Cisco Service Control Application for Broadband User Guide

Release 3.7.x
December 10, 2013

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

Text Part Number: OL-24178-09

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned 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. (1110R)

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 Service Control Application for Broadband User Guide

CONTENTS

CHAPTER 3

CHAPTER 9

About this Guide

Revised: December 10, 2013, OL-24178-09

Introduction

This document describes who should read *Cisco Service Control Application for Broadband User Guide,* how it is organized, its document conventions, and how to obtain documentation and technical assistance.

This guide assumes a basic familiarity with the concept of the Service Control solution, the Service Control Engine (SCE) platforms, and related components.

Document Revision History

Table 1 records changes to this document.

Table 1 Document Revision History

Revision	Cisco Service Control Release and Date	Change Summary
OL-24178-09	Release 3.7.x December 10, 2013	• Added the "Downgrading Protocol Packs" section on page 4-29.
OL-24178-08	Release 3.7.x August 08, 2013	• Updated the "How to Add a Subscriber" section on page 11-15
OL-24178-07	Release 3.7.x July 19, 2013	• Updated the "Installing Protocol Packs" section on page 4-21
OL-24178-06	Release 3.7.x June 13, 2013	Updated these sections: • "Flavor Types and Parameters" section on page 7-60 • "How to Add a Set of Redirection URLs" section on page 10-52
OL-24178-05	Release 3.7.x May 10, 2013	Updated the "How to Set Global Controller Bandwidth for Virtual Links" section on page 9-24.
OL-24178-05	Release 3.7.x January 10, 2013	Updated Chapter 10, "Using the Service Configuration Editor: Additional Options."
OL-24178-05	Release 3.7.x December 10, 2012	Updated Chapter 10, "Using the Service Configuration Editor: Additional Options."
OL-24178-05	Release 3.7.x August 28, 2012	Added information regarding the following: Hitless Upgrade of the SLI.
OL-24178-05	Release 3.7.x March 22, 2012	Added information regarding the following: • How to Manage Transaction Usage RDRs • How to Add Filter Rules for IPv6 Configuration • How to Configure the Upstream Configuration of the Global Bandwidth Controller for IPv6 • Procedure to run the asFetch.bat script and get the .csv file
OL-24178-04	Release 3.7.x January 06, 2012	Updated with information pertaining to Cisco SCA BB Release 3.7.2. Updated Chapter 7 with information on BGP Autonomous System Dynamic Detection.
OL-24178-03	Release 3.7.x December 14, 2011	Improved the quality of the user documentation by adding customer and internal feedback.

Table 1 Document Revision History (continued)

Revision	Cisco Service Control Release and Date	Change Summary
OL-24178-02	Release 3.7.x September 20, 2011	Improved the quality of the user documentation by adding customer and internal feedback.
OL-24178-01	Release 3.7.x June 13, 2011	These are the changes from the Cisco SCA BB Release 3.6.x: • Updated Chapter Getting Started with information on Anonymous Group Manager Tool. • Updated Chapter 7 with the Managing OS Fingerprinting section. • Updated The Advanced Service Configuration Properties section in Chapter 10, Using the Service Configuration Editor: Additional Options. • New Chapter Using the Anonymous Group Manager Tool.

Organization

Table 2 lists the document organization of this guide.

Table 2 Document Organization

Section	Title	Description
1	Cisco Service Control Overview, page 1-1	Provides a general overview of the Cisco Service Control solution.
2	System Overview, page 2-1	Provides a functional overview of the Cisco Service Control solution.
3	Traffic Processing Overview, page 3-1	Provides a technical overview of the Cisco Service Control solution.
4	Getting Started, page 4-1	Guides you through the process of installing or upgrading Cisco SCA BB and describes the concept of the Console as a collection of tools.
5	Using the Network Navigator, page 5-1	Explains how to use the Network Navigator to create a model of all devices that are part of the Cisco Service Control solution and how to manage the devices remotely.
6	Using the Service Configuration Editor, page 6-1	Explains how to use the Service Configuration Editor to manage service configurations.
7	Using the Service Configuration Editor: Traffic Classification, page 7-1	Explains how to configure service configurations to perform traffic classification.
8	Using the Service Configuration Editor: Traffic Accounting and Reporting, page 8-1	Explains how to configure service configurations to perform traffic reporting.
9	Using the Service Configuration Editor: Traffic Control, page 9-1	Explains how to configure service configurations to perform traffic control.
10	Using the Service Configuration Editor: Additional Options, page 10-1	Documents additional, advanced options available in the Service Configuration Editor.
11	Using the Subscriber Manager GUI Tool, page 11-1	Explains how to use the Subscriber Manager GUI tool to configure subscribers on the SCMS Subscriber Manager database.
12	Using the Anonymous Group Manager Tool, page 12-1	Explains how to use the Anonymous Group Manager GUI tool to configure the anonymous groups and subscribers in Cisco SCEs.
13	Using the Signature Editor, page 13-1	Documents the Signature Editor tool, which can create files for updating protocols in Cisco SCA BB.
14	Additional Management Tools and Interfaces, page 14-1	Documents and explains other tools that are available for use with Cisco SCA BB.

Related Publications

Use this *Cisco Service Control Application for Broadband User Guide* with the following Cisco documentation:

- *Cisco Service Control Application for Broadband Reference Guide*
- *Cisco Service Control Application for Broadband Service Configuration API Programmer Guide*
- *Cisco Service Control Management Suite Collection Manager User Guide*
- *Cisco Service Control Management Suite Subscriber Manager User Guide*
- *Cisco Service Control Application Reporter User Guide*
- *Cisco Insight v2 User Guide*
- *Cisco Service Control Mobile Solution Guide*
- *Cisco Service Control Usage-Based Services Solution Guide*
- *Cisco Service Control for Managing Remote Cable MSO Links Solution Guide*
- The SCE platform installation and configuration guides:
  - *Cisco SCE 1000 2xGBE Installation and Configuration Guide*
  - *Cisco SCE 2000 Installation and Configuration Guide*
  - *Cisco SCE 8000 10GBE Installation and Configuration Guide*
  - *Cisco SCE 8000 GBE Installation and Configuration Guide*
- *Cisco SCE 2000 and SCE 1000 CLI Command Reference*
- *Cisco SCE 8000 CLI Command Reference*
- *Cisco SCE 2000 and SCE 1000 Software Configuration Guide*
- *Cisco SCE 8000 10GBE Software Configuration Guide*
- *Cisco SCE 8000 10GBE Software Configuration Guide*

Conventions

This document uses the following conventions:

Table 3 Document Conventions

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required 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 includes the quotation mark.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
< >	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 material not covered in the manual.

Tip Means *the following information will help you solve a problem.* The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning **Means *reader be warned*. In this situation, you might perform an action that could result in bodily injury.**

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

Cisco Service Control Overview

Revised: August 08, 2013, OL-24178-09

Introduction

This chapter provides a general overview of the Cisco Service Control solution. It introduces the Cisco service control concept and capabilities.

It also briefly describes the hardware capabilities of the service control engine (SCE) platform and the Cisco-specific applications that together compose the Cisco service control solution.

- Cisco Service Control Solution, page 1-2
- Cisco Service Control Capabilities, page 1-3
- SCE Platform Description, page 1-4
- Management and Collection, page 1-6

Cisco Service Control Solution

The Cisco service control solution is delivered through a combination of hardware and specific software solutions that address various service control challenges. Service providers can use the SCE platform to support classification, analysis, and control of Internet and IP traffic.

Service control enables service providers to:

- Capitalize on existing infrastructure.
- Analyze, charge for, and control IP network traffic at multigigabit wire line speeds.
- Identify and target high-margin content-based services and enable their delivery.

As the downturn in the telecommunications industry has shown, the business models of the IP Service Providers require rework to make them profitable. Having spent billions of dollars to build ever larger data links, providers have incurred massive debts and faced rising costs. At the same time, access and bandwidth have become commodities where prices continually fall and profits disappear. Service providers have realized that they must offer value-added services to derive more revenue from the traffic and services running on their networks.

Cisco service control solutions allow IP Service Providers to capture profits from IP Services through detailed monitoring, precise, real-time control, and awareness of services as they are delivered.

Service Control for Broadband Service Providers

Service providers of any access technology (DSL, cable, mobile, and so on) targeting residential and business consumers must find new ways to get maximum leverage from their existing infrastructure, while differentiating their offerings with enhanced IP Services.

The Cisco service control application for broadband adds a layer of service intelligence and control to existing networks that can:

- Report and analyze network traffic at subscriber and aggregate level for capacity planning
- Provide customer-intuitive tiered application services and guarantee application service level agreements (SLAs)
- Implement different service levels for different types of customers, content, or applications
- Identify network abusers who are violating the acceptable use policy (AUP)
- Identify and manage peer-to-peer traffic, NNTP (news) traffic, and spam abusers
- Enforce the AUP
- Integrate Service Control solutions easily with existing network elements and business support systems (BSS) and operational support systems (OSS)

Cisco Service Control Capabilities

The core of the Cisco service control solution is the network hardware device: the Service Control Engine (SCE). The core capabilities of the SCE platform, which support a wide range of applications for delivering service control solutions, include:

- Subscriber 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 subscriber.
  - Subscriber awareness—The ability to map between IP flows and a specific subscriber to maintain the state of each subscriber transmitting traffic through the SCE platform and to enforce an appropriate policy on this subscriber's traffic.

    Subscriber awareness is achieved either through dedicated integrations with subscriber management repositories, such as a DHCP or a RADIUS server, or through sniffing of RADIUS or DHCP traffic.
  - 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 SCE platform understands the bundling connection between the flows and treats them accordingly.
- Application-layer, stateful, real-time traffic control—The ability to perform advanced control functions, including granular bandwidth (BW) metering and shaping, quota management, and redirection, using application-layer, stateful, real-time traffic transaction processing. This feature requires highly adaptive protocol and application-level intelligence.
- Programmability—The ability to add new protocols quickly and adapt to new services and applications in the service provider environment. Programmability is achieved using the Cisco Service Modeling Language (SML).

  Programmability allows new services to be deployed quickly and provides an easy upgrade path for network, application, or service growth.
- Robust and flexible back-office integration—The ability to integrate with existing third-party systems at the service provider, including provisioning systems, subscriber repositories, billing systems, and OSS systems. The SCE provides a set of open and well-documented APIs that allows a quick integration process.
- Scalable high-performance service engines—The ability to perform all of these operations at wire speed.

SCE Platform Description

The SCE family of programmable network devices performs application-layer stateful-flow inspection of IP traffic, and controls the traffic based on configurable rules. The SCE platform devices use ASIC components and reduced instruction set computer (RISC) processors to exceed beyond packet counting and expand into the contents of network traffic.

The SCE platform devices:

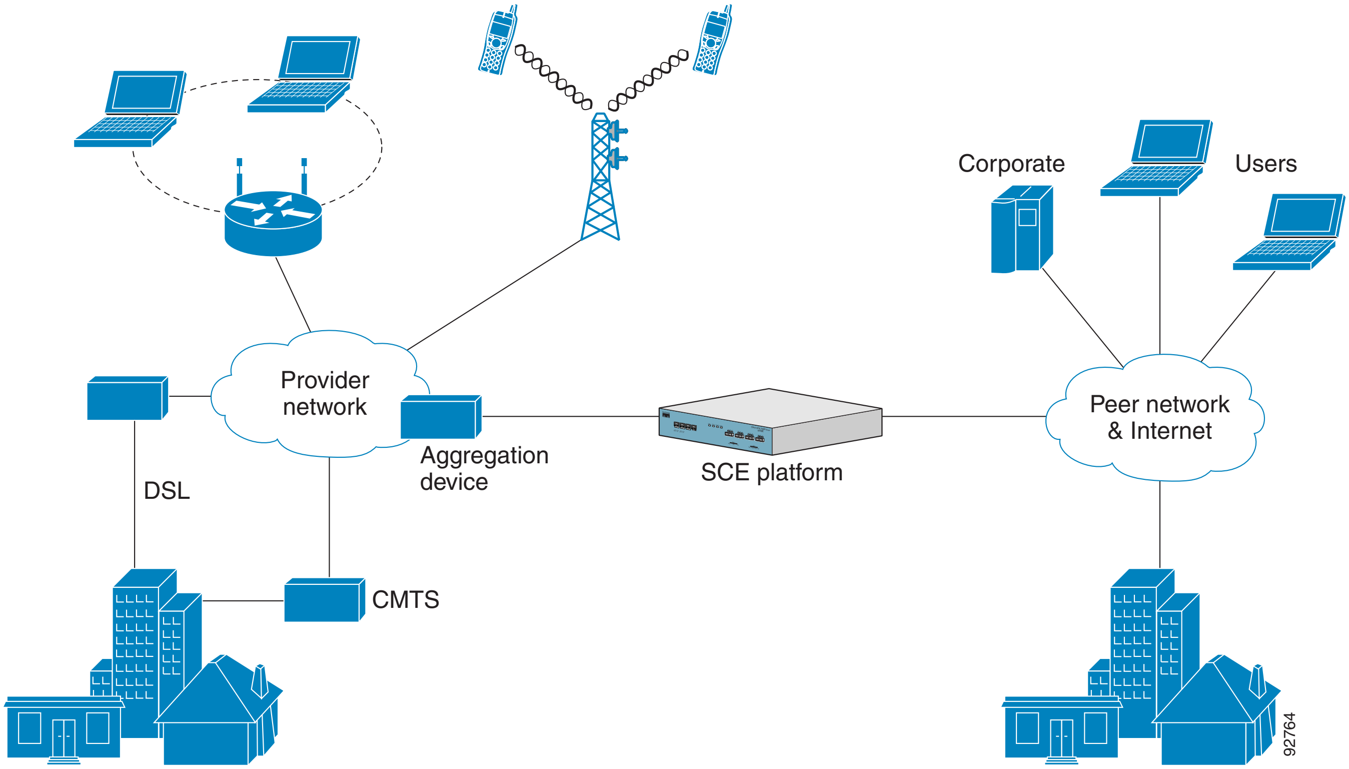
- Are programmable.
- Provide stateful inspection of bidirectional traffic flows, and mapping these flows with user ownership.
- Provide real-time classification of network use. The classification provides the basis of the SCE platform advanced traffic-control and bandwidth-shaping functionality.

Where most bandwidth shaper functionality ends, the SCE platform provides further control and shaping options, including:

- Layer 7 stateful wire-speed packet inspection and classification
- Robust support for more than 600 protocols and applications, including:
  - General—HTTP, HTTPS, FTP, Telnet, Network News Transfer Protocol (NNTP), Simple Mail Transfer Protocol (SMTP), Post Office Protocol 3 (POP3), Internet Message Access Protocol (IMAP), Wireless Application Protocol (WAP), and others
  - Peer-to-Peer (P2P) file sharing—FastTrack-KazaA, Gnutella, BitTorrent, Winny, Hotline, eDonkey, DirectConnect, Piolet, and others
  - P2P VoIP—Skype, Skinny, DingoTel, and others
  - Streaming and Multimedia—Real Time Streaming Protocol (RTSP), Session Initiation Protocol (SIP), HTTP streaming, Real Time Protocol (RTP) and Real Time Control Protocol (RTCP), and others
- Programmable system core for flexible reporting and bandwidth control
- Transparent network and BSS and OSS integration into existing networks
- Subscriber awareness that relates traffic and usage to specific customers

Figure 1-1 illustrates a common deployment of an SCE platform in a network.

Figure 1-1 SCE Platform in the Network



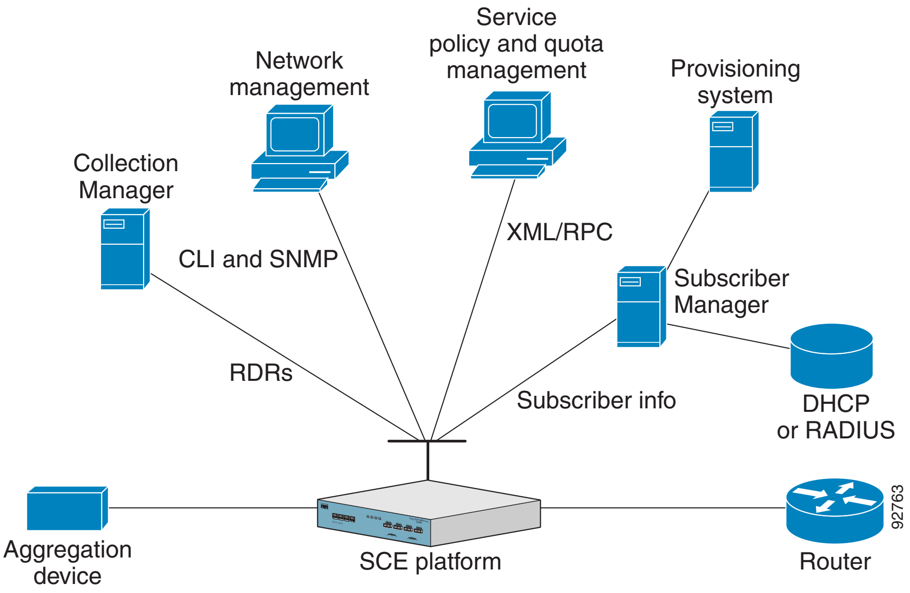
Management and Collection

The Cisco service control solution includes a complete management infrastructure that provides the following management components to manage all aspects of the solution:

- Network management
- Subscriber management
- Service Control management

These management interfaces are designed to comply with common management standards and to integrate easily with existing OSS infrastructure (see Figure 1-2).

Figure 1-2 Service Control Management Infrastructure



Network Management

The Cisco service control solution provides complete network Fault, Configuration, Accounting, Performance, Security (FCAPS) Management.

Two interfaces provide network management:

- Command-line interface (CLI)—Accessible through the Console port or through a Telnet connection, the CLI is used for configuration and security functions.
- SNMP—Provides fault management (through SNMP traps) and performance-monitoring functionality.

Subscriber Management

Where the Cisco service control application for broadband (Cisco SCA BB) enforces policies on different subscribers and tracks usage on an individual subscriber basis, the Cisco SCMS Subscriber Managermay be used as middleware software for bridging between OSS and SCE platforms. Subscriber information is stored in the Subscriber Manager database and can be distributed between multiple platforms according to actual subscriber placement.

The Subscriber Manager provides subscriber awareness by mapping network IDs to subscriber IDs. It can obtain subscriber information using dedicated integration modules that integrate with AAA devices, such as RADIUS or DHCP servers.

Subscriber information may be obtained in one of two ways:

- Push Mode—The Subscriber Manager pushes subscriber information to the SCE platform automatically upon logon of a subscriber.
- Pull Mode—The Subscriber Manager sends subscriber information to the SCE platform in response to a query from the SCE platform.

Service Configuration Management

Service configuration management is the ability to configure the general service definitions of a service control application. A service configuration file containing settings for traffic classification, accounting and reporting, and control is created and applied to an SCE platform. The Cisco SCA BB application provides tools to automate the distribution of these configuration files to SCE platforms. This standards-based approach makes it easy to manage multiple devices in a large network.

Service Control provides a GUI to edit and create these files and a complete set of APIs to automate their creation.

Data Collection

Data collection occurs as follows:

1. SCE Platform analyzes and process the data passing through it and generates Raw Data Records (RDRs).
2. SCE Platform then forwards these RDRs to Cisco service control management suite collection manager using a simple TCP-based protocol (RDR-Protocol).

   The collection manager software is an implementation of a collection system that receives RDRs from one or more SCE platforms.
3. The collection manager collects these records and processes them in one of its adapters. Each adapter performs a specific action on the RDR.

RDRs contain various information and statistics, depending on the configuration of the system. The main categories of RDRs include:

- Transaction RDRs—Records generated for each *transaction*, where a transaction is a single event detected in network traffic. The identification of a transaction depends on the particular application and protocol.
- Subscriber Usage RDRs—Records generated per subscriber, describing the traffic generated by that subscriber for a defined interval.
- Link RDRs—Records generated per link, describing the traffic carried on the link for a defined interval.
- Zone RDRs—Records generated per zone, describing the traffic carried on the zone for a defined interval.

CHAPTER 2

System Overview

Revised: August 08, 2013, OL-24178-09

Introduction

The Cisco Service Control Application for Broadband (Cisco SCA BB) is the Cisco Service Control solution that allows broadband service providers to gain network-traffic visibility, to control the distribution of network resources, and to optimize traffic in accordance with their business strategies. It enables service providers to reduce network costs, improve network performance and customer experience, and create new service offerings and packages.

- System Components, page 2-2
- Subscribers and Subscriber Modes, page 2-4
- Service Configuration, page 2-8

System Components

The Cisco Service Control solution consists of four main components:

- The Service Control Engine (SCE) platform—A flexible and powerful dedicated network-usage monitor that is purpose-built to analyze and report on network transactions at the application level.

  For more information about the installation and operation of the SCE platform, see *Cisco SCE Platform Installation and Configuration Guides*.

- The SCMS Subscriber Manager—A middleware software component that is used where dynamic binding of subscriber information and policies are required. The Subscriber Manager manages subscriber information and provisions it in real time to multiple SCE platforms. The Subscriber Manager can store subscriber policy information internally, and act as a stateful bridge between the AAA system (such as RADIUS and DHCP) and the SCE platforms.

  For more information about the installation and operation of the Subscriber Manager, see *Cisco Service Control Management Suite Subscriber Manager User Guide.*

  The Quota Manager (QM) is an optional component of the Subscriber Manager. It enables Service Control solution providers to manage subscriber quota across subscriber sessions with a high degree of flexibility.

  For more information about the installation and operation of the QM, see *Cisco Service Control Management Suite Quota Manager User Guide.*

- The Service Control Management Suite (SCMS) Collection Manager (CM)—An implementation of a collection system that receives Raw Data Records (RDRs) from one or more SCE platforms. It collects usage information and statistics, and stores them in a database. The CM also converts subscriber usage information and statistics into simple text-based files for further processing and collection by external systems.

  For more information about the installation and operation of the CM, see *Cisco Service Control Management Suite Collection Manager User Guide.*

- The Service Control Application (SCA) Reporter—A software component that processes data stored by the CM and provides a set of insightful reports from this data. The SCA Reporter can run as a standalone or as an integrated part of the Console.

  For more information about the installation and operation of the Reporter, see *Cisco Service Control Application Reporter User Guide.*

Together, the SCE platform, the SCMS Collection Manager, the SCMS Subscriber Manager, and the SCA Reporter are designed to support detailed classification, analysis, reporting, and control of IP network traffic. The SCMS Collection Manager, the SCA Reporter, and the SCMS Subscriber Manager are optional components; not all deployments of the Cisco Service Control solution require them. Sites that employ third-party collection and reporting applications, those that do not require dynamic subscriber-aware processing, and those that use a RADIUS or DHCP sniffing option may not require all of these components.

Figure 2-1 illustrates the flow of information in the Cisco Service Control solution.

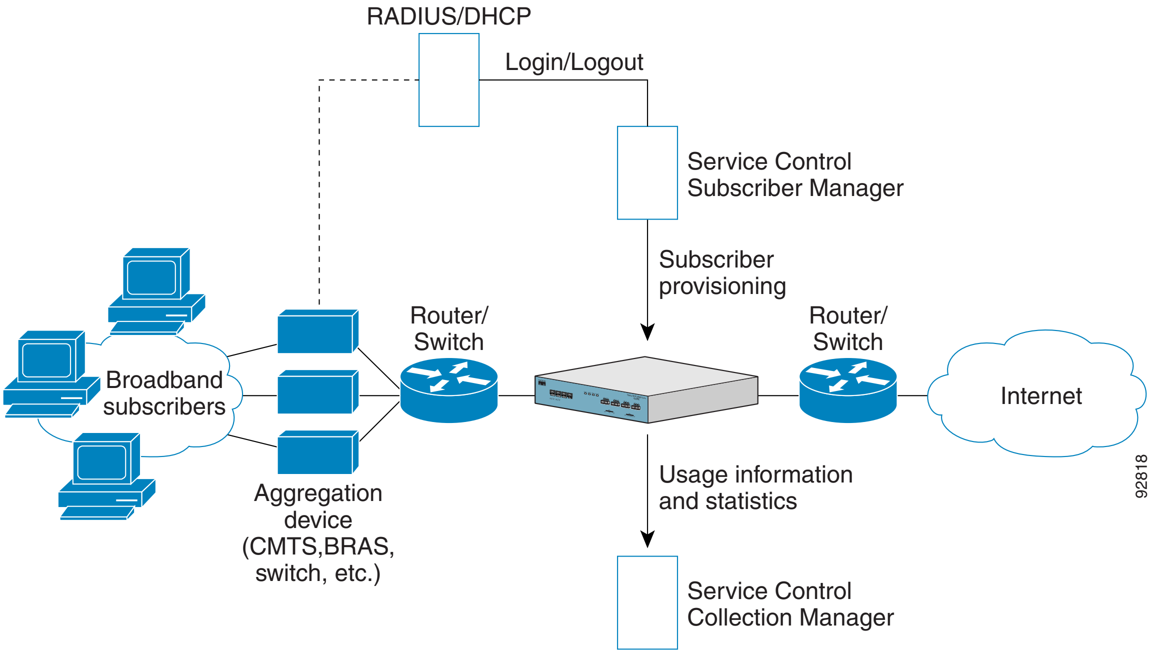
- Horizontal flow—Represents traffic between subscribers and an IP network.

  The SCE platform monitors traffic flow.

- Vertical flow—Represents transmission of the Raw Data Records (RDRs) from the SCE platform to the CM.

  The Subscriber Manager may be added to the control flow to provide subscriber data. This allows Cisco SCA BB to conduct subscriber-level analysis and control.

Figure 2-1 Flow of Information in Cisco SCA BB



Subscribers and Subscriber Modes

One of the fundamental entities in the Cisco Service Control solution is a *subscriber.* A subscriber is the most granular entity on which Cisco SCA BB can individually monitor, account, and enforce a policy. In the most granular instance of the Cisco SCA BB system a subscriber is an actual customer of the service provider on whom an individual policy is implemented. However, you may also configure Cisco SCA BB to monitor and control traffic at a higher granularity, such as when monitoring or controlling traffic by subnets or aggregation devices.

One of the most important decisions you must take when designing a service control solution is what subscribers in the system represent. This decision determines which subscriber mode is used, which in turn determines what (if any) integrations are required and what policies to define. The following sections describe the different subscriber modes supported and, for each mode, the functions supported, any prerequisites, and the components needed.

Cisco SCA BB supports the following four subscriber modes:

- Subscriberless mode—No subscribers are defined. Control and link-level analysis functions are provided at a global platform resolution.
- Anonymous subscriber mode—IP addresses are controlled and monitored individually. The SCE platform automatically identifies IP addresses as they are used and assigns them to a package.
- Static subscriber mode—Incoming IP addresses are bound and grouped statically into "subscribers" as configured by the system operator.
- Subscriber-aware mode—Subscriber information is dynamically bound to the IP address currently in use by the subscriber. Subscriber-aware mode can be achieved by integrating Cisco SCA BB with the system (RADIUS, DHCP) that assigns IP addresses to subscribers, or by sniffing this information. Policy information is either administered to Cisco SCA BB directly or provisioned dynamically via an integration.

Subscriberless Mode

Subscriberless mode is the choice for sites where control and analysis functions are required only at a global platform resolution. It can be used, for example, to monitor and control the total P2P traffic over the link.

Subscriberless mode requires no integration; hence, the SCMS Subscriber Manager is not required.

Note The number of subscribers or inbound IP addresses does not influence the Subscriberless mode. Hence, the total number of subscribers using the monitored link is unlimited from the point of view of the SCE platform.

Anonymous Subscriber Mode

Anonymous subscriber mode provides the means to analyze and control network traffic at subscriber-inbound IP address granularity.

Use this mode when:

- You do not require subscriber-differentiated control or subscriber-level quota tracking
- Analysis on an IP level is sufficient
- When offline IP-address/subscriber binding can be performed

For example, you can identify which subscribers generate the most P2P traffic by identifying the top IP addresses and correlating them to individual subscribers using RADIUS or DHCP logs. The total bandwidth of P2P traffic allowed for each subscriber can also be limited.

Anonymous subscriber mode requires no integration or static configuration of the IP addresses used, so the SCMS Subscriber Manager is not required.

In this mode, ranges of IP addresses are configured directly on the SCE platform. SCE Platform dynamically creates "anonymous" subscribers for these IP addresses, using the IP address as the subscriber name.

Note The total number of concurrently active anonymous subscribers supported by the SCE platform is the same as the total number of concurrently active subscribers.

Static Subscriber Mode

Static subscriber mode binds incoming IP addresses together into groups, so that traffic from and to defined subscribers can be controlled as a group. For example, you can define all traffic from and to a particular network subnet (used by multiple subscribers concurrently) as a (virtual) "subscriber" and controlled or viewed as a group.

Static subscriber mode supports cases in which the entity controlled by the Cisco Service Control solution uses a constant IP address or address range that does not change dynamically, such as:

- Environments where the subscriber IP addresses do not change dynamically via, for example, DHCP or RADIUS
- Deployments in which a group of subscribers using a common pool of IP addresses (such as all those served by a particular aggregation device) are managed together to provide a shared bandwidth to the entire group

The system supports the definition of static subscribers directly on an SCE platform; it does not require external management software (such as the SCMS Subscriber Manager). Use the SCE platform CLI to define the list of subscribers, their IP addresses, and the associated package.

Subscriber-Aware Mode

In subscriber-aware mode, the subscriber information (OSS ID and policy) that is dynamically bound to the (IP) address currently in use by the subscribers are populated on the SCE.

The subscriber information is populated regardless of the IP address in use and provides differentiated and dynamic control per subscriber and subscriber-level analysis. Use this mode to control and analyze traffic on a subscriber level, to monitor subscriber usage, and to assign and enforce different control policies (packages) for different subscribers.

In this mode, the SCMS Subscriber Manager may provision the SCE platform with subscriber information.

Subscriber Modes: Summary

Table 2-1 summarizes the different subscriber modes supported by the system.

Table 2-1 Summary of Subscriber Modes

Mode	Features Supported	Main Advantages	Use for...
Subscriberless mode	• Global (platform-level) analysis and control	• No subscriber configuration required.	Global control solution or subscriber-level analysis. Examples: • Control P2P uploads at peering points. • Limit total bandwidth of P2P to a specified percentage.
Anonymous subscriber mode	• Global analysis and control • Individual IP address-level analysis and control	• No subscriber configuration required; only define subscriber IP address ranges used. • Provide subscriber-level control without integration.	IP-level analysis or control that is not differentiated per subscriber, and where offline IP-address/subscriber binding is sufficient. Examples: • Limit P2P bandwidth per subscriber. • Identify top subscribers by identifying top IP addresses and correlating them with RADIUS or DHCP logs.

Table 2-1 Summary of Subscriber Modes (continued)

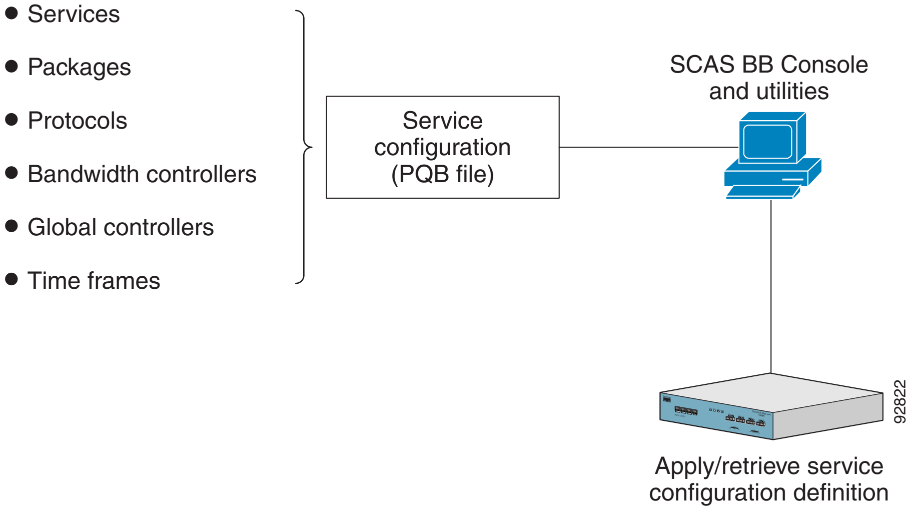
Mode	Features Supported	Main Advantages	Use for...
Static subscriber mode	• Global analysis and control • Control based on individual or group IP addresses as configured statically to the SCE platform	• One-time static subscriber configuration, with no integration requirements. • Manage subscriber traffic in logical groups.	Control of traffic of groups of subscribers. Example: • Assign a bandwidth limit for P2P traffic for each group of subscribers using a single CMTS device.
Subscriber-aware mode	• Full system functionality	• Differentiated and dynamic control per subscriber. • Subscriber-level analysis, regardless of IP address in use.	Control and analysis of traffic on a subscriber level. Examples: • Monitor subscriber-usage, regardless of IP addresses. • Assign different control policies (packages) to different subscribers, and change packages dynamically.

Service Configuration

Service configuration defines the way the SCE platform analyses and controls traffic. In general terms, as illustrated in Figure 2-2, service configuration defines the following:

- Protocol and service classification
- Packages and policies
- Bandwidth controllers
- Global controllers

Figure 2-2 Service Configuration


● Services
● Packages
● Protocols
● Bandwidth controllers
● Global controllers
● Time frames
Service configuration (PQB file)
SCAS BB Console and utilities
Apply/retrieve service configuration definition
92822

Service configuration is accomplished using one of the following:

- The Console
- The Cisco SCA BB Service Configuration Utility
- The Service Configuration API

The Cisco SCA BB Console

The Cisco SCA BB Console is a set of GUI tools that are used to manage, configure, and monitor the solution components.

The Console is fully documented in the remainder of this guide.

The Service Configuration Utility

The Cisco SCA BB Service Configuration Utility (**servconf**) is a simple command-line utility that you can use to apply PQB configuration files onto SCE platforms or to retrieve the current configuration from an SCE platform and save it as a PQB file. The utility configures SCE platforms with the service configuration defined in a PQB file. You can install and execute it in a Windows or Solaris environment.

For full documentation of **servconf,** see The Cisco SCA BB Service Configuration Utility, page 14-2.

The Service Configuration API

The Service Configuration API is a set of Java classes used to:

- Program and manage service configurations
- Apply service configurations to the SCE platforms
- Integrated applications with third-party systems

The service configuration API allows service providers to automate and simplify management and operational tasks.

The Service Configuration API is documented in *Cisco Service Control Application for Broadband Service Configuration API Programmer Guide.*

CHAPTER 3

Traffic Processing Overview

Revised: August 08, 2013, OL-24178-09

Introduction

This chapter describes how the Cisco SCA BB installed on a Service Control Engine (SCE) platform processes traffic.

The chapter also describes the main elements (service configuration entities) of the Cisco SCA BB system and explains how they relate to each other.

This chapter consists of these sections:

Routing Environment

Traffic processing depends on the routing environment. The Cisco Service Control solution can operate in two typical routing schemes:

- Symmetric (Normal)—For most flows the inbound and outbound traffic is routed through one SCE platform. For a marginal number of flows, only one direction goes through this SCE platform.
- Asymmetric—For a significant number of flows, only one direction (inbound or outbound) is routed through the SCE platform. For other flows, both directions go through this SCE platform.

  A flow is bidirectional when the inbound and outbound traffic of the flow passes through the same SCE platform. A unidirectional flow is one where only one of the inbound traffic and the outbound traffic go through the SCE platform.

  The Cisco Service Control solution can handle both unidirectional and bidirectional flows. The SCE platform can be configured to operate in either a symmetric or an asymmetric routing environment. The traffic processing capabilities of the SCE platform in the asymmetric environment are a subset of its capabilities in the symmetric environment.

  When the Cisco Service Control solution is deployed in an asymmetric routing environment, and unidirectional classification is enabled, the SCE platform classification is better tuned to identify traffic based on a single direction. The SCE platform handles unidirectional flows independently, with no synchronization with other SCE platforms that might handle the opposite direction of the flow.

Traffic Processing

There are three stages of traffic processing:

- Traffic classification—Cisco SCA BB analyses traffic flows and determines their type (for example, browsing, e-mail, file sharing, or voice).
- Traffic accounting and reporting—Cisco SCA BB performs bookkeeping and generates Raw Data Records (RDRs) that let you analyze and monitor the network.
- Traffic control—Cisco SCA BB limits and prioritizes traffic flows according to their service, subscriber-package, subscriber quota state, and so on.

The three stages are described in these sections:

- Traffic Classification, page 3-3
- Traffic Accounting and Reporting, page 3-11
- Traffic Control, page 3-15

You can control how classification, reporting, and control perform by editing the service configurations and by applying these configurations to the SCE platform.

Traffic Classification

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

For each commercial service that a provider offers to its subscribers, a corresponding service is defined in the Cisco Service Control solution. You can use this service to classify and identify the traffic, report on its usage, and control it.

Cisco SCE internal architecture has two concepts that aid traffic classification:

- Hardware flow—created entirely in hardware, with a maximum limit of 32 million flows on SCE 8000.
- Software flow—created in software, with a maximum limit of 16 million flows on SCE 8000.

Each flow context is unidirectional. Flows are opened based on the following logic:

- If the flow is on *filter list* or *traffic rule* with *ignore*, it is ignored and bypassed
- If the packet is Non-IP, it is ignored and bypassed
- If the packet is larger than 1600 bytes, it is ignored and bypassed
- If the packet is a TCP-retransmit packet or has a wrong checksum, it is ignored and bypassed
- If the packet matches any of the active attack filters, it is ignored and bypassed
- If the packet is TCP and the flow is in half-open state (3 way handshake), hardware flow is created for each direction
- If the packet is TCP and is in established state, software flows (2 unidirectional) are created for the first payload packet
- If the packet is UDP, hardware flows are created for first packet in each direction.
- If the packet is UDP, software flow is created for the 5th packet.

  Creating flow on the fifth packet helps to avoid creation of software flows for port-scans, and thus, protect SCE from DoS conditions. Port-scans are still detected because their flows are opened in hardware temporarily. Also, some flows are still opened on the first packet, based on SCA-BB GUI options (Advanced settings).
- If the flow is non-TCP, non-UDP but still IP (for example, ICMP), hardware flow is opened for each direction on first packet
- If the flow is non-TCP, non-UDP but still IP (for example, ICMP), software flow is opened for each direction on second packet

User counters, Service Counters, and Protocol counters are updated, and RDRs are generated only for software flows.

- Services, page 3-4
- Protocols, page 3-6
- Initiating Side, page 3-7
- Zones, page 3-8
- Flavors, page 3-9
- Mapping Flow Attributes to Services, page 3-10

Services

In the traffic classification process, Cisco SCA BB categorizes network sessions into services.

Services are the building blocks for:

- Service configurations (because Cisco SCA BB can enforce different rules on different services)
- Aggregated usage reporting

From the point of view of a provider, a service is a network product sold to a subscriber. The service is usually a network application—such as browsing, e-mail, file sharing, or voice—that the subscriber uses. From a technical point of view, a service consists of one or more service elements, each of which enables a decision about the service associated with a network traffic flow type.

A number of services are predefined in the default service configuration. You can modify these services and add additional services to a service configuration. A service configuration can contain up to 500 services. See "Default Service Configuration Reference Tables" chapter of *Cisco Service Control Application for Broadband Reference Guide* for a list of services.

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

Traffic is classified and mapped to services based on some or all of the following service elements:

- Protocol—The protocol used. This classification allows, for example, the mapping of browsing flows and e-mail flows to separate services.
- Initiating side—Whether the subscriber side or the network side generated the flow. This classification allows, for example, the mapping of subscriber-initiated and network-initiated peer-to-peer traffic to separate services.
- Zone—Lists of IP addresses of the network-side host of the flow. This classification allows, for example, the mapping of all voice flows going to a specified server to a specific service.
- Flavor—Specific Layer 7 properties such as host names of the network-side host of the flow. This classification allows, for example, the mapping of all HTTP flows where the URL matches a certain pattern to a specific service.

Note Flavors are not used for classification when unidirectional classification is enabled.

Cisco SCA BB uses these flow mappings to map each network connection passing through it to a service. You define rules for the different services to implement control policies. The classification rules can contain Layer 3 and Layer 4 parameters (such as port numbers and IP addresses), and also Layer 7 parameters (such as host name and user agent for HTTP connections).

Note Cisco SCA BB cannot achieve 100% classification of all P2P services, because some P2P applications are persistent in trying to connect. They use many alternate protocols and connection schemes. Their native protocol is encrypted and this encryption tends to change whenever a new version is released. This means that if you try to block the P2P traffic, the client may eventually connect in some cases. A better approach may be to limit bandwidth for this traffic to make it ineffective instead of trying for a complete block.

Service Elements

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

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

Note When unidirectional classification is enabled, the flavor of a service element is always the wild-card value.

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

- The flow uses the specified protocol of the service element.
- The flow matches the initiating side specified for the service element.
- The destination of the flow is an address that belongs to the specified zone of the service element.
- The flow matches the specified flavor of the service element.

If a flow matches two service elements and one is more specific than the other, the flow is mapped to the more specific of the two. For example, Service A is defined for browsing and Service B is defined for browsing to a specific list of URLs. A browsing flow to a URL on the list of Service B matches both services, but is mapped to Service B.

If a flow matches one parameter of one service element and a different parameter of another service element, precedence is given first to matching flavors, then to protocols, then to zones, and finally to the initiating side. For example, Service A is defined for e-mail and Service B is defined for all traffic to a specific network zone. An e-mail flow to the specific network zone matches both services, but is mapped to Service A.

Examples of Services

Table 3-1 contains examples of services and their network parameters.

Table 3-1 Examples of Services and Service Parameters

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

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 Cisco SCA BB 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, Cisco SCA BB maps the flow to the HTTP protocol.

The default service 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, Cisco SCA BB maps the flow to the Generic TCP or Generic UDP protocol.

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

When unidirectional classification is enabled protocol classification is performed in the normal way, with one exception: unidirectional UDP flows. In this case, Cisco SCA BB tries to classify the protocol using the destination port of the first packet. If no exact match is found, Cisco SCA BB tries to classify the protocol using the source port.

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.

If a traffic flow meets all the following criteria, it is mapped to a specific protocol:

- 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 is 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 is mapped to Protocol B.

If a flow matches the signature of one protocol element and the port of another protocol element; it is 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 is mapped to Protocol A.

Easy Definition of Port-Based Protocols

All generic (unclassified) traffic on a specific port can be assigned to a protocol, by adding the protocol-element in the form <"Generic" signature, specific port> to that protocol. When the "Generic" signature on a specific port is assigned to a protocol, the "Behavioral" signatures are automatically assigned to that protocol as well. For example, in the default configuration, the "Generic" signature on port 555 is assigned to the H20 protocol, and therefore the "Behavioral Upload/Download" signature on port 555 is also automatically assigned to the H20 protocol.

This assignment is done automatically, so you do not need to do the assignment manually. These protocol-elements that are added automatically are not displayed in the GUI. If, on the other hand, you want to assign the “Behavioral Upload/Download” signature on a specific port to a different protocol, you can do it by creating an appropriate protocol-element and assigning it to the other protocol.

Note In the default configuration, the HTTP protocol definition accepts not just the HTTP signature, but also all other generic (unclassified) traffic on port 80, by including the protocol-element <“Generic” signature, port 80>. As described previously, when a protocol-element in this form, <“Generic” signature, specific port>, is used in a certain protocol definition, the SCE maps both the generic and the behavioral signatures, on the specified port, to that protocol.

For HTTP traffic, this means that traffic on port 80, which is classified as “Behavioral Upload/Download” signature, would also be assigned to the HTTP protocol. As described earlier, the purpose of this behavior is to allow easy definition of port-based protocols. Nevertheless, this behavior can be avoided, by adding the protocol-element <“Behavioral” signature, specific port> to a different protocol.

Signatures

Cisco SCA BB examines traffic flows using the deep-packet-inspection capabilities of the SCE platform, and compares each flow with an installed set of protocol signatures to identify the network application that generated the flow.

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

When unidirectional classification is enabled and a unidirectional flow (inbound or outbound) passes through the SCE platform, the flow is matched against a special set of unidirectional protocol signatures. When a bidirectional flow passes through the SCE platform, the protocol library tries to match it to one of its standard (bidirectional) protocol signatures.

Cisco periodically publishes protocol packs containing new signatures and updates to existing signatures. You can use these protocol packs to update the set of signatures installed on Cisco SCA BB, enhancing its classification capabilities.

Dynamic Signatures

Most signatures used by Cisco SCA BB are predefined and hard-coded. Cisco SCA BB also allows you to add dynamic signatures, which can be user-defined.

You can create and edit dynamic signatures in the Signature Editor tool. The Dynamic Signature Script (DSS) engine in Cisco SCA BB carries out the classification using these user-defined signatures in addition to the predefined signatures.

Initiating Side

The SCE platform is usually located between the subscribers of the provider and the network. Based on the initiating side, flows are called Subscriber-initiated flows and network-initiated flows. Flows initiated by the subscriber towards the network are called subscriber-initiated flow, while the flows initiated from the network towards the subscriber are called network-initiated flows.

You can limit some flow-types to one initiating side. For example, with HTTP you can restrict the direction of the flow to subscriber-initiated, because HTTP is always subscriber-initiated when the subscriber ventures outward to surf the Internet. A network-initiated HTTP-flow means, that probably a web server is open on the local machine of the subscriber for receiving incoming HTTP traffic. The provider can block network-initiated HTTP.

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 network flow of the subscriber mapped to a service 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 service element based on its destination IP address.

Examples of Zones:

- A “walled garden”—A range of IP addresses of a server farm with premium video content, for which the provider would like to limit access to specific subscribers 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.

Zone Items

A zone is a collection of related zone items.

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

Table 3-2 gives examples of zone items.

Table 3-2 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.)

For details on managing zones and zone items, see the “Managing Zones” section on page 7-34.

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 services in the Cisco Service Control solution. A protocol flavor uses an additional protocol attribute in classifying a service, making this service a flavor of the service 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 service.

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

Note Flavors are not used for traffic classification when unidirectional classification is enabled.

Flavor Items

A flavor is a collection of flavor items.

The type of a flavor item depends on the flavor type. For a list of available flavor types, see Flavor Types and Parameters, page 7-60.

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

DSCP ToS

One flavor type is TOS. This allows DSCP ToS to be used as a classification criterion so that a packet carrying a specific marking can be assigned to a predefined service with, for example, unlimited bandwidth or reported. The DSCP ToS classification process takes precedence over other classification mechanisms to allow external devices, such as a voice gateway, to dictate how the flow is treated. DSCP ToS-based classification is an excellent way of marking proprietary managed services where Cisco SCA BB does not recognize the applications but identifies them via the DSCP ToS field.

Content Filtering

Content filtering involves classification and control of HTTP flows according to the requested URL. The classification of the URL is performed by accessing an external database.

Service providers require effective Web filtering for their subscribers, for various purposes such as avoiding litigation and providing parental control. The problem is that the Web is huge and constantly growing, and Cisco SCA BB and the SCE platform are not designed to track and maintain the huge database of URLs required for effective filtering.

Cisco SCA BB provides content filtering by integrating with SurfControl Content Portal Authority (CPA). SurfControl’s technology enhances Cisco SCA BB URL classification capabilities by eliminating the need for a network administrator to manage a URL database or interact with the server, while creating a powerful filtering solution. It provides complete coverage of the web’s most trafficked sites and access to the most accurate and relevant database of URLs classified by risk category, such as sexually explicit, racist, hacker, and so on.

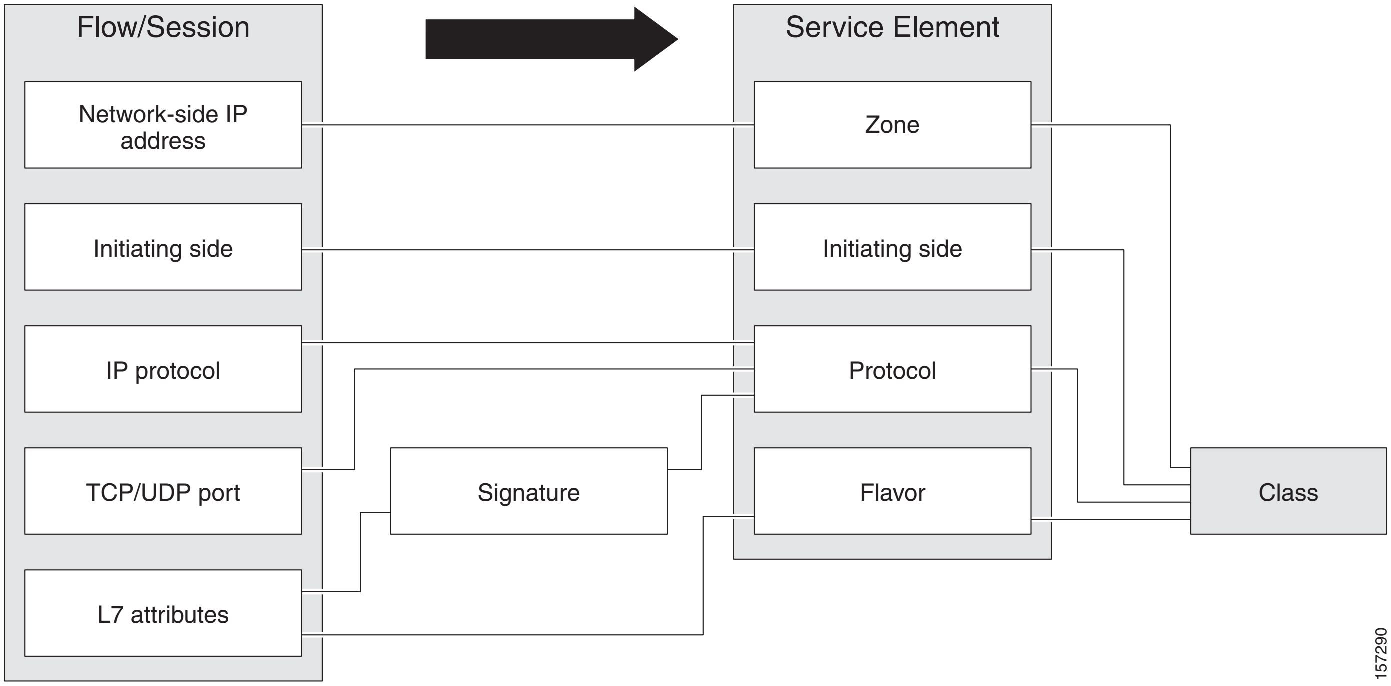
The integration of SurfControl's CPA into Cisco SCA BB provides the required web-filtering solution. Cisco SCA BB, running on the SCE platform, contacts a CPA server to categorize the website that a subscriber requests. The returned category is then used to classify the HTTP flow. This classification is then used for the normal Cisco SCA BB traffic control and reporting.

Note Cisco SCA BB includes an internal database of URLs used by the HTTP URL flavor classification. When a URL is found in both the internal database and the external content filtering database, the URL is classified according to the internal database.

Mapping Flow Attributes to Services

Figure 3-1 illustrates the mappings of flow elements of a session to service elements of a service.

Figure 3-1 Mapping Flow Attributes to a Service



Traffic Accounting and Reporting

You can use data gathered by the SCE platforms for real-time signaling, billing, and reporting.

Various metrics are collected in different scopes—global (per entire link), per service (or group of services), per package (or group of packages), and per subscriber—based on user-defined usage counters.

- Global control bandwidth is based on Layer 1 volume.
- Subscriber bandwidth control (and accounting and reporting) is based on Layer 3 volume.

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

- The SCE platform generates and transmits Raw Data Records (RDRs) that contain flow, usage, and other data.
- The SCE platform maintains an SNMP MIB that external systems can query.

Usage Accounting

Cisco SCA BB collects and maintains various network metrics, per service, in different scopes.

The network metrics are:

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

Note For VoIP services, 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 service accounting takes place in the following scopes:

- Per subscriber
- Per group of subscribers (package)
- Per link (global)

Several services may share the same service usage counter. For example, in the default service configuration, the SMTP service and the POP3 service share the E-Mail Counter. The service hierarchy determines how to assign services to usage counters, as explained in the following section. Similarly, several packages may share the same package usage counter, and the package hierarchy determines how to assign packages to usage counters. For details, see The Package Hierarchy, page 3-12.

The Service Hierarchy

Services are arranged in a hierarchal tree. A single default service is at the root, and you can place each new service anywhere in the tree. For more information see, Services, page 3-4.

Services inherit the rule of their parents. When a rule is defined for a particular service (in a specific package), unless explicitly specified, the same rule of the parent package controls all the child services.

Service Usage Counters

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

There are two categories of usage counters for services:

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

A global usage counter and a subscriber usage counter are assigned to each service. The use of a service can be accounted either exclusively for traffic classified to it or with the traffic of its parent service. For example, if a service 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 subscriber usage counter are independent. For the same service, one usage counter may be the same for parent and child, whereas the other is exclusive to the child.

The Package Hierarchy

Packages are arranged in a hierarchal tree. A single default package is the root of the tree, and you can place new packages anywhere in the tree. For more information see, Packages, page 3-15.

Package Usage Counters

The package hierarchy allows you to organize packages according to their semantics and provides for sharing package usage counters. You can define a maximum of 1024 different exclusive package usage counters per service configuration, one of which is used for the Unknown Subscriber Traffic package.

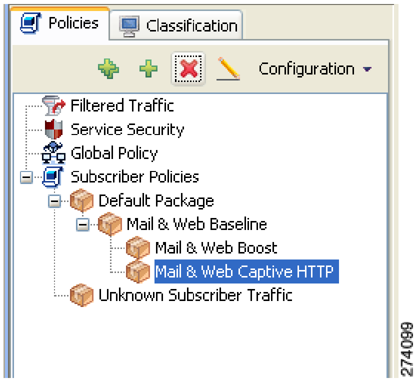
Usage reporting at a package level is grouped as follows:

- Package assigned an exclusive package usage counter—All traffic associated with this package is accounted separately in the assigned counter, along with any children that are not assigned exclusive counters.
- Package *not* assigned an exclusive package usage counter—All traffic associated with this package is accounted together with its parent package.

Figure 3-2, shows an example of a package tree. In this example, if the Mail & Web Baseline package is allocated an exclusive counter, but neither child package is assigned an exclusive counter, then all Package Usage RDRs and derived reports (such as “Package Bandwidth per Service”) would group usage of subscribers assigned to all three packages.

However, if the Mail & Web Boost package also had an exclusive counter, the traffic for Main & Web Baseline and Mail & Web Captive HTTP would be accounted together, but traffic for Mail & Web Boost would be accounted separately. (In general this is not an efficient configuration. You should use the hierarchical structure to group packages that can share the same counter.)

Figure 3-2 Example Package Tree



Reporting

SCE platforms running Cisco SCA BB generate and transmit Raw Data Records (RDRs) that contain information relevant to the service provider.

RDRs contain a wide variety of information and statistics, depending on the configuration of the system.

RDRs are transmitted using a Cisco proprietary protocol. To use RDRs, you require the Cisco Service Control Management Suite (SCMS) Collection Manager (CM) or to develop software to process the RDRs.

The data in some RDRs can also be exported using the NetFlow reporting protocol, which has become an industry standard. NetFlow reporting allows the Cisco SCA BB solution to be more easily integrated with your existing data collectors.

- RDRs, page 3-14
- NetFlow, page 3-14

RDRs

The following are the main categories of RDRs:

- Usage RDRs—Generated periodically. These RDRs contain the state of the usage counters, per service and per accounting scope. There are four types of usage RDRs:
    - Link Usage RDRs—Global usage per service, for the entire link.
    - Package Usage RDRs—Usage per group of subscribers, per service.
    - Subscriber Usage RDRs—Usage per subscriber, per service. These RDRs are generated for all subscribers. The Cisco Service Control Management Suite (SCMS) Collection Manager (CM) and Cisco Service Control Application (SCA) Reporter use these RDRs to generate top-subscriber reports and aggregated usage billing records.
    - Real-Time Subscriber Usage RDRs—Generated for selected subscribers only. The SCMS Collection Manager and SCA Reporter use these RDRs by to generate detailed subscriber 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 billing.
- Real-Time Signaling RDRs—Generated to indicate specific network events such as flow start or end. These RDRs are used to signal external systems to allow real-time actions across the network.
- Malicious Traffic RDRs—Generated to indicate that the SCE platform has detected a traffic anomaly, such as a DDoS attack. These RDRs are used to detect attacks and attackers to mitigate them.

NetFlow

The following information can be exported using the NetFlow protocol

- Usage—Generated periodically. These RDRs contain the state of the usage counters, per service and per accounting scope.
- Malicious Traffic—Generated to indicate that the SCE platform has detected a traffic anomaly, such as a DDoS attack.

Traffic Control

Traffic Control provides means to block, limit, or prioritize traffic flows according to service, subscriber package, subscriber quota state, and so on.

- Packages, page 3-15
- Unknown Subscriber Traffic, page 3-15
- Rules, page 3-16
- Bandwidth Management, page 3-16
- Quota Management, page 3-19

Packages

A package is a collection of rules describing subscriber policy. The package defines the group of services delivered to a specific group of subscribers and the behavior of the system for each service. It may contain restrictions on network flows, guidelines for prioritization of the flows, and instructions about how to report flows.

Each subscriber in the network is provided with a reference to a package to which that subscriber belongs. The following list describes how the system references each subscriber in the network:

1. Maps each network flow to a service by matching the flow with a service element
2. Identifies the subscriber to whom the flow pertains, according to the network ID of the subscriber (usually the IP address of the subscriber)
3. Identifies the package to which the subscriber belongs
4. Applies the correct rule to the service of the network flow of the subscriber

Another scheme is described in Virtual Links Mode, page 3-15.

Virtual Links Mode

In normal mode, you define bandwidth controllers for each package (see Bandwidth Management, page 3-16). In Virtual Links mode, you define template bandwidth controllers. The actual bandwidth parameters are assigned to a subscriber when the subscriber enters the system. These parameters depend on the package of the subscriber and the direction of the virtual link.

For more information, see Managing Quotas, page 9-83.

Unknown Subscriber Traffic

The SCE platform tries to identify the subscriber responsible for every traffic flow that it processes. The platform looks at the IP address or VLAN tag of the traffic flow, and checks its internal database for a subscriber identified by this IP Address or VLAN tag. If such a subscriber is not found in the database, the traffic flow is mapped to the Unknown Subscriber Traffic category.

Rules

A rule is a set of instructions that tell the SCE platform how to treat network flows of a specific service. A rule may:

- Specify that a flow should:
  - be blocked
  - be granted a certain amount of bandwidth
  - have the DSCP ToS of its packets marked with a given value (see DSCP ToS Marking, page 3-23)
- Define an aggregate volume or session limit, after which a set of different restrictions are enforced on the flow
- Specify how a flow is reported for billing or analysis purposes

Calendars

You can use calendars to divide the hours of the week into four time frames.

After you have configured a calendar, you can add Time-Based Rules, page 3-16 to a package that uses the calendar.

Time-Based Rules

A time-based rule is a rule that applies to only one time frame. Time-based rules allow you to set rule parameters that are only applied at specific times. You might, for example, want to define different rules for peak, off-peak, nighttime, and weekend usage.

You can add time-based rules to any rule. If a time-based rule is not defined for a time frame, the parent rule is enforced.

Often, you need rules for different time frames to be similar. When you add a time-based rule, the settings of the parent rule are copied to the new time-based rule; you can make any needed changes. Subsequent changes to the parent rule do not affect the time-based rule.

Bandwidth Management

The physical link bandwidth is an absolute limit on the bandwidth that can pass through the system. You can limit the total bandwidth passing through the SCE platform to a value lower than the physical link bandwidth. For example, if another device connected to the SCE platform on the IP stream has limited BW capacity, you can limit the bandwidth passing through the SCE platform to match the capacity of the other device.

Bandwidth control in Cisco SCA BB is accomplished in two stages:

- Global control
- Subscriber bandwidth control
- Global control bandwidth is based on Layer 1 volume.
- Subscriber bandwidth control (and accounting and reporting) is based on Layer 3 volume.

Global Bandwidth Control

Global controllers control the total bandwidth use. Global controllers are virtual queues in SCE platforms. You configure them for the entire system, rather than for individual subscribers.

Global controllers provide constraints for large, global volumes of traffic, such as "Total Gold Subscriber Traffic", or "Total P2P Traffic". Each global controller defines the maximum percentage of total available bandwidth allocated to all traffic of a particular type. Using a global controller, you can limit total traffic of services such as P2P in the system to any bandwidth between 16 kb/s and 1000 Mb/s. In this way, you keep the total bandwidth consumed by this traffic under control.

The upstream and downstream interfaces are each assigned one default global controller that, by default, controls 100 percent of the link traffic. You can add up to 1023 more global controllers for each interface on Cisco SCE Gigabit Ethernet hardware and up to 4095 more global contraollers on Cisco SCE 10 Gigabit Ethernet hardware and you can assign a maximum percentage of the total link limit to each global controller separately.

For each global controller, you can define separate values for the maximum percentage of total available bandwidth separately for each time frame. (See Calendars, page 3-16.)

In dual-link systems, you can define different bandwidth values for each link. You can also set a limit on the aggregated bandwidth passing on the two links.

Virtual Links mode uses template global controllers. Template global controllers are templates of virtual queues; they are applied to as many separate physical links as exist in the system. For each physical link, actual bandwidth parameters depend on the link. (For more information, see Managing Quotas, page 9-83.)

Subscriber Bandwidth Control

Subscriber BW Controllers (BWCs) controls the bandwidth used by individual subscribers.

Each BWC controls available bandwidth for selected services. Services controlled by a particular BWC are defined per package, but bandwidth control is per service.

The following parameters specify a BWC:

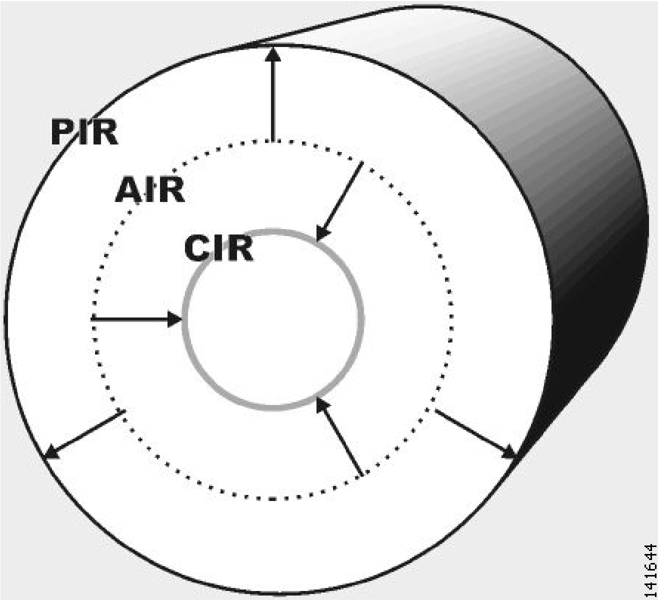
- Committed Information Rate (CIR)—The minimum bandwidth that must be granted to the services that a BWC control.
- Peak Information Rate (PIR)—The maximum bandwidth that can be allocated to the services that a BWC control.
- Global Controller—The global controller to which this BWC links
- Assurance Level (AL)—The rate of change of available bandwidth under conditions of traffic congestion

Figure 3-3 illustrates the maximum available bandwidth (Admitted Information Rate [AIR]) ranges between the CIR and the PIR. The actual consumed bandwidth is always less than the AIR.

The BWC has a third parameter that controls how the AIR is determined at different congestion conditions. When the network is not congested the system allows the PIR and when the network is highly congested the system provides the CIR. In between these two extremes, a third parameter—Assurance Level (AL)—determines the AIR. The AL controls how fast the AIR would decrease from the PIR to the CIR as congestion builds, or increase from the CIR to the PIR as congestion decreases. A higher AL ensures a higher AIR compared to a similar BWC with a lower AL.

The BWC ensures that even when the network is congested (PIR-congestion) at least the CIR is granted. Similarly, the BWC ensures that even when there is little traffic associated with a BWC the PIR is not exceeded.

Figure 3-3 Bandwidth Control Levels



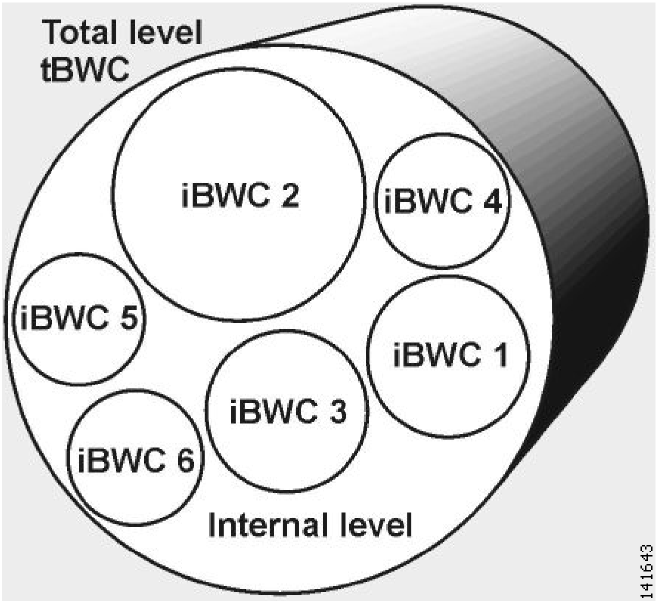
Bandwidth may be thought of in terms of a virtual pipe of adjustable width. The PIR is the maximum allowed width of the virtual pipe. The CIR is the minimum width to which the pipe can contract. The actual pipe width is the AIR. During Network congestion, the system contracts each pipe differently to differentiate between subscribers and between their services.

Primary and Internal Bandwidth Control

In Cisco SCA BB each subscriber has an independent set of BWCs, consisting of a single Primary (Total) BWC (tBWC) that controls the total bandwidth available to the subscriber and several Internal BWCs (iBWCs) that control the available bandwidth of some services of that subscriber, as illustrated in Figure 3-4. For example, one BWC may control the Streaming Service; another may control the Download and E-mail Services together.

The PIR defines the maximum bandwidth for the associated services; the CIR defines the minimum bandwidth for them.

Figure 3-4 Bandwidth Control on Two Levels



You can link iBWCs to traffic in the following way:

1. In the package general definitions, add a subscriber BWC, defined by its CIR, PIR, AL, and CoS.
2. When defining a rule, assign each service to one subscriber BWC.

Quota Management

You can assign subscribers a quota limit on selected services.

Each subscriber has 16 quota buckets, each of which you can define for volume or sessions. When a subscriber uses a certain service, the amount of consumed volume or number of sessions is subtracted from one of the buckets.

The service configuration determines which bucket to use for each service. Consumption of volume buckets is measured in units of L3 kilobytes. Consumption of session buckets is measured by the number of sessions. For example, you can define that the Browsing and E-Mail services consume quota from Bucket #1, that the P2P service consumes quota from Bucket #2, and that all other services are not bound to any particular bucket.

External quota provisioning systems can use the Quota Provisioning API to modify the quota in each bucket dynamically. For example, you can increase the quota of a certain bucket when a subscriber purchases additional quota. These external systems can also query the amount of remaining quota in each bucket. This can be used, for example, to show subscribers in a personal web page how much of their quota remains. For details on Quota Provisioning API, see *Cisco SCMS SCE Subscriber API Programmer's Guide.*

External quota provisioning can also be acquired using the Quota Manager (QM), an off-the-shelf solution provided by Cisco. For more information about the installation and operation of the QM, see *Cisco Service Control Management Suite Quota Manager User Guide.*

External quota provisioning can also be acquired using the Gy quota model and Gx quota model. For more information, see *Cisco Service Control Mobile Solution Guide*.

Note External quota provisioning is not supported when unidirectional classification is enabled.

The internal Cisco SCA BB quota provisioning system replenishes each quota bucket by a fixed amount at fixed intervals.

Subscribers can be notified when they breach the quota in any bucket.

Subscriber Notification

The subscriber notification feature lets you push web-based messages (such as notifications of quota depletion) to a subscriber by redirecting the subscriber HTTP traffic to relevant web pages. HTTP redirection starts when the subscriber notification is activated and ceases when the notification is dismissed.

Note Subscriber notification is not supported when unidirectional classification is enabled.

Other Traffic Processing Features

This section outlines other traffic processing features provided by Cisco SCA BB.

- Service Security, page 3-21
- Traffic Filters, page 3-22
- Traffic Forwarding to Value Added Services Servers, page 3-23

Service Security

Cisco SCA BB includes service security functionality to help protect network operators and their subscribers from attacks and malicious traffic:

- DoS attacks
- DDoS attacks
- VoIP threats
- Worms
- Hacker activity
- Malicious takeover of subscriber computers:
  - Spam zombies
  - E-mail based viruses

Although it is never possible to provide complete protection from network threats, the Cisco Service Control solution provides insight into malicious activity in a network, and can mitigate large-scale eruptions of malicious activity that compromise overall network performance.

Networks operators can use Cisco SCA BB to:

- Monitor network traffic for suspicious activity
- Block malicious traffic
- Notify subscribers that are creating or have been affected by malicious traffic

Detecting Malicious Traffic

Cisco SCA BB uses three threat detection mechanisms:

- Anomaly Detection—This set of mechanisms monitors the rate of connections (both successful and unsuccessful) to and from each host IP address. High connection rates or a low ratio between successful and unsuccessful connections indicate malicious activity.

  Anomaly detection characteristics can indicate the following categories of malicious activity:

  - IP sweep—Scanning multiple IP addresses, all on the same port (a behavior typical of worms)
  - Port scan—Scanning all ports at one IP address (a behavior typical of hackers)
  - DoS attack—An attack (on a single IP address) from a single IP address
  - DDoS attack—An attack (on a single IP address) from multiple IP addresses

Note Cisco SCA BB identifies a DoS attack with spoofing (using many fake IP addresses instead of one real address) as a DDoS attack.

- The anomaly detection mechanism is effective in addressing new threats as they appear. It does not need knowledge about their exact nature and Layer 7 signatures, but is based on the characteristics of their network activity.
- Mass mailing activity detection—This mechanism monitors SMTP session rates for individual subscribers (using SCE platform subscriber-awareness; it can work in subscriber-aware or anonymous subscriber mode). A high rate of SMTP sessions from an individual subscriber is usually an indicator of malicious activity that involves sending e-mail (either mail-based viruses or spam-zombie activity).
- Signature-based detection—The stateful Layer 7 capabilities of the SCE platform are used to detect malicious activity that is not easily detectable by the other mechanisms. Operators can add signatures for such threats, achieving a quick response time in addressing new threats.
- RFC compliance detection—This mechanism monitors the SMTP traffic for RFC compliance. Non-compliant traffic is marked as spam.

Responding to Malicious Traffic

You can define the following actions when configuring the detection mechanisms described in the preceding section:

- Monitor the network for malicious activity detected by each of these mechanisms.

  You can display graphs in the Console based on data collected for malicious activity analysis.
- Automatically block malicious activity detected by the SCE platform to avoid threat propagation and adverse effects to the network.
- Notify subscribers that are involved in malicious activity by redirecting their web sessions to a captive portal.

Cisco SCA BB provides a high level of flexibility in tuning the detection methods to define malicious activity and in configuring the actions to be taken when malicious activity is detected.

Traffic Filters

Filter rules are part of service configurations. Filter rules allow you to instruct the SCE platform to ignore some types of flow (based on the Layer 3 and Layer 4 properties of the flow) and to transmit the flows unchanged.

When a traffic flow enters the SCE platform, the platform checks whether a filter rule applies to the flow. If a filter rule applies to this traffic flow, the SCE platform performs one of the following actions:

- Bypass—The SCE platform passes the traffic flow to its transmit queues without generating any RDRs (the flow does not appear in records generated for analysis purposes) and without enforcing any service configuration rules.
- Quick forward—A flow filter rule action whose aim is to ensure low latency for delay sensitive flows. The packets of quick-forwarded flows are duplicated and sent through different paths: one copy goes directly to the transmit queue and thus suffers only a minimal delay, the other copy goes through the normal packet path.

A filter rule can also set the DSCP ToS value of the filtered traffic. See DSCP ToS Marking, page 3-23.

It is recommended that you add filter rules for OSS protocols (such as DHCP) and routing protocols (such as BGP) that might traverse the SCE platform. These protocols usually should not be affected by policy enforcement, and their low volume makes them insignificant for reporting.

A number of filter rules are included in the default service configuration.

Flows of certain protocols can also be filtered according to the Layer 7 characteristics of the flow.

DSCP ToS Marking

DSCP ToS marking is used in IP networks to signal the type and priority of a flow between network elements. Typically, those elements that have an insight on how to treat the traffic throughout the network performs the DSCP ToS marking. Such an element can be the element generating traffic—a voice gateway, for example. Cisco SCA BB, being application aware, can, for example, allocate bandwidth resources based on the business model and the specific needs of latency sensitive applications.

Traffic Forwarding to Value Added Services Servers

Traffic forwarding to Value Added Services (VAS) servers allows the Cisco Service Control solution to use an external expert system (VAS server) for additional traffic processing. The SCE reroutes traffic to the preconfigured location of the VAS server. After processing, the traffic is sent back to the SCE, which then sends it to its original destination.

Note VAS traffic forwarding is not supported when unidirectional classification is enabled.

Service Configurations

A service configuration implements and enforces the business strategy and vision of the provider.

A service configuration can take effect only after it is propagated to the appropriate SCE platform. Cisco SCA BB enforces the service configuration by analyzing the network traffic passing through them.

A service configuration consists of:

- Traffic classification settings—Services, such as web browsing, file sharing, and VoIP. Each service consists of elements that define how network traffic is mapped to the service. The configuration building blocks of services are protocols, zones, flavors, and signatures.
- Traffic accounting and reporting settings—Settings that determine how traffic flows and network usage accounting are reported.
- Traffic control settings—Packages, which consist of a set of rules (such as bandwidth rate limit and quota limits) defined for different services. The main configuration building blocks of packages are rules, quota buckets, subscriber BWCs, and global controllers.

Defining Service Configurations in Practice

In practice, defining service 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 service configuration.
3. Gather data.
4. Analyze.
5. Do one or both of the following:
   - Continue traffic discovery by partitioning the traffic into (additional) services.
   - Create rules to limit and prioritize traffic according to services and subscriber packages.

CHAPTER 4

Getting Started

Revised: December 10, 2013, OL-24178-09

Introduction

The module guides you through the process of installing or upgrading the Cisco SCA BB:

- Describes the concept of the Console as a collection of tools, presents each tool and its role. This module also describes how to launch the tools and navigate between these tools.
- Explains how to install Protocol Packs, which contain new and updated protocol signatures
- Concludes with a QuickStart that describes how to apply your first service configuration and generate your first report

How to Install Cisco SCA BB

Note The Cisco SCA BB application can only be installed in the administrator user group of Windows XP. During installation the Cisco SCA BB application changes registry entries, therefore installation in normal user groups is not allowed. The installer must have administrator privileges assigned.

You install Cisco SCA BB in two stages:

1. Install the Cisco SCA BB front ends:
   - The Cisco SCA BB Console
   - The Cisco SCA BB Service Configuration Utility, the Cisco SCA BB Signature Configuration Utility, and the Cisco SCA BB Real-Time Monitoring Configuration Utility
2. Install the Cisco SCA BB application components:
   - The Cisco SCA BB Service Modeling Language Loadable Image (SLI) and the Cisco SCA BB Service Control Engine (SCE) applicative management plug-in
   - The Cisco SCA BB Subscriber Manager applicative management plug-in (for systems with a Cisco SCMS Subscriber Manager)

If you are upgrading an existing installation of Cisco SCA BB, see How to Upgrade the SCE Using the SCE Software Upgrade Wizard, page 4-8 or Working with Protocol Packs, page 4-20.

The Cisco SCA BB Installation Package

The Cisco SCA BB installation package is a ZIP file located in the CCO.

The installation package consists of the following files:

- The installer for the Console: scas-bb-console-<version>-<build>.exe.
- A Cisco installation application package file (PQI file) for each type of SCE platform. Each PQI file is located in a subfolder whose name is the platform name.
- The file scas_bb_util.tgz, which contains the files for the Cisco SCA BB Service Configuration Utility (**servconf**), the Cisco SCA BB Signature Configuration Utility (**sigconf**), the Cisco SCA BB Real-Time Monitoring Configuration Utility (**rtmcmd)** (together with real-time monitoring report templates), and the BGP Autonomous System Dynamic Detection scripts and files (**routerInfo.properties**, **asFetch.bat**, **asFetch.sh**).
- The file PCubeEngageMib.mib, which defines the SCAS BB MIB, located in the SNMP subfolder.
- The Cisco SCA BB Service Configuration Java API distribution file: serviceconfig-java-api-dist.tgz.
- The file surfcontrol.xml, which lists the content categories for content filtering using SurfControl Content Port Authority, located in the URL Filtering subfolder.

Installing Cisco SCA BB Application Components

Cisco SCA BB has two software components that reside on the SCE platform:

- The Cisco SCA BB SLI, which performs traffic processing
- The Cisco SCA BB SCE applicative management plug-in, which performs some service configuration operations

Cisco SCA BB also has one software component that resides on the Subscriber Manager device:

- The Cisco SCA BB Subscriber Manager applicative management plug-in, which performs some application-specific subscriber management operations

To install these components from the Console, see How to Install PQI Files on SCE Devices, page 5-25 and Managing Collection Manager Devices, page 5-30.

To install these components from a command line, see Installing PQI Files from the Command Line, page 14-12.

Prerequisites

Before installing Cisco SCA BB, verify that the SCE platform and, if used, the SCMS Subscriber Manager are operational and are running appropriate versions of their software.

- How to Verify that the SCE Platform is Operational, page 4-3
- How to Verify that the SCE Platform is Running an Appropriate Version of the OS, page 4-3
- How to Verify that the Subscriber Manager is Correctly Installed, page 4-3
- How to Verify that an Appropriate Version of the Subscriber Manager is Running, page 4-4

How to Verify that the SCE Platform is Operational

Step 1 Verify that the status LED on the SCE flashes green. (Orange—booting up; flashing orange—warning; red—failure.)

How to Verify that the SCE Platform is Running an Appropriate Version of the OS

Step 1 At the SCE platform CLI prompt `(SCE#)`, type `show version`.

Step 2 Press **Enter**.

The response shows the version of the OS running on the SCE platform.

How to Verify that the Subscriber Manager is Correctly Installed

Step 1 Open a Telnet session to the Subscriber Manager.

Step 2 Go to the Subscriber Manager bin directory and type `p3sm --sm-status`.

Step 3 Press **Enter**.

The response to this command displays the operational status of the Subscriber Manager.

How to Verify that an Appropriate Version of the Subscriber Manager is Running

Step 1 Open a Telnet session to the Subscriber Manager.

Step 2 Go to the Subscriber Manager bin directory and type `p3sm version`.

Step 3 Press **Enter**.

The response to this command displays the Subscriber Manager version.

How to Install Cisco SCA BB Front Ends

You should install the following Cisco SCA BB front ends:

- The Console
- The Cisco SCA BB Service Configuration Utility (**servconf**), the Cisco SCA BB Signature Configuration Utility (**sigconf**), and the Cisco SCA BB Real-Time Monitoring Configuration tool (**rtmcmd**) (together with associated real-time monitoring report templates)
  - **servconf** requires access to the Java Runtime Environment (JRE) (see Installing the Java Runtime Environment, page 4-4).

Hardware Requirements

- At least 1024-MB RAM is required to run the Console.
- The minimal supported screen resolution for the Console is 1024x768 pixels.

Operating System Requirements

The SCA Reporter GUI front end can be installed on any computer running Windows 2000, Windows XP, Windows Vista, or Windows 7.

Installing the Java Runtime Environment

The Cisco SCA BB Service Configuration Utility, **servconf,** requires access to JRE version 1.6.

To verify that the JRE is installed, run **java -version** from the command prompt. The Java version should start with 1.6.

If a different version of JRE is also installed on the workstation, you may need to tell **servconf** where to find the appropriate JRE. Do this by setting the JAVA_HOME environment variable to point to the JRE 1.6 installation directory. For example:

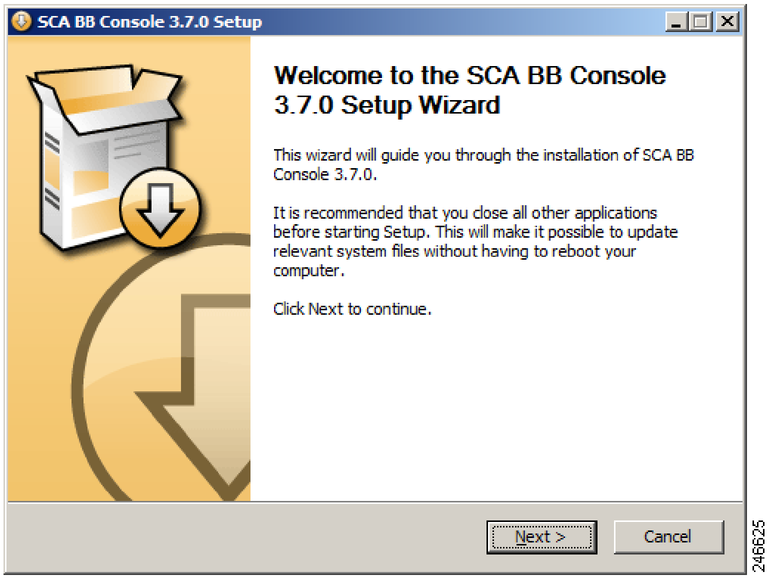
```
JAVA_HOME=C:\Program Files\Java\j2re1.6_08
```

How to Install the Console

Step 1 Navigate to the Console installation file, sca-bb-console-3.7.0.exe, and double-click it.

The Welcome page of the Cisco SCA BB Console 3.7.0 Setup wizard appears (see Figure 4-1).

Figure 4-1 Welcome to the Cisco SCA BB Console 3.7.0 Setup Wizard



SCA BB Console 3.7.0 Setup

Welcome to the SCA BB Console 3.7.0 Setup Wizard

This wizard will guide you through the installation of SCA BB Console 3.7.0.

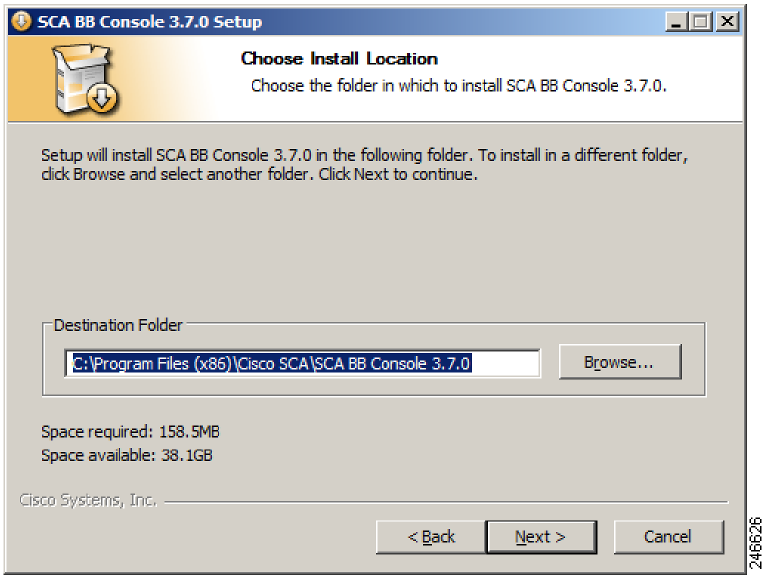
It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

Step 2 Click **Next**.

The Install Location page of the Setup wizard opens (see Figure 4-2).

Figure 4-2 Choose Install Location



SCA BB Console 3.7.0 Setup

Choose Install Location

Choose the folder in which to install SCA BB Console 3.7.0.

Setup will install SCA BB Console 3.7.0 in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.

Destination Folder: C:\Program Files (x86)\Cisco SCA\SCA BB Console 3.7.0

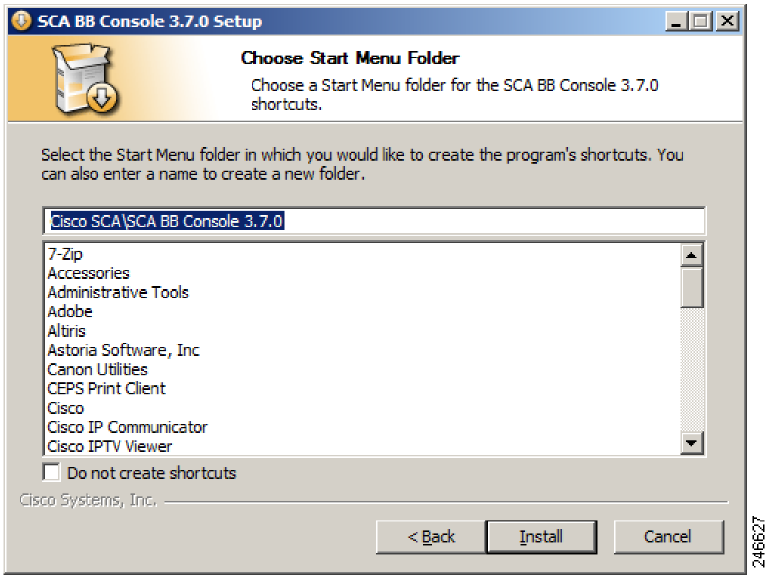
Space required: 158.5MB
Space available: 38.1GB

Step 3 (Optional) Click **Browse** and choose a different destination folder.

Step 4 Click **Next**.

The Start Menu Folder page of the Setup wizard opens (see Figure 4-3).

Figure 4-3 Choose Start Menu Folder



SCA BB Console 3.7.0 Setup

Choose Start Menu Folder

Choose a Start Menu folder for the SCA BB Console 3.7.0 shortcuts.

Select the Start Menu folder in which you would like to create the program's shortcuts. You can also enter a name to create a new folder.

Cisco SCA\SCA BB Console 3.7.0

7-Zip
Accessories
Administrative Tools
Adobe
Altiris
Astoria Software, Inc
Canon Utilities
CEPS Print Client
Cisco
Cisco IP Communicator
Cisco IPTV Viewer

□ Do not create shortcuts

Cisco Systems, Inc.

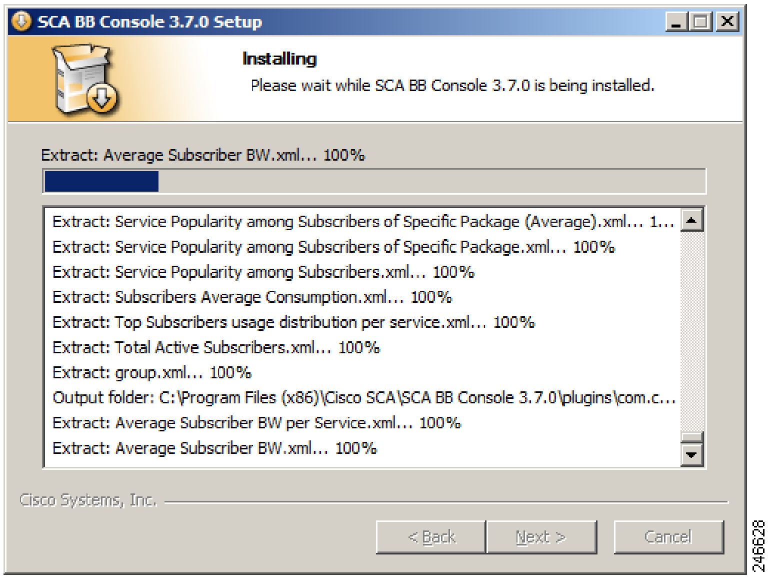
Step 5 (Optional) Enter a different Start Menu folder in the Start Menu Folder field.

Step 6 (Optional) Check the **Do not create shortcuts** check box.

Step 7 Click **Install**.

The Installing page of the Setup wizard opens (see Figure 4-4).

Figure 4-4 Installing



SCA BB Console 3.7.0 Setup

Installing

Please wait while SCA BB Console 3.7.0 is being installed.

Extract: Average Subscriber BW.xml... 100%

```
Extract: Service Popularity among Subscribers of Specific Package (Average).xml... 1...
Extract: Service Popularity among Subscribers of Specific Package.xml... 100%
Extract: Service Popularity among Subscribers.xml... 100%
Extract: Subscribers Average Consumption.xml... 100%
Extract: Top Subscribers usage distribution per service.xml... 100%
Extract: Total Active Subscribers.xml... 100%
Extract: group.xml... 100%
Output folder: C:\Program Files (x86)\Cisco SCA\SCA BB Console 3.7.0\plugins\com.c...
Extract: Average Subscriber BW per Service.xml... 100%
Extract: Average Subscriber BW.xml... 100%
```

Cisco Systems, Inc.

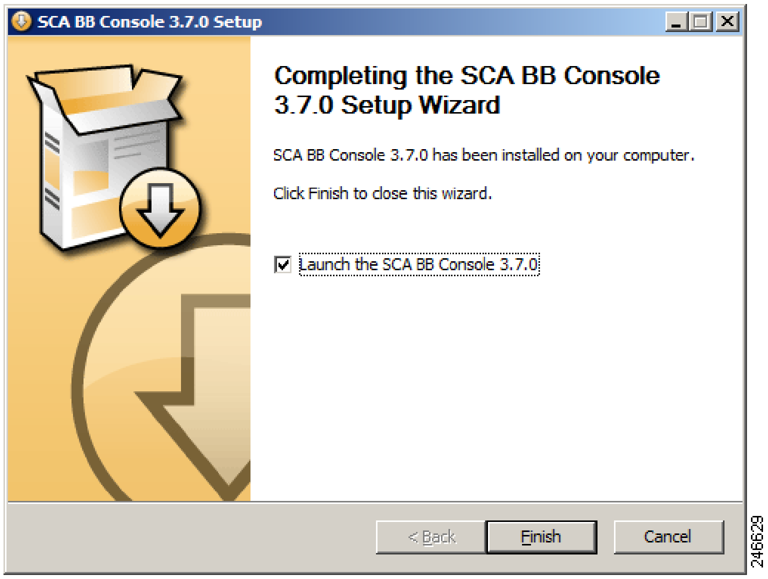
Step 8 Wait until the installation is complete.

The Next button is enabled.

Step 9 Click **Next**.

The Installation Complete page of the Setup wizard opens (see Figure 4-5).

Figure 4-5 Completing the Cisco SCA BB Console 3.7.0 Setup Wizard



SCA BB Console 3.7.0 Setup

Completing the SCA BB Console 3.7.0 Setup Wizard

SCA BB Console 3.7.0 has been installed on your computer.

Click Finish to close this wizard.

☑ Launch the SCA BB Console 3.7.0

Step 10 To launch the Console, check the **Run SCA BB Console after installation** check box.

Step 11 Click **Finish**.

The Cisco SCA BB Console 3.7.0 Setup wizard closes.

The Console is now installed on the machine.

A shortcut is added to the Start menu.

How to Install the Cisco SCA BB Configuration Utilities

Step 1 From the Cisco SCA BB installation package, extract the scas_bb_util.tgz file, and copy it to a work station having Windows, Solaris, or Linux operating system.

Step 2 Unpack the file to a new folder. The Cisco SCA BB Service Configuration Utility (**servconf**), the Cisco SCA BB Real-Time Monitoring Configuration Utility (**rtmcmd)** (and associated real-time monitoring report templates), the Cisco SCA BB Signature Configuration Utility (**sigconf**), and the BGP Autonomous System Dynamic Detection scripts and files (**routerInfo.properties**, **asFetch.bat**, **asFetch.sh**) are located in the bin folder. This folder also stores the BGPRouter<*number*>.csv file generated by the asFetch.bat script after fetching the BGP AS information from the router.

How to Upgrade Cisco SCA BB Components

Upgrading Cisco SCA BB includes upgrading each of these software components:

- SCE Firmware
- The SCE PQI file
- Protocol Pack SPQI file
- Policy file

Note This section describes the upgrade of Cisco SCA BB application components only. For a full description of the entire Cisco solution upgrade procedure, consult the solution upgrade document accompanying the formal release.

- When you upgrade old PQB files, some protocol IDs are changed automatically. Messages such as the following may be displayed to indicate the change:

```
Protocol ID of BaiBao changed from 80 to 43
Protocol ID of PPLive changed from 81 to 44
```

- When you upgrade a device with a new SPQI or PQI file, all other devices that are not upgraded may fail.
- New Cisco SCA BB releases do not use the default Dynamic Signature Script (DSS) file (see that it was installed for a previous Cisco SCA BB release).
- If a protocol pack for the new release is available, install it after the product installation is complete. Do *not* install an old protocol pack on top of a new product installation.

How to Upgrade the SCE Using the SCE Software Upgrade Wizard

You can upgrade the SCE using the Network Navigator Tool via the SCE Software Upgrade wizard.

Step 1 Open the Network Navigator.

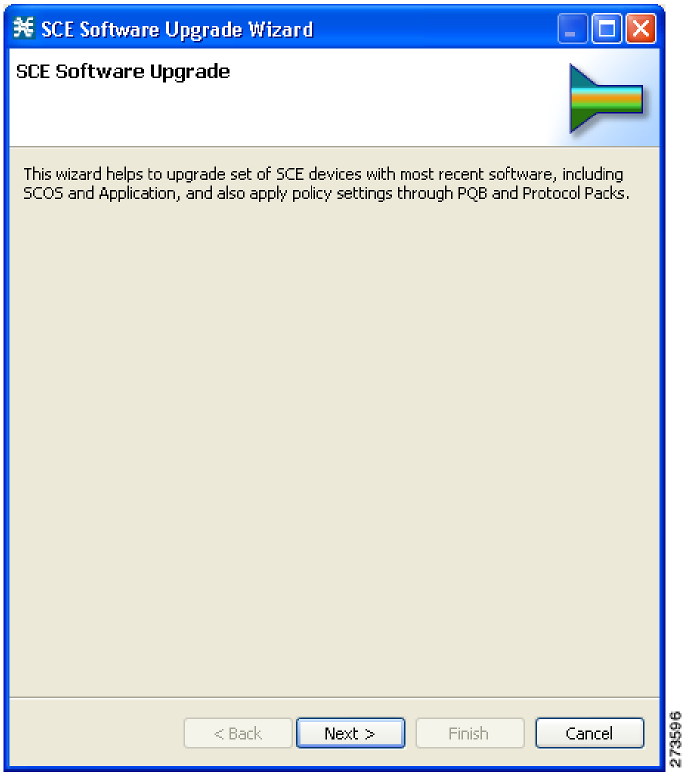
Step 2 Choose one or more devices in the Site Manager tree.

Step 3 Right-click one of the selected devices.

Step 4 From the popup menu that appears, choose SCE Software Upgrade wizard.

The SCE Software Upgrade wizard appears (see Figure 4-6).

Figure 4-6 SCE Software Upgrade

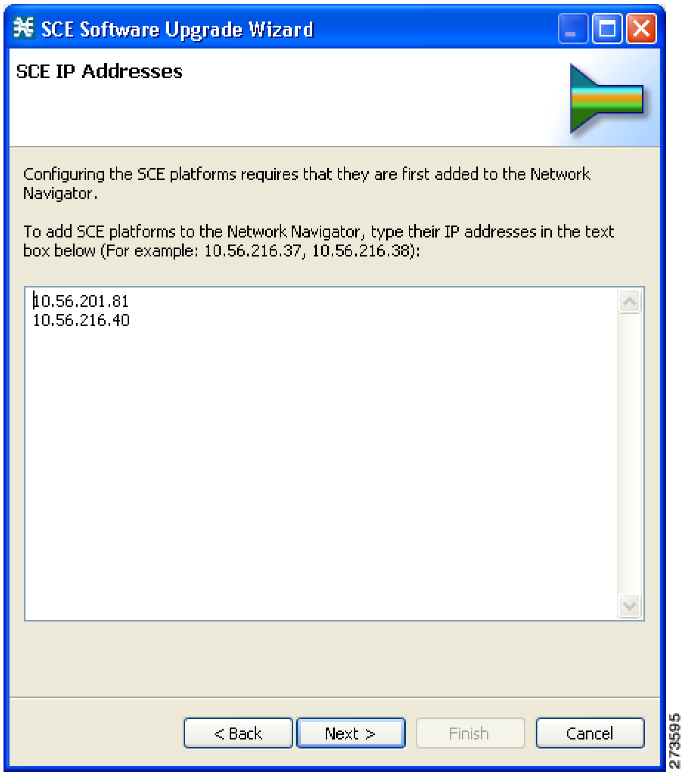


This wizard helps to upgrade set of SCE devices with most recent software, including SCOS and Application, and also apply policy settings through PQB and Protocol Packs.

Step 5 Click **Next**.

The SCE IP Addresses page of the SCE Software Upgrade wizard opens (see Figure 4-7).

Figure 4-7 SCE IP Address



SCE IP Addresses

Configuring the SCE platforms requires that they are first added to the Network Navigator.

To add SCE platforms to the Network Navigator, type their IP addresses in the text box below (For example: 10.56.216.37, 10.56.216.38):

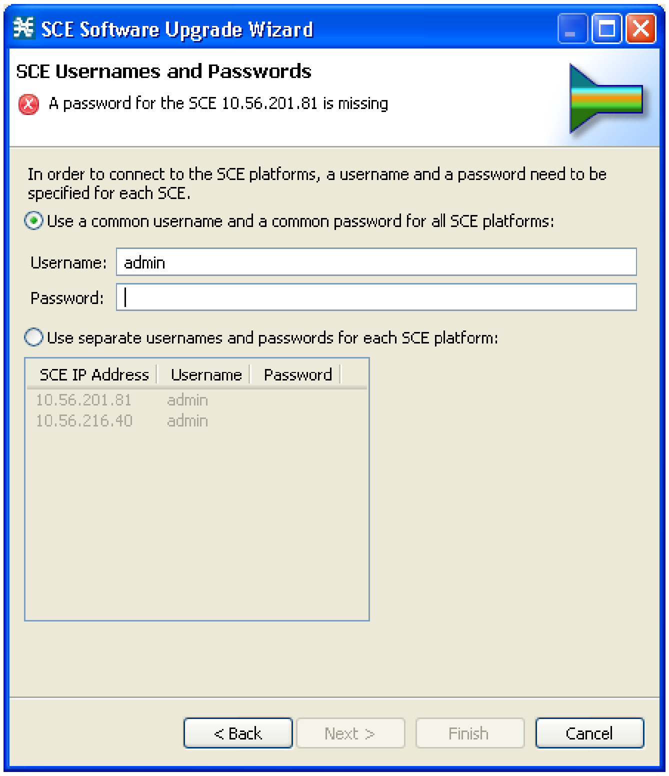
```
10.56.201.81
10.56.216.40
```

Step 6 (Optional) In the edit box, enter additional IP addresses.

Step 7 Click **Next**.

The SCE Usernames and Passwords page of the SCE Software Upgrade wizard opens (see Figure 4-8).

Figure 4-8 SCE Usernames and Passwords



SCE Software Upgrade Wizard

SCE Usernames and Passwords

A password for the SCE 10.56.201.81 is missing

In order to connect to the SCE platforms, a username and a password need to be specified for each SCE.

● Use a common username and a common password for all SCE platforms:

Username: admin

Password:

○ Use separate usernames and passwords for each SCE platform:

SCE IP Address	Username	Password
10.56.201.81	admin	
10.56.216.40	admin	

Step 8 Enter the usernames and passwords for the SCE devices.

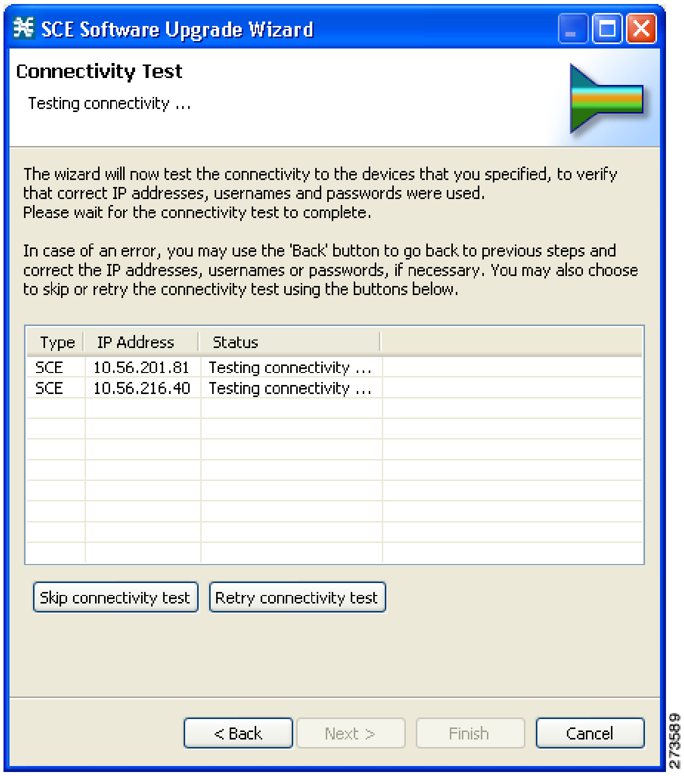
Do one of the following:

- To use the same username and password for all the SCE devices that you are adding, enter the username in the Username field and the password in the Password field.
- To provide a different username and password pair for each SCE device, click the **Use separate usernames and passwords for each SCE platform** radio button, and, for each SCE device, enter the username and password in the appropriate cell of the table.

Step 9 Click **Next**.

The Connectivity Test page of the SCE Software Upgrade wizard opens (see Figure 4-9).

Figure 4-9 Connectivity Test



SCE Software Upgrade Wizard

Connectivity Test

Testing connectivity ...

The wizard will now test the connectivity to the devices that you specified, to verify that correct IP addresses, usernames and passwords were used.
Please wait for the connectivity test to complete.

In case of an error, you may use the 'Back' button to go back to previous steps and correct the IP addresses, usernames or passwords, if necessary. You may also choose to skip or retry the connectivity test using the buttons below.

Type	IP Address	Status
SCE	10.56.201.81	Testing connectivity ...
SCE	10.56.216.40	Testing connectivity ...

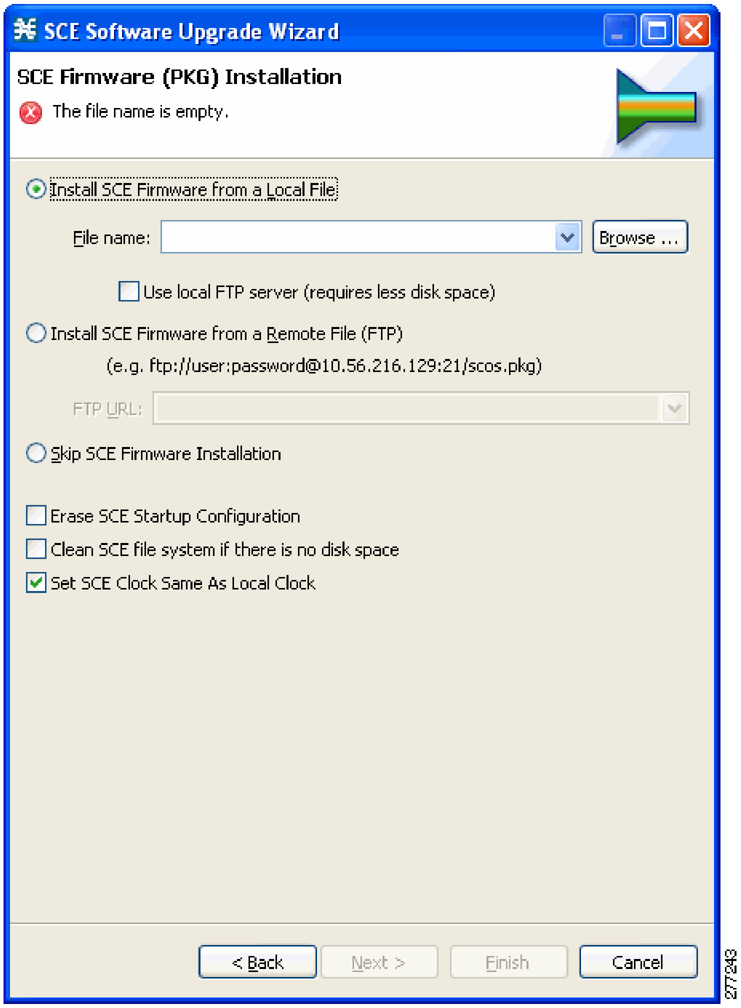
The wizard tests to see that the connections to the defined devices can be made.

Note If a connection to one or more of the devices cannot be made or if there is some problem with the connection (such as invalid version of the device) an error is displayed next to the device. You can skip these tests by clicking **Skip connectivity test**. The connections are validated when you click **Finish** at the end of the wizard.

Step 10 Click **Next**.

The SCE Firmware (PKG) Installation page of the SCE Software Upgrade wizard opens (see Figure 4-10).

Figure 4-10 SCE Firmware (PKG) Installation



SCE Software Upgrade Wizard

SCE Firmware (PKG) Installation

The file name is empty.

● Install SCE Firmware from a Local File

File name: Browse ...

□ Use local FTP server (requires less disk space)

○ Install SCE Firmware from a Remote File (FTP)

(e.g. ftp://user:password@10.56.216.129:21/scos.pkg)

FTP URL:

○ Skip SCE Firmware Installation

□ Erase SCE Startup Configuration

□ Clean SCE file system if there is no disk space

☑ Set SCE Clock Same As Local Clock

Choose the SCE Firmware installation file.

Do one of the following:

- To install SCE Firmware from a local file, click **Browse**.

  A Select file dialog box appears.

  Browse to the SCE Firmware installation file that you are installing.

  Check the Use local FTP server check box to reduce the disk space usage.

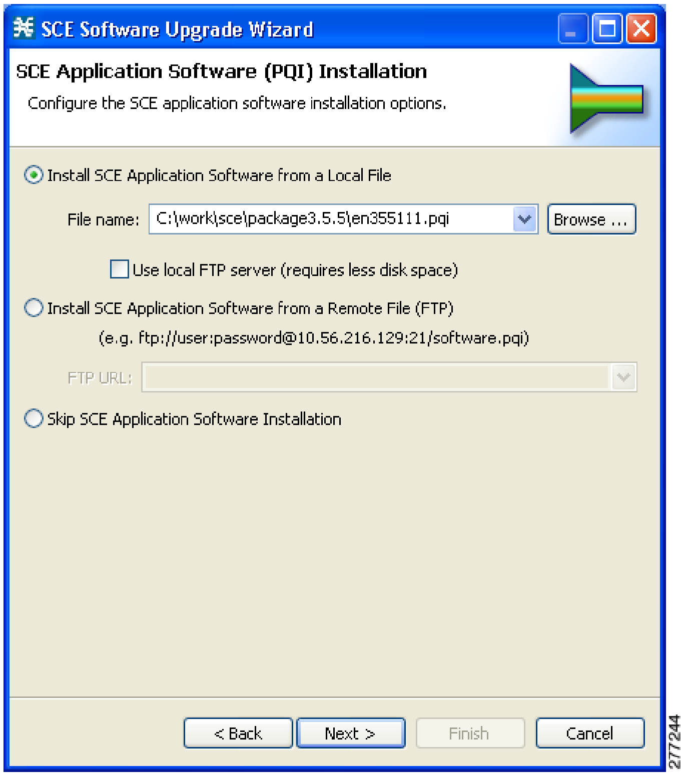
- To download SCE Firmware from a remote site, choose the **Install SCE Firmware from a Remote File (FTP)** radio button and in the FTP URL field, enter the URL.

Step 11 Click the **Skip SCE Firmware Installation** radio button.

Step 12 Click **Next**.

The SCE Application Software (PQI) Installation page of the SCE Software Upgrade wizard opens (see Figure 4-11).

Figure 4-11 SCE Application Software (PQI) Installation



SCE Software Upgrade Wizard

SCE Application Software (PQI) Installation

Configure the SCE application software installation options.

● Install SCE Application Software from a Local File

File name: C:\work\sce\package3.5.5\en355111.pqi

□ Use local FTP server (requires less disk space)

○ Install SCE Application Software from a Remote File (FTP)

(e.g. ftp://user:password@10.56.216.129:21/software.pqi)

FTP URL:

○ Skip SCE Application Software Installation

Step 13 Choose the PQI installation file.

Do one of the following:

- To install the PQI file from a local file, click **Browse**.

  A Select file dialog box appears.

  Browse to the PQI file that you are installing.

  Check the Use local FTP server check box to reduce the disk space usage.

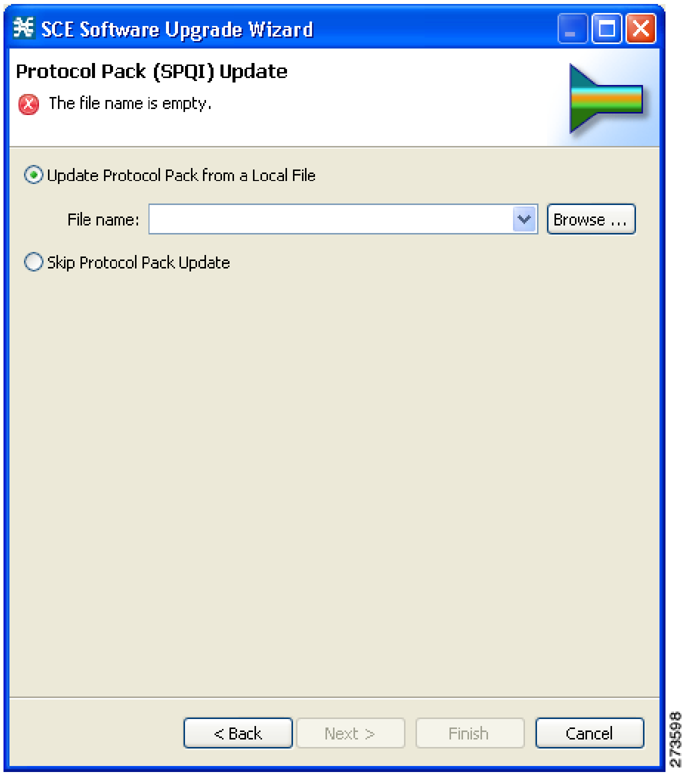
- To download a PQI file from a remote site, choose the **Install SCE Application Software from a Remote File (FTP)** radio button and in the FTP URL field, enter the URL.

  Click the **Skip SCE Software Application Installation** radio button.

Step 14 Click **Next**.

The Protocol Pack (SPQI) Update page of the SCE Software Upgrade wizard opens (see Figure 4-12).

Figure 4-12 Protocol Pack (SPQI) Update



SCE Software Upgrade Wizard

Protocol Pack (SPQI) Update

The file name is empty.

● Update Protocol Pack from a Local File

File name:

○ Skip Protocol Pack Update

Step 15 Update the protocol pack.

Do one of the following:

- To update the SPQI file from a local file, click **Browse**.

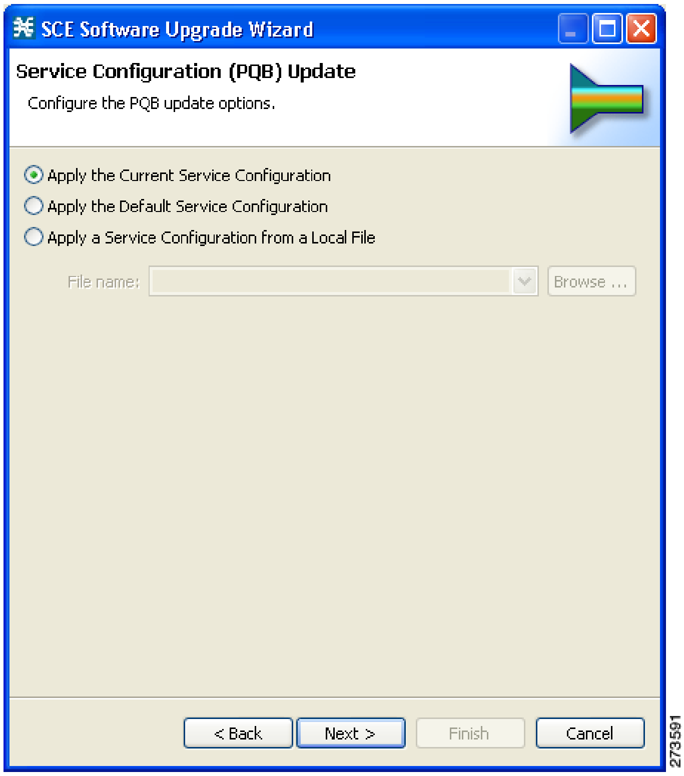
  A Select file dialog box appears.

  Browse to the SPQI file that you are updating.
- Click the **Skip Protocol Pack Update** radio button.

Step 16 Click **Next**.

The Service Configuration (PQB) Update page of the SCE Software Upgrade wizard opens (see Figure 4-13).

Figure 4-13 Service Configuration (PQB) Update



SCE Software Upgrade Wizard

Service Configuration (PQB) Update

Configure the PQB update options.

● Apply the Current Service Configuration
○ Apply the Default Service Configuration
○ Apply a Service Configuration from a Local File

File name:

Step 17 Choose one of the PQB update options.

- **Apply the Current Service Configuration**—Keep the existing service configuration.
- **Apply the Default Service Configuration**—Apply the default service configuration delivered with the product.
- **Apply the Service Configuration from a Local File**—Apply a service configuration from a local file.

Step 18 If you selected the Apply the Service Configuration from a Local File radio button, click **Browse**.

A Select file dialog box appears.

Browse to the file containing the service configuration.

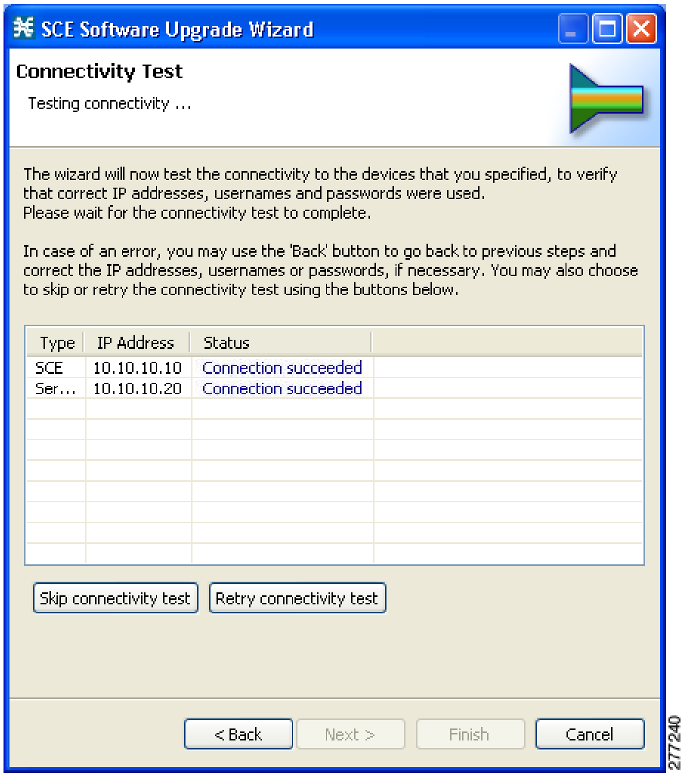
Step 19 Click **Next**.

The Connectivity Test window of the SCE Software Upgrade wizard opens (see Figure 4-14).

The connectivity test verifies the connections to the defined devices.

Note If a connection to one or more of the devices cannot be made or if there is some problem with the connection (such as invalid version of the device), an error is displayed next to the device. You can skip these tests by clicking **Skip connectivity test**. The connections are validated when you click **Finish** at the end of the wizard.

Figure 4-14 Connectivity Test



SCE Software Upgrade Wizard

Connectivity Test

Testing connectivity ...

The wizard will now test the connectivity to the devices that you specified, to verify that correct IP addresses, usernames and passwords were used.
Please wait for the connectivity test to complete.

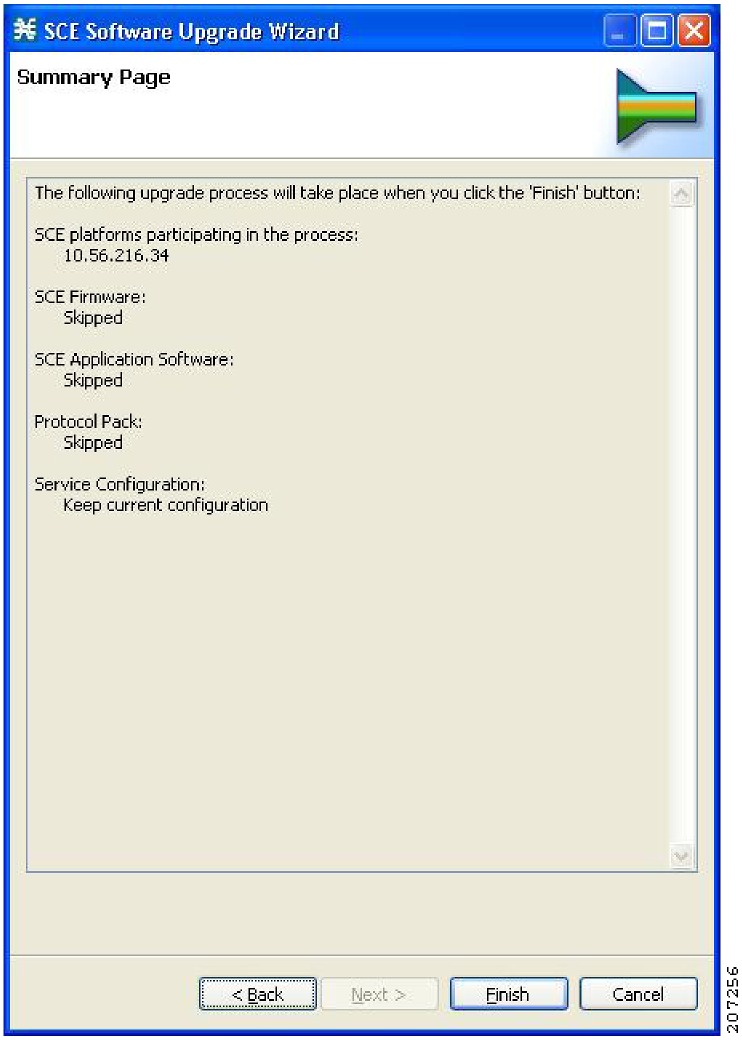
In case of an error, you may use the 'Back' button to go back to previous steps and correct the IP addresses, usernames or passwords, if necessary. You may also choose to skip or retry the connectivity test using the buttons below.

Type	IP Address	Status
SCE	10.10.10.10	Connection succeeded
Ser...	10.10.10.20	Connection succeeded

Step 20 Click **Next**.

The Confirmation page of the SCE Software Upgrade wizard opens (see Figure 4-15).

Figure 4-15 Summary Page



The following upgrade process will take place when you click the 'Finish' button:

SCE platforms participating in the process:
10.56.216.34

SCE Firmware:
Skipped

SCE Application Software:
Skipped

Protocol Pack:
Skipped

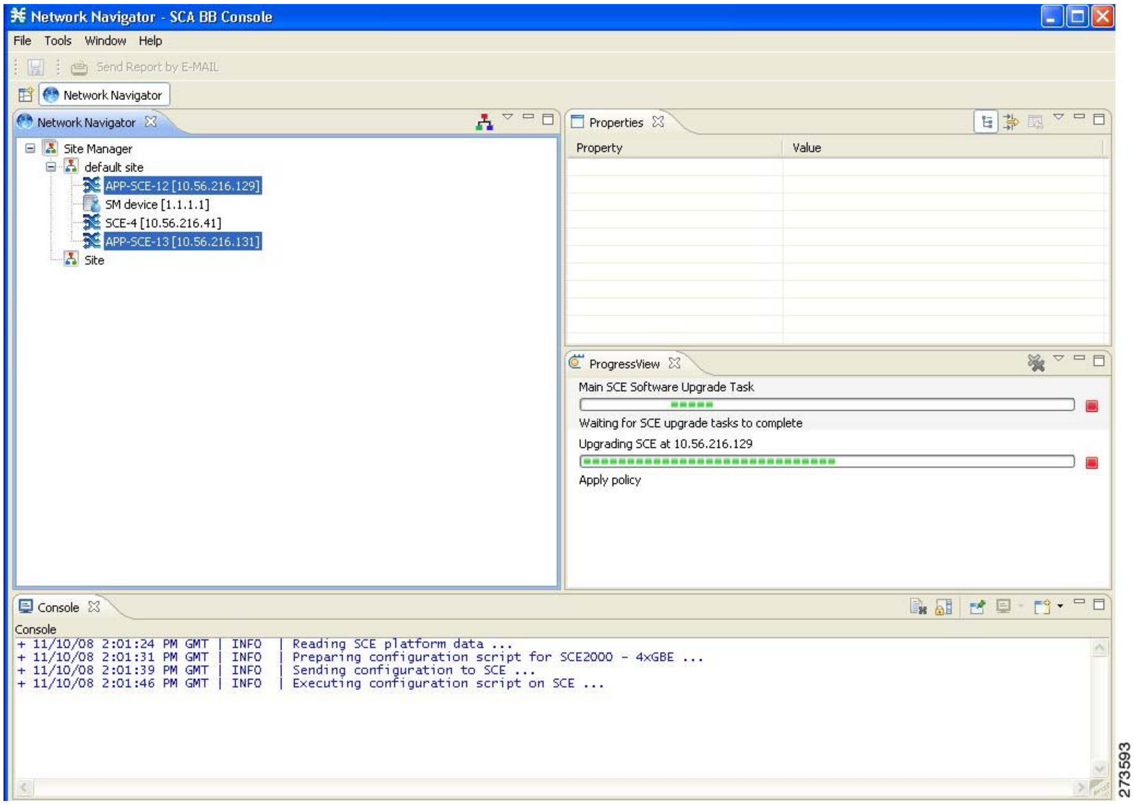
Service Configuration:
Keep current configuration

The actions that the wizard is about to take are listed on the page.

Step 21 Click **Finish**.

You can view the progress in the Progress view (see Figure 4-16).

Figure 4-16 Progress



Main SCE Software Upgrade Task

Waiting for SCE upgrade tasks to complete

Upgrading SCE at 10.56.216.129

Apply policy

```
+ 11/10/08 2:01:24 PM GMT | INFO  | Reading SCE platform data ...
+ 11/10/08 2:01:31 PM GMT | INFO  | Preparing configuration script for SCE2000 - 4xGBE ...
+ 11/10/08 2:01:39 PM GMT | INFO  | Sending configuration to SCE ...
+ 11/10/08 2:01:46 PM GMT | INFO  | Executing configuration script on SCE ...
```

Working with Protocol Packs

Cisco SCA BB uses stateful Layer 7 capabilities for classification of traffic flows.

When the system handles a traffic flow, the flow is assigned a signature ID according to the set of Layer 3 to Layer 7 parameters (the signature) characterizing this flow. Typically, these signatures come embedded in Cisco SCA BB.

To enable rapid response to the ever-changing protocol environment, Cisco SCA BB was enhanced to allow signatures to be updated dynamically. You can load a protocol support plug-in onto an operational system, enhancing the protocol support of the system without compromising the stability of the system (no update of an existing software component is required) and without any service downtime.

- Protocol Packs, page 4-20
- Installing Protocol Packs, page 4-21
- Installing the Service Hierarchy Tree, page 4-21
- How to Verify Version Compatibility for Protocol Packs, page 4-28
- How to Verify the Installation of a Protocol Pack, page 4-28
- Hitless Upgrade of the SLI, page 4-30

Protocol Packs

Periodically, Cisco publishes protocol packs containing new and improved protocol signatures for Cisco SCA BB. A typical protocol pack is a file containing signatures for detecting network worms, popular peer-to-peer applications, and other relevant protocols. When loaded into SCE platforms, these signatures improve Cisco SCA BB classification abilities.

Note You can install a protocol pack on an SCE platform only if a PQI is already installed on the platform.

A protocol pack for Cisco SCA BB may be either a DSS file or an SPQI file:

- Loading a DSS file to the SCE platform requires no downtime of Cisco SCA BB or the platform.
- Loading an SPQI file to the SCE platform entails updating the SCE application:
  - If hitless upgrade (see Hitless Upgrade of the SLI, page 4-30) is enabled, there is no downtime of the SCE platform when loading the SPQI file.
  - If hitless upgrade is *not* enabled, loading an SPQI file requires a short downtime (up to one minute) of the SCE platform. During that time, network traffic bypasses the platform and is neither controlled nor reported.

Note If hitless upgrade is disabled, SPQI installation can cause the loss of the following subscriber data from all subscribers: package ID, real-time monitoring flag, and quota settings. Subscribers are assigned default values for these properties.

Installing Protocol Packs

You install a protocol pack on an SCE platform using one of the following:

- The Cisco SCA BB Service Configuration Utility, page 14-2
- The Network Navigator tool (see How to Install a Protocol Pack, page 5-20)

Note If the protocol pack is an SPQI file you can enable and configure the hitless upgrade option using Hitless Upgrade CLI commands. (See Hitless Upgrade of the SLI, page 4-30.)

The tool or utility performs the following steps:

1. Retrieves the current service configuration from the SCE platform and (optionally) stores a backup copy in a folder that you specify.
2. Imports the signatures that are in the DSS or SPQI file into the service configuration. This action overwrites any DSS that was previously imported into the service configuration.
3. For each new signature that includes a Buddy Protocol attribute (an attribute that points to an existing protocol) (see The Buddy Protocol, page 13-4)—Adds the new signature to all services that include the buddy protocol.
4. If the protocol pack is an SPQI file—Replaces the SCE application. This action causes a short (up to one minute) downtime in SCE platform service.
5. Applies the new service configuration to the SCE platform.

If the protocol pack is an SPQI file and the hitless upgrade option is enabled, you can monitor the progress of the upgrade using Hitless Upgrade CLI Commands, page 4-31.

Note Cisco SCE does not support direct downgrade of higher PP versions to a lower PP version. While downgrading the protcol pack from a higher version to a lower version, the Cisco SCA BB console displays an error message and prevents you from applying the policy on the Cisco SCE. To downgrade from a higher PP version to a lower PP version, see the "Downgrading Protocol Packs" section on page 4-29.

Installing the Service Hierarchy Tree

Opening a PQB using the Client (GUI) exposes its service hierarchy tree (signatures, flavors, protocols, and so on). The client defines the Service Configuration Hierarchy.

When loading a PQB file from the SCE, the PQB Hierarchy Tree must be of the same version as the one in the client. In other words, the PQB must be the same version as the Client, otherwise the PQB doe not open.

Because the client can be connected with different SCE with different versions, and each PQB can have different Service Hierarchy Tree definition, you must install the relevant Service Hierarchy Tree in the Client (GUI) before opening a PQB.

The client can install the service hierarchy tree according to the SCE version. The GUI installation comes with a fixed set of service hierarchy elements which are placed in a specific version-related jar file. You can select between different jar files related to different versions.

Note The SCE service hierarchy tree is different than the client version. When installing a service hierarchy tree for a SCE:

- Always back up user PQB before upgrade to PPXY and keep a copy since the PQB is changed.
- Remove/Reinstall Service Tree Protocol.

To view, install, and remove the service hierarchy tree use the following procedures:

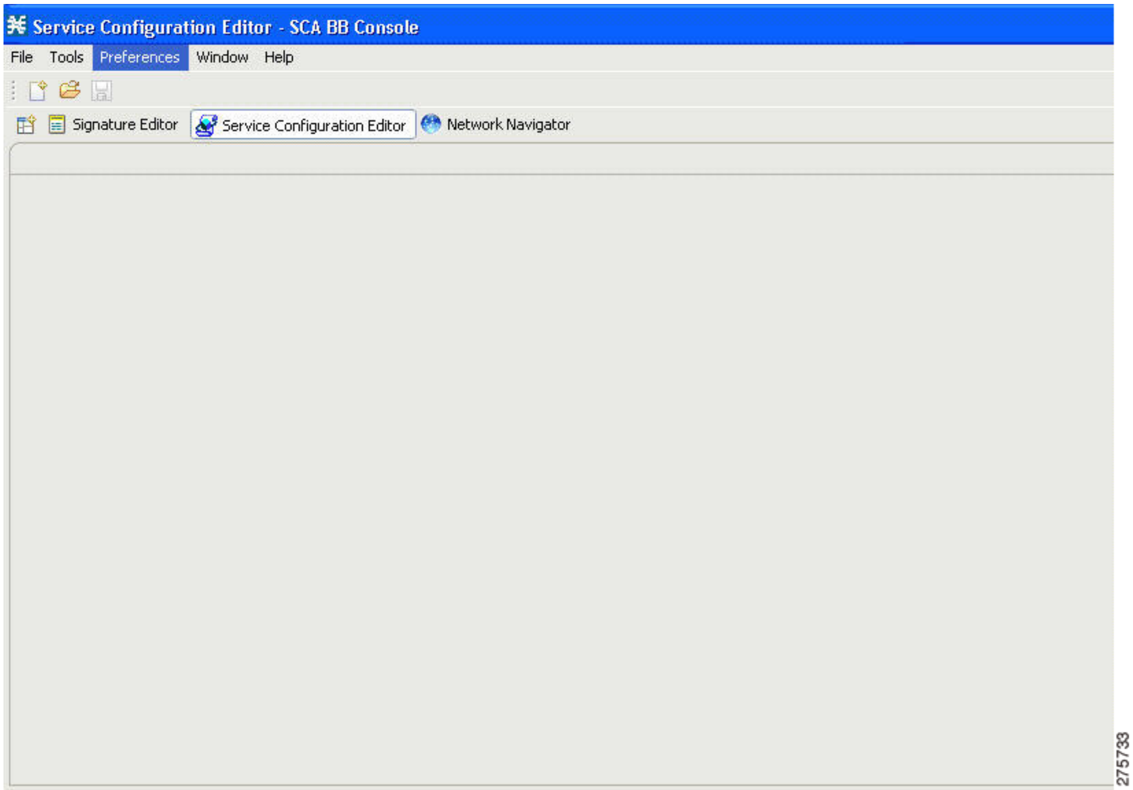
- View and Install Service Hierarchy Tree, page 4-23
- Remove Service Hierarchy Tree, page 4-27

View and Install Service Hierarchy Tree

Step 1 To view the service hierarchy tree, open the Protocol Pack tab.

Step 2 From the toolbar, select Service Configuration Editor (see Figure 4-17).

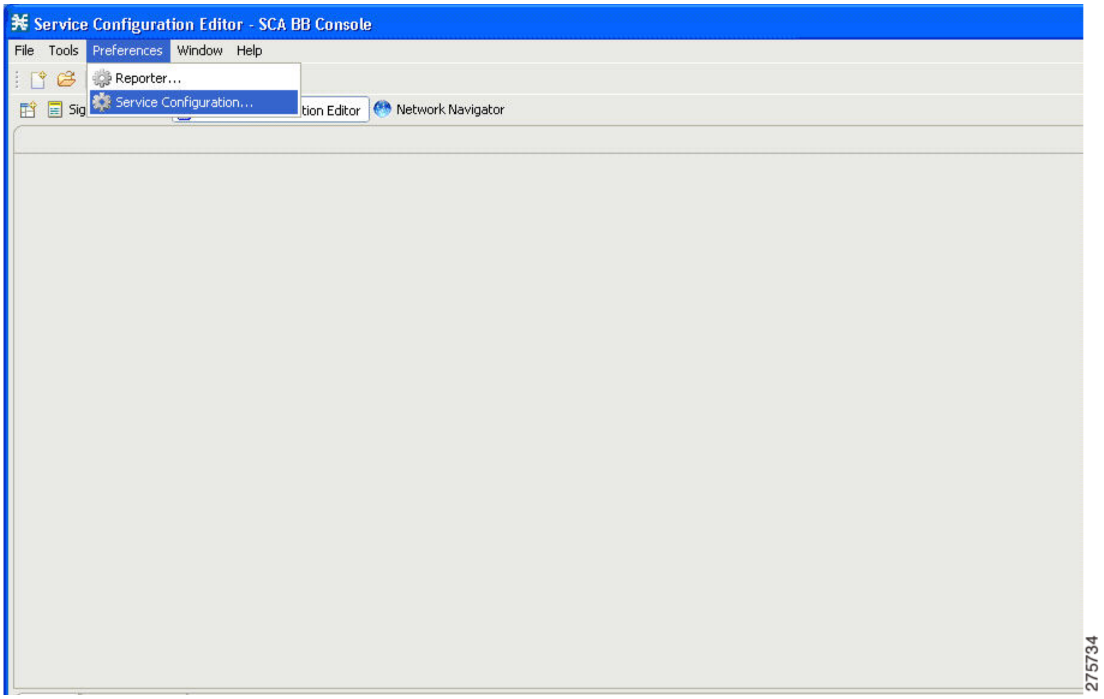
Figure 4-17 Service Configuration Editor - Preferences


Service Configuration Editor - SCA BB Console
File
Tools
Preferences
Window
Help
Signature Editor
Service Configuration Editor
Network Navigator
275733

Step 3 Select Preferences and then select Service Configuration.

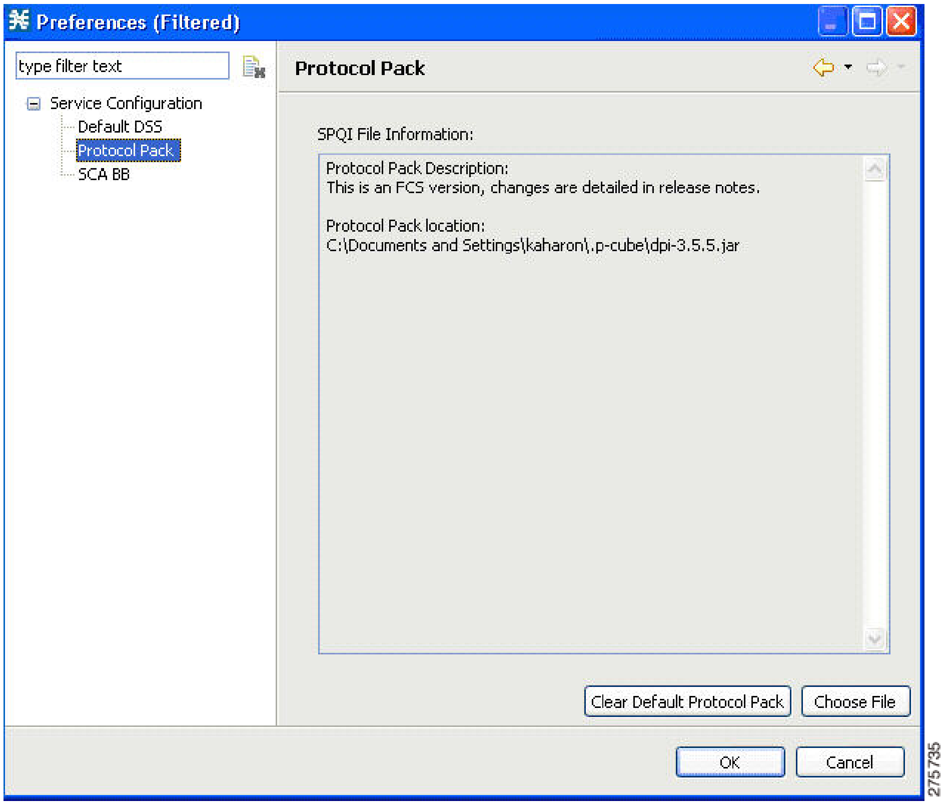
A Preferences window opens (see Figure 4-18).

Figure 4-18 Service Configuration Editor - Service Configuration



Step 4 Select Protocol Pack from the Service Configuration tree (see Figure 4-19). The upper window provides information related to service hierarchy tree related to the GUI.

Figure 4-19 Preferences (Filtered)



Preferences (Filtered)

type filter text

- Service Configuration
  - Default DSS
  - Protocol Pack
  - SCA BB

Protocol Pack

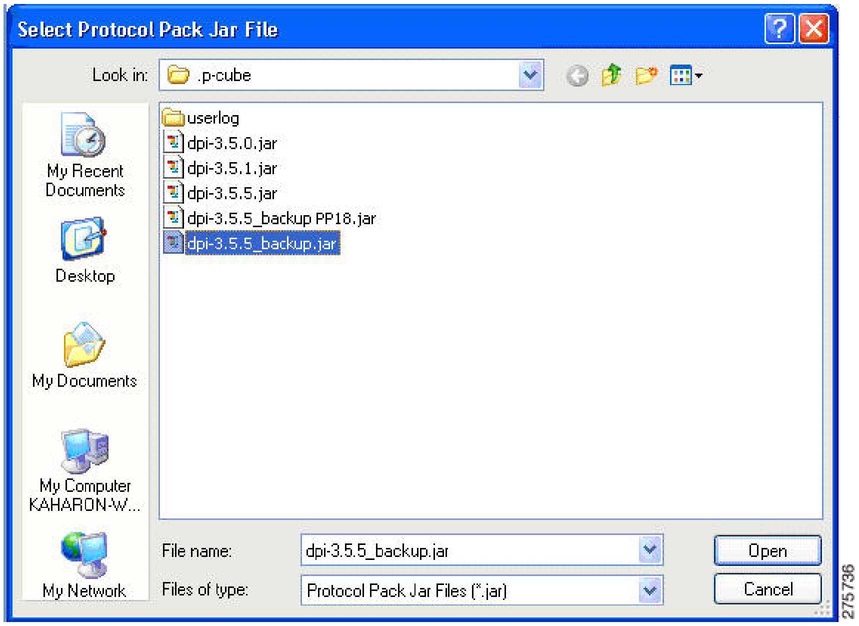
SPQI File Information:

Protocol Pack Description:
This is an FCS version, changes are detailed in release notes.

Protocol Pack location:
C:\Documents and Settings\kaharon\.p-cube\dpi-3.5.5.jar

Step 5 To install a new service hierarchy tree, click the **Choose File** button and select either a jar file or an SPQI file (see Figure 4-20).

Figure 4-20 Select Protocol Pack



Select Protocol Pack Jar File

Look in: .p-cube

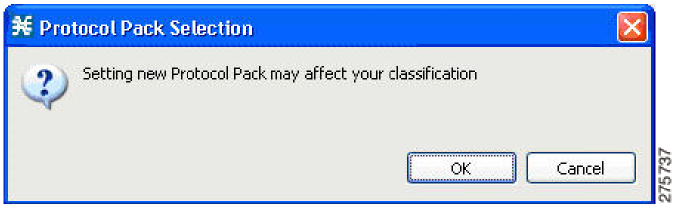
userlog
dpi-3.5.0.jar
dpi-3.5.1.jar
dpi-3.5.5.jar
dpi-3.5.5_backup PP18.jar
dpi-3.5.5_backup.jar

File name: dpi-3.5.5_backup.jar

Files of type: Protocol Pack Jar Files (*.jar)

Step 6 Click Open, and approve the warning message (see Figure 4-21) by clicking **OK**.

Figure 4-21 Protocol Pack Selection Warning Message

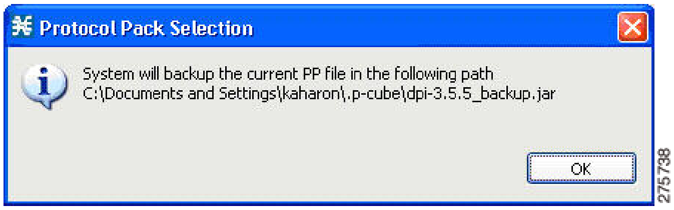


Protocol Pack Selection

Setting new Protocol Pack may affect your classification

Step 7 To back up the current protocol pack and install the new service hierarchy tree, approve the backup message (see Figure 4-22) by clicking OK.

