



Cisco Application Performance Assurance Device Console User Guide

August 2007

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Customer Order Number:
Text Part Number: OL-14180-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco Application Performance Assurance Device Console User Guide
© 2007 Cisco Systems, Inc. All rights reserved.



CONTENTS

About this Guide vii

CHAPTER 1

General Overview 1-1

- Information About the Cisco Application Performance Assurance Concept 1-1
 - The Cisco Application Performance Assurance Solution 1-1
 - Application Performance Assurance for Enterprises 1-2
- Cisco Application Performance Assurance Capabilities 1-2
- The Application Performance Assurance Technology 1-2
- Information About Management and Collection 1-3
 - Device Management 1-3
 - User Management 1-3
 - Class Configuration Management 1-4
 - Data Collection 1-4

CHAPTER 2

Traffic Processing Overview 2-1

- Routing Environment 2-1
- Traffic Processing 2-1
- Traffic Classification 2-1
 - Classes 2-2
 - Class Elements 2-2
 - Examples of Classes 2-3
 - Signatures 2-3
 - Protocols 2-3
 - Protocol Elements 2-4
 - Initiating Side 2-4
 - Zones 2-4
 - Zone Elements 2-4
 - EXAMPLES OF ZONES: 2-5
 - EXAMPLE OF ASSIGNING A ZONE TO A SESSION: 2-5
- Flavors 2-5
 - Flavor Elements 2-5
- Mapping Flow Attributes to Classes 2-5
- Traffic Monitoring 2-6
 - Usage Monitoring 2-6

The Class Hierarchy	2-7
Class Usage Counters	2-7
Reporting	2-7
Configurations	2-8

CHAPTER 3

Device Setup and Management 3-1

Logging into the Device Console	3-1
Managing Device Connections	3-2
How to View Devices	3-2
How to Add Devices	3-3
What to Do Next	3-4
How to Edit Device Connection Parameters	3-4
How to Delete Devices	3-5
How to Connect to a Device	3-6
How to Disconnect from a Device	3-6
How to Monitor Devices from the Dashboard	3-7
Managing Devices	3-7
Managing Device Configurations	3-7
Device Configuration	3-10
Fault Management	3-22
Fault Configurations	3-33
Viewing and Configuring Statistics	3-36
Statistics Configuration	3-36
Viewing Statistics	3-38
Installing Configuration Files	3-41
How to Install Traffic Control Application Files (PQI)	3-41
How to Install Traffic Configuration Files (PQB)	3-42

CHAPTER 4

Traffic Management 4-1

Managing Traffic Management Configurations	4-1
How to Retrieve the Traffic Management Configuration	4-2
Connecting to a Device	4-2
What to Do Next	4-2
How to Apply Configuration Changes	4-2
How to Export a Traffic Management Configuration	4-3
How to Import a Traffic Management Configuration	4-3
What to Do Next	4-4
Traffic Classification	4-4
Classes	4-4

How to Add Classes	4-4
What to Do Next	4-6
How to Edit Classes	4-6
What to Do Next	4-8
How to Delete Classes	4-8
What to Do Next	4-9
Managing Class Elements	4-10
Signatures	4-15
How to View Signatures	4-15
Protocols	4-15
How to Add Protocols	4-16
What to Do Next	4-16
How to Edit Protocols	4-16
What to Do Next	4-17
How to Delete Protocols	4-17
What to Do Next	4-18
Managing Protocol Elements	4-18
How to Add Protocol Elements	4-18
What to Do Next	4-19
How to Edit Protocol Elements	4-19
What to Do Next	4-20
How to Delete Protocol Elements	4-21
What to Do Next	4-21
Zones	4-21
How to Add Zones	4-22
What to Do Next	4-23
How to Edit Zones	4-23
What to Do Next	4-23
How to Delete Zones	4-24
What to Do Next	4-24
Managing Zone Elements	4-24
How to Add Zone Elements	4-24
How to Edit Zone Elements	4-25
How to Delete Zone Elements	4-26
Flavors	4-27
How to Add Flavors	4-27
What to Do Next	4-28
How to Edit Flavors	4-28
What to Do Next	4-30

How to Delete Flavors	4-30
What to Do Next	4-31
Managing Flavor Elements	4-31
How to Add Flavor Elements	4-31
How to Edit Flavor Elements	4-32
How to Delete Flavor Elements	4-34
Traffic Monitoring	4-35
How to Configure Usage RDRs	4-35
How to Configure Transaction RDRs	4-36
How to Configure Real-Time User RDRs	4-37
How to Configure Transaction Usage RDRs	4-37

CHAPTER 5

User Management 5-1

Managing User Configurations	5-1
How to Retrieve the User Configuration	5-1
What to Do Next	5-2
How to Apply Configuration Changes	5-2
How to Export a User Configuration	5-2
How to Import the User Configuration	5-3
What to Do Next	5-4
User Identification	5-4
How to View Users	5-4
How to Add Users	5-5
What to Do Next	5-6
How to Edit Users	5-6
What to Do Next	5-7
How to Delete Users	5-7
What to Do Next	5-8
How to View Groups	5-8
How to Add Groups	5-8
What to Do Next	5-10
How to Edit Groups	5-10
What to Do Next	5-11
How to Delete Groups	5-11
What to Do Next	5-11
How to Monitor Active Users	5-11

CHAPTER 6

Reporting 6-1

Information About Report Groups	6-1
---------------------------------	-----

Report Instance Properties	6-2
Information About Monitoring Reports	6-4
Granularity	6-4
Metrics	6-5
Information About Traffic Discovery Reports	6-6
Criteria	6-6
Order Property	6-6
Global Monitoring Group	6-6
User Monitoring Group	6-7
Traffic Discovery Group	6-8
Demographic Data and Class Popularity Reports Group	6-8
Web and Streaming Reports Group	6-9
Mail and News Reports Group	6-9
P2P Reports Group	6-10
VoIP Reports Group	6-10
Reporting Overview	6-11
Viewing Completed Reports and Reports in Progress	6-11
Deleting Reports in Progress	6-12
Viewing Report Results	6-12
Data Retrieval	6-13
Viewing Scheduled Data Retrieval Tasks	6-13
Adding Scheduled Data Retrieval Tasks	6-14
Activating Scheduled Data Retrieval Tasks	6-15
Deactivating Scheduled Data Retrieval Tasks	6-16
Deleting Scheduled Data Retrieval Tasks	6-17
Retrieving Data from Archive	6-17
Managing Report Instances	6-17
Creating a Report Instance	6-18
Modifying an Existing Report Instance	6-19
Deleting a Report Instance	6-20

CHAPTER 7

Administrative User Management 7-1

Viewing Administrative User Accounts	7-1
Adding Administrative User Accounts	7-2
Editing Administrative User Accounts	7-3
Adding Device Credentials for an Admin User	7-4
Editing Device Credentials for an Admin User	7-5
Deleting Administrative User Accounts	7-7

APPENDIX **A**

Admin User Roles A-1

Explanation of Roles A-1



About this Guide

Revised: August 15, 2007, OL-14180-01

This preface describes who should read the *Cisco Application Performance Assurance Device Console User Guide*, how it is organized, its document conventions, and how to obtain documentation and technical assistance.

This guide provides information about the data structures created and used by the Network Enhanced Module for Application Performance Assurance (NME-APA). It is intended for the administrators and engineers who are responsible for daily operation of the NME-APA.

This introduction provides information about the following topics:

- [Document Revision History, page vii](#)
- [Organization, page viii](#)
- [Related Publications, page ix](#)
- [Conventions, page ix](#)
- [Obtaining Documentation, page x](#)
- [Obtaining Technical Assistance, page xi](#)

Document Revision History

Table 1

NME-APA Release	Part Number	Publication Date
Release 1.0	OL-14180-01	August, 2007

Organization

The major sections of this guide are as described in [Table 2](#).

Table 2

Chapter	Title	Description
Chapter 1	General Overview, page 1-1	Provides an overview of the Application Performance Assurance solution.
Chapter 2	Traffic Processing Overview, page 2-1	Describes how the Cisco Network Module Enhanced Application Performance Assurance (NME-APA) processes traffic.
Chapter 3	Device Setup and Management, page 3-1	Explains the methods by which the operator can use the Application Performance Assurance (APA) Device Console to configure the Network Module Enhanced Application Performance Assurance (NME-APA) devices on the network, manage any events associated with the devices, and monitor their performance using a series of configurable device statistics.
Chapter 4	Traffic Management, page 4-1	Explains the methods by which the operator of the Application Performance Assurance (APA) Device Console identifies and defines the traffic that will be available for reporting from the Network Module Enhanced Application Performance Assurance (NME-APA).
Chapter 5	User Management, page 5-1	Explains the methods by which the operator of the Application Performance Assurance (APA) Device Console defines the individuals and groups that provide the basis of the system reporting from the Network Module Enhanced Application Performance Assurance (NME-APA).
Chapter 6	Reporting, page 6-1	Explains the methods by which the operator of the Application Performance Assurance (APA) Device Console defines the data retrieval parameters, as well as the means of converting this data into usable reports from the Network Module Enhanced Application Performance Assurance (NME-APA).

Table 2

Chapter	Title	Description
Chapter 7	Administrative User Management, page 7-1	Explains the methods by which the operator of the Application Performance Assurance (APA) Device Console maintains security of the Network Module Enhanced Application Performance Assurance (NME-APA) devices by managing administrative user accounts and access rights for logging into the APA Device Console.
Appendix A	Admin User Roles, page A-1	Describes the Cisco Application Performance Assurance (APA) administrative user roles.

Related Publications

Your NME-APA device and the software running on it contain extensive features and functionality, which are documented in the following resources:

- For information on installing the Device Console, refer to the *Cisco Application Performance Assurance Device Console Installation Guide* .
- For information on using the Device Console, refer to the *Cisco Application Performance Assurance Device Console User Guide* .
- For initial installation and startup information, refer to the *Cisco Network Module Enhanced Application Performance Assurance User Guide* .
- For troubleshooting information, refer to the *Cisco Application Performance Assurance Troubleshooting Guide* .
- Cisco CLI software, refer to the *Cisco Application Performance Assurance CLI Reference Guide*
- For international agency compliance, safety, and statutory information for wide-area network (WAN) interfaces for the NME-APA device, refer to the *Regulatory Compliance and Safety Information for Cisco Network Enhanced Module Application Performance Assurance (NME-APA)*.
- For installation of the APA Device Console, refer to the Cisco Application Performance Assurance Device Console Installation Guide
- To view Cisco documentation or obtain general information about the documentation, refer to *Obtaining Documentation* .

Conventions

This document uses the following conventions:

Table 3

Convention	Description
boldface font	Commands and keywords are in boldface .
<i>italic font</i>	Arguments for which you supply values are in <i>italics</i> .

Table 3 (continued)

Convention	Description
[]	Elements in square brackets are optional.
{x y z}	Alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string, or the string will include the quotation marks.
screen font	Terminal sessions and information that the system displays are in <code>screen font</code> .
boldface screen font	Information you must enter is in boldface screen font .
<i>italic screen font</i>	Arguments for which you supply values are in <i>italic screenfont</i> .
<>	Nonprinting characters, such as passwords, are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

**Note**

Means *reader take note* . Notes contain helpful suggestions or references to materials not covered in this manual.

**Caution**

Means *reader be careful* . In this situation, you might do something that could result in equipment damage or loss of data.

**Warning**

Means *reader be warned* . In this situation, you might do something that could result in bodily injury.

Obtaining Documentation

- The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- <http://www.cisco.com>
- <http://www-china.cisco.com>
- <http://www-europe.cisco.com>

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package that ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the networking Products MarketPlace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/pcgi-bin/marketplace/welcome.pl>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Attn Document Resource Connection

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides [Cisco.com](http://www.cisco.com) as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at any time, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to <http://www.cisco.com>.

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website <http://www.cisco.com/tac>.

P3 and P4 level problems are defined as follows:

- P3—Your network is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for [Cisco.com](http://www.cisco.com), go to <http://tools.cisco.com/RPF/register/register.do>.

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at <http://www.cisco.com/tac/caseopen>.

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>.

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.



CHAPTER 1

General Overview

This module provides a general overview of the Cisco Application Performance Assurance solution. It introduces the Cisco Application Performance Assurance concept and the Application Performance Assurance capabilities.

It also briefly describes the hardware capabilities of the Network Module Enhanced Application Performance Assurance (NME-APA) and the Cisco specific applications that together compose the total Cisco Application Performance Assurance solution.

- [Information About the Cisco Application Performance Assurance Concept, page 1-1](#)
- [Cisco Application Performance Assurance Capabilities, page 1-2](#)
- [The Application Performance Assurance Technology, page 1-2](#)
- [Information About Management and Collection, page 1-3](#)

Information About the Cisco Application Performance Assurance Concept

- [The Cisco Application Performance Assurance Solution, page 1-1](#)
- [Application Performance Assurance for Enterprises, page 1-2](#)

The Cisco Application Performance Assurance Solution

The Cisco Application Performance Assurance solution is delivered through a combination of purpose-built hardware and specific software solutions that address various traffic management challenges faced by enterprises. The NME-APA is designed to support classification and analysis of Internet/IP traffic.

Cisco Application Performance Assurance enables enterprises to accommodate more traffic while capitalizing on their existing infrastructure. With the power of Application Performance Assurance, enterprises have the ability to analyze IP network traffic at high speeds. The Cisco Application Performance Assurance solution also gives enterprises the tools they need to identify and target overhead content-based traffic.

Application Performance Assurance for Enterprises

Enterprises of any industry must find new ways to get maximum leverage from their existing infrastructure, while differentiating their offerings with enhanced IP capabilities.

The Cisco Application Performance Assurance solution adds a new layer of service intelligence to existing networks that can:

- Report and analyze network traffic at user and aggregate level for capacity planning
- Identify network abusers who are violating the Acceptable Use Policy
- Identify peer-to-peer and NNTP (news) traffic
- Integrate Application Performance Assurance solutions easily with existing network elements and BSS/OSS systems

Cisco Application Performance Assurance Capabilities

The core of the Cisco Application Performance Assurance solution is the application for managing traffic including:

- User and application awareness—Application-level drilling into IP traffic for real-time understanding and controlling of usage and content at the granularity of a specific user.
 - User awareness—The ability to map between IP flows and a specific user in order to maintain the state of each user transmitting or receiving traffic through the NME-APA.
 - Application awareness—The ability to understand and analyze traffic up to the application protocol layer (Layer 7).

For application protocols implemented using bundled flows (such as FTP, which is implemented using Control and Data flows), the NME-APA understands the bundling connection between the flows and treats them accordingly.

- Programmability—The ability to quickly add new protocols and easily adapt to new services and applications in the ever-changing enterprise environment. Programmability is achieved using the Cisco Service Modeling Language (SML).

Programmability provides an easy upgrade path for network and application growth.

- Robust and flexible back-office integration—The ability to integrate with existing third-party systems at the enterprise, including provisioning systems, user repositories, billing systems, and OSS systems. The NME-APA provides a set of open and well-documented APIs that allows a quick and robust integration process.
- Scalable high-performance service engines—The ability to perform all these operations at high-speed.

The Application Performance Assurance Technology

The network devices are capable of performing application-layer stateful-flow inspection of IP traffic, and controlling that traffic based on configurable rules. The network device uses ASIC components and RISC processors to go beyond packet counting and delve deeper into the contents of network traffic. Providing programmable, stateful inspection of bidirectional traffic flows and mapping these flows with user ownership, it provides real-time classification of network usage. This information provides the basis

of the advanced traffic-control and bandwidth-shaping functionality. Where most bandwidth shaper functionality ends, the Cisco Application Performance Assurance solution provides more control and shaping options, including:

- Layer 7 stateful packet inspection and classification
- Robust support for over 600 protocols and applications, including:
 - General—HTTP, HTTPS, FTP, TELNET, NNTP, SMTP, POP3, IMAP, WAP, and others
 - P2P file sharing—FastTrack-Kazaa, Gnutella, BitTorrent, Winny, Hotline, eDonkey, DirectConnect, Piolet, and others
 - P2P VoIP—Skype, Skinny, DingoTel, and others
 - Streaming and Multimedia—RTSP, SIP, HTTP streaming, RTP/RTCP, and others
- Programmable system core for flexible reporting
- Transparent network and BSS/OSS integration into existing networks
- User awareness that relates traffic and usage to specific customers

Information About Management and Collection

The Cisco Application Performance Assurance solution includes a complete management infrastructure that provides the following management components to manage all aspects of the solution:

- Device management
- User management
- Application Performance Assurance

These management interfaces are designed to comply with common management standards and to integrate easily with existing OSS infrastructure.

Device Management

Cisco provides network Fault, Configuration, Performance, and Security Management.

Three interfaces are provided for network management:

- Graphical User Interface (GUI)—Accessible through the intranet, the GUI is used for configuration and security functions.
- SNMP—Provides fault management (via SNMP traps) and performance monitoring functionality.
- Command-line interface (CLI)—Accessible through a Telnet connection, the CLI is used for configuration and security functions.

User Management

Where the Cisco Application Performance Assurance solution tracks usage on an individual user basis, the Cisco Application Performance Assurance solution also provides the capability to store user information in a local database.

Class Configuration Management

Class configuration management is the ability to configure the general class definitions of a network application. A class configuration file containing settings for traffic classification, accounting and reporting, and control is created and applied to the NME-APA. The APA Device Console application provides a tool to distribute these configuration files to devices. This simple, standards-based approach makes it easy to manage multiple devices in a large network.

The APA Device Console provides an easy-to-use GUI to edit and create these files.

Data Collection

The Cisco Application Performance Assurance solution generates usage data and statistics and manages them as Raw Data Records (RDRs), using a simple TCP-based protocol (RDR-Protocol). The Cisco Application Performance Assurance solution implements the collection system and processing them on the local machine. The data is then stored for analysis and reporting functions, and for the collection and presentation of data to additional OSS systems.



CHAPTER 2

Traffic Processing Overview

This module describes how the Cisco Network Module Enhanced Application Performance Assurance (NME-APA) processes traffic.

The module also defines the main elements (configuration entities) and explains how they relate to each other.

- [Routing Environment, page 2-1](#)
- [Traffic Processing, page 2-1](#)
- [Traffic Classification, page 2-1](#)
- [Traffic Monitoring, page 2-6](#)
- [Configurations, page 2-8](#)

Routing Environment

The Cisco Application Performance Assurance solution operates in a Symmetric routing environment. Inbound and outbound traffic is routed through one NME-APA. For a marginal number of flows only one direction goes through the NME-APA.

Traffic Processing

There are two stages of traffic processing:

- Traffic classification— analyses traffic flows and determines their type (for example, browsing, e-mail, file sharing, or voice).
- Traffic accounting and reporting— performs bookkeeping and generates Raw Data Records (RDRs) that let you analyze and monitor the network.

These two stages are described in the following sections.

You control how classification and reporting are performed by editing configurations and applying them to the NME-APA.

Traffic Classification

Traffic processing starts with traffic classification , which categorizes network sessions into classes.

For each network application traversing an enterprise's infrastructure, a corresponding class is defined in the Cisco Application Performance Assurance solution. You can use this class to classify and identify the traffic and report on its usage.

Classes

In the traffic classification process, categorizes network sessions into *classes*.

Classes are the building blocks for:

- Class configurations
- Aggregated usage reporting

From an enterprise's point of view, a class is usually a network application—such as browsing, e-mail, file sharing, or voice—that the user uses. From a technical point of view, a class consists of one or more class elements, each of which enables a decision about the class associated with a network traffic flow type.

A number of classes are predefined in the default configuration. You can modify these classes and add additional classes to a configuration.

A configuration can contain up to 500 classes.

The classification process occurs when a flow is established. The process examines the first few packets of the session and decides to which class the session belongs. The session is then assigned a class ID that remains the same during the session's life cycle.

Traffic is classified and mapped to classes on the basis of some or all of the following class elements:

- Protocol—The protocol used. This allows, for example, the mapping of browsing flows and e-mail flows to separate classes.
- Zone—Lists of IP addresses of the network-side host of the flow. This allows, for example, the mapping of all voice flows going to a specified server to a specific class.
- Flavor—Specific Layer 7 properties such as host names of the network-side host of the flow. This allows, for example, the mapping of all HTTP flows where the URL matches a certain pattern to a specific class.

The NME-APA uses these flow mappings to map each network connection passing through it to a class.

Class Elements

A class consists of one or more class elements; different network traffic flow types are mapped to different class elements.

A class element maps a specific protocol, initiating side, zone, and flavor to the selected class. Some or all of these parameters can take wild-card values.



Note

When asymmetric routing classification mode is enabled, the flavor of a class element is always the wild-card value.

A traffic flow is mapped to a specific class if it meets all four of the following criteria:

- The flow uses the specified *protocol* of the class element.
- The flow matches the *initiating side* specified for the class element.

- The destination of the flow is an address that belongs to the specified *zone* of the class element.
- The flow matches the specified *flavor* of the class element.
- If a flow matches two class elements and one is more specific than the other, the flow will be mapped to the more specific of the two. For example: Class A is defined for browsing and Class B is defined for browsing to a specific list of URLs. A browsing flow to a URL on Class B's list matches both classes, but will be mapped to Class B.
- If a flow matches one parameter of one class element and a different parameter of another class element, precedence will be given first to matching flavors, then to protocols, then to zones, and finally to the initiating side. For example: Class A is defined for e-mail and Class B is defined for all traffic to a specific network zone. An e-mail flow to the specific network zone matches both classes, but will be mapped to Class A.

Examples of Classes

The following table contains examples of classes and their network parameters.

Table 2-1 **Examples of Classes and Class Parameters**

Class Name	Protocol	Initiating Side	Zone	Flavor
Web Browsing	HTTP HTTPS	User-initiated		
Web Hosting (network-initiated browsing)	HTTP HTTPS	Network-initiated		
Local SMTP	SMTP		Local-mail servers (215.53.64.0/24)	

Signatures

The NME-APA examines traffic flows using its deep-packet-inspection capabilities, and compares each flow with an installed set of protocol signatures to identify the network application that generated the flow.

The NME-APA comes with a set of predefined signatures for common network applications and protocols, such as browsing, e-mail, file sharing, and VoIP.

Protocols

One of the main classifications of a flow is the protocol of a session (that is, of the network application that generated the session).

A protocol, as defined in the system, is a combination of one or more signatures, one or more port numbers, and a transport type. The protocol of the network flow is identified according to these parameters. For example, if the port number is 80, the transport type is TCP, and content matches the HTTP signature, the NME-APA maps the flow to the HTTP protocol.

The default configuration contains a long list of predefined protocols. You can add additional protocols.

When a TCP or UDP flow does not match a specific protocol definition, the NME-APA maps the flow to the Generic TCP or Generic UDP protocol.

When a non-TCP/UDP flow does not match a specific protocol definition, the NME-APA maps the flow to the Generic IP protocol.

Protocol Elements

A protocol is a collection of protocol elements.

A protocol element maps a specific signature, IP protocol, and port range to the selected protocol. Some or all of these parameters can take wild-card values; port numbers can take range values.

A traffic flow is mapped to a specific protocol if it meets all three of the following criteria:

- The flow matches the specified signature of the protocol element.
- The flow protocol matches the IP Protocol of the protocol element.
- The flow matches the specified port range of the protocol element.

If a flow matches two protocol elements and one is more specific than the other, the flow will be mapped to the more specific of the two. For example: Protocol A is defined for flows that match the FTP signature and Protocol B is defined for flows that match the FTP signature on TCP port 21. An FTP flow on port 21 matches both protocols, but will be mapped to Protocol B.

If a flow matches the signature of one protocol element and the port of another protocol element, it will be mapped to the matching signature. For example: Protocol A is defined for flows that match the FTP signature and Protocol B is defined for flows on TCP port 21. An FTP flow on port 21 matches both protocols, but will be mapped to Protocol A.

Initiating Side

The Application Performance Assurance solution is located between the enterprise's users and the network. User-initiated flows are initiated by the user toward the network; network-initiated flows are initiated from the network toward the user.

You can monitor some flow-types to one initiating side. For example, with HTTP you can monitor the user-initiated traffic separately from the network-initiated traffic. HTTP is always user-initiated when the user ventures outward to surf the Internet. If the direction of the HTTP flow is network-initiated, this probably means that a web server is open on the user's local machine for receiving incoming HTTP traffic. The enterprise can monitor the network-initiated HTTP and use other criteria to evaluate if the traffic is legitimate.

Zones

A zone is a collection of network-side IP addresses.

You configure zones by arranging IP addresses in groups connected by a common purpose. A user's network flow mapped to a class may be applied to a zone. In practice, zones often define geographical areas.

Zones are used to classify network sessions; each network session can be assigned to a class element based on its destination IP address.

Zone Elements

A zone is a collection of related zone elements.

A zone element is an IP address or a range of IP addresses.

Table 2-2 Examples of Zone Items

Network Address	Example
IP address	123.123.3.2
IP address range (and mask)	123.3.123.0/24 This means that the first 24 bits of the IP address must be included as specified and the final 8 bits can take any value. (That is, all IP addresses in the range 123.3.123.0 to 123.3.123.255.)

EXAMPLES OF ZONES:

- A “walled garden”—A range of IP addresses of a server farm with premium video content, for which the enterprise would like to limit access to specific users and to assure traffic priority.
- A zone to differentiate between off-net and on-net flows.

EXAMPLE OF ASSIGNING A ZONE TO A SESSION:

- Zone A and Zone B are two user-defined zones. Zone A includes the IP address range 10.1.0.0/16, and Zone B includes the IP address range 10.2.0.0/16. Analysis of a new session shows that its network IP address is 10.1.1.1—the session belongs to zone A.

Flavors

Flavors are advanced classification elements that classify network sessions according to signature-specific Layer 7 properties.

Flavors provide an additional level of granularity in defining classes in the Cisco Application Performance Assurance solution. A protocol flavor uses an additional protocol attribute in classifying a class, making this class a flavor of the class based on the protocol only. For example, the user-agent attribute of the HTTP protocol could be added as a protocol flavor, enabling the definition of all HTTP traffic generated by the same browser type (indicated in the user-agent field) as one class.

Examples of flavor types are HTTP User Agent and SIP Source Domain.

Flavor Elements

A flavor is a collection of flavor elements .

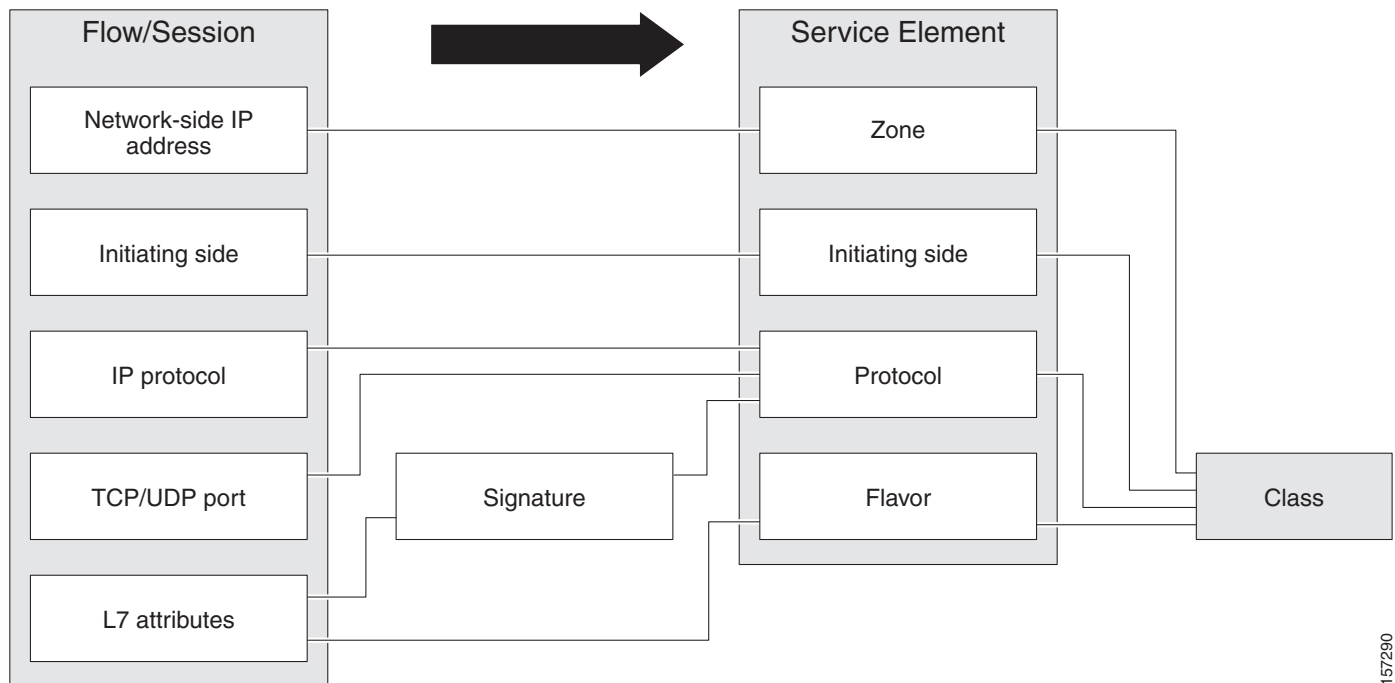
The type of a flavor element depends on the flavor type.

