ExtremeManagement™

IP Flow Configuration using Extreme Fabric Orchestrator

Release 1.2
NN48100-504
Issue 03.01
December 2017

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Extreme Networks, Inc. assumes no liability for any errors. Extreme Networks, Inc. reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Extreme Networks shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Extreme Networks. End User agrees to indemnify and hold harmless Extreme Networks, Extreme Networks’ agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Extreme Networks is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Extreme Networks. Extreme Networks is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Extreme Networks does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Extreme Networks provides a limited warranty on Extreme Networks hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Extreme Networks’ standard warranty language, as well as information regarding support for this product while under warranty is available to Extreme Networks customers and other parties through the Extreme Networks Support website: http://www.extremenetworks.com/support under the link ““Policies” or such successor site as designated by Extreme Networks. Please note that if You acquired the product(s) from an authorized Extreme Networks Channel Partner outside of the United States and Canada, the warranty is provided to You by said Extreme Networks Channel Partner and not by Extreme Networks.

“Hosted Service” means an Extreme Networks hosted service subscription that You acquire from either Extreme Networks or an authorized Extreme Networks Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Extreme Networks or Extreme Networks Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN EXTREME NETWORKS HOSTED SERVICE SUBSCRIPTION FROM EXTREME NETWORKS OR AN EXTREME NETWORKS CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE EXTREME NETWORKS WEBSITE, https://extremeportal.force.com OR SUCH SUCCESSOR SITE AS DESIGNATED BY EXTREME NETWORKS, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE EXTREME NETWORKS WEBSITE, https://extremeportal.force.com OR SUCH SUCCESSOR SITE AS DESIGNATED BY EXTREME NETWORKS, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS EXTREME NETWORKS SOFTWARE, PURCHASED FROM EXTREME NETWORKS INC., ANY EXTREME NETWORKS AFFILIATE, OR AN EXTREME NETWORKS CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH EXTREME NETWORKS OR AN EXTREME NETWORKS CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY EXTREME NETWORKS IN WRITING, EXTREME NETWORKS DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN EXTREME NETWORKS, AN EXTREME NETWORKS AFFILIATE OR AN EXTREME NETWORKS CHANNEL PARTNER; EXTREME NETWORKS RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND EXTREME NETWORKS INC. OR THE APPLICABLE EXTREME NETWORKS AFFILIATE (“EXTREME NETWORKS”).

Extreme Networks grants You a license within the scope of the license types described below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Extreme Networks or an Extreme Networks Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Extreme Networks in writing. Extreme Networks may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Extreme Networks through electronic means established by Extreme Networks specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Extreme Networks, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail 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.

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 Extreme Networks' prior consent and payment of an upgrade fee.

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 Extreme Networks. All content on this site, the documentation, Hosted Service, and the product provided by Extreme Networks including the selection, arrangement and design of the content is owned either by Extreme Networks 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 Extreme Networks. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Extreme Networks 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, unless otherwise stated, that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Extreme Networks 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 Extreme Networks' website at:http://www.extremenetworks.com/support/policies/software-licensing or such successor site as designated by Extreme Networks. 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 only 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 EXTREME NETWORKS CHANNEL PARTNER'S HOSTING OF EXTREME NETWORKS 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 EXTREME NETWORKS CHANNEL PARTNER'S HOSTING OF EXTREME NETWORKS PRODUCTS MUST BE AUTHORIZED IN WRITING BY EXTREME NETWORKS AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE EXTREME NETWORKS CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE EXTREME NETWORKS CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE EXTREME NETWORKS CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE EXTREME NETWORKS CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE EXTREME NETWORKS 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

You acknowledge and agree that it is Your responsibility 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 Extreme Networks product is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Security Vulnerabilities

Information about Extreme Networks' security support policies can be found in the Global Technical Assistance Center Knowledgebase at https://gtacknowledge.extremenetworks.com/.

Downloading Documentation

For the most current versions of Documentation, see the Extreme Networks Support website: http://documentation.extremenetworks.com, or such successor site as designated by Extreme Networks.

Contact Extreme Networks Support

See the Extreme Networks Support website:http://www.extremenetworks.com/support for product or Hosted Service notices and articles, or to report a problem with your Extreme Networks product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Extreme Networks Support website:http://www.extremenetworks.com/support/contact/ (or such successor site as designated by Extreme Networks), scroll to the bottom of the page, and select Contact Extreme Networks Support.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Extreme Networks are the registered or unregistered Marks of Extreme Networks, Inc., its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Extreme Networks or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Extreme Networks or the applicable third party.

Extreme Networks is a registered trademark of Extreme Networks, Inc.

