IP Flow Configuration using Avaya Fabric Orchestrator

account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link "Heritage Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may

contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

Customer acknowledges and agrees that it is responsible for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Contents

Contents

Chapter 1: Introduction

Purpose

This document provides an overview of the *IP Flow Configuration using Avaya Fabric Orchestrator*, NN48100–504 application and how to use it to manage your network.

Related resources

Documentation

The following table lists the documents related to this product. Download the documents from the Avaya Support website at http://support.avaya.com.

Document title	Use this document for:	Audience
Avaya Fabric Orchestrator Solution Description, NN48100–100	Description of each verified reference configuration.	System administrator
Deploying Avaya Fabric Orchestrator, NN48100–101	Installing, configuring, initial administration, and basic maintenance checklist and procedures.	System administrator
Getting Started and Locating the latest software and Release Notes for Avaya Fabric Orchestrator, NN48100–102	Locating the latest software and product release notes.	System administrator
Network Monitoring using Avaya Fabric Orchestrator, NN48100–500	Monitoring the managed objects in AFO.	System administrator
Network Configuration using Avaya Fabric Orchestrator, NN48100–501	Configuring and managing Avaya Enterprise family of devices from discovered network.	System administrator

Table continues…

Document title	Use this document for:	Audience
Bulk Device Configuration Management using Avaya Fabric Orchestrator, NN48100–502	Performing a variety of management tasks across multiple device types using a web-based interface.	System administrator
Virtualization Configuration using Avaya Fabric Orchestrator, NN48100–503	Connecting the vCenter server to AFO, to help the data center administrator to configure the network changes that apply to the data center.	System administrator
IP Flow Configuration using Avaya Fabric Orchestrator, NN48100–504	Collecting and analyzing IP flows from IPFIX-, NetFlow v5-, and NetFlow v9- enabled devices.	System administrator
Administration using Avaya Fabric Orchestrator, NN48100–600	AFO System administration procedures.	System administrator
Avaya Fabric Orchestrator Traps and Trends Reference, NN48100–700	Viewing a list of supported traps and trends.	System administrator
Avaya Fabric Orchestrator Supported Devices, Device MIBs, and Legacy Devices Reference, NN48100–701	Confirming support for devices and MIBs.	System administrator

Training

Ongoing product training is available. For more information or to register, you can access the Web site at http://avaya-learning.com/.

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:

  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.

  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

  😊 **Note:**

  Videos are not available for all products.

Subscribing to e-notifications

Subscribe to e-notifications to receive an email notification when documents are added to or changed on the Avaya Support website.

About this task

You can subscribe to different types of general notifications, for example, Product Correction Notices (PCN), which apply to any product or a specific product. You can also subscribe to specific types of documentation for a specific product, for example, Application & Technical Notes for Virtual Services Platform 7000.

Procedure

1. In an Internet browser, go to https://support.avaya.com.

2. Type your username and password, and then click **Login**.

3. Under **My Information**, select **SSO login Profile**.

4. Click **E-NOTIFICATIONS**.

5. In the GENERAL NOTIFICATIONS area, select the required documentation types, and then click **UPDATE**.

6. Click **OK**.

7. In the PRODUCT NOTIFICATIONS area, click **Add More Products**.

8. Scroll through the list, and then select the product name.

9. Select a release version.

10. Select the check box next to the required documentation types.

11. Click **Submit**.

Searching a documentation collection

On the Avaya Support website, you can download the documentation library for a specific product and software release to perform searches across an entire document collection. For example, you can perform a single, simultaneous search across the collection to quickly find all occurrences of a particular feature. Use this procedure to perform an index search of your documentation collection.

Before you begin

- Download the documentation collection zip file to your local computer.
- You must have Adobe Acrobat or Adobe Reader installed on your computer.

Procedure

1. Extract the document collection zip file into a folder.

2. Navigate to the folder that contains the extracted files and open the file named *<product_name_release>*.pdx.

3. In the Search dialog box, select the option **In the index named *<product_name_release>*.pdx**.

4. Enter a search word or phrase.

5. Select any of the following to narrow your search:

   - Whole Words Only
   - Case-Sensitive
   - Include Bookmarks
   - Include Comments

6. Click **Search**.

   The search results show the number of documents and instances found. You can sort the search results by Relevance Ranking, Date Modified, Filename, or Location. The default is Relevance Ranking.

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Chapter 2: New in this document

IP Flow Configuration using Avaya Fabric Orchestrator, NN48100–504 is a new document for Release 1.0 so all the features are new in this release. See *Avaya Fabric Orchestrator Release Notes* for a list of supported features.

Chapter 3: IP Flow overview

This chapter describes the Avaya Fabric Orchestrator IP Flow (AFO IP Flow) manager user interface and management tools.

User interface

The Avaya Fabric Orchestrator IP Flow user interface has the following tabs:

- Administration — provides the AFO IP Flow management tools.
- Top 10 Views — provides the top 10 reports that show the heaviest traffic patterns.

AFO IP Flow Administration tab

The AFO IP Flow Administration tab provides the tools you require for IP Flow management.

The Administration tab displays the following panes:

- Administration and analysis pane
- Display pane

Administration and analysis pane

The Administration and analysis pane is located on the left side of the user interface, and contains the management tools for AFO IP Flow administration.

- Applications — Applications Manager
- Dashboard — Device Manager Event Viewer
- Packet Capture — Packet Capture Manager
- Thresholds — Thresholds Manager
- Top Reports — Top 10 Views Report
- Trend Analysis — Protocols and applications data

Display pane

The display pane is located on the right side of the user interface. The data on the display pane corresponds with the tool that you select from the Administration and analysis pane.

Comments on this document? infodev@avaya.com

For Administration items, the display pane shows detailed information relevant to the selected item, or it provides a dialog box for entering new or editing existing data. After you select IP Flow, the IP Flow Administration > Dashboard item is the default selection.