The default configuration includes some predefined flavors, such as HTTP Streaming Agents (a flavor of HTTP) and Vonage (a flavor of SIP).

Mapping Flow Attributes to Classes

The following figure illustrates the mappings of flow elements of a session to class elements of a class.

Figure 2-1



157290

Traffic Monitoring

You can use data gathered by the Application Performance Assurance solutions for reporting.

Various metrics are collected in different scopes—global (per entire link), per class (or group of classes), per policy (or policy profile), and per user—based on user-defined usage counters.

The values from the usage counters can be either pushed or pulled:

- The Application Performance Assurance solution generates and transmits Raw Data Records (RDRs) that contain flow, usage, and other data.
- The Application Performance Assurance solution maintains an SNMP MIB that can be queried by external systems.

Usage Monitoring

The NME-APA collects and maintains various network metrics, per class, in different scopes.

The network metrics are:

- Upstream volume (L3 kilobytes)
- Downstream volume (L3 kilobytes)
- Sessions
- Active users
- Concurrent sessions
- Session duration

**Note**

For VoIP classes, such as SIP and MGCP, the concurrent sessions usage counter counts concurrent voice calls, and the session duration usage counter measures voice call duration.

Per class accounting takes place in the following scopes:

- Per user
- Per group of users (package)
- Per link (global)

Several classes may share the same class usage counter. For example, in the default configuration, the SMTP service and the POP3 service share the E-Mail Counter. The assignment of classes to usage counters is determined by the class hierarchy, as explained in the following section.

The Class Hierarchy

Classes are arranged in a hierarchal tree. A single default class is at the root, and you can place each new class anywhere in the tree.

Classes inherit the matching rules of their parents.

Class Usage Counters

The class hierarchy provides a way to share usage counters and to organize classes according to their semantics. Classes are accounted in groups, as defined in the class hierarchy. Each class is assigned usage counters.

There are two categories of usage counters for classes:

- Global—Used for Link Usage RDRs and reports
- User—Used for Real-Time User Usage RDRs and reports

A global usage counter and a user usage counter are assigned to each class. The use of a class can be accounted either exclusively for traffic classified to it or in conjunction with the traffic of its parent class. For example, if a class called Premium Video Content is defined as a child of Streaming, the operator can either define a special usage counter for Premium Video Content or configure it to use the same usage counter as Streaming. The global usage counter and the user usage counter are independent; for the same class, one usage counter may be the same for parent and child, whereas the other is exclusive to the child.

Reporting

Application Performance Assurance solutions running generate and accumulate Raw Data Records (RDRs) that contain information relevant to the enterprise.

The following are the main categories of RDRs:

- Usage RDRs—Generated periodically. These RDRs contain the state of the usage counters, per class and per accounting scope. There are four types of usage RDRs:
 - Link Usage RDRs—Global usage per class, for the entire link.
 - Usage RDRs—Usage per group of users, per class.

- User Usage RDRs—Usage per user, per class. These RDRs are generated for all users. The Cisco Application Performance Assurance solution uses these RDRs to generate top-user reports and aggregated usage records.
- Real-Time User Usage RDRs—Generated for selected users only. The Cisco Application Performance Assurance solution uses these RDRs by to generate detailed user activity reports.
- Transaction RDRs—Generated for a sample of the flows. These RDRs are used to create statistical histograms such as Top TCP Ports.
- Transaction Usage RDRs—Generated for every flow according to user-defined filters. These RDRs contain detailed Layer 7 information for browsing, streaming, and voice flows. They are used for flow-based reporting.

Configurations

A *configuration* implements and enforces the enterprise's business strategy and vision.

A configuration can take effect only after it is propagated to the appropriate NME-APA. The NME-APA enforces the configuration by analyzing the network traffic passing through it.

A configuration consists of:

- Traffic classification settings—Classes, such as web browsing, file sharing, and VoIP. Each class consists of elements that define how network traffic is mapped to the class. The configuration building blocks of classes are protocols, zones, flavors, and signatures.
- Traffic monitoring and reporting settings—Settings that determine how traffic flows and network usage are reported.

In practice, defining configurations is an iterative process.

It is recommended that you use the following sequence of steps:

1. Set up the system.
2. Apply the default configuration.
3. Gather data.
4. Analyze.
5. Continue traffic discovery by partitioning the traffic into (additional) classes.



CHAPTER 3

Device Setup and Management

This module explains the methods by which the operator can use the Application Performance Assurance (APA) Device Console to configure the Network Module Enhanced Application Performance Assurance (NME-APA) devices on the network, manage any events associated with the devices, and monitor their performance using a series of configurable device statistics.

- [Logging into the Device Console, page 3-1](#)
- [Managing Device Connections, page 3-2](#)

Logging into the Device Console

From a web browser, browse to the IP address of the machine that is hosting the APA Device Console.

- Step 1** From a web browser, browse to the IP address of the machine that is hosting the APA Device Console. The APA Device Console login screen appears.

Figure 3-1

CISCO

APA
Device
Console
v1.0.0.0

* Username:

* Password:

Device Name/IP Address:

Copyright 2007, Cisco Systems Inc
All rights reserved

231756

**Note**

The initial login information for the APA Device Console is:

username: cisco

password: cisco

The Device Console will force you to change the password.

Step 2 Enter your Device Console username and password.

The APA Device Console screen appears.

Managing Device Connections

- [How to View Devices, page 3-2](#)
- [How to Add Devices, page 3-3](#)
- [How to Edit Device Connection Parameters, page 3-4](#)
- [How to Delete Devices, page 3-5](#)
- [How to Connect to a Device, page 3-6](#)
- [How to Disconnect from a Device, page 3-6](#)
- [How to Monitor Devices from the Dashboard, page 3-7](#)
- [Managing Devices, page 3-7](#)
- [Viewing and Configuring Statistics, page 3-36](#)
- [Installing Configuration Files, page 3-41](#)

How to View Devices

Step 1 In the Navigation pane, select **Connect**.
A list of configured devices appears in the Configuration pane.

Figure 3-2

Devices					
	IP Address / Host Name	Name	Description	Group	Status
<input type="radio"/>	NME-APA_1.cisco.com	NME-APA_1	Primary NME-APA device	Cisco	Available
<input type="radio"/>	172.16.1.1	NME-APA_2	Secondary NME-APA Device	Cisco	Connected
<input type="button" value="Connect"/> <input type="button" value="Disconnect"/> <input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Help"/>					

231764

How to Add Devices

- Step 1** In the Navigation pane, select **Connect**.
A list of configured devices appears in the Configuration pane.

Figure 3-3

Devices					
	IP Address / Host Name	Name	Description	Group	Status
<input type="radio"/>	NME-APA_1.cisco.com	NME-APA_1	Primary NME-APA device	Cisco	Available
<input type="radio"/>	172.16.1.1	NME-APA_2	Secondary NME-APA Device	Cisco	Connected
<input type="button" value="Connect"/> <input type="button" value="Disconnect"/> <input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Help"/>					

231764

- Step 2** Click **Add**.
The Add Device screen appears in the Configuration pane.

Figure 3-4

Add Device

Name:

IP Address / Host Name:

Group:

Description:

OK

Cancel

231743

- Step 3** In the Name field, enter a meaningful name for the device.
- Step 4** In the IP Address / Host Name field, enter the IP address or host name used to connect to the device.
- Step 5** In the Group field, enter the name of the group of devices with to associate the new device.
- Step 6** In the Description field, enter a meaningful description of the device.
- Step 7** Click **OK**.
The list of configured devices reappears in the Configuration pane.
The new device is added to the list of configured devices.



Note

If the APA Device Console can establish connectivity with an added device, the APA Device Console displays *Available* in the Availability field for the device.

**Note**

If the APA Device Console cannot establish connectivity with an added device, the APA Device Console displays *Offline* in the Availability field for the device.

What to Do Next

For information on how to connect to an added device, see [How to Connect to a Device, page 3-6](#).

How to Edit Device Connection Parameters

- Step 1** In the Navigation pane, select **Connect**.
A list of configured devices appears in the Configuration pane.

Figure 3-5

Devices					
	IP Address / Host Name	Name	Description	Group	Status
<input type="radio"/>	NME-APA_1.cisco.com	NME-APA_1	Primary NME-APA device	Cisco	Available
<input type="radio"/>	172.16.1.1	NME-APA_2	Secondary NME-APA Device	Cisco	Connected
<input type="button" value="Connect"/> <input type="button" value="Disconnect"/> <input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Help"/>					

231764

- Step 2** Select the radio button next to the device you want to edit.
- Step 3** Click **Edit**.
The Edit Device screen appears in the Configuration pane.

Figure 3-6

Edit Device	
IP Address / Host Name:	NME-APA_1.cisco.com
Name:	<input type="text" value="NME-APA_1"/>
Group:	<input type="text" value="Cisco"/>
Description:	<input type="text" value="Primary NME-APA device"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

231781

- Step 4** In the Name field, enter a meaningful name for the device.

**Note**

The Name entered here must match the Device Name entered in [Adding Device Credentials for an Admin User, page 7-4](#).

Step 5 In the Group field, enter the name of the group of devices with which you want the new device associated.

Step 6 In the Description field, enter a meaningful description of the device.

Step 7 Click **OK**.

The list of configured devices appears in the Configuration pane.

The parameters of the edited device are shown in the list of configured devices.

**Note**

If the APA Device Console can establish connectivity with an added device, the APA Device Console displays *Available* in the Availability field for the device.

**Note**

If the APA Device Console cannot establish connectivity with an added device, the APA Device Console displays *Offline* in the Availability field for the device.

How to Delete Devices

Step 1 In the Navigation pane, select **Connect**.

A list of configured devices appears in the Configuration pane.

Figure 3-7

Devices					
	IP Address / Host Name	Name	Description	Group	Status
<input type="radio"/>	NME-APA_1.cisco.com	NME-APA_1	Primary NME-APA device	Cisco	Available
<input type="radio"/>	172.16.1.1	NME-APA_2	Secondary NME-APA Device	Cisco	Connected
<input type="button" value="Connect"/> <input type="button" value="Disconnect"/> <input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Help"/>					

231764

Step 2 Select the radio button next to the device you want to delete.

Step 3 Click **Delete**.

The list of configured devices appears in the Configuration pane.

The device is deleted and is removed from the list of configured devices.

How to Connect to a Device

Step 1 In the Navigation pane, select **Connect**.

A list of configured devices appears in the Configuration pane.



Note

Available in a device's Availability field indicates that the APA Device Console can connect to the device.



Note

Connected in a device's Availability field indicates that the APA Device Console is already connected to the device.



Note

Offline in a device's Availability field indicates that the APA Device Console cannot connect to the device. See [How to Edit Device Connection Parameters, page 3-4](#) to verify the device's IP address/Hostname.



Note

In order to connect to a device, the user must have valid device credentials configured. To configure device credentials for an Admin User, see [Adding Device Credentials for an Admin User, page 7-4](#).

Figure 3-8

Devices					
	IP Address / Host Name	Name	Description	Group	Status
<input type="radio"/>	NME-APA_1.cisco.com	NME-APA_1	Primary NME-APA device	Cisco	Available
<input type="radio"/>	172.16.1.1	NME-APA_2	Secondary NME-APA Device	Cisco	Connected
<div>Connect Disconnect Add Edit Delete Help</div>					

231764

Step 2 Select the radio button next to the device to which you want to connect and click **Connect**.

The device's Availability field displays Connected.

The device's configurations are loaded into the APA Device Console.

How to Disconnect from a Device

Step 1 In the Navigation pane, select **Connect**.

A list of configured devices appears in the Configuration pane.



Note

Available in a device's Availability field indicates that the APA Device Console can connect to the device.

**Note**

Connected in a device's Availability field indicates that the APA Device Console is already connected to the device.

**Note**

Offline in a device's Availability field indicates that the APA Device Console cannot connect to the device. See [How to Edit Device Connection Parameters, page 3-4](#) to verify the device's IP address/Hostname.

Figure 3-9

Devices					
	IP Address / Host Name	Name	Description	Group	Status
<input type="radio"/>	NME-APA_1.cisco.com	NME-APA_1	Primary NME-APA device	Cisco	Available
<input type="radio"/>	172.16.1.1	NME-APA_2	Secondary NME-APA Device	Cisco	Connected
<input type="button" value="Connect"/> <input type="button" value="Disconnect"/> <input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Help"/>					

231764

- Step 2** Select the radio button next to the device you want to disconnect from and click **Disconnect**. The device's Availability field displays Available.

How to Monitor Devices from the Dashboard

- Step 1** From the Navigation pane, select **Dashboard**

Managing Devices

- [Managing Device Configurations, page 3-7](#)
- [Device Configuration, page 3-10](#)
- [Fault Management, page 3-22](#)
- [Fault Configurations, page 3-33](#)

Managing Device Configurations

The APA Device Console is a Graphical User Interface (GUI) which gives the NME-APA operator an intuitive method of modifying NME-APA configurations. Configuration changes are made to an NME-APA device through a process of retrieving the device's configuration for display in the APA Device Console, modifying the configuration parameters in the APA Device Console, and applying the modified configuration back to the NME-APA device.

NME-APA device configurations can also be stored offline in configuration files and restored to NME-APA devices through the configuration Export and Import functions.

**Note**

The APA Device Console must first be connected to a NME-APA device. For information on connecting to a device, see [Managing Device Connections, page 3-2](#).

- [How to Retrieve the Device Configuration, page 3-8](#)
- [How to Apply Configuration Changes, page 3-8](#)
- [How to Export a Device Configuration, page 3-9](#)
- [How to Import the Device Configuration, page 3-9](#)

How to Retrieve the Device Configuration

Once you connect to a device, the device's configurations are loaded into the APA Device Console. You may reload the device's active configurations into the APA Device Console by using the retrieve function.

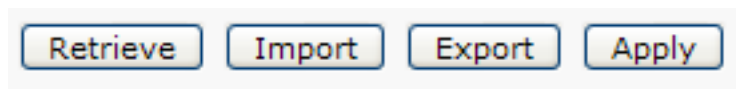
**Note**

Retrieving a device's configurations will replace all settings and parameters in the APA Device Console. All unsaved settings and parameters will be lost.

Step 1 In the Navigation pane, select **Device Management > Configuration** and any of the Device Management tabs.

The Retrieve button is displayed in the lower section of the screen.

Figure 3-10



Step 2 Click **Retrieve**.

The device configuration is retrieved and loaded into the APA Device Console.

What to Do Next

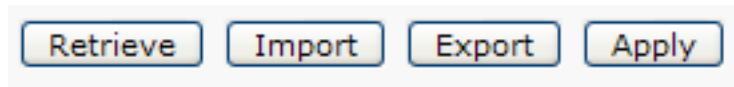
To save the configuration to a file, see [How to Export a Device Configuration, page 3-9](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 3-8](#).

How to Apply Configuration Changes

Modifications made to a device's configuration in the APA Device Console are not used until they are applied to the device.

Step 1 In the Navigation pane, select **Device Management > Configuration** and any of the Device Management tabs.

The Apply button is displayed in the lower section of the screen.

Figure 3-11**Step 2** Click **Apply**.

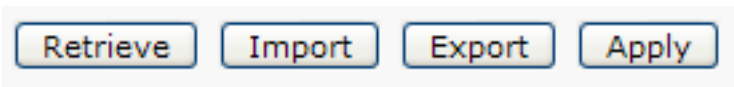
The device configuration is applied to the device.

How to Export a Device Configuration

A device configuration can be exported and saved to a file so that it can be archived or applied to other devices.

Step 1 In the Navigation pane, select **Device Management > Configuration** and any of the Device Management tabs.

The Export button is displayed in the lower section of the screen.

Figure 3-12**Step 2** Click **Export**.

The Export Configuration dialog box appears.

Figure 3-13**Step 3** Enter a file name for the configuration file.**Step 4** Click **Export**.

The device configuration is exported to a file.

**Note**

To view a list of exported configuration files or to delete exported configuration files, see [How to Import the Device Configuration, page 3-9](#).

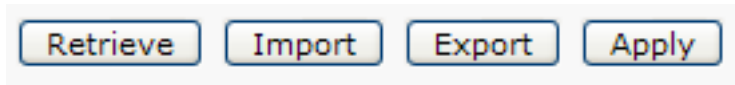
How to Import the Device Configuration

An exported device configuration can be imported into the APA Device Console so that it can be modified or applied to a device.

Step 1 In the Navigation pane, select **Device Management > Configuration** and any of the Device Management tabs.

The Import button is displayed in the lower section of the screen.

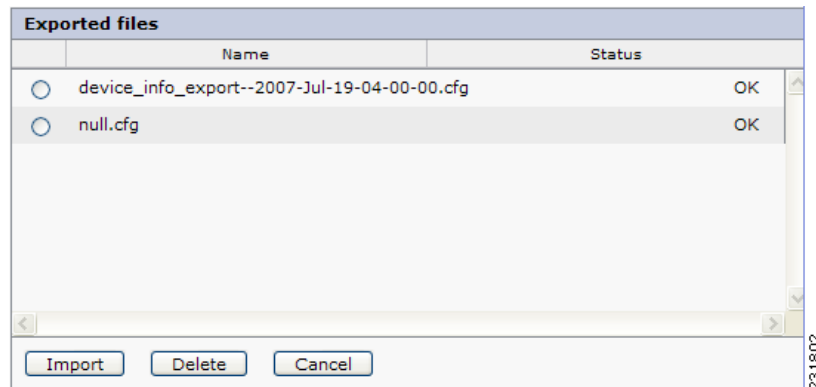
Figure 3-14



Step 2 Click **Import**.

The Import Configuration dialog box appears.

Figure 3-15



Step 3 Select the radio button next to the file you want to import.

Step 4 Click **Import**.

The device configuration is imported to the APA Device Console.

What to Do Next

To save the configuration to a file, see [How to Export a Device Configuration, page 3-9](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 3-8](#).

Device Configuration

This module contains information about configuring settings and services of the connected NME-APA device.

- [How to Configure Basic Settings, page 3-11](#)
- [Time Settings, page 3-11](#)
- [SNMP Settings, page 3-13](#)
- [Security Settings, page 3-18](#)

How to Configure Basic Settings

- Step 1** In the Navigation pane, select **Device Management > Configuration**.
The Device Configuration screen appears in the Configuration pane open to the Basic tab.

Figure 3-16

The screenshot shows the 'Basic' tab of the Device Configuration screen. The fields are as follows:

- Device Name: NME-APA_1
- IP Address/Host Name: NME-APA_1
- Domain Name: (empty text box)
- DNS Servers: (Format: IP Address x.x.x.x) with three empty text boxes below it.

At the bottom left are 'Save' and 'Reset' buttons. On the right side, there is a vertical text label '231768'.

- Step 2** In the Domain field, enter the domain to which the device belongs.
- Step 3** In the DNS Servers fields, enter one or more IP addresses of the DNS servers that the device should use for domain name resolution.
- Step 4** Click **Save**.
The basic settings are saved in the configuration.

What to Do Next

To save the configuration to a file, see [How to Export a Device Configuration, page 3-9](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 3-8](#).

Time Settings

The APA Device Console allows the operator to enter the current time or enter SNTP server information.

- [How to Configure the Device's Time, page 3-11](#)
- [How to Configure the SNTP client, page 3-12](#)

How to Configure the Device's Time

- Step 1** In the Navigation pane, select **Device Management > Configuration**.
- Step 2** Click the **Time** tab.
The Time tab opens.

Figure 3-17

- Step 3** In the Date field, enter the current date in yyyy-Mmm-dd format or click to open a calendar.
- Step 4** In the Time fields, enter the current hour, minute, and second and select the device's time zone from the drop-down list.
- Step 5** If device's location changes time for Daylight Saving Time, enter the number of minutes to offset during Daylight Savings Time in the **Shift from Daylight Savings Time** field.
- Step 6** If the device's location changes time for Daylight Saving Time, enter the date, hour and minute to begin Daylight Savings Time in the **Daylight Savings start** fields or click to open a calendar.
- Step 7** If the device's location changes time for Daylight Saving Time, enter the date, hour and minute to end Daylight Savings Time in the **Daylight Savings end** fields or click to open a calendar.
- Step 8** Click **Save**.

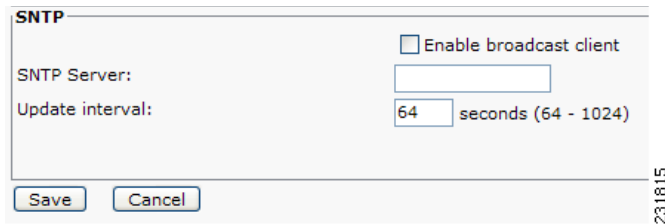
The current time is saved in the configuration.

What to Do Next

To save the configuration to a file, see [How to Export a Device Configuration, page 3-9](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 3-8](#).

How to Configure the SNTP client

- Step 1** In the Navigation pane, select **Device Management > Configuration**.
- Step 2** Click the **Time** tab.
- The Time tab opens, displaying the SNTP box in the lower portion of the screen.

Figure 3-18A screenshot of a configuration dialog box titled "SNTP". It contains a checkbox labeled "Enable broadcast client" which is currently unchecked. Below this, there are two input fields: "SNTP Server:" and "Update interval:". The "Update interval:" field has the value "64" entered, followed by the text "seconds (64 - 1024)". At the bottom of the dialog are two buttons: "Save" and "Cancel".

SNTP

☐ Enable broadcast client

SNTP Server:

Update interval: seconds (64 - 1024)

- Step 3** Check the **Enable broadcast client** check box.
- Step 4** In the SNTP Server field, enter the IP address of your SNTP server.
- Step 5** In the Update interval field, enter the number of seconds between SNTP updates.
- Step 6** Click **Save**.

The SNTP settings are saved in the configuration.

What to Do Next

To save the configuration to a file, see [How to Export a Device Configuration, page 3-9](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 3-8](#).

SNMP Settings

- [How to Configure the SNMP Agent, page 3-13](#)
- [Trap Managers, page 3-14](#)

How to Configure the SNMP Agent

-
- Step 1** In the Navigation pane, select **Device Management > Configuration** and select the **SNMP** tab in the Configuration pane.

The SNMP configuration screen appears in the Configuration pane.

Figure 3-19

SNMP Agent

☒ Enable

Location:

Contact:

Community String

☒ Public Read Only

☐ Read Only

Trap Groups

☐ System Reset

☐ Telnet

☐ Alarm

Trap Managers

	Trap Host Name / IP Address	Community String	SNMP Version
<input type="radio"/>	198.162.0.2	Cisco	2c

231769

- Step 2** In the SNMP Agent box, check the **Enable** check box.
- Step 3** In the Location field, enter a meaningful name for the device's location.
- Step 4** In the Contact field, enter the username of a contact person who has all management information regarding the device.
- Step 5** In the Community String box, check the upper check box.
By default, the upper community string is set to read-only and the lower community string is set to READ/WRITE. You can change this by clicking on the drop-down arrow next to the Community String field that you want to change.
- Step 6** In the upper Community String field, enter the device's read-only community string.
- Step 7** In the lower Community String field, enter the device's read-write community string.
- Step 8** In the Trap Groups box, check the check boxes next to the trap groups that you want to enable.
Many Trap Groups are enabled by default. You must uncheck them if you do not want them enabled.
- Step 9** Click **Save**.
The SNMP agent settings are saved in the configuration.

What to Do Next

To save the configuration to a file, see [How to Export a Device Configuration, page 3-9](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 3-8](#).

Trap Managers

This module contains information about how to configure SNMP Trap Managers.

- [How to View Trap Managers, page 3-15](#)

- [How to Add Trap Managers, page 3-15](#)
- [How to Edit Trap Managers, page 3-16](#)
- [How to Remove Trap Managers, page 3-17](#)

How to View Trap Managers

Step 1 In the Navigation pane, select **Device Management > Configuration**.

Step 2 Select the **SNMP** tab in the Configuration pane.

The SNMP configuration screen appears in the Configuration pane, displaying the Trap Managers in the lower section.

Figure 3-20

Trap Managers		
	Trap Host Name / IP Address	Community String
<input type="radio"/>	192.168.0.2	Cisco
SNMP Version		
2c		
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Remove"/>		

231821

How to Add Trap Managers

Step 1 In the Navigation pane, select **Device Management > Configuration**.

Step 2 Select the **SNMP** tab in the Configuration pane.

The SNMP configuration screen appears in the Configuration pane, displaying the Trap Managers in the lower section.

Figure 3-21

Trap Managers		
	Trap Host Name / IP Address	Community String
<input type="radio"/>	192.168.0.2	Cisco
SNMP Version		
2c		
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Remove"/>		

231821

Step 3 Click **Add**.

The Add Trap Manager box appears in the upper section of the Configuration pane.

Figure 3-22

The image shows a 'Add Trap Manager' dialog box with the following fields and controls:

- Tabs: Basic, Time, **SNMP**, Security
- IP Address: [Text Input Field]
- Community String: [Text Input Field]
- SNMP Version: [2c ▼]
- Buttons: OK, Cancel

- Step 4** In the Host field, enter the hostname or IP address of the Trap Manager.
- Step 5** In the Community String field, enter the community string of the Trap Manager.
- Step 6** In the SNMP Version drop-down list, select SNMP version 2c.



Note SNMP Version 2c is the only version currently supported.

- Step 7** Click **OK**.
- The SNMP Trap Manager is saved in the configuration.

What to Do Next

To save the configuration to a file, see [How to Export a Device Configuration, page 3-9](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 3-8](#).

How to Edit Trap Managers

- Step 1** In the Navigation pane, select **Device Management > Configuration**.
- Step 2** Select the **SNMP** tab in the Configuration pane.
- The SNMP configuration screen appears in the Configuration pane, displaying the Trap Managers in the lower section.

Figure 3-23

Trap Managers			
	Trap Host Name / IP Address	Community String	SNMP Version
<input type="radio"/>	192.168.0.2	Cisco	2c
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Remove"/>			

- Step 3** Select the radio button next to the Trap Manager you want to edit.
- Step 4** Click **Edit**.
- The Edit Trap Manager box appears in the upper section of the Configuration pane.

Figure 3-24

Basic Time **SNMP** Security

Edit Trap Manager

Host: 198.162.0.2

Community String: Cisco

SNMP Version: 2c

OK Cancel

- Step 5** In the Host field, edit the hostname or IP address of the Trap Manager.
- Step 6** In the Community String field, edit the community string of the Trap Manager.
- Step 7** In the SNMP Version drop-down list, select the SNMP version that the Trap Manager uses.
- Step 8** Click **OK**.

The modified SNMP Trap Manager is saved in the configuration.

What to Do Next

To save the configuration to a file, see [How to Export a Device Configuration, page 3-9](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 3-8](#).

How to Remove Trap Managers

- Step 1** In the Navigation pane, select **Device Management >Configuration** and select the **SNMP** tab in the Configuration pane.
- The SNMP configuration screen appears in the Configuration pane, displaying the Trap Managers in the lower section.

Figure 3-25

Trap Managers		
Trap Host Name / IP Address	Community String	SNMP Version
<input type="radio"/> 192.168.0.2	Cisco	2c

Add Edit Remove

- Step 2** Select the radio button next to the Trap Manager you want to remove.
- Step 3** Click **Remove**.

The Trap Manager box reappears in the lower section of the Configuration pane without the removed Trap Manager.

The Trap Manager is removed from the configuration.

What to Do Next

To save the configuration to a file, see [How to Export a Device Configuration, page 3-9](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 3-8](#).

Security Settings

- [Authentication, page 3-18](#)
- [How to Change the Device Enable Password, page 3-18](#)
- [Device Users, page 3-19](#)

Authentication

The APA Device Console has the capability to use more robust user management technologies. This capability is disabled for the current release but will be enabled in a future release.

Step 1 In the Navigation pane, select **Device Management > Configuration**.

Step 2 Select the **Security** tab in the Configuration pane.

The Security configuration screen appears in the Configuration pane, displaying the Authentication box in the upper section.

Figure 3-26

Authentication

Authentication Type:

Authentication Server:

Server Host:

Server Port:

Encryption Key:

Time Out:

231757

How to Change the Device Enable Password

The APA Device Console provides an interface for changing device's enable passwords.

Step 1 In the Navigation pane, select **Device Management > Configuration**.

Step 2 Select the **Security** tab in the Configuration pane.

The Security configuration screen appears in the Configuration pane, displaying the Device Enable Password box in the middle section.

Figure 3-27

Device Enable Password	
	Access Level
<input type="radio"/>	0
<input type="radio"/>	5
<input type="radio"/>	10
<input type="radio"/>	15

Step 3 Select the radio button next to the Access Level password you want to change.

Step 4 Click **Change**.

The Change Enable Password box appears in the upper section of the Configuration pane.

Figure 3-28

Change Enable Password User

Access Level: 0

Enable Password:

Confirm Enable Password:

Step 5 In the Enable Password field, enter the new enable password.

Step 6 In the Confirm Enable Password field, reenter the new enable password.

Step 7 Click **OK**.

The modified enable password is saved in the configuration.

What to Do Next

To save the configuration to a file, see [How to Export a Device Configuration, page 3-9](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 3-8](#).

Device Users

The APA Device Console provides an interface for managing device user accounts.

