation/NetFlow Monitoring/
Outbound NetFlow Traffic	This filter looks for NetFlow events coming from internal sources targeting the external network.	Filter	/All Filters/ArcSight Foundation/NetFlow Monitoring/
QoSient Argus Events	This filter looks for events coming from the Argus connectors.	Filter	/All Filters/ArcSight Foundation/NetFlow Monitoring/
Well-Known Ports	This filter selects events in which the Target Port is not NULL, and is less than or equal to 1024.	Filter	/All Filters/ArcSight Foundation/NetFlow Monitoring/

Queries

Resource	Description	Type	URI
List of Top Bandwidth Usage Events	<p>This query selects the source address, destination address, destination port, flow counts and total bytes (Bytes In + Bytes Out) from NetFlow events in the last hour.</p> <p>This query is used by the query viewers List of Top Bandwidth Usage Events.</p>	Query	/All Queries/ArcSight Foundation/NetFlow Monitoring/

Resource	Description	Type	URI
Top Bandwidth Usage Events	This query selects the source address, destination address, destination port, flow counts and total bytes (Bytes In + Bytes Out) from NetFlow events in the last hour. This query is used by the trend Top Bandwidth Usage Events.	Query	/All Queries/ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Destination	This query selects the destination address and total bytes (Bytes In + Bytes Out) from NetFlow events in the last hour.	Query	/All Queries/ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Destination and Port	This query selects the destination address, destination port, flow counts and total bytes (Bytes In + Bytes Out) from NetFlow events in the last hour.	Query	/All Queries/ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Non-Well-Known Port	This query selects the destination port and total bytes (Bytes In + Bytes Out) from NetFlow events where destination port is non-well-known in the last hour.	Query	/All Queries/ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Source	This query selects the source address and total bytes (Bytes In + Bytes Out) from NetFlow events in the last hour.	Query	/All Queries/ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Source and Port	This query selects the source address, destination port, flow counts and total bytes (Bytes In + Bytes Out) from NetFlow events in the last hour.	Query	/All Queries/ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Source-Destination Pairs	This query selects the source address, destination address, flow counts and total bytes (Bytes In + Bytes Out) from NetFlow events in the last hour.	Query	/All Queries/ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Source-Destination Pairs and Port	This query selects the source address, destination address, destination port, flow counts and total bytes (Bytes In + Bytes Out) from NetFlow events in the last hour.	Query	/All Queries/ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Well-Known Port	This query selects the destination port and total bytes (Bytes In + Bytes Out) from NetFlow events where destination port is well-known in the last hour.	Query	/All Queries/ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Day - Trend on Trend	This query selects bandwidth usage information by day from the trend Top Bandwidth Usage by Hour.	Query	/All Queries/ArcSight Foundation/NetFlow Monitoring/Trend/

Resource	Description	Type	URI
Top Bandwidth Usage by Destination - Trend	This query selects the destination address, destination zone, flow counts, and total bytes from the trend Top Bandwidth Usage Events.	Query	/All Queries/ArcSight Foundation/NetFlow Monitoring/Trend/
Top Bandwidth Usage by Destination - Trend on Trend	This query selects the destination address, destination zone, flow counts and total bytes from the trend Top Bandwidth Usage by Destination.	Query	/All Queries/ArcSight Foundation/NetFlow Monitoring/Trend/
Top Bandwidth Usage by Hour - Trend	This query selects bandwidth usage information by hour from the trend Top Bandwidth Usage Events.	Query	/All Queries/ArcSight Foundation/NetFlow Monitoring/Trend/
Top Bandwidth Usage by Hour - Trend on Trend	This query selects bandwidth usage information by hour from the trend Top Bandwidth Usage by Hour.	Query	/All Queries/ArcSight Foundation/NetFlow Monitoring/Trend/
Top Bandwidth Usage by Port - Trend	This query selects destination port, flow counts and total bytes from the trend Top Bandwidth Usage Events.	Query	/All Queries/ArcSight Foundation/NetFlow Monitoring/Trend/
Top Bandwidth Usage by Port - Trend on Trend	This query selects target Port, flow counts and total bytes from the trend Top Bandwidth Usage by Port.	Query	/All Queries/ArcSight Foundation/NetFlow Monitoring/Trend/
Top Bandwidth Usage by Source - Trend	This query selects the source address, source zone and total bytes from the trend Top Bandwidth Usage Events.	Query	/All Queries/ArcSight Foundation/NetFlow Monitoring/Trend/
Top Bandwidth Usage by Source - Trend on Trend	This query selects the source address, source zone and total bytes from the trend Top Bandwidth Usage by Source.	Query	/All Queries/ArcSight Foundation/NetFlow Monitoring/Trend/