Example of the Avaya Fabric Orchestrator IP Flow Administration tab

The following figure shows the Avaya Fabric Orchestrator IP Flow Administration tab user interface.
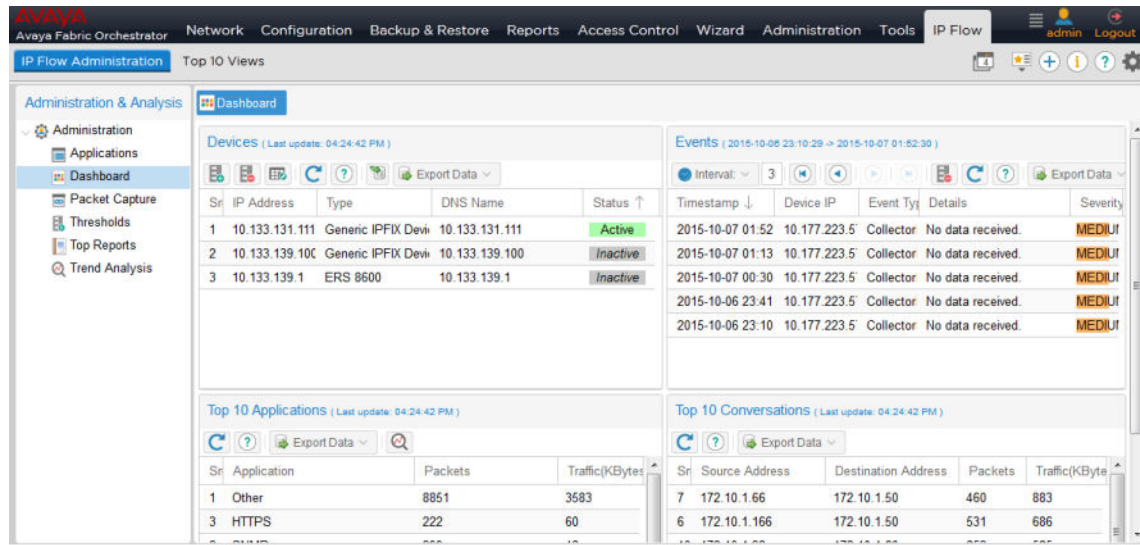
Figure 1: Avaya Fabric Orchestrator IP Flow user interface

For more information about administration management tools, see Management tools on page 16.

AFO IP Flow Top 10 Views tab

The AFO IP Flow Top 10 Views tab shows the top 10 reports with the heaviest IP traffic patterns.

The Top 10 Views tab displays the following panes:

- Administration and analysis pane
- Display pane

Administration and analysis pane

The Administration and analysis pane for the Top 10 Views tab is located on the left side of the user interface and contains a list of reports by type.

- Top 10 Applications — shows the applications, such as SNMP or SSH, that have consumed the most bandwidth.

- Top 10 Conversations — shows the sources and destination addresses that have exchanged the most traffic.

- Top 10 Hosts — shows the hosts, by source and destination, that have sent or received the most traffic.

- Top 10 Ports — shows the ports that have exchanged the most traffic.

- Top 10 Protocols — shows the protols that have caused the most traffic.
- Top 10 Subnets — shows the subnets, by source and destination, that have sent or received the most traffic.

For more information about the Top 10 Views, see Top 10 Views on page 22.

Display pane

The display pane is located on the right side of the user interface. The data on the display pane corresponds with the tool that you select from the Administration and analysis pane.

For the Top 10 Views, the display pane has the following sections.

- In the left section, a table provides details about the Top 10 view you select. Up to 10 items appear; one row for each item.
- In the right section, traffic details appear in chart format.

Example of the AFO IP Flow Top 10 Views user interface

The following figure shows the Avaya Fabric Orchestrator IP Flow Top 10 Views tab user interface.
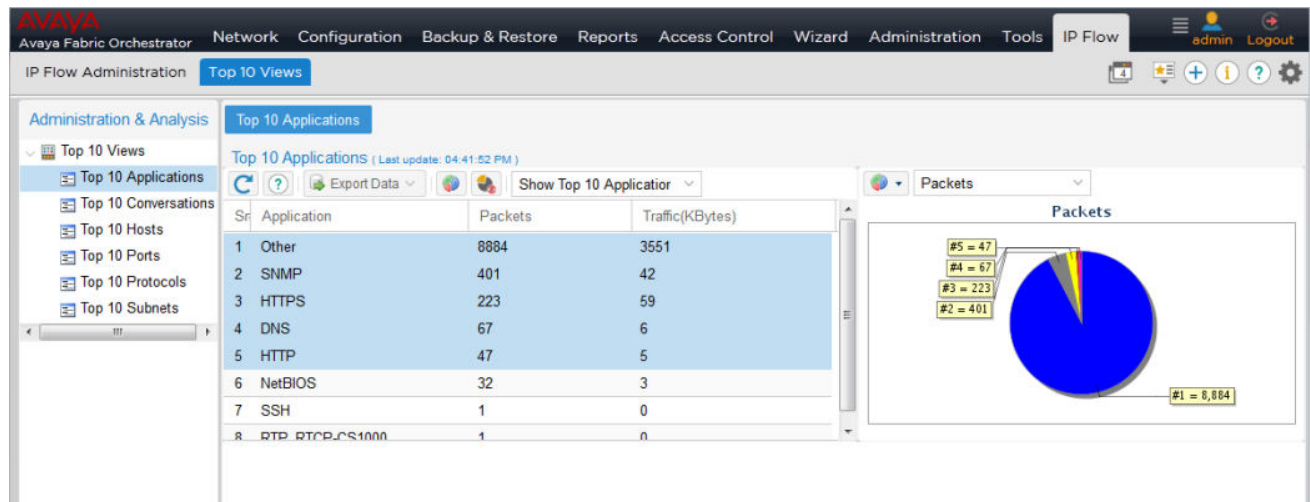
Figure 2: Example of the Avaya Fabric Orchestrator IP Flow Top 10 Views user interface

Management tools

You select the required Avaya Fabric Orchestrator IP Flow management tool from the Administration Analysis pane.

The Administration tools are:

- Applications manager on page 17
- Dashboard on page 18
- Device manager on page 19
- Event viewer on page 19

-
-
-

The Top 10 tools include Top 10 Applications, Top 10 Conversations, Top 10 Hosts, Top 10 Ports, Top 10 Protocols, and Top 10 Subnets. All are covered under

The Configuration tools are:

-
-
-

Applications manager

Avaya Fabric Orchestrator IP Flow supports a predefined list of well known application names together with their standard protocol and port information. An application that does not belong to this list is displayed as Other in the Top 10 Applications report. From the applications manager you can add new applications to the predefined list so that they are identified in the Top 10 Applications report.

You define an application by providing a name and an expression. The name can be up to 64 printable characters. Expressions are composed of keywords and operators.

Figure 3: Add Application

Table 1: Keywords

Keyword	Definition
protocol	the name of the protocol
port	the port used by the protocol

Table 2: Operators

Operator	Operation
ll (two lowercase Ls)	OR
	AND
=	EQUAL TO
~	NOT EQUAL TO
<	GREATER THAN
<=	GREATER THAN OR EQUAL TO
>	LESS THAN
>=	LESS THAN OR EQUAL TO

There is a space between keywords, operators, and values.

After you select Applications from the Administration Analysis, a table of all available applications appears, along with their expressions. Use the default expressions as a guide when formulating your own expressions.

For instructions on using the applications manager, see Applications manager on page 28.