- [How to View Device Users, page 3-19](#)
- [How to Add Device Users, page 3-20](#)
- [How to Edit Device Users, page 3-21](#)
- [How to Remove Device Users, page 3-22](#)

How to View Device Users

Step 1 In the Navigation pane, select **Device Management > Configuration**.

Step 2 Select the **Security** tab in the Configuration pane.

The Security configuration screen appears in the Configuration pane, displaying the Device Users box in the lower section.

Figure 3-29

Device Users		
	Device User Name	Access Level
<input type="radio"/>	hypham	15
<input type="radio"/>	test	15
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>		

231777

How to Add Device Users

Step 1 In the Navigation pane, select **Device Management > Configuration**.

Step 2 Select the **Security** tab in the Configuration pane.

The Security configuration screen appears in the Configuration pane, displaying the Device Users box in the lower section.

Figure 3-30

Device Users		
	Device User Name	Access Level
<input type="radio"/>	hypham	15
<input type="radio"/>	test	15
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>		

231777

Step 3 Click **Add**.

The Add Device User box appears in the upper section of the Configuration pane.

Figure 3-31

Add Device User	
Name:	<input type="text"/>
Password:	<input type="password"/>
Confirm Password:	<input type="password"/>
Access Level:	5 <input type="button" value="v"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

231742

Step 4 In the Name field, enter the User's user name.

Step 5 In the Password field, enter the User's password.

Step 6 In the Confirm Password field, reenter the User's password.

Step 7 In the Access Level drop-down list, select the User's access level.

- Step 8** Click **OK**.
The new User is saved in the configuration.

What to Do Next

To save the configuration to a file, see [How to Export a Device Configuration, page 3-9](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 3-8](#).

How to Edit Device Users

- Step 1** In the Navigation pane, select **Device Management > Configuration**.
Step 2 Select the **Security** tab in the Configuration pane.
The Security configuration screen appears in the Configuration pane, displaying the Device Users box in the lower section.

Figure 3-32

Device Users		
	Device User Name	Access Level
<input type="radio"/>	hypham	15
<input type="radio"/>	test	15
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>		

231777

- Step 3** Select the radio button next to the Device User you want to edit.
Step 4 Click **Edit**.
The Edit Device User box appears in the upper section of the Configuration pane.

Figure 3-33

Edit Device User	
Name:	test10
Password:	<input type="text"/>
Confirm Password:	<input type="text"/>
Access Level:	10 <input type="button" value="v"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

231780

- Step 5** In the Password field, enter the User's new password.
Step 6 In the Confirm Password field, reenter the User's new password.
Step 7 In the Access Level drop-down list, select the User's access level.
Step 8 Click **OK**.
The modified Device User is saved in the configuration.

What to Do Next

To save the configuration to a file, see [How to Export a Device Configuration, page 3-9](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 3-8](#).

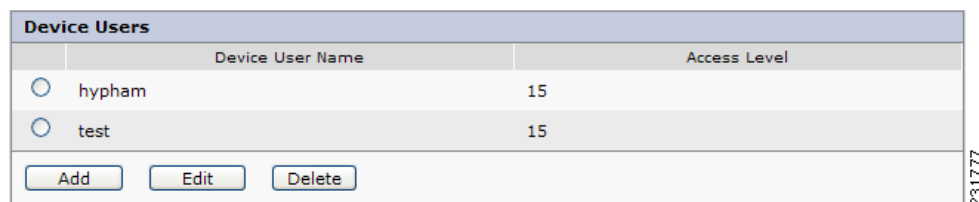
How to Remove Device Users

Step 1 In the Navigation pane, select **Device Management > Configuration**.

Step 2 Select the **Security** tab in the Configuration pane.

The Security configuration screen appears in the Configuration pane, displaying the Device Users box in the lower section.

Figure 3-34



Device Users	
	Device User Name
<input type="radio"/>	hypham
<input type="radio"/>	test

Access Level: 15

Buttons: Add, Edit, Delete

Step 3 Select the radio button next to the Device User you want to remove.

Step 4 Click **Remove**.

The Device Users box reappears in the lower section of the Configuration pane without the removed Device User.

The Device User is removed from the configuration.

What to Do Next

To save the configuration to a file, see [How to Export a Device Configuration, page 3-9](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 3-8](#).

Fault Management

This module contains information about configuring faults for the connected NME-APA device. Events are messages that are generated as a result of fault conditions being met. Events can be used to track fault conditions and to notify operators and engineers of the occurrence of fault conditions.

- [Active Events, page 3-22](#)
- [Cleared Events, page 3-27](#)

Active Events

Active Events are those events which have occurred but have not been cleared by an operator.

- [How to View Active Events, page 3-23](#)
- [How to Acknowledge Active Events, page 3-24](#)
- [How to Send Active Event Notifications, page 3-24](#)
- [How to Annotate Active Events, page 3-25](#)

- [How to Clear Active Events, page 3-26](#)
- [How to Refresh the Display of Active Events, page 3-27](#)
- [How to Sort Active Events, page 3-27](#)

How to View Active Events

- Step 1** In the Navigation pane, select **Device Management > Fault Management**.
The Fault Management screen appears in the Configuration pane open to the Active tab.

Figure 3-35

Active

Cleared

Active Events [Total: 179]

<input type="checkbox"/>	Event ID ▼	Device ID	Severity	Time of Occurrence	Last Changed	Event Group	Status
<input type="checkbox"/>	10244	171.71.8.109		2007-Aug-16 11:29:32	2007-Aug-16 11:29:32	Telnet	Active
<input type="checkbox"/>	10243	171.71.8.109		2007-Aug-16 11:26:32	2007-Aug-17 09:57:12	Telnet	Acknowledged
<input type="checkbox"/>	10242	171.71.8.109		2007-Aug-16 11:26:32	2007-Aug-17 09:57:12	Telnet	Acknowledged
<input type="checkbox"/>	10241	171.71.8.109		2007-Aug-16 11:25:32	2007-Aug-16 11:25:32	Telnet	Active
<input type="checkbox"/>	10240	171.71.8.109		2007-Aug-16 11:25:21	2007-Aug-16 11:25:21	System Reset	Active

Acknowledge

Notify

Annotate

Clear

Refresh

Help

- Step 2** To view details of an event, click on the event's **Event ID**.
The Event Details window appears.

Figure 3-36

Event Details	
Event ID:	10244
Notification ID:	.1.3.6.1.4.1.9.9.630.0.2
Description:	Telnet Session Started
Severity:	Info
Date/Time:	2007-Aug-16 11:29:32
Status:	Active
Additional Info:	1 171.71.9.149
Comments:	

OK Cancel

- Step 3** To close the window, click **OK** or **Cancel**.

How to Acknowledge Active Events

- Step 1** In the Navigation pane, select **Device Management > Fault Management**.
The Fault Management screen appears in the Configuration pane open to the Active tab.

Figure 3-37

Active

Cleared

Active Events [Total: 179]

<input type="checkbox"/>	Event ID ▾	Device ID	Severity	Time of Occurrence	Last Changed	Event Group	Status	
<input type="checkbox"/>	10244	171.71.8.109		2007-Aug-16 11:29:32	2007-Aug-16 11:29:32	Telnet	Active	
<input type="checkbox"/>	10243	171.71.8.109		2007-Aug-16 11:26:32	2007-Aug-17 09:57:12	Telnet	Acknowledged	
<input type="checkbox"/>	10242	171.71.8.109		2007-Aug-16 11:26:32	2007-Aug-17 09:57:12	Telnet	Acknowledged	
<input type="checkbox"/>	10241	171.71.8.109		2007-Aug-16 11:25:32	2007-Aug-16 11:25:32	Telnet	Active	
<input type="checkbox"/>	10240	171.71.8.109		2007-Aug-16 11:25:21	2007-Aug-16 11:25:21	System Reset	Active	

Acknowledge

Notify

Annotate

Clear

Refresh

Help

201737

- Step 2** Check the check box next to the event or events that you want to acknowledge.

- Step 3** Click **Acknowledge**.

The event's Status field changes to *Acknowledged*.

How to Send Active Event Notifications

- Step 1** In the Navigation pane, select **Device Management > Fault Management**.
The Fault Management screen appears in the Configuration pane open to the Active tab.

Figure 3-38

ActiveCleared

Active Events [Total: 179]

<input type="checkbox"/>	Event ID ▼	Device ID	Severity	Time of Occurrence	Last Changed	Event Group	Status
<input type="checkbox"/>	10244	171.71.8.109		2007-Aug-16 11:29:32	2007-Aug-16 11:29:32	Telnet	Active
<input type="checkbox"/>	10243	171.71.8.109		2007-Aug-16 11:26:32	2007-Aug-17 09:57:12	Telnet	Acknowledged
<input type="checkbox"/>	10242	171.71.8.109		2007-Aug-16 11:26:32	2007-Aug-17 09:57:12	Telnet	Acknowledged
<input type="checkbox"/>	10241	171.71.8.109		2007-Aug-16 11:25:32	2007-Aug-16 11:25:32	Telnet	Active
<input type="checkbox"/>	10240	171.71.8.109		2007-Aug-16 11:25:21	2007-Aug-16 11:25:21	System Reset	Active

AcknowledgeNotifyAnnotateClearRefreshHelp

- Step 2** Check the check box next to the event or events for which you want to send notifications.

- Step 3** Click **Notify**.

The Event Notification window appears.

Figure 3-39

Notify

SMTP Server: mailman.cisco.com

Sender: user1@cisco.com

Sender Comments (Optional): Comments

Recipient Address(es): user2@cisco.com

OK Cancel

- Step 4** In the Sender Address field, enter the e-mail address that should be displayed the From field of the notification.
- Step 5** In the Sender Comments field, enter text to be sent with the Event Notification.
- Step 6** In the Recipient Address(es) field, enter the e-mail address or addresses of the people who should receive the notification.
- Step 7** Click **Submit**.
- The notification is sent and the Event Notification window closes.

How to Annotate Active Events

- Step 1** In the Navigation pane, select **Device Management > Fault Management**.
- The Fault Management screen appears in the Configuration pane open to the Active tab.

Figure 3-40

Active Events [Total: 179]

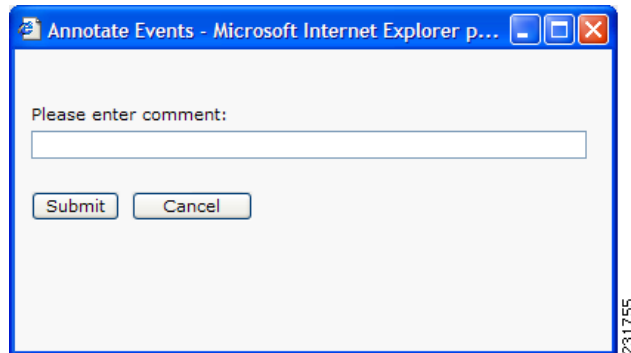
<input type="checkbox"/>	Event ID	Device ID	Severity	Time of Occurrence	Last Changed	Event Group	Status
<input type="checkbox"/>	10244	171.71.8.109	Information	2007-Aug-16 11:29:32	2007-Aug-16 11:29:32	Telnet	Active
<input type="checkbox"/>	10243	171.71.8.109	Information	2007-Aug-16 11:26:32	2007-Aug-17 09:57:12	Telnet	Acknowledged
<input type="checkbox"/>	10242	171.71.8.109	Information	2007-Aug-16 11:26:32	2007-Aug-17 09:57:12	Telnet	Acknowledged
<input type="checkbox"/>	10241	171.71.8.109	Information	2007-Aug-16 11:25:32	2007-Aug-16 11:25:32	Telnet	Active
<input type="checkbox"/>	10240	171.71.8.109	Warning	2007-Aug-16 11:25:21	2007-Aug-16 11:25:21	System Reset	Active

Acknowledge Notify Annotate Clear Refresh Help

- Step 2** Check the check box next to the event or events to which you want to add a comment.
- Step 3** Click **Annotate**.

The Annotate Events window appears.

Figure 3-41



Step 4 In the Please enter comments field, enter the comments that you want to add to the event or events.

Step 5 Click **Submit**.

The comment is saved.



Note

A new comment will replace any existing text in an event's Comments field.

How to Clear Active Events

Step 1 In the Navigation pane, select **Device Management > Fault Management**.

The Fault Management screen appears in the Configuration pane open to the Active tab.

Figure 3-42

<input type="checkbox"/>	Event ID	Device ID	Severity	Time of Occurrence	Last Changed	Event Group	Status
<input type="checkbox"/>	10244	171.71.8.109	Information	2007-Aug-16 11:29:32	2007-Aug-16 11:29:32	Telnet	Active
<input type="checkbox"/>	10243	171.71.8.109	Information	2007-Aug-16 11:26:32	2007-Aug-17 09:57:12	Telnet	Acknowledged
<input type="checkbox"/>	10242	171.71.8.109	Information	2007-Aug-16 11:26:32	2007-Aug-17 09:57:12	Telnet	Acknowledged
<input type="checkbox"/>	10241	171.71.8.109	Information	2007-Aug-16 11:25:32	2007-Aug-16 11:25:32	Telnet	Active
<input type="checkbox"/>	10240	171.71.8.109	Warning	2007-Aug-16 11:25:21	2007-Aug-16 11:25:21	System Reset	Active

Acknowledge Notify Annotate Clear Refresh Help

Step 2 Check the check box next to the event or events which you want to clear.

Step 3 Click **Clear**.

The Active Events list reappears with the cleared event removed.

How to Refresh the Display of Active Events

- Step 1** In the Navigation pane, select **Device Management > Fault Management**.
The Fault Management screen appears in the Configuration pane open to the Active tab.

Figure 3-43

Active

Cleared

Active Events [Total: 179]

<input type="checkbox"/>	Event ID ▼	Device ID	Severity	Time of Occurrence	Last Changed	Event Group	Status
<input type="checkbox"/>	10244	171.71.8.109		2007-Aug-16 11:29:32	2007-Aug-16 11:29:32	Telnet	Active
<input type="checkbox"/>	10243	171.71.8.109		2007-Aug-16 11:26:32	2007-Aug-17 09:57:12	Telnet	Acknowledged
<input type="checkbox"/>	10242	171.71.8.109		2007-Aug-16 11:26:32	2007-Aug-17 09:57:12	Telnet	Acknowledged
<input type="checkbox"/>	10241	171.71.8.109		2007-Aug-16 11:25:32	2007-Aug-16 11:25:32	Telnet	Active
<input type="checkbox"/>	10240	171.71.8.109		2007-Aug-16 11:25:21	2007-Aug-16 11:25:21	System Reset	Active

Acknowledge

Notify

Annotate

Clear

Refresh

Help

- Step 2** Click **Refresh**.
The Active Events list reappears with the updated list of Active Events.

How to Sort Active Events

- Step 1** In the Navigation pane, select **Device Management > Fault Management**.
The Fault Management screen appears in the Configuration pane open to the Active tab.

Figure 3-44

Active

Cleared

Active Events [Total: 179]

<input type="checkbox"/>	Event ID ▼	Device ID	Severity	Time of Occurrence	Last Changed	Event Group	Status
<input type="checkbox"/>	10244	171.71.8.109		2007-Aug-16 11:29:32	2007-Aug-16 11:29:32	Telnet	Active
<input type="checkbox"/>	10243	171.71.8.109		2007-Aug-16 11:26:32	2007-Aug-17 09:57:12	Telnet	Acknowledged
<input type="checkbox"/>	10242	171.71.8.109		2007-Aug-16 11:26:32	2007-Aug-17 09:57:12	Telnet	Acknowledged
<input type="checkbox"/>	10241	171.71.8.109		2007-Aug-16 11:25:32	2007-Aug-16 11:25:32	Telnet	Active
<input type="checkbox"/>	10240	171.71.8.109		2007-Aug-16 11:25:21	2007-Aug-16 11:25:21	System Reset	Active

Acknowledge

Notify

Annotate

Clear

Refresh

Help

- Step 2** Click on the column heading by which you would like to sort the events.
The Active Events list reappears sorted by the selected column.

Cleared Events

Cleared Events are events which have occurred and have been cleared by an operator.

- [How to View Cleared Events, page 3-28](#)
- [How to Annotate Cleared Events, page 3-29](#)
- [How to Send Cleared Event Notifications, page 3-30](#)
- [How to Delete Cleared Events, page 3-31](#)
- [How to Refresh the Display of Cleared Events, page 3-31](#)
- [How to Sort Cleared Events, page 3-32](#)

How to View Cleared Events

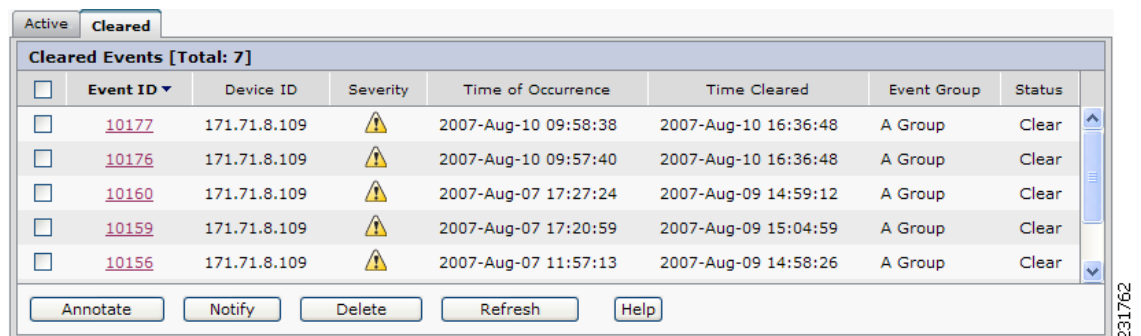
Step 1 In the Navigation pane, select **Device Management > Fault Management**.

The Fault Management screen appears in the Configuration pane.

Step 2 Click the **Cleared** tab.

The Cleared tab opens.

Figure 3-45



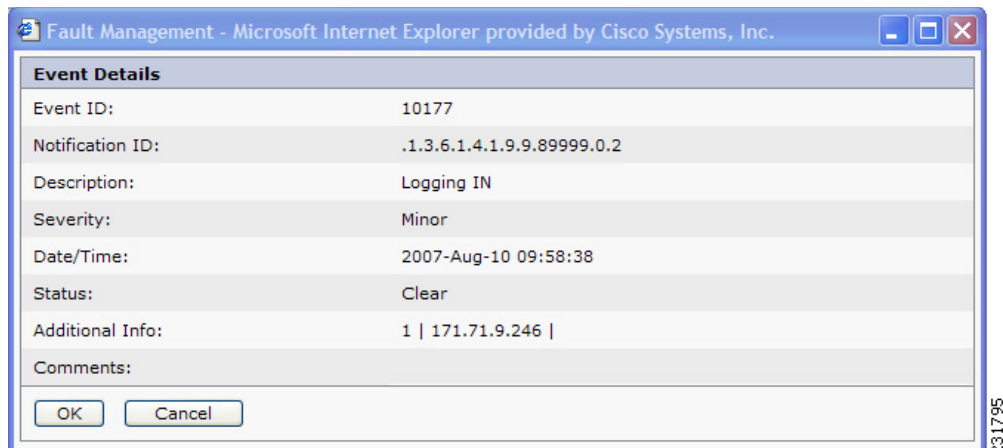
Cleared Events [Total: 7]							
<input type="checkbox"/>	Event ID	Device ID	Severity	Time of Occurrence	Time Cleared	Event Group	Status
<input type="checkbox"/>	10177	171.71.8.109	Warning	2007-Aug-10 09:58:38	2007-Aug-10 16:36:48	A Group	Clear
<input type="checkbox"/>	10176	171.71.8.109	Warning	2007-Aug-10 09:57:40	2007-Aug-10 16:36:48	A Group	Clear
<input type="checkbox"/>	10160	171.71.8.109	Warning	2007-Aug-07 17:27:24	2007-Aug-09 14:59:12	A Group	Clear
<input type="checkbox"/>	10159	171.71.8.109	Warning	2007-Aug-07 17:20:59	2007-Aug-09 15:04:59	A Group	Clear
<input type="checkbox"/>	10156	171.71.8.109	Warning	2007-Aug-07 11:57:13	2007-Aug-09 14:58:26	A Group	Clear

Buttons: Annotate, Notify, Delete, Refresh, Help

Step 3 To view details of an event, click on the event's **Event ID**.

The Event Details window appears.

Figure 3-46



Event Details	
Event ID:	10177
Notification ID:	.1.3.6.1.4.1.9.9.89999.0.2
Description:	Logging IN
Severity:	Minor
Date/Time:	2007-Aug-10 09:58:38
Status:	Clear
Additional Info:	1 171.71.9.246
Comments:	

Buttons: OK, Cancel

Step 4 To close the window, click **OK** or **Cancel**.

How to Annotate Cleared Events

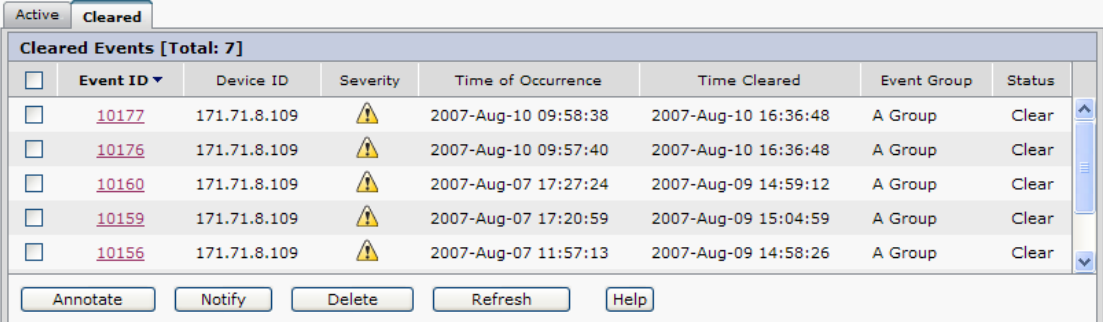
Step 1 In the Navigation pane, select **Device Management > Fault Management**.

The Fault Management screen appears in the Configuration pane.

Step 2 Click the **Cleared** tab.

The Cleared tab opens.

Figure 3-47



Cleared Events [Total: 7]							
<input type="checkbox"/>	Event ID	Device ID	Severity	Time of Occurrence	Time Cleared	Event Group	Status
<input type="checkbox"/>	10177	171.71.8.109	Warning	2007-Aug-10 09:58:38	2007-Aug-10 16:36:48	A Group	Clear
<input type="checkbox"/>	10176	171.71.8.109	Warning	2007-Aug-10 09:57:40	2007-Aug-10 16:36:48	A Group	Clear
<input type="checkbox"/>	10160	171.71.8.109	Warning	2007-Aug-07 17:27:24	2007-Aug-09 14:59:12	A Group	Clear
<input type="checkbox"/>	10159	171.71.8.109	Warning	2007-Aug-07 17:20:59	2007-Aug-09 15:04:59	A Group	Clear
<input type="checkbox"/>	10156	171.71.8.109	Warning	2007-Aug-07 11:57:13	2007-Aug-09 14:58:26	A Group	Clear

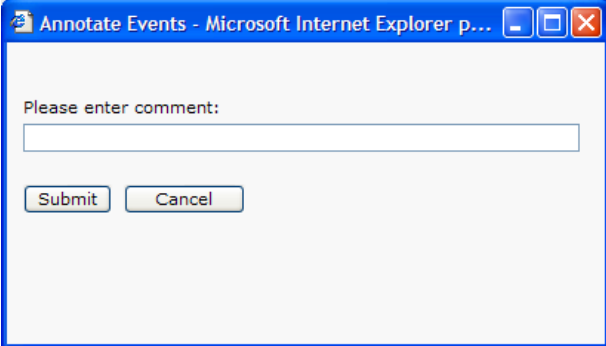
Buttons: Annotate, Notify, Delete, Refresh, Help

Step 3 Check the check box next to the event or events to which you want to add a comment.

Step 4 Click **Annotate**.

The Annotate Events window appears.

Figure 3-48



Annotate Events - Microsoft Internet Explorer p...

Please enter comment:

Submit Cancel

Step 5 In the Please enter comments field, enter the comments that you want to add to the event or events.

Step 6 Click **Submit**.

The comment is saved.

**Note**

A new comment will replace any existing text in an event's Comments field.

How to Send Cleared Event Notifications

Step 1 In the Navigation pane, select **Device Management > Fault Management**.

The Fault Management screen appears in the Configuration pane.

Step 2 Click the **Cleared** tab.

The Cleared tab opens.

Figure 3-49

Cleared Events [Total: 7]							
<input type="checkbox"/>	Event ID ▾	Device ID	Severity	Time of Occurrence	Time Cleared	Event Group	Status
<input type="checkbox"/>	10177	171.71.8.109	⚠	2007-Aug-10 09:58:38	2007-Aug-10 16:36:48	A Group	Clear
<input type="checkbox"/>	10176	171.71.8.109	⚠	2007-Aug-10 09:57:40	2007-Aug-10 16:36:48	A Group	Clear
<input type="checkbox"/>	10160	171.71.8.109	⚠	2007-Aug-07 17:27:24	2007-Aug-09 14:59:12	A Group	Clear
<input type="checkbox"/>	10159	171.71.8.109	⚠	2007-Aug-07 17:20:59	2007-Aug-09 15:04:59	A Group	Clear
<input type="checkbox"/>	10156	171.71.8.109	⚠	2007-Aug-07 11:57:13	2007-Aug-09 14:58:26	A Group	Clear

Step 3 Check the check box next to the event or events for which you want to send notifications.

Step 4 Click **Notify**.

The Event Notification window appears.

Figure 3-50

Notify

SMTP Server: mailman.cisco.com

Sender: user1@cisco.com

Sender Comments: (Optional) Comments

Recipient Address(es): user2@cisco.com

OK Cancel

**Note**

The SMTP Server listed in the Event Notification window is configured in the

- Step 5** In the Sender Address field, enter the e-mail address that should be displayed the From field of the notification.
- Step 6** In the Sender Comments field, enter text to be sent with the Event Notification.
- Step 7** In the Recipient Address(es) field, enter the e-mail address or addresses of the people who should receive the notification.
- Step 8** Click **Submit**.
The notification is sent and the Event Notification window closes.
- Step 9** Click **Submit**.
The notification is sent and the Event Notification window closes.

How to Delete Cleared Events

- Step 1** In the Navigation pane, select **Device Management > Fault Management**.
The Fault Management screen appears in the Configuration pane.
- Step 2** Click the **Cleared** tab.
The Cleared tab opens.

Figure 3-51

<input type="checkbox"/>	Event ID	Device ID	Severity	Time of Occurrence	Time Cleared	Event Group	Status
<input type="checkbox"/>	10177	171.71.8.109	Warning	2007-Aug-10 09:58:38	2007-Aug-10 16:36:48	A Group	Clear
<input type="checkbox"/>	10176	171.71.8.109	Warning	2007-Aug-10 09:57:40	2007-Aug-10 16:36:48	A Group	Clear
<input type="checkbox"/>	10160	171.71.8.109	Warning	2007-Aug-07 17:27:24	2007-Aug-09 14:59:12	A Group	Clear
<input type="checkbox"/>	10159	171.71.8.109	Warning	2007-Aug-07 17:20:59	2007-Aug-09 15:04:59	A Group	Clear
<input type="checkbox"/>	10156	171.71.8.109	Warning	2007-Aug-07 11:57:13	2007-Aug-09 14:58:26	A Group	Clear

Buttons: Annotate, Notify, Delete, Refresh, Help

- Step 3** Check the check box next to the event or events for which you want to send notifications.
- Step 4** Click **Delete**.
The Cleared Events list reappears without the deleted Cleared Events.

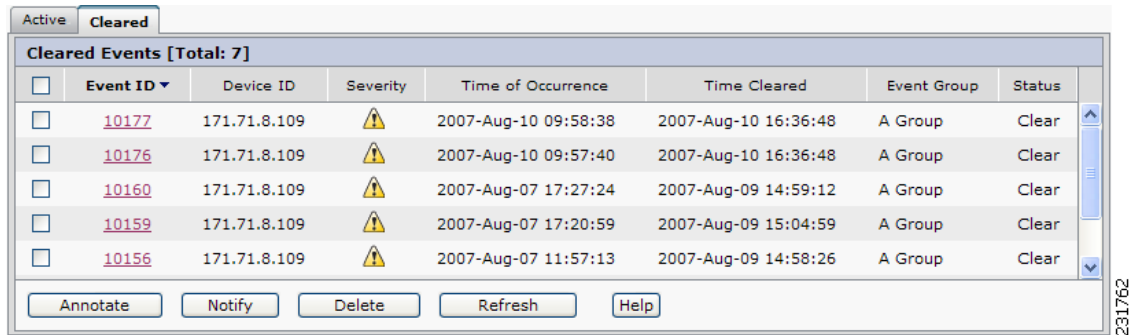
How to Refresh the Display of Cleared Events

- Step 1** In the Navigation pane, select **Device Management > Fault Management**.
The Fault Management screen appears in the Configuration pane.

231762

- Step 2** Click the **Cleared** tab.
The Cleared tab opens.