Trends

Resource	Description	Type	URI
Top Bandwidth Usage Events	<p>This trend stores bandwidth usage information reported by NetFlow, which contains hour of end time, source address, source zone, destination address, destination zone, destination port, flow counts and total bytes.</p> <p>This trend is the base trend, collecting a broad amount of aggregated NetFlow data for a short period of time, that is to be used by several other trends to further aggregate data and store for a longer period of time.</p> <p>The default retention period for this trend is 8 days.</p>	Trend	/All Trends/ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Destination	<p>This trend stores top bandwidth usage information by destination, which includes destination address, destination zone, flow counts and total bytes.</p> <p>This trend depends on the trend /All Trends/ArcSight Foundation/NetFlow Monitoring/Top Bandwidth Usage Events, and should be scheduled to run after it has completed its run.</p>	Trend	/All Trends/ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Hour	<p>This trend stores hourly information of top bandwidth usage, which includes hour of end time, flow counts and total bytes.</p> <p>This trend depends on the trend /All Trends/ArcSight Foundation/NetFlow Monitoring/Top Bandwidth Usage Events, and should be scheduled to run after it has completed its run.</p>	Trend	/All Trends/ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Port	<p>This trend stores top bandwidth usage information by port, which includes destination port, flow counts and total bytes.</p> <p>This trend depends on the trend /All Trends/ArcSight Foundation/NetFlow Monitoring/Top Bandwidth Usage Events, and should be scheduled to run after it has completed its run.</p>	Trend	/All Trends/ArcSight Foundation/NetFlow Monitoring/

Resource	Description	Type	URI
Top Bandwidth Usage by Source	<p>This trend stores top bandwidth usage information by source, which includes source address, source zone, flow counts and total bytes.</p> <p>This trend depends on the trend /All Trends/ArcSight Foundation/NetFlow Monitoring/Top Bandwidth Usage Events, and should be scheduled to run after it has completed its run.</p>	Trend	/All Trends/ArcSight Foundation/NetFlow Monitoring/

Test Filters

Most of the content in the NetFlow Monitoring Foundation Package relies on event categorization fields to identify events of interest. For some use cases, you may need to test key filters to verify that they actually capture the required events. This section provides general instructions for testing filters.

The NetFlow Monitoring Foundation Package provides a key filter to capture NetFlow events:

- ◆ [/All Filters/ArcSight Foundation/NetFlow Monitoring/NetFlow Traffic Reporting Devices.](#)



Perform the following procedure on a **test system** first.

To ensure that a filter captures the relevant events:

- 1 Generate or import the required events and verify that they are being processed by ArcSight ESM by viewing them in an active channel or query viewer.

To generate relevant events, either:

- ◆ Set up a connector to capture events from a target system and perform the actions that would generate the required events on that system
- or
- ◆ Import into ArcSight ESM an existing events file that contains relevant events.

Alternatively, you can use imported events to identify that these types of events have already been processed by ArcSight ESM and ensure that the start and end time of the active channel or query viewer covers the event time of these events

- 2 Navigate to the filter, right-click it, and then choose **Create Channel with Filter**. If you see the events of interest in the newly created channel, then you know that the conditions are set appropriately.
- 3 If you do not see the events of interest:
 - ◆ Verify that the configuration of the active channel is suitable for the events in question. For example, ensure that the event time is within the start and end time of the channel.