Figure 4-22 Protocol Pack Selection Backup Message



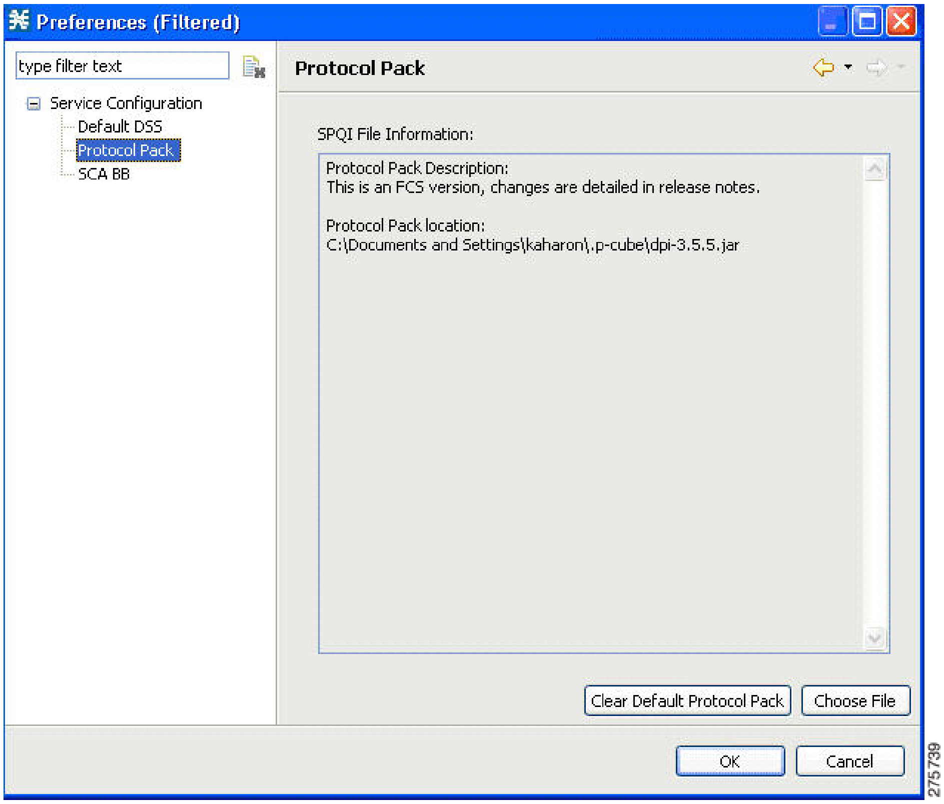
Protocol Pack Selection

System will backup the current PP file in the following path
C:\Documents and Settings\kaharon\.p-cube\dpi-3.5.5_backup.jar

Remove Service Hierarchy Tree

Step 1 To remove the service hierarchy tree and to return to the default configuration, click the Clear Default Protocol Pack button in the Preferences window (see Figure 4-23).

Figure 4-23 Preferences (Filtered)



Preferences (Filtered)

type filter text

Service Configuration
- Default DSS
- Protocol Pack
- SCA BB

Protocol Pack

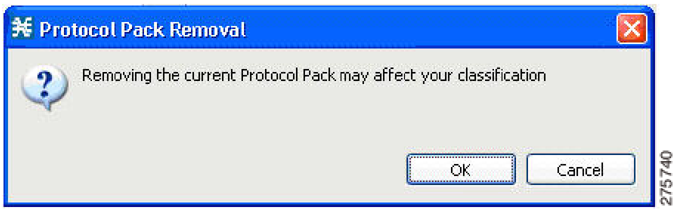
SPQI File Information:

Protocol Pack Description:
This is an FCS version, changes are detailed in release notes.

Protocol Pack location:
C:\Documents and Settings\kaharon\.p-cube\dpi-3.5.5.jar

Step 2 Accept the operation by clicking **OK** on the Protocol Pack Removal message screen (see Figure 4-24).

Figure 4-24 Protocol Pack Removal Message



Protocol Pack Removal

Removing the current Protocol Pack may affect your classification

The service hierarchy tree is removed from the system, and when a new PQB is opened, the client installs the default service classifications.

How to Verify Version Compatibility for Protocol Packs

A protocol pack is compatible only with specific versions of the SCE application. When working with protocol packs, verify that the protocol pack version matches the SCE application version. For example, only use a protocol pack for 3.7.0 on SCE application version 3.7.0.

The version compatibility information for each protocol pack is included in the release notes of the protocol pack.

Step 1 Verify that the correct version of **servconf** is installed and running correctly.

- From the command prompt, type `servconf --version`.
- Press **Enter**.

The version of the utility should match that of the protocol pack.

Step 2 Verify that the correct version of the SCE application is installed.

- At the SCE platform CLI prompt `(SCE#)`, type `show version`.
- Press **Enter**.

The application version should match that of the protocol pack.

Step 3 Verify that a service configuration (PQB) is applied to the SCE platform.

- In the Console, retrieve and view the current PQB.

How to Verify the Installation of a Protocol Pack

Step 1 At the SCE platform CLI prompt `(SCE#)`, type **show version**.

Step 2 Press **Enter**.

The response shows the version of the OS running on the SCE platform. This response includes information about the installed protocol pack version.

Step 3 Retrieve the PQB from the SCE platform and view it using the Console.

Step 4 Verify that the new protocols from the protocol pack were added to the service configuration.

The problems that may cause the installation of a protocol pack to fail and their remedies include:

- Missing or incorrect version of the JRE—Install the correct version of the JRE (see Installing the Java Runtime Environment, page 4-4).
- Incorrect or missing SCE application version on the SCE platform—Verify that the correct version of the SCE application is installed (see How to Verify Version Compatibility for Protocol Packs, page 4-28).
- No service configuration (PQB) is applied to the SCE platform—Create a new PQB and apply it using the Console.
- **servconf** failed to import the new signatures into the PQB—Use the `--force-signature` update signature option when running **servconf** (see servconf Syntax, page 14-2).

When reporting problems to Cisco, please include the **servconf** log file, located at <user.home>\.p-cube\servconf.log. With Windows, this usually maps to C:\Documents and Settings\<username>\.p-cube\servconf.log or C:\Users\<username>\.p-cube\servconf.log.

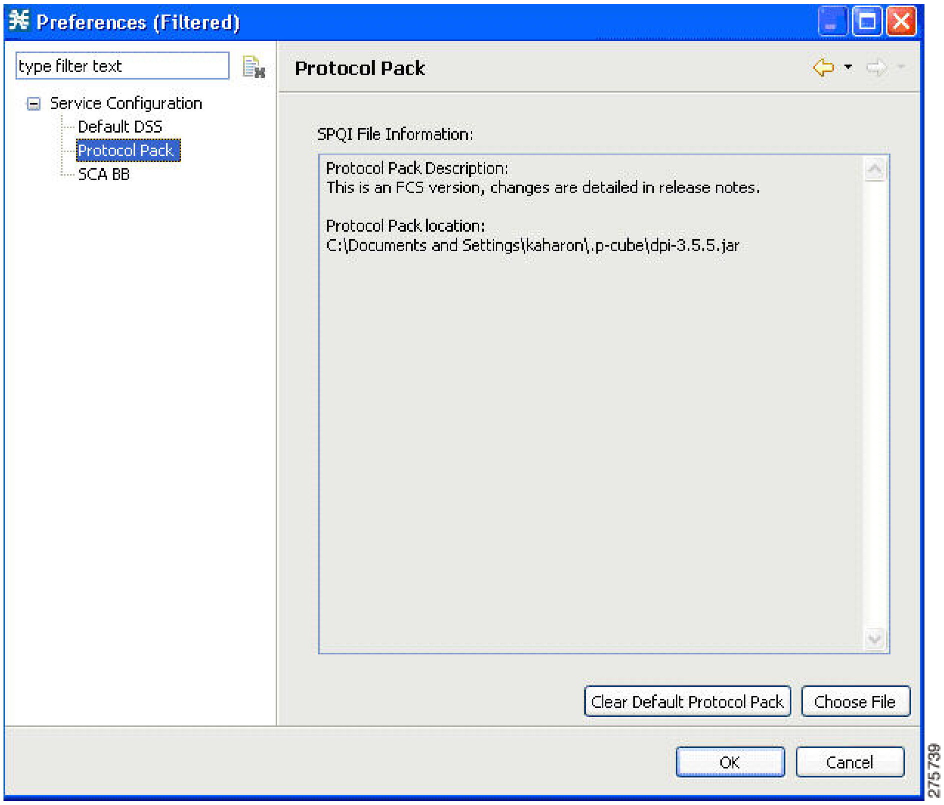
Downgrading Protocol Packs

To downgrade from a higher protocol pack version to a lower protocol pack version, perform these steps:

Note When you apply a PQB file on a Cisco SCE using the Cisco SCA BB console, ensure that the version of the PQB file created is less than or equal to the Cisco SCOS and the protocol pack versions installed on the Cisco SCE.

Step 1 Click the **Clear Default Protocol Pack** button in the **Preferences** window (see Figure 4-25).

Figure 4-25 Preferences (Filtered)



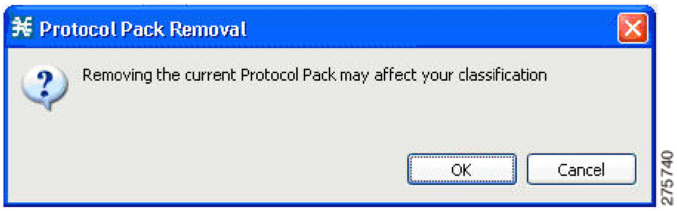
SPQI File Information:

Protocol Pack Description:
This is an FCS version, changes are detailed in release notes.

Protocol Pack location:
C:\Documents and Settings\kaharon\.p-cube\dpi-3.5.5.jar

Step 2 Accept the operation by clicking **OK** on the Protocol Pack Removal message screen (see Figure 4-26).

Figure 4-26 Protocol Pack Removal Message


Protocol Pack Removal

Removing the current Protocol Pack may affect your classification

Step 3 Close and reopen the Cisco Service Control Application for Broadband and apply the default service classifications.

Hitless Upgrade of the SLI

Hitless upgrade is the Cisco SCA BB method of upgrading the software components that reside on the SCE platform without incurring any service downtime.

- Hitless upgrade of Protocol Packs is available on SCE 8000.
- Hitless upgrade is available on SCE 2000 and SCE 1000_2U platforms.
- Hitless upgrade is not available on SCE 1000_1.5U platforms.

To know whether the Cisco SCE 2000 supports hitless upgrade for a particular PP release, see the *Cisco Service Control Application for Broadband Protocol Pack Notes*.

If hitless upgrade is enabled, classification, reporting, and control continue uninterrupted when you install an SPQI file (see Working with Protocol Packs, page 4-20). You can install SPQI files using either the Console or **servconf,** the Cisco SCA BB Service Configuration Utility. An SPQI file is a package that includes the required (SLI) files.

Note When you apply a new policy or during Protocol Pack upgrade, there is a delay of 30 seconds before the rules are applied to the new flows.

After the new application is loaded on the SCE platform:

- The new application services all new flows and bundles.
- The old application continues to service existing flows (and new flows that belong to bundles of existing flows).
- Both applications share available memory.

Until all old flows die or are killed, the hitless upgrade is considered to be in progress. To make the hitless upgrade process bounded, you can set criteria that triggers the explicit killing of all flows still executing on the old application. Two such criteria exist:

- When a specified amount of time has passed since the process started.
- When the number of old flows goes below a specified threshold.

The default value for the first criterion is 60 (minutes); the default value for the second is zero (flows). This means that the replace operation is guaranteed to complete after no more than one hour (sooner, if all old flows die naturally). But the application does not kill any old flow before one hour completes.

These criteria are configurable by CLI commands.

You can initiate the explicit killing of all old flows using a manual command.

Hitless Upgrade CLI Commands

You can configure, monitor, and control hitless upgrade using the SCE platform Command-Line Interface (CLI). For more information about the SCE platform CLI, see *Cisco SCE 8000 CLI Command Reference.*

The commands listed here are explained in the following section.

Use the following CLI commands to configure the criteria for completing a hitless upgrade:

```
replace completion time <minutes>
no replace completion time
default replace completion time
replace completion num-flows <num>
no replace completion num-flows
default replace completion num-flows
```

These commands are line interface configuration commands. To run these commands you must enter line interface configuration mode and see the `SCE(config if)#` prompt displayed. For details on interface configuration mode, see How to Enter Line Interface Configuration Mode, page 4-32.

The following two CLI commands are EXEC mode commands.

Use the following CLI command to monitor the progress of a hitless upgrade:

```
show applications slot <num> replace
```

Use the following CLI command to force immediate completion of a hitless upgrade:

```
application slot <num> replace force completion
```

Description of Hitless Upgrade CLI Commands

Table 4-1 describes the hitless upgrade CLI commands listed in the previous section.

Table 4-1 Hitless Upgrade CLI Commands

Command	Description
replace completion time <*minutes*>	Sets the time criterion for killing all old flows and completing the hitless upgrade. Specifying a value of zero disables this criterion—the hitless upgrade is completed only when the number-of-flows criterion is met.
no replace completion time	Sets the time criterion for completing the hitless upgrade to zero.
default replace completion time	Resets the time criterion for completing the replace operation to the default value of 60.
replace completion num-flows <*num*>	Sets the number-of-flows criterion for completing the hitless upgrade operation. When the number of old flows drops below the number specified by this criterion, the remaining flows are killed and the hitless upgrade is complete.

Table 4-1 Hitless Upgrade CLI Commands (continued)

Command	Description
no replace completion num-flows	Sets the number-of-flows criterion for completing the hitless upgrade to zero.
default replace completion num-flows	Resets the number-of-flows criterion for completing the hitless upgrade to the default value of zero.
show applications slot <*num*> **replace**	Shows the current hitless upgrade state: • Current replace stage • Current completion criteria • Current completion status (elapsed time and number of flows on each traffic processor) • Whether this task is an upgrade or a downgrade • Values for spare memory
application slot <*num*> **replace force completion**	Forces the current hitless upgrade process to complete (killing all old flows).

How to Enter Line Interface Configuration Mode

To run line interface configuration commands, enter the line interface configuration mode and see the `SCE(config if)#` prompt displayed.

Step 1 At the SCE platform CLI prompt `(SCE#,` type **configure**.

Step 2 Press **Enter**.

The `SCE(config)#` prompt appears.

Step 3 Type **interface LineCard 0**.

Step 4 Press **Enter**.

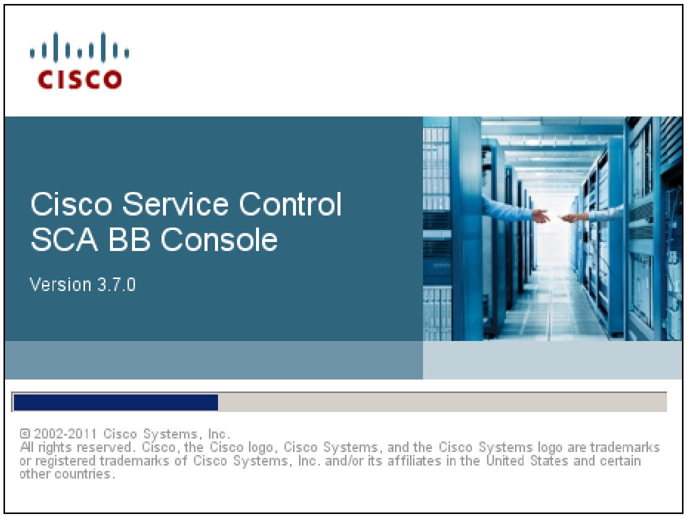
The `SCE(config if)#` prompt appears.

How to Launch the Console

Step 1 Choose **Start > All Programs > Cisco SCA > SCA BB Console 3.7.0 > SCA BB Console 3.7.0**.

The Cisco SCA BB Console splash screen appears (see Figure 4-27).

Figure 4-27 Cisco SCA BB Console



Cisco Service Control
SCA BB Console

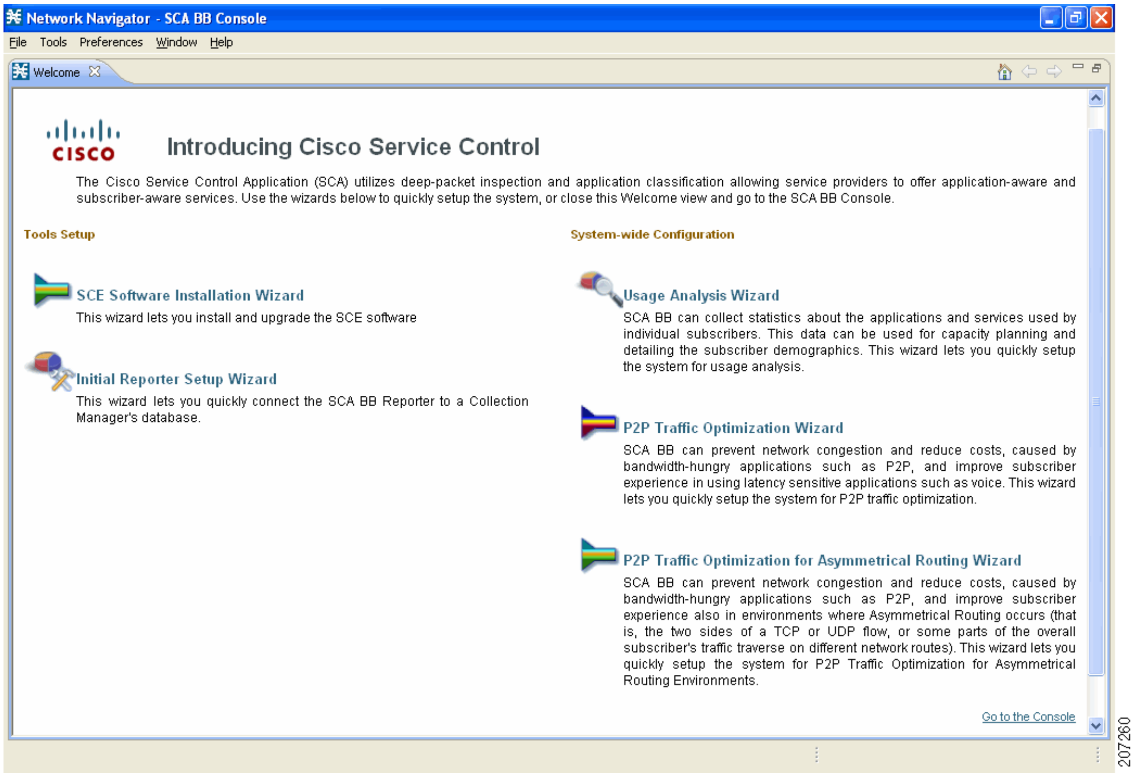
Version 3.7.0

© 2002-2011 Cisco Systems, Inc.
All rights reserved. Cisco, the Cisco logo, Cisco Systems, and the Cisco Systems logo are trademarks or registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

After the Console has loaded, the main window of the Console appears.

The first time that you launch the Console, the Welcome view is open in the main window (see Figure 4-28).

Figure 4-28 Welcome - Introducing Cisco Service Control



Introducing Cisco Service Control

The Cisco Service Control Application (SCA) utilizes deep-packet inspection and application classification allowing service providers to offer application-aware and subscriber-aware services. Use the wizards below to quickly setup the system, or close this Welcome view and go to the SCA BB Console.

Tools Setup

SCE Software Installation Wizard

This wizard lets you install and upgrade the SCE software

Initial Reporter Setup Wizard

This wizard lets you quickly connect the SCA BB Reporter to a Collection Manager's database.

System-wide Configuration

Usage Analysis Wizard

SCA BB can collect statistics about the applications and services used by individual subscribers. This data can be used for capacity planning and detailing the subscriber demographics. This wizard lets you quickly setup the system for usage analysis.

P2P Traffic Optimization Wizard

SCA BB can prevent network congestion and reduce costs, caused by bandwidth-hungry applications such as P2P, and improve subscriber experience in using latency sensitive applications such as voice. This wizard lets you quickly setup the system for P2P traffic optimization.

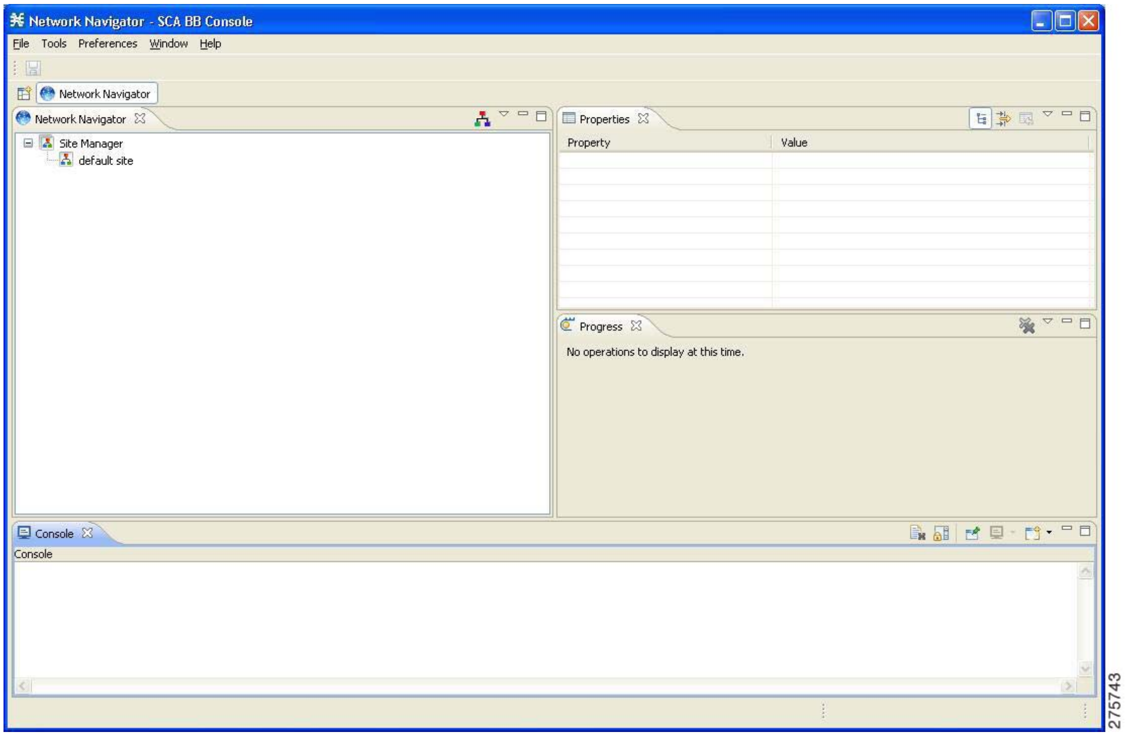
P2P Traffic Optimization for Asymmetrical Routing Wizard

SCA BB can prevent network congestion and reduce costs, caused by bandwidth-hungry applications such as P2P, and improve subscriber experience also in environments where Asymmetrical Routing occurs (that is, the two sides of a TCP or UDP flow, or some parts of the overall subscriber's traffic traverse on different network routes). This wizard lets you quickly setup the system for P2P Traffic Optimization for Asymmetrical Routing Environments.

Step 2 Close the Welcome view and click **Go to the console**.

The Welcome view closes. The Network Navigator tool is open in the Console (see Figure 4-29).

Figure 4-29 Network Navigator



Note When you close the Console, it remembers which tools are open, which is the active tool, and whether the Welcome view is displayed. The Console then applies this view the next time you launch the Console.

How to Use the Console

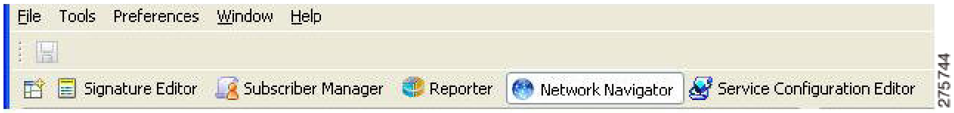
The Console is the front end of Cisco SCA BB. You use it to configure the services that the SP offers to you.

The Console consists of the following tools:

- Network Navigator tool
- Service Configuration Editor tool
- Signature Editor tool
- Subscriber Manager GUI tool
- Anonymous Groups Manager GUI tool
- Reporter tool

The Console GUI has a menu bar and a standard toolbar (see Figure 4-30). Underneath the toolbar is another bar that displays the button of any open Console tool. When you launch a tool, a button is added to this bar. To switch between open tools, click the appropriate button on the bar.

Figure 4-30 Menu Bar and Toolbar of the Console GUI



Note: The title of the Console window shows the active tool and the active service configuration.

The Welcome View of the Console links to a number of Configuration Wizards that can configure the initial, basic configuration of your system.

- Configuration Wizards, page 4-37
- The Network Navigator Tool, page 4-72
- The Service Configuration Editor Tool, page 4-73
- The Signature Editor Tool, page 4-75
- The Subscriber Manager GUI Tool, page 4-76
- The Anonymous Group Manager Tool, page 4-77
- The Reporter Tool, page 4-78
- Online Help, page 4-79

Configuration Wizards

The configuration wizards available from the Welcome view are (three of these wizards can also be executed from the Network Navigator tool):

- Usage Analysis wizard—Creates a simple model of devices and connects to them.
- The P2P Traffic Optimization wizards:
  - P2P Traffic Optimization wizard—Creates a simple model of devices, connects to them, and limits P2P traffic to a specified percentage of total available bandwidth.
  - P2P Traffic Optimization at a Peering Point wizard—Creates a simple model of devices, connects to them, limits P2P traffic to a specified percentage of total available bandwidth, and allows you to enable asymmetric routing classification mode.
- Reporter database Configuration wizard—Connects the Cisco SCA BB Reporter tool to a database.

Asymmetric Routing

Traffic processing depends on the routing environment. The Cisco Service Control solution can operate in two typical routing schemes: symmetric and asymmetric. In asymmetric routing, for a significant number of flows, only one direction (inbound or outbound) is routed through the SCE platform.

Anonymous Subscriber Mode

Anonymous subscriber mode is a mode in which entities defined as IP addresses are treated as subscribers.

How to Use the Usage Analysis Wizard

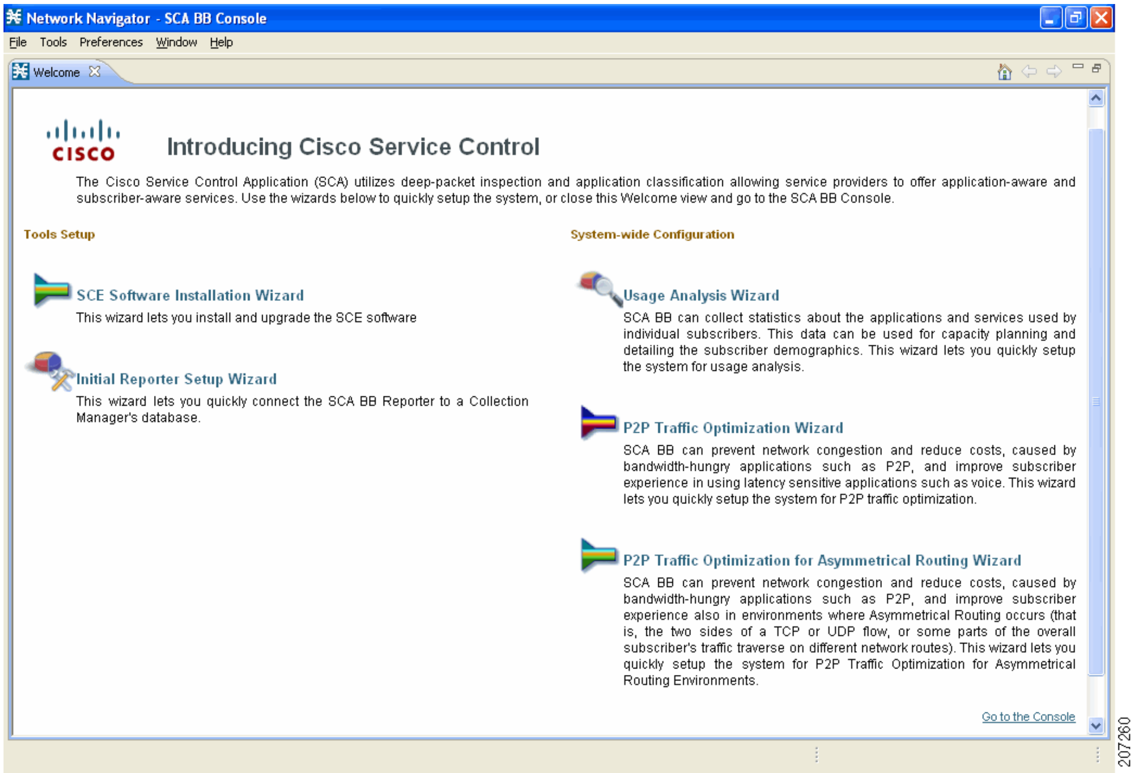
The Usage Analysis wizard allows you to create a simple model of devices and connect to them.

Note If they do not exist, devices defined in the wizard are added to the default site in the Site Manager tree.

Step 1 From the Console main menu, choose **Help > Welcome**.

The Welcome view opens (see Figure 4-31).

Figure 4-31 Welcome - Introducing Cisco Service Control



Introducing Cisco Service Control

The Cisco Service Control Application (SCA) utilizes deep-packet inspection and application classification allowing service providers to offer application-aware and subscriber-aware services. Use the wizards below to quickly setup the system, or close this Welcome view and go to the SCA BB Console.

Tools Setup

SCE Software Installation Wizard

This wizard lets you install and upgrade the SCE software

Initial Reporter Setup Wizard

This wizard lets you quickly connect the SCA BB Reporter to a Collection Manager's database.

System-wide Configuration

Usage Analysis Wizard

SCA BB can collect statistics about the applications and services used by individual subscribers. This data can be used for capacity planning and detailing the subscriber demographics. This wizard lets you quickly setup the system for usage analysis.

P2P Traffic Optimization Wizard

SCA BB can prevent network congestion and reduce costs, caused by bandwidth-hungry applications such as P2P, and improve subscriber experience in using latency sensitive applications such as voice. This wizard lets you quickly setup the system for P2P traffic optimization.

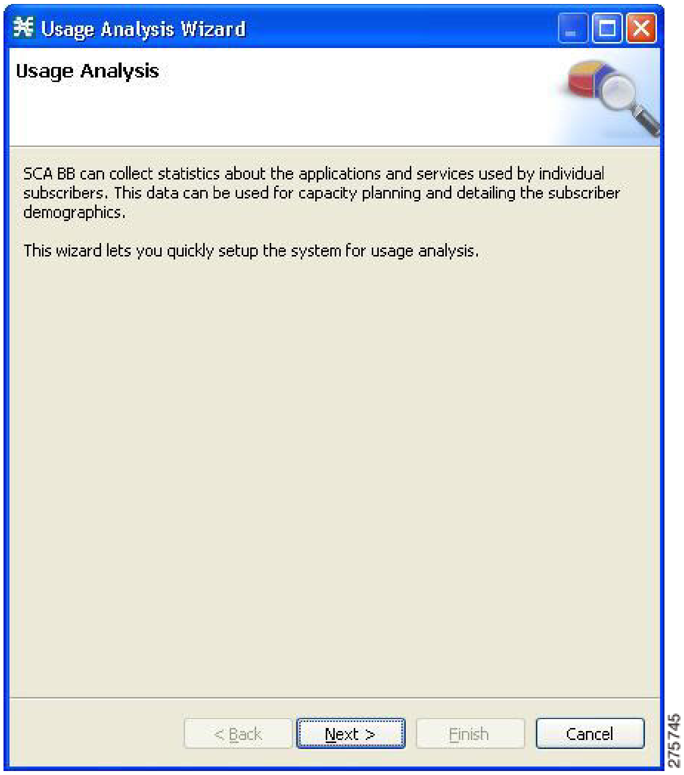
P2P Traffic Optimization for Asymmetrical Routing Wizard

SCA BB can prevent network congestion and reduce costs, caused by bandwidth-hungry applications such as P2P, and improve subscriber experience also in environments where Asymmetrical Routing occurs (that is, the two sides of a TCP or UDP flow, or some parts of the overall subscriber's traffic traverse on different network routes). This wizard lets you quickly setup the system for P2P Traffic Optimization for Asymmetrical Routing Environments.

Step 2 Click **Usage Analysis Wizard**.

The Welcome page of the Usage Analysis wizard appears (see Figure 4-32).

Figure 4-32 Usage Analysis



Usage Analysis

SCA BB can collect statistics about the applications and services used by individual subscribers. This data can be used for capacity planning and detailing the subscriber demographics.

This wizard lets you quickly setup the system for usage analysis.

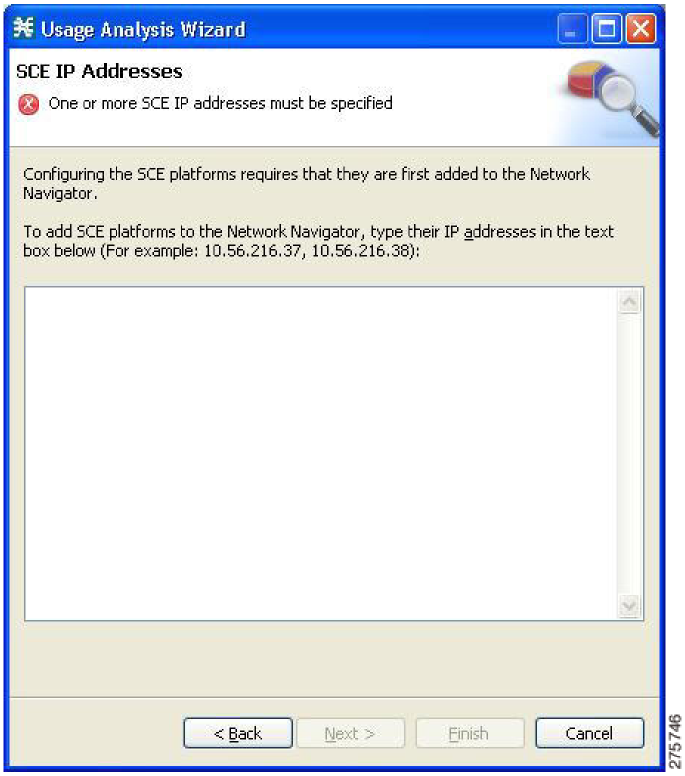
Note You can also execute the Usage Analysis wizard from the Network Navigator tool:

1. Select one or more devices in the Site Manager tree.
2. Right-click one of the selected devices.
3. From the popup menu that appears, select **Configuration Wizards > Usage Analysis Configuration**.
4. You can set only one CM and one Reporter database in the wizard. If you select more than one CM or Reporter database, only one CM and one Reporter database is selected and a warning message is displayed. Click **OK** to continue.

Step 3 Click **Next**.

The SCE IP Addresses page of the Usage Analysis wizard opens (see Figure 4-33).

Figure 4-33 SCE IP Addresses



Usage Analysis Wizard

SCE IP Addresses

One or more SCE IP addresses must be specified

Configuring the SCE platforms requires that they are first added to the Network Navigator.

To add SCE platforms to the Network Navigator, type their IP addresses in the text box below (For example: 10.56.216.37, 10.56.216.38):

Step 4 In the edit box, enter the IP addresses of the SCE devices that should be added to the model.

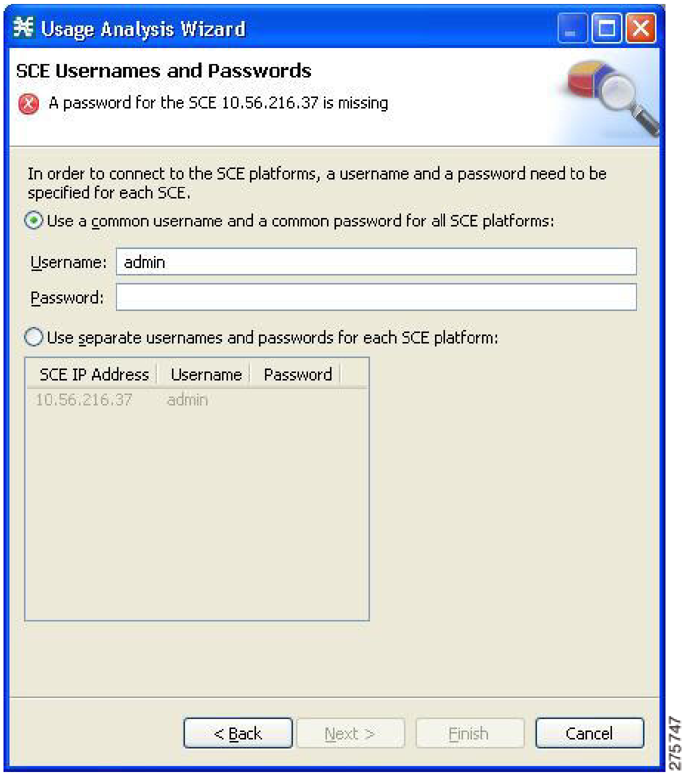
If you started from the Network Navigator, the IP addresses of the SCE devices that you selected are displayed in the edit box. You can add additional addresses.

Note You can work with up to 20 SCE devices at one time using the wizard.

Step 5 Click **Next**.

The SCE Usernames and Passwords page of the Usage Analysis wizard opens (see Figure 4-34).

Figure 4-34 SCE Usernames and Passwords



Usage Analysis Wizard

SCE Usernames and Passwords

A password for the SCE 10.56.216.37 is missing

In order to connect to the SCE platforms, a username and a password need to be specified for each SCE.

● Use a common username and a common password for all SCE platforms:

Username: admin

Password:

○ Use separate usernames and passwords for each SCE platform:

SCE IP Address	Username	Password
10.56.216.37	admin	

Step 6 Enter the usernames and passwords for the SCE devices.

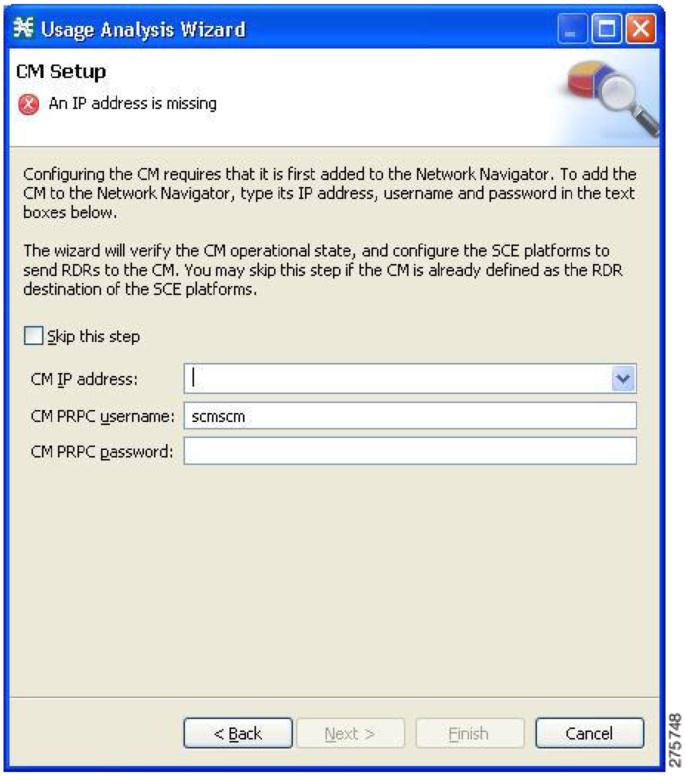
Do one of the following:

- To use the same username and password for all the SCE devices that you are adding, enter the username in the Username field and the password in the Password field.
- To provide a different username and password pair for each SCE device, select the **Use separate usernames and passwords for each SCE platform** radio button, and, for each SCE device, enter the username and password in the appropriate cell of the table.

Step 7 Click **Next**.

The CM Setup page of the Usage Analysis wizard opens (see Figure 4-35).

Figure 4-35 CM Setup



Usage Analysis Wizard

CM Setup

An IP address is missing

Configuring the CM requires that it is first added to the Network Navigator. To add the CM to the Network Navigator, type its IP address, username and password in the text boxes below.

The wizard will verify the CM operational state, and configure the SCE platforms to send RDRs to the CM. You may skip this step if the CM is already defined as the RDR destination of the SCE platforms.

□ Skip this step

CM IP address:

CM PRPC username: scmscm

CM PRPC password:

Step 8 Define the SCSM Collection Manager (CM) to use with this configuration.

Do one of the following:

- Enter the IP address, username, and password of the CM device in the appropriate fields.

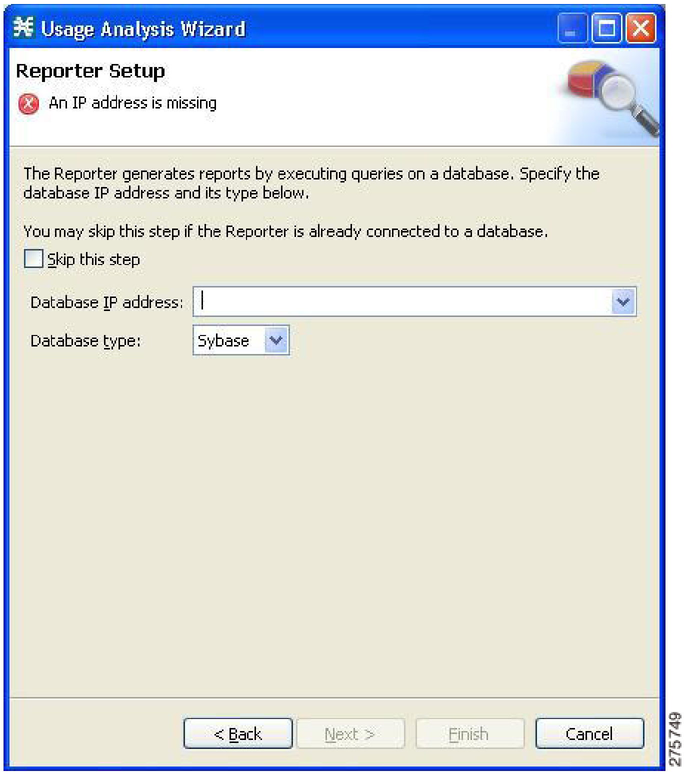
  If you started from the Network Navigator, this information is retrieved and displayed. You can modify these parameters.

- Check the **Skip this step** check box.

Step 9 Click **Next**.

The Reporter Setup page of the Usage Analysis wizard opens (see Figure 4-36).

Figure 4-36 Reporter Setup



Reporter Setup

An IP address is missing

The Reporter generates reports by executing queries on a database. Specify the database IP address and its type below.

You may skip this step if the Reporter is already connected to a database.

□ Skip this step

Database IP address:

Database type: Sybase

Step 10 Define the database to which the Reporter tool should connect.

Do one of the following:

- Enter the IP address of the database and select the database type.

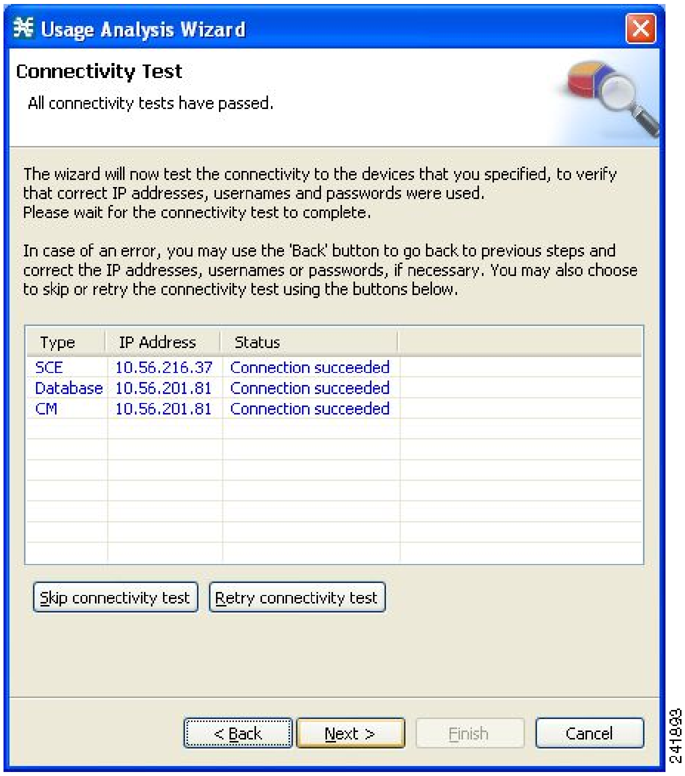
  If you started from the Network Navigator, this information is retrieved and displayed. You can modify these parameters.

- Check the **Skip this step** check box.

Step 11 Click **Next**.

The Connectivity Test page of the Usage Analysis wizard opens (see Figure 4-37).

Figure 4-37 Connectivity Test



Usage Analysis Wizard

Connectivity Test

All connectivity tests have passed.

The wizard will now test the connectivity to the devices that you specified, to verify that correct IP addresses, usernames and passwords were used.
Please wait for the connectivity test to complete.

In case of an error, you may use the 'Back' button to go back to previous steps and correct the IP addresses, usernames or passwords, if necessary. You may also choose to skip or retry the connectivity test using the buttons below.

Type	IP Address	Status
SCE	10.56.216.37	Connection succeeded
Database	10.56.201.81	Connection succeeded
CM	10.56.201.81	Connection succeeded

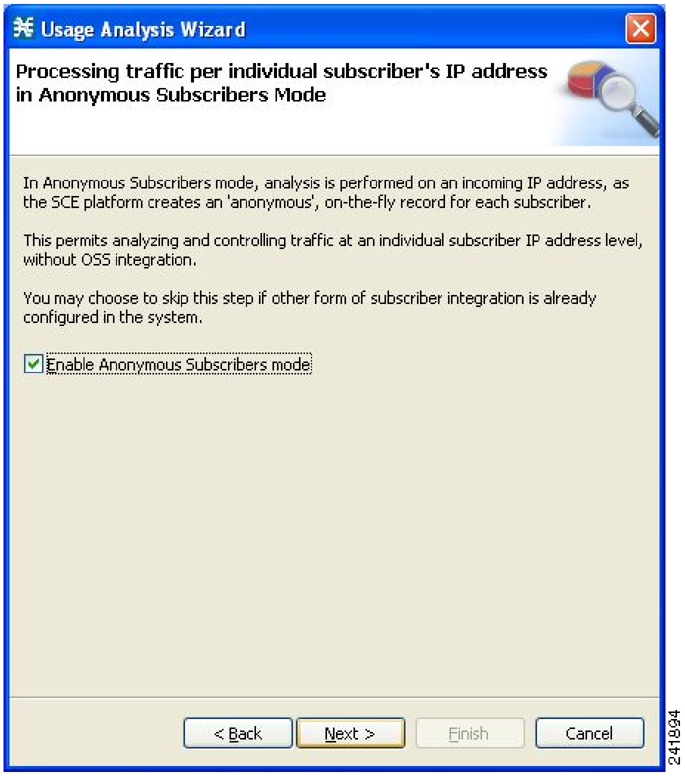
The wizard tests to see that the connections to the defined devices can be made.

Note If a connection to one or more of the devices cannot be made or if there is some problem with the connection (such as invalid version of the device) an error is displayed next to the device. You can skip these tests by clicking **Skip connectivity test**. The connections are validated when you click **Finish** at the end of the wizard.

Step 12 Click **Next**.

The Anonymous Subscribers page of the Usage Analysis wizard opens (see Figure 4-38).

Figure 4-38 Anonymous Subscribers



Usage Analysis Wizard

Processing traffic per individual subscriber's IP address in Anonymous Subscribers Mode

In Anonymous Subscribers mode, analysis is performed on an incoming IP address, as the SCE platform creates an 'anonymous', on-the-fly record for each subscriber.

This permits analyzing and controlling traffic at an individual subscriber IP address level, without OSS integration.

You may choose to skip this step if other form of subscriber integration is already configured in the system.

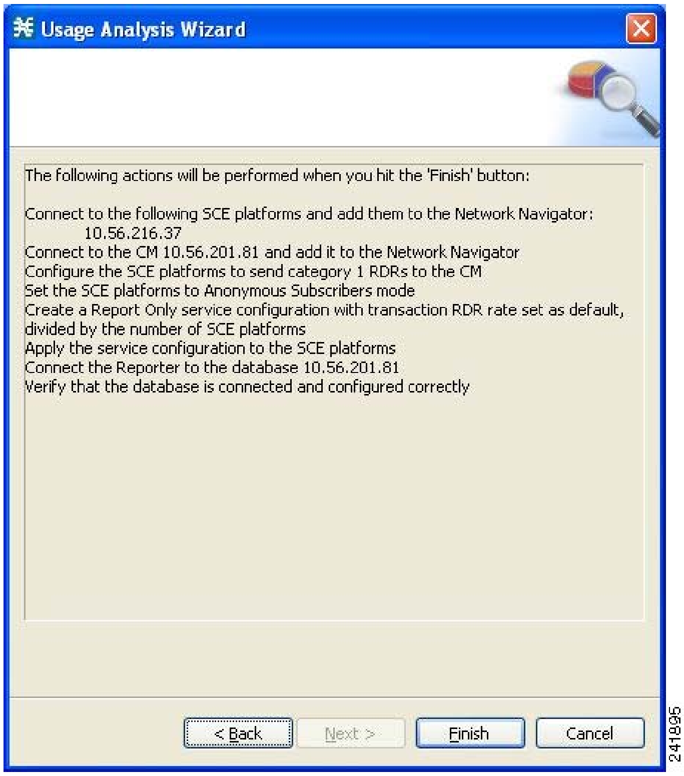
☑ Enable Anonymous Subscribers mode

Step 13 To disable anonymous subscriber mode, clear the **Enable Anonymous Subscribers mode** check box.

Step 14 Click **Next**.

The Confirmation page of the Usage Analysis wizard opens (see Figure 4-39).

Figure 4-39 Confirmation



The following actions will be performed when you hit the 'Finish' button:

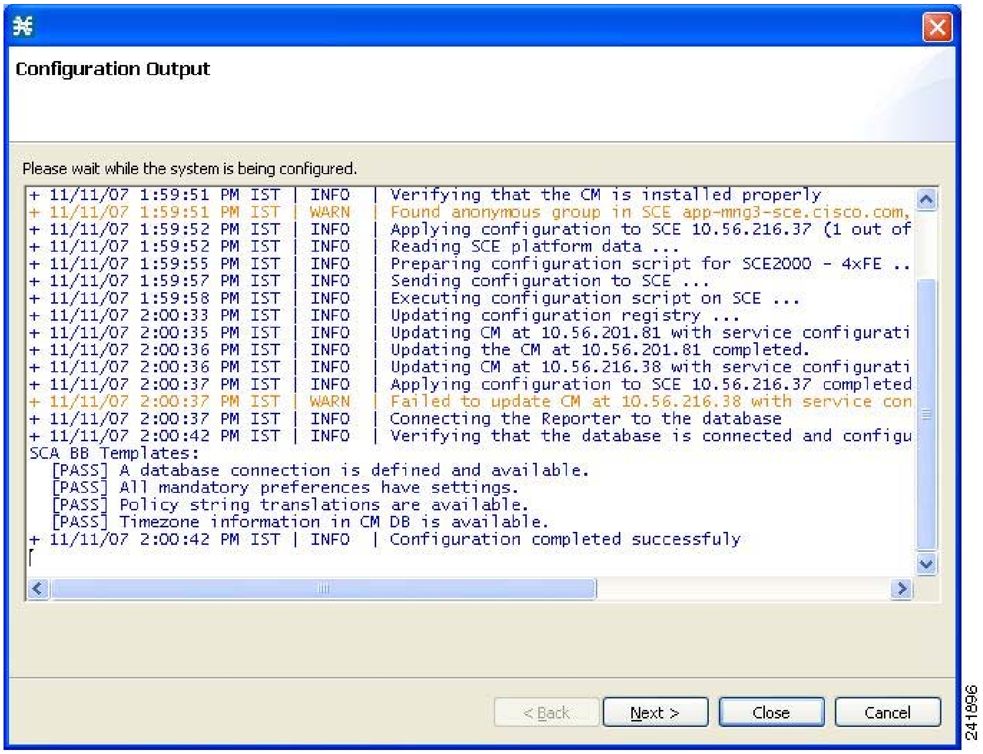
Connect to the following SCE platforms and add them to the Network Navigator:
10.56.216.37
Connect to the CM 10.56.201.81 and add it to the Network Navigator
Configure the SCE platforms to send category 1 RDRs to the CM
Set the SCE platforms to Anonymous Subscribers mode
Create a Report Only service configuration with transaction RDR rate set as default, divided by the number of SCE platforms
Apply the service configuration to the SCE platforms
Connect the Reporter to the database 10.56.201.81
Verify that the database is connected and configured correctly

The actions that the wizard is about to take are listed on the page.

Step 15 Click **Finish**.

The Configuration Output page of the Usage Analysis wizard opens (see Figure 4-40).

Figure 4-40 Configuration Output

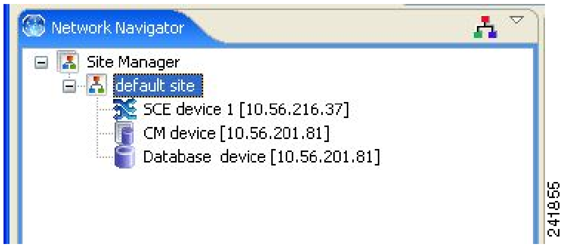


Please wait while the system is being configured.

```
+ 11/11/07 1:59:51 PM IST | INFO  | Verifying that the CM is installed properly
+ 11/11/07 1:59:51 PM IST | WARN  | Found anonymous group in SCE app-mng3-sce.cisco.com,
+ 11/11/07 1:59:52 PM IST | INFO  | Applying configuration to SCE 10.56.216.37 (1 out of
+ 11/11/07 1:59:52 PM IST | INFO  | Reading SCE platform data ...
+ 11/11/07 1:59:55 PM IST | INFO  | Preparing configuration script for SCE2000 - 4xFE ..
+ 11/11/07 1:59:57 PM IST | INFO  | Sending configuration to SCE ...
+ 11/11/07 1:59:58 PM IST | INFO  | Executing configuration script on SCE ...
+ 11/11/07 2:00:33 PM IST | INFO  | Updating configuration registry ...
+ 11/11/07 2:00:35 PM IST | INFO  | Updating CM at 10.56.201.81 with service configurati
+ 11/11/07 2:00:36 PM IST | INFO  | Updating the CM at 10.56.201.81 completed.
+ 11/11/07 2:00:36 PM IST | INFO  | Updating CM at 10.56.216.38 with service configurati
+ 11/11/07 2:00:37 PM IST | INFO  | Applying configuration to SCE 10.56.216.37 completed
+ 11/11/07 2:00:37 PM IST | WARN  | Failed to update CM at 10.56.216.38 with service con
+ 11/11/07 2:00:37 PM IST | INFO  | Connecting the Reporter to the database
+ 11/11/07 2:00:42 PM IST | INFO  | Verifying that the database is connected and configu
SCA BB Templates:
   [PASS] A database connection is defined and available.
   [PASS] All mandatory preferences have settings.
   [PASS] Policy string translations are available.
   [PASS] Timezone information in CM DB is available.
+ 11/11/07 2:00:42 PM IST | INFO  | Configuration completed successfuly
```

New devices are added to the default site of the Site Manager tree in the Network Navigator (see Figure 4-41).

Figure 4-41 Site Manager Tree



The wizard attempts to connect to all devices that you defined. The operation fails if:

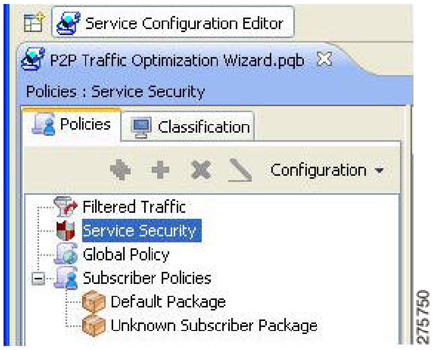
- The wizard cannot connect to any of the SCE devices that you listed in Step 4.
- You defined a CM in Step 8, but the wizard cannot connect to it.
- You defined a database in Step 10, but the wizard cannot connect to it.

If you defined a CM in Step 8, the SCE devices are configured so that the only category 1 RDR destination is the CM.

Note RDR categories are the mechanism by which different types of RDRs can be sent to different collectors. For more information about RDR categories, see either the "Raw Data Formatting: The RDR Formatter and NetFlow Exporting" chapter of *Cisco SCE8000 10GBE Software Configuration Guide or the* "Raw Data Formatting: The RDR Formatter and NetFlow Exporting" chapter of *Cisco SCE8000 GBE Software Configuration Guide.*

A new service configuration named Usage Analysis is created, and opens in the Service Configuration Editor (see Figure 4-42).

Figure 4-42 Service Configuration Editor



The service configuration has the following characteristics:

- Report Only mode.
- The maximum Transaction RDR rate is set as the default value (250) divided by the number of SCE devices. To configure the Transaction RDR see How to Manage Transaction RDRs, page 8-6. The content and structure is listed in "Transaction RDR" section in the "Raw Data Records: Formats and Field Contents" chapter of *Cisco Service Control Application for Broadband Reference Guide.*

The service configuration is applied to the SCE devices.

If you defined a database in Step 10:

- The Cisco SCA BB Reporter tool is connected to the selected database.
- The first SCE platform entered in Step 4 is selected as the source of service configuration data.
- The Next button is enabled.

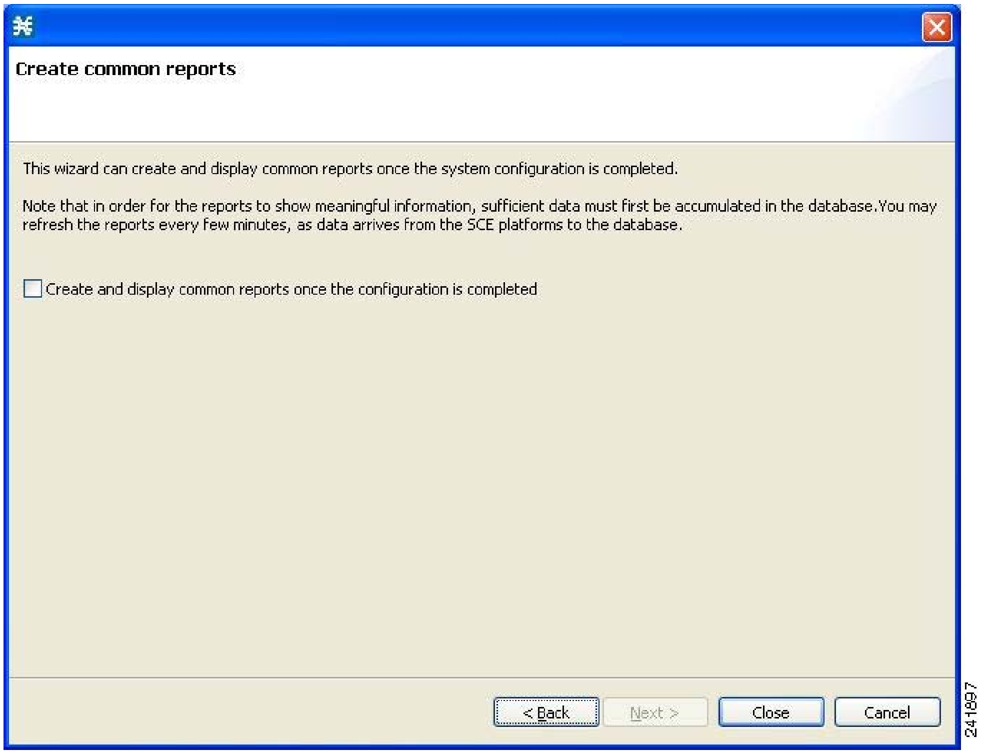
Step 16 If you did not define a database in Step 10, click **Close**.

The Usage Analysis wizard closes.

Step 17 Click **Next**.

The Create common reports page of the Usage Analysis wizard opens (see Figure 4-43).

Figure 4-43 Create Common Reports



Create common reports

This wizard can create and display common reports once the system configuration is completed.

Note that in order for the reports to show meaningful information, sufficient data must first be accumulated in the database.You may refresh the reports every few minutes, as data arrives from the SCE platforms to the database.

□ Create and display common reports once the configuration is completed

Step 18 To create reports, check the **Create and display common reports** check box.

Note Report instances are created for four predefined report types:

- Global Bandwidth per Service
- Global Active Subscribers per Service
- Top P2P Protocols
- Global Hourly Call Minutes per Service (VoIP)

Step 19 Click **Close**.

The wizard closes.

The Reporter tool opens in the Console.

Report instances of each of the four report types open in the Report View of the Reporter tool.

How to Use the P2P Traffic Optimization Wizards

There are two wizards for optimizing P2P traffic:

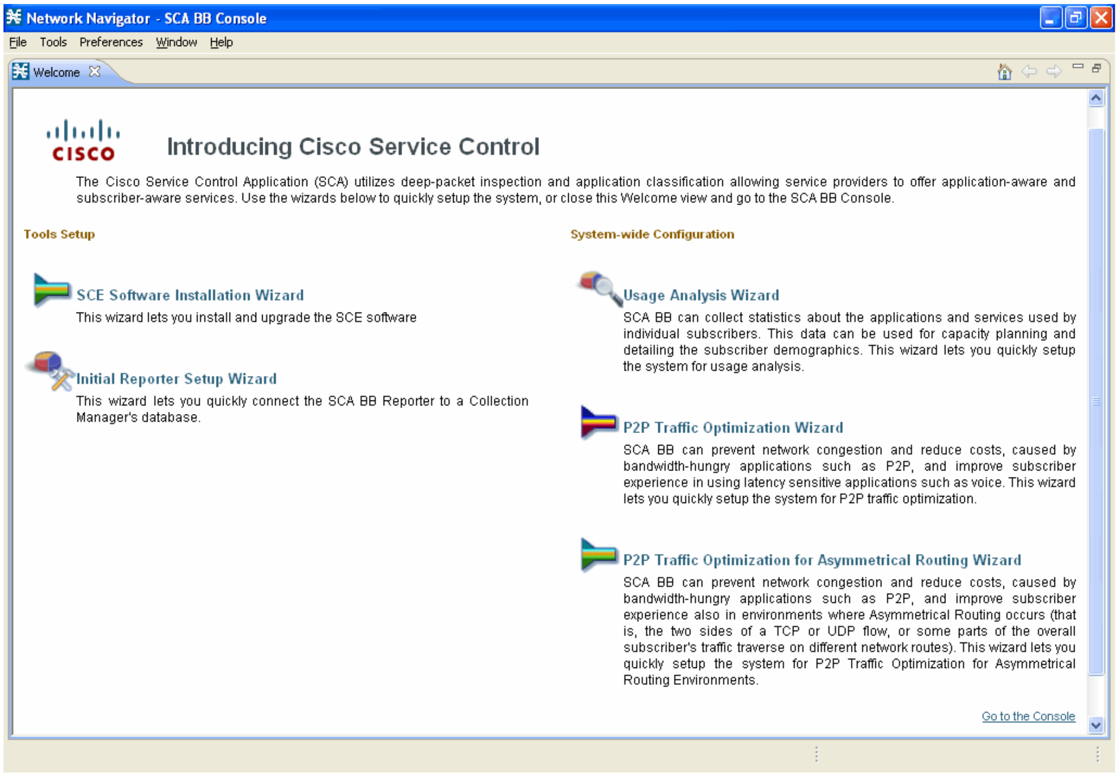
- The P2P Traffic Optimization wizard allows you to create a simple model of devices, connect to them, and limit P2P traffic to a specified percentage of total available bandwidth.
- The P2P Traffic Optimization at a Peering Point wizard allows you to create a simple model of devices, connect to them, limit P2P traffic to a specified percentage of total available bandwidth, and enable asymmetric routing classification mode.

Note If they do not exist, devices defined in the wizard are added to the default site in the Site Manager tree.

Step 1 From the Console main menu, choose **Help > Welcome**.

The Welcome view opens (see Figure 4-44).

Figure 4-44 Welcome - Introducing Cisco Service Control


Network Navigator - SCA BB Console
File Tools Preferences Window Help
Welcome
207260

Introducing Cisco Service Control

The Cisco Service Control Application (SCA) utilizes deep-packet inspection and application classification allowing service providers to offer application-aware and subscriber-aware services. Use the wizards below to quickly setup the system, or close this Welcome view and go to the SCA BB Console.

Tools Setup

SCE Software Installation Wizard

This wizard lets you install and upgrade the SCE software

Initial Reporter Setup Wizard

This wizard lets you quickly connect the SCA BB Reporter to a Collection Manager's database.

System-wide Configuration

Usage Analysis Wizard

SCA BB can collect statistics about the applications and services used by individual subscribers. This data can be used for capacity planning and detailing the subscriber demographics. This wizard lets you quickly setup the system for usage analysis.

P2P Traffic Optimization Wizard

SCA BB can prevent network congestion and reduce costs, caused by bandwidth-hungry applications such as P2P, and improve subscriber experience in using latency sensitive applications such as voice. This wizard lets you quickly setup the system for P2P traffic optimization.

P2P Traffic Optimization for Asymmetrical Routing Wizard

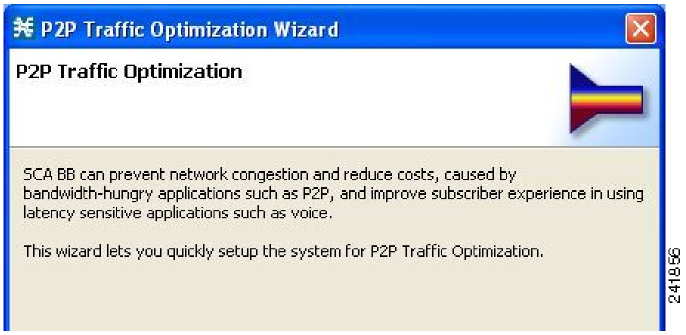
SCA BB can prevent network congestion and reduce costs, caused by bandwidth-hungry applications such as P2P, and improve subscriber experience also in environments where Asymmetrical Routing occurs (that is, the two sides of a TCP or UDP flow, or some parts of the overall subscriber's traffic traverse on different network routes). This wizard lets you quickly setup the system for P2P Traffic Optimization for Asymmetrical Routing Environments.

Go to the Console

Step 2 Click **P2P Traffic Optimization Wizard** or **P2P Traffic Optimization for Asymmetrical Routing Wizard**.

The Welcome page of the selected wizard appears (see Figure 4-45 or Figure 4-46).

Figure 4-45 P2P Traffic Optimization



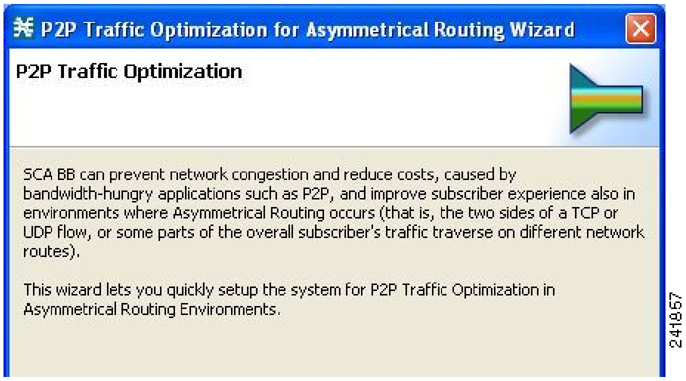
P2P Traffic Optimization Wizard

P2P Traffic Optimization

SCA BB can prevent network congestion and reduce costs, caused by bandwidth-hungry applications such as P2P, and improve subscriber experience in using latency sensitive applications such as voice.

This wizard lets you quickly setup the system for P2P Traffic Optimization.

Figure 4-46 P2P Traffic Optimization for Asymmetrical Routing



P2P Traffic Optimization for Asymmetrical Routing Wizard

P2P Traffic Optimization

SCA BB can prevent network congestion and reduce costs, caused by bandwidth-hungry applications such as P2P, and improve subscriber experience also in environments where Asymmetrical Routing occurs (that is, the two sides of a TCP or UDP flow, or some parts of the overall subscriber's traffic traverse on different network routes).

This wizard lets you quickly setup the system for P2P Traffic Optimization in Asymmetrical Routing Environments.

Note You can also execute the P2P Traffic Optimization wizard from the Network Navigator tool.

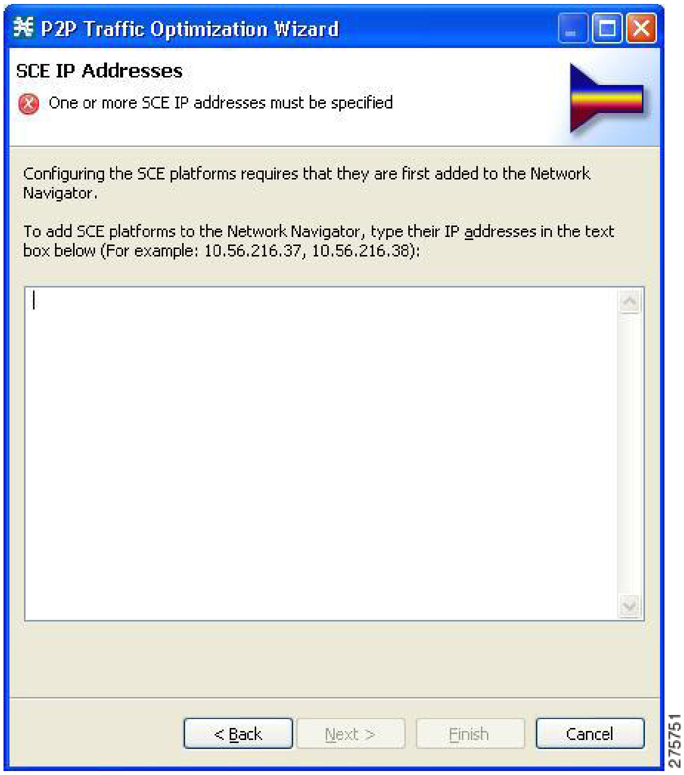
1. Select one or more devices in the Site Manager tree.
2. Right-click one of the selected devices.
3. From the popup menu that appears, choose **Configuration Wizards > P2P Traffic Optimization Wizard** or **Configuration Wizards > P2P Traffic Optimization for Asymmetrical Routing Wizard**.

Note You can set only one CM and one Reporter database in the wizard. If you select more than one CM or Reporter database, only one CM and one Reporter database is selected and a warning message is displayed. Click **OK** to continue.

Step 3 Click **Next**.

The SCE IP Addresses page of the P2P Traffic Optimization wizard opens (see Figure 4-47).

Figure 4-47 SCE IP Addresses



P2P Traffic Optimization Wizard

SCE IP Addresses

One or more SCE IP addresses must be specified

Configuring the SCE platforms requires that they are first added to the Network Navigator.

To add SCE platforms to the Network Navigator, type their IP addresses in the text box below (For example: 10.56.216.37, 10.56.216.38):

Step 4 In the edit box, enter the IP addresses of the SCE devices that should be added to the model.

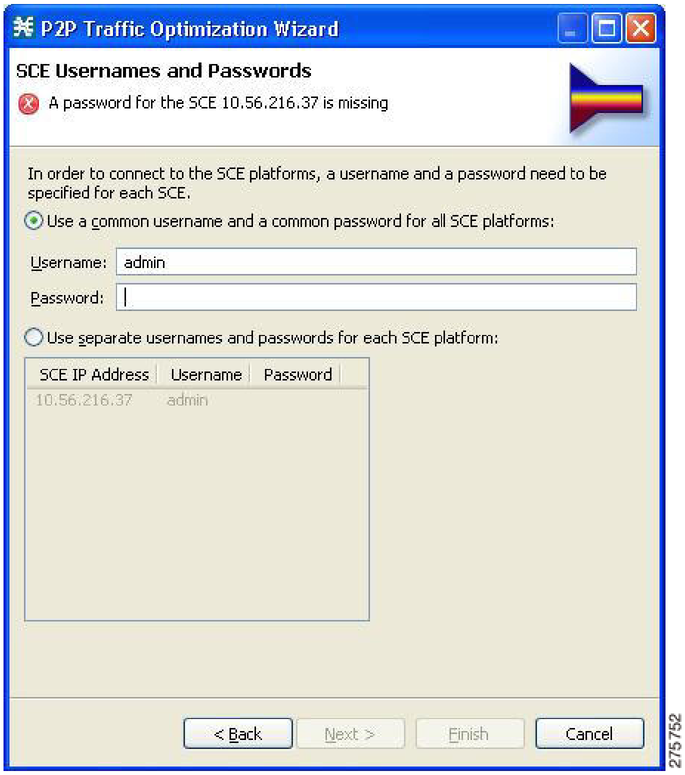
If you started from the Network Navigator, the IP addresses of the SCE devices that you selected are displayed in the edit box. You can add additional addresses.

Note You can work with up to 20 SCE devices at one time using the wizard.

Step 5 Click **Next**.

The SCE Usernames and Passwords page of the P2P Traffic Optimization wizard opens (see Figure 4-48).

Figure 4-48 SCE Usernames and Passwords



P2P Traffic Optimization Wizard

SCE Usernames and Passwords

A password for the SCE 10.56.216.37 is missing

In order to connect to the SCE platforms, a username and a password need to be specified for each SCE.

● Use a common username and a common password for all SCE platforms:

Username: admin

Password:

○ Use separate usernames and passwords for each SCE platform:

SCE IP Address	Username	Password
10.56.216.37	admin	

Step 6 Enter the usernames and passwords for the SCE devices.

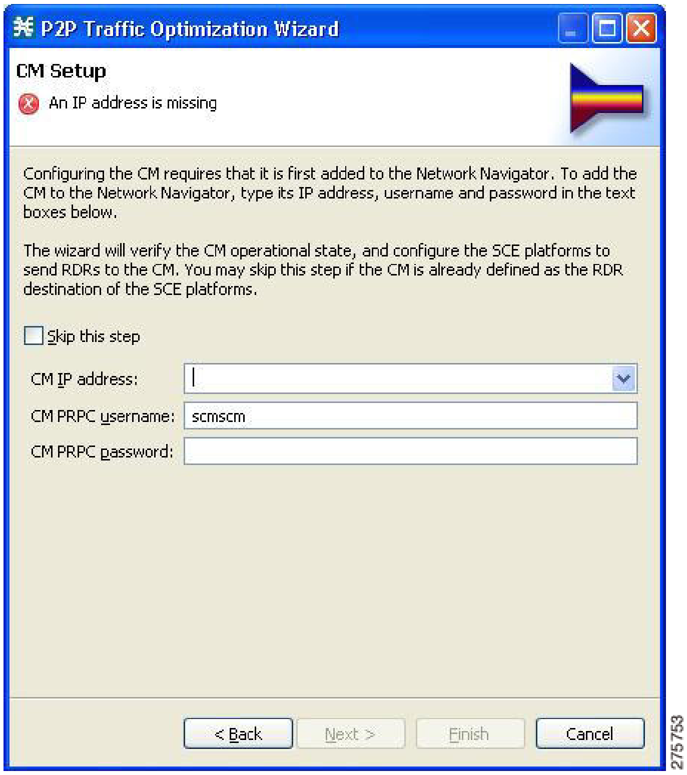
Do one of the following:

- To use the same username and password for all the SCE devices that you are adding, enter the username in the Username field and the password in the Password field.
- To provide a different username and password pair for each SCE device, click the **Use separate usernames and passwords for each SCE platform** radio button, and, for each SCE device, enter the username and password in the appropriate cell of the SCE device table.

Step 7 Click **Next**.

The CM Setup page of the P2P Traffic Optimization wizard opens (see Figure 4-49).

Figure 4-49 CM Setup



P2P Traffic Optimization Wizard

CM Setup

An IP address is missing

Configuring the CM requires that it is first added to the Network Navigator. To add the CM to the Network Navigator, type its IP address, username and password in the text boxes below.

The wizard will verify the CM operational state, and configure the SCE platforms to send RDRs to the CM. You may skip this step if the CM is already defined as the RDR destination of the SCE platforms.

□ Skip this step

CM IP address:

CM PRPC username: scmscm

CM PRPC password:

Step 8 Define the SCMS Collection Manager (CM) to use with this configuration.

Do one of the following:

- Enter the IP address, username, and password of the CM device in the appropriate fields.

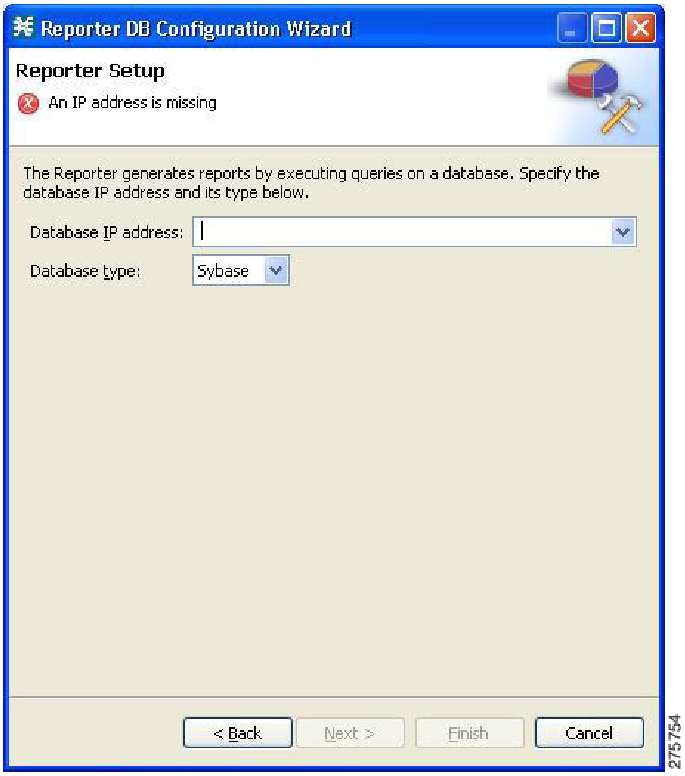
  If you started from the Network Navigator, this information is retrieved and displayed. You can modify these parameters.

- Check the **Skip this step** check box.

Step 9 Click **Next**.

The Reporter Setup page of the P2P Traffic Optimization wizard opens (see Figure 4-50).

Figure 4-50 Reporter Setup



Reporter Setup

An IP address is missing

The Reporter generates reports by executing queries on a database. Specify the database IP address and its type below.

Database IP address:

Database type: Sybase

Step 10 Define the database to which the Reporter tool should connect.

Do one of the following:

- Enter the IP address of the database and select the database type.

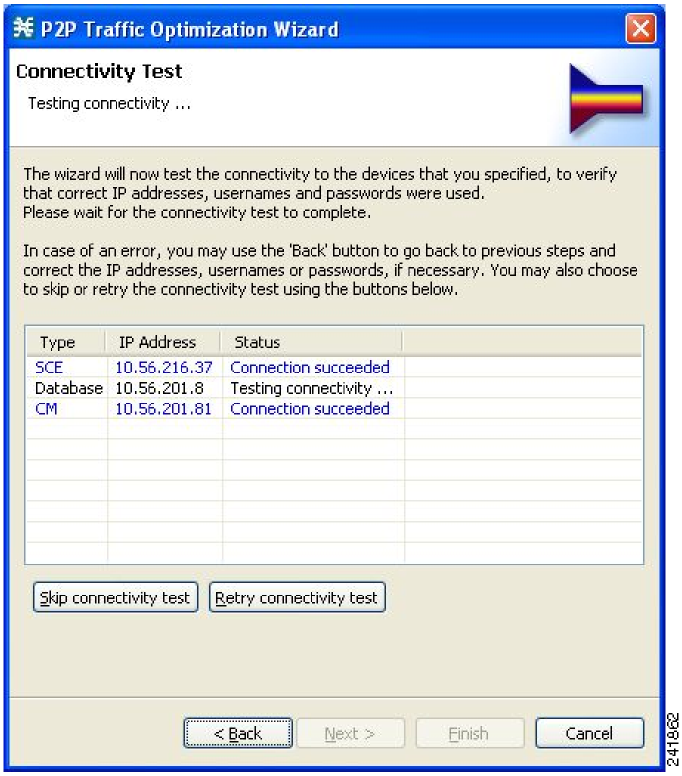
  If you started from the Network Navigator, this information is retrieved and displayed. You can modify these parameters.

- Check the **Skip this step** check box.

Step 11 Click **Next**.

The Connectivity Test page of the P2P Traffic Optimization wizard opens (see Figure 4-51).

Figure 4-51 Connectivity Test



P2P Traffic Optimization Wizard

Connectivity Test

Testing connectivity ...

The wizard will now test the connectivity to the devices that you specified, to verify that correct IP addresses, usernames and passwords were used.
Please wait for the connectivity test to complete.

In case of an error, you may use the 'Back' button to go back to previous steps and correct the IP addresses, usernames or passwords, if necessary. You may also choose to skip or retry the connectivity test using the buttons below.

Type	IP Address	Status
SCE	10.56.216.37	Connection succeeded
Database	10.56.201.8	Testing connectivity ...
CM	10.56.201.81	Connection succeeded

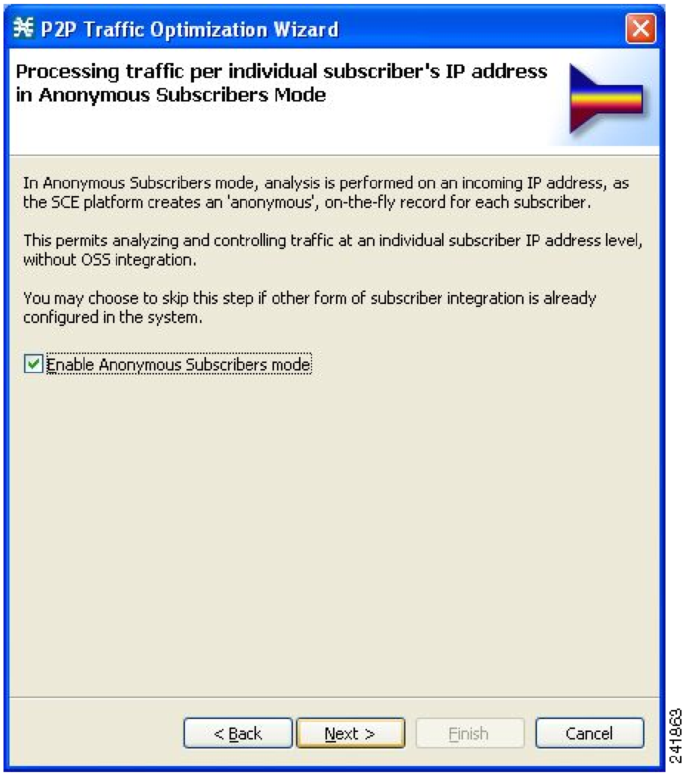
The wizard tests to see that the connections to the defined devices can be made.

Note If a connection to one or more of the devices cannot be made or if there is some problem with the connection (such as invalid version of the device), an error is displayed next to the device. You can skip these tests by clicking **Skip connectivity test.** The connections are validated when you click **Finish** at the end of the wizard.

Step 12 Click **Next**.

The Anonymous Subscribers page of the P2P Traffic Optimization wizard opens (see Figure 4-52).

Figure 4-52 Anonymous Subscribers



P2P Traffic Optimization Wizard

Processing traffic per individual subscriber's IP address in Anonymous Subscribers Mode

In Anonymous Subscribers mode, analysis is performed on an incoming IP address, as the SCE platform creates an 'anonymous', on-the-fly record for each subscriber.

This permits analyzing and controlling traffic at an individual subscriber IP address level, without OSS integration.

You may choose to skip this step if other form of subscriber integration is already configured in the system.

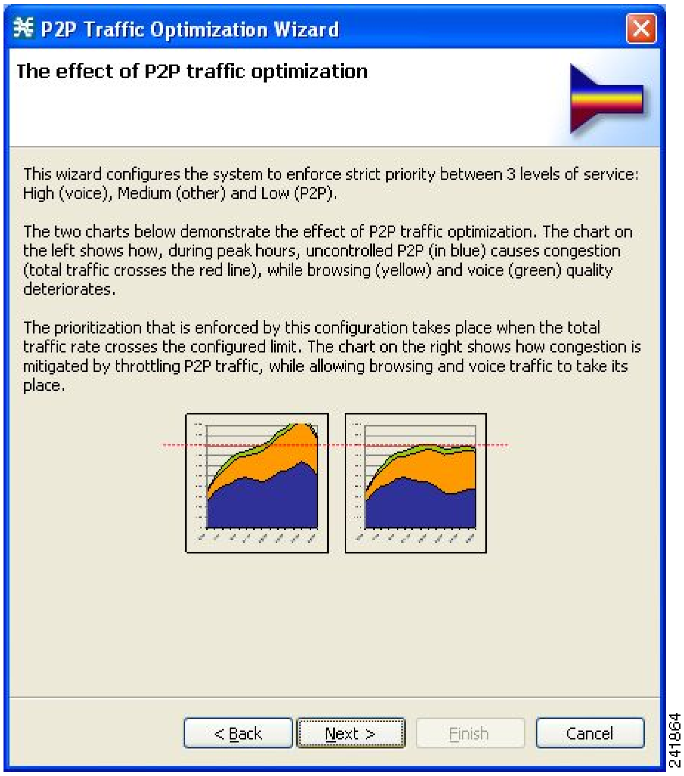
☑ Enable Anonymous Subscribers mode

Step 13 To disable anonymous subscriber mode, uncheck the **Enable Anonymous Subscribers mode** check box.

Step 14 Click **Next**.

The effect of P2P traffic optimization page of the P2P Traffic Optimization wizard opens (see Figure 4-53).

Figure 4-53 Effect of P2P Traffic Optimization



P2P Traffic Optimization Wizard

The effect of P2P traffic optimization

This wizard configures the system to enforce strict priority between 3 levels of service: High (voice), Medium (other) and Low (P2P).

The two charts below demonstrate the effect of P2P traffic optimization. The chart on the left shows how, during peak hours, uncontrolled P2P (in blue) causes congestion (total traffic crosses the red line), while browsing (yellow) and voice (green) quality deteriorates.

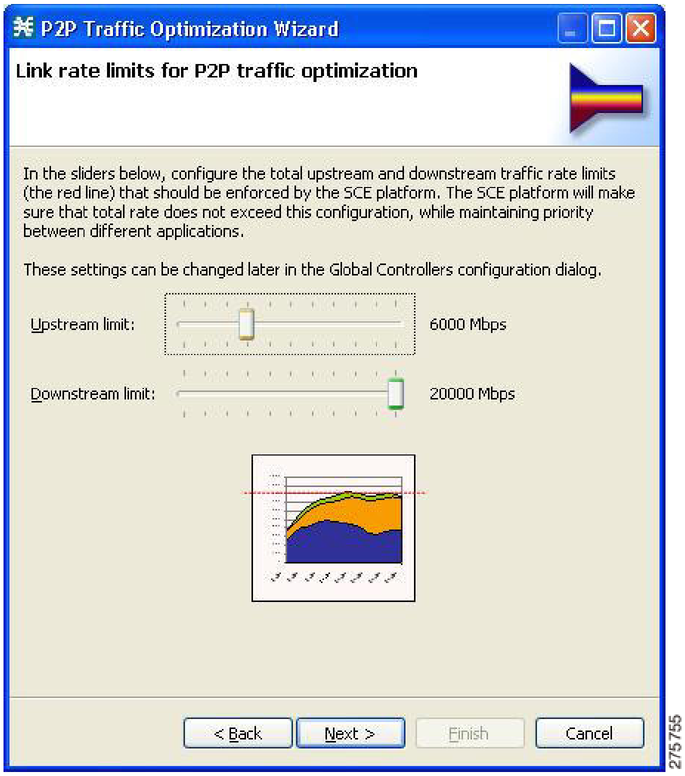
The prioritization that is enforced by this configuration takes place when the total traffic rate crosses the configured limit. The chart on the right shows how congestion is mitigated by throttling P2P traffic, while allowing browsing and voice traffic to take its place.

This page explains why you should optimize (limit) P2P traffic.

Step 15 Click **Next**.

The Link Rate Limits for P2P Traffic Optimization page of the P2P Traffic Optimization wizard opens (see Figure 4-54).

Figure 4-54 Link Rate Limits



P2P Traffic Optimization Wizard

Link rate limits for P2P traffic optimization

In the sliders below, configure the total upstream and downstream traffic rate limits (the red line) that should be enforced by the SCE platform. The SCE platform will make sure that total rate does not exceed this configuration, while maintaining priority between different applications.

These settings can be changed later in the Global Controllers configuration dialog.

Upstream limit: 6000 Mbps

Downstream limit: 20000 Mbps

Step 16 Use the sliders to configure the upstream and downstream link rate limits.

The scale of each slider is the percentage of the aggregated bandwidth of both links.

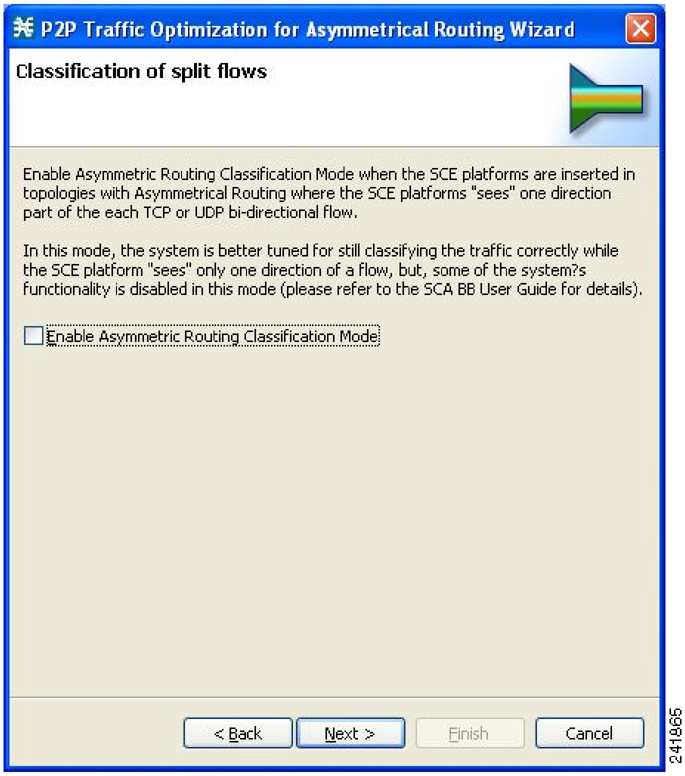
Step 17 If you are running the P2P Traffic Optimization wizard, go to Step 20.

If you are running the P2P Traffic Optimization for Asymmetrical Routing wizard, continue at the next step.

Step 18 Click **Next**.

The Classification of split flows page of the P2P Traffic Optimization wizard opens (see Figure 4-55).

Figure 4-55 Classification of Split Flows



P2P Traffic Optimization for Asymmetrical Routing Wizard

Classification of split flows

Enable Asymmetric Routing Classification Mode when the SCE platforms are inserted in topologies with Asymmetrical Routing where the SCE platforms "sees" one direction part of the each TCP or UDP bi-directional flow.

In this mode, the system is better tuned for still classifying the traffic correctly while the SCE platform "sees" only one direction of a flow, but, some of the system?s functionality is disabled in this mode (please refer to the SCA BB User Guide for details).

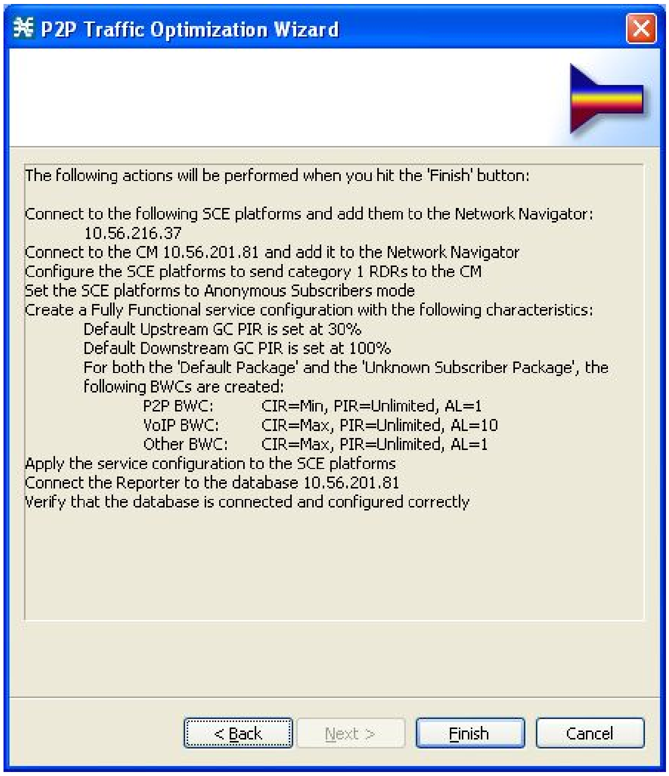
☐ Enable Asymmetric Routing Classification Mode

Step 19 To enable asymmetric routing classification mode, check the **Enable Asymmetric Routing Classification Mode** check box.

Step 20 Click **Next**.

The Confirmation page of the P2P Traffic Optimization wizard opens (see Figure 4-56).

Figure 4-56 Confirmation



P2P Traffic Optimization Wizard

The following actions will be performed when you hit the 'Finish' button:

Connect to the following SCE platforms and add them to the Network Navigator:
        10.56.216.37
Connect to the CM 10.56.201.81 and add it to the Network Navigator
Configure the SCE platforms to send category 1 RDRs to the CM
Set the SCE platforms to Anonymous Subscribers mode
Create a Fully Functional service configuration with the following characteristics:
        Default Upstream GC PIR is set at 30%
        Default Downstream GC PIR is set at 100%
        For both the 'Default Package' and the 'Unknown Subscriber Package', the following BWCs are created:
                P2P BWC: CIR=Min, PIR=Unlimited, AL=1
                VoIP BWC: CIR=Max, PIR=Unlimited, AL=10
                Other BWC: CIR=Max, PIR=Unlimited, AL=1
Apply the service configuration to the SCE platforms
Connect the Reporter to the database 10.56.201.81
Verify that the database is connected and configured correctly

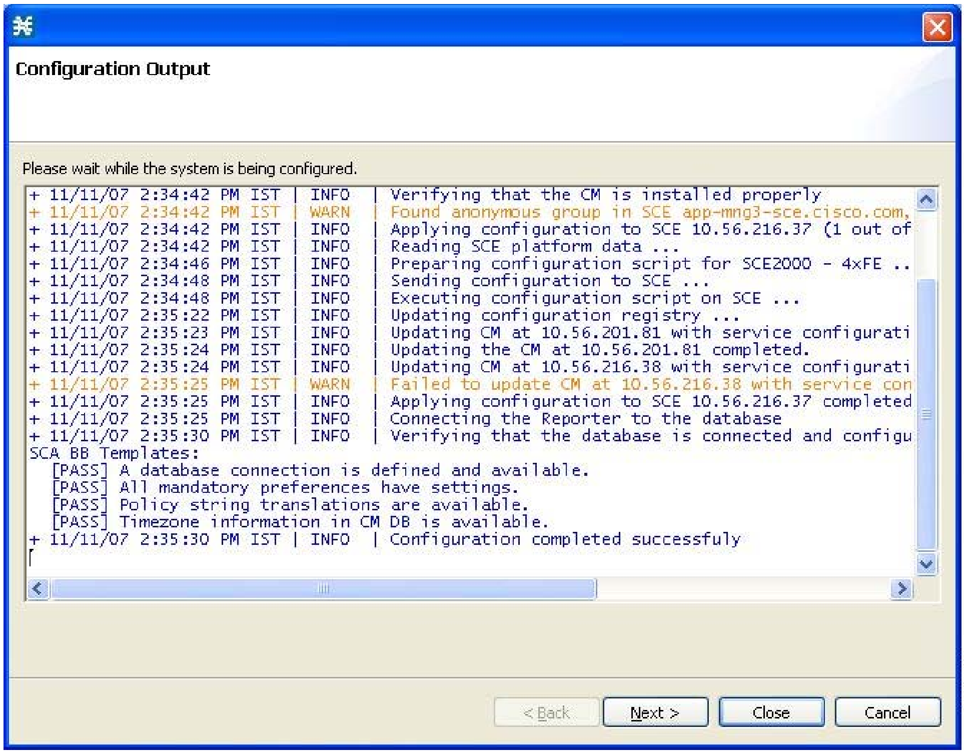
The actions that the wizard is about to take are listed on the page.

For an explanation of the bandwidth controller parameters, see Subscriber BWC Parameters, page 9-29.

Step 21 Click **Finish**.

The Configuration Output page of the P2P Traffic Optimization wizard opens (see Figure 4-57).

Figure 4-57 Configuration Output



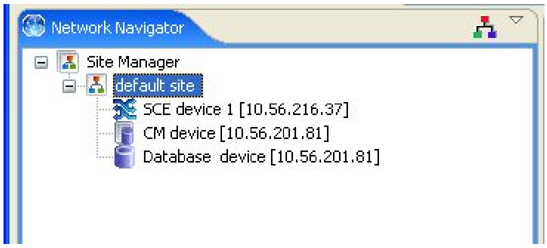
Configuration Output

Please wait while the system is being configured.

```
+ 11/11/07 2:34:42 PM IST | INFO  | Verifying that the CM is installed properly
+ 11/11/07 2:34:42 PM IST | WARN  | Found anonymous group in SCE app-mng3-sce.cisco.com,
+ 11/11/07 2:34:42 PM IST | INFO  | Applying configuration to SCE 10.56.216.37 (1 out of
+ 11/11/07 2:34:42 PM IST | INFO  | Reading SCE platform data ...
+ 11/11/07 2:34:46 PM IST | INFO  | Preparing configuration script for SCE2000 - 4xFE ..
+ 11/11/07 2:34:48 PM IST | INFO  | Sending configuration to SCE ...
+ 11/11/07 2:34:48 PM IST | INFO  | Executing configuration script on SCE ...
+ 11/11/07 2:35:22 PM IST | INFO  | Updating configuration registry ...
+ 11/11/07 2:35:23 PM IST | INFO  | Updating CM at 10.56.201.81 with service configurati
+ 11/11/07 2:35:24 PM IST | INFO  | Updating the CM at 10.56.201.81 completed.
+ 11/11/07 2:35:24 PM IST | INFO  | Updating CM at 10.56.216.38 with service configurati
+ 11/11/07 2:35:25 PM IST | WARN  | Failed to update CM at 10.56.216.38 with service con
+ 11/11/07 2:35:25 PM IST | INFO  | Applying configuration to SCE 10.56.216.37 completed
+ 11/11/07 2:35:25 PM IST | INFO  | Connecting the Reporter to the database
+ 11/11/07 2:35:30 PM IST | INFO  | Verifying that the database is connected and configu
SCA BB Templates:
   [PASS] A database connection is defined and available.
   [PASS] All mandatory preferences have settings.
   [PASS] Policy string translations are available.
   [PASS] Timezone information in CM DB is available.
+ 11/11/07 2:35:30 PM IST | INFO  | Configuration completed successfuly
```

New devices are added to the default site of the Site Manager tree in the Network Navigator (see Figure 4-58).

Figure 4-58 Network Navigator



The wizard attempts to connect to all devices that you defined. The operation fails if:

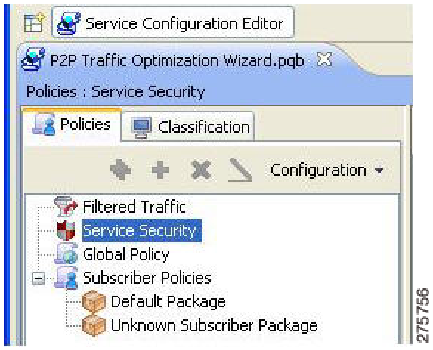
- The wizard cannot connect to any of the SCE devices that you listed in Step 4.
- You defined a CM in Step 8, but the wizard cannot connect to it.
- You defined a database in Step 10, but the wizard cannot connect to it.

If you defined a CM in Step 8, the SCE devices are configured so that the only category 1 RDR destination is the CM.

Note RDR categories are the mechanism by which different types of RDRs can be sent to different collectors. For more information about RDR categories, see "Raw Data Records: Formats and Field Contents" chapter of *Cisco Service Control Application for Broadband Reference Guide.*

A new service configuration named P2P Traffic Optimization (or P2P Traffic Optimization for Asymmetrical Routing) is created, and opens in the Service Configuration Editor (see Figure 4-59).

Figure 4-59 Service Configuration Editor



The service configuration has the following characteristics:

- Full functionality mode.
- The upstream and downstream default AGCs are set with the link limit values defined in Step 16.
- For both the default package and the Unknown Subscriber Traffic package, the following upstream and downstream BWCs are created (Table 4-2):

Table 4-2 BWCs for Default and Unknown Subscriber Traffic Packages

Packages	CIR	PIR	AL
P2P	0	<value set in global controller>	1
VoIP	<value set in global controller>	<value set in global controller>	10
P2P	<value set in global controller>	<value set in global controller>	1

The service configuration is applied to the SCE devices.

If you defined a database in Step 10:

1. The Cisco SCA BB Reporter tool is connected to the selected database.
2. The first SCE platform entered in Step 4 is selected as the source of service configuration data.
3. The Next button is enabled.

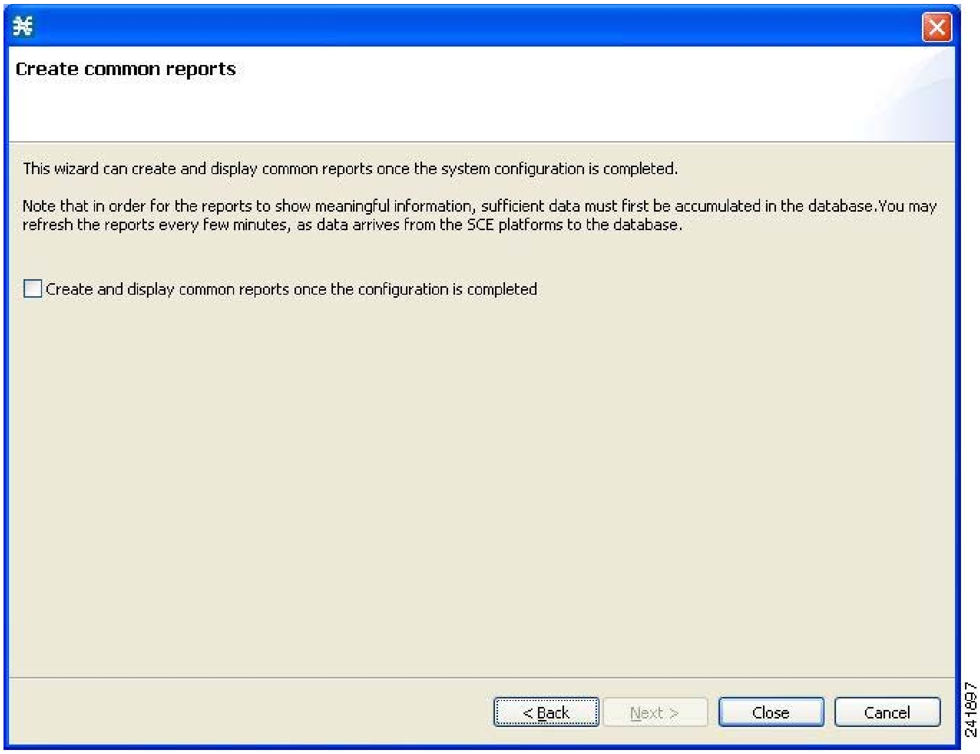
Step 22 If you did not define a database in Step 10, click **Finish**.

The P2P Traffic Optimization wizard closes.

Step 23 Click **Next**.

The Create common reports page of the P2P Traffic Optimization wizard opens (see Figure 4-60).

Figure 4-60 Create Common Reports



Create common reports

This wizard can create and display common reports once the system configuration is completed.

Note that in order for the reports to show meaningful information, sufficient data must first be accumulated in the database.You may refresh the reports every few minutes, as data arrives from the SCE platforms to the database.

□ Create and display common reports once the configuration is completed

Step 24 To create reports, check the **Create and display common reports** check box.

Note Report instances are created for four predefined report types:

- Global Bandwidth per Service
- Global Active Subscribers per Service
- Top P2P Protocols
- Global Hourly Call Minutes per Service (VoIP)

Step 25 Click **Close**.

The wizard closes.

The Reporter tool opens in the Console.

Report instances of each of the four report types open in the Report View of the Reporter tool.

How to Use the Reporter DB Configuration Wizard

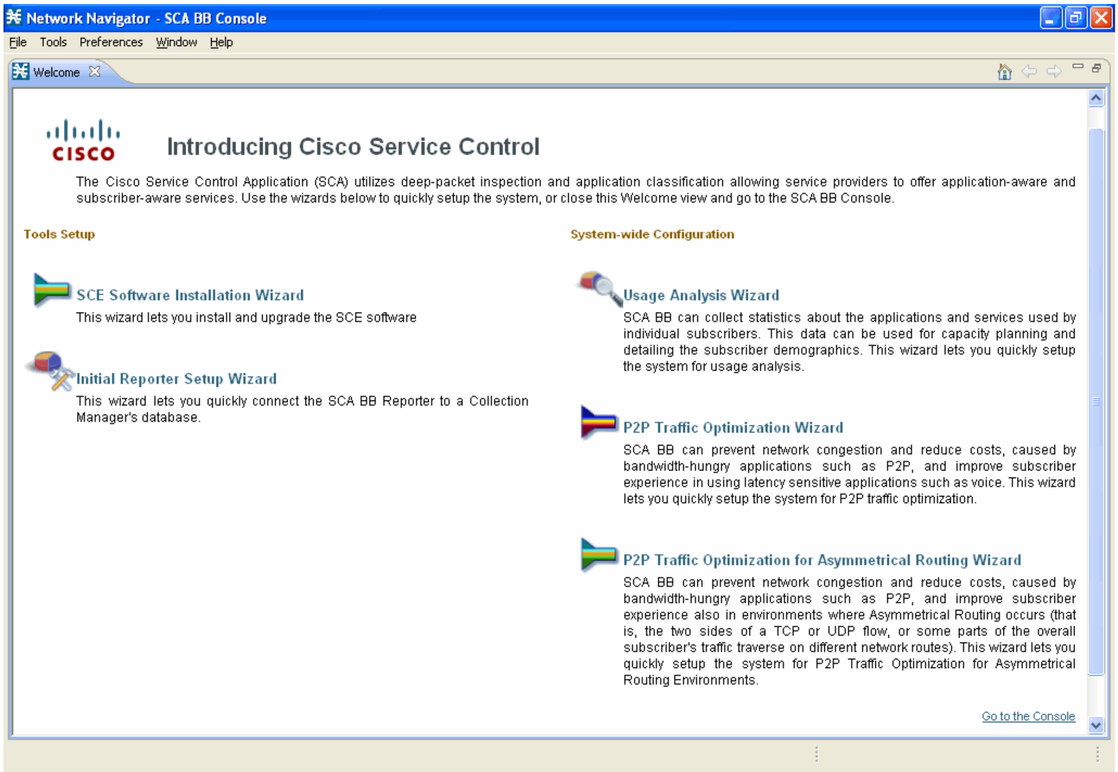
The Reporter DB Configuration wizard allows you to connect the Reporter to a database.

Caution You should run the Reporter DB Configuration wizard only after you have applied a service configuration to the SCE platform.

Step 1 From the Console main menu, choose **Help > Welcome**.

The Welcome view opens (see Figure 4-61).

Figure 4-61 Welcome - Introducing Cisco Service Control



Introducing Cisco Service Control

The Cisco Service Control Application (SCA) utilizes deep-packet inspection and application classification allowing service providers to offer application-aware and subscriber-aware services. Use the wizards below to quickly setup the system, or close this Welcome view and go to the SCA BB Console.

Tools Setup

SCE Software Installation Wizard

This wizard lets you install and upgrade the SCE software

Initial Reporter Setup Wizard

This wizard lets you quickly connect the SCA BB Reporter to a Collection Manager's database.

System-wide Configuration

Usage Analysis Wizard

SCA BB can collect statistics about the applications and services used by individual subscribers. This data can be used for capacity planning and detailing the subscriber demographics. This wizard lets you quickly setup the system for usage analysis.

P2P Traffic Optimization Wizard

SCA BB can prevent network congestion and reduce costs, caused by bandwidth-hungry applications such as P2P, and improve subscriber experience in using latency sensitive applications such as voice. This wizard lets you quickly setup the system for P2P traffic optimization.

P2P Traffic Optimization for Asymmetrical Routing Wizard

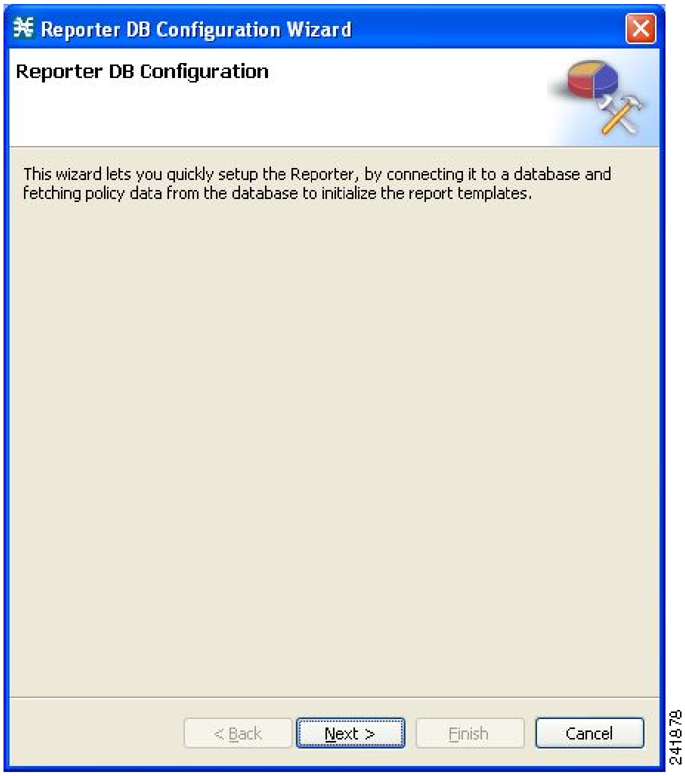
SCA BB can prevent network congestion and reduce costs, caused by bandwidth-hungry applications such as P2P, and improve subscriber experience also in environments where Asymmetrical Routing occurs (that is, the two sides of a TCP or UDP flow, or some parts of the overall subscriber's traffic traverse on different network routes). This wizard lets you quickly setup the system for P2P Traffic Optimization for Asymmetrical Routing Environments.

Go to the Console

Step 2 Click **Initial Reporter Setup Wizard**.

The Welcome page of the Reporter DB Configuration wizard appears (see Figure 4-62).

Figure 4-62 Reporter DB Configuration



Reporter DB Configuration Wizard

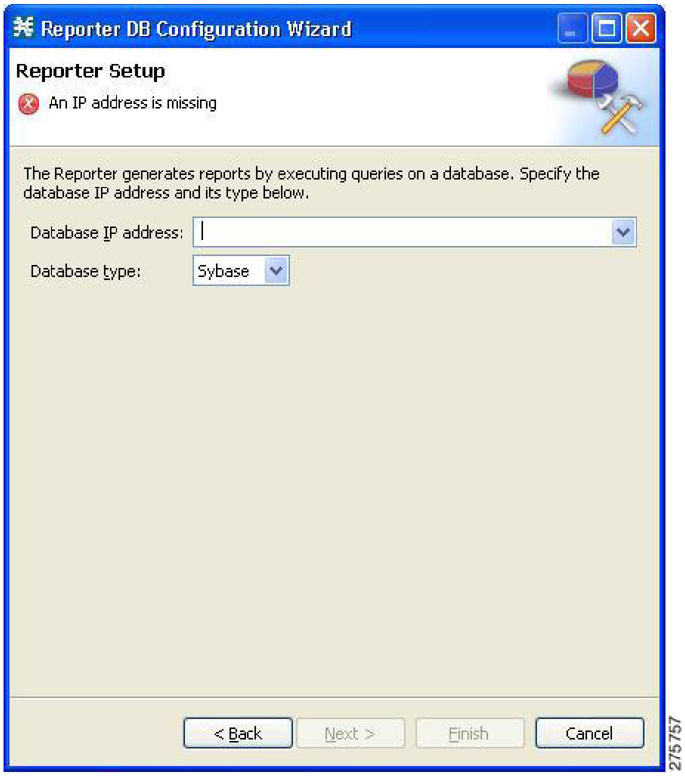
Reporter DB Configuration

This wizard lets you quickly setup the Reporter, by connecting it to a database and fetching policy data from the database to initialize the report templates.

Step 3 Click **Next**.

The Reporter Setup page of the Reporter DB Configuration wizard opens (see Figure 4-63).

Figure 4-63 Reporter Setup



Reporter DB Configuration Wizard

Reporter Setup

An IP address is missing

The Reporter generates reports by executing queries on a database. Specify the database IP address and its type below.

Database IP address:

Database type: Sybase

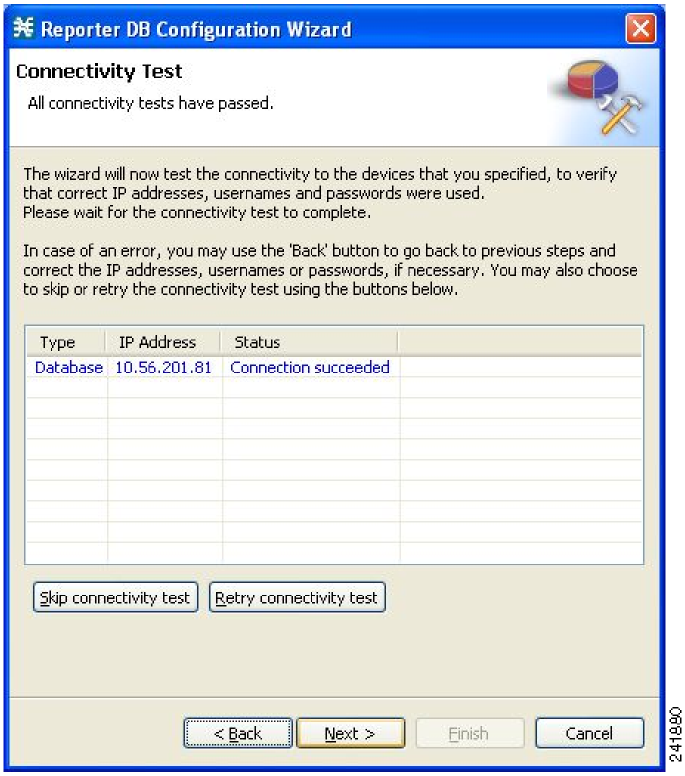
Step 4 In the Configure the IP address of the database field, enter the IP address of the database.

Step 5 From the Select the correct database type drop-down list, select the type of the database.

Step 6 Click **Next**.

The Connectivity Test window of the Reporter DB Configuration wizard opens (see Figure 4-64).

Figure 4-64 Connectivity Test



Reporter DB Configuration Wizard

Connectivity Test

All connectivity tests have passed.

The wizard will now test the connectivity to the devices that you specified, to verify that correct IP addresses, usernames and passwords were used.
Please wait for the connectivity test to complete.

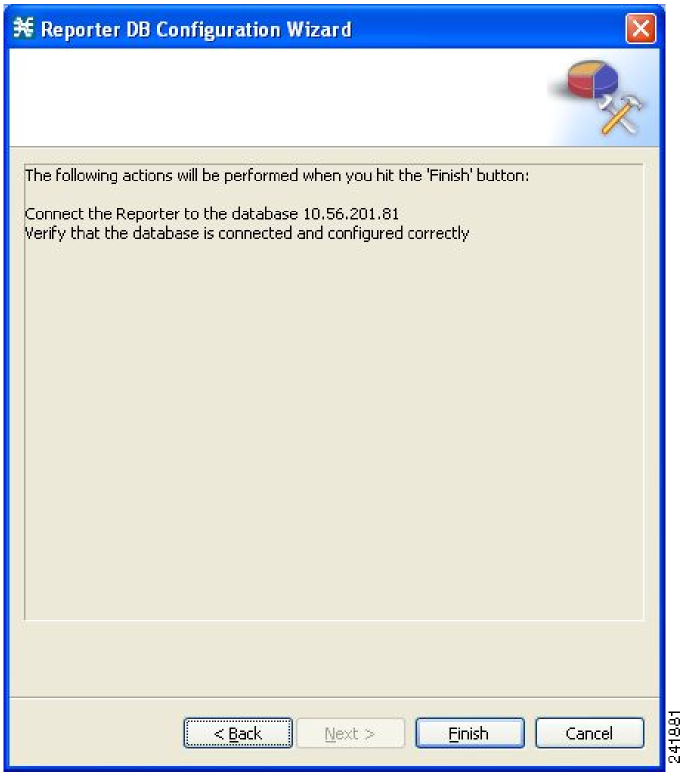
In case of an error, you may use the 'Back' button to go back to previous steps and correct the IP addresses, usernames or passwords, if necessary. You may also choose to skip or retry the connectivity test using the buttons below.

Type	IP Address	Status
Database	10.56.201.81	Connection succeeded

Step 7 Click **Next**.

The Confirmation window of the Reporter DB Configuration wizard opens (see Figure 4-65).

Figure 4-65 Confirmation



The following actions will be performed when you hit the 'Finish' button:

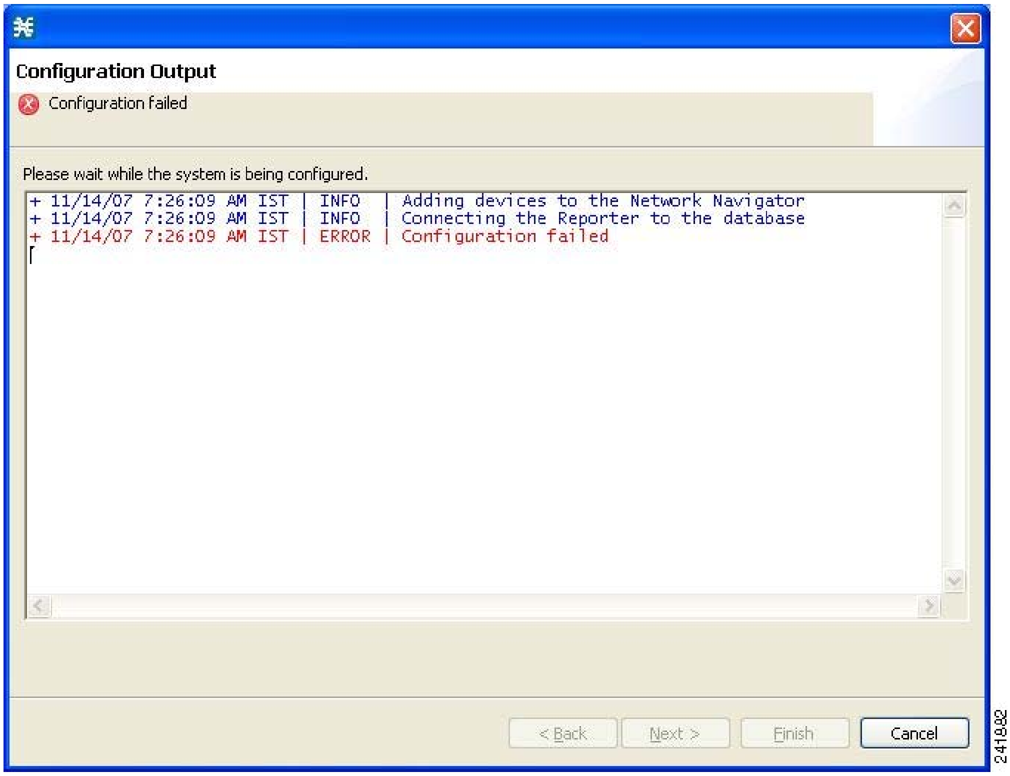
Connect the Reporter to the database 10.56.201.81
Verify that the database is connected and configured correctly

The actions that the wizard is about to take are listed on the page.

Step 8 Click **Finish**.

The Configuration Output page of the Reporter DB Configuration wizard opens (see Figure 4-66).

Figure 4-66 Configuration Output



Configuration Output

Configuration failed

Please wait while the system is being configured.

```
+ 11/14/07 7:26:09 AM IST | INFO  | Adding devices to the Network Navigator
+ 11/14/07 7:26:09 AM IST | INFO  | Connecting the Reporter to the database
+ 11/14/07 7:26:09 AM IST | ERROR | Configuration failed
```

The wizard attempts to connect the Cisco SCA BB Reporter tool to the selected database. The operation fails if the wizard cannot connect to the database.

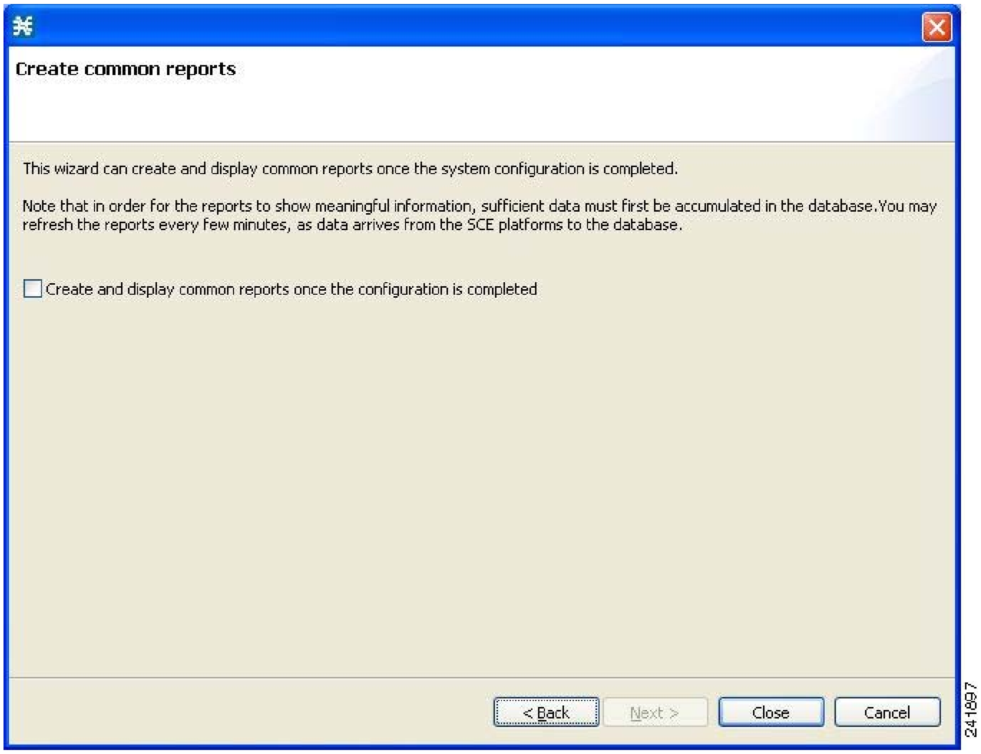
The database is queried for its service configuration data and the first SCE device in the response is chosen as the source of service configuration data.

The database device is added to the Site Manager tree in the Network Navigator.

Step 9 Click **Next**.

The Create common reports page of the Reporter DB Configuration wizard opens (see Figure 4-67).

Figure 4-67 Create Common Reports



Create common reports

This wizard can create and display common reports once the system configuration is completed.

Note that in order for the reports to show meaningful information, sufficient data must first be accumulated in the database.You may refresh the reports every few minutes, as data arrives from the SCE platforms to the database.

□ Create and display common reports once the configuration is completed

Step 10 To create reports, check the **Create and display common reports** check box.

Note Report instances are created for four predefined report types:

- Global Bandwidth per Service
- Global Active Subscribers per Service
- Top P2P Protocols
- Global Hourly Call Minutes per Service (VoIP)

Step 11 Click **Close**.

The wizard closes.

The Reporter tool opens in the Console.

Report instances of each of the four report types open in the Report View of the Reporter tool.

The Network Navigator Tool

The Network Navigator is a tool that allows you to create and manage a simple model of all local and remote devices that are part of the Cisco Service Control solution.

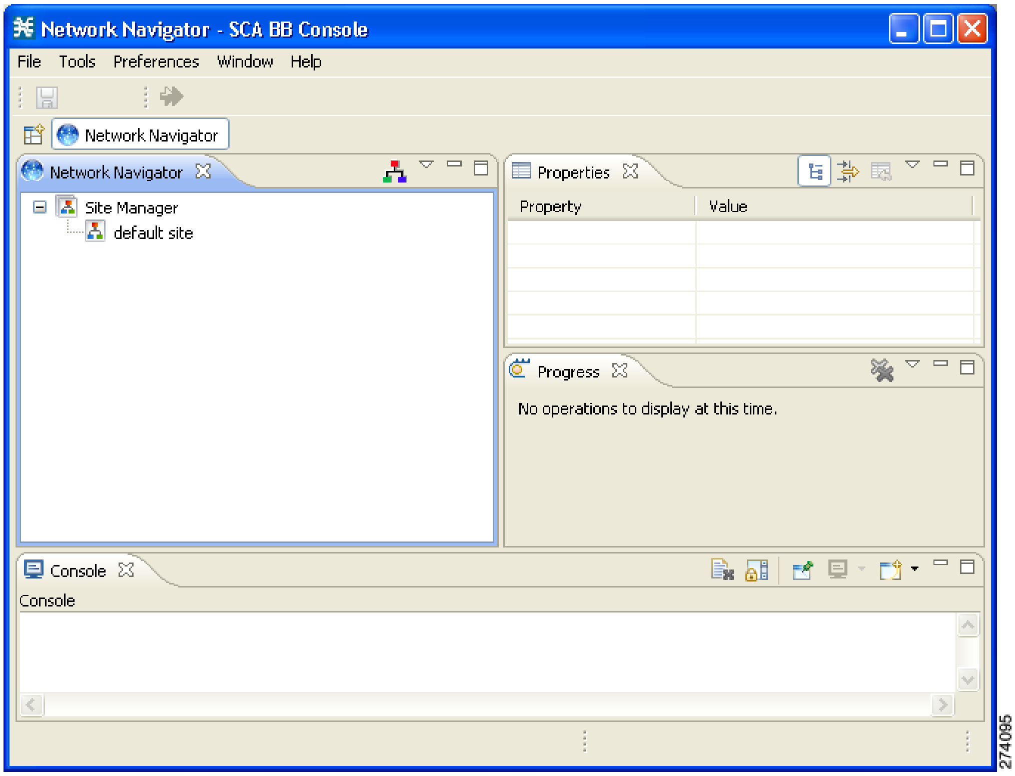
For more information about the Network Navigator, see Using the Network Navigator, page 5-1.

How to Open the Network Navigator Tool

Step 1 From the Console main menu, choose **Tools > Network Navigator**.

The Network Navigator tool opens (see Figure 4-68).

Figure 4-68 Network Navigator



How to Close the Network Navigator Tool

Step 1 Right-click the **Network Navigator** button.

Step 2 From the popup menu that appears, select **Close**.

The Network Navigator tool closes.

The Service Configuration Editor Tool

The Service Configuration Editor is a tool that allows you to create service configurations. A service configuration is a data structure that defines how the SCE platform analyses network traffic, what rules apply to the traffic, and what actions the SCE platform takes to enforce these rules.

Most of this document discusses using the Service Configuration Editor. See Using the Service Configuration Editor, page 6-1.

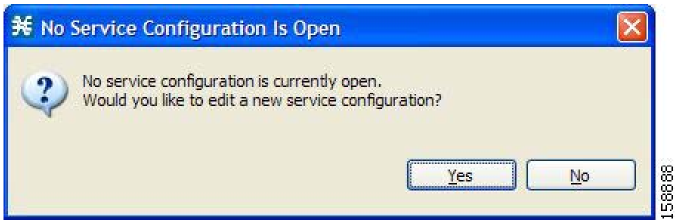
- How to Open the Service Configuration Editor Tool, page 4-73
- How to Close the Service Configuration Editor Tool, page 4-74

How to Open the Service Configuration Editor Tool

Step 1 From the Console main menu, choose **Tools > Service Configuration Editor**.

A No Service Configuration Is Open dialog box appears (see Figure 4-69).

Figure 4-69 No Service Configuration Is Open



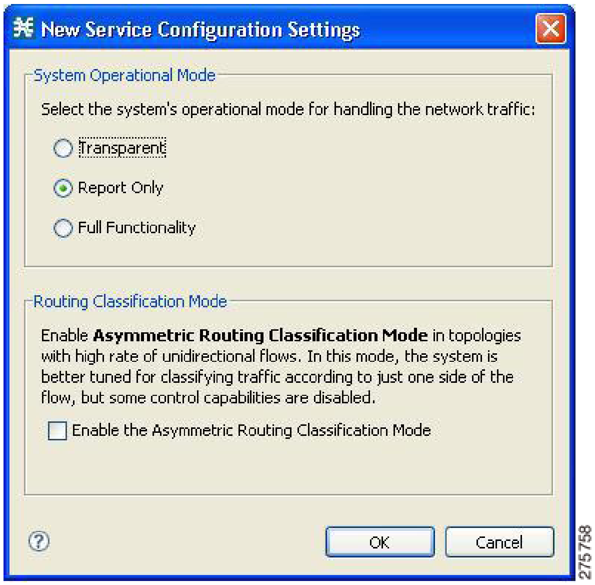
No Service Configuration Is Open

No service configuration is currently open.
Would you like to edit a new service configuration?

Step 2 Click **Yes**.

A New Service Configuration Settings dialog box appears (see Figure 4-70).

Figure 4-70 New Service Configuration Settings



New Service Configuration Settings

System Operational Mode

Select the system's operational mode for handling the network traffic:

○ Transparent
● Report Only
○ Full Functionality

Routing Classification Mode

Enable **Asymmetric Routing Classification Mode** in topologies with high rate of unidirectional flows. In this mode, the system is better tuned for classifying traffic according to just one side of the flow, but some control capabilities are disabled.

□ Enable the Asymmetric Routing Classification Mode

Step 3 Select one of the **System Operational Mode** radio buttons.

- **Transparent**—The system does not generate RDRs and does not enforce active rules on the network traffic.
- **Report only**—The system generates RDRs only. No active rule enforcement is performed on the network traffic.
- **Full functionality**—The system enforces active rules on the network traffic and performs reporting functions (that is, generates RDRs).

Note You can change the system operational mode at any time.

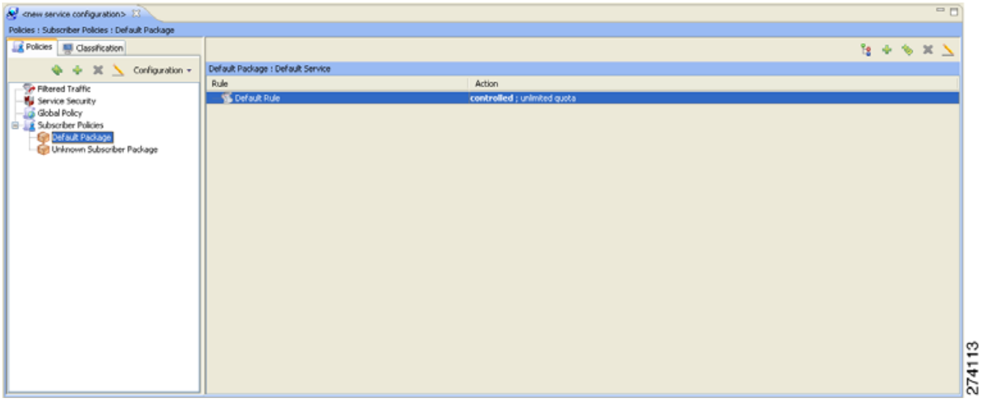
Step 4 (Optional, but highly recommended if your system has a high proportion of unidirectional flows) To switch to asymmetric routing classification mode, check the **Enable the Asymmetric Routing Classification Mode** check box.

Note It is recommended that you do not change the routing classification mode after creating a service configuration, as this causes loss of service configuration data. (See Asymmetric Routing Classification Mode, page 10-56.)

Step 5 Click **OK**.

A default service configuration opens in the Service Configuration Editor tool (see Figure 4-71).

Figure 4-71 Service Configuration Editor



<new service configuration>
Policies : Subscriber Policies : Default Package
Policies
Classification
Configuration
Filtered Traffic
Service Security
Global Policy
Subscriber Policies
Default Package
Unknown Subscriber Package
Default Package : Default Service
274113

Rule	Action
Default Rule	**controlled** ; unlimited quota

How to Close the Service Configuration Editor Tool

Step 1 Right-click the **Service Configuration Editor** button.

Step 2 From the popup menu that appears, select **Close**.

The Service Configuration Editor tool closes.

The Signature Editor Tool

The *Signature Editor* is a tool that allows you to create and modify files that can add and modify protocols and protocol signatures in Cisco SCA BB.

For more information about the Signature Editor, see Using the Signature Editor, page 13-1.

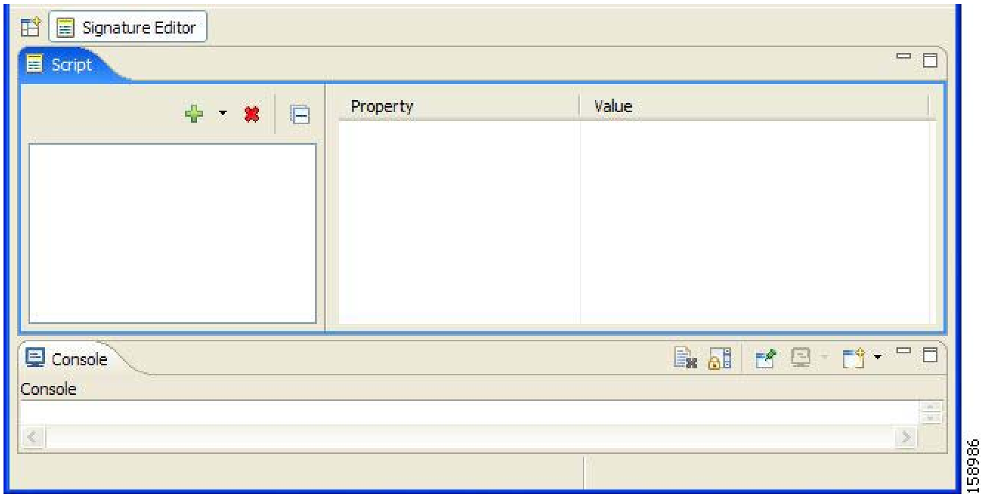
- How to Open the Signature Editor Tool, page 4-75
- How to Close the Signature Editor Tool, page 4-75

How to Open the Signature Editor Tool

Step 1 From the Console main menu, choose **Tools > Signature Editor**.

The Signature Editor tool opens (see Figure 4-72).

Figure 4-72 Signature Editor Tool



How to Close the Signature Editor Tool

Step 1 Right-click the **Signature Editor** button.

Step 2 From the popup menu that appears, select **Close**.

The Signature Editor tool closes.

The Subscriber Manager GUI Tool

The Subscriber Manager GUI is a tool that allows you to connect to an SCMS Subscriber Manager and then manage subscribers, assign packages to subscribers, edit subscriber parameters, and manually add subscribers.

For more information about connecting to an SCMS Subscriber Manager and using the Subscriber Manager GUI, see Using the Subscriber Manager GUI Tool, page 11-1.

For more information about the SCMS Subscriber Manager, see *Cisco Service Control Management Suite Subscriber Manager User Guide.*

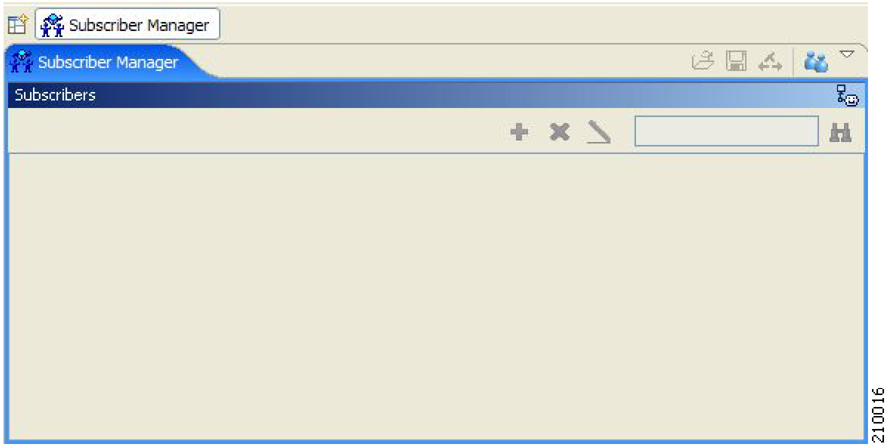
- How to Open the Subscriber Manager GUI Tool, page 4-76
- How to Close the Subscriber Manager GUI Tool, page 4-76

How to Open the Subscriber Manager GUI Tool

Step 1 From the Console main menu, choose **Tools > Subscriber Manager**.

The Subscriber Manager GUI tool opens (see Figure 4-73).

Figure 4-73 Subscriber Manager



How to Close the Subscriber Manager GUI Tool

Step 1 Right-click the **Subscriber Manager** button.

Step 2 From the popup menu that appears, select **Close**.

The Subscriber Manager GUI tool closes.

The Anonymous Group Manager Tool

The Anonymous Group Manager GUI allows you to manage anonymous groups within a SCE. You can create, edit, delete anonymous groups, and list all configured groups for a selected SCE. For a selected group, the GUI lists all anonymous subscribers that are part of the group.

For more information, see Using the Anonymous Group Manager Tool.

For more information about the SCMS Subscriber Manager, see the *Cisco Service Control Management Suite Subscriber Manager User Guide.*

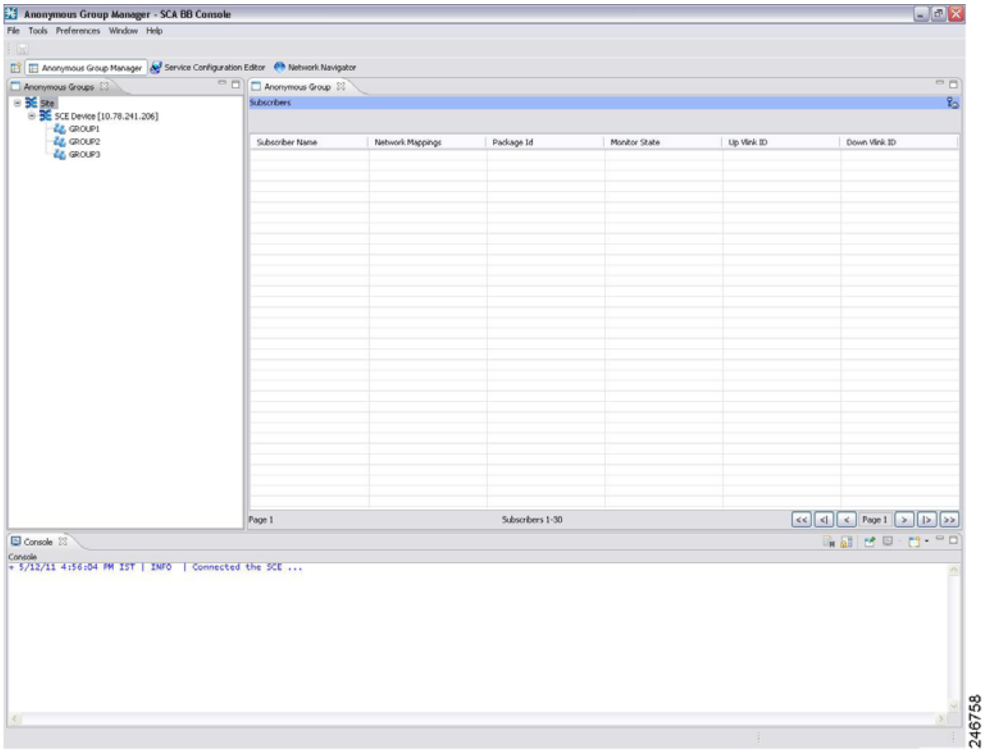
- How to Open the Anonymous Group Manager Tool, page 4-77
- How to Close the Anonymous Group Manager Tool, page 4-78

How to Open the Anonymous Group Manager Tool

Step 1 From the Console main menu, choose **Tools > Anonymous Group Manager**.