Figure 3-52



Cleared Events [Total: 7]							
<input type="checkbox"/>	Event ID ▼	Device ID	Severity	Time of Occurrence	Time Cleared	Event Group	Status
<input type="checkbox"/>	10177	171.71.8.109	⚠	2007-Aug-10 09:58:38	2007-Aug-10 16:36:48	A Group	Clear
<input type="checkbox"/>	10176	171.71.8.109	⚠	2007-Aug-10 09:57:40	2007-Aug-10 16:36:48	A Group	Clear
<input type="checkbox"/>	10160	171.71.8.109	⚠	2007-Aug-07 17:27:24	2007-Aug-09 14:59:12	A Group	Clear
<input type="checkbox"/>	10159	171.71.8.109	⚠	2007-Aug-07 17:20:59	2007-Aug-09 15:04:59	A Group	Clear
<input type="checkbox"/>	10156	171.71.8.109	⚠	2007-Aug-07 11:57:13	2007-Aug-09 14:58:26	A Group	Clear

Annotate Notify Delete Refresh Help

- Step 3** Click **Refresh**.
The Cleared Events list reappears with the updated list of Cleared Events.

How to Sort Cleared Events

- Step 1** In the Navigation pane, select **Device Management > Fault Management**.
The Fault Management screen appears in the Configuration pane.
- Step 2** Click the **Cleared** tab.
The Cleared tab opens.

Figure 3-53



Cleared Events [Total: 7]							
<input type="checkbox"/>	Event ID ▼	Device ID	Severity	Time of Occurrence	Time Cleared	Event Group	Status
<input type="checkbox"/>	10177	171.71.8.109	⚠	2007-Aug-10 09:58:38	2007-Aug-10 16:36:48	A Group	Clear
<input type="checkbox"/>	10176	171.71.8.109	⚠	2007-Aug-10 09:57:40	2007-Aug-10 16:36:48	A Group	Clear
<input type="checkbox"/>	10160	171.71.8.109	⚠	2007-Aug-07 17:27:24	2007-Aug-09 14:59:12	A Group	Clear
<input type="checkbox"/>	10159	171.71.8.109	⚠	2007-Aug-07 17:20:59	2007-Aug-09 15:04:59	A Group	Clear
<input type="checkbox"/>	10156	171.71.8.109	⚠	2007-Aug-07 11:57:13	2007-Aug-09 14:58:26	A Group	Clear

Annotate Notify Delete Refresh Help

- Step 3** Click on the column heading by which you would like to sort the events.
The Cleared Events list reappears sorted by the selected column.

Fault Configurations









This module contains information about configuring Faults. Faults conditions are predefined but the descriptions and severity of the fault conditions can be modified.

- [How to View Fault Configurations, page 3-33](#)
- [How to Edit Fault Configurations, page 3-33](#)
- [How to Reset Fault Configurations, page 3-34](#)
- [How to Suppress or Unsuppress Fault Configurations, page 3-35](#)
- [How to Configure Email Server Settings for Sending Fault Notifications, page 3-35](#)

How to View Fault Configurations

- Step 1** In the Navigation pane, select **Device Management > Fault Management > Fault Configuration**. The Fault Configuration screen appears in the Configuration pane.









Figure 3-54

Fault Configuration							
<input type="checkbox"/>	Notification ID	Default Description	Current Description	Default Severity	Current Severity	Notify	Suppressed
<input type="checkbox"/>	.1.3.6.1.4.1.9.9.138.2.0.1	User Log full/Clo...	User Log full/Clo...				No
<input type="checkbox"/>	.1.3.6.1.4.1.9.9.138.2.0.2	Alarm Cleared	Alarm Cleared				No
<input type="checkbox"/>	.1.3.6.1.4.1.9.9.630.0.1	Telnet Session Ended	Telnet Session Ended				No
<input type="checkbox"/>	.1.3.6.1.4.1.9.9.630.0.2	Telnet Session St...	Telnet Session St...				No
<input type="button" value="Reset"/> <input type="button" value="(Un)Suppress"/> <input type="button" value="Help"/>							

How to Edit Fault Configurations

- Step 1** In the Navigation pane, select **Device Management > Fault Management > Fault Configuration**. The Fault Configuration screen appears in the Configuration pane.

Figure 3-55

Fault Configuration							
<input type="checkbox"/>	Notification ID	Default Description	Current Description	Default Severity	Current Severity	Notify	Suppressed
<input type="checkbox"/>	.1.3.6.1.4.1.9.9.138.2.0.1	User Log full/Clo...	User Log full/Clo...				No
<input type="checkbox"/>	.1.3.6.1.4.1.9.9.138.2.0.2	Alarm Cleared	Alarm Cleared				No
<input type="checkbox"/>	.1.3.6.1.4.1.9.9.630.0.1	Telnet Session Ended	Telnet Session Ended				No
<input type="checkbox"/>	.1.3.6.1.4.1.9.9.630.0.2	Telnet Session St...	Telnet Session St...				No
<input type="button" value="Reset"/> <input type="button" value="(Un)Suppress"/> <input type="button" value="Help"/>							

- Step 2** Click on the **Notification ID** of the Fault Configuration that you want to edit. The Edit Fault Configuration window appears.

Figure 3-56

231782

- Step 3** In the New Event description field, enter meaningful text to describe the modified fault configuration. If left blank, the Default Event description is used.
- Step 4** In the New Email field, enter the e-mail address of the person to be notified when the event occurs. If left blank, the Default Email is used.
- Step 5** Click **Submit**.
- The new Fault Configuration settings are saved.

How to Reset Fault Configurations

- Step 1** In the Navigation pane, select **Device Management > Fault Management > Fault Configuration**. The Fault Configuration screen appears in the Configuration pane.

Figure 3-57

Fault Configuration							
<input type="checkbox"/>	Notification ID	Default Description	Current Description	Default Severity	Current Severity	Notify	Suppressed
<input type="checkbox"/>	.1.3.6.1.4.1.9.9.138.2.0.1	User Log full/Clo...	User Log full/Clo...				No
<input type="checkbox"/>	.1.3.6.1.4.1.9.9.138.2.0.2	Alarm Cleared	Alarm Cleared				No
<input type="checkbox"/>	.1.3.6.1.4.1.9.9.630.0.1	Telnet Session Ended	Telnet Session Ended				No
<input type="checkbox"/>	.1.3.6.1.4.1.9.9.630.0.2	Telnet Session St...	Telnet Session St...				No
<input type="button" value="Reset"/> <input type="button" value="(Un)Supress"/> <input type="button" value="Help"/>							









231793

- Step 2** Click **Reset**.
- The Fault Configuration is now set to the default description and severity as defined by the MIB.

How to Suppress or Unsuppress Fault Configurations

- Step 1** In the Navigation pane, select **Device Management > Fault Management > Fault Configuration**.
The Fault Configuration screen appears in the Configuration pane.

Figure 3-58

Fault Configuration							
<input type="checkbox"/>	Notification ID	Default Description	Current Description	Default Severity	Current Severity	Notify	Suppressed
<input type="checkbox"/>	.1.3.6.1.4.1.9.9.138.2.0.1	User Log full/Clo...	User Log full/Clo...				No
<input type="checkbox"/>	.1.3.6.1.4.1.9.9.138.2.0.2	Alarm Cleared	Alarm Cleared				No
<input type="checkbox"/>	.1.3.6.1.4.1.9.9.630.0.1	Telnet Session Ended	Telnet Session Ended				No
<input type="checkbox"/>	.1.3.6.1.4.1.9.9.630.0.2	Telnet Session St...	Telnet Session St...				No
<input type="button" value="Reset"/> <input type="button" value="(Un)Suppress"/> <input type="button" value="Help"/>							

- Step 2** Click on the **Notification ID** of the Fault Configuration that you want to suppress.
- Step 3** Click **(Un)Suppress**.
The Fault Configuration's Suppressed field switches from true to false or vice versa.

How to Configure Email Server Settings for Sending Fault Notifications

- Step 1** In the Navigation pane, select **Device Management > Fault Management > Fault Configuration**.
The Fault Configuration screen appears in the Configuration pane with the Email Configuration box in the lower section.

Figure 3-59

Email Configuration	
Outgoing Mail Server & Port:	<input type="text" value="mailman.cisco.com"/> <input type="text" value="25"/>
Username:	<input type="text" value="user1"/>
Password:	<input type="password"/>
<input type="button" value="Save"/> <input type="button" value="Help"/>	

- Step 2** In the Outgoing Mail Server &Port field, enter the DNS name of the Email Server should be used for sending Fault Notifications and the Port Number on the server which receives SMTP requests.
- Step 3** In the Username field, enter a valid username with rights to send email through the Email Server.
- Step 4** In the Password field, enter the password for the username entered in the Username field.
- Step 5** Click **Save**.

The Email Configuration settings are saved and all Fault Notifications will be sent with these settings.

Viewing and Configuring Statistics

- [Statistics Configuration, page 3-36](#)
- [Viewing Statistics, page 3-38](#)

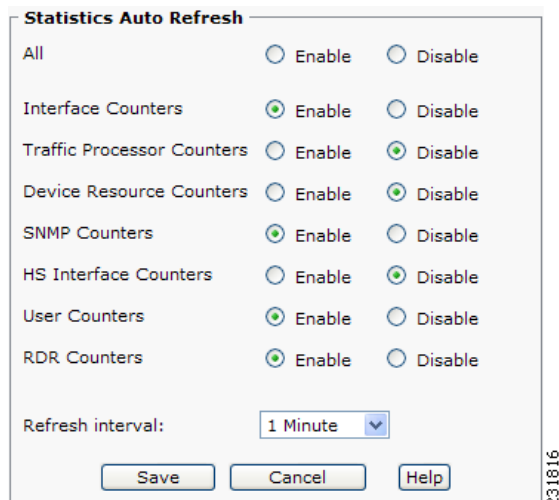
Statistics Configuration

- [How to View Statistics Configurations, page 3-36](#)
- [How to Refresh Statistics Automatically, page 3-36](#)
- [How to Log Statistics, page 3-38](#)

How to View Statistics Configurations

- Step 1** In the Navigation pane, select **Device Management > Statistics > Statistics Configuration**.
The Statistics Configuration screen appears in the Configuration pane.

Figure 3-60



The screenshot shows a dialog box titled "Statistics Auto Refresh". It contains a list of statistics categories, each with "Enable" and "Disable" radio buttons. The "Refresh interval" is set to "1 Minute". At the bottom are "Save", "Cancel", and "Help" buttons. A vertical text "231816" is visible on the right side of the dialog box.

Category	Enable	Disable
All	<input type="radio"/>	<input type="radio"/>
Interface Counters	<input checked="" type="radio"/>	<input type="radio"/>
Traffic Processor Counters	<input type="radio"/>	<input checked="" type="radio"/>
Device Resource Counters	<input type="radio"/>	<input checked="" type="radio"/>
SNMP Counters	<input checked="" type="radio"/>	<input type="radio"/>
HS Interface Counters	<input type="radio"/>	<input checked="" type="radio"/>
User Counters	<input checked="" type="radio"/>	<input type="radio"/>
RDR Counters	<input checked="" type="radio"/>	<input type="radio"/>

Refresh interval:

231816

How to Refresh Statistics Automatically

- Step 1** In the Navigation pane, select **Device Management > Statistics > Statistics Configuration**.
The Statistics Configuration screen appears in the Configuration pane, displaying the Statistics box in the upper section.

Figure 3-61

Statistics Auto Refresh

All ☐ Enable ☐ Disable

Interface Counters ☒ Enable ☐ Disable

Traffic Processor Counters ☐ Enable ☒ Disable

Device Resource Counters ☐ Enable ☒ Disable

SNMP Counters ☒ Enable ☐ Disable

HS Interface Counters ☐ Enable ☒ Disable

User Counters ☒ Enable ☐ Disable

RDR Counters ☒ Enable ☐ Disable

Refresh interval: 1 Minute ▼

Save Cancel Help

231816

Step 2 To enable all statistics, select the All **Enable** radio button.

All Enable forces the individual statistics to the enabled state and All Disable forces the individual statistics to the disabled state.

Figure 3-62

Display Statistics Group

All ☐ Enable ☐ Disable

Interface Counters ☒ Enable ☐ Disable

Traffic Processor Counters ☒ Enable ☐ Disable

Device Resource Counters ☒ Enable ☐ Disable

SNMP Counters ☒ Enable ☐ Disable

HS Interface Counters ☒ Enable ☐ Disable

User Counters ☒ Enable ☐ Disable

RDR Counters ☒ Enable ☐ Disable

Refresh interval: 60 Minutes ▼

Save Reset Help

231818

Step 3 To enable individual statistics, select the **Enable** radio button of the Statistics you want to enable.

Step 4 In the Polling interval drop-down list, select the number of minutes between statistics updates.

Step 5 Click **Save**.

The Statistics Configuration is saved.

How to Log Statistics

**Note**

This function is currently disabled but it will be enabled in a future release.

- Step 1** In the Navigation pane, select **Device Management > Statistics > Statistics Configuration**.
The Statistics Configuration screen appears in the Configuration pane, displaying the Automatic Enable/Disable Statistics box in the lower section.

Figure 3-63



- Step 2** Select the **Enable** radio button.
- Step 3** In the Frequency drop-down list, select the number of minutes between enabling statistics.

Viewing Statistics

- [Device Statistics, page 3-38](#)
- [How to View User Counters, page 3-40](#)
- [How to View RDR Counters, page 3-41](#)

Device Statistics

- [How to View Interface Statistics, page 3-38](#)
- [How to View Traffic Processors, page 3-39](#)
- [How to View Resource Counters, page 3-39](#)
- [How to View SNMP Counters, page 3-40](#)
- [How to View HS Interfaces, page 3-40](#)

How to View Interface Statistics

- Step 1** In the Navigation pane, select **Device Management > Statistics > Device Statistics**.
The Device Statistics screen appears in the Configuration pane open to the Interface tab displaying the Interfaces' counters and statistics.

Figure 3-64

Interface			
Counter	Interface 1		Interface 2
ifIndex	2		3
ifDescr	FastEthernet0/1		FastEthernet0/2
ifType	6		6

How to View Traffic Processors

- Step 1** In the Navigation pane, select **Device Management > Statistics > Device Statistics**.
The Device Statistics screen appears in the Configuration pane.
- Step 2** Click the **Traffic Processors** tab.
The Traffic Processors tab opens displaying the Traffic Processors' counters and statistics.

Figure 3-65

Traffic Processor		
Counter	Value	
Handled Packets	220724	
Handled Flows	29	
Active Flows	1	

How to View Resource Counters

- Step 1** In the Navigation pane, select **Device Management > Statistics > Device Statistics**.
The Device Statistics screen appears in the Configuration pane.
- Step 2** Click the **Resource Counters** tab.
The Resource Counters tab opens displaying the device resources' counters and values.

Figure 3-66

Disk Usage	
Counter	Value
Time	19:20:33
Media Size	18514308

How to View SNMP Counters

- Step 1** In the Navigation pane, select **Device Management > Statistics > Device Statistics**.
The Device Statistics screen appears in the Configuration pane.
- Step 2** Click the **SNMP Counters** tab.
The SNMP Counters tab opens displaying the SNMP counters and values.

Figure 3-67

Counter	Value
snmpInPkts	2575
snmpOutPkts	2574
snmpInBadVersions	0

How to View HS Interfaces

- Step 1** In the Navigation pane, select **Device Management > Statistics > Device Statistics**.
The Device Statistics screen appears in the Configuration pane.
- Step 2** Click the **HS Interfaces** tab.
The HS Interfaces tab opens displaying the HS Interfaces counters and statistics.

Figure 3-68

Counter	Interface 1	Interface 2
ifType	6	6
ifName	FastEthernet0/1	FastEthernet0/2
ifInMulticastPkts	n	n

How to View User Counters

- Step 1** In the Navigation pane, select **Device Management > Statistics > User Counters**.
The User Counters screen appears in the Configuration pane displaying the User counters and values.

Figure 3-69

User Counters		
Counter	Value	
Used Users space	0	211942
Free Users space	499	
Used IP Address mappings	0	

How to View RDR Counters

- Step 1** In the Navigation pane, select **Device Management > Statistics > RDR Counters**.
The RDR Counters screen appears in the Configuration pane displaying the RDR counters and values.

Figure 3-70

RDR Formatter		
Object	Value	
Reports Sent	116	211941
Reports Discarded	0	
Report Rate	0	

Installing Configuration Files

- [How to Install Traffic Control Application Files \(PQI\), page 3-41](#)
- [How to Install Traffic Configuration Files \(PQB\), page 3-42](#)

How to Install Traffic Control Application Files (PQI)

This procedure installs the Traffic Control Application file on a device or a group of devices.

- Step 1** In the Navigation pane, select **Device Management > Installation**.
The Installation screen appears in the Configuration pane.

Figure 3-71

The screenshot shows a configuration dialog box with two main sections: **Destination** and **Source**. The **Destination** section contains a text field labeled "Device/Group:". The **Source** section contains two radio buttons: "Traffic Control Application (.PQI)" and "Traffic Management Configuration (.PQB)". Below the radio buttons is a text field labeled "Image File:" followed by a "Browse..." button. At the bottom of the dialog are three buttons: "Apply", "Cancel", and "Help". A vertical text label "231763" is positioned to the right of the dialog box.

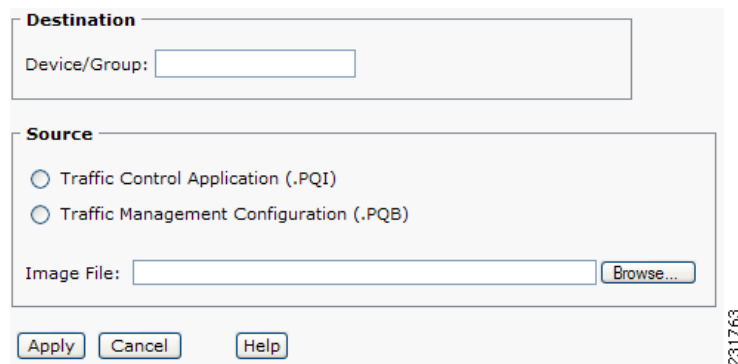
- Step 2** In the Device/Group field, enter the name of the device or group of devices on which you want to install the PQI file.
- Step 3** Click on the Traffic Control Application (.PQI) radio button.
- Step 4** Click **Browse**.
A File Upload dialog box appears.
- Step 5** Browse to the PQI file that you are installing.
- Step 6** Click **Open**.
The File Upload dialog box closes.
- Step 7** Click **Apply**.
A progress bar appears and a completion message is displayed when installation is complete.
The PQI file is installed on the selected device or group of devices.
-

How to Install Traffic Configuration Files (PQB)

This procedure installs the Traffic Configuration file on a device or a group of devices.

- Step 1** In the Navigation pane, select **Device Management > Installation**.
The Installation screen appears in the Configuration pane.

Figure 3-72



The screenshot shows a configuration dialog box with two main sections: **Destination** and **Source**. The **Destination** section contains a text field labeled "Device/Group:". The **Source** section contains two radio buttons: "Traffic Control Application (.PQI)" and "Traffic Management Configuration (.PQB)". Below the radio buttons is a text field labeled "Image File:" followed by a "Browse..." button. At the bottom of the dialog are three buttons: "Apply", "Cancel", and "Help". A vertical text label "231763" is positioned to the right of the dialog box.

- Step 2** In the Device/Group field, enter the name of the device or group of devices on which you want to install the PQB file.
- Step 3** Click on the **Traffic Management Configuration (.PQB)** radio button.
- Step 4** Click **Browse**.
A File Upload dialog box appears.
- Step 5** Browse to the PQB file that you are installing.
- Step 6** Click **Open**.
The File Upload dialog box closes.
- Step 7** Click **Apply**.
A progress bar appears and a completion message is displayed when installation is complete.
The PQB file is installed on the selected device or group of devices.
-



CHAPTER 4

Traffic Management

This module explains the methods by which the operator of the Application Performance Assurance (APA) Device Console identifies and defines the traffic that will be available for reporting from the Network Module Enhanced Application Performance Assurance (NME-APA).

- [Managing Traffic Management Configurations, page 4-1](#)
- [Traffic Classification, page 4-4](#)
- [Signatures, page 4-15](#)
- [Protocols, page 4-15](#)
- [Zones, page 4-21](#)
- [Flavors, page 4-27](#)
- [Traffic Monitoring, page 4-35](#)

Managing Traffic Management Configurations

The APA Device Console is a Graphical User Interface (GUI) which gives the NME-APA operator an intuitive method of modifying NME-APA configurations. Configuration changes are made to an NME-APA device through a process of retrieving the device's configuration for display in the APA Device Console, modifying the configuration parameters in the APA Device Console, and applying the modified configuration back to the NME-APA device.

NME-APA device configurations can also be stored offline in configuration files and restored to NME-APA devices through the configuration Export and Import functions.



Note

The APA Device Console must first be connected to a NME-APA device. For information on connecting to a device, see [Managing Device Connections, page 3-2](#).

- [How to Retrieve the Traffic Management Configuration, page 4-2](#)
- [How to Apply Configuration Changes, page 4-2](#)
- [How to Export a Traffic Management Configuration, page 4-3](#)
- [How to Import a Traffic Management Configuration, page 4-3](#)

How to Retrieve the Traffic Management Configuration

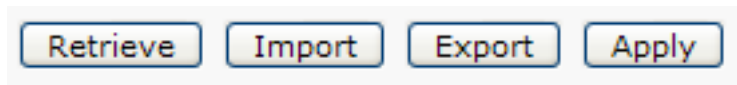
- [Connecting to a Device, page 4-2](#)
- [What to Do Next, page 4-2](#)

Connecting to a Device

Before retrieving a configuration, the APA Device Console must be connected to a device.

-
- Step 1** In the Navigation pane, select any of the children of the **Traffic Management** node.
- The associated screen Configuration screen appears in the Configuration pane, displaying the Retrieve button in the bottom section.

Figure 4-1



- Step 2** Click **Retrieve**.
- The traffic management configuration is retrieved from the NME-APA device and loaded into the APA Device Console.
-

What to Do Next

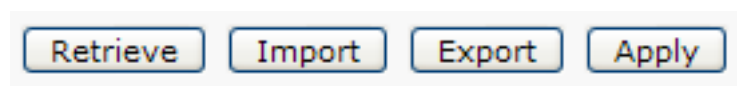
To save the configuration to a file, see [How to Export a Traffic Management Configuration, page 4-3](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 4-2](#).

How to Apply Configuration Changes

The APA Device Console allows you to modify a device's traffic management configuration without implementing the configuration on the device. Once you are ready to use the modified configuration, you must apply it to the device.

-
- Step 1** In the Navigation pane, select any of the children of the **Traffic Management** node.
- The associated Configuration screen appears in the Configuration pane, displaying the Retrieve button in the bottom section.

Figure 4-2



- Step 2** Click **Apply**.

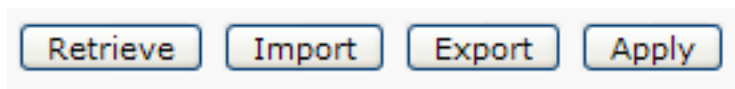
The traffic management configuration is applied to the device.

How to Export a Traffic Management Configuration

A traffic management configuration can be exported and saved to a file so that it can be archived or applied to other devices.

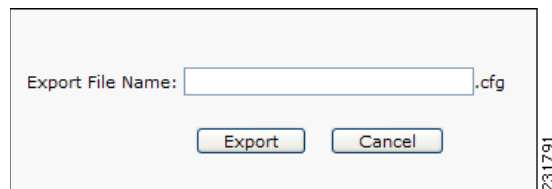
- Step 1** In the Navigation pane, select any of the children of the **Traffic Management** node. The associated Configuration screen appears in the Configuration pane, displaying the Export button in the bottom section.

Figure 4-3



- Step 2** Click **Export**. The Export Configuration dialog box appears.

Figure 4-4



- Step 3** Enter a file name for the configuration file.
- Step 4** Click **Export**. The traffic management configuration is exported to a file.



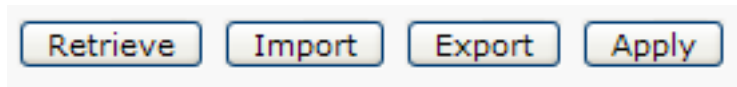
Note To view a list of exported configuration files or to delete exported configuration files, see [How to Import a Traffic Management Configuration, page 4-3](#).

How to Import a Traffic Management Configuration

Traffic Management Configuration

- Step 1** In the Navigation pane, select any of the children of the **Traffic Management** node. The associated Configuration screen appears in the Configuration pane, displaying the Import button in the bottom section.

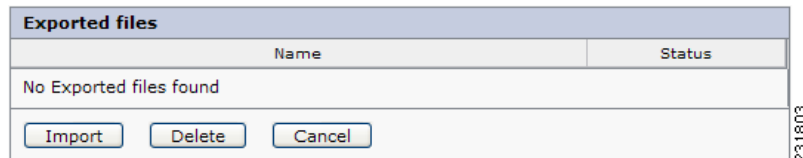
Figure 4-5



Step 2 Click **Import**.

The Import Device Configuration dialog box appears.

Figure 4-6



Step 3 Select the radio button next to the configuration file you want to import.

Step 4 Click **Import**.

The traffic management configuration is imported to the APA Device Console.

What to Do Next

To save the configuration to a file, see [How to Export a Traffic Management Configuration, page 4-3](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 4-2](#).

Traffic Classification

The options in the Global Settings screen are currently disabled and will be enabled in future releases.

Classes

- [How to Add Classes, page 4-4](#)
- [How to Edit Classes, page 4-6](#)
- [How to Delete Classes, page 4-8](#)
- [Managing Class Elements, page 4-10](#)

How to Add Classes

Step 1 In the Navigation pane, select **Traffic Management>Applications>Classes**.

Step 2 Click on the names of the Class Groups until you navigate to the group to which you want to add the new Class.

For the highest level Classes, the list of configured Class Groups appears in the Configuration pane.

Figure 4-7

Classes		
	Class	Type
<input type="radio"/>	Generic	Group (4)
<input type="radio"/>	E-Mail	Group (3)
<input type="radio"/>	Browsing	Group (2)
<input type="radio"/>	Newsgroups	Application
<input type="radio"/>	P2P	Group (7)
<input type="radio"/>	VoIP	Group (9)
<input type="radio"/>	Instant Messaging	Application
<input type="radio"/>	Gaming	Application
<input type="radio"/>	FTP	Application
<input type="radio"/>	Net Admin	Application
<input type="radio"/>	Streaming	Group (3)
<input type="radio"/>	Tunneling	Application
<input type="radio"/>	Oracle	Application
<input type="radio"/>	Citrix	Application
<input type="radio"/>	SAP	Application
<input type="radio"/>	MS SQL	Application
<input type="radio"/>	ActiveX	Application
<input type="button" value="Add Class"/> <input type="button" value="Delete Class"/>		

231761

For lower level classes, the list of Child Classes is shown in the Child Classes box in the lower portion of the Configuration pane when the desired parent class has been selected.

Figure 4-8

Child Classes		
	Class	Type
<input type="radio"/>	Generic TCP	Application
<input type="radio"/>	Generic UDP	Application
<input type="radio"/>	Generic IP	Application
<input type="radio"/>	Generic Upload/Download	Application
<input type="button" value="Add Class"/> <input type="button" value="Delete Class"/>		

231739

Step 3 Click **Add Class**.

The Classes Configuration screen appears in the Configuration pane.

Figure 4-9

Class Details

Name: Generic TCP

Description:

ID: 2

Class Counters

☒ Map to an exclusive Global Counter

Name: Generic TCP Counter

Index: 5

☒ Map to an exclusive User Usage Counter

Name: Generic TCP Counter

Index: 5

Save Cancel Help

231740

- Step 4** In the Name field of the Class Details box, enter the name of the new Class.
- Step 5** In the Description field of the Class Details box, enter a meaningful description of the new Class.
- Step 6** In the ID drop-down list, assign an ID number to the new Class.
- Step 7** Click **Save**.

The new Class is saved in the configuration.

The Class Configuration screen of the parent Class Group reappears in the Configuration pane.

What to Do Next

To save the configuration to a file, see [How to Export a Traffic Management Configuration, page 4-3](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 4-2](#).

How to Edit Classes

- Step 1** In the Navigation pane, select **Traffic Management>Applications>Classes**.
- Step 2** Click on the names of the Class Groups until you navigate to the group containing the Class you want to edit.
- For the highest level Classes, the list of configured Class Groups appears in the Configuration pane.

Figure 4-10

Classes		
	Class	Type
<input type="radio"/>	Generic	Group (4)
<input type="radio"/>	E-Mail	Group (3)
<input type="radio"/>	Browsing	Group (2)
<input type="radio"/>	Newsgroups	Application
<input type="radio"/>	P2P	Group (7)
<input type="radio"/>	VoIP	Group (9)
<input type="radio"/>	Instant Messaging	Application
<input type="radio"/>	Gaming	Application
<input type="radio"/>	FTP	Application
<input type="radio"/>	Net Admin	Application
<input type="radio"/>	Streaming	Group (3)
<input type="radio"/>	Tunneling	Application
<input type="radio"/>	Oracle	Application
<input type="radio"/>	Citrix	Application
<input type="radio"/>	SAP	Application
<input type="radio"/>	MS SQL	Application
<input type="radio"/>	ActiveX	Application
<input type="button" value="Add Class"/> <input type="button" value="Delete Class"/>		

231761

For lower level classes, the list of Child Classes is shown in the Child Classes box in the lower portion of the Configuration pane.