All non-Extreme Networks trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

For additional information on Extreme Networks trademarks, please see: http://www.extremenetworks.com/company/legal/

Contents

Chapter 1: Preface

Purpose

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

Training

Ongoing product training is available. For more information or to register, you can access the Web site at www.extremenetworks.com/education/.

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short online feedback form. You can also email us directly at internalinfodev@extremenetworks.com

Getting Help

Product purchased from Extreme Networks

If you purchased your product from Extreme Networks, use the following support contact information to get help.

If you require assistance, contact Extreme Networks using one of the following methods:

- GTAC (Global Technical Assistance Center) for Immediate Support
  - Phone: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact
  - Email: support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- GTAC Knowledge – Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- The Hub – A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- Support Portal – Manage cases, downloads, service contracts, product licensing, and training and certifications.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Product purchased from Avaya

If you purchased your product from Avaya, use the following support contact information to get help.

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.

Extreme Networks Documentation

To find Extreme Networks product guides, visit our documentation pages at:

Current Product Documentation	www.extremenetworks.com/documentation/
Archived Documentation (for previous versions and legacy products)	www.extremenetworks.com/support/documentation-archives/
Release Notes	www.extremenetworks.com/support/release-notes

Open Source Declarations

Some software files have been licensed under certain open source licenses. More information is available at: www.extremenetworks.com/support/policies/software-licensing.

Subscribing to service notifications

Subscribe to receive an email notification for product and software release announcements, Vulnerability Notices, and Service Notifications.

About this task

You can modify your product selections at any time.

Procedure

1. In an Internet browser, go to http://www.extremenetworks.com/support/service-notification-form/ .
2. Type your first and last name.
3. Type the name of your company.
4. Type your email address.
5. Type your job title.
6. Select the industry in which your company operates.
7. Confirm your geographic information is correct.
8. Select the products for which you would like to receive notifications.
9. Click **Submit**.

Chapter 2: New in this document

The following sections document what is new in *IP Flow Configuration using Extreme Fabric Orchestrator*, NN48100–504. See *Extreme Fabric Orchestrator Release Notes* for a list of supported features.

Features

There are no feature changes.

Chapter 3: IP Flow overview

This chapter describes the IP Flow manager user interface and management tools.

User interface

The IP Flow user interface has the following tabs:

- IP Flow Application — Provides the IP Flow management tools.
- Top 10 Views — Provides the top 10 reports that show the heaviest traffic patterns.

IP Flow Administration tab

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

The Administration tab displays the following panes:

- Administration & Analysis pane
- Display pane

Administration & Analysis pane

The Administration & Analysis pane is located on the left side of the user interface, and contains the management tools for 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

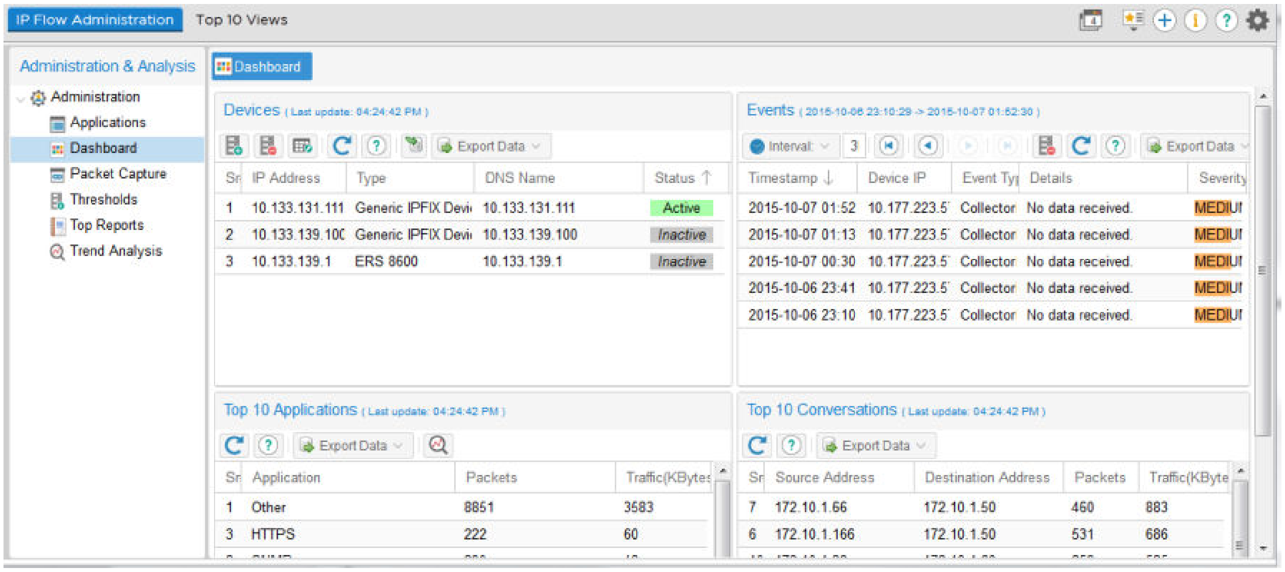
Display pane

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.