Collector Notification dialog box

The Avaya Fabric Orchestrator IP Flow establishes the maximum number of flows for each minute which Avaya Fabric Orchestrator IP Flow can collect. You use the Collector Notification dialog box to enter an e-mail address to which Avaya Fabric Orchestrator IP Flow sends a message after the number of flows exceeds the maximum.

For instructions on configuring the e-mail address, see Configuring collector information section in *Administration using Avaya Fabric Orchestrator*, NN48100–600.

Dashboard

The Dashboard opens automatically in the Display pane after you launch Avaya Fabric Orchestrator IP Flow. The Dashboard provides access to two management tools, Device Manager and Event Viewer, and two Top 10 Views, Top 10 Applications and Top 10 Conversations. For more information on these tools, see:

- Device manager on page 19
- Event viewer on page 19
- Top 10 Views on page 22

In the case of the Top 10 Views, the primary data table is provided. The Top 10 charted data and the subreports are available after you launch Top 10 Applications or Top 10 Conversations from the Administration Analysis pane.

Device manager

Select Dashboard from the Administration Analysis pane to open the device manager in the display pane.

The device manager provides basic device information in tabular format with each row of the table representing a device. The Avaya Fabric Orchestrator IP Flow collects and analyzes data only from the devices listed in this table. A green (active) status indicates that the Avaya Fabric Orchestrator IP Flow receives data from the device.

IP traffic for each device in the device table is displayed in chart form below the table. After you add or delete a device, the chart updates automatically to reflect the change in the device table.

You can add devices to or delete them from the device table. For instructions on using the device manager, see Device manager on page 31.

Event viewer

Select Dashboard from the Administration Analysis pane to open the Event viewer in the display pane.

The Event viewer lists all events which occurred because thresholds that are reached. You can configure a time interval (start and end time; day, hour, minute, second) which shows only those events which occurred during the interval. The event viewer refreshes automatically every two minutes.

For instructions on using the event viewer, see Event viewer on page 33. To configure thresholds, see Threshold manager on page 35.

Look back time dialog box

Look back time establishes the time interval over which the Avaya Fabric Orchestrator IP Flow analyzes collected data. This is the data which provides the content for all Top 10 Views.

The default look back time is 36 hours. The time resets automatically to the default if the session expires or after you log off the Avaya Fabric Orchestrator IP Flow.

For instructions about setting the look back time, see Configuring the capture duration and look back time section in *Administration using Avaya Fabric Orchestrator*, NN48100–600.

Packet Capture Duration dialog box

After you initiate a packet capture of ERS 8600 flow data, Avaya Fabric Orchestrator IP Flow collects packets for one minute. In low traffic conditions, there may not be enough packets to trigger the packet capture feature on the ERS 8600 and you receive a message indicating that the PCAP

file could not be generated. Use the Packet Capture Duration dialog to increase the capture time in one minute increments up to a maximum of 5 minutes.

For instructions about configuring the packet capture duration, see Configuring the capture duration and look back time section in *Administration using Avaya Fabric Orchestrator*, NN48100–600.

Packet capture manager

Select Packet Capture from the Administration and Analysis pane to open the PCAP dialog box for the packet capture manager in the display pane. You can configure the packet capture on slot/ports of ERS 8600 devices. You use the PCAP dialog box to select the ERS 8600 from which you want to capture packets. After you select the ERS 8600 the Config PCAP dialog box appears which you use to configure the packet capture criteria and then start a capture. Capture results appear in a data table which includes the time of the packet capture, the IP address of the source and destination hosts, the source and destination ports, the protocol, and information which provides insight into the nature of the packet (for example, Echo (ping) reply).

For packet capture operations, the Avaya Fabric Orchestrator IP Flow communicates with the secondary CPU of the ERS 8600. To establish this communication path:

At the ERS 8600

- Ensure that the device has Dual CPU (8692 cards).

- File capture is set to use PCMCIA device.

- PCMCIA cards is inserted in each CPU slot of the device.

- PCAP file size is set to 2MB.

- Assign an IP address to the management port of the secondary CPU.

- Ensure that boot config flag: "ha-cpu" is set to "false".

- Ensure that the FTP service/daemon runs on the secondary CPU.

At the Avaya Fabric Orchestrator IP Flow

- AFO IP Flow must have collecting some traffic data from the same ERS 8600 device before a PCAP operation can be invoked for it.

- Use the Device and Server Credentials Editor to configure the SNMP (v1 or v3) and FTP credentials for all ERS 8600s from which you want to capture packets. To launch the Device and Server Credentials Editor, click Credentials in the "Administration & Analysis" pane. See Avaya Unified Communications Management Fundamentals (NN48014-100), for more information.

Verification with JDM (Java Device Manager)

IF you have a JDM application installation, you can open JDM with the ERS 8600 device and go to **Edit** > **Diagnostics** > **PCAP** > **PCapStat** to view the PacketCapacityCount value with a periodic refresh.

If the PacketCapacityCount value reaches 217 within the given time frame (as specified in AFO IP Flow user interface), then the ERS device generates a PCAP file. You can capture transmitted packets only, received packets only, or both.

The packet capture manager creates a buffer on the selected ERS 8600 for the captured packets. The buffer is set at 2 MB. After the buffer is filled, the Avaya Fabric Orchestrator IP Flow analyzes the data and displays the results in the Avaya Fabric Orchestrator IP Flow packet capture window. Avaya Fabric Orchestrator IP Flow also saves the data to a file on the ERS 8600 PCMCIA card. On subsequent captures, the buffer and the file on the PCMCIA card are overwritten.

In the default configuration, the packet capture process continues for one minute. In low traffic periods, you can extend this time.

For instructions about using the packet manager, see Using packet capture manager to capture packets. In the default configuration, the packet capture process continues for one minute. In low traffic periods, you can extend this time. See Packet Capture Duration dialog box for more information.

Thresholds manager

Select Thresholds from the Administration and Analysis pane to open the thresholds manager in the display pane. A list of all thresholds added to the Avaya Fabric Orchestrator IP Flow appears. There are no predefined thresholds.

A threshold defines a traffic flow which, after exceeded, triggers an event. A threshold is set on a per device per protocol basis. If you delete a device that has a threshold, the threshold disables. The threshold is reenabled if you add the device again.

A threshold can be any percent of total traffic from 1 to 999, and can be for a collection interval of 2, 3, 5, 10, 15, 20, or 30 minutes. A severity of low, medium, or high can be assigned to the event.

The event can be an SNMP trap, an e-mail message, or a packet capture.

- SNMP trap event — The IP address of the trap receiver and the read community are required to configure an SNMP trap event.

- e-mail message event — It requires an e-mail address to configure an e-mail message event. The SMTP server configuration is also required for an e-mail message event. Use the AFO global preferences to configure the SMTP server. You do not have to specify the same e-mail address for every threshold, but every e-mail address uses the same SMTP server.