The Anonymous Group Manager tool opens (see Figure 4-74).

Figure 4-74 Anonymous Group Manager



Subscriber Name	Network Mappings	Package Id	Monitor State	Up Vlink ID	Down Vlink ID

```
+ 5/12/11 4:56:04 PM IST | INFO  | Connected the SCE ...
```

How to Close the Anonymous Group Manager Tool

Step 1 Right-click the **Anonymous Group Manager** button.

Step 2 From the popup menu that appears, select **Close**.

The Anonymous Group Manager tool closes.

The Reporter Tool

The Cisco Service Control Application (SCA) Reporter is a tool that allows you to query the Cisco Service Control Management Suite (SCMS) Collection Manager (CM) RDR database, and present the results in a chart or a table. This valuable tool helps you to understand the habits and resource consumption of the applications and subscribers that use your network. It also helps you evaluate the efficacy of various rules and the possible impact of their implementation on the network. You can view the reports in both tabular and chart formats, export them, save them, and edit their appearance.

You can run the SCA Reporter as a standalone or inside the Reporter tool in the Console.

Note From SCA Reporter, if you launch reports that retrieve large number of records (around 800,000 and above), the processing might take a considerable amount of time. There might be a delay in launch of the reports and the system might appear to be halted. In rare instances, the console may close. To avoid such issues, use the time range for the report query.

For more information about the SCA Reporter, see *Cisco Service Control Application Reporter User Guide.*

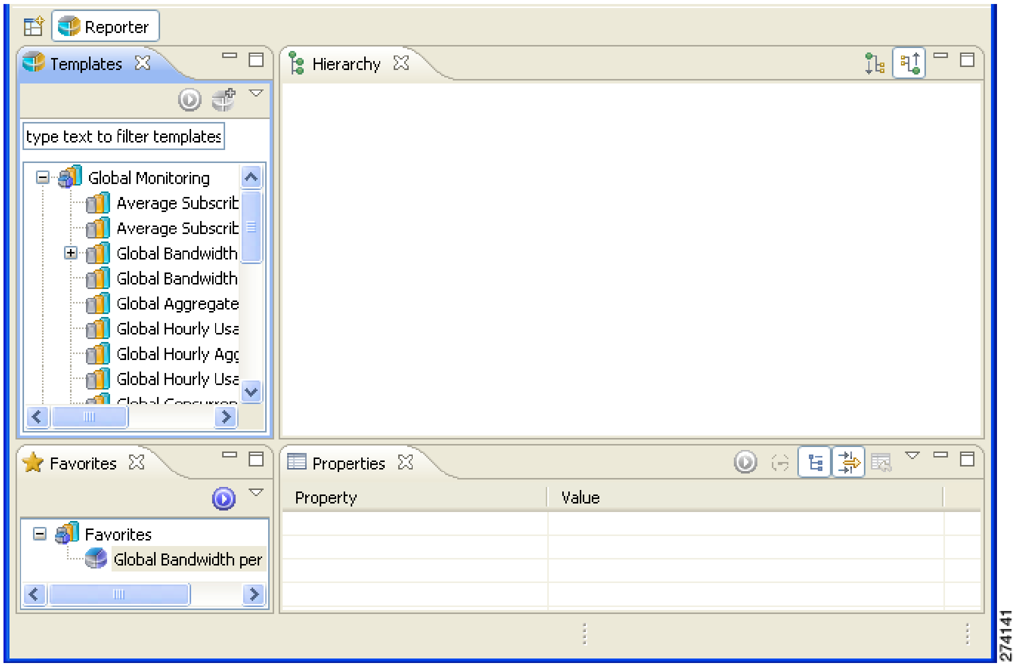
- How to Open the Reporter Tool, page 4-78
- How to Close the Reporter Tool, page 4-79

How to Open the Reporter Tool

Step 1 From the Console main menu, choose **Tools > Reporter**.

The Reporter tool opens (see Figure 4-75).

Figure 4-75 **Reporter**



Note You can use the SCA Reporter to generate reports only if the Console is connected to a database. (See How to Make Databases Accessible to the SCA Reporter, page 5-31.)

How to Close the Reporter Tool

Step 1 Right-click the **Reporter** button.

Step 2 From the popup menu that appears, select **Close**.

The Reporter tool closes.

Online Help

You can access relevant parts of this user guide from the Console.

- How to Access Online Help, page 4-80
- How to Search Online Help, page 4-81

How to Access Online Help

Step 1 From the Console main menu, choose **Help > Help Contents**.

Online help opens in a separate window.

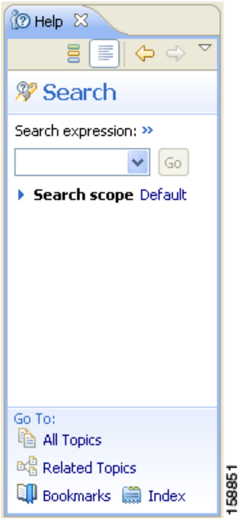
How to Search Online Help

You can also search online help from the current tool.

Step 1 From the Console main menu, choose **Help** > **Search**.

The Help view opens next to the current tool (see Figure 4-76).

Figure 4-76 Help



Step 2 Enter a word, phrase, or more complex search expression in the **Search expression** field.

The Go button is enabled.

Note Click >> (**Expand**) for an explanation of how to construct search expressions.

Step 3 Click **Go**.

Help topics containing your search expression are listed under Local Help.

Step 4 Click a help topic to view its contents.

Note You can bookmark topics for later reference.

Step 5 By clicking the appropriate link at the bottom of the Help view, you can switch to:

- All topics
- Related topics
- Bookmarks

QuickStart with the Console

This QuickStart section helps you get started with the Console. The section includes an example of using the Network Navigator tool and the Service Configuration Editor to apply the default service configuration to an SCE platform.

Example: How to Configure the Console and Apply the Default Service Configuration

In this example, you add an SCE device to the default site and apply the default service configuration to the SCE.

Step 1 Launch the Console.

Choose **Start > All Programs > Cisco SCA > SCA BB Console 3.7.0 > SCA BB Console 3.7.0**.

Step 2 If necessary, close the Welcome view.

Step 3 Open the Network Navigator.

From the Console main menu, choose **Tools > Network Navigator**.

This step sets up the Console for network device operations.

Note The Network Navigator tool is open the first time you launch the Console.

You should now be able to see the default site displayed in the Network Navigator view.

Step 4 Add an SCE device to the default site.

a. Right-click the default site, and, from the popup menu that appears, select **New > SCE**.

The Create new SCE wizard appears.

In the Address field, enter the actual IP address of an SCE platform.

b. Click **Finish**.

The Create new SCE wizard closes.

The new device is added to the site.

Step 5 Check the SCE platform version and operational state.

a. Right-click the SCE device and, from the popup menu that appears, select **Online Status**.

A Password Management dialog box appears.

b. Enter the username and password for managing the SCE.

c. Enter the SNMP RO Community String.

d. Click **Extract**.

The SCE online status is retrieved.

e. Check that the system and application versions are correct, and that the operational state is Active.

Step 6 Open the Service Configuration Editor.

- From the Console main menu, choose **Tools > Service Configuration Editor**.

  The Service Configuration Editor opens.

  A No Service Configuration Is Open dialog box appears.

Step 7 Create a new service configuration.

a. Click **Yes** in the No Editor Is Open dialog box.

A New Service Configuration Settings dialog box appears.

b. Click **OK**.

A default service configuration opens in the Service Configuration Editor tool.

Step 8 Apply the service configuration to the SCE platform.

a. From the toolbar, select the **Apply Service Configuration to SCE Devices** (⏩) icon.

A Password Management dialog box appears.

b. Enter the username and password for managing the SCE and click **Apply**.

The service configuration is applied to the SCE platform.

CHAPTER 5

Using the Network Navigator

Revised: August 08, 2013, OL-24178-09

Introduction

To manage a network entity—Service Control Engine (SCE) platform, Subscriber Manager (SM), or Collection Manager (CM)—from the Console, you must first define it as a device in the Network Navigator.

This chapter describes how to use the Network Navigator tool to create a model of all local and remote sites and devices that are part of the Cisco Service Control solution, how to manage the devices remotely, and other functionality that is part of the Network Navigator tool.

The Usage Analysis wizard, which can be used to create a simple model of devices and connect to them, is also described in this chapter.

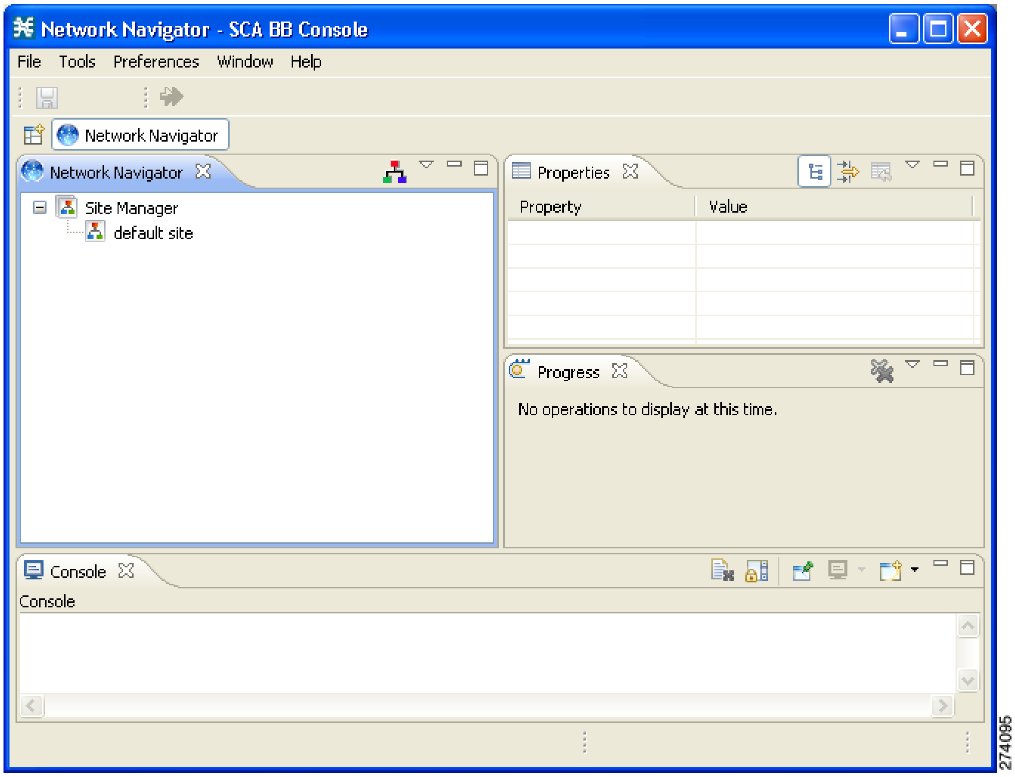
This chapter consists of these sections:

The Network Navigator Tool

The Network Navigator tool (Figure 5-1) contains four views:

- Network Navigator view—Displays all sites and devices that you have defined as part of your system, in the Site Manager tree.
- Properties view—Displays the editable properties of the node selected in the Site Manager tree in the Network Navigator view.
- Progress view—Displays a progress bar when you perform an operation on a site or device in the Site Manager tree.
- Console view—Displays log messages concerning actions performed in the Network Navigator tool.

Figure 5-1 The Network Navigator Tool



No operations to display at this time.

Managing Sites

You can manage an SCE, Subscriber Manager, or CM from the Console only if the network entity is defined as a device in the Network Navigator. After a device is added to the Network Navigator, you can perform management and monitoring operations on the device.

You can also perform operations on a group of devices. For example, you can apply the same service configuration to a group of SCE platforms. The Network Navigator allows you to group devices by adding them under the same site. A site is a group of devices that can be managed together. At installation, the Network Navigator contains a default site with no devices. You can add devices to this site or add additional sites, as described in the following sections.

Grouping devices in sites can also help to manage the passwords for these devices (see Password Management, page 5-8).

- How to Add a Site to the Site Manager, page 5-3
- How to Add Devices to a Site, page 5-4
- How to Delete Sites, page 5-7

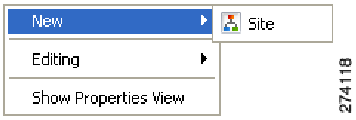
How to Add a Site to the Site Manager

Before adding devices, you must add your sites to the Site Manager. To add a device to a site, complete these steps:

Step 1 In the Network Navigator view, right-click the Site Manager node.

A popup menu appears (Figure 5-2).

Figure 5-2 Site Manager Menu



Step 2 From the menu, select **New > Site**.

A new Site node is added to the Site Manager.

Step 3 In the Properties view, enter a name for the site in the Name cell.

Step 4 (Optional) In the Version cell, enter a version number.

How to Add Devices to a Site

You can add SCE, Subscriber Manager, CM, or database devices to a site.

- How to Add SCE Devices to a Site, page 5-4
- How to Add Subscriber Manager Devices to a Site, page 5-4
- How to Add Collection Manager Devices to a Site, page 5-5
- How to Add Database Devices to a Site, page 5-6
- How to Delete Devices, page 5-7

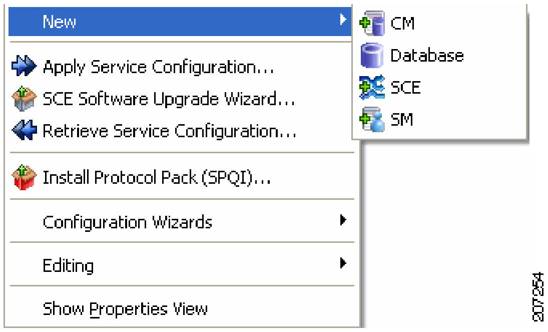
How to Add SCE Devices to a Site

To use the Network Navigator to configure, monitor, and update the software of an SCE platform, you must first add the SCE platform to a site.

Step 1 In the Site Manager tree, right-click a site.

A popup menu appears (Figure 5-3).

Figure 5-3 Site Manager Tree Menu


New
Apply Service Configuration...
SCE Software Upgrade Wizard...
Retrieve Service Configuration...
Install Protocol Pack (SPQI)...
Configuration Wizards
Editing
Show Properties View
CM
Database
SCE
SM
207254

Step 2 From the menu, select **New > SCE**.

The Create New SCE wizard appears.

Step 3 In the Address field, enter the IP address of the SCE.

Step 4 (Optional) In the Name field, enter a meaningful name for the SCE.

Step 5 Click **Finish**.

The Create New SCE wizard closes.

The new device is added to the site.

How to Add Subscriber Manager Devices to a Site

To use the Network Navigator to configure, monitor, and update the software of an Subscriber Manager, you must first add the Subscriber Manager to a site.

Step 1 In the Site Manager tree, right-click a site.

A popup menu appears.

Step 2 From the menu, select **New > SM**.

The Create New SM wizard appears.

Step 3 In the Address field, enter the IP address of the SCMS Subscriber Manager.

Step 4 (Optional) In the Name field, enter a meaningful name for the Subscriber Manager.

Step 5 Click **Finish**.

The Create New SM wizard closes.

The new device is added to the site.

How to Add Collection Manager Devices to a Site

To use the Network Navigator to monitor a Collection Manager, you must first add the Collection Manager to a site.

Step 1 In the Site Manager tree, right-click a site.

A popup menu appears.

Step 2 From the menu, select **New > CM**.

The Create New CM wizard appears.

Step 3 In the Address field, enter the IP address of the Collection Manager.

Step 4 (Optional) In the Name field, enter a meaningful name for the Collection Manager.

Step 5 Click **Finish**.

The Create New CM wizard closes.

The new device is added to the site.

How to Add Database Devices to a Site

To use the Reporter tool to produce reports, you must first connect to a database.

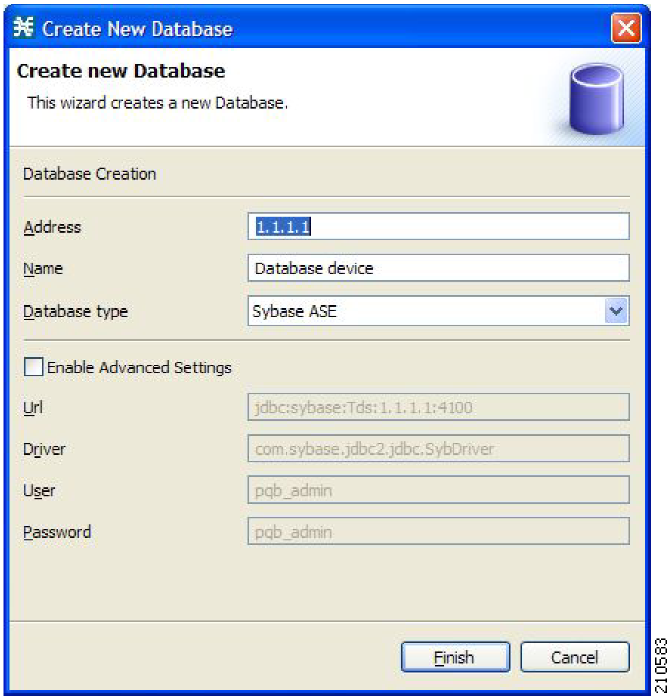
Step 1 In the Site Manager tree, right-click a site.

A popup menu appears.

Step 2 From the menu, select **New > Database**.

The Create New Database wizard appears (Figure 5-4).

Figure 5-4 Create New Database



Create New Database

Create new Database

This wizard creates a new Database.

Database Creation

Address: 1.1.1.1

Name: Database device

Database type: Sybase ASE

□ Enable Advanced Settings

Url: jdbc:sybase:Tds:1.1.1.1:4100

Driver: com.sybase.jdbc2.jdbc.SybDriver

User: pqb_admin

Password: pqb_admin

Step 3 In the Address field, enter the IP address of the database.

Step 4 (Optional) In the Name field, enter a meaningful name for the database.

Step 5 From the Database type drop-down list, select a database type.

Step 6 (Optional) Check the **Enable Advanced Settings** check box and enter new values in the Url, Driver, User, and Password fields.

Step 7 Click **Finish**.

The Create New Database wizard closes.

The new device is added to the site.

How to Delete Devices

Step 1 In the Site Manager tree, right-click a device.

A popup menu appears.

Step 2 From the menu, select **Delete**.

The device is deleted and removed from the Site Manager tree.

How to Delete Sites

Step 1 In the Site Manager tree, right-click a site in the Site Manager tree.

A popup menu appears.

- Enter your password if prompted.

Step 2 From the menu, select **Delete**.

The site and all its devices are deleted and the site is removed from the Site Manager tree.

Managing Devices

The Network Navigator allows you to manage SCE, Subscriber Manager, CM, and database devices.

Note The Usage Analysis wizard allows you to create a simple model of devices and connect to them. (See How to Use the Usage Analysis Wizard, page 4-38.)

- Password Management, page 5-8
- Managing SCE Devices, page 5-9
- Managing Subscriber Manager Devices, page 5-27
- Managing Collection Manager Devices, page 5-30
- Managing Database Devices, page 5-31

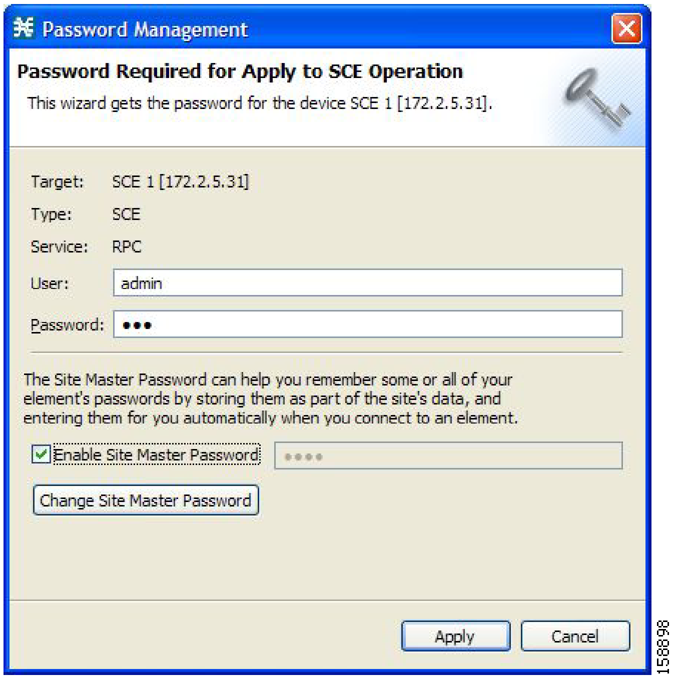
Password Management

Normally, before you can access a device (SCE, Subscriber Manager, CM, or database), you must enter its password. When you try to perform any operation on a site device, the Network Navigator first asks for the device username and password. (Repeating the same operation on the same device does not always require a second entry of the password.)

When performing operations on multiple devices, password entry can become tedious. The Site Master Password can help you remember some or all usernames and passwords of your element by storing them as part of the site data, and entering them for you automatically when you connect to an element.

The Site Master Password protects saved usernames and passwords in the password manager. The Password Management dialog box (Figure 5-5) prompts you for the master password of the site when you wish to activate the site password manager. If you have multiple sites, each site requires a separate master password.

Figure 5-5 The Password Management Dialog Box



Password Management

Password Required for Apply to SCE Operation

This wizard gets the password for the device SCE 1 [172.2.5.31].

Target: SCE 1 [172.2.5.31]

Type: SCE

Service: RPC

User: admin

Password: •••

The Site Master Password can help you remember some or all of your element's passwords by storing them as part of the site's data, and entering them for you automatically when you connect to an element.

☑ Enable Site Master Password ••••

For each site, when the Password Management dialog box appears, check the **Enable Site Master Password** check box.

Managing SCE Devices

- How to Configure SCE and CM Devices Using a Wizard, page 5-10
- How to Generate Tech Support Info Files for SCE Devices, page 5-17
- How to Retrieve the Online Status of SCE Devices, page 5-19
- How to Install a Protocol Pack, page 5-20
- How to Apply Service Configurations to SCE Devices, page 5-22
- How to Retrieve Service Configurations from SCE Devices, page 5-24
- How to Install PQI Files on SCE Devices, page 5-25
- How to Install an SCE OS Software Package on SCE Devices, page 5-26

How to Configure SCE and CM Devices Using a Wizard

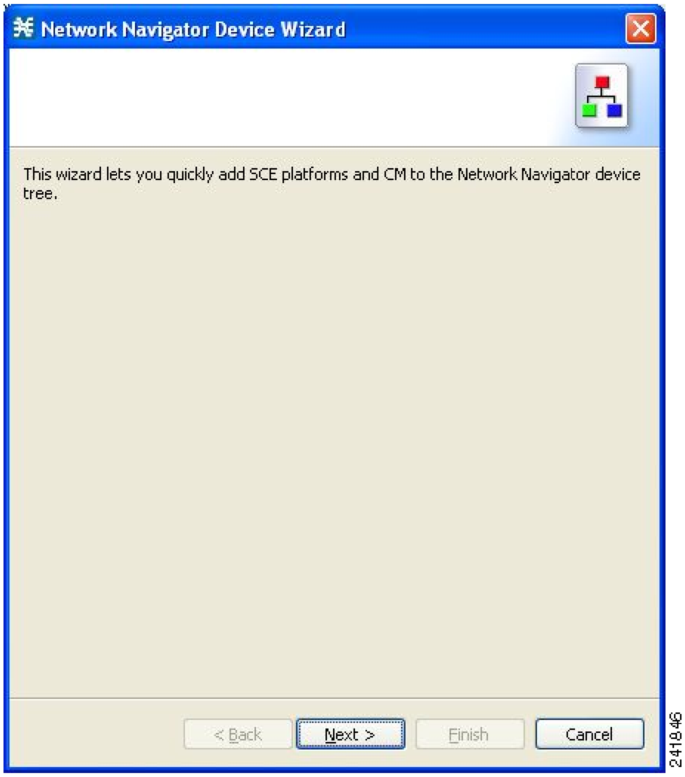
The Network Navigator Device wizard allows you to configure SCA and CM devices and connect to them.

Note If they do not exist, devices defined in the wizard are added to the default site in the Site Manager tree.

Step 1 In the Network Navigator view toolbar, click the **Configure SCE and CM devices** ( ) icon.

The Welcome window of the Network Navigator Device wizard appears (Figure 5-6).

Figure 5-6 Welcome - Network Navigator Device

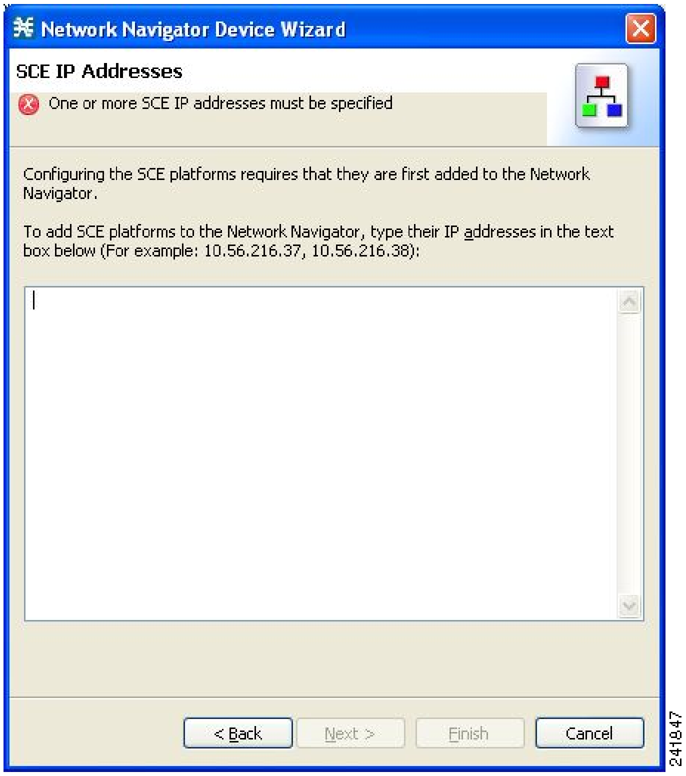


This wizard lets you quickly add SCE platforms and CM to the Network Navigator device tree.

Step 2 Click **Next**.

The SCE IP Addresses page of the Network Navigator Device wizard opens (Figure 5-7).

Figure 5-7 SCE IP Addresses



Network Navigator Device Wizard

SCE IP Addresses

One or more SCE IP addresses must be specified

Configuring the SCE platforms requires that they are first added to the Network Navigator.

To add SCE platforms to the Network Navigator, type their IP addresses in the text box below (For example: 10.56.216.37, 10.56.216.38):

Step 3 In the edit box, enter the IP addresses of the SCE devices that should be added to the model.

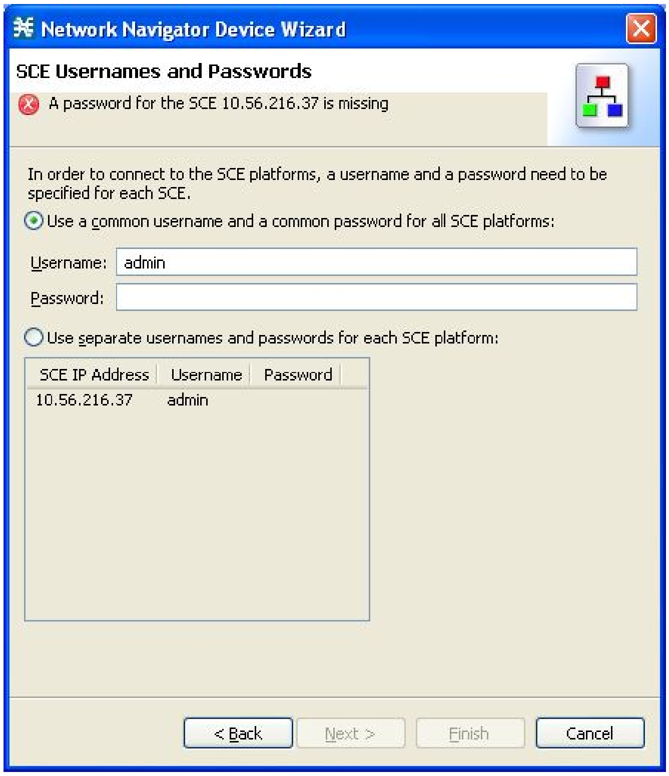
If you started from the Network Navigator, the IP addresses of the SCE devices that you selected are displayed in the edit box. You can add additional addresses.

Note You can work with up to 20 SCE devices at one time using the wizard.

Step 4 Click **Next**.

The SCE Usernames and Passwords page of the Network Navigator Device wizard opens (Figure 5-8).

Figure 5-8 SCE Usernames and Passwords



Network Navigator Device Wizard

SCE Usernames and Passwords

A password for the SCE 10.56.216.37 is missing

In order to connect to the SCE platforms, a username and a password need to be specified for each SCE.

● Use a common username and a common password for all SCE platforms:

Username: admin

Password:

○ Use separate usernames and passwords for each SCE platform:

SCE IP Address	Username	Password
10.56.216.37	admin	

Step 5 Enter the usernames and passwords for the SCE devices.

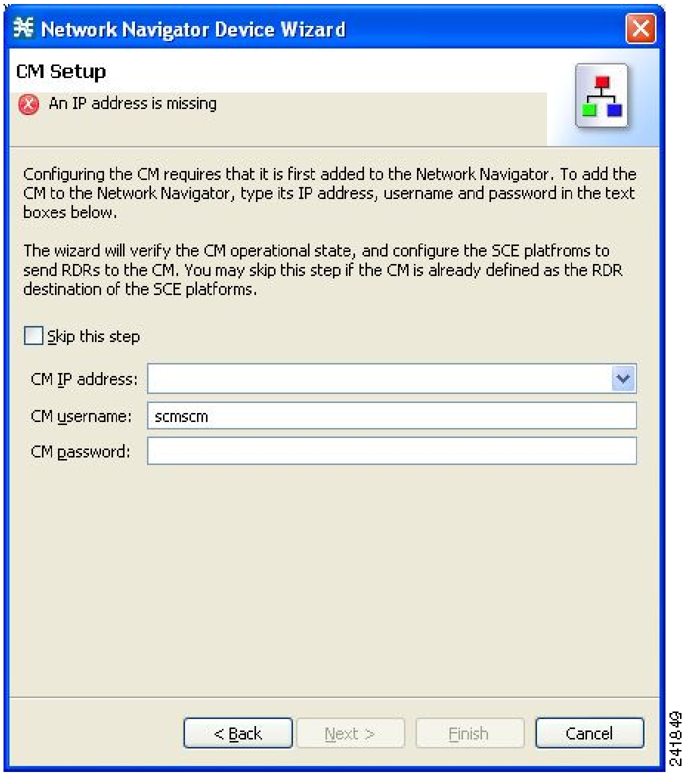
Do one of the following:

- To use the same username and password for all the SCE devices that you are adding, enter the username in the Username field and the password in the Password field.
- To provide a different username and password pair for each SCE device, check the **Use separate usernames and passwords for each SCE device** radio button, and, for each SCE device, enter the username and password in the appropriate cell of the SCE device table.

Step 6 Click **Next**.

The CM Setup page of the Network Navigator Device wizard opens (Figure 5-9).

Figure 5-9 CM Setup



Network Navigator Device Wizard

CM Setup

An IP address is missing

Configuring the CM requires that it is first added to the Network Navigator. To add the CM to the Network Navigator, type its IP address, username and password in the text boxes below.

The wizard will verify the CM operational state, and configure the SCE platfroms to send RDRs to the CM. You may skip this step if the CM is already defined as the RDR destination of the SCE platforms.

☐ Skip this step

CM IP address:

CM username: scmscm

CM password:

Step 7 Define the SCMS Collection Manager to use with this configuration.

Do one of the following:

- Enter the IP address, username, and password of the CM device in the appropriate fields.

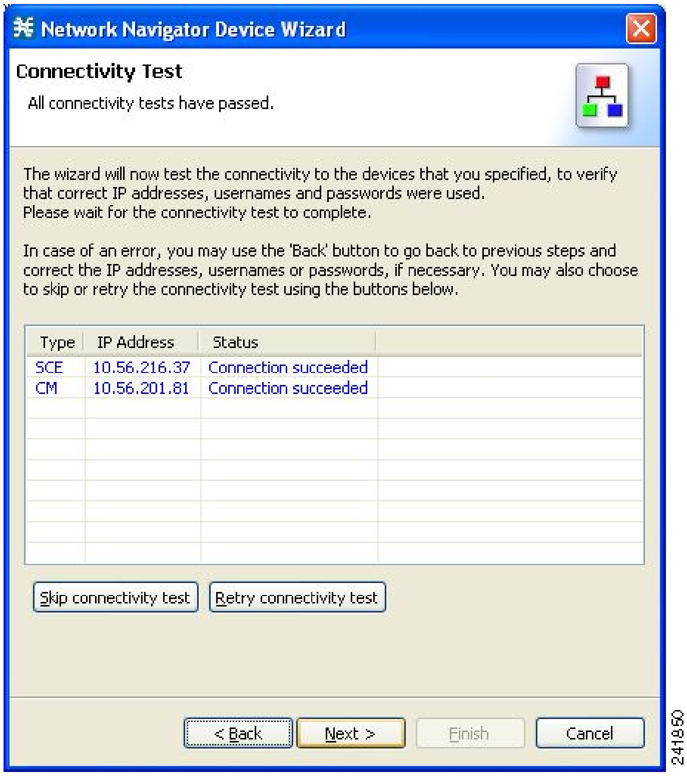
  If you started from the Network Navigator, this information is retrieved and displayed. You can modify these parameters.

- Check the **Skip this step** check box.

Step 8 Click **Next**.

The Connectivity Test page of the Network Navigator Device wizard opens (Figure 5-10).

Figure 5-10 Connectivity Test



Network Navigator Device Wizard

Connectivity Test

All connectivity tests have passed.

The wizard will now test the connectivity to the devices that you specified, to verify that correct IP addresses, usernames and passwords were used.
Please wait for the connectivity test to complete.

In case of an error, you may use the 'Back' button to go back to previous steps and correct the IP addresses, usernames or passwords, if necessary. You may also choose to skip or retry the connectivity test using the buttons below.

Type	IP Address	Status
SCE	10.56.216.37	Connection succeeded
CM	10.56.201.81	Connection succeeded

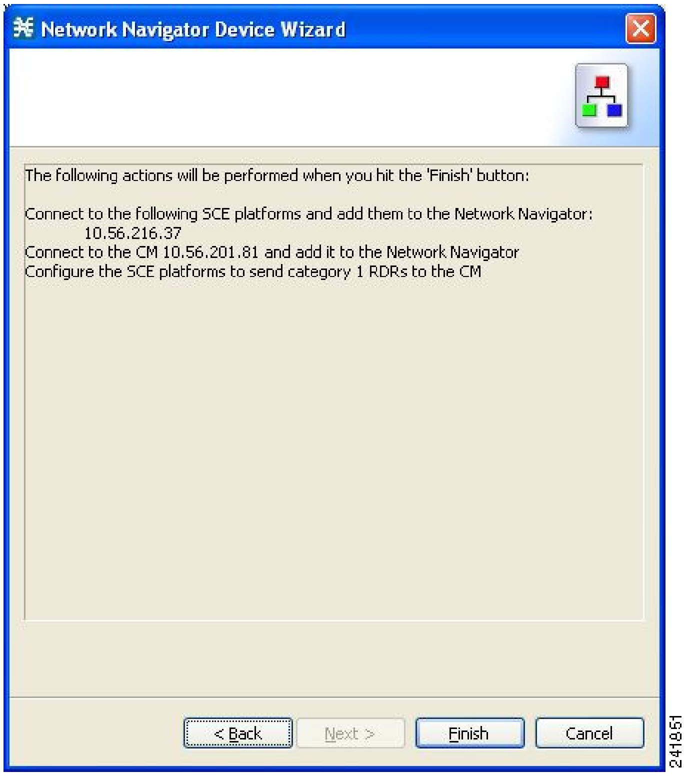
The wizard tests to see that the connections to the defined devices can be made.

Note If a connection to one or more of the devices cannot be made or if there is some problem with the connection (such as invalid version of the device) an error is displayed next to the device. You can skip these tests by clicking **Skip Connections**. The connections are validated when you click **Finish** at the end of the wizard.

Step 9 Click **Next**.

The Confirmation page of the Network Navigator Device wizard opens (Figure 5-11).

Figure 5-11 Confirmation



The following actions will be performed when you hit the 'Finish' button:

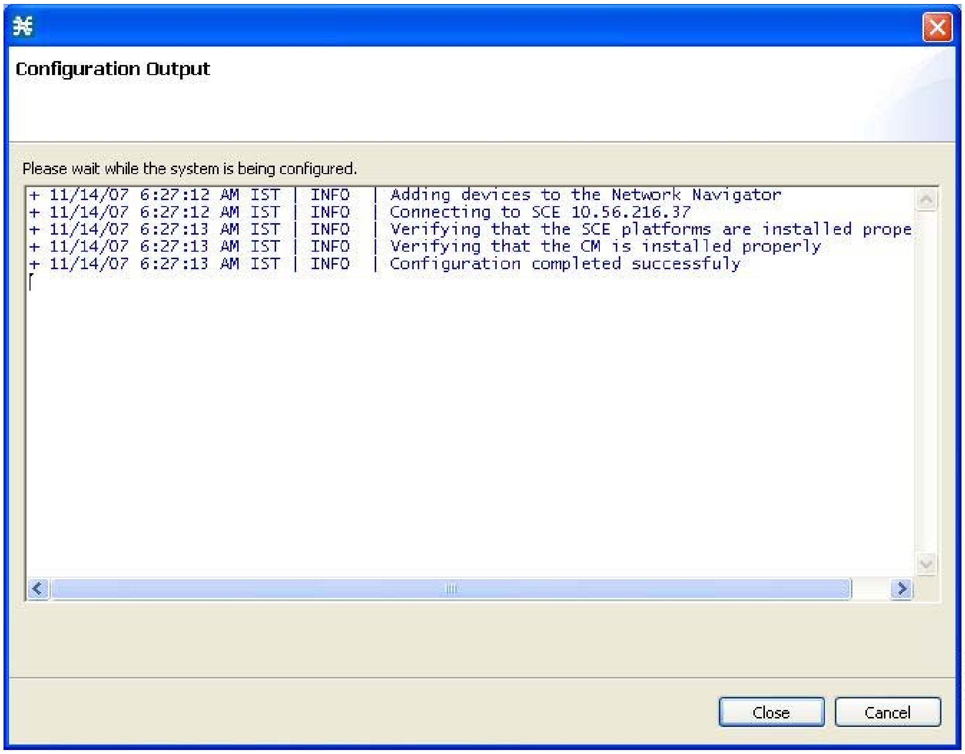
Connect to the following SCE platforms and add them to the Network Navigator:
10.56.216.37
Connect to the CM 10.56.201.81 and add it to the Network Navigator
Configure the SCE platforms to send category 1 RDRs to the CM

The actions that the wizard is about to take are listed on the page.

Step 10 Click **Finish**.

The Configuration Output page of the Network Navigator Device wizard opens (Figure 5-12).

Figure 5-12 Configuration Output



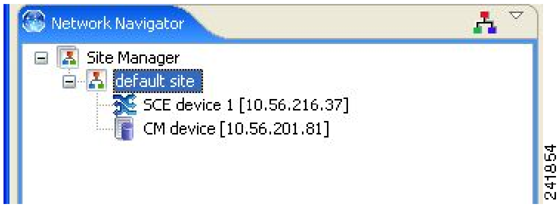
Configuration Output

Please wait while the system is being configured.

```
+ 11/14/07 6:27:12 AM IST | INFO  | Adding devices to the Network Navigator
+ 11/14/07 6:27:12 AM IST | INFO  | Connecting to SCE 10.56.216.37
+ 11/14/07 6:27:13 AM IST | INFO  | Verifying that the SCE platforms are installed prope
+ 11/14/07 6:27:13 AM IST | INFO  | Verifying that the CM is installed properly
+ 11/14/07 6:27:13 AM IST | INFO  | Configuration completed successfuly
```

New devices are added to the default site in the Site Manager tree in the Network Navigator (Figure 5-13).

Figure 5-13 Network Navigator



The wizard attempts to connect to all devices that you defined. The operation fails if:

- The wizard cannot connect to any of the SCE devices that you listed in Step 3.
- You defined a CM in Step 7, but the wizard cannot connect to it.

If you defined a CM in Step 7, the SCE devices are configured so that the only category 1 RDR destination is the CM.

Note RDR categories are the mechanism by which different types of RDRs can be sent to different collectors. For more information about RDR categories, see either the “Raw Data Formatting: The RDR Formatter and NetFlow Exporting” chapter of *Cisco SCE8000 10GBE Software Configuration Guide or the* “Raw Data Formatting: The RDR Formatter and NetFlow Exporting” chapter of *Cisco SCE8000 GBE Software Configuration Guide.*

A new service configuration is created:

- Report Only mode.
- The maximum Transaction RDR rate is set as the default value (250) divided by the number of SCE devices. (To configure the Transaction RDR, see How to Manage Transaction RDRs, page 8-6; the content and structure of the Transaction RDR is listed in the “Transaction RDR” section in the “Raw Data Records: Formats and Field Contents” chapter of *Cisco Service Control Application for Broadband Reference Guide.)*

Step 11 Click **Finish**.

The Network Navigator Device wizard closes.

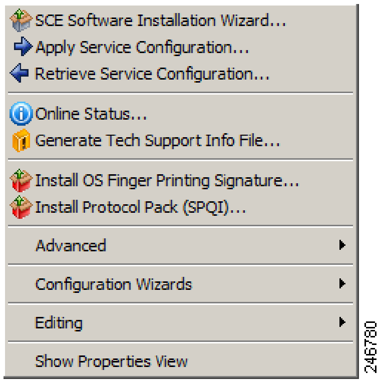
How to Generate Tech Support Info Files for SCE Devices

This operation generates the support file, for the SCE platform, for the use of Cisco technical support staff.

Step 1 In the Site Manager tree, right-click an SCE device.

A popup menu appears (Figure 5-14).

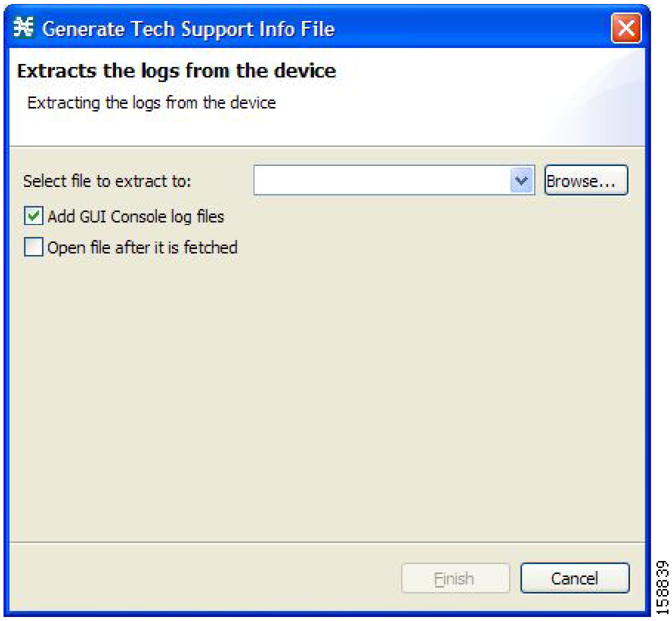
Figure 5-14 Site Manager Tree Menu


SCE Software Installation Wizard...
Apply Service Configuration...
Retrieve Service Configuration...
Online Status...
Generate Tech Support Info File...
Install OS Finger Printing Signature...
Install Protocol Pack (SPQI)...
Advanced
Configuration Wizards
Editing
Show Properties View
246780

Step 2 From the menu, select **Generate Tech Support Info File**.

The Generate Tech Support Info File dialog box appears (Figure 5-15).

Figure 5-15 Generate Tech Support Info File



Generate Tech Support Info File

Extracts the logs from the device

Extracting the logs from the device

Select file to extract to:

☑ Add GUI Console log files

□ Open file after it is fetched

Step 3 Click **Browse**.

A Select File dialog box appears.

Step 4 Browse to the folder where you want to save the tech support info file.

Step 5 In the File name field, enter a new file name, or select an existing ZIP file.

Step 6 Click **Open** to select the file.

If the file exists, it is overwritten when you generate the tech support info.

The Select File dialog box closes.

Step 7 (Optional) To add log files to the output tech support info file, check the **Add GUI Console log files** check box.

Step 8 (Optional) Check the **Open file after it is fetched** check box.

Step 9 Click **Finish**.

The Generate Tech Support Info File dialog box closes.

A Password Management dialog box appears.

Step 10 Enter the appropriate password. (For more information, see Password Management, page 5-8.)

Step 11 Click **Generate**.

The Password Management dialog box closes.

A Generate tech support info file progress bar appears.

The file is generated.

How to Retrieve the Online Status of SCE Devices

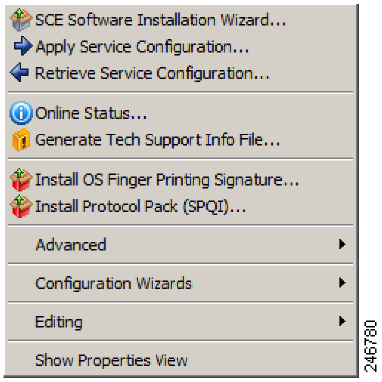
This operation provides information about the current software version and operational status of the SCE platform. The enhanced SCE online statuses are categorized as:

- System—displays the platform information
- Configuration—displays the Hostname
- Status—displays the operational mode and total traffic on the SCE

For more information on monitoring SCE online status, see *Cisco SCA BB Demo Kit Quick Start Guide.*

Step 1 In the Site Manager tree, right-click an SCE device.

A popup menu appears.


SCE Software Installation Wizard...
Apply Service Configuration...
Retrieve Service Configuration...
Online Status...
Generate Tech Support Info File...
Install OS Finger Printing Signature...
Install Protocol Pack (SPQI)...
Advanced
Configuration Wizards
Editing
Show Properties View
246780

Step 2 From the menu, select **Online Status**.

A Password Management dialog box appears.

Step 3 Enter the appropriate password. (For more information, see Password Management, page 5-8.)

Step 4 Enter the SNMP RO Community String.

If SNMP is not already enabled on the SCE, it gets enabled.

If RO communities are not configured on the SCE or if only RW communities are configured on the SCE, the SNMP RO community you provide here is added to the SCE.

If only RO communities are configured on the SCE, the SNMP RO community you provide here is validated first against the RO communities configured on SCE. If the RO community is valid, the online status window is launched. If the RO community is not valid, a validation message appears.

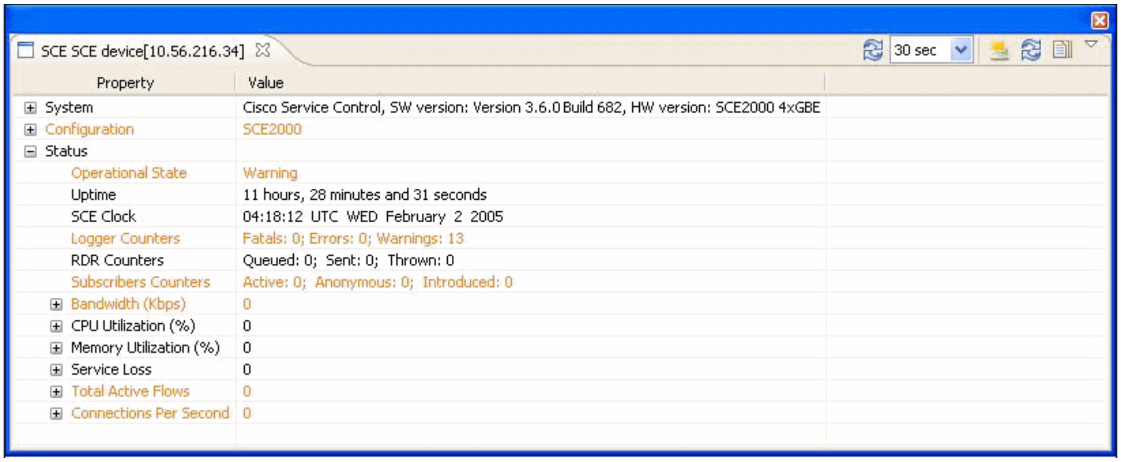
Step 5 Click **Extract**.

The Password Management dialog box closes.

An Extracting info progress bar appears.

The SCE online status is retrieved (Figure 5-16).

Figure 5-16 SCE Online Status



SCE SCE device[10.56.216.34]

30 sec

Property	Value
⊞ System	Cisco Service Control, SW version: Version 3.6.0 Build 682, HW version: SCE2000 4xGBE
⊞ Configuration	SCE2000
⊟ Status	
Operational State	Warning
Uptime	11 hours, 28 minutes and 31 seconds
SCE Clock	04:18:12 UTC WED February 2 2005
Logger Counters	Fatals: 0; Errors: 0; Warnings: 13
RDR Counters	Queued: 0; Sent: 0; Thrown: 0
Subscribers Counters	Active: 0; Anonymous: 0; Introduced: 0
⊞ Bandwidth (Kbps)	0
⊞ CPU Utilization (%)	0
⊞ Memory Utilization (%)	0
⊞ Service Loss	0
⊞ Total Active Flows	0
⊞ Connections Per Second	0

207261

How to Install a Protocol Pack

You can install a protocol pack on a single SCE platform, on selected SCE platforms, or on all SCE platforms at one or more selected sites. For more information about protocol packs, see Working with Protocol Packs, page 4-20.

Note Cisco recommends the use of SCE Software Upgrade wizard when installing a protocol pack on multiple SCE platforms.

- How to Install a Protocol Pack on a Single SCE Platform, page 5-20
- How to Install a Protocol Pack on Multiple SCE Platforms, page 5-21

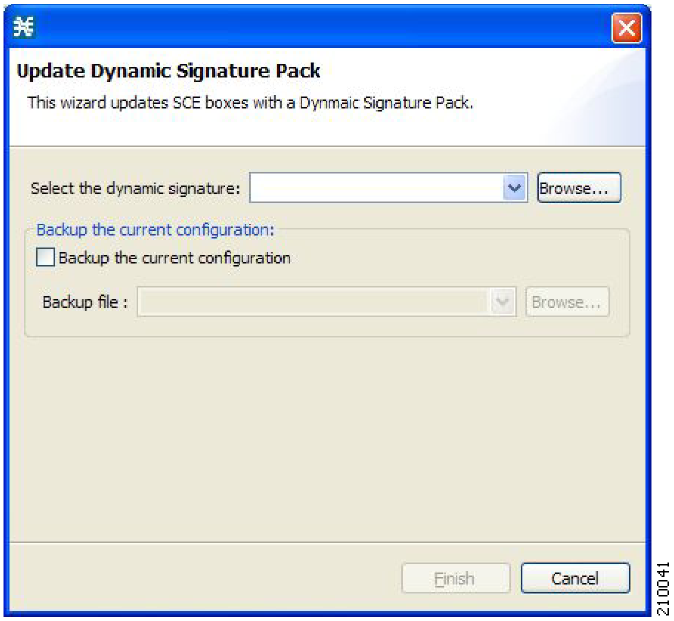
How to Install a Protocol Pack on a Single SCE Platform

Step 1 In the Site Manager tree, right-click the SCE on which you plan to install the protocol pack.

Step 2 From the popup menu that appears, select **Update Dynamic Signature Pack**.

The Update Dynamic Signature Pack dialog box appears (Figure 5-17).

Figure 5-17 Update Dynamic Signature Pack



Update Dynamic Signature Pack

This wizard updates SCE boxes with a Dynmaic Signature Pack.

Select the dynamic signature:

Backup the current configuration:

□ Backup the current configuration

Backup file :

Step 3 Click **Browse**.

A Select file dialog box appears.

Step 4 From the Files of type drop-down list, select ***.spqi** or ***.dss**, depending on the file to be installed.

Step 5 Browse to the file to be installed.

Step 6 Click **Open**.

The Select file dialog box closes.

Step 7 (Recommended) Check the **Backup the current configuration** check box, click **Browse**, and select a backup file.

Step 8 Click **Finish**.

A Password Management dialog box appears.

Step 9 Enter the appropriate password.

For more information, see Password Management, page 5-8.

Step 10 Click **Update**.

The Password Management dialog box closes.

An Update Dynamic Signature Pack progress bar appears.

The service configuration on the SCE platform is updated.

How to Install a Protocol Pack on Multiple SCE Platforms

You can install a protocol pack on multiple SCE Platforms using the SCE Software Upgrade wizard. See How to Upgrade the SCE Using the SCE Software Upgrade Wizard, page 4-8.

How to Apply Service Configurations to SCE Devices

You can apply a service configuration to a single SCE platform, to selected SCE platforms, or to all SCE platforms at one or more selected sites.

Note The service configuration that you are applying must be open in the Service Configuration Editor.

Caution If anomaly-based detection of malicious traffic is enabled, any access control list (ACL) that is configured on the Service Control Engine (SCE) platform but is not applied to anything (for example, an interface, an access map, or an SNMP community string) might be deleted when a service configuration is applied to the platform.

Workaround:
Disable anomaly-based detection of malicious traffic.
In the Network Traffic tab, select **Service Security**.
In the Service Security Dashboard, clear the **Enable anomaly detection** check box.

- How to Apply a Service Configuration to a Single SCE Platform, page 5-23
- How to Apply a Service Configuration to Multiple SCE Platforms, page 5-24

How to Apply a Service Configuration to a Single SCE Platform

Step 1 In the Site Manager tree, right-click an SCE device.

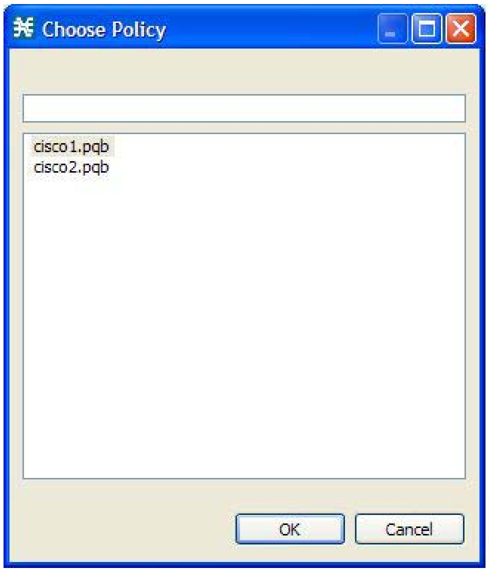
A popup menu appears.

Step 2 From the menu, select **Apply Service Configuration**.

The Choose Policy dialog box appears (Figure 5-18), listing all service configurations that are open in the Service Configuration Editor.

Note If only one service configuration is open in the Service Configuration Editor, a Password Management dialog box appears. Continue at Step 5. (If no service configurations are open in the Service Configuration Editor, an error message is displayed.)

Figure 5-18 Choose Policy


Choose Policy

cisco1.pqb
cisco2.pqb

Step 3 Select a service configuration from the list.

Step 4 Click **OK**.

A Password Management dialog box appears.

Step 5 Enter the appropriate password. (For more information, see Password Management, page 5-8.)

Step 6 Click **Apply**.

The Password Management dialog box closes.

An Applying service configuration to SCE progress bar appears.

The service configuration is applied to the selected SCE platform.

How to Apply a Service Configuration to Multiple SCE Platforms

Step 1 In the Site Manager tree, select sites or SCE devices to which you are applying the service configuration and right-click one of them.

Step 2 From the popup menu that appears, select **Apply Service Configuration**.

The Choose Policy dialog box appears, listing all service configurations that are open in the Service Configuration Editor.

Note If only one service configuration is open in the Service Configuration Editor, a Password Management dialog box appears. Continue at Step 4. (If no service configurations are open in the Service Configuration Editor, an error message is displayed.)

Step 3 Select a service configuration from the list and click **OK**.

A separate Password Management dialog box appears for each SCE device that you have selected.

Step 4 For each SCE device, enter the password and click **Apply**.

The service configuration is applied to each selected SCE platform in turn.

How to Retrieve Service Configurations from SCE Devices

You can retrieve service configurations from a single SCE platform, from selected SCE platforms, or from all SCE platforms at one or more selected sites.

- How to Retrieve Service Configurations from a Single SCE Platform, page 5-24
- How to Retrieve Service Configurations from Multiple SCE Platforms, page 5-25

How to Retrieve Service Configurations from a Single SCE Platform

Step 1 In the Site Manager tree, right-click an SCE device.

A popup menu appears.

- Enter your password if prompted.

Step 2 From the menu, select **Retrieve Service Configuration**.

A Password Management dialog box appears.

Step 3 Enter the appropriate password. (For more information, see Password Management, page 5-8.)

Step 4 Click **Retrieve**.

The Password Management dialog box closes.

A Retrieving from SCE progress bar appears.

The service configuration is retrieved from the SCE platform and opened in the Service Configuration Editor.

How to Retrieve Service Configurations from Multiple SCE Platforms

Step 1 In the Site Manager tree, select sites or SCE devices whose service configurations you want to retrieve, and right-click one of them.

Step 2 From the popup menu that appears, select **Retrieve Service Configuration**.

A separate Password Management dialog box appears for each SCE device that you have selected.

Step 3 For each SCE device, enter the password and click **Retrieve**.

The service configuration is retrieved from each SCE platform in turn, and is opened in the Service Configuration Editor.

How to Install PQI Files on SCE Devices

This operation installs the Cisco SCA BB on the SCE platform.

Note It is recommended to use the SCE Software Upgrade wizard when installing a PQI file on multiple SCE devices. See How to Upgrade the SCE Using the SCE Software Upgrade Wizard, page 4-8.

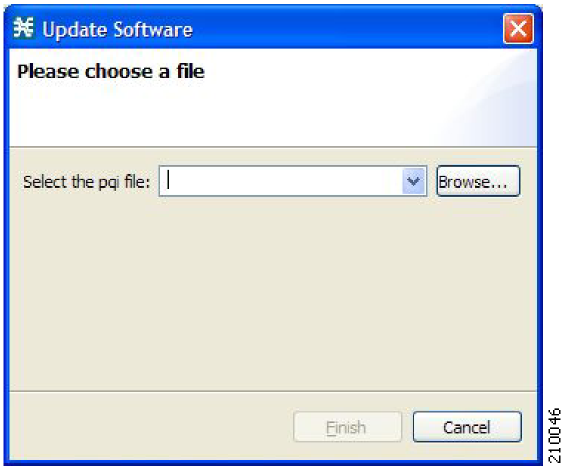
Note Installing a PQI file usually takes a few minutes.

Step 1 In the Site Manager tree, select an SCE device.

Step 2 From the Console main menu, choose **Network > Install Application Software (PQI)**.

The Update Software dialog box appears (Figure 5-19).

Figure 5-19 Update Software



Step 3 Click **Browse**.

A Select file dialog box appears.

Step 4 Browse to the PQI file that you are installing.

Step 5 Click **Open**.

The Select file dialog box closes.

Step 6 Click **Finish**.

A Password Management dialog box appears.

Step 7 Enter the appropriate password. (For more information, see Password Management, page 5-8.)

Step 8 Click **Apply**.

The Password Management dialog box closes.

An Updating software to SCE progress bar appears.

The PQI file is installed on the selected SCE.

How to Install an SCE OS Software Package on SCE Devices

This operation installs the SCE OS software package (the operating system software and firmware of the SCE platform).

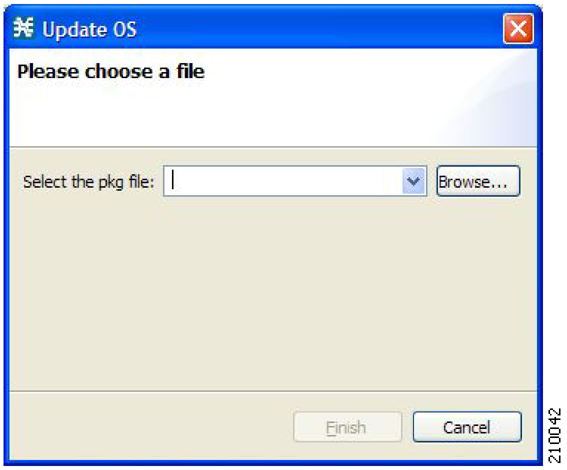
Note It is recommended to use the SCE Software Upgrade wizard when installing an SCE OS software package on multiple SCE platforms. See How to Upgrade the SCE Using the SCE Software Upgrade Wizard, page 4-8.

Step 1 In the Site Manager tree, select an SCE device.

Step 2 From the Console main menu, choose **Network > Upgrade SCE Platform Firmware (PKG)**.

The Update OS dialog box appears (Figure 5-20).

Figure 5-20 Update OS



Update OS

Please choose a file

Select the pkg file:

Step 3 Click **Browse**.

A Select file dialog box appears.

Step 4 Browse to the PKG file containing the OS that you are installing.

Step 5 Click **Open**.

The Select file dialog box closes.

Step 6 Click **Finish**.

A Password Management dialog box appears.

Step 7 Enter the appropriate password. (For more information, see Password Management, page 5-8.)

Step 8 Click **Apply**.

The Password Management dialog box closes.

An Updating software to SCE progress bar appears.

The PQI file is installed on the selected SCE.

Managing Subscriber Manager Devices

- How to Generate Tech Support Info Files for Subscriber Manager Devices, page 5-27
- How to Retrieve the Online Status of Subscriber Manager Devices, page 5-28
- How to Connect to Subscriber Manager Devices, page 5-29

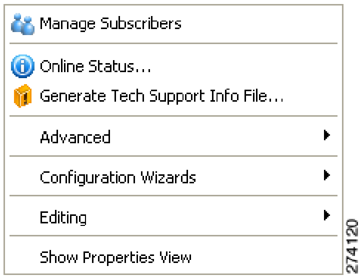
How to Generate Tech Support Info Files for Subscriber Manager Devices

This operation generates the support file, for the Subscriber Manager, for the use of Cisco technical support staff.

Step 1 In the Site Manager tree, right-click an Subscriber Manager device.

A popup menu appears (Figure 5-21).

Figure 5-21 Site Manager Tree Menu



Step 2 From the menu, select **Generate Tech Support Info File**.

The Generate Tech Support Info File dialog box appears.

Step 3 Click **Browse**.

A Select File dialog box appears.

Step 4 Browse to the folder where you want to save the tech support info file.

Step 5 In the File name field, enter a new file name, or select an existing ZIP file.

Step 6 Click **Open** to select the file.

If the file exists, it is overwritten.

The Select File dialog box closes.

Step 7 (Optional) To add log files to the output tech support info file, check the **Add GUI Console log files check box**.

Step 8 Check the **Open file after it is fetched** check box.

Step 9 Click **Finish**.

The Generate Tech Support Info File dialog box closes.

A Password Management dialog box appears.

Step 10 Enter the appropriate password. (For more information, see Password Management, page 5-8.)

Step 11 Click **Generate**.

The Password Management dialog box closes.

A Generate tech support info file progress bar appears.

The file is generated.

How to Retrieve the Online Status of Subscriber Manager Devices

This operation provides information about the current software version and operational status of the Subscriber Manager Device.

Step 1 In the Site Manager tree, right-click an Subscriber Manager device.

A popup menu appears.

Step 2 From the menu, select **Online Status**.

A Password Management dialog box appears.

Step 3 Enter the appropriate password. (For more information, see Password Management, page 5-8.)

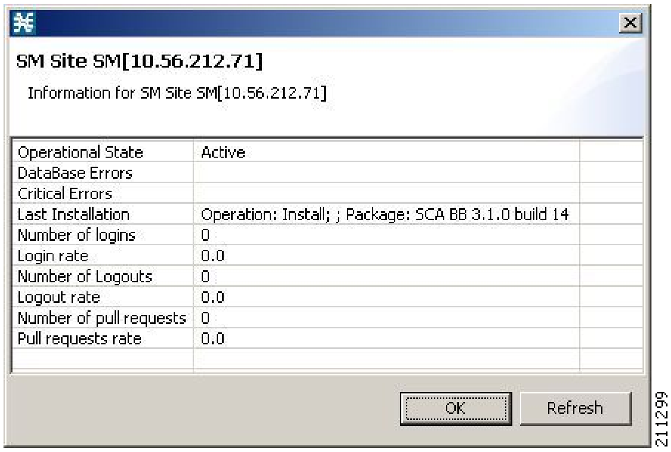
Step 4 Click **Extract**.

The Password Management dialog box closes.

An Extracting info progress bar appears.

The SCMS Subscriber Manager online status is retrieved (Figure 5-22).

Figure 5-22 SCMS Subscriber Manager Online Status



SM Site SM[10.56.212.71]

Information for SM Site SM[10.56.212.71]

Operational State	Active	
DataBase Errors		
Critical Errors		
Last Installation	Operation: Install; ; Package: SCA BB 3.1.0 build 14	
Number of logins	0	
Login rate	0.0	
Number of Logouts	0	
Logout rate	0.0	
Number of pull requests	0	
Pull requests rate	0.0	

How to Connect to Subscriber Manager Devices

To manage subscribers using the Subscriber Manager GUI tool, you must connect to an Subscriber Manager device.

Note The Subscriber Manager GUI tool performs authentication on the SCMS Subscriber Manager by opening a PRPC connection to port 14374 and attempting to log in using the username and password that you entered in the Password Management dialog box. If a PRPC server with this user is not running on the SCMS Subscriber Manager, authentication fails.
If you have changed the PRPC port on the SCMS Subscriber Manager, see User Authentication, page 5-40.

Step 1 In the Site Manager tree, right-click an Subscriber Manager device.

A popup menu appears.

Step 2 From the menu, select **Manage Subscribers**.

A Password Management dialog box appears.

Step 3 Enter the appropriate password. (For more information, see Password Management, page 5-8.)

Step 4 Click **Connecting**.

The Password Management dialog box closes.

A Connecting to progress bar appears.

You connect to the Subscriber Manager, and the Console switches to the Subscriber Manager GUI tool.

For an explanation of how to proceed, see Using the Subscriber Manager GUI Tool, page 11-1.

Managing Collection Manager Devices

You can configure Collection Manager devices using a wizard. (See How to Configure SCE and CM Devices Using a Wizard, page 5-10.)

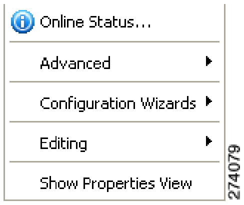
How to Retrieve the Online Status of CM Devices

This operation provides information about the current software version and operational status of the Collection Manager.

Step 1 In the Site Manager tree, right-click a CM device.

A popup menu appears (Figure 5-23).

Figure 5-23 Site Manager Tree Menu



Step 2 From the menu, select **Online Status**.

A Password Management dialog box appears.

Step 3 Enter the appropriate password. (For more information, see Password Management, page 5-8.)

Step 4 Click **Extract**.

The Password Management dialog box closes.

An Extracting info progress bar appears.

The SCMS Collection Manager online status is retrieved.

For an example of a retrieved online status window (for an SCE platform), see How to Retrieve the Online Status of SCE Devices, page 5-19.

Managing Database Devices

This section provides information on managing database devices.

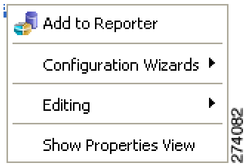
How to Make Databases Accessible to the SCA Reporter

- The Reporter DB Configuration wizard allows you to connect the Reporter to a single database. (See How to Use the Reporter DB Configuration Wizard, page 4-65.)
- An alternative procedure is described in the "*Configuring Properties*" section in the "*Using the Cisco Service Control Application Reporter*" chapter of *Cisco Service Control Application Reporter User Guide.*

Step 1 In the Site Manager tree, right-click a database device.

A popup menu appears (Figure 5-24).

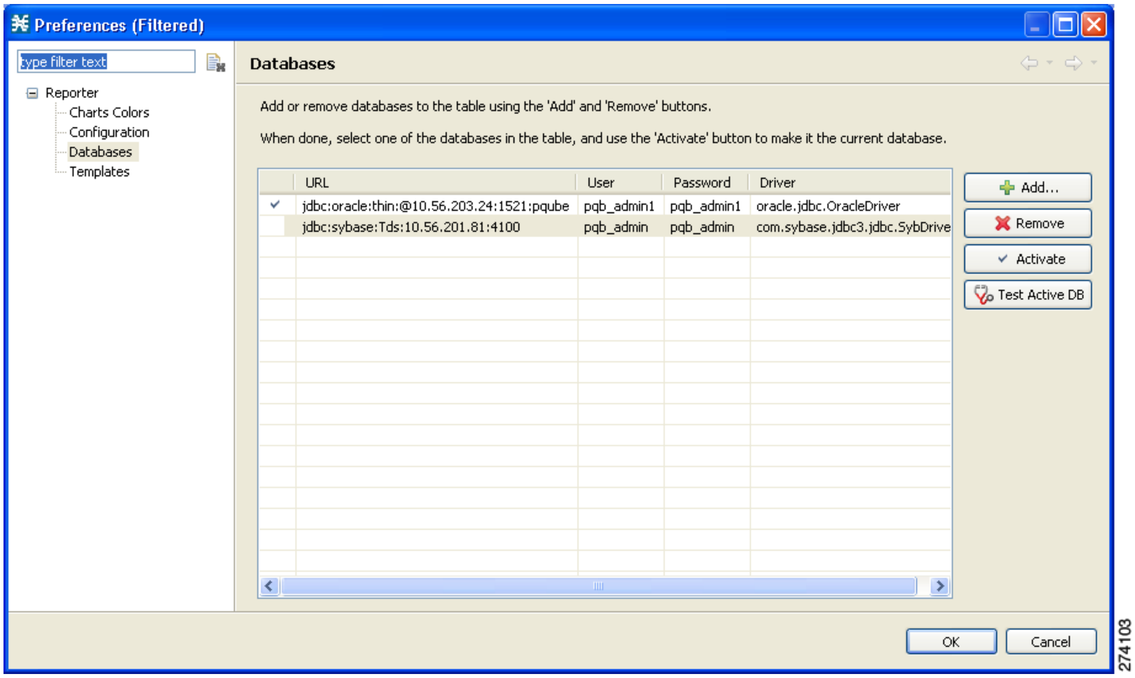
Figure 5-24 Site Manager Tree Menu



Step 2 From the menu, select **Add to Reporter**.

The Preferences dialog box appears (Figure 5-25).

Figure 5-25 Preferences



Add or remove databases to the table using the 'Add' and 'Remove' buttons.

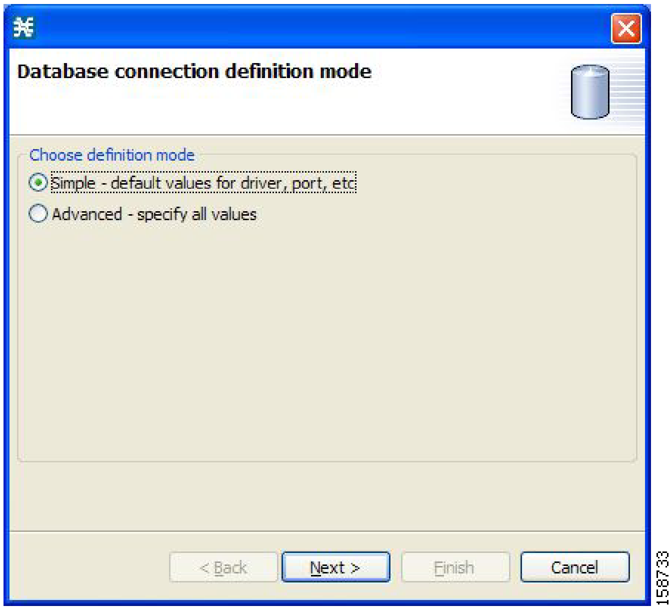
When done, select one of the databases in the table, and use the 'Activate' button to make it the current database.

	URL	User	Password	Driver
✓	jdbc:oracle:thin:@10.56.203.24:1521:pqube	pqb_admin1	pqb_admin1	oracle.jdbc.OracleDriver
	jdbc:sybase:Tds:10.56.201.81:4100	pqb_admin	pqb_admin	com.sybase.jdbc3.jdbc.SybDrive

Step 3 Click **Add**.

The Add Database wizard appears (Figure 5-26).

Figure 5-26 Add Database



Database connection definition mode

Choose definition mode

● Simple - default values for driver, port, etc

○ Advanced - specify all values

Step 4 Select one of the **Choose definition mode** radio buttons:

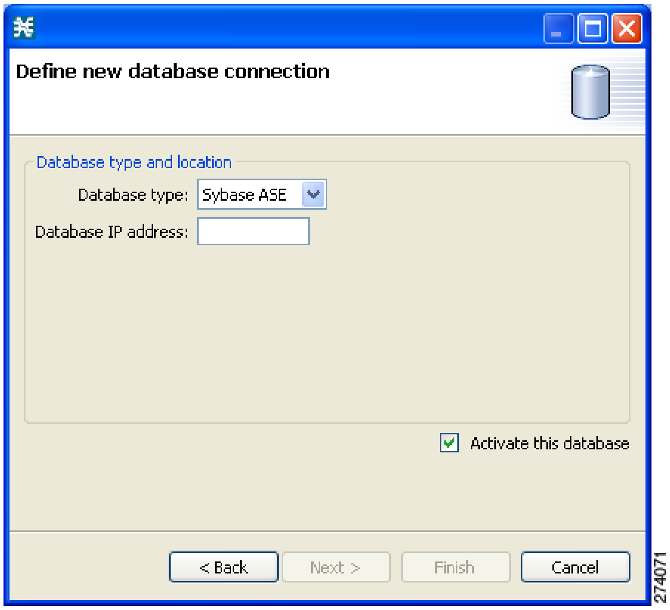
- **Simple - default values of driver, port, etc.**
- **Advanced - specify all values**

Step 5 Click **Next**.

The Define new database connection page of the Add Database wizard opens:

- If you selected Simple in Step 4, the Define new database connection page looks like Figure 5-27.

Figure 5-27 Define New Database Connection - Simple



Define new database connection

Database type and location

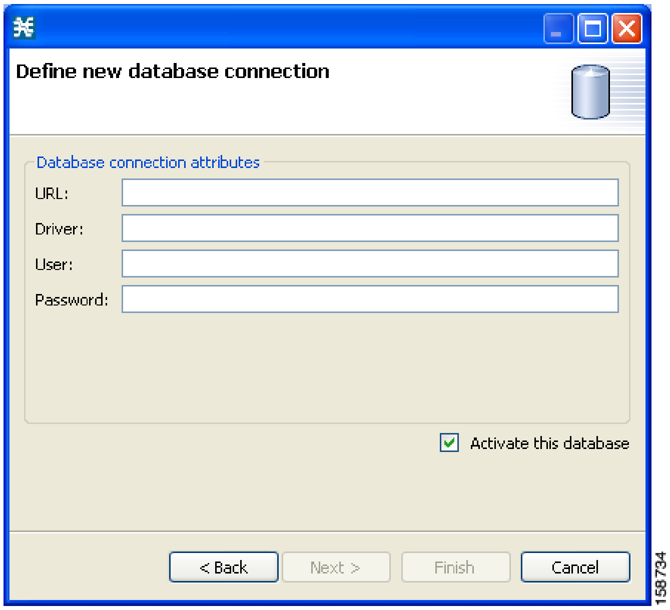
Database type: Sybase ASE

Database IP address:

☑ Activate this database

- If you selected Advanced in Step 4, the Define new database connection page looks like Figure 5-28.

Figure 5-28 Define New Database Connection - Advanced



Define new database connection

Database connection attributes

URL:

Driver:

User:

Password:

☑ Activate this database

Step 6 Fill in all the fields.

Step 7 Click **Finish**.

The Add Database wizard closes.

The definition of the database is added to the list in the Preferences dialog box.

Step 8 Repeat Steps 3 to 7 for other databases.

Step 9 If necessary, delete databases from the list in the Preferences dialog box.

Step 10 Make sure that the correct database is activated.

Step 11 Click **OK**.

The Preferences dialog box closes.

Working with Network Navigator Configuration Files

After you add sites and devices to the Network Navigator, you can export this data to a file to back up your settings and to share them with other users, who can import your Network Navigator settings into their Console.

If you use the Site Master Password to store the passwords of the network devices, the passwords are also exported, in encrypted form. This means that other users who import this data need to only provide the Site Master Password to access the devices.

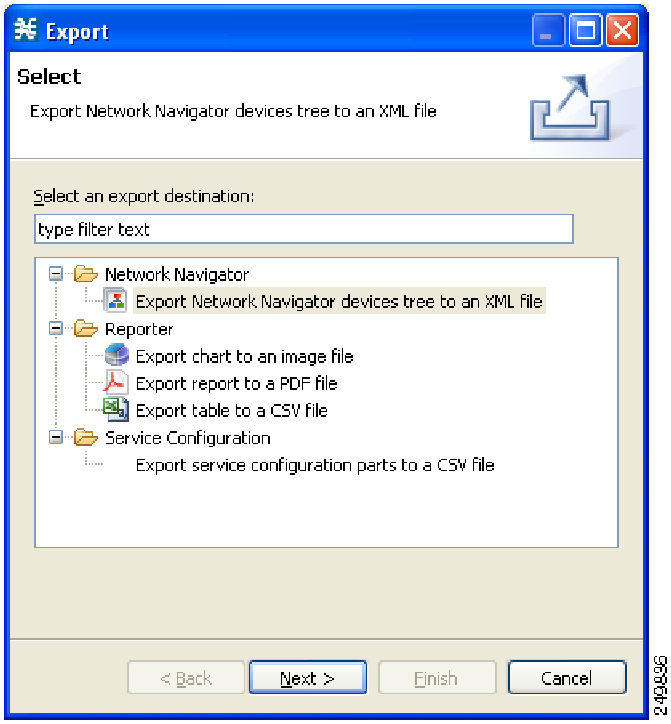
- How to Export a Network Navigator Configuration, page 5-35
- How to Import a Network Navigator Configuration, page 5-37

How to Export a Network Navigator Configuration

Step 1 From the Console main menu, choose **File > Export**.

The Export dialog box appears (Figure 5-29).

Figure 5-29 Export



Select

Export Network Navigator devices tree to an XML file

Select an export destination:

type filter text

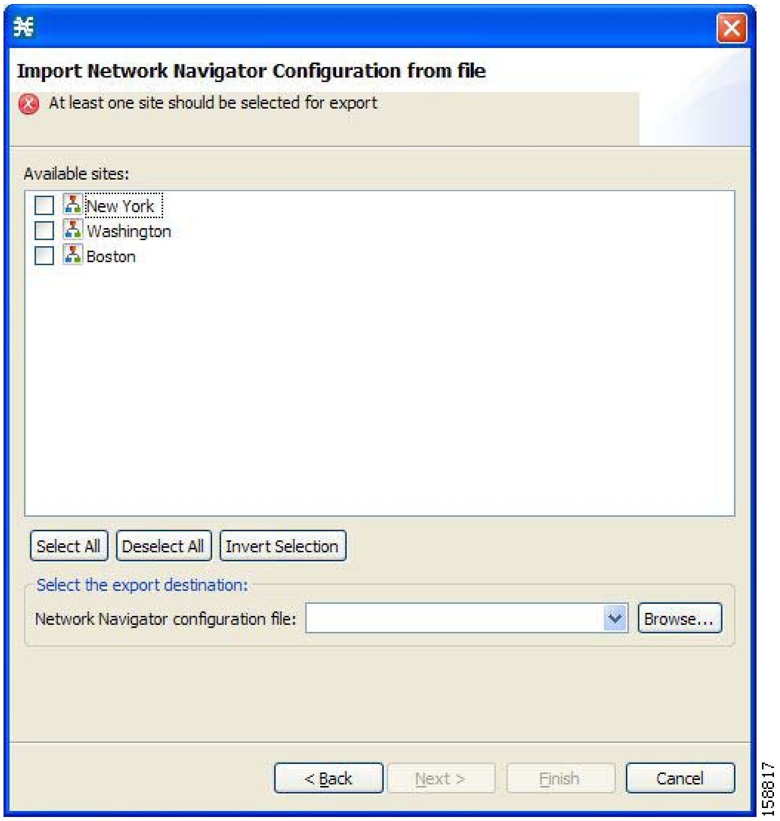
- Network Navigator
  - Export Network Navigator devices tree to an XML file
- Reporter
  - Export chart to an image file
  - Export report to a PDF file
  - Export table to a CSV file
- Service Configuration
  - Export service configuration parts to a CSV file

Step 2 From the export destination list, select **Network Navigator Configuration to a file**.

Step 3 Click **Next**.

The Export Network Navigator Configuration to a file dialog box appears (Figure 5-30).

Figure 5-30 Import Network Navigator Configuration from File



Import Network Navigator Configuration from file

At least one site should be selected for export

Available sites:

- □ New York
- □ Washington
- □ Boston

Select the export destination:

Network Navigator configuration file:

The Available sites pane lists all of the sites in the configuration.

Step 4 Select the sites to export, using the check boxes and the select buttons.

Step 5 In the Select the export destination area, click **Browse**.

An Open dialog box appears.

Step 6 Browse to the folder where you want to save the configuration file.

Step 7 In the File name field, enter a new file name, or select an existing site_xml file.

Step 8 Click **Open** to select the file.

Note If the file exists, it is overwritten.

The Open dialog box closes.

Step 9 Click **Finish**.

The Export Network Navigator Configuration dialog box closes.

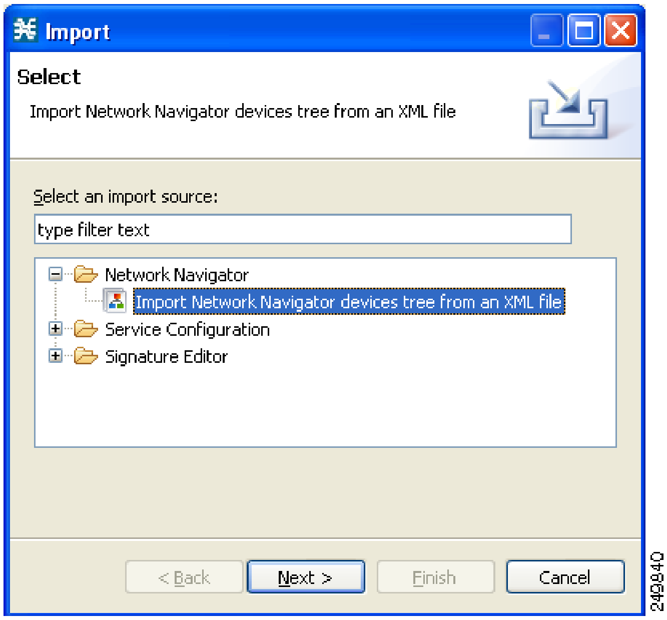
The configuration is saved to the file.

How to Import a Network Navigator Configuration

Step 1 From the Console main menu, choose **File > Import**.

The Import dialog box appears (Figure 5-31).

Figure 5-31 Import



Import

Select

Import Network Navigator devices tree from an XML file

Select an import source:

type filter text

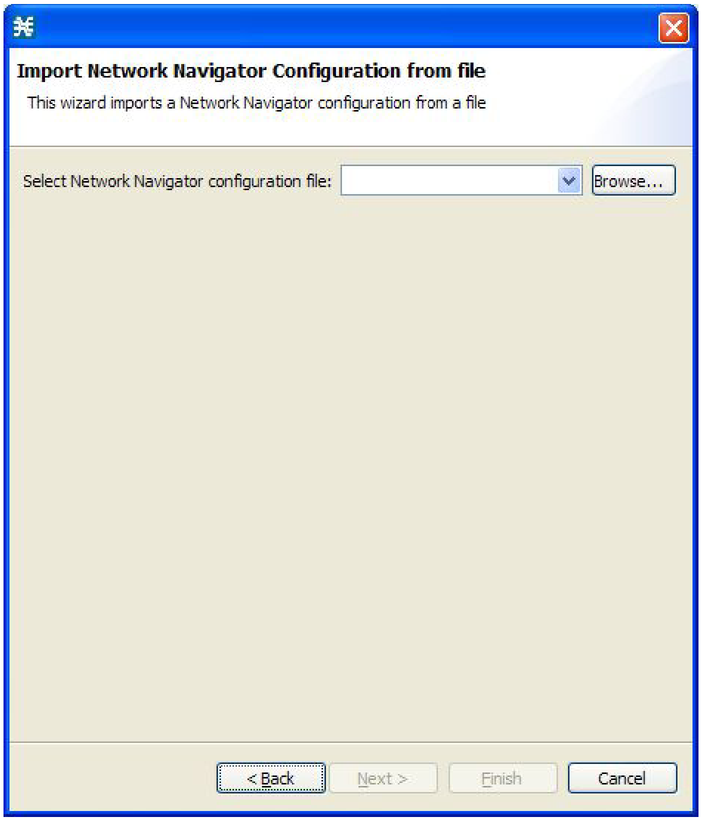
- Network Navigator
  - Import Network Navigator devices tree from an XML file
- Service Configuration
- Signature Editor

Step 2 From the import source list, select **Network Navigator Configuration from file**.

Step 3 Click **Next**.

The Import Network Navigator Configuration from file dialog box appears (Figure 5-32).

Figure 5-32 Import Network Navigator Configuration from File



Import Network Navigator Configuration from file

This wizard imports a Network Navigator configuration from a file

Select Network Navigator configuration file:

Step 4 Click **Browse**.

An Open dialog box appears.

Step 5 Browse to the folder containing the file to import, and select a site_xml file.

Step 6 Click **Open** to select the file.

The Open dialog box closes.

Step 7 Click **Finish**.

The Import Network Navigator Configuration dialog box closes.

The configuration is imported from the file.

Network Settings Requirements

- Firewall/NAT Requirements, page 5-39
- User Authentication, page 5-40
- How to Disable PRPC Authentication, page 5-40

Firewall/NAT Requirements

Table 5-1 lists the firewall/NAT open port settings required for the Network Navigator to operate properly.

The ports listed in the table are the default values. If you change a port in a device, you must modify the firewall/NAT settings accordingly. (Modifying the Console settings to connect to a different PRPC port is described in the following section.)

Table 5-1 Required Firewall/NAT Settings

Source	Destination	Comments
Workstation	SCE port 14374/TCP	PRPC—Required for all SCE operations
SCE	Workstation port 21/TCP	FTP—Required for the following SCE operations: • Install OS • Generate Tech Support Info File
SCE	Workstation ports 21000/TCP to 21010/TCP	FTP—Alternative to port 21/TCP, required if another application on the workstation is using port21/TCP.
Workstation	Subscriber Manager port 14374/TCP	PRPC—Required for all Subscriber Manager operations
Workstation	CM port 14375/TCP	PRPC—Required for the CM Online Status operation and for CM authentication

The SCA Reporter may have additional requirements for connecting to the database. For more information, see *Cisco Service Control Application Reporter User Guide.*

User Authentication

User authentication is performed when a Proprietary Remote Procedure Call (PRPC) connection is made to an SCE platform, a CM, or an Subscriber Manager. For authentication to succeed, a PRPC server must be running at the destination, and you must know the username and password of a user of the server.

Note If you change a PRPC server port in a device (SM/CM/SCE), you must add a line to the configuration file *engage.ini*:

```
<IP address of device>.rpc.port=<port number>
```

For example:

```
10.56.216.37.rpc.port=222
```

Add one line for each (non-default) port that you use.

The file *engage.ini* is located in the folder *Program files\Cisco SCA\SCA BB Console 3.7.0\plugins\policy.contribution_3.7.0\config\*.

You define the username and password using the user/password mechanism in the SCE platform or a command-line utility in the Subscriber Manager and CM.

For more information about defining users, see the following:

- SCE—See either the "TACACS+ Authentication, Authorization, and Accounting" section in the "Configuring the Management Interface and Security" chapter of *Cisco SCE8000 10GBE Software Configuration Guide or the* "TACACS+ Authentication, Authorization, and Accounting" section in the "Configuring the Management Interface and Security" chapter of *Cisco SCE8000 GBE Software Configuration Guide.*
- Collection Manager—"Managing Users" section in the "Managing the Collection Manager" chapter of *Cisco Service Control Management Suite Collection Manager User Guide.*
- Subscriber Manager—"Information About the p3rpc Utility" section in the "Command-Line Utilities" appendix of *Cisco Service Control Management Suite Subscriber Manager User Guide.*

Note PRPC authentication from the Cisco SCA BB Console to any CM/SM/SCE IP addresses other than the real IP address of the device is not supported. This is especially important when the CM/Subscriber Manager/SCE resides on the inside interface of a NATing router or firewall
Workaround:

Redesign your network so that the SCA BB Console is given the real IP address of the CM/SM/SCE. Disable PRPC authentication on the SCE/CM/Subscriber Manager/SCE as described in the following sections.

How to Disable PRPC Authentication

- How to Disable PRPC Authentication on an SCE Platform, page 5-41
- How to Disable PRPC Authentication on a CM, page 5-41
- How to Disable PRPC Authentication on an Subscriber Manager, page 5-41

How to Disable PRPC Authentication on an SCE Platform

Step 1 Use the CLI to disable PRPC authentication.

Run the following CLI in config mode:

```
ip rpc-adapter security-level none
```

How to Disable PRPC Authentication on a CM

Step 1 Edit the CM configuration file.

Edit the cm/um/config/p3cm.cfg configuration file:

```
[RPC.Server]
security_level=none
```

Step 2 Reload the CM process.

How to Disable PRPC Authentication on an Subscriber Manager

Step 1 Edit the Subscriber Manager configuration file.

Edit the ~pcube/sm/server/root/config/p3sm.cfg configuration file:

```
[RPC.Server]
security_level=none
```

Step 2 Load the configuration.

Run the following CLU:

```
p3sm --load-config
```

CHAPTER 6

Using the Service Configuration Editor

Revised: August 08, 2013, OL-24178-09

Introduction

To configure a Service Control Engine (SCE) platform to handle traffic, you must define a service configuration and apply it to the platform. Use the Service Configuration Editor tool to create, define, and manage service configurations.

This module describes how to use the Service Configuration Editor tool.

- Service Configurations, page 6-1
- Managing Service Configurations, page 6-2

Service Configurations

A *service configuration* is a data structure that defines how the SCE platform analyses network traffic, what rules apply to the traffic, and what actions the SCE platform takes to enforce these rules.

A service configuration consists of the following two main elements:

- Services—Define the categories to which transactions are classified
- Packages—Define how the SCE platform acts upon transactions from different services

Service configurations are stored as PQB files.

Managing Service Configurations

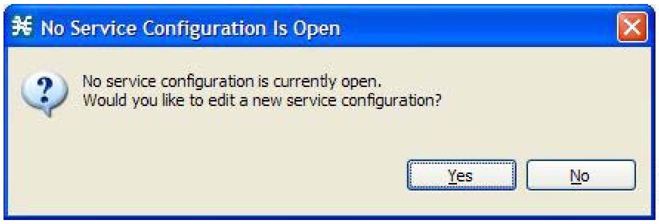
This section explains how to:

- Manage service configurations
- Export and import service configuration data
- Apply service configurations to SCE platforms and retrieve them

Opening the Service Configuration Editor Tool

If no service configurations are open when you open or switch to the Service Configuration Editor tool, a No Service Configuration Is Open dialog box appears (see Figure 6-1).

Figure 6-1 No Service Configuration Is Open



No service configuration is currently open.
Would you like to edit a new service configuration?

- To create a new service configuration (see How to Add New Service Configurations, page 6-2), click **Yes**.
- To open an existing service configuration (see How to Open Existing Service Configurations, page 6-4), click **No**.

The Configuration option is included in the main menu only when at least one service configuration is open.

You can have many service configurations open at a time; each is displayed in its own view, and you click a view to make the service configuration of the view active.

When a service configuration has unsaved changes, an asterisk precedes its name on the view.

How to Add New Service Configurations

You can add a new service configuration whenever necessary.

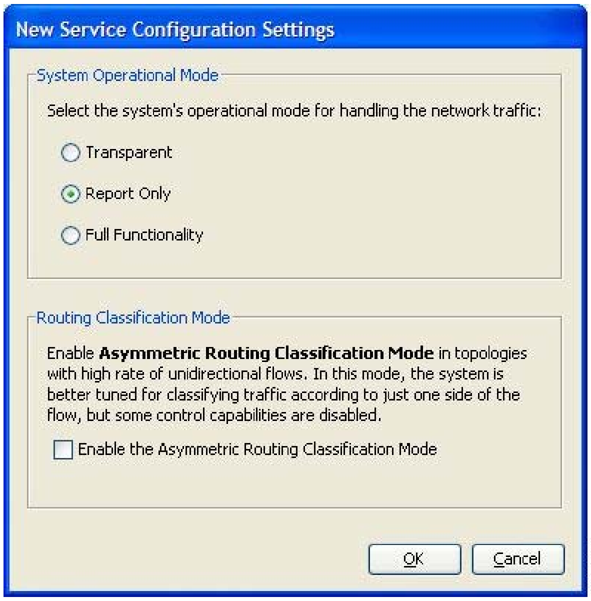
Note You cannot add a second new service configuration until you have saved the first one.

When a new service configuration opens, it contains the default service configuration supplied with SCA BB. This includes a default package, which contains a default service rule.

Step 1 In the Console toolbar, click (**New Service Configuration**).

A New Service Configuration Settings dialog box appears (Figure 6-2).

Figure 6-2 New Service Configuration Settings



New Service Configuration Settings

System Operational Mode

Select the system's operational mode for handling the network traffic:

○ Transparent

● Report Only

○ Full Functionality

Routing Classification Mode

Enable **Asymmetric Routing Classification Mode** in topologies with high rate of unidirectional flows. In this mode, the system is better tuned for classifying traffic according to just one side of the flow, but some control capabilities are disabled.

□ Enable the Asymmetric Routing Classification Mode

Step 2 Select an operational mode for the service configuration.

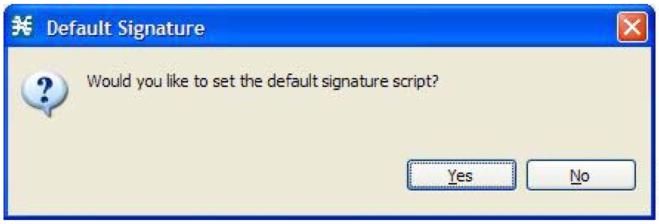
Step 3 Select a routing classification mode for the system.

Selecting asymmetric routing classification mode gives more accurate protocol classification in topologies with a high rate of unidirectional flows. Several classification, reporting, and control features are not supported when this mode is enabled (see Asymmetric Routing Classification Mode, page 10-56).

Step 4 Click **OK**.

If you have set a default DSS file (see The Default DSS File, page 7-53), a Default Signature message appears (Figure 6-3).

Figure 6-3 Default Signature



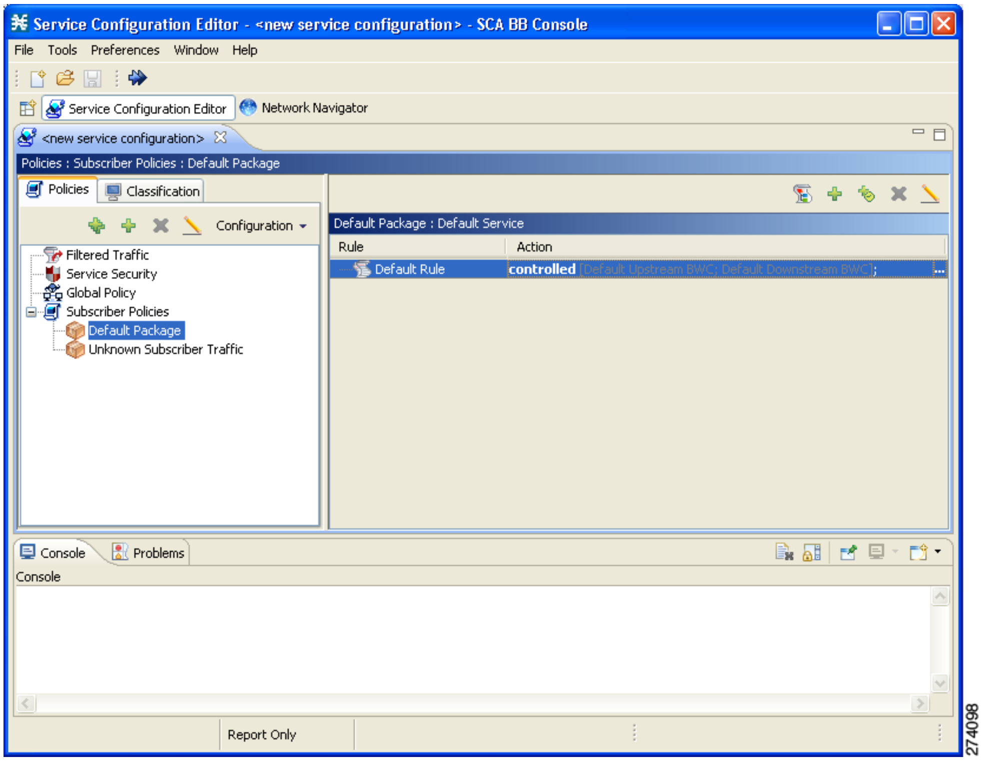
Default Signature

Would you like to set the default signature script?

- (Recommended) Click **Yes** to import the default DSS file.
- Click **No** to continue without importing the default DSS file.

The new service configuration is added to the Console window, open on the Network Traffic tab, and becomes the active service configuration (Figure 6-4).

Figure 6-4 Service Configuration Editor


Service Configuration Editor - <new service configuration> - SCA BB Console
File
Tools
Preferences
Window
Help
Service Configuration Editor
Network Navigator
<new service configuration>
Policies : Subscriber Policies : Default Package
Policies
Classification
Configuration
Filtered Traffic
Service Security
Global Policy
Subscriber Policies
Default Package
Unknown Subscriber Traffic
Default Package : Default Service
Console
Problems
Console
Report Only
274098

Rule	Action
Default Rule	controlled [Default Upstream BWC; Default Downstream BWC];

How to Open Existing Service Configurations

You can open a saved service configuration for viewing or for editing, or to apply it to an SCE platform.

Service configuration files have the extension PQB.

Step 1 In the Console toolbar, click the **Open A Service Configuration File** (📂) icon. Alternatively, you can choose **File > Open Service Configuration** from the Console main menu.

An Open dialog box appears.

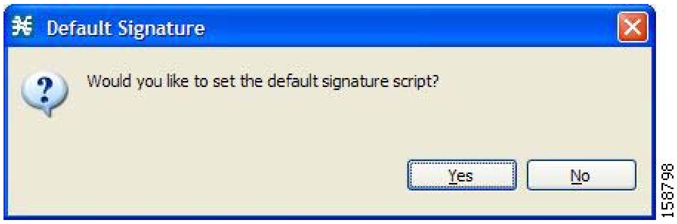
Step 2 Browse to a service configuration file.

Step 3 Click **Open**.

The Open dialog box closes.

If the default DSS file has not been imported into the service configuration, a Default Signature message appears (Figure 6-5).

Figure 6-5 Default Signature



Default Signature

Would you like to set the default signature script?

If the default DSS file has not been imported into the service configuration, a Default Signature message appears.

- (Recommended) Click **Yes** to import the default DSS file.
- Click **No** to continue without importing the default DSS file.

The service configuration is loaded into the Console:

- This service configuration becomes the active service configuration.
- The title of the Console window includes the name of the service configuration.

How to Save the Current Service Configuration

You can save the active service configuration.

- How to Save the Current Service Configuration to a Service Configuration File, page 6-5
- How to Save the Current Service Configuration to the File from Which it Was Loaded, page 6-6

How to Save the Current Service Configuration to a Service Configuration File

Step 1 From the Console main menu, choose **File > Save As**.

A Save As dialog box appears.

Step 2 If prompted, enter your password.

Step 3 Browse to the folder where you want to save the file containing the service configuration.

Step 4 In the File name field, enter a new file name, or select an existing PQB file.

Step 5 Click **Save**.

The service configuration is saved to the selected file. If the file exists, it is overwritten.

During processing, a Saving Service Configuration File message appears.

How to Save the Current Service Configuration to the File from Which it Was Loaded

Step 1 In the Console toolbar, click the **Save** (💾) icon.

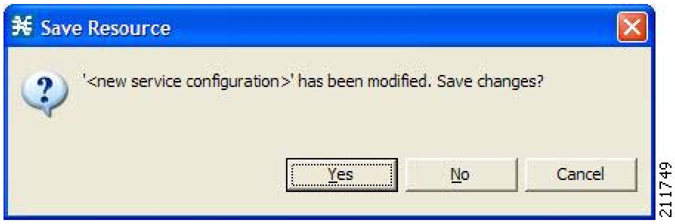
If the current service configuration was not loaded from a PQB file (that is, if it is new, or it was retrieved from an SCE platform), the Save As dialog box opens as in the previous procedure.

How to Close Service Configurations

Step 1 On the service configuration view, click the **Close** (☒) icon.

- If there are no unsaved changes, the service configuration view closes.
- If there are unsaved changes a Save Resource message appears (Figure 6-6).

Figure 6-6 Save Resource



'<new service configuration>' has been modified. Save changes?

- Click **Yes**:
  - If this is an existing edited service configuration, the changes are saved and the service configuration view closes.
  - If this is a new service configuration, a Save As dialog box opens.

  Enter a name for the service configuration and click **Save**.

  The Save As dialog box closes, the changes are saved, and the service configuration view closes.

How to Export Service Configuration Data

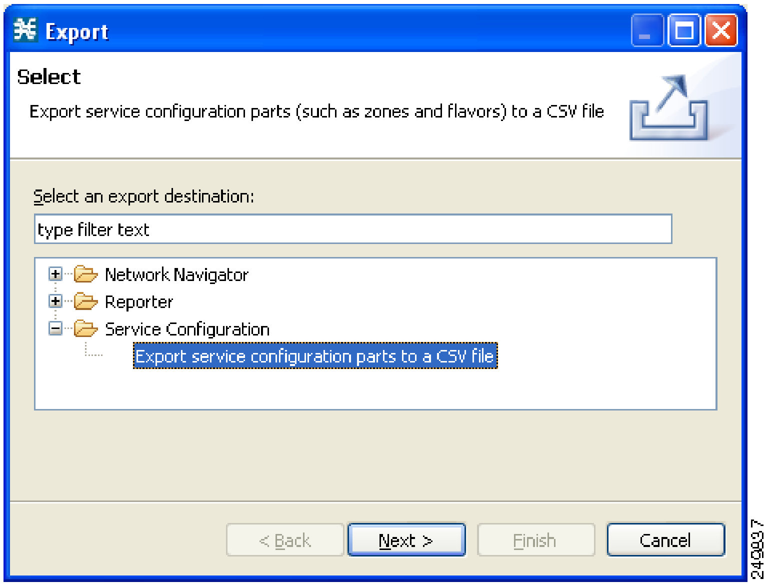
You can export service configuration data from the current service configuration to CSV files. The CSV file formats are described in the "CSV File Formats" chapter of *Cisco Service Control Application Suit for Broadband Reference Guide.*

Each type of service configuration element is exported to a separate file.

Step 1 From the Console main menu, choose **File > Export**.

The Export dialog box appears (Figure 6-7).

Figure 6-7 Export



Export

Select

Export service configuration parts (such as zones and flavors) to a CSV file

Select an export destination:

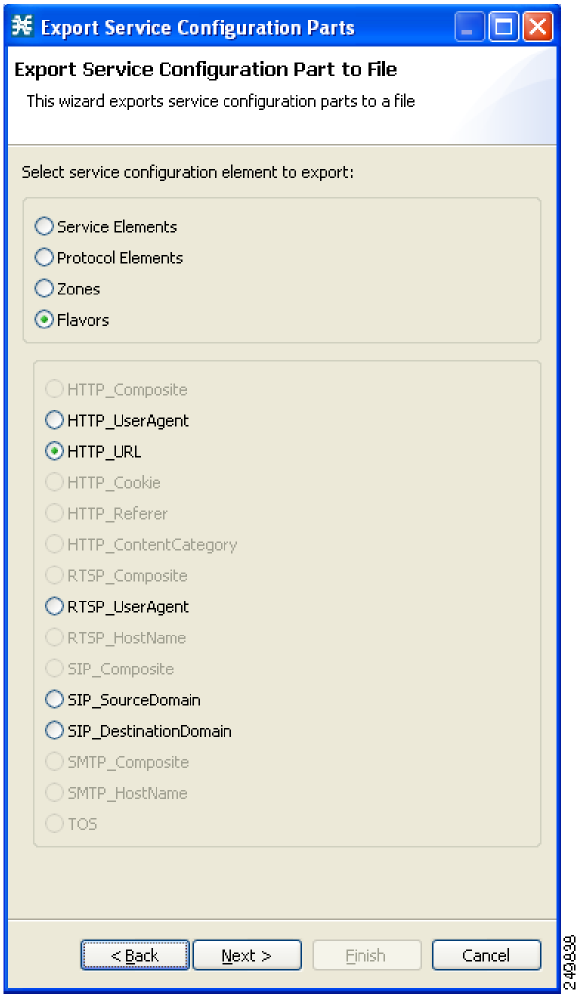
type filter text

Step 2 From the export destination list, select **Export service configuration parts to CSV file**.

Step 3 Click **Next**.

The Export Service Configuration Parts dialog box appears (Figure 6-8).

Figure 6-8 Export Service Configuration Parts to File



Export Service Configuration Parts

Export Service Configuration Part to File

This wizard exports service configuration parts to a file

Select service configuration element to export:

○ Service Elements
○ Protocol Elements
○ Zones
● Flavors

○ HTTP_Composite
○ HTTP_UserAgent
● HTTP_URL
○ HTTP_Cookie
○ HTTP_Referer
○ HTTP_ContentCategory
○ RTSP_Composite
○ RTSP_UserAgent
○ RTSP_HostName
○ SIP_Composite
○ SIP_SourceDomain
○ SIP_DestinationDomain
○ SMTP_Composite
○ SMTP_HostName
○ TOS

Step 4 Select one of the **Select service configuration element to export** radio buttons.

The radio buttons are:

- **Service Elements**
- **Protocol Elements**
- **Zones**
- **Flavors**

If you select Flavors, the flavors in the flavor area of the dialog box are enabled.

If you select Zones or Flavors, you have a choice to export the data in Standard format or Easy format.

In Easy format for flavor CSV files, lines in the files are in single URL format. for example, http://*.cisco.com/files*. Similarly, in Easy format for zone CSV files, lines in the files contains only zone items. For example, 1.0.0.0/32.

For more details on Standard format and Easy format, see the *Cisco Service Control Application for Broadband Reference Guide*.

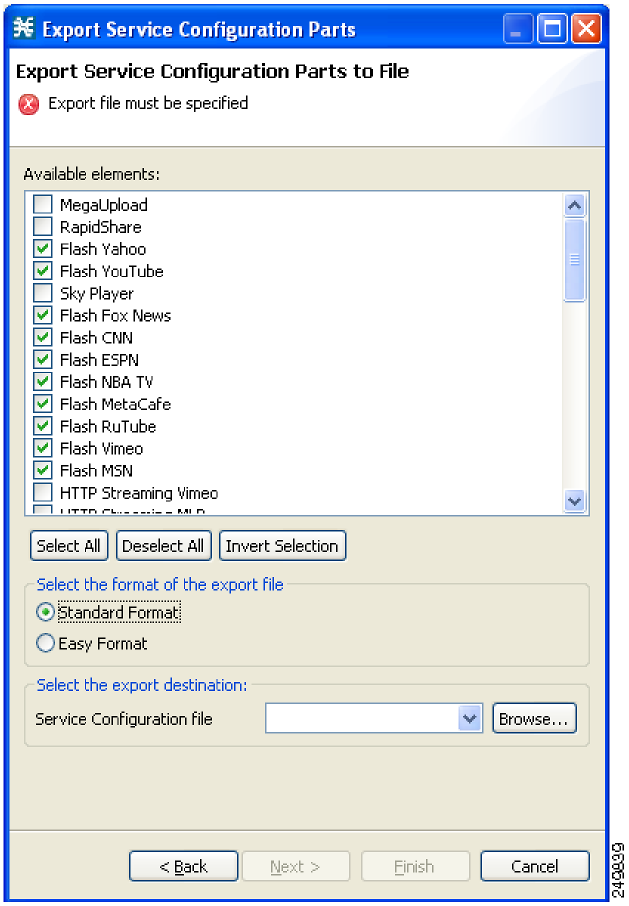
Note Only those flavors for which a flavor type is defined in this service configuration are enabled.

Step 5 If you selected Flavors, select one of the **flavor type** radio buttons.

Step 6 Click **Next**.

The second screen of the Export Service Configuration Parts dialog box opens (Figure 6-9).

Figure 6-9 Export Service Configuration Parts to File



Export Service Configuration Parts to File

Export file must be specified

Available elements:

- ☐ MegaUpload
- ☐ RapidShare
- ☑ Flash Yahoo
- ☑ Flash YouTube
- ☐ Sky Player
- ☑ Flash Fox News
- ☑ Flash CNN
- ☑ Flash ESPN
- ☑ Flash NBA TV
- ☑ Flash MetaCafe
- ☑ Flash RuTube
- ☑ Flash Vimeo
- ☑ Flash MSN
- ☐ HTTP Streaming Vimeo
- ☐ HTTP Streaming MLB

Select the format of the export file

- ● Standard Format
- ○ Easy Format

Select the export destination:

Service Configuration file

The Available elements pane lists all elements in the service configuration of the selected type.

Step 7 Select the elements to export, using the check boxes and the select buttons.

Step 8 (Only for Zones and Flavors) Select the format of the export file.

Step 9 In the Select the export destination area, click **Browse**.

An Open dialog box appears.

Step 10 Browse to the folder where you want to save the file containing the service configuration elements.

Step 11 In the File name field, enter a new file name, or select an existing CSV file.

(Only for Zones and Flavors) For Easy format, you must select the folder and the file name is the Zone or Flavor name.

Step 12 Click **Open** to select the file.

If the file exists, it is overwritten.

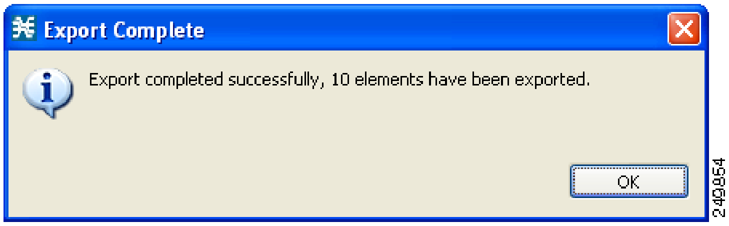
The Open dialog box closes.

Step 13 Click **Finish**.

The selected service configuration elements are exported to the file.

An Export Complete message appears (Figure 6-10).

Figure 6-10 Export Complete



Export Complete

Export completed successfully, 10 elements have been exported.

Step 14 Click **OK**.

The Export Service Configuration Parts dialog box closes.

How to Import Service Configuration Data

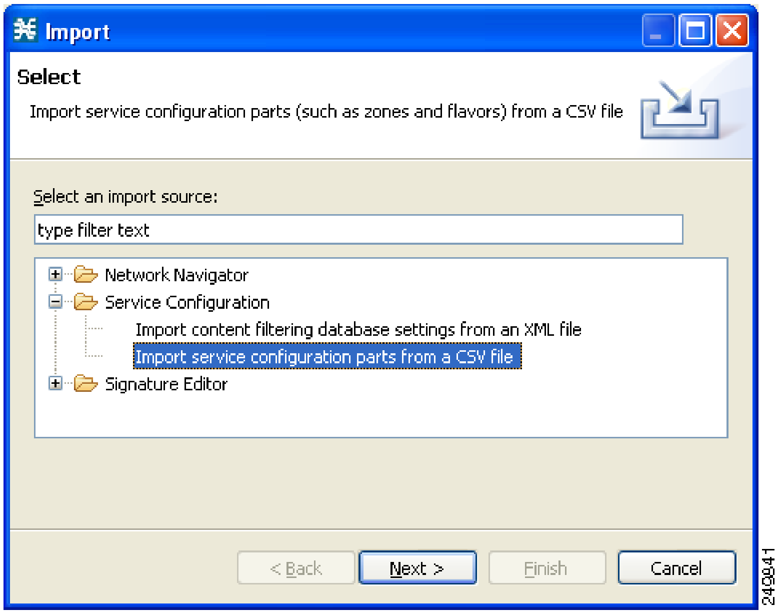
You can import service configuration data to the current service configuration from CSV files. The CSV file formats are described in the "CSV File Formats" chapter of *Cisco Service Control Application Suit for Broadband Reference Guide.*

Each type of service configuration element is imported from a separate file.

Step 1 From the Console main menu, choose **File > Import**.

The Import dialog box appears (Figure 6-11).

Figure 6-11 Import



Import

Select

Import service configuration parts (such as zones and flavors) from a CSV file

Select an import source:

type filter text

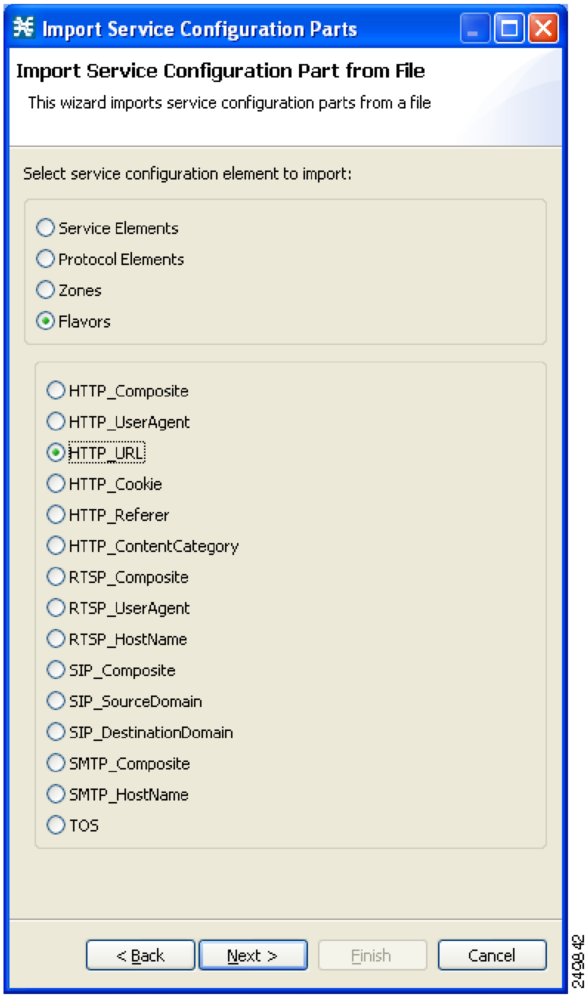
Network Navigator
Service Configuration
Import content filtering database settings from an XML file
Import service configuration parts from a CSV file
Signature Editor
< Back
Next >
Finish
Cancel
240941

Step 2 From the Select an import source list, select **Import service configuration parts from CSV file**.

Step 3 Click **Next**.

The Import Service Configuration Parts dialog box appears (Figure 6-12).

Figure 6-12 Import Service Configuration Parts from File



Import Service Configuration Part from File

This wizard imports service configuration parts from a file

Select service configuration element to import:

○ Service Elements
○ Protocol Elements
○ Zones
● Flavors

○ HTTP_Composite
○ HTTP_UserAgent
● HTTP_URL
○ HTTP_Cookie
○ HTTP_Referer
○ HTTP_ContentCategory
○ RTSP_Composite
○ RTSP_UserAgent
○ RTSP_HostName
○ SIP_Composite
○ SIP_SourceDomain
○ SIP_DestinationDomain
○ SMTP_Composite
○ SMTP_HostName
○ TOS

Step 4 Select one of the **Select service configuration element to import** radio buttons.

The radio buttons are:

- **Service Elements**
- **Protocol Elements**
- **Zones**
- **Flavors**

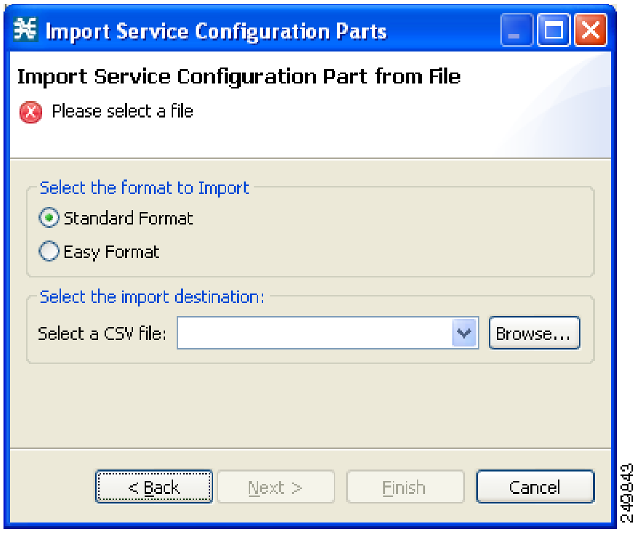
If you select Flavors, the flavors in the flavor area of the dialog box are enabled.

Step 5 If you selected Flavors, select one of the **flavor type** radio buttons.

Step 6 Click **Next**.

The second screen of the Import Service Configuration Parts dialog box opens (Figure 6-13).

Figure 6-13 Import Service Configuration Parts from File



Import Service Configuration Parts

Import Service Configuration Part from File

Please select a file

Select the format to Import

● Standard Format

○ Easy Format

Select the import destination:

Select a CSV file:

Step 7 (Only for Zones and Flavors) Select the format to Import.

Step 8 Click **Browse**.

An Open dialog box appears.

Step 9 Browse to the folder containing the file to import, and select a CSV file.

Step 10 Click **Open** to select the file.

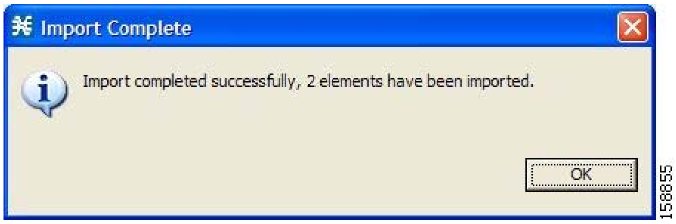
The Open dialog box closes.

Step 11 Click **Finish**.

The configuration elements are imported from the file.

An Import Complete message appears (Figure 6-14).

Figure 6-14 Import Complete



Import Complete

Import completed successfully, 2 elements have been imported.

Step 12 Click **OK**.

The Import Service Configuration Parts dialog box closes.

Applying and Retrieving Service Configurations

For a new or edited service configuration to take effect, you must apply it to the SCE platform. Until you do, the SCE platform continues to enforce the previous service configuration.

You can use the Service Configuration Editor to apply a service configuration to an SCE platform, but not to retrieve a service configuration.

You can apply or retrieve a service configuration using:

- The Network Navigator Tool, page 5-2
- **servconf,** the Cisco SCA BB Service Configuration Utility (see The Cisco SCA BB Service Configuration Utility, page 14-2)
- How to Validate the Current Service Configuration, page 6-14
- How to Apply a Service Configuration to SCE Platforms, page 6-15

How to Validate the Current Service Configuration

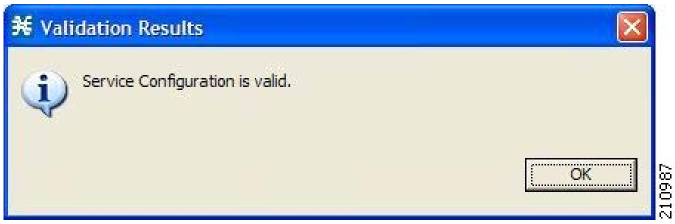
Use the Validate option to validate the new or updated service configuration currently displayed. The validation process checks for overall service configuration coherence, and points out possible pitfalls in the service configuration.

The Validate process runs automatically when you select Apply Service Configuration to SCE devices. The Validation Results dialog box appears only if the procedure found errors or issued warnings about the current service configuration.

Step 1 From the Console main menu, choose **File** > **Validate**.

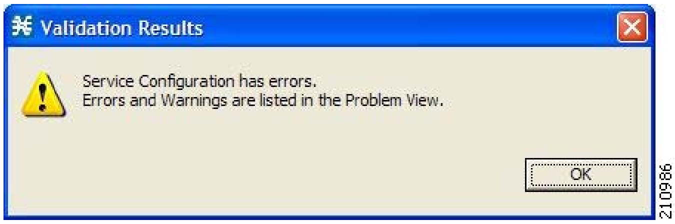
The Validation Results dialog box appears (Figure 6-15 or Figure 6-16).

Figure 6-15 Validation Results - Service Configuration is valid



Service Configuration is valid.

Figure 6-16 Validation Results - Service Configuration has errors



Service Configuration has errors.
Errors and Warnings are listed in the Problem View.

Any problems with the service configuration are listed in the Problems view.

Step 2 Click **OK**.

The Service Configuration Validation dialog box closes.

How to Apply a Service Configuration to SCE Platforms

When you click **Apply Service Configuration to SCE Devices,** the validation process runs automatically on the current service configuration.

Note You can use the **Validate** menu command to validate the service configuration manually.

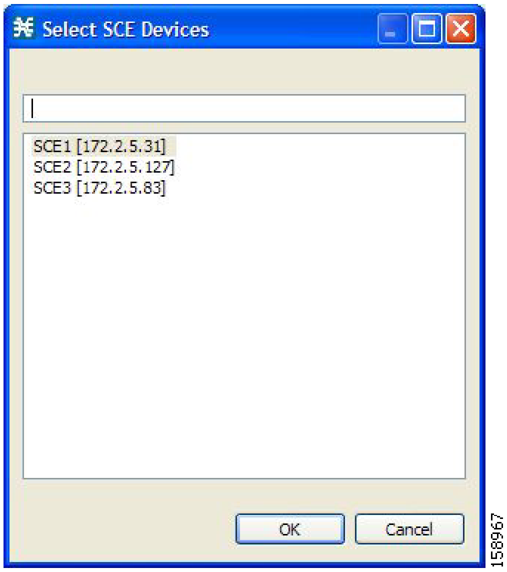
Caution If anomaly-based detection of malicious traffic is enabled, any access control list (ACL) that is configured on the Service Control Engine (SCE) platform but is not applied to anything (for example, an interface, an access map, or an SNMP community string) might be deleted when a service configuration is applied to the platform.

Workaround:
Disable anomaly-based detection of malicious traffic.
In the Network Traffic tab, select **Service Security**.
In the Service Security Dashboard, clear the **Enable anomaly detection** check box.

Step 1 In the Console toolbar, click the **Apply Service Configuration to SCE Devices** ( ).

The Select SCE Devices dialog box appears (Figure 6-17).

Figure 6-17 Select SCE Devices



SCE1 [172.2.5.31]
SCE2 [172.2.5.127]
SCE3 [172.2.5.83]

All SCE platforms defined in the Network Navigator are listed in the dialog box.

Step 2 Select one or more SCE platforms from the list.

Step 3 Click **OK**.

A Password Management dialog box appears for each platform selected.

Step 4 Enter the appropriate password.

Step 5 Click **Apply**.

The Password Management dialog box closes.

An Applying service configuration to SCE progress bar appears for each SCE platform selected.

The validation process runs on the service configuration.

- If there is a problem and the validation process ends with a warning or error, the Validation Results dialog box appears. Click **OK**, modify the service configuration based on the information provided in the Problems view, and then repeat this procedure.
- If the validation process runs successfully, the service configuration is applied to the selected SCE platforms.

CHAPTER 7

Using the Service Configuration Editor: Traffic Classification

Revised: August 08, 2013, OL-24178-09

Introduction

Traffic classification is the first step in creating a Cisco SCA BB service configuration. Traffic is classified according to services.

For each commercial service that providers offer to their subscribers, a corresponding service is defined in the Cisco Service Control solution. You can use this service to classify and identify the traffic, report on its usage, and control it.

This module explains how to work with services and their elements and subelements.

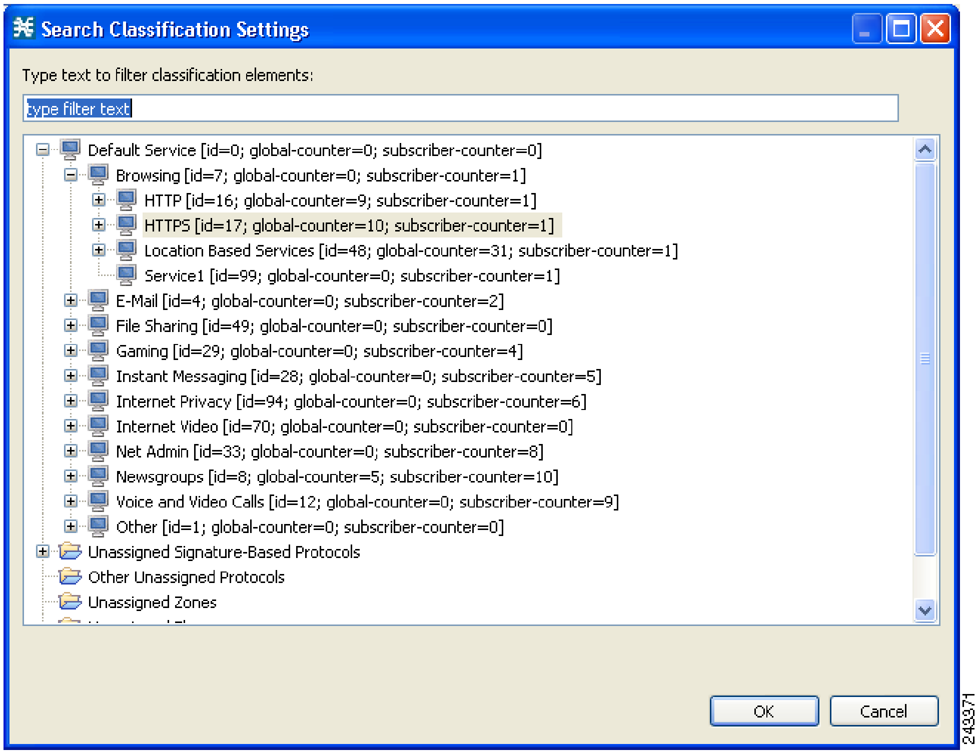
How to Search Traffic Classification Settings

You can search for any classification detail by name or numeric ID, such as services, protocols, port number, or counter assignments. You can also search for protocols or signatures that are not assigned to a service.

Step 1 In the **Classification** tab, click the **Search Classification Settings** ( ) icon.

The Search Classification Settings dialog box appears (Figure 7-1).

Figure 7-1 Search Classification Settings



Search Classification Settings

Type text to filter classification elements:

type filter text

```
⊟ Default Service [id=0; global-counter=0; subscriber-counter=0]
   ⊟ Browsing [id=7; global-counter=0; subscriber-counter=1]
      ⊞ HTTP [id=16; global-counter=9; subscriber-counter=1]
      ⊞ HTTPS [id=17; global-counter=10; subscriber-counter=1]
      ⊞ Location Based Services [id=48; global-counter=31; subscriber-counter=1]
        Service1 [id=99; global-counter=0; subscriber-counter=1]
   ⊞ E-Mail [id=4; global-counter=0; subscriber-counter=2]
   ⊞ File Sharing [id=49; global-counter=0; subscriber-counter=0]
   ⊞ Gaming [id=29; global-counter=0; subscriber-counter=4]
   ⊞ Instant Messaging [id=28; global-counter=0; subscriber-counter=5]
   ⊞ Internet Privacy [id=94; global-counter=0; subscriber-counter=6]
   ⊞ Internet Video [id=70; global-counter=0; subscriber-counter=0]
   ⊞ Net Admin [id=33; global-counter=0; subscriber-counter=8]
   ⊞ Newsgroups [id=8; global-counter=5; subscriber-counter=10]
   ⊞ Voice and Video Calls [id=12; global-counter=0; subscriber-counter=9]
   ⊞ Other [id=1; global-counter=0; subscriber-counter=0]
⊞ Unassigned Signature-Based Protocols
  Other Unassigned Protocols
  Unassigned Zones
```

Step 2 Enter the text to search.

Note You can include the following wildcards in the search:

- ?—any character
- • *—any string

The dialog box is populated with the search results.

Step 3 Double-click the item to take you to the screen where you can edit it. For example, if you double-click a protocol, the protocol dialog box opens on the selected protocol.

Managing Services

Services are used to classify controlled traffic.

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

Traffic is classified based on some or all of the following:

- Protocol—The protocol used by the transaction, as identified by the Service Control Engine (SCE) platform
- Initiating side—Where the transaction was initiated
- Zone—IP address of the network-side host of the transaction
- Flavor—Specific Layer 7 properties of the transaction; for example, host names of the network-side host of the transaction

A service configuration can contain up to 500 services and 10,000 service elements. Every service element in a service configuration must be unique.

Service Parameters

A service is defined by the following parameters:

- General parameters:
  - Name—A unique name
  - Description—(Optional) A description of the service
- Hierarchy parameters:
  - Parent Service

    The default service, which is the base of the service hierarchy, does not have a parent.

Note The parent service is important when services share usage counters (see next parameter).

  - Service Usage Counters—Used by the system to generate data about the total use of each service. A service can use either its own usage counters, or those of the parent service.

    Each usage counter has:

  - A name assigned by the system (based on the service name).

Note An asterisk is appended to a service usage counter name whenever the counter applies to more than one service.

  - A unique counter index—A default value of the counter index provided by the system. Do not modify this value.
- Advanced parameter:
  - Service Index—A unique number by which the system recognizes the service (changing the service name does not affect SCE platform activity). The system provides a default value of the service index. Do not modify this value.

These parameters are defined when you add a new service (see How to Add a Service to a Service Configuration, page 7-4). You can modify them at any time (see How to Edit Services, page 7-9).

Adding and Defining Services

A number of services are predefined in the Console installation. You can add additional services to a service configuration, subject to the limit of 500 services (including predefined services) per service configuration.

After you have added and defined a new service, you can add service elements to the service (see How to Add Service Elements, page 7-12).

- How to Add a Service to a Service Configuration, page 7-4
- How to Define Hierarchical Settings for a Service, page 7-5
- How to Set the Service Index, page 7-7
- How to View Services, page 7-8

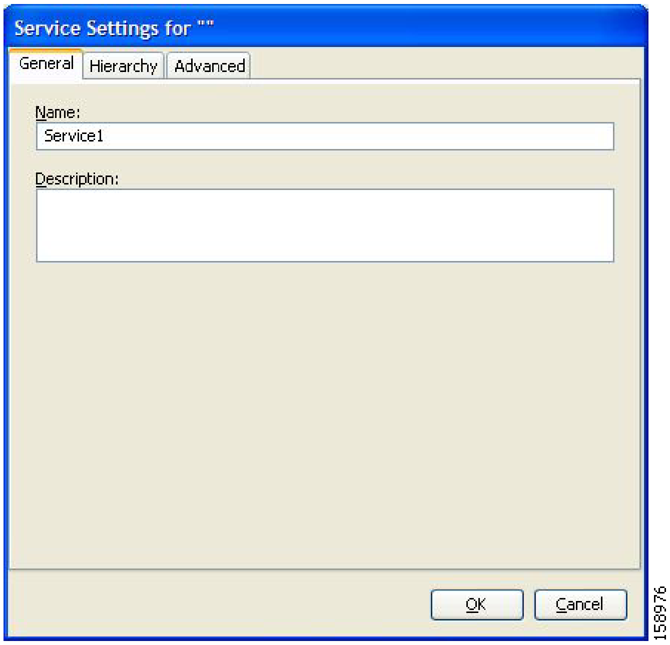
How to Add a Service to a Service Configuration

Step 1 In the Services tab, select a service from the service tree. This service is the parent of the service you are adding.

Step 2 In the left pane, click the **Add Service** (✚) icon.

The Service Settings dialog box appears (Figure 7-2).

Figure 7-2 Service Settings



Service Settings for ""

Name: Service1

Description:

Step 3 In the Name field, enter a unique and relevant name for the service.

Step 4 In the Description field, enter a meaningful and useful description of the service.

Step 5 To set exclusive usage counters for this service, or to change the parent service you selected when adding the service, continue with the instructions in the How to Define Hierarchical Settings for a Service, page 7-5 section.

Step 6 (Optional) To specify an index for this service, continue with the instructions in the How to Set the Service Index, page 7-7 section.

Note The system automatically assigns a free number for the new service. Modify this number only where a specific index value must be assigned to a specific service.

Step 7 Click **OK**.

The Service Settings dialog box closes.

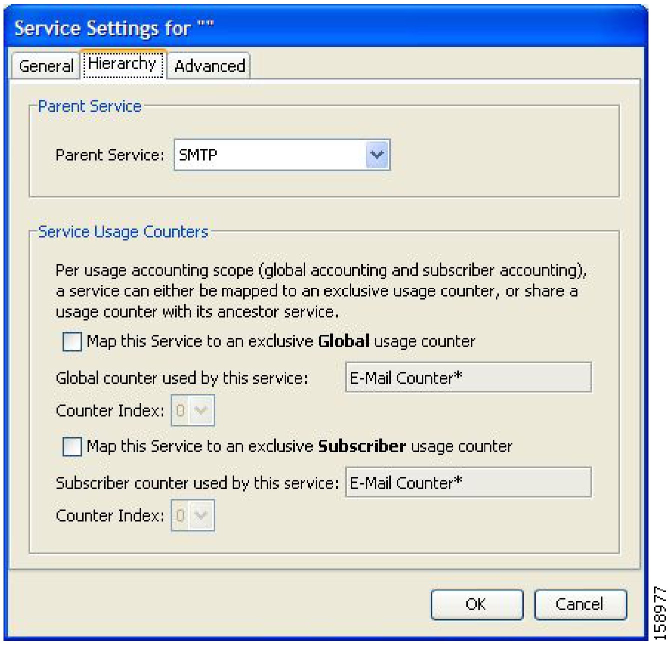
The service is added to the service tree as a child to the service you selected in the hierarchy.

How to Define Hierarchical Settings for a Service

Step 1 In the Service Settings dialog box, click the **Hierarchy** tab.

The Hierarchy tab opens (Figure 7-3).

Figure 7-3 Hierarchy Tab



Parent Service

Parent Service: SMTP

Service Usage Counters

Per usage accounting scope (global accounting and subscriber accounting), a service can either be mapped to an exclusive usage counter, or share a usage counter with its ancestor service.

□ Map this Service to an exclusive **Global** usage counter

Global counter used by this service: E-Mail Counter*

Counter Index: 0

□ Map this Service to an exclusive **Subscriber** usage counter

Subscriber counter used by this service: E-Mail Counter*

Counter Index: 0

Step 2 To set a different parent service, select the desired parent from the Parent Service drop-down list.

Step 3 By default, a new service uses the global usage counter of its parent service. To define an exclusive global usage counter, check the **Map this Service to an exclusive Global usage counter** check box.

The name in the read-only Global counter of this service field changes to reflect your choice.

The Counter Index drop-down list is enabled.

(Optional) Select a value for the counter index from the Counter Index drop-down list.

Note The system provides a default value of the counter index. Do not modify this value.

Step 4 By default, a new service uses the subscriber usage counter of its parent service. To define an exclusive subscriber usage counter, check the **Map this Service to an exclusive Subscriber usage counter** check box.

The name in the read-only Subscriber counter of this service field changes to reflect your choice.

The Counter Index drop-down list is enabled.

(Optional) Select a value for the counter index from the Counter Index drop-down list.

Note The system provides a default value of the counter index. Do not modify this value.

Step 5 To specify an index for this service, continue with the instructions in the How to Set the Service Index, page 7-7 section.

Note The system automatically assigns a free number for the new service. Modify this number only where a specific index value must be assigned to a specific service.

Step 6 Click **OK**.

The Service Settings dialog box closes.

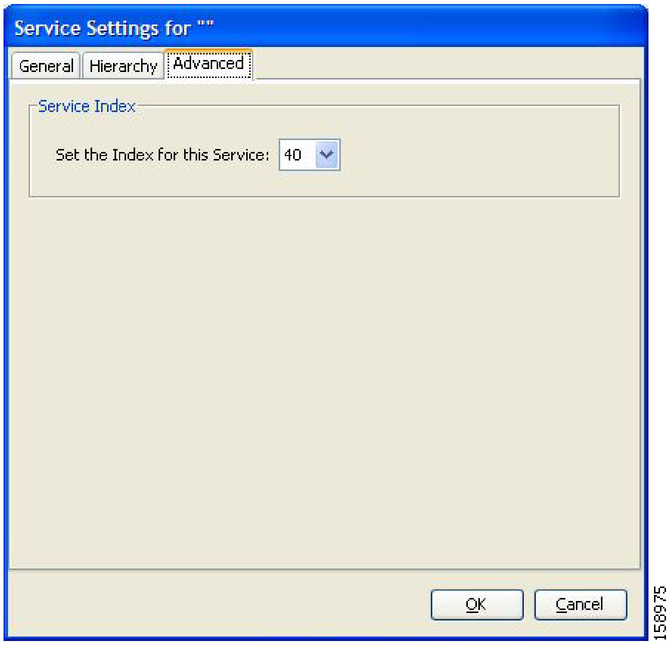
The service is added to the service tree as a child to the service selected in the Parent Service drop-down list.

How to Set the Service Index

Step 1 In the Service Settings dialog box, click the **Advanced** tab.

The Advanced tab opens (Figure 7-4).

Figure 7-4 Advanced Tab



Service Settings for ""

Set the Index for this Service: 40

Step 2 From the Set the Index for this Service drop-down list, select a service index.

The service index must be an integer in the range from 1 to 499; zero is reserved for the default service.

Note The system automatically assigns a free number for the new service. Modify this number only where a specific index value must be assigned to a specific service.

Step 3 Click **OK**.

The Service Settings dialog box closes.

The service is added to the service tree as a child to the service selected in the Parent Service drop-down list.

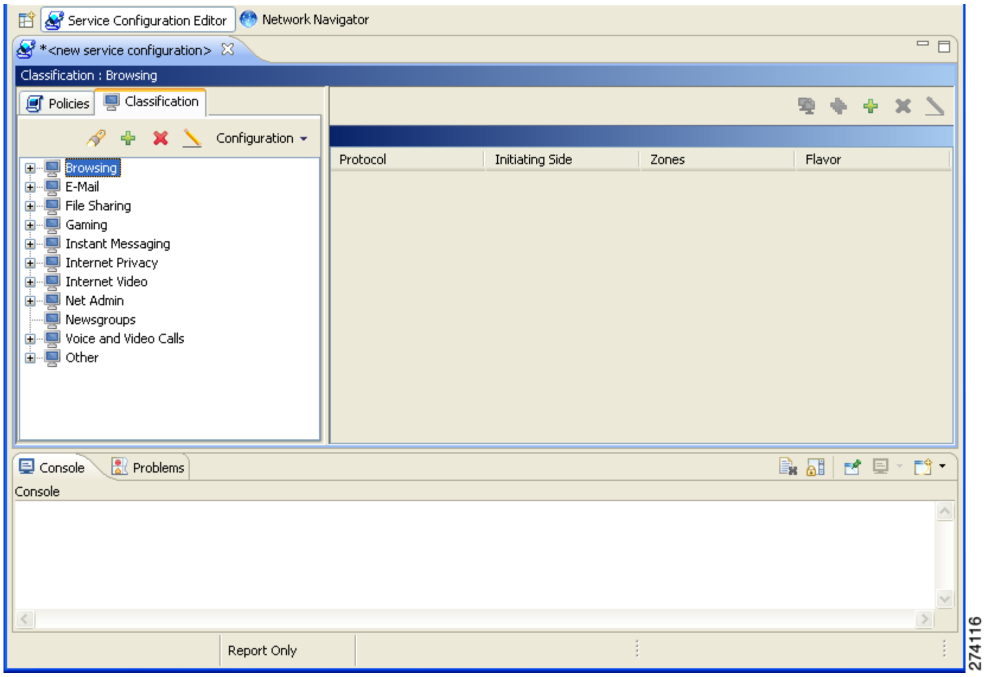
How to View Services

You can view a hierarchy tree of all existing services and see their associated service elements.