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

Example of the IP Flow Administration tab

The following figure shows the IP Flow Administration tab user interface.



Devices (Last update: 04:24:42 PM)

Sr	IP Address	Type	DNS Name	Status ↑
1	10.133.131.111	Generic IPFIX Devi	10.133.131.111	Active
2	10.133.139.10(	Generic IPFIX Devi	10.133.139.100	Inactive
3	10.133.139.1	ERS 8600	10.133.139.1	Inactive

Events (2015-10-06 23:10:29 -> 2015-10-07 01:52:30)

Timestamp ↓	Device IP	Event Ty	Details	Severity
2015-10-07 01:52	10.177.223.5	Collector	No data received.	MEDIUI
2015-10-07 01:13	10.177.223.5	Collector	No data received.	MEDIUI
2015-10-07 00:30	10.177.223.5	Collector	No data received.	MEDIUI
2015-10-06 23:41	10.177.223.5	Collector	No data received.	MEDIUI
2015-10-06 23:10	10.177.223.5	Collector	No data received.	MEDIUI

Top 10 Applications (Last update: 04:24:42 PM)

Sr	Application	Packets	Traffic(KBytes
1	Other	8851	3583
3	HTTPS	222	60

Top 10 Conversations (Last update: 04:24:42 PM)

Sr	Source Address	Destination Address	Packets	Traffic(KByte
7	172.10.1.66	172.10.1.50	460	883
6	172.10.1.166	172.10.1.50	531	686

Figure 1: IP Flow user interface

For more information about administration management tools, see Management tools on page 13.

IP Flow Top 10 Views tab

The 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 & Analysis pane
- Display pane

Administration & Analysis pane

The Administration & 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 consume the most bandwidth.
- Top 10 Conversations — Shows the sources and destination addresses that exchange the most traffic.
- Top 10 Hosts — Shows the hosts, by source and destination, that send or receive the most traffic.

- Top 10 Ports — Shows the ports that exchange the most traffic.
- Top 10 Protocols — Shows the protocols that cause the most traffic.
- Top 10 Subnets — Shows the subnets, by source and destination, that send or receive the most traffic.

For more information about the Top 10 Views, see Top 10 Views on page 20.

Display pane

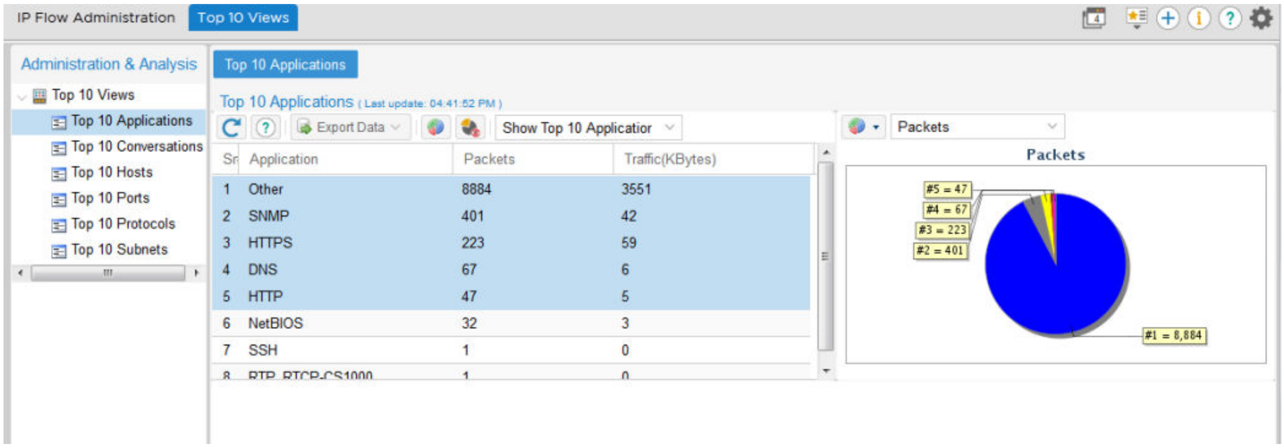
The display pane is on the right side of the user interface. The data on the display pane corresponds with the tool that you select from the Administration & Analysis pane.

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

- In the left middle section, a table provides details about the Top 10 views 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 IP Flow Top 10 Views user interface

The following figure shows the IP Flow Top 10 Views tab user interface.