- packet capture event — It requires an e-mail address to configure a packet capture event, as well as the parameters needed to configure the required packet capture itself (for more information, see Packet capture manager on page 20). After the packet capture event triggers, the packet capture runs. The captured data is sent to the specified e-mail address. The packet capture event must be set to 5 minutes or greater otherwise an error is generated.

You can add, edit, delete, and find thresholds. You can also enable or disable thresholds, refresh the thresholds table, and export the data to the following formats: PDF, CSV, SML, and HTML. For more information about using the thresholds manager, see Threshold manager on page 35.

Top Reports

You can generate a top views report, with content that you select, between two host IPv4 addresses for a specific start date and time and end date and time.

Use the Top Reports to obtain similar information to the Top 10 views but customized to your needs. You can also generate a report for events or specific conversations.

AFO generates the report as a PDF file.

Trend Analysis

With the AFO IP Flow trend analysis management tool, you can view charts with the latest trends based on protocols and applications. Trend analysis is an effective tool used for capacity planning and troubleshooting.

Trend analysis can help you spot a pattern for bandwidth use in your network in terms of which protocol or application is consuming the most bandwidth, and at what peak time.

Top 10 Views

Top 10 Views is a collection of reports that shows your heaviest traffic patterns. After you select one of the Top 10 Views from the Top 10 Views tab Administration and Analysis pane, Avaya Fabric Orchestrator IP Flow analyzes the collected IP traffic data for an interval of time, which starts after you select the view and extends backward by the amount specified in the Look Back Time dialog box. After the analysis is complete, the resulting report appears in the display pane.

You can generate a report by application (Top 10 Applications), conversation (Top 10 Conversations), host (Top 10 Hosts), port (Top 10 Ports), protocol (Top 10 Protocols), or subnet (Top 10 Subnets).

All Top 10 reports appear in the same way. Taking the Top 10 Protocols as an example, this report shows up to 10 of the most heavily used protocols. The traffic appears in tabular form, with one row for each protocol. If there are less than 10 protocols in the table, then less than 10 active protocols were in the analyzed data. The top five protocols are selected (highlighted) automatically after the report opens. The traffic for the selected protocols appears in chart format to the right of the report.

The Top 10 Applications report coordinates with the Applications manager. If your Top 10 Applications report has "Other" as one of the applications, that is because the application is not one of the ones supported in the default configuration. You can use the applications manager to add applications to Avaya Fabric Orchestrator IP Flow. These applications are then available for display in the Top 10 Applications report. See Applications manager on page 17 for more information.

In the case of the Top 10 Hosts, two sets of data appear: the top 10 source hosts and the top 10 destination hosts. Similarly, for Top 10 Subnets, the top 10 source and destination subnets appear.

You can use Ctrl+left-click to change the selected rows. Refresh the chart to update it to reflect the new selection. You can change the format of the chart (pie or bar) and you can change the way in which the traffic measures in the chart (by bytes or by packets).

If you right-click a row in a Top 10 Applications, Top 10 Conversations, Top 10 Hosts, or Top 10 Protocols table, a list of subreports appears. These subreports present data for the selected row. For example, if you right-click the TCP row from the Top 10 Protocols table, the additional reports are Top 10 Src-Hosts, Top 10 Dst-Hosts, Top 10 Devices, and Top 10 Conversations. If you select Top 10 Dst-Hosts, then another table appears. This table shows the destination hosts with the heaviest TCP traffic.

For instructions on using Top 10 Views, see

Chapter 4: Common icons and procedures

The following icons and procedures are common to many Avaya Fabric Orchestrator IP Flow (AFO IP Flow) activities.

Icons

The following table describes icons in Avaya Fabric Orchestrator IP Flow. Each icon initiates a specific action.

Table 3: Icons

Icon	Action
	Adds an item. The item depends on the management tool. For example, if you use the application manager, this button opens the Add Application dialog box. If you use the threshold manager, this button opens the Add Threshold dialog box.
	Deletes the selected item.
	Searches for an application or threshold.
	Enable or disable an application or threshold.
	Displays the currently running applications.
	Starts an editing session for the selected item. After you start an editing session for an item, the dialog box is the same as the one used to add the item except that the editing dialog box contains the information specified after you added the item. Editing items involves modifying that information to reflect the new specification.

Table continues…

Icon	Action
	For information on the dialog box, see the specific management tool.
↻	Refreshes the data presented in a table or chart.
?	Launches the on-line help.
Export Data ⌄	Lists formats for exported data. For more information, see Exporting data on page 26.
	On the Device dashboard, imports devices from the monitoring server.
	Shows chart, pie chart or bar chart.
	Hides a Top 10 View chart to expand the Top 10 View table to the full width of the display pane.
<<	For a Top 10 View chart, << restores a chart which was previously hidden. For the Administration Analysis pane, << hides the pane.
>>	For the Administration Analysis pane, >> restores a pane which was previously hidden.

Expanding or collapsing the Administration and Analysis tree

About this task

Use this procedure to expand or collapse the Administration Analysis tree or a branch.

Procedure

1. From the Avaya Fabric Orchestrator IP Flow Administration & Analysis pane click the arrow to the left of the item icon.

   The branch expands after the arrow is pointing to the right.

2. Click the arrow again to collapse the view.

Opening a management tool

About this task

Use this procedure to open a management tool.

Procedure

From the Administration branch of the Administration & Analysis pane, click a tool.

The tool appears in the display pane. A tab with the tool name appears at the top of the display pane.

Closing a management tool

About this task

Use this procedure to close a management tool.

Procedure

1. In the display pane, if the management tool you want to close is not in the foreground, click the tab for the management tool.

2. Click the x in the right corner of the management tool tab.

Sorting data in a table

About this task

Use this procedure to sort table data.

Procedure

Click the heading of the column that you want to sort.

The arrow in the title indicates if the data is sorted in ascending or descending order.

OR

Right-click the heading of the column to sort and select the sort options.

You can select ascending or descending order and you can select which columns to display.

Exporting data

About this task

Use this procedure to export data from the Avaya Fabric Orchestrator IP Flow database. You can save or view exported data in PDF, CSV, XML, or HTML format.

Procedure

1. With the required data visible in the display pane, click **Export Data**.

   The Export Data list appears.

2. From the Export Data list, select the required format: PDF, CSV, XML, or HTML.

   A message appears prompting you to open or save the file.

3. Click **SAVE** to save the file.

   The file saves to the root level (the desktop on Windows) of your local computer.

   OR

   Click **Open** to open the file immediately.

   The data appears in the requested file format.

Deleting text

About this task

Use this procedure to delete text from fields in a dialog box or window. This procedure deletes all text.

Procedure

Click **Reset**.

All fields previously containing text are now blank.