Figure 4-11

Child Classes		
	Class	Type
<input type="radio"/>	Generic TCP	Application
<input type="radio"/>	Generic UDP	Application
<input type="radio"/>	Generic IP	Application
<input type="radio"/>	Generic Upload/Download	Application
<input type="button" value="Add Class"/> <input type="button" value="Delete Class"/>		

231739

- Step 3** Click on the name of the Class you want to edit.
The Class Configuration screen appears in the Configuration pane.

Figure 4-12

Class Details

Name: Generic TCP

Description:

ID: 2

Class Counters

☒ Map to an exclusive Global Counter

Name: Generic TCP Counter

Index: 5

☒ Map to an exclusive User Usage Counter

Name: Generic TCP Counter

Index: 5

Save Cancel Help

231740

- Step 4** In the Name field of the Class Details box, edit the name of Class.
- Step 5** In the Description field of the Class Details box, edit the meaningful description of the Class.
- Step 6** In the ID drop-down list, assign an ID number to the Class.
- Step 7** Click **Save**.

The modified Class is saved in the configuration.

The Class Configuration screen of the parent Class Group reappears in the Configuration pane.

What to Do Next

To save the configuration to a file, see [How to Export a Traffic Management Configuration, page 4-3](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 4-2](#).

How to Delete Classes

- Step 1** In the Navigation pane, select **Traffic Management>Applications>Classes**.
- Step 2** Click on the names of the Class Groups until you navigate to the group containing the Class you want to edit.

For the highest level Classes, the list of configured Class Groups appears in the Configuration pane.

Figure 4-13

Classes		
	Class	Type
<input type="radio"/>	Generic	Group (4)
<input type="radio"/>	E-Mail	Group (3)
<input type="radio"/>	Browsing	Group (2)
<input type="radio"/>	Newsgroups	Application
<input type="radio"/>	P2P	Group (7)
<input type="radio"/>	VoIP	Group (9)
<input type="radio"/>	Instant Messaging	Application
<input type="radio"/>	Gaming	Application
<input type="radio"/>	FTP	Application
<input type="radio"/>	Net Admin	Application
<input type="radio"/>	Streaming	Group (3)
<input type="radio"/>	Tunneling	Application
<input type="radio"/>	Oracle	Application
<input type="radio"/>	Citrix	Application
<input type="radio"/>	SAP	Application
<input type="radio"/>	MS SQL	Application
<input type="radio"/>	ActiveX	Application
<input type="button" value="Add Class"/> <input type="button" value="Delete Class"/>		

For lower level classes, the list of Child Classes is shown in the Child Classes box in the lower portion of the Configuration pane.

Figure 4-14

Child Classes		
	Class	Type
<input type="radio"/>	Generic TCP	Application
<input type="radio"/>	Generic UDP	Application
<input type="radio"/>	Generic IP	Application
<input type="radio"/>	Generic Upload/Download	Application
<input type="button" value="Add Class"/> <input type="button" value="Delete Class"/>		

Step 3 Select the radio button next to the Class you want to delete.

Step 4 Click **Delete Class**.

The Class is removed from the list of Child Classes.

What to Do Next

To save the configuration to a file, see [How to Export a Traffic Management Configuration, page 4-3](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 4-2](#).

Managing Class Elements

- [How to Add Class Elements, page 4-10](#)
- [How to Edit Class Elements, page 4-12](#)
- [How to Delete Class Elements, page 4-13](#)

How to Add Class Elements

- Step 1** In the Navigation pane, select **Traffic Management>Applications>Classes**.
- Step 2** Click on the names of the Class Groups until you navigate to the group containing the Class you want to edit.

For the highest level Classes, the list of configured Class Groups appears in the Configuration pane.

Figure 4-15

Classes		
	Class	Type
<input type="radio"/>	Generic	Group (4)
<input type="radio"/>	E-Mail	Group (3)
<input type="radio"/>	Browsing	Group (2)
<input type="radio"/>	Newsgroups	Application
<input type="radio"/>	P2P	Group (7)
<input type="radio"/>	VoIP	Group (9)
<input type="radio"/>	Instant Messaging	Application
<input type="radio"/>	Gaming	Application
<input type="radio"/>	FTP	Application
<input type="radio"/>	Net Admin	Application
<input type="radio"/>	Streaming	Group (3)
<input type="radio"/>	Tunneling	Application
<input type="radio"/>	Oracle	Application
<input type="radio"/>	Citrix	Application
<input type="radio"/>	SAP	Application
<input type="radio"/>	MS SQL	Application
<input type="radio"/>	ActiveX	Application
<input type="button" value="Add Class"/> <input type="button" value="Delete Class"/>		

For lower level classes, the list of Child Classes is shown in the Child Classes box in the lower portion of the Configuration pane.

Figure 4-16

Child Classes	
Class	Type
<input type="radio"/> Generic TCP	Application
<input type="radio"/> Generic UDP	Application
<input type="radio"/> Generic IP	Application
<input type="radio"/> Generic Upload/Download	Application
<input type="button" value="Add Class"/> <input type="button" value="Delete Class"/>	

231739

Step 3 Click on the name of the Class to which you want to add a Class Element.

The Class Configuration screen appears in the Configuration pane, displaying the Elements box in the middle portion of the screen.

Figure 4-17

Elements			
	Protocol	Initiating Side	Zone Flavor
<input type="radio"/> Generic TCP		Initiated by either side	* *
<input type="radio"/> Generic Non-Established TCP		Initiated by either side	* *
<input type="button" value="Add New Element"/> <input type="button" value="Delete"/>			

231760

Step 4 Click Add New Element.

The Element Details screen appears in the Configuration pane.

Figure 4-18

Element Details	
Protocol	<input type="text" value="Generic TCP"/>
Initiating Side	<input type="text" value="Initiated by either side"/>
Zone	<input type="text" value="*"/>
Flavor	<input type="text" value="*"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>	

231748

Step 5 In the Protocol drop-down list, select the protocol that the Element uses.

Step 6 In the Initiating Side drop-down list, select the method by which communication is initiated.

Step 7 In the Zone drop-down list, select the zone that the Element uses.

Step 8 In the Flavor drop-down list, select the flavor that the Element uses.

Step 9 Click Save.

The new Class Element is saved in the configuration.

The Class Configuration screen of the parent Class reappears in the Configuration pane.

How to Edit Class Elements

- Step 1** In the Navigation pane, select **Traffic Management>Applications>Classes**.
- Step 2** Click on the names of the Class Groups until you navigate to the group containing the Class you want to edit.
- For the highest level Classes, the list of configured Class Groups appears in the Configuration pane.

Figure 4-19

Classes		
	Class	Type
<input type="radio"/>	Generic	Group (4)
<input type="radio"/>	E-Mail	Group (3)
<input type="radio"/>	Browsing	Group (2)
<input type="radio"/>	Newsgroups	Application
<input type="radio"/>	P2P	Group (7)
<input type="radio"/>	VoIP	Group (9)
<input type="radio"/>	Instant Messaging	Application
<input type="radio"/>	Gaming	Application
<input type="radio"/>	FTP	Application
<input type="radio"/>	Net Admin	Application
<input type="radio"/>	Streaming	Group (3)
<input type="radio"/>	Tunneling	Application
<input type="radio"/>	Oracle	Application
<input type="radio"/>	Citrix	Application
<input type="radio"/>	SAP	Application
<input type="radio"/>	MS SQL	Application
<input type="radio"/>	ActiveX	Application
<input type="button" value="Add Class"/> <input type="button" value="Delete Class"/>		

231761

For lower level classes, the list of Child Classes is shown in the Child Classes box in the lower portion of the Configuration pane.

Figure 4-20

Child Classes		
	Class	Type
<input type="radio"/>	Generic TCP	Application
<input type="radio"/>	Generic UDP	Application
<input type="radio"/>	Generic IP	Application
<input type="radio"/>	Generic Upload/Download	Application
<input type="button" value="Add Class"/> <input type="button" value="Delete Class"/>		

231739

- Step 3** Click on the name of the Class to which you want to add a Class Element.
- The Class Configuration screen appears in the Configuration pane, displaying the Elements box in the middle portion of the screen.

Figure 4-21

Elements				
	Protocol	Initiating Side	Zone	Flavor
<input type="radio"/>	Generic TCP	Initiated by either side	*	*
<input type="radio"/>	Generic Non-Established TCP	Initiated by either side	*	*
<input type="button" value="Add New Element"/> <input type="button" value="Delete"/>				

231760

- Step 4** Click the Element that you want to edit.
The Element Details screen appears in the Configuration pane.

Figure 4-22

Element Details	
Protocol	Generic TCP
Initiating Side	Initiated by either side
Zone	*
Flavor	*
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>	

231748

- Step 5** In the Protocol drop-down list, select the protocol that the Element uses.
Step 6 In the Initiating Side drop-down list, select the method by which communication is initiated.
Step 7 In the Zone drop-down list, select the zone that the Element uses.
Step 8 In the Flavor drop-down list, select the flavor that the Element uses.
Step 9 Click **Save**.

The modified Class Element is saved in the configuration.

The Class Configuration screen of the parent Class reappears in the Configuration pane.

How to Delete Class Elements

- Step 1** In the Navigation pane, select **Traffic Management>Applications>Classes**.
Step 2 Click on the names of the Class Groups until you navigate to the group containing the Class you want to edit.
 For the highest level Classes, the list of configured Class Groups appears in the Configuration pane.

Figure 4-23

Classes		
	Class	Type
<input type="radio"/>	Generic	Group (4)
<input type="radio"/>	E-Mail	Group (3)
<input type="radio"/>	Browsing	Group (2)
<input type="radio"/>	Newsgroups	Application
<input type="radio"/>	P2P	Group (7)
<input type="radio"/>	VoIP	Group (9)
<input type="radio"/>	Instant Messaging	Application
<input type="radio"/>	Gaming	Application
<input type="radio"/>	FTP	Application
<input type="radio"/>	Net Admin	Application
<input type="radio"/>	Streaming	Group (3)
<input type="radio"/>	Tunneling	Application
<input type="radio"/>	Oracle	Application
<input type="radio"/>	Citrix	Application
<input type="radio"/>	SAP	Application
<input type="radio"/>	MS SQL	Application
<input type="radio"/>	ActiveX	Application
<input type="button" value="Add Class"/> <input type="button" value="Delete Class"/>		

231761

For lower level classes, the list of Child Classes is shown in the Child Classes box in the lower portion of the Configuration pane.

Figure 4-24

Child Classes		
	Class	Type
<input type="radio"/>	Generic TCP	Application
<input type="radio"/>	Generic UDP	Application
<input type="radio"/>	Generic IP	Application
<input type="radio"/>	Generic Upload/Download	Application
<input type="button" value="Add Class"/> <input type="button" value="Delete Class"/>		

231739

Step 3 Click on the name of the Class to which you want to add a Class Element.

The Class Configuration screen appears in the Configuration pane, displaying the Elements box in the middle portion of the screen.

Figure 4-25

Elements				
	Protocol	Initiating Side	Zone	Flavor
<input type="radio"/>	Generic TCP	Initiated by either side	*	*
<input type="radio"/>	Generic Non-Established TCP	Initiated by either side	*	*
<input type="button" value="Add New Element"/> <input type="button" value="Delete"/>				

Step 4 Select the radio button next to the Class Element you want to delete.

Step 5 Click **Delete**.

The Element is removed from the list of Class Elements.

Signatures

How to View Signatures

Step 1 In the Navigation pane, select **Traffic Management>Applications>Signatures**.

The list of Signatures appears in the Configuration pane.

Figure 4-26

Signatures		
Script		
Signatures		
Show All	Total: 140	
Name	ID	Assigned to protocols
ActiveX	537395200	ActiveX
ATM	537133056	aim

Step 2 You can filter for certain categories of Signatures by selecting a Signature Category from the drop-down list.

The list of Signatures is not editable.

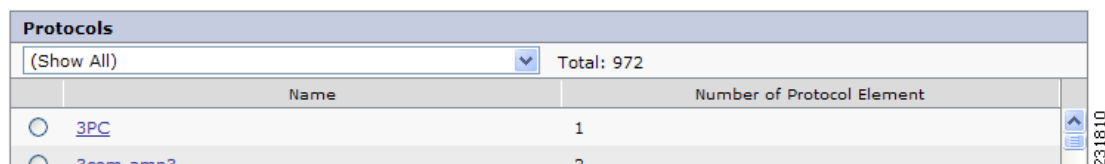
Protocols

- [How to Add Protocols, page 4-16](#)
- [How to Edit Protocols, page 4-16](#)
- [How to Delete Protocols, page 4-17](#)
- [Managing Protocol Elements, page 4-18](#)

How to Add Protocols

- Step 1** In the Navigation pane, select **Traffic Management>Applications>Protocols**.
The list of configured Protocols appears in the Configuration pane.

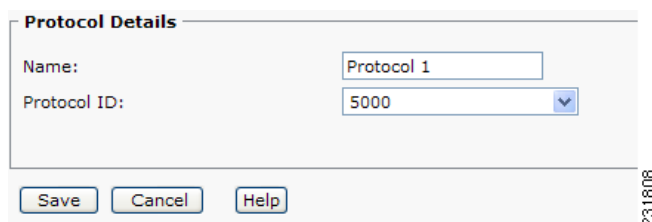
Figure 4-27



Protocols	
(Show All)	Total: 972
Name	Number of Protocol Element
3PC	1
3com-amp3	2

- Step 2** Click **Add Protocol**.
The Protocol Details screen appears in the Configuration pane.

Figure 4-28



Protocol Details

Name:

Protocol ID:

- Step 3** In the Name field, enter the name of the new Protocol.
- Step 4** In the Protocol ID drop-down list, assign an ID number to the new Protocol.
- Step 5** In the Select Parent drop-down list, select a category for the new Protocol .
- Step 6** Click **Save**.
The new Protocol is saved in the configuration.
The Protocol Configuration screen reappears in the Configuration pane.

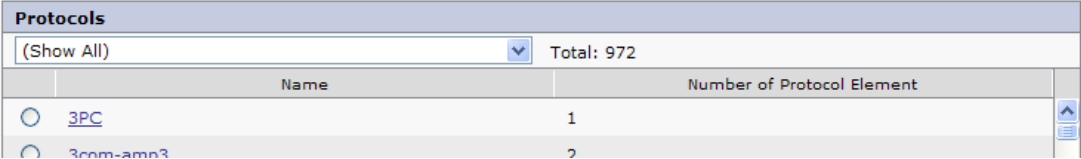
What to Do Next

To save the configuration to a file, see [How to Export a Traffic Management Configuration, page 4-3](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 4-2](#).

How to Edit Protocols

- Step 1** In the Navigation pane, select **Traffic Management>Applications>Protocols**.
The list of configured Protocols appears in the Configuration pane.

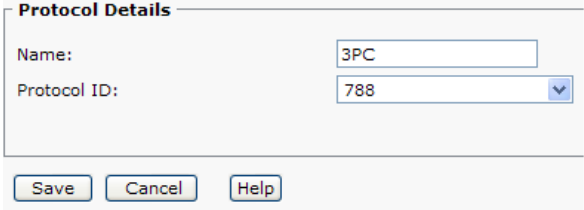
Figure 4-29



Protocols	
(Show All) Total: 972	
Name	Number of Protocol Element
3PC	1
3com-amp3	2

- Step 2** Click the name of the Protocol you want to edit.
The Protocol Details screen appears in the Configuration pane.

Figure 4-30



Protocol Details

Name:

Protocol ID:

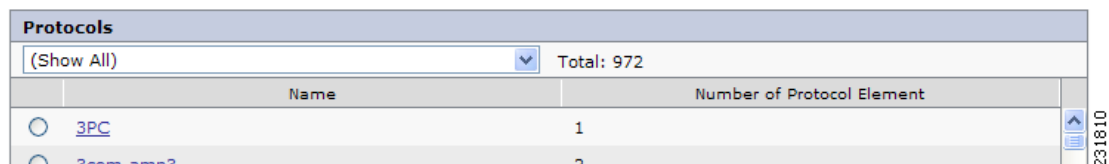
- Step 3** In the Name field, modify the name of the new Protocol.
- Step 4** In the Protocol ID drop-down list, assign an ID number to the Protocol.
- Step 5** In the Select Parent drop-down list, select a category for the new Protocol .
- Step 6** Click **Save**.
The modified Protocol is saved in the configuration.
The Protocol Configuration screen reappears in the Configuration pane.

What to Do Next

To save the configuration to a file, see [How to Export a Traffic Management Configuration, page 4-3](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 4-2](#).

How to Delete Protocols

- Step 1** In the Navigation pane, select **Traffic Management>Applications>Protocols**.
The list of configured Protocols appears in the Configuration pane.

Figure 4-31

Protocols	
(Show All) Total: 972	
Name	Number of Protocol Element
3PC	1
3com-amp3	2

Step 2 Select the radio button next to the Protocol you want to delete.

Step 3 Click **Delete Protocol**.

The Protocol is removed from the list of Protocols.

What to Do Next

To save the configuration to a file, see [How to Export a Traffic Management Configuration, page 4-3](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 4-2](#).

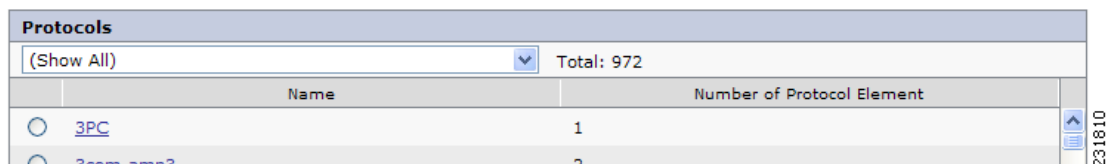
Managing Protocol Elements

- [How to Add Protocol Elements, page 4-18](#)
- [How to Edit Protocol Elements, page 4-19](#)
- [How to Delete Protocol Elements, page 4-21](#)

How to Add Protocol Elements

Step 1 In the Navigation pane, select **Traffic Management>Applications>Protocols**.

The list of configured Protocols appears in the Configuration pane.

Figure 4-32

Protocols	
(Show All) Total: 972	
Name	Number of Protocol Element
3PC	1
3com-amp3	2

Step 2 Click the name of the Protocol to which you want to add an Element.

The Protocol Details screen appears in the Configuration pane, displaying the Protocol Elements box in the lower portion of the screen.

Figure 4-33

Protocol Elements		
Signature	IP Protocol	Port Range
*	3PC	*

Step 3 Click **Add New Element**.

The Element Details screen appears in the Configuration pane.

Figure 4-34

Element Details

Signature: *
 IP Protocol: 3PC
 Port Range Min: *
 Port Range Max: *

Step 4 In the Signature drop-down list, select a Signature for the Element.

Step 5 In the IP Protocol drop-down list, select a Protocol for the Element.

Step 6 In the Port Range Min field, enter the lowest port number for the Element.

Step 7 In the Port Range Max field, enter the highest port number for the Element.

Step 8 Click **Save**.

The new Protocol Element is saved in the configuration.

The Protocol Details screen reappears in the Configuration pane.

What to Do Next

To save the configuration to a file, see [How to Export a Traffic Management Configuration, page 4-3](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 4-2](#).

How to Edit Protocol Elements

Step 1 In the Navigation pane, select **Traffic Management>Applications>Protocols**.

The list of configured Protocols appears in the Configuration pane.

Figure 4-35

Protocols		
(Show All) ▼		Total: 972
	Name	Number of Protocol Element
<input type="radio"/>	3PC	1
<input type="radio"/>	3com-amp3	2

Step 2 Click the name of the Protocol of which you want to edit an Element.

The Protocol Details screen appears in the Configuration pane, displaying the Protocol Elements box in the lower portion of the screen.

Figure 4-36

Protocol Elements			
	Signature	IP Protocol	Port Range
<input type="radio"/>	*	3PC	*
<input type="button" value="Add New Element"/> <input type="button" value="Delete"/>			

Step 3 Click the name of the Element that you want to Edit.

The Element Details screen appears in the Configuration pane.

Figure 4-37

Element Details	
Signature	<input type="text" value="*"/>
IP Protocol	<input type="text" value="3PC"/>
Port Range Min	<input type="text" value="*"/>
Port Range Max	<input type="text" value="*"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>	

Step 4 In the Signature drop-down list, select a Signature for the Element.

Step 5 In the IP Protocol drop-down list, select a Protocol for the Element.

Step 6 In the Port Range Min field, edit the lowest port number for the Element.

Step 7 In the Port Range Max field, edit the highest port number for the Element.

Step 8 Click **Save**.

The modified Protocol Element is saved in the configuration.

The Protocol Details screen reappears in the Configuration pane.

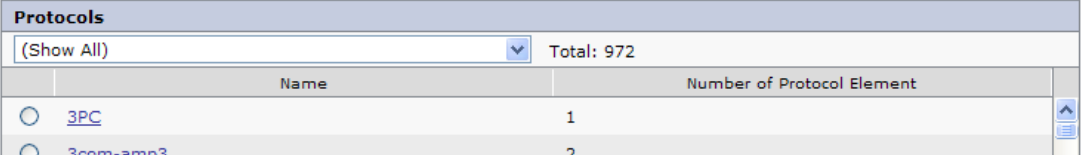
What to Do Next

To save the configuration to a file, see [How to Export a Traffic Management Configuration, page 4-3](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 4-2](#).

How to Delete Protocol Elements

- Step 1** In the Navigation pane, select **Traffic Management>Applications>Protocols**.
The list of configured Protocols appears in the Configuration pane.

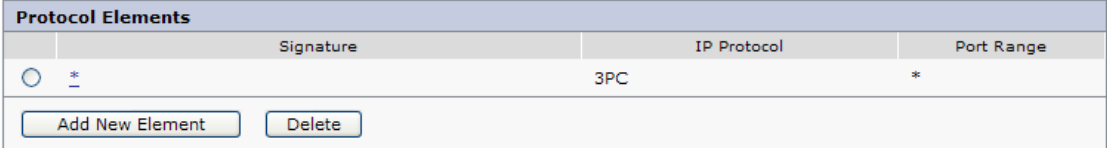
Figure 4-38



Protocols		
(Show All) ▼		Total: 972
	Name	Number of Protocol Element
<input type="radio"/>	3PC	1
<input type="radio"/>	3com-amp3	2

- Step 2** Click the name of the Protocol for which you want to delete an Element.
The Protocol Details screen appears in the Configuration pane, displaying the Protocol Elements box in the lower portion of the screen.

Figure 4-39



Protocol Elements			
	Signature	IP Protocol	Port Range
<input type="radio"/>	*	3PC	*

- Step 3** Select the radio button next to the Protocol Element you want to delete.
Step 4 Click **Delete**.

The Protocol Element is removed from the list of Protocol Elements.

What to Do Next

To save the configuration to a file, see [How to Export a Traffic Management Configuration, page 4-3](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 4-2](#).

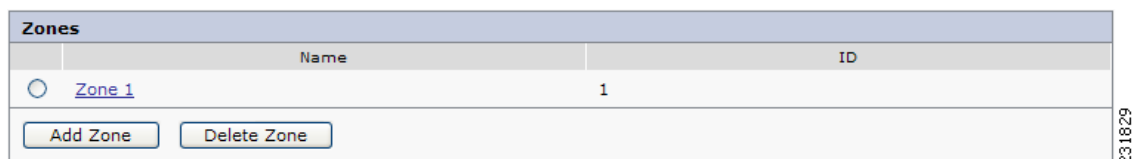
Zones

- [How to Add Zones, page 4-22](#)
- [How to Edit Zones, page 4-23](#)
- [How to Delete Zones, page 4-24](#)
- [Managing Zone Elements, page 4-24](#)

How to Add Zones

- Step 1** In the Navigation pane, select **Traffic Management>Applications>Zones**.
The list of configured Zones appears in the Configuration pane.

Figure 4-40

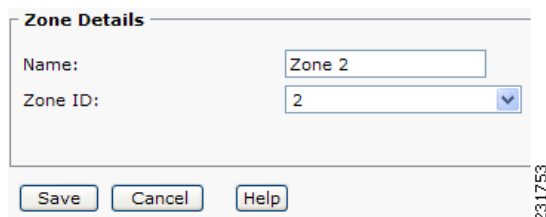


Zones	
Name	ID
Zone 1	1

Add Zone Delete Zone

- Step 2** Click **Add Zone**.
The Zone Details screen appears in the Configuration pane.

Figure 4-41



Zone Details

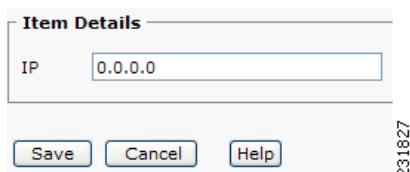
Name: Zone 2

Zone ID: 2

Save Cancel Help

- Step 3** In the Name field, enter a meaningful name for the new Zone.
- Step 4** In the Zone ID drop-down list, assign an ID number to the new Zone.
- Step 5** Click **Save**.
The Zone Item Details screen appears in the Configuration pane.

Figure 4-42



Item Details

IP: 0.0.0.0

Save Cancel Help

- Step 6** In the IP field, enter the IP address of the Zone.
- Step 7** Click **Save**.
The new Zone is saved in the configuration.
The Zone Configuration screen reappears in the Configuration pane.

What to Do Next

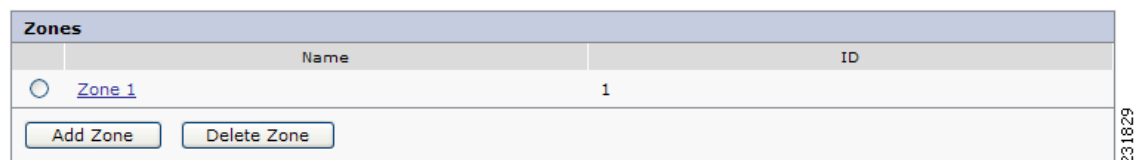
To save the configuration to a file, see [How to Export a Traffic Management Configuration, page 4-3](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 4-2](#).

How to Edit Zones

Step 1 In the Navigation pane, select **Traffic Management>Applications>Zones**.

The list of configured Zones appears in the Configuration pane.

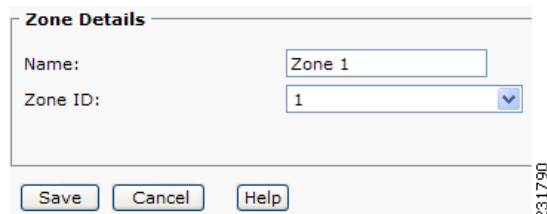
Figure 4-43



Step 2 Click on the Zone that you want to edit.

The Zone Details screen appears in the Configuration pane.

Figure 4-44



Step 3 In the Name field, enter a meaningful name for the new Zone.

Step 4 In the Zone ID drop-down list, assign an ID number to the Zone.

Step 5 Click **Save**.

The modified Zone is saved in the configuration.

The Zone Configuration screen reappears in the Configuration pane.

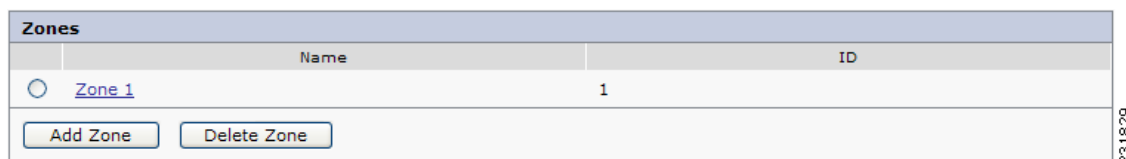
What to Do Next

To save the configuration to a file, see [How to Export a Traffic Management Configuration, page 4-3](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 4-2](#).

How to Delete Zones

- Step 1** In the Navigation pane, select **Traffic Management>Applications>Zones**.
The list of configured Zones appears in the Configuration pane.

Figure 4-45



- Step 2** Select the radio button next to the Zone you want to delete.
- Step 3** Click **Delete**.
The Zone is removed from the list of Zones.

What to Do Next

To save the configuration to a file, see [How to Export a Traffic Management Configuration, page 4-3](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 4-2](#).

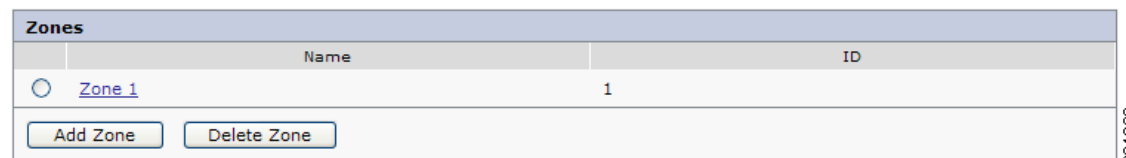
Managing Zone Elements

- [How to Add Zone Elements, page 4-24](#)
- [How to Edit Zone Elements, page 4-25](#)
- [How to Delete Zone Elements, page 4-26](#)

How to Add Zone Elements

- Step 1** In the Navigation pane, select **Traffic Management>Applications>Zones**.
The list of configured Zones appears in the Configuration pane.

Figure 4-46



Step 2 Click on the Zone to which you want to add an Item.