Top 10 Applications (Last update: 04:41:52 PM)

Show Top 10 Applicatior

Sr	Application	Packets	Traffic(KBytes)
1	Other	8884	3551
2	SNMP	401	42
3	HTTPS	223	59
4	DNS	67	6
5	HTTP	47	5
6	NetBIOS	32	3
7	SSH	1	0
8	RTP_RTCP-CS1000	1	0

Figure 2: Example of the IP Flow Top 10 Views user interface

Management tools

You select the required IP Flow management tool from the Administration & Analysis pane.

The Administration tools are:

- Applications Manager on page 14.
- Dashboard on page 15.
- Device Manager on page 16.
- Event Viewer on page 16.

- Packet Capture Manager on page 17.
- Thresholds Manager on page 18.
- Trend Analysis on page 19.

The Top 10 Views include:

- Top 10 Applications
- Top 10 Conversations
- Top 10 Hosts
- Top 10 Ports
- Top 10 Protocols
- Top 10 Subnets

All are covered under Top 10 Views on page 20.

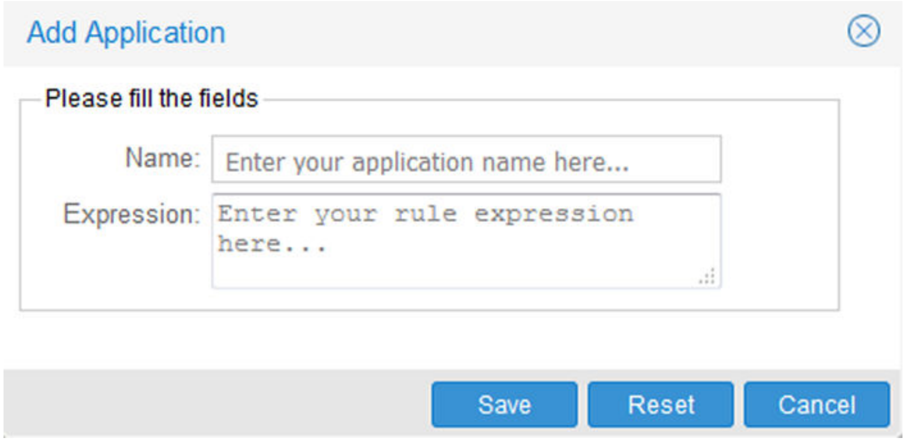
The Configuration tools are:

- Collector Notification dialog box on page 15.
- Look back time dialog box on page 16.
- Packet Capture Duration dialog box on page 17.

Applications Manager

IP Flow supports a predefined list of well-known application names together with the standard protocol and port information of those applications. The system displays an application that does not belong to this list as other in the Top 10 Applications report. From the applications manager you can add new applications to the predefined list so that the new applications 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. You compose expressions with keywords and operators.



Add Application

Please fill the fields

Name: Enter your application name here...

Expression: Enter your rule expression here...

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	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 **IP Flow** > **IP Flow Administration**, and then from the IP Flow Administration & Analysis pane, select **Administration** > **Applications**, 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 27.

Collector Notification dialog box

IP Flow establishes the maximum number of flows for each minute that IP Flow can collect. You use the Collector Notification dialog box to enter an e-mail address where the 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 Extreme Fabric Orchestrator*, NN48100–600.

Dashboard

The Dashboard opens automatically in the Display pane after you launch 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 16.
- Event Viewer on page 16.

- Top 10 Views on page 20.

In the case of the Top 10 Views, the system provides the primary data table. 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

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

Select **IP Flow** > **IP Flow Administration**, and in the Administration & Analysis pane, select **Administration** > **Dashboard** to open the device manager in the display pane.

The system displays IP traffic for each device in the device table 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 or delete devices from the device table. For instructions on using the device manager, see Device Manager on page 30.

Event Viewer

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

Select **IP Flow** > **IP Flow Administration**, and in the Administration & Analysis pane, select **Administration** > **Dashboard** to open the Event Viewer in the display pane.

For instructions on using the Event Viewer, see Event Viewer on page 32. To configure thresholds, see Threshold Manager on page 34.

Look back time dialog box

Look back time establishes the time interval over which IP Flow analyzes collected data. This is the data that provides the content for all Top 10 Views. You can access Loop back time settings from **Dashboard** > **Preferences** > **IP Flow**.

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

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

Packet Capture Duration dialog box

After you initiate a packet capture of ERS 8600 flow data, IP Flow collects packets for one minute. In low traffic conditions, not enough packets may exist to trigger the packet capture feature on the ERS 8600, and you will receive a message that the system cannot generate the PCAP file. Use the Packet Capture Duration dialog to increase the capture time in one minute increments of 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 Extreme Fabric Orchestrator*, NN48100–600.