Changing the displayed columns

About this task

Use this procedure to change the columns displayed in a table.

Procedure

1. Right-click a heading in the table.

2. Move the cursor to **Columns**.

3. From the list of columns, click the heading or selection box to hide a column, or to reselect a column that was hidden previously.

   A green check mark in the selection box indicates that the column is selected.

Chapter 5: Managing IP Flow

The following sections provide the procedures for managing and configuring AFO IP Flow.

Applications manager

Applications manager procedures in this module include:

Adding an application

About this task

Use this procedure to add an application to Avaya Fabric Orchestrator IP Flow (AFO IP Flow).

Prerequisites:

- Determine a name for the application which you want to add.
- Develop the expression for the application.

Procedure

1. From the AFO menu bar, select **IP Flow** > **IP Flow Administration**.

2. From the IP Flow Administration & Analysis pane, select **Administration** > **Applications**.

3. Click the plus sign (**+**) in the applications manager menu bar.

4. In the Name field, type the name of the application.

5. In the Expression field, type the expression for the application.

6. Click **Save**.

   OR

Click **Reset** to reset the fields to their default values.

Variable Definitions

Variable	Value
Name	Up to 64 printable characters
Expression	Composed of keywords (protocol, port) and operators (ll, , =, ~, >, >=. <, <=)

Deleting an application

About this task

Use this procedure to delete an application.

Procedure

1. From the AFO menu bar, select **IP Flow** > **IP Flow Administration**.

2. From the IP Flow Administration & Analysis pane, select **Administration** > **Applications**.

3. In the applications table, click in the row of the application you want to delete.

   To delete more than one application, hold down the **Ctrl** key and click the additional rows.

4. Click the minus sign (**-**) in the application manager menu bar.

5. Click **Yes** when prompted to confirm the deletion.

   The Avaya Fabric Orchestrator IP Flow deletes the application from the database and the corresponding row is removed from the applications table.

Editing an application

About this task

Use this procedure to edit an existing application.

Prerequisites:

- It requires familiarity with <u>Adding an application</u> on page 28 for this procedure.

Procedure

1. From the AFO menu bar, select **IP Flow** > **IP Flow Administration**.

2. From the Administration & Analysis pane, select **Administration** > **Applications**.

3. In the applications table, do one of the following:

   - Double-click in the row of the application you want to edit.

     OR

   - Click in the row of the application you want to edit and click **Edit**.

4. Change the Name or the Expression as needed to meet your new requirements.

5. Click **Save**.

    OR

    Click **Reset** to reset the fields to their default values.

Variable Definitions

Variable	Value
Name	Up to 64 printable characters
Expression	Composed of keywords (protocol, port) and operators (ll, , =, ~, >, >=. <, <=)

Locating an application

Use this procedure to locate a specific application within the list of applications.

Procedure

1. From the AFO menu bar, select **IP Flow** > **IP Flow Administration**.

2. From the Administration & Analysis pane, select **Administration** > **Applications**.

3. Click **Find Application(s)**.

4. In the Find Application dialog box, enter search information.

    a. Find By — Select expression, or name.

    b. Keyword — Enter a keyword associated with the application expression or name

    c. Criteria — Select Contains or Exact Match to describe the keyword entry.

5. Click **Find**.

Enabling or disabling an application

Use this procedure to enable or disable an application.

Procedure

1. From the AFO menu bar, select **IP Flow** > **IP Flow Administration**.

2. From the Administration & Analysis pane, select **Administration** > **Applications**.

3. In the Applications display pane, select an application.

4. Click **Enable/Disable Application**.

5. When prompted to confirm you really want to disable the application, click **Yes**.

Viewing active applications

Use this procedure to view the list of applications that are currently active in the network.

Procedure

1. From the AFO menu bar, select **IP Flow** > **IP Flow Administration**.

2. From the Administration & Analysis pane, select **Administration** > **Applications**.

3. Click **Show Currently Running Applications**.

Device manager

Device manager procedures in this module include:

Adding a device

About this task

Use this procedure to add a device to the Avaya Fabric Orchestrator IP Flow (AFO IP Flow) database.

Based on your license, you can add up to ten devices.

Procedure

1. From the AFO menu bar, select **IP Flow** > **IP Flow Administration**.

2. From the Administration & Analysis pane, select **Administration** > **Dashboard**.

3. In the Devices panel, click the plus sign (**+**).

4. In the Device IP field, enter the IP address of the device.

5. In the Type field, select the type of device.

6. (Optional) In the DNS Name field, enter the DNS name of the device.

7. Click **Save**.

Variable Definitions

Table 4: Variable definitions for adding a device

Variable	Value
DNS Name	Domain Name Server. Optional field.
Device IP	IP address. Mandatory field.
Type	Device type. Mandatory field.

Deleting a device

About this task

Use this procedure to delete a device.

Procedure

1. From the AFO menu bar, select **IP Flow** > **IP Flow Administration**.

2. From the Administration & Analysis pane, select **Administration** > **Dashboard**.

3. In the device table on the Dashboard, click on the row of the device you want to delete.

   To delete more than one device, hold down the **Ctrl** key and click the additional rows.

4. Click the minus sign (**-**) in the device manager menu bar.

5. Click **Yes** when prompted to confirm the deletion.

Editing a device

About this task

Use this procedure to edit an existing device.

🛈 **Important:**

You cannot change the IP address or device type. To do either, delete the device (Deleting a device on page 32) and add a new device (Adding a device on page 31).

Prerequisites:

• It requires familiarity with Adding a device on page 31 for this procedure.

Procedure

1. From the AFO menu bar, select **IP Flow** > **IP Flow Administration**.

2. From the Administration & Analysis pane, select **Administration** > **Dashboard**.

3. From the Dashboard, perform one of the following in the device table:

   • Select the row that you want to edit, then click on **Edit Device**.

   • Or, double-click on the row of the device you want to edit.

4. In the Edit Device dialog box, change the DNS Name.

5. Click **Save**.

   Or

   Click **Reset** to reset the fields to their default values.

Importing devices from the AFO Monitoring server

Use this procedure to import devices from the AFO Monitoring server.

Procedure

1. From the AFO menu bar, select **IP Flow** > **IP Flow Administration**.

2. From the Administration & Analysis pane, select **Administration** > **Dashboard**.

3. From the Devices panel, click **Import Devices from Monitoring Server**.

4. When prompted to confirm you really want to import devices from the Monitoring Server, click **Yes**.

Event viewer

Event viewer procedures include:

• [Displaying events within a time range](#) on page 33

• [Editing the events time range](#) on page 34

Displaying events within a time range

About this task

Use this procedure to display the events that occurred in your network within a specific time range.