Step 1 In the current service configuration, click the **Classification** tab.

The Classification tab appears (Figure 7-5).

Figure 7-5 Classification Tab

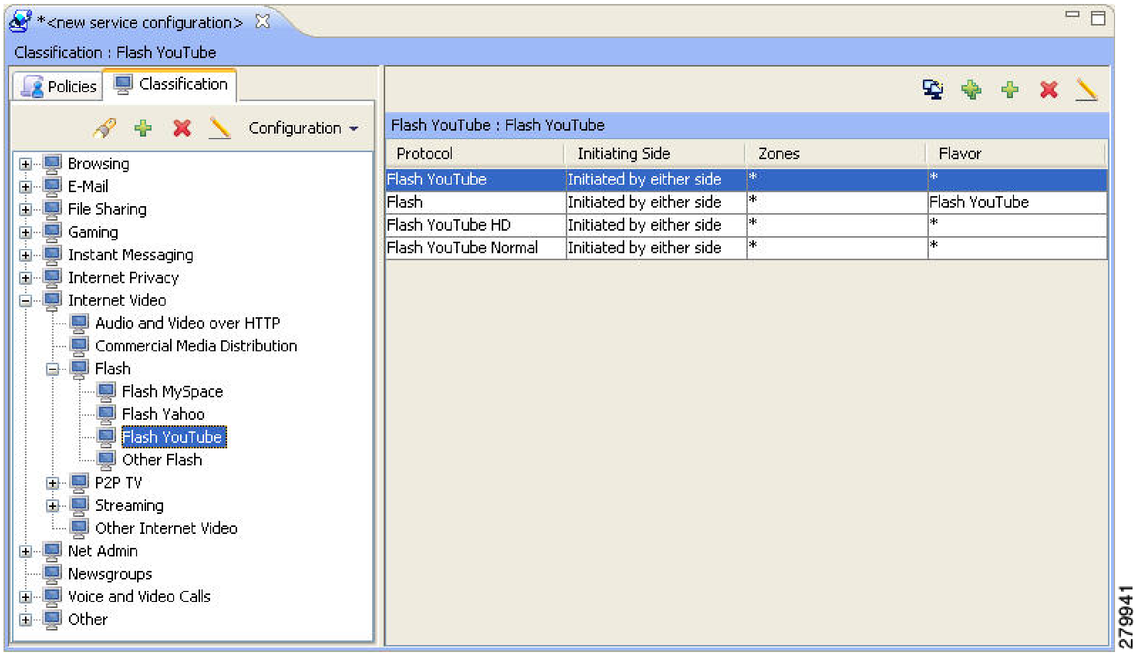


A list of all services is displayed in the service tree (left pane).

Step 2 Click a service in the hierarchy to display its service elements.

A list of all service elements defined for this service is displayed in the right (Service Elements) pane (Figure 7-6).

Figure 7-6 Service Elements



Flash YouTube : Flash YouTube

Protocol	Initiating Side	Zones	Flavor
Flash YouTube	Initiated by either side	*	*
Flash	Initiated by either side	*	Flash YouTube
Flash YouTube HD	Initiated by either side	*	*
Flash YouTube Normal	Initiated by either side	*	*

Step 3 To view more information about a service, select a service from the service tree and click the **Edit Service** (✏) icon.

The Service Settings dialog box appears.

Step 4 Click **OK**.

The Service Settings dialog box closes.

How to Edit Services

You can modify the parameters of a service, even those parameters included in the Console installation.

To add, modify, or delete service elements, see Managing Service Elements, page 7-11.

Step 1 In the Services tab, select a service from the service tree.

Step 2 In the left pane, click the **Edit Service** (✏) icon.

The Service Settings dialog box appears.

Step 3 (Optional) Give a new name to the service.

Enter a new name in the Name field.

Step 4 (Optional) Give a new description for the service.

Enter a new description in the Description field.

Step 5 To change hierarchical settings, click the **Hierarchy** tab.

The Hierarchy tab opens.

a. To set a different parent service, select the desired service from the Parent Service drop-down list.

b. To share a global usage counter with the parent service, uncheck the **Map this Service to an exclusive Global usage counter** check box.

The name of the parent service's counter is displayed in the Global counter used by this service field.

c. To define an exclusive global usage counter, check the **Map this Service to an exclusive Global usage counter** check box.

The name in the read-only Global counter of this service field changes to reflect your choice.

The Counter Index drop-down list is enabled.

Note The system provides a default value of the counter index. Do not modify this value.

d. To share a subscriber usage counter with the parent service, uncheck the **Map this Service to an exclusive Subscriber usage counter** check box.

The name of the parent service's counter is displayed in the Subscriber counter used by this service field.

e. To define an exclusive subscriber usage counter, check the **Map this Service to an exclusive Subscriber usage counter** check box.

The name in the read-only Subscriber counter of this service field changes to reflect your choice.

The Counter Index drop-down list is enabled.

Note The system provides a default value of the counter index. Do not modify this value.

Step 6 To change the service index:

a. In the Service Settings dialog box, click the **Advanced** tab.

The Advanced tab opens.

b. From the Set the Index for this Service drop-down list, select a service index.

The service index must an integer in the range from 1 to 499; zero is reserved for the default service.

Note The system provides a default value of the service index. Do not modify this value.

Step 7 Click **OK**.

The Service Settings dialog box closes.

The changes to the service are saved.

How to Delete Services

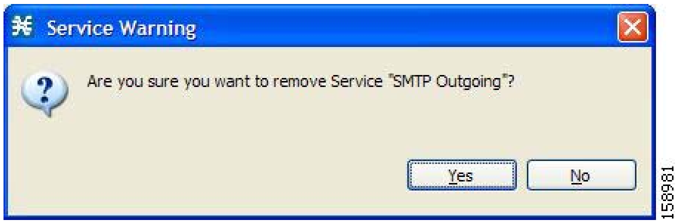
You can delete all services, even those services in the Console installation, except for the default service.

Step 1 In the Services tab, select a service from the service tree.

Step 2 In the left pane, click the **Delete Service** (✖) icon.

Step 3 A Service Warning message appears (Figure 7-7).

Figure 7-7 Service Warning



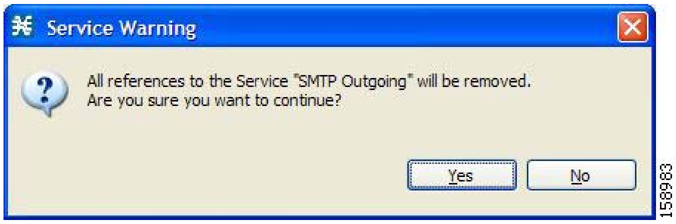
Service Warning

Are you sure you want to remove Service "SMTP Outgoing"?

Step 4 Click **Yes**.

- If any package has a rule for this service (see Managing Rules, page 9-61), a second Service Warning message appears (Figure 7-8).

Figure 7-8 Service Warning



Service Warning

All references to the Service "SMTP Outgoing" will be removed.
Are you sure you want to continue?

- Click **Yes**.

The service is deleted and is no longer displayed in the service tree. Any rules for the service are also deleted.

Children of the deleted service are not deleted; they move up one level in the service tree.

Managing Service Elements

A service is a collection of service elements; to complete the definition of a service, you must define its service elements. A service element maps a specific protocol, initiating side, zone, and flavor to the selected service.

For more information, see Managing Protocols, page 7-22, Managing Zones, page 7-34, and Managing Flavors, page 7-60.

A service configuration can contain up to 10,000 service elements. Every service element must be unique.

A service element maps a traffic flow, that meets all the following criteria, to its service:

- The flow uses the specified protocol of the service element.
- The flow is initiated by the side (network, subscriber, or either) specified for the service element.
- The destination of the flow is an address that belongs to the specified zone of the service element.
- The flow matches the specified flavor of the service element.
- The service element is the most specific service element satisfying the first four criteria.

How to Add Service Elements

When necessary, you can add new service elements to a service. (The most useful service elements are included in the Console installation.) A service may have any number of service elements (subject to the limit of 10,000 service elements per service configuration).

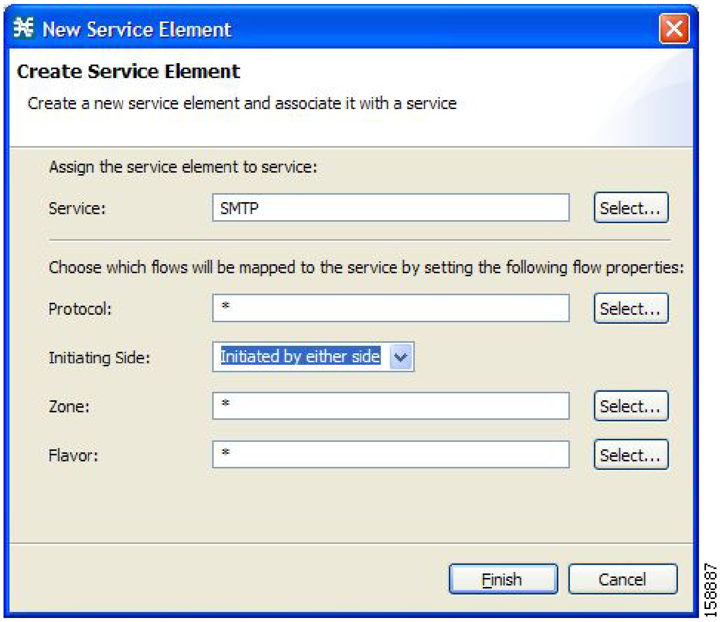
Note Every service element must be unique. If, at any stage, the new service element is the same as an existing one, an error message is displayed in the dialog box, and the Finish button is dimmed. To proceed, modify the value in at least one field.

Step 1 In the Services tab, select a service from the service tree.

Step 2 In the right (Service Elements) pane, click the **Add Service Element** (✚).

The New Service Element dialog box appears (Figure 7-9).

Figure 7-9 New Service Element



New Service Element

Create Service Element

Create a new service element and associate it with a service

Assign the service element to service:

Service: SMTP

Choose which flows will be mapped to the service by setting the following flow properties:

Protocol: *

Initiating Side: Initiated by either side

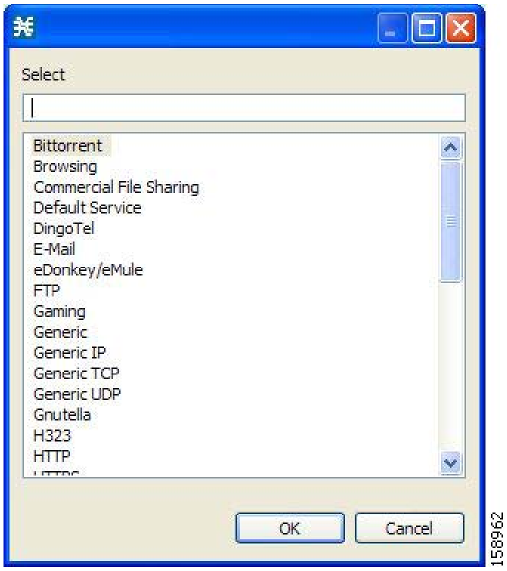
Zone: *

Flavor: *

Step 3 To change the service to which this service element is assigned, click the **Select** button next to the Service field.

The Select a Service dialog box appears (Figure 7-10), displaying a list of all services.

Figure 7-10 Select a Service



Step 4 Select a service from the list.

Step 5 Click **OK**.

The Select a Service dialog box closes.

The selected service is displayed in the Service field of the New Service Element dialog box.

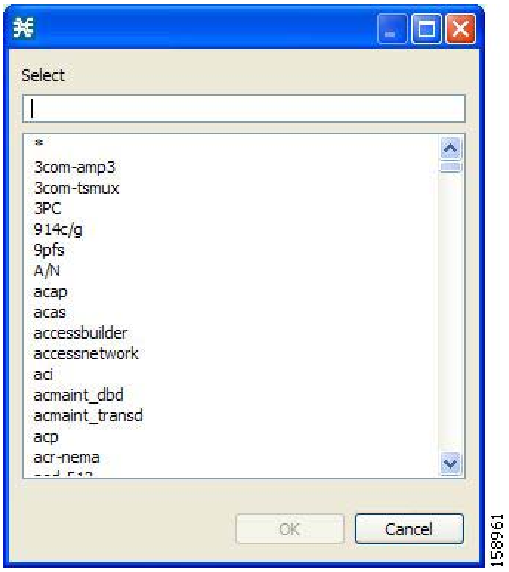
Step 6 Click the **Select** button next to the Protocol field.

Note The default value (an asterisk, *) means that no protocol checking is performed when testing whether a flow maps to this service element.

The Select a Protocol dialog box appears (Figure 7-11), displaying a list of all protocols.

Note If you select a flavor (Step 15) before you select a protocol, only protocols relevant to the selected flavor are displayed.

Figure 7-11 Select a Protocol



Select

*
3com-amp3
3com-tsmux
3PC
914c/g
9pfs
A/N
acap
acas
accessbuilder
accessnetwork
aci
acmaint_dbd
acmaint_transd
acp
acr-nema

Step 7 Select a protocol from the list. You can type in the field at the top of the dialog box to help locate the desired protocol.

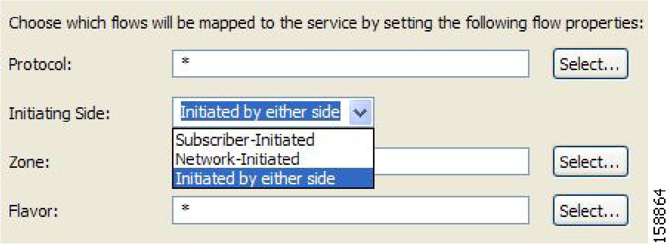
Step 8 Click **OK**.

The Select a Protocol dialog box closes.

The selected protocol is displayed in the Protocol field of the New Service Element dialog box.

Step 9 In the Initiating Side field (Figure 7-12), click the drop-down arrow.

Figure 7-12 Initiating Side Field



Choose which flows will be mapped to the service by setting the following flow properties:

Protocol: *

Initiating Side: Initiated by either side

Subscriber-Initiated
Network-Initiated
Initiated by either side

Zone:

Flavor: *

Step 10 Select the appropriate initiating side from the drop-down list.

The following options are available:

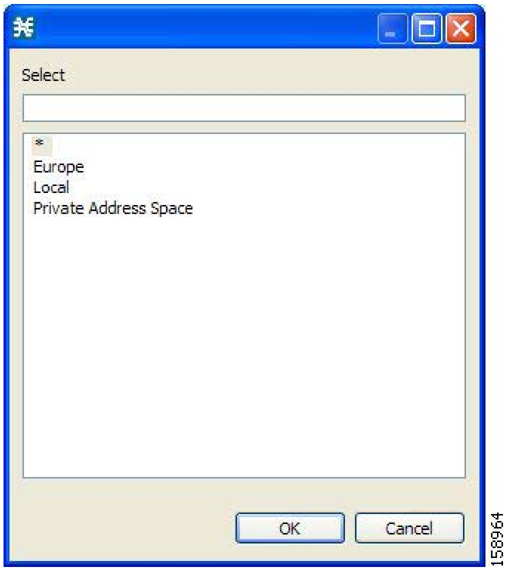
- **Subscriber-Initiated**—Transactions are initiated at the subscriber side towards (a server at) the network side.
- **Network-Initiated**—Transactions are initiated at the network side towards (a server at) the subscriber side.
- **Initiated by either side**

Step 11 Click the **Select** button next to the Zone field.

Note The default value (an asterisk, *) means that no zone checking is performed when testing whether a flow maps to this service element.

The Select a Zone dialog box appears (Figure 7-13), displaying a list of all zones.

Figure 7-13 Select a Zone



Select

*
Europe
Local
Private Address Space

Step 12 Select a zone from the list.

Step 13 Click **OK**.

The Select a Zone dialog box closes.

The selected zone is displayed in the Zone field of the New Service Element dialog box.

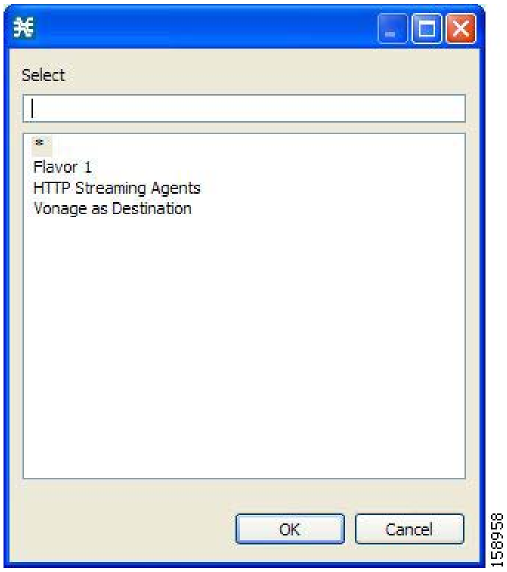
Step 14 Click the **Select** button next to the Flavor field.

Note The default value (an asterisk, *) means that no flavor checking is performed when testing whether a flow maps to this service element.

The Select a Flavor dialog box appears (Figure 7-14), displaying a list of all flavors relevant to the protocol selected in Step 7.

Note You can only select a ToS flavor if you select the default value (*, meaning any protocol) for the protocol.

Figure 7-14 Select a Flavor



Step 15 Select a flavor from the list.

Step 16 Click **OK**.

The Select a Flavor dialog box closes.

The selected flavor is displayed in the Flavor field of the New Service Element dialog box.

Step 17 Click **Finish**.

The New Service Element dialog box closes.

The new service element is added to the service.

A new row, representing the service element, is added to the service element list in the Service Elements pane.

How to Duplicate Service Elements

Duplicating an existing service element is a useful way to add a new service element similar to an existing service element. It is faster to duplicate a service element and then modify it than to define the service element from beginning.

Note Every service element must be unique. If, at any stage, the new service element is the same as an existing one, an error message is displayed in the dialog box, and the Finish button is dimmed. To proceed, modify the value in at least one field.

Step 1 In the Services tab, select a service from the service tree.

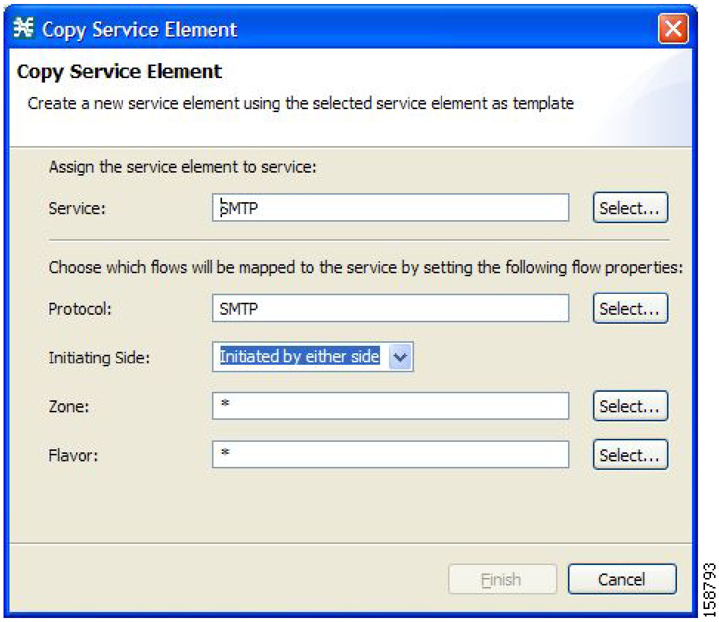
A list of associated service elements is displayed in the Service Elements pane.

Step 2 In the Service Elements pane, select a service element to duplicate.

Step 3 Click the **Duplicate Service Element** (✚) icon.

The Copy Service Element dialog box appears (Figure 7-15).

Figure 7-15 Copy Service Element



Copy Service Element

Create a new service element using the selected service element as template

Assign the service element to service:

Service: SMTP

Choose which flows will be mapped to the service by setting the following flow properties:

Protocol: SMTP

Initiating Side: Initiated by either side

Zone: *

Flavor: *

Step 4 Modify the service element (see How to Edit Service Elements, page 7-17).

Note Before you can save the new service element, you must change the value in at least one field.

How to Edit Service Elements

You can modify all service elements, even those service elements that are included in the Console installation.

Note Every service element must be unique. If, at any stage, the modified service element is the same as an existing one, an error message is displayed in the dialog box, and the Finish button is dimmed. To proceed, modify the value in at least one field.

Step 1 In the Services tab, select a service from the service tree.

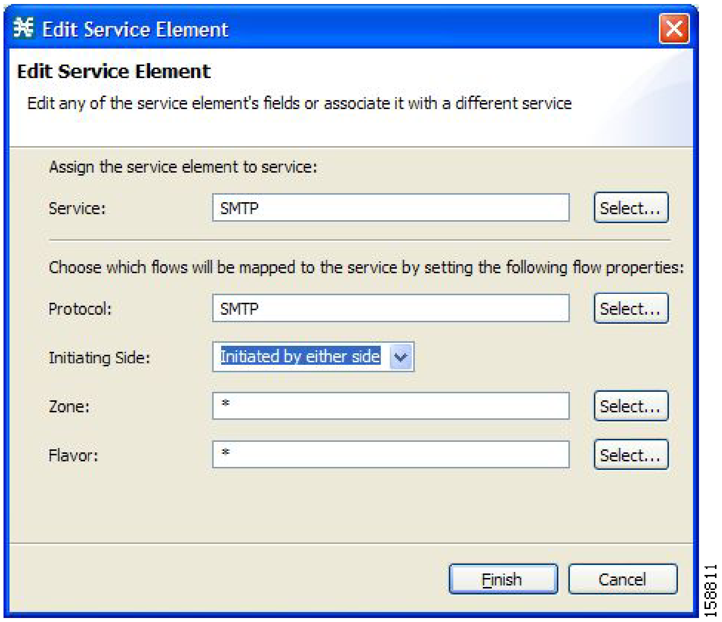
A list of associated service elements is displayed in the Service Elements pane.

Step 2 In the Service Elements pane, select a service element to edit.

Step 3 In the Service Elements pane, click the **Edit Service Element** (✎) icon.

The Edit Service Element dialog box appears (Figure 7-16).

Figure 7-16 Edit Service Element



Edit Service Element

Edit Service Element

Edit any of the service element's fields or associate it with a different service

Assign the service element to service:

Service: SMTP

Choose which flows will be mapped to the service by setting the following flow properties:

Protocol: SMTP

Initiating Side: Initiated by either side

Zone: *

Flavor: *

Step 4 To change the service to which this service element is assigned, click the **Select** button next to the Service field.

The Select a Service dialog box appears, displaying a list of all services.

Step 5 Select a service from the list.

Step 6 Click **OK**.

The Select a Service dialog box closes.

The selected service is displayed in the Service field of the Edit Service Element dialog box.

Step 7 To change the protocol of this service element, click the **Select** button next to the Protocol field.

Note An asterisk (*) means that no protocol checking is performed when testing whether a flow maps to this service element.

The Select a Protocol dialog box appears, displaying a list of all protocols.

Step 8 Select a protocol from the list; you can type in the field at the top of the dialog box to help locate the desired protocol.

Step 9 Click **OK**.

The Select a Protocol dialog box closes.

The selected protocol is displayed in the Protocol field of the Edit Service Element dialog box.

Step 10 To change the initiating side of this service element, click the drop-down arrow in the Initiating Side field.

Step 11 Select the appropriate initiating side from the drop-down list.

The following options are available:

- **Subscriber-Initiated**—Transactions are initiated at the subscriber side towards (a server at) the network side.
- **Network-Initiated**—Transactions are initiated at the network side towards (a server at) the subscriber side.
- **Initiated by either side**

Step 12 To change the zone of this service element, click the **Select** button next to the Zone field.

Note An asterisk (*) means that no zone checking is performed when testing whether a flow maps to this service element.

The Select a Zone dialog box appears, displaying a list of all zones.

Step 13 Select a zone from the list.

Step 14 Click **OK**.

The Select a Zone dialog box closes.

The selected zone is displayed in the Zone field of the Edit Service Element dialog box.

Step 15 To change the flavor of this service element, click the **Select** button next to the Flavor field.

Note An asterisk (*) means that no flavor checking is performed when testing whether a flow maps to this service element.

The Select a Flavor dialog box appears, displaying a list of all flavors.

Step 16 Select a flavor from the list.

Step 17 Click **OK**.

The Select a Flavor dialog box closes.

The selected flavor is displayed in the Flavor field of the Edit Service Element dialog box.

Step 18 Click **Finish**.

The Edit Service Element dialog box closes.

The changes to the service element are saved.

The changes to the service element appear in the service element list in the Service Elements pane.

How to Delete Service Element

You can delete all service elements, even those service elements that are included in the Console installation.

Step 1 In the Services tab, select a service from the service tree.

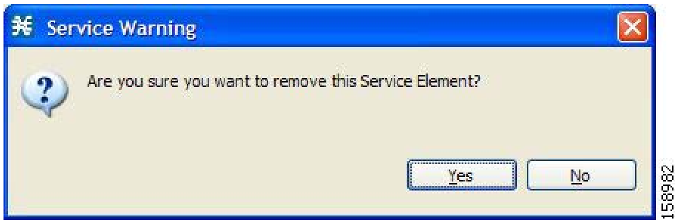
A list of associated service elements is displayed in the Service Elements pane.

Step 2 In the Service Elements pane, select a service element to delete.

Step 3 In the Service Elements pane, click the **Delete Service Element** (✖) icon.

A Service Warning message appears (Figure 7-17).

Figure 7-17 Service Warning



Service Warning

Are you sure you want to remove this Service Element?

Step 4 Click **Yes**.

The service element is deleted and is no longer part of the selected service.

How to Move Service Elements

You can move an existing service element from one service to a different service.

Step 1 In the Services tab, select a service from the service tree.

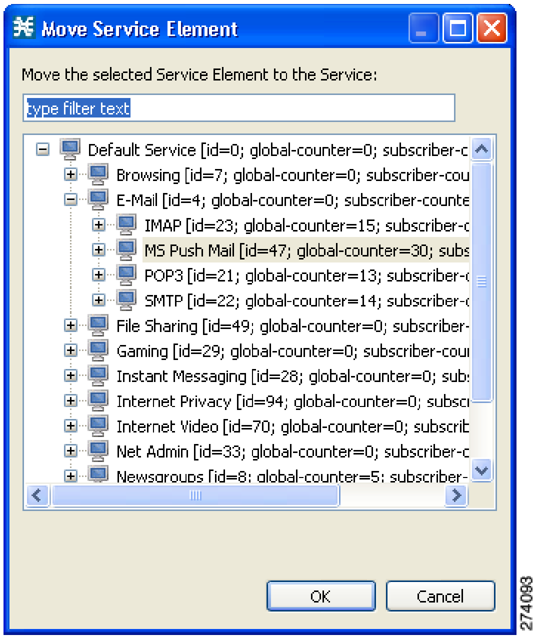
A list of associated service elements is displayed in the Service Elements pane.

Step 2 In the Service Elements pane, select a service element to move.

Step 3 Click the **Move Service Element to Another Service** ( ) icon.

The Move Service Element dialog box appears (Figure 7-18), displaying the complete service tree.

Figure 7-18 Move Service Element



Move Service Element

Move the selected Service Element to the Service:

type filter text

```
⊟ Default Service [id=0; global-counter=0; subscriber-c
    ⊞ Browsing [id=7; global-counter=0; subscriber-cou
    ⊟ E-Mail [id=4; global-counter=0; subscriber-counte
        ⊞ IMAP [id=23; global-counter=15; subscriber-c
        ⊞ MS Push Mail [id=47; global-counter=30; subs
        ⊞ POP3 [id=21; global-counter=13; subscriber-c
        ⊞ SMTP [id=22; global-counter=14; subscriber-c
    ⊞ File Sharing [id=49; global-counter=0; subscriber-
    ⊞ Gaming [id=29; global-counter=0; subscriber-cour
    ⊞ Instant Messaging [id=28; global-counter=0; sub:
    ⊞ Internet Privacy [id=94; global-counter=0; subscri
    ⊞ Internet Video [id=70; global-counter=0; subscrib
    ⊞ Net Admin [id=33; global-counter=0; subscriber-c
    ⊞ Newsgroups [id=8; global-counter=5; subscriber-
```

Step 4 From the service tree, select a service.

Step 5 Click **OK**.

The Move Service Element dialog box closes.

The service element is moved to the selected service.

Managing Protocols

A protocol is composed of an application protocol signature, the destination port or ports, a unique name, and an optional description.

Protocols are used to define service elements (see the "Managing Service Elements" section on page 7-11).

You can add new protocols (for example, to classify a new gaming protocol that uses a specific port). You can also edit or delete existing ones.

A service configuration can contain up to 10,000 protocols.

Cisco SCA BB supports many commercial and common protocols.

For a complete list of protocols included with the current release of Cisco SCA BB, see the "Information About Protocols" section in the "Default Service Configuration Reference Tables" chapter of *Cisco Service Control Application for Broadband Reference Guide.*

- Viewing Protocols, page 7-22
- How to Add Protocols, page 7-26
- How to Edit Protocols, page 7-27
- How to Delete Protocols, page 7-28
- Managing Protocol Elements, page 7-28

As new protocols are released, Cisco provides files containing the new protocol signatures so that you can add the signatures to your service configuration. See the "How to Import a Dynamic Signature Script into a Service Configuration" section on page 7-51.

Viewing Protocols

- How to View Protocols, page 7-23
- How to Filter the Protocols List, page 7-24

How to View Protocols

You can view a list of all protocols and their associated protocol elements.

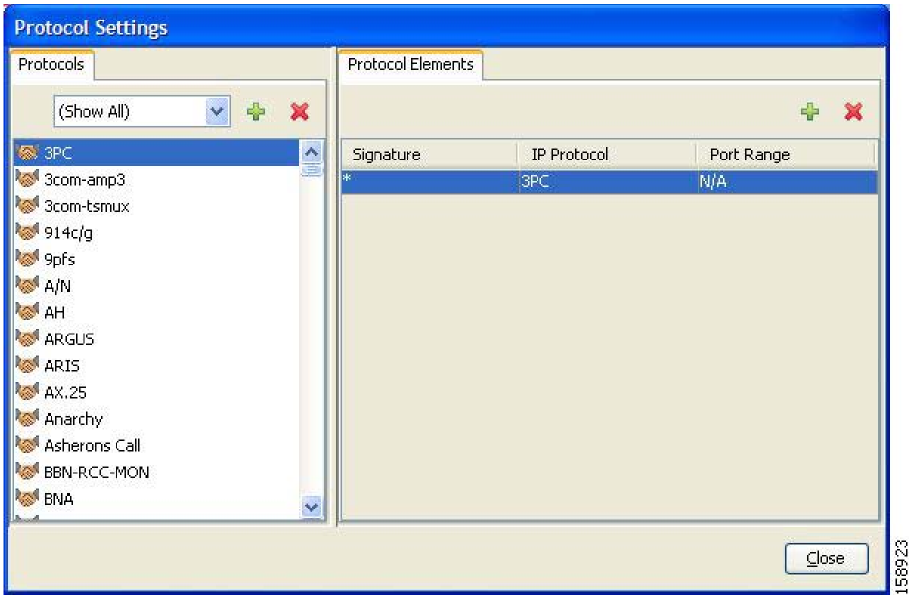
The protocols are listed in ASCII sort order (that is, 0... 9, A... Z, a... z).

The protocol elements are not sorted; they are listed in the order in which they were added to the protocol.

Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > Protocols**.

The Protocol Settings dialog box appears (Figure 7-19).

Figure 7-19 Protocol Settings



- 3PC
- 3com-amp3
- 3com-tsmux
- 914c/g
- 9pfs
- A/N
- AH
- ARGUS
- ARIS
- AX.25
- Anarchy
- Asherons Call
- BBN-RCC-MON
- BNA

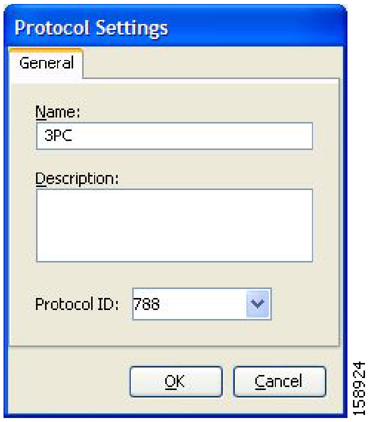
Signature	IP Protocol	Port Range
*	3PC	N/A

The Protocols tab displays a list of existing protocols.

Step 2 Double-click a protocol to view its description and ID.

The Protocol Settings dialog box appears (Figure 7-20), displaying the protocol name, description, and ID.

Figure 7-20 Protocol Settings



Protocol Settings

General

Name: 3PC

Description:

Protocol ID: 788

Step 3 Click **Cancel**.

The Protocol Settings dialog box closes.

Step 4 To view a list of protocol elements, select a protocol in the list in the Protocol Settings dialog box.

Protocol elements are displayed in the Protocol Elements tab.

Step 5 Click **Close**.

The Protocol Settings dialog box closes.

How to Filter the Protocols List

You can filter the protocols by type, so that the Protocols tab displays only the selected type of protocol.

The categories of protocols include:

- Generic Protocols—Generic IP, Generic TCP, and Generic UDP protocols, used for transactions that are not specifically mapped to a protocol by any other protocol type.
- IP Protocols—Protocols (such as ICMP), other than TCP and UDP protocols, identified according to the IP protocol number of the transaction.
- Port-Based Protocols—TCP and UDP protocols, classified according to their well-known ports. The default service configuration includes more than 750 common port-based protocols.
- Signature-Based Protocols—Protocols classified according to a Layer 7 application signature. Includes the most common protocols, such as HTTP and FTP, and a large group of popular P2P protocols.
- P2P Protocols—Peer-to-peer file-sharing application protocols, classified according to a Layer 7 application signature.
- VoIP Protocols—Voice-over-IP application protocols, classified according to a Layer 7 application signature.

- SIP Protocols—Protocols classified according to a Layer 7 application signature that is SIP or has SIP characteristics.
- Worm Protocols—Protocols classified according to a Layer 7 application signature that is based on traffic patterns of internet worms.
- Packet Stream Pattern Based Protocols—Protocols classified according to a Layer 7 application signature that is based on the pattern of the packet stream (for example, the stream's symmetry, average packet size, and rate) rather than on the payload content of the packet.
- Unidirectionally Detected Protocols—Protocols having a unidirectional signature.
- Behavioral Protocols
- E-Mail and Newsgroup Protocols
- Gaming Protocols
- HTTP Protocols
- Instant Messaging Protocols
- Net Admin Protocols
- Video Protocols
- Tunneling Protocols
- ClickStream Protocols

Note Some protocols belong to more than one category. In particular, all predefined P2P, VoIP, SIP, Worm, and Packet Stream Pattern-Based Protocols are also defined as Signature-Based Protocols.

Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > Protocols**.

The Protocol Settings dialog box appears.

Step 2 From the drop-down list in the Protocols tab, select the type of protocol to display.

The protocols of the selected type appear in the Protocols tab.

Step 3 Click **Close**.

The Protocol Settings dialog box closes.

Note The setting in the drop-down list is not saved. The next time you open the Protocol Settings dialog box, all protocols are displayed.

How to Add Protocols

You can add new protocols to a service configuration, subject to the limit of 10,000 protocols per service configuration.

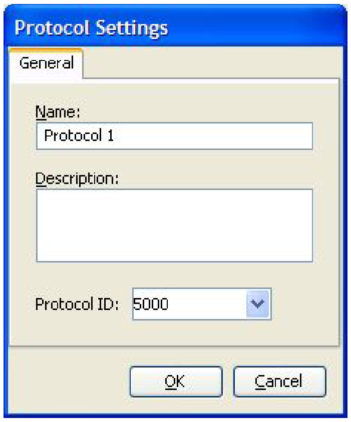
Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > Protocols**.

The Protocol Settings dialog box appears.

Step 2 In the Protocols tab, click the **Add Protocol** (✚) icon.

The Protocol Settings dialog box appears (Figure 7-21).

Figure 7-21 Protocol Settings



Protocol Settings

General

Name: Protocol 1

Description:

Protocol ID: 5000

Step 3 In the Name field, enter a unique name for the new protocol.

Step 4 (Optional) From the Protocol ID drop-down list, select an ID for the protocol.

The protocol ID must be an integer in the range from 5000 to 9998; lower values are reserved for protocols provided by Cisco SCA BB.

Note The system provides the value of the protocol ID. Do not modify this field.

Step 5 Click **OK**.

The Protocol Settings dialog box closes.

The new protocol is displayed in the Protocols tab. You can now add protocol elements to it. See How to Add Protocol Elements, page 7-29.

How to Edit Protocols

You can modify the parameters of a protocol, even those for those protocols that are included in the Console installation.

To add, modify, or delete protocol elements, see Managing Protocol Elements, page 7-28.

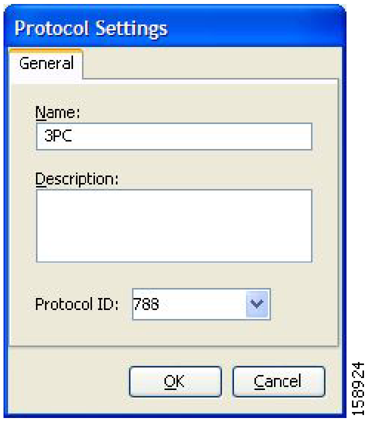
Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > Protocols**.

The Protocol Settings dialog box appears.

Step 2 In the Protocols tab, double-click a protocol.

A second Protocol Settings dialog box appears (Figure 7-22).

Figure 7-22 Protocol Settings



Protocol Settings

Name: 3PC

Description:

Protocol ID: 788

Step 3 Modify fields in the Protocol Settings dialog box.

- In the Name field, enter a new name for the protocol.
- From the Protocol ID drop-down list, select an ID for the protocol.

  The protocol ID must be an integer in the range from 5000 to 9998; lower values are reserved for protocols provided by Cisco SCA BB.

Note The system provides the protocol ID. Do not modify this field.

Step 4 Click **OK**.

The Protocol Settings dialog box closes.

The new values of the protocol parameters are saved.

Step 5 Click **Close**.

The Protocol Settings dialog box closes.

How to Delete Protocols

You can delete all protocols, even those protocols that are included in the Console installation.

Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > Protocols**.

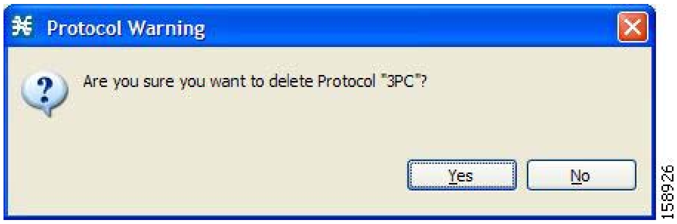
The Protocol Settings dialog box appears.

Step 2 In the Protocols tab, select a Protocol.

Step 3 In the Protocols tab, click the **Delete Protocol** (✖) icon.

A Protocol Warning message appears (Figure 7-23).

Figure 7-23 Protocol Warning

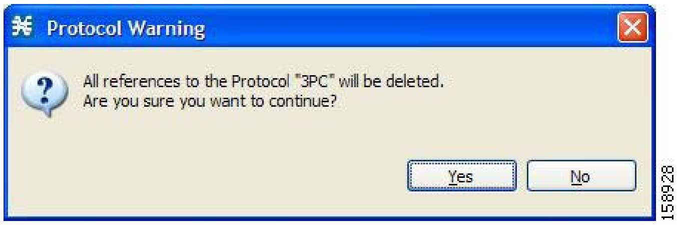

Protocol Warning

Are you sure you want to delete Protocol "3PC"?

Step 4 Click **Yes**.

- If any service element maps the selected protocol to a service (see Managing Service Elements, page 7-11), a second Protocol Warning message appears (see Figure 7-24) (even if the service is not used by any package).

Figure 7-24 Protocol Warning


Protocol Warning

All references to the Protocol "3PC" will be deleted.
Are you sure you want to continue?

- Click **Yes**.

The Protocol is deleted from the Protocols tab.

Step 5 Click **Close**.

The Protocol Settings dialog box closes.

Managing Protocol Elements

A protocol is a collection of protocol elements.

To complete the definition of a protocol, you must define its protocol elements. A protocol element maps a specific signature, IP protocol, and port range to the selected protocol. Every protocol element in a service configuration must be unique.

If a traffic flow meets all of the following four criteria, it is mapped to a specific protocol:

- The flow belongs to the specified signature of the protocol element.
- The flow protocol is the specified IP protocol of the protocol element.
- (If the IP protocol is TCP or UDP) The destination port is within the specified port range of the protocol element.
- The protocol element is the most specific protocol element satisfying the first three criteria.

How to Add Protocol Elements

You can add any number of protocol elements to a protocol.

Note When you set the parameters of the protocol element, the values of the parameters are saved as you enter them.

Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > Protocols**.

The Protocol Settings dialog box appears.

Step 2 In the Protocols tab, select a protocol.

Step 3 In the Protocol Elements tab, click the **Add Protocol Element** (➕) icon.

A protocol element is added to the protocol.

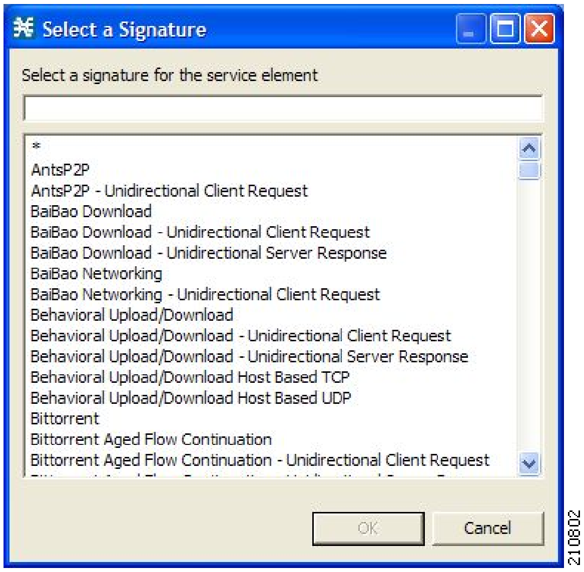
A new row, representing the protocol element, is added to the protocol element list in the Protocol Element tab.

Step 4 Click in the Signature cell of the protocol element, and then click the **Browse** button that appears in the cell.

Note The default value (an asterisk, *) means that no signature checking is performed when testing whether a flow maps to this protocol element.

The Select a Signature dialog box appears (Figure 7-25), displaying a list of all signatures.

Figure 7-25 Select a Signature



Select a Signature

Select a signature for the service element

*
AntsP2P
AntsP2P - Unidirectional Client Request
BaiBao Download
BaiBao Download - Unidirectional Client Request
BaiBao Download - Unidirectional Server Response
BaiBao Networking
BaiBao Networking - Unidirectional Client Request
Behavioral Upload/Download
Behavioral Upload/Download - Unidirectional Client Request
Behavioral Upload/Download - Unidirectional Server Response
Behavioral Upload/Download Host Based TCP
Behavioral Upload/Download Host Based UDP
Bittorrent
Bittorrent Aged Flow Continuation
Bittorrent Aged Flow Continuation - Unidirectional Client Request

Step 5 Select a signature from the list.

Note Select the Generic signature to allow a flow that has no matching signature in the protocol signature database to be mapped to this protocol element (if the flow also matches the IP protocol and port range of the protocol element).

Step 6 Click **OK**.

The Select a Signature dialog box closes.

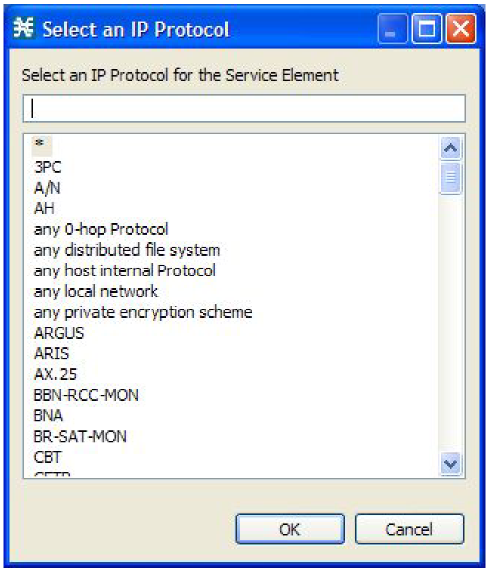
The selected signature is displayed in the Signature cell of the Protocol Settings dialog box.

Step 7 Click in the IP Protocol cell of the protocol element, and then click the **Browse** button that appears in the cell.

Note The default value (an asterisk, *) means that no IP protocol checking is performed when testing whether a flow maps to this protocol element.

The Select an IP Protocol dialog box appears (Figure 7-26), displaying a list of all IP protocols.

Figure 7-26 Select an IP Protocol



Select an IP Protocol

Select an IP Protocol for the Service Element

*
3PC
A/N
AH
any 0-hop Protocol
any distributed file system
any host internal Protocol
any local network
any private encryption scheme
ARGUS
ARIS
AX.25
BBN-RCC-MON
BNA
BR-SAT-MON
CBT

Step 8 Select an IP protocol from the list.

Step 9 Click **OK**.

The Select an IP Protocol dialog box closes

The selected IP protocol is displayed in the IP Protocol cell of the Protocol Settings dialog box.

Step 10 In the Port Range cell, enter a port or range of ports. (For a range of ports, use a hyphen between the first and last ports in the range.)

Note Specifying a port range is only possible when the specified IP protocol is either TCP or UDP (or undefined, taking the wild-card value, *).

Only a flow whose port matches one of these ports are mapped to this protocol element.

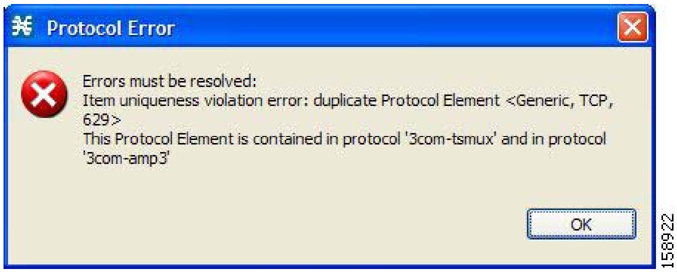
The protocol element is defined.

Step 11 Click **Close**.

The Protocol Settings dialog box closes.

- Instead, if the protocol element that you have defined is not unique in this service configuration, a Protocol Error message appears (Figure 7-27).

Figure 7-27 Protocol Error



Protocol Error

Errors must be resolved:
Item uniqueness violation error: duplicate Protocol Element <Generic, TCP, 629>
This Protocol Element is contained in protocol '3com-tsmux' and in protocol '3com-amp3'

a. Click **OK**.

b. Modify or delete the protocol element.

c. Click **Close**.

The Protocol Settings dialog box closes.

How to Edit Protocol Elements

You can modify all protocol elements, even those protocol elements that are included in the Console installation.

Note All changes to the protocol element are saved as you make them.

Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > Protocols**.

The Protocol Settings dialog box appears.

Step 2 In the Protocols tab, select a protocol.

Step 3 In the Protocol Elements tab, select a protocol element.

Step 4 Click in the Signature cell of the protocol element, and then click the **Browse** button that appears in the cell.

The Select a Signature dialog box appears.

Step 5 Select a signature from the list.

Step 6 Click **OK**.

The Select a Signature dialog box closes.

Step 7 Click in the IP Protocol cell of the protocol element, and then click the **Browse** button that appears in the cell.

The Select an IP Protocol dialog box appears.

Step 8 Select an IP protocol from the list.

Step 9 Click **OK**.

The Select an IP Protocol dialog box closes.

Step 10 In the Port Range cell of the protocol element, enter a port or range of ports.

Changes to the protocol element are saved as you make them.

Step 11 Click **Close**.

The Protocol Settings dialog box closes.

- Instead, if the protocol element that you have modified is not unique in this service configuration, a Protocol Error message appears.

a. Click **OK**.

b. Modify or delete the protocol element.

c. Click **Close**.

The Protocol Settings dialog box closes.

How to Delete Protocol Elements

You can delete all protocol elements, even those protocol elements that are included in the Console installation.

Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > Protocols**.

The Protocol Settings dialog box appears.

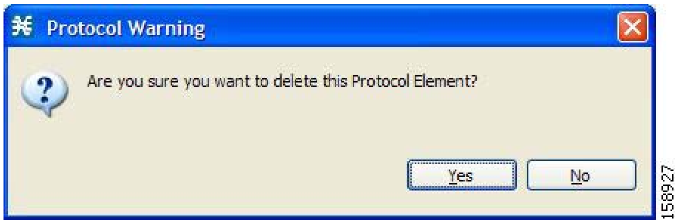
Step 2 Select a protocol in the Protocols tab.

Step 3 In the Protocol Elements tab, select a protocol element.

Step 4 In the Protocol Elements tab, click the **Delete Protocol Element** (✖) icon.

A Protocol Warning message appears (Figure 7-28).

Figure 7-28 Protocol Warning



Protocol Warning

Are you sure you want to delete this Protocol Element?

Step 5 Click **Yes**.

The protocol element is deleted from the Protocol Elements tab.

Step 6 Click **Close**.

The Protocol Settings dialog box closes.

Managing Zones

A zone is a collection of destination IP addresses; usually the addresses in one zone are related in some way.

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

A service configuration can contain up to 10,000 zone items on Cisco SCE 2000 and up to 20,000 on Cisco SCE 8000. Every zone item must be unique.

- How to View Zones, page 7-35
- How to Add Zones, page 7-36
- How to Edit Zones, page 7-38
- How to Delete Zones, page 7-39
- Managing Zone Items, page 7-40
- Importing zones, see How to Import Service Configuration Data, page 6-11
- Exporting zones, see How to Export Service Configuration Data, page 6-7

BGP Autonomous System Dynamic Detection

The BGP Autonomous System (BGP AS) Dynamic Detection feature enables you to provision the BGP autonomous system as IP prefixes to the Cisco SCE zones.

With the BGP AS Dynamic Detection feature, you can:

- Add the complete AS number node and all the IP prefixes under it to a new zone.
- Add the IP Prefixes obtained from the AS number nodes to an existing zone.
- Add IP prefixes to a new zone.
- Delete IP prefixes from a zone.

For details, see the following sections:

- BGP AS Dynamic Detection Workflow, page 7-42
- Enabling BGP AS Dynamic Detection, page 7-42
- Collecting and Storing the BGP Autonomous System (AS) Details, page 7-43
- Creating a New Zone with Select BGP AS Numbers and Prefixes, page 7-44
- Understanding BGP AS Numbers and Prefixes Color Schema, page 7-45
- Updating a Zone with Select BGP AS Numbers and Prefixes, page 7-45
- Deleting IP Prefixes from a Zone, page 7-45

How to View Zones

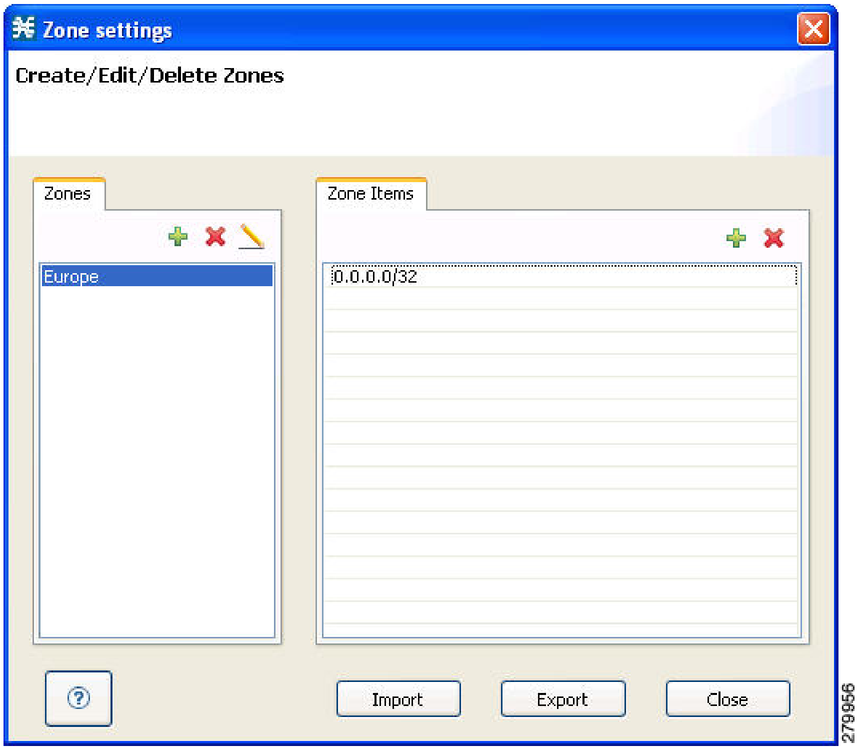
You can view a list of all zones and their associated zone items.

Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > Zones**.

The Zone Settings dialog box appears (Figure 7-29).

The Zones tab displays a list of all zones. The first zone in the list is selected, and its zone items are displayed in the Zone Items tab.

Figure 7-29 Zone Settings



Step 2 Click a zone in the list to display its zone items.

The zone items of the selected zone are displayed in the Zone Items tab.

Step 3 Click **Close**.

Timesaver If you enable the automatic zone provisioning, an Advanced Import button will be available. Click the **Advanced Import** button to import the BGP AS numbers and prefixes to create Zones. See the "Creating a New Zone with Select BGP AS Numbers and Prefixes" section on page 7-44.

How to Add Zones

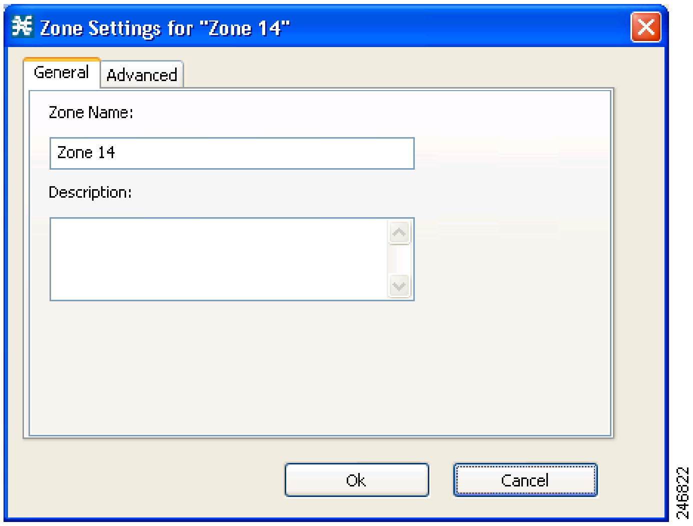
Step 1 From the Classification tab in the left pane, choose **Configuration** > **Classification** > **Zones**.

The Zone Settings dialog box appears.

Step 2 In the Zones tab, click the **Add Zone** (✚) icon.

The Zone Settings dialog box appears (Figure 7-30).

Figure 7-30 Zone Settings


Zone Settings for "Zone 14"

Zone Name: Zone 14

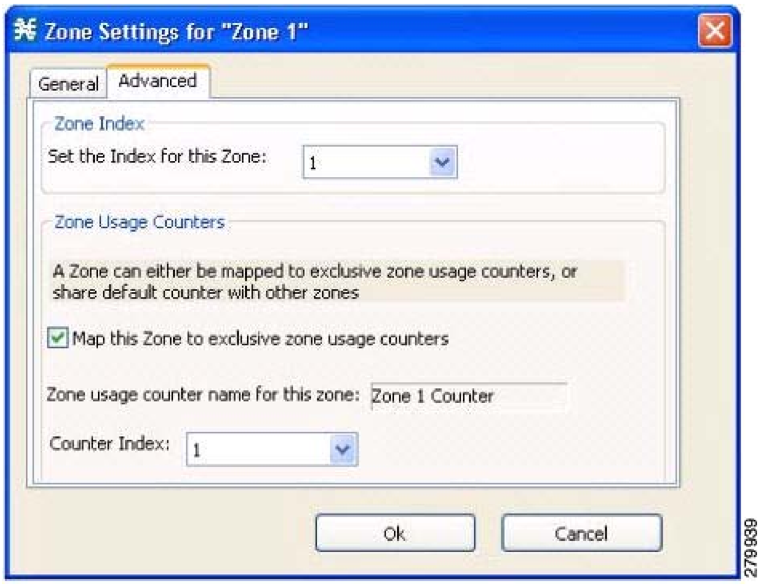
Description:

Step 3 In the Name field, enter a unique name for the new zone.

Step 4 From the Advanced tab, from the Zone Index drop-down list, select an ID for the zone. The zone ID must be a positive integer in the range from 1 to 32767.

Note The system provides the value of the zone ID. Do not modify this field.

Figure 7-31 Zone Settings - Advanced Tab



Zone Settings for "Zone 1"

General | Advanced

Zone Index

Set the Index for this Zone: 1

Zone Usage Counters

A Zone can either be mapped to exclusive zone usage counters, or share default counter with other zones

☑ Map this Zone to exclusive zone usage counters

Zone usage counter name for this zone: Zone 1 Counter

Counter Index: 1

Step 5 Check the **Map this Zone to exclusive zone usage counters** check box to map the Zone to exclusive zone usage counters, or share default counter with other zones.

The Zone Settings dialog box appears (Figure 7-31).

Step 6 From the Counter Index drop-down list, select an index for the zone.

The Counter Index must be a positive integer in the range from 1 to 1023.

Step 7 Click **OK**.

The Zone Settings dialog box closes.

The new zone is added to the Zones tab. You can now add zone items. (See How to Add Zone Items, page 7-40.)

How to Edit Zones

You can modify zone parameters at any time.

To add, modify, or delete zone items, see Managing Zone Items, page 7-40.

Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > Zones**.

The Zone Settings dialog box appears.

Step 2 In the Zones tab, select a zone.

Step 3 Click the **Edit Zone** (✏) icon.

The Zone Settings dialog box appears.

Step 4 Modify fields in the dialog box.

- In the Name field, enter a new name for the zone.
- From the Zone Index drop-down list, select an ID for the zone.

  The zone ID must be a positive integer in the range from 1 to 32767.

Note The system provides the value of the zone ID. Do not modify this field.

Step 5 Click **OK**.

The Zone Settings dialog box closes.

The new values of the zone parameters are saved.

Step 6 Click **Close**.

The Zone Settings dialog box closes.

How to Delete Zones

You can delete any or all zones.

Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > Zones**.

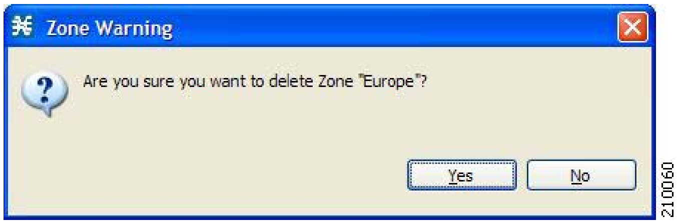
The Zone Settings dialog box appears.

Step 2 In the Zones tab, select a zone.

Step 3 In the Zones tab, click the **Delete Zone** (✖) icon.

A Zone Warning message appears (Figure 7-32).

Figure 7-32 Zone Warning



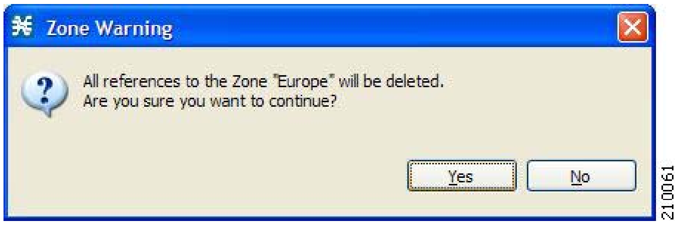
Zone Warning

Are you sure you want to delete Zone "Europe"?

Step 4 Click **OK**.

- If any service element references the selected zone, a second Zone Warning message appears (Figure 7-33).

Figure 7-33 Zone Warning



Zone Warning

All references to the Zone "Europe" will be deleted.
Are you sure you want to continue?

- Click **Yes**.

  Every service element that references the selected zone is deleted.

The zone is deleted and is no longer displayed in the Zones tab.

Step 5 Click **Close**.

The Zone Settings dialog box closes.

Managing Zone Items

A zone is a collection of related zone items. A zone item is an IP address or a range of IP addresses.

A service configuration can contain up to 20,000 zone items on SCE8000 and up to 10,000 zone items on SCE2000. Every zone item must be unique.

How to Add Zone Items

You can add several zone items to a zone. Limit is 10,000 zone items per service configuration on SCE2000 and 20,000 zone items per service configuration on SCE8000.

Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > Zones**.

The Zone Settings dialog box appears.

Step 2 In the Zones tab, select a zone.

Step 3 In the Zone Items tab, click the **Add Zone Item** (✚) icon.

A new line is added to the Zone Items table.

Step 4 Double-click the new list item and enter a valid value.

A valid value is either a single IP address (for example, 63.111.106.7) or a range of IP addresses (for example, 194.90.12.0/24).

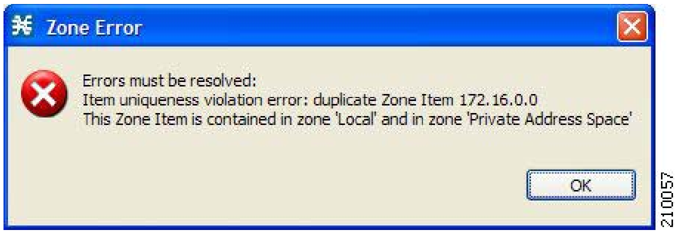
Step 5 Repeat Steps 3 and 4 for other IP addresses that are part of this zone.

Step 6 Click **Close**.

The Zone Settings dialog box closes.

- Instead, if the zone item that you have defined is not unique in this service configuration, a Zone Error message appears (Figure 7-34).

Figure 7-34 Zone Error



Zone Error

Errors must be resolved:
Item uniqueness violation error: duplicate Zone Item 172.16.0.0
This Zone Item is contained in zone 'Local' and in zone 'Private Address Space'

a. Click **OK**.

b. Modify or delete the zone item.

c. Click **Close**.

The Zone Settings dialog box closes.

How to Edit Zone Items

Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > Zones**.

The Zone Settings dialog box appears.

Step 2 In the Zones tab, select a zone.

Step 3 In the Zone Items tab, double-click a zone item.

Step 4 Enter a new value for the zone item.

A valid value is either a single IP address (for example, 63.111.106.7) or a range of IP addresses (for example, 194.90.12.0/24).

Step 5 Click **Close**.

The Zone Settings dialog box closes.

- Instead, if the zone item that you have modified is not unique in this service configuration, a Zone Error message appears.

a. Click **OK**.

b. Modify or delete the zone item.

c. Click **Close**.

The Zone Settings dialog box closes.

How to Delete Zone Items

Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > Zones**.

The Zone Settings dialog box appears.

Step 2 In the Zones tab, select a zone.

Step 3 In the Zone Items tab, select a zone item.

Step 4 In the Zone Items tab, click the **Delete Zone Item** (✖) icon.

The zone item is deleted.

Step 5 Click **Close**.

The Zone Settings dialog box closes.

BGP AS Dynamic Detection Workflow

This section provides details on the BGP AS Dynamic Detection workflow:

1. When you run the asFetch.bat script, the script downloads the AS number and IP prefixes from the configured BGP router using the SNMP MIBs
2. The script converts the prefixes to IP ranges and stores the details in a local file. If you configure a scheduler to run the script periodically, during each run, the IP file gets overwritten with a new one.
3. Cisco SCA BB:
   a. Maps each zone name to the parameter of SCA BB zone configuration, such as Zone Index.
   b. Pushes parameters such as zone and zone items (BGP routes) to the Cisco SCE while applying the configuration.
   c. Configures the Services configured on various zones and pushes the configuration to the SCE.
4. Cisco SCE controls the service bandwidth based on the services configured on various zones.

Enabling BGP AS Dynamic Detection

By default, BGP AS Dynamic Detection is disabled on Cisco SCA BB.

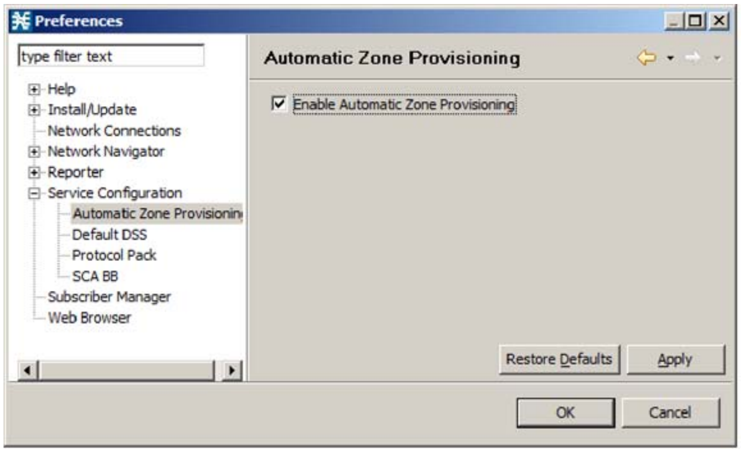
To enable BGP AS Dynamic Detection, complete these steps:

Step 1 Choose **Windows > Preferences**.

Step 2 In the Preferences window, expand the Service Configuration.

Step 3 Click **Automatic Zone Provisioning**.

Step 4 Check the **Enable Automatic Zone Provisioning** check box.



Automatic Zone Provisioning

☑ Enable Automatic Zone Provisioning

Step 5 Click **Apply**.

Step 6 Click **OK**.

Collecting and Storing the BGP Autonomous System (AS) Details

The Cisco SCA BB asFetch script uses SNMP MIBs to fetch the BGP AS numbers and prefixes. Cisco SCA BB, Release 3.7.2, supports only SNMP version 2.

The routerInfo.properties file, asFetch.bat, and asFetch.sh are in the sca_bb_util\bin folder.

To collect and store the BGP AS details, complete these steps:

Step 1 Enter the router IP and SNMP community string in the routerInfo.properties file.

Step 2 Run the asFetch.bat script.

The script fetches the AS number and IP prefix details and saves them in the BGPRouter<*number*>.csv file that is present in the same folder in which you have extracted the asFetch script. Prior to performing Step 2, ensure that the following prerequisites are fulfilled:

- If AS numbers and IP prefixes have to be generated for more than one router IP, enter the router IP address of the community string separated by a comma (,) in the routerInfo.properties file.
- Run the asFetch.bat file to generate the BGPRouter<*number*>.csv files based on the number of IP addresses entered in the properties file. For example, if two IP addresses are specified in the properties file, The BGPRouter1.csv and BGPRouter2.csv files get generated.These .csv files contain the AS number and IP prefix details. These files can be imported from the Zone settings window.

You can run the script manually or use a scheduler to run the script periodically.

Creating a New Zone with Select BGP AS Numbers and Prefixes

Before attempting to add the BGP AS numbers and prefixes to zones, enable automatic zone provisioning and run the asFetch script to get the BGP AS details into the BGPRouter<*number*>.csv file.

To create a new zone and add select BGP AS numbers and prefixes, complete the following steps:

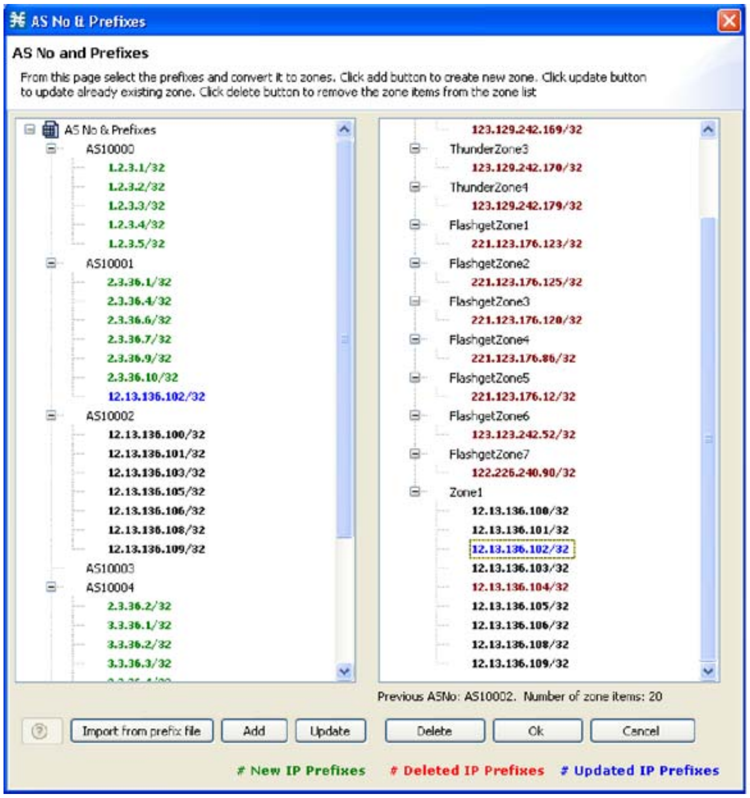
Step 1 From the Service Configuration Editor window, choose **Configuration > Classification > Zones**.

Step 2 In the Zone Settings window, click **Advanced Import**.

Step 3 Browse to the folder in which the BGPRouter<*number*>.csv file is saved, and select the BGPRouter<*number*>.csv file.

Step 4 Click **Open**.

The AS No & Prefixes dialog box appears.



AS No & Prefixes

AS No and Prefixes

From this page select the prefixes and convert it to zones. Click add button to create new zone. Click update button to update already existing zone. Click delete button to remove the zone items from the zone list

Previous ASNo: AS10002. Number of zone items: 20

Step 5 Select the corresponding AS Number.

Step 6 Click **Add**.

Step 7 Enter a New Zone Name.

Step 8 Click **OK**.

Step 9 Click **OK**.

Understanding BGP AS Numbers and Prefixes Color Schema

The AS Number and Prefixes dialog box uses various colors to indicate new prefixes, prefixes added to a zone, or changes to the AS Number to which the prefix belongs.

Green color indicates a new prefix that does not belong to any zone. After you add the prefix to a zone, the color of the prefix in the prefix list and the zone changes to black. If you remove the prefix from the zone, the color of the prefix in the prefix list changes to green again.

Blue color indicates that the prefix has moved from one AS to another. This helps you decide whether to move the prefix to another zone.

Red color indicates that the prefix is not a part of the AS Numbers and Prefixes list.

Updating a Zone with Select BGP AS Numbers and Prefixes

To update a zone with select BGP AS numbers and prefixes, complete the following steps:

Step 1 From the Service Configuration Editor window, choose **Configuration > Classification > Zones**.

Step 2 In the Zone Settings window, click **Advanced Import**.

Step 3 Browse to the folder in which the BGPRouter<number>.csv file is saved and select the BGPRouter<*number*>.csv file.

Step 4 Click **Open**.

The AS No & Prefixes dialog box appears.

Step 5 Select the corresponding AS Number.

Step 6 Click **Update**.

Step 7 Choose a zone from the drop-down list.

Step 8 Click **OK**.

Step 9 Click **OK**.

Timesaver From the AS No & Prefixes dialog box, you can drag and drop the required AS numbers and IP prefixes to the required zones.

Deleting IP Prefixes from a Zone

You can delete IP prefixes only from a zone and not from the AS Numbers and Prefixes list.

To delete IP prefixes from a zone:

Step 1 Select the prefixes you want to delete.

Step 2 Click **Delete**.

Managing Protocol Signatures

A protocol signature is a set of parameters that uniquely identify a protocol.

- Viewing Signatures, page 7-46
- Dynamic Signatures, page 7-49

Viewing Signatures

- How to View Signatures, page 7-47
- How to Filter the Signatures List, page 7-48

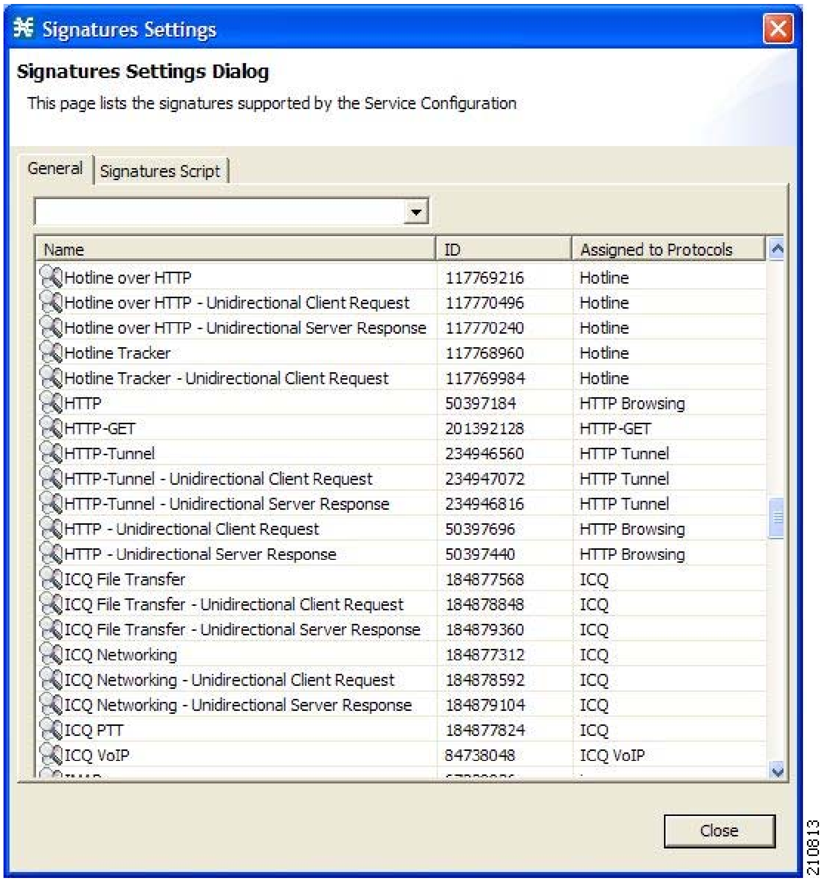
How to View Signatures

You can view a list of all signatures and the protocol to which each is assigned.

Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > Signatures Settings**.

The Signatures Settings dialog box appears (Figure 7-35).

Figure 7-35 Signatures Settings



Signatures Settings

Signatures Settings Dialog

This page lists the signatures supported by the Service Configuration

General | Signatures Script

Name	ID	Assigned to Protocols
Hotline over HTTP	117769216	Hotline
Hotline over HTTP - Unidirectional Client Request	117770496	Hotline
Hotline over HTTP - Unidirectional Server Response	117770240	Hotline
Hotline Tracker	117768960	Hotline
Hotline Tracker - Unidirectional Client Request	117769984	Hotline
HTTP	50397184	HTTP Browsing
HTTP-GET	201392128	HTTP-GET
HTTP-Tunnel	234946560	HTTP Tunnel
HTTP-Tunnel - Unidirectional Client Request	234947072	HTTP Tunnel
HTTP-Tunnel - Unidirectional Server Response	234946816	HTTP Tunnel
HTTP - Unidirectional Client Request	50397696	HTTP Browsing
HTTP - Unidirectional Server Response	50397440	HTTP Browsing
ICQ File Transfer	184877568	ICQ
ICQ File Transfer - Unidirectional Client Request	184878848	ICQ
ICQ File Transfer - Unidirectional Server Response	184879360	ICQ
ICQ Networking	184877312	ICQ
ICQ Networking - Unidirectional Client Request	184878592	ICQ
ICQ Networking - Unidirectional Server Response	184879104	ICQ
ICQ PTT	184877824	ICQ
ICQ VoIP	84738048	ICQ VoIP

Step 2 Click **Close**.

The Signatures Settings dialog box closes.

How to Filter the Signatures List

You can filter the signature by type, so that the Signatures Settings dialog box lists only the selected type of signature.

The signature categories are:

- DSS Contributed Signatures
- Not Assigned to any Protocol
- P2P Signatures
- VoIP Signatures
- SIP Signatures
- Worm Signatures
- Packet Stream Pattern Based Protocols Signatures
- Unidirectionally Detected Signatures
- Behavioral Signatures
- E-Mail and Newsgroups Signatures
- Gaming Signatures
- HTTP Signatures
- Instant Messaging Signatures
- Net Admin Signatures
- Video Signatures
- Tunneling Signatures
- ClickStream Signatures

Note Some signatures belong to more than one category.

Step 1 From the Console main menu, choose **Configuration > Classification > Signatures Settings**.

The Signatures Settings dialog box appears.

Step 2 From the drop-down list, select the type of signature to display.

The signatures of the selected type appear in the dialog box.

Step 3 Click **Close**.

The Signatures Settings dialog box closes.

Dynamic Signatures

New protocols are being introduced all the time. Dynamic signatures is a mechanism that allows new protocols to be added to the protocol list and, from there, to service configurations. Dynamic Signature is especially useful for classifying the traffic of a new protocol (for example, a new P2P protocol in a P2P-Control solution).

- Installing new signatures to an active service configuration is described in Working with Protocol Packs, page 4-20.
- Creating and modifying signatures is described in Using the Signature Editor, page 13-1.
- Using **servconf,** the Cisco SCA BB Server Configuration Utility, to apply signatures is described in The Cisco SCA BB Service Configuration Utility, page 14-2.

The following sections describe working with dynamic signatures in the Service Configuration Editor.

- Dynamic Signature Script Files, page 7-49.
- The Default DSS File, page 7-53.

Dynamic Signature Script Files

Dynamic signatures are provided in special Dynamic Signatures Script (DSS) files that you can add to a service configuration using either the Console or the Service Configuration API. After a DSS file is imported into a service configuration, the new protocols it describes:

- Appear in the protocol list.
- May be added to services.
- Are used when viewing reports.

To simplify the configuration of new protocols added by a DSS, the DSS may specify a Buddy Protocol for a new protocol. If, when loading a DSS, the application encounters the Buddy Protocol, it automatically duplicates the set of service elements that use the Buddy Protocol, and replaces all references to the Buddy Protocol with references to the new protocol. The association of the new protocol to services matches that of the Buddy Protocol.

The following configuration actions are performed automatically when you import a DSS into a service configuration:

- Signatures are updated and new signatures are loaded.
- Protocol elements are created for new signatures of existing protocols.
- New protocols are added to the protocol list, and protocol elements are created for them.
- Service elements are created for new protocols according to the configuration of Buddy Protocols.

The import procedure preserves all service and protocol settings.

Note After importing a DSS, associate the newly added protocols with services.

Cisco or its partners releases DSS files periodically in accordance with customer requirements and market needs.

DSS files contain new protocols and signatures, and update previously defined signatures. Updating a service configuration with the new DSS is explained in How to Import a Dynamic Signature Script into a Service Configuration, page 7-51.

Note You can create your own DSS files or modify the Cisco release DSS file using the Signature Editor tool (see Managing DSS Files, page 13-2).

- How to View Information About the Current Dynamic Signatures, page 7-50
- How to Import a Dynamic Signature Script into a Service Configuration, page 7-51
- How to Remove Dynamic Signatures, page 7-52

How to View Information About the Current Dynamic Signatures

Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > Signatures Settings**.

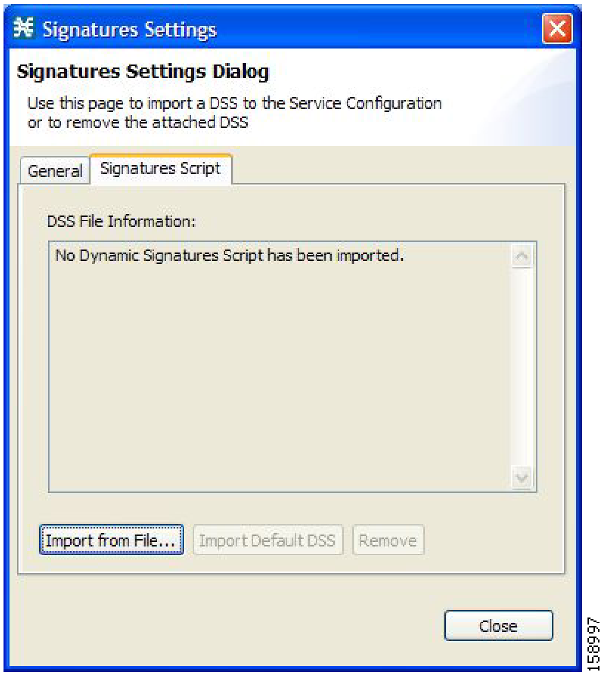
The Signatures Settings dialog box appears.

Step 2 Click the **Signatures Script** tab.

The Signatures Script tab opens (Figure 7-36).

- If no DSS file was imported into the current service configuration, the Signatures Settings dialog box displays a message informing you of this.

Figure 7-36 Signature Settings



Signatures Settings

Signatures Settings Dialog

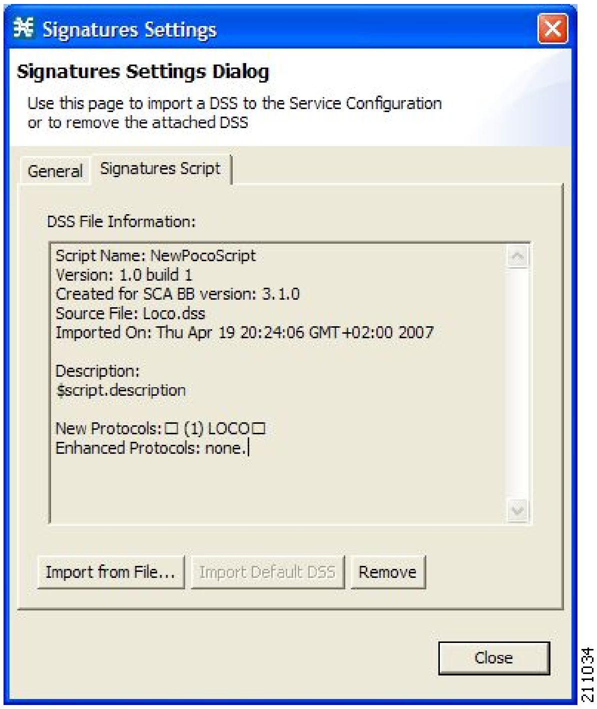
Use this page to import a DSS to the Service Configuration or to remove the attached DSS

DSS File Information:

No Dynamic Signatures Script has been imported.

- If a DSS file was imported into the current service configuration, the Signatures Settings dialog box displays information about the current dynamic signatures and the DSS file from which they were imported (Figure 7-37).

Figure 7-37 Signature Settings



Signatures Settings Dialog

Use this page to import a DSS to the Service Configuration
or to remove the attached DSS

DSS File Information:

Script Name: NewPocoScript
Version: 1.0 build 1
Created for SCA BB version: 3.1.0
Source File: Loco.dss
Imported On: Thu Apr 19 20:24:06 GMT+02:00 2007

Description:
$script.description

New Protocols:□ (1) LOCO□
Enhanced Protocols: none.

Step 3 Click **Close**.

The Signatures Settings dialog box closes.

How to Import a Dynamic Signature Script into a Service Configuration

You can import signatures into a service configuration from a DSS file provided by Cisco or one of its partners (described in this section), or from a DSS file that you have created or modified using the Signature Editor tool (see Managing DSS Files, page 13-2).

Note It is recommended that you import the latest default DSS file (see How to Import the Default DSS File Automatically, page 7-57) when creating a service configuration, and that you use this option only to apply a new DSS to existing service configuration.

Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > Signatures Settings**.

The Signatures Settings dialog box appears.

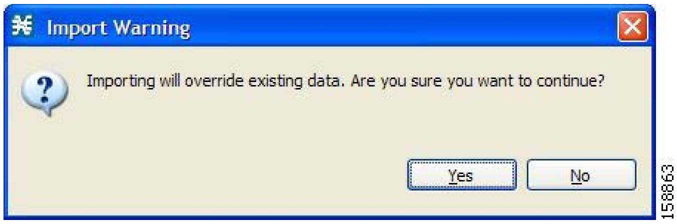
Step 2 Click the **Signatures Script** tab.

The Signatures Script tab opens.

Step 3 Click **Import from File**.

An Import Warning message appears (Figure 7-38).

Figure 7-38 Import Warning



Import Warning

Importing will override existing data. Are you sure you want to continue?

Step 4 Click **Yes**.

The Import from file dialog box appears.

Step 5 Browse to the DSS file and click **Open**.

The Import from file dialog box closes.

The signatures in the DSS file are imported into the service configuration.

Information about the imported signatures and their DSS file is displayed in the Signatures Settings dialog box.

Step 6 Click **Close**.

The Signatures Settings dialog box closes.

How to Remove Dynamic Signatures

You can remove the installed dynamic signatures from a service configuration.

Note The DSS file is not deleted.

Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > Signatures Settings**.

The Signatures Settings dialog box appears.

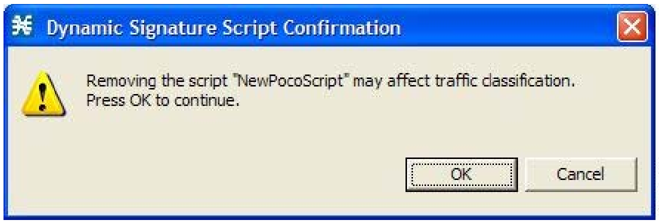
Step 2 Click the **Signatures Script** tab.

The Signatures Script tab opens.

Step 3 Click **Remove**.

A Dynamic Signature Script Confirmation message appears (Figure 7-39).

Figure 7-39 Dynamic Signature Script Confirmation



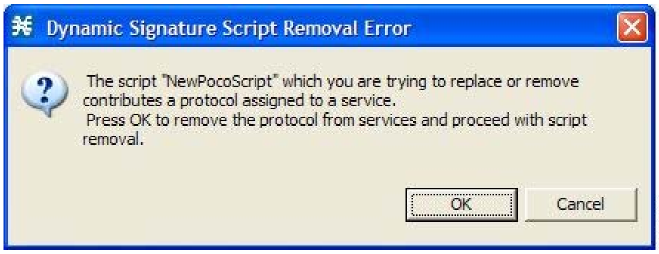
Dynamic Signature Script Confirmation

Removing the script "NewPocoScript" may affect traffic classification.
Press OK to continue.

Step 4 Click **OK**.

- If any service element references a protocol whose signature is included in the imported DSS file, a Dynamic Signature Script Removal Error message appears (Figure 7-40).

Figure 7-40 Dynamic Signature Script Removal Error



Dynamic Signature Script Removal Error

The script "NewPocoScript" which you are trying to replace or remove contributes a protocol assigned to a service.
Press OK to remove the protocol from services and proceed with script removal.

- Click **Yes**.

  Every service element that references a protocol whose signature is included in the imported DSS file is deleted.

The dynamic signatures are removed from the service configuration.

The Remove button is dimmed.

If the dynamic signatures were imported from the default DSS file, the Import Default DSS button is enabled.

Step 5 Click **Close**.

The Signatures Settings dialog box closes.

The Default DSS File

Whenever a protocol pack becomes available from Cisco (or one of its partners), you should update offline service configurations (stored as PQB files on the workstation). The protocol pack (see Protocol Packs, page 4-20) is provided as either an SPQI file or a DSS file.

You can either offer updates automatically to every service configuration created or edited at the workstation, or apply them from the workstation to the SCE platform. You make the latest update available by installing the most recent DSS or SPQI file as the default DSS file. You can install the file on the workstation either from the Console or by using The Cisco SCA BB Signature Configuration Utility, page 14-9.

- The default DSS file is automatically offered for import when you perform any service configuration operation (such as creating a new service configuration or editing an existing one) from the Console on a service configuration that was not yet updated.
- The default DSS file is imported by default when any service configuration operation (such as applying an existing service configuration) is performed using **servconf,** The Cisco SCA BB Signature Configuration Utility, page 14-9. You can disable this option.

Note Users are expected to update the default DSS on their management workstation whenever they obtain a new protocol pack, as explained in the following section.

- Setting and Clearing the Default DSS File, page 7-54
- Importing Dynamic Signatures from the Default DSS File, page 7-57

Setting and Clearing the Default DSS File

The default DSS file should normally be the latest protocol pack provided by Cisco (or one of its partners). If necessary, modify the protocol pack using the Signature Editor tool (see How to Edit DSS Files, page 13-16) to add signatures of new protocols until they become available from Cisco.

Whenever a new protocol pack becomes available, set it as the default DSS file. There is no need to clear the current default DSS file; it is overwritten by the new protocol pack.

- How to Set a Protocol Pack as the Default DSS File, page 7-55
- How to Clear the Default DSS File, page 7-56

How to Set a Protocol Pack as the Default DSS File

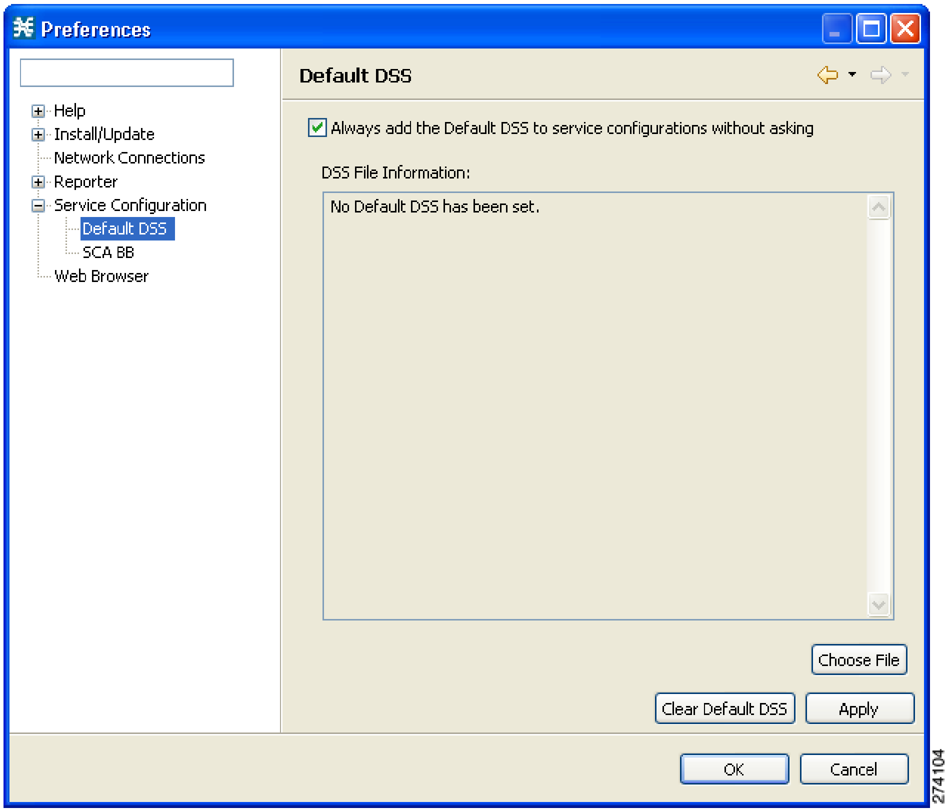
Step 1 From the Console main menu, choose **Window > Preferences**.

The Preferences dialog box appears (Figure 7-41).

Step 2 From the menu tree in the left pane of the dialog box, choose **Service Configuration > Default DSS**.

The Default DSS area opens in the right pane of the dialog box.

Figure 7-41 Preferences



☑ Always add the Default DSS to service configurations without asking

DSS File Information:

No Default DSS has been set.

Step 3 Click **Choose File**.

An Open dialog box appears.

Step 4 From the Files of type drop-down list, select the file type of the protocol pack.

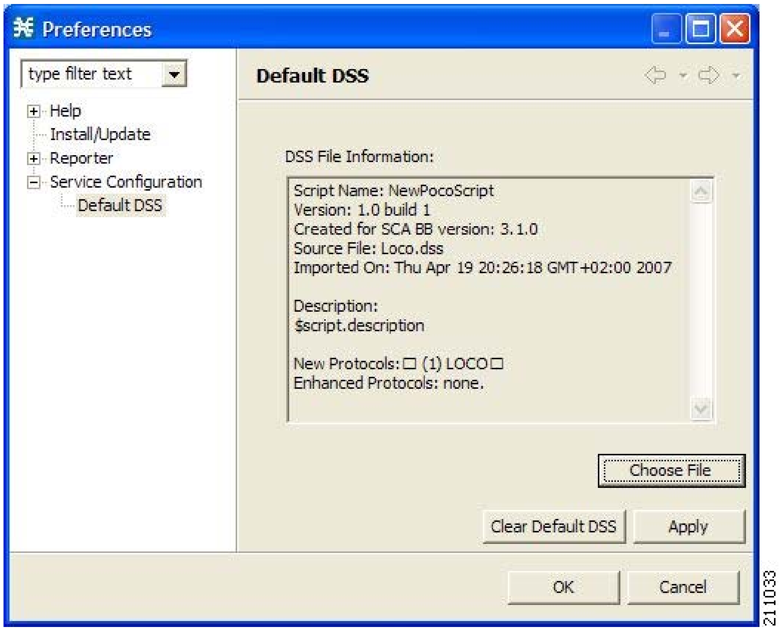
Step 5 Browse to the protocol pack.

Step 6 Click **Open**.

The Open dialog box closes.

Information about the default DSS file is displayed in the Default DSS area of the Preferences dialog box (Figure 7-42).

Figure 7-42 Preferences - Default DSS



DSS File Information:

Script Name: NewPocoScript
Version: 1.0 build 1
Created for SCA BB version: 3.1.0
Source File: Loco.dss
Imported On: Thu Apr 19 20:26:18 GMT+02:00 2007

Description:
$script.description

New Protocols:□ (1) LOCO□
Enhanced Protocols: none.

Step 7 Click **OK**.

The DSS file is copied to C:\Documents and Settings\<username>\.p-cube\default3.6.5.dss as the default DSS file. In Windows 7, the DSS file is copied to C:\Users\<username>\.p-cube\.

The Preferences dialog box closes.

How to Clear the Default DSS File

Step 1 From the Console main menu, choose **Window > Preferences**.

The Preferences dialog box appears.

Step 2 From the menu tree in the left pane of the dialog box, choose **Service Configuration > Default DSS**.

The Default DSS area opens in the right pane of the dialog box.

Step 3 Click **Clear Default DSS**.

The default DSS file, C:\Documents and Settings\<username>\.p-cube\default3.6.5.dss, is deleted. In Windows 7, the default DSS file is C:\Users\<username>\.p-cube\default3.6.5.dss.

All information is deleted from the Default DSS area.

Note Deleting the default DSS file does not remove the imported dynamic signatures from the current service configuration.

Step 4 Click **OK**.

The Preferences dialog box closes.

Importing Dynamic Signatures from the Default DSS File

If a default DSS file is installed, the application offers to import the dynamic signatures from the file when you create a new service configuration or when you open an existing service configuration that has not imported the signatures. Alternatively, you can manually import the dynamic signatures.

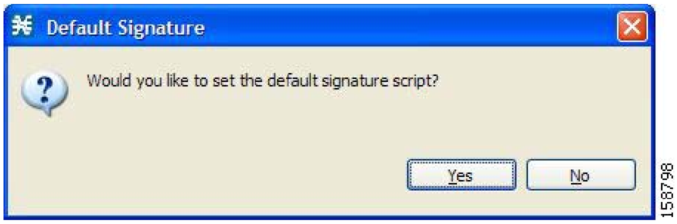
- How to Import the Default DSS File Automatically, page 7-57
- How to Import the Default DSS File Manually, page 7-58

How to Import the Default DSS File Automatically

Step 1 Open an existing service configuration or create a new one.

A Default Signature message appears (Figure 7-43).

Figure 7-43 Default Signature


Default Signature

Would you like to set the default signature script?

Step 2 Click **Yes** to import the default DSS file; click **No** to continue without importing the default DSS file.

How to Import the Default DSS File Manually

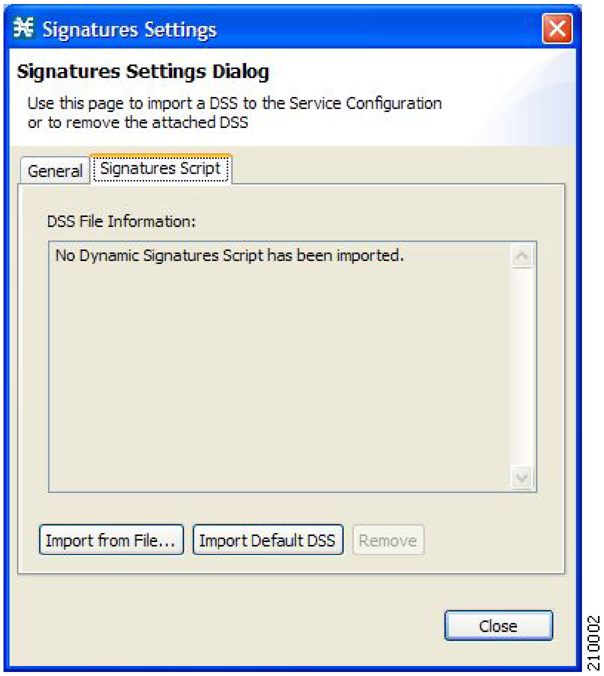
Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > Signatures Settings**.

The Signatures Settings dialog box appears (Figure 7-44).

Step 2 Click the **Signatures Script** tab.

The Signatures Script tab opens, with the Import Default DSS button enabled.

Figure 7-44 Signatures Settings



Signatures Settings

Signatures Settings Dialog

Use this page to import a DSS to the Service Configuration or to remove the attached DSS

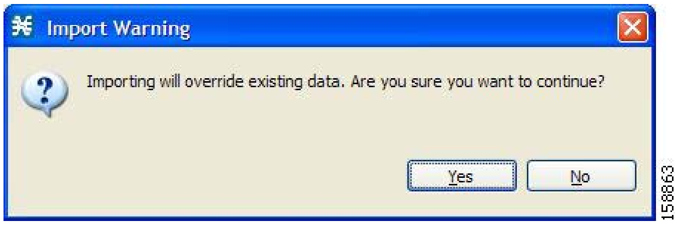
DSS File Information:

No Dynamic Signatures Script has been imported.

Step 3 Click **Import Default DSS**.

An Import Warning message appears (Figure 7-45).

Figure 7-45 Import Warning



Import Warning

Importing will override existing data. Are you sure you want to continue?

Step 4 Click **Yes**.

The signatures in the default DSS file are imported into the service configuration.

The Import Default DSS button is dimmed.

Information about the imported signatures and the default DSS file is displayed in the Signatures Settings dialog box.

Step 5 Click **Close**.

The Signatures Settings dialog box closes.

Managing Flavors

Flavors are advanced classification elements that are used to classify network sessions.

Flavors are based on specific Layer 7 properties. For example, users can associate an HTTP flow with a service based on different parts of the destination URL of the flow.

Flavors are supported only for small number of protocols, and for each such protocol there are different applicable flavor types. Flavor types are listed in the table in the following section.

There is a maximum number of flavor items for each flavor type (see Maximum Number of Flavor Items per Flavor Type, page 7-68). For each flavor type, every flavor item must be unique.

Note If unidirectional classification is enabled in the active service configuration, flavors are not used for traffic classification.

- Flavor Types and Parameters, page 7-60
- How to View Flavors, page 7-63
- How to Add Flavors, page 7-65
- How to Edit Flavors, page 7-66
- How to Delete Flavors, page 7-66
- Managing Flavor Items, page 7-67
- Importing Flavor, see How to Import Service Configuration Data, page 6-11
- Exporting Flavor, see How to Export Service Configuration Data, page 6-7

Flavor Types and Parameters

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

When Layer 7 application properties are used as session parameters, such as with an HTTP User Agent, They are treated as character strings.

Layer 7 parameter-based flavor items may apply to the Layer 7 prefix (parameter beginning), Layer 7 suffix (parameter end), or a combination of Layer 7 prefixes and suffixes. A partial string must be followed by “*” in a prefix and preceded by “*” in a suffix.

Table 7-1 lists available flavor types.

Table 7-1 Cisco SCA BB Flavors

Flavor Type	Matched Session Parameters	Valid Values
HTTP Composite	HTTP User Agent, HTTP URL, HTTP Cookie and HTTP Referer flavors serve as session parameters.	<HTTP User Agent flavor, HTTP URL flavor, HTTP Cookie flavor, HTTP Referer flavor> • The flavors can be chosen using flavor browsing.
HTTP User Agent	HTTP User-Agent retrieved from the HTTP <User-Agent prefix> Request header field, from the beginning of the Request header until the first "/". For example, if the HTTP Request header field is Mozilla/4.0, the HTTP User Agent retrieved is Mozilla. If you want to configure the HTTP User Agent flavor with a Forward slash (/), set the value of the GT_CLS_ENABLE_FULL_USER_AGENT_BASED_FLAVOR_CALCULATION tunable to True.	<User-Agent prefix> Examples: • <Moz*> matches all HTTP sessions with User-Agent field starting with "Moz". • <Mozilla> matches all HTTP sessions with User-Agent field equal to "Mozilla". • The maximum key length is 32 characters.
HTTP URL	• Host—Retrieved either from the HTTP Host header field or from the Request URL. In the latter case, the section from the beginning of the URL until the first "/" is considered the Host. • Path—Retrieved from the HTTP URL, the section from the first "/" to the "?". • URL parameters—Any string following the "?" (You do not need to start the parameters prefix with "?").	<host suffix, path prefix, path suffix, URL parameters prefix> • At least one parameter must be specified. Unspecified parameters should be left as "*". • For example: <*cisco.com,*,*,*> matches all HTTP sessions with the Host ending with "cisco.com", regardless of the values of Path and Parameters. • The maximum key length for all keys is 512 characters.
HTTP Cookie	Cookie "Key-Value" pairs that are retrieved from the HTTP Request header Cookie field. A Cookie may consist of many "Key-Value" pairs; however, only the first three pairs are calculated. The Cookie flavor calculation stops when one of the "Key-Value" pairs matches the specification, or when it has exceeded the three pair limit.	<key prefix, value prefix> • For example: <act*,*> matches any Cookie pair where the Key begins with "act", regardless of the Value. • A flavor can be configured so that the Value field is required to be empty. In this case, this field should be left empty in the flavor item. • White spaces are not allowed, "=" is not allowed, and "*" is only allowed at the end of the Key or Value. • The maximum key length is 100 characters for both the Key and Value fields

Table 7-1 Cisco SCA BB Flavors (continued)

Flavor Type	Matched Session Parameters	Valid Values
HTTP Referer	Similar to HTTP URL, but the parameters are retrieved from the Referer HTTP header field.	<host suffix, path prefix, path suffix, URL parameters prefix> • At least one parameter must be specified. Unspecified parameters should be left as "*". • For example: <*cisco.com,*,*,*> matches all HTTP sessions with the Host ending with "cisco.com", regardless of the values of Path and Parameters. • The maximum key length for all keys is 512 characters
HTTP Content Category	Content Categories can be imported using the Import dialog box or the HTTP Content Filtering Settings dialog box.	Value selected from Select a Content Category dialog box.
RTSP User Agent	RTSP User-Agent field that is retrieved from the RTSP message header.	<RTSP User Agent prefix> • For example: <abc*> matches all RTSP sessions where the User-Agent starts with "abc". • The maximum key length is 128 characters
RTSP Host Name	RTSP Host field that is retrieved from the RTSP message header.	<RTSP Host suffix> • For example: <*abc> matches all RTSP sessions where the Host ends with "abc". • The maximum key length is 128 characters
RTSP Composite	RTSP User Agent and RTSP Host Name flavors serve as session parameters.	<RTSP User Agent flavor, RTSP Host Name flavor>
SIP Source Domain	SIP Source Host field that is retrieved from the SIP message header.	<SIP Host suffix> • For example: <*abc> • The maximum key length is 128 characters
SIP Composite	SIP Source Host and SIP Destination Host serve as session parameters.	<SIP source domain, SIP destination domain>
SIP Destination Domain	SIP Destination Host field that is retrieved from the SIP message header.	<SIP Host suffix> • For example: <*abc> • The maximum key length is 128 characters
SMTP Host Name	SMTP Host field that is retrieved from the SMTP message header	• <SMTP Host suffix> • For example: <*abc> • The maximum key length is 128 characters
ToS	DSCP value extracted from the IP header	DSCP ToS (integer from 0 through 63)

Note Composite Flavors are pairs of two defined flavors.

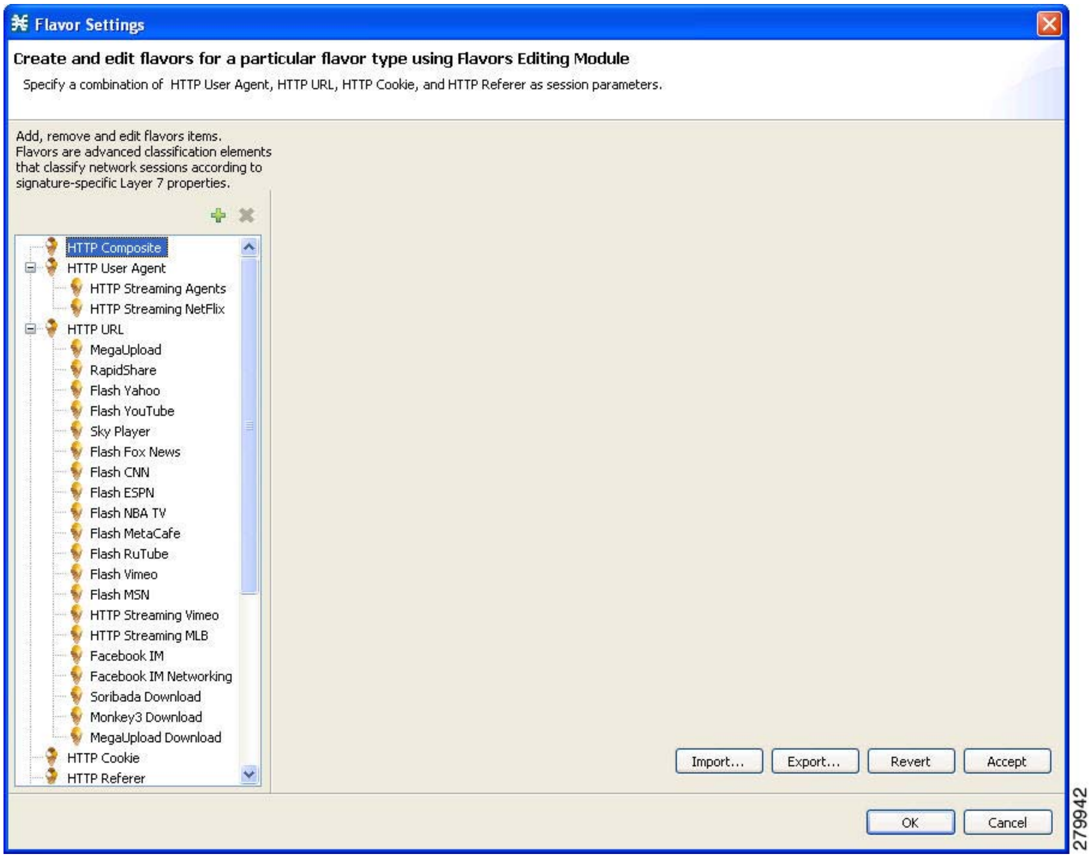
How to View Flavors

You can view a list of all flavors and their associated flavor items.

Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > Flavors**.

The dialog box appears (Figure 7-46).

Figure 7-46 Flavor Settings



Flavor Settings

Create and edit flavors for a particular flavor type using Flavors Editing Module

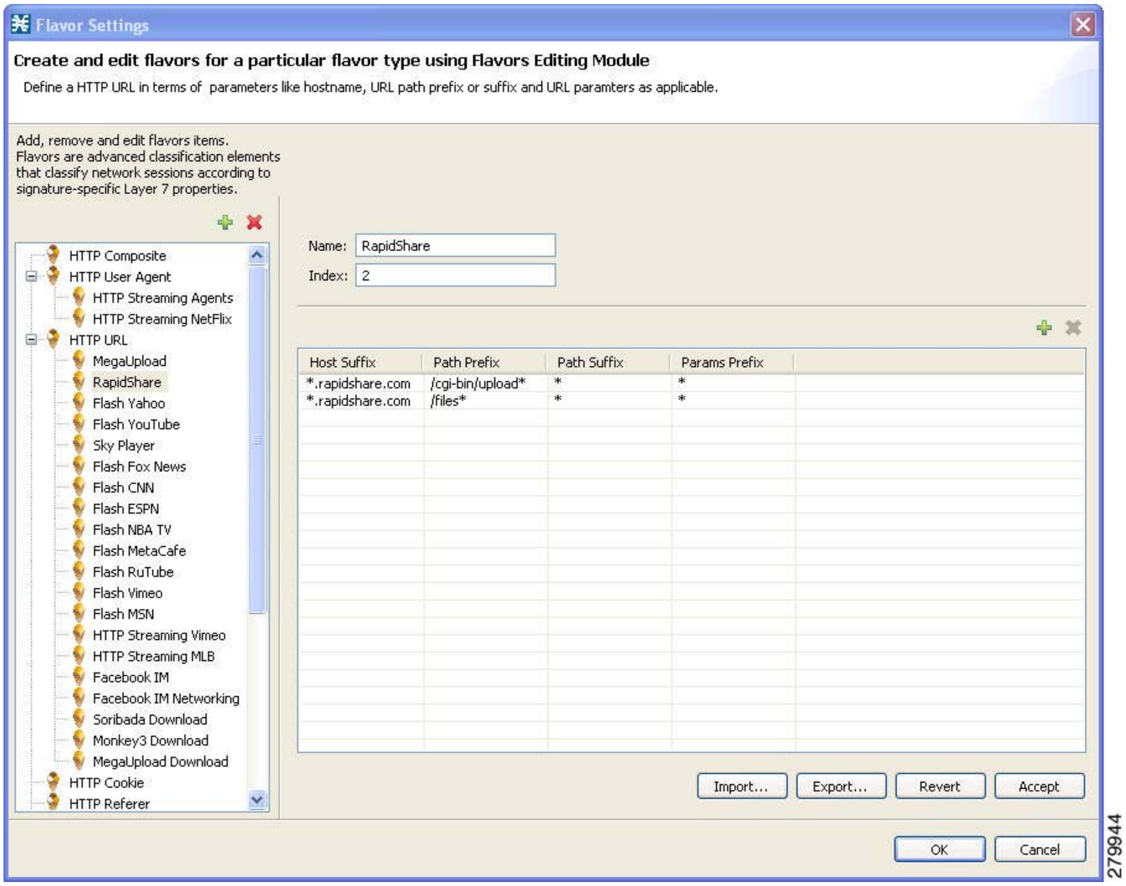
Specify a combination of HTTP User Agent, HTTP URL, HTTP Cookie, and HTTP Referer as session parameters.

Add, remove and edit flavors items. Flavors are advanced classification elements that classify network sessions according to signature-specific Layer 7 properties.

The left area displays a tree showing all flavors of each flavor type.

Step 2 Click a flavor in the tree to display its flavor items (Figure 7-47).

Figure 7-47 Flavor Settings



Flavor Settings

Create and edit flavors for a particular flavor type using Flavors Editing Module

Define a HTTP URL in terms of parameters like hostname, URL path prefix or suffix and URL paramters as applicable.

Add, remove and edit flavors items.
Flavors are advanced classification elements that classify network sessions according to signature-specific Layer 7 properties.

Name: RapidShare

Index: 2

Host Suffix	Path Prefix	Path Suffix	Params Prefix
*.rapidshare.com	/cgi-bin/upload*	*	*
*.rapidshare.com	/files*	*	*

The flavor items are displayed in the right area.

Step 3 Click **OK**.

The Flavor Settings dialog box closes.

How to Add Flavors

You can import flavors from a CSV file. CSV files can be created by exporting flavors or created manually as described in the “CSV File Formats” chapter of *Cisco Service Control Application Suite for Broadband Reference Guide*.

You can add any number of flavors to a service configuration.

Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > Flavors**.

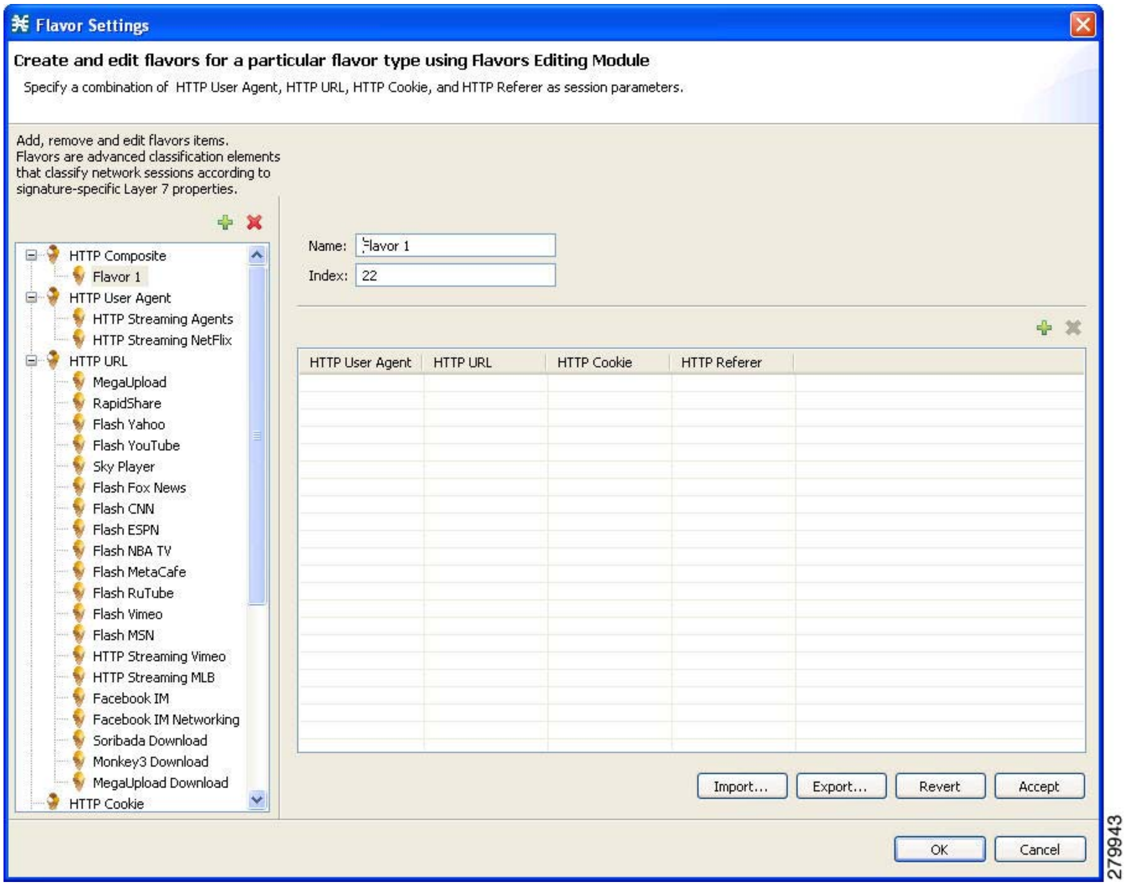
The Flavor Settings dialog box appears (Figure 7-48).

Step 2 In the flavor tree, select a flavor type.

Step 3 Click the **Add Flavor** (✚) icon.

A new flavor of the selected type is added to the flavor tree.

Figure 7-48 Flavor Settings - Adding Flavors



Flavor Settings

Create and edit flavors for a particular flavor type using Flavors Editing Module

Specify a combination of HTTP User Agent, HTTP URL, HTTP Cookie, and HTTP Referer as session parameters.

Add, remove and edit flavors items. Flavors are advanced classification elements that classify network sessions according to signature-specific Layer 7 properties.

Name: Flavor 1

Index: 22

Step 4 In the Name field, enter a name for the new flavor.

Note You can use the default name for the flavor. It is recommended that you enter a meaningful name.

Step 5 (Optional) In the Index field, enter a unique integer value.

Note Cisco SCA BB provides a value for the Index. There is no need to change it.

The flavor index must be a positive integer in the range from 1 to 2147483647.

You have defined the flavor. You can now add flavor items. (See How to Add Flavor Items, page 7-69.)

How to Edit Flavors

You can modify flavor parameters at any time.

To add, modify, or delete flavor items, see Managing Flavor Items, page 7-67.

Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > Flavors**.

The Flavor Settings dialog box appears.

Step 2 In the flavor tree, select a flavor.

The name and index of the flavor (and its flavor items) are displayed in the right area.

Step 3 Modify fields in the dialog box:

- In the Name field, enter a new name for the flavor.
- In the Index field, enter a new, unique index for the flavor.

  The flavor index must be a positive integer in the range from 1 to 2147483647.

Step 4 Click **OK**.

The Flavor Settings dialog box closes.

How to Delete Flavors

You can delete any or all flavors.

Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > Flavors**.

The Flavor Settings dialog box appears.

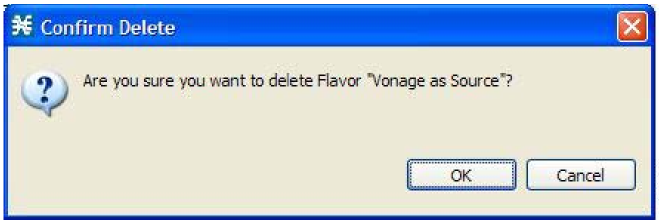
Step 2 In the flavor tree, right-click a flavor.

A popup menu appears.

Step 3 Click the **Delete** (✖) icon.

A Confirm Delete message appears (Figure 7-49).

Figure 7-49 Confirm Delete



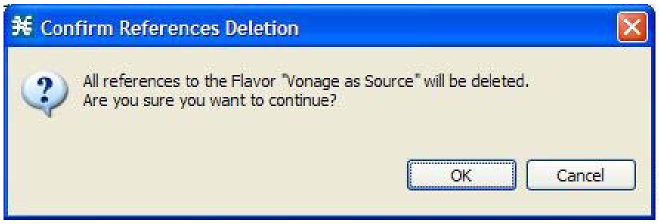
Confirm Delete

Are you sure you want to delete Flavor "Vonage as Source"?

Step 4 Click **OK**.

- If any service element references the selected flavor, a Confirm References Delete message appears (Figure 7-50).

Figure 7-50 Confirm References Deletion



Confirm References Deletion

All references to the Flavor "Vonage as Source" will be deleted.
Are you sure you want to continue?

- Click **Yes**.

  Every service element that references the selected flavor is deleted.

The flavor is deleted and is no longer displayed in the flavor tree.

Step 5 Click **Close**.

The Flavor Settings dialog box closes.

Managing Flavor Items

A flavor is a collection of related flavor items.

A flavor item is a value of a property or properties of a flow. These properties depend on the flavor type (see Flavor Types and Parameters, page 7-60).

There is a maximum number of flavor items for each flavor type. For each flavor type, every flavor item must be unique.

- Maximum Number of Flavor Items per Flavor Type, page 7-68
- How to Add Flavor Items, page 7-69
- How to Edit Flavor Items, page 7-70
- How to Delete Flavor Items, page 7-71

Maximum Number of Flavor Items per Flavor Type

Table 7-2 lists the maximum number of flavor items for each flavor type.

Table 7-2 Maximum Number of Flavor Items per Flavor Type

Flavor Type	Maximum No. of Flavor Items
HTTP Composite	10,000
HTTP User Agent	128
HTTP URL	100,000
HTTP Cookie	100
HTTP Referer	100
HTTP Content Category	—
RTSP Composite	10,000
RTSP User Agent	128
RTSP Host Name	10,000
SIP Composite	10,000
SIP Source Domain	128
SIP Destination Domain	128
SMTP Host Name	10,000
ToS	64

How to Add Flavor Items

You can add any number of flavor items to a flavor (subject to the limitation of the total number of each type of flavor item per service configuration, as listed in the previous section).

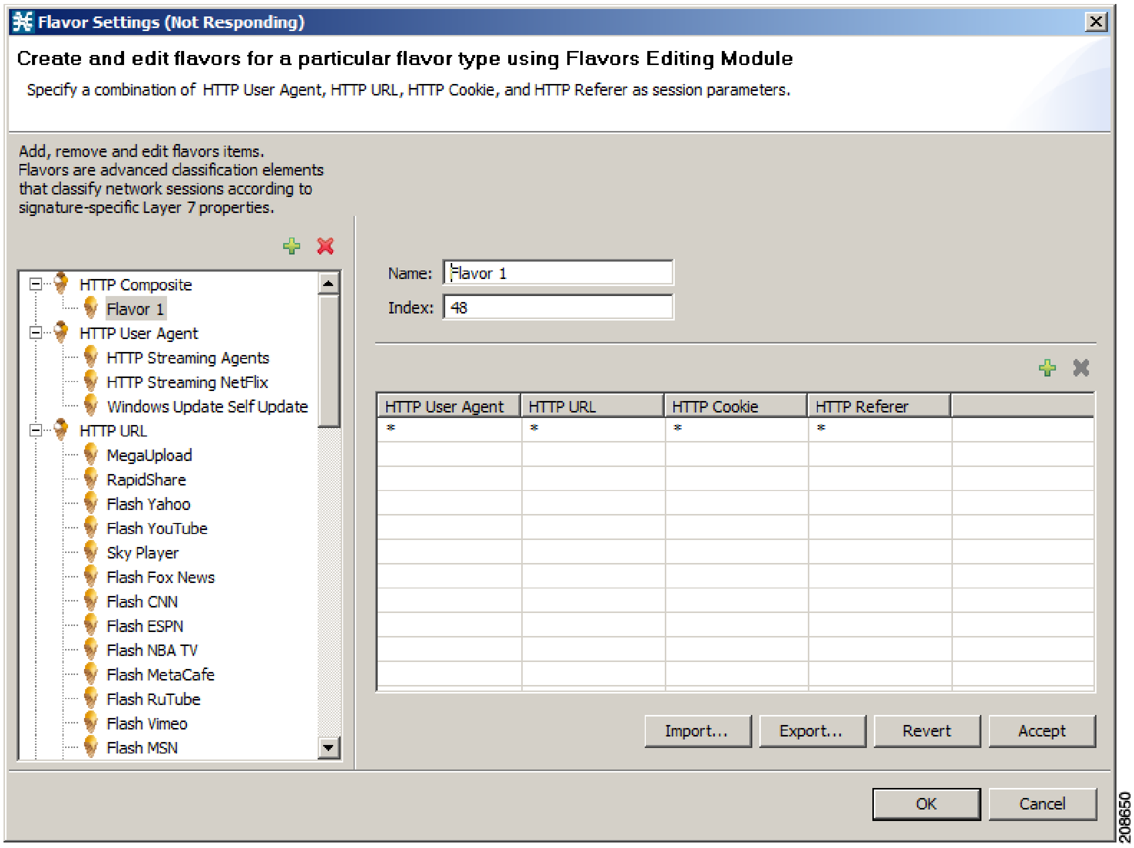
Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > Flavors**.

The Flavor Settings dialog box appears (Figure 7-51).

Step 2 In the flavor tree, click a flavor.

Step 3 Above the flavor item list, click the **Create New Flavor Item** ✚ icon.

Figure 7-51 Flavor Settings



Flavor Settings (Not Responding)

Create and edit flavors for a particular flavor type using Flavors Editing Module

Specify a combination of HTTP User Agent, HTTP URL, HTTP Cookie, and HTTP Referer as session parameters.

Add, remove and edit flavors items.
Flavors are advanced classification elements that classify network sessions according to signature-specific Layer 7 properties.

Name: Flavor 1

Index: 48

HTTP User Agent	HTTP URL	HTTP Cookie	HTTP Referer	
*	*	*	*	

A new flavor item is added to the flavor item list. The number and type of parameters in the flavor item depend on the flavor type (see Flavor Types and Parameters, page 7-60).

The new flavor item has a default value of all wild cards (*, asterisks).

Step 4 For each cell of the new flavor item, click the asterisk and then enter an appropriate value.

For composite flavors and for the HTTP Content Category flavor:

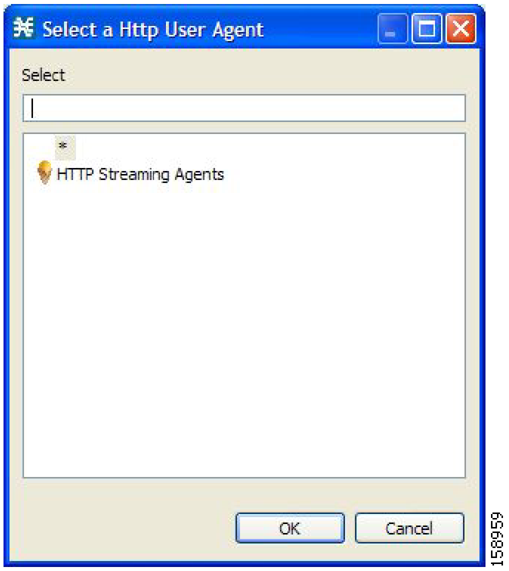
a. Click the asterisk.

A Browse button is displayed in the cell.

b. Click the **Browse** button.

A Select dialog box appears (Figure 7-52), displaying all valid values for the parameter.

Figure 7-52 Select an HTTP User Agent



c. Select an appropriate value from the list.

d. Click **OK**.

The Select dialog box closes.

The selected value is displayed in the cell.

Step 5 Repeat Steps 3 and 4 for other flavor items.

Step 6 Click **OK**.

The Flavor Settings dialog box closes.

How to Edit Flavor Items

Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > Flavors**.

The Flavor Settings dialog box appears.

Step 2 In the flavor tree, select a flavor.

Step 3 In the flavor item list, select a flavor item.

Step 4 For each cell of the selected flavor item, click the asterisk and then enter an appropriate value.

For composite flavors and for the HTTP Content Category flavor:

a. Click the asterisk.

A Browse button is displayed in the cell.

b. Click the **Browse** button.

A Select dialog box appears, displaying all valid values for the parameter.

c. Select an appropriate value from the list.

d. Click **OK**.

The Select dialog box closes.

The selected value is displayed in the cell.

Step 5 Click **OK**.

The Flavor Settings dialog box closes.

How to Delete Flavor Items

Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > Flavors**.

The Flavor Settings dialog box appears.

Step 2 In the flavor tree, select a flavor.

Step 3 In the flavor item list, right-click anywhere in a flavor item.

A popup menu appears.

Step 4 Click the **Delete** (❌) icon.

The flavor item is deleted and is no longer displayed in the flavor item list.

Step 5 Click **Close**.

The Flavor Settings dialog box closes.

Example: How to Import a List of URLs and Block Them

The following example shows how to import a URL file and configure the SCE to block these URLs

Step 1 Create a new flavor under the HTTP URL flavor type, as described in How to Add Flavors, page 7-65.

Step 2 Import a CSV file containing the URLS you wish to block.

For further information, see How to Import Service Configuration Data, page 6-11.

Note The CSV file formats are described in the "CSV File Formats" chapter of *Cisco Service Control Application Suit for Broadband Reference Guide*.

Step 3 Define a Service.

For further information, see How to Add a Service to a Service Configuration, page 7-4.

Step 4 Within the defined Service, add a service element that uses the new Flavor.

For further information, see How to Add Service Elements, page 7-12.

Step 5 Add a rule to the package in which you want to block the URLs, and associate it with the new Service.

For further information, see How to Add Rules to a Package, page 9-63.

Step 6 Configure the rule to block the flow.

For further information, see How to Define Per-Flow Actions for a Rule, page 9-66.

Managing Content Filtering

Content filtering involves classification and control of HTTP flows according to the requested URL. The classification of the URL is performed by accessing an external database.

Cisco SCA BB provides content filtering by integrating with a SurfControl Content Portal Authority (CPA) server.

Note Content filtering is not supported when unidirectional classification is enabled.

- Information About Content Filtering, page 7-73
- The Content Filtering CLI, page 7-74
- How to Configure the RDR Formatter, page 7-75
- How to Enter Line Interface Configuration Mode, page 7-76
- Managing Content Filtering Settings, page 7-76

Information About Content Filtering

The Cisco HTTP Content Filtering solution consists of:

- The SCE application
- The Cisco CPA client
- The SurfControl CPA server

The SCE application classifies each HTTP flow according to the category returned by the CPA server. This classification is then used for Cisco SCA BB traffic control and reporting. For example, you can define a rule to block browsing of the “Adult/Sexually Explicit” category or to generate reports on the volume consumed by browsing the “Kids” or “Shopping” categories.

- The SCE Application, page 7-73
- The Cisco CPA Client, page 7-73
- The SurfControl CPA Server, page 7-74

The SCE Application

The Cisco service control application runs on the SCE platform. It forwards HTTP URLs that it extracts from traffic to the CPA client and uses the categorization results to classify the original HTTP flow to a service. This classification is then used for normal Cisco SCA BB traffic control and reporting.

The SCE application communicates with the CPA client using Raw Data Records (RDRs). See How to Configure the RDR Formatter, page 7-75.

The Cisco CPA Client

The Cisco CPA client runs on the SCE platform. It sends URL queries to the CPA server for categorization, and updates Cisco SCA BB with the categorization results.

The CPA client is installed as part of the Cisco SCA BB application (PQI) installation. Use the SCE platform Command-Line Interface (CLI) (see The Content Filtering CLI, page 7-74) to configure and monitor the client.

The SurfControl CPA Server

The CPA server runs on a dedicated machine. It receives categorization requests from the CPA client, connects to the SurfControl Content Database, and responds with the category ID of the queried URL.

The SurfControl CPA Server is installed on a separate server that must be accessible from the SCE platform. Details of the installation are not within the scope of this document.

The Content Filtering CLI

Use the SCE platform Command-Line Interface (CLI) to configure and monitor content filtering using SurfControl CPA. For more information about the SCE platform CLI, see *Cisco SCE8000 CLI Command Reference.*

- CPA Client CLI Commands, page 7-74
- Description of CPA Client CLI Commands, page 7-74

CPA Client CLI Commands

The commands listed here are explained in the following section.

- Use the following CLI commands to configure the Cisco CPA client:

```
[no] cpa-client
cpa-client destination <address> [port <port>]
cpa-client retries <number_of_retries>
```

- These commands are line interface configuration commands. To run these commands you must enter line interface configuration mode (see How to Enter Line Interface Configuration Mode, page 7-76).
- Use the following CLI command in EXEC mode to monitor the status of the Cisco CPA client:

```
show interface LineCard <slot> cpa-client
```

Description of CPA Client CLI Commands

Table 7-3 gives a description of the Cisco CPA client CLI commands listed in the previous section and their default values.

Table 7-3 CPA Client CLI Commands

Command	Description	Default Value
[no] cpa-client	Enables or disables the CPA client	Disabled
cpa-client destination <address> [**port** <port>]	Enables the CPA client and sets the CPA server IP address and port	• Address—not defined • Port—9020

Table 7-3 CPA Client CLI Commands (continued)

Command	Description	Default Value
cpa-client retries <number_of_retries>	Sets the number of retries to send to the CPA server	3
show interface LineCard <slot> **cpa-client**	Monitors the CPA client status (See the following table)	—

Table 7-4 lists the information shown when monitoring the Cisco CPA client.

Table 7-4 CPA Client: Monitored Parameters

Parameter	Description
Mode	Enabled or disabled
CPA Address	—
CPA Port	—
CPA Retries	—
Status	(If enabled) Active or error (and last error description)
Counters	• Number of successful queries • Number of queries that failed because of no server response • Number of pending queries • Rate of queries per second (average over the last 5 seconds)
Timestamps	• CPA started • Last query • Last response • Last error

How to Configure the RDR Formatter

To enable the RDR formatter to issue HTTP categorization requests, configure the RDR formatter on the SCE platform.

Step 1 Make the appropriate SCE platform CLI command.

```
#>RDR-formatter destination 127.0.0.1 port 33001 category number 4 priority 100
```

Related Info

For more information about configuring the RDR formatter, see either the “Raw Data Formatting: The RDR Formatter and NetFlow Exporting” chapter of *Cisco SCE8000 10GBE Software Configuration Guide* or the “Raw Data Formatting: The RDR Formatter and NetFlow Exporting” *chapter of Cisco SCE8000 GBE Software Configuration Guide*.

How to Enter Line Interface Configuration Mode

To run line interface configuration commands you must enter line interface configuration mode and see the `SCE(config if)#` prompt displayed.

Step 1 At the SCE platform CLI prompt `(SCE#)`, type `configure`.

Step 2 Press **Enter**.

The `SCE(config)#` prompt appears.

Step 3 Type `interface LineCard 0`.

Step 4 Press **Enter**.

The `SCE(config if)#` prompt appears.

Managing Content Filtering Settings

Applying HTTP URL content filtering requires the following steps in the Service Configuration Editor:

1. Import the content filtering configuration file into your service configuration.

   By default, Cisco SCA BB creates a separate flavor (of type HTTP Content Category) for each content category and a service element for each new flavor. A new top-level service, “HTTP Browsing with Categories”, is created, comprising these service elements.

2. Create new services and map the new category flavors to them.
3. Create additional rule entries for ClickStream services for each flavor.

   You must configure ClickStream Services with the HTTP Browsing services for optimal HTTP content filtering.

4. Add content filtering rules to existing packages or create new packages that include content filtering rules.
5. Enable content filtering for selected packages.
6. Apply the service configuration.

- Importing Content Filtering Categories, page 7-76
- How to Enable Content Filtering, page 7-84
- How to View Content Filtering Settings, page 7-85
- How to Configure Content Filtering, page 7-85
- How to Remove Content Filtering Settings, page 7-86

Importing Content Filtering Categories

Before you can control HTTP flows based on content, you must import an XML file provided with the installation.

After you unzip the installation package, this file is located in the URL Filtering subfolder.

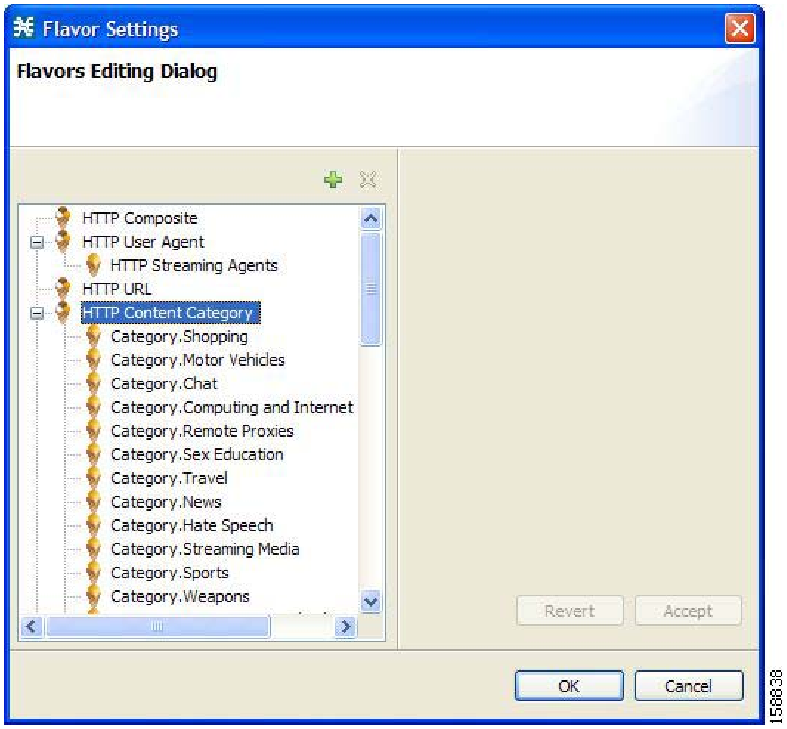
Note You cannot import content filtering categories when unidirectional classification is enabled.

- HTTP Content Category Flavors, page 7-77
- HTTP Browsing with Categories Service Elements, page 7-78
- How to Import Content Filtering Categories Using the Import Dialog Box, page 7-78
- How to Import Content Filtering Categories Using the HTTP Content Filtering Settings Dialog Box, page 7-82

HTTP Content Category Flavors

By default, Cisco SCA BB creates a separate flavor (of type HTTP Content Category) for each content category when importing the XML file (Figure 7-53).

Figure 7-53 Flavor Settings

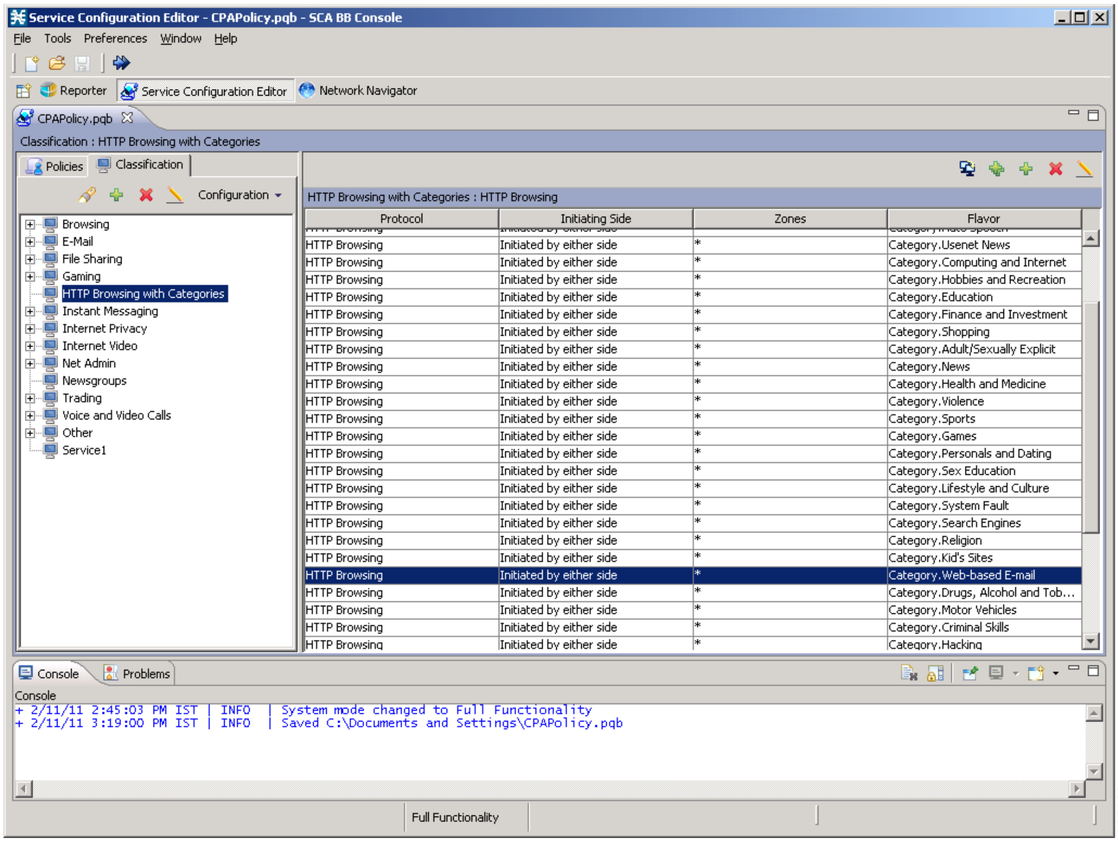


You can create additional HTTP Content Category Flavors that include two or more content categories. (See How to Add Flavors, page 7-65.)