The Zone Details screen appears in the Configuration pane, displaying the Zone Elements box in the lower portion of the screen.

Figure 4-47

Zone Items	
<input type="radio"/>	192.16.1.1 IP / Mask

Step 3 Click **Add New Element**.

The Item Details screen appears in the Configuration pane.

Figure 4-48

Item Details

IP

Step 4 In the IP field, enter the IP address of the new Zone Item.

Step 5 Click **Save**.

The new Zone Item is saved in the configuration.

The Zone Details screen reappears in the Configuration pane.

How to Edit Zone Elements

Step 1 In the Navigation pane, select **Traffic Management>Applications>Zones**.

The list of configured Zones appears in the Configuration pane.

Figure 4-49

Zones	
Name	ID
Zone 1	1

Step 2 Click on the Zone to which you want to add an Item.

The Zone Details screen appears in the Configuration pane, displaying the Zone Elements box in the lower portion of the screen.

Figure 4-50

Zone Items	
	IP / Mask
<input type="radio"/>	192.16.1.1

- Step 3** Click on the Zone Item you want to edit.
The Item Details screen appears in the Configuration pane.

Figure 4-51

Item Details

IP

- Step 4** In the IP field, edit the IP address of the Zone Item.
- Step 5** Click **Save**.
The modified Zone Item is saved in the configuration.
The Zone Details screen reappears in the Configuration pane.

How to Delete Zone Elements

- Step 1** In the Navigation pane, select **Traffic Management>Applications>Zones**.
The list of configured Zones appears in the Configuration pane.

Figure 4-52

Zones	
Name	ID
<input type="radio"/> Zone 1	1

- Step 2** Click on the Zone for which you want to delete an Item.
The Zone Details screen appears in the Configuration pane, displaying the Zone Elements box in the lower portion of the screen.

Figure 4-53

Zone Items	
<input type="radio"/>	192.16.1.1 IP / Mask

Step 3 Select the radio button next to the Zone Item you want to delete.

Step 4 Click **Delete**.

The Zone Item is removed from the list of Zone Elements.

Flavors

- [How to Add Flavors, page 4-27](#)
- [How to Edit Flavors, page 4-28](#)
- [How to Delete Flavors, page 4-30](#)
- [Managing Flavor Elements, page 4-31](#)

How to Add Flavors

Step 1 In the Navigation pane, select **Traffic Management>Applications>Flavors**.

The list of Flavor Groups appears in the Configuration pane.

Figure 4-54

Flavor Groups

	Name	ID	Number in Group
<input type="radio"/>	HTTP Composite	0	0
<input type="radio"/>	HTTP User Agent	1	1
<input type="radio"/>	HTTP URL	2	0
<input type="radio"/>	RTSP Composite	16	0
<input type="radio"/>	RTSP User Agent	17	0
<input type="radio"/>	RTSP Host Name	19	0
<input type="radio"/>	SIP Composite	32	0
<input type="radio"/>	SIP Source Domain	36	1
<input type="radio"/>	SIP Destination Domain	37	1
<input type="radio"/>	SMTP Host Name	51	0

Add Flavor

Help

31798

Step 2 Click on the Flavor Group to which you want to add the new Flavor.

The list of Flavors in the Flavor Group appear in the Configuration pane.

Figure 4-55

Flavor		
	Name	ID
<input type="radio"/>	HTTP Streaming Agents	100
<div>Add FlavorDelete Flavor</div>		

You can also go directly to the list of Flavors by selecting your desired Flavor Group from the Navigation pane.

Step 3 Click **Add Flavor**.

The Flavor Details box appears at the top of the screen.

Figure 4-56

Flavor Details	
Name:	<input type="text" value="Flavor 1"/>
Flavor ID:	<input type="text" value="1"/>
<div>SaveCancel</div>	

Step 4 In the Name field, enter a meaningful name of the new Flavor.

Step 5 In the Flavor ID field, enter the ID number of the new Flavor.

Step 6 Click **Save**.

The new Flavor is saved in the configuration.

The Flavor list the parent Flavor Group reappears in the Configuration pane.

What to Do Next

To save the configuration to a file, see [How to Export a Traffic Management Configuration, page 4-3](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 4-2](#).

How to Edit Flavors

Step 1 In the Navigation pane, select **Traffic Management>Applications>Flavors**.

The list of Flavor Groups appears in the Configuration pane.

Figure 4-57

Flavor Groups			
	Name	ID	Number in Group
<input type="radio"/>	HTTP Composite	0	0
<input type="radio"/>	HTTP User Agent	1	1
<input type="radio"/>	HTTP URL	2	0
<input type="radio"/>	RTSP Composite	16	0
<input type="radio"/>	RTSP User Agent	17	0
<input type="radio"/>	RTSP Host Name	19	0
<input type="radio"/>	SIP Composite	32	0
<input type="radio"/>	SIP Source Domain	36	1
<input type="radio"/>	SIP Destination Domain	37	1
<input type="radio"/>	SMTP Host Name	51	0
<input type="button" value="Add Flavor"/> <input type="button" value="Help"/>			

231798

- Step 2** Click on the Flavor Group in which you want to edit a Flavor.
The list of Flavors in the Flavor Group appear in the Configuration pane.

Figure 4-58

Flavor	
	ID
<input type="radio"/> HTTP Streaming Agents	100
<input type="button" value="Add Flavor"/> <input type="button" value="Delete Flavor"/>	

231799

You can also go directly to the list of Flavors by selecting your desired Flavor Group from the Navigation pane.

- Step 3** Click the name of the Flavor you want to edit.
The Flavor Details box appears at the top of the screen.

Figure 4-59

Flavor Details

Name:

Flavor ID:

231783

- Step 4** In the Name field, edit th meaningful name of the Flavor.
Step 5 In the Flavor ID field, edit the ID number of the Flavor.
Step 6 Click **Save**.
 The modified Flavor is saved in the configuration.

The Flavor list of the parent Flavor Group reappears in the Configuration pane.

What to Do Next

To save the configuration to a file, see [How to Export a Traffic Management Configuration, page 4-3](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 4-2](#).

How to Delete Flavors

Step 1 In the Navigation pane, select **Traffic Management>Applications>Flavors**.

The list of Flavor Groups appears in the Configuration pane.

Figure 4-60

Flavor Groups			
	Name	ID	Number in Group
<input type="radio"/>	HTTP Composite	0	0
<input type="radio"/>	HTTP User Agent	1	1
<input type="radio"/>	HTTP URL	2	0
<input type="radio"/>	RTSP Composite	16	0
<input type="radio"/>	RTSP User Agent	17	0
<input type="radio"/>	RTSP Host Name	19	0
<input type="radio"/>	SIP Composite	32	0
<input type="radio"/>	SIP Source Domain	36	1
<input type="radio"/>	SIP Destination Domain	37	1
<input type="radio"/>	SMTP Host Name	51	0
<input type="button" value="Add Flavor"/> <input type="button" value="Help"/>			

231798

Step 2 Click on the Flavor Group to which you want to add the new Flavor.

The list of Flavors in the Flavor Group appear in the Configuration pane.

Figure 4-61

Flavor		
	Name	ID
<input type="radio"/>	HTTP Streaming Agents	100
<input type="button" value="Add Flavor"/> <input type="button" value="Delete Flavor"/>		

231799

You can also go directly to the list of Flavors by selecting your desired Flavor Group from the Navigation pane.

Step 3 Select the radio button next to the Flavor you want to delete.

Step 4 Click **Delete**.

The Flavor is removed from the list of Flavors.

What to Do Next

To save the configuration to a file, see [How to Export a Traffic Management Configuration, page 4-3](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 4-2](#).

Managing Flavor Elements

- [How to Add Flavor Elements, page 4-31](#)
- [How to Edit Flavor Elements, page 4-32](#)
- [How to Delete Flavor Elements, page 4-34](#)

How to Add Flavor Elements

- Step 1** In the Navigation pane, select **Traffic Management>Applications>Flavors**.
The list of Flavor Groups appears in the Configuration pane.


Figure 4-62

Flavor Groups			
	Name	ID	Number in Group
<input type="radio"/>	HTTP Composite	0	0
<input type="radio"/>	HTTP User Agent	1	1
<input type="radio"/>	HTTP URL	2	0
<input type="radio"/>	RTSP Composite	16	0
<input type="radio"/>	RTSP User Agent	17	0
<input type="radio"/>	RTSP Host Name	19	0
<input type="radio"/>	SIP Composite	32	0
<input type="radio"/>	SIP Source Domain	36	1
<input type="radio"/>	SIP Destination Domain	37	1
<input type="radio"/>	SMTP Host Name	51	0
<input type="button" value="Add Flavor"/> <input type="button" value="Help"/>			

231798

- Step 2** Click on the Flavor Group to which the Flavor belongs.
The list of Flavors in the Flavor Group appear in the Configuration pane.



Figure 4-63

Flavor	
Name	ID
 HTTP Streaming Agents	100
<input type="button" value="Add Flavor"/> <input type="button" value="Delete Flavor"/>	

You can also go directly to the list of Flavors by selecting your desired Flavor Group from the Navigation pane.

- Step 3** Click on the Flavor to which you want to add a Flavor Element.
The Flavor Elements are displayed in the box below the Flavor Details.

Figure 4-64

HTTP Streaming Agents	
User Agent	
 contype	
 NSPlayer	

- Step 4** Click **Add New Element**.
The Flavor Item Details screen appears in the Configuration pane.

Figure 4-65

Flavor Item Details	
User Agent Name:	<input type="text" value="*"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

- Step 5** In the Host Suffix field, enter the Host Suffix of the Flavor.
Step 6 Click **Save**.
The new Flavor Element is saved in the configuration.
The Flavor Details screen reappears in the Configuration pane.

How to Edit Flavor Elements

- Step 1** In the Navigation pane, select **Traffic Management>Applications>Flavors**.
The list of Flavor Groups appears in the Configuration pane.

Figure 4-66

Flavor Groups		
	Name	ID
<input type="radio"/>	HTTP Composite	0
<input type="radio"/>	HTTP User Agent	1
<input type="radio"/>	HTTP URL	2
<input type="radio"/>	RTSP Composite	16
<input type="radio"/>	RTSP User Agent	17
<input type="radio"/>	RTSP Host Name	19
<input type="radio"/>	SIP Composite	32
<input type="radio"/>	SIP Source Domain	36
<input type="radio"/>	SIP Destination Domain	37
<input type="radio"/>	SMTP Host Name	51
<input type="button" value="Add Flavor"/> <input type="button" value="Help"/>		

- Step 2** Click on the Flavor Group to which the Flavor belongs.
The list of Flavors in the Flavor Group appear in the Configuration pane.

Figure 4-67

Flavor	
	ID
<input type="radio"/> HTTP Streaming Agents	100
<input type="button" value="Add Flavor"/> <input type="button" value="Delete Flavor"/>	

You can also go directly to the list of Flavors by selecting your desired Flavor Group from the Navigation pane.

- Step 3** Click on the Flavor for which you want to edit a Flavor Element.
The Flavor Elements are displayed in the box below the Flavor Details.

Figure 4-68

HTTP Streaming Agents	
	User Agent
<input checked="" type="radio"/> contype	
<input type="radio"/> NSPlayer	

- Step 4** Click on the Flavor Element that you want to edit.
The Flavor Item Details screen appears in the Configuration pane.

Figure 4-69



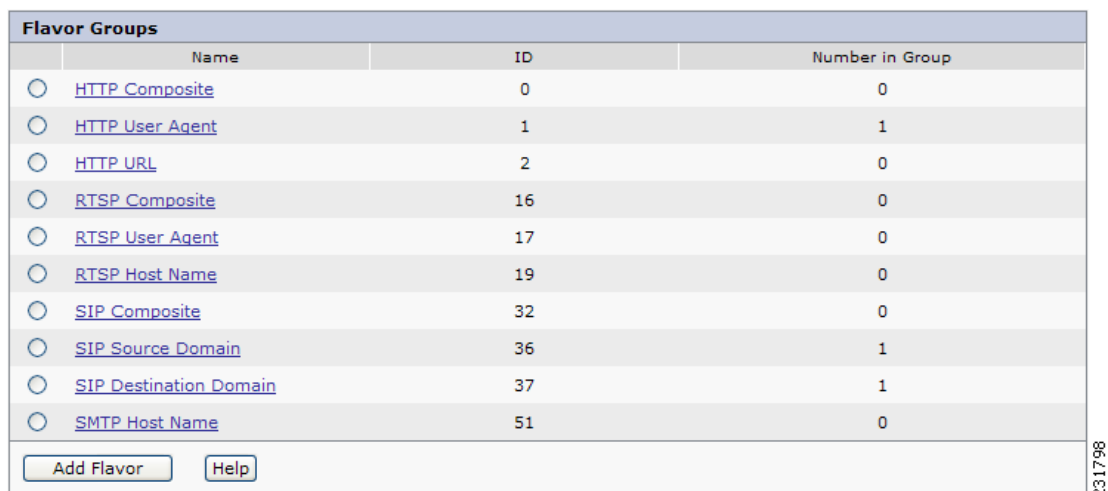
The dialog box titled "Flavor Item Details" contains a label "User Agent Name:" followed by a text input field containing the value "contype". Below the input field are two buttons: "Save" and "Cancel".

- Step 5** In the Host Suffix field, edit the Host Suffix of the Flavor.
- Step 6** Click **Save**.
The modified Flavor Element is saved in the configuration.
The Flavor Details screen reappears in the Configuration pane.

How to Delete Flavor Elements

- Step 1** In the Navigation pane, select **Traffic Management>Applications>Flavors**.
The list of Flavor Groups appears in the Configuration pane.

Figure 4-70



	Name	ID	Number in Group
<input type="radio"/>	HTTP Composite	0	0
<input type="radio"/>	HTTP User Agent	1	1
<input type="radio"/>	HTTP URL	2	0
<input type="radio"/>	RTSP Composite	16	0
<input type="radio"/>	RTSP User Agent	17	0
<input type="radio"/>	RTSP Host Name	19	0
<input type="radio"/>	SIP Composite	32	0
<input type="radio"/>	SIP Source Domain	36	1
<input type="radio"/>	SIP Destination Domain	37	1
<input type="radio"/>	SMTP Host Name	51	0

At the bottom of the table are two buttons: "Add Flavor" and "Help".

- Step 2** Click on the Flavor Group to which the Flavor belongs.
The list of Flavors in the Flavor Group appear in the Configuration pane.

Figure 4-71

Flavor		
	Name	ID
<input type="radio"/>	HTTP Streaming Agents	100
<input type="button" value="Add Flavor"/> <input type="button" value="Delete Flavor"/>		

You can also go directly to the list of Flavors by selecting your desired Flavor Group from the Navigation pane.

- Step 3** Click on the Flavor for which you want to edit a Flavor Element.
The Flavor Elements are displayed in the box below the Flavor Details.

Figure 4-72

HTTP Streaming Agents		
	User Agent	
<input type="radio"/>	contype	
<input type="radio"/>	NSPlayer	

- Step 4** Select the radio button next to the Flavor Element you want to delete.
Step 5 Click **Delete**.
The Flavor Element is removed from the list of Flavor Elements.

Traffic Monitoring

- [How to Configure Usage RDRs, page 4-35](#)
- [How to Configure Transaction RDRs, page 4-36](#)
- [How to Configure Real-Time User RDRs, page 4-37](#)
- [How to Configure Transaction Usage RDRs, page 4-37](#)

How to Configure Usage RDRs

- Step 1** In the Navigation pane, select **Traffic Management>Applications>Monitoring**.
The Monitoring Configuration screen appears in the Configuration pane, displaying the Usage RDRs tab.

Figure 4-73

Usage RDR's Transaction RDR's Real-Time User RDR's Transaction Usage RDR's

Link Usage RDRs

☒ Enable Link Usage RDRs once every minutes for each traffic class

Policy Profile Usage RDRs

☒ Enable Policy Profile Usage RDRs once every minutes for each traffic class

User Usage RDRs

☒ Enable User Usage RDRs once every minutes for each traffic class

Limit the total rate of User Usage RDRs to RDRs per second

Step 2 Modify the fields to produce the desired statistics.

How to Configure Transaction RDRs

- Step 1** In the Navigation pane, select **Traffic Management>Applications>Monitoring**.
The Monitoring Configuration screen appears in the Configuration pane, displaying the Usage RDRs tab.
- Step 2** Select the Transaction RDRs tab.
The Transaction RDRs screen appears.

Figure 4-74

Usage RDR's **Transaction RDR's** Real-Time User RDR's Transaction Usage RDR's

Transaction RDRs represent single network transactions. They can be used to generate statistical histograms that help understand what kind of traffic is traversing the network.

☒ Generate Transaction RDRs

Limit the total rate of Transaction RDRs to RDRs per second

The relativeweight of Transaction RDR rate, for a certain class, determines the relative number of RDRs that will be generated for this class, compared with other classes.

Enabled	Service	Relative Weight
<input checked="" type="checkbox"/>	Default Service	<input type="text" value="10"/>
<input checked="" type="checkbox"/>	Generic	<input type="text" value="10"/>

Step 3 Modify the fields to produce the desired reporting.

How to Configure Real-Time User RDRs

- Step 1** In the Navigation pane, select **Traffic Management>Applications>Monitoring**.
The Monitoring Configuration screen appears in the Configuration pane, displaying the Usage RDRs tab.
- Step 2** Select the Real-Time User RDRs tab.
The Real-Time User RDRs screen appears.

Figure 4-75

Usage RDR's Transaction RDR's **Real-Time User RDR's** Transaction Usage RDR's

Real-Time User Usage RDRs are generated at fixed intervals. They report the amount of usage consumed by an individual user for each class (which was actually used) to allow more granular monitoring of selected users.

☒ Generate Real-Time User Usage RDRs once every minute for each traffic class

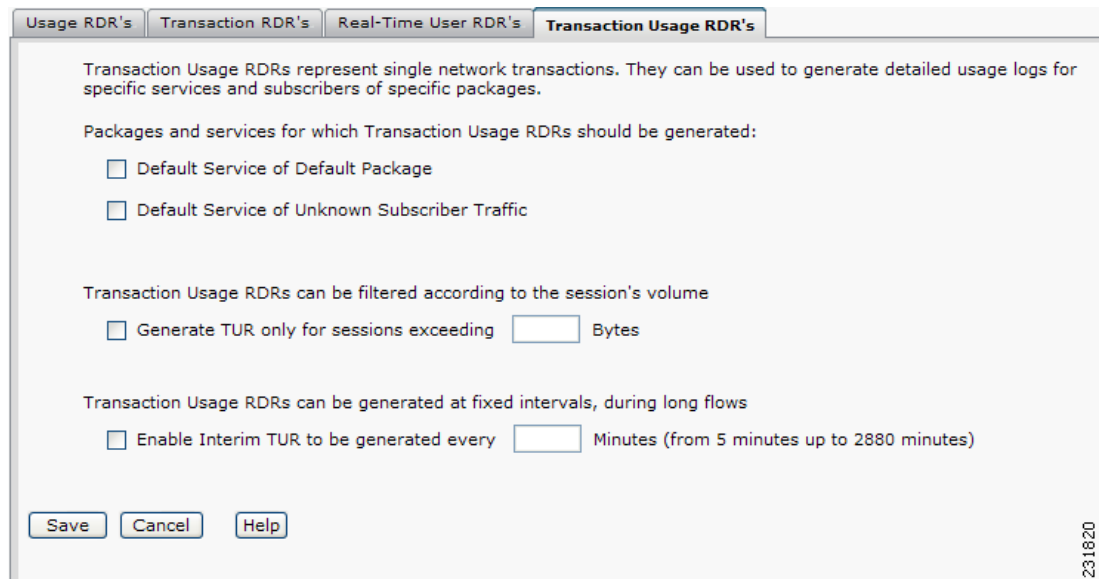
Limit the total rate of Real-Time User Usage RDRs to RDRS per second

- Step 3** Modify the fields to produce the desired statistics.

How to Configure Transaction Usage RDRs

- Step 1** In the Navigation pane, select **Traffic Management>Applications>Monitoring**.
The Monitoring Configuration screen appears in the Configuration pane, displaying the Usage RDRs tab.
- Step 2** Select the Transaction Usage RDRs tab.
The Transaction Usage RDRs screen appears.

Figure 4-76



The image shows a configuration window titled "Transaction Usage RDR's". It has four tabs: "Usage RDR's", "Transaction RDR's", "Real-Time User RDR's", and "Transaction Usage RDR's" (which is selected). The main text area contains the following information:

Transaction Usage RDRs represent single network transactions. They can be used to generate detailed usage logs for specific services and subscribers of specific packages.

Packages and services for which Transaction Usage RDRs should be generated:

- ☐ Default Service of Default Package
- ☐ Default Service of Unknown Subscriber Traffic

Transaction Usage RDRs can be filtered according to the session's volume

- ☐ Generate TUR only for sessions exceeding Bytes

Transaction Usage RDRs can be generated at fixed intervals, during long flows

- ☐ Enable Interim TUR to be generated every Minutes (from 5 minutes up to 2880 minutes)

At the bottom, there are three buttons: "Save", "Cancel", and "Help".

Step 3 Modify the fields to produce the desired statistics.



CHAPTER 5

User Management

This module explains the methods by which the operator of the Application Performance Assurance (APA) Device Console defines the individuals and groups that provide the basis of the system reporting from the Network Module Enhanced Application Performance Assurance (NME-APA).

- [Managing User Configurations, page 5-1](#)
- [User Identification, page 5-4](#)
- [How to Monitor Active Users, page 5-11](#)

Managing User Configurations

The APA Device Console is a Graphical User Interface (GUI) which gives the NME-APA operator an intuitive method of modifying NME-APA configurations. Configuration changes are made to an NME-APA device through a process of retrieving the device's configuration for display in the APA Device Console, modifying the configuration parameters in the APA Device Console, and applying the modified configuration back to the NME-APA device.

NME-APA device configurations can also be stored offline in configuration files and restored to NME-APA devices through the configuration Export and Import functions.



Note

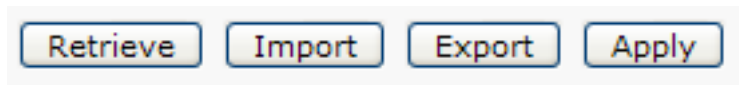
The APA Device Console must first be connected to a NME-APA device. For information on connecting to a device, see [Managing Device Connections, page 3-2](#).

- [How to Retrieve the User Configuration, page 5-1](#)
- [How to Apply Configuration Changes, page 5-2](#)
- [How to Export a User Configuration, page 5-2](#)
- [How to Import the User Configuration, page 5-3](#)

How to Retrieve the User Configuration

Step 1 In the Navigation pane, select **User Management > Provisioning**.

The User Provisioning screen appears in the Configuration pane, displaying the Retrieve button in the bottom section.

Figure 5-1

Step 2 Click **Retrieve** .

The user configuration is retrieved and loaded into the APA Device Console.

What to Do Next

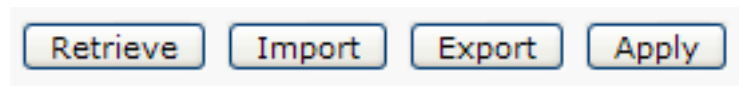
To save the configuration to a file, see [How to Export a User Configuration, page 5-2](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 5-2](#).

How to Apply Configuration Changes

The Excelsior interface allows you to modify a device's configuration without affecting the device. To use the modified configuration, you must apply it to the device.

Step 1 In the Navigation pane, select **User Management > Provisioning** .

The User Provisioning screen appears in the Configuration pane, displaying the Apply button in the bottom section.

Figure 5-2

Step 2 Click **Apply** .

The user configuration is applied to the device.

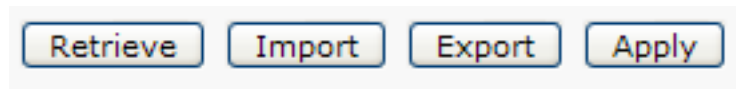
How to Export a User Configuration

A user configuration can be exported and saved to a file so that it can be archived or applied to other devices.

Step 1 In the Navigation pane, select **User Management > Provisioning** .

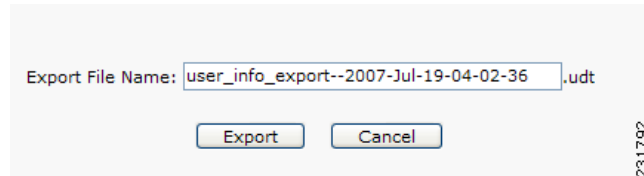
The User Provisioning screen appears in the Configuration pane, displaying the Export button in the bottom section.

Figure 5-3



- Step 2** Click **Export** .
The Export Configuration dialog box appears.

Figure 5-4



- Step 3** Enter a file name for the configuration file.
Step 4 Click **Export** .
The user configuration is exported to a file.

**Note**

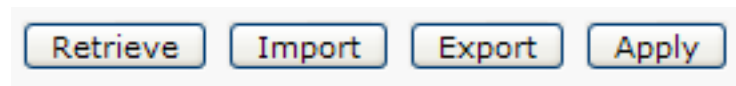
To view a list of exported configuration files or to delete exported configuration files, see [How to Import the User Configuration, page 5-3](#).

How to Import the User Configuration

User Configuration

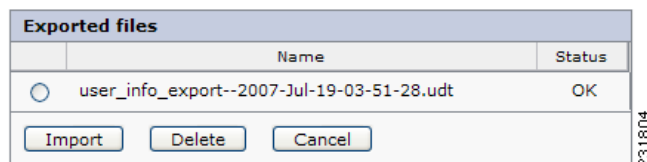
- Step 1** In the Navigation pane, select **User Management >Provisioning** .
The User Provisioning screen appears in the Configuration pane, displaying the Import button in the bottom section.

Figure 5-5



- Step 2** Click **Import** .
The Import Configuration dialog box appears.

Figure 5-6



Step 3 Select the radio button next to the file you want to import.

Step 4 Click **Import** .

The user configuration is imported to the APA Device Console.

What to Do Next

To save the configuration to a file, see [How to Export a User Configuration, page 5-2](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 5-2](#).

User Identification

This module describes the methods by which the operator correlates users or groups with IP address or VLAN information. The NME-APA uses this correlation to identify and report on the users or groups who transmit or receive traffic on the network.

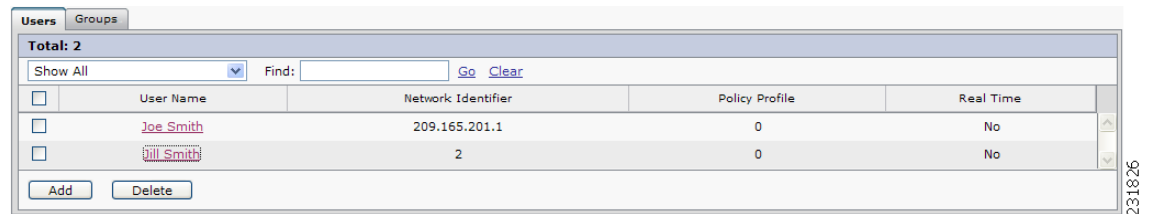
- [How to View Users, page 5-4](#)
- [How to Add Users, page 5-5](#)
- [How to Edit Users, page 5-6](#)
- [How to Delete Users, page 5-7](#)
- [How to View Groups, page 5-8](#)
- [How to Add Groups, page 5-8](#)
- [How to Edit Groups, page 5-10](#)
- [How to Delete Groups, page 5-11](#)

How to View Users

Step 1 In the Navigation pane, select **User Management >Provisioning** .

The User Provisioning screen appears in the Configuration pane with the User tab displaying the list of Users.

Figure 5-7



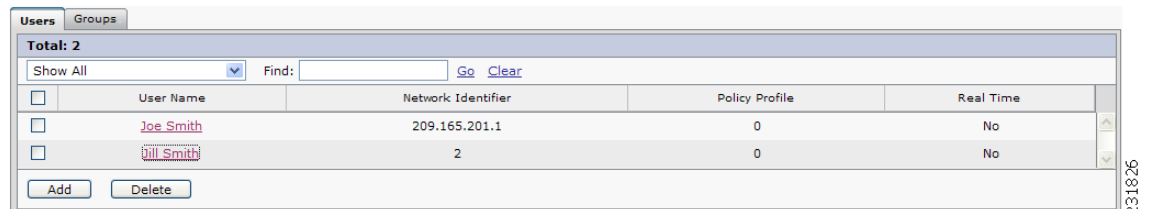
Users				
Total: 2				
Show All Find: Go Clear				
	User Name	Network Identifier	Policy Profile	Real Time
<input type="checkbox"/>	Joe Smith	209.165.201.1	0	No
<input type="checkbox"/>	Bill Smith	2	0	No

Add Delete

How to Add Users

- Step 1** In the Navigation pane, select **User Management > Provisioning** .
- The User Provisioning screen appears in the Configuration pane with the User tab displaying the list of Users.