Procedure

1. From the AFO menu bar, select **IP Flow** > **IP Flow Administration**.

2. From the Administration & Analysis pane, select **Administration** > **Dashboard**.

3. With the Dashboard visible, the event viewer provides a list of events which occurred during the time interval selected, which is displayed above the list.

Editing the events time range

About this task

Use this procedure to configure a time interval which shows only those events which occurred during the interval.

Procedure

1. From the AFO menu bar, select **IP Flow** > **IP Flow Administration**.

2. From the Administration & Analysis pane, select **Administration** > **Dashboard**.

3. On the Events viewer menu, click the **Interval** down arrow.

4. Select a time interval to display events for that period.

   - 1h

   - 3h

   - 6h

   - 9h

5. From the Events panel, click on one of the four arrows to view the first, previous, next or last interval.

   Events that occurred during the selected time interval appear.

6. To Save, click **Export Data**, and select a format from the drop down menu: **PDF**, **CSV**, **XML**, or **HTML**.

7. To save the file, click **SAVE**.

   The file saves to the root level (the desktop on Windows) of your local computer.

   OR

   Click **Open** to open the file immediately.

Using packet capture manager to capture packets

About this task

Use this procedure to capture packets on an ERS 8600 device.

Before you begin

You must configure SNMP and FTP credentials for the device before you can capture packets from the device.

Procedure

1. From the AFO menu bar, select **IP Flow** > **IP Flow Administration**.

2. From the Administration & Analysis pane, select **Administration** > **Packet Capture**.

3. Click **Packet Capture**.

4. From the Device IP list, select the IP address of the device from which you want to capture packets.

5. Click **OK**.

   The Configure PCAP dialog box appears.

6. From the Slot/Port list, select the slot/port combination for which you want to capture the packets.

7. From the Mode list, select the packets to capture: transmitted, received, or both.

8. Click **Start Capture** to start capturing packets.

   The Avaya Fabric Orchestrator IP Flow (AFO IP Flow) collects the packets until the buffer is full, analyzes the data, and displays it in a table below the Configure PCAP dialog box.

   OR

   Click **Reset** to reset the fields to the default values.

Threshold manager

Threshold manager procedures include:

Adding a threshold to a device

About this task

Use this procedure to add a threshold.

Prerequisites:

- You must add a device to the Avaya Fabric Orchestrator IP Flow (AFO IP Flow) database before you can add a threshold. See Adding a device on page 31.
- To use the Email notification type, you must configure the SMTP server as part of AFO global preferences. For more information, see *Administration using Avaya Fabric Orchestrator*, NN48100–600.

Procedure

1. From the AFO menu bar, select **IP Flow** > **IP Flow Administration**.

2. From the Administration & Analysis pane, select **Administration** > **Thresholds**.

3. Click the plus sign (**+**) to open the Add Threshold dialog box.

4. In the Name field, enter a name for the threshold.

5. In the Device field, select the device to monitor.

6. In the Description field, enter a short description of the threshold.

7. In the Protocol/Application field, select the protocol or application to analyze.

8. In the Traffic Utilization (%) field, enter the percentage of traffic utilization which, if exceeded, generates an event.

9. From the Time (minutes) list, select the time interval over which the threshold manager collects data.

10. From the Severity list, select the priority level of the event notification.

11. In the Event field, do one of the following:

    - Select **Email** to send an e-mail message after the event occurs.
    - Select **Trap** to send a trap after the event occurs.
    - Select **Syslog** to log a message to a Syslog server.
    - Select **Pcap** to initiate a packet capture after the event occurs.

12. Click **Configure event**.

13. Do one of the following:

    - If you selected Email in step 11 on page 36, the Mail Address dialog box appears. Go to step 14 on page 36.
    - If you selected Trap in step 11 on page 36, the Add Trap dialog box appears. Go to step 16 on page 37.
    - If you select Syslog in step 11 on page 36, the Add Syslog Receiver dialog box appears. Go to step 19 on page 37.
    - If you selected Pcap in step 11 on page 36, the Add Pcap dialog box appears. Go to step 21 on page 37.

14. In the To field, type the e-mail address(es) to which you want notifications sent.

    For multiple addresses, insert a comma between each address.

15. Go to 24 on page 37.

16. In the Trap Receiver field, type the name or IP address of the trap receiver.

17. In the Read Community field, type the community string associated with the trap receiver.

18. Go to

19. In the Syslog Receiver Address field, type the IP address for the Syslog server.

20. In the Syslog Port field, type the UDP port number used to communicate with the Syslog server.

21. In the To field, type the e-mail address(es) to which you want to send the captured data.

    For multiple addresses, insert a comma between each address.

22. From the Slot/Port list, select the slot/ port combination for which you want to capture the packets.

23. From the Mode list, select the packets to capture: transmitted, received, or both.

24. Click **Apply**.

    The dialog box closes.

25. Click **Save**.

    A row for the new threshold is added to the thresholds table.

Variable Definitions

Variable	Value
Name	Specifies the name of the threshold. This is a mandatory field.
Device	Specifies the IP address of the device.
Description	Specifies the threshold description. Maximum of 255 characters. .
Threshold Type	The threshold type of application or protocol.
Protocol/Application	Specifies the application or protocol for the threshold event. This is a mandatory field.
Traffic Utilization (%)	Specifies the condition for the threshold. This is a mandatory field.
Time (minutes)	Specifies the time interval for threshold to monitor the utilization. This is a mandatory field.
Severity	Specifies a user assigned severity level: High, Medium, Low. This is a mandatory field.
Event	Specifies the event type: . • Email • Trap • Syslog • Pcap

Table continues…

Variable	Value
	This is a mandatory field. Click **Configure event** to provide configuration details.

Deleting a threshold

About this task

Use this procedure to delete a threshold.

Procedure

1. From the AFO menu bar, select **IP Flow** > **IP Flow Administration**.

2. From the Administration & Analysis pane, select **Administration** > **Thresholds**.

3. In the threshold table, click in the row of the threshold you want to delete.

   To delete more than one threshold, hold down the **Ctrl** key and click the additional rows.

4. Click the minus sign (**-**).

5. Click **Yes** to confirm the deletion.

   The Avaya Fabric Orchestrator IP Flow deletes the threshold from the database and the corresponding row is removed from the threshold table.

Editing a threshold

About this task

Use this procedure to edit a threshold previously added to the Avaya Fabric Orchestrator IP Flow database.

> ### Important:
> You cannot change the name of a threshold or the device to which the threshold is applied. To do either, delete the threshold (Deleting a threshold on page 38) and add a new threshold (Adding a threshold to a device on page 35).

Prerequisites:

- The user must be familiar with Adding a threshold to a device on page 35 for this procedure.