Packet Capture Manager

You can configure the packet capture on slot/ports of ERS 8600 devices. You use the PCAP dialog box to select the ERS 8600 for which you want to capture packets. After you select the ERS 8600, the Config PCAP dialog box appears. You configure the packet capture criteria, and start a capture.

Select **IP Flow** > **IP Flow Administration**, and in the Administration & Analysis, select **Administration** > **Packet Capture** to open the PCAP dialog box for the packet capture manager in the display pane.

Capture results appear in a data table that includes the:

- Packet capture time
- Source and destination host IP addresses
- Source and destination ports
- Protocol
- Information that provides insight into the nature of the packet (for example, Echo (ping) reply).

For packet capture operations, 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).
- Configure file capture to use the PCMCIA device.
- Insert PCMCIA cards in each CPU slot of the device.
- Configure PCAP file size to 2 MB.
- 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 IP Flow:

- IP Flow must collect some traffic data from the same ERS 8600 device before a PCAP operation can be invoked for the ERS 8600.
- 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 **Administration** > **Credentials**.

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 the 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 IP Flow analyzes the data and displays the results in the IP Flow packet capture window. 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 on page 33.

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 on page 17 for more information.

Thresholds Manager

A threshold defines a traffic flow. After a threshold traffic flow is exceeded, the system triggers an event. You configure a threshold for each device for each protocol. If you delete a device that has a threshold, the threshold is disabled. You can re-enable the threshold if you add the device again.

Select **IP Flow** > **IP Flow Administration**, and in the Administration & Analysis, select **Administration** > **Thresholds** to open the thresholds manager in the display pane. A list of all thresholds added to IP Flow appears. No predefined thresholds exist.

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

You can configure the event to be an SNMP trap, an e-mail message, or a packet capture.

- SNMP trap event — You must add the IP address of the trap receiver and the read community to configure an SNMP trap event.
- E-mail message event — You must configure an e-mail address to configure an e-mail message event. You must also add the SMTP server configuration for an e-mail message event. Use the 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 — You must configure 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 Using packet capture manager to capture packets on page 33. After the packet capture event triggers, the packet capture runs. The system sends the captured data to the specified e-mail address. You must configure the packet capture event to 5 minutes or greater or the system generates an error.

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.

Top Reports

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

Select **IP Flow** > **IP Flow Administration**, and then under Administration & Analysis select **Administration** > **Top Reports** to configure a top report.

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.

The system generates the report as a PDF file.

Trend Analysis

With the 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 by viewing which protocol or application consumes the most bandwidth, and at what peak time.

Select **IP Flow** > **IP Flow Administration**, and then in the Administration & Analysis pane, select **Administration** > **Trend Analysis** to configure the trend analysis management tool.

Top 10 Views

Top 10 Views is a collection of reports that show your heaviest traffic patterns.

Select **IP Flow** > **Top 10 Views**, and then under Administration & Analysis select **Top 10 Views** to access the Top 10 Views options.

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 of time specified in the Look Back Time dialog box. After the analysis finishes, the report appears in the display pane.

You can generate the following reports:

- Top 10 Applications
- Top 10 Conversations
- Top 10 Hosts
- Top 10 Ports
- Top 10 Protocols
- 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 less than 10 protocols exist in the table, then less than 10 active protocols exist in the analyzed data. The system highlights the top five protocols 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 one of the applications displays as `other`, it means the application is not an application supported in the default configuration. You can use the Applications Manager to add applications to IP Flow. The added applications are then available for display in the Top 10 Applications report. See the Applications Manager on page 14 for more information.

In the case of the Top 10 Hosts, two sets of data appear:

- Top 10 source hosts
- Top 10 destination hosts

Changing the view

You can use `Ctrl+left-click` to change the selected rows. Refresh the chart to update and make the chart 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).

Top 10 Subnets

Similarly, for Top 10 Subnets, the top 10 source and destination subnets appear.

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 on 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 Top 10 Views reports on page 42.

Chapter 4: Common icons and procedures

The following icons and procedures are common to many IP Flow activities.

Icons

The following table describes icons in 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.
🔓	Enables or disables an application or threshold.
📡	Displays the currently running applications.
✎	Starts an editing session for the selected item. The editing dialog box displays the same information as the initial configuration dialog box. For information on the dialog box, see the specific management tool.
⟳	Refreshes the data presented in a table or chart.
?	Launches the online help.

Table continues…

Icon	Action
Export Data ⌄	Lists formats for exported data.
⤵	Imports devices from the monitoring server. The icon exists on the device dashboard.
◕	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.
<<	Restores a chart which was previously hidden for a Top 10 View chart. Hides the pane for the Administration & Analysis pane
>>	Restores a pane which was previously hidden for the Administration & Analysis.