Figure 5-8

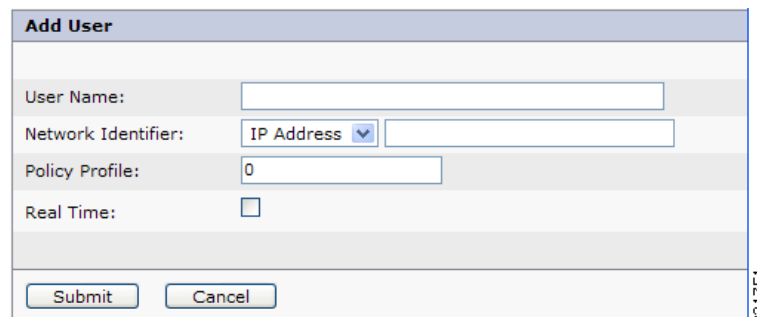


Users				
Total: 2				
Show All Find: Go Clear				
	User Name	Network Identifier	Policy Profile	Real Time
<input type="checkbox"/>	Joe Smith	209.165.201.1	0	No
<input type="checkbox"/>	Bill Smith	2	0	No

Add Delete

- Step 2** Click **Add** .
- The User Management dialog box appears.

Figure 5-9



Add User	
User Name:	<input type="text"/>
Network Identifier:	IP Address <input type="text"/>
Policy Profile:	0
Real Time:	<input type="checkbox"/>
Submit Cancel	

- Step 3** In the User Name field, enter a meaningful name for the user.
- Step 4** In the Network Identifier drop-down list, select a type of network identifier.
- Step 5** In the Network Identifier field, enter the information that will be used to identify the user.

If you selected IP Address, you must enter a valid IP Address in the Network Identifier field.

If you selected IP Range, you may enter a valid IP Address range in the Network Identifier field in slash notation or a list of IP Addresses in a comma separated list.

If you selected VLAN, you must enter the name of the VLAN.

Step 6 In the Profile Policy field, enter the number of the profile policy to associate with this user.

Step 7 If you want the traffic for this user to be logged in real-time, check the Real Time checkbox.

Step 8 Click **Submit**.

The User Management dialog box disappears and the new user is added to the list of users in the Provisioning screen.

What to Do Next

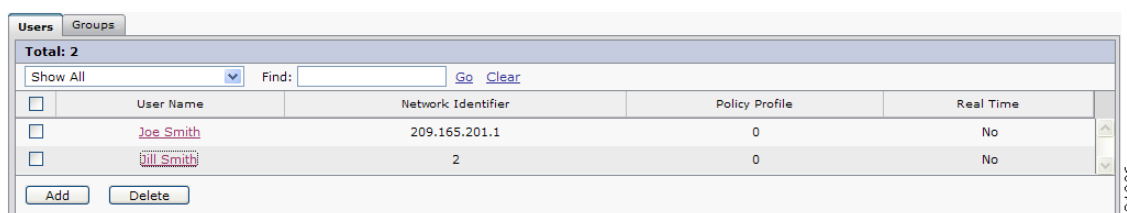
To save the configuration to a file, see [How to Export a User Configuration, page 5-2](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 5-2](#).

How to Edit Users

Step 1 In the Navigation pane, select **User Management >Provisioning**.

The User Provisioning screen appears in the Configuration pane with the User tab displaying the list of Users.

Figure 5-10



Total: 2			
Show All [v] Find: [] Go Clear			
<input type="checkbox"/>	User Name	Network Identifier	Policy Profile
<input type="checkbox"/>	Joe Smith	209.165.201.1	0
<input type="checkbox"/>	Jill Smith	2	0

Real Time: No

Add Delete

Step 2 Click on the User you want to edit.

The User Management dialog box appears.

Figure 5-11

- Step 3** In the User Name field, enter a meaningful name for the user.
- Step 4** In the Network Identifier drop-down list, select a type of network identifier.
- Step 5** In the Network Identifier field, enter the information that will be used to identify the user.
 If you selected IP Address, you must enter a valid IP Address in the Network Identifier field.
 If you selected IP Range, you may enter a valid IP Address range in the Network Identifier field in slash notation or a list of IP Addresses in a comma separated list.
 If you selected VLAN, you must enter the name of the VLAN.
- Step 6** In the Profile Policy field, enter the number of the profile policy to associate with this user.
- Step 7** If you want the traffic for this user to be logged in real-time, check the Real Time checkbox.
- Step 8** Click **Submit** .
- The User Management dialog box disappears and the modified user information is displayed in the list of users in the Provisioning screen.

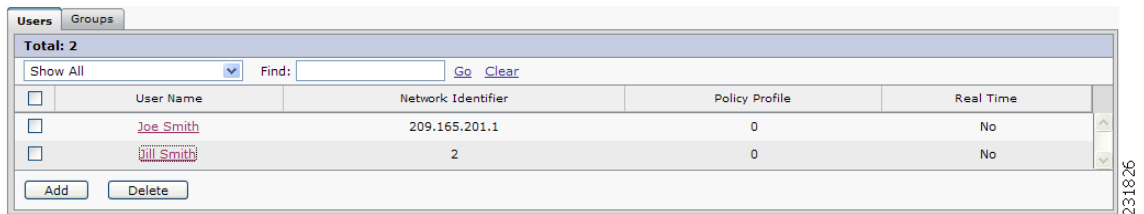
What to Do Next

To save the configuration to a file, see [How to Export a User Configuration, page 5-2](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 5-2](#).

How to Delete Users

- Step 1** In the Navigation pane, select **User Management >Provisioning** .
- The User Provisioning screen appears in the Configuration pane with the User tab displaying the list of Users.

Figure 5-12



Step 2 Select the checkboxes next to the User or Users you want to delete.

Step 3 Click **Delete**.

The User or Users are removed from the list.

What to Do Next

To save the configuration to a file, see [How to Export a User Configuration, page 5-2](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 5-2](#).

How to View Groups

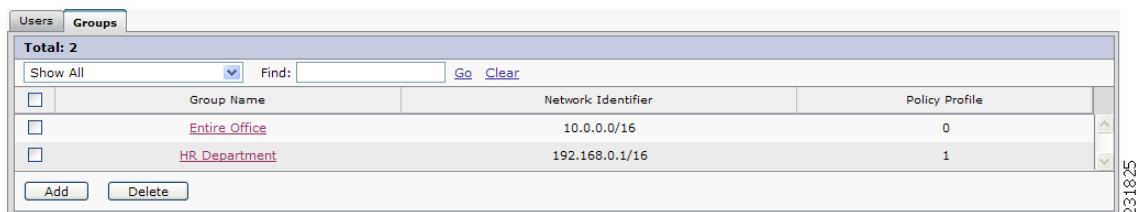
Step 1 In the Navigation pane, select **User Management >Provisioning**.

The User Provisioning screen appears in the Configuration pane with the User tab displaying the list of Users.

Step 2 Select the **Groups** tab.

The Group Provisioning screen appears in the Configuration pane displaying the list of Groups.

Figure 5-13



How to Add Groups

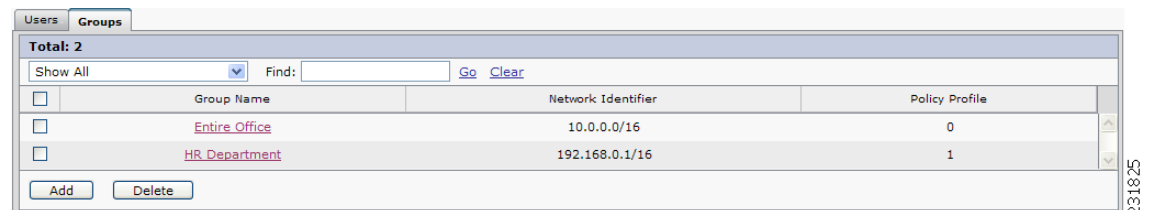
Step 1 In the Navigation pane, select **User Management >Provisioning**.

The User Provisioning screen appears in the Configuration pane with the User tab displaying the list of Users.

Step 2 Select the **Groups** tab.

The Group Provisioning screen appears in the Configuration pane displaying the list of Groups.

Figure 5-14



Step 3 Click **Add**.

The User Management dialog box appears.

Figure 5-15

The screenshot shows the 'Add Group' dialog box. It has three input fields: 'Group Name' with an empty text box, 'Network Identifier' with a dropdown menu set to 'IP Address' and an empty text box, and 'Policy Profile' with a text box containing '0'. At the bottom are 'Submit' and 'Cancel' buttons. A vertical label '231746' is on the right side of the image.

Step 4 In the User Name field, enter a meaningful name for the group.

Step 5 In the Network Identifier drop-down list, select a type of network identifier.

Step 6 In the Network Identifier field, enter the information that will be used to identify the group.

If you selected IP Address, you must enter a valid IP Address in the Network Identifier field.

If you selected IP Range, you may enter a valid IP Address range in the Network Identifier field in slash notation or a list of IP Addresses in a comma separated list.

If you selected VLAN, you must enter the name of the VLAN.

Step 7 In the Profile Policy field, enter the number of the profile policy to associate with this group.

Step 8 Click **Submit**.

The User Management dialog box disappears and new group is displayed in the list of groups in the Provisioning screen.

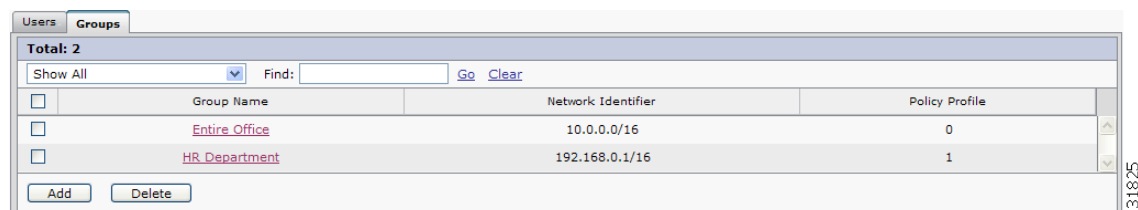
What to Do Next

To save the configuration to a file, see [How to Export a User Configuration, page 5-2](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 5-2](#).

How to Edit Groups

- Step 1** In the Navigation pane, select **User Management >Provisioning** .
- The User Provisioning screen appears in the Configuration pane with the User tab displaying the list of Users.
- Step 2** Select the **Groups** tab.
- The Group Provisioning screen appears in the Configuration pane displaying the list of Groups.

Figure 5-16



- Step 3** Click on the Group or Groups you want to edit.
- The User Management dialog box appears.

Figure 5-17

- Step 4** In the User Name field, enter a meaningful name for the group.
- Step 5** In the Network Identifier drop-down list, select a type of network identifier.
- Step 6** In the Network Identifier field, enter the information that will be used to identify the group.
- If you selected IP Address, you must enter a valid IP Address in the Network Identifier field.
- If you selected IP Range, you may enter a valid IP Address range in the Network Identifier field in slash notation or a list of IP Addresses in a comma separated list.
- If you selected VLAN, you must enter the name of the VLAN.
- Step 7** In the Profile Policy field, enter the number of the profile policy to associate with this group.

Step 8 Click **Submit** .

The User Management dialog box disappears and the modified group information is displayed in the list of groups in the Provisioning screen.

What to Do Next

To save the configuration to a file, see [How to Export a User Configuration, page 5-2](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 5-2](#).

How to Delete Groups

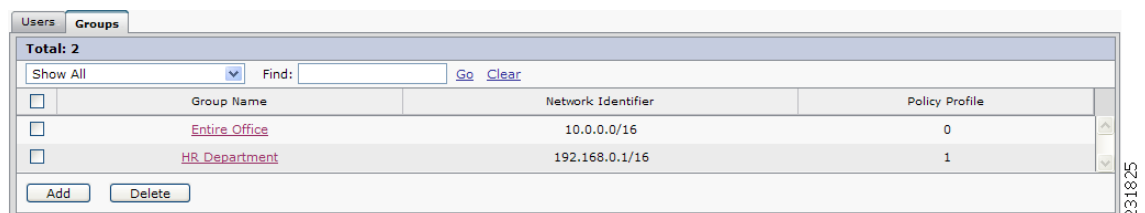
Step 1 In the Navigation pane, select **User Management >Provisioning** .

The User Provisioning screen appears in the Configuration pane with the User tab displaying the list of Users.

Step 2 Select the **Groups** tab.

The Group Provisioning screen appears in the Configuration pane displaying the list of Groups.

Figure 5-18



Total: 2			
Show All [v] Find: [] Go Clear			
<input type="checkbox"/>	Group Name	Network Identifier	Policy Profile
<input type="checkbox"/>	Entire Office	10.0.0.0/16	0
<input type="checkbox"/>	HR Department	192.168.0.1/16	1

Add Delete

Step 3 Select the checkboxes next to the Group or Groups you want to delete.**Step 4** Click **Delete** .

The Group or Groups are removed from the list.

What to Do Next

To save the configuration to a file, see [How to Export a User Configuration, page 5-2](#). To apply the configuration to a device, see [How to Apply Configuration Changes, page 5-2](#).

How to Monitor Active Users

The APA Device Console provides the operator with a real-time view of the users who are passing traffic through the NME-APA.

- Step 1** In the Navigation pane, select **User Management >Monitoring** .
The User Monitoring screen appears in the Configuration pane.

Figure 5-19

Active Users		
User Name	Network Identifier	Policy Profile
No active users available		

231807



CHAPTER 6

Reporting

This module explains the methods by which the operator of the Application Performance Assurance (APA) Device Console defines the data retrieval parameters, as well as the means of converting this data into usable reports from the Network Module Enhanced Application Performance Assurance (NME-APA).

- [Information About Report Groups, page 6-1](#)
- [Reporting Overview, page 6-11](#)
- [Data Retrieval, page 6-13](#)
- [Managing Report Instances, page 6-17](#)

Information About Report Groups

The APA Device Console includes report groups that you use to generate report instances. The groups are organized according to common themes. Each report group allows you to create new report instances. Default filter values are assigned to the properties, some of which are common to all the instances in a given group. You can impose additional constraints by configuring the properties.

You generate a report instance by selecting a report group from the list of available groups in the Groups view.

There are two main categories of reports:

- **Monitoring reports**—Show how network resources are used for selected classes at various granularities (global, package, user)
- **Traffic Discovery reports**—Provide statistical information about network activity and help identify the characteristics of the traffic traversing the network

Report Instance Properties

The following table lists properties that appear in report groups that belong to more than one group group. (Properties of report instances that belong to only one group group are listed with the description of the group.)

Table 6-1 Common Properties of Report Instances

Property	Field Type	Default	Comments
Items to Focus on			
One of the following is included in most report groups:			
Classes to view	Multiple Choice	(not set)	When not set, all classes are selected.
Select classes to view	Multiple Choice	(not set)	When not set, all classes are selected.
Focus on the class	Single Choice	(not set)	When not set, all classes are selected.
One of the following is included in many report groups:			
Package	Single Choice	(not set)	Mandatory property.
Name of user to focus on	Free Text	(not set)	Mandatory property for User group report instances. IP address (decimal format) or user name.
Time Boundaries —See note following table.			
Starting after date	Time/Date	(not set)	
Ending before date	Time/Date	(not set)	When not set, the report is bound to the current time.
From the last number of hours	Free Text	24	Table D-2 Ignored when the Starting After Date and Ending Before Date properties are both set.
From the last number of Days	Free Text	7	

Table 6-1 Common Properties of Report Instances (continued)

Property	Field Type	Default	Comments
Specific Time	Date/Time	(not set)	Mandatory property. Appears in three report instance types instead of the other three time boundary properties. The selected time is rounded to the nearest hour/day.
Traffic Parameters			
Link to Focus	Multiple Choice	(not set)	List of available links to focus.
One of the following is included in many report groups:			
Traffic Direction	Single Choice	Depends on report group	Depends on report group: <ul style="list-style-type: none"> • Direction only • Direction and metric
Metric to order	Single Choice	Depends on report group	Depends on report group and metric: <ul style="list-style-type: none"> • Metric only • Metric and direction
Data Show			
Pick BW Over	Single Choice	1 Hour	
NME-APA IP to view	Single Choice	At installation: (not set) Thereafter: most recent assigned value	Mandatory property. IP address of specific NME-APA device.
Units of results	Single Choice	Depends on report group	
Limit number of results	Free Text	10	
Average Data by Hour	Boolean	TRUE	If this option is selected, a single, average value is calculated for each hour of the report. This option is recommended when generating the report for 24 or more hours.
Show other Consumption	Boolean	FALSE	

Table 6-1 Common Properties of Report Instances (continued)

Property	Field Type	Default	Comments
Aggregation Period	Single Choice	Hourly	
User Id	Free Text	(not set)	Pattern that represent group of users.

- All report instances include the **NME-APA IP to view** property, which enables filtering to a specific NME-APA platform. This property is mandatory and *persistent*. Persistent means that the current value is used for all subsequent reports until the value is changed.
- Time Boundaries properties occur in all report instances except for Top Users, Top Talkers, and Relative Consumption of Top Users. These properties are:
 - Starting After Date
 - Ending Before Date
 - From the Last Number of Hours/Days

The property **From the last number of hours/days** is set to a default value in all report instances. When all three Time Boundaries properties are set, the **From the last number of hours/days** property is ignored. When the property **Ending before date** is not set, the report is bound to the current time.

Information About Monitoring Reports

Monitoring reports provide information about the distribution and consumption of network resources. This information helps you understand how the network is used at different granularities (such as for the entire link, for traffic generated by all users in a particular package usage counter, or for traffic generated by a particular user). These reports are critical for tuning the Class Control solution's configuration according to changing network patterns.

Monitoring reports are created from Link Usage, Package Usage, and Real-Time User Usage Raw Data Records (RDRs). These RDRs (that are generated by the NME-APA platform) provide periodic usage information (at the various granularities) that is processed according to the selected report group to provide the final report.

Monitoring reports typically show a specific *metric* for a set of *class usage counters* at a selected *granularity*, such as bandwidth for P2P and Browsing class usage counters at a link granularity, or volume for the Streaming class usage counter for users in the Gold package usage counter.

You select the class usage counters on which to report via the APA Device Console. The available class usage counters are those defined in the class configuration of the NME-APA platform from which the reports are generated.

- [Granularity, page 6-4](#)
- [Metrics, page 6-5](#)

Granularity

A report instance's granularity controls which traffic the generated report addresses. Three granularities are supported:

- **Global**—Provides visibility into all traffic processed by the NME-APA platforms being reported on. Use global granularity to view the global distribution of network resources (for example, total P2P bandwidth for the last 24 hours).
- **User**—Provides insight into the activity of a single user defined in the Class Control solution. Use user granularity to view how a particular user is using network resources (for example, the number of P2P sessions generated by a particular user for each hour during the last 12 hours). User reports are available for those users flagged for real-time reporting. (For a description of managing real-time user reporting, see the “Using the Class Configuration Editor: Traffic Accounting and Reporting” chapter of the *Cisco Service Control Application for Broadband User Guide*.)

Each report group generates reports in a specific granularity. Each type of report is accessible from the corresponding report group group:

- Global report groups are accessible from the [Global Monitoring Group, page 6-6](#).
- User report groups are accessible from the [User Monitoring Group, page 6-7](#).

Metrics

A metric is the statistic being reported on. The following metrics are available:

- **Bandwidth**—The total bandwidth consumed by the selected classes. By default, a bandwidth report is displayed as a stacked-area chart, where each area indicates the bandwidth used by a particular class.

When generating a bandwidth report, you can select the direction: upstream, downstream, or both.

You can also display an hourly average of bandwidth. This is recommended when you are generating a report for many hours. In this case a single data point per hour is usually sufficient: it reduces the quantity of data displayed, improving performance and the visualization of the data.

- **Volume**—The total volume (in kilobytes or megabytes) for a specific period of time, for the selected class usage counters. As opposed to the bandwidth metric, which provides normalized volume over time, volume reports give the total volume consumed, grouped by specific time durations. By default, a volume report is displayed as a stacked-bar chart, where each bar/series indicates the volume of a particular class usage counter.

Volume reports give the accumulated usage either for specific durations of time (hours or days), or for the entire duration of the report. For example: a Global Hourly Usage Volume report displays a bar that accounts for the total volume consumed by each class usage counter during each hour of the selected time frame, and a Global Aggregated Usage Volume per Class report accounts for all volume of each class usage counter for the entire time frame of the report.

- **Sessions**—The number of sessions. A session is a single network transaction (for example, RTSP stream or P2P file download). By default, a sessions report is displayed as a stacked-bar chart, where each bar/series indicates the total number of sessions of a particular class usage counter.

Like volume reports, sessions reports can be grouped into specific durations (hours or days), in order to account for the total number of sessions in a particular hour/day consumed by a particular class usage counter.

Information About Traffic Discovery Reports

Traffic discovery reports provide raw statistics for analyzing network activities. They are useful for obtaining information about the general activity in the IP network, and they are the key for defining the system's class configuration.

Traffic discovery reports are based on the information in Transaction RDRs.

Traffic discovery reports generate histograms and distribution charts that are grouped by a selected *criterion* and sorted by the selected *order parameter*. For example: a Top Protocols report is sorted by Total Volume, and a Top Web-hosts report is sorted by Hit-Count.

- [Criteria, page 6-6](#)
- [Order Property, page 6-6](#)

Criteria

Each report group focuses on a particular criterion based on Layers 3 to 7, such as:

- Top Servers IP addresses
- Top Server Port numbers
- Top HTTP web-hosts
- Top NNTP news-groups

Order Property

The Metric to order property indicates the value by which the report will be sorted. Possible values are:

- Upstream Volume
- Downstream Volume
- Both Directions Volume—Total upstream and downstream volume
- Hit-Count—Number of transactions

You can limit each report to a specific number of results, which allows you to focus on the top areas of activity (according to the selected value).

Global Monitoring Group

The Global Monitoring group of report groups allows you to view statistics about the traffic bandwidth or volume that was consumed. The bandwidth/volume consumption can be displayed per class for the entire link.

The Global Monitoring group includes the following report groups:

- Global Aggregated Usage Volume per Class—Shows the total volume of traffic (upstream and downstream) for each class usage counter (for all traffic, regardless of user or package)
- Global Bandwidth per Class—Shows the distribution of bandwidth among the different classes defined in the system for all traffic, regardless of user or package
- Global Concurrent Session per Class—Shows the distribution of concurrent sessions among the different class usage counters defined in the system
- Global Hourly Aggregated Minutes per Class—Shows the total number of minutes used for each class usage counter defined in the system, grouped by hour
- Global Hourly Usage Sessions per Class—Shows the distribution of sessions among the different class usage counters defined in the system, grouped by hour
- Global Hourly Usage Volume per Class—Shows the distribution of volume among the different class usage counters defined in the system, grouped by hour

User Monitoring Group

The User Monitoring group of report groups allows you to view statistics about the bandwidth or volume of traffic used by the user. The reports are provided per class usage counter for the total volume consumed by the user. A Top Users report identifies the users that consume the largest traffic volume. User bandwidth and volume reports can be generated for those users configured for real-time monitoring. See “Selecting Users for Real-Time Usage Monitoring” in the “Additional Management Tools and Interfaces” chapter of the *Cisco Service Control Application for Broadband User Guide* for a description of how to configure real-time users.

The User Monitoring group includes the following report groups:

- User Daily Usage Volume per Class—Shows the daily distribution of volume among the different class usage counters defined in the system for a particular user
- Daily Peak BW for Specific User
- User Daily Usage Sessions per Class—Shows the daily distribution of sessions among the different class usage counters defined in the system for a particular user
- Top Users—Shows a list of the top user volume consumption in a specific hour/day
- User Hourly Usage Sessions per Class—Shows the hourly distribution of sessions among the different class usage counters defined in the system for a particular user
- User Hourly Usage Volume per Class—Shows the hourly distribution of volume among the different class usage counters defined in the system for a particular user
- User Bandwidth per Class—Shows the distribution of bandwidth among the different class usage counters defined in the system for a particular user
- User Hourly Aggregated Minutes per Class—Shows the total number of minutes used for each class usage counter for a specific package usage counter defined in the system, grouped by hour
- User Aggregated Usage Volume per Class—Shows the most popular class usage counter for a particular user

Traffic Discovery Group

The Traffic Discovery group of report groups allows you to view statistics compiled from the source and destination IP addresses and ports of the system traffic.

These reports cannot be generated using data collected from an NME-APA platform running in asymmetric routing classification mode.



Note

The reports in this group are not per user; they supply general port and IP address information.

Table 6-2 *Property of Traffic Discovery - Statistics Group Groups only*

Property	Field Type	Default	Comments
Traffic Parameters			
Transport Protocol	Single choice	TCP	

The Traffic Discovery - Statistics group includes the following report groups:

- Top IP Protocols—Shows the most popular IP protocol for certain classes

- Top Client IP to Server Port—Shows the most popular client IP to server port for certain classes
- Top Server IP to Server Port—Shows the most popular server IP to server port for certain classes
- Top Client IP to Server IP and Server Port—Shows the most popular server IP and server port for certain classes.
- Top Client—Shows the most popular client IP for certain classes

**Note**

Client refers to the IP address of the flow initiator. It may be located on the User side or on the Network side.

- Top Servers—Shows the most popular servers for certain classes

**Note**

Server refers to the IP address of the other side of the flow initiator. It may be located on the User side or on the Network side.

- Top Protocols—Shows the most popular protocol for certain classes
- Top Class Ports—Shows the most popular server ports of a certain class or classes
- Top Client IP to Server IP—Shows the most popular client IP to server IP for certain classes
- Top Server Ports—Shows the most popular server ports for certain classes

Demographic Data and Class Popularity Reports Group

The Demographic Data and Class Popularity group of report groups allows you to view statistics of the demographic data.

The Demographic Data and Class Popularity group includes the following report groups:

- Class Popularity among Users—Shows the percentage of users using a specific class defined in the system
- Relative Consumption of Top Users—Shows the relative consumption of a specific number of users compared to “other”
- Global Active User per Class—Shows the distribution of users among the different classes defined in the system for all traffic, regardless of user or package
- Class Popularity among Users (Average)—Shows the total number of users using a specific class compared to users using all other classes
- Package Active User per Class—Shows the distribution of bandwidth among the different classes defined in the system for specific user package

Web and Streaming Reports Group

The Web and Streaming group of report groups allows you to compile statistics presenting the most popular servers or hosts for the various predefined system classes (such as Browsing, Streaming, and Downloading) and for user-defined classes.

These reports cannot be generated using data collected from an NME-APA platform running in asymmetric routing classification mode.

Table 6-3 *Property of Web and Streaming Group Groups only*

Property	Field Type	Default	Comments
Items to Focus on			
Where host is contained	Free Text	(not set)	Filter to hosts containing the given pattern.

The Web and Streaming group includes the following report groups:

- Top FTP Servers—Shows the most popular FTP file hosts
- Top Class Servers—Shows the most popular servers of a certain class or classes
- Top Rtsp Hosts—Shows the most popular real-time streaming protocol (RTSP) servers
- Top Web Hosts—Shows the most popular web servers
- Top MMS Servers—Shows the most popular MMS hosts

Mail and News Reports Group

The Mail and News group of report groups allows you to view statistics of the mail and news traffic.

These reports cannot be generated using data collected from an NME-APA platform running in asymmetric routing classification mode.

The Mail and News group includes the following report groups:

- Top E-mail Account Owners—Shows the top e-mail account owners
- Top NNTP Consumers—Shows the top NNTP consumers
- Top Newsgroups—Shows the most popular newsgroups
- SMTP Server Distribution by User Packages—Shows the most popular SMTP servers, grouped by the package of the requesting user
- Top NNTP Servers—Shows the most popular NNTP hosts
- Top SMTP Servers—Shows the most popular SMTP hosts
- Top E-mail Recipients—Shows the top e-mail recipients
- NNTP Server Distribution by User Packages—Shows the most popular NNTP servers, grouped by the package of the requesting user
- POP3 Server Distribution by User Packages—Shows the most popular POP3 servers, grouped by the package of the requesting user
- Top POP3 Servers—Shows the most popular POP3 hosts
- Top User to Newsgroup—Shows the top user to newsgroup for certain classes
- Top E-mail Sender—Shows the top e-mail sender

P2P Reports Group

The P2P group of report groups allows you to view statistics of the P2P traffic.

These reports cannot be generated using data collected from an NME-APA platform running in asymmetric routing classification mode.

The P2P group includes the following report groups:

- Top P2P Uploaders—Shows the most popular P2P upload consumers
- Top P2P Consumers—Shows a list of the top P2P user volume consumption
- Top P2P Protocols—Shows the most popular P2P protocol for certain classes
- Top P2P Downloaders—Shows the top P2P download consumers
- Top P2P File Extensions—Shows the top file extensions transferred by P2P consumers

VoIP Reports Group

The VoIP group of report groups allows you to view statistics of the VoIP traffic.

These reports cannot be generated using data collected from an NME-APA platform running in asymmetric routing classification mode.