HTTP Browsing with Categories Service Elements

By default, Cisco SCA BB creates a service element for each flavor created when importing the XML file. A new top-level service, HTTP Browsing with Categories, is created, comprising these service elements (Figure 7-54).

Figure 7-54 Service Configuration Editor



Protocol	Initiating Side	Zones	Flavor
HTTP Browsing	Initiated by either side	*	Category.Usenet News
HTTP Browsing	Initiated by either side	*	Category.Computing and Internet
HTTP Browsing	Initiated by either side	*	Category.Hobbies and Recreation
HTTP Browsing	Initiated by either side	*	Category.Education
HTTP Browsing	Initiated by either side	*	Category.Finance and Investment
HTTP Browsing	Initiated by either side	*	Category.Shopping
HTTP Browsing	Initiated by either side	*	Category.Adult/Sexually Explicit
HTTP Browsing	Initiated by either side	*	Category.News
HTTP Browsing	Initiated by either side	*	Category.Health and Medicine
HTTP Browsing	Initiated by either side	*	Category.Violence
HTTP Browsing	Initiated by either side	*	Category.Sports
HTTP Browsing	Initiated by either side	*	Category.Games
HTTP Browsing	Initiated by either side	*	Category.Personals and Dating
HTTP Browsing	Initiated by either side	*	Category.Sex Education
HTTP Browsing	Initiated by either side	*	Category.Lifestyle and Culture
HTTP Browsing	Initiated by either side	*	Category.System Fault
HTTP Browsing	Initiated by either side	*	Category.Search Engines
HTTP Browsing	Initiated by either side	*	Category.Religion
HTTP Browsing	Initiated by either side	*	Category.Kid's Sites
HTTP Browsing	Initiated by either side	*	Category.Web-based E-mail
HTTP Browsing	Initiated by either side	*	Category.Drugs, Alcohol and Tob…
HTTP Browsing	Initiated by either side	*	Category.Motor Vehicles
HTTP Browsing	Initiated by either side	*	Category.Criminal Skills
HTTP Browsing	Initiated by either side	*	Category.Hacking

```
+ 2/11/11 2:45:03 PM IST | INFO  | System mode changed to Full Functionality
+ 2/11/11 3:19:00 PM IST | INFO  | Saved C:\Documents and Settings\CPAPolicy.pqb
```

Note To view this new service, you must save and close the service configuration and then reopen it.

How to Import Content Filtering Categories Using the Import Dialog Box

You can import content filtering categories using either the **File** > **Import** menu option or the **Configuration > Classification > Content Filtering** menu option.

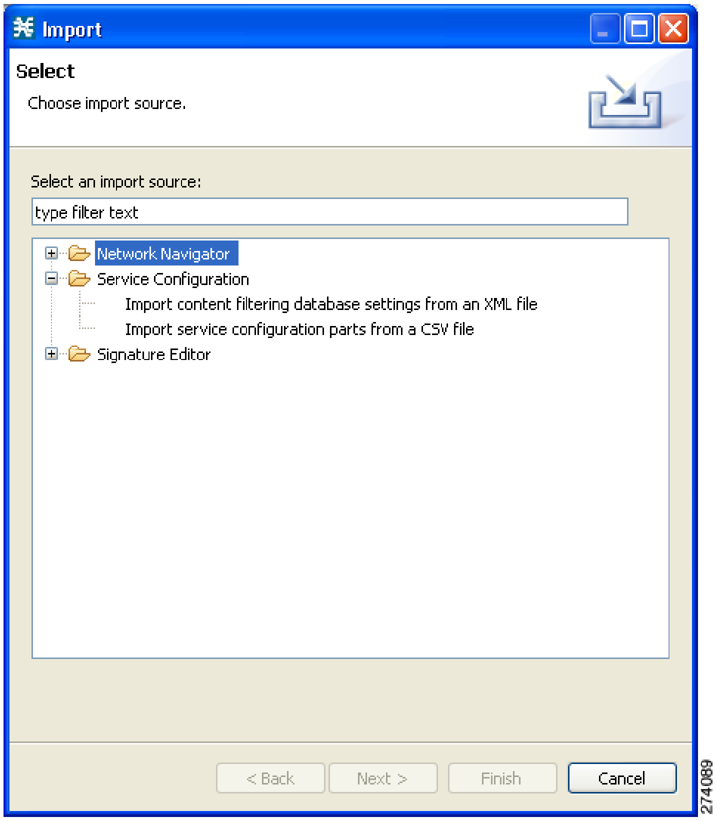
This procedure explains how to import using the **File** > **Import** menu option.

Note This is equivalent to the following procedure.

Step 1 From the Console main menu, choose **File** > **Import**.

The Import dialog box appears (Figure 7-55).

Figure 7-55 Import



Import

Select

Choose import source.

Select an import source:

type filter text

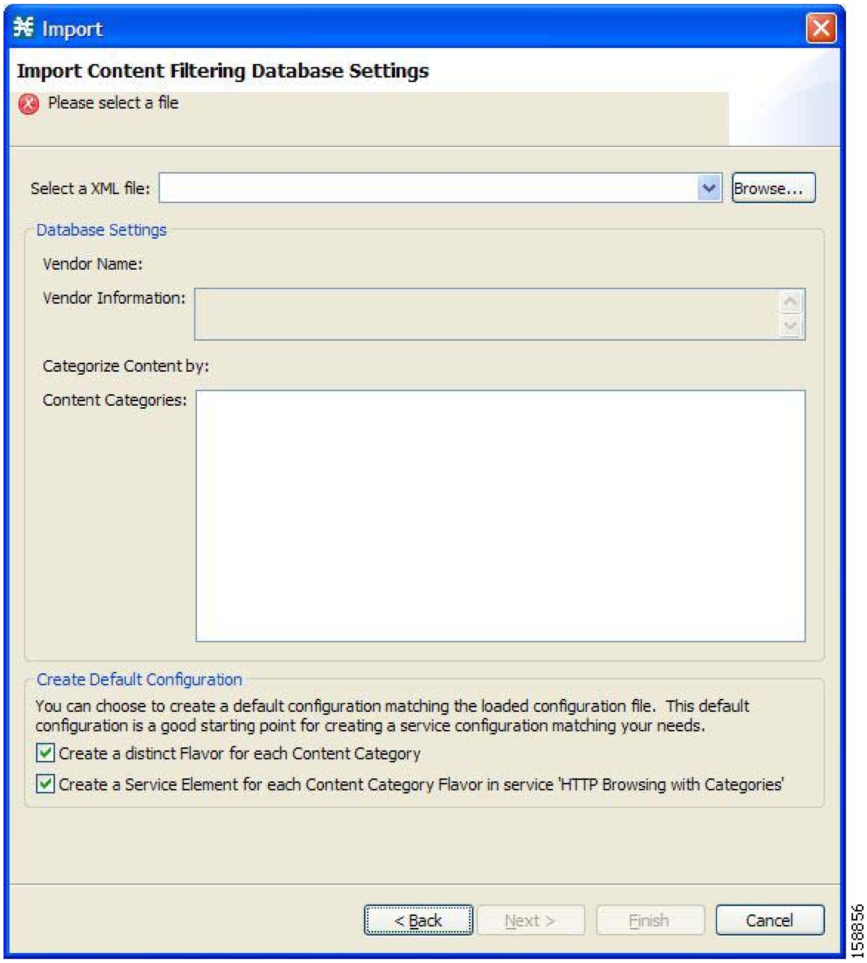
Network Navigator
Service Configuration
Import content filtering database settings from an XML file
Import service configuration parts from a CSV file
Signature Editor
< Back
Next >
Finish
Cancel
274089

Step 2 From the import source list, select **Import content filtering database settings from an XML file**.

Step 3 Click **Next**.

The Import Content Filtering Database Settings dialog box appears (Figure 7-56).

Figure 7-56 Import Content Filtering Database Settings


Import
Import Content Filtering Database Settings
Please select a file
Select a XML file:
Browse...
Database Settings
Vendor Name:
Vendor Information:
Categorize Content by:
Content Categories:
Create Default Configuration
You can choose to create a default configuration matching the loaded configuration file. This default configuration is a good starting point for creating a service configuration matching your needs.
☑ Create a distinct Flavor for each Content Category
☑ Create a Service Element for each Content Category Flavor in service 'HTTP Browsing with Categories'
< Back
Next >
Finish
Cancel
158856

Step 4 Click the **Browse** button next to the Select an XML file field.

An Open dialog box appears.

Step 5 Browse to the folder containing the file to import, and select it.

Note For CPAof SurfControl, the file is named surfcontrol.xml.

Step 6 Click **Open** to select the file.

The Open dialog box closes.

Information about the content of the XML file is displayed in the Database Settings pane of the Import Content Filtering Database Settings dialog box.

Step 7 By default, Cisco SCA BB creates a separate flavor (of type HTTP Content Category) for each content category when importing the XML file.

- To disable this option, uncheck the Create a distinct Flavor for each Content Category check box.

Note It is recommended that you do not disable this option.

Step 8 By default, Cisco SCA BB creates a service element for each flavor created in the previous Step. A new top-level service, HTTP Browsing with Categories, is created, comprising these service elements.

- To disable this option, uncheck the **Create a Service Element for each Content Category Flavor in Service 'HTTP Browsing with Categories'** check box.

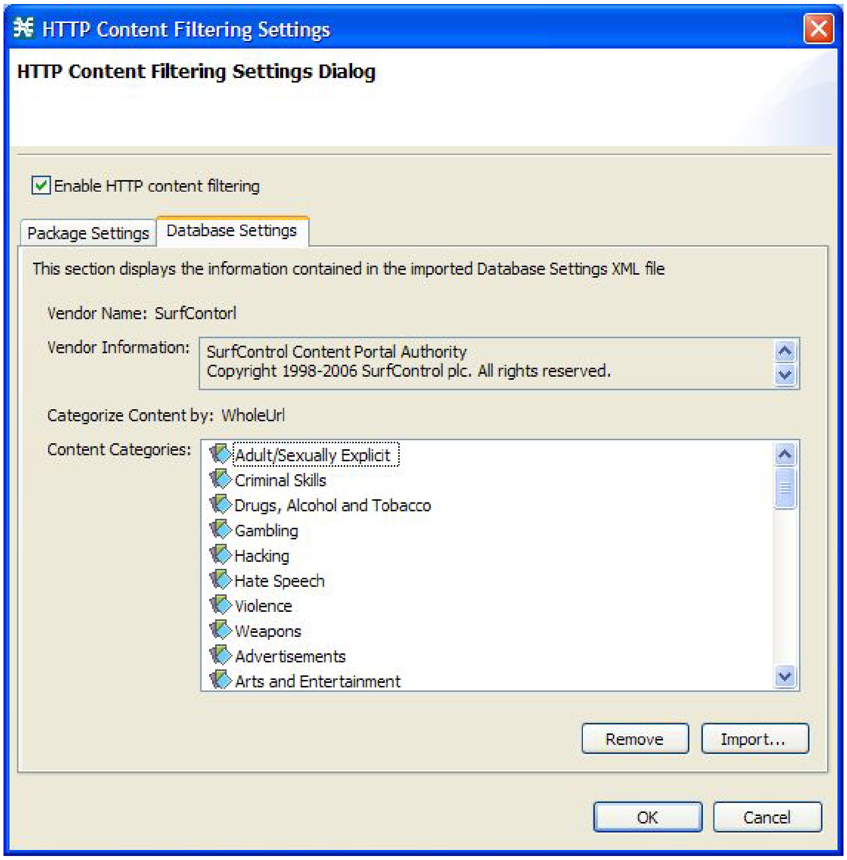
Note It is recommended that you do not disable this option.

Step 9 Click **Finish**.

The Import Content Filtering Database Settings dialog box closes.

Information from the imported file is displayed in the Database Settings tab of the HTTP Content Filtering Settings dialog box (Figure 7-57).

Figure 7-57 HTTP Content Filtering Settings



HTTP Content Filtering Settings

HTTP Content Filtering Settings Dialog

☑ Enable HTTP content filtering

This section displays the information contained in the imported Database Settings XML file

Vendor Name: SurfContorl

Vendor Information: SurfControl Content Portal Authority
Copyright 1998-2006 SurfControl plc. All rights reserved.

Categorize Content by: WholeUrl

Content Categories:
Adult/Sexually Explicit
Criminal Skills
Drugs, Alcohol and Tobacco
Gambling
Hacking
Hate Speech
Violence
Weapons
Advertisements
Arts and Entertainment

Step 10 Click **OK**.

The HTTP Content Filtering Settings dialog box closes.

How to Import Content Filtering Categories Using the HTTP Content Filtering Settings Dialog Box

You can import content filtering categories using either the **File** > **Import** menu option or the **Configuration > Classification > Content Filtering** menu option.

This procedure explains how to import using the **Configuration > Classification > Content Filtering** menu option.

Note This is equivalent to the How to Import Content Filtering Categories Using the Import Dialog Box, page 7-78 procedure.

Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > Content Filtering**.

The HTTP Content Filtering Settings dialog box appears.

Step 2 Click the **Database Settings** tab.

The Database Settings tab opens.

Step 3 Click **Import**.

The Import Content Filtering Database Settings dialog box appears.

Step 4 Click the **Browse** button next to the Select an XML file field.

An Open dialog box appears.

Step 5 Browse to the folder containing the file to import, and select it.

Note For the CPA of SurfControl, the file is named surfcontrol.xml.

Step 6 Click **Open** to select the file.

The Open dialog box closes.

Information about the content of the XML file is displayed in the Database Settings pane of the Import Content Filtering Database Settings dialog box.

Step 7 By default, Cisco SCA BB creates a separate flavor (of type HTTP Content Category) for each content category when importing the XML file.

- To disable this option, uncheck the Create a distinct Flavor for each Content Category check box.

Note It is recommended that you do not disable this option.

Step 8 By default, Cisco SCA BB creates a service element for each flavor created in the previous Step. A new top-level service, HTTP Browsing with Categories, is created, comprising these service elements.

- To disable this option, uncheck the **Create a Service Element for each Content Category Flavor in Service 'HTTP Browsing with Categories'** check box.

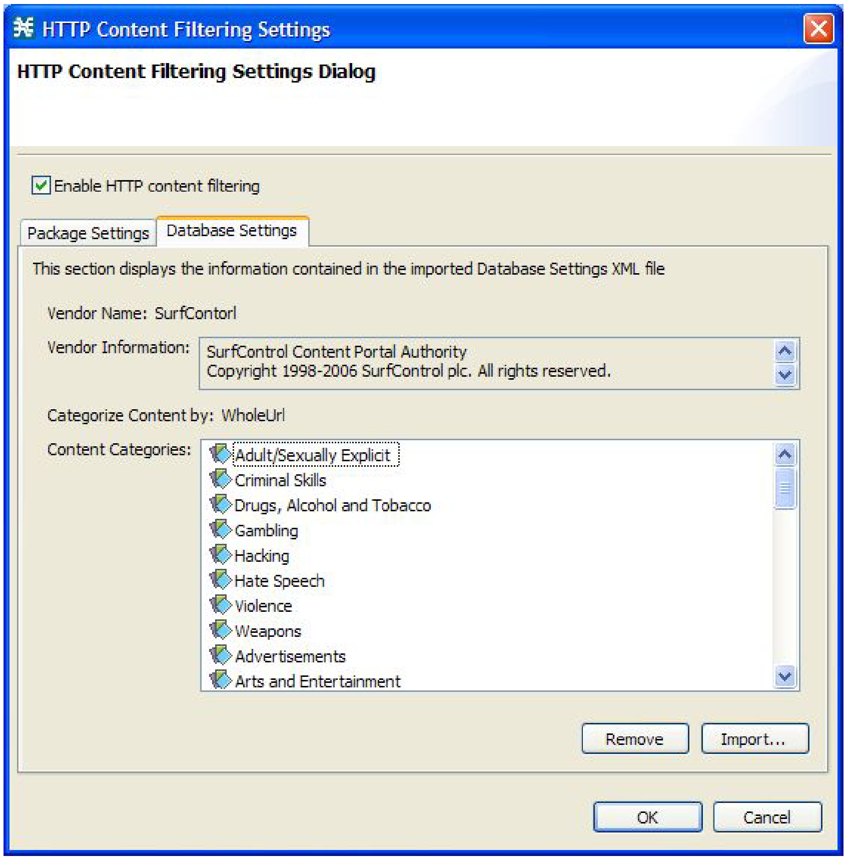
Note It is recommended that you do not disable this option.

Step 9 Click **Finish**.

The Import Content Filtering Database Settings dialog box closes.

Information from the imported file is displayed in the Database Settings tab of the HTTP Content Filtering Settings dialog box (Figure 7-58).

Figure 7-58 HTTP Content Filtering Settings



HTTP Content Filtering Settings

HTTP Content Filtering Settings Dialog

☑ Enable HTTP content filtering

This section displays the information contained in the imported Database Settings XML file

Vendor Name: SurfContorl

Vendor Information: SurfControl Content Portal Authority
Copyright 1998-2006 SurfControl plc. All rights reserved.

Categorize Content by: WholeUrl

Content Categories:
- Adult/Sexually Explicit
- Criminal Skills
- Drugs, Alcohol and Tobacco
- Gambling
- Hacking
- Hate Speech
- Violence
- Weapons
- Advertisements
- Arts and Entertainment

Step 10 Click **OK**.

The HTTP Content Filtering Settings dialog box closes.

How to Enable Content Filtering

You can specify the packages where content filtering is enabled. For packages where content filtering is disabled, HTTP flows are classified normally.

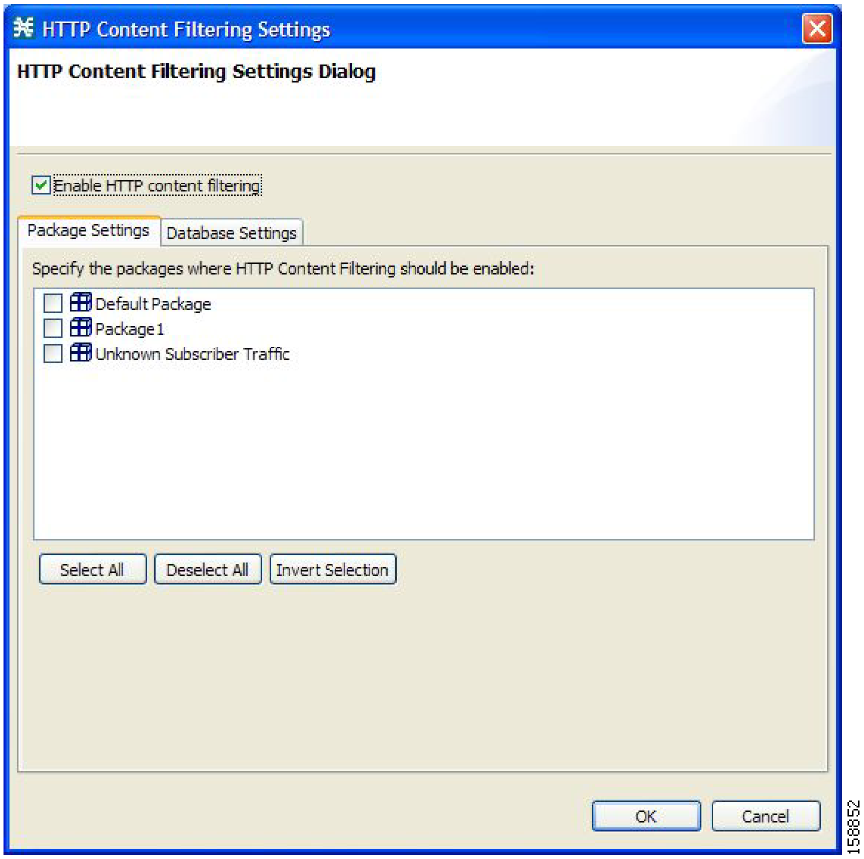
To configure content filtering, complete the following steps:

Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > Content Filtering**.

The HTTP Content Filtering Settings dialog box appears (Figure 7-59).

The Package Settings tab displays a list of all packages defined for the current service configuration.

Figure 7-59 HTTP Content Filtering Settings



HTTP Content Filtering Settings

HTTP Content Filtering Settings Dialog

☑ Enable HTTP content filtering

Package Settings | Database Settings

Specify the packages where HTTP Content Filtering should be enabled:

- ☐ Default Package
- ☐ Package1
- ☐ Unknown Subscriber Traffic

Step 2 Check the **Enable HTTP content filtering** check box.

Step 3 Check the check box next to each package for which content filtering is to be applied.

Step 4 Click **OK**.

The HTTP Content Filtering Settings dialog box closes.

How to View Content Filtering Settings

You can view whether content filtering is enabled and to which packages content filtering is applied, and information about the content filtering vendor and the content categories of the vendor.

Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > Content Filtering**.

The HTTP Content Filtering Settings dialog box appears.

The Package Settings tab displays a list of all packages defined for the current service configuration, and shows for which packages content filtering is enabled.

Step 2 Click the **Database Settings** tab.

The Database Settings tab opens.

This tab displays information about the content filtering vendor and the content categories of the vendor.

Step 3 Click **OK**.

The HTTP Content Filtering Settings dialog box closes.

How to Configure Content Filtering

While configuring Content Filtering, you must enter the ClickStream-New Page and ClickStream-New Site services along with HTTP Browsing protocol services for optimal HTTP content filtering.

The term ClickStream refers to all events generated by user clicks, including enter. If configured, SCE identifies the HTTP transactions on the flows that were initialized due to direct user actions such as click on a link, enter a URL in the browser address bar and press enter.

To configure Content Filtering, complete the following steps:

Step 1 Open Cisco SCA BB Service Configuration Editor with the default content filtering file (PQB).

Step 2 Add a new service *Service1*.

Step 3 Verify that you do not have duplicate service elements. Cisco SCA BB does not allow duplicate service elements.

Step 4 Move the desired service element from *HTTP Browsing with Categories* to *Service1*.

Step 5 In *Service1*, add a service element using protocol *ClickStream–New Page* and with the same Flavor selected in Step 4.

Step 6 In *Service1,* add a service element using protocol *ClickStream–New Site* and with the same Flavor selected in Step 4.

Step 7 Save the service configuration file (PQB).

Step 8 Use the service to create rules in the desired package.

Example: Configuring Content Filtering for Web Based E-mail

To configure content filtering for Web Based E-mail, complete the following steps:

Step 1 Open Cisco SCA BB Service Configuration Editor with the default content filtering file (PQB).

Step 2 Add a new service *Service1*.

Step 3 Move the service element *Category.Web-based E-mail* from *HTTP Browsing with Categories* to *Service1*.

Step 4 In *Service1*, add a service element using protocol *ClickStream–New Page* and Flavor *Category.Web-based E-mail*.

Step 5 In *Service1*, add a service element using protocol *ClickStream–New Site* and Flavor *Category.Web-based E-mail*.

Step 6 Save the service configuration file (PQB) and use the service to create rules in the desired package.

How to Remove Content Filtering Settings

You can remove all content filtering settings at any time.

Removing the settings:

- Removes content category flavor items from flavors
- Deletes all the content category flavor items
- Disables content filtering

Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > Content Filtering**.

The HTTP Content Filtering Settings dialog box appears.

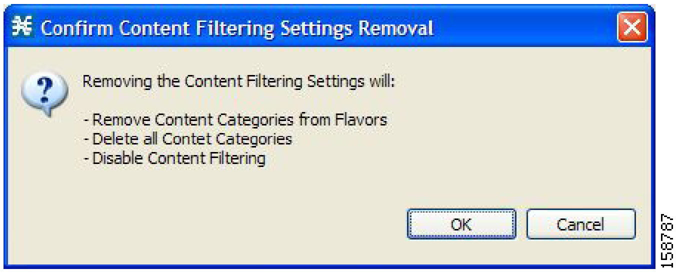
Step 2 Click the **Database Settings** tab.

The Database Settings tab opens.

Step 3 Click **Remove**.

A Confirm Content Filtering Settings Removal dialog box appears (Figure 7-60).

Figure 7-60 Confirm Content Filtering Settings Removal



Confirm Content Filtering Settings Removal

Removing the Content Filtering Settings will:

- Remove Content Categories from Flavors
- Delete all Contet Categories
- Disable Content Filtering

Step 4 Click **OK**.

All content filtering settings are removed.

Vendor Name, Vendor Information, and Content Categories are deleted from the HTTP Content Filtering Settings dialog box.

Step 5 Click **OK**.

The HTTP Content Filtering Settings dialog box closes.

- Generic Protocols—Generic IP, Generic TCP, and Generic UDP protocols, used for transactions that are not specifically mapped to a protocol by any other protocol type.
- IP Protocols—Protocols (such as ICMP), other than TCP and UDP protocols, identified according to the IP protocol number of the transaction.
- Port-Based Protocols—TCP and UDP protocols, classified according to their well-known ports. The default service configuration includes more than 750 common port-based protocols.
- Signature-Based Protocols—Protocols classified according to a Layer 7 application signature. Includes the most common protocols, such as HTTP and FTP, and a large group of popular P2P protocols.
- P2P Protocols—Peer-to-peer file-sharing application protocols classified according to a Layer 7 application signature.
- VoIP Protocols—Voice-over-IP application protocols classified according to a Layer 7 application signature.
- SIP Protocols—Protocols classified according to a Layer 7 application signature that is SIP or has SIP characteristics.
- Worm Protocols—Protocols classified according to a Layer 7 application signature that is based on traffic patterns of Internet worms.
- Packet Stream Pattern Based Protocols—Protocols classified according to a Layer 7 application signature that is based on the pattern of the packet stream (for example, the stream’s symmetry, average packet size, and rate) rather than on the packet’s payload content.
- Unidirectionally Detected Protocols—Protocols having a unidirectional signature.

Note Some protocols belong to more than one category. In particular, all predefined P2P, VoIP, SIP, Worm, and Packet Stream Pattern-Based Protocols are also defined as Signature-Based Protocols.

Step 1 From the **Classification** tab in the left pane, choose **Configuration > Classification > Protocols**.

The Protocol Settings dialog box appears.

Step 2 From the drop-down list in the Protocols tab, select the type of protocol to display.

The protocols of the selected type appear in the Protocols tab.

Step 3 Click **Close**.

The Protocol Settings dialog box closes.

Note The setting in the drop-down list is not saved. The next time you open the Protocol Settings dialog box, all protocols are displayed.

Managing OS Fingerprinting

Cisco SCE detects the operating system (OS) used by a subscriber by using the passive OS Fingerprinting. In passive OS fingerprinting, TCP and IP header received from target host is analyzed to identify the OS.

Cisco SCE uses OS fingerprinting signatures to identify the subscriber OS. By default, Cisco SCOS contains a signature file that contains a default set of OS. Details of unknown OS may be added to the signature files using the Cisco SCA BB Console.

Cisco SCE also determines whether the subscriber is behind a NAT and whether the same subscriber is connecting using multiple OS. If multiple OS is detected for the same subscriber, Cisco SCE considers the subscriber as using a NAT.

From the Cisco SCA BB Console, you can also configure SCE to send the OS information of the subscriber in Gx messages.

Note The OS Fingerprinting feature is supported only on SCE 8000 devices.

Limitations:

- OS information is available only for logged-in or active subscribers.
- The signature database is built based on the default settings used by various OS. If the user changes the default parameters like TCP window size through registries, it would not be possible or may lead to wrong classification of the OS.
- If the subscriber has only one flow, then OS type is be detected. Subscribers that have only UDP flows are not detected
- If all users behind a NAT use the same OS, it will not be possible to identify NAT.
- If a subscriber runs multiple OS using VMWare, it may be detected as NAT even though the subscriber is not in a NAT environment
- OS finger printing is not done continuously for any subscriber. So, if a subscriber changes OS or moves to a NAT environment during the time when he is not sampled, OS Information and NAT cannot be detected.

Managing OS Fingerprinting

You can configure OS Fingerprinting using the Cisco SCA BB Console.

- How to Enable OS Fingerprinting, page 7-89
- How to Install OS Fingerprinting Signatures, page 7-89
- How to View Subscriber OS Information, page 7-90

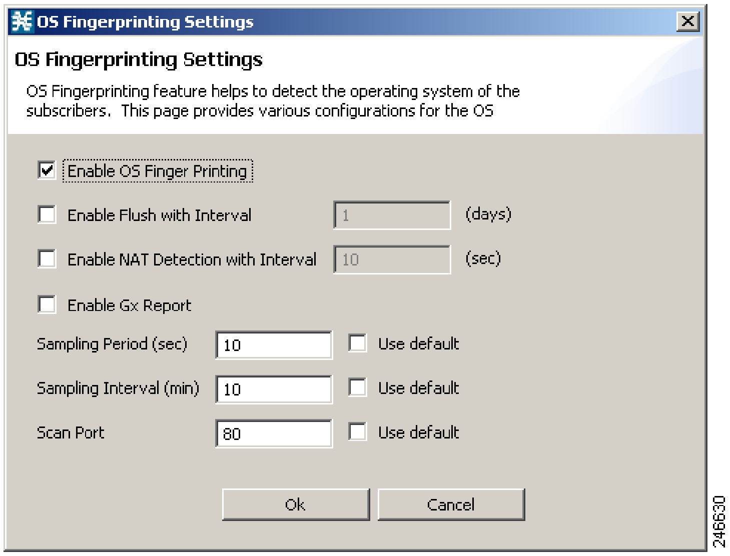
How to Enable OS Fingerprinting

Step 1 In Service Configuration Editor, select **Configuration > OS Finger Print...**.

The OS Fingerprinting Settings dialog box appears (Figure 7-61).

Step 2 Check the Enable OS Finger Printing check box.

Figure 7-61 OS Finger Print Settings Dialog Box



OS Fingerprinting Settings

OS Fingerprinting Settings

OS Fingerprinting feature helps to detect the operating system of the subscribers. This page provides various configurations for the OS

☑ Enable OS Finger Printing

☐ Enable Flush with Interval 1 (days)

☐ Enable NAT Detection with Interval 10 (sec)

☐ Enable Gx Report

Sampling Period (sec) 10 ☐ Use default

Sampling Interval (min) 10 ☐ Use default

Scan Port 80 ☐ Use default

Step 3 Enable Flush with Interval—Check the Enable Flush with Interval check box and enter the interval in days to configure the interval after which the OS information will be reset.

Step 4 (Optional) Enable NAT Detection with Interval—Check the Enable NAT Detection with Interval check box and enter the interval in seconds to configure the time period with-in which multiple OS detection will trigger NAT identification. Default value is 10 seconds.

Step 5 (Optional) Enable Gx Report—Check the Enable Gx Report check box to enable Gx Reports.

Step 6 Sampling Period (sec)—Configure how long flows from a subscriber will finger-printed. Default is 10 seconds. Check the **Use default** check box to use the default period.

Step 7 Sampling Interval (min)—Enter the time in minutes to configure the frequency at which flows will be finger-printed. Default is 10 minutes. Check the **Use default** check box to use default interval.

Step 8 (Optional) Scan Port—Enter a value for Scan Port used for opening OS finger printing flows. Check the **Use default** check box to use the default port—port 80—for the flows. Ports 20, 21, 69, and 5060 are not allowed.

Step 9 Click **Ok**.

How to Install OS Fingerprinting Signatures

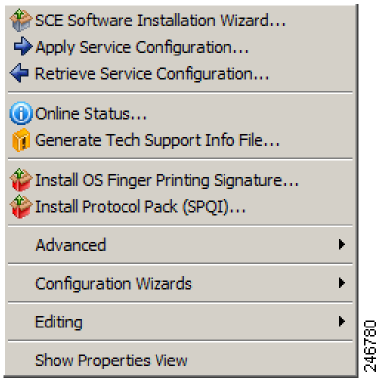
Step 1 (Optional) Using Network Navigator, add the device on which you need to install the signatures.

Step 2 Enable OS Fingerprinting. See the How to Enable OS Fingerprinting section.

Step 3 Apply the configuration to the device.

Step 4 In the Site Manager tree, right-click an SCE device. A popup menu appears.

Step 5 From the menu, select **Install OS Finger Printing Signature...**.


SCE Software Installation Wizard...
Apply Service Configuration...
Retrieve Service Configuration...
Online Status...
Generate Tech Support Info File...
Install OS Finger Printing Signature...
Install Protocol Pack (SPQI)...
Advanced
Configuration Wizards
Editing
Show Properties View
246780

The Password Management dialog box appears. For details on password management, see the "Password Management" section on page 5-8.

Step 6 Enter the User Name and Password, and click **Update**.

The Update OSFP Signature window appears.

Step 7 Enter the path to signature file in the Select OSFP Signature File field or Browse to the signature file.

Step 8 Click **Finish**.

A confirmation message appears in the Console.

How to View Subscriber OS Information

Step 1 Enable OS Fingerprinting. See the How to Enable OS Fingerprinting section.

Step 2 Apply the configuration to the device.

Step 3 From Subscriber Manager, view the Subscriber list. See Figure 11-6.

Step 4 Right-click on the device, and select **View Online Status**.

The online status of the subscriber appears near the console panel with the OS information. The OS Fingerprinting is available for Anonymous Groups through Anonymous Group Manager GUI Tool.

How To Disable OS Fingerprinting

Step 1 In the Service Configuration Editor, select **Configuration > OS Finger Print...**.

The OS Finger Printing Settings dialog box appears.

Step 2 Uncheck the Enable OS Finger Printing check box.

The OS Fingerprinting CLI

Use the following CLI command in EXEC mode to monitor the OS details of the subscriber:

```
show os-fingerprinting party-name
```

The following is a sample output of the command. In this example, Cisco SCE has detected a NAT and behind the NAT two OS. One is iOS with an index number 65 and another OS that is not known to Cisco SCE:

```
SCE8000#> show os-fingerprinting party-name 192.168.0.5@testofp
Subscriber 192.168.0.5@testofp OS-Info:
 IP Address:192.168.0.5
   OS-INFO:
    1. INDEX: 65        OS Name: iOS
    UNKNOWN OS FOUND
    NAT DETECTED
```

CHAPTER 8

Using the Service Configuration Editor: Traffic Accounting and Reporting

Revised: August 08, 2013, OL-24178-09

Introduction

This chapter explains how to work with usage counters and Raw Data Records (RDRs).

Traffic Accounting and Reporting is the second step in creating a Cisco SCA BB service configuration.

- Usage Counters, page 8-1
- Raw Data Records, page 8-2
- NetFlow Records, page 8-2
- Managing RDR Settings, page 8-3

Usage Counters

The Cisco SCA BB collects and maintains various network metrics (such as volume and number of sessions) per service. This accounting takes place per subscriber, per group of subscribers (package or group of packages), and for the entire link.

Service Usage Counters

The system uses the service usage counters to generate data about the total use of each service. A service can use either its own usage counters, or the usage counters of its parent service. For example, in the default service configuration the SMTP and POP3 services share the E-Mail service usage counters. Service hierarchy determines the assignment of services to usage counters. For details on how to configure the service hierarchy, see How to Edit Services, page 7-9.

Package Usage Counters

The Cisco SCA BB also collects and maintains various network metrics per package.

The system uses the package usage counters to generate data about the total use of each package. A package can use either its own usage counters, or the usage counters of its parent package. The package hierarchy determines the assignment of packages to usage counters. For details on how to configure the package hierarchy, see How to Set Advanced Package Options, page 9-57.

Raw Data Records

Service Control Engine (SCE) platforms generate and transmit Raw Data Records (RDRs) that contain information relevant to the service provider. These RDRs contain a wide variety of information and statistics, depending on the configuration of the system.

- All RDR data is based on Layer 3 volume.
- RDRs are not generated for filtered traffic. For details, see Filtering the Traffic Flows, page 10-23.

The content and structure of each type of RDR is listed in the “Raw Data Records: Formats and Field Contents” chapter of *Cisco Service Control Application for Broadband Reference Guide*.

NetFlow Records

- You enable and disable the export of NetFlow records using the CLI.

  You can export records per supported RDR type. The data in the following RDR types can be exported using NetFlow:

  - Subscriber Usage RDR
  - Package Usage RDR
  - Link Usage RDR
  - Zone Usage RDR
- The NetFlow records can be sent to more than one collection device.
- NetFlow records can be generated concurrently with RDRs.

Managing RDR Settings

This section explains how to configure the generation of the different types of RDRs.

The content and structure of each type of RDR is listed in the "Raw Data Records: Formats and Field Contents" chapter of *Cisco Service Control Application for Broadband Reference Guide*.

- RDRs are not generated for filtered traffic (see Filtering the Traffic Flows, page 10-23).
- All RDR data is based on Layer 3 volume.

The RDR Settings Dialog Box

The RDR Settings dialog box allows you to control the generation of RDRs for an entire service configuration. This dialog box contains seven tabs:

- Usage RDRs tab—Allows you to enable the generation each type of Usage RDR, and define their generation intervals
- Transaction RDRs tab—Allows you to enable the generation of Transaction RDRs and define their maximum rate of generation
- Quota RDRs tab—Allows you to enable the generation of each type of Quota RDR, and define their generation parameters
- Transaction Usage RDRs tab—Allows you to specify the packages and services for which Transaction Usage RDRs are generated
- Log RDRs tab—Allows you to specify the packages and services for which Log RDRs are generated
- Real-Time Subscriber RDRs tab—Allows you to enable the generation of Real-Time Subscriber Usage RDRs, and define their generation intervals and maximum rate of generation
- Real-Time Signaling RDRs tab—Allows you to specify the packages and services for which Real-Time Signaling RDRs are generated

Note Media Flow RDRs and Malicious Traffic Periodic RDRs are enabled and configured in the How to Edit Advanced Service Configuration Options, page 10-64.

How to Manage Usage RDRs

The four types of Usage RDRs contain data about total usage of all services included in a service usage counter:

- Link Usage RDRs—For the entire link
- Package Usage RDRs—For all subscribers to a particular package
- Subscriber Usage RDRs—For a particular subscriber
- Virtual Links Usage RDRs—For a particular group of virtual links
- Zone Usage RDRs—For the entire zone

You can enable or disable the generation of each type of Usage RDR, and set the generation interval for each type of Usage RDR. You can limit the generation rate of Subscriber Usage RDRs. This is advisable when there are a large number of subscribers.

By default, all four types of Usage RDRs are enabled. (Virtual Links Usage RDRs are enabled by default only if Virtual Links mode was enabled when you created the service configuration.)

Note Usage RDRs are not generated for blocked sessions. A session is blocked if the service to which the session is mapped is blocked for the package for this subscriber (see How to Define Per-Flow Actions for a Rule, page 9-66), or if the subscriber has exceeded the allowed quota for this service (see Managing Quotas, page 9-83).

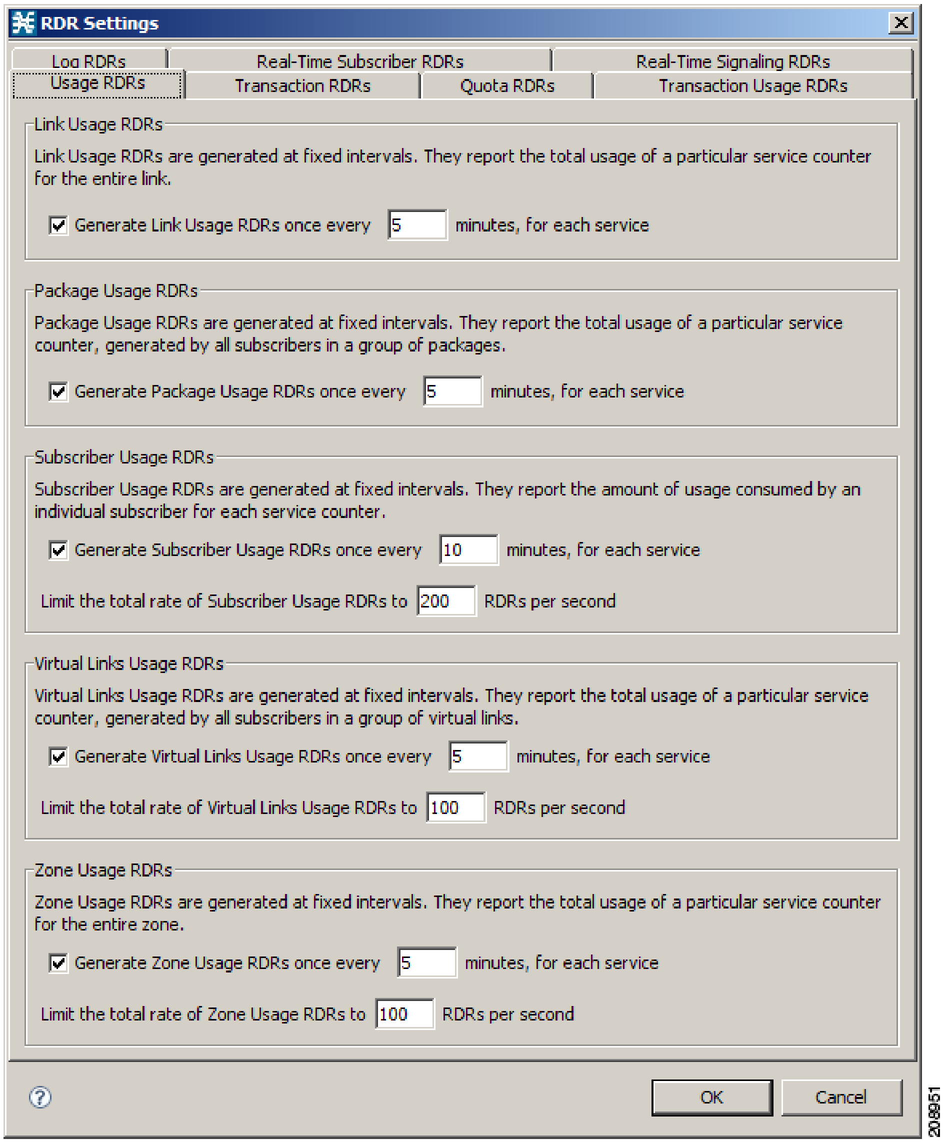
For detailed information regarding the RDR purpose, default destination, content, generation logic, tag, and fields, see the following sections in *Cisco Service Control Application for Broadband Reference Guide*:

- Link Usage RDR
- Package Usage RDR
- Subscriber Usage RDR
- Virtual Link Usage RDR
- Zone Usage RDR

Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > RDR Settings**.

The RDR Settings dialog box appears (Figure 8-1).

Figure 8-1 RDR Settings



Link Usage RDRs

Link Usage RDRs are generated at fixed intervals. They report the total usage of a particular service counter for the entire link.

☑ Generate Link Usage RDRs once every 5 minutes, for each service

Package Usage RDRs

Package Usage RDRs are generated at fixed intervals. They report the total usage of a particular service counter, generated by all subscribers in a group of packages.

☑ Generate Package Usage RDRs once every 5 minutes, for each service

Subscriber Usage RDRs

Subscriber Usage RDRs are generated at fixed intervals. They report the amount of usage consumed by an individual subscriber for each service counter.

☑ Generate Subscriber Usage RDRs once every 10 minutes, for each service

Limit the total rate of Subscriber Usage RDRs to 200 RDRs per second

Virtual Links Usage RDRs

Virtual Links Usage RDRs are generated at fixed intervals. They report the total usage of a particular service counter, generated by all subscribers in a group of virtual links.

☑ Generate Virtual Links Usage RDRs once every 5 minutes, for each service

Limit the total rate of Virtual Links Usage RDRs to 100 RDRs per second

Zone Usage RDRs

Zone Usage RDRs are generated at fixed intervals. They report the total usage of a particular service counter for the entire zone.

☑ Generate Zone Usage RDRs once every 5 minutes, for each service

Limit the total rate of Zone Usage RDRs to 100 RDRs per second

Step 2 To enable the generation of a selected type of Usage RDR, check the appropriate **Generate Usage RDRs** check box.

To disable the generation of a selected type of Usage RDR, uncheck the appropriate **Generate Usage RDRs** check box.

Step 3 To change the generation interval for a selected type of Usage RDR, enter the interval in minutes between each generation of this type of Usage RDRs in the appropriate Generate Usage RDRs field.

Step 4 To limit the generation rate of Subscriber Usage RDRs, enter the maximum number of Subscriber Usage RDRs to be generated per second in the Limit the Total Rate of Subscriber Usage RDRs field.

Step 5 Click **OK**.

The RDR Settings dialog box closes.

The new configuration for the generation of Usage RDRs is saved.

How to Manage Transaction RDRs

Each Transaction RDRs contain data about a single network transaction. The SCE platform can generate Transaction RDRs for selected service types. You can use these RDRs, for example, to generate statistical histograms that help understand the traffic traversing the network.

You can enable or disable the generation of Transaction RDRs, set the maximum number of Transaction RDRs generated per second, and select for which services these RDRs are generated. You can also assign a relative weight to each service. The relative weight determines the relative number of Transaction RDRs that are generated for this service, compared to other services.

By default, at most 100 Transaction RDRs are generated per second, and all services are given the same weight.

For detailed information regarding the RDR purpose, default destination, content, generation logic, tag, and fields, see the "Transaction RDR" section in *Cisco Service Control Application for Broadband Reference Guide*.

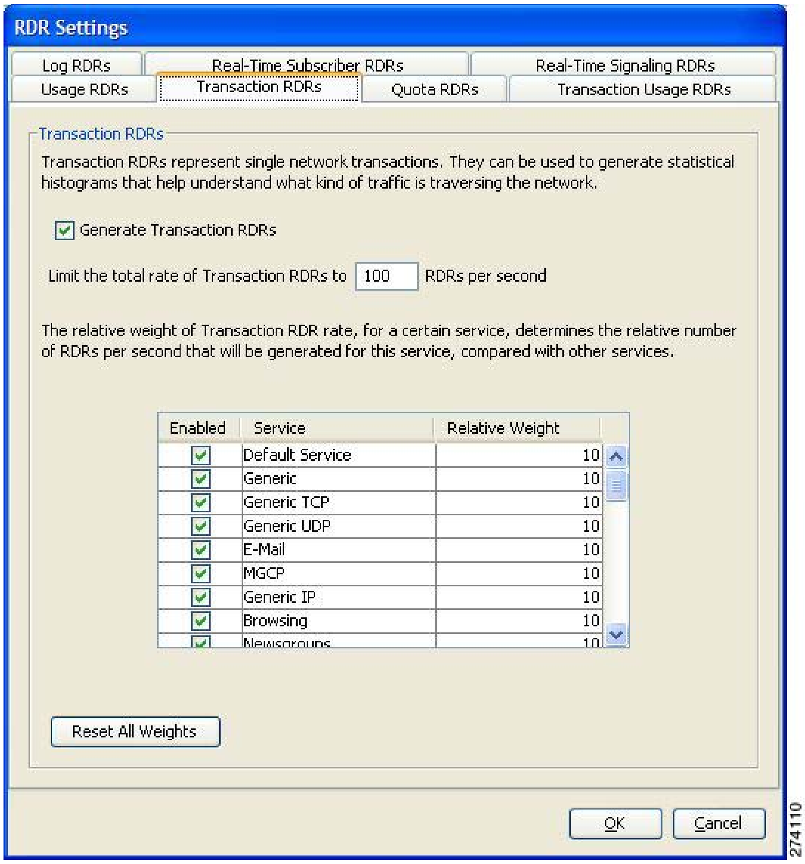
Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > RDR Settings**.

The RDR Settings dialog box appears.

Step 2 Click the **Transaction RDRs** tab.

The Transaction RDRs tab opens (Figure 8-2).

Figure 8-2 Transaction RDRs Tab



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 100 RDRs per second

The relative weight of Transaction RDR rate, for a certain service, determines the relative number of RDRs per second that will be generated for this service, compared with other services.

Enabled	Service	Relative Weight
☑	Default Service	10
☑	Generic	10
☑	Generic TCP	10
☑	Generic UDP	10
☑	E-Mail	10
☑	MGCP	10
☑	Generic IP	10
☑	Browsing	10
☑	Newsgroups	10

Step 3 To enable the generation of Transaction RDRs, check the **Generate Transaction RDRs** check box.

To disable the generation of Transaction RDRs, uncheck the **Generate Transaction RDRs** check box.

Step 4 To change the maximum generation rate for Transaction RDRs, enter the desired rate in the Limit the Total Rate of Transaction RDRs field.

Step 5 To disable the generation of Transaction RDRs for a selected service, uncheck the **Enabled** check box next to the service name.

Step 6 To set the relative weight for a selected service, double-click in the appropriate cell in the **Relative Weight** column, and enter the desired weight.

Step 7 Click **OK**.

The RDR Settings dialog box closes.

The new configuration for the generation of Transaction RDRs is saved.

How to Manage Quota RDRs

Each Quota RDR contains data for a single subscriber. There are four types of Quota RDRs:

- Quota Breach RDRs—Generated when a quota breach occurs, that is, when services that try to consume from a depleted quota bucket.

  A breached service is handled according to its breach-handling settings. For example, when the quota for a service is consumed, you can block its flows.
- Remaining Quota RDRs—Generated as quota is consumed, but only if a bucket state has change since the last Remaining Quota RDR was generated.
- Quota Threshold Breach RDRs—Generated when the remaining quota in a bucket falls below a threshold. External systems can treat this RDR as a quota request and provision the subscriber with an additional quota before the bucket is depleted.
- Quota State Restore RDRs—Generated when a subscriber is introduced. When a subscriber logs out, their remaining quota is stored in the Cisco Service Control Management Suite (SCMS) Subscriber Manager (SM). When the subscriber logs in again, this quota is restored from the SM.

You can enable or disable the generation each type of Quota RDR and define the rate of generation of these RDRs.

- For Remaining Quota RDRs, you can set the generation interval, and limit the generation rate (advisable when there are a large number of subscribers).
- For Quota Threshold RDRs, you can configure the threshold.

By default, all Quota RDRs are disabled.

For detailed information regarding the RDR purpose, default destination, content, generation logic, tag, and fields, see the following sections in *Cisco Service Control Application for Broadband Reference Guide*:

- Quota Breach RDR
- Remaining Quota RDR
- Quota Threshold Breach RDR
- Quota State Restore RDR

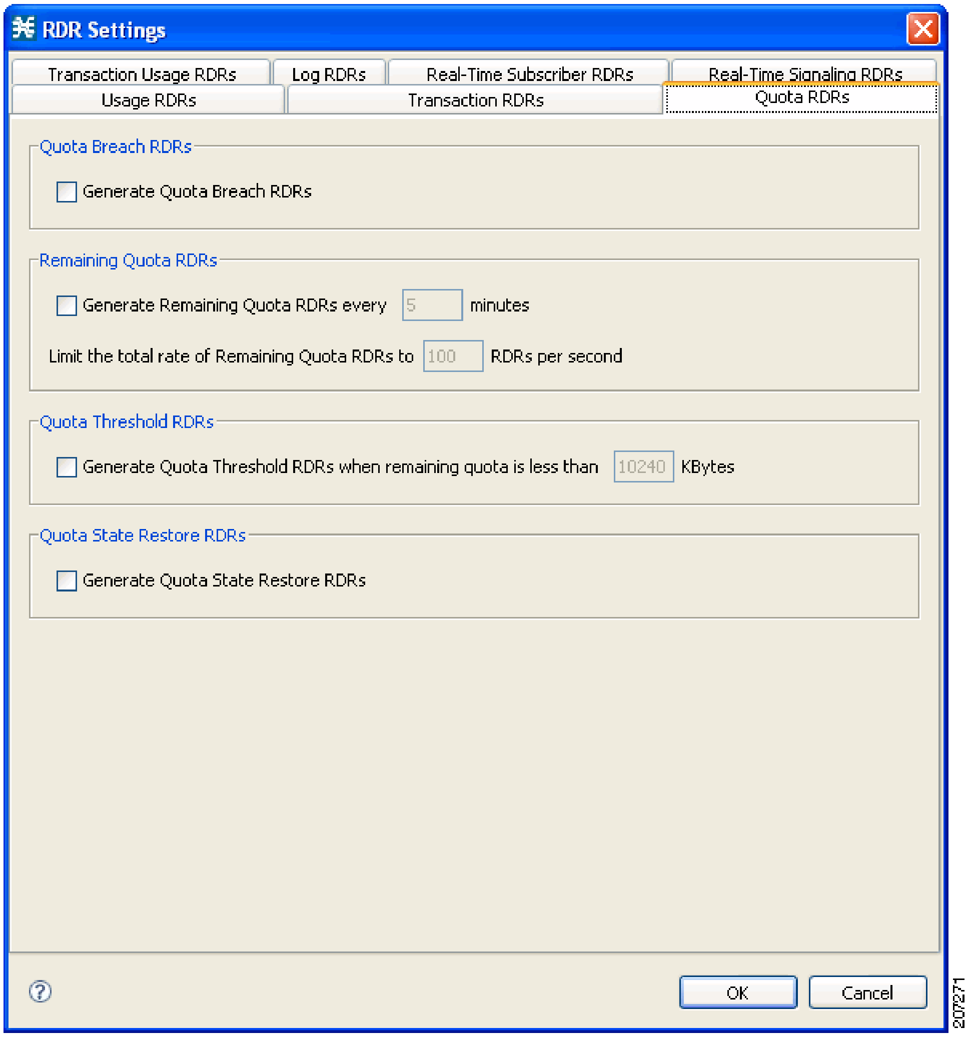
Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > RDR Settings**.

The RDR Settings dialog box appears.

Step 2 Click the **Quota RDRs** tab.

The Quota RDRs tab opens (Figure 8-3).

Figure 8-3 Quota RDRs Tab



Quota Breach RDRs

□ Generate Quota Breach RDRs

Remaining Quota RDRs

□ Generate Remaining Quota RDRs every 5 minutes

Limit the total rate of Remaining Quota RDRs to 100 RDRs per second

Quota Threshold RDRs

□ Generate Quota Threshold RDRs when remaining quota is less than 10240 KBytes

Quota State Restore RDRs

□ Generate Quota State Restore RDRs

Step 3 To enable the generation of Quota Breach RDRs, check the **Generate Quota Breach RDRs** check box.

Step 4 To enable the generation of Remaining Quota RDRs, check the **Generate Remaining Quota RDRs** check box.

Step 5 To change the generation interval of Remaining Quota RDRs, in the Generate Remaining Quota RDRs field, enter the interval in minutes between each generation of the RDR.

Step 6 To limit the maximum generation rate of Remaining Quota RDRs, in the Limit the Total Rate of Remaining Quota RDRs field, enter the maximum number of Remaining Quota RDRs to be generated per second.

Step 7 To enable the generation of Quota Threshold RDRs, check the **Generate Quota Threshold RDRs** check box.

Step 8 To change the Threshold for Quota Threshold RDRs, in the Generate Quota Threshold RDRs field, enter the threshold for which Quota Threshold RDRs are generated.

Step 9 To enable the generation of Quota State Restore RDRs, check the **Generate Quota State Restore RDRs** check box.

Step 10 Click **OK**.

The RDR Settings dialog box closes.

The new configuration for the generation of Quota RDRs is saved.

How to Manage Transaction Usage RDRs

Transaction Usage RDRs are generated for all transactions of selected packages or for selected services per package. Each Transaction Usage RDR contains data about a single network transaction. You can use these RDRs, for example, to build detailed usage logs for specific services and subscribers for transaction-based billing.

Caution Generating and collecting an RDR for each transaction can compromise performance. Enable Transaction Usage RDR generation only for services and packages that must be monitored or controlled.

You can select the packages and services for which Transaction Usage RDRs are generated. The following RDRs are also generated for these packages and services:

- HTTP Transaction Usage RDR
- RTSP Transaction Usage RDR
- VoIP Transaction Usage RDR

By default, no Transaction Usage RDRs are generated.

Note Media Flow RDRs are enabled using the Advance Service Configuration Options. When enabled, Media Flow RDRs are generated at the end of every SIP and Skype media flow. You can use the Media Flow RDRs to distinguish between SIP voice and video calls. For details on enabling Media Flow RDRs, see How to Edit Advanced Service Configuration Options, page 10-64.

For details on the RDR purpose, default destination, content, generation logic, tag, and fields, see the following sections in *Cisco Service Control Application for Broadband Reference Guide*:

- Transaction Usage RDR
- HTTP Transaction Usage RDR
- RTSP Transaction Usage RDR
- VoIP Transaction Usage RDR

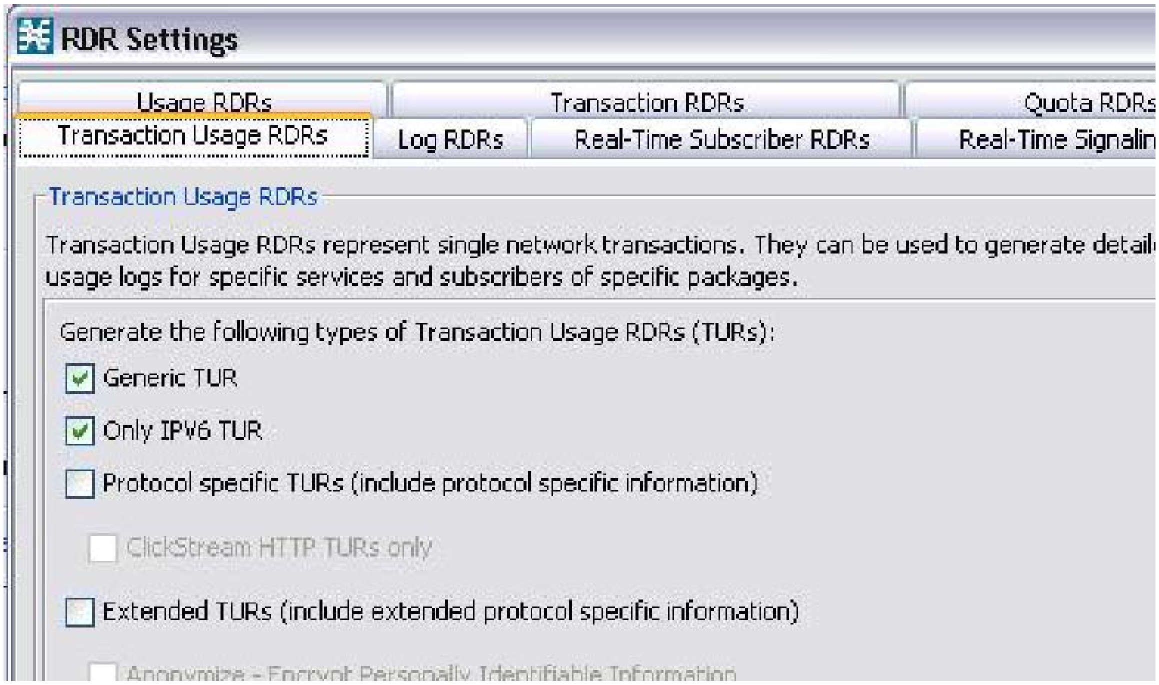
Step 1 From the Classification tab in the left pane of Service Configuration Editor window, choose **Configuration > Classification > RDR Settings**.

The RDR Settings dialog box appears.

Step 2 Click the **Transaction Usage RDRs** tab.

The information under the Transaction Usage RDRs tab is dispalyed(Figure 8-4).

Figure 8-4 Transaction Usage RDRs Tab



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

Generate the following types of Transaction Usage RDRs (TURs):

☑ Generic TUR

☑ Only IPV6 TUR

□ Protocol specific TURs (include protocol specific information)

□ ClickStream HTTP TURs only

□ Extended TURs (include extended protocol specific information)

□ Anonymize - Encrypt Personally Identifiable Information

Step 3 Check one or more of the following types of Transaction Usage RDRs to be generated:

- **Generic TUR**
- **Only IPV6 TUR**
- **Protocol Specific TURs (include protocol specific information)**
- **Extended TURs (include extended protocol specific information)**

If you select Only IPV6 TUR, the Only IPV6 TUR checkbox is enabled. Check this box to generate only the IPv6 TUR.

If you check Protocol specific TURs, the ClickStream HTTP TURs only checkbox is enabled. Check this box to generate only the HTTP TUR with clickstream signature for the selected service and packages.

If you check Extended TURS, the Anonymize - Encrypt Personally Identifiable Information checkbox is enabled. Check this box to anonymize data.

Step 4 (Optional) To enable the generation of Transaction Usage RDRs for a selected package, check the check box next to the package name in the package tree.

The package expands to show all component services of the package; all services are checked.

Step 5 Enable the generation of Transaction Usage RDRs for selected services of a package.

a. Expand the node of the desired package.

b. Check the check box next to the service name of each service for which a Transaction Usage RDR is to be generated.

Step 6 (Optional) Limit the generation of Transaction Usage RDRs by session size.

a. Check the **Generate TUR only for sessions exceeding** check box.

The Bytes field is enabled.

b. Enter the minimum session size in bytes for which a Transaction Usage RDR should be generated for the session.

Step 7 (Optional) Enable the generation of additional, interim Transaction Usage RDRs for long flows. (Usually, a Transaction Usage RDR is generated only when a flow closes.)

a. Check the **Enable Interim TUR to be generated every** check box.

The Minutes field is enabled.

b. Enter the required time in minutes between each generation of a Transaction Usage RDR for each flow.

Step 8 Click **OK**.

The RDR Settings dialog box closes.

The new configuration for the generation of Transaction Usage RDRs is saved.

How to Manage Log RDRs

Log RDRs, which provide information about system events, are generated in response to specific actions or state changes. There are two types of Log RDRs:

- Blocking RDRs—Generated each time a transaction is blocked
- Breach RDRs—Generated each time a bucket exceeds the global threshold

You can set the maximum number of Log RDRs generated per second. You can select the packages and services for which Blocking RDRs are generated.By default:

- Blocking RDRs are generated for all packages
- Breach RDRs are always generated

Note At most, 20 Log RDRs are generated for each second.

For details on the RDR purpose, default destination, content, generation logic, tag, and fields, see the following sections in *Cisco Service Control Application for Broadband Reference Guide*:

- Blocking RDR
- Quota Breach RDR

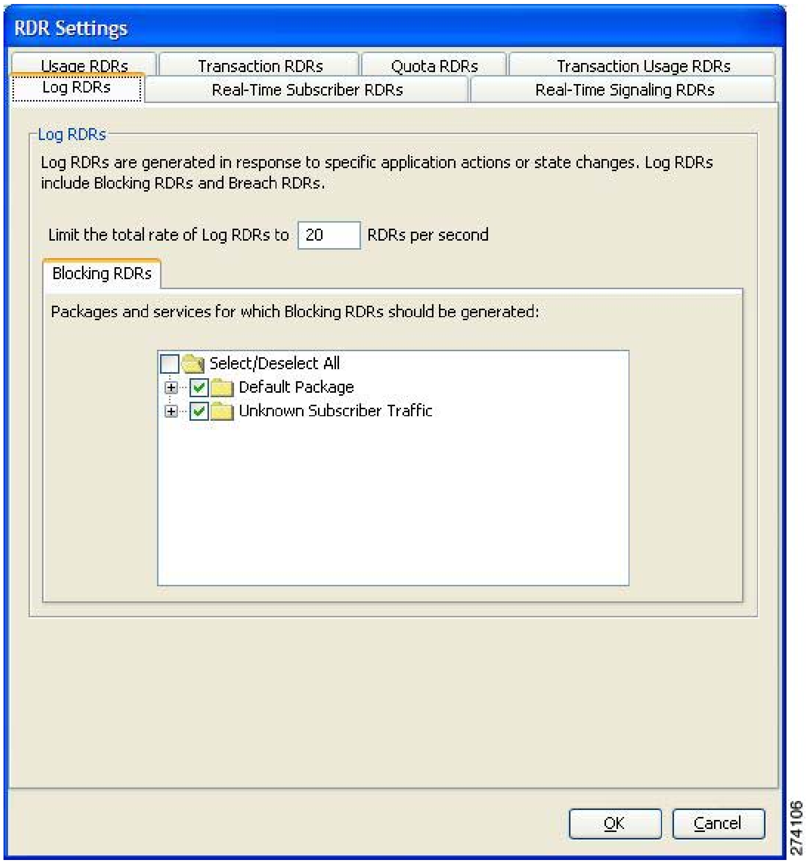
Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > RDR Settings**.

The RDR Settings dialog box appears.

Step 2 Click the **Log RDRs** tab.

The Log RDRs tab opens (Figure 8-5).

Figure 8-5 Log RDRs Tab



Log RDRs are generated in response to specific application actions or state changes. Log RDRs include Blocking RDRs and Breach RDRs.

Limit the total rate of Log RDRs to 20 RDRs per second

Packages and services for which Blocking RDRs should be generated:

- □ Select/Deselect All
- ☑ Default Package
- ☑ Unknown Subscriber Traffic

Step 3 To change the maximum generation rate for Log RDRs, enter the desired rate in the Limit the Total Rate of Log RDRs field.

Step 4 To enable the generation of Blocking RDRs for selected packages, check the check box next to the package name in the package tree.

The package expands to show all component services of the package; all the services are checked.

Step 5 Enable the generation of Blocking RDRs for selected services of a package.

a. Expand the node of the desired package.

b. Check the check box next to the service name of each desired service.

Step 6 Click **OK**.

The RDR Settings dialog box closes.

The new configuration for the generation of Log RDRs is saved.

How to Manage Real-Time Subscriber Usage RDRs

Real-Time Subscriber Usage RDRs, which report subscriber usage, are generated for each individual subscriber for each service used, at specified intervals. These RDRs permit a more granular monitoring of selected subscribers when necessary.

For details on selecting the subscribers to be monitored, see Selecting Subscribers for Real-Time Usage Monitoring, page 14-15.

Caution Generating and collecting Real-Time Subscriber Usage RDRs for many subscribers can compromise performance. Enable Real-Time Subscriber Usage RDR generation only for subscribers that must be monitored.

You can enable or disable the generation of Real-Time Subscriber Usage RDRs, set the generation interval for these RDRs, and set the maximum number generated per second.

By default, Real-Time Subscriber Usage RDRs:

- Are enabled (but only for selected subscribers)
- Are generated for each subscriber once every minute
- Are limited to 100 RDRs generated per second

For details on the RDR purpose, default destination, content, generation logic, tag, and fields, see the “Real-Time Subscriber Usage RDR” section in *Cisco Service Control Application for Broadband Reference Guide*.

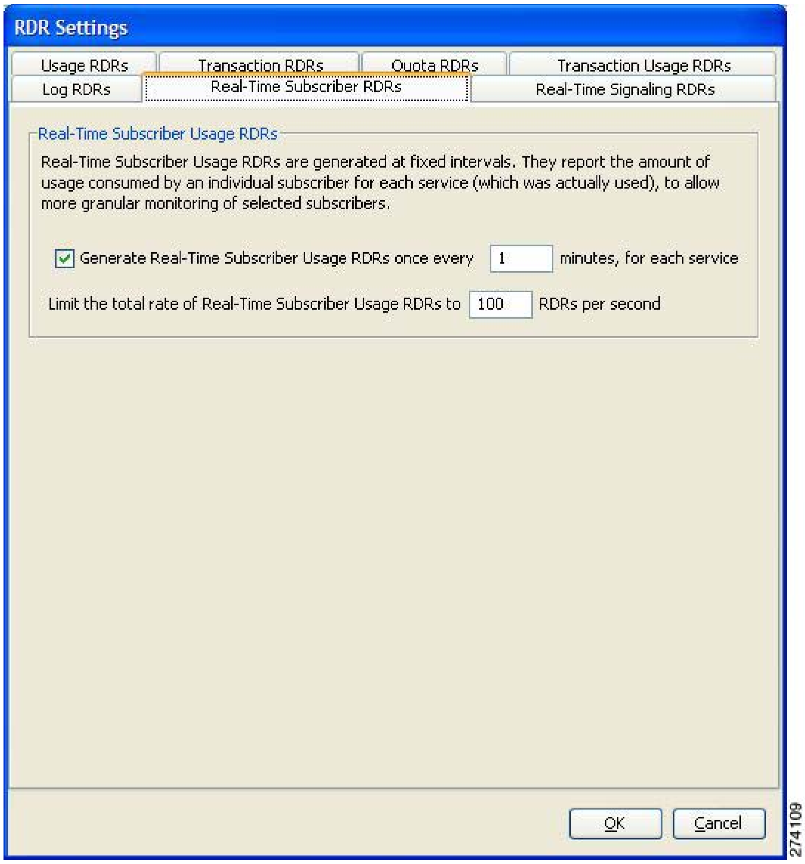
Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > RDR Settings**.

The RDR Settings dialog box appears.

Step 2 Click the **Real-Time Subscriber RDRs** tab.

The Real-Time Subscriber RDRs tab opens (Figure 8-6).

Figure 8-6 Real-Time Subscriber RDRs Tab



RDR Settings

Real-Time Subscriber Usage RDRs

Real-Time Subscriber Usage RDRs are generated at fixed intervals. They report the amount of usage consumed by an individual subscriber for each service (which was actually used), to allow more granular monitoring of selected subscribers.

☑ Generate Real-Time Subscriber Usage RDRs once every 1 minutes, for each service

Limit the total rate of Real-Time Subscriber Usage RDRs to 100 RDRs per second

Step 3 To enable the generation of Real-Time Subscriber Usage RDRs, check the **Generate Real-Time Subscriber Usage RDRs** check box.

Step 4 To change the generation interval for Real-Time Subscriber Usage RDRs, enter the desired interval in minutes between each generation of the RDRs in the Generate Real-Time Subscriber Usage RDRs field.

Step 5 To limit the generation rate of Real-Time Subscriber Usage RDRs, enter the maximum number of Real-Time Subscriber Usage RDRs to be generated per second in the Limit the total rate of Real-Time Subscriber Usage RDRs field.

Step 6 Click **OK**.

The RDR Settings dialog box closes.

The new configuration for the generation of Real-Time Subscriber Usage RDRs is saved.

How to Manage Real-Time Signaling RDRs

Real-Time Signaling RDRs can be used to signal external systems concerning events detected by the SCE platform, allowing real-time actions to be taken across the network.

Real-Time Signaling RDRs, are generated at the beginning and end of a flow, at specified intervals after the beginning of the flow, and at the beginning and end of a network attack.

There are two groups of Real-Time Signaling RDRs:

- Flow Signaling RDRs:
  - Flow Start Signaling RDRs
  - Flow Stop Signaling RDRs
  - Flow Interim Signaling RDRs
- Attack Signaling RDRs:
  - Attack Start Signaling RDRs
  - Attack Stop Signaling RDRs

You can enable or disable the generation of Flow Signaling RDRs for selected packages, or for selected services per package. You can set the generation interval for Flow Interim Signaling RDRs, which can be generated only if Flow Start and Flow Stop Signaling RDRs are enabled.

You can enable or disable the generation of Attack Signaling RDRs for selected packages.

Note Malicious Traffic Periodic RDRs are enabled and configured in How to Edit Advanced Service Configuration Options, page 10-64.

For detailed information regarding the RDR purpose, default destination, content, generation logic, tag, and fields, see the following sections in the *Cisco Service Control Application for Broadband Reference Guide*:

- Flow Start RDR
- Flow End RDR
- Ongoing Flow RDR
- Attack Start RDR
- Attack End RDR

By default, no Real-Time Signaling RDRs are generated.

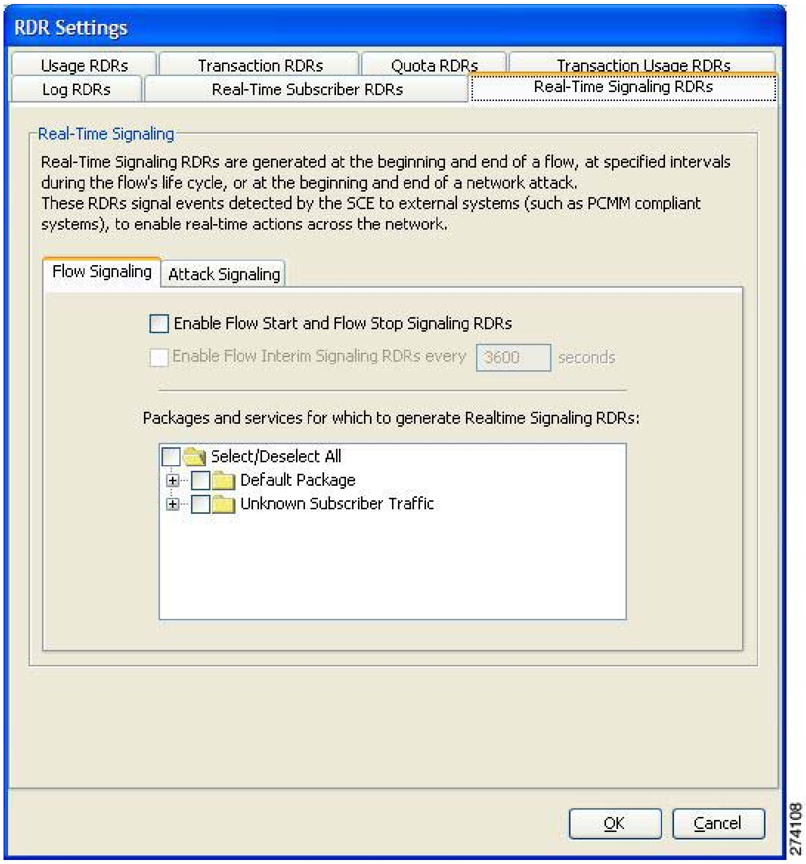
Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > RDR Settings**.

The RDR Settings dialog box appears.

Step 2 Click the **Real-Time Signaling RDRs** tab.

The Real-Time Signaling RDRs tab opens (Figure 8-7).

Figure 8-7 Real-Time Signaling RDRs Tab



Real-Time Signaling RDRs are generated at the beginning and end of a flow, at specified intervals during the flow's life cycle, or at the beginning and end of a network attack.
These RDRs signal events detected by the SCE to external systems (such as PCMM compliant systems), to enable real-time actions across the network.

□ Enable Flow Start and Flow Stop Signaling RDRs

□ Enable Flow Interim Signaling RDRs every 3600 seconds

Packages and services for which to generate Realtime Signaling RDRs:

□ Select/Deselect All
□ Default Package
□ Unknown Subscriber Traffic

Step 3 To enable the generation of Flow Start and Flow Stop Signaling RDRs, check the **Enable Flow Start and Flow Stop Signaling RDRs** check box.

Note Generation of Flow Start and Flow Stop Signaling RDRs is not supported when unidirectional classification is enabled. If you try to check the Enable Flow Start and Flow Stop Signaling RDRs check box when unidirectional classification is enabled, an RDR Settings Error message appears.

Click **OK**, and continue at Step 8.

The Enable Flow Interim Signaling RDRs check box is enabled.

Step 4 To enable the generation of Flow Interim Signaling RDRs, check the **Enable Flow Interim Signaling RDRs** check box.

The Enable Flow Interim Signaling RDRs field is enabled.

Step 5 To change the generation interval for Flow Interim Signaling RDRs, enter the interval in minutes between each generation of the RDRs in the Enable Flow Interim Signaling RDRs field.

Step 6 To enable the generation of Flow Interim Signaling RDRs for selected packages, check the check box next to the package name in the package tree.

The package expands to show all component services of the package; all the services are checked.

Step 7 To enable the generation of Flow Interim Signaling RDRs for selected services of a package:

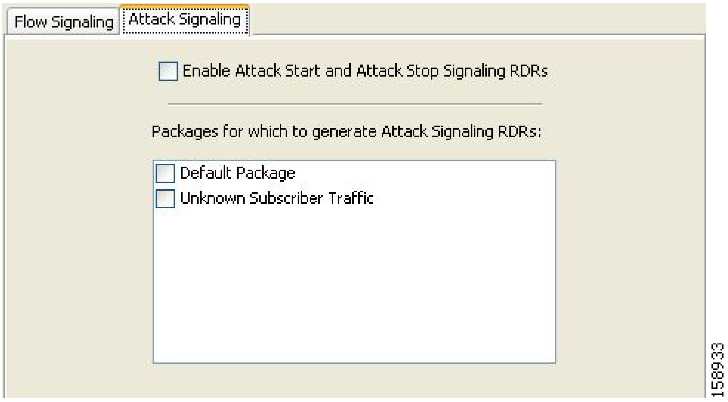
a. Expand the node of the desired package.

b. Check the check box next to the service name of each desired service.

Step 8 To enable the generation of Attack Signaling RDRs:

a. In the body of the Real-Time Signaling RDRs tab, click the **Attack Signaling** tab (Figure 8-8).

Figure 8-8 Attack Signaling Tab



□ Enable Attack Start and Attack Stop Signaling RDRs

Packages for which to generate Attack Signaling RDRs:

□ Default Package
□ Unknown Subscriber Traffic

b. Check the **Enable Attack Start and Attack Stop Signaling RDRs** check box.

Step 9 To enable the generation of Attack Signaling RDRs for selected packages, check the check box next to the package name in the package list.

Step 10 Click **OK**.

The RDR Settings dialog box closes.

The new configuration for the generation of Real-Time Signaling RDRs is saved.

CHAPTER 9

Using the Service Configuration Editor: Traffic Control

Revised: August 08, 2013, OL-24178-09

Introduction

The Traffic Control capabilities of the Service Control Engine (Service Control platform, and the Cisco Service Control Application for Broadband) are used to limit and prioritize traffic flows. Control of traffic is based on parameters such as the service of the flow, the package of the subscriber, and the quota state of the subscriber.

Managing Bandwidth

The upstream and downstream interfaces are each assigned one default global controller. You can add additional global controllers.

The number of global controllers a service configuration can contain varies based on the SCE hardware. The maximum number of global controllers including the default global controllers are:

- Cisco SCE 2000—1024 upstream and 1024 downstream
- Cisco SCE 8000 multi-Gigabit Ethernet—1024 upstream and 1024 downstream
- Cisco SCE 8000 10 Gigabit Ethernet—4096 upstream and 4096 downstream

After you have defined global controllers, you can add subscriber BW controllers (BWCs) to packages, and map these subscriber BWCs to different global controllers.

Note In release 3.7.5, the global bandwidth controller for IPv6 works in the subscriberless mode. The IPv6 traffic is mapped to a default subscriber (N/A). Bandwidth control should be performed on the Unknown Subscriber Package. The maximum and the default package ID of the Unknown Subscriber value is 4999.

Caution If you enable or disable Virtual Links mode, all user-defined global controllers are deleted from the service configuration. A subscriber BWC that pointed to a user-defined global controller now points to the default global controller. (Other parameters of these subscriber BWCs remain unchanged.)

Managing Global Bandwidth

The upstream and downstream interfaces are each assigned one default global controller that, by default, controls the total link traffic. Based on the Cisco SCE hardware, the number of global controllers you can add to a service configuration varies. For details, see the "Managing Bandwidth" section on page 9-2.

You can also define the bandwidth total link limit to be less than the physical capacity of the Cisco SCE platform for each interface separately. When another device that has limited BW capacity is next to the SCE platform on the IP stream, you can have this limitation enforced in a policy-aware manner by the SCE platform, instead of having it enforced arbitrarily by the other device.

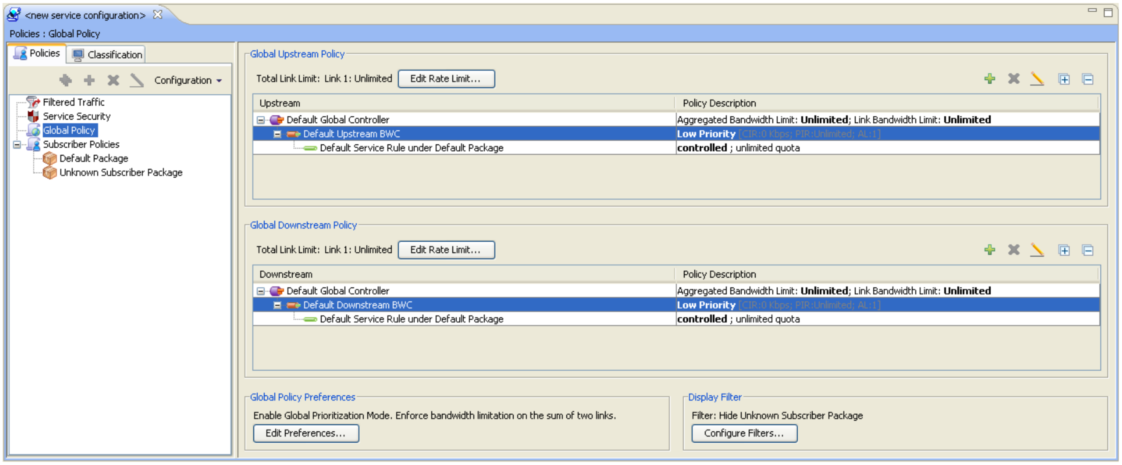
How to View Global Controller Settings

Note Global controller bandwidth is based on Layer 1 volume.
Accounting, reporting, and subscriber bandwidth control in Cisco SCA BB is based on Layer 3 volume.

Step 1 In the Policies tab, click **Global Policy**.

The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane (Figure 9-1).

Figure 9-1 Global Bandwidth Settings



Total Link Limit: Link 1: Unlimited

Upstream	Policy Description
Default Global Controller	Aggregated Bandwidth Limit: **Unlimited**; Link Bandwidth Limit: **Unlimited**
Default Upstream BWC	**Low Priority** [CIR:0 Kbps; PIR:Unlimited; AL:1]
Default Service Rule under Default Package	**controlled** ; unlimited quota

Total Link Limit: Link 1: Unlimited

Downstream	Policy Description
Default Global Controller	Aggregated Bandwidth Limit: **Unlimited**; Link Bandwidth Limit: **Unlimited**
Default Downstream BWC	**Low Priority** [CIR:0 Kbps; PIR:Unlimited; AL:1]
Default Service Rule under Default Package	**controlled** ; unlimited quota

Enable Global Prioritization Mode. Enforce bandwidth limitation on the sum of two links.

Filter: Hide Unknown Subscriber Package

The two check boxes near the top of the Global Controllers tab are used only in dual-link systems (see How to Define Global Controllers, page 9-11).

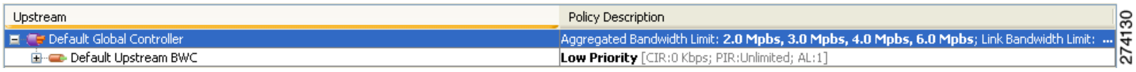
The main part of the pane contains the Upstream area listing upstream global controllers and the Downstream area listing downstream global controllers. Each list has two columns:

- **Upstream** or **Downstream**—Displays the hierarchy of global controllers, bandwidth controllers, and service rules. Each global controller has the bandwidth controllers that are connected to it listed as children. Each bandwidth controller has the service rules associated with it listed as children.
- **Policy Description**—Summarizes the details of the global controller, bandwidth controller, or service rule in the corresponding column. In the rows containing the global controller details, the maximum bandwidth value permitted to this global controller is displayed.

  For each global controller, you can set different values for the maximum bandwidth for each of the four time frames defined by the default calendar. For details, see Managing Calendars, page 9-76.

  - A single value in this field indicates that the maximum bandwidth for this global controller is constant.
  - If each time frame has a different maximum bandwidth, the maximum bandwidth for each time frame is displayed, separated by commas (Figure 9-2).

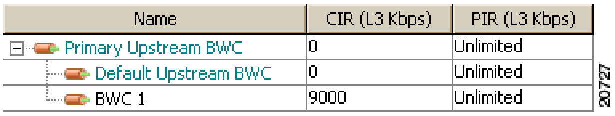
Figure 9-2 Time Frame Display



Upstream	Policy Description
Default Global Controller	Aggregated Bandwidth Limit: **2.0 Mpbs, 3.0 Mpbs, 4.0 Mpbs, 6.0 Mpbs**; Link Bandwidth Limit: ...
Default Upstream BWC	**Low Priority** [CIR:0 Kbps; PIR:Unlimited; AL:1]

- If two time frames have the same maximum bandwidth, the value is not repeated (Figure 9-3). (So **40,,,100** means that the first three time frames have a maximum bandwidth of 40 percent of the total link limit, and the fourth time frame has a maximum bandwidth equal to the total link limit.)

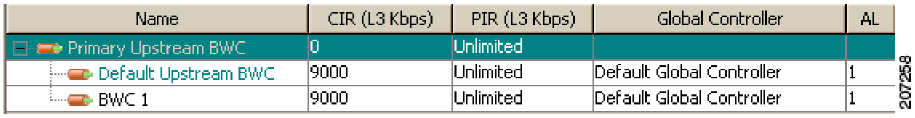
Figure 9-3 Time Frame Details



Name	CIR (L3 Kbps)	PIR (L3 Kbps)
Primary Upstream BWC	0	Unlimited
Default Upstream BWC	0	Unlimited
BWC 1	9000	Unlimited

Above the area (Upstream or Downstream) of each interface, the total link limit is displayed (Figure 9-4).

Figure 9-4 Total Link Time



Name	CIR (L3 Kbps)	PIR (L3 Kbps)	Global Controller	AL
Primary Upstream BWC	0	Unlimited		
Default Upstream BWC	9000	Unlimited	Default Global Controller	1
BWC 1	9000	Unlimited	Default Global Controller	1

How to Filter Global Controllers

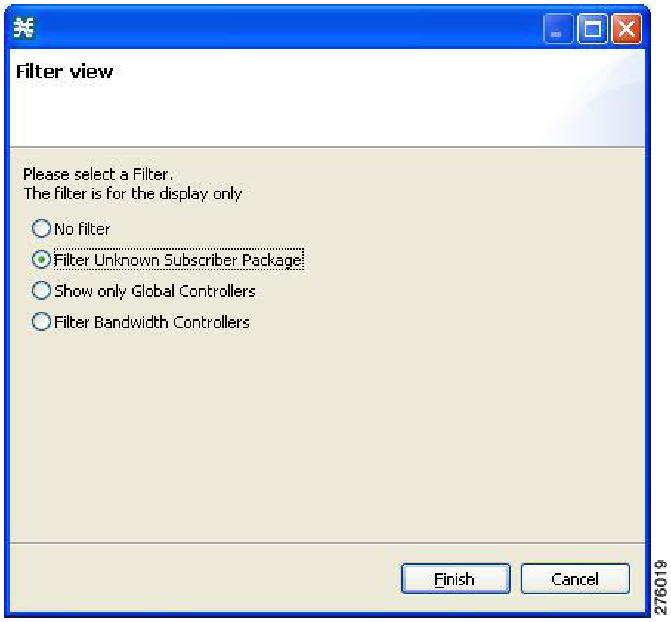
Step 1 In the Policies tab, click **Global Policy**.

The Global Bandwidth Settings are displayed in the right (Rule) pane.

Step 2 Click **Configure Filters**.

The Filter View dialog box appears (Figure 9-5).

Figure 9-5 Filter View



Please select a Filter.
The filter is for the display only

○ No filter
● Filter Unknown Subscriber Package
○ Show only Global Controllers
○ Filter Bandwidth Controllers

Step 3 Choose one of the filter radio buttons:

- **No Filter**
- **Filter Unknown Subscriber Package**
- **Show only Global Controllers**
- **Filter Bandwidth Controllers**

Step 4 Click **Finish**.

The Filter View dialog box closes and the right (Rule) pane is filtered according to your selection.

How to Edit the Total Link Limits

You can limit the total bandwidth for each SCE link passing through the SCE platform.

For example, if a device connected to the SCE platform on the IP stream has limited BW capacity, you can limit the bandwidth for each SCE link passing through the SCE platform to match the capacity of the other device.

Note The total bandwidth here means the limit for each SCE link and not the aggregated limit on all the links.

The total link limits, for each SCE link, for upstream and downstream traffic are defined independently.

To edit the total link limits, complete the following steps:

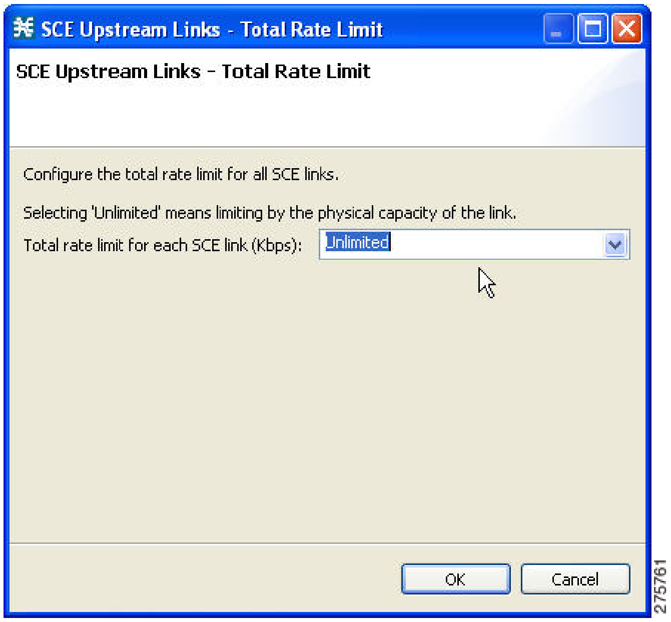
Step 1 In the Policies tab, click **Global Policy**.

The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.

Step 2 In the Upstream or Downstream section, click **Edit Rate Limit** (Figure 9-6).

Note The display appearance of Figure 9-6 depends on the global controller mode setting.

Figure 9-6 SCE Upstream Links - Total Rate Limit



SCE Upstream Links - Total Rate Limit

SCE Upstream Links - Total Rate Limit

Configure the total rate limit for all SCE links.

Selecting 'Unlimited' means limiting by the physical capacity of the link.

Total rate limit for each SCE link (Kbps): Unlimited

Step 3 Select the total rate limit in the Total rate limit for each SCE link (Kbps) field.

Step 4 Click **OK**.

Your changes are saved.

The Global Controller Settings dialog box closes.

How to Add Global Controllers

Based on the Cisco SCE hardware, the number of global controllers you can add to a service configuration varies. For details, see the "Managing Bandwidth" section on page 9-2.

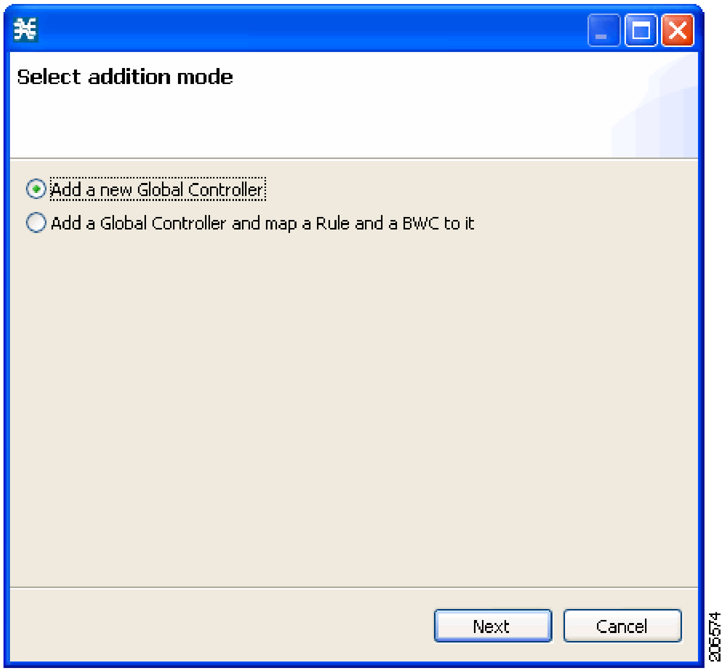
Step 1 In the Policies tab, click **Global Policy**.

The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.

Step 2 Above the area (Upstream or Downstream) of the desired interface, click the **Add** (✚) icon.

The Select Addition mode dialog box appears (Figure 9-7).

Figure 9-7 Select Addition Mode



Select addition mode

● Add a new Global Controller

○ Add a Global Controller and map a Rule and a BWC to it

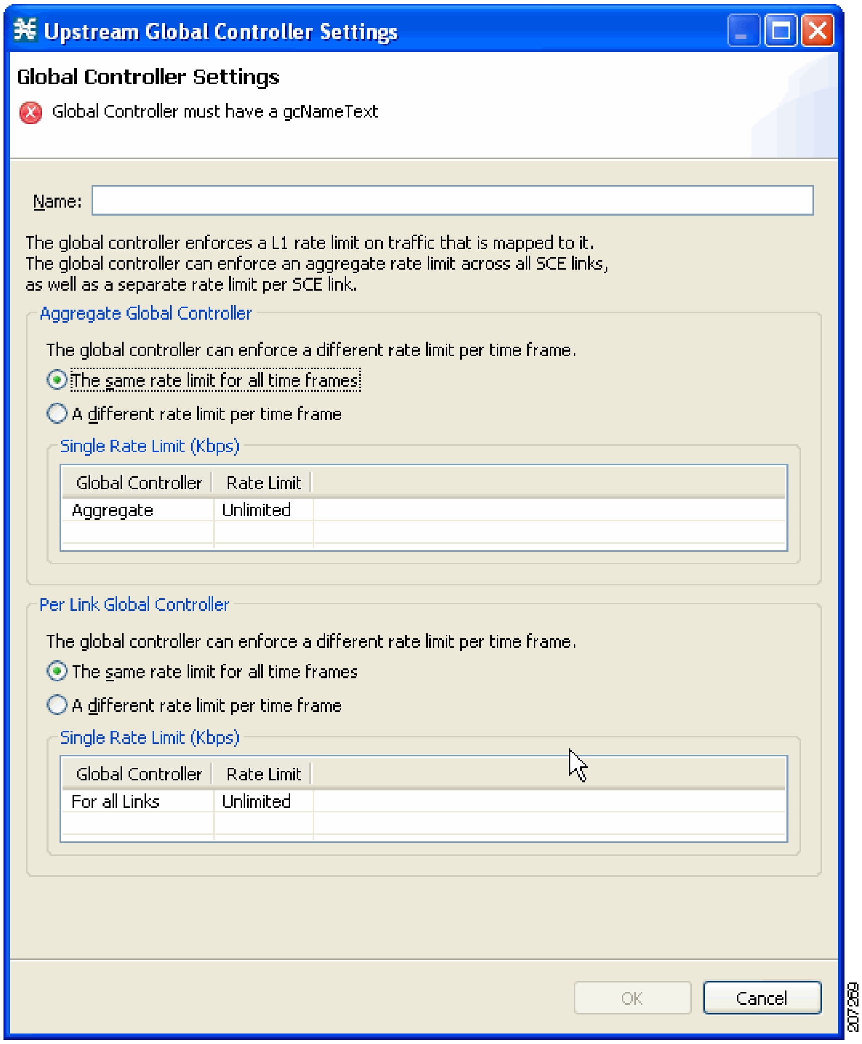
Step 3 Choose the **Add a new Global Controller** radio button, to add a new global controller.

Step 4 Click **Finish**.

The Global Controller Settings dialog box appears (Figure 9-8).

Note The display of Figure 9-8 depends on the global controller mode setting.

Figure 9-8 Upstream Global Controller Settings



Upstream Global Controller Settings

Global Controller Settings

Global Controller must have a gcNameText

Name:

The global controller enforces a L1 rate limit on traffic that is mapped to it.
The global controller can enforce an aggregate rate limit across all SCE links,
as well as a separate rate limit per SCE link.

Aggregate Global Controller

The global controller can enforce a different rate limit per time frame.

● The same rate limit for all time frames

○ A different rate limit per time frame

Single Rate Limit (Kbps)

Global Controller	Rate Limit
Aggregate	Unlimited

Per Link Global Controller

The global controller can enforce a different rate limit per time frame.

● The same rate limit for all time frames

○ A different rate limit per time frame

Single Rate Limit (Kbps)

Global Controller	Rate Limit
For all Links	Unlimited

Step 5 In the **Name** field enter a meaningful name.

Step 6 To edit the maximum bandwidth of the global controller, continue with the instructions in the section How to Set the Maximum Bandwidth of Global Controllers, page 9-9.

Step 7 Click **OK**.

Your changes are saved.

The Global Controller Settings dialog box closes.

How to Set the Maximum Bandwidth of Global Controllers

You can edit the maximum bandwidth that a global controller can carry.

You can set a different maximum bandwidth for each of the four available time frames.

You can set different values for each link and for the aggregated BW of all links.

Step 1 In the Policies tab, click **Global Policy**.

The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.

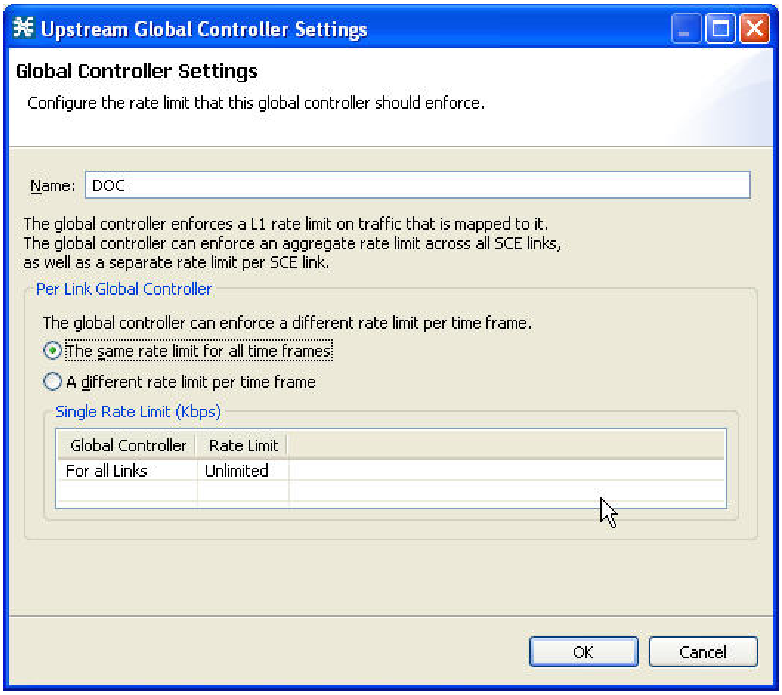
Step 2 Select a global controller.

Step 3 Click the Edit (✎) icon.

The Global Controller Settings dialog box appears (Figure 9-9).

Note The display of Figure 9-9 depends on the global controller mode setting.

Figure 9-9 Upstream Global Controller Settings



Upstream Global Controller Settings

Global Controller Settings

Configure the rate limit that this global controller should enforce.

Name: DOC

The global controller enforces a L1 rate limit on traffic that is mapped to it.
The global controller can enforce an aggregate rate limit across all SCE links,
as well as a separate rate limit per SCE link.

Per Link Global Controller

The global controller can enforce a different rate limit per time frame.

● The same rate limit for all time frames

○ A different rate limit per time frame

Single Rate Limit (Kbps)

Global Controller	Rate Limit
For all Links	Unlimited

Step 4 Set a single value for the maximum bandwidth limit that this global controller carries.

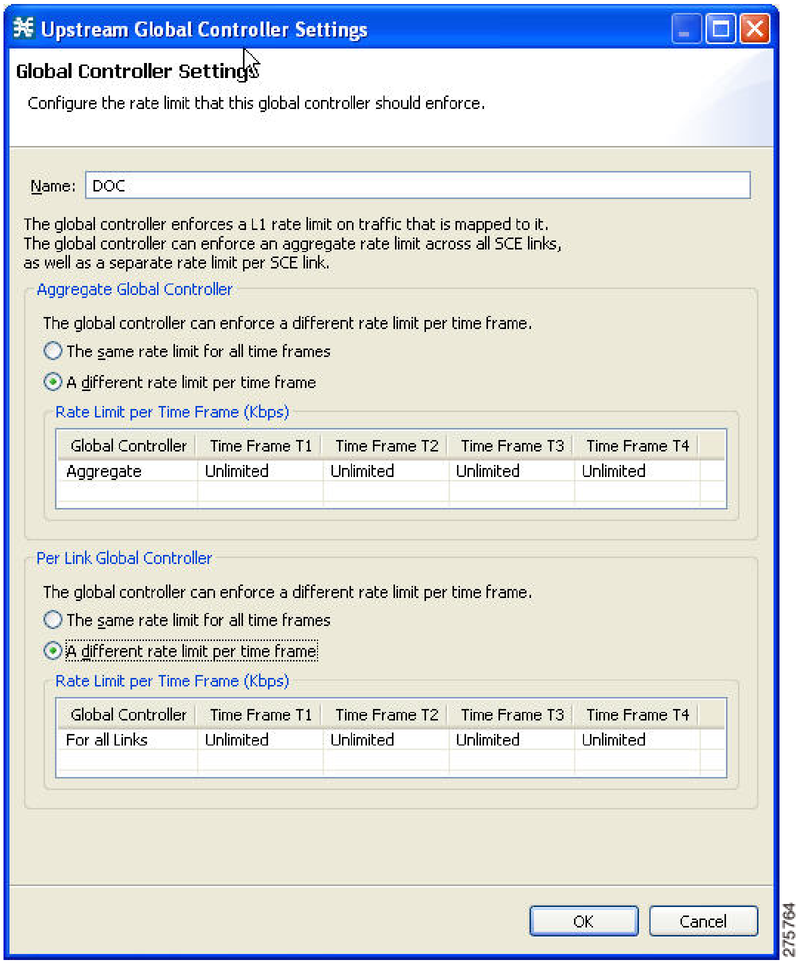
- Choose the **The same rate limit for all time frames** radio button, and in the Single Rate Limit (Kbps) field, enter the desired value in Kbps for the maximum bandwidth.

Step 5 Set the maximum limit that this global controller carries to vary according to time frame.

- Choose the **A different rate limit per time frame** radio button, and enter the desired value for each time frame (Figure 9-10).

Note The display of Figure 9-10 depends on the global controller mode setting.

Figure 9-10 Upstream Global Controller Settings



Upstream Global Controller Settings

Global Controller Settings

Configure the rate limit that this global controller should enforce.

Name: DOC

The global controller enforces a L1 rate limit on traffic that is mapped to it.
The global controller can enforce an aggregate rate limit across all SCE links,
as well as a separate rate limit per SCE link.

Aggregate Global Controller

The global controller can enforce a different rate limit per time frame.

○ The same rate limit for all time frames

● A different rate limit per time frame

Rate Limit per Time Frame (Kbps)

Global Controller	Time Frame T1	Time Frame T2	Time Frame T3	Time Frame T4
Aggregate	Unlimited	Unlimited	Unlimited	Unlimited

Per Link Global Controller

The global controller can enforce a different rate limit per time frame.

○ The same rate limit for all time frames

● A different rate limit per time frame

Rate Limit per Time Frame (Kbps)

Global Controller	Time Frame T1	Time Frame T2	Time Frame T3	Time Frame T4
For all Links	Unlimited	Unlimited	Unlimited	Unlimited

Note These values are applied to the time frames of the default calendar.

Step 6 Click **OK**.

Your changes are saved.

The value in the Policy Description column changes to reflect the new bandwidth limits.

Step 7 Repeat Step 2 through Step 6 for other global controllers.

How to Delete Global Controllers

You can delete unused global controllers at any time. The default global controller and the Total Link Limit cannot be deleted.

Step 1 In the Policies tab, click **Global Policy**.

The Global Bandwidth Settings dialog box appears.

Step 2 Select a global controller.

Step 3 Click the **Delete** (✖) icon.

Note If a subscriber BWC is using the specified global controller (see How to Edit Package Subscriber BWCs, page 9-30), a global controller cannot be removed message is displayed. The global controller cannot be deleted until you unassign it from all subscriber BWCs.

The global controller is deleted.

Step 4 Click **OK**.

Your changes are saved.

The Global Bandwidth Settings dialog box closes.

How to Define Global Controllers

This section describes how to define global controllers in both dual-link and multi-gigabit Ethernet systems.

In both systems, you can define each link separately with equal rates or you can define each link separately with different rates.

Alternatively, you can apply bandwidth limitations as an aggregate for all links or as an aggregate with individual control of each links.

You can:

1. Control each link separately with equal rate to all links.
2. Control each link separately without with different rate per link.
3. Control the links in aggregate and in addition maximum rate per-link, which is equal between all links.
4. Control the links in aggregate and in addition maximum rate per-link, which is different between the links.
5. Control the links in Virtual Link mode.

Note If Virtual Links mode is enabled, bandwidth limitations are applied to the sum of the all links.

Note Any attempt to change the global controller bandwidth for invalid link results in an error message during apply policy, similar to the following:

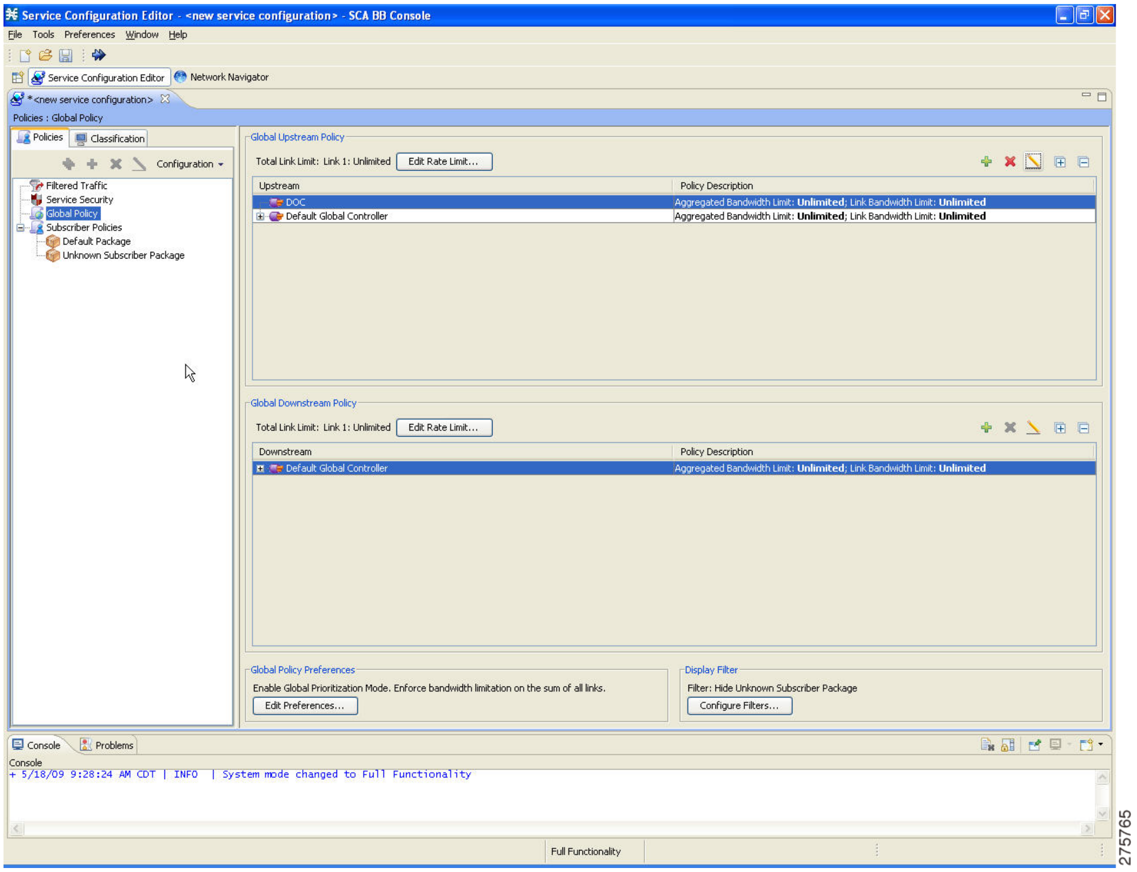
"Invalid value set on Link ID 6 for upstream GC 'Default Global Controller'. Link ID 6 does not exist. Available Link IDs: 1, 2, 3, 4"

To activate the respective edit dialog of the Global Controller settings (Figure 9-11):

- Double click on a global controller row in the global controller table view on the right main panel of the Global Policy setting.
- Click on the edit button that is located on the top right main panel of the Global Policy setting.

Note The behavior is the same whether you configure upstream or downstream GC.

Figure 9-11 Global Controller Settings Activation



Total Link Limit: Link 1: Unlimited

Upstream	Policy Description
DOC	Aggregated Bandwidth Limit: **Unlimited**; Link Bandwidth Limit: **Unlimited**
Default Global Controller	Aggregated Bandwidth Limit: **Unlimited**; Link Bandwidth Limit: **Unlimited**

Total Link Limit: Link 1: Unlimited

Downstream	Policy Description
Default Global Controller	Aggregated Bandwidth Limit: **Unlimited**; Link Bandwidth Limit: **Unlimited**

Enable Global Prioritization Mode. Enforce bandwidth limitation on the sum of all links.

Filter: Hide Unknown Subscriber Package

```
+ 5/18/09 9:28:24 AM CDT | INFO  | System mode changed to Full Functionality
```

Refer to the following sections for configuration details:

- How to Set Global Controller Bandwidth Limits with Equal Rate for All Links, page 9-13
- How to Set Global Controller Bandwidth Limits Separately with a Different Rate Per Link, page 9-15
- How to Set Global Controller Bandwidth Limits as the Sum of All Links with an Equal Rate Per Link, page 9-18
- How to Set Global Controller Bandwidth Limits as the Sum of All Links with a Different Rate Per Link, page 9-21
- How to Set Global Controller Bandwidth for Virtual Links, page 9-24

How to Set Global Controller Bandwidth Limits with Equal Rate for All Links

Use the following procedure to configure the global controller with equal rate for all links.

Step 1 In the Policies tab, click **Global Policy**.

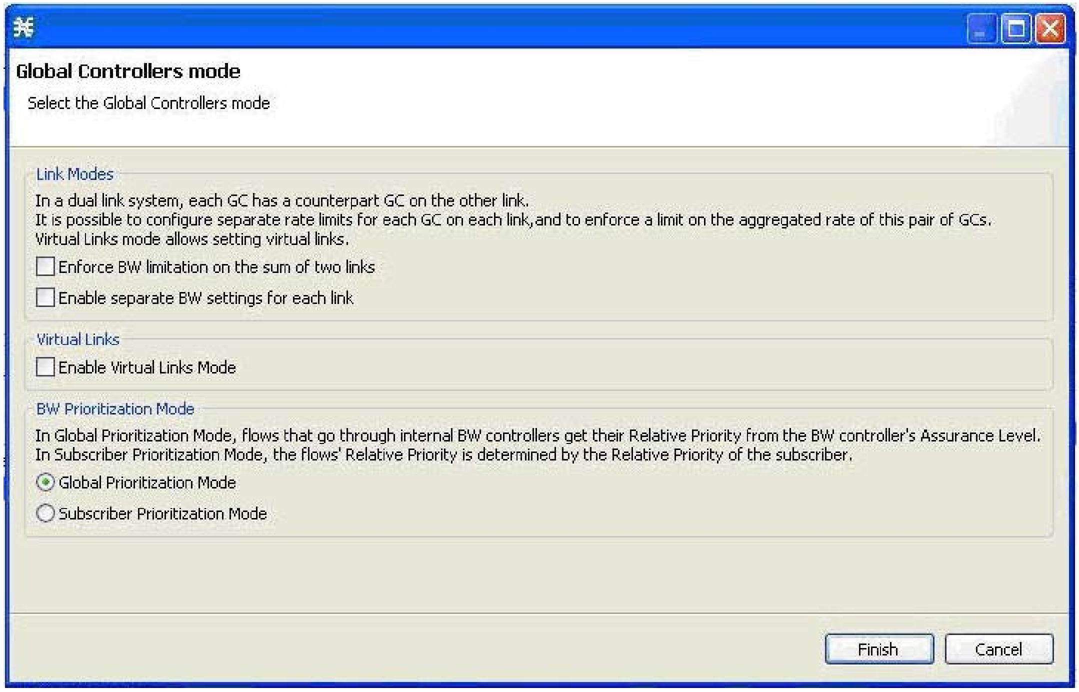
The Global Bandwidth Settings dialog box in the right (Rule) pane.

Step 2 Add global controllers, as described in How to Add Global Controllers, page 9-7.

Step 3 Click **Edit Preferences**.

The Global Controllers mode dialog box appears (Figure 9-12).

Figure 9-12 Global Controllers Mode



Global Controllers mode

Select the Global Controllers mode

Link Modes

In a dual link system, each GC has a counterpart GC on the other link.
It is possible to configure separate rate limits for each GC on each link,and to enforce a limit on the aggregated rate of this pair of GCs.
Virtual Links mode allows setting virtual links.

□ Enforce BW limitation on the sum of two links

□ Enable separate BW settings for each link

Virtual Links

□ Enable Virtual Links Mode

BW Prioritization Mode

In Global Prioritization Mode, flows that go through internal BW controllers get their Relative Priority from the BW controller's Assurance Level.
In Subscriber Prioritization Mode, the flows' Relative Priority is determined by the Relative Priority of the subscriber.

● Global Prioritization Mode

○ Subscriber Prioritization Mode

Step 4 Verify that the Link Modes check boxes are unchecked.

Step 5 Click **Finish**.

The Global Controllers mode dialog box closes.

Step 6 In the Policies tab, click **Global Policy**.

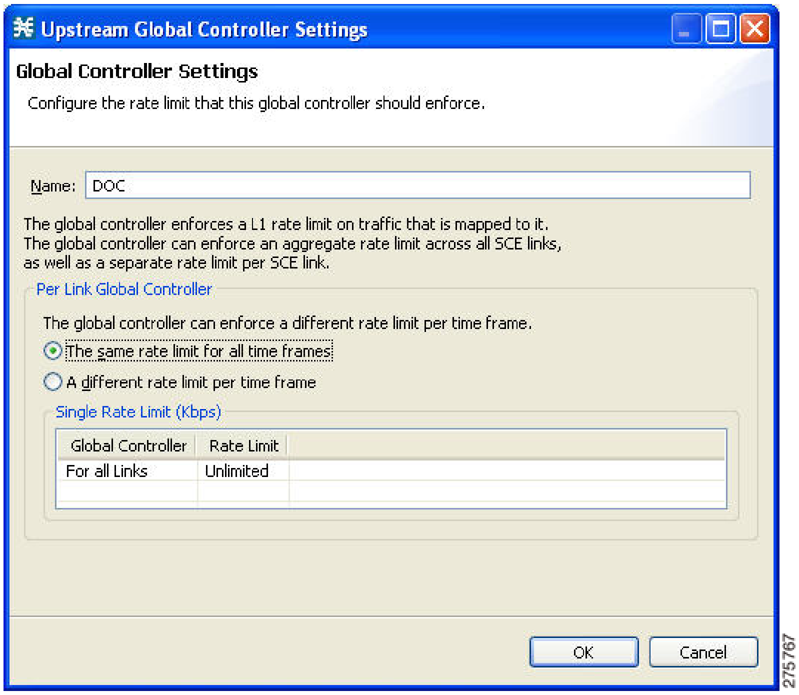
The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.

Step 7 Select a global controller.

Step 8 Click the Edit (✎) icon.

The Global Controller Settings dialog box appears (Figure 9-13).

Figure 9-13 Upstream Global Controller Settings



Global Controller Settings

Configure the rate limit that this global controller should enforce.

Name: DOC

The global controller enforces a L1 rate limit on traffic that is mapped to it.
The global controller can enforce an aggregate rate limit across all SCE links,
as well as a separate rate limit per SCE link.

Per Link Global Controller

The global controller can enforce a different rate limit per time frame.

● The same rate limit for all time frames

○ A different rate limit per time frame

Single Rate Limit (Kbps)

Global Controller	Rate Limit
For all Links	Unlimited

Note If the rate limit for all time frames is to be the same, use Step 9. If the rate limit for all time frames is to vary by time frame, use Step 10.

Step 9 Set a single value for the maximum bandwidth limit that this global controller carries.

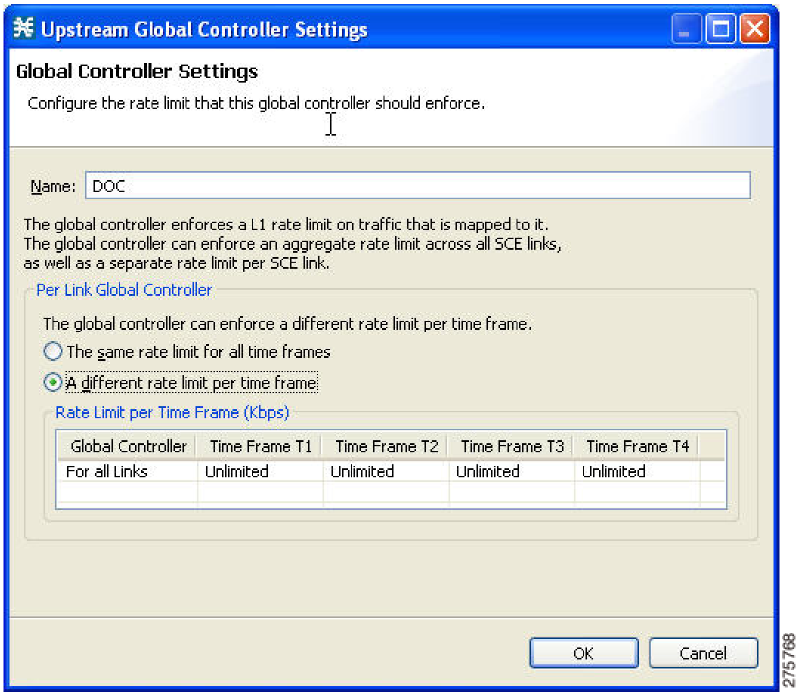
- **a.** Choose the **The same rate limit for all time frames** radio button.
- **b.** Enter the desired value in Kbps for the maximum bandwidth in the Rate limit for the Per Link Global Controller (in Kbps) field.

Step 10 Set the maximum limit that this global controller carries to vary according to time frame.

a. Choose the **A different rate limit per time frame** radio button.

b. Enter the desired value for each time frame (Figure 9-14).

Figure 9-14 Upstream Global Controller Settings



Upstream Global Controller Settings

Global Controller Settings

Configure the rate limit that this global controller should enforce.

Name: DOC

The global controller enforces a L1 rate limit on traffic that is mapped to it.
The global controller can enforce an aggregate rate limit across all SCE links,
as well as a separate rate limit per SCE link.

Per Link Global Controller

The global controller can enforce a different rate limit per time frame.

○ The same rate limit for all time frames

● A different rate limit per time frame

Rate Limit per Time Frame (Kbps)

Global Controller	Time Frame T1	Time Frame T2	Time Frame T3	Time Frame T4
For all Links	Unlimited	Unlimited	Unlimited	Unlimited

Step 11 Click **OK**.

Your changes are saved.

How to Set Global Controller Bandwidth Limits Separately with a Different Rate Per Link

Use the following procedure to configure the global controller with a different rate per link.

Step 1 In the Policies tab, click **Global Policy**.

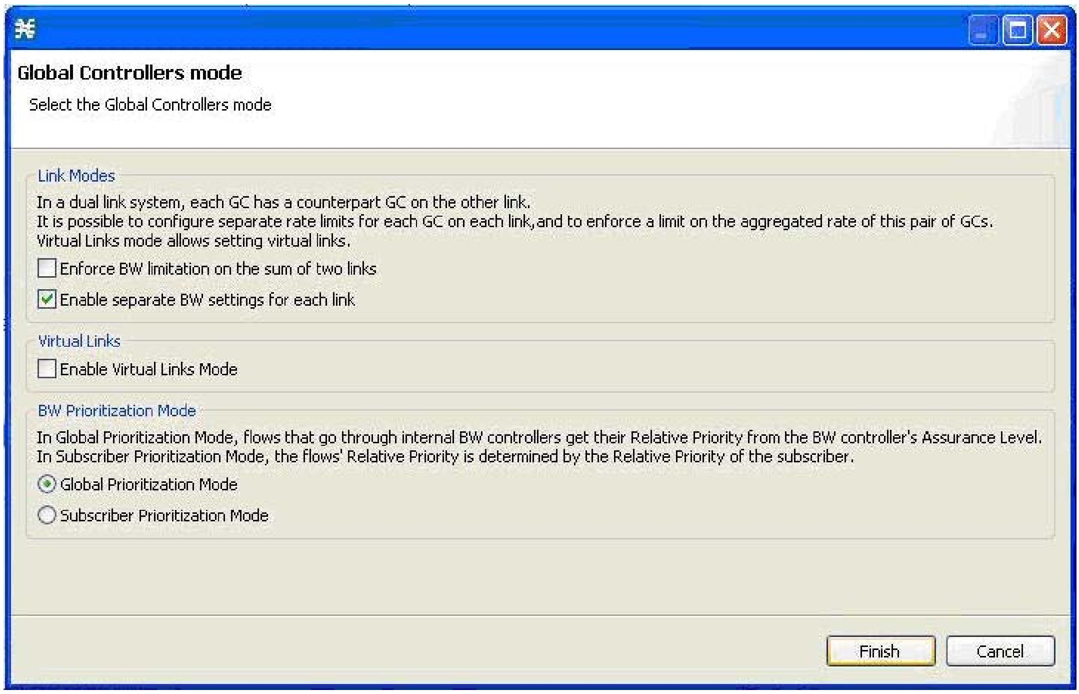
The Global Bandwidth Settings dialog box in the right (Rule) pane.

Step 2 Add global controllers, as described in How to Add Global Controllers, page 9-7.

Step 3 Click **Edit Preferences**.

The Global Controllers mode dialog box appears (Figure 9-15).

Figure 9-15 Global Controller Mode



Global Controllers mode

Select the Global Controllers mode

Link Modes

In a dual link system, each GC has a counterpart GC on the other link.
It is possible to configure separate rate limits for each GC on each link,and to enforce a limit on the aggregated rate of this pair of GCs.
Virtual Links mode allows setting virtual links.

□ Enforce BW limitation on the sum of two links

☑ Enable separate BW settings for each link

Virtual Links

□ Enable Virtual Links Mode

BW Prioritization Mode

In Global Prioritization Mode, flows that go through internal BW controllers get their Relative Priority from the BW controller's Assurance Level.
In Subscriber Prioritization Mode, the flows' Relative Priority is determined by the Relative Priority of the subscriber.

● Global Prioritization Mode

○ Subscriber Prioritization Mode

Step 4 Check the **Enable separate BW setting for each link** check box.

Step 5 Click **Finish**.

The Global Controllers mode dialog box closes.

Step 6 In the Policies tab, click **Global Policy**.

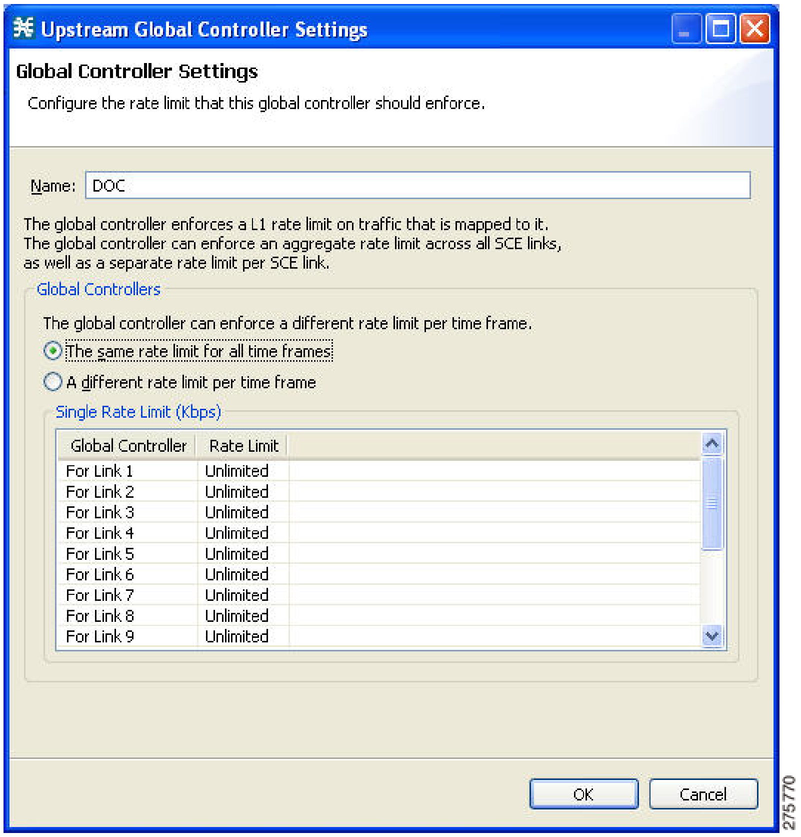
The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.

Step 7 Select a global controller.

Step 8 Click the Edit (✎) icon.

The Global Controller Settings dialog box appears (Figure 9-16).

Figure 9-16 Downstream Global Controller Settings



Upstream Global Controller Settings

Global Controller Settings

Configure the rate limit that this global controller should enforce.

Name: DOC

The global controller enforces a L1 rate limit on traffic that is mapped to it.
The global controller can enforce an aggregate rate limit across all SCE links,
as well as a separate rate limit per SCE link.

Global Controllers

The global controller can enforce a different rate limit per time frame.

● The same rate limit for all time frames

○ A different rate limit per time frame

Single Rate Limit (Kbps)

Global Controller	Rate Limit
For Link 1	Unlimited
For Link 2	Unlimited
For Link 3	Unlimited
For Link 4	Unlimited
For Link 5	Unlimited
For Link 6	Unlimited
For Link 7	Unlimited
For Link 8	Unlimited
For Link 9	Unlimited

Note If the rate limit for all time frames is to be the same, use Step 9. If the rate limit for all time frames is to vary by time frame, use Step 10.

Step 9 Set a single value for the maximum bandwidth limit that this global controller carries for each link.

a. Choose the **The same rate limit for all time frames** radio button.

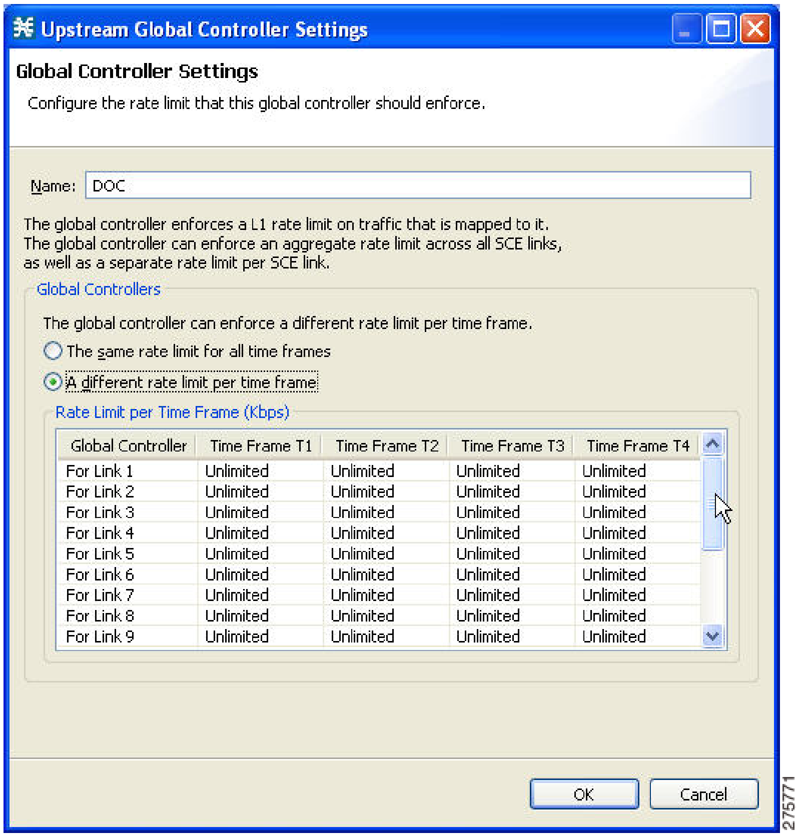
b. Enter the desired value in Kbps for the maximum bandwidth in the Rate limit for the Per Link Global Controller (in Kbps) field.

Step 10 Set the maximum limit that this global controller carries to vary according to time frame for each link.

a. Choose the **A different rate limit per time frame** radio button.

b. Enter the desired value for each time frame (Figure 9-17).

Figure 9-17 Upstream Global Controller Settings



Upstream Global Controller Settings

Global Controller Settings

Configure the rate limit that this global controller should enforce.

Name: DOC

The global controller enforces a L1 rate limit on traffic that is mapped to it.
The global controller can enforce an aggregate rate limit across all SCE links,
as well as a separate rate limit per SCE link.

Global Controllers

The global controller can enforce a different rate limit per time frame.

○ The same rate limit for all time frames

● A different rate limit per time frame

Rate Limit per Time Frame (Kbps)

Global Controller	Time Frame T1	Time Frame T2	Time Frame T3	Time Frame T4
For Link 1	Unlimited	Unlimited	Unlimited	Unlimited
For Link 2	Unlimited	Unlimited	Unlimited	Unlimited
For Link 3	Unlimited	Unlimited	Unlimited	Unlimited
For Link 4	Unlimited	Unlimited	Unlimited	Unlimited
For Link 5	Unlimited	Unlimited	Unlimited	Unlimited
For Link 6	Unlimited	Unlimited	Unlimited	Unlimited
For Link 7	Unlimited	Unlimited	Unlimited	Unlimited
For Link 8	Unlimited	Unlimited	Unlimited	Unlimited
For Link 9	Unlimited	Unlimited	Unlimited	Unlimited

Step 11 Click **OK**.

Your changes are saved.

How to Set Global Controller Bandwidth Limits as the Sum of All Links with an Equal Rate Per Link

In this link control mode, the maximum bandwidth limitation is configured as sum of all links. When you create a GC in this mode, you can configure the aggregate global controller of the link and configure the maximum rate per link. In this mode, you can enforce bandwidth limitation on the sum of all links and control the links in aggregate and in addition maximum per-link which is equal between all links.

Use the following procedure to configure global controller as the sum of all links with an equal rate per link.

Step 1 In the Policies tab, click **Global Policy**.

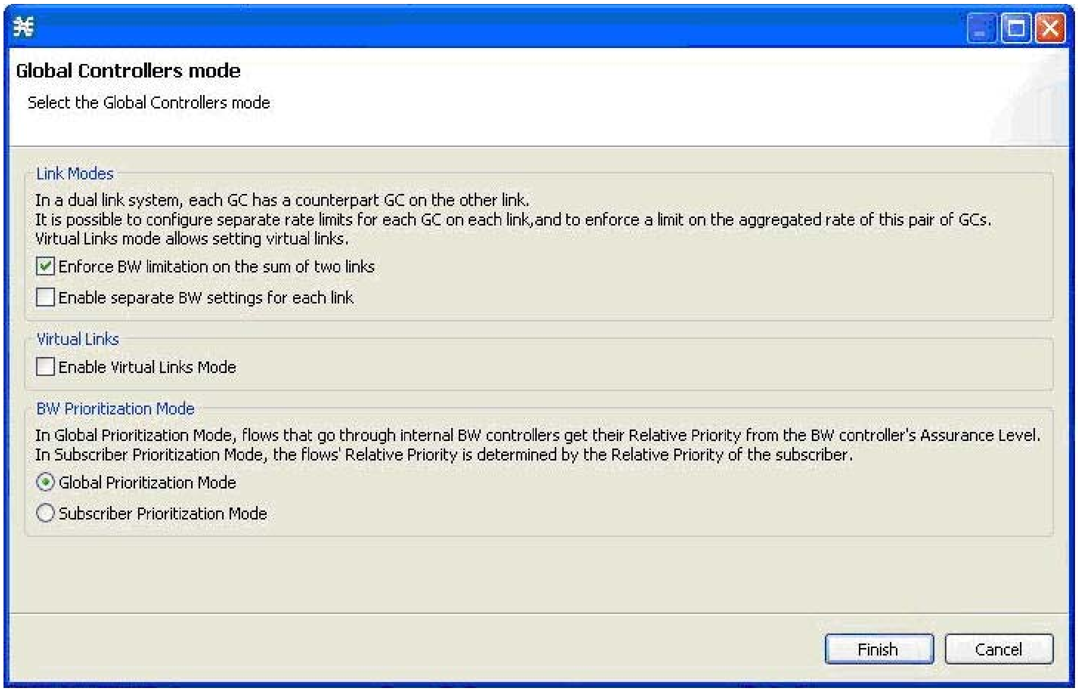
The Global Bandwidth Settings dialog box in the right (Rule) pane.

Step 2 Add global controllers, as described in How to Add Global Controllers, page 9-7.

Step 3 Click **Edit Preferences**.

The Global Controllers mode dialog box appears (Figure 9-18).

Figure 9-18 Global Controllers Mode



Global Controllers mode

Select the Global Controllers mode

Link Modes

In a dual link system, each GC has a counterpart GC on the other link.
It is possible to configure separate rate limits for each GC on each link,and to enforce a limit on the aggregated rate of this pair of GCs.
Virtual Links mode allows setting virtual links.

☑ Enforce BW limitation on the sum of two links

☐ Enable separate BW settings for each link

Virtual Links

☐ Enable Virtual Links Mode

BW Prioritization Mode

In Global Prioritization Mode, flows that go through internal BW controllers get their Relative Priority from the BW controller's Assurance Level.
In Subscriber Prioritization Mode, the flows' Relative Priority is determined by the Relative Priority of the subscriber.

● Global Prioritization Mode

○ Subscriber Prioritization Mode

Step 4 Check the **Enforce BW limitation on the sum of the links** check box.

Step 5 Click **Finish**.

The Global Controllers mode dialog box closes.

Step 6 In the Policies tab, click **Global Policy**.

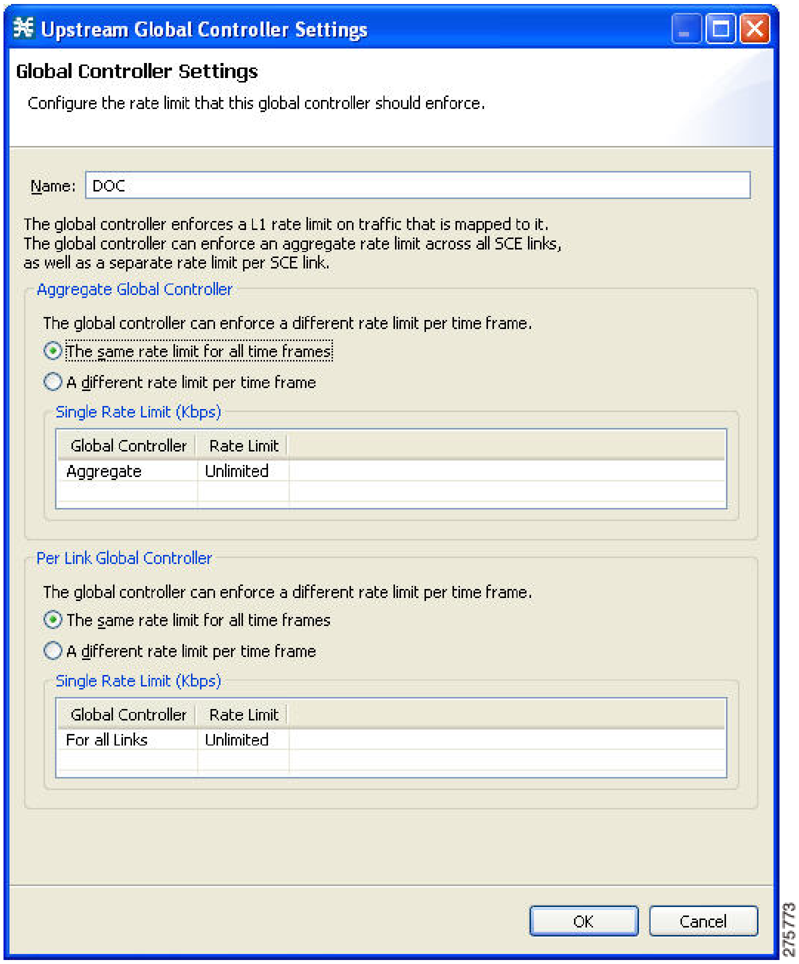
The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.

Step 7 Select a global controller.

Step 8 Click the Edit (✎) icon.

The Global Controller Settings dialog box appears (Figure 9-19).

Figure 9-19 Upstream Global Controller Settings



Upstream Global Controller Settings

Global Controller Settings

Configure the rate limit that this global controller should enforce.

Name: DOC

The global controller enforces a L1 rate limit on traffic that is mapped to it.
The global controller can enforce an aggregate rate limit across all SCE links,
as well as a separate rate limit per SCE link.

Aggregate Global Controller

The global controller can enforce a different rate limit per time frame.

● The same rate limit for all time frames

○ A different rate limit per time frame

Single Rate Limit (Kbps)

Global Controller	Rate Limit
Aggregate	Unlimited

Per Link Global Controller

The global controller can enforce a different rate limit per time frame.

● The same rate limit for all time frames

○ A different rate limit per time frame

Single Rate Limit (Kbps)

Global Controller	Rate Limit
For all Links	Unlimited

OK Cancel

Note If the rate limit for all time frames is to be the same, use Step 9. If the rate limit for all time frames is to vary by time frame, use Step 10.

Step 9 Set a single value for the maximum bandwidth limit that this global controller carries.

a. Choose the **The same rate limit for all time frames** radio button on the Aggregate Global Controller tab.

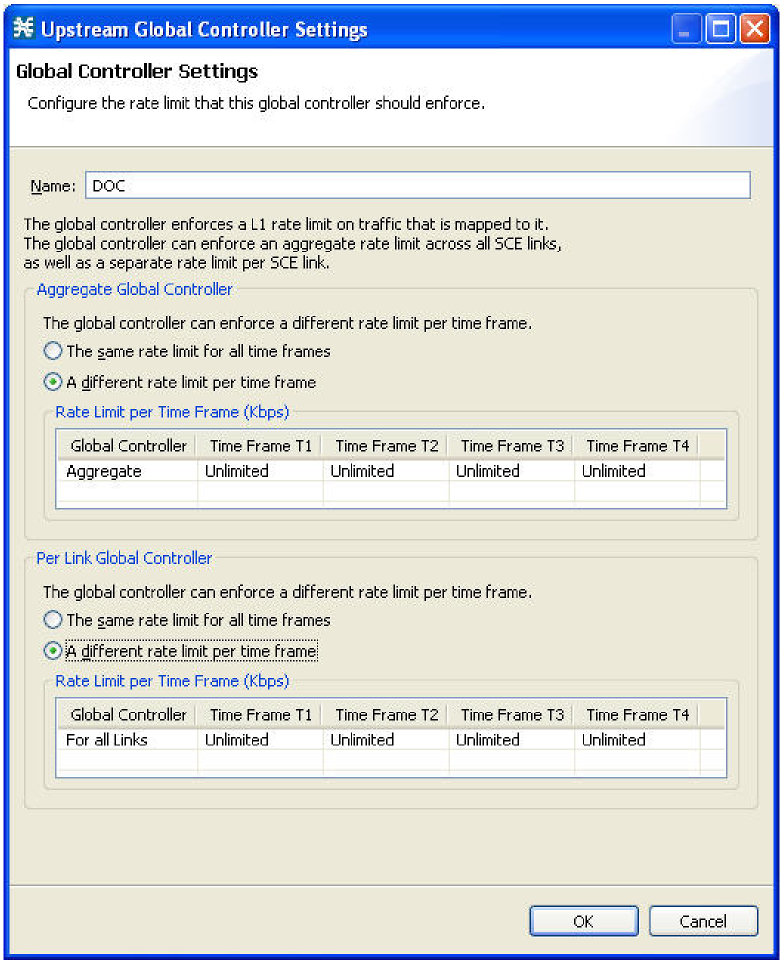
b. Enter the desired value in Kbps for the maximum bandwidth in the Rate limit for the Per Link Global Controller (in Kbps) field.

Step 10 Set the maximum limit that this global controller carries to vary according to time frame.

a. Choose the **A different rate limit per time frame** radio button the Aggregate Global Controller tab.

b. Enter the desired value for each time frame (Figure 9-20).