Expanding or collapsing the Administration & Analysis tree

About this task

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

Procedure

1. Select **IP Flow** > **IP Flow Administration**.
2. From the 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.
3. Click the arrow again to collapse the view.

Opening a management tool

About this task

Use this procedure to open a management tool.

Procedure

1. Select **IP Flow** > **IP Flow Administration**.
2. From the IP Flow Administration & Analysis pane, under Administration, 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. Select **IP Flow** > **IP Flow Administration**.
2. In the display pane, if the management tool you want to close is not in the foreground, click the tab for the management tool.
3. 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

1. Select **IP Flow** > **IP Flow Administration**.
2. In the display pane, 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 IP Flow database. You can save or view exported data in PDF, CSV, XML, or HTML format.

Procedure

1. Select **IP Flow** > **IP Flow Administration**.
2. With the required data visible in the display pane, click **Export Data**.

   The Export Data list appears.
3. 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.
4. 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

1. Select **IP Flow** > **IP Flow Administration**.
2. In the display pane, 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. Select **IP Flow** > **IP Flow Administration**.
2. In the display pane, right-click a heading in the table.
3. Move the cursor to **Columns**.
4. 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 IP Flow.

Applications Manager

Use the following procedures to configure the Applications Manager.

Adding an application

Use this procedure to add an application to IP Flow.

Before you begin

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

Procedure

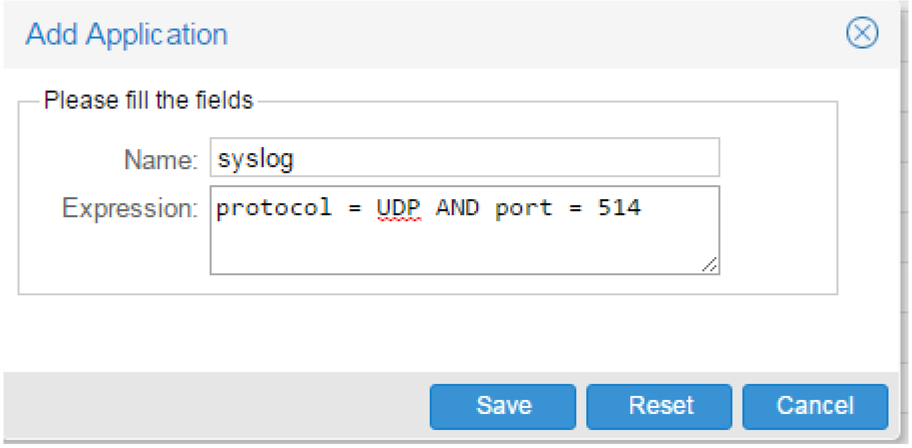
1. Select **IP Flow** > **IP Flow Administration**.
2. From the IP Flow Administration & Analysis pane, select **Administration** > **Applications**.
3. Click the plus sign (**+**) in the applications manager menu bar.
4. In the Name field, type the name of the application.
5. In the Expression field, type the expression for the application.
6. Click **Save**.

   OR

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

Example

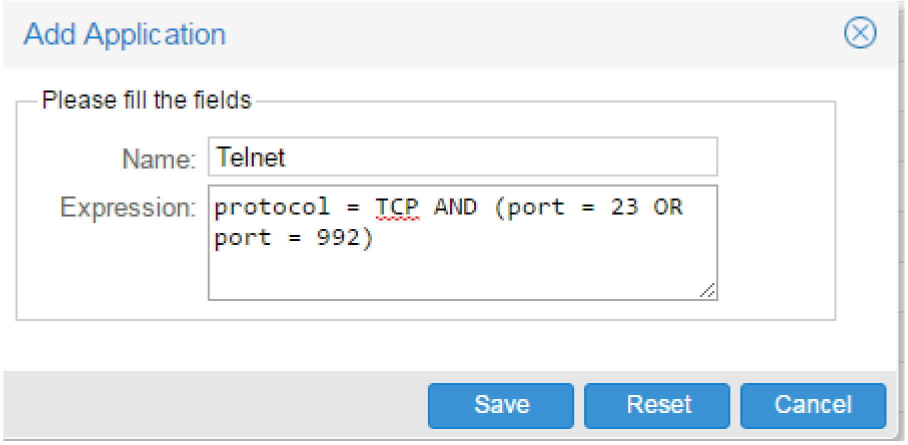
The following displays examples with the expression field filled out.