Procedure

1. From the AFO menu bar, select **IP Flow** > **IP Flow Administration**.

2. From the Administration & Analysis pane, select **Administration** > **Thresholds**.

3. In the threshold table, do one of the following

   - Double-click in the row of the threshold you want to edit.

- Click in the row of the threshold you want to edit and click **Edit** in the threshold manager menu bar.

4. Change the threshold parameters as needed to meet your new requirements.

5. Click **Save** to save the changes and close the dialog box.

   OR

   Click **Reset** to reset the fields to their default values.

Variable Definitions

Variable	Value
Name	Specifies the name of the threshold.
	You cannot edit this field for an active threshold.
Device	Specifies the IP address of the device.
	You cannot edit this field for an active threshold.
Description	Specifies the threshold description. Maximum of 255 characters. .
Threshold Type	The threshold type of application or protocol.
Protocol/Application	Specifies the application or protocol for the threshold event.
	This is a mandatory field.
Traffic Utilization (%)	Specifies the condition for the threshold.
Time (minutes)	Specifies the time interval for threshold to monitor the utilization.
Severity	Specifies a user assigned severity level: High, Medium, Low.
Event	Specifies the event type: .
	• Email
	• Trap
	• Syslog
	• Pcap
	Click **Configure event** to provide configuration details.

Finding a threshold

About this task

Use this procedure to find a threshold in the threshold table.

Procedure

1. From the AFO menu bar, select **IP Flow** > **IP Flow Administration**.

2. From the Administration & Analysis pane, select **Administration** > **Thresholds**.

3. From the threshold manager menu bar, click **Find**.

4. In the Find By field, select the search parameter: Name, Device IP, or Description.

5. In the Keyword field, enter the value of the parameter.

6. In the Criteria field, select the search constraints: Exact Match or Contains .

7. Do one of the following:

   • Click **Find** to initiate the search.

   The dialog box closes and the threshold table is updated so that all thresholds meeting the search definition are highlighted. If there are no matches, an information message appears.

   • Click **Close** to close the dialog box without executing a search.

Variable Definitions

Variable	Value
Find By	You can search on the name of the threshold (Name), the IP address of the device to which the threshold applies (Device IP), or the description of the threshold (Description). The Name, Device IP, and Description correspond to the columns in the threshold table.
Keyword	Keyword corresponds to the value of the Name, Device IP, or Threshold as it appears in the threshold table.
Criteria	Exact Match returns thresholds where the data in the table matches the keyword exactly. Contains returns thresholds where the data in the table contains the keyword but may contain other data.

Top views reports

You can generate a top views report, with content that you select, between two host IPv4 addresses for a specific start date and time and end date and time.

Generating a top views report

Use this procedure to generate a report of the top views between two host IPv4 addresses for a specific date and time.

Procedure

1. From the AFO menu bar, select **IP Flow** > **IP Flow Administration**.

2. From the Administration & Analysis pane, select **Administration** > **Top Reports**.

3. In the Select Date and Time section, from the drop down menus, perform the following actions:

   a. Select the Start Date.

    b. Select the End Date.

    c. Select the Start Time.

    d. Select the End Time.

4. From the Select Report Content section, select the content for your report. You can select one or more of the following options:

- Applications
- Protocols
- All Conversations
- Hosts
- Device Ports
- Specific Conversations
- Events
- Subnets

5. In the Host IPs field, enter two IPv4 addresses.

6. Click **Generate Report**.

Trend analysis data

With the AFO IP Flow trend analysis management tool, you can view charts with the latest trends based on protocols and applications. Trend analysis is an effective tool used for capacity planning and troubleshooting.

Analyzing trends

AFO IP Flow provides two default trend analysis:

- for Top 10 Applications
- for Top 10 Protocols

Before you begin

- To successfully plan capacity, you must use the AFO IP Flow trend-analysis tool on a long term basis. After you use the trending tool against the AFO IP Flow server, you affect the performance of the server. If you use trending as a troubleshooting tool, the performance of the server is less affected because of the short duration of the monitoring session. But if you plan to use trending as a long-term capacity-planning tool, you must consider the impact it may have on the AFO IP Flow server.

- Trending requires the use of memory, and CPU time. Therefore, you must ensure that the AFO IP Flow server is standard and adequate.

- To limit any negative performance effects on the AFO IP Flow server process, limit the sampling rate. For a medium-term collection aimed at trend analysis, use a sampling rate of Minute. For a long-term collection, or if the AFO IP Flow server exists across a slow WAN link or has low performance issues, increase the sampling rate to Hour.

About this task

This procedure describes how to perform a trend analysis in Avaya Fabric Orchestrator IP Flow.

Procedure

1. From the AFO menu bar, select **IP Flow** > **IP Flow Administration**.

2. From the Administration & Analysis pane, select **Administration** > **Trend Analysis**.

3. ✱ **Note:**

   You can analyze a trend for a specific protocol or application or for all protocols and applications. You can select appropriate option in Protocol and Application fields.

   Select the trending data that you want to analyze, Protocols, or Applications You can perform the procedure for both trending data options.

4. In the Resolution drop down menu, select a resolution time.

   - SECOND
   - MINUTE
   - HOUR

5. In the View drop down menu, select the trending time period.

   - Last 1 Hour
   - Last 3 Hours
   - Last 6 Hours
   - Last 9 Hours
   - Last 12 Hours
   - All Data

6. If you are analyzing the protocols trending data, then in the Protocol drop down menu, select a protocol.

   - All
   - UDP
   - TCP

7. If you are analyzing the applications trending data, then in the Application drop down menu, select an application.

   - All
   - HTTP
   - HTTPS

- NetBIOS
- Other
- SNMP

8. In the Device drop down menu, select a device.

- All
- IP address for a specific device

9. Click **Refresh Protocol Trending Graph**, or click **Refresh Application Trending Graph**.

10. To select trending sampling interval, click the Resolution selection box and select appropriate interval (i.e. Second, Minute or Hour).

> ✳ **Note:**
>
> Please note that in current release you will not be able to customize trending charts but can save the trend-analyzed data in PDF, XML, CSV or HTML format.

11. (Optional) To save the trend-analyzed data, click **Export Data**, and select the format you want to save the data to.

- PDF
- XML
- CSV
- HTML

Top 10 Views reports

Procedures for the Top 10 Views include:

Displaying a Top 10 report

About this task

Use this procedure to display a report on the Top 10 Applications, Top 10 Conversations, Top 10 Hosts, Top 10 Ports, Top 10 Protocols, or Top 10 Subnets.

Procedure

1. From the AFO menu bar, select **IP Flow** > **Top 10 Views**.

2. From the Administration & Analysis pane, expand Top 10 Views, and perform one of the following actions:

   • To display a Top 10 Applications report, click **Top 10 Applications**.

   • To display a Top 10 Conversations report, click **Top 10 Conversations**.