- ◆ Modify the filter's condition to capture the events of interest. After applying the change, repeat Step 2 to verify that the modified filter captures the required events.

**Note**

For a use case to process and display complete information, filters should capture similar events from different systems.

Also, you may need to fine-tune the filter's condition to minimize occurrences of false positives.

Appendix A

Compare Changes, Back Up, and Uninstall Package

This chapter provides instructions for comparing resource changes, backing up, and uninstalling the NetFlow Monitoring Foundation Package.

Generate a List of Resource Changes


Before backing up a foundation package, you may want to generate a list of resource changes since the last time the package was exported to a package bundle. The current resources associated with the selected package are compared against the resources saved in the package bundle and any new, modified, or deleted resources are reported.



Every time a package is exported, the change history is reset.

To generate a list of resource changes:

- 1 Log into the ArcSight Console as a user with administrative privileges.
- 2 In the Packages tab of the Navigator panel, navigate to the foundation group.

For the NetFlow Monitoring Foundation Package, navigate to [ArcSight Foundations/Netflow Monitoring](#).
- 3 Right-click the foundation package () and select **Compare Archive with Current Package Contents**.

In the Viewer panel, a list of resources associated with the package are displayed. In the right column called [Change Since Archive](#), any changes with the resource since the last export are displayed, either [Added](#), [Modified](#), or [Removed](#).
- 4 Optional—For future reference, copy and paste the cells from this table into a spreadsheet.


Back Up the NetFlow Monitoring Foundation Package

ArcSight recommends that you have a backup of the current state before making content changes or installing/uninstalling foundation packages. This will enable you to preserve any configurations you have made and reinstall the package at a later time. Before backing up a foundation, you may want to get a list of changed resources. You may want to back up only those resources that have been modified or added. For detailed instructions, see [“Generate a List of Resource Changes” on page 23](#).

You can back up the foundation content to a package bundle file that ends in the `.arb` extension as described in the process below.

To back up a foundation package:

- 1 Log into the ArcSight Console as ArcSight Administrator.
- 2 In the Packages tab of the Navigator panel, navigate to the foundation group.

For the NetFlow Monitoring Foundation Package, navigate to [ArcSight Foundations/Netflow Monitoring](#).
- 3 Right-click the foundation package () and select **Export Package(s) to Bundle**.

The Package Bundle Export dialog displays.
- 4 In the Package Bundle Export dialog, browse for a directory location, specify a file name and click **Next**.

The Progress tab of the Export Packages dialog displays the progress of the export.
- 5 When the export is finished, click **OK**.


The resources are saved into the package bundle file that ends with the `.arb` extension. You can restore the contents of this package at a later time by importing this package bundle file.

Uninstall the NetFlow Monitoring Foundation Package

The NetFlow Monitoring Foundation Package depends on the Network Filters package, which is part of the ArcSight Administration Foundation that is installed automatically with ArcSight ESM. The Network Filters package is also required by other resources in the ESM standard content, and as such, is not uninstalled during the uninstall process.

Before uninstalling the NetFlow Monitoring Foundation Package, ArcSight recommends backing up the package to preserve any configurations you have made. For detailed instructions, see [“Back Up the NetFlow Monitoring Foundation Package” on page 24](#). You may also want to generate a list of changes before the uninstall. For detailed instructions, see [“Generate a List of Resource Changes” on page 23](#).

To uninstall the NetFlow Monitoring Foundation Package:

- 1 Log into the ArcSight ESM Console as ArcSight Administrator.
- 2 Click the Packages tab in the Navigator panel.
- 3 In the Packages tab of the Navigator panel, navigate to [ArcSight Foundations/Netflow Monitoring](#).
- 4 Right-click the [Netflow Monitoring](#) package () and select **Uninstall Package**.

- 5 In the Uninstall Packages dialog, click **OK**.

If you see a conflict in the Uninstalling Packages dialog, select **Continue without saving changes**, and then click **OK**.