Table 6-4 *Property of VoIP Group Groups only*

Property	Field Type	Default	Comments
Data Show			
Codec to filter	Multiple Choice	(not set)	

The VoIP group includes the following report groups:

- Global Hourly Call Minutes per VoIP Class—Shows the distribution of call minutes among the different VoIP class usage counters defined in the system, grouped by day
- User Bandwidth per VoIP Class—Shows the distribution of bandwidth among the different VoIP classes defined in the system for the traffic of users in a specific package
- Global VoIP Codec Distribution
- Global VoIP Packets Loss
- Top SIP Domains—Shows the most popular SIP Domains
- Global VoIP MOS Distribution
- Package Hourly Call Minutes per VoIP Class—Shows the distribution of call minutes among the different VoIP class usage counters defined in the system, grouped by day
- Global Hourly Average VoIP MOS
- User Hourly Call Minutes per VoIP Class—Shows the distribution of call minutes among the different VoIP class usage counters defined in the system, grouped by day
- Global Hourly Average VoIP Packets Loss
- Global VoIP MOS
- Global VoIP Jitter

- **Top Talkers**—Shows a list of the top talker volume/session/minutes consumption in a specific hour/day for a specific/all VoIP classes
- **Package Bandwidth per VoIP Class**—Shows the distribution of bandwidth among the different VoIP classes defined in the system for the traffic of users in a specific package
- **Packet Concurrent Calls per VoIP Class**—Shows the distribution of concurrent sessions among the different VoIP class usage counters defined in the system, grouped by day
- **Global Concurrent Calls per VoIP Class**—Shows the distribution of concurrent sessions among the different VoIP class usage counters defined in the system, grouped by day
- **Global Bandwidth per VoIP Class**—Shows the distribution of bandwidth among the different VoIP classes defined in the system for all traffic, regardless of user or package
- **Global Hourly Average VoIP Jitter**

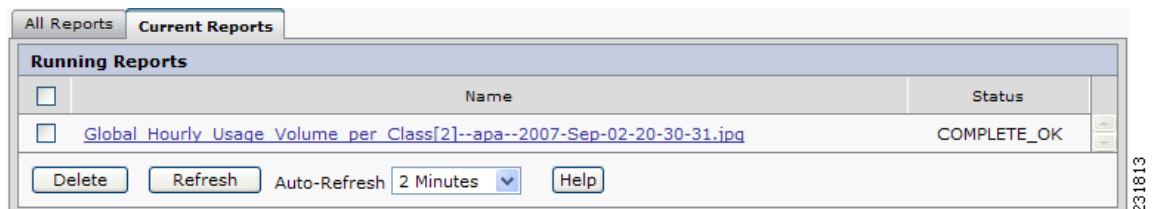
Reporting Overview

- [Viewing Completed Reports and Reports in Progress, page 6-11](#)
- [Deleting Reports in Progress, page 6-11](#)
- [Viewing Report Results, page 6-12](#)

Viewing Completed Reports and Reports in Progress

- Step 1** In the Navigation pane, select **Reporting >Running Reports** .
- The Reports screen appears in the Configuration pane, displaying the list of all Reports.
- Step 2** Select the **Current Reports** tab.
- The Running Reports screen appears listing all reports that are running and those that have completed.

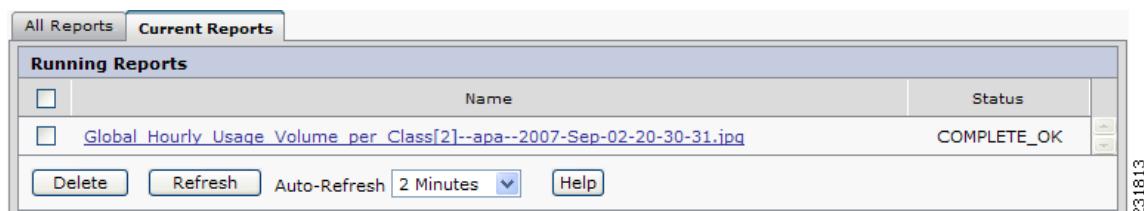
Figure 6-1



To set the frequency for refreshing the list of reports, select the desired frequency in the **Auto-Refresh** drop-down list.

Deleting Reports in Progress

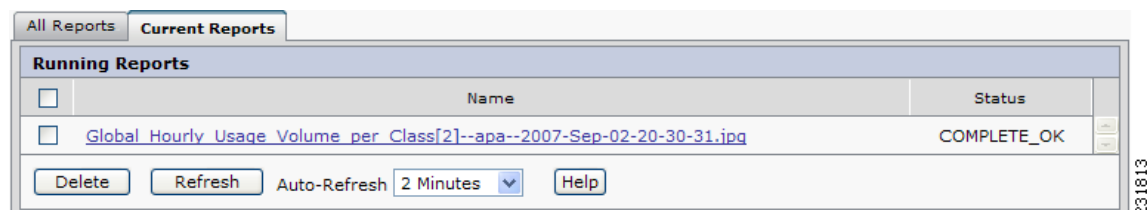
- Step 1** In the Navigation pane, select **Reporting >Running Reports** .
- The Reports screen appears in the Configuration pane, displaying the list of all Reports.
- Step 2** Select the **Current Reports** tab.
- The Running Reports screen appears listing all reports that are running.

Figure 6-2

- Step 3** Select the checkboxes beside the Report or Reports that you want to delete.
- Step 4** Click **Delete** .
- The Report is removed from the list.

Viewing Report Results

- Step 1** In the Navigation pane, select **Reporting >Running Reports** .
- The Reports screen appears in the Configuration pane, displaying the list of all Reports.
- Step 2** Select the **Current Reports** tab.
- The Running Reports screen appears listing all reports that are running.

Figure 6-3

- Step 3** Click on the report that you want to view.
- The Report Result window appears with the results of the report displayed.

**Note**

If the file is a .jpg, you can save it using your browser's Save Picture function. If the file is a .csv, you can right-click on the provided link and select "Save As..."

Data Retrieval

Data can be retrieved immediately by clicking on the **Retrieve Data Now** button in the Data Retrieval screen.



Note

You must be connected to a device to retrieve data.

- [Viewing Scheduled Data Retrieval Tasks, page 6-13](#)
- [Adding Scheduled Data Retrieval Tasks, page 6-14](#)
- [Activating Scheduled Data Retrieval Tasks, page 6-15](#)
- [Deactivating Scheduled Data Retrieval Tasks, page 6-16](#)
- [Deleting Scheduled Data Retrieval Tasks, page 6-16](#)
- [Retrieving Data from Archive, page 6-17](#)

Viewing Scheduled Data Retrieval Tasks

Step 1 In the Navigation pane, select **Reporting >Data Retrieval**.

The Data Retrieval screen appears in the Configuration pane, displaying the Data Retrieval Tasks box in the lower portion.

Figure 6-4

Last Retrieval

Status: COMPLETE_OK
End Time: 2007-Jul-22:21:26:15
Device: 171.71.8.109

Retrive Data Now

Connected Device: tcchen-lnx

[Retrieve Data Now](#)

Data Retrieval Tasks

Task	Device	Start Time	Recurrences	Frequency (Mins)	Status
Currently there are no scheduled RDR Retrieval tasks					

[Add](#) [Activate](#) [Deactivate](#) [Delete](#)

[Import](#) [Export](#)

The **Last Retrieval** in the upper portion of the screen indicates when the last successful Data Retrieval occurred.

Adding Scheduled Data Retrieval Tasks

Step 1 In the Navigation pane, select **Reporting >Data Retrieval** .

The Data Retrieval screen appears in the Configuration pane, displaying the Data Retrieval Tasks box in the lower portion.

Figure 6-5

Last Retrieval

Status: COMPLETE_OK
End Time: 2007-Jul-22:21:26:15
Device: 171.71.8.109

Retrive Data Now

Connected Device: tcchen-lnx

Data Retrieval Tasks

Task	Device	Start Time	Recurrences	Frequency (Mins)	Status
Currently there are no scheduled RDR Retrieval tasks					

The **Last Retrieval** in the upper portion of the screen indicates when the last successful Data Retrieval occurred.

Step 2 Click **Add** .

The Add RDR Task window appears.

Figure 6-6

Add RDR Task - Microsoft Internet Explorer provided by Cisco Syste...

Task Name:

Start Date & Time:

Start Time: Hrs Mins

Repeat Every: Hours Minutes

End After: Occurrences

Device:

Device Level-15 Password:

Step 3 In the Task Name field, enter a meaningful name for the task.

Step 4 Click on the Calendar to select a date.

The Start Date & Time field is disabled, forcing the user to select the date with the Calendar.

- Step 5** In the Start Time fields, enter the hour and minute at which you want the task to begin.
- Step 6** In the Repeat Every field, enter the interval between retrievals in hours and minutes.
- Step 7** In the End After field, enter the number of times you want the retrieval task to occur.
- Step 8** In the Device drop-down list, select the device from which you want to retrieve data.
- Step 9** In the Device Level-15 Password field, enter the enable 15 password for the selected device.
- Step 10** Click **Submit** .

The Data Retrieval screen reappears with the new Data Retrieval Task listed.

Figure 6-7

Data Retrieval Tasks						
	Task	Device	Start Time	Recurrences	Frequency (Mins)	Status
<input type="radio"/>	Hourly Retrieval	apa	2007-09-03 12:00:00	10	60	INACTIVE
<input type="button" value="Add"/> <input type="button" value="Activate"/> <input type="button" value="Deactivate"/> <input type="button" value="Delete"/>						

211940

Activating Scheduled Data Retrieval Tasks

- Step 1** In the Navigation pane, select **Reporting >Data Retrieval** .

The Data Retrieval screen appears in the Configuration pane, displaying the Data Retrieval Tasks box in the lower portion.

Figure 6-8

Data Retrieval Tasks						
	Task	Device	Start Time	Recurrences	Frequency (Mins)	Status
<input type="radio"/>	Hourly Retrieval	apa	2007-09-03 12:00:00	10	60	INACTIVE
<input type="button" value="Add"/> <input type="button" value="Activate"/> <input type="button" value="Deactivate"/> <input type="button" value="Delete"/>						

211940

- Step 2** Select the radio button next to the Retrieval Task that you want to activate.
Active in a task's Status indicates that it will run according to its time parameters. *Inactive* in a task's Status indicates that it will not run until it is activated.
- Step 3** Click **Activate** .
 The Data Retrieval Task shows Active in its Status field and will run according to its time parameters.

Figure 6-9

Data Retrieval Tasks						
	Task	Device	Start Time	Recurrences	Frequency (Mins)	Status
<input type="radio"/>	Hourly Retrieval	apa	2007-09-03 12:00:00	10	60	ACTIVE
<input type="button" value="Add"/> <input type="button" value="Activate"/> <input type="button" value="Deactivate"/> <input type="button" value="Delete"/>						

211931

Deactivating Scheduled Data Retrieval Tasks

Step 1 In the Navigation pane, select **Reporting >Data Retrieval** .

The Data Retrieval screen appears in the Configuration pane, displaying the Data Retrieval Tasks box in the lower portion.

Figure 6-10

Data Retrieval Tasks						
	Task	Device	Start Time	Recurrences	Frequency (Mins)	Status
<input type="radio"/>	Hourly Retrieval	apa	2007-09-03 12:00:00	10	60	ACTIVE
<input type="button" value="Add"/> <input type="button" value="Activate"/> <input type="button" value="Deactivate"/> <input type="button" value="Delete"/>						

211931

Step 2 Select the radio button next to the Retrieval Task that you want to deactivate.

Active in a task's Status indicates that it will run according to its time parameters. *Inactive* in a task's Status indicates that it will not run until it is activated.

Step 3 Click **Deactivate** .

The Data Retrieval Task shows Inactive in its Status field and will not run until it is activated.

Figure 6-11

Data Retrieval Tasks						
	Task	Device	Start Time	Recurrences	Frequency (Mins)	Status
<input type="radio"/>	Hourly Retrieval	apa	2007-09-03 12:00:00	10	60	INACTIVE
<input type="button" value="Add"/> <input type="button" value="Activate"/> <input type="button" value="Deactivate"/> <input type="button" value="Delete"/>						

211940

Deleting Scheduled Data Retrieval Tasks

Step 1 In the Navigation pane, select **Reporting >Data Retrieval** .

The Data Retrieval screen appears in the Configuration pane, displaying the Data Retrieval Tasks box in the lower portion.

Figure 6-12

Data Retrieval Tasks						
	Task	Device	Start Time	Recurrences	Frequency (Mins)	Status
<input type="radio"/>	Hourly Retrieval	apa	2007-09-03 12:00:00	10	60	INACTIVE
<div> Add Activate Deactivate Delete </div>						

211940

Step 2 Select the radio button next to the Retrieval Task you want to delete.

Step 3 Click **Delete** .

The Retrieval Task is removed from the list.

Retrieving Data from Archive



Note

This function is currently disabled but will be enabled in a future release.

Step 1 In the Navigation pane, select **Reporting >Data Retrieval >Retrieval from Archive** .

The Retrieval from Archive screen appears in the Configuration pane

Managing Report Instances

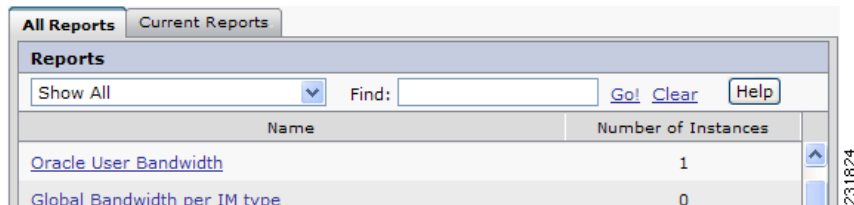
- [Creating a Report Instance, page 6-17](#)
- [Modifying an Existing Report Instance, page 6-19](#)
- [Deleting a Report Instance, page 6-20](#)

Creating a Report Instance

Step 1 In the Navigation pane, select **Reporting >Running Reports** .

The Reports screen appears in the Configuration pane, displaying the list of all Reports.

Figure 6-13



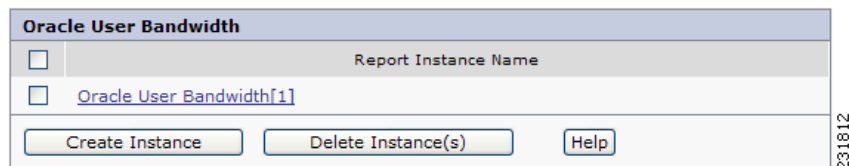
You can filter the Reports by selecting the desired alphabetical range from the **Show All** drop-down list.

**Note**

You can also go directly to your desired group of reports by selecting one of the child nodes under Running Reports in the Navigation pane.

- Step 2** Select from the list the type of report which you would like to use to create a report instance.
The list of associated report instances appears.

Figure 6-14



- Step 3** Click **Create Instance** .
The Modify Report Instance screen appears in the Configuration pane.

Figure 6-15

The screenshot shows the 'Modify Report Instance (Oracle User Bandwidth)' configuration screen. It contains several fields and buttons:

- Name of the Report Instance***: Oracle User Bandwidth[1]
- Traffic Direction***: Both Directions (dropdown)
- Average Data by Hour***: false (dropdown)
- Units of results***: Kbit/s (dropdown)
- Name of user to focus on***: (empty text box)
- From the last number of hours**: 24 (text box)
- Starting after date**: (calendar icon) [] Hrs [] Mins [] Secs
- Ending before date**: (calendar icon) [] Hrs [] Mins [] Secs
- Buttons**: Save, Run Report (JPEG), Run Report (CSV), Cancel

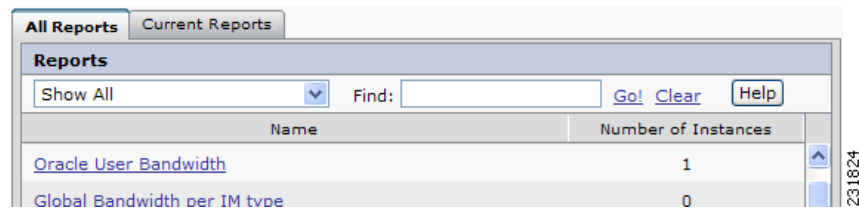
- Step 4** Modify the Report Instance parameters to produce the desired report.
Step 5 Click **Save** .

The Report Instance is saved and can be viewed on the Running Reports screen.

Modifying an Existing Report Instance

- Step 1** In the Navigation pane, select **Reporting >Running Reports** .
The Reports screen appears in the Configuration pane, displaying the list of all Reports.

Figure 6-16



You can filter the Reports by selecting the desired alphabetical range from the **Show All** drop-down list.

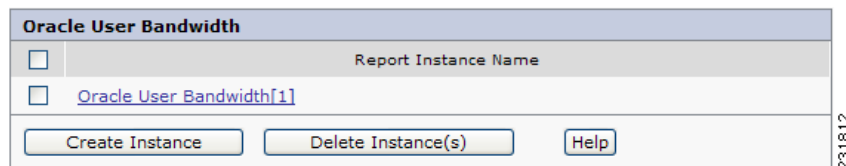


Note

You can also go directly to your desired group of reports by selecting one of the child nodes under Running Reports in the Navigation pane.

- Step 2** Select from the list the type of report which you would like to use to create a report instance.
The list of associated report instances appears.

Figure 6-17



- Step 3** Click on the Report Instance you want to modify.
The Modify Report Instance screen appears in the Configuration pane.

Figure 6-18

Modify Report Instance (Oracle User Bandwidth)

Name of the Report Instance*

Traffic Direction*

Average Data by Hour*

Units of results*

Name of user to focus on*

From the last number of hours

Starting after date

Ending before date

Step 4 Modify the Report Instance parameters to produce the desired report.
Changing the name of the Report Instance will rename the Report Instance.

Step 5 Click **Save** .
The Report Instance is saved and can be viewed on the Running Reports screen.

Deleting a Report Instance

Step 1 In the Navigation pane, select **Reporting >Running Reports** .
The Reports screen appears in the Configuration pane, displaying the list of all Reports.

Figure 6-19

Reports	
Name	Number of Instances
Oracle User Bandwidth	1
Global Bandwidth per IM type	0

You can filter the Reports by selecting the desired alphabetical range from the **Show All** drop-down list.



Note

You can also go directly to your desired group of reports by selecting one of the child nodes under Running Reports in the Navigation pane.

Step 2 Select from the list the type of report which you would like to use to create an report instance.
The list of associated report instances appears.

Figure 6-20

The screenshot shows a web interface titled "Oracle User Bandwidth". It features a table with two columns: a checkbox column and a "Report Instance Name" column. One instance, "Oracle User Bandwidth[1]", is listed. Below the table are three buttons: "Create Instance", "Delete Instance(s)", and "Help". A vertical label "231812" is positioned to the right of the table.

	Report Instance Name
<input type="checkbox"/>	Oracle User Bandwidth[1]

Create Instance Delete Instance(s) Help

231812

Step 3 Select the checkboxes next to the Report Instance or Instances that you want to delete.

Step 4 Click **Delete Instance(s)**.

The Report Instance or Instances are deleted from the list.



CHAPTER 7

Administrative User Management

This module explains the methods by which the operator of the Application Performance Assurance (APA) Device Console maintains security of the Network Module Enhanced Application Performance Assurance (NME-APA) devices by managing administrative user accounts and access rights for logging into the APA Device Console.

- [Viewing Administrative User Accounts, page 7-1](#)
- [Adding Administrative User Accounts, page 7-2](#)
- [Editing Administrative User Accounts, page 7-3](#)
- [Adding Device Credentials for an Admin User, page 7-4](#)
- [Editing Device Credentials for an Admin User, page 7-5](#)
- [Deleting Administrative User Accounts, page 7-7](#)

Viewing Administrative User Accounts

- Step 1** In the Navigation pane, select **Admin >Admin User Management** .
The Admin User Management screen appears in the Configuration pane.

Figure 7-1

APA Device Console Users				
	User	Description	Role	Configured Devices
<input type="radio"/>	root	root -- IT Manager	IT Manager	
<input checked="" type="radio"/>	joesmith		IT Manager	NME-APA_1
<div>Add Edit Delete Help</div>				

Administrative user accounts are listed with along with their devices.

Adding Administrative User Accounts

- Step 1** In the Navigation pane, select **Admin >Admin User Management** .
The Admin User Management screen appears in the Configuration pane.

Figure 7-2

APA Device Console Users				
	User	Description	Role	Configured Devices
<input type="radio"/>	root	root -- IT Manager	IT Manager	
<input checked="" type="radio"/>	joesmith		IT Manager	NME-APA_1
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Help"/>				

231754

Administrative user accounts are listed with along with their devices.

- Step 2** Click **Add** .
The SCaTE User box appears in the Configuration pane.

Figure 7-3

APA Device Console User
 Name:
 Description:
 Access Level:
 Role:
 Password:
 Confirm Password:

Devices
 Device Name:
 User Name:
 Password:
 Confirm Password:
 Access Level:
 Enable Password:
 Confirm Enable Password:

231738

- Step 3** In the Name field, enter a user name for the user to use when logging into the interface.
- Step 4** In the Description field, enter a meaningful description of the user.
- Step 5** In the Role drop-down list, select the most appropriate role of the user in your organization.
- Step 6** In the Password field, enter a password for the user to use when logging into the interface.
- Step 7** In the Confirm Password field, reenter the user's password.
The next section configures the new user's connection to a device.

Step 8 In the Device Name field, enter the name of the device to which this user will connect.



Note The device name entered here must match the device name entered when the device is added to the APA Device Console in [Managing Device Connections, page 3-2](#).

Step 9 In the User Name field, enter the user name with which the User will login to the device.



Note The user name entered here must match a valid user name on the NME-APA device.

Step 10 In the Password field, enter the password of the user name on the device.



Note The user name entered here must match the password for the above user name on the NME-APA device.

Step 11 In the Confirm Password field, reenter the password of the user name on the device .

Step 12 In the Access Level drop-down list, select the access level with which the User will login to the device.

Step 13 In the Enable Password field, enter the enable password of the device.

Step 14 In the Confirm Enable Password field, reenter the enable password of the device.

Step 15 Click **OK** .

The Admin User is saved in the configuration.

The Admin User Management as screen reappears in the Configuration pane.

Editing Administrative User Accounts

Step 1 In the Navigation pane, select **Admin >Admin User Management** .

The Admin User Management screen appears in the Configuration pane.

Figure 7-4

APA Device Console Users				
	User	Description	Role	Configured Devices
<input type="radio"/>	root	root -- IT Manager	IT Manager	
<input checked="" type="radio"/>	joesmith		IT Manager	NME-APA_1
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Help"/>				

231754

Administrative user accounts are listed with along with their devices.

Step 2 Select the radio button next to the User you want to edit.

Step 3 Click **Edit** .

The SCAtE User box appears in the Configuration pane.

Figure 7-5

APA Device Console User

Name:

Description:

Access Level:

Role:

Password:

Confirm Password:

- Step 4** In the Name field, edit the user name that the user enters when logging into the APA Device Console.
- Step 5** In the Description field, edit the meaningful description of the user.
- Step 6** In the Role drop-down list, select the most appropriate role of the user in your organization.
- Step 7** In the Password field, edit the password for the user to use when logging into the APA Device Console.
- Step 8** In the Confirm Password field, reenter the user's new password.
- Step 9** Click **OK**.

The modified Admin User is saved in the configuration.

The Admin User Management as screen reappears in the Configuration pane.

Adding Device Credentials for an Admin User

- Step 1** In the Navigation pane, select **Admin >Admin User Management**.
- The Admin User Management screen appears in the Configuration pane.

Figure 7-6

APA Device Console Users			
	User	Description	Role
<input type="radio"/>	root	root -- IT Manager	IT Manager
<input checked="" type="radio"/>	joesmith		IT Manager

[NME-APA_1](#)

- Administrative user accounts are listed with along with their devices.
- Step 2** Select the radio button next to the User you want to edit.
 - Step 3** Click **Edit**.
- The SCAtE User box appears in the Configuration pane.
- You may edit the User's details at this point as well.

Step 4 Click **Add New Device** .

The Devices box will appear in the lower portion of the Configuration pane.

Figure 7-7
Step 5 In the Device Name field, edit the name of the device to which this user will connect.**Note**

The device name entered here must match the device name entered when the device is added to the APA Device Console in [Managing Device Connections, page 3-2](#).

Step 6 In the User Name field, edit the user name with which the User will login to the device.**Note**

The user name entered here must match a valid user name on the NME-APA device.

Step 7 In the Password field, edit the password of the user name on the device.**Note**

The user name entered here must match the password for the above user name on the NME-APA device.

Step 8 In the Confirm Password field, reenter the modified password of the user name on the device .**Step 9** In the Enable Password field, edit the enable password of the device.**Step 10** In the Confirm Enable Password field, reenter the modified enable password of the device.**Step 11** Click **OK** .

The Device Credentials are saved in the configuration.

The Admin User Management as screen reappears in the Configuration pane.

Editing Device Credentials for an Admin User

Step 1 In the Navigation pane, select **Admin >Admin User Management** .

The Admin User Management screen appears in the Configuration pane.

Figure 7-8

APA Device Console Users				
	User	Description	Role	Configured Devices
<input type="radio"/>	root	root -- IT Manager	IT Manager	
<input checked="" type="radio"/>	joesmith		IT Manager	NME-APA_1
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Help"/>				

Administrative user accounts are listed with along with their devices.

Step 2 Click on the Configured Device.

The Devices box will appear in the lower portion of the Configuration pane.

Figure 7-9

Devices

Device Name:

User Name:

Password:

Confirm Password:

Access Level:

Enable Password:

Confirm Enable Password:

Step 3 In the Device Name field, edit the name of the device to which this user will connect.



Note

The device name entered here must match the device name entered when the device is added to the APA Device Console in [Managing Device Connections, page 3-2](#).

Step 4 In the User Name field, edit the user name with which the User will login to the device.



Note

The user name entered here must match a valid user name on the NME-APA device.

Step 5 In the Password field, edit the password of the user name on the device.



Note

The user name entered here must match the password for the above user name on the NME-APA device.

Step 6 In the Confirm Password field, reenter the modified password of the user name on the device .

Step 7 In the Access Level drop-down list, select the access level with which the User will login to the device.

- Step 8** In the Enable Password field, edit the enable password of the device.
- Step 9** In the Confirm Enable Password field, reenter the modified enable password of the device.
- Step 10** Click **OK** .
- The Device Credentials are saved in the configuration.
- The Admin User Management screen reappears in the Configuration pane.

Deleting Administrative User Accounts

- Step 1** In the Navigation pane, select **Admin >Admin User Management** .
- The Admin User Management screen appears in the Configuration pane.

Figure 7-10

APA Device Console Users				
	User	Description	Role	Configured Devices
<input type="radio"/>	root	root -- IT Manager	IT Manager	
<input checked="" type="radio"/>	joesmith		IT Manager	NME-APA_1
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Help"/>				

231754

Administrative user accounts are listed with along with their devices.

- Step 2** Select the radio button next to the User you want to delete.
- Step 3** Click **Delete** .
- The User is removed from the list.



APPENDIX **A**

Admin User Roles

This appendix describes the Cisco Application Performance Assurance (APA) administrative user roles.

Explanation of Roles

The following table lists the activities that are allowed to each of the Admin User Roles.

Table A-1 Admin User Roles

Role	Jobs	Workflows	Access-Level
IT Administrator	<ol style="list-style-type: none"> 1. Keeps network running 	<ol style="list-style-type: none"> 1. Adding/ removing NME-APA devices on site 2. Initial installation and configuration 2. Initial configuration of protocols, services and policies 3. Further configuration of protocols, services and policies 4. Report configuration 5. Reporting data retrieval and generation the reports 6. Using and interpretation of the real-time monitoring results 7. Weekly adjustment and reviewing the policies 8. Fault management 9. Capacity/performance management (based on statistics) 10. Local upgrades 11. Local backups 12. Sets up new users consuming services - User management 	15
IT Manager	<ol style="list-style-type: none"> 1. Identifies policies 2. Deployment schedules and targets 3. Runs reports on a regular basis 4. Organizational responsibility 5. Owner of the master password 	<ol style="list-style-type: none"> 1. Defines reports 2. Customizes reports 3. Runs reports 4. Sets up password structure 5. Network architecture. Spots trends re: capacity and responds to network needs. 	15

Table A-1 Admin User Roles (continued)

Role	Jobs	Workflows	Access-Level
IT Technician	<ol style="list-style-type: none"> 1. Manage the fault components 2. Runs reports 	<ol style="list-style-type: none"> 1. Runs reports 2. Distributes reports as appropriate 3. Views and investigates alarms and statistics 4. Low level alarm resolution 5. Uses real-time monitoring 6. Initiate trouble tickets 7. Escalates severe alarms 8. Collates local information 	5
Service Admin	<ol style="list-style-type: none"> 1. Sole role is to prepare devices for managed service rollout 	<ol style="list-style-type: none"> 1. Central staging- setup and configuration of initial policies 	15

Table A-1 Admin User Roles (continued)

Role	Jobs	Workflows	Access-Level
Field Engineer	<ol style="list-style-type: none"> 1. Manages customer installations and configurations onsite 	<ol style="list-style-type: none"> 1. Uploads configuration files to APA Device Console 2. Modifies policy configurations as required 3. Sets up initial report templates 4. Installs the pre-configured module into the router and runs initial diagnostics 5. Ensures ability to integrate into central NMS 6. Sets up password structure onsite 7. Performs final test, perhaps provides initial usage training 	10
Service Manager	<ol style="list-style-type: none"> 1. Identifies policies 2. Deployment schedules and targets 3. Runs reports on a regular basis 4. Organizational responsibility 5. Owner of the master password 	<ol style="list-style-type: none"> 1. Defines reports 2. Customizes reports 3. Runs reports 4. Sets up password structure 5. Network architecture. Spots capacity trends and responds to network needs 	15