Figure 9-20 Upstream Global Controller Settings



Upstream Global Controller Settings

Global Controller Settings

Configure the rate limit that this global controller should enforce.

Name: DOC

The global controller enforces a L1 rate limit on traffic that is mapped to it.
The global controller can enforce an aggregate rate limit across all SCE links,
as well as a separate rate limit per SCE link.

Aggregate Global Controller

The global controller can enforce a different rate limit per time frame.

○ The same rate limit for all time frames

● A different rate limit per time frame

Rate Limit per Time Frame (Kbps)

Global Controller	Time Frame T1	Time Frame T2	Time Frame T3	Time Frame T4
Aggregate	Unlimited	Unlimited	Unlimited	Unlimited

Per Link Global Controller

The global controller can enforce a different rate limit per time frame.

○ The same rate limit for all time frames

● A different rate limit per time frame

Rate Limit per Time Frame (Kbps)

Global Controller	Time Frame T1	Time Frame T2	Time Frame T3	Time Frame T4
For all Links	Unlimited	Unlimited	Unlimited	Unlimited

Step 11 Click **OK**.

Your changes are saved.

How to Set Global Controller Bandwidth Limits as the Sum of All Links with a Different Rate Per Link

In this link control mode, the maximum bandwidth is the sum of links but bandwidth settings can be configured for each link up the maximum bandwidth for all links. When you create a GC in this mode you can configure the aggregate global controller of the link and in addition specify a bandwidth limitation per link. This mode is used when the SCE serves multiple edge devices and you want to enforce two rules: One aggregate rule on all the links together and one rule per specific link. In this mode, you can enforce bandwidth limitation on the sum of all links and enable separate bandwidth settings for each link. You can control the links in aggregate and set maximum rate per-link which is different between the links.

Use the following procedure to configure global controller as the sum of all links with a different rate per link.

Step 1 In the Policies tab, click **Global Policy**.

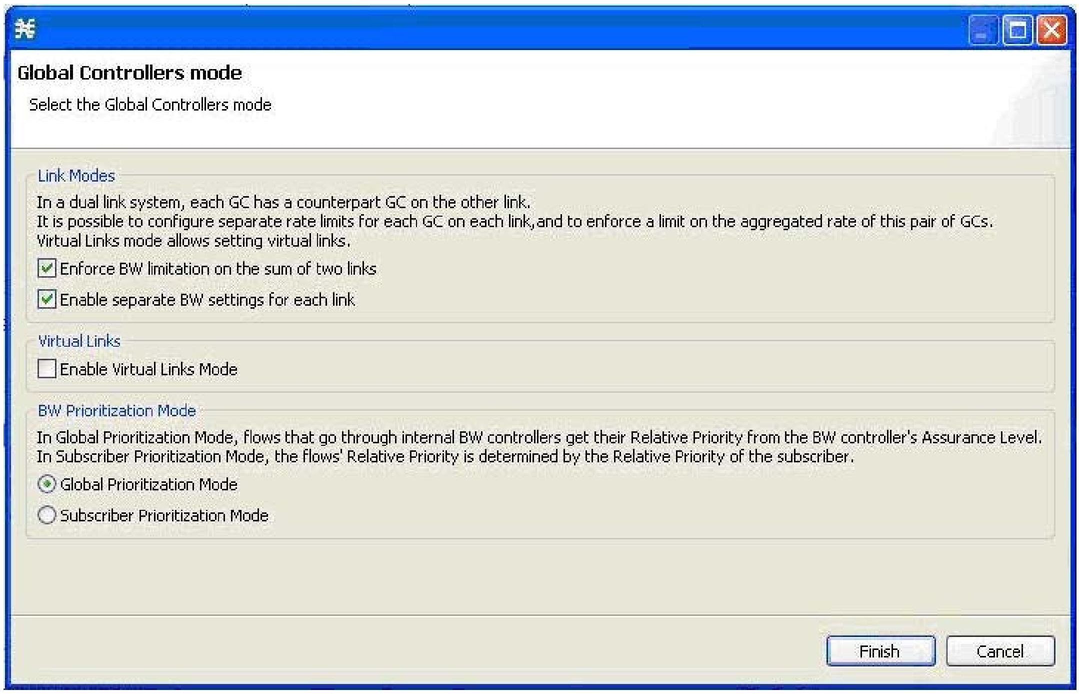
The Global Bandwidth Settings dialog box in the right (Rule) pane.

Step 2 Add global controllers, as described in How to Add Global Controllers, page 9-7.

Step 3 Click **Edit Preferences**.

The Global Controllers mode dialog box appears (Figure 9-21).

Figure 9-21 Global Controllers Mode



Global Controllers mode

Select the Global Controllers mode

Link Modes

In a dual link system, each GC has a counterpart GC on the other link.
It is possible to configure separate rate limits for each GC on each link,and to enforce a limit on the aggregated rate of this pair of GCs.
Virtual Links mode allows setting virtual links.

☑ Enforce BW limitation on the sum of two links

☑ Enable separate BW settings for each link

Virtual Links

□ Enable Virtual Links Mode

BW Prioritization Mode

In Global Prioritization Mode, flows that go through internal BW controllers get their Relative Priority from the BW controller's Assurance Level.
In Subscriber Prioritization Mode, the flows' Relative Priority is determined by the Relative Priority of the subscriber.

● Global Prioritization Mode

○ Subscriber Prioritization Mode

Step 4 Check the **Enforce BW limitation on the sum of the links and Enable separate BW setting for each link** check boxes.

Step 5 Click **Finish**.

The Global Controllers mode dialog box closes.

Step 6 In the Policies tab, click **Global Policy**.

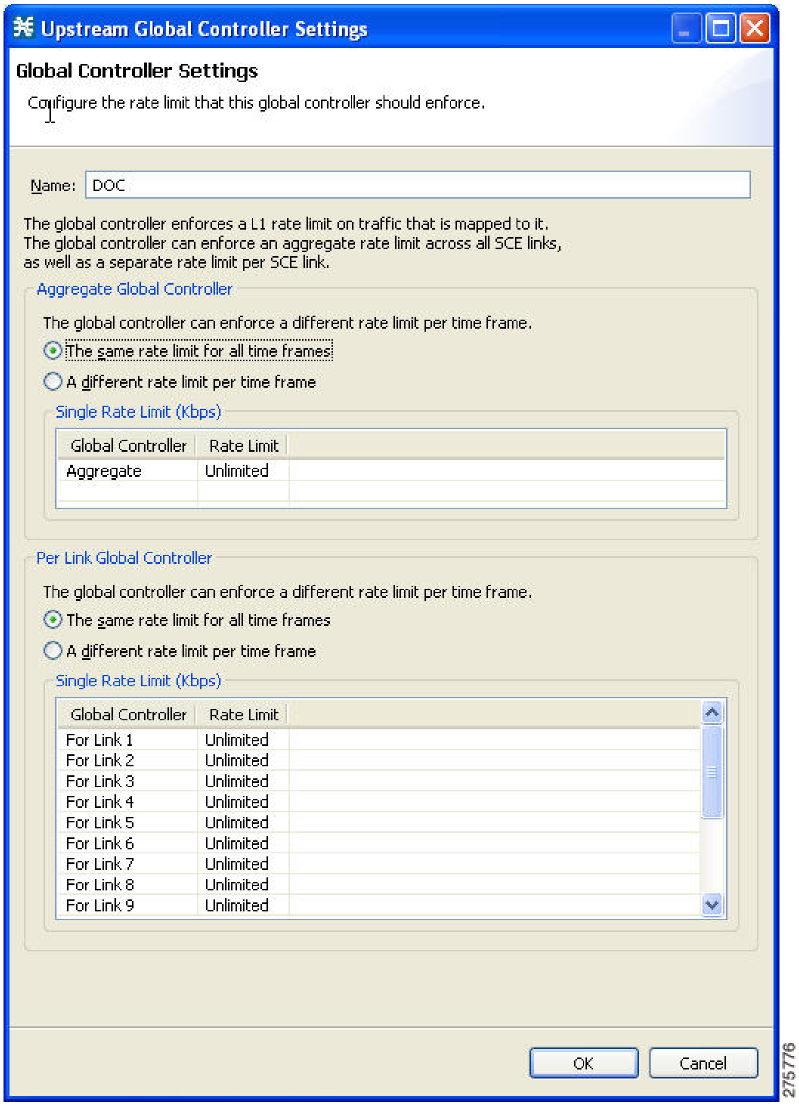
The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.

Step 7 Select a global controller.

Step 8 Click the Edit (✎) icon.

The Global Controller Settings dialog box appears (Figure 9-22).

Figure 9-22 Upstream Global Controller Settings



Upstream Global Controller Settings

Global Controller Settings

Configure the rate limit that this global controller should enforce.

Name: DOC

The global controller enforces a L1 rate limit on traffic that is mapped to it.
The global controller can enforce an aggregate rate limit across all SCE links,
as well as a separate rate limit per SCE link.

Aggregate Global Controller

The global controller can enforce a different rate limit per time frame.

● The same rate limit for all time frames

○ A different rate limit per time frame

Single Rate Limit (Kbps)

Global Controller	Rate Limit
Aggregate	Unlimited

Per Link Global Controller

The global controller can enforce a different rate limit per time frame.

● The same rate limit for all time frames

○ A different rate limit per time frame

Single Rate Limit (Kbps)

Global Controller	Rate Limit
For Link 1	Unlimited
For Link 2	Unlimited
For Link 3	Unlimited
For Link 4	Unlimited
For Link 5	Unlimited
For Link 6	Unlimited
For Link 7	Unlimited
For Link 8	Unlimited
For Link 9	Unlimited

Note If the rate limit for all time frames is to be the same, use Step 9. If the rate limit for all time frames is to vary by time frame, use Step 10.

Step 9 Set a single value for the maximum bandwidth limit that this global controller carries.

a. Choose the **The same rate limit for all time frames** radio button on the Per Link Global Controller tab.

b. Enter the desired value in Kbps for the maximum bandwidth in the Rate limit for the Link 1 (in Kbps) field.

c. Repeat Step 9b for each link.

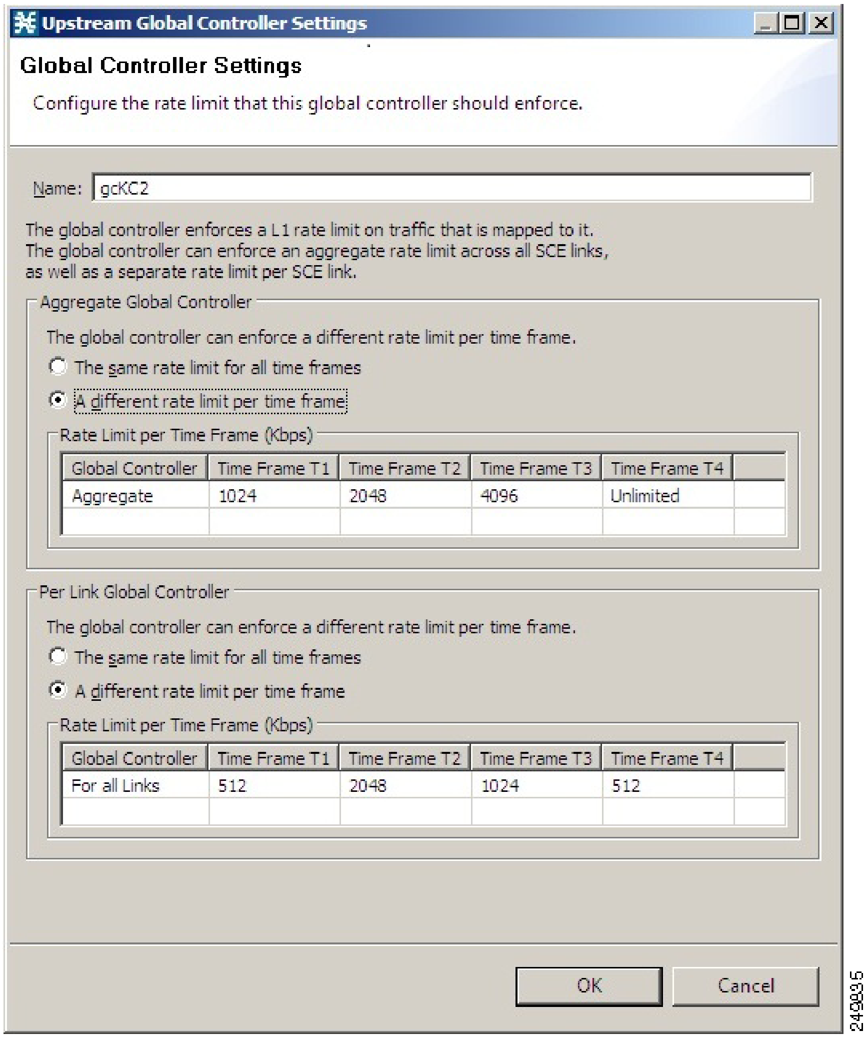
Step 10 Set the maximum limit that this global controller carries to vary according to time frame.

a. Choose the **A different rate limit per time frame** radio button the Per Link Global Controller tab.

b. Enter the desired value for each time frame.

c. Repeat Step 10b for each link (Figure 9-23).

Figure 9-23 Downstream Global Controller Settings



Upstream Global Controller Settings

Global Controller Settings

Configure the rate limit that this global controller should enforce.

Name: gcKC2

The global controller enforces a L1 rate limit on traffic that is mapped to it.
The global controller can enforce an aggregate rate limit across all SCE links,
as well as a separate rate limit per SCE link.

Aggregate Global Controller

The global controller can enforce a different rate limit per time frame.

○ The same rate limit for all time frames

● A different rate limit per time frame

Rate Limit per Time Frame (Kbps)

Global Controller	Time Frame T1	Time Frame T2	Time Frame T3	Time Frame T4
Aggregate	1024	2048	4096	Unlimited

Per Link Global Controller

The global controller can enforce a different rate limit per time frame.

○ The same rate limit for all time frames

● A different rate limit per time frame

Rate Limit per Time Frame (Kbps)

Global Controller	Time Frame T1	Time Frame T2	Time Frame T3	Time Frame T4
For all Links	512	2048	1024	512

Step 11 Click **OK**.

Your changes are saved.

How to Set Global Controller Bandwidth for Virtual Links

In this mode, you can control each link separately using configured rate templates and default rates. The template rate limits are applied to newly created virtual links. The default rate limits are applied to the default virtual link (virtual link 0).

Use the following procedure to configure Global Controller for Virtual links.

Step 1 In the Policies tab, click **Global Policy**.

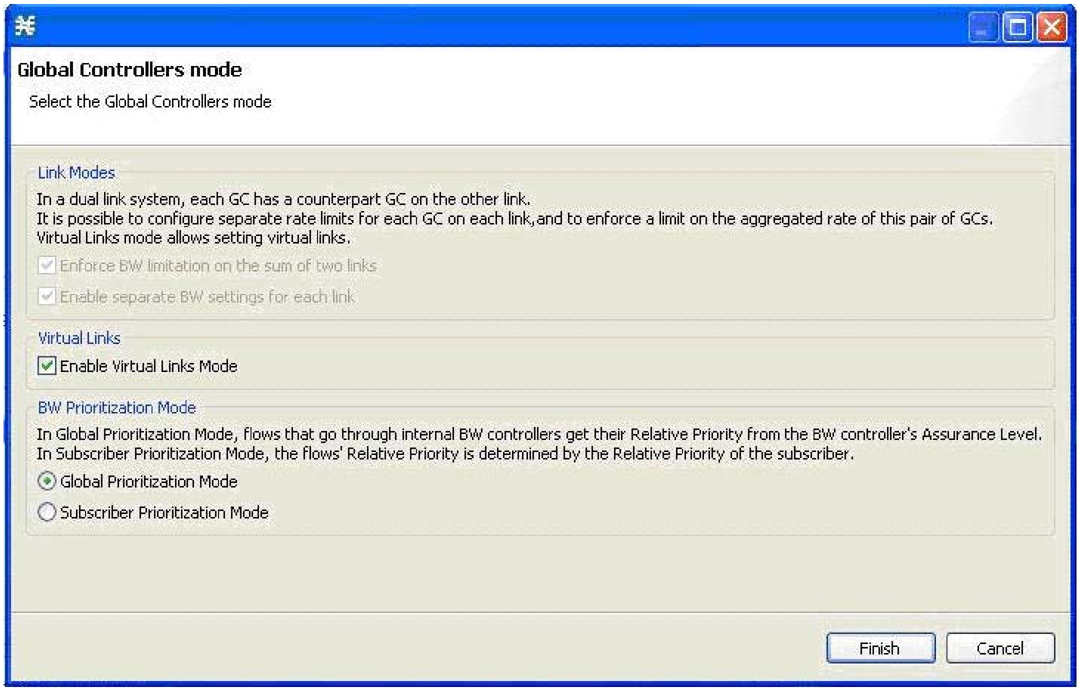
The Global Bandwidth Settings dialog box in the right (Rule) pane.

Step 2 Add global controllers, as described in How to Add Global Controllers, page 9-7.

Step 3 Click **Edit Preferences**.

The Global Controllers mode dialog box appears (Figure 9-24).

Figure 9-24 Global Controllers Mode



Global Controllers mode

Select the Global Controllers mode

Link Modes

In a dual link system, each GC has a counterpart GC on the other link.
It is possible to configure separate rate limits for each GC on each link,and to enforce a limit on the aggregated rate of this pair of GCs.
Virtual Links mode allows setting virtual links.

☑ Enforce BW limitation on the sum of two links

☑ Enable separate BW settings for each link

Virtual Links

☑ Enable Virtual Links Mode

BW Prioritization Mode

In Global Prioritization Mode, flows that go through internal BW controllers get their Relative Priority from the BW controller's Assurance Level.
In Subscriber Prioritization Mode, the flows' Relative Priority is determined by the Relative Priority of the subscriber.

● Global Prioritization Mode

○ Subscriber Prioritization Mode

Step 4 Check the **Enable Virtual Links Mode** check box.

Step 5 Click **Finish**.

The Global Controllers mode dialog box closes.

Note By default, the Virtual Link Mode works only in Subscriber Prioritization Mode.

Step 6 In the Policies tab, click **Global Policy**.

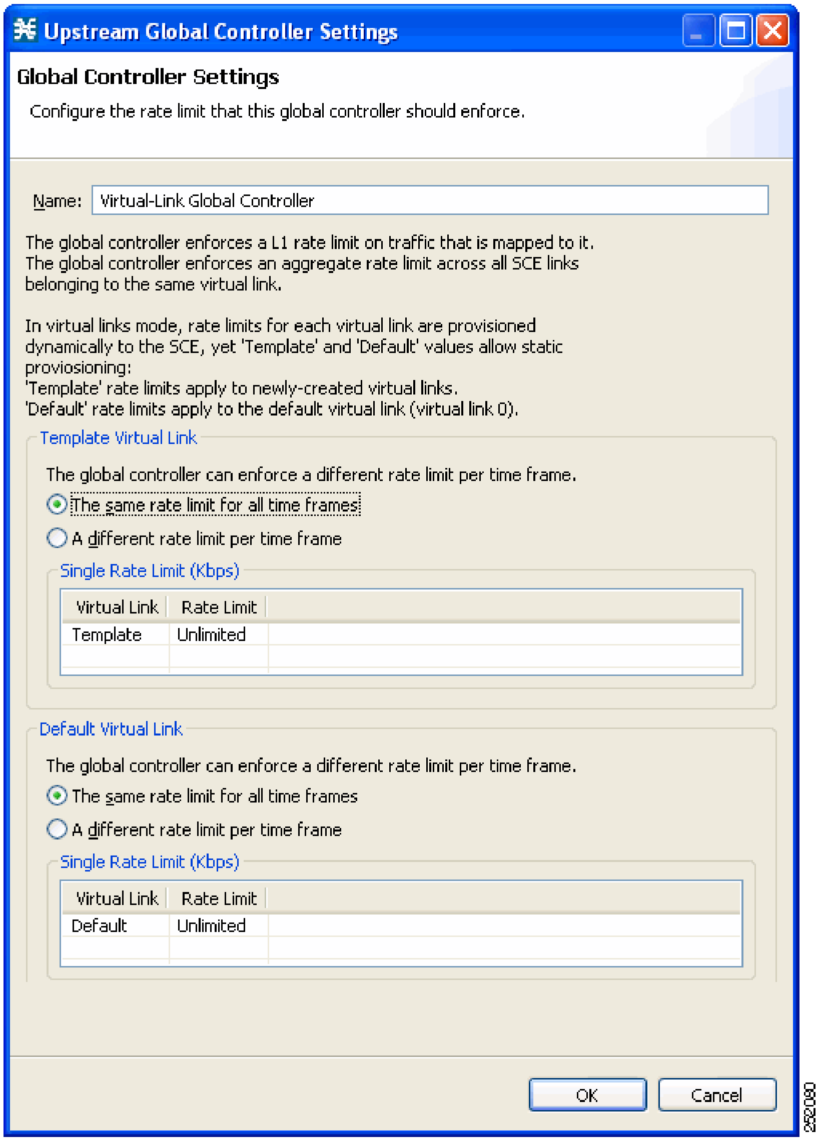
The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.

Step 7 Select a global controller.

Step 8 Click (**Edit**).

The Global Controller Settings dialog box appears (Figure 9-25).

Figure 9-25 Upstream Global Controller Settings



Upstream Global Controller Settings

Global Controller Settings

Configure the rate limit that this global controller should enforce.

Name: Virtual-Link Global Controller

The global controller enforces a L1 rate limit on traffic that is mapped to it.
The global controller enforces an aggregate rate limit across all SCE links
belonging to the same virtual link.

In virtual links mode, rate limits for each virtual link are provisioned
dynamically to the SCE, yet 'Template' and 'Default' values allow static
proviosioning:
'Template' rate limits apply to newly-created virtual links.
'Default' rate limits apply to the default virtual link (virtual link 0).

Template Virtual Link

The global controller can enforce a different rate limit per time frame.

● The same rate limit for all time frames

○ A different rate limit per time frame

Single Rate Limit (Kbps)

Virtual Link	Rate Limit
Template	Unlimited

Default Virtual Link

The global controller can enforce a different rate limit per time frame.

● The same rate limit for all time frames

○ A different rate limit per time frame

Single Rate Limit (Kbps)

Virtual Link	Rate Limit
Default	Unlimited

Note If the rate limit for all time frames is to be the same for the Template Virtual Link, use Step 9. If the rate limit for all time frames is to vary by time frame for the Template Virtual Link, use Step 10.

Step 9 Set a single value for the maximum bandwidth limit that this global controller carries.

- **a.** Choose the **The same rate limit for all time frames** radio button on the Template Virtual Link tab.
- **b.** Enter the desired value in Kbps for the maximum bandwidth in the Rate limit for the Link 1 (in Kbps) field.

Step 10 Set the maximum limit that this global controller carries to vary according to time frame.

a. Choose the **A different rate limit per time frame** radio button the Template Virtual Link tab.

b. Enter the desired value for each time frame.

Note If the rate limit for all time frames is to be the same for the Default Virtual Link, use Step 11. If the rate limit for all time frames is to vary by time frame for the Default Virtual Link, use Step 12.

Step 11 Set a single value for the maximum bandwidth limit that this global controller carries.

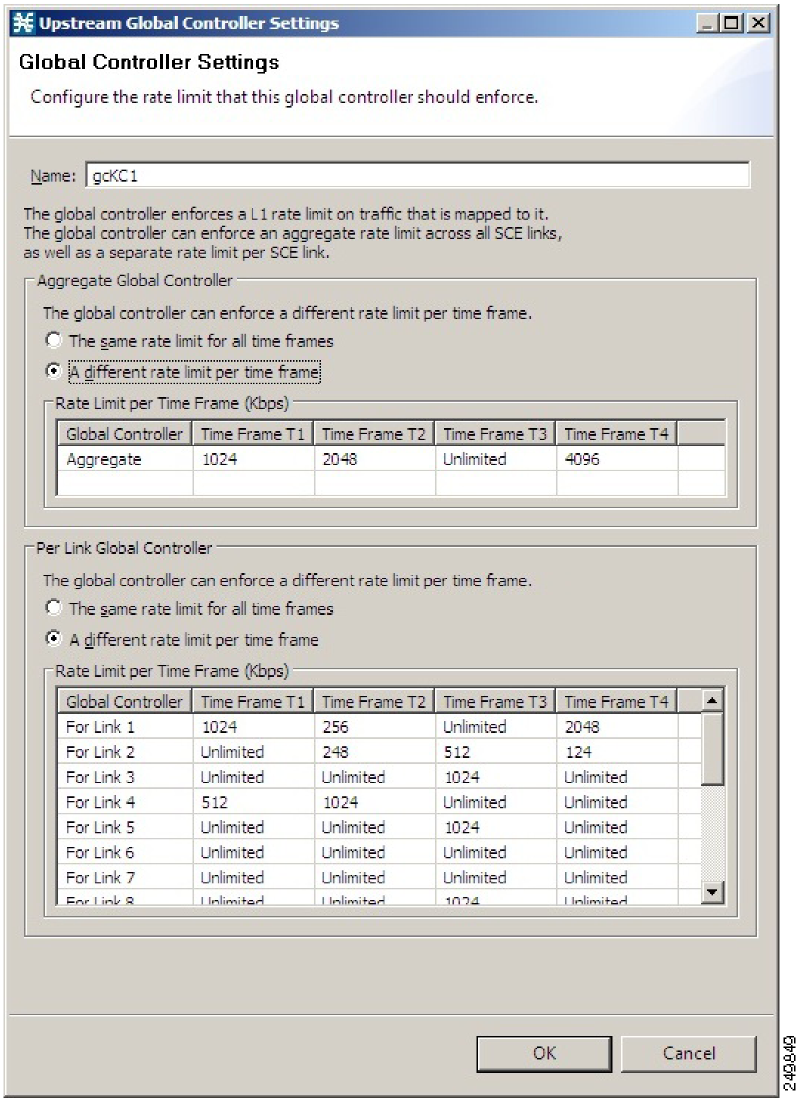
a. Choose the **The same rate limit for all time frames** radio button on the Default Virtual Link tab.

b. Enter the desired value in Kbps for the maximum bandwidth in the Rate limit for the Link 1 (in Kbps) field.

Step 12 Set the maximum limit that this global controller carries to vary according to time frame.

- **a.** Choose the **A different rate limit per time frame** radio button the Default Virtual Link tab.
- **b.** Enter the desired value for each time frame (Figure 9-26).

Figure 9-26 Upstream Global Controller Settings



Global Controller Settings

Configure the rate limit that this global controller should enforce.

Name: gcKC1

The global controller enforces a L1 rate limit on traffic that is mapped to it.
The global controller can enforce an aggregate rate limit across all SCE links,
as well as a separate rate limit per SCE link.

Aggregate Global Controller

The global controller can enforce a different rate limit per time frame.

○ The same rate limit for all time frames

● A different rate limit per time frame

Rate Limit per Time Frame (Kbps)

Global Controller	Time Frame T1	Time Frame T2	Time Frame T3	Time Frame T4
Aggregate	1024	2048	Unlimited	4096

Per Link Global Controller

The global controller can enforce a different rate limit per time frame.

○ The same rate limit for all time frames

● A different rate limit per time frame

Rate Limit per Time Frame (Kbps)

Global Controller	Time Frame T1	Time Frame T2	Time Frame T3	Time Frame T4
For Link 1	1024	256	Unlimited	2048
For Link 2	Unlimited	248	512	124
For Link 3	Unlimited	Unlimited	1024	Unlimited
For Link 4	512	1024	Unlimited	Unlimited
For Link 5	Unlimited	Unlimited	1024	Unlimited
For Link 6	Unlimited	Unlimited	Unlimited	Unlimited
For Link 7	Unlimited	Unlimited	Unlimited	Unlimited
For Link 8	Unlimited	Unlimited	1024	Unlimited

Step 13 Click **OK**.

Your changes are saved.

Managing Subscriber Bandwidth

After you have defined global controllers, you can add subscriber BWCs to packages and map these subscriber BWCs to different global controllers.

A Subscriber BWC controls subscriber bandwidth consumption for upstream or downstream flows. It controls and measures the bandwidth of an aggregation of traffic flows of a service or group of services.

Each package has its own set of BWCs that determine the bandwidth available per package subscriber for each available service.

The two Primary BWCs, one for upstream traffic and one for downstream traffic, allocate bandwidth to specific subscribers. Bandwidth is allocated based on the Committed Information Rate (CIR), the Peak Information Rate (PIR), and the Subscriber relative priority settings. You can configure these parameters, but the Primary BWCs cannot be deleted.

There are two default BWCs, one for upstream traffic and one for downstream traffic. By default, all services are mapped to one of these two BWCs. The BWC mechanism controls rate subpartitioning within the default BWC rate control, based on the CIR, PIR, and AL. You can configure these parameters, but the default BWCs cannot be deleted.

You can add up to 32 user-defined BWCs per package:

- Subscriber BWCs operate at the service-per-subscriber level. They allocate bandwidth for services for each subscriber, based upon the CIR, PIR, global controller, and Assurance Level (AL) set for the BWC. Each rule defines a link between the flow of the service and one of the BWCs (unless the flows are to be blocked). See How to Define Per-Flow Actions for a Rule, page 9-66.
- Extra BWCs also operate at the subscriber level. Extra BWCs (based on the CIR, PIR, global controller, and AL) can be allocated for services that are not included in the Primary BWC. These are services that are not often used but have strict bandwidth requirements, for example, video conference calls. The Extra BWCs are BWCs that control a single service (or service group). BWCs cannot borrow bandwidth from Extra BWCs and vice versa.

Each user-defined BWC controls either downstream or upstream traffic.

Caution If you enable or disable Virtual Links mode, all user-defined global controllers are deleted from the service configuration. A BWC that pointed to a user-defined global controller now points to the default global controller. Other parameters of these BWCs remain unchanged.

The Cisco SCE supports a maximum of 2000 BWCs. You cannot apply a PQB file to a Cisco SCE if the file contains more than 2000 BWCs. But, the Subscriber BWCs with same values for GC Index, AL Level, PIR, and CIR are considered as a single BWC; even if the BWCs are mapped to different flows. So, in effect, Cisco SCA BB may support more than 2000 BWCs.

- Subscriber BWC Parameters, page 9-29
- How to Edit Package Subscriber BWCs, page 9-30

Subscriber BWC Parameters

The Subscriber BW Controllers tab of the Package Settings dialog box has the following configuration parameters:

- Name—A unique name for each BWC.
- CIR (L3 Kbps)—The minimum bandwidth that must be granted to traffic controlled by the BWC.

- PIR (L3 Kbps)—The maximum bandwidth allowed to traffic controlled by the BWC.

Note The minimum bandwidth for a subscriber BWC is 16 Kbps with a granularity of 1 Kbps and the maximum bandwidth is 500000 Kbps.

- Global Controller—The global controller with which this BWC is associated. The global controllers are virtual queues that are part of the bandwidth control mechanism. Direct traffic with similar bandwidth control properties to the same global controller.
- Assurance Level—How fast bandwidth either decreases from the PIR to the CIR as congestion builds or else increases from the CIR to the PIR as congestion decreases. A higher AL ensures a higher bandwidth compared to a similar BWC with a lower AL. The lowest assurance value is 1, the highest is Persistent (10).

  Assurance Level 10 (persistent) never goes below the relevant CIR, unless the total line rate cannot sustain this value.
- Subscriber relative priority—Assurance Level given to the Primary BWC of the subscriber. It determines the assurance given to all the subscriber traffic when competing for bandwidth with subscribers to other packages. The lowest value is 1; the highest is 10.

Note Subscriber bandwidth control (and accounting and reporting) is based on Layer 3 volume.
Global controller bandwidth is based on Layer 1 volume.

How to Edit Package Subscriber BWCs

Step 1 In the Policies tab, click **Global Policy**.

The Global Bandwidth Settings dialog box in the right (Rule) pane.

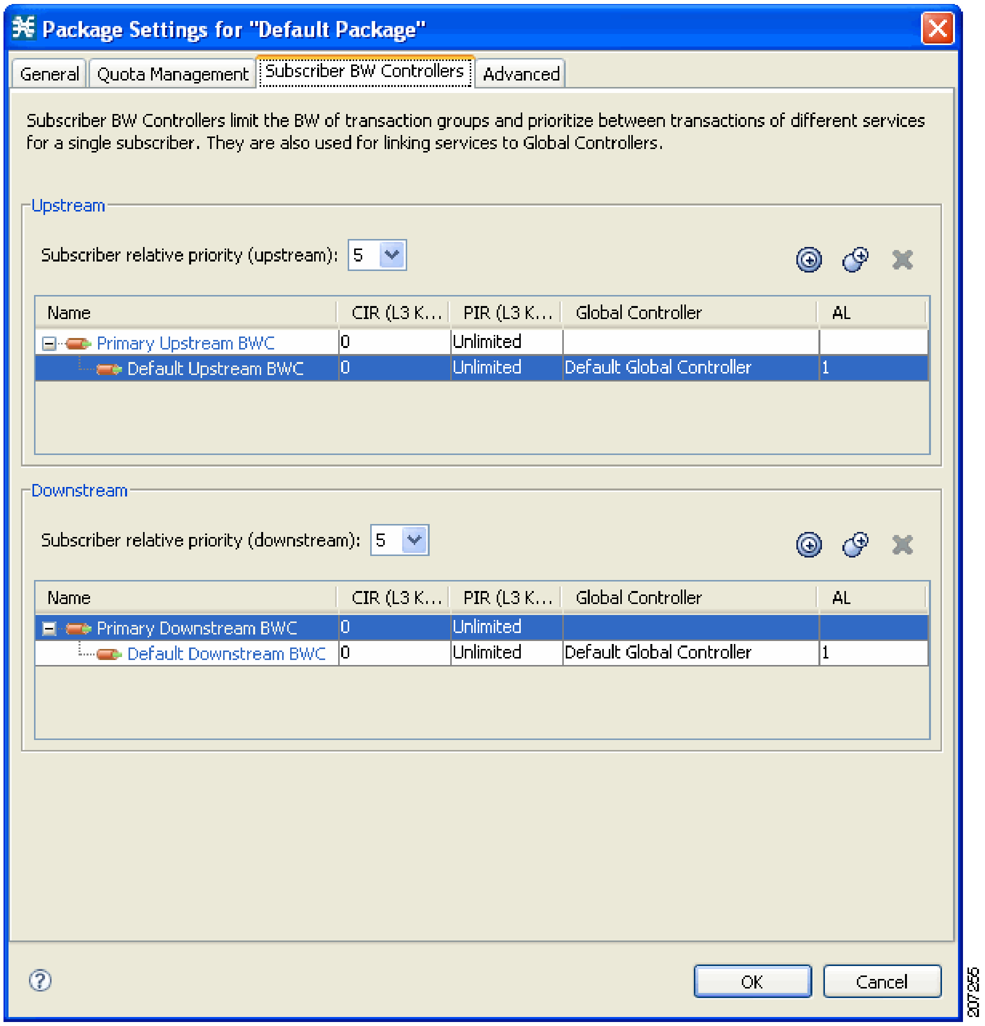
Step 2 In the right (Rule) pane, select a BWC and click the Edit (✎) icon.

The Package Settings dialog box appears.

Step 3 In the Package Settings dialog box, click the **Subscriber BW Controllers** tab.

The Subscriber BW Controllers tab opens (Figure 9-27).

Figure 9-27 Subscriber BW Controllers Tab



Package Settings for "Default Package"
General
Quota Management
Subscriber BW Controllers
Advanced
OK
Cancel
207255

Subscriber BW Controllers limit the BW of transaction groups and prioritize between transactions of different services for a single subscriber. They are also used for linking services to Global Controllers.

Upstream

Subscriber relative priority (upstream): 5

Name	CIR (L3 K...	PIR (L3 K...	Global Controller	AL
Primary Upstream BWC	0	Unlimited		
Default Upstream BWC	0	Unlimited	Default Global Controller	1

Downstream

Subscriber relative priority (downstream): 5

Name	CIR (L3 K...	PIR (L3 K...	Global Controller	AL
Primary Downstream BWC	0	Unlimited		
Default Downstream BWC	0	Unlimited	Default Global Controller	1

Step 4 Set your requirements for upstream bandwidth control in the Upstream area of the dialog box.

a. Select a value from the Subscriber relative priority drop-down list.

b. Set the parameters for the Primary Upstream BWC.

- In the CIR field, enter the BWC CIR in Kbps.
- In the PIR field, select **Unlimited** from the drop-down list, or enter the BWC PIR in Kbps.

c. To add BWCs to the package, click the **Add a sub BW Controller** (⊕) icon once for each additional BWC.

d. To add Extra BWCs to the package, click the **Add an extra BW Controller** (⊕) icon once for each additional BWC.

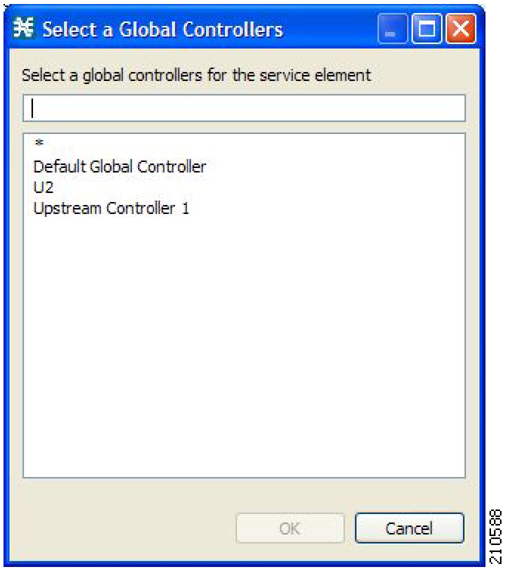
e. Set the parameters for each BWC (including the Primary and Default BWCs).

- (Optional) In the Name field, enter a meaningful name for each BWC. (You cannot rename the Primary or Default BWCs.)
- In the CIR field, enter a value for the BWC CIR in Kbps.
- In the PIR field, select **Unlimited** from the drop-down list, or enter a value for the BWC PIR in Kbps.
- To set the global controller, with which this BWC is associated:

  Click in the Global Controller cell of the BWC, and then click the **Browse** button that appears.

  The Select a Global Controller dialog box appears (Figure 9-28).

Figure 9-28 Select a Global Controller



Select a Global Controllers

Select a global controllers for the service element

*
Default Global Controller
U2
Upstream Controller 1

- Select a global controller and click **OK**.
- Select a value from the AL drop-down list.

Step 5 Repeat Step 3 for downstream bandwidth control in the Downstream area of the dialog box.

Step 6 Click **OK**.

The Package Settings dialog box closes.

All changes to the BWC settings are saved.

The effect of Assurance Level on bandwidth allocation for subscriber BWCs will be as follows:

If there are 4 BWCs namely “Priority”, “Gold”, “Silver” and “default” with Assurance Levels 9, 6, 3 and 1 respectively, the “priority” BWC gets the bandwidth first, followed by the "Gold" and the "Silver" BWC. The “default” BWC will be the last to get the bandwidth.

Managing Bandwidth: A Practical Example

This section explains how to achieve effective bandwidth control by combining the configuration of global controllers and subscriber BWCs, and gives a practical example.

- How to Configure Total Bandwidth Control, page 9-33
- Example: How to Limit P2P and Streaming Traffic Using the Console, page 9-33

How to Configure Total Bandwidth Control

Step 1 Configure the necessary global controllers.

Ascertain which services are likely to be problematic, and what the maximum total bandwidth should be for each. You do not need to configure services and packages that are unlikely to be problematic; you can include them in the default global controllers.

Step 2 Configure the subscriber BWCs for the package.

a. Add a subscriber BWC for each type of upstream or downstream traffic that you want to limit, and configure the CIR and the PIR accordingly.

b. Select an appropriate global controller for each subscriber BWC.

Step 3 For each service that is to have its own BWC, create a rule and select appropriate upstream and downstream BWCs.

Example: How to Limit P2P and Streaming Traffic Using the Console

Note This example assumes that the traffic flow is bidirectional; you may decide that you only need upstream controllers or downstream controllers.

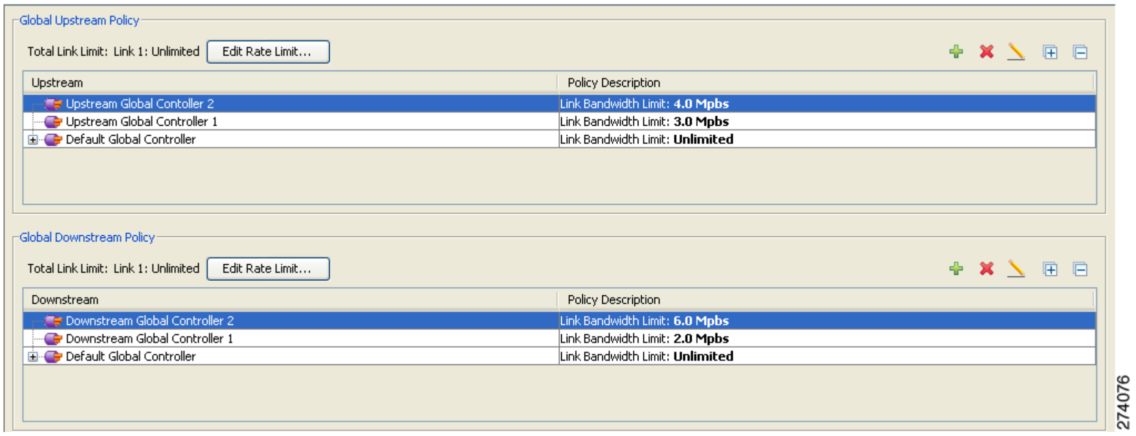
Note The P2P Traffic Optimization wizards allow you to create a simple model of devices, connect to them, and limit P2P traffic to a specified bandwidth. (See How to Use the P2P Traffic Optimization Wizards, page 4-50.)

Step 1 In the Policies tab, click **Global Policy**.

The Global Bandwidth Settings dialog box in the right (Rule) pane.

Step 2 Add two upstream global controllers and two downstream global controllers and assign the desired bandwidth to each global controller (Figure 9-29).

Figure 9-29 Global Bandwidth Settings



Global Upstream Policy

Total Link Limit: Link 1: Unlimited [Edit Rate Limit...]

Upstream	Policy Description
Upstream Global Contoller 2	Link Bandwidth Limit: **4.0 Mpbs**
Upstream Global Controller 1	Link Bandwidth Limit: **3.0 Mpbs**
Default Global Controller	Link Bandwidth Limit: **Unlimited**

Global Downstream Policy

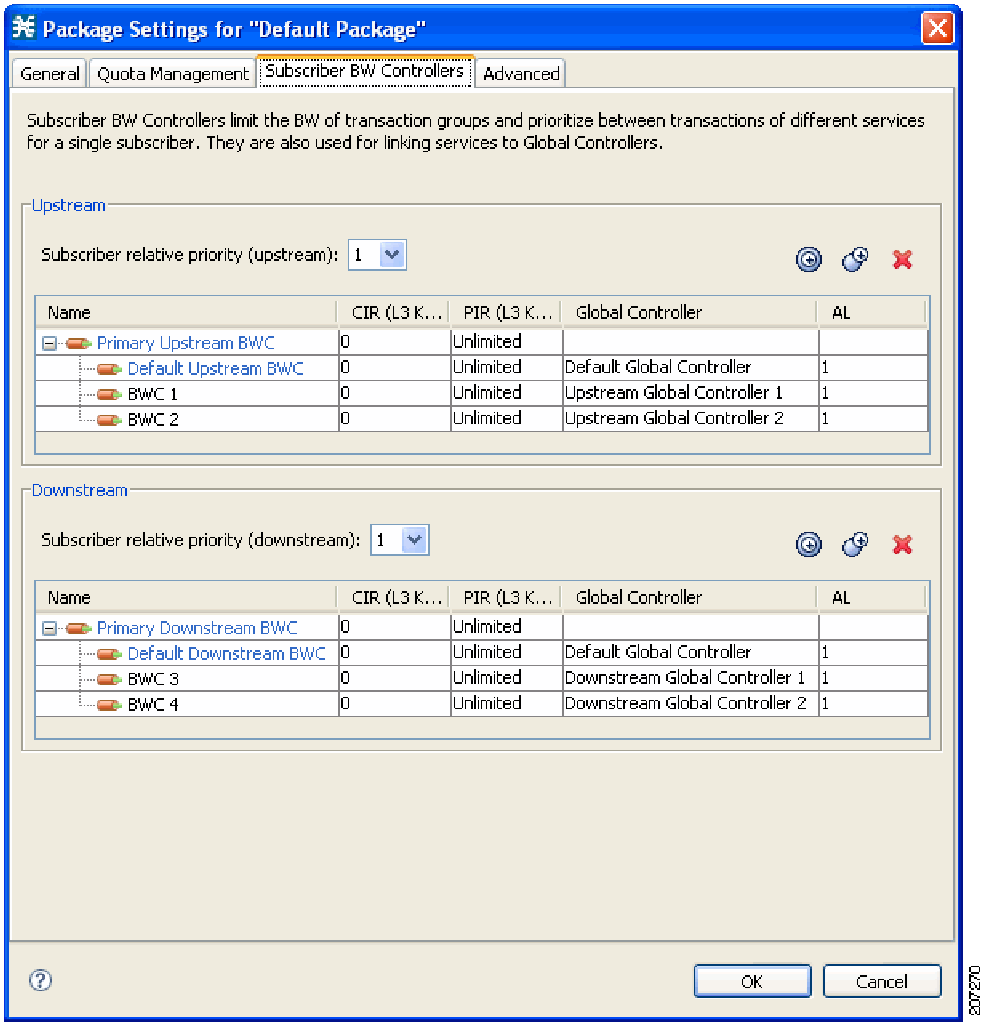
Total Link Limit: Link 1: Unlimited [Edit Rate Limit...]

Downstream	Policy Description
Downstream Global Controller 2	Link Bandwidth Limit: **6.0 Mpbs**
Downstream Global Controller 1	Link Bandwidth Limit: **2.0 Mpbs**
Default Global Controller	Link Bandwidth Limit: **Unlimited**

(Here, Upstream Controller 1 and Downstream Controller 1 is used for P2P traffic, and Upstream Controller 2 and Downstream Controller 2 is used for streaming traffic.)

Step 3 In a Package Settings dialog box (Figure 9-30), add two upstream BWCs and two downstream BWCs, map them to the appropriate global controllers, and set their parameters (CIR, PIR, AL).

Figure 9-30 Package Settings


Package Settings for "Default Package"
General
Quota Management
Subscriber BW Controllers
Advanced
Upstream
Downstream
OK
Cancel
207270

Subscriber BW Controllers limit the BW of transaction groups and prioritize between transactions of different services for a single subscriber. They are also used for linking services to Global Controllers.

Upstream

Subscriber relative priority (upstream): 1

Name	CIR (L3 K...	PIR (L3 K...	Global Controller	AL
Primary Upstream BWC	0	Unlimited		
Default Upstream BWC	0	Unlimited	Default Global Controller	1
BWC 1	0	Unlimited	Upstream Global Controller 1	1
BWC 2	0	Unlimited	Upstream Global Controller 2	1

Downstream

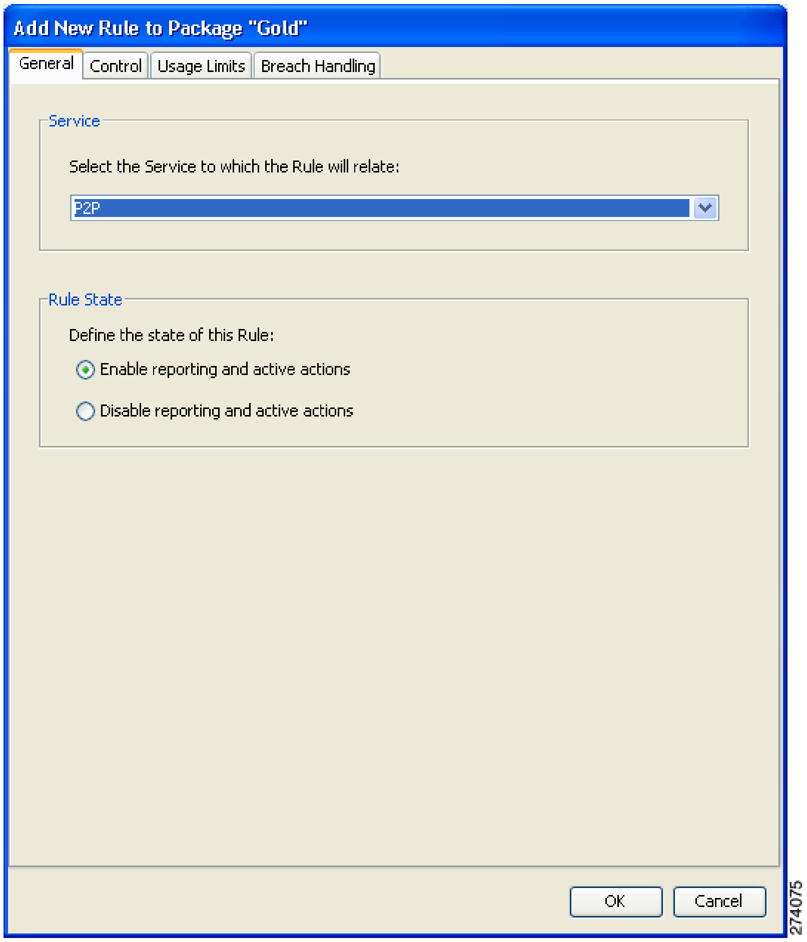
Subscriber relative priority (downstream): 1

Name	CIR (L3 K...	PIR (L3 K...	Global Controller	AL
Primary Downstream BWC	0	Unlimited		
Default Downstream BWC	0	Unlimited	Default Global Controller	1
BWC 3	0	Unlimited	Downstream Global Controller 1	1
BWC 4	0	Unlimited	Downstream Global Controller 2	1

(Here, BWC1 is for upstream P2P traffic and BWC3 is for downstream P2P traffic; BWC2 is for upstream streaming traffic and BWC4 is for downstream streaming traffic.)

Step 4 Add a rule for the P2P service (Figure 9-31).

Figure 9-31 Add New Rule to Package



Add New Rule to Package "Gold"

Service

Select the Service to which the Rule will relate:

P2P

Rule State

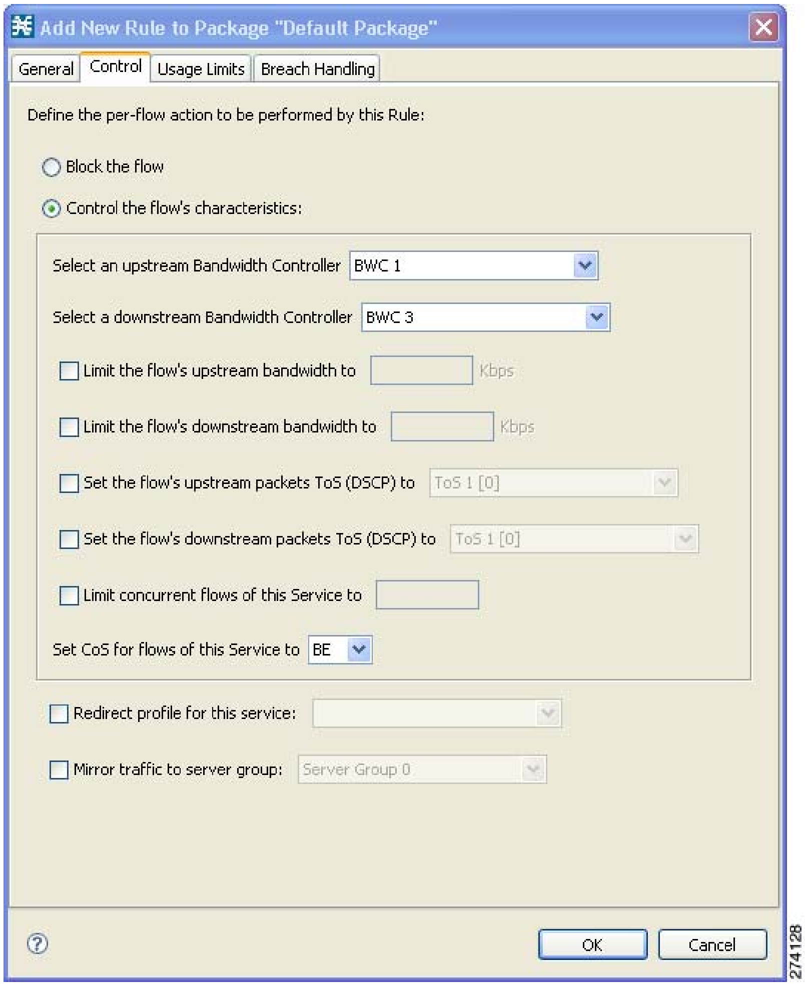
Define the state of this Rule:

● Enable reporting and active actions

○ Disable reporting and active actions

Step 5 In the Control tab (Figure 9-32), assign BWC 1 as the upstream BWC and BWC 3 as the downstream BWC.

Figure 9-32 Control Tab



Add New Rule to Package "Default Package"

General | Control | Usage Limits | Breach Handling

Define the per-flow action to be performed by this Rule:

○ Block the flow

● Control the flow's characteristics:

Select an upstream Bandwidth Controller: BWC 1

Select a downstream Bandwidth Controller: BWC 3

□ Limit the flow's upstream bandwidth to ____ Kbps

□ Limit the flow's downstream bandwidth to ____ Kbps

□ Set the flow's upstream packets ToS (DSCP) to: ToS 1 [0]

□ Set the flow's downstream packets ToS (DSCP) to: ToS 1 [0]

□ Limit concurrent flows of this Service to ____

Set CoS for flows of this Service to: BE

□ Redirect profile for this service:

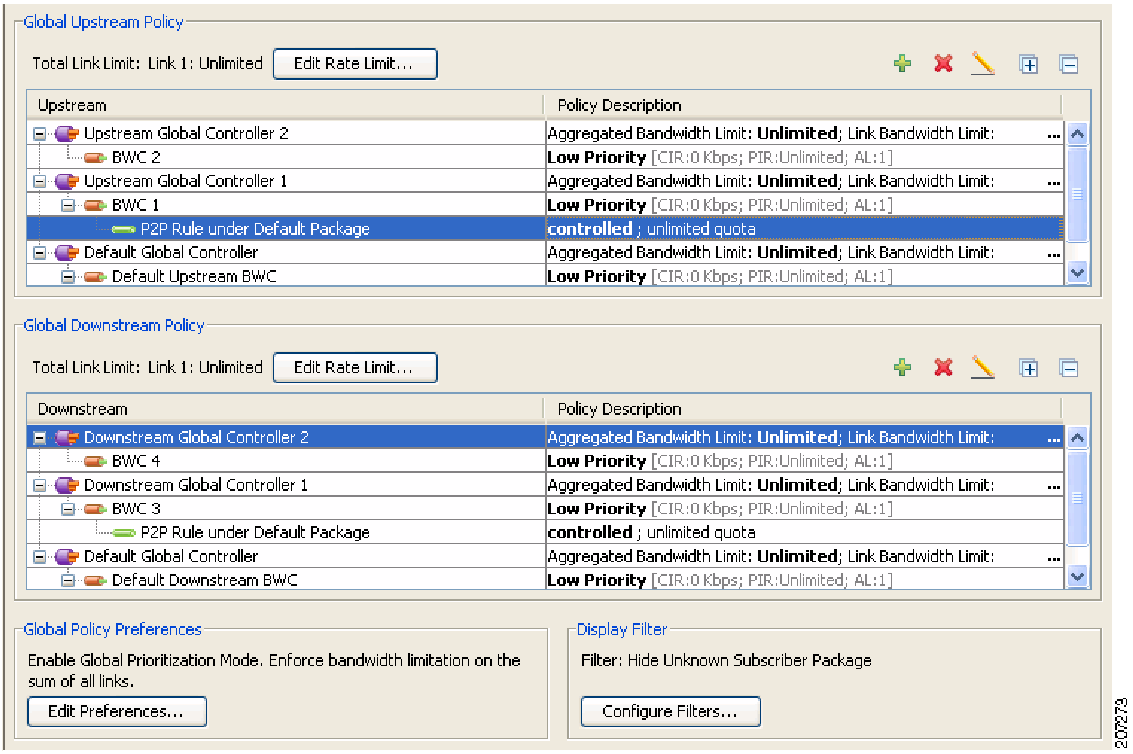
□ Mirror traffic to server group: Server Group 0

Step 6 Repeat Step 4 and Step 5 for the Streaming service, using BWC 2 as the upstream BWC and BWC 4 as the downstream BWC.

All subscriber traffic using these services are added to the virtual queue total for these queues. In turn, the bandwidth available to the subscriber for these protocols fluctuate, depending on how “full” these queues are.

Step 7 Click Global Policy to view the hierarchy of the GCs, BWCs, and rules (Figure 9-33).

Figure 9-33 Rule Hierarchy



Global Upstream Policy

Total Link Limit: Link 1: Unlimited [Edit Rate Limit...]

Upstream	Policy Description
Upstream Global Controller 2	Aggregated Bandwidth Limit: **Unlimited**; Link Bandwidth Limit: ...
BWC 2	**Low Priority** [CIR:0 Kbps; PIR:Unlimited; AL:1]
Upstream Global Controller 1	Aggregated Bandwidth Limit: **Unlimited**; Link Bandwidth Limit: ...
BWC 1	**Low Priority** [CIR:0 Kbps; PIR:Unlimited; AL:1]
P2P Rule under Default Package	**controlled** ; unlimited quota
Default Global Controller	Aggregated Bandwidth Limit: **Unlimited**; Link Bandwidth Limit: ...
Default Upstream BWC	**Low Priority** [CIR:0 Kbps; PIR:Unlimited; AL:1]

Global Downstream Policy

Total Link Limit: Link 1: Unlimited [Edit Rate Limit...]

Downstream	Policy Description
Downstream Global Controller 2	Aggregated Bandwidth Limit: **Unlimited**; Link Bandwidth Limit: ...
BWC 4	**Low Priority** [CIR:0 Kbps; PIR:Unlimited; AL:1]
Downstream Global Controller 1	Aggregated Bandwidth Limit: **Unlimited**; Link Bandwidth Limit: ...
BWC 3	**Low Priority** [CIR:0 Kbps; PIR:Unlimited; AL:1]
P2P Rule under Default Package	**controlled** ; unlimited quota
Default Global Controller	Aggregated Bandwidth Limit: **Unlimited**; Link Bandwidth Limit: ...
Default Downstream BWC	**Low Priority** [CIR:0 Kbps; PIR:Unlimited; AL:1]

Global Policy Preferences

Enable Global Prioritization Mode. Enforce bandwidth limitation on the sum of all links.

[Edit Preferences...]

Display Filter

Filter: Hide Unknown Subscriber Package

[Configure Filters...]

How to Configure a Rule, Bandwidth Controller, and Global Controller Using the Wizard

You can configure a rule, BWC, and GC together from the Global Policy window.

Step 1 In the Policies tab, click **Global Policy**.

The Global Bandwidth Settings are displayed in the right (Rule) pane.

Step 2 Above the area (Upstream or Downstream) of the desired interface, click the **Add** (✚) icon.

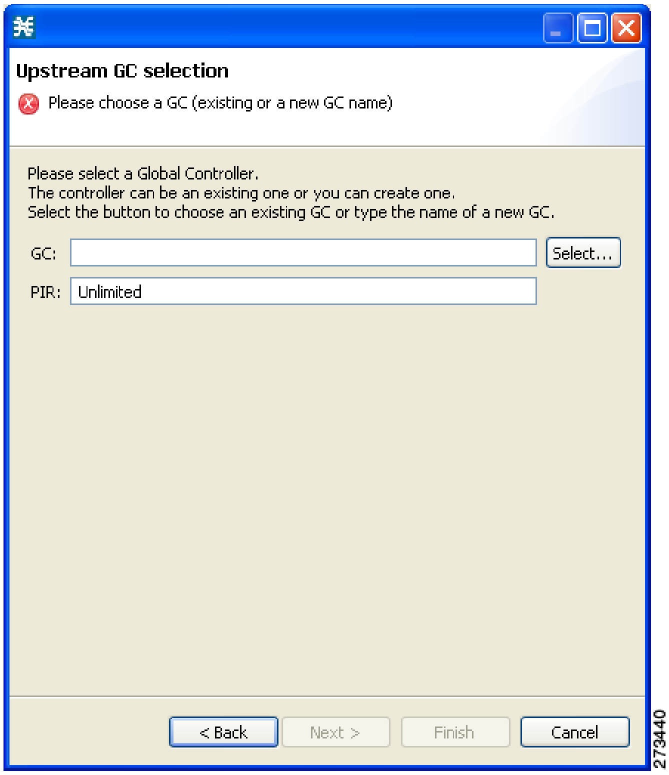
The Select addition mode dialog box appears.

Step 3 Choose the **Add a Global Controller and map a Rule and BWC to it** radio button.

Step 4 Click **Finish**.

The GC Selection dialog box appears (Figure 9-34).

Figure 9-34 Upstream GC Selection



Upstream GC selection

Please choose a GC (existing or a new GC name)

Please select a Global Controller.
The controller can be an existing one or you can create one.
Select the button to choose an existing GC or type the name of a new GC.

GC:

PIR: Unlimited

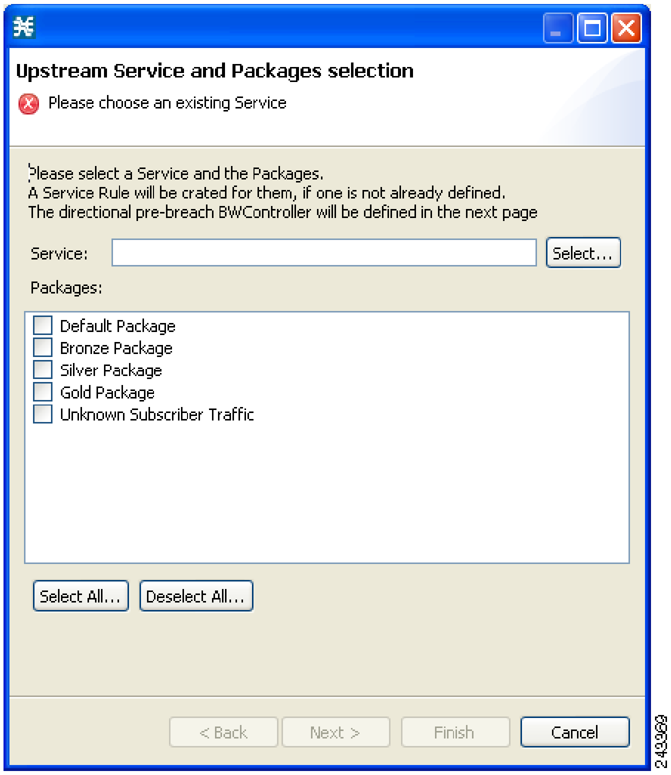
Step 5 In the GC field, enter a new GC name, or click **Select** to choose an existing GC.

Step 6 (Optional) In the PIR field, enter the maximum bandwidth limit that this global controller carries in Kbps.

Step 7 Click **Next**.

The Service and Packages selection dialog box appears (Figure 9-35).

Figure 9-35 Upstream Service and Packages Selection



Upstream Service and Packages selection

Please choose an existing Service

Please select a Service and the Packages.
A Service Rule will be crated for them, if one is not already defined.
The directional pre-breach BWController will be defined in the next page

Service:

Packages:

□ Default Package
□ Bronze Package
□ Silver Package
□ Gold Package
□ Unknown Subscriber Traffic

Step 8 In the Service field, select an existing service.

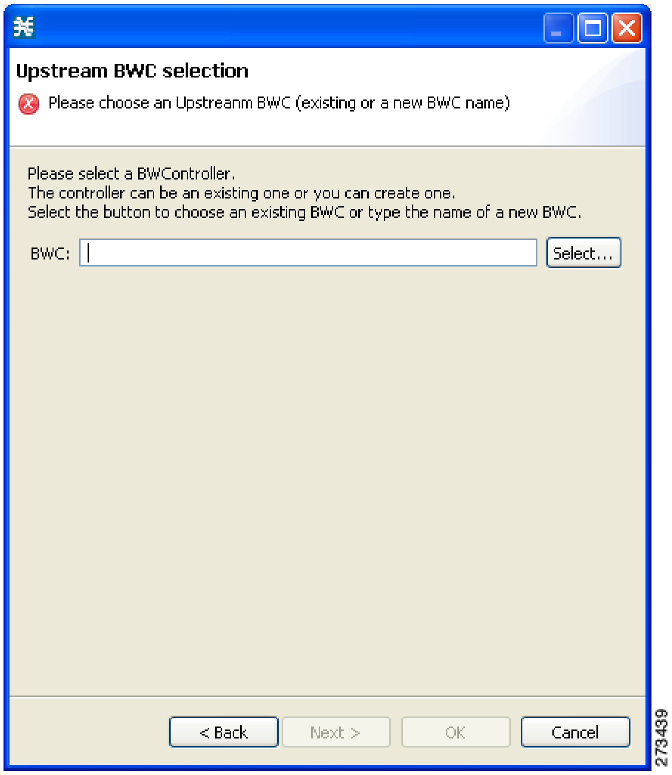
Step 9 In the Packages section, select one or more packages for the rule to apply to.

If a rule does not exist for the service, it is created. The new, or existing rule is then mapped to the selected package or packages.

Step 10 Click **Next**.

The BWC selection dialog box appears (Figure 9-36).

Figure 9-36 Upstream BWC Selection



Upstream BWC selection

Please choose an Upstreanm BWC (existing or a new BWC name)

Please select a BWController.
The controller can be an existing one or you can create one.
Select the button to choose an existing BWC or type the name of a new BWC.

BWC:

Step 11 Enter a new BWC name, or click **Select** to choose an existing BWC.

Step 12 Click **OK**.

How to Configure the Upstream Configuration of the Global Bandwidth Controller for IPv6

You can configure the upstream configuration of the global bandwidth controller for IPv6 from the Global Policy window. For details on managing the bandwidth, see the "Managing Bandwidth" section on page 9-2. Perform the following procedures:

Step 1 In the Service Configuration Editor window, click the **Policies** tab.

Step 2 Under the Policies tab, click **Global Policy**.

The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.

Step 3 Above the area (Upstream or Downstream) of the corresponding interface, click the **Add** (➕) icon.

The Select Addition mode dialog box is displayed.

Step 4 Click the **Add a Global Controller and map a Rule and a BWC to it** radio button to add a global controller with a rule mapped to it and a BWC added to it.

Step 5 Select an existing global controller by clicking the **Select** button or create a new global controller by typing the name of a global controller.

Step 6 Enter the PIR value and click **Next**.

Step 7 Select the service to control and check the Unknown Subscriber Package check box and Click **Next**.

Step 8 Select an existing BWC by clicking the **Select** button or create a new BWC by typing the name of the BWC. Click **Next**.

Step 9 Double-click on the unknown subscriber package to verify the bandwidth controller and the global controller association.

Follow the same procedure for the downstream configuration of the global bandwidth controller for IPv6.

How to Set BW Management Prioritization Mode

Relative priority is the level of assurance that an internal BWC (iBWC) receives when competing against other iBWCs for bandwidth.

The relative priority of one of the following modes determines the relative priority of the flow that goes through an iBWC:

- The iBWC—In Global Prioritization Mode
- The subscriber—In Subscriber Prioritization Mode

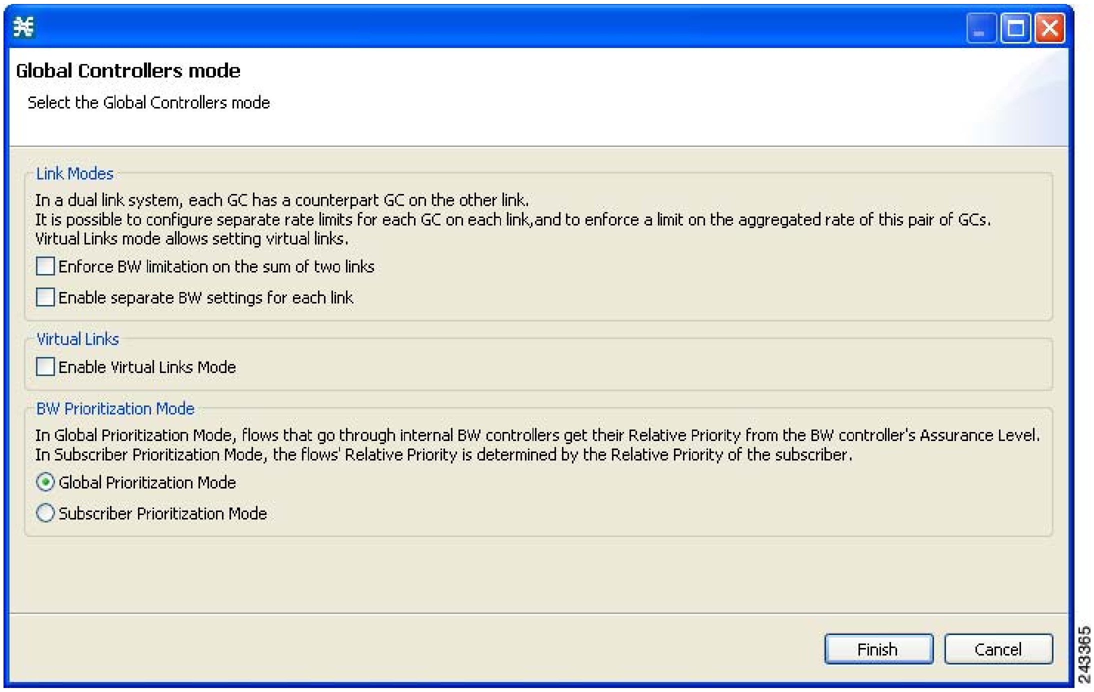
Step 1 In the Policies tab, click **Global Policy**.

The Global Bandwidth Settings are displayed in the right (Rule) pane.

Step 2 Click **Edit Preferences**.

The Global Controllers mode dialog box appears (Figure 9-37).

Figure 9-37 Global Controllers Mode



Global Controllers mode

Select the Global Controllers mode

Link Modes

In a dual link system, each GC has a counterpart GC on the other link.
It is possible to configure separate rate limits for each GC on each link,and to enforce a limit on the aggregated rate of this pair of GCs.
Virtual Links mode allows setting virtual links.

□ Enforce BW limitation on the sum of two links

□ Enable separate BW settings for each link

Virtual Links

□ Enable Virtual Links Mode

BW Prioritization Mode

In Global Prioritization Mode, flows that go through internal BW controllers get their Relative Priority from the BW controller's Assurance Level.
In Subscriber Prioritization Mode, the flows' Relative Priority is determined by the Relative Priority of the subscriber.

● Global Prioritization Mode

○ Subscriber Prioritization Mode

Step 3 Select one of the **BW Prioritization Mode** radio buttons.

- **Global Prioritization Mode**
- **Subscriber Prioritization Mode**

Step 4 Click **OK**.

The Global Controllers mode dialog box closes.

The selected BW management parameter is saved.

Managing Virtual Links

In Virtual Links mode, template bandwidth controllers are defined for packages. Actual bandwidth parameters are assigned when a subscriber enters the system. This bandwidth depends on the package of the subscriber and the physical link assigned to the subscriber. The package of the subscriber defines the template controllers.

For each service configuration that has Virtual Links mode enabled, there is one default upstream virtual link and one default downstream virtual link. The upstream and downstream interfaces are each assigned one default template global controller.

You can add additional template global controllers. You can add, modify, and delete virtual links using a command-line interface (CLI).

The number of directional template global controllers limits the maximum number of virtual links. The number of template global controllers times the number of virtual links cannot exceed 1024 or 4096. Based on the Cisco SCE hardware, the number of global controllers varies. For details, see the "Managing Bandwidth" section on page 9-2.

To support the DOCSIS 3.0 Downstream bonding, a two level virtual link hierarchy is created for the wideband channels. The wideband channels are associated with the Aggregate Global Control (AGC) that provides a constant output signal despite variations in input signal strength. Wideband channels are associated with three AGCs in a two level hierarchy. At the lower level of the hierarchy, all the DOCSIS 3.0 modems for wideband are aggregated into one AGC and the other AGC contains both legacy and 3.0 modems. The AGC at the top level of the hierarchy is used to limit the aggregated bandwidth of the wideband channel.

For more information on the support for DOCSIS 3.0 solution, see *Cisco Service Control for Managing Remote Cable MSO Links Solution Guide.*

For more information on managing the virtual links global controllers, see Managing Virtual Links Global Controllers, page 9-48.

Caution If you enable or disable Virtual Links mode, all user-defined global controllers are deleted from the service configuration. A subscriber BWC that pointed to a user-defined global controller now points to the default global controller. (Other parameters of these subscriber BWCs remain unchanged.)

Note While applying a policy in virtual link mode, if the new template includes a different number of global controllers than the currently applied template, you must choose the Reset all Virtual Links to Template Rate Limits. Otherwise, selecting apply results in en error message, similar to the following:

"Template Upstream Virtual Link differ from the one in the SCE - cannot apply without the force template virtual link option."

The following steps outline configuring a service configuration in Virtual Links mode. The procedure is similar to that for configuring any service configuration, but virtual links must be added using the CLI.

1. Create a new service configuration.
2. Open the Global Bandwidth Settings dialog box and check the Enable Virtual Links Mode check box.
3. Create template global controllers.
4. Create packages.

Add subscriber BW controllers to the packages and associate them with appropriate global controllers.

5. Apply the service configuration.

   The bandwidth values of the default global controllers are set; the values of all other global controllers are not set – these global controllers are templates.

6. Add virtual links using the CLI.

   Each virtual link gets a set of global controllers with the PIR values of the template global controller configuration.

   If necessary, you can use the CLI to change the PIR values of the global controller.

7. A subscriber is introduced to the SCE platform. Upstream and downstream virtual links are associated with the subscriber as well as a package.

8. Rule resolution for each flow of the subscriber is according to the package of the subscriber and the global controller configuration of the virtual link.

Collection Manager Virtual Links Names Utility

The Collection Manager (CM) includes a command-line utility for managing the names of virtual links.

For more information about the CM Virtual Links Names Utility, see the “Managing Virtual Links” section in the “Managing the Collection Manager” chapter of *Cisco Service Control Management Suite Collection Manager User Guide*.

How to Enable Virtual Links Mode

To use virtual links, you must enable Virtual Links mode.

Caution If you enable or disable Virtual Links mode, all user-defined global controllers are deleted from the service configuration.

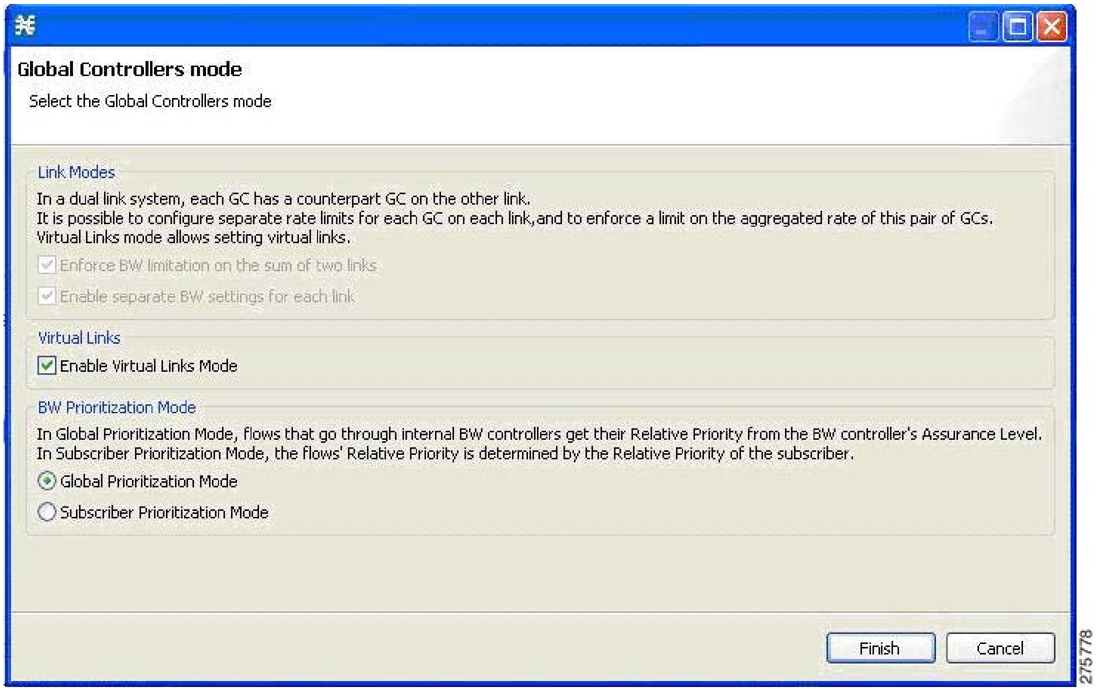
Step 1 In the Policies tab, click **Global Policy**.

The Global Bandwidth Settings are displayed in the right (Rule) pane.

Step 2 Click **Edit Preferences**.

The Global Controllers mode dialog box appears (Figure 9-38).

Figure 9-38 Global Controllers Mode



Global Controllers mode

Select the Global Controllers mode

Link Modes

In a dual link system, each GC has a counterpart GC on the other link.
It is possible to configure separate rate limits for each GC on each link,and to enforce a limit on the aggregated rate of this pair of GCs.
Virtual Links mode allows setting virtual links.

☑ Enforce BW limitation on the sum of two links

☑ Enable separate BW settings for each link

Virtual Links

☑ Enable Virtual Links Mode

BW Prioritization Mode

In Global Prioritization Mode, flows that go through internal BW controllers get their Relative Priority from the BW controller's Assurance Level.
In Subscriber Prioritization Mode, the flows' Relative Priority is determined by the Relative Priority of the subscriber.

● Global Prioritization Mode

○ Subscriber Prioritization Mode

Step 3 Check the **Enable Virtual Links Mode** check box.

Note If you have already added global controllers or if you selected asymmetric routing classification mode, a warning message appears. To continue, click **OK**.

The Virtual Links Global Controllers tab opens.

Step 4 Click **Finish**.

The Global Bandwidth Settings dialog box closes.

How to View Virtual Links Global Controller Settings

Note Global controller bandwidth is based on Layer 1 volume.
(Accounting, reporting, and subscriber bandwidth control in Cisco SCA BB is based on Layer 3 volume.)

Step 1 In the Policies tab, click **Global Policy**.

The Global Bandwidth Settings are displayed in the right (Rule) pane.

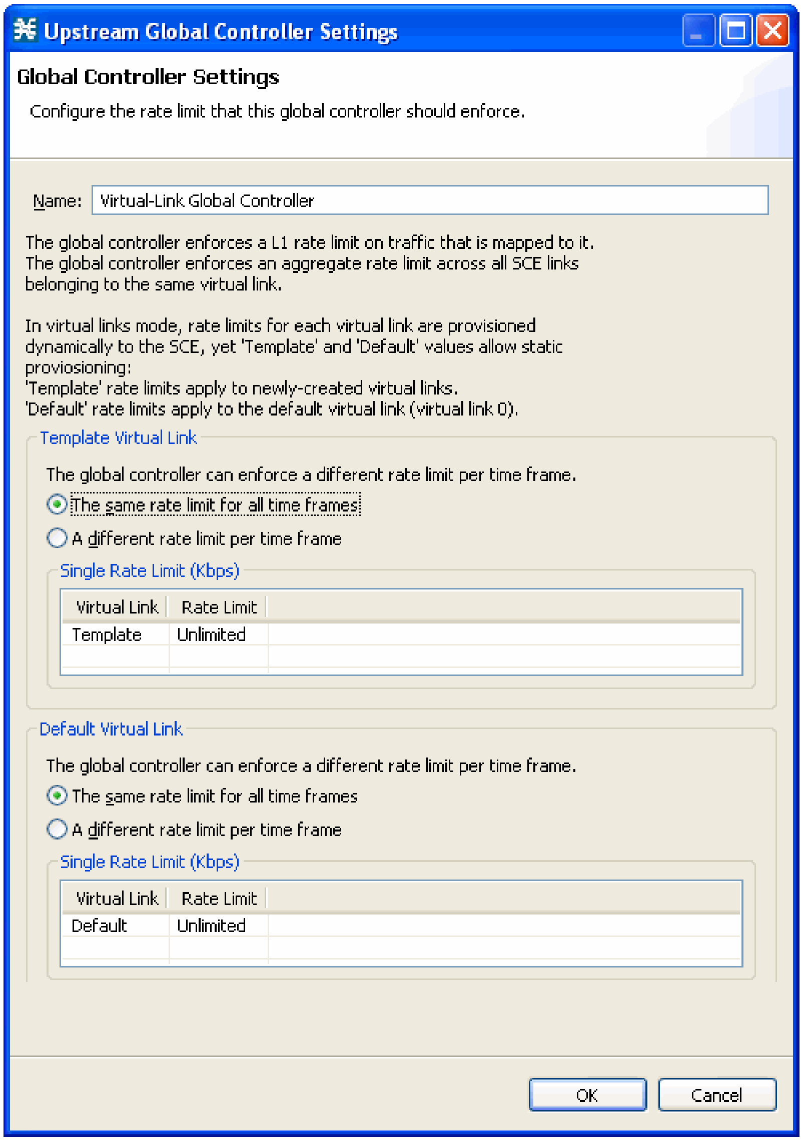
The maximum amount of bandwidth that can be used by any global controller is displayed at the top of the Global Bandwidth Settings:

- **Total Link Upstream Bandwidth Limit: Link 1**
- **Total Link Downstream Bandwidth Limit: Link 1**

Step 2 Select a global controller, and click the **Edit** (✏) icon.

The Global Controller Settings dialog box appears (Figure 9-39).

Figure 9-39 Upstream Global Controller Settings



Global Controller Settings

Configure the rate limit that this global controller should enforce.

Name: Virtual-Link Global Controller

The global controller enforces a L1 rate limit on traffic that is mapped to it.
The global controller enforces an aggregate rate limit across all SCE links belonging to the same virtual link.

In virtual links mode, rate limits for each virtual link are provisioned dynamically to the SCE, yet 'Template' and 'Default' values allow static proviosioning:
'Template' rate limits apply to newly-created virtual links.
'Default' rate limits apply to the default virtual link (virtual link 0).

Template Virtual Link

The global controller can enforce a different rate limit per time frame.

● The same rate limit for all time frames

○ A different rate limit per time frame

Single Rate Limit (Kbps)

Virtual Link	Rate Limit
Template	Unlimited

Default Virtual Link

The global controller can enforce a different rate limit per time frame.

● The same rate limit for all time frames

○ A different rate limit per time frame

Single Rate Limit (Kbps)

Virtual Link	Rate Limit
Default	Unlimited

The values of the global controllers defined in the dialog box depends on the values displayed in the Global Bandwidth Settings. So, for example, if the Total Link Upstream Bandwidth Limit: Link 1 has a value of 10 Mbps then the upstream default global controller value cannot exceed 10 Mbps.

The **Name** field contains a unique name assigned to the global controller. The system automatically assigns the names Controller 1, Controller 2, and so on.

The dialog box contains the following two tabs:

- **Template Virtual Link**—The default maximum value of the total link limit permitted to global controllers of any created virtual links, either for all time frames or per time frame.
- **Default Virtual Link**—The maximum value of the total link limit permitted to global controllers of the default virtual link, either for all time frames or per time frame.

Step 3 Click **OK**.

The Global Bandwidth Settings dialog box closes.

Managing Virtual Links Global Controllers

Virtual link global controllers can be added edited and deleted in the same way as regular global controllers. For more information, see the following sections:

- How to Add Global Controllers, page 9-7
- How to Set the Maximum Bandwidth of Global Controllers, page 9-9
- How to Delete Global Controllers, page 9-11
- Managing Subscriber Bandwidth, page 9-29

How to Edit the Virtual Links Total Link Limits

You can limit the total bandwidth passing through the physical link.

The total link limits for upstream and downstream traffic are defined independently.

In Virtual Links mode, bandwidth limitations are applied to the sum of all links.

Step 1 In the Policies tab, click **Global Policy**.

The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.

Step 2 In the Upstream or Downstream section, click **Edit Rate Limit**.

The Total Rate Limit dialog box appears.

Step 3 In the **Total Rate Limit for each SCE link (Kbps)** field, enter the maximum bandwidth of the SCE platform capacity that the platform carries, or enter Unlimited.

Step 4 Click **OK**.

The Total Rate Limit dialog box closes.

The Total Link Bandwidth Limit: Link 1 field is updated.

Managing Virtual Links with CLI Commands

You can configure, enable, and disable virtual links using the SCE platform Command-Line Interface (CLI). For more information about the SCE platform CLI, see *Cisco SCE8000 CLI Command Reference*.

- Use the following CLI commands to manage virtual links:

```
virtual-links index <index> direction [upstream | downstream]
virtual-links index <VL index> direction [upstream | downstream] gc <gc index> set-PIR
value <PIR 1, PIR2, PIR3, PIR4>
virtual-links index <VL index> direction [upstream | downstream] gc <gc index> set-PIR
value <PIR for all timeframes>
virtual-links index <VL index> direction [upstream | downstream] gc <gc index>
reset-PIR
no virtual-links index <index> direction [upstream | downstream]
```

  These commands are line interface configuration commands. To run these commands see How to Enter Line Interface Configuration Mode, page 9-50.

- Use the following CLI command to set the virtual links index of a subscriber:

```
subscriber name <name> property name [vlUp | vlDown] value <vl index>
```

  This command is a line interface configuration command. To run this command, see How to Enter Line Interface Configuration Mode, page 9-50.

- Use the following CLI command in EXEC mode to monitor the status of virtual links:

```
Show interface LineCard 0 virtual-links [all | changed | different-from-template]
```

Description of Virtual Links CLI Commands

Table 9-1 gives a description of the virtual links CLI commands.

Table 9-1 Virtual Links CLI Commands

Command	Description
virtual-links index <index> direction [upstream | downstream]	Add a virtual link
virtual-links index <VL index> direction [upstream | downstream] gc <gc index> set-PIR value <PIR 1, PIR2, PIR3, PIR4>	Update the global controller PIR values of a virtual link - separate values for each time frame
virtual-links index <VL index> direction [upstream | downstream] gc <gc index> set-PIR value <PIR for all timeframes>	Update the global controller PIR values of a virtual link - one value for all time frames
virtual-links index <VL index> direction [upstream | downstream] gc <gc index> reset-PIR	Update the global controller PIR values of a virtual link - take the values defined in the template global controller
no virtual-links index <index> direction [upstream | downstream]	Delete a virtual link
subscriber name <name> property name [vlUp | vlDown] value <vl index>	Set a virtual links index for the subscriber

Table 9-1 Virtual Links CLI Commands (continued)

Command	Description
show interface LineCard 0 virtual-links all	Show information about all virtual links
Show interface LineCard 0 virtual-links [all | changed | different-from-template]	Show information about virtual links whose PIR is changed or differs from the value defined in the template global controller

How to Enter Line Interface Configuration Mode

Step 1 At the SCE platform CLI prompt `(SCE#)`, type **configure**.

Step 2 Press **Enter**.

The `SCE(config)#` prompt appears.

Step 3 Type **interface LineCard 0**.

Step 4 Press **Enter**.

The `SCE(config if)#` prompt appears.

Managing Packages

A package is a description of subscriber policy. It is a collection of rules that defines the reaction of the system when it encounters flows that are mapped to the service to which the rule is related. It is recommended that you first define services (see Managing Services, page 7-3) and only then add and define packages.

Every Cisco SCA BB service configuration contains a package, the default package, which is the root package and cannot be deleted.

A subscriber is mapped to the default package in one of the following conditions:

- No other package is specifically assigned to the subscriber
- A nonexistent package is assigned to the subscriber.

A service configuration can contain up to 5000 packages.

- Package Parameters, page 9-51
- How to View Packages, page 9-53
- How to Add Packages, page 9-55
- How to Set Advanced Package Options, page 9-57
- How to Duplicate Packages, page 9-58
- How to Edit Packages, page 9-59
- How to Delete Packages, page 9-60

Package Parameters

The following parameters define a package:

- General parameters:
  - Package Name—A unique name for the package
  - Description—(Optional) A description of the package
- Quota Management parameters:
  - Quota Management Mode—Specifies how the subscriber quotas are managed—by external quota manager or replenished periodically by Cisco SCA BB.
  - Aggregation Period Type—The quota aggregation period used when quotas are replenished periodically.
  - Quota Buckets—16 resource buckets used for quota management.
- Subscriber BW Controllers parameters:
  - Subscriber relative priority—The relative priority given to subscribers of the package at times of Network congestion.

    Separate priorities are defined for upstream and downstream flows.
  - Subscriber Bandwidth Controllers—A list of BW controllers (BWCs) that are available to services that are part of the package. Various parameters are defined for each BWC, including a mapping to a global controller.

    Separate BWCs are defined for upstream and downstream flows.

- Advanced parameters:
  - Package Index—The unique number by which the system recognizes a package. Changing the package name does not affect SCE platform activity. The system provides a default value of the package index. Do not modify this value.
  - Parent Package—The package one level higher in the package hierarchy. The parent package is important when packages share usage counters. The default package is the base of the package hierarchy, and does not have a parent.
  - Package Usage Counter—Used by the system to generate data about the total use by each package. A package can use either an exclusive package usage counter or the package usage counter of the parent package.

    Each usage counter has:
  - A name assigned by the system (based on the package name).

Note An asterisk is appended to a package usage counter name whenever the counter applies to more than one package.

  - A unique counter index—The system provides a default value of the counter index. Do not modify this value.
  - Calendar—The calendar used as the basis for the time-based rules of the package.
  - VAS Traffic Forwarding Table—The forwarding table used by the package.

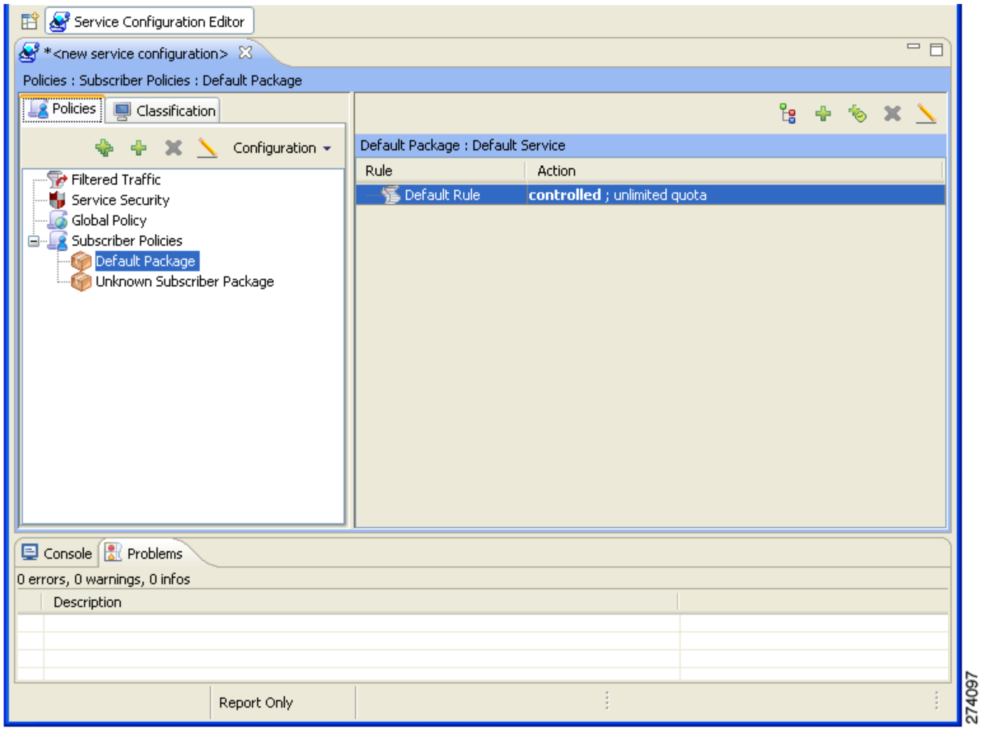
These parameters are defined when you add a new package (see How to Add Packages, page 9-55). You can modify them at any time (see How to Edit Packages, page 9-59).

How to View Packages

You can view a hierarchy tree of all existing packages, and you can see a list of services for which specific rules are defined for any selected package.

Step 1 In the current service configuration, click the **Policies** tab (Figure 9-40).

Figure 9-40 Policies Tab


Service Configuration Editor
*<new service configuration>
Policies : Subscriber Policies : Default Package
Policies
Classification
Configuration
Filtered Traffic
Service Security
Global Policy
Subscriber Policies
Default Package
Unknown Subscriber Package
Default Package : Default Service
Rule
Action
Default Rule
controlled ; unlimited quota
Console
Problems
0 errors, 0 warnings, 0 infos
Description
Report Only
274097

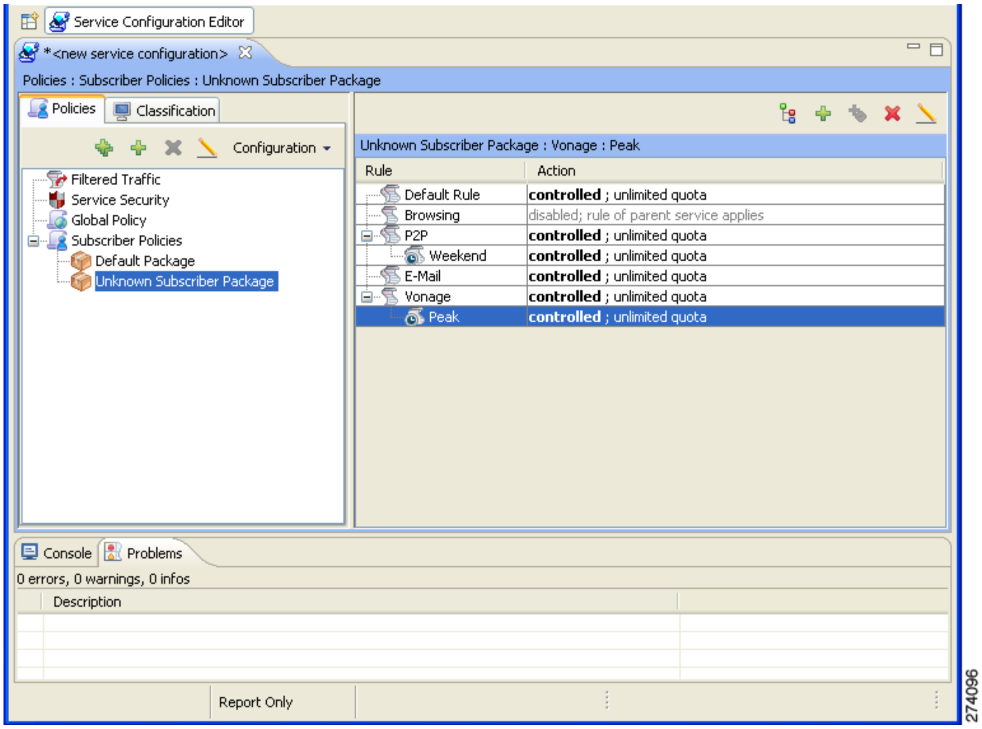
A list of all packages is displayed in the package tree.

Note To view more information about a package, open the Package Settings dialog box (see How to Edit Packages, page 9-59).

Step 2 Click a package in the hierarchy to display the rules of the package.

A list of all rules of this package is displayed in the right (Rule) pane (Figure 9-41).

Figure 9-41 Service Configuration Editor



Policies : Subscriber Policies : Unknown Subscriber Package

- Filtered Traffic
- Service Security
- Global Policy
- Subscriber Policies
  - Default Package
  - Unknown Subscriber Package

Unknown Subscriber Package : Vonage : Peak

Rule	Action
Default Rule	**controlled** ; unlimited quota
Browsing	disabled; rule of parent service applies
P2P	**controlled** ; unlimited quota
Weekend	**controlled** ; unlimited quota
E-Mail	**controlled** ; unlimited quota
Vonage	**controlled** ; unlimited quota
Peak	**controlled** ; unlimited quota

0 errors, 0 warnings, 0 infos

Description

How to Add Packages

A default package is predefined in the Console installation. You can add additional packages to a service configuration, subject to the limit of 5000 packages per service configuration.

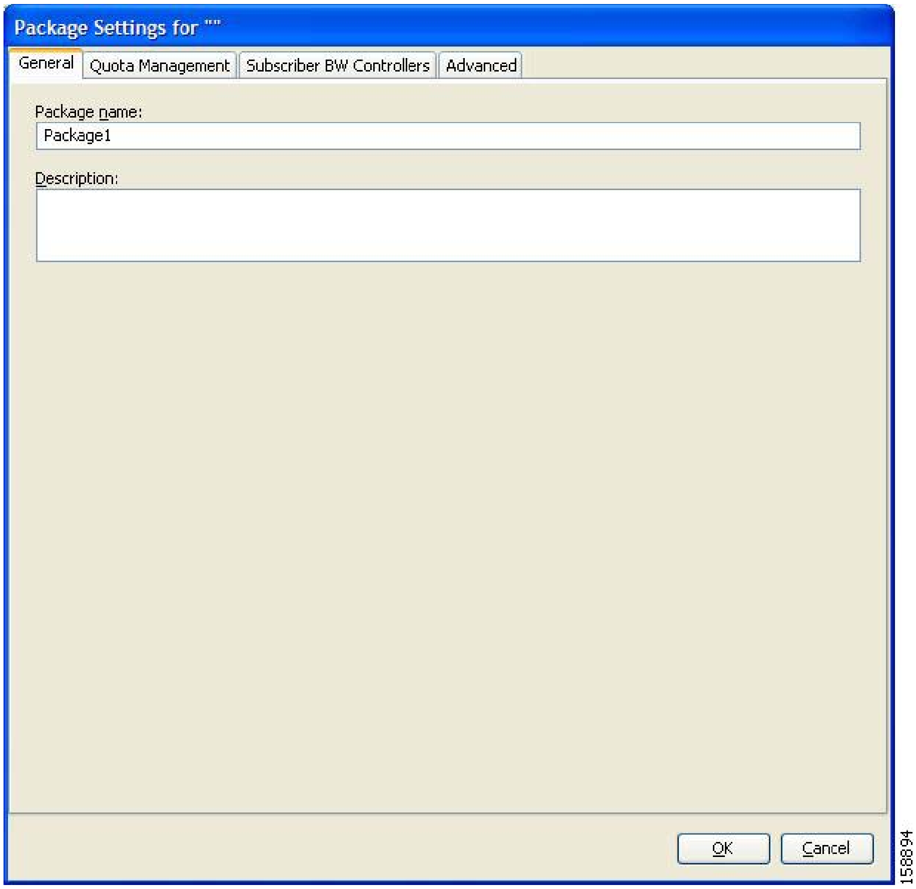
After you have added a new package, you can define rules for the package (see How to Add Rules to a Package, page 9-63).

Step 1 In the Policies tab, select a package from the package tree. This package is the parent of the package you are adding.

Step 2 In the Policies tab, click the **Add Package** (✚) icon.

The Package Settings dialog box appears (Figure 9-42).

Figure 9-42 Package Settings


Package Settings for ""

Package name: Package1

Description:

Step 3 In the Package name field, enter a unique and relevant name for the package.

Step 4 (Optional) In the Description field, enter a meaningful and useful description of the package.

Step 5 To configure parameters in the Advanced tab, continue with the instructions in the following section.

Step 6 Click **OK**.

The Package Settings dialog box closes.

The new package is added as a child to the package selected in the package tree and becomes the selected package. The default service rule is displayed in the right (Rule) pane.

To edit the default service rule, and to add new rules to the package, see Managing Rules, page 9-61.

What to Do Next

To configure parameters in the Quota Management tab see How to Edit Quota Management Settings for Packages, page 9-91.

To configure parameters in the Subscriber BW Controllers tab, see How to Edit Package Subscriber BWCs, page 9-30.

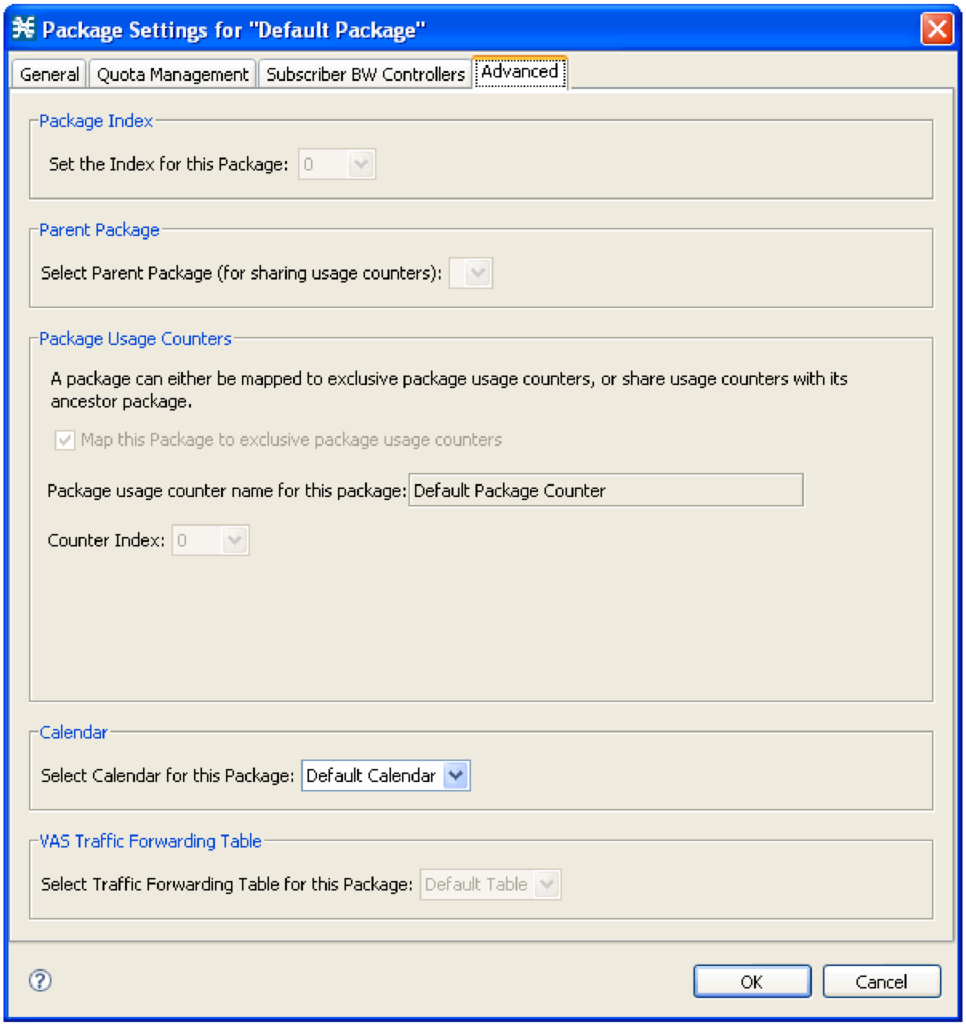
How to Set Advanced Package Options

You can change the index for the package, specify an exclusive usage counter, or select a calendar for the package in the Advanced tab.

Step 1 In the Package Settings dialog box, click the **Advanced** tab.

The Advanced tab opens (Figure 9-43).

Figure 9-43 Advanced Tab



Package Settings for "Default Package"

Package Index

Set the Index for this Package: 0

Parent Package

Select Parent Package (for sharing usage counters):

Package Usage Counters

A package can either be mapped to exclusive package usage counters, or share usage counters with its ancestor package.

☑ Map this Package to exclusive package usage counters

Package usage counter name for this package: Default Package Counter

Counter Index: 0

Calendar

Select Calendar for this Package: Default Calendar

VAS Traffic Forwarding Table

Select Traffic Forwarding Table for this Package: Default Table

Step 2 To change the package index for this package, from the Set the Index for this Package drop-down list, select a package index.

Note The system provides a default value of the index. Do not modify this value unless a specific index value must be assigned to the package.

Step 3 To set a different parent package for this package, select the desired parent from the Select Parent Package drop-down list.

Step 4 By default, a new package uses an exclusive usage counter. To share the parent package usage counter, uncheck the **Map this Service to exclusive package usage counters** check box.

The name in the read-only Package usage counter name for this package field changes to reflect your choice.

The Counter Index drop-down list is dimmed.

Step 5 To change the counter index (if you are using an exclusive package usage counter), select a value for the index from the Counter Index drop-down list.

Note The system provides a default value of the index. Do not modify this value.

Step 6 To set a calendar for this package (to use its time frames for time-based rules), select the desired calendar from the Select Calendar for this Package drop-down list.

Step 7 To set a VAS traffic-forwarding table for this package, select the desired traffic-forwarding table from the Select Traffic Forwarding Table for this Package drop-down list.

Note If VAS traffic forwarding is disabled (the default), the drop-down list is dimmed. To enable VAS traffic forwarding, see How to Enable VAS Traffic Forwarding, page 10-67.

Step 8 Click **OK**.

The Package Settings dialog box closes.

The new package is added as a child to the selected parent package and becomes the selected package. The default service rule is displayed in the right (Rule) pane.

To edit the default service rule, and to add new rules to the package, see Managing Rules, page 9-61.

How to Duplicate Packages

Duplicating an existing package is a useful way to create a new package similar to an existing package. It is faster to duplicate a package and then modify it than to define the package from beginning.

A duplicated package is added at the same level in the package tree as the original package.

Step 1 In the Policies tab, select a package from the package tree.

Step 2 In the Policies tab, click the **Duplicate Package** (✚) icon.

A duplicate package is created with all the same attributes as the original package. If the package is duplicated several times, the name of the new package is the name of the selected package followed by “(1)”, “(2)”, and so on.

Step 3 Modify the package parameters (see How to Edit Packages, page 9-59).

How to Edit Packages

You can modify the parameters of a package (including the default package) at any time.

Step 1 In the Policies tab, select a package from the package tree.

Step 2 In the Policies tab, click the **Edit Package** (✎)icon.

The Package Settings dialog box appears.

Step 3 In the Package name field, enter a new name for the package.

Step 4 In the Description field, enter a new description of the package.

Step 5 (Optional) Change quota management settings, see Editing Package Quota Management Settings (Using the Quota Management Tab (Packages) How to Edit Quota Management Settings for Packages, page 9-91.

Step 6 (Optional) Change bandwidth control settings, see How to Edit Package Subscriber BWCs, page 9-30.

Step 7 To change advanced settings, click the Advanced tab.

The Advanced tab opens.

a. To change the package index for this package, from the Set the Index for this Package drop-down list, select a Package Index.

Note The system provides a default value of the counter index. Do not modify this value unless a specific index value must be assigned to the package.

b. To change the parent package of this package, select the desired parent from the Select Parent Package drop-down list.

c. To share the parent package usage counter, uncheck the **Map this Service to exclusive package usage counters** check box.

The name in the read-only Package usage counter name for this package field changes to reflect your choice.

The Counter Index drop-down list is dimmed.

d. To use an exclusive package usage counter, check the **Map this Service to exclusive package usage counters** check box.

The name in the read-only Package usage counter name for this package field changes to reflect your choice.

The Counter Index drop-down list is dimmed.

e. To change the counter index if you are using the exclusive package usage counter, select a value for the index from the Counter Index drop-down list.

Note The system provides a default value of the counter index. Do not modify this value.

f. To change the calendar used by this package, select the desired calendar from the Select Calendar for this Package drop-down list.

g. To change the VAS traffic-forwarding table for this package, select the desired traffic-forwarding table from the Select Traffic Forwarding Table for this Package drop-down list.

Note If VAS traffic forwarding is disabled (the default), the drop-down list is dimmed. To enable VAS traffic forwarding, see How to Enable VAS Traffic Forwarding, page 10-67.

Step 8 Click **OK**.

The Package Settings dialog box closes.

All changes to the package parameters are saved.

How to Delete Packages

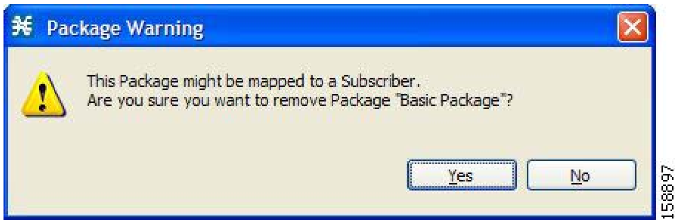
You can delete user-defined packages. The default package cannot be deleted.

Step 1 In the Policies tab, select a package from the package tree.

Step 2 In the Policies tab, click the **Delete Package** (✖) icon.

A Package Warning message appears (Figure 9-44).

Figure 9-44 Package Warning



Package Warning

This Package might be mapped to a Subscriber.
Are you sure you want to remove Package "Basic Package"?

Step 3 Click **Yes**.

The package is deleted and is no longer displayed in the package tree.

Managing Rules

After you have defined services and basic packages, you can define rules for the package.

You can configure rules to do some or all of the following:

- Block the service
- Define maximum bandwidth for the service
- Change the DSCP ToS value of packets in a flow
- Set a quota for the service
- Define behavior when the quota for this service is breached

A rule usually applies at all times. To allow additional flexibility, you can divide the week into four separate time frames. You can define subrules—time-based rules—for each time frame.

Note In Cisco SCA BB, the maximum number of unique rules that can be applied is limited to 5000. If the number of unique rules exceeds the maximum limit, an error occurs. The number of unique rules are identified from the Package ID, Service, and Timeframe fields.

The Default Service Rule

A default service rule is assigned to every package. It cannot be deleted or disabled.

The default values of this rule are:

- Admit (do not block) traffic.
- Map traffic to the default BWCs.
- Do not limit quotas for either upstream or downstream traffic.

Rule Hierarchy

The SCE platform applies the most specific rule to any flow.

For example, if you define rules for E-Mail and POP3:

- Any flow mapped to the SMTP or IMAP service is handled according to the e-mail rule.

- Any flow mapped to the POP3 service is handled according to the POP3 rule

This means, for example, that POP3 can have its own usage limits, whereas SMTP and IMAP must share usage limits.

Note If you add a rule for a child service, the settings for the parent rule are not copied to the new rule. All new rules start with default values.

Indicates any rule that also applies to child services.

Indicates any rule that does not apply to any child services.

Time-based rules are shown as children of the relevant rule. The icon for a time-based rule also shows if the rule applies to child services (or).

See also How to Display the Services Affected by a Rule, page 9-70.

How to View the Rules of a Package

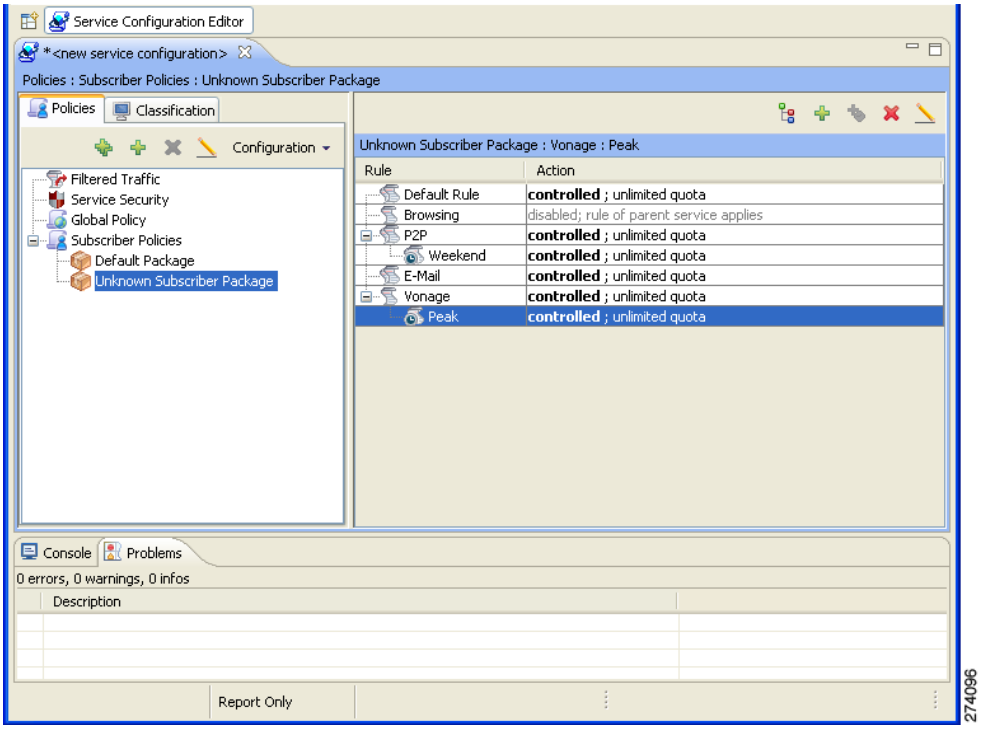
You can view a list of the rules of a package.

The listing for each rule includes an icon, the name of the service or group of services to which the rule applies, whether the rule is enabled or disabled, and a brief description of the rule.

Step 1 In the Policies tab, select a package from the package tree.

A list of all rules defined for this package is displayed in the right (Rule) pane (Figure 9-45).

Figure 9-45 Service Configuration Editor



Policies : Subscriber Policies : Unknown Subscriber Package

- Filtered Traffic
- Service Security
- Global Policy
- Subscriber Policies
  - Default Package
  - Unknown Subscriber Package

Unknown Subscriber Package : Vonage : Peak

Rule	Action
Default Rule	**controlled** ; unlimited quota
Browsing	disabled; rule of parent service applies
P2P	**controlled** ; unlimited quota
Weekend	**controlled** ; unlimited quota
E-Mail	**controlled** ; unlimited quota
Vonage	**controlled** ; unlimited quota
Peak	**controlled** ; unlimited quota

0 errors, 0 warnings, 0 infos

Description

What to Do Next

To see more information about a rule, open the Edit Rule for Service dialog box (see How to Edit Rules, page 9-68).

To see more information about a time-based rule, open the Edit Time-Based Rule for Service dialog box (see How to Edit Time-Based Rules, page 9-74).

How to Add Rules to a Package

A default service rule is assigned to every package. You can add additional rules to a package.

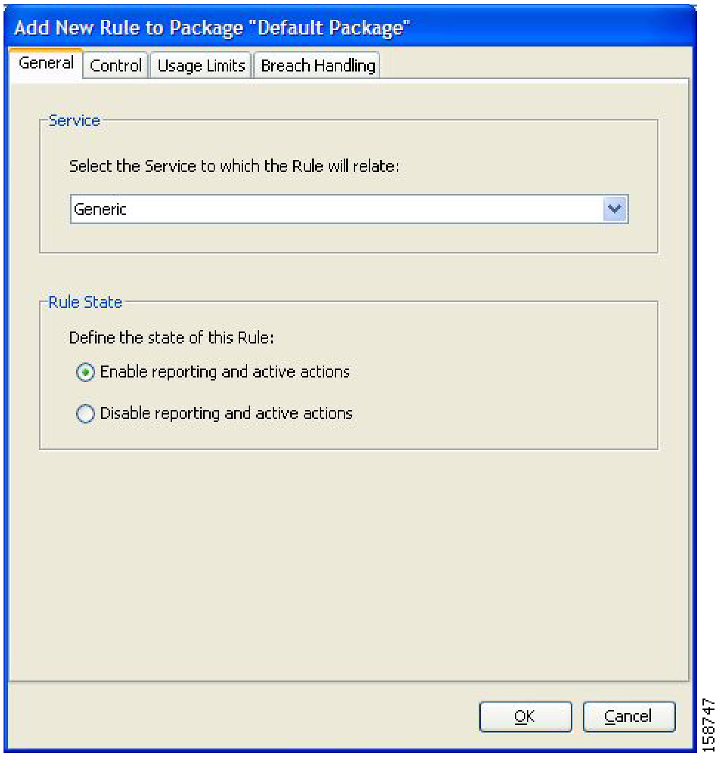
Adding time-based rules is described in the section How to Add Time-Based Rules to a Rule, page 9-72.

Step 1 In the Policies tab, select a package from the package tree.

Step 2 In the right (Rule) pane, click the **Add Rule** (✚) icon.

The Add New Rule to Package dialog box appears (Figure 9-46).

Figure 9-46 Add New Rule to Package



Service

Select the Service to which the Rule will relate: Generic

Rule State

Define the state of this Rule:

● Enable reporting and active actions

○ Disable reporting and active actions

Step 3 In the Service area of the Add New Rule to Package dialog box, select a service from the Select the Service to Which the Rule Relates drop-down list.

Note Services for which a rule is already defined for this package are dimmed.

Step 4 In the Rule State area, select one of the **Define the State of this Rule** radio buttons.

- **Enable reporting and active actions**
- **Disable reporting and active actions**

> **Note** You can enable or disable a rule at any time (see How to Edit Rules, page 9-68).

Step 5 (Optional) Set behavior per traffic flow for this rule, continue with the instructions in the section How to Define Per-Flow Actions for a Rule, page 9-66.

Step 6 Click **OK**.

The Add New Rule to Package dialog box closes.

The new rule is added to the list of rules displayed in the right (Rule) pane.

What to Do Next

Usage limits and breach handling are part of quota management (see Managing Quotas, page 9-83):

- To configure parameters in the Usage Limits tab, see How to Select Quota Buckets for Rules, page 9-93.
- To configure parameters in the Breach Handling tab, see How to Edit Breach-Handling Parameters for a Rule, page 9-94.

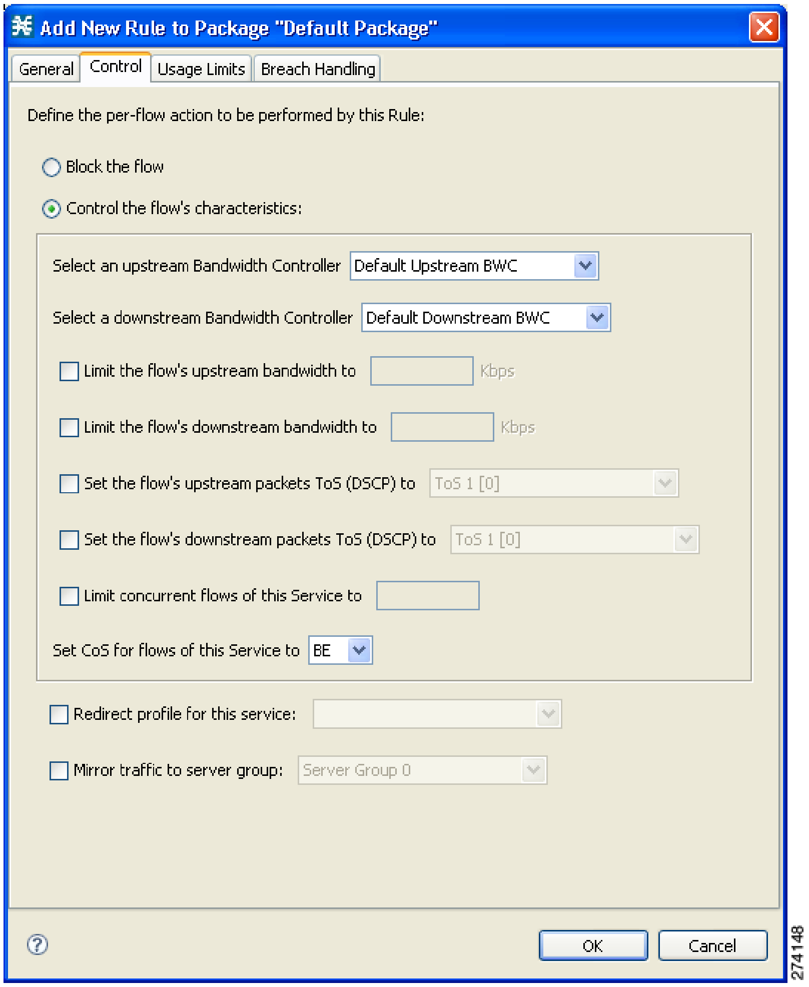
How to Define Per-Flow Actions for a Rule

The Control tab of the Add New Rule to Package dialog box allows you to set behavior per traffic flow for sessions that are mapped to the current service.

Step 1 In the Add New Rule to Package dialog box, click the **Control** tab.

The Control tab opens (Figure 9-47).

Figure 9-47 Control Tab



Add New Rule to Package "Default Package"

Define the per-flow action to be performed by this Rule:

○ Block the flow

● Control the flow's characteristics:

Select an upstream Bandwidth Controller: Default Upstream BWC

Select a downstream Bandwidth Controller: Default Downstream BWC

□ Limit the flow's upstream bandwidth to ____ Kbps

□ Limit the flow's downstream bandwidth to ____ Kbps

□ Set the flow's upstream packets ToS (DSCP) to ToS 1 [0]

□ Set the flow's downstream packets ToS (DSCP) to ToS 1 [0]

□ Limit concurrent flows of this Service to ____

Set CoS for flows of this Service to BE

□ Redirect profile for this service:

□ Mirror traffic to server group: Server Group 0

To control flows that are mapped to the service of this rule, continue at Step 3.

Step 2 To block flows that are mapped to the service of this rule, select the **Block the flow** radio button and continue at Step 12.

Step 3 Select the **Control the flow's characteristics** radio button.

The options in the Flow Characteristic area are enabled.

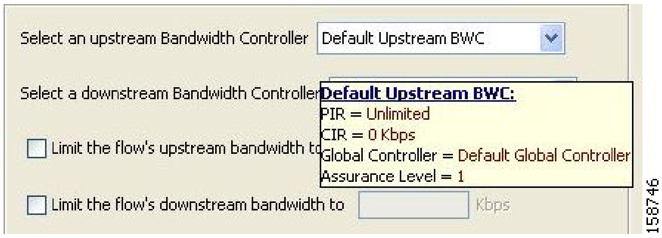
Step 4 From the upstream Bandwidth Controller drop-down list, select an upstream BWC. This sets up bandwidth metering of all concurrent flows mapped to this rule, based on the characteristics of the selected BWC.

The BWCs in this drop-down list are defined when creating or editing the package.

Caution For time-based rules: If you need different global controller settings for different time frames, define maximum bandwidths per time frame for one global controller. Do not create a separate global controller for each time frame.

When the mouse is placed over the drop-down list, a tooltip appears (Figure 9-48). The tool tip contains the properties of the selected BWC, such as Peak Information Rate [PIR], Committed Information Rate [CIR], Global Controller, and Assurance Level.

Figure 9-48 Drop-Down List Tips



Select an upstream Bandwidth Controller: Default Upstream BWC

Select a downstream Bandwidth Controller

Default Upstream BWC:
PIR = Unlimited
CIR = 0 Kbps
Global Controller = Default Global Controller
Assurance Level = 1

□ Limit the flow's upstream bandwidth to

□ Limit the flow's downstream bandwidth to Kbps

Step 5 From the downstream Bandwidth Controller drop-down list, choose a downstream BWC.

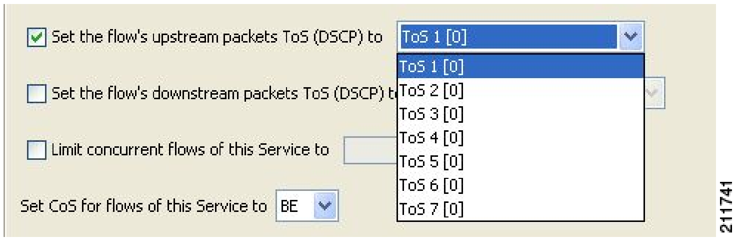
Step 6 (Optional) To set a per-flow upstream bandwidth limit, check the **Limit the flow's upstream bandwidth** check box and enter a value in the Kbps field.

Note Per-flow bandwidth has a granularity of 1 Kbps up to 57 Mbps.

Step 7 (Optional) To set a per-flow downstream bandwidth limit, check the **Limit the flow's downstream bandwidth** check box and enter a value in the Kbps field.

Step 8 (Optional) To change the DSCP ToS marker of all packets in upstream flows, check the **Set the flow's upstream packets ToS (DSCP) to** check box and select a value from the drop-down list (Figure 9-49).

Figure 9-49 Drop Down List Values



☑ Set the flow's upstream packets ToS (DSCP) to: ToS 1 [0]

□ Set the flow's downstream packets ToS (DSCP) to

□ Limit concurrent flows of this Service to

Set CoS for flows of this Service to: BE

Step 9 (Optional) To change the DSCP ToS marker of all packets in downstream flows, check the **Set the flow's downstream packets ToS (DSCP) to** check box and select a value from the drop-down list.

Step 10 (Optional) To set the maximum number of concurrent flows (mapped to this rule) permitted to a subscriber, check the **Limit concurrent flows of this Service** check box and enter a value in the associated field.

Step 11 From the Set CoS for flows of this Service drop-down list, select a class-of-service.

Step 12 (Optional) To enable subscriber redirection, check the **Redirect profile for this service** check box and choose a redirect profile from the drop-down list.

Step 13 (Optional) To enable traffic mirroring, check the **Mirror traffic to server group** check box and choose a server group from the drop-down list.

Note The Mirror traffic to server group check box is only enabled when Traffic Mirroring is enabled in the VAS Settings dialog box.

Step 14 Click **OK**.

The Add New Rule to Package dialog box closes.

The new rule is added to the list of rules displayed in the right (Rule) pane.

How to Edit Rules

You can edit any rule, including the default service rule.

Note You cannot disable the default service rule.

Note The tabs of the Edit Rule for Service dialog box are the same as the tabs of the Add New Rule to Package dialog box, except for the General tab—you cannot change the service to which the rule applies.

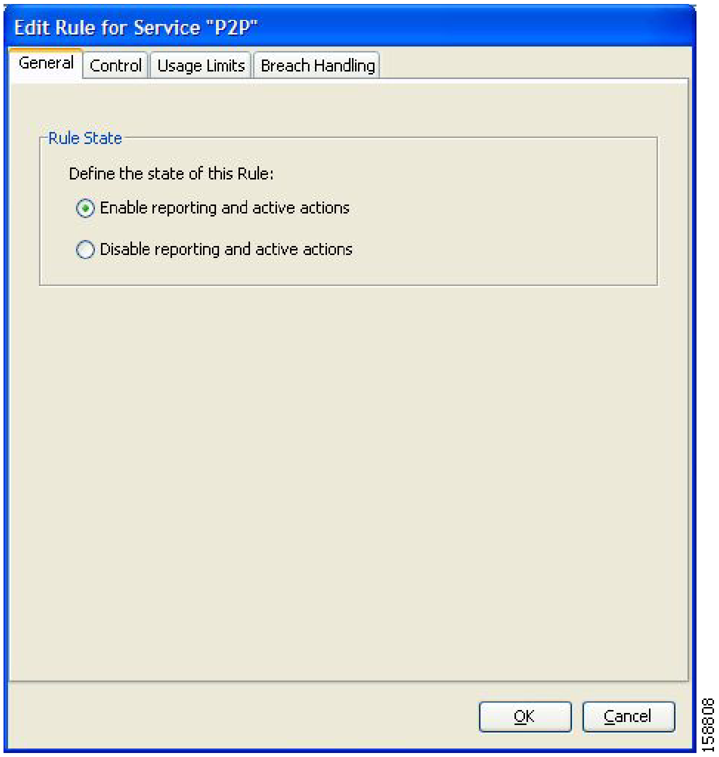
Step 1 In the Policies tab, select a package from the package tree.

Step 2 In the right (Rule) pane, select a rule.

Step 3 Click ✎ (**Edit Rule**).

The Edit Rule for Service dialog box appears (Figure 9-50).

Figure 9-50 Edit Rule for Service



Edit Rule for Service "P2P"

Rule State

Define the state of this Rule:

● Enable reporting and active actions

○ Disable reporting and active actions

Step 4 In the Rule State area, select one of the **Define the State of this Rule** radio buttons.

- **Enable reporting and active actions**
- **Disable reporting and active actions**

Step 5 Change behavior per traffic flow.

a. Click the **Control** tab.

The Control tab opens.

b. Follow the instructions in How to Define Per-Flow Actions for a Rule, page 9-66.

Step 6 Change usage limits.

a. Click the **Usage Limits** tab.

The Usage Limits tab opens.

b. Follow the instructions in How to Select Quota Buckets for Rules, page 9-93.

Step 7 Define behavior when a quota is breached.

a. Click the **Breach Handling** tab.

The Breach Handling tab opens.

b. Follow the instructions in How to Edit Breach-Handling Parameters for a Rule, page 9-94.

Step 8 Click **OK**.

The Edit Rule for Service dialog box closes.

All changes to the rule are saved.

How to Delete Rules

You can delete any user-defined rule. The default service rule cannot be deleted.

Note You can *disable* a rule without losing its profile. For details, see Step 4 of How to Edit Rules, page 9-68. This feature allows you to enable the rule again later, without having to reset all its parameters. You cannot disable the default service rule.

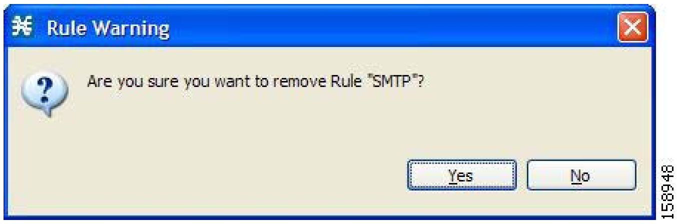
Step 1 In the Policies tab, select a package from the package tree.

Step 2 In the right (Rule) pane, select a rule.

Step 3 In the Rule pane, click the **Delete Rule** (✖) icon.

A Rule Warning message appears (Figure 9-51).

Figure 9-51 Rule Warning



Rule Warning

Are you sure you want to remove Rule "SMTP"?

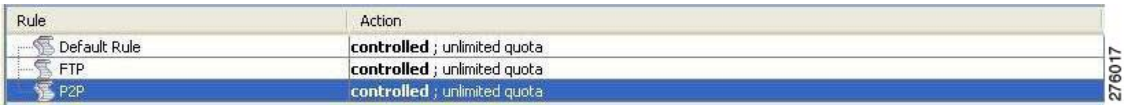
Step 4 Click **Yes**.

The selected rule is deleted.

How to Display the Services Affected by a Rule

You can define a service as the child of another service (the parent service is a service group). Until you define a separate rule for a child service, the rule of the parent service applies to the child service. A rule that affects any of child services of a service is indicated in the rules list by a different icon, as illustrated for the P2P rule and the FTP rule in Figure 9-52.

Figure 9-52 Rules



Rule	Action
Default Rule	**controlled** ; unlimited quota
FTP	**controlled** ; unlimited quota
P2P	**controlled** ; unlimited quota

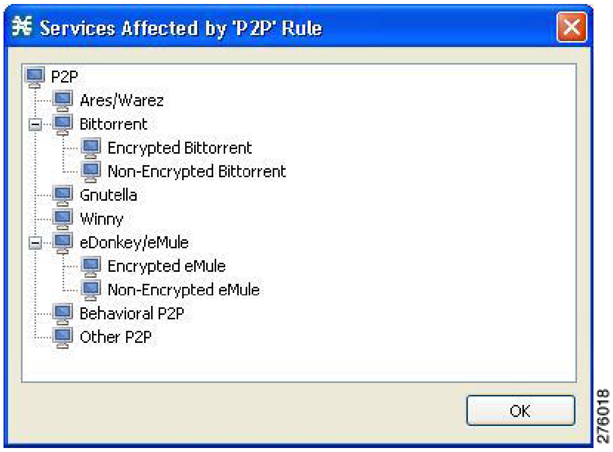
You can display all (child) services that are affected by a rule.

Note The default service rule applies to all services for which a specific rule is *not* defined.

Step 1 In the right (Rule) pane of the Policies tab, select a rule and click the **Show All Services Affected By This Rule** (🖧).

The Services Affected dialog box appears (Figure 9-53).

Figure 9-53 Services Affected



Services Affected by 'P2P' Rule

- P2P
  - Ares/Warez
  - Bittorrent
    - Encrypted Bittorrent
    - Non-Encrypted Bittorrent
  - Gnutella
  - Winny
  - eDonkey/eMule
    - Encrypted eMule
    - Non-Encrypted eMule
  - Behavioral P2P
  - Other P2P

Step 2 Click **OK**.

The Services Affected dialog box closes.

Managing Time-Based Rules

The Console allows you to divide the week into four time frames (see Managing Calendars, page 9-76). A time-based rule is a rule that applies to one time frame.

You can add time-based rules to any rule. If a time-based rule is not defined for a time frame, the parent rule is enforced.

Often, you want the rules for the different time frames to be similar. When you add a time-based rule, the settings of the parent rule are copied to the new time-based rule; you can make any needed changes. Subsequent changes to the parent rule do not affect the time-based rule.

You must define the calendar before defining the related time-based rules.

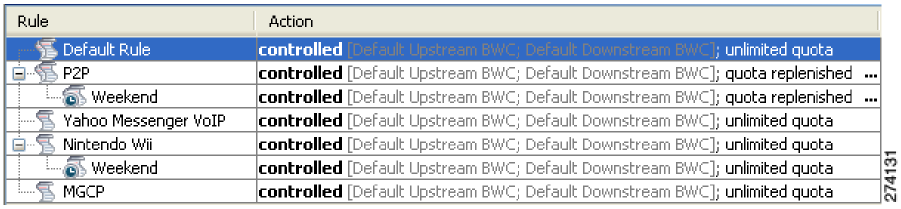
How to Add Time-Based Rules to a Rule

Adding a time-based rule to a rule allows you to specify alternate rule parameters applicable only for a specific time frame. If a time-based rule is not defined for a time frame, the parent rule is enforced.

- When you add a time-based rule, all parameters are initially set to the values defined for the parent rule. Subsequent changes to the parent rule do not change the time-base rule.
- The tabs of the Add New Time-Based Rule dialog box are the same as the tabs of the Add New Rule to Package dialog box, except for the General tab. In the Add New Rule to Package dialog box, you select a service; in the Add New Time-Based Rule dialog box, you select a time frame.

A service whose time-based rule affects any of its child services is indicated in the rules list by a modified icon, as illustrated for the Weekend time-based rule of the P2P rule in Figure 9-54.

Figure 9-54 P2P Weekend Based Time Rule



Rule	Action
Default Rule	**controlled** [Default Upstream BWC; Default Downstream BWC]; unlimited quota
P2P	**controlled** [Default Upstream BWC; Default Downstream BWC]; quota replenished ...
Weekend	**controlled** [Default Upstream BWC; Default Downstream BWC]; quota replenished ...
Yahoo Messenger VoIP	**controlled** [Default Upstream BWC; Default Downstream BWC]; unlimited quota
Nintendo Wii	**controlled** [Default Upstream BWC; Default Downstream BWC]; unlimited quota
Weekend	**controlled** [Default Upstream BWC; Default Downstream BWC]; unlimited quota
MGCP	**controlled** [Default Upstream BWC; Default Downstream BWC]; unlimited quota

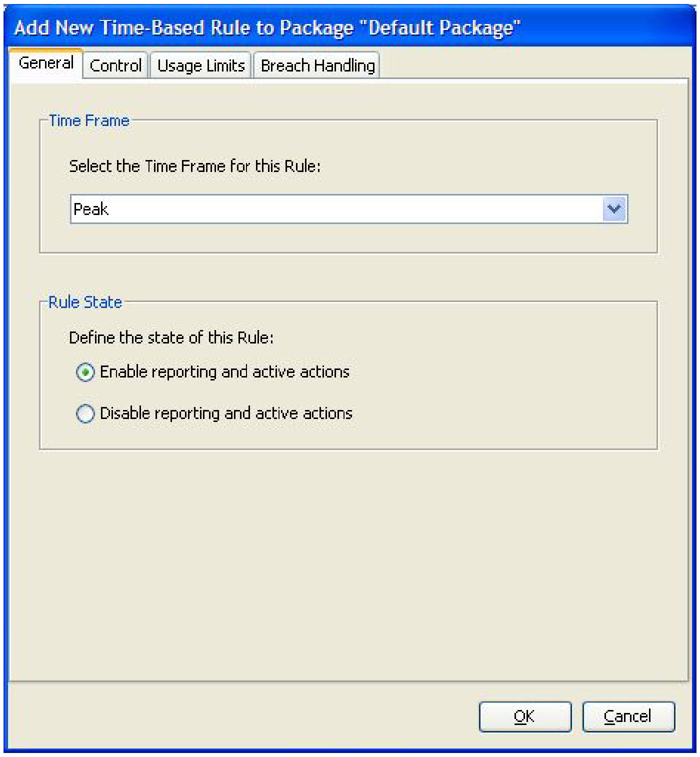
Step 1 In the Policies tab, select a package from the package tree.

Step 2 In the right (Rule) pane, select a rule.

Step 3 Click the **Add Time-Based Rule** ( ) icon.

The Add New Time-Based Rule dialog box appears (Figure 9-55).

Figure 9-55 Add New Time-Based Rule



Add New Time-Based Rule to Package "Default Package"

Time Frame

Select the Time Frame for this Rule:

Peak

Rule State

Define the state of this Rule:

● Enable reporting and active actions

○ Disable reporting and active actions

158748

Step 4 In the Time Frame area, from the Select the Time Frame for this Rule drop-down list, select one of the four time frames.

Step 5 In the Rule State area, select one of the **Define the State of this Rule** radio buttons.

- **Enable reporting and active actions**
- **Disable reporting and active actions**

Step 6 Define behavior per traffic flow.

a. Click the **Control** tab.

The Control tab opens.

b. Follow the instructions in How to Define Per-Flow Actions for a Rule, page 9-66.

Step 7 Change usage limits.

a. Click the **Usage Limits** tab.

The Usage Limits tab opens.

b. Follow the instructions in How to Select Quota Buckets for Rules, page 9-93.

Step 8 Define behavior when a quota is breached.

a. Click the **Breach Handling** tab.

The Breach Handling tab opens.

b. Follow the instructions in How to Edit Breach-Handling Parameters for a Rule, page 9-94.

Step 9 Click **OK**.

The Add New Time-Based Rule dialog box closes.

The new time-based rule is displayed as a child of the rule in the Rule pane.

How to Edit Time-Based Rules

You can edit time-based rules.

Note The tabs of the Edit Time-Based Rule for Service dialog box are the same as the tabs of the Add New Time-Based Rule dialog box, except for the General tab. You cannot change the time frame to which the rule applies.

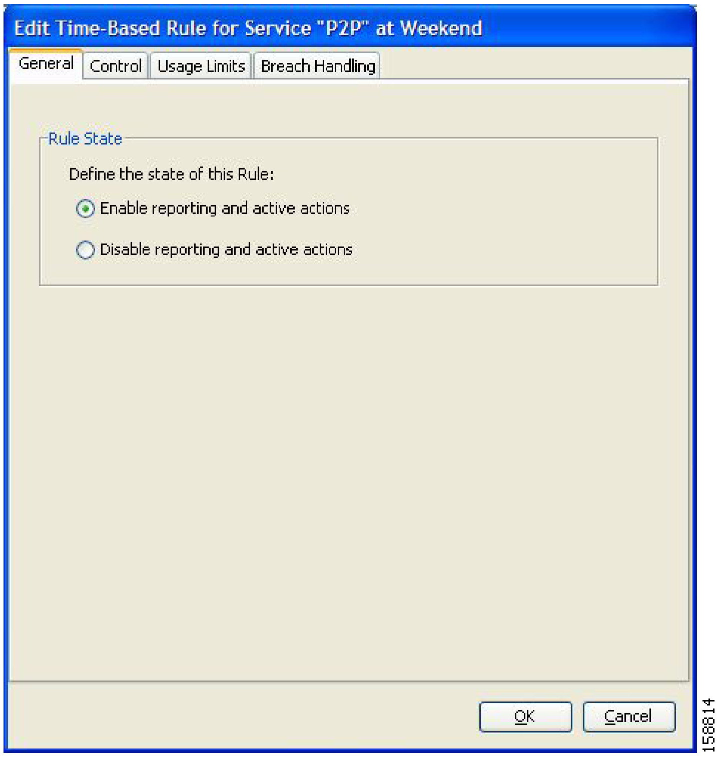
Step 1 In the Policies tab, select a package from the package tree.