ESM displays the progress of the uninstall in the Progress tab of the Uninstalling Packages dialog.

- 6 When the uninstall process is finished, click **OK**.

Index

A

- ARB file 4
- assign user permissions 5

B

- back up 5, 24

C

- changed resources list, generating 23
- configuration 9

D

- dashboards
 - netflow bandwidth usage overview dashboard 11
 - overview 9
 - resources 11
 - top netflow bandwidth usage monitoring dashboard 10
- data monitors 15
 - Inbound Bandwidth (Bytes Per Second) 15
 - Outbound Bandwidth (Bytes Per Second) 15
- data processing resources 15, 16
 - data monitors 15
 - filters 16
 - trends 19

E

- environment
 - prepare 3
 - verify 4

F

- filters 16
 - Inbound NetFlow Traffic 16
 - NetFlow Traffic Reporting Devices 16
 - NetFlow V5 Events 16
 - NetFlow V9 Events 16
 - Non-Well-Known Ports 16
 - Outbound NetFlow Traffic 16
 - QoSient Argus Events 16
 - testing 20
 - Well-Known Ports 16
- foundation
 - back up 24
 - configuration 9
 - generate list of changes 23
 - install 4

- uninstall 24

I

- install
 - package 4
 - troubleshoot 4

M

- model devices 3

P

- package
 - back up 24
 - generate list of changes 23
 - uninstall 24
- permissions
 - assign 5
- platforms, supported 1
- presentation resources 9
 - dashboards 9
 - query viewers 12
 - reports 14

Q

- queries 16
 - List of Top Bandwidth Usage Events 16
 - Top Bandwidth Usage by Day - Trend on Trend 17
 - Top Bandwidth Usage by Destination 17
 - Top Bandwidth Usage by Destination - Trend 18
 - Top Bandwidth Usage by Destination - Trend on Trend 18
 - Top Bandwidth Usage by Destination and Port 17
 - Top Bandwidth Usage by Hour - Trend 18
 - Top Bandwidth Usage by Hour - Trend on Trend 18
 - Top Bandwidth Usage by Non-Well-Known Port 17
 - Top Bandwidth Usage by Port - Trend 18
 - Top Bandwidth Usage by Port - Trend on Trend 18
 - Top Bandwidth Usage by Source 17
 - Top Bandwidth Usage by Source - Trend 18
 - Top Bandwidth Usage by Source - Trend on Trend 18
 - Top Bandwidth Usage by Source and Port 17
 - Top Bandwidth Usage by Source-Destination Pairs 17
 - Top Bandwidth Usage by Source-Destination Pairs and Port 17
 - Top Bandwidth Usage by Well-Known Port 17
 - Top Bandwidth Usage Events 17

query viewers 12

- List of Top Bandwidth Usage Events 12
- Top Bandwidth Usage by Destination 12
- Top Bandwidth Usage by Destination and Port 12
- Top Bandwidth Usage by Non-Well-Known Port 13
- Top Bandwidth Usage by Source 13
- Top Bandwidth Usage by Source and Port 13
- Top Bandwidth Usage by Source-Destination Pairs 13
- Top Bandwidth Usage by Source-Destination Pairs and Port 13
- Top Bandwidth Usage by Well-Known Port 14

R

reports 14

- Top Bandwidth Usage by Destination 14
- Top Bandwidth Usage by Destination Port 14
- Top Bandwidth Usage by Source 15
- Top Bandwidth Usage Daily Report 14
- Top Bandwidth Usage Weekly Report 14

resources, list of changes 23

S

supported platforms 1

T

- testing filters 20
- TotalBytes variable 7
- trends 19
 - Top Bandwidth Usage by Destination 19
 - Top Bandwidth Usage by Hour 19
 - Top Bandwidth Usage by Port 19
 - Top Bandwidth Usage by Source 20
 - Top Bandwidth Usage Events 19
- troubleshooting, installation 4

U

- uninstall foundation 5, 24
- user permissions 5

V

- variable, TotalBytes 7