Please fill the fields

Name: syslog

Expression: protocol = UDP AND port = 514



Please fill the fields

Name: Telnet

Expression: protocol = TCP AND (port = 23 OR port = 992)

Variable Definitions

Variable	Value
Name	Specifies a name for the application in up to 64 printable characters
Expression	Specifies an expression composed of keywords (protocol, port) and operators (ll, , =, ~, >, >=. <, <=)

Deleting an application

About this task

Use this procedure to delete an application.

Procedure

1. 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 to delete an application.
5. Click **Yes** when prompted to confirm the deletion.

   IP Flow deletes the application from the database, and the corresponding row is removed from the applications table.

Editing an application

Use this procedure to edit an existing application.

Procedure

1. 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	Specifies a name for the application of up tp to 64 printable characters
Expression	Specifies an 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. 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. 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 if 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. Select **IP Flow** > **IP Flow Administration**.
2. From the Administration & Analysis pane, select **Administration** > **Applications**.
3. Click **Show Currently Running Applications**.

Device Manager

Use the following procedures to configure the Device Manager.

Adding a device

About this task

Use this procedure to add a device to the IP Flow database.

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

Procedure

1. 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

Use the following table to understand the Add Devices fields.

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

Deleting a device

About this task

Use this procedure to delete a device.

Procedure

1. 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

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 31) and add a new device (Adding a device on page 30).

Procedure

1. 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 Monitoring server

Use this procedure to import devices from the Monitoring server.

Procedure

1. 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

Use the following procedures to configure the Event Viewer.

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. 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 the system displays above the list.

Editing the events time range

About this task

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

Procedure

1. 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.

Using packet capture manager to capture packets

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. 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**.
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 system collects the packets until the buffer is full, analyzes the data, and displays the data in a table below the Configure PCAP dialog box.

   OR

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

Threshold Manager

Use the following procedures to configure the Threshold Manager.

Adding a threshold to a device

About this task

Use this procedure to add a threshold.

Prerequisites:

- You must add a device to the IP Flow database before you can add a threshold. See Adding a device on page 30.
- To use the Email notification type, you must configure the SMTP server as part of global preferences. For more information, see *Administration using Extreme Fabric Orchestrator*, NN48100–600.

Procedure

1. 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 35, the Mail Address dialog box appears. Go to step 14 on page 35.
    - If you selected Trap in step 11 on page 35, the Add Trap dialog box appears. Go to step 16 on page 35.
    - If you select Syslog in step 11 on page 35, the Add Syslog Receiver dialog box appears. Go to step 19 on page 35.
    - If you selected Pcap in step 11 on page 35, the Add Pcap dialog box appears. Go to step 21 on page 35.
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 36.
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 24 on page 36.
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. You can use a maximum of 255 characters.
Threshold Type	Specifies 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 the system to monitor the utilization. This is a mandatory field.
Severity	Specifies a user assigned severity level as one of the following: High, Medium, Low. This is a mandatory field.
Event	Specifies the event type as one of the following: • Email • Trap • Syslog • Pcap 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. 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.

   IP Flow deletes the threshold from the database and the corresponding row is removed from the threshold table.

Editing a threshold

Use this procedure to edit a threshold previously added to the 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 36) and add a new threshold (Adding a threshold to a device on page 34).

Procedure

1. 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.

Table continues…

Variable	Value
Description	Specifies the threshold description. You can use a maximum of 255 characters.
Threshold Type	Specifies 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 as one of the following: High, Medium, Low.
Event	Specifies the event type as one of the following: • Email • Trap • Syslog • Pcap

Finding a threshold

About this task

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

Procedure

1. 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 no matches exist, 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 they appear in the threshold table.
Criteria	The Exact Match option returns thresholds where the data in the table matches the keyword exactly. The Contains option returns thresholds where the data in the table contains the keyword but may contain other data.

Top views reports

You can generate a Top 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. 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 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

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

IP Flow provides two default trend analysis:

- Protocols trending data
- Applications trending data

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

Before you begin

- To successfully plan capacity, you must use the IP Flow trend-analysis tool on a long-term basis. Using the trending tool against the IP Flow server, can affect the performance of the server. If you use trending as a troubleshooting tool over a short time frame, the server performance is not affected as much as if you do trend analysis over a longer period of time. But if you use trending as a long-term capacity-planning tool, you must consider the affect the tool can have on the IP Flow server performance.
- Trending requires the use of memory, and CPU time. Therefore, you must ensure that the IP Flow server is adequate to use the tool.
- To limit any negative performance effects on the IP Flow server process, limit the sampling rate. For a medium-term collection aimed at trend analysis, use a sampling rate of a minute. Increase the sampling rate to an hour for a long-term collection, or if the IP Flow server exists across a slow WAN link, or has low performance issues.