Step 2 In the right (Rule) pane, select a time-based rule.

Step 3 Click the **Edit Rule** (✎) icon.

The Edit Time-Based Rule for Service dialog box appears (Figure 9-56).

Figure 9-56 Edit Time-Based Rule for Service



Edit Time-Based Rule for Service "P2P" at Weekend

Rule State

Define the state of this Rule:

● Enable reporting and active actions

○ Disable reporting and active actions

Step 4 In the Rule State area, select one of the **Define the State of this Rule** radio buttons.

- **Enable reporting and active actions**
- **Disable reporting and active actions**

Step 5 Define behavior per traffic flow.

a. Click the **Control** tab.

The Control tab opens.

b. Follow the instructions in How to Define Per-Flow Actions for a Rule, page 9-66.

Step 6 Change usage limits.

a. Click the **Usage Limits** tab.

The Usage Limits tab opens.

b. Follow the instructions in How to Select Quota Buckets for Rules, page 9-93.

Step 7 Define behavior when a quota is breached.

a. Click the **Breach Handling** tab.

The Breach Handling tab opens.

b. Follow the instructions in How to Edit Breach-Handling Parameters for a Rule, page 9-94.

Step 8 Click **OK**.

The Edit Time-Based Rule for Service dialog box closes.

All changes to the time-based rule are saved.

How to Delete Time-Based Rules

You can delete any time-based rule.

Note You can *disable* a rule without losing its profile (see How to Edit Time-Based Rules, page 9-74). This allows you to enable the rule again later, without having to reset all its parameters.

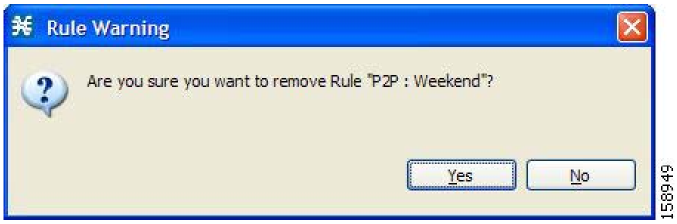
Step 1 In the Policies tab, select a package from the package tree.

Step 2 In the right (Rule) pane, select a time-based rule.

Step 3 In the Rule pane, click the **Delete Rule** (✖) icon.

A Rule Warning message appears (Figure 9-57).

Figure 9-57 Rule Warning



Are you sure you want to remove Rule "P2P : Weekend"?

Step 4 Click **Yes**.

The selected rule is deleted.

Managing Calendars

Calendars are used to divide the hours of the week into four time frames.

After you have configured a calendar, you can add time-based rules to a package that uses the calendar. A time-based rule is a rule that applies to only one time frame. Time-based rules allow you to set rule parameters that apply only at specific times. You might, for example, want to define different rules for peak, off-peak, nighttime, and weekend usage.

Each service configuration includes one default calendar. You can add nine more calendars, each with a different time-frame configuration. You can use different calendars for different packages. You can also use different calendars where a service provider has customers in more than one time zone by configuring calendars with a one-hour offset from each other.

- How to View Calendars, page 9-76
- How to Add Calendars, page 9-77
- How to Rename the Time Frames, page 9-77
- How to Delete Calendars, page 9-78
- How to Configure the Time Frames, page 9-79

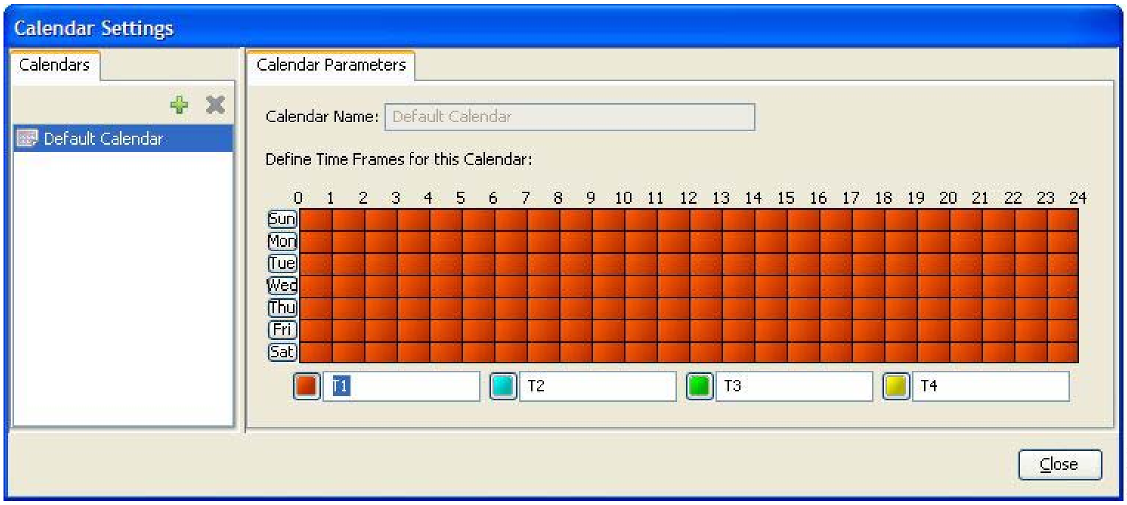
How to View Calendars

You can view a list of existing calendars and their time frames.

Step 1 From the Policies tab of the left pane, choose **Configuration > Policies > Weekly Calendars**.

The Calendar Settings dialog box appears (Figure 9-58).

Figure 9-58 Calendar Settings


Calendar Settings

Calendars

Default Calendar

Calendar Parameters

Calendar Name: Default Calendar

Define Time Frames for this Calendar:

🟥 T1
🟦 T2
🟩 T3
🟨 T4

The Calendars tab displays a list of existing calendars. Click a calendar in the list to display its time-frame settings.

The time frames for the selected calendar are displayed and configured in the Calendar Parameters tab.

Step 2 Click **Close**.

The Calendar Settings dialog box closes.

How to Add Calendars

Each service configuration includes one default calendar. You can add up to nine more calendars.

Step 1 From the Policies tab of the left pane, choose **Configuration > Policies > Weekly Calendars**.

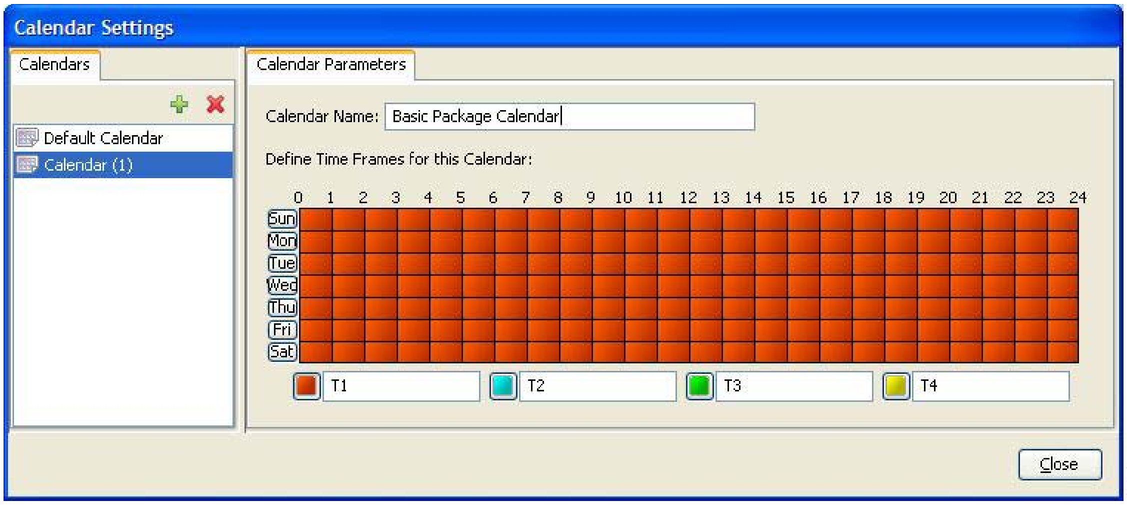
The Calendar Settings dialog box appears.

Step 2 In the Calendar tab, click the **Add** (✚) icon.

A new calendar is added with the name Calendar (1).

Step 3 In the Calendar Parameters tab (Figure 9-59), click in the Calendar Name field and enter the name for this calendar.

Figure 9-59 Calendar Parameters Tab



Calendar Settings

Calendars: Default Calendar, Calendar (1)

Calendar Name: Basic Package Calendar

Define Time Frames for this Calendar:

Step 4 Click **Close**.

The Calendar Settings dialog box closes, and the new calendar name is saved.

How to Rename the Time Frames

By default, the time frames are named T1, T2, T3, and T4. You can change these names at any time; for example, you may want to name the time frames Peak, Off Peak, Night, and Weekend.

Note Although you can configure the time frames differently in each calendar, the names of the time frames are the same in all of the calendars. If you change the name when configuring one calendar, the names are also changed for all other calendars.

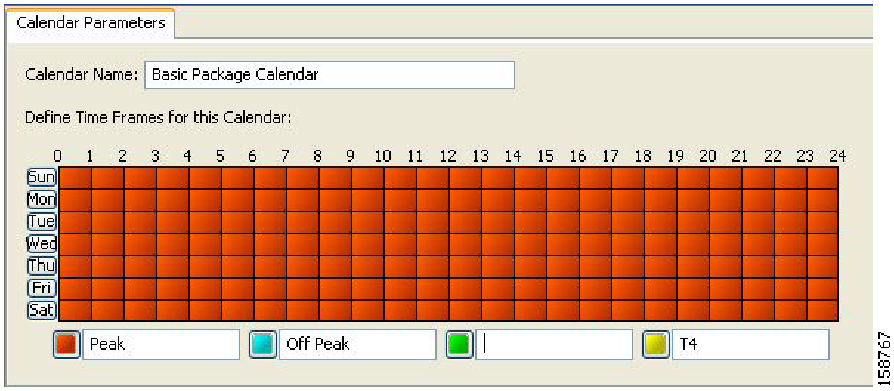
Step 1 From the Policies tab of the left pane, choose **Configuration > Policies > Weekly Calendars**.

The Calendar Settings dialog box appears.

In the Calendar Parameters tab (Figure 9-60), below the grid, each of the four time frames is listed in a field next to a colored square.

Step 2 Click in a Time Frame Name field, and enter a new name for the time frame.

Figure 9-60 Calendar Parameters Tab



Calendar Parameters

Calendar Name: Basic Package Calendar

Define Time Frames for this Calendar:

🟥 Peak
🟦 Off Peak
🟩 |
🟨 T4

Step 3 Repeat Step 2 for the other three time frames.

Step 4 Click **Close**.

The Calendar Settings dialog box closes, and the changes to the names of the time frames are saved.

How to Delete Calendars

You can delete any user-added calendar. The default calendar cannot be deleted.

Note A calendar used by a package cannot be deleted. (When you select the calendar, the Delete icon is dimmed.) To delete the calendar, you must first select a different calendar for each package using the calendar that is deleted.
See How to Set Advanced Package Options, page 9-57 for information about changing the calendar associated with a package.

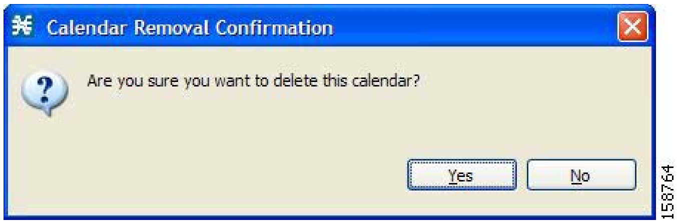
Step 1 From the Policies tab of the left pane, choose **Configuration > Policies > Weekly Calendars**.

The Calendar Settings dialog box appears.

Step 2 In the Calendar tab, select a calendar and click the **Delete** (✖) icon.

A Calendar Removal Confirmation message appears (Figure 9-61).

Figure 9-61 Calendar Removal Confirmation



Calendar Removal Confirmation

Are you sure you want to delete this calendar?

Step 3 Click **Yes**.

The calendar is deleted.

Step 4 Click **Close**.

The Calendar Settings dialog box closes.

How to Configure the Time Frames

By default, all the hours of the week belong to one time frame. The Console allows you to assign each of the 168 (24x7) hours of the week to one of four separate time frames. These time frames allow you to supply time-dependent differentiated services and to impose constraints on any service.

You might want, for example, to divide the week as follows:

- Peak
- Off Peak
- Night
- Weekend

You can define different time frames for each calendar.

Step 1 From the Policies tab of the left pane, choose **Configuration > Policies > Weekly Calendars**.

The Calendar Settings dialog box appears.

Step 2 In the Calendars tab, select a calendar to configure.

In the Calendar Parameters tab, the selected calendar's **Define Time Frames for this Calendar** grid is displayed. The grid, representing one week, is laid out in a format of 24 hours x 7 days. Each cell represents one hour.

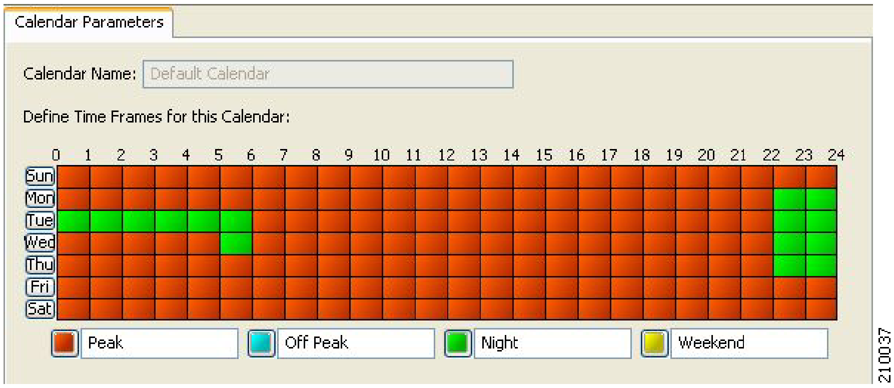
Below the grid, the name of each time frame appears next to a colored button.

Step 3 Click one of the colored buttons.

Step 4 Select all the cells in the grid that represent hours that are part of the selected time frame.

You can select a group of cells by holding down the mouse button and dragging across the cells (Figure 9-62).

Figure 9-62 Calendar Parameters Tab



Calendar Name: Default Calendar

Define Time Frames for this Calendar:

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sun	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
Mon	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩
Tue	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩
Wed	🟥	🟥	🟥	🟥	🟥	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩
Thu	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩
Fri	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
Sat	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥

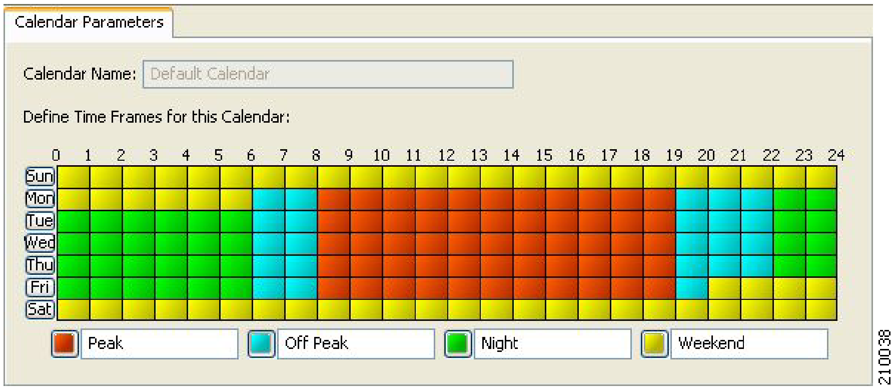
🟥 Peak 🟦 Off Peak 🟩 Night 🟨 Weekend

The changes are written to the service configuration as you make them.

Step 5 Repeat Steps 3 and 4 for the other time frames until you have mapped the entire grid.

You have now mapped the week into four different time frames. Figure 9-63 illustrates a possible time partition plan.

Figure 9-63 Time Partition Plan Example



Calendar Name: Default Calendar

Define Time Frames for this Calendar:

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sun	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Mon	🟨	🟨	🟨	🟨	🟨	🟨	🟦	🟦	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟦	🟦	🟦	🟩	🟩
Tue	🟩	🟩	🟩	🟩	🟩	🟩	🟦	🟦	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟦	🟦	🟦	🟩	🟩
Wed	🟩	🟩	🟩	🟩	🟩	🟩	🟦	🟦	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟦	🟦	🟦	🟩	🟩
Thu	🟩	🟩	🟩	🟩	🟩	🟩	🟦	🟦	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟦	🟦	🟦	🟩	🟩
Fri	🟩	🟩	🟩	🟩	🟩	🟩	🟦	🟦	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟦	🟨	🟨	🟨	🟨
Sat	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨

🟥 Peak 🟦 Off Peak 🟩 Night 🟨 Weekend

Step 6 Click **Close**.

The Calendar Settings dialog box closes.

How to Manage DSCP ToS Marker Values

Cisco SCA BB can change the value of the DSCP ToS marker of packets of flows that match a filter rule or a service rule.

For details on how to change the value of the DSCP ToS marker, see the following steps:

- For Filter Rule—see Step 11 of How to Add Filter Rules, page 10-27
- For Service Rule—see Steps 10 and 11 of How to Define Per-Flow Actions for a Rule, page 9-66 and Step 9 of How to Edit Breach-Handling Parameters for a Rule, page 9-94

Cisco SCA BB supports seven ToS Marker Classes. You assign each class a specific value to apply to the packets of a flow.

Note If you have used DSCP marking on a Cisco SCA BB release before 3.1.5 and you are converting your old service configurations, you must reconfigure the service configurations to obtain the same network behavior as in the former release.

DSCP ToS Marking

DSCP ToS marking is used in IP networks as a means to signal the type and priority of a flow between network elements.

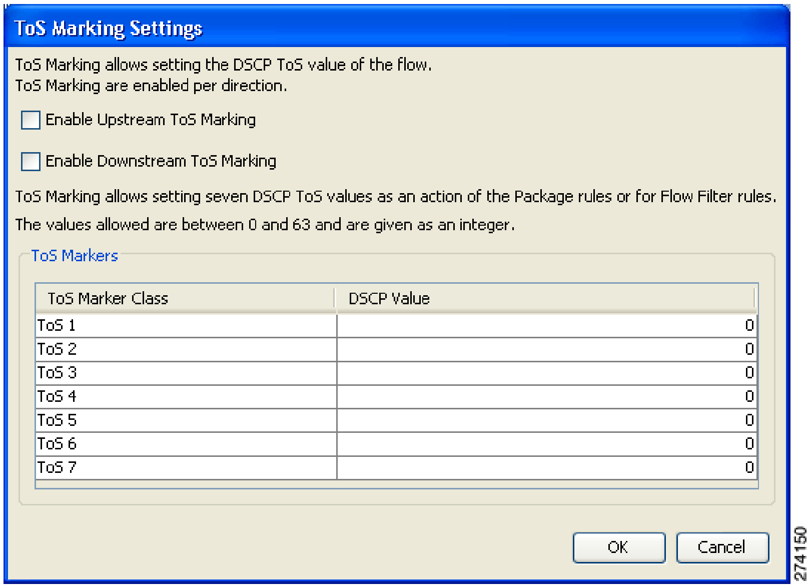
The default marking option is not to mark the packet. The classification may take a few packets to finalize. So after the ToS marking is enabled, the first few packets may still be processed under the default option and therefore may not be marked.

Caution In an MPLS environment, the SCE platform does not map the DSCP bits to the EXP bits of the MPLS header.

Step 1 From the Policies tab of the left pane, choose **Configuration > Policies > ToS Marking Settings**.

The ToS Marking Settings dialog box appears (Figure 9-64).

Figure 9-64 ToS Marking Settings



ToS Marking Settings

ToS Marking allows setting the DSCP ToS value of the flow.
ToS Marking are enabled per direction.

□ Enable Upstream ToS Marking

□ Enable Downstream ToS Marking

ToS Marking allows setting seven DSCP ToS values as an action of the Package rules or for Flow Filter rules.
The values allowed are between 0 and 63 and are given as an integer.

ToS Markers

ToS Marker Class	DSCP Value
ToS 1	0
ToS 2	0
ToS 3	0
ToS 4	0
ToS 5	0
ToS 6	0
ToS 7	0

Step 2 (Optional) To enable DSCP ToS marking on upstream flows, check the **Enable Upstream ToS Marking** check box.

If Upstream ToS Marking is disabled, it overrides filter rule and service rule settings.

Step 3 (Optional) To enable DSCP ToS marking on downstream flows, check the **Enable Downstream ToS Marking** check box.

If Downstream ToS Marking is disabled, it overrides filter rule and service rule settings.

Step 4 Give unique names to the ToS Marker Classes.

Note You can use the default names for the ToS Marker Classes, but it is recommended that you provide meaningful names.

Step 5 Assign values to the ToS Marker Classes.

Values must be in the range from 0 to 63.

Note When defining filter rules and service rules, the names and values of ToS Marker Classes are displayed in drop-down lists in the format “name [value]”. For example, “ToS 1 [23]” or “My P2P ToS [1]”

Step 6 Click **OK**.

Your changes are saved.

The ToS Marking Settings dialog box closes.

Managing Quotas

How to Add Quota Profiles

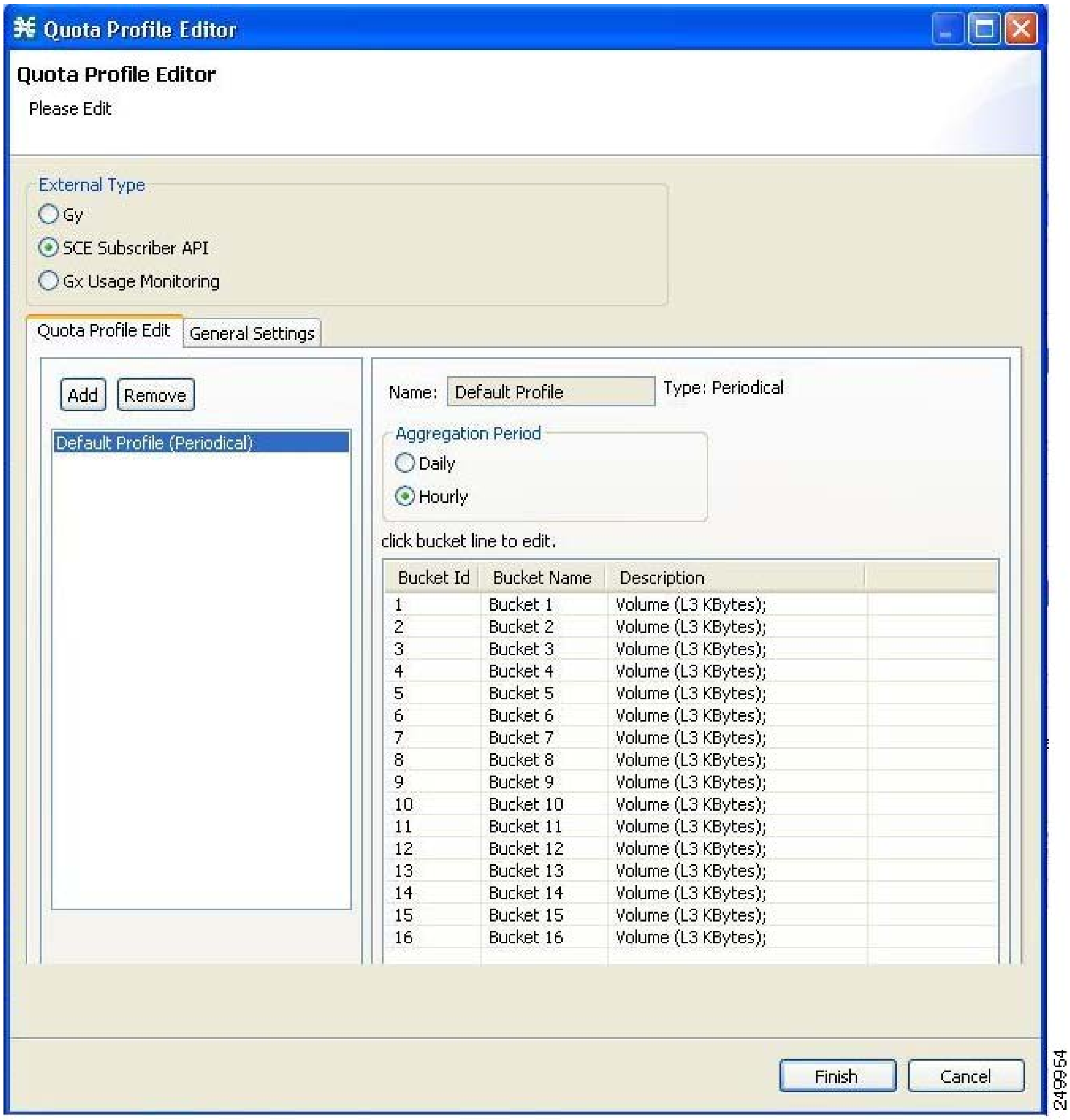
You can add and define new profiles and edit existing profiles. Additionally, you can add up to 16 new buckets.

You also define the quota buckets associated with the package. Rules can use quota buckets to set limits to the consumption of particular service groups (see How to Select Quota Buckets for Rules, page 9-93).

Step 1 From the Policies tab in the left pane, choose **Configuration > Policies > Quota Settings**.

The Quota Profile Editor dialog box appears (Figure 9-65).

Figure 9-65 Quota Profile Editor



External Type

○ Gy
● SCE Subscriber API
○ Gx Usage Monitoring

Default Profile (Periodical)

Name: Default Profile Type: Periodical

Aggregation Period

○ Daily
● Hourly

click bucket line to edit.

Bucket Id	Bucket Name	Description
1	Bucket 1	Volume (L3 KBytes);
2	Bucket 2	Volume (L3 KBytes);
3	Bucket 3	Volume (L3 KBytes);
4	Bucket 4	Volume (L3 KBytes);
5	Bucket 5	Volume (L3 KBytes);
6	Bucket 6	Volume (L3 KBytes);
7	Bucket 7	Volume (L3 KBytes);
8	Bucket 8	Volume (L3 KBytes);
9	Bucket 9	Volume (L3 KBytes);
10	Bucket 10	Volume (L3 KBytes);
11	Bucket 11	Volume (L3 KBytes);
12	Bucket 12	Volume (L3 KBytes);
13	Bucket 13	Volume (L3 KBytes);
14	Bucket 14	Volume (L3 KBytes);
15	Bucket 15	Volume (L3 KBytes);
16	Bucket 16	Volume (L3 KBytes);

Step 2 Select one of the **External Type** radio buttons.

- Gy—The Gy quota model enables the Gy interface adapter to be used for the external quota management. For more information, see *Cisco Service Control Mobile Solution Guide.*
- SCE Subscriber API—The Subscriber API enables the external applications (policy servers) to connect directly to the SCE for subscriber provisioning. For more information, see *Cisco SCMS SCE Subscriber API Programmer Guide.*
- Gx Usage Monitoring—Gx Usage Monitoring enables the Gx interface to generate usage monitoring reports. For more information, see *Cisco Service Control Mobile Solution Guide*.

Note Using periodical quota management, you can scatter quota replenishment so that the quota of all subscribers is not replenished at the same time. (See Quota Replenish Scatter, page 9-91.)

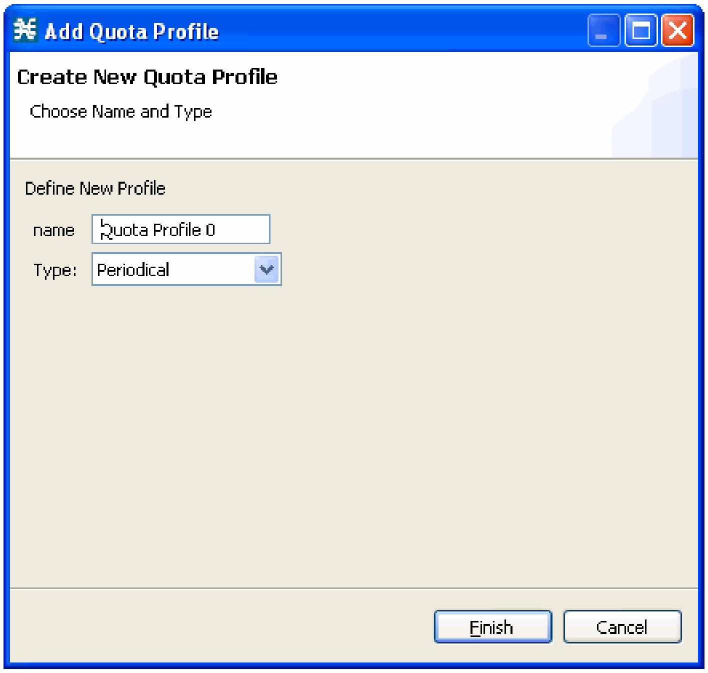
Step 3 For Periodical quota profile, select one of the Aggregation Period radio buttons to specify when the quota is renewed for the package:

- Hourly—Replenishes quota at each hour change
- Daily—Replenishes quota at midnight

Step 4 In the **Quota Profile Edit** tab, click **Add**.

The Add Quota Profile dialog box appears ().

Figure 9-66 Add Quota Profile



Add Quota Profile

Create New Quota Profile

Choose Name and Type

Define New Profile

name: Quota Profile 0

Type: Periodical

Step 5 In the Name field, enter a unique name for the new quota profile.

Step 6 Select the Type from the drop-down list.

- Periodical
- Subscriber SCE API

Step 7 Click **Finish**.

The Add Quota Profile window closes.

The new profile is added to the list of profiles displayed in the left (Quota Profile Edit) pane.

How to Edit Quota Profiles

You can edit the profiles to update the bucket profile.

Note You cannot edit or remove the default profile.

Step 1 From the Policies tab in the left pane, choose **Configuration > Policies > Quota Settings**.

The Quota Profile Editor dialog box appears (Figure 9-71).

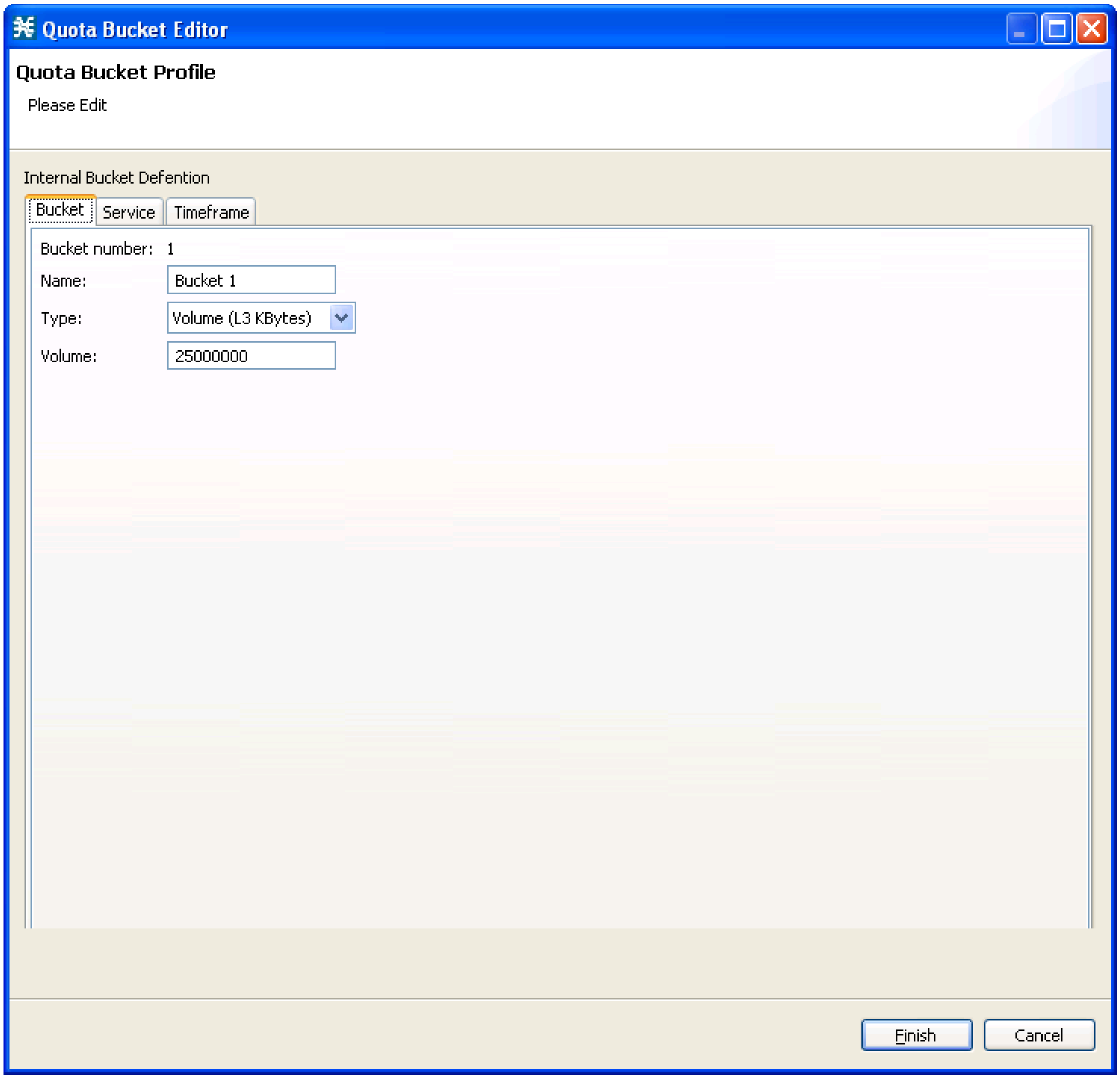
Step 2 Select a quota profile from the profile tree.

All the buckets defined for the selected profile are listed on the right pane.

Step 3 Double-click a bucket line in the right pane.

The Quota Bucket Editor window appears (Figure 9-67).

Figure 9-67 Quota Bucket Editor



Quota Bucket Editor

Quota Bucket Profile

Please Edit

Internal Bucket Defention

Bucket number: 1

Name: Bucket 1

Type: Volume (L3 KBytes)

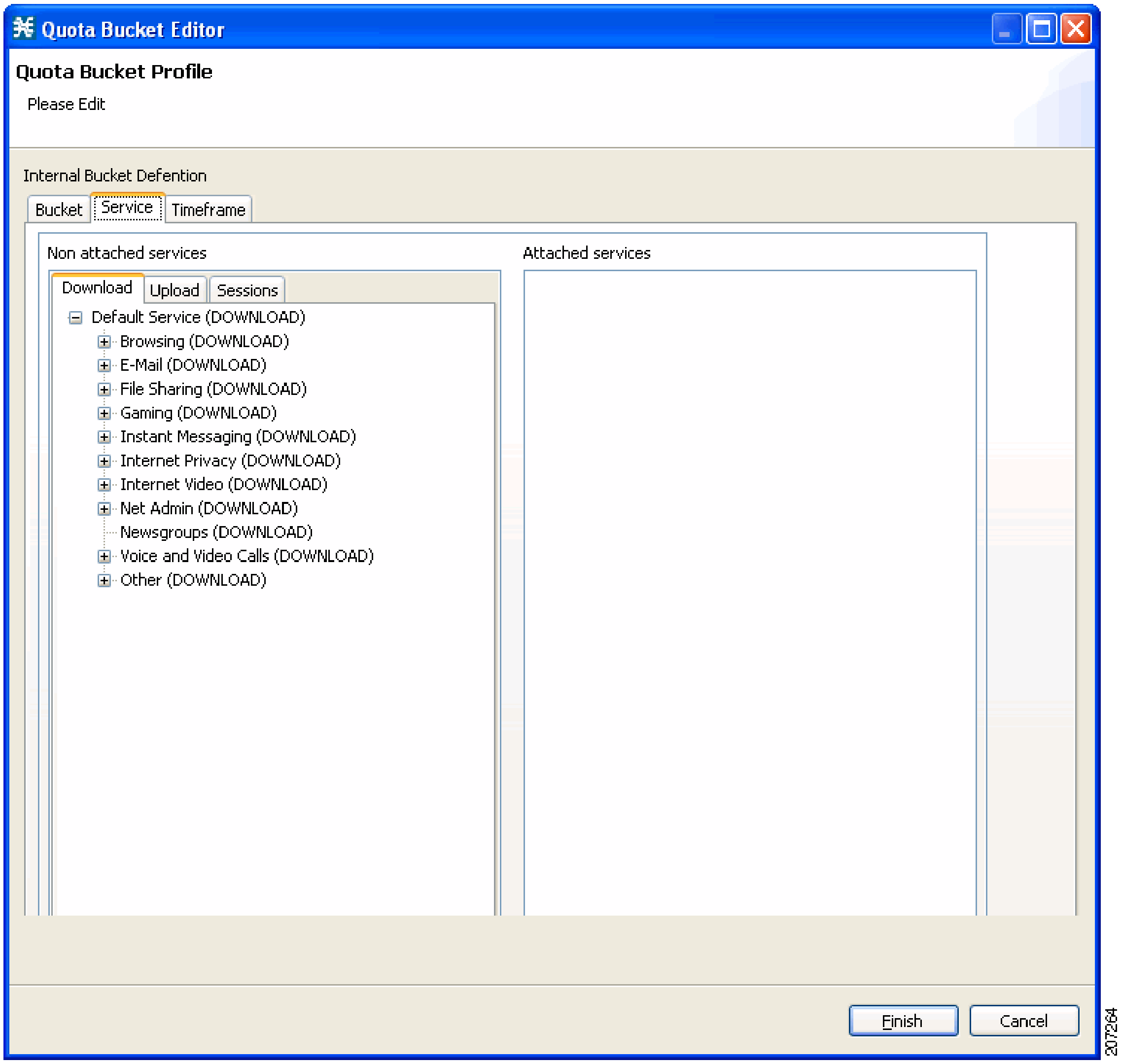
Volume: 25000000

Step 4 Change the Name, Type, and Volume.

Note You can use the default name for the bucket. It is recommended that you enter a meaningful name.

Step 5 Click on the Service tab, to associate the services to the quota profile (Figure 9-68).

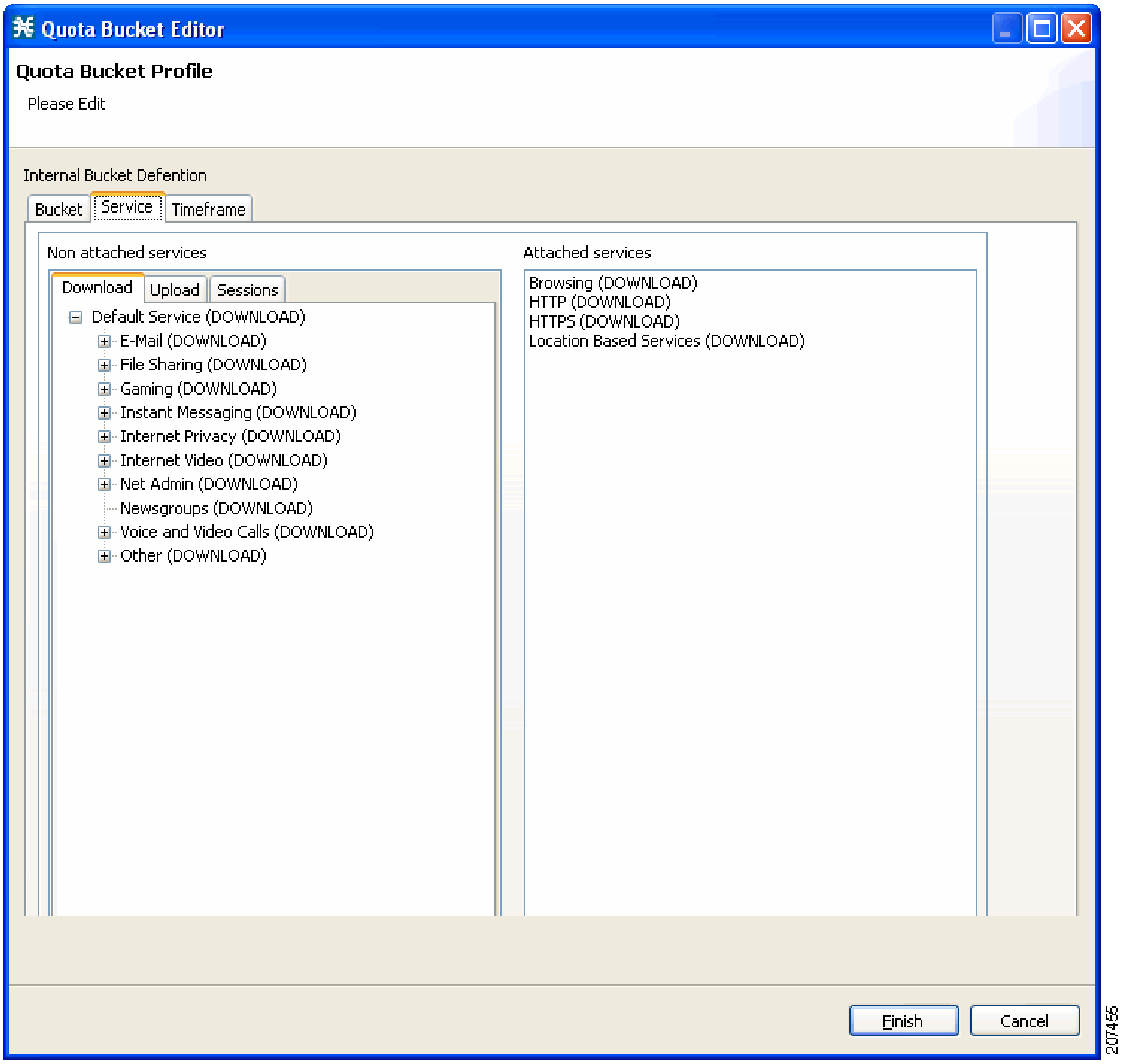
Figure 9-68 Quota Bucket Editor - Service



Step 6 Select a service from the Non Attached Service pane and move it to the Attached Service pane on the right.

The selected service is moved along with its sub services (Figure 9-69).

Figure 9-69 Quota Bucket Editor - Attached Service



Quota Bucket Editor

Quota Bucket Profile

Please Edit

Internal Bucket Defention

Bucket | Service | Timeframe

Non attached services

Download | Upload | Sessions

- Default Service (DOWNLOAD)
  - E-Mail (DOWNLOAD)
  - File Sharing (DOWNLOAD)
  - Gaming (DOWNLOAD)
  - Instant Messaging (DOWNLOAD)
  - Internet Privacy (DOWNLOAD)
  - Internet Video (DOWNLOAD)
  - Net Admin (DOWNLOAD)
  - Newsgroups (DOWNLOAD)
  - Voice and Video Calls (DOWNLOAD)
  - Other (DOWNLOAD)

Attached services

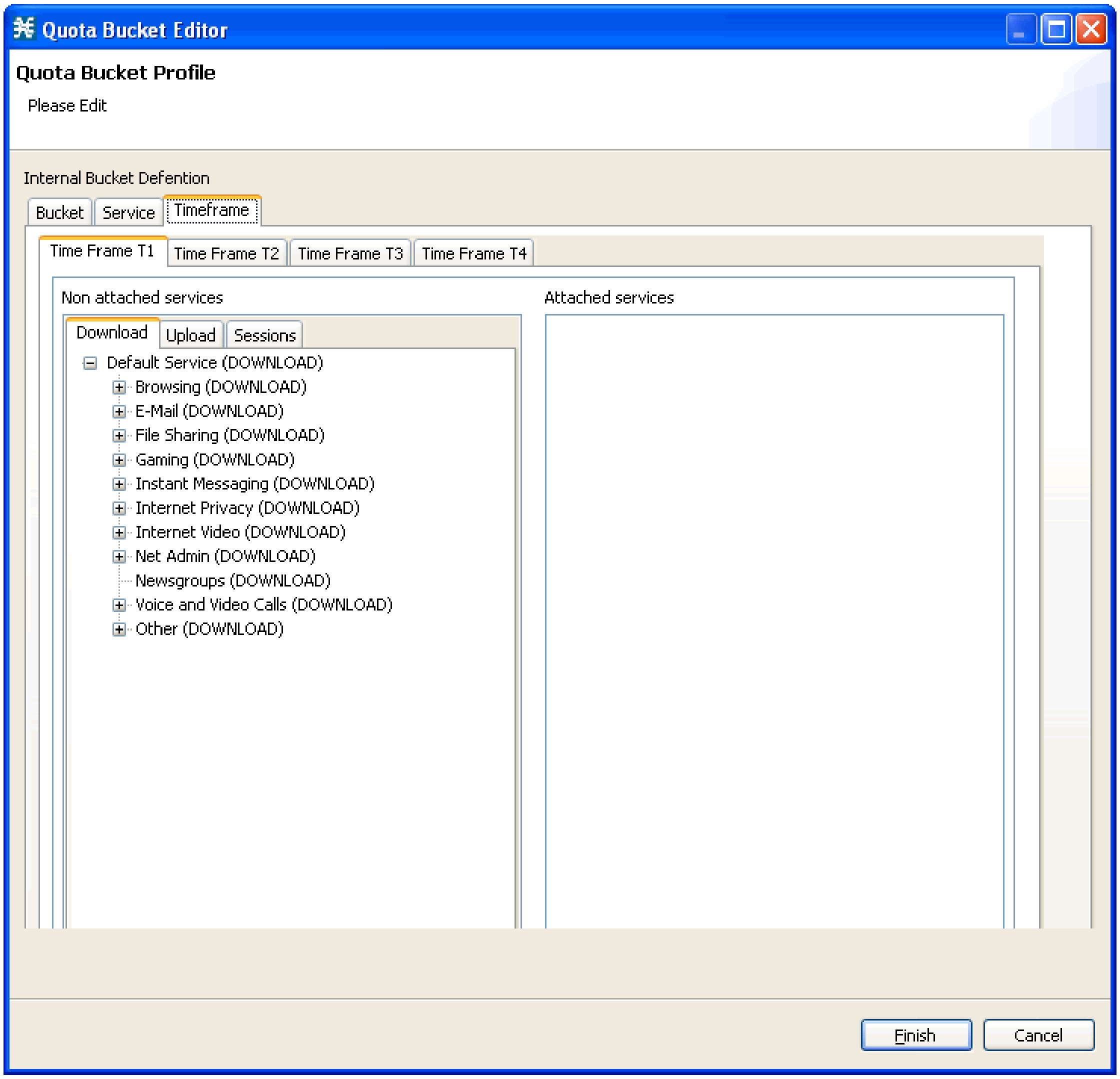
Browsing (DOWNLOAD)
HTTP (DOWNLOAD)
HTTPS (DOWNLOAD)
Location Based Services (DOWNLOAD)

Based on the bucket type, you can select services from the following tabs:

- Download
- Upload
- Session

Step 7 Click on the Timeframe tab, to associate different timeframes to the quota profile (Figure 9-70).

Figure 9-70 Quota Bucket Editor - Timeframe



Step 8 Select a service from the Non Attached Service pane and move it to the Attached Service pane on the right.

The selected service is moved along with its sub services.

Based on the bucket type, you can select services from the following tabs:

- Download
- Upload
- Session

Step 9 Click **Finish**.

The Quota Bucket Editor closes.

Step 10 Click Finish. The Quota Profile Editor closes.

What to Do Next

To select a service to which the rule relates to, see How to Add Rules to a Package, page 9-63.

How to Delete Quota Profiles

Note The default profile cannot be deleted.

Step 1 From the Policies tab in the left pane, choose **Configuration** > **Policies** > **Quota Settings**.

The Quota Profile Editor dialog box appears (Figure 9-71).

Step 2 Select a quota profile from the profile tree.

Step 3 Click **Remove**.

Step 4 Click **Finish**.

The Quota Profile Editor dialog box closes.

How to Edit Quota Management Settings for Packages

You can define whether an external quota manager or the Cisco SCA BB performs the quota management for a package.

Quota Replenish Scatter

By default, if subscriber quota is replenished using periodical quota management, the quota of all subscribers is replenished at the same time. To smooth quota replenishment, you can scatter the time of quota replenishment.

To activate this feature, enter a non-zero value for the Length of the time frame for quota replenish scatter (minutes) property of the Advanced Options tab of the Systems Settings dialog box (see Managing Advanced Service Configuration Options, page 10-58). By default, this property has a value of zero, that is, all quota is replenished at the same time.

Quota for each subscriber is replenished at a random time within the quota replenish scatter time frame, with replenish events split evenly before and after the quota aggregation time.

Best results are obtained if the scatter time frame is the same length as the quota aggregation period, which should completely smooth replenish events. Do not enter a value larger than the quota replenish period. Therefore, for an hourly quota replenish period, set the scatter to 60 minutes.

The quota replenish scatter function is independent of all other quota management parameters.

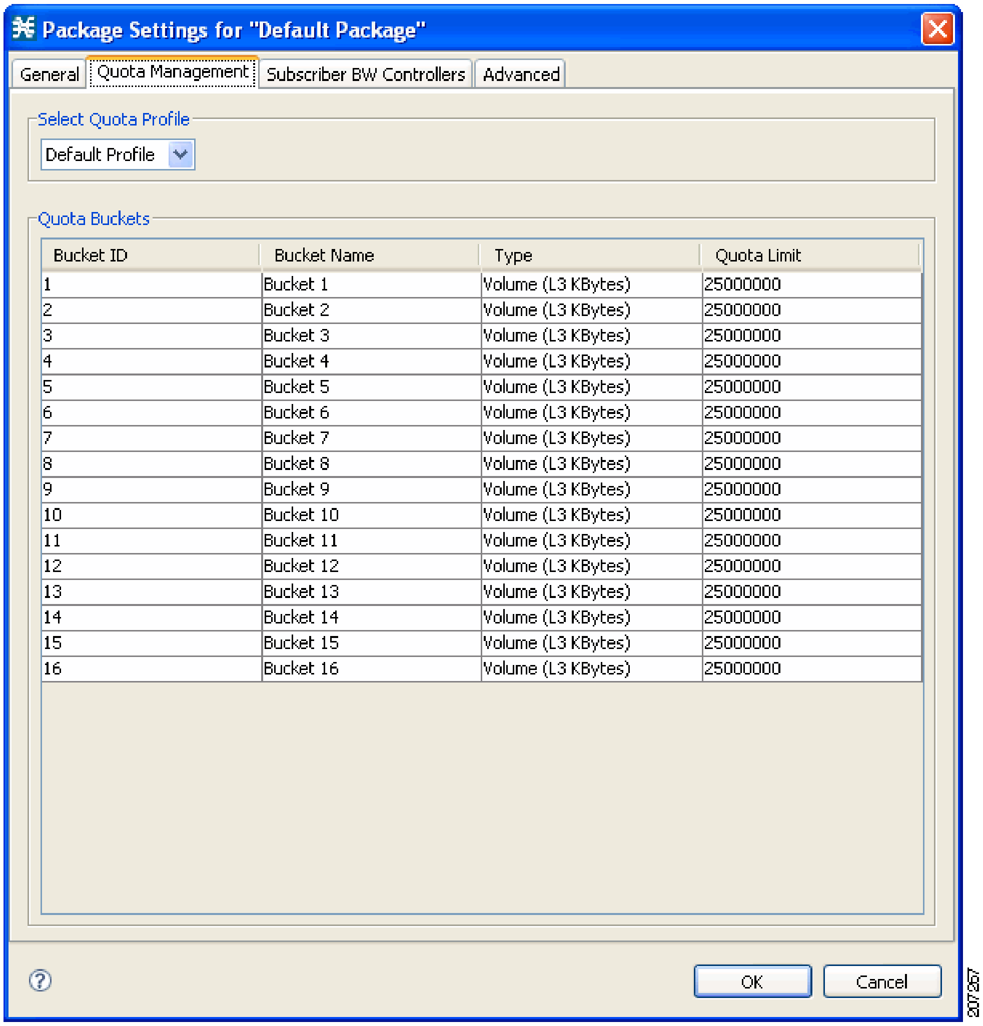
Step 1 In the Policies tab, select a package from the package tree, and click the **Edit Package** (✏) icon.

The Package Settings dialog box appears.

Step 2 In the Package Settings dialog box, click the **Quota Management** tab.

The Quota Management tab opens (Figure 9-71).

Figure 9-71 Quota Management Tab


Package Settings for "Default Package"
General
Quota Management
Subscriber BW Controllers
Advanced
OK
Cancel
207257

Select Quota Profile: Default Profile

Quota Buckets

Bucket ID	Bucket Name	Type	Quota Limit
1	Bucket 1	Volume (L3 KBytes)	25000000
2	Bucket 2	Volume (L3 KBytes)	25000000
3	Bucket 3	Volume (L3 KBytes)	25000000
4	Bucket 4	Volume (L3 KBytes)	25000000
5	Bucket 5	Volume (L3 KBytes)	25000000
6	Bucket 6	Volume (L3 KBytes)	25000000
7	Bucket 7	Volume (L3 KBytes)	25000000
8	Bucket 8	Volume (L3 KBytes)	25000000
9	Bucket 9	Volume (L3 KBytes)	25000000
10	Bucket 10	Volume (L3 KBytes)	25000000
11	Bucket 11	Volume (L3 KBytes)	25000000
12	Bucket 12	Volume (L3 KBytes)	25000000
13	Bucket 13	Volume (L3 KBytes)	25000000
14	Bucket 14	Volume (L3 KBytes)	25000000
15	Bucket 15	Volume (L3 KBytes)	25000000
16	Bucket 16	Volume (L3 KBytes)	25000000

Step 3 Select the Select quota profile from the drop-down list.

Step 4 Click **OK**.

The Package Settings dialog box closes.

All changes to the quota management settings are saved.

How to Select Quota Buckets for Rules

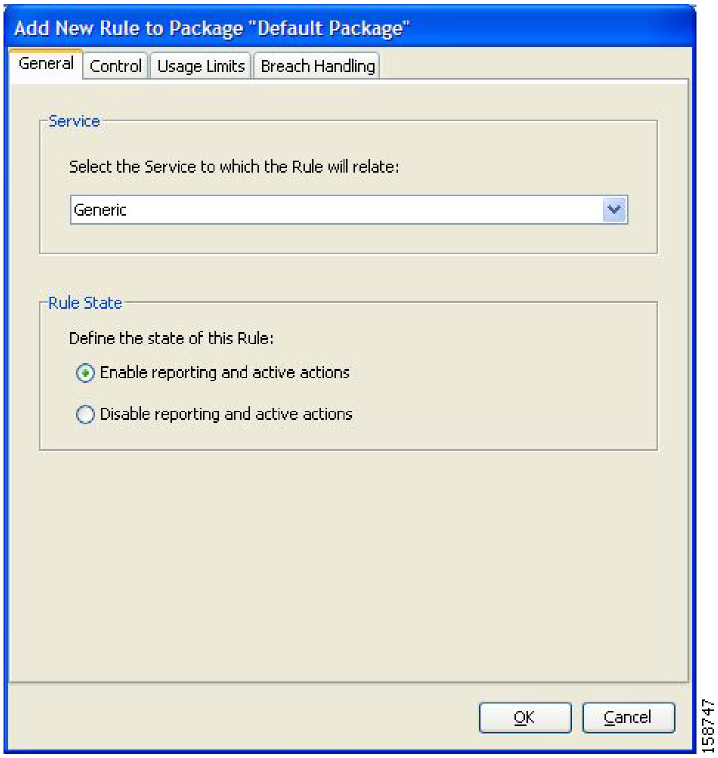
Select the quota buckets that the flows mapped to a rule uses. The quota buckets are defined during package setup (see How to Edit Quota Management Settings for Packages, page 9-91). If no quota bucket is appropriate for the rule, add a new quota bucket to the package or edit an existing bucket.

Step 1 In the Network Traffic tab, select a package from the package tree.

Step 2 In the right (Rule) pane, click the **Add Rule** (✚) icon.

The Add New Rule to Package dialog box appears (Figure 9-72).

Figure 9-72 Add New Rule to Package



Service

Select the Service to which the Rule will relate:

Generic

Rule State

Define the state of this Rule:

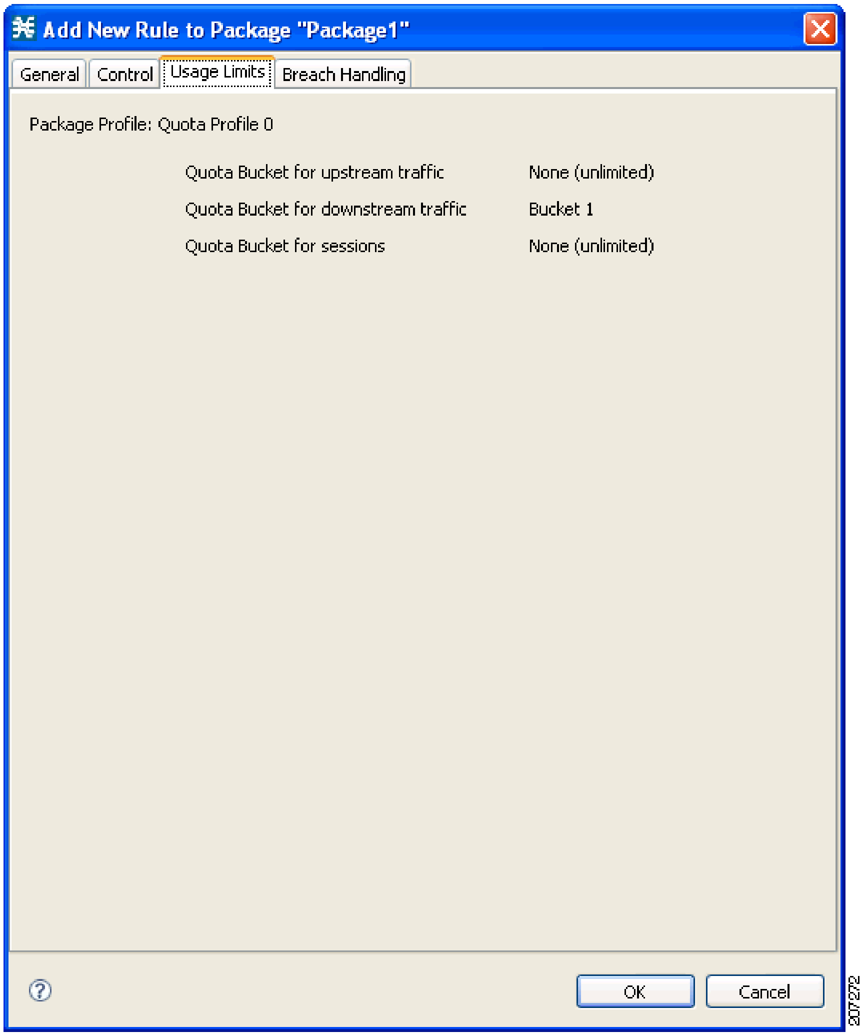
● Enable reporting and active actions

○ Disable reporting and active actions

Step 3 In the Service area, select a service from the Select the Service to Which the Rule Relates drop-down list.

Step 4 Click the **Usage Limits** tab (Figure 9-73).

Figure 9-73 Usage Limits Tab



Package Profile: Quota Profile 0

Quota Bucket for upstream traffic	None (unlimited)
Quota Bucket for downstream traffic	Bucket 1
Quota Bucket for sessions	None (unlimited)

Step 5 The Usage Limits tab displays the package profile details.

The quota bucket selected for the rule is displayed. For more information on adding services to quota profile, see Step 5 of the How to Edit Quota Profiles, page 9-86 section.

Step 6 Click **OK**.

The Edit Rule for Services dialog box closes.

How to Edit Breach-Handling Parameters for a Rule

You can define the SCE platform behavior when an aggregated volume limit or the total number-of-sessions limit is exceeded. You can also notify subscribers when they exceed their quotas.

Breach-Handling Parameters

The following are the configuration parameters in the Breach Handling tab of the Edit Rule for Service Settings dialog box.

- You determine what happens to flows identified as belonging to this rule when a quota is breached:
  - No changes to active control—Flows mapped to this rule are not affected when quota is breached. Cisco SCA BB can generate Quota Breach RDRs even when this option is selected (see How to Manage Quota RDRs, page 8-8).
  - Block the flow—Flows mapped to this rule are blocked when quota is breached.

    Redirect to—Redirect the flow to a specified, protocol-dependent URL, where a posted web page explains the reason for the redirection. URL redirection sets are defined in the System Settings dialog box. (See How to Add a Set of Redirection URLs, page 10-52.) Only three protocol types support redirection: HTTP, HTTP Streaming, and RTSP. Redirection is not supported when unidirectional classification is enabled.
  - Control the flow characteristics—The behaviors of flows mapped to this rule change when quota is breached:

    Select an upstream Bandwidth Controller—Map the traffic flow of this rule to a specific upstream BW controller (BWC). This sets up bandwidth metering of all concurrent flows mapped to this rule, based on the characteristics of the selected BWC.

    Select a downstream Bandwidth Controller—The same functionality as the previous option, but for downstream flow.

    Limit the flow’s upstream bandwidth—Set a per-flow upstream bandwidth limit (for flows mapped to the service of this rule).

    Limit the flow’s downstream bandwidth—Set a per-flow downstream bandwidth limit.

    Set the flow's upstream packets ToS—Set the DSCP ToS marker of all packets of upstream flows.

    Set the flow's downstream packets ToS—Set the DSCP ToS marker of all packets of downstream flows.

    Limit concurrent flows of this Service—Set the maximum number of concurrent flows (mapped to this rule) permitted to a subscriber.
- Activate a Subscriber Redirect—Activate a Subscriber Redirect when subscribers exceed their quota limit.
- Activate a Subscriber Notification—Activate a Subscriber Notification when subscribers exceed their quota limit. This notification can, for example, convey the quota breach situation to the subscriber and explain how to obtain additional quota.

Note Subscriber notification is not supported when unidirectional classification is enabled.

To define Subscriber Notifications, see Managing Subscriber Notifications, page 10-41.

- Activate Traffic Mirroring—Activate traffic mirroring when subscribers exceed their quota limit

Step 1 In the Policies tab, select a package from the package tree.

Step 2 In the right (Rule) pane, select a rule.

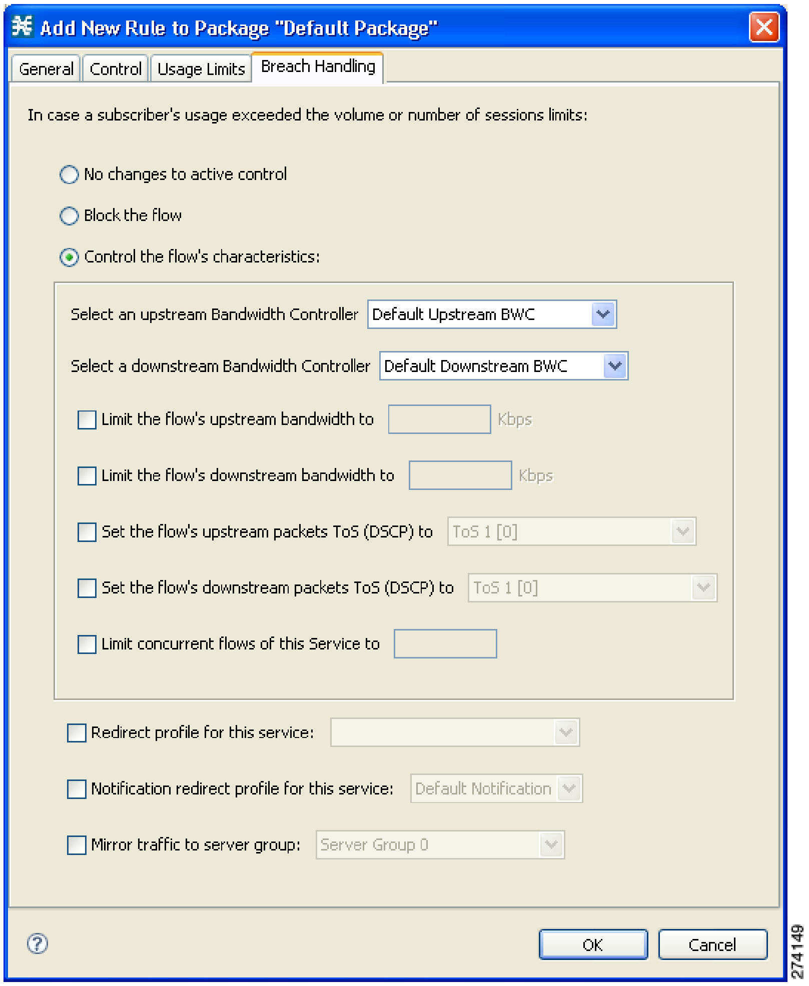
Step 3 Click the **Edit Rule** (✎) icon.

The Edit Rule for Service dialog box appears.

Step 4 Click the Breach Handling tab.

The Breach Handling tab opens (Figure 9-74).

Figure 9-74 Breach Handling Tab



Add New Rule to Package "Default Package"

General | Control | Usage Limits | Breach Handling

In case a subscriber's usage exceeded the volume or number of sessions limits:

○ No changes to active control

○ Block the flow

● Control the flow's characteristics:

Select an upstream Bandwidth Controller: Default Upstream BWC

Select a downstream Bandwidth Controller: Default Downstream BWC

□ Limit the flow's upstream bandwidth to ____ Kbps

□ Limit the flow's downstream bandwidth to ____ Kbps

□ Set the flow's upstream packets ToS (DSCP) to: ToS 1 [0]

□ Set the flow's downstream packets ToS (DSCP) to: ToS 1 [0]

□ Limit concurrent flows of this Service to ____

□ Redirect profile for this service:

□ Notification redirect profile for this service: Default Notification

□ Mirror traffic to server group: Server Group 0

Step 5 Set the behavior of the flow when quota is breached.

- To block the flow when quota is breached, continue at Step 6.
- To change the characteristics of the flow when quota is breached, continue at Step 10.
- To leave the flow unchanged when quota is breached, select the **No changes to active control** radio button and continue at Step 11.

Step 6 To block the flow, select the **Block the flow** radio button.

Step 7 Continue at Step 10, page 350.

Step 8 Change the characteristics of the flow.

Select the **Control the flow's characteristics** radio button.

The options in the Flow Characteristic area are enabled:

- From the upstream Bandwidth Controller drop-down list, select an upstream BWC

  The BWCs in this drop-down list are defined when creating or editing the package.

When the mouse is placed over the drop-down list, a tooltip appears. The tooltip contains the properties of the selected BWC, such as PIR, CIR, AL, and Global Controller.

- From the downstream Bandwidth Controller drop-down list, select a downstream BWC.
- (Optional) Check the **Limit the flow's upstream bandwidth** check box and enter a value in the Kbps field.
- (Optional) Check the **Limit the flow's downstream bandwidth** check box and enter a value in the Kbps field.
- (Optional) Check the **Set the flow's upstream packets ToS (DSCP) to** check box and select a value from the drop-down list.
- (Optional) Check the **Set the flow's downstream packets ToS (DSCP) to** check box and select a value from the drop-down list.
- (Optional) Check the Limit concurrent flows of this Service check box and enter a value in the associated field.(Optional) To enable subscriber

Step 9 (Optional) To enable subscriber redirect, check the check box, and select a redirect profile from the drop-down list.

Step 10 (Optional) To enable subscriber notification, check the Notification redirect profile for this service check box and select a notification redirect profile from the drop-down list.

Note A subscriber notification can be activated in addition to any of the three breach-handling options.

Note Subscriber notification is not supported when unidirectional classification is enabled. If you try to check the Activate a Subscriber Notification check box when unidirectional classification is enabled, a Rule Error message appears.

Step 11 Click **OK** to continue.

Step 12 (Optional) To enable mirror traffic to a server group, check Mirror traffic to server group and choose a server group to send the mirror traffic to.

Note The Mirror traffic to server group check box is only enabled when Traffic Mirroring is enabled in the VAS Settings dialog box.

Step 13 Click **OK**.

The Edit Rule for Service dialog box closes.

All changes to the rule are saved.

Example: Creating Tiered Subscriber Services

Tiered subscriber services can be implemented using the Cisco SCA BB Console. Because the definition of such services is open ended, this section describes how to define two of the tiers outlined in the value proposition description. The two tiers are defined as follows:

- Silver
  - Weekly bandwidth limited to 4.2 GB (corresponds to a daily limit of 600 MB)
  - Email and browsing services are limited to 256 kbps
  - Audio and video streaming services are limited to 64 kbps
  - P2P services are limited to 28 kbps
- Gold
  - Weekly bandwidth limited to 5.6 GB (corresponds to a daily limit of 800 MB)
  - Email and browsing services are not bandwidth limited
  - Audio and video streaming services are limited to 128 kbps
  - P2P services are limited to 28 kbps

The following steps are applicable to both the 'Silver' and 'Gold' packages.

Step 1 Create a new package as described in How to Add Packages, page 9-55.

Step 2 Enable periodical (internal) quota management.

a. Set the aggregation period to Daily

b. b) Set the quota limit to the desired value and give the quota bucket a meaningful name

For further information, see How to Edit Quota Management Settings for Packages, page 9-91.

Step 3 Add the bandwidth controllers for the required services and set the PIR to the desired rate.

Note Each service that is bandwidth limited requires a sub bandwidth controller that is a child of the primary bandwidth controller, not an extra bandwidth controller.

For further information, see How to Edit Package Subscriber BWCs, page 9-30.

Step 4 Add a rule to the package for each bandwidth limited service.

For further information, see How to Add Rules to a Package, page 9-63.

Step 5 Configure the rule to control the characteristics of the flow with the bandwidth controller for the relevant service.

For further information, see How to Define Per-Flow Actions for a Rule, page 9-66.

Step 6 Set the usage limit for the package to use the quota bucket defined in Step 2.

For further information, see the How to Select Quota Buckets for Rules, page 9-93 section.

Unknown Subscriber Traffic

SCE platform processes a traffic flow that does not match any filter rule (see Filtering the Traffic Flows, page 10-23). SCE platform tries to identify the subscriber responsible for the traffic flow. The platform checks its internal database for a subscriber identified by the IP address or VLAN tag of the traffic flow. If no such subscriber exists, the traffic flow is mapped to the Unknown Subscriber Traffic category.

The Unknown Subscriber Traffic category is included in the tree in the Network Traffic tab but is not part of the package hierarchy. The Unknown Subscriber Traffic category cannot be deleted.

Note Traffic of one unknown subscriber cannot be distinguished from traffic of other unknown subscribers. Therefore, you cannot set either per-subscriber usage limits or subscriber-level metering with subscriber BWCs. You can use subscriber BWCs only to link a selected service to a global controller.

The Unknown Subscriber Traffic category behaves like a package with the following parameters:

- Package Name = Unknown Subscriber Traffic
- Package Index = 4999
- One package usage counter:
  - Counter Name = Unknown Subscriber Traffic Counter
  - Counter Index = 1023

You can:

- Edit the Unknown Subscriber Traffic package settings:
  - Add extra BWCs (see How to Edit Package Subscriber BWCs, page 9-30).
  - Select a calendar (see How to Set Advanced Package Options, page 9-57).
- Edit the default service rule for the Unknown Subscriber Traffic category:
  - Change the Rule State (see How to Edit Rules, page 9-68).
  - Change per-flow actions for the rule (see How to Define Per-Flow Actions for a Rule, page 9-66).
- Add rules to the Unknown Subscriber Traffic package:
  - Add rules (see How to Add Rules to a Package, page 9-63); edit (see How to Edit Rules, page 9-68) and delete (see How to Delete Rules, page 9-70) these rules.
  - Add time-based rules (see How to Add Time-Based Rules to a Rule, page 9-72); edit (see How to Edit Time-Based Rules, page 9-74) and delete (see How to Delete Time-Based Rules, page 9-75) these rules.

CHAPTER 10

Using the Service Configuration Editor: Additional Options

Revised: August 08, 2013, OL-24178-09

Introduction

This chapter explains how to use additional, advanced functionality available in the Service Configuration Editor.

This chapter consists of these sections:

The Service Security Dashboard

The Service Security Dashboard allows you to view and control all Cisco SCA BB security functionality.

The Dashboard is a gateway to a set of features that help you protect your network from security threats such as worms, DDoS attacks, and spam zombies. It allows configuration of the detection mechanisms (for example, attack thresholds) and of the actions to be taken when an attack is detected.

The Dashboard also allows you to access malicious traffic reports in the Reporter tool.

⚠ **Caution** If anomaly-based detection of malicious traffic is enabled, any access control list (ACL) that is configured on the Service Control Engine (SCE) platform but is not applied to anything (for example, an interface, an access map, or an SNMP community string) might be deleted when a service configuration is applied to the platform.

Workaround:

Disable anomaly-based detection of malicious traffic. (Clear the **Enable anomaly detection** check box.)

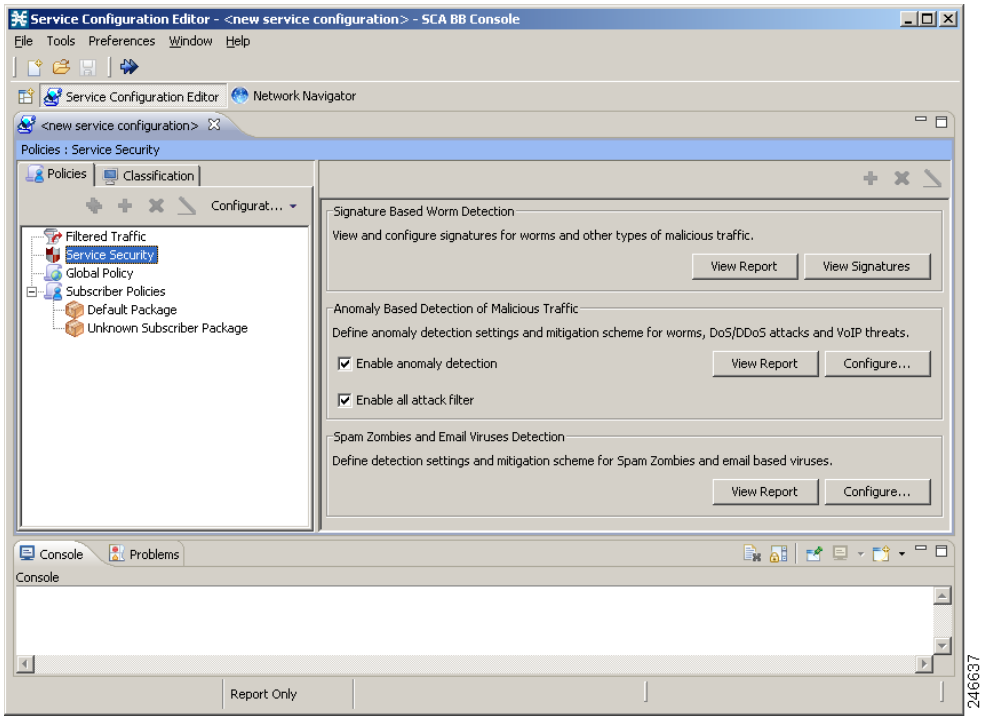
- How to View the Service Security Dashboard, page 10-3
- Managing Worm Detection, page 10-3
- Managing Anomaly Detection, page 10-4
- Managing Spam Detection, page 10-17
- Viewing Malicious Traffic Reports, page 10-21

How to View the Service Security Dashboard

Step 1 In the Network Traffic tab, select **Service Security**.

Step 2 The Service Security Dashboard is displayed in the right pane (Figure 10-1).

Figure 10-1 Service Security Dashboard



Service Configuration Editor - <new service configuration> - SCA BB Console
File
Tools
Preferences
Window
Help
Service Configuration Editor
Network Navigator
<new service configuration>
Policies : Service Security
Policies
Classification
Configurat...
Filtered Traffic
Service Security
Global Policy
Subscriber Policies
Default Package
Unknown Subscriber Package
Signature Based Worm Detection
View Report
View Signatures
Anomaly Based Detection of Malicious Traffic
View Report
Configure...
Spam Zombies and Email Viruses Detection
View Report
Configure...
Console
Problems
Console
Report Only
246637

View and configure signatures for worms and other types of malicious traffic.

Define anomaly detection settings and mitigation scheme for worms, DoS/DDoS attacks and VoIP threats.

☑ Enable anomaly detection

☑ Enable all attack filter

Define detection settings and mitigation scheme for Spam Zombies and email based viruses.

Managing Worm Detection

Cisco SCA BB uses three mechanisms for detecting worms:

- Signature-based detection—The stateful Layer 7 capabilities of the SCE platform can detect malicious activity that is not easily detectable by other mechanisms. You can add signatures for new worms.
- Anomaly-based detection—Overall traffic analysis can detect anomalies that might indicate worm activity. See Managing Anomaly Detection, page 10-4.
- Mass-mailing based detection—E-mail traffic analysis can detect anomalies that might indicate e-mail-based worms. See How to Configure Spam Detection Settings, page 10-18.

How to View Supported Worm Signatures

Step 1 In the Service Security Dashboard, click **View Signatures**.

The Signatures Settings dialog box appears, with Worm Signatures selected in the Signature Type drop-down list.

All supported worm signatures are listed.

Step 2 Click **Close**.

The Signatures Settings dialog box closes.

How to Add New Worm Signatures to a Service Configuration

Either import the latest DSS or SPQI file provided by Cisco or create a DSS file containing any worm signatures that you wish to add to the service configuration.

Related Information

For more information, see Managing Protocol Signatures, page 7-46.

Managing Anomaly Detection

The most comprehensive threat detection method is anomaly detection.

- Anomaly Detection, page 10-4
- Anomaly Detection Parameters, page 10-5
- How to View Anomaly Detection Settings, page 10-7
- How to Add Anomaly Detectors, page 10-9
- Editing Anomaly Detectors, page 10-13
- How to Delete Anomaly Detectors, page 10-17

Anomaly Detection

The basic principle of anomaly detection is monitoring successful (correctly established for TCP, bidirectional for other protocols) and unsuccessful (not properly established for TCP, unidirectional for other protocols) connection rates both to and from any IP address viewed by the system, and triggering an anomaly detection condition based of one of the following criteria:

- The total connection rate exceeds a predefined threshold.
- The suspicious connection rate exceeds a predefined threshold *and* the ratio of suspicious to unsuspicious connections exceeds a predefined threshold.

The ratio metric is a robust indicator of malicious activity, and together with a rate qualifier it serves as a reliable identifier for malicious activity.

Anomaly detection is divided into three categories based on the directional nature of the detected anomaly condition. The concepts used for the three categories are identical, but the nature of the detected malicious activity is different for each category.

- Scan/Sweep detector—Detects malicious activity based on an anomaly in connection rates *from* an IP address.
- DoS detector—Detects an anomaly in the connection rate between a pair of IP addresses: one of them is attacking the other. This can be either an isolated attack or part of a larger scale DDoS attack.
- DDoS detector—Detects an anomaly in the connection rate coming *to* an IP address, which means that it is being attacked. The attack can be by either a single IP address (DoS) or multiple IP addresses.

Note When the IP address common to all flows of an attack is on the network side, the Cisco SCE may require more flows (than the configured threshold) to detect the attack. For example, on Cisco SCE 2000, if the configured threshold is 100 flows per second, these type of attacks are detected only if there are more than 300 flows per second.

For all kinds of anomaly detection conditions, maximum flexibility is provided by the ability to define detection thresholds and the trigger actions to be taken for each:

- Flow direction
- Flow protocol
- (Optional) Port uniqueness for TCP and UDP

Note The GUI configuration described here replaces the CLI command set for configuring the Attack Filtering Module of the SCE platform, which was available in previous releases.

Anomaly Detection Parameters

For each anomaly detector category (Scan/Sweep, DoS, DDoS) there is one default detector. You can add additional detectors of each category. Detectors in each category are checked in order; the first match (according to the threshold settings of the detector) triggers detection. You set the order in which detectors are checked; the default detector is checked last.

Anomaly detectors can contain up to 12 anomaly types associated with malicious traffic:

- Network initiated—Malicious traffic initiated from the network side:
  - TCP—Aggregate TCP traffic on all ports
  - TCP Specific Ports—TCP traffic on any single port
  - UDP—Aggregate UDP traffic on all ports
  - UDP Specific Ports—UDP traffic on any single port
  - ICMP—Aggregate ICMP traffic on all ports
  - Other—Aggregate traffic using other protocol types on all ports
- Subscriber initiated—Malicious traffic initiated from the subscriber side:
  - TCP
  - TCP Specific Ports
  - UDP

  - UDP Specific Ports
  - ICMP
  - Other

Note ICMP and Other anomaly types are not available for DoS attack detectors.

Each anomaly type on a detector has the following attributes associated with it:

- Detection thresholds—There are two thresholds, crossing either of them means that an attack is defined to be in progress:
  - Session Rate threshold—The number of sessions (per second) over specified ports for a single IP address that trigger the anomaly detection condition.
  - Suspected sessions threshold—Suspected sessions are sessions that are not properly established (for TCP), or that are unidirectional sessions (for other protocols). Exceeding both the Suspected Session Rate *and* the Suspected Session Ratio triggers the anomaly detection condition. (A relatively high session rate with a low response rate typically indicates malicious activity.)

    Suspected Session Rate—The number of suspected sessions (per second) over specified ports for a single IP address.

    Suspected Session Ratio—The ratio (as a percentage) between the suspected session rate and the total session rate. A high ratio indicates that many sessions received no response, an indication of malicious activity.
- Actions—Zero or more of the following actions may be taken when an anomaly detection condition is triggered (by default, no action is enabled):

Note Logging of the anomaly to an on-device log file and generation of RDRs is not configurable per anomaly type.

  - Alert User—Generate an SNMP trap indicating the beginning and end of an anomaly. For details on SNMP traps, see the “SCA BB Proprietary MIB Reference” chapter of *Cisco Service Control Application for Broadband Reference Guide* for information about the Cisco proprietary MIB.
  - Notify Subscriber—Notify the relevant subscriber of the malicious activity by redirecting the browsing sessions to a captive portal. To configure network attack subscriber notification, see Managing Subscriber Notifications, page 10-41.
  - Block Attack—Block the relevant sessions. Blocking is performed based on the specification of the malicious traffic that triggered the anomaly detection condition. If subscriber notification is enabled for the anomaly type, blocking is not applied to the port relevant for browsing (by default, this is TCP port 80; see Managing Advanced Service Configuration Options, page 10-58).

User-defined detectors can also have one or more of the following attributes:

- IP address list—Limit detection to the listed IP address ranges. This applies to the source IP when detecting IP sweeps and port scans. It applies to the destination IP when detecting DoS and DDoS attacks.
- TCP port list—Limit detection to the listed destination TCP ports. This list is applied to TCP Specific Ports anomaly types only.

- UDP port list—Limit detection to the listed destination UDP ports. This list is applied to UDP Specific Ports anomaly types only.

How to View Anomaly Detection Settings

You can view a list of all anomaly detectors. The anomaly detectors are displayed in a tree, grouped according to detector category (Scan/Sweep, DoS, or DDoS).

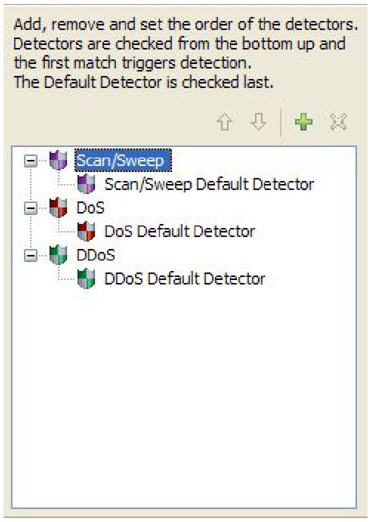
For each anomaly detector, you can view its associated parameters and see a list of all anomaly types included in the detector, together with their parameters.

Step 1 In the Service Security Dashboard, in the Anomaly Based Detection of Malicious Traffic pane, click **Configure**.

The Anomaly Detection Settings dialog box appears.

The detector tree is displayed in the left area of the dialog box; the right area is empty (Figure 10-2).

Figure 10-2 Detector Tree



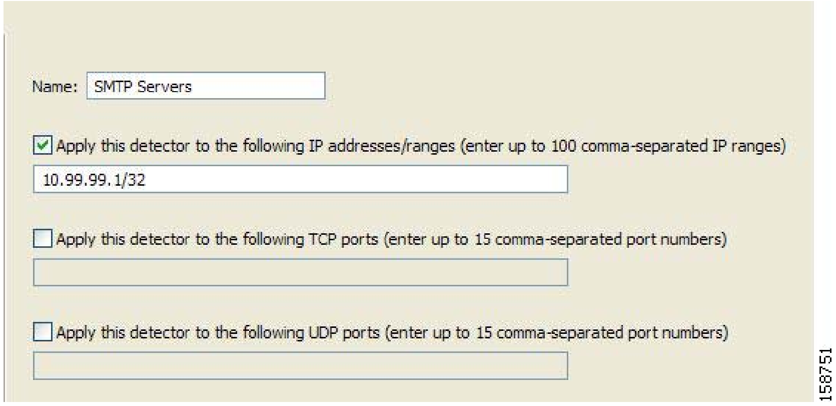
Add, remove and set the order of the detectors. Detectors are checked from the bottom up and the first match triggers detection.
The Default Detector is checked last.

- Scan/Sweep
  - Scan/Sweep Default Detector
- DoS
  - DoS Default Detector
- DDoS
  - DDoS Default Detector

Step 2 In the detector tree, select a detector.

The detector parameters are displayed in the upper right area of the dialog box (Figure 10-3).

Figure 10-3 Detector Parameters



Name: SMTP Servers

☑ Apply this detector to the following IP addresses/ranges (enter up to 100 comma-separated IP ranges)

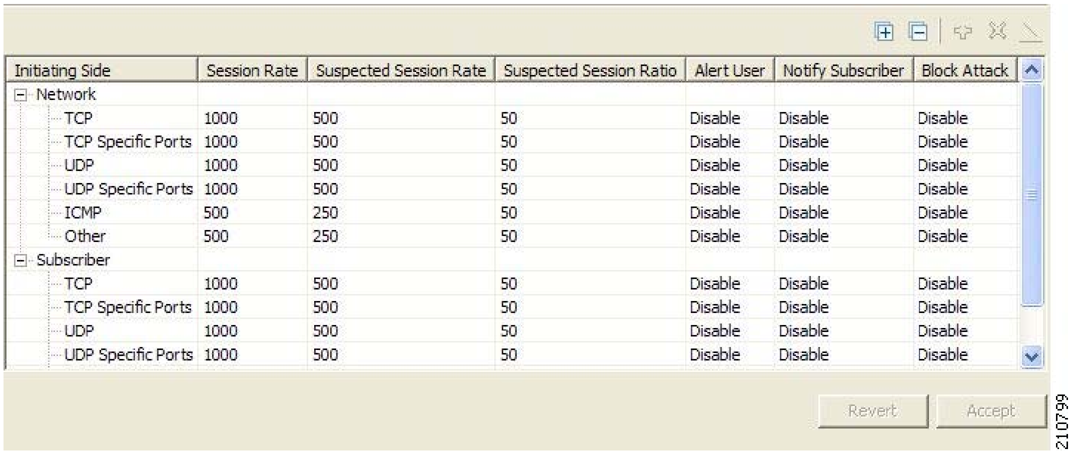
10.99.99.1/32

□ Apply this detector to the following TCP ports (enter up to 15 comma-separated port numbers)

□ Apply this detector to the following UDP ports (enter up to 15 comma-separated port numbers)

The anomaly types defined for a detector are listed in the lower right area of the dialog box, together with the value of each parameter. The following screen capture shows the default parameter values for the Scan/Sweep default detector (Figure 10-4).

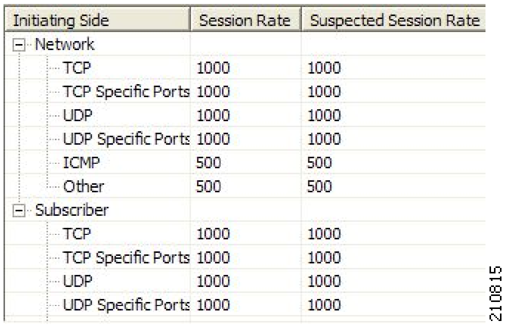
Figure 10-4 Detector Defined Anomaly Types



Initiating Side	Session Rate	Suspected Session Rate	Suspected Session Ratio	Alert User	Notify Subscriber	Block Attack
⊟ Network						
TCP	1000	500	50	Disable	Disable	Disable
TCP Specific Ports	1000	500	50	Disable	Disable	Disable
UDP	1000	500	50	Disable	Disable	Disable
UDP Specific Ports	1000	500	50	Disable	Disable	Disable
ICMP	500	250	50	Disable	Disable	Disable
Other	500	250	50	Disable	Disable	Disable
⊟ Subscriber						
TCP	1000	500	50	Disable	Disable	Disable
TCP Specific Ports	1000	500	50	Disable	Disable	Disable
UDP	1000	500	50	Disable	Disable	Disable
UDP Specific Ports	1000	500	50	Disable	Disable	Disable

If unidirectional classification is enabled, the Suspected Session Rate is set equal to the Session Rate, which effectively disables anomaly detection by the suspected session trigger (Figure 10-5).

Figure 10-5 Session Rate to Suspected Session Rate Comparison



Initiating Side	Session Rate	Suspected Session Rate
⊟ Network		
TCP	1000	1000
TCP Specific Ports	1000	1000
UDP	1000	1000
UDP Specific Ports	1000	1000
ICMP	500	500
Other	500	500
⊟ Subscriber		
TCP	1000	1000
TCP Specific Ports	1000	1000
UDP	1000	1000
UDP Specific Ports	1000	1000

Step 3 Click **OK**.

The Anomaly Detection Settings dialog box closes.

How to Add Anomaly Detectors

You can add new anomaly detectors. A service configuration can contain up to 100 anomaly detectors.

You define IP address ranges and TCP and UDP ports for the new detector, and one anomaly type.

After you have defined the detector, you can add other anomaly types (see Editing Anomaly Detectors, page 10-13).

Step 1 In the Service Security Dashboard, in the Anomaly Based Detection of Malicious Traffic pane, click **Configure**.

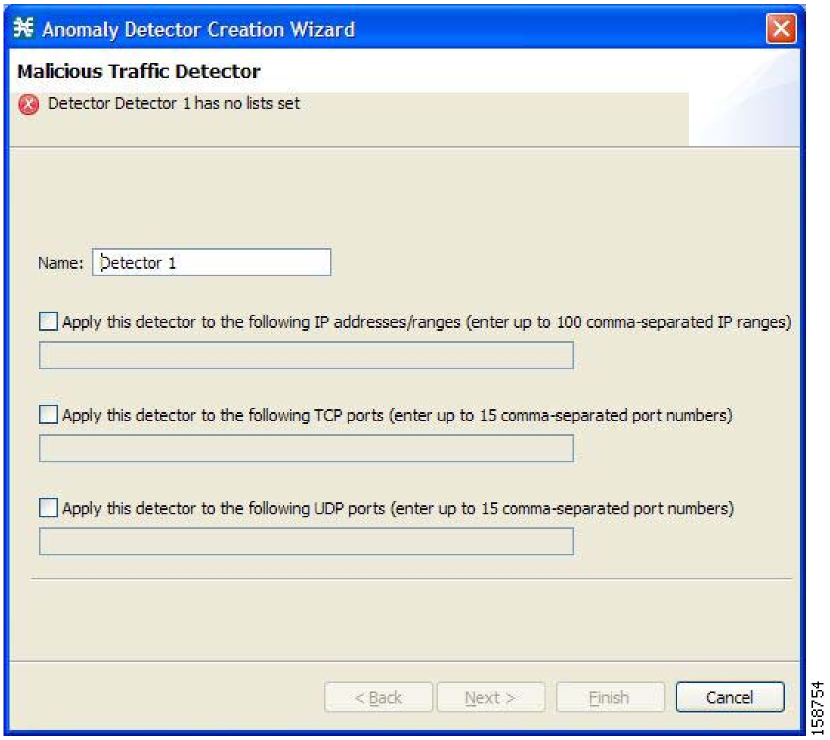
The Anomaly Detection Settings dialog box appears.

Step 2 In the detector tree, select a detector category.

Step 3 Click the **Add** (✚) icon.

The Anomaly Detector Creation wizard appears (Figure 10-6), open to the Malicious Traffic Detector page.

Figure 10-6 Anomaly Detector Creation Wizard - Malicious Traffic Detector



Anomaly Detector Creation Wizard

Malicious Traffic Detector

Detector Detector 1 has no lists set

Name: Detector 1

□ Apply this detector to the following IP addresses/ranges (enter up to 100 comma-separated IP ranges)

□ Apply this detector to the following TCP ports (enter up to 15 comma-separated port numbers)

□ Apply this detector to the following UDP ports (enter up to 15 comma-separated port numbers)

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

Step 5 Check one or more of the check boxes to limit the scope of the detector.

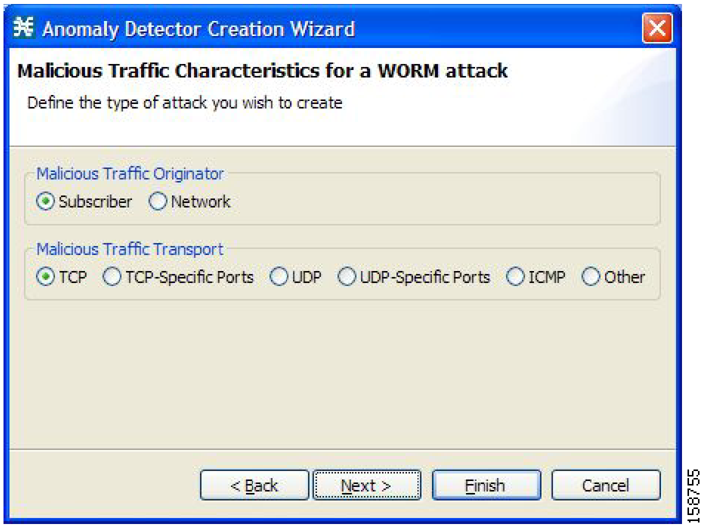
The relevant fields are enabled.

Step 6 Enter lists of IP addresses or ports in the relevant fields.

Step 7 Click **Next**.

The Malicious Traffic Characteristics for a WORM attack page of the Anomaly Detector Creation wizard opens (Figure 10-7).

Figure 10-7 Malicious Traffic Characteristics for a Worm Attack



Anomaly Detector Creation Wizard

Malicious Traffic Characteristics for a WORM attack

Define the type of attack you wish to create

Malicious Traffic Originator

● Subscriber ○ Network

Malicious Traffic Transport

● TCP ○ TCP-Specific Ports ○ UDP ○ UDP-Specific Ports ○ ICMP ○ Other

Step 8 Depending on the detector type that you are defining, select the originating side or the target side.

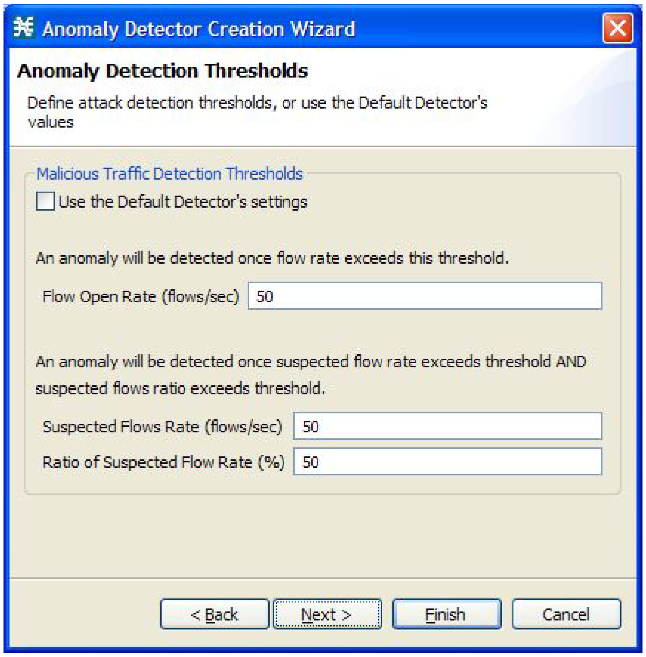
- If you are defining a Scan/Sweep detector or a DoS detector, select the originating side for the anomaly type you are defining.
- If you are defining a DDoS detector, select the target side for the anomaly type you are defining.

Step 9 Select a transport type for the anomaly type that you are defining.

Step 10 Click **Next**.

The Anomaly Detection Thresholds page of the Anomaly Detector Creation wizard opens (Figure 10-8).

Figure 10-8 Anomaly Detection Thresholds



Anomaly Detector Creation Wizard

Anomaly Detection Thresholds

Define attack detection thresholds, or use the Default Detector's values

Malicious Traffic Detection Thresholds

□ Use the Default Detector's settings

An anomaly will be detected once flow rate exceeds this threshold.

Flow Open Rate (flows/sec): 50

An anomaly will be detected once suspected flow rate exceeds threshold AND suspected flows ratio exceeds threshold.

Suspected Flows Rate (flows/sec): 50

Ratio of Suspected Flow Rate (%): 50

Step 11 Set the detector settings for this anomaly type.

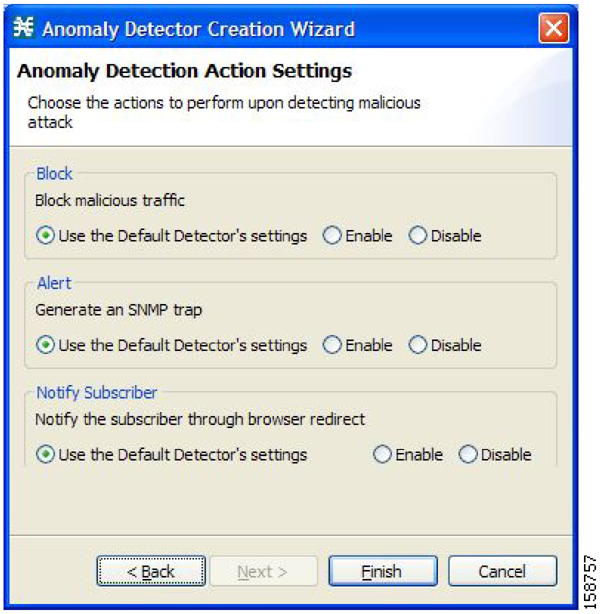
Do one of the following:

- To use the setting for the default detector, check the **Use the Default Detector's settings** check box.
- Enter values in the Flow Open Rate, Suspected Flows Rate, and Ratio of Suspected Flow Rate fields.

Step 12 Click **Next**.

The Anomaly Detection Action Settings page of the Anomaly Detector Creation wizard opens (Figure 10-9).

Figure 10-9 Anomaly Detection Action Settings



Anomaly Detector Creation Wizard

Anomaly Detection Action Settings

Choose the actions to perform upon detecting malicious attack

Block

Block malicious traffic

● Use the Default Detector's settings ○ Enable ○ Disable

Alert

Generate an SNMP trap

● Use the Default Detector's settings ○ Enable ○ Disable

Notify Subscriber

Notify the subscriber through browser redirect

● Use the Default Detector's settings ○ Enable ○ Disable

Step 13 Select Block, Alert, and Notify Subscriber actions.

Step 14 Click **Finish**.

The Anomaly Detector Creation wizard closes.

The new detector is added to the detector tree.

What to Do Next

You can now add additional anomaly types to the detector. (See Editing Anomaly Detectors, page 10-13.)

Editing Anomaly Detectors

You can perform the following actions on a user-defined anomaly detector:

- Edit detector parameters.
- Edit anomaly types.
- Add anomaly types.
- Delete anomaly types.
- Change the order of the detectors in the detector tree.

  For each detector category, detectors are checked, *bottom-up,* in the order that they are listed in the detector tree; the default detector is checked last.

You can edit the anomaly types of the three default detectors.

How to Edit Detector Parameters

Step 1 In the Service Security Dashboard, in the Anomaly Based Detection of Malicious Traffic pane, click **Configure**.

The Anomaly Detection Settings dialog box appears.

Step 2 In the detector tree, select a detector.

The detector parameters are displayed in the upper right area of the dialog box.

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

Step 4 Check or uncheck the IP address range and ports check boxes.

Step 5 Enter or modify lists of IP addresses or ports in the relevant fields.

Step 6 Click **OK**.

The Anomaly Detection Settings dialog box closes.

Your changes are saved.

How to Edit Anomaly Types

Step 1 In the Service Security Dashboard, in the Anomaly Based Detection of Malicious Traffic pane, click **Configure**.

The Anomaly Detection Settings dialog box appears.

Step 2 In the detector tree, select a detector.

Information about the anomaly types is displayed in the lower right area of the dialog box.

Step 3 Double-click an anomaly type.

The Anomaly Detector Creation wizard appears, open to the Anomaly Detection Thresholds page (see How to Add an Anomaly Type, page 10-15).

Step 4 Set the detector settings for this anomaly type.

Do one of the following:

- To use the setting of the default detector, check the **Use the Default Detector's settings** check box.
- Change the values in the Flow Open Rate, Suspected Flows Rate, and Ratio of Suspected Flow Rate fields.

Step 5 Click **Next**.

The Anomaly Detection Action Settings page of the Anomaly Detector Creation wizard opens.

Step 6 Change Block, Alert, and Notify Subscriber actions.

Step 7 Click **Finish**.

The Anomaly Detector Creation wizard closes.

The anomaly type is updated with your changes.

Step 8 Repeat Steps 3 to 7 (or Steps 2 to 7) for other anomaly types.

Step 9 Click **OK**.

The Anomaly Detection Settings dialog box closes.

How to Add an Anomaly Type

Step 1 In the Service Security Dashboard, in the Anomaly Based Detection of Malicious Traffic pane, click **Configure**.

The Anomaly Detection Settings dialog box appears.

Step 2 In the detector tree, select a detector.

The anomaly types are listed in the lower right area of the dialog box.

Step 3 Click the **Create New Detector Item Under Detector Items Feature** (➕) icon.

The Anomaly Detector Creation wizard appears, open to the Malicious Traffic Characteristics for a WORM attack page (see How to Add Anomaly Detectors, page 10-9).

Step 4 Select an origin for the anomaly type you are defining.

Step 5 Select a transport type for the anomaly type you are defining.

Step 6 Click **Next**.

The Anomaly Detection Thresholds page of the Anomaly Detector Creation wizard opens.

Step 7 Set the detector settings for this anomaly type.

Do one of the following:

- To use the settings of the default detector, check the **Use the Default Detector's settings** check box.
- Enter values in the Flow Open Rate, Suspected Flows Rate, and Ratio of Suspected Flow Rate fields.

Step 8 Click **Next**.

The Anomaly Detection Action Settings page of the Anomaly Detector Creation wizard opens.

Step 9 Select Block, Alert, and Notify Subscriber actions.

Step 10 Click **Finish**.

The Anomaly Detector Creation wizard closes.

The new anomaly type is added to the anomaly type list.

Step 11 Repeat Steps 3 to 10 (or Steps 2 to 10) for other anomaly types.

Step 12 Click **OK**.

The Anomaly Detection Settings dialog box closes.

How to Delete an Anomaly Type

Step 1 In the Service Security Dashboard, in the Anomaly Based Detection of Malicious Traffic pane, click **Configure**.

The Anomaly Detection Settings dialog box appears.

Step 2 In the detector tree, select a detector.

The anomaly types are listed in the lower right area of the dialog box.

Step 3 In the anomaly type list, select an anomaly type.

Step 4 Click the **Delete** (✖) icon.

The selected anomaly type is deleted from the anomaly type list.

Step 5 Repeat Steps 3 and 4 (or Steps 2 to 4) for other anomaly types.

Step 6 Click **OK**.

The Anomaly Detection Settings dialog box closes.

How to Change the Order in which Detectors are Checked

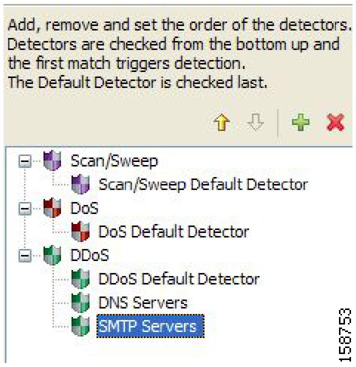
Step 1 In the Service Security Dashboard, in the Anomaly Based Detection of Malicious Traffic pane, click **Configure**.

The Anomaly Detection Settings dialog box appears.

Step 2 In the detector tree, select a detector.

The move up arrow, the move down arrow, or both are enabled, depending on the detectors location in the tree (Figure 10-10).

Figure 10-10 Detector Tree



Add, remove and set the order of the detectors. Detectors are checked from the bottom up and the first match triggers detection. The Default Detector is checked last.

Step 3 Using these navigation arrows, move the detector to its desired location.

Step 4 Repeat Steps 2 and 3 for other detectors.

Step 5 Click **OK**.

The Anomaly Detection Settings dialog box closes.

Your changes are saved.

How to Delete Anomaly Detectors

You can delete any or all user-defined detectors.

You cannot delete the three default detectors.

Step 1 In the Service Security Dashboard, in the Anomaly Based Detection of Malicious Traffic pane, click **Configure**.

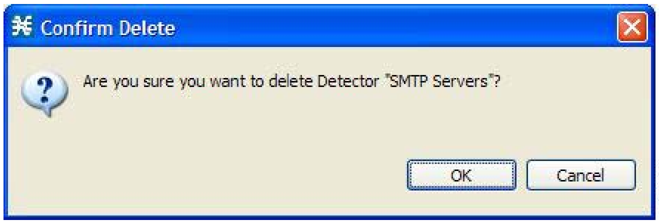
The Anomaly Detection Settings dialog box appears.

Step 2 In the detector tree, select one or more user-defined detectors.

Step 3 Click the **Delete** (✖) icon.

A Confirm Delete message appears (Figure 10-11).

Figure 10-11 Confirm Delete



Are you sure you want to delete Detector "SMTP Servers"?

Step 4 Click **OK**.

The selected detectors are deleted and are no longer displayed in the detector tree.

Step 5 Click **OK**.

The Anomaly Detection Settings dialog box closes.

Managing Spam Detection

The anomalous e-mail detection method monitors SMTP session rates for individual subscribers. A high rate of SMTP sessions from an individual subscriber is usually an indicator of malicious activity that involves sending e-mail (either mail-based viruses or spam-zombie activity).

This method works only if the system is configured in subscriber-aware or anonymous subscriber mode. This allows the SCE to accurately account the number of SMTP sessions generated per subscriber.

The detection method is based on the following:

- Typical broadband subscribers generate few SMTP sessions (at most a single session each time they send an e-mail message).
- Typical broadband subscribers normally use the SMTP server of the ISP (as configured in their mail client) as their only mail relay, and do not communicate with off-net SMTP servers.
- Spam zombies create many SMTP sessions, mainly to off-net servers (the mail servers of the destined recipient of the messages).

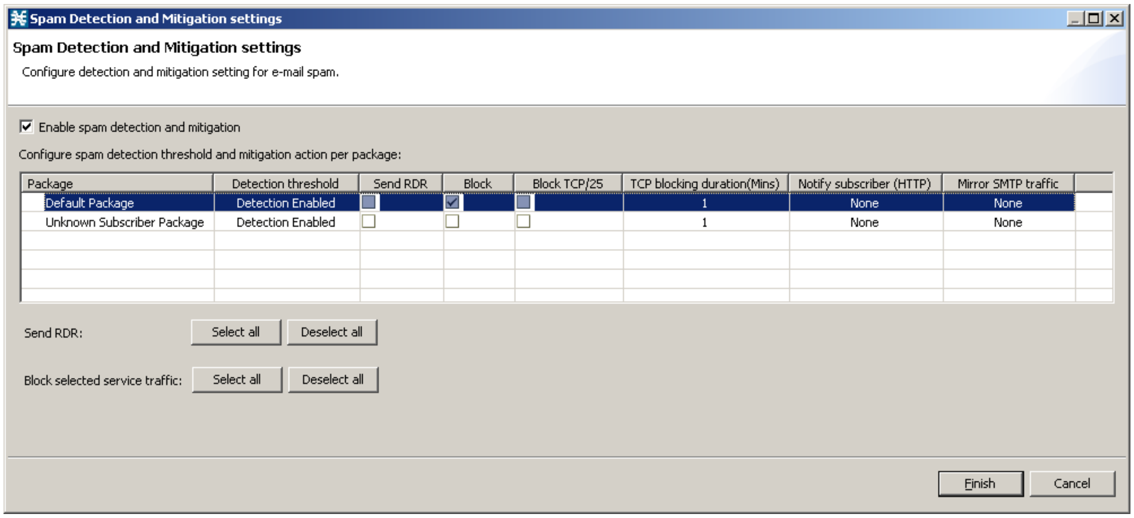
When configuring spam detection, you select an appropriate service to monitor. By default, this is the built-in SMTP service.

How to Configure Spam Detection Settings

Step 1 In the Service Security Dashboard, in the Spam Zombies and Email Viruses Detection pane, click **Configure**.

The Spam Detection and Mitigation settings dialog box appears (Figure 10-12).

Figure 10-12 Spam Detection and Mitigation Settings



Spam Detection and Mitigation settings

Spam Detection and Mitigation settings

Configure detection and mitigation setting for e-mail spam.

☑ Enable spam detection and mitigation

Configure spam detection threshold and mitigation action per package:

Package	Detection threshold	Send RDR	Block	Block TCP/25	TCP blocking duration(Mins)	Notify subscriber (HTTP)	Mirror SMTP traffic
Default Package	Detection Enabled	☐	☑	☐	1	None	None
Unknown Subscriber Package	Detection Enabled	☐	☐	☐	1	None	None

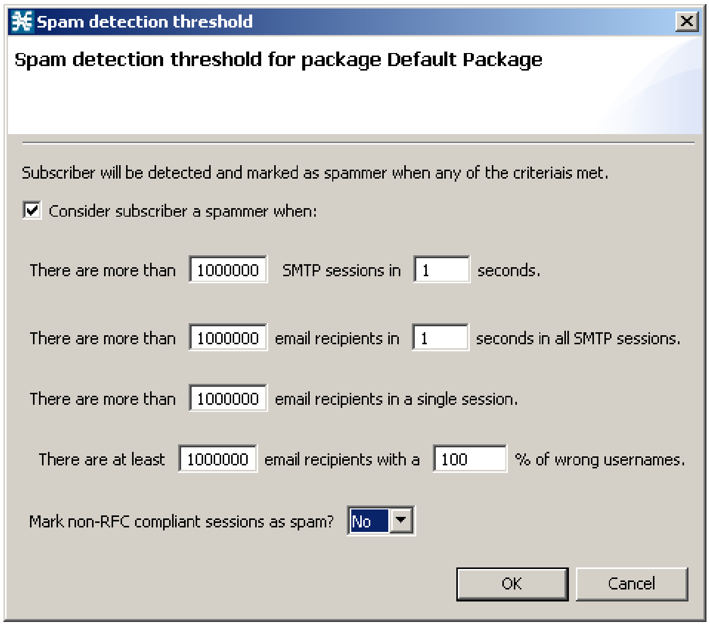
Step 2 (Optional) To disable spam detection, uncheck the **Enable Spam detection and mitigation** check box. All other fields are disabled. If you are disabling spam detection, continue at Step 6.

Step 3 For each package, do the following:

a. Define the quota to be used for indicating anomalous e-mail activity. We recommend that the values for these fields should be based on some baseline monitoring of subscriber activity.

- Click in the Detection threshold column. A **More** (...) button appears.
- Click the More button. The Spam Detection Threshold window appears (Figure 10-13).
- Define when to consider the subscriber as a spammer.
- Define whether to mark non-RFC compliant sessions as spam.
- Click **OK**.

Figure 10-13 Spam Detection Threshold



Spam detection threshold

Spam detection threshold for package Default Package

Subscriber will be detected and marked as spammer when any of the criteriais met.

☑ Consider subscriber a spammer when:

There are more than 1000000 SMTP sessions in 1 seconds.

There are more than 1000000 email recipients in 1 seconds in all SMTP sessions.

There are more than 1000000 email recipients in a single session.

There are at least 1000000 email recipients with a 100 % of wrong usernames.

Mark non-RFC compliant sessions as spam? No

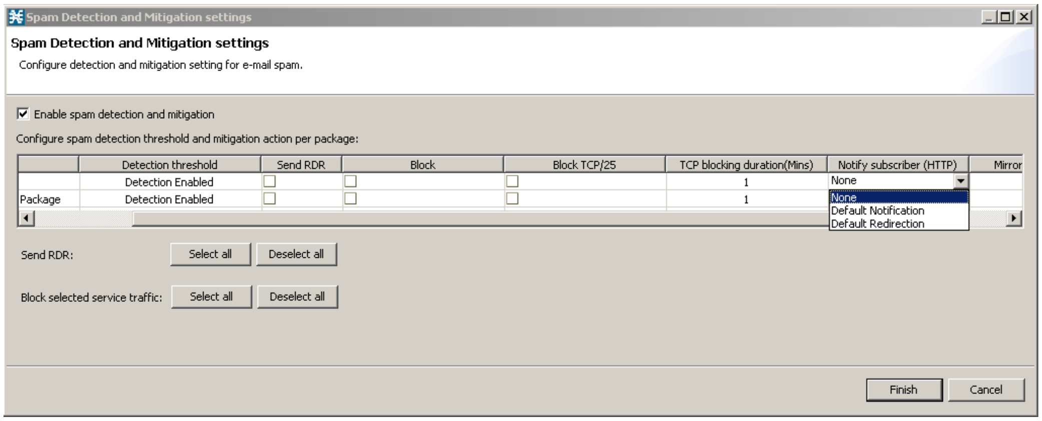
b. Define one or more actions to be taken upon detecting mass-mailing activity. Available actions are:

- **Send RDR—**Sends a Raw Data Record (RDR) to the Collection Manager (CM). A second RDR is sent when the status of the subscriber as a spammer is removed. The Collection Manager collects these RDRs in CSV files for logging purposes. Alternatively, you can implement your own RDR collectors to receive these RDRs and respond in real-time.
- **Block—**Blocks SMTP as a classified service.
- **Block TCP/25—**Blocks only the TCP port 25.
- **TCP blocking duration (Mins)—**Defines the duration for which the TCP port 25 should be blocked.
- **Notify Subscriber (HTTP)—**Redirects the subscriber browsing sessions to a captive portal presenting a message from the operator. This is done using “subscriber notification”. Options are None, Default Notification, Default Redirection.
- **Mirror SMTP traffic—**Diverts spam SMTP traffic to an inline spam detection service.

Note For the send RDR action, one RDR is sent when the subscriber is marked as a spammer and a second RDR is sent once the subscriber is no longer considered a spammer. However, when using the block and mirror actions, the action begins when the subscriber is marked as a spammer and is maintained until the subscriber is no longer considered a spammer.

Note Block SMTP Traffic and Mirror SMTP traffic cannot both be selected. If you select one, the other is disabled.

Step 4 If you selected Notify Subscriber (HTTP), choose or enter a notify subscriber.



Spam Detection and Mitigation settings

Configure detection and mitigation setting for e-mail spam.

☑ Enable spam detection and mitigation

Configure spam detection threshold and mitigation action per package:

	Detection threshold	Send RDR	Block	Block TCP/25	TCP blocking duration(Mins)	Notify subscriber (HTTP)	Mirror
	Detection Enabled	□	□	□	1	None	
Package	Detection Enabled	□	□	□	1		

Step 5 If you selected Mirror SMTP traffic, choose a server group.

Step 6 Click **Finish**.

The Spam Detection and Mitigation settings dialog box closes.

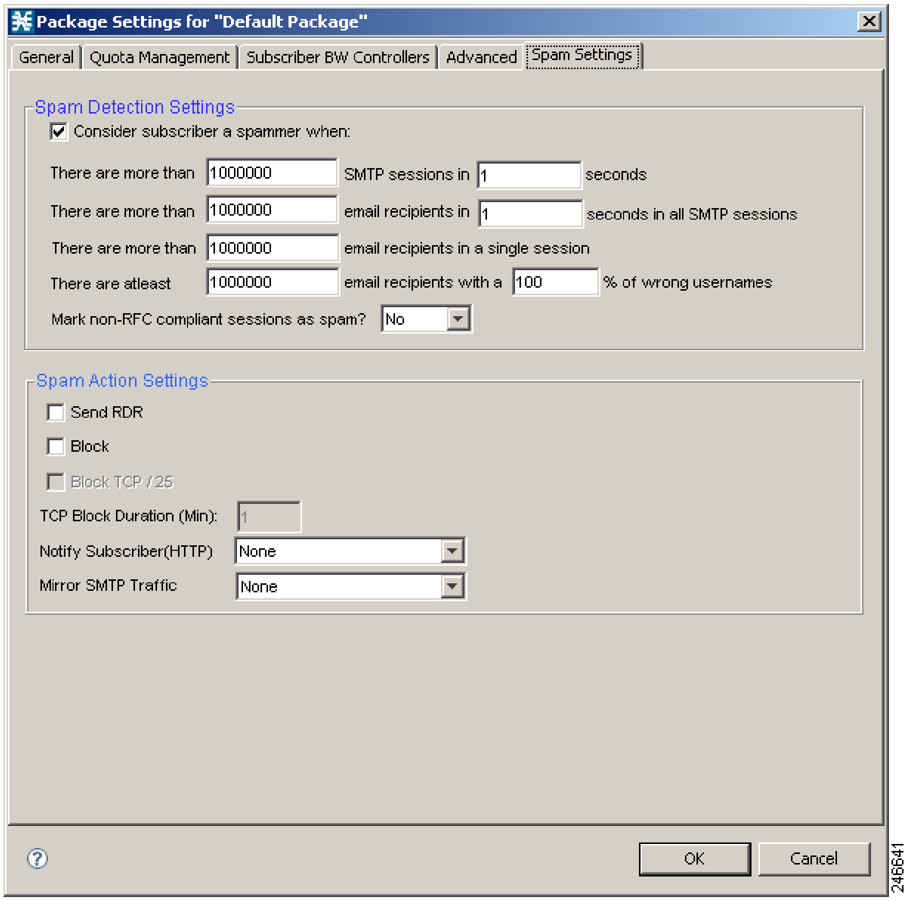
How to Configure Outgoing Spam Mitigation Settings per Package from Subscriber Policies

To configure the outgoing spam mitigation settings per package from subscriber policies, complete these steps:

Step 1 In the Service Configuration Editor Policies tab, select a Package from the **Subscriber Policies**.

Step 2 Right-click on the Package and select **Edit Package**. The Package Settings window appears.

Step 3 Click Spam Settings tab to view the Spam Detection Settings and Spam Action Settings.



Package Settings for "Default Package"

General | Quota Management | Subscriber BW Controllers | Advanced | Spam Settings

Spam Detection Settings

☑ Consider subscriber a spammer when:

There are more than 1000000 SMTP sessions in 1 seconds

There are more than 1000000 email recipients in 1 seconds in all SMTP sessions

There are more than 1000000 email recipients in a single session

There are atleast 1000000 email recipients with a 100 % of wrong usernames

Mark non-RFC compliant sessions as spam? No

Spam Action Settings

□ Send RDR

□ Block

□ Block TCP / 25

TCP Block Duration (Min): 1

Notify Subscriber(HTTP) None

Mirror SMTP Traffic None

Step 4 Select the **Consider Subscriber a spammer when:** check box to enable the spam detection.

Step 5 Define when to consider the subscriber a spammer and the actions to be taken.

Step 6 Click **OK**.

For more details on spam mitigation, see the *Cisco Service Control Service Security: Outgoing Spam Mitigation Solution Guide*.

Viewing Malicious Traffic Reports

Information about detected traffic anomalies is stored in the Collection Manager database. You can use this information for network trending, detection of new threats, and tracking of malicious hosts or subscribers.

- Malicious Traffic Reports, page 10-21
- How to View a Service Security Report, page 10-22

Malicious Traffic Reports

A number of reports dealing with malicious traffic can be displayed in the SCA Reporter tool:

- Global reports:
  - Global Scan or Attack Rate
  - Global DoS Rate
  - Infected Subscribers
  - Infected Subscribers versus Active Subscribers
  - DoS Attacked Subscribers
  - Top Scanned or Attacked ports
- Individual subscriber or hosts reports:
  - Top Scanning or Attacking hosts
  - Top DoS Attacked hosts
  - Top DoS Attacked Subscribers
  - Top Scanning or Attacking Subscribers

How to View a Service Security Report

Step 1 In the Service Security Dashboard, in the relevant pane, click **View Report**.

A Choose a report dialog box appears, displaying a tree of relevant reports.

Step 2 Select a report from the report tree.

Step 3 Click **OK**.

The Choose a report dialog box closes.

The Reporter tool opens in the Console, and displays the requested report.

Step 4 For information about manipulating and saving the report, see the “Working with Reports” chapter of *Cisco Service Control Application Reporter User Guide.*

Filtering the Traffic Flows

Filter rules are part of service configurations. They allow you to instruct the Service Control Engine (SCE) platform, based on a flow's Layer 3 and Layer 4 properties, to:

- Bypass—Ignore the flow and transmit it unchanged.
- Quick forward—Duplicate the flow and send one copy directly to the transmit queue to ensure minimal delay. The second copy goes through the normal packet path.

When a traffic flow enters the SCE platform, the platform checks whether a filter rule applies to this flow.

If a filter rule applies to this traffic flow, the SCE platform passes the traffic flow to its transmit queues. No RDR generation or service configuration enforcement is performed; these flows do not appear in any records generated for analysis purposes and are not controlled by any rule belonging to the active service configuration.

It is recommended that you add filter rules for OSS protocols (such as DHCP) and routing protocols (such as BGP) that might traverse the SCE platform. These protocols usually should not be affected by policy enforcement, and their low volume makes them insignificant for reporting.

A number of predefined filter rules are included in every new service configuration.

Note By default, some, but not all, of the predefined filter rules are active.

Flows of certain protocols can also be filtered according to the Layer 7 characteristics of the flow (see Managing Advanced Service Configuration Options, page 10-58). Like other filtered flows, Layer 7 filtered flows are not controlled, but can be classified and reported. The flows of the protocols that can be filtered are typically short and their overall volume is negligible. So filtering these protocols has little effect on network bandwidth and on the accuracy of the Cisco SCA BB reports.

- Information About Traffic Filtering, page 10-23
- How to View Filter Rules for a Package, page 10-26
- How to Add Filter Rules, page 10-27
- How to Add Filter Rules for IPv6 Configuration, page 10-33
- How to Edit Filter Rules, page 10-39
- How to Delete Filter Rules, page 10-39
- How to Activate and Deactivate Filter Rules, page 10-40

Information About Traffic Filtering

For certain types of traffic, service providers may need to reduce the latency and jitter introduced by the SCE platform or even to bypass the SCE platform to avoid traffic control as well. Typically, such decisions are made for a portion of the traffic, to reduce latency for delay sensitive applications, such as voice, and to bypass mission-critical traffic, such as routing protocols. The Cisco SCA BB Filtered Traffic mechanism is used to address this need.

Note To reduce latency, SCE platform automatically handles most voice traffic. For details, see Automatic Quick Forwarding of Media Flows, page 10-26.

- The Cisco SCA BB Filtered Traffic Mechanism, page 10-24
- Filter Rule Actions, page 10-25
- Filter Rules and Service Rules, page 10-25
- Automatic Quick Forwarding of Media Flows, page 10-26

The Cisco SCA BB Filtered Traffic Mechanism

The Cisco SCA BB Filtered Traffic mechanism reduces latency or completely bypasses portions of the traffic by defining *filter rules* that match relevant flows and assign the correct action to them. A filter rule matches a packet according to its Layer 3 and Layer 4 properties, such as IP address, port number, and DSCP ToS, as well as the SCE platform interface (subscriber or network) from which the packet arrived. For packets that match a filter rule, the following actions can be applied:

- Bypass the current packet (to reduce latency and avoid traffic control).

  When this action is applied, the current packet is directly transmitted from the SCE platform without going through any service configuration processing or reporting. You must map the bypassed packet to a Class of Service (CoS) to assign it to one of the transmit queues of the SCE platform.

  Possible values for CoS are BE, AF1, AF2, AF3, AF4, and EF; where EF implies high processing priority and the other classes imply normal processing priority.

- Quick forward the flow (to reduce latency).

  When this action is applied, the current packet and all subsequent packets belonging to the same flow are duplicated and sent through two different paths: the original packet goes directly to the transmit queue, and thus has only a minimal delay, while a copy of the packet goes through the normal service configuration processing path for classification and reporting, and is then discarded.

- Assign the flow to the high priority processing input queue (to reduce latency).

Note Not all platforms support this option.

When this action is applied, the current packet and all subsequent packets belonging to the same flow enter the high priority processing input queue. They go through the normal service configuration processing path ahead of other packets that arrive simultaneously. You should map the flow to the EF CoS to assign it to the high processing priority transmit queue of the SCE platform.

Note In an MPLS environment, the SCE platform does not map the DSCP bits to the EXP bits of the MPLS header.

A filter rule can perform DSCP ToS marking (by changing the DSCP ToS field of the packet) of the matched traffic with any of the above actions.

Note DSCP ToS marking and the assignment to CoS only take place when the operational mode of the system is Full Functionality (see System Operational Mode, page 10-56).

The Cisco SCE processes the traffic based on the Class of Service (CoS). Possible values for CoS are BE, AF1, AF2, AF3, AF4, and EF; where EF implies high processing priority and the other classes imply normal processing priority.

In SCE 8000, if there are 4 output queues—EF, AF*n*,AF1, and BE, this is how the queues are prioritized:

- EF—Gets the highest priority and strictly gets priority over all other queues.
- AF1 and AF*n* (AF2, AF3, AF4)—Gets the weighted priority on top of AF1. For each *n* packets of AF*n*, one packet is sent for AF1. The value of *n* can be configured from the FPGA. The default value is 3.
- BE—Gets lowest priority. BE packets are transmitted only if packets for transmission are not available in other queues.

The SCE transmits only the received packet and do not generate the traffic internally; other than rarely transmit inject for reset or redirect. So, there can never be a long time in which lower priority queues are starved.

When there are only buckets—EF and the rest. In CoS other than EF (AF1,AF2,AF3,AF4,BE), the order of priority would be AF1 > AF2 > and so on. However, the bandwidth is allocated in the order EF > AF*n* > AF1 > BE. Queues AF2, AF3, and AF4 would have the same weight.

Filter Rule Actions

The Bypass and Quick forward actions apply to different scopes of traffic:

- The Bypass action only bypasses the current packet; every subsequent packet of the same flow goes through the Filtered Traffic mechanism. This means, for example, that when traffic is to be bypassed based on its destination port number, two rules should be created to match packets from both sides of a bidirectional flow.

  For example, to bypass all traffic to destination port 23, two filter rules are needed, one for packets arriving from the subscriber side addressed to network side port 23, and another for packets arriving from the network side addressed to subscriber side port 23.
- The Quick forward action is applied to the entire flow; once identified, all subsequent packets do not go through the filter rule mechanism, instead going through normal service configuration processing.

A packet may match more than one filter rule. If both Bypass and Quick forward are matched, the packet/flow is bypassed with minimum delay. Furthermore, if only Bypass is matched, the packet/flow is also be bypassed with minimum delay.

Filter Rules and Service Rules

Filter rule actions to reduce latency allow the flow to be controlled by the SCE platform. This means that the flow can be blocked or given limited bandwidth if it matches a service rule. For example, if a filter rule is applied to reduce latency, but a service configuration rule is applied to block the same traffic, the traffic is blocked.

The Bypass action is designed to avoid service configuration processing; bypassed traffic is not affected by service rules.

Automatic Quick Forwarding of Media Flows

The SCE platform reduces the latency of delay-sensitive voice and video media flows by applying the quick-forwarding action to SIP, MGCP, H323, Skinny, and RTSP media flows during classification. That is, when a media flow is classified as being of one of these types, it is subjected to quick forwarding immediately. The SCE platform does this automatically, regardless of filter rule configuration. These media flows might still be blocked or given limited bandwidth if they match a service rule.

Filtering L2TP Traffic

If you know the version of the L2TP tunnel that is being used, configure the relevant filters. If you do not know the version, enable filter for both type of tunnels (L2TPv2 and L2TPv3).

Note The L2TPv3 data encapsulation is done directly over IP with protocol ID 115. Cisco SCA BB provides a filter for this type of traffic and you can enable it from Cisco SCA BB.
However, L2TPv2 protocol data encapsulation is done over UDP protocol at Layer 4 with default destination port 1701. Cisco SCA BB does not provide any filter for this type of traffic. To filter L2TPv2 traffic, create a new filter with the transport type as UDP and destination UDP port value as 1701.

How to View Filter Rules for a Package

You can view a list of the filter rules included in a service configuration.

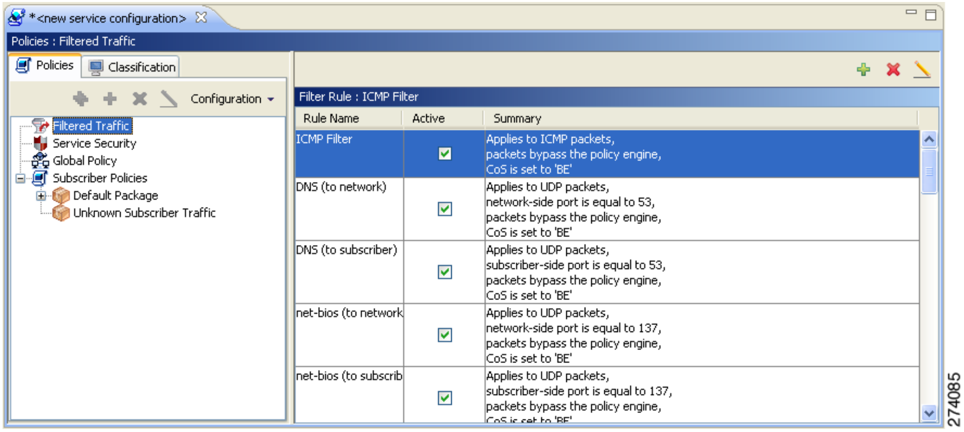
The listing for each filter rule includes the name, the status, and a brief description (generated by the system) of the rule.

To see more information about a filter rule, open the Edit Filter Rule dialog box (see How to Edit Filter Rules, page 10-39).

Step 1 In the Policies tab, select the **Filtered Traffic** node.

A list of all filter rules is displayed in the right (Rule) pane (Figure 10-14).

Figure 10-14 Filter Rules



Rule Name	Active	Summary
ICMP Filter	☑	Applies to ICMP packets, packets bypass the policy engine, CoS is set to 'BE'
DNS (to network)	☑	Applies to UDP packets, network-side port is equal to 53, packets bypass the policy engine, CoS is set to 'BE'
DNS (to subscriber)	☑	Applies to UDP packets, subscriber-side port is equal to 53, packets bypass the policy engine, CoS is set to 'BE'
net-bios (to network	☑	Applies to UDP packets, network-side port is equal to 137, packets bypass the policy engine, CoS is set to 'BE'
net-bios (to subscrib	☑	Applies to UDP packets, subscriber-side port is equal to 137, packets bypass the policy engine, CoS is set to 'BE'

How to Add Filter Rules

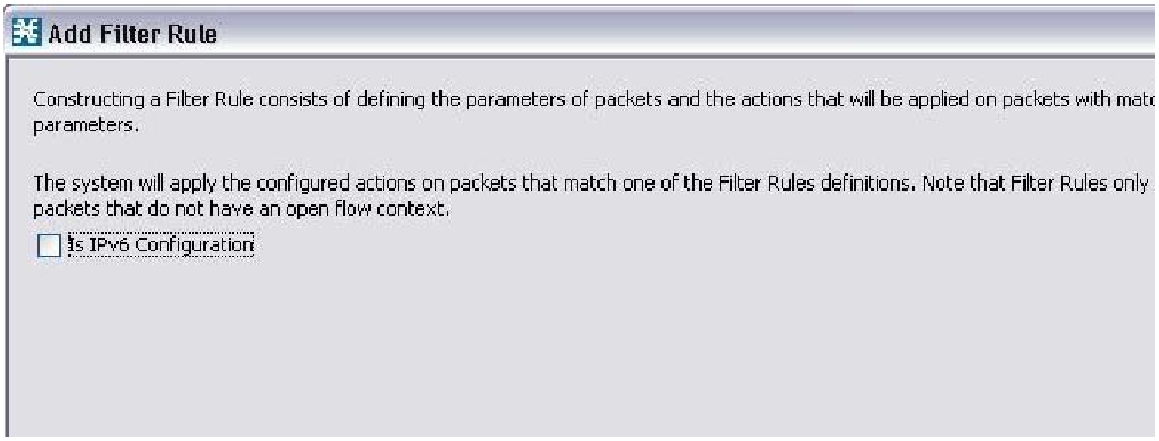
The Add Filter Rule wizard guides you through the process of adding a filter rule.

Step 1 In the Policies tab of Service Configuration Editor window, select the **Filtered Traffic** node.

Step 2 Click ✚ (**Add Rule)** in the right (Rule) pane.

The Add Filter Rule wizard appears (Figure 10-15).

Figure 10-15 Add Filter Rule



Constructing a Filter Rule consists of defining the parameters of packets and the actions that will be applied on packets with matc parameters.

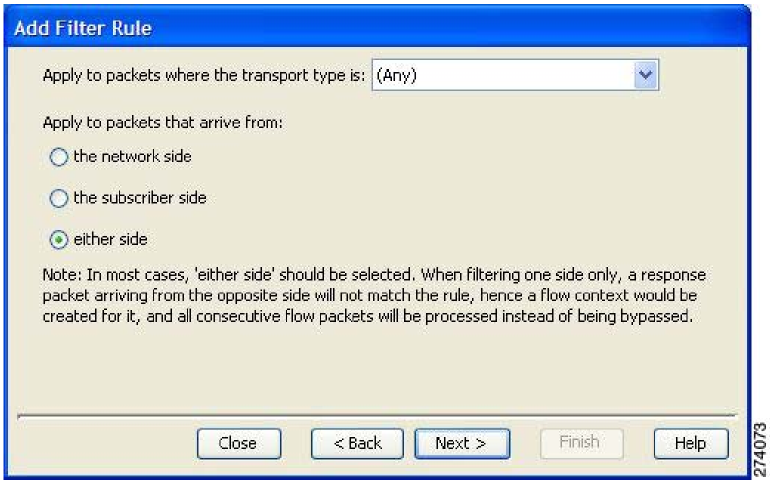
The system will apply the configured actions on packets that match one of the Filter Rules definitions. Note that Filter Rules only packets that do not have an open flow context.

☐ Is IPv6 Configuration

Step 3 Click **Next**.

The Transport Type and Direction screen of the Add Filter Rule wizard appears (Figure 10-16).

Figure 10-16 Transport Type and Direction



Add Filter Rule

Apply to packets where the transport type is: (Any)

Apply to packets that arrive from:

○ the network side

○ the subscriber side

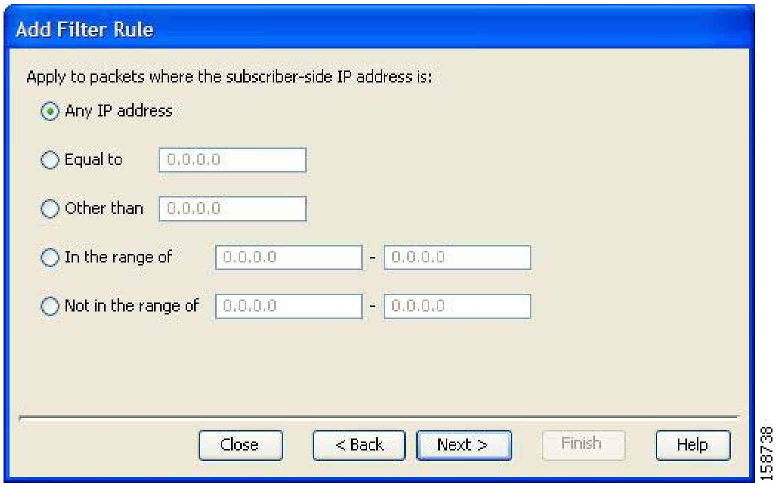
● either side

Note: In most cases, 'either side' should be selected. When filtering one side only, a response packet arriving from the opposite side will not match the rule, hence a flow context would be created for it, and all consecutive flow packets will be processed instead of being bypassed.

Step 4 Select the transport type and initiating side and click **Next**.

The Subscriber-Side IP Address screen of the Add Filter Rule wizard appears (Figure 10-17).

Figure 10-17 Subscriber-Side IP Address



Add Filter Rule

Apply to packets where the subscriber-side IP address is:

● Any IP address

○ Equal to 0.0.0.0

○ Other than 0.0.0.0

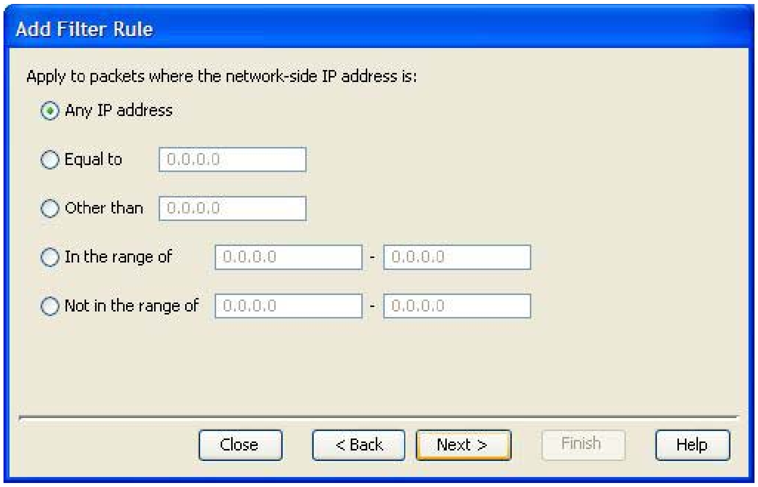
○ In the range of 0.0.0.0 - 0.0.0.0

○ Not in the range of 0.0.0.0 - 0.0.0.0

Step 5 Define the subscriber-side IP address and click **Next**.

The Network-Side IP Address screen of the Add Filter Rule wizard appears (Figure 10-18).

Figure 10-18 Network-Side IP Address



Add Filter Rule

Apply to packets where the network-side IP address is:

● Any IP address

○ Equal to 0.0.0.0

○ Other than 0.0.0.0

○ In the range of 0.0.0.0 - 0.0.0.0

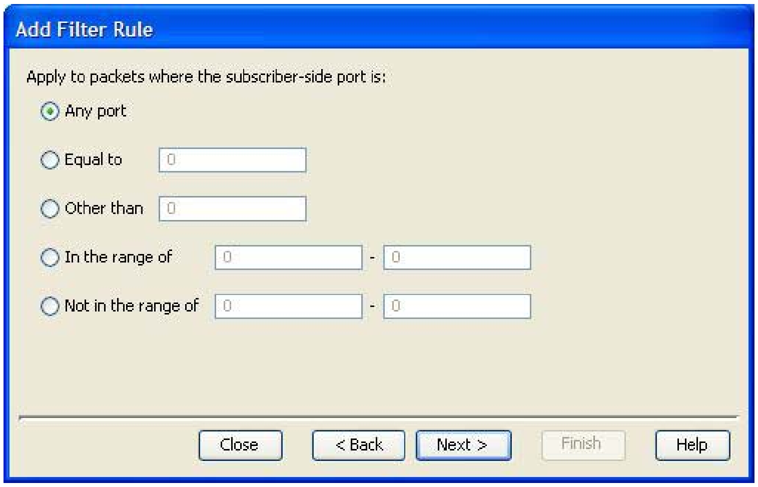
○ Not in the range of 0.0.0.0 - 0.0.0.0

Step 6 Define the network-side IP address and click **Next**.