   • To display a Top 10 Hosts report, click **Top 10 Hosts**.

   • To display a Top 10 Ports report, click **Top 10 Ports**.

   • To display a Top 10 Protocols report, click **Top 10 Protocols**.

   • To display a Top 10 Subnets report, click **Top 10 Subnets**.

Configuring Top 10 Applications View

By default, AFO IP Flow shows the top most 10 applications which consume the higher network bandwidth in an increasing order of traffic usage. But user can choose a specific set of applications in Top 10 Applications view even if these applications may not consume sufficient amount of network traffic.

About this task

Use this procedure to choose your own set of applications for monitoring. This ability provides an immense flexibility in network application monitoring.

Once you specify the set of applications, same set of applications is listed in AFO IP Flow dashboard. You can bring back the default set of Top 10 Applications by clicking on Show Top 10 Applications option in the selection box.

Procedure

1. From the AFO home page, select **IP Flow** > **Top 10 Views**.

2. From the Administration and Analysis pane, select **Top 10 Views** > **Top 10 Applications**.

3. From the drop down menu in the display pane, select **Choose Top 10 Applications**.
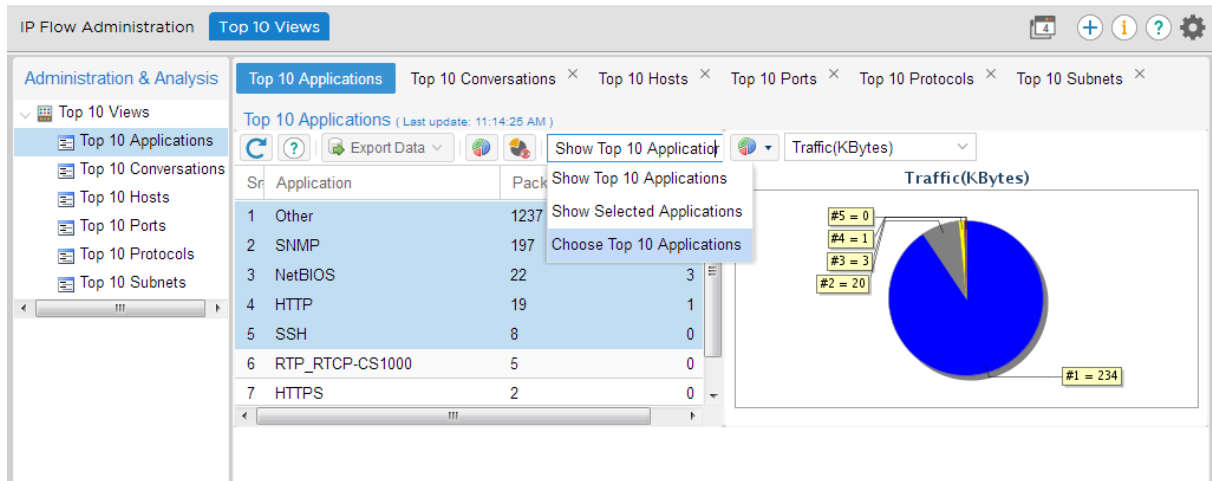
The Choose Your Top 10 Applications window displays.

4. Right click on an application and select or deselect it using the pop-up window options.

You can use **Ctrl** or **Shift** key to make multiple selections.

In the dialog box, application names are always listed in an increasing order of their traffic consumption(usage), 1 being the top most consumer. To identify the top consumers easily, the first 10 application names are always rendered in bold, green font.

If any of the top consuming entries are removed, the appropriate **Monitor** column(s) will display a value of **No** and be rendered in bold, red font. This is to indicate that top consuming application names are now removed from user view. Similarly, if you choose a non-top consuming application to monitor, the related **Monitor** column displays a value of **Yes** and be rendered in bold, red font.

5. **(Optional)** Click **Set to Default** to bring back the default Top Application entries.

6. Click **Save** to save the changes.

7. Click **Close** to return to the Top 10 Applications window.

Displaying a Top 10 Applications subreport

About this task

Use this procedure to display a subreport from the Top 10 Applications report.

Procedure

1. From the AFO home page, select **IP Flow** > **Top 10 Views**.

2. From the Administration and Analysis pane, select **Top 10 Views** > **Top 10 Applications**.

3. Right-click the row of the application for which you want a subreport.

4. In the subreport list, select a subreport.

Displaying a Top 10 Conversations subreport

About this task

Use this procedure to display a subreport from the Top 10 Conversations report.

Procedure

1. From the AFO home page, select **IP Flow** > **Top 10 Views**.

2. From the Administration and Analysis pane, select **Top 10 Views** > **Top 10 Conversations**.

3. Right-click the row of the conversation for which you want a subreport.

4. From the subreport list, select a subreport.

Displaying a Top 10 Hosts subreport

About this task

Use this procedure to display a subreport from the Top 10 Hosts report.

Procedure

1. From the AFO home page, select **IP Flow** > **Top 10 Views**.

2. From the Administration and Analysis pane, select **Top 10 Views** > **Top 10 Hosts**.

3. Right-click the row of the host for which you want a subreport.

4. From the subreport list, select a subreport.

Displaying a Top 10 Ports subreport

About this task

Use this procedure to display the subreport from the Top 10 Ports report.

Procedure

1. From the AFO home page, select **IP Flow** > **Top 10 Views**.

2. From the Administration & Analysis pane, **Top 10 Views** > **Top 10 Ports**.

3. Right-click the row of the port for which you want a subreport.

4. From the subreport list, select a subreport.

Displaying a Top 10 Protocols subreport

About this task

Use this procedure to display the subreport from the Top 10 Protocols report.

Procedure

1. From the AFO home page, select **IP Flow** > **Top 10 Views**.
2. From the Administration and Analysis pane, select **Top 10 Views** > **Top 10 Protocols**.
3. Right-click the row of the protocol for which you want a subreport.
4. From the subreport list, select a subreport.

Displaying a Top 10 Subnets subreport

About this task

Use this procedure to display a subreport from the Top 10 Subnets report.

Procedure

1. From the AFO home page, select **IP Flow** > **Top 10 Views**.
2. From the Administration and Analysis pane, select **Top 10 Views** > **Top 10 Subnets**.
3. Right-click the row of the host for which you want a subreport.
4. From the subreport list, select a subreport.

Expanding a subreport

About this task

Use this procedure to expand a minimized report linked to a Top 10 View.

Procedure

On the selected report, click the Expand arrow.

The report expands.

Minimizing a subreport

About this task

Use this procedure to minimize a subreport.

Procedure

From the subreport, click the Collapse arrow.

The subreport is minimized.

Closing a subreport

About this task

Use this procedure to close a subreport.

Procedure

In the subreport section, click the **x** in the right-hand corner.