Procedure

1. Select **IP Flow** > **IP Flow Administration**.
2. From the Administration & Analysis pane, select **Administration** > **Trend Analysis**.
3. 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

   The drop down values are populated based on the data collected on the device. The list shows all the available protocols. It is empty if there is no active device in IpFlow.
7. If you are analyzing the applications trending data, then in the Application drop-down menu, select an application.
   - All

   The drop down values are populated based on the data collected on the device. The list shows all the available applications. It is empty if there is no active device in IpFlow.
8. In the Device drop-down menu, select a device.
   - All
   - IP address for a specific device

   The drop down values are populated based on the data collected on the device. The list shows all the available devices. It is empty if there is no active device in IpFlow.
9. Click **Refresh Protocol Trending Graph**, or click **Refresh Application Trending Graph**.
10. To select a trending sampling interval, click the Resolution selection box and select the appropriate interval (For instance: second, minute, or hour).

Note:

Please note that in current release you cannot customize trending charts, but you 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

Use the following procedures to configure Top 10 Views reports.

Displaying a Top 10 Views 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. 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

Use this procedure to choose your own set of applications for monitoring.

After you specify the set of applications, the system lists the same set of applications in the IP Flow dashboard. You can bring back the default set of Top 10 Applications by clicking on the **Show Top 10 Applications** option in the selection box.

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

About this task

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

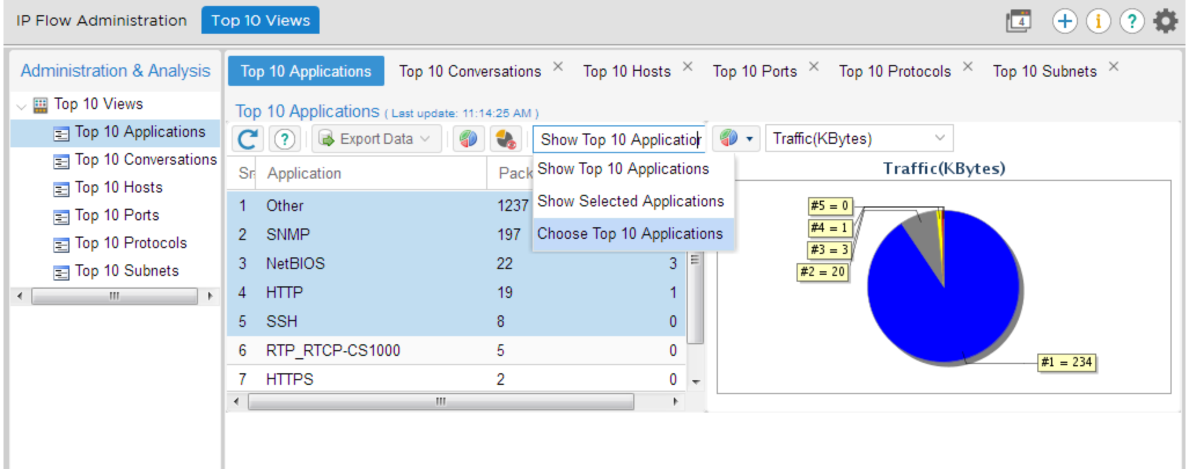
In the dialog box, the system lists application names in an increasing order of their traffic consumption, with 1 being the highest consumer. To identify the top consumers, the first 10 application names are rendered in bold, green font.

If you remove any of the highest consuming entries, the appropriate **Monitor** column or columns display a value of **No** and display in bold, red font. This indicates that the top consuming application names have been 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 displays in bold, red font.

Procedure

1. Select **IP Flow** > **Top 10 Views**.
2. From the Administration & Analysis pane, select **Top 10 Views** > **Top 10 Applications**.
3. From the drop down menu in the display pane, select **Choose Top 10 Applications**.



Sr	Application	Pack	
1	Other	1237	
2	SNMP	197	
3	NetBIOS	22	3
4	HTTP	19	1
5	SSH	8	0
6	RTP_RTCP-CS1000	5	0
7	HTTPS	2	0

4. Right click on an application and select or deselect it using the pop-up window options.
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. Select **IP Flow** > **Top 10 Views**.
2. From the Administration & 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. Select **IP Flow** > **Top 10 Views**.
2. From the Administration & 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. Select **IP Flow** > **Top 10 Views**.
2. From the Administration & 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. 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. Select **IP Flow** > **Top 10 Views**.
2. From the Administration & 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. Select **IP Flow** > **Top 10 Views**.
2. From the Administration & 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

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

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

1. Select **IP Flow** > **Top 10 Views**.
2. From the Administration & Analysis pane, select **Top 10 Views**, and select a Top 10 View.
3. Right-click the row of the host for which you want a subreport, and select a subreport from the list.
4. In the subreport section, click the **x** in the right-hand corner.