If the transport type selected in Step 4 was not TCP or UDP, the ToS screen of the Add Filter Rule wizard appears. Go to Step 9.

If the transport type selected in Step 4 was TCP or UDP, the Subscriber-Side Port screen of the Add Filter Rule wizard appears (Figure 10-19).

Figure 10-19 Subscriber-Side Port



Add Filter Rule

Apply to packets where the subscriber-side port is:

● Any port

○ Equal to 0

○ Other than 0

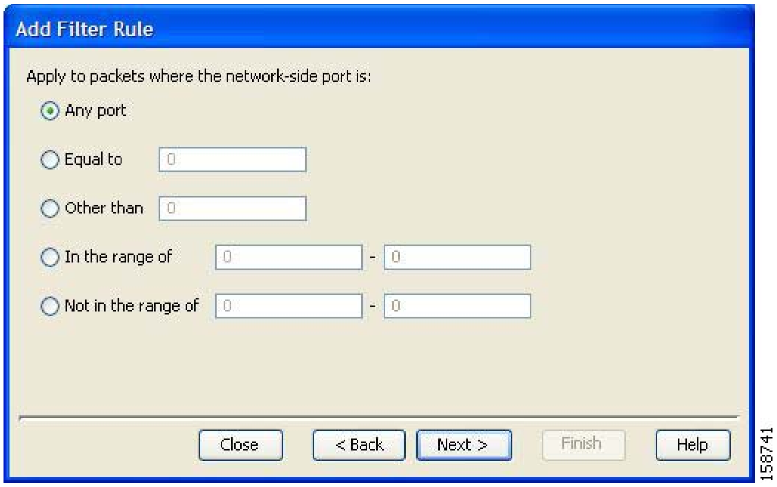
○ In the range of 0 - 0

○ Not in the range of 0 - 0

Step 7 Define the subscriber-side port and click **Next**.

The Network-Side Port screen of the Add Filter Rule wizard appears (Figure 10-20).

Figure 10-20 Network-Side Port



Add Filter Rule

Apply to packets where the network-side port is:

● Any port

○ Equal to 0

○ Other than 0

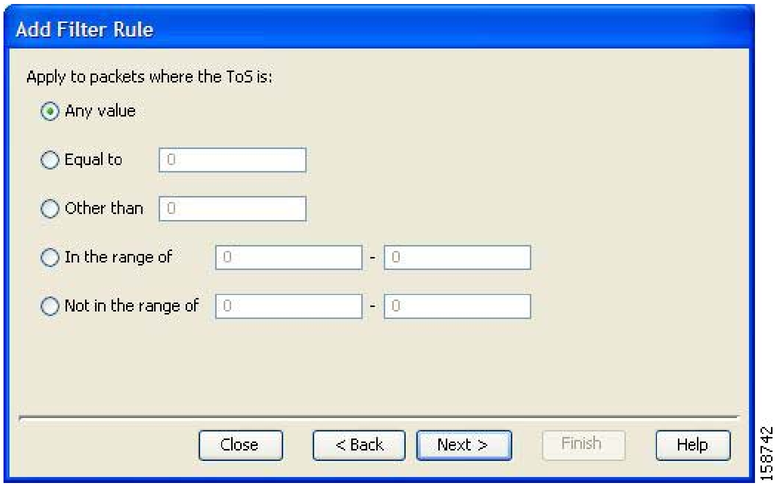
○ In the range of 0 - 0

○ Not in the range of 0 - 0

Step 8 Define the network-side port and click **Next**.

The Type of Service (ToS) screen of the Add Filter Rule wizard appears (Figure 10-21).

Figure 10-21 ToS



Add Filter Rule

Apply to packets where the ToS is:

● Any value

○ Equal to 0

○ Other than 0

○ In the range of 0 - 0

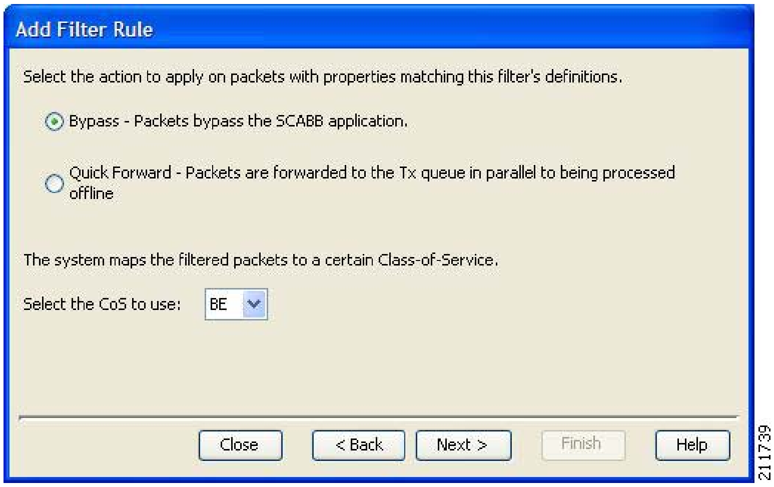
○ Not in the range of 0 - 0

Step 9 Define the ToS and click **Next**.

Note The acceptable values for ToS are 0 to 63.

The Action and Class-of-Service screen of the Add Filter Rule wizard appears (Figure 10-22).

Figure 10-22 Action and Class-of-Service



Add Filter Rule

Select the action to apply on packets with properties matching this filter's definitions.

● Bypass - Packets bypass the SCABB application.

○ Quick Forward - Packets are forwarded to the Tx queue in parallel to being processed offline

The system maps the filtered packets to a certain Class-of-Service.

Select the CoS to use: BE

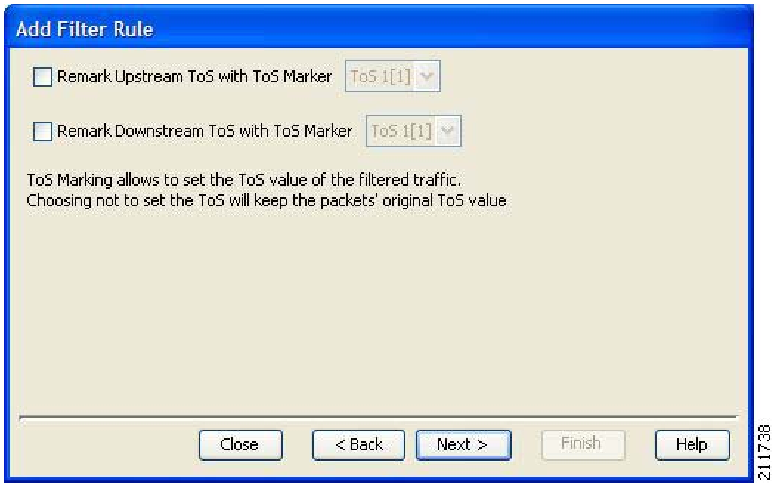
Step 10 Select the radio button for the required action.

- **Bypass** —Packets that match this filter rule are not passed to Cisco SCA BB.
- **Quick Forward** —The SCE platform ensures low latency for packets that match this filter rule (use for delay sensitive flows). Packets are duplicated and passed to Cisco SCA BB for processing.

Step 11 Select a Class-of-Service value, and click **Next**.

The ToS Marking screen of the Add Filter Rule wizard appears (Figure 10-23).

Figure 10-23 ToS Marking



Add Filter Rule

□ Remark Upstream ToS with ToS Marker ToS 1[1]

□ Remark Downstream ToS with ToS Marker ToS 1[1]

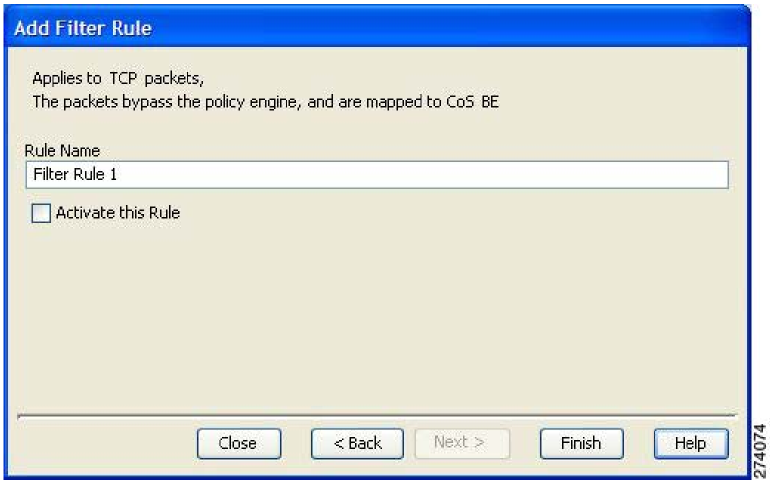
ToS Marking allows to set the ToS value of the filtered traffic.
Choosing not to set the ToS will keep the packets' original ToS value

Step 12 (Optional) To change the DSCP ToS marker of packets in the filtered traffic, check the **Remark Upstream ToS with ToS Marker** and **Remark Downstream ToS with ToS Marker** check boxes, as required, select the required ToS marker from the drop-down list, and click **Next**.

- Disabling directional DSCP ToS marking in the ToS Marking Settings dialog box (see How to Manage DSCP ToS Marker Values, page 9-81) overrides DSCP ToS marking in that direction by a filter (that is, the DSCP ToS value are not changed). In this case, the Problems View displays a Warning.
- If you filter for a flow in one direction in Step 4 but select ToS marking in the other direction in this Step, the filter rule is created, but no DSCP ToS remarking occurs. In this case, the Problems View displays a Warning.
- If you select Quick Forward in the previous Step, Cisco SCA BB receives the *original* package and processes it. That is, the application see the original DSCP ToS value regardless of the ToS marking action selected in the filter rule.

The Finish page of the Add Filter Rule wizard opens (Figure 10-24).

Figure 10-24 Finish


Add Filter Rule

Applies to TCP packets,
The packets bypass the policy engine, and are mapped to CoS BE

Rule Name
Filter Rule 1

☐ Activate this Rule

Step 13 In the Rule Name field, enter a unique name for the new filter rule.

Note You can use the default name for the filter rule. It is recommended that you enter a meaningful name.

Step 14 (Optional) To activate the filter rule, check the **Activate this rule** check box. Traffic is filtered according to the rule only when it is activated.

Step 15 Click **Finish**.

The Add Filter Rule wizard closes. The filter rule is added and is displayed in the Filter Rule table.

How to Add Filter Rules for IPv6 Configuration

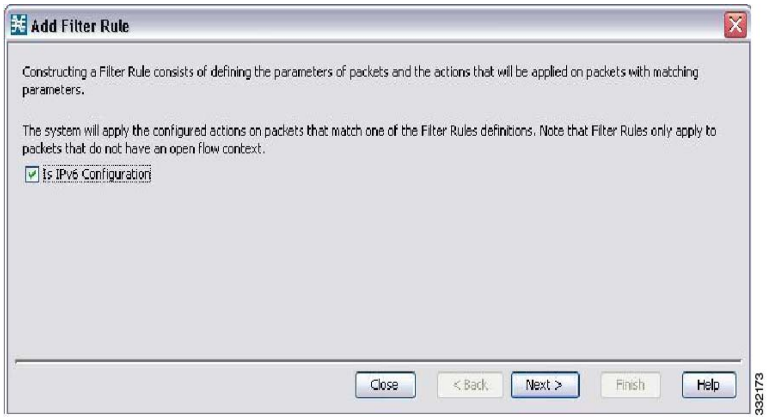
The Add Filter Rule wizard guides you through the process of adding a filter rule for IPv6 configuration.

Step 1 In the Policies tab of Service Configuration Editor window, select the **Filtered Traffic** node.

Step 2 Click ✚ (**Add Rule**) in the right (Rule) pane.

The Add Filter Rule wizard appears (Figure 10-25).

Figure 10-25 Add Filter Rule Wizard



Add Filter Rule

Constructing a Filter Rule consists of defining the parameters of packets and the actions that will be applied on packets with matching parameters.

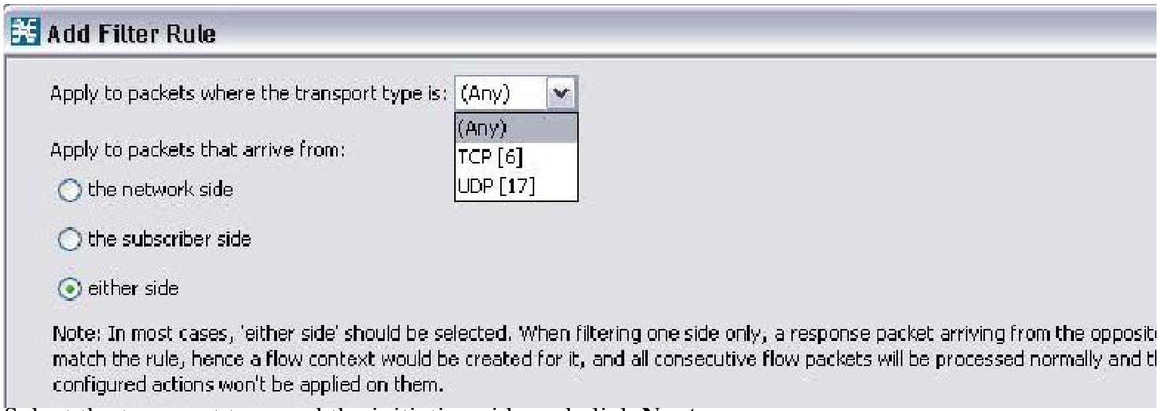
The system will apply the configured actions on packets that match one of the Filter Rules definitions. Note that Filter Rules only apply to packets that do not have an open flow context.

☑ Is IPv6 Configuration

Step 3 Select the **Is IPv6 Configuration** check box and click **Next**.

The Transport Type and Direction screen of the Add Filter Rule wizard appears (Figure 10-26).

Figure 10-26 Transport Type and Direction



Add Filter Rule

Apply to packets where the transport type is: (Any)
- (Any)
- TCP [6]
- UDP [17]

Apply to packets that arrive from:

○ the network side

○ the subscriber side

● either side

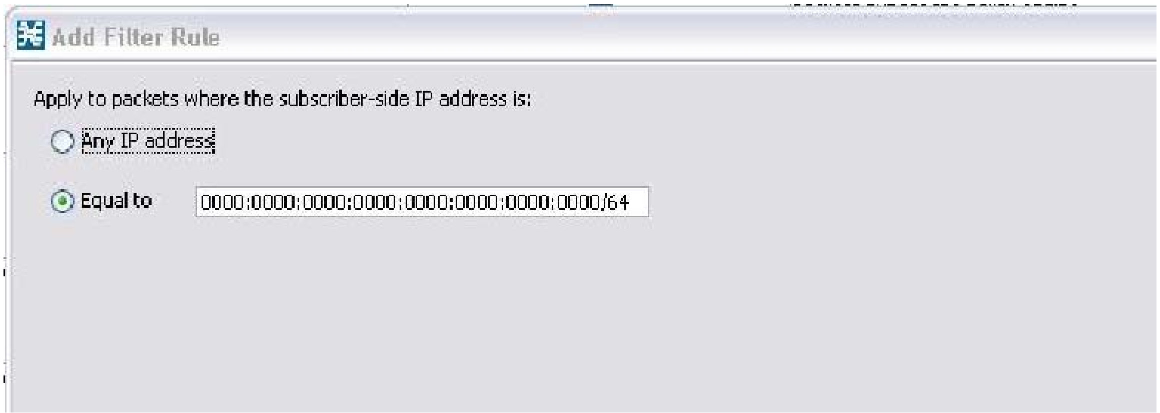
Note: In most cases, 'either side' should be selected. When filtering one side only, a response packet arriving from the opposit
match the rule, hence a flow context would be created for it, and all consecutive flow packets will be processed normally and t
configured actions won't be applied on them.

Step 4 Select the transport type and the initiating side and click **Next**.

The Subscriber-Side IP Address screen of the Add Filter Rule wizard appears (Figure 10-27).

Note The transport type drop-down will contain only the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) values.

Figure 10-27 Subscriber-Side IP Address



Add Filter Rule

Apply to packets where the subscriber-side IP address is:

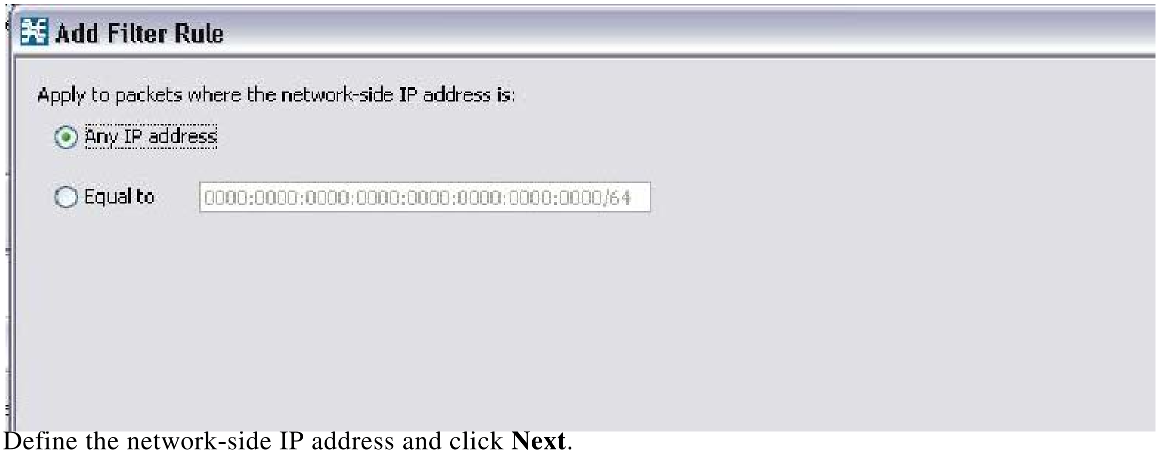
○ Any IP address

● Equal to 0000:0000:0000:0000:0000:0000:0000:0000/64

Step 5 Define the subscriber-side IP address and click **Next**.

The Network-Side IP Address screen of the Add Filter Rule wizard appears (Figure 10-28).

Figure 10-28 Network-Side IP Address



Apply to packets where the network-side IP address is:

● Any IP address

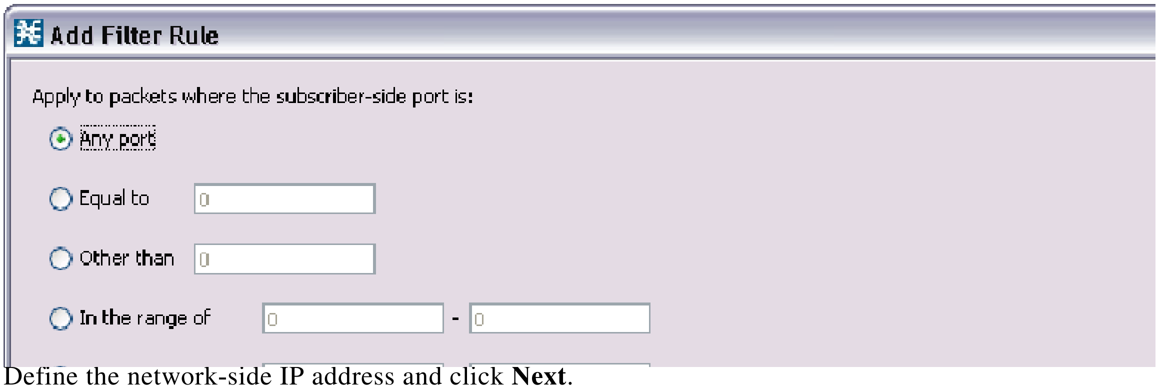
○ Equal to 0000:0000:0000:0000:0000:0000:0000:0000/64

Step 6 Define the network-side IP address and click **Next**.

If the transport type selected in Step 4 was not TCP or UDP, the ToS screen of the Add Filter Rule wizard appears. Go to Step 9.

If the transport type selected in Step 4 was TCP or UDP, the Subscriber-Side Port screen of the Add Filter Rule wizard appears (Figure 10-29).

Figure 10-29 Subscriber-Side Port



Apply to packets where the subscriber-side port is:

● Any port

○ Equal to 0

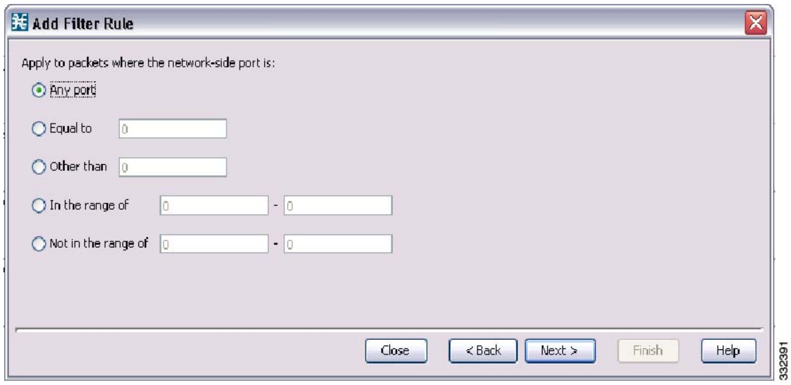
○ Other than 0

○ In the range of 0 - 0

Step 7 Define the network-side IP address and click **Next**.

The Network-Side Port screen of the Add Filter Rule wizard appears (Figure 10-30).

Figure 10-30 Network-Side Port



Add Filter Rule

Apply to packets where the network-side port is:

● Any port

○ Equal to 0

○ Other than 0

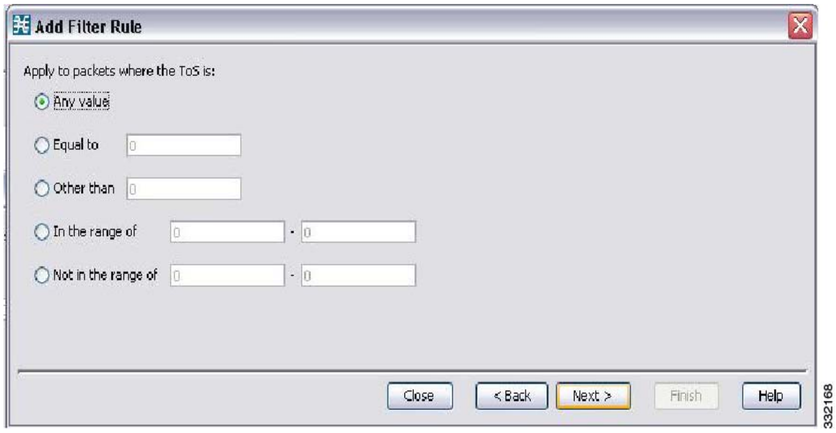
○ In the range of 0 - 0

○ Not in the range of 0 - 0

Step 8 Define the network-side port and click **Next**.

The ToS screen of the Add Filter Rule wizard appears (Figure 10-31).

Figure 10-31 ToS



Add Filter Rule

Apply to packets where the ToS is:

● Any value

○ Equal to 0

○ Other than 0

○ In the range of 0 - 0

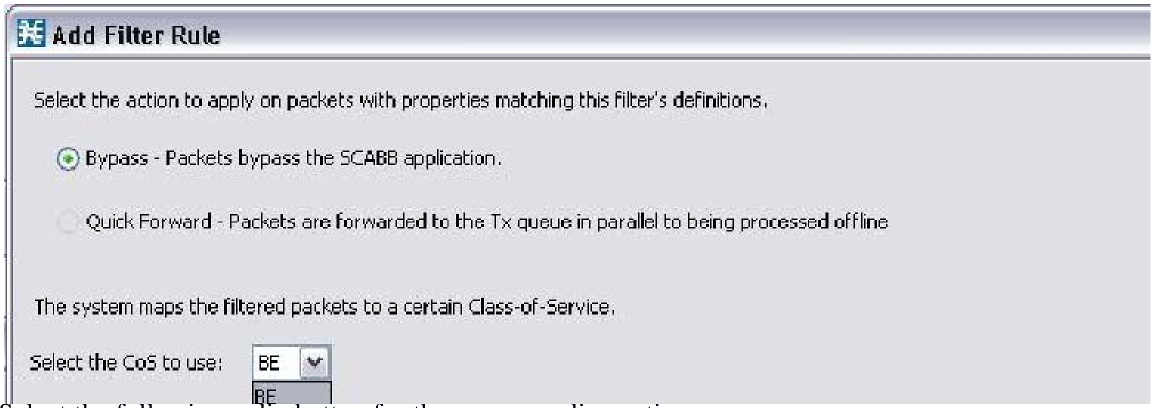
○ Not in the range of 0 - 0

Step 9 Define the ToS and click **Next**.

Note The acceptable values for ToS are 0 to 63.

The Action and Class-of-Service screen of the Add Filter Rule wizard appears (Figure 10-32).

Figure 10-32 Action and Class-of-Service



Add Filter Rule

Select the action to apply on packets with properties matching this filter's definitions.

● Bypass - Packets bypass the SCABB application.

○ Quick Forward - Packets are forwarded to the Tx queue in parallel to being processed offline

The system maps the filtered packets to a certain Class-of-Service.

Select the CoS to use: BE

Step 10 Select the following radio button for the corresponding action:

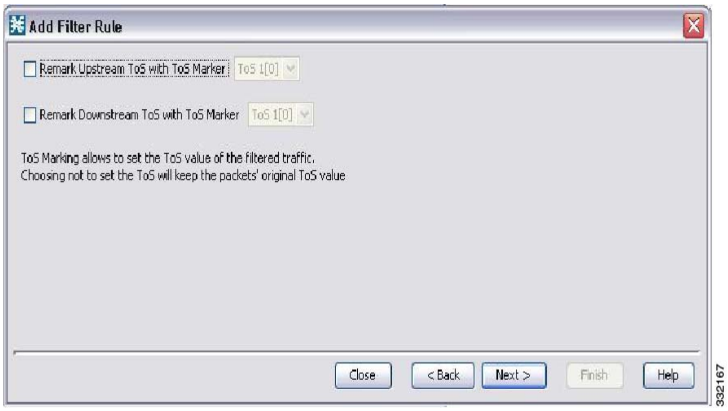
Bypass —Packets that match this filter rule are not passed to Cisco SCA BB.

Note By default, the Quick Forward radio button is disabled.

Step 11 Select a Class-of-Service value, and click **Next**.

The ToS Marking screen of the Add Filter Rule wizard appears (Figure 10-33).

Figure 10-33 ToS Marking



Add Filter Rule

□ Remark Upstream ToS with ToS Marker: ToS 1[0]

□ Remark Downstream ToS with ToS Marker ToS 1[0]

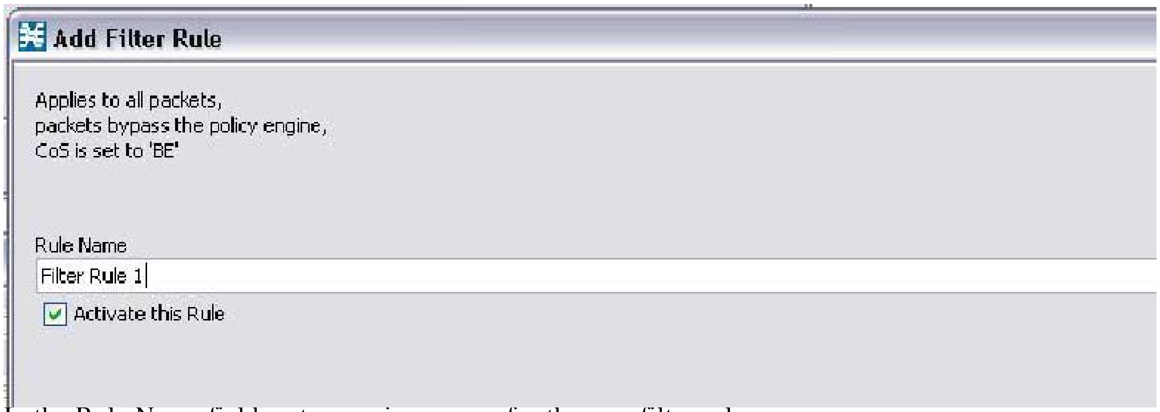
ToS Marking allows to set the ToS value of the filtered traffic.
Choosing not to set the ToS will keep the packets' original ToS value

Step 12 (Optional) To change the DSCP ToS marker of packets in the filtered traffic, check the **Remark Upstream ToS with ToS Marker** and **Remark Downstream ToS with ToS Marker** check boxes, select the required ToS marker from the drop-down list, and click **Next**.

- Disabling the directional DSCP ToS marking in the ToS Marking Settings dialog box (see How to Manage DSCP ToS Marker Values, page 9-81) overrides the DSCP ToS marking in that direction by a filter (that is, the DSCP ToS value is not changed). In this scenario, the Problems View displays a warning message.
- If you apply a filter for a flow in one direction in Step 4, but select ToS marking in the other direction in this step, the filter rule is created, but no DSCP ToS remarking occurs. In this scenario, the Problems View displays a warning message.

The Finish screen of the Add Filter Rule wizard appears (Figure 10-34).

Figure 10-34 Finish



Add Filter Rule

Applies to all packets,
packets bypass the policy engine,
CoS is set to 'BE'

Rule Name
Filter Rule 1

☑ Activate this Rule

Step 13 In the Rule Name field, enter a unique name for the new filter rule.

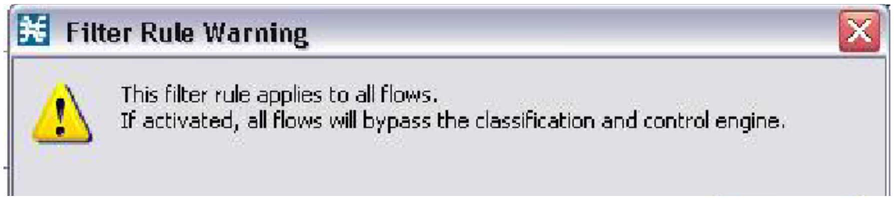
Note You can use the default name for the filter rule. We recommend that you enter a meaningful name.

Step 14 (Optional) To activate the filter rule, check the **Activate this rule** check box. Traffic is filtered according to the rule only when it is activated.

Step 15 Click **Finish**.

The Add Filter Rule wizard closes. The Filter Rule Warning message is displayed, as shown in Figure 10-35. The filter rule that has been added is displayed in the Filter Rule table.

Figure 10-35 Filter Rule Warning Message



Filter Rule Warning

This filter rule applies to all flows.
If activated, all flows will bypass the classification and control engine.

How to Edit Filter Rules

You can view and edit the parameters of a filter rule.

Step 1 In the Policies tab of Service Configuration Editor window, select the Filtered Traffic node.

A list of all filter rules is displayed in the right (Rule) pane.

Step 2 Select a rule in the Filter Rule table.

Step 3 Click the **Edit Rule** (✎) icon.

The Introduction page of the Edit Filter Rule wizard appears.

The Edit Filter Rule wizard is the same as the Add Filter Rule wizard.

Step 4 Follow the instructions in the section How to Add Filter Rules, Steps 4 to 14.

Step 5 Click **Finish**.

The filter rule is changed and the corresponding changes are displayed in the Filter Rule table.

How to Delete Filter Rules

You can delete filter rules. This is useful, for example, when you want the system to resume handling the IP addresses and their attributes according to the individual rules that were previously defined for each subscriber IP address.

Step 1 In the Policies tab, select the **Filtered Traffic** node.

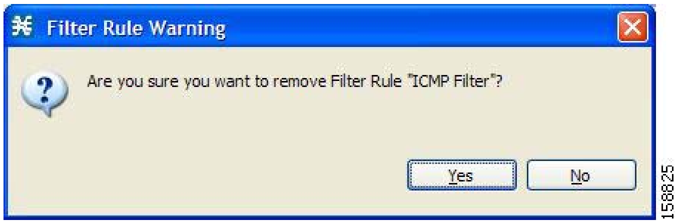
A list of all filter rules is displayed in the right (Rule) pane.

Step 2 Select a rule in the Filter Rule table.

Step 3 Click the **Delete Rule** (✖) icon.

A Filter Rule Warning message is displayed (Figure 10-36).

Figure 10-36 Filter Rule Warning



Filter Rule Warning

Are you sure you want to remove Filter Rule "ICMP Filter"?

Step 4 Click **Yes**.

The filter rule is deleted and is no longer displayed in the Filter Rule table.

How to Activate and Deactivate Filter Rules

You can activate or deactivate filter rules at any time. Deactivating a filter rule has the same effect as deleting it, but the parameters are retained in the service configuration, and you can reactivate the filter rule at a later date.

Step 1 In the Policies tab, select the **Filtered Traffic** node.

A list of all filter rules is displayed in the right (Rule) pane.

Step 2 Select a rule in the Filter Rule table.

Step 3 To activate the rule, check the **Active** check box.

Step 4 To deactivate the rule, uncheck the **Active** check box.

Step 5 Repeat Steps 3 and 4 for other rules.

Managing Subscriber Notifications

The subscriber notification feature pushes web-based messages to a subscriber by redirecting the subscriber HTTP traffic to relevant web pages. These web pages contain information relevant to the subscriber, such as notifications of quota depletion. HTTP redirection starts when the subscriber notification is activated and ceases when the notification is dismissed.

Note Subscriber notification is not supported when unidirectional classification is enabled.

Each set of subscriber redirection parameters comprises a notification redirect profile. The Cisco SCA BB supports a maximum of 128 redirect profiles, including notification and redirect profiles. There are 3 default redirect profiles that cannot be deleted: Default Notification, Network Attack Notification, and Default Redirection. You configure which notification redirect profile to use when defining rules.

- Subscriber Notification Parameters, page 10-41
- Network Attack Notification, page 10-42
- How to Add a Notification Redirect Profile, page 10-44
- How to Add a Set of Redirection URLs, page 10-52

Subscriber Notification Parameters

Each redirect profile of type notification contains the following subscriber notification parameters:

Note The Activation trigger configuration options are only available for redirect profile of type redirect.

- Name—Each profile must have a unique name.

Note You cannot change the name of the Default Notification or the Network Attack Notification.

- Redirect profile type—Each profile must be one of two types:
  - Notification
  - Redirect
- Set of Redirection URLs—A configurable set of destination URLs, to which the HTTP flows of the subscriber are redirected after redirection is activated. This web page usually contains the message that needs to be conveyed to the subscriber. The redirection set can optionally include one, or several parameters appended to the destination URL including the redirect reason and subscriber ID.

  The destination web server can use these parameters to carry a more purposeful message to the subscriber.
- Activation frequency—Indicates when to activate the notification redirect. The activation frequency is one of the following:

  Note The Periodically option is only available for redirect profile of type redirect.

  - Only once—The subscriber is redirected to the notification only the first time the conditions are met.

For example, if a quota was exceeded, the subscriber browses to the destination URL that informs them of this fact, only once (even though the subscriber remains in a breach state).

- Always—The subscriber is redirected to the notification every time the conditions are met.

  For example, if a quota was exceeded, the subscriber is continuously redirected to the notification until the subscriber completes the procedure to refresh their quota.

- Until the subscriber browses to—Every time the conditions are met, the subscriber is redirected to the notification, until the subscriber proceeds from the destination URL to a different, final URL.

  For example, if a quota was exceeded, the web page at the destination URL may ask the subscriber to press an **Acknowledge** button after reading the message. The acknowledge URL would be defined as the dismissal URL and would deactivate further notifications.

  The dismissal URL is composed of the URL hostname and the URL path, separated by a colon, in the following format:

  ```
  [*]<hostname>:<path>[*]
  ```

  - <**hostname**> may optionally be preceded by a wildcard (*), to match all hostnames with the same suffix.
  - The path element must always start with “/”.
  - <**path**> may be followed by a wildcard (*), to match all paths with a common prefix.

    For example, the entry ***.some-isp.net:/redirect/*** matches all the following URLs:

    - www.some-isp.net/redirect/index.html
    - support.some-isp.net/redirect/info/warning.asp
    - noquota.some-isp.net/redirect/acknowledge.aspx?ie=UTF-8

- List of Allowed URLs—A list of URLs that are not blocked and redirected even though redirection is activated.

  After redirection is activated, all HTTP flows, except flows to the destination URL and to the dismissal URL, are blocked and redirected to the destination URL. However, subscribers can be permitted to access an additional set of URLs. This is useful, for example, to give subscribers access to additional support information.

  Allowed URLs have the same format as the dismissal URL.

These parameters are defined when you add a new notification redirect profile (see How to Add a Set of Redirection URLs, page 10-52). You can modify them at any time.

Network Attack Notification

Subscriber notification informs a subscriber in real-time about current attacks involving IP addresses mapped to that subscriber. (Enabling these notifications is described in The Service Security Dashboard, page 10-2.) Cisco SCA BB notifies the subscriber about the attack by redirecting HTTP flows originating from the subscriber to a server that supplies information about the attack.

One subscriber notification, Network Attack Notification, is dedicated to providing these notifications; it cannot be deleted. A Network Attack Notification is not dismissed at the end of an attack; subscribers *must* respond to it.

To allow redirection when blocking traffic, the system is configured to leave open one specified TCP port (by default, port 80). See Managing Advanced Service Configuration Options, page 10-58.

Caution In earlier releases of Cisco SCA BB, configuring network attack notifications was performed using CLI commands. CLI commands should no longer be used for this purpose.

- Network Attack Notification Parameters, page 10-43
- Example of URL with Description Tail, page 10-44

Network Attack Notification Parameters

When a network attack is detected, HTTP flows of the subscriber are redirected to a configurable destination URL. This web page should display the warning that needs to be conveyed to the subscriber.

Optionally, the destination URL can include a query part containing notification parameters. The destination web server can use these parameters to create a more specific warning to the subscriber.

The query part of the URL has the following format:

```
?ip=<ip>&side=<side>&dir=<dir>&prot=<protocol>&no=<open-flows>&nd=<suspected-flows>&to=<op
en-flows-threshold>&td=<suspected-flows-threshold>&ac=<action>&nh=>handled-flows>
```

The meaning of each field in the tail is described in Table 10-1:

Table 10-1 Description Tail Fields

Field	Description	Possible Values
ip	Detected IP address	
side	—	• s—Subscriber • n—Network
dir	—	• s—Source • d—Destination
protocol	—	• TCP • UDP • ICMP • OTHER
open-flows	Number of open flows	—
suspected flows	Number of attack-suspected flows	—
open-flows-threshold	Threshold for open flows	—
suspected-flows-threshold	Threshold for attack-suspected flows	—
action	—	• R—Report • B—Block and report
handled-flows	Number of flows handled since the attack began (Non-zero only during and at the end of an attack)	—

Example of URL with Description Tail

```
http://www.some-isp.net/warning?ip=80.178.113.222&side=s&proto=TCP&no=34&nd=4&to=34&td=10&
ac=B&nh=100
```

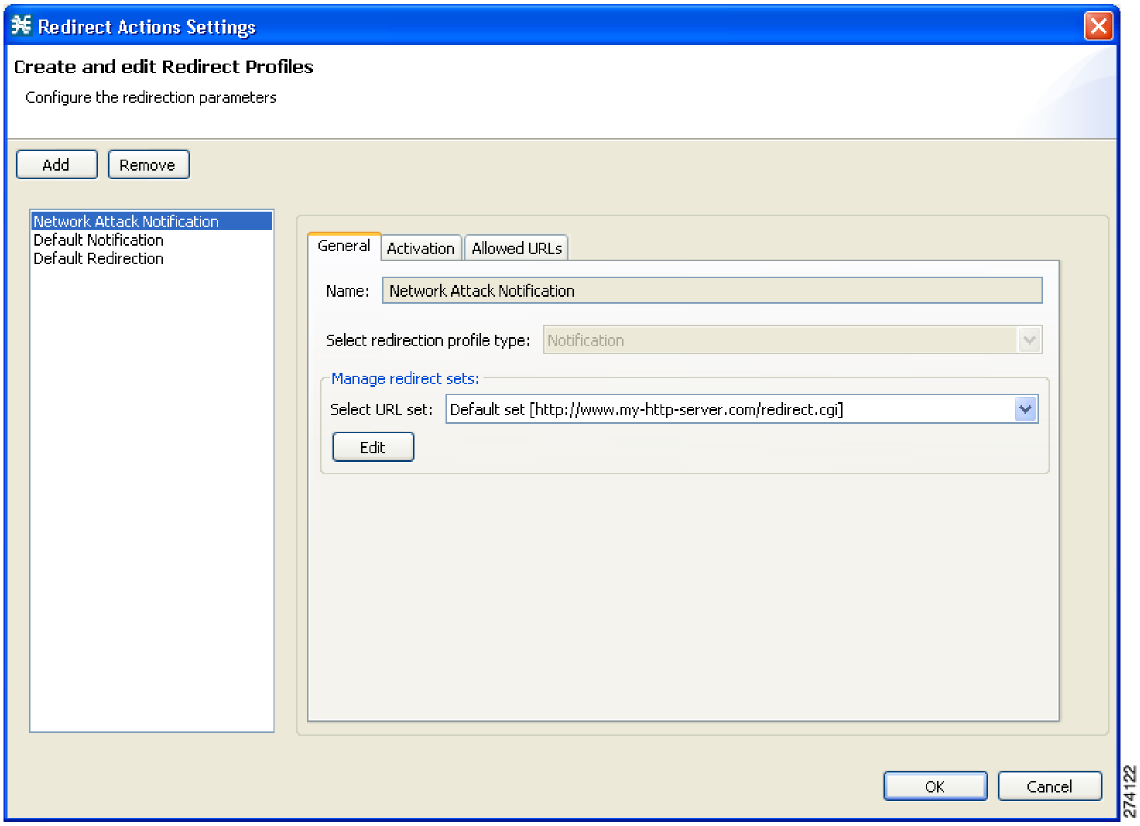
How to Add a Notification Redirect Profile

Note Creating a notification redirect profile does not activate the subscriber notification feature. After the notification redirect profile is defined, it must be activated for a particular package

Step 1 From the Policies tab in the left pane, choose **Configuration > Policies > Subscriber Redirection**.

The Redirect Actions Settings dialog box appears (Figure 10-37).

Figure 10-37 Redirect Action Settings - General Tab



Redirect Actions Settings

Create and edit Redirect Profiles

Configure the redirection parameters

- Network Attack Notification
- Default Notification
- Default Redirection

Name: Network Attack Notification

Select redirection profile type: Notification

Manage redirect sets:

Select URL set: Default set [http://www.my-http-server.com/redirect.cgi]

Step 2 Click **Add**.

A new redirection profile containing the default redirection URL set is added to the redirection profile list.

Step 3 In the Name field, enter a unique name for the new notification redirect profile.

> **Note** You can use the default name for the notification redirect profile. It is recommended that you enter a meaningful name

Step 4 In the Select redirection profile type field, select **Notification**.

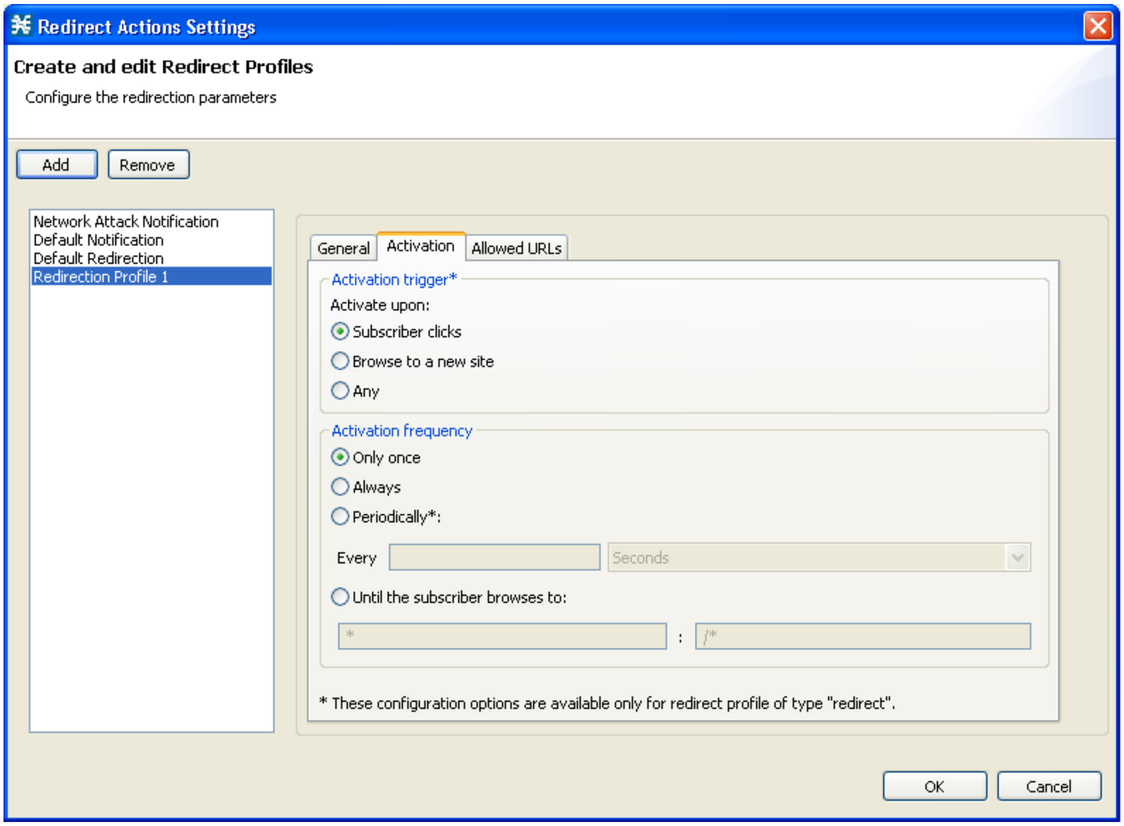
Do not skip this step or a redirect profile is created instead of a notification redirect profile.

Step 5 Choose a URL set.

Step 6 Click the **Activation** tab.

The Activation tab opens (Figure 10-38).

Figure 10-38 Activation Tab



Create and edit Redirect Profiles

Configure the redirection parameters

Network Attack Notification
Default Notification
Default Redirection
Redirection Profile 1

Activation trigger*

Activate upon:

● Subscriber clicks

○ Browse to a new site

○ Any

Activation frequency

● Only once

○ Always

○ Periodically*:

Every [ ] Seconds

○ Until the subscriber browses to:

[*] : [/*]

* These configuration options are available only for redirect profile of type "redirect".

Step 7 Configure the frequency in which the redirection is triggered. Choose one of the Activation frequency radio buttons:

- **Only once**
- **Always**
- **Until the subscriber browses to**

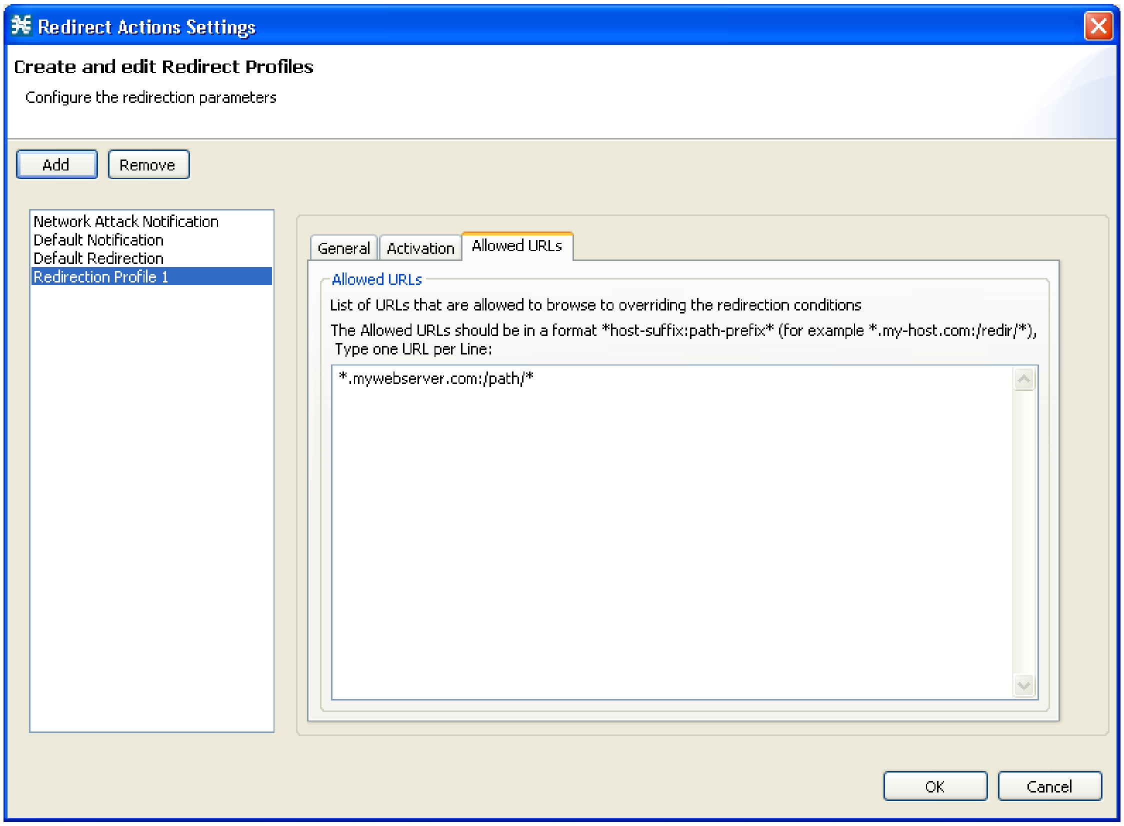
Step 8 If you chose the Until the subscriber browses to: radio button, enter the dismissal URL host-suffix and path-prefix in the fields provided.

Note We recommend that you avoid configuring the same host for redirection URL and redirection dismissal URL. The redirection is done based on the first GET request in a flow. If the same host is configured, with the changes in the URL path, the GET request corresponding the dismissal URL may use the same flow that was created for the redirect URL. This is the expected behavior with the default configuration. You can change the default configuration by increasing the number of HTTP GET detections in the flow. To modify the number of HTTP GET detections from the Cisco SCA BB, use the Advanced Service Configuration Options. Note that increasing the number of HTTP GET detections may impact the performance of the Cisco SCE.

Step 9 Click the Allowed URLs tab.

The Allowed URLs tab opens (Figure 10-39).

Figure 10-39 Allowed URLs Tab



List of URLs that are allowed to browse to overriding the redirection conditions

The Allowed URLs should be in a format *host-suffix:path-prefix* (for example *.my-host.com:/redir/*), Type one URL per Line:

.mywebserver.com:/path/

Step 10 (Optional) Enter any allowed URLs, one per line.

Step 11 Click **OK**.

The Redirect Actions Settings dialog box closes.

The notification redirect profile is added to the profile list.

Managing Subscriber Redirection

The rules for a package may deny access to selected protocols. When a subscriber to the package tries to access a blocked protocol, the traffic flow can be redirected to a server where a posted web page explains the reason for the redirection (for example, a “Silver” subscriber trying to access a service available only to “Gold” subscribers). This web page can offer subscribers the opportunity to upgrade their packages. You configure which redirection profile to use when defining rules.

Note Redirection is not supported when unidirectional classification is enabled.

Each redirect profile consists of a set of redirect parameters. The Cisco SCA BB supports a maximum of 128 redirect profiles, including notification redirect and redirect profiles.

Subscriber Redirect Parameters

Each redirect profile of type redirect contains the following parameters:

- Name—Each profile must have a unique name.

Note You cannot change the name of the Default Redirection Profile.

- Redirect profile type—Each profile must be one of two types:
  - Notification
  - Redirect
- Set of Redirection URLs—A configurable set of destination URLs, to which the subscriber’s HTTP flows are redirected after redirection is activated. The redirection set can optionally include one, or several parameters appended to the destination URL including the redirect reason or subscriber ID.
- Activation trigger—The action that initiates the redirect. The activation trigger is one of the following:
  - Subscriber clicks—When the redirect is activated through a subscriber clicking a link.
  - Browse to a new site—When the redirect is activated through browsing.
  - Any—When the redirect is activated either via a link or browsing.

- Activation frequency—Indicates when to activate the redirect. The activation frequency is one of the following:
  - Only once—The subscriber is redirected only the first time the conditions are met.
  - Always—The subscriber is redirected every time the conditions are met.
  - Periodically—The redirection is based on a periodic counter and the counter is reset after the redirection is complete.
  - Triggering events
  - KBytes
  - Until the subscriber browses to—Every time the conditions are met, the subscriber is redirected, until the subscriber proceeds from the destination URL to a different, final URL.

    The dismissal URL is composed of the URL hostname and the URL path, separated by a colon, in the following format:

    ```
    [*]<hostname>:<path>[*]
    ```
  - **<hostname>** may optionally be preceded by a wildcard (*), to match all hostnames with the same suffix.
  - The path element must always start with "/".
  - **<path>** may be followed by a wildcard (*), to match all paths with a common prefix.

    For example, the entry ***.some-isp.net:/redirect/*** matches all the following URLs:

    • www.some-isp.net/redirect/index.html

    • support.some-isp.net/redirect/info/warning.asp

    • noquota.some-isp.net/redirect/acknowledge.aspx?ie=UTF-8
- List of Allowed URLs—A list of URLs that are not blocked and redirected even though redirection is activated.

  After redirection is activated, all HTTP flows, except flows to the destination URL and to the dismissal URL, are blocked and redirected to the destination URL. However, subscribers can be permitted to access an additional set of URLs. This is useful, for example, to give subscribers access to additional support information.

  Allowed URLs have the same format as the dismissal URL. But, for Allowed URLs, you must specify the HTTP port and the port must be 80. If the URL contains any port other than 80, the URL is considered as a normal URL and is redirected.

These parameters are defined when you add a new notification redirect profile. You can modify them at any time.

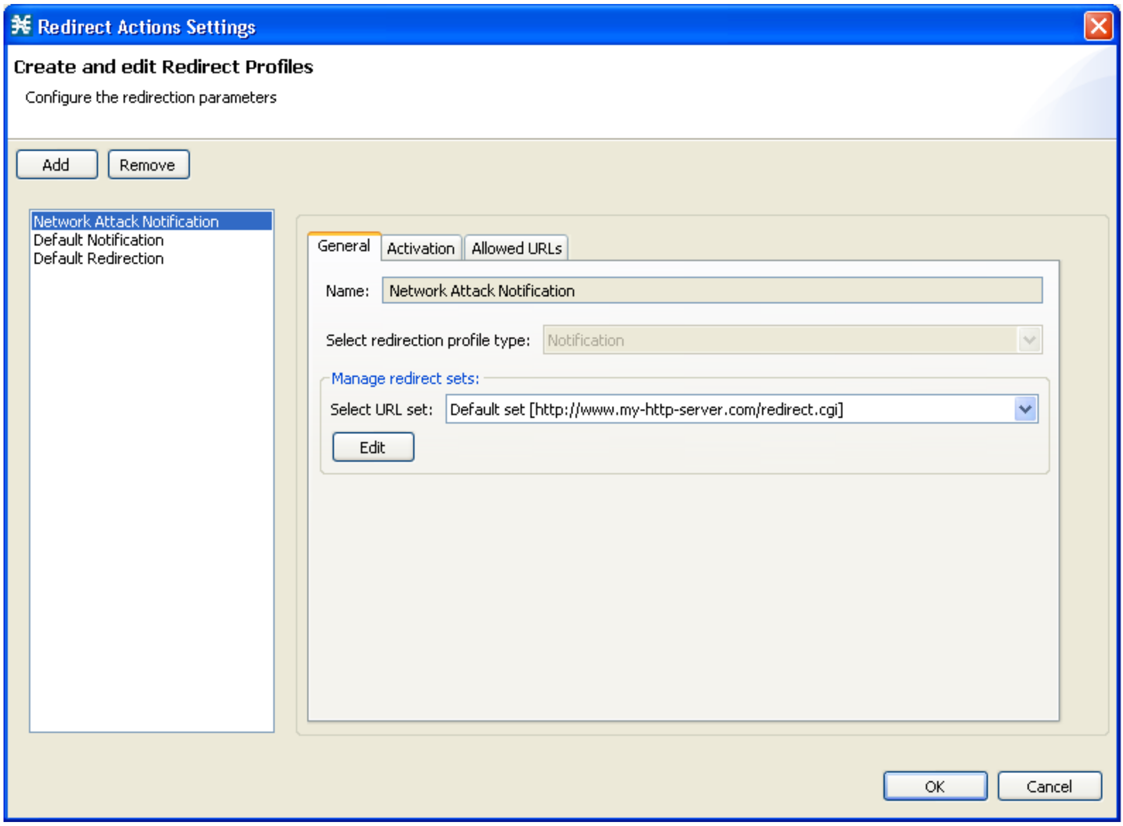
How to Add a Redirect Profile

A redirect profile contains a set of redirection URLs as well as conditions in which to use the redirect feature, such as the action that triggers the redirect, or the frequency in which the redirect occurs.

Step 1 From the Policies tab in the left pane, choose **Configuration > Policies > Subscriber Redirection**.

The Redirect Actions Settings dialog box appears (Figure 10-40).

Figure 10-40 Redirect Actions Settings - General Tab



Redirect Actions Settings

Create and edit Redirect Profiles

Configure the redirection parameters

Network Attack Notification
Default Notification
Default Redirection

Name: Network Attack Notification

Select redirection profile type: Notification

Manage redirect sets:

Select URL set: Default set [http://www.my-http-server.com/redirect.cgi]

Step 2 Click **Add**.

A new redirect profile containing the default redirection URL set is added to the redirect profile list.

Step 3 In the Name field, enter a unique name for the new redirect profile.

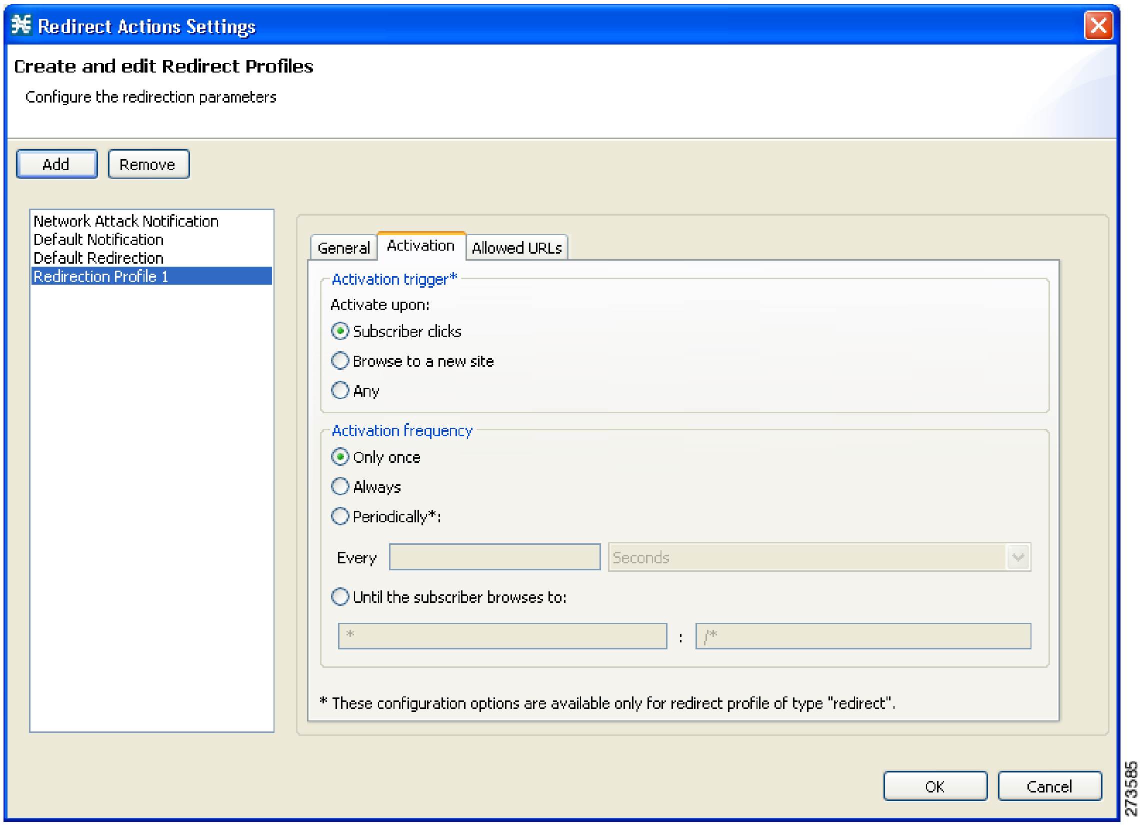
Note You can use the default name for the redirect profile, but it is recommended that you enter a meaningful name.

Step 4 Choose a URL set.

Step 5 Click the **Activation** tab.

The Activation tab opens (Figure 10-41).

Figure 10-41 Activation Tab



Step 6 Configure the activity that triggers the redirection. Choose one of the Activation trigger radio buttons:

- **Subscriber clicks**
- **Browse to a new site**
- **Any**

Step 7 Configure the frequency in which the redirection is triggered. Select one of the Activation frequency radio buttons:

- **Only once**
- **Always**
- **Periodically**
- **Until the subscriber browses to**

Step 8 If you selected the Periodically radio button, enter a number and an increment in the Every fields, to specify the frequency in which the redirection occurs.

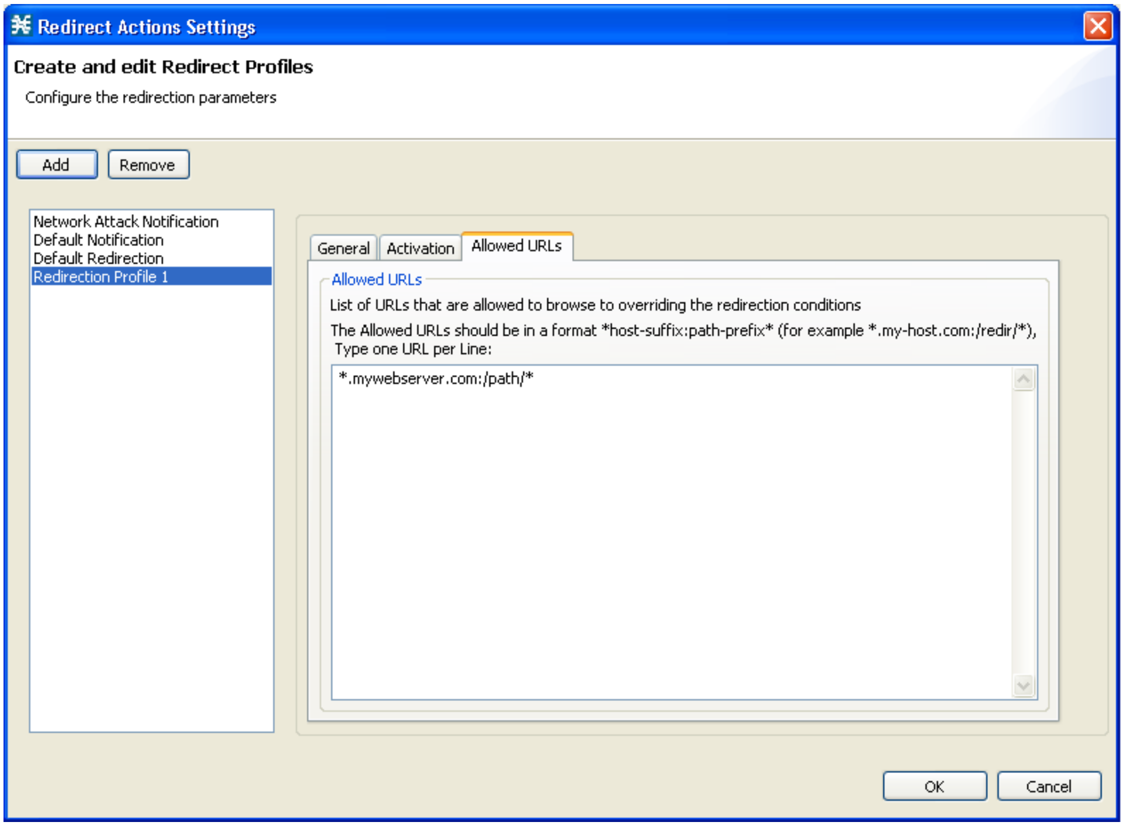
Step 9 If you selected the Until the subscriber browses to: radio button, enter the dismissal URL in the fields provided.

Step 10 Click the Allowed URLs tab.

The Allowed URLs tab opens (Figure 10-42).

Tip Enter all configured redirection URLs to the Allowed URLs list to prevent a redirection loop.

Figure 10-42 Allowed URLs Tab



Redirect Actions Settings

Create and edit Redirect Profiles

Configure the redirection parameters

Network Attack Notification
Default Notification
Default Redirection
Redirection Profile 1

Allowed URLs

List of URLs that are allowed to browse to overriding the redirection conditions

The Allowed URLs should be in a format *host-suffix:path-prefix* (for example *.my-host.com:/redir/*),
Type one URL per Line:

```
*.mywebserver.com:/path/*
```

Step 11 (Optional) Enter a URL, or multiple URLs (with HTTP port 80), that can be browsed, overriding the redirect conditions.

Note All URLs with HTTP port other than 80 is redirected.

Step 12 Click **OK**.

The Redirect Actions Settings dialog box closes.

The Redirection profile is added to the redirection profile list.

How to Delete a Redirection Profile

You cannot delete the Default Redirection Profile.

Step 1 From the Policies tab in the left pane, choose **Configuration** > **Policies > Subscriber Redirection**.

The Redirect Actions Settings dialog box appears.

Step 2 Click the name of the profile.

Step 3 Click **Remove**.

Step 4 Click **OK**.

The Redirect Actions Settings dialog box closes.

The Redirection settings are saved.

How to Add a Set of Redirection URLs

The Console Redirection feature supports only three protocols:

- HTTP Browsing
- HTTP Streaming
- RTSP Streaming

Each redirection set contains one redirection option for each of these three protocols. The system provides a default redirection set, which cannot be deleted. You can add up to 127 additional sets.

Each redirection URL includes the URL specified name, the Subscriber ID, and the Service ID in the following format:

```
<URL>?n=<subscriber-ID>&s=<service-ID>
```

Optionally, the URL can contain one or multiple parameters appended to it.

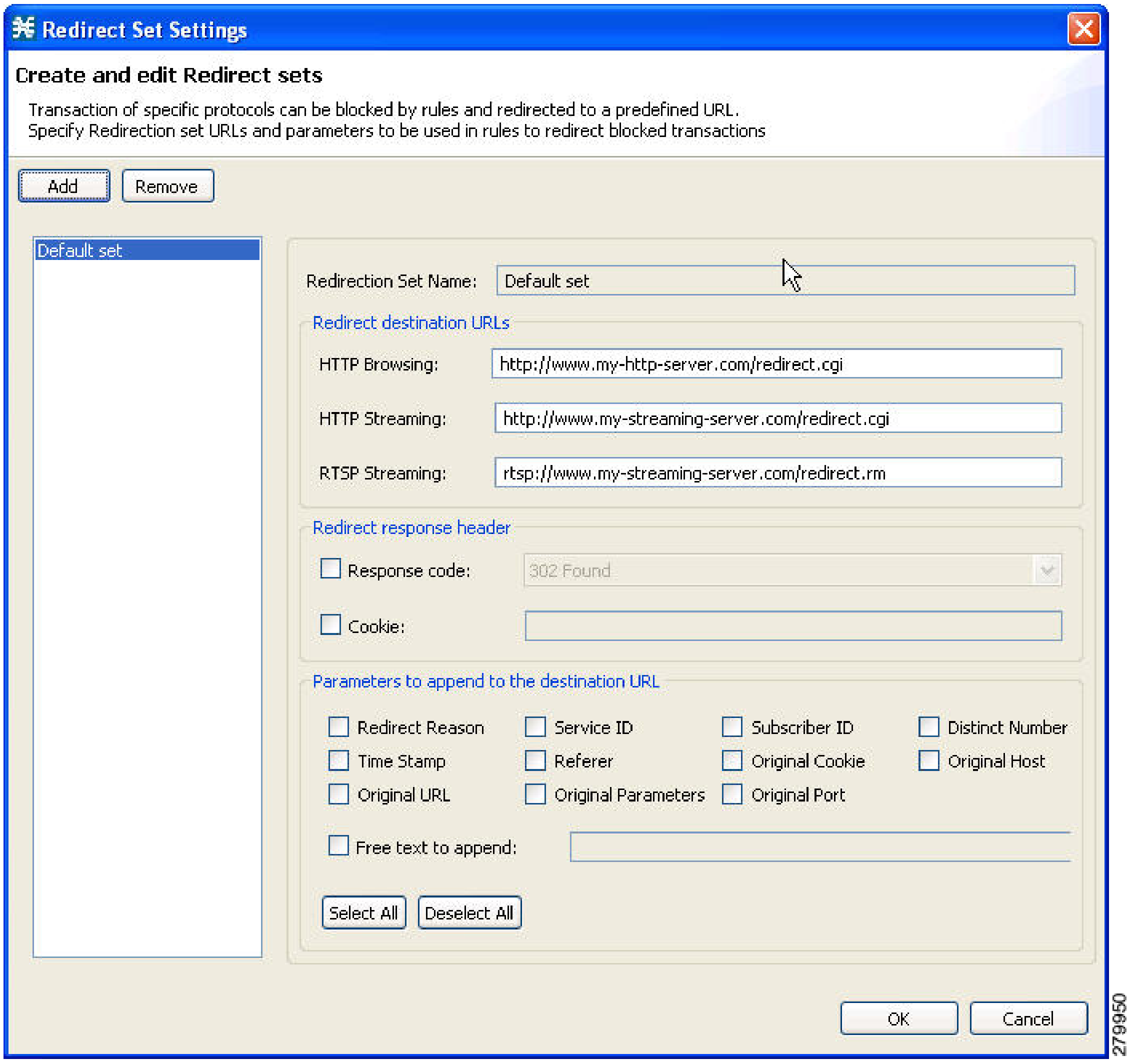
Step 1 From the Policies tab of the left pane, choose **Configuration > Policies > Subscriber Redirection**.

The Redirect Actions Settings dialog box appears.

Step 2 In the General tab, click **Edit**.

The Redirect Set Settings dialog box appears (Figure 10-43).

Figure 10-43 Redirect Set Settings



Redirect Set Settings

Create and edit Redirect sets

Transaction of specific protocols can be blocked by rules and redirected to a predefined URL.
Specify Redirection set URLs and parameters to be used in rules to redirect blocked transactions

Add | Remove

Default set

Redirection Set Name: Default set

Redirect destination URLs

HTTP Browsing: http://www.my-http-server.com/redirect.cgi

HTTP Streaming: http://www.my-streaming-server.com/redirect.cgi

RTSP Streaming: rtsp://www.my-streaming-server.com/redirect.rm

Redirect response header

□ Response code: 302 Found

□ Cookie:

Parameters to append to the destination URL

□ Redirect Reason □ Service ID □ Subscriber ID □ Distinct Number
□ Time Stamp □ Referer □ Original Cookie □ Original Host
□ Original URL □ Original Parameters □ Original Port

□ Free text to append:

Select All | Deselect All

OK | Cancel

Step 3 Click **Add**.

A new redirection set containing the default redirection URLs is added.

Step 4 In the Redirection Set Name field, enter unique name for the new redirection set.

Note You can use the default name for the redirection set, but it is recommended that you provide a meaningful name.

Step 5 Enter new values in the Redirection destination URLs section of the new redirection set.

Timesaver Enter all configured redirection URLs to the Allowed URLs list to prevent a redirection loop.

Step 6 (Optional) To include a response code, check the Response code check box, and choose a response code from the drop-down list. see Table 10-2 for a listing and description of the redirection parameters.

Step 7 (Optional) To include a cookie, check the Cookie check box, and enter a value. see Table 10-2 for a listing and description of the redirection parameters.

Step 8 (Optional) Check the check boxes of any parameters you wish to append to the destination URL see Table 10-2 for a listing and description of the redirection parameters.

If you check the Free text to append check box, enter text into the text box to append to the URL. see Table 10-2 for a listing and description of the redirection parameters. The examples in Table 10-2 is based on the following URL redirection:

http://<*URL*>?n=N/A&reason=2&s=119&id=0:10&ts=1327285422&str=this is free text to append content&referer=&cookie=&host=<*URL*>&url=/p-cube.htm&params=

Note "<" and ">" do not appear in redirect URL.
Maximum length of destination URL including parameters is 500 characters.
Cookie and Referer parameters are allowed only for HTTP traffic.

Table 10-2 Redirection Parameters

Parameter	Description	Example
Redirect Reason	In case of notification—notification number. In case of DDOS attack—DDOS attack ID. In case of redirect—not valid.	2
Service ID	The ID of the service as was classified by the SCE.	119
Subscriber ID	Subscriber name as it appears in SCE.	—
Distinct Number	Unique identifier of redirected flow, in format <redirected flow number:cpu number>.	0:10
Time Stamp	Time in seconds, in UNIX format.	1327285422
Referer	Referer as it appears in the original flow request. If the referer parameter is not set then ““ appears.	—
Original Cookie	Cookie string as it appears in the original flow request. If the cookie parameter is not set then ““ appears.	—
Original Host	Host name as it appears in the original flow request.	<*URL*>
Original URL	URL as it appears in the original flow request.	/p-cube.htm
Original Parameters	URL parameters as they appear in the original flow request. If the URL parameters are not set then ““ appears.	—

Table 10-2 Redirection Parameters (continued)

Parameter	Description	Example
Original Port	Server port number that is added to the redirect host parameter.	—
Free text to append	Free text.	this is free text to append content

Step 9 Click **OK**.

Your settings are saved and the Redirect Set Settings dialog box closes.

Note Keep the total number of characters appended to the redirect URL below 1200. To keep it below 1200, we recommend that you enable only the required parameters under the Parameters to append to the destination URL pane.

How to Delete a Set of Redirection URLs

Step 1 From the Policies tab of the left pane, choose **Configuration > Policies > Subscriber Redirection**.

The Redirect Actions Settings dialog box appears.

Step 2 In the General tab, click **Edit**.

The Redirect Set Settings dialog box appears.

Step 3 Click the name of the redirection set.

Step 4 Click **Remove**.

Step 5 Click **OK**.

The Redirect Set Settings dialog box closes.

The Redirection settings are saved.

Managing the System Settings

The Console allows you to determine various system parameters that control:

- The operational state of the system
- Enabling and disabling asymmetric routing classification mode
- Advanced service configuration options

Setting the System Modes

From the Console, you can select:

- The operational mode of the system
- Asymmetric routing classification mode

Information About the System Modes

- System Operational Mode, page 10-56
- Asymmetric Routing Classification Mode, page 10-56

System Operational Mode

The operational mode of the system defines how the system handles network traffic.

Note Each rule has its own operational mode (state). If this differs from the system mode, the "lower" of the two modes is used. For example, if a rule is enabled, but the system mode is report-only, the rule generates only RDRs.

The three operational modes are:

- Full Functionality—The system enforces active rules on the network traffic and performs reporting functions (that is, generates RDRs).
- Report Only—The system generates RDRs only. No active rule enforcement is performed on the network traffic.
- Transparent—The system does not generate RDRs and does not enforce active rules on the network traffic.

Asymmetric Routing Classification Mode

Enabling unidirectional classification significantly improves classification accuracy when the SCE platform is deployed in an environment with a high rate of unidirectional flows.

- Unsupported Features, page 10-57
- Protocol Classification, page 10-57
- Switching to Asymmetric Routing Classification Mode, page 10-57
- Switching from Asymmetric Routing Classification Mode, page 10-57

Unsupported Features

The following Cisco SCA BB features are not supported when unidirectional classification is enabled:

- Flavors
- External quota provisioning
- Subscriber notification
- Redirection
- Flow Signaling RDRs
- Content filtering
- VAS traffic forwarding

When unidirectional classification is enabled, the service configuration editor indicates (in the Problems View) if the service configuration is consistent with the features that are supported in this mode.

The following features, which are not part of the service configuration, are also affected when unidirectional classification is enabled:

- Subscriber-Aware Mode (a mode in which subscriber information is dynamically bound to the IP address currently in use by the subscriber) is not supported.
- Enhanced flow open mode must be enabled.

The system gives no indication if the state of the above features is consistent with the state of the routing classification mode.

Protocol Classification

When unidirectional classification is enabled, protocol classification is performed in the normal way except for unidirectional UDP flows. Because it is impossible to know the server side of a unidirectional UDP flow, Cisco SCA BB tries to classify the protocol using the destination port of the first packet; if no exact match is found, Cisco SCA BB tries to classify the protocol using the source port.

Switching to Asymmetric Routing Classification Mode

If you create a service configuration in symmetric mode and switch to asymmetric routing classification mode:

- Flavors are not used for classification.
- Periodic quota management mode is used.
- Data is not lost when you switch to asymmetric routing classification mode, but you cannot apply the service configuration to an SCE platform until all unsupported features are removed from the service configuration.

Switching from Asymmetric Routing Classification Mode

If you create a service configuration in asymmetric routing classification mode:

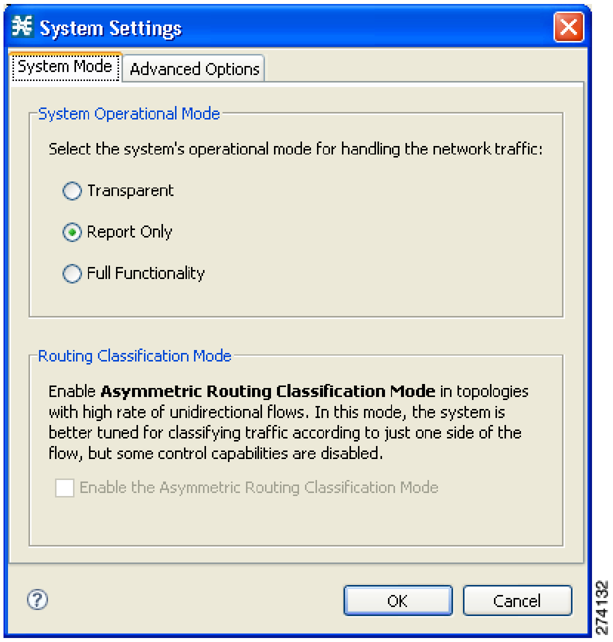
- The Suspected Session Rate is set equal to the Session Rate for all anomaly detectors.
- No flavors are created in the default service configuration, and no service elements have specified flavors.
- The quota management mode is periodic, with a daily aggregation period.
- Asymmetric routing classification mode limitations remain if you switch to symmetric mode. To change them, you must edit the service configuration.

How to Set the Operational and Topological Modes of the System

Step 1 From the Policies tab of the left pane, choose **Configuration > Policies > System Settings**.

The System Settings dialog box appears (Figure 10-44).

Figure 10-44 System Settings



System Operational Mode

Select the system's operational mode for handling the network traffic:

○ Transparent

● Report Only

○ Full Functionality

Routing Classification Mode

Enable **Asymmetric Routing Classification Mode** in topologies with high rate of unidirectional flows. In this mode, the system is better tuned for classifying traffic according to just one side of the flow, but some control capabilities are disabled.

□ Enable the Asymmetric Routing Classification Mode

Step 2 Select one of the **System Operational Mode** radio buttons:

- **Transparent**
- **Report Only**
- **Full Functionality**

Step 3 To change the routing classification mode, check or uncheck the **Enable the Asymmetric Routing Classification Mode** check box.

Step 4 Click **OK**.

The System Settings dialog box closes.

The new System Mode setting is saved.

Managing Advanced Service Configuration Options

Advanced service configuration options control the more sophisticated and less frequently changed attributes of the system. It is recommended that you do not change these options.

- The Advanced Service Configuration Properties, page 10-59
- How to Edit Advanced Service Configuration Options, page 10-64

The Advanced Service Configuration Properties

Table 10-3 lists the advanced service configuration properties:

Table 10-3 Advanced Service Configuration Properties

Property	Default Value	Description
Bandwidth Management		
Level of BWC enforcement on networking flows of P2P and IM applications.	SCE to use Default Service BWCs	Specifies the level of BWC enforcement on networking flows of P2P and IM applications.
Use Global Bandwidth Management in Virtual Links Mode	FALSE	Specifies whether to use the Global Bandwidth Management in Virtual Links Mode.
Classification		
Apply this order of priority between different criteria for service classification	Zone > Flavor > Protocol > Init-Side	Specifies the order of priority between different criteria for service classification. Values are: • Flavor > Protocol > Zone > Init-Side • Zone > Flavor > Protocol > Init-Side
ClickStream Event recognition	TRUE	Specifies whether to recognize ClickStream Events.
Enable sending ‘404, Page Not Found’ upon blocking	FALSE	Specifies whether to send ‘404, Page Not Found’ upon blocking.
Guruguru detailed inspection mode enabled	FALSE	The Guruguru protocol is used by the Guruguru file-sharing application popular in Japan. Cisco SCA BB provides two inspection modes for classification of this protocol: • Default—Suitable for networks where little Guruguru traffic is expected. This mode is usual in all countries except Japan. • Detailed—Suitable for networks where Guruguru traffic is expected to be common. This mode is used in Japanese networks only.
Kuro detailed inspection mode enabled	FALSE	The Kuro protocol is used by the Kuro file-sharing application popular in Japan. Cisco SCA BB provides two inspection modes for classification of this protocol: • Default—Suitable for networks where little Kuro traffic is expected. This is usual in all countries except Japan. • Detailed—Suitable for networks where Kuro traffic is expected to be common. This mode is used in Japanese networks only.
Number of HTTP GET detections	1	Specifies the number of HTTP GET detections. The Cisco SCE classifies the HTTP based on the number of GET requests configured. Range is 1 to 65535, and the default value is 1. **Note** Since the Deep HTTP Inspection feature examines all packets in a single HTTP stream until the configured number of requests has been found, any value higher than 1 may impact the performance of the Cisco SCE.

Table 10-3 Advanced Service Configuration Properties (continued)

Property	Default Value	Description
Soribada detailed inspection mode enabled	FALSE	The Soribada protocol is used by the Soribada file-sharing application popular in Japan. Cisco SCA BB provides two inspection modes for classification of this protocol: • Default—Suitable for networks where little Soribada traffic is expected. This is usual in all countries except Japan. • Detailed—Suitable for networks where Soribada traffic is expected to be common. This mode is used in Japanese networks only.
TCP destination port signatures	1720:H323	TCP destination port numbers for signatures that require a port hint for correct classification. Valid values are comma-separated items, each item in the form <port-number>:<signature-name>. Applicable signature names are: H323, Radius Access, Radius Accounting, and DHCP.
UDP destination port signatures	67:DHCP, 68:DHCP, 1812:Radius Access, 1645:Radius Access, 1813:Radius Accounting, 1646:Radius Accounting	UDP destination port numbers for signatures that require a port hint for correct classification. Valid values are comma-separated items, each item in the form <port-number>:<signature-name>. Applicable signature names are: H323, Radius Access, Radius Accounting, and DHCP.
UDP ports for which flow should be opened on first packet	5060, 5061, 67, 68, 69, 1812, 1813, 1645, 1646, 2427, 2727, 9201, 9200, 123, 1900, 5190, 10000	Enhanced flow-open mode is disabled on the specified UDP ports, to allow classification according to the first packet of the flow.
UDP source port signatures	1812:Radius Access, 1645:Radius Access, 1813:Radius Accounting, 1646:Radius Accounting	UDP source port numbers for signatures that require a port hint for correct classification. Valid values are comma-separated items, each item in the form <port-number>:<signature-name>. Applicable signature names are: H323, Radius Access, Radius Accounting, and DHCP.

Table 10-3 Advanced Service Configuration Properties (continued)

Property	Default Value	Description
V-Share detailed inspection mode enabled	FALSE	The V-Share protocol is used by the V-Share file-sharing application popular in Japan. Cisco SCA BB provides two inspection modes for classification of this protocol: • Default—Suitable for networks where little V-Share traffic is expected. This mode is usual in all countries except Japan. • Detailed—Suitable for networks where V-Share traffic is expected to be common. This mode is used in Japanese networks only.
Winny detailed inspection mode enabled	FALSE	The Winny P2P protocol is used by the Winny file-sharing application popular in Japan. Cisco SCA BB provides two inspection modes for classification of this protocol: • Default—Suitable for networks where little Winny traffic is expected. This is usual in all countries except Japan. • Detailed—Suitable for networks where Winny traffic is expected to be common. This mode is used in Japanese networks only.
WinnyP aggressive classification enabled	FALSE	
WinnyP classification enabled	FALSE	
Malicious Traffic		
Malicious Traffic RDRs enabled	TRUE	Specifies whether to generate Malicious Traffic RDRs.
Number of seconds between Malicious Traffic RDRs on the same attack	60	A Malicious Traffic RDR is generated when an attack is detected. Malicious Traffic RDRs are then generated periodically, at user-configured intervals, for the duration of the attack.
TCP port that should remain open for Subscriber Notification	80	You can choose to block flows that are part of any detected network attack, but this may hinder subscriber notification of the attack. The specified TCP port is not blocked to allow notification of the attack to be sent to the subscriber.
Multi Stage Classification		
Blocking	FALSE	Specifies whether to block the sub services under the main service.
Enable	TRUE	Specifies whether to enable the sub service classification of a service. Multi stage classification describes the application level services that can be enabled or disabled. By default sub service classification of the services is enabled. For example, Google talk service contains Google talk file transfer, Google talk Networking, Google talk VoIP as sub services.
Policy Check		
Ongoing policy check mode enabled	TRUE	Specifies whether policy changes affect flows that are already open.
Time to bypass between policy checks (seconds)	30	Maximum time (in seconds) that may pass before policy changes affect flows that are already open.
Quota Management		

Table 10-3 Advanced Service Configuration Properties (continued)

Property	Default Value	Description
Grace period before first breach (seconds)	2	The time (in seconds) to wait after a quota limit is breached before the breach action is performed. Policy servers should use this period to provision quota to a subscriber that just logged in.
Length of the time frame for quota replenish scatter (minutes)	0	The size of the window across which to scatter the periodic quota replenishment randomly.
Time to bypass between policy checks for quota limited flows	30	Maximum time (in seconds) that may pass before a quota breach affects flows that are already open.
Volume to bypass between policy checks for quota limited flows	0	Maximum flow volume (in bytes) that may pass before a quota breach affects flows that are already open. A value of zero means that unlimited volume may pass.
Redirection		
Adds original host to redirection URL	FALSE	Specifies whether to add the original host to the redirection URL.
Adds original URL to redirect URL	FALSE	Specifies whether to add the original URL to the redirection URL.
Maximum redirect URL Length	500	Specifies the maximum length of the redirect URL.
Redirect subscriber ID format	Complete - n=<user>@<realm>	Specifies the redirect subscriber ID format to be configured. Valid Options are: • Complete - n=<user>@<realm> (default) • User only - n=<user> • Realm only - r=<realm> • Separately -n<user>&r=<realm> If the subscriber name does not match the format of <user>@<realm>, the full subscriber name is appended to the URL, regardless of the redirect subscriber format configured.
Reporting		
Extract Full User Agent details	FALSE	Specifies whether to extract full user agent details.
Flow Accounting RDRs enabled	FALSE	Specifies whether to generate Flow Accounting RDRs.
Flow Accounting RDRs interval for each Service (in seconds)	60	Specifies the interval at which the Flow Accounting RDRs are generated for each service.
Flow Accounting RDRs limit per second	100	Specifies the limit of Flow Accounting RDRs to be generated each second.

Table 10-3 Advanced Service Configuration Properties (continued)

Property	Default Value	Description
Hide Subscriber IP and ID in RDRs	FALSE	Specifies whether to hide the IP address and Subscriber ID in the following RDRs: • Transaction RDR • Transaction Usage RDR • HTTP Transaction Usage RDR • RTSP Transaction Usage RDR • VoIP Transaction Usage RDR • Video Transaction Usage RDR • Blocking RDR • Flow Start RDR • Flow End RDR • Flow Ongoing RDR • Media Flow RDR • Spam RDR See the *Cisco Service Control for Broadband Reference Guide* for details on the RDRs.
Media Flow RDRs enabled	TRUE	Specifies whether to generate Media Flow RDRs.
Minimal volume for generating HTTP Transaction Usage RDR (bytes)	0	Specifies the minimum volume for generating HTTP Transaction Usage RDR.
Minimal volume for generating RTSP Transaction Usage RDR (bytes)	0	Specifies the minimum volume for generating RTSP Transaction Usage RDR.
Minimal volume for generating Video Transaction Usage RDR (bytes)	1024000	Specifies the minimum volume for generating Video Transaction Usage RDRs.
Video Transaction Usage RDRs enabled	FALSE	Specifies whether to generate Video Transaction Usage RDRs.
Enable VSA Fields for Subscriber, HTTP Transaction, and Video Transaction RDRs	FALSE	Specifies whether to generate VSA fields for Subscriber, HTTP Transaction, and Video Transaction RDRs.
Subscriber Accounting RDR enabled	FALSE	Specifies whether to generate Subscriber Accounting RDRs. The Subscriber Accounting RDR is used for SM-ISG integration. For more information, see either the ISG documentation in the “Managing the SCMP” chapter of *Cisco SCE8000 10GBE Software Configuration Guide* or the “Managing the SCMP” chapter of *Cisco SCE8000 10GBE Software Configuration Guide*.

How to Edit Advanced Service Configuration Options

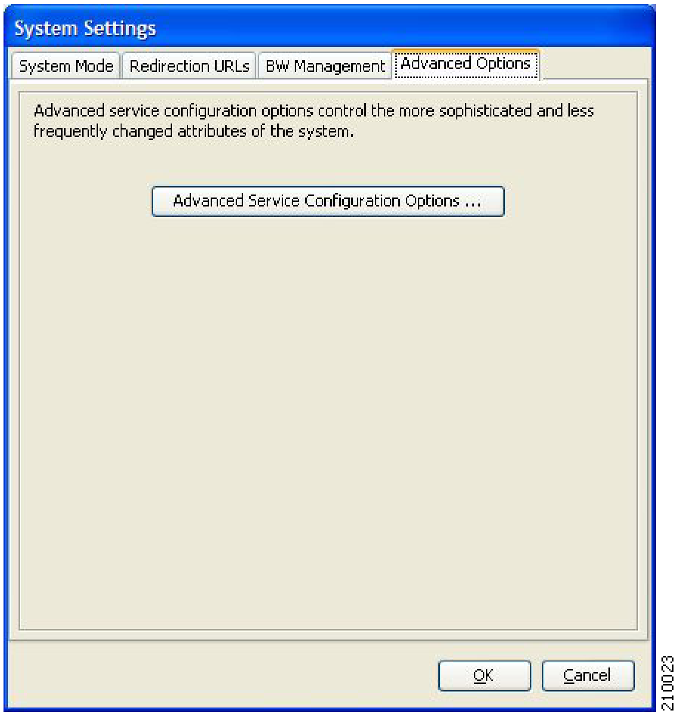
Step 1 From the Policies tab of the left pane, choose **Configuration > Policies > System Settings**.

The System Settings dialog box appears.

Step 2 Click the **Advanced Options** tab.

The Advanced Options tab opens (Figure 10-45).

Figure 10-45 Advanced Options Tab

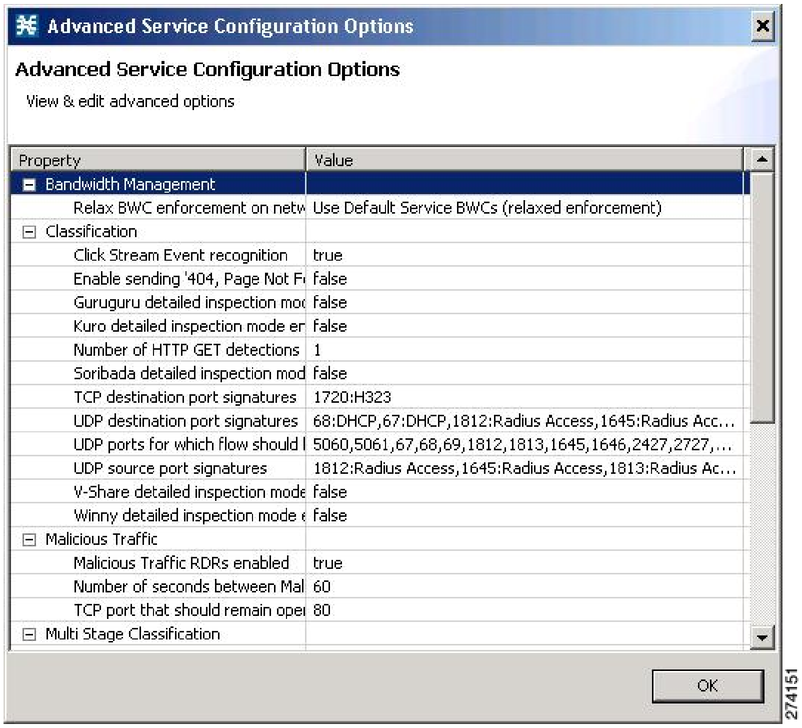


Advanced service configuration options control the more sophisticated and less frequently changed attributes of the system.

Step 3 Click **Advanced Service Configuration Options**.

The Advanced Service Configuration Options dialog box opens (Figure 10-46).

Figure 10-46 Advanced Service Configuration Options



Advanced Service Configuration Options

View & edit advanced options

Property	Value
⊟ Bandwidth Management	
Relax BWC enforcement on netw	Use Default Service BWCs (relaxed enforcement)
⊟ Classification	
Click Stream Event recognition	true
Enable sending '404, Page Not Fo	false
Guruguru detailed inspection moc	false
Kuro detailed inspection mode er	false
Number of HTTP GET detections	1
Soribada detailed inspection mod	false
TCP destination port signatures	1720:H323
UDP destination port signatures	68:DHCP,67:DHCP,1812:Radius Access,1645:Radius Acc...
UDP ports for which flow should I	5060,5061,67,68,69,1812,1813,1645,1646,2427,2727,...
UDP source port signatures	1812:Radius Access,1645:Radius Access,1813:Radius Ac...
V-Share detailed inspection mode	false
Winny detailed inspection mode e	false
⊟ Malicious Traffic	
Malicious Traffic RDRs enabled	true
Number of seconds between Mal	60
TCP port that should remain opei	80
⊟ Multi Stage Classification	

Step 4 Make your changes to the configuration options.

Step 5 Click **OK**.

The Advanced Service Configuration Options dialog box closes.

The changes to the advanced options are saved.

Step 6 Click **OK**.

The System Settings dialog box closes.

Managing VAS Settings

Value Added Service (VAS) settings includes the following features:

- Traffic mirroring—Traffic mirroring allows using the SCE to mirror a portion of the traffic based on its application and subscriber awareness. Traffic to be mirrored continues forwarding as is, and copies of the packets are sent to the corresponding VAS VLAN, thereby minimizing traffic.
- Traffic forwarding—Traffic forwarding servers allows you to use an external expert system (VAS server) for additional traffic processing, such as intrusion detection and content filtering to subscribers. After processing, flows are sent back to the SCE platform, which then sends them to their original destinations.

  The flows to be forwarded are selected based on the subscriber package and the flow type (IP protocol type and destination port number).

VAS mirroring has the following limitations:

- The SCE 2000 and SCE8000 both support traffic mirroring.
- Traffic mirroring is supported on any SCE platform that has at least 2 ports.
- An SCE8000 can contain 64 distinct VLANs.
- An SCE 2000 supports 8 distinct VLANs.

VAS forwarding has the following limitations:

- Only the SCE 2000 4xGBE and SCE8000 platforms support VAS traffic forwarding.
- A single SCE platform can support up to eight VAS servers.
- A service configuration can contain up to 64 traffic-forwarding tables.
- A traffic-forwarding table can contain up to 64 table parameters.
- VAS traffic forwarding is not supported when unidirectional classification is enabled.

Note Because of the complexity of the VAS settings features, VAS flows are not subject to global bandwidth control.

To use VAS traffic forwarding:

– You must configure VAS services on the SCE platform. Additional information is available in the “Value Added Services (VAS) Traffic Forwarding” chapter of the *Cisco SCE2000, SCE1000Software Configuration Guide* and “Intelligent Traffic Mirroring” chapter of the *Cisco SCE8000 GBE Software Configuration Guide* and *Cisco SCE8000 10GBE Software Configuration Guide*.

– You must also assign the VAS traffic-forwarding tables to packages in the Advanced tab of the Edit Packages dialog. VAS traffic-forwarding is based on per-package configuration of where to forward what traffic. To set a VAS traffic-forwarding table for a package, see the “How to Set Advanced Package Options” section on page 9-57.

How to Enable VAS Traffic Forwarding

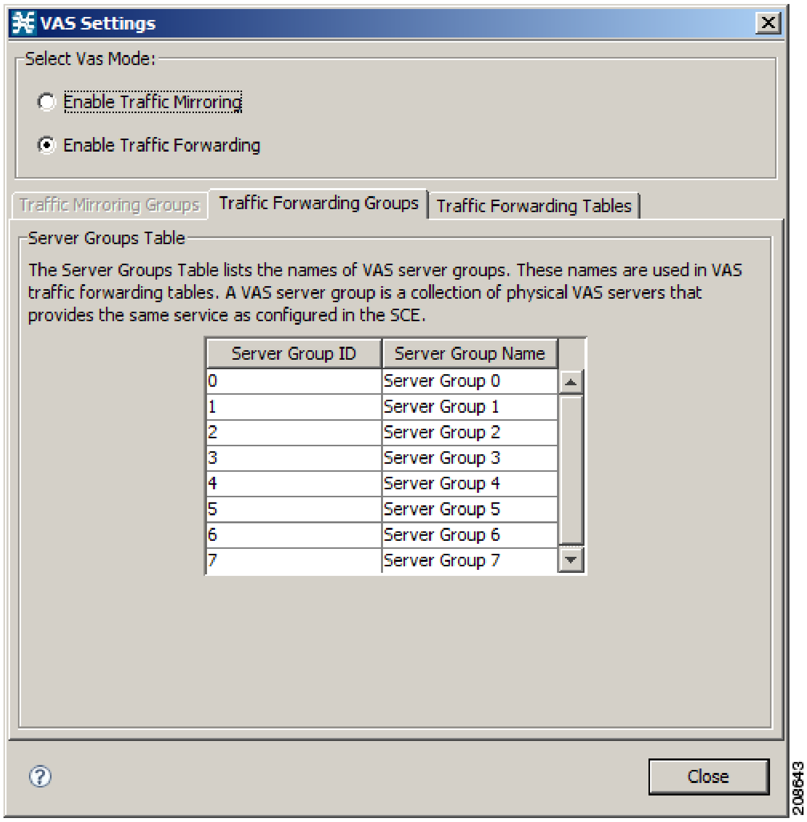
By default, VAS traffic forwarding is disabled. You can enable it at any time.

Note VAS traffic forwarding is not supported when unidirectional classification is enabled.

Step 1 From the Policies tab of the left pane, choose **Configuration > Policies > VAS Settings**.

The VAS Settings dialog box appears (Figure 10-47).

Figure 10-47 VAS Settings - Enable Traffic Forwarding



VAS Settings

Select Vas Mode:

○ Enable Traffic Mirroring

● Enable Traffic Forwarding

Traffic Mirroring Groups | Traffic Forwarding Groups | Traffic Forwarding Tables

Server Groups Table

The Server Groups Table lists the names of VAS server groups. These names are used in VAS traffic forwarding tables. A VAS server group is a collection of physical VAS servers that provides the same service as configured in the SCE.

Server Group ID	Server Group Name
0	Server Group 0
1	Server Group 1
2	Server Group 2
3	Server Group 3
4	Server Group 4
5	Server Group 5
6	Server Group 6
7	Server Group 7

Step 2 Click the **Enable Traffic Forwarding** radio button.

Note VAS traffic forwarding is not supported in asymmetric routing classification mode. If you try to check the Enable Traffic Forwarding radio button when asymmetric routing classification mode is enabled, a VAS Error message appears.

Click **OK**, and continue at Step 4.

A VAS warning message appears.

Step 3 Click **OK**.

Step 4 Click **Close**.

The VAS Settings dialog box closes.

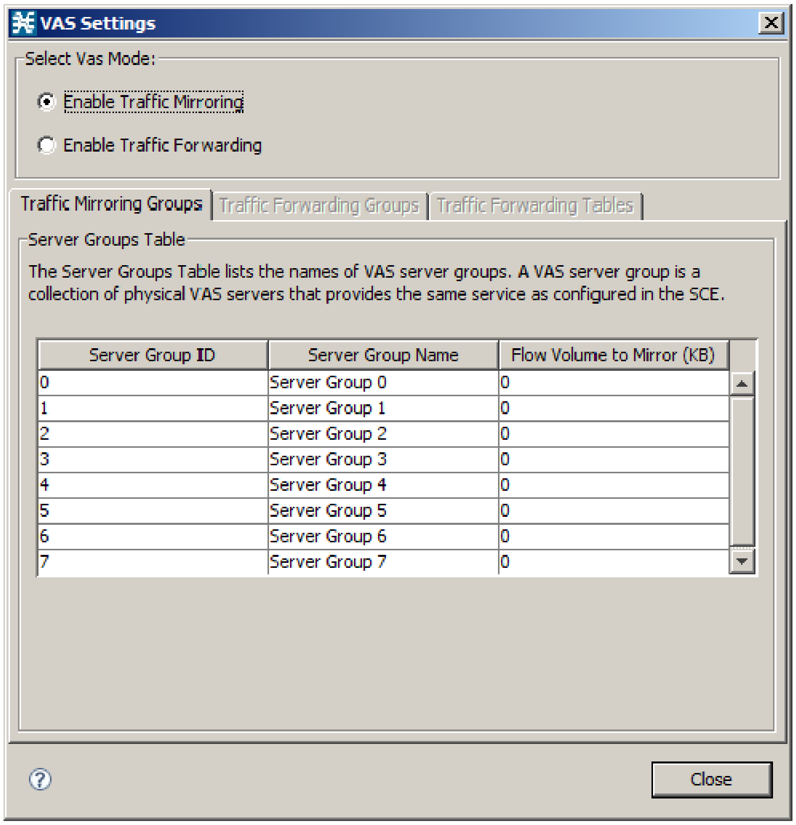
How to Enable VAS Traffic Mirroring

Traffic Mirroring in enabled and configured in the VAS Setting dialog box. However, you configure which server group to use when defining rules.

Step 1 From the Policies tab of the left pane, choose **Configuration > Policies > VAS Settings**.

The VAS Settings dialog box appears (Figure 10-48).

Figure 10-48 VAS Settings - Enable Traffic Mirroring



VAS Settings

Select Vas Mode:

● Enable Traffic Mirroring

○ Enable Traffic Forwarding

Traffic Mirroring Groups | Traffic Forwarding Groups | Traffic Forwarding Tables

Server Groups Table

The Server Groups Table lists the names of VAS server groups. A VAS server group is a collection of physical VAS servers that provides the same service as configured in the SCE.

Server Group ID	Server Group Name	Flow Volume to Mirror (KB)
0	Server Group 0	0
1	Server Group 1	0
2	Server Group 2	0
3	Server Group 3	0
4	Server Group 4	0
5	Server Group 5	0
6	Server Group 6	0
7	Server Group 7	0

Step 2 Choose the **Enable Traffic Mirroring** radio button.

A VAS warning message appears.

Step 3 Click **OK**.

Step 4 Click **Close**.

The VAS Settings dialog box closes.

How to Rename VAS Server Groups

An SCE platform can forward flows to up to eight different VAS server groups. By default, the eight server groups are named "Server Group n", where n takes a value from 0 to 7. Give the server groups meaningful names; the names you give appears in the drop-down list in the Control and Breach Handling tabs of the Add Rule to Package dialog box (see How to Set Advanced Package Options, page 9-57) and in the Server Group field of the table parameters added to each traffic-forwarding table (see Managing VAS Table Parameters, page 10-74).

Step 1 From the Policies tab of the left pane, choose **Configuration > Policies > VAS Settings**.

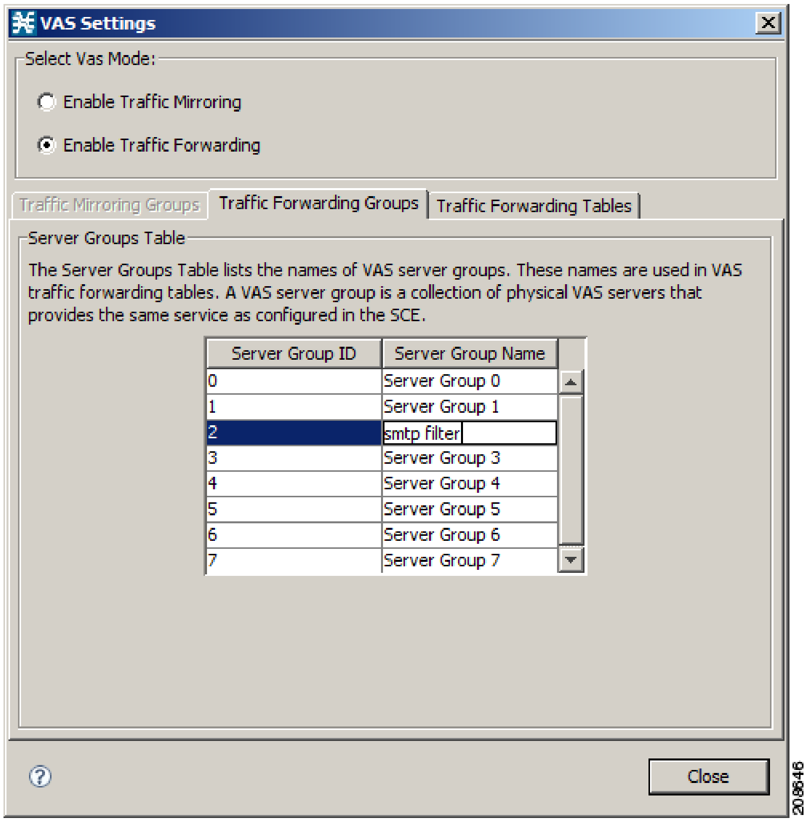
The VAS Settings dialog box appears (Figure 10-49).

Step 2 In the table in the Server Groups Table area, double-click in a cell containing a server group name.

Step 3 Enter a meaningful name in the cell.

Step 4 Repeat Step 2 and Step 3 for other server groups you wish to rename.

Figure 10-49 Traffic Forwarding Groups Tab



VAS Settings

Select Vas Mode:

○ Enable Traffic Mirroring

● Enable Traffic Forwarding

Traffic Mirroring Groups | Traffic Forwarding Groups | Traffic Forwarding Tables

Server Groups Table

The Server Groups Table lists the names of VAS server groups. These names are used in VAS traffic forwarding tables. A VAS server group is a collection of physical VAS servers that provides the same service as configured in the SCE.

Server Group ID	Server Group Name
0	Server Group 0
1	Server Group 1
2	smtp filter
3	Server Group 3
4	Server Group 4
5	Server Group 5
6	Server Group 6
7	Server Group 7

Step 5 Click **Close**.

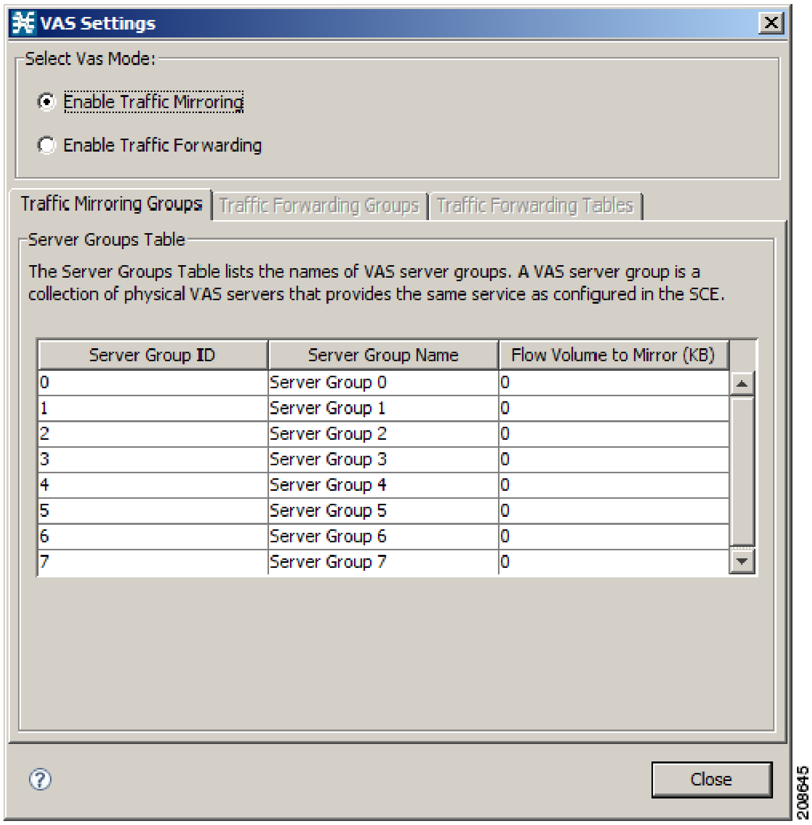
The VAS Settings dialog box closes.

How to Configure VAS Traffic-Mirroring

Step 1 From the Policies tab of the left pane, choose **Configuration > Policies > VAS Settings**.

The VAS Settings dialog box appears (Figure 10-50).

Figure 10-50 Traffic Mirroring Groups Tab



Select Vas Mode:

● Enable Traffic Mirroring

○ Enable Traffic Forwarding

Server Groups Table

The Server Groups Table lists the names of VAS server groups. A VAS server group is a collection of physical VAS servers that provides the same service as configured in the SCE.

Server Group ID	Server Group Name	Flow Volume to Mirror (KB)
0	Server Group 0	0
1	Server Group 1	0
2	Server Group 2	0
3	Server Group 3	0
4	Server Group 4	0
5	Server Group 5	0
6	Server Group 6	0
7	Server Group 7	0

Step 2 Click the **Enable Traffic Forwarding** radio button.

Step 3 For each server group, in the **Flow Volume to Mirror (KB)** column, enter the maximum amount of volume to mirror, in KB.

Step 4 Click **Close**.

The VAS Settings dialog box closes.

How to View VAS Traffic-Forwarding Tables

Cisco SCA BB decides whether a flow passing through an SCE platform should be forwarded to a VAS server group based on a traffic-forwarding table. Each entry (table parameter) in a traffic-forwarding table defines to which VAS server group the specified flows should be forwarded.

Step 1 From the Policies tab of the left pane, choose **Configuration > Policies > VAS Settings**.

The VAS Settings dialog box appears.

Step 2 Click the **Enable Traffic Forwarding** radio button.

Step 3 Click the **Traffic Forwarding Tables** tab.

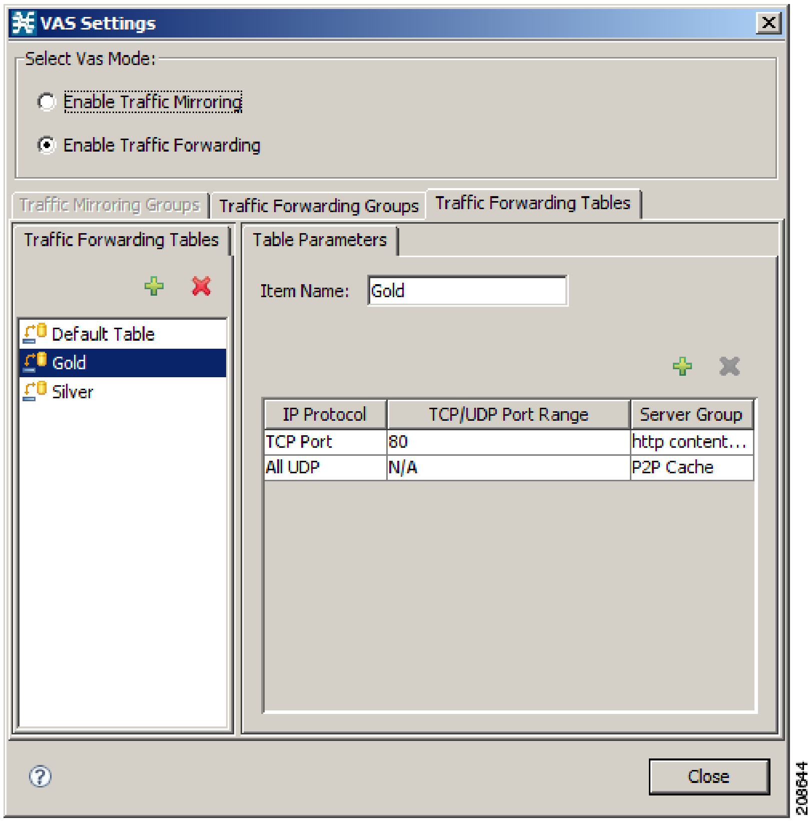
The Traffic Forwarding Tables tab opens.

A list of all traffic-forwarding tables is displayed in the Traffic Forwarding Tables area.

Step 4 Click a table in the list of traffic-forwarding tables to display its table parameters.

A list of all table parameters defined for this traffic-forwarding table opens in the Table Parameters tab (Figure 10-51).

Figure 10-51 Traffic Forwarding Tables Tab



VAS Settings

Select Vas Mode:

○ Enable Traffic Mirroring

● Enable Traffic Forwarding

Traffic Mirroring Groups | Traffic Forwarding Groups | Traffic Forwarding Tables

Traffic Forwarding Tables

- Default Table
- Gold
- Silver

Table Parameters

Item Name: Gold

IP Protocol	TCP/UDP Port Range	Server Group
TCP Port	80	http content...
All UDP	N/A	P2P Cache

Close

Step 5 Click **Close**.

The VAS Settings dialog box closes.

How to Delete VAS Traffic-Forwarding Tables

You can delete all user-created traffic-forwarding tables. The default traffic-forwarding table cannot be deleted.

Note A traffic-forwarding table cannot be deleted while it is associated with a package.

Step 1 From the Policies tab of the left pane, choose **Configuration > Policies > VAS Settings**.

The VAS Settings dialog box appears.

Step 2 Click the **Enable Traffic Forwarding** radio button.

Step 3 Click the **Traffic Forwarding Tables** tab.

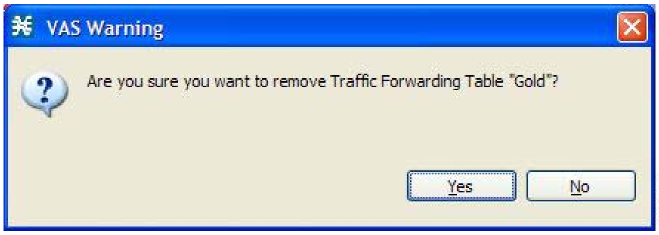
The Traffic Forwarding Tables tab opens.

Step 4 From the list of traffic-forwarding tables in the Traffic Forwarding Tables area, select a table.

Step 5 Click the **Delete** (✖) icon.

A VAS Warning message appears (Figure 10-52).

Figure 10-52 VAS Warning



VAS Warning

Are you sure you want to remove Traffic Forwarding Table "Gold"?

Step 6 Click **Yes**.

The selected table is deleted and is no longer displayed in the list of traffic-forwarding tables.

Step 7 Click **Close**.

The VAS Settings dialog box closes.

How to Add VAS Traffic-Forwarding Tables

A default traffic-forwarding table is included in the service configuration. You can add up to 63 more traffic-forwarding tables, and then assign different traffic-forwarding tables to different packages.

Step 1 From the Policies tab in the left pane, choose **Configuration > Policies > VAS Settings**.

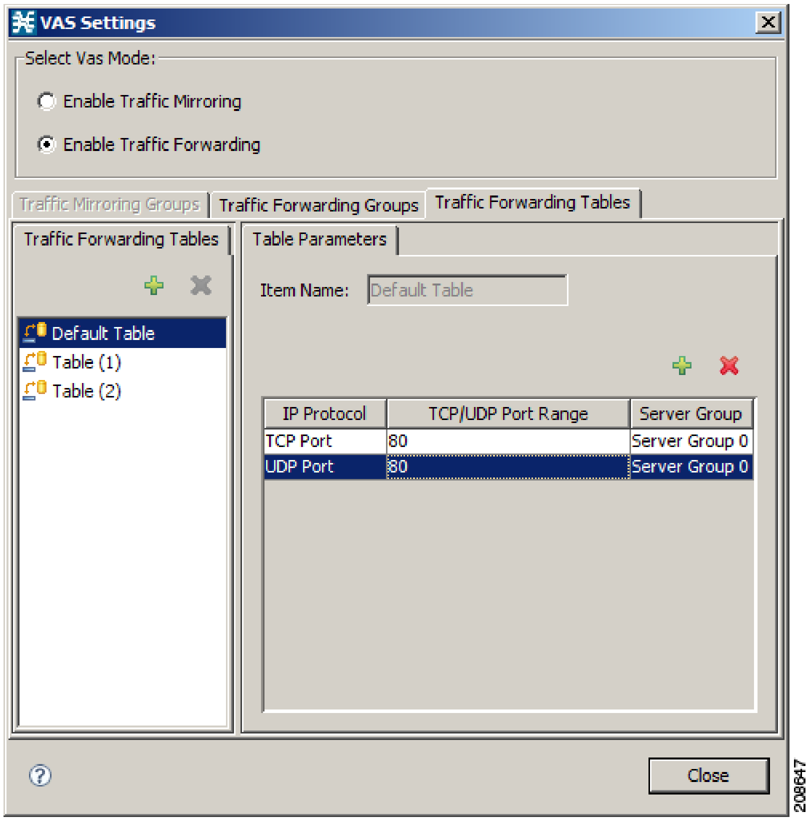
The VAS Settings dialog box appears.

Step 2 Click the **Enable Traffic Forwarding** radio button.

Step 3 Click the **Traffic Forwarding Tables** tab.

The Traffic Forwarding Tables tab opens (Figure 10-53).

Figure 10-53 VAS Settings - Add VAS Traffic-Forwarding Tables


VAS Settings
Traffic Mirroring Groups
Traffic Forwarding Groups
Traffic Forwarding Tables
Traffic Forwarding Tables
Table Parameters
Close
208647

Select Vas Mode:

○ Enable Traffic Mirroring

● Enable Traffic Forwarding

Traffic Forwarding Tables:

- Default Table
- Table (1)
- Table (2)

Item Name: Default Table

IP Protocol	TCP/UDP Port Range	Server Group
TCP Port	80	Server Group 0
UDP Port	80	Server Group 0

Step 4 In the Traffic Forwarding Tables area, click the **Add** (✚) icon.

A new table named Table (n), where *n* is a value from 1 through 63, is added to the list of traffic-forwarding tables in the Traffic Forwarding Tables area.

The table name is also displayed in the Item Name box in the Table Parameters tab.

Step 5 In the Item Name field, enter a unique and relevant name for the traffic-forwarding table.

You can now add table parameters to the new traffic-forwarding table, see How to Add VAS Table Parameters, page 10-75.

Managing VAS Table Parameters

A table parameter is an IP protocol type, an associated TCP/UDP port (where applicable), and a VAS server group or a range of IP addresses.

A traffic-forwarding table is a collection of related table parameters.

A traffic-forwarding table can contain up to 64 table parameters.

- How to Add VAS Table Parameters, page 10-75
- How to Edit VAS Table Parameters, page 10-75
- How to Delete VAS Table Parameters, page 10-77

How to Add VAS Table Parameters

You can add up to 64 table parameters to a traffic-forwarding table.

Step 1 From the Policies tab in the left pane, choose **Configuration** > **Policies** > **VAS Settings**.

The VAS Settings dialog box appears.

Step 2 Click the **Enable Traffic Forwarding** radio button.

Step 3 Click the **Traffic Forwarding Tables** tab.

The Traffic Forwarding Tables tab opens.

Step 4 From the list of traffic-forwarding tables in the Traffic Forwarding Tables area, select a table.

Step 5 In the Traffic Parameters tab, click the **Add** (✚) icon.

A new table parameter is added to the list of table parameters in the Table Parameters tab.

Note Each new table parameter has the default values as listed in Table 10-4.

Table 10-4 Table Parameter Default Values

Parameter	Default value
IP Protocol	TCP Port
TCP/UDP Port Range	80
Server Group	Server Group 0

You can now edit the new table parameter, as described in the following section.

Step 6 Click **Close**.

The VAS Settings dialog box closes.

How to Edit VAS Table Parameters

Step 1 From the Policies tab in the left pane, choose **Configuration** > **Policies** > **VAS Settings**.

The VAS Settings dialog box appears.

Step 2 Click the **Enable Traffic Forwarding** radio button.

Step 3 Click the **Traffic Forwarding Tables** tab.

The Traffic Forwarding Tables tab opens.

Step 4 From the list of traffic-forwarding tables in the Traffic Forwarding Tables area, select a table.

Step 5 In the table in the Table Parameters tab select a protocol, port, and server group.

a. Click in a cell in the IP Protocol column, and, from the drop-down list that opens, select an IP protocol type (Figure 10-54).

Figure 10-54 Table Parameters Tab

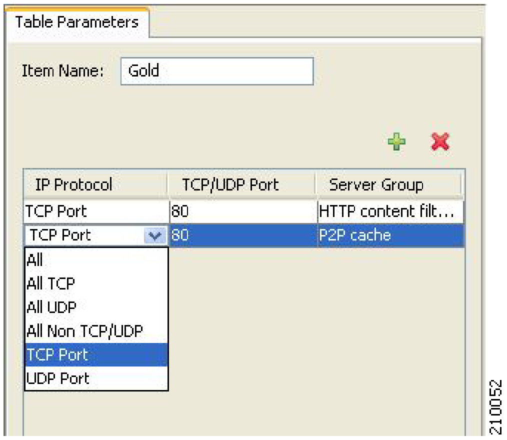


Table Parameters

Item Name: Gold

IP Protocol	TCP/UDP Port	Server Group
TCP Port	80	HTTP content filt...
TCP Port	80	P2P cache

If you select All, All TCP, All UDP, or All Non TCP/UDP, "N/A" appears in the TCP/UDP Port cell when you move to another cell in the table.

b. If you selected TCP Port or UDP Port, double-click in the cell in the TCP/UDP Port Range column, and enter the port number or a range of ports.

c. Click in the cell in the Server Group column, and, from the drop-down list that opens, select a server group (Figure 10-55).

Figure 10-55 Tables Parameters Tab

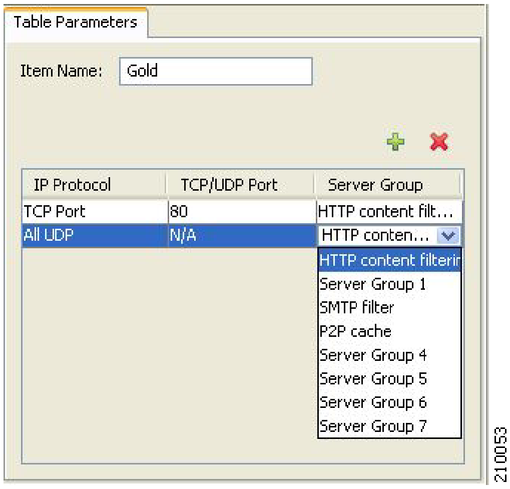


Table Parameters

Item Name: Gold

IP Protocol	TCP/UDP Port	Server Group
TCP Port	80	HTTP content filt...
All UDP	N/A	HTTP conten...

Step 6 Click **Close**.

The VAS Settings dialog box closes.

How to Delete VAS Table Parameters

Step 1 From the Policies tab in the left pane, choose **Configuration > Policies > VAS Settings**.

The VAS Settings dialog box appears.

Step 2 Click the **Enable Traffic Forwarding** radio button.

Step 3 Click the **Traffic Forwarding Tables** tab.

The Traffic Forwarding Tables tab opens.

Step 4 From the list of traffic-forwarding tables in the Traffic Forwarding Tables area, select a table.

Step 5 From the list of table parameters in the Table Parameters tab, select a table parameter.

Step 6 Click the **Delete** (❌) icon.

The selected table parameter is deleted and is no longer displayed in the list of table parameters.

Step 7 Click **Close**.

The VAS Settings dialog box closes.

Managing the Protected URL Database

The SCE Protected URL Database is a database that contains a “blacklist,” a list of websites that are considered off limits or dangerous. You can configure the SCE to apply a specific action, such as blocking a site, when a subscriber attempts to access a site listed on the blacklist.

The database is encrypted so that no one, including the operator, can view the blacklist. The blacklist is managed on the SCE and cannot be withdrawn to the management PC.

RDRs are created when a subscriber attempts to access a link included in the blacklist. However, the RDRs do not contains the URL or Host information of the site.

To enable the blacklist feature, you must do the following:

- Define an HTTP flavor
- Create a blacklist service
- Assign the HTTP flavor to the blacklist service
- Create a rule for the blacklist service
- Assign black list entries to the flavor, using the CLI

For more information about the Protected URL Database, see the *Cisco Service Control URL Blacklisting Solution Guide*.

CHAPTER 11

Using the Subscriber Manager GUI Tool

Revised: August 08, 2013, OL-24178-09

Introduction

This chapter describes how to use the Subscriber Manager (SM) graphical user interface (GUI) tool to configure subscribers in the Cisco Service Control Management Suite (SCMS) SM database.

The SM GUI tool is especially useful when the SCMS SM holds a static list of subscribers. It is not applicable when Cisco SCA BB is operating in subscriberless mode (a mode in which control and analysis functions are available only at a global platform resolution) or in anonymous subscriber mode (a mode in which entities defined as IP addresses or VLANs are treated as subscribers).

Using the SM GUI Tool

The SM GUI tool allows you to manage subscribers on an SCMS SM. The SCMS SM functions as middleware software that bridges between the OSS and the Service Control Engine (SCE) platforms. SCE platforms use the subscriber information to provide subscriber-aware functionality, per-subscriber reporting, and policy enforcement. Subscriber information is stored in the SCMS SM database and can be distributed between multiple platforms according to actual subscriber placement.

You can use the SM GUI tool to import and export subscriber files, and to perform operations on individual subscribers, such as:

- Add and delete a subscriber
- Edit parameters and show data of an existing subscriber
- Add and remove subscriber mappings
- Import subscribers from a CSV file
- Export subscribers to a CSV file
- Find subscriber or subscribers in a certain domain (filter)

Note To access an SCMS SM from the SM GUI tool, you must first add the SCMS SM to the Site Manager tree in the Network Navigator tool (see How to Add Subscriber Manager Devices to a Site, page 5-4).

The SM GUI tool provides only a subset of the functionality that the SM Command-Line Utility provides. For more information about the SCMS SM, see the *Cisco Service Control Management Suite Subscriber Manager User Guide.*

Connecting to an SCMS SM

You can connect to an SCMS SM:

- From the Network Navigator tool
- From anywhere else in the Console
- From the Subscriber Manager GUI tool

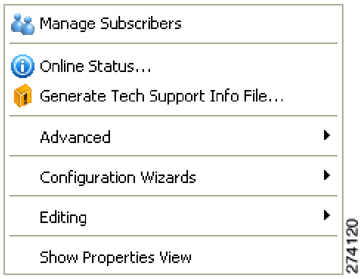
Note The SM GUI tool performs authentication on the SCMS SM by opening a PRPC connection to port 14374 and attempting to log in using the username and password that you entered in the Password Management dialog box. If a PRPC server with this user is not running on the SCMS SM, authentication fails. If you have changed the PRPC port on the SCMS SM, see User Authentication, page 5-40.

How to Connect to an SCMS SM from the Network Navigator

Step 1 In the Site Manager tree in the Network Navigator tab, right-click an SM device.

A popup menu appears (Figure 11-1).

Figure 11-1 SM Device Popup Menu



Step 2 From the menu, select **Manage Subscribers**.

A Password Management dialog box appears.

Step 3 Enter the appropriate password. (For more information, see Password Management, page 5-8).

Step 4 Click **Connecting**.

The Password Management dialog box closes.

A Connecting to progress bar appears.

The system connects to the SCMS SM.

How to Connect to an SCMS Subscriber Manager from the Console

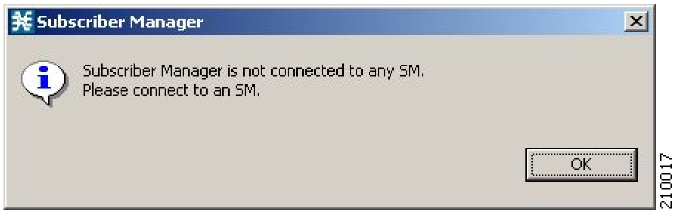
Note If you are already in the Subscriber Manager GUI tool, start at Step 3.

Step 1 From the Console main menu, choose **Tools > Subscriber Manager**.

The Subscriber Manager GUI tool opens.

A Subscriber Manager is not connected message appears (Figure 11-2).

Figure 11-2 Subscriber Manager is not Connected



Subscriber Manager is not connected to any SM.
Please connect to an SM.

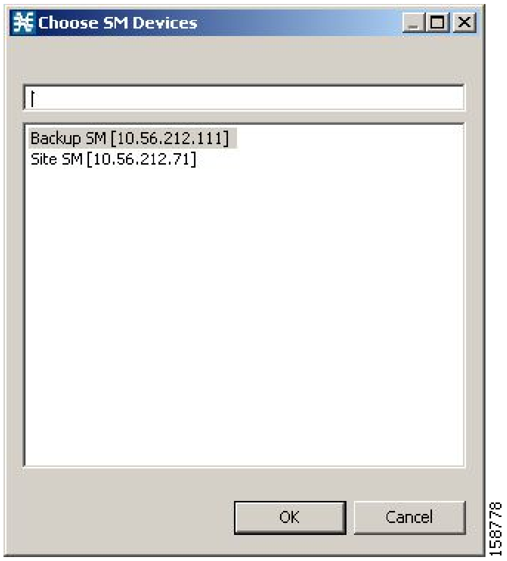
Step 2 Click **OK**.

The Subscriber Manager is not connected message closes.

Step 3 In the Subscriber Manager GUI toolbar, click the **Connect to an SM** ( ) icon.

If more than one SCMS SM device is configured in the Network Navigator, the Choose SM Devices dialog box appears (Figure 11-3).

Figure 11-3 Choose SM Devices



Choose SM Devices

Backup SM [10.56.212.111]
Site SM [10.56.212.71]

Step 4 Select a device and click **OK**.

A Password Management dialog box appears.

Step 5 Enter the appropriate password. (For more information, see Password Management, page 5-8.)

Step 6 Click **Connecting**.

The Password Management dialog box closes.

A Connecting to progress bar appears.

The system connects to the SCMS SM. The **Import subscribers from CSV file** ( ), the **Export subscribers to CSV file** ( ), and the **Disconnect from SM** ( ) icons are enabled.

How to Disconnect from the Current SCMS Subscriber Manager

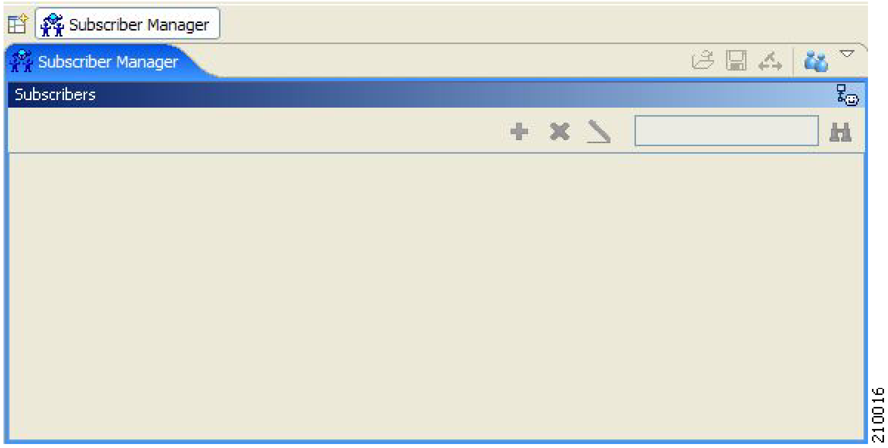
Step 1 In the SM GUI toolbar, click the **Disconnect from SM** ( ) icon.

The Console disconnects from the SCMS Subscriber Manager, but the SM GUI tool remains open.

The **Import subscribers from CSV file** ( ), the **Export subscribers to CSV file** ( ), and the **Disconnect from SM** ( ) icons are dimmed.

The subscriber list is empty (Figure 11-4).

Figure 11-4 Subscriber Manager List



Working with Subscriber CSV Files

Because of the large number of subscribers that must be introduced into the system, it is not feasible to enter subscriber information manually. Usually a RADIUS server (or some similar source) generates the subscriber information. This information is then imported into the SM GUI tool.

You can also export updated subscriber information to a CSV file.

The format of subscriber CSV files is described in the "CSV File Formats" chapter of *Cisco Service Control Application for Broadband Reference Guide*.

- How to Import Subscriber Information from a CSV File, page 11-6
- How to Export Subscriber Information to a CSV File, page 11-7

How to Import Subscriber Information from a CSV File

You can import subscriber data that was exported to a CSV file into the SM GUI tool.

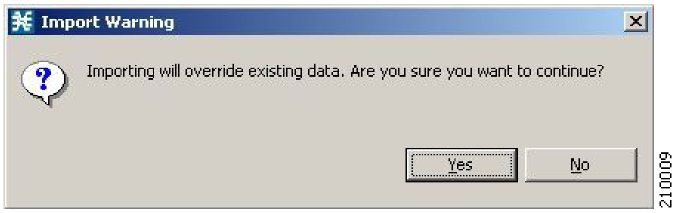
Step 1 In the SM GUI toolbar, click the **Import subscribers from CSV file** (📂) icon.

An Import from File dialog box appears.

Step 2 Browse to the file that is to be imported and click **Open**.

An Import Warning message appears (Figure 11-5).

Figure 11-5 Import Warning



Import Warning

Importing will override existing data. Are you sure you want to continue?

Step 3 Click **Yes**.

The Import from File dialog box closes.

The selected file is imported into the SM GUI tool; the imported subscribers are listed in the subscriber list.

How to Export Subscriber Information to a CSV File

You can export subscriber information to a CSV file (for example, when data in the SCMS SM database is updated).

Step 1 Select the subscribers whose data you want to save (see Selecting Subscribers, page 11-14).

Step 2 In the SM toolbar, click the **Export subscribers to CSV file** 💾 icon.

An Export to File dialog box appears.

Step 3 Browse to the folder in which you want to save the exported file.

Step 4 In the File name field, enter a file name.

Step 5 Click **Save**.

The Export to File dialog box closes.

The selected subscribers are saved to the CSV file.

Managing Subscribers

After importing subscribers into the system, you can maintain and update the database.

You can perform the following operations:

- Add and delete subscribers
- Edit information for existing subscribers
- Add and remove subscriber mappings

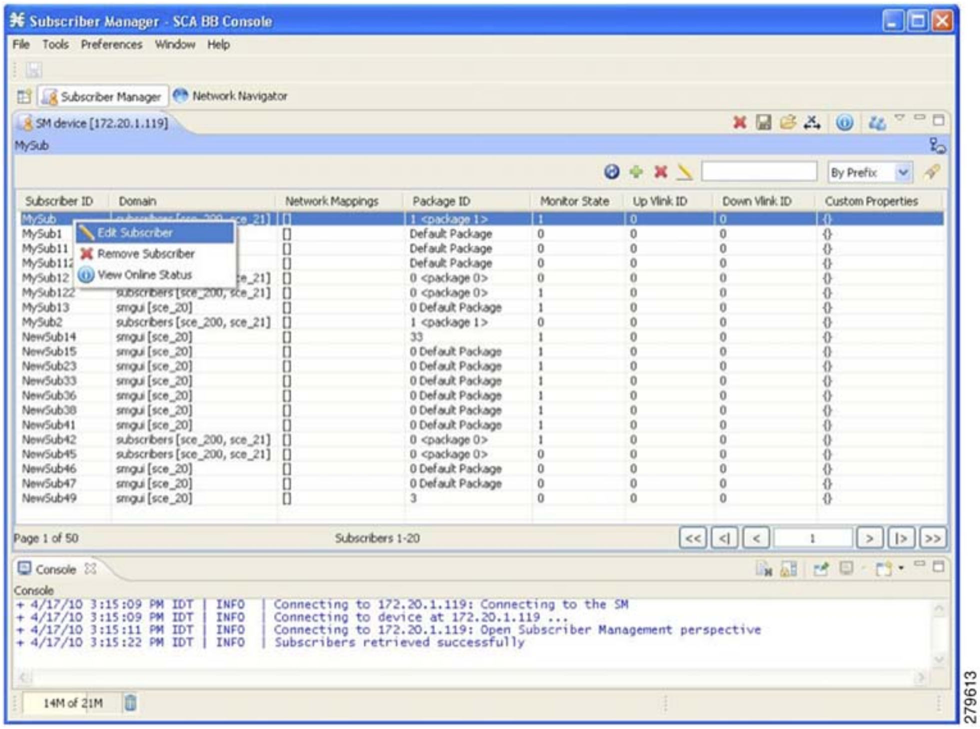
Subscriber Information

In the SM GUI, you can see a list of all the subscribers currently introduced into Cisco SCA BB (Figure 11-6). Use this list to manage individual subscribers or groups of subscribers. Use the Find function to display a subset of the subscribers (see How to Find a Subscriber or Group of Subscribers, page 11-13).

The SM GUI is composed of a console view at the bottom and a device view at the top. The console shows the log messages. The device view has the following columns:

- Subscriber ID—Name of the subscriber in the system.
- Domain—Domain to which the subscriber is assigned. The names of the SCE platforms that belong to each domain appear in square brackets.
- Network Mappings—IP address, range of IP addresses, or VLAN tag mapped to the subscriber.
- Properties—Various properties assigned to the subscriber (Package ID, Monitor State, Up Vlink ID, Down Vlink ID).
- Custom Properties—Displayed as key value pairs.

Figure 11-6 Subscriber Manager GUI - Subscriber List



Subscriber ID	Domain	Network Mappings	Package ID	Monitor State	Up Vlink ID	Down Vlink ID	Custom Properties
MySub	subscribers [sce_200, sce_21]	[]	1 <package 1>	1	0	0	{}
MySub1		[]	Default Package	0	0	0	{}
MySub11		[]	Default Package	0	0	0	{}
MySub112		[]	Default Package	0	0	0	{}
MySub12	e_21]	[]	0 <package 0>	0	0	0	{}
MySub122	subscribers [sce_200, sce_21]	[]	0 <package 0>	1	0	0	{}
MySub13	smgui [sce_20]	[]	0 Default Package	1	0	0	{}
MySub2	subscribers [sce_200, sce_21]	[]	1 <package 1>	0	0	0	{}
NewSub14	smgui [sce_20]	[]	33	1	0	0	{}
NewSub15	smgui [sce_20]	[]	0 Default Package	1	0	0	{}
NewSub23	smgui [sce_20]	[]	0 Default Package	1	0	0	{}
NewSub33	smgui [sce_20]	[]	0 Default Package	1	0	0	{}
NewSub36	smgui [sce_20]	[]	0 Default Package	1	0	0	{}
NewSub38	smgui [sce_20]	[]	0 Default Package	1	0	0	{}
NewSub41	smgui [sce_20]	[]	0 Default Package	1	0	0	{}
NewSub42	subscribers [sce_200, sce_21]	[]	0 <package 0>	1	0	0	{}
NewSub45	subscribers [sce_200, sce_21]	[]	0 <package 0>	0	0	0	{}
NewSub46	smgui [sce_20]	[]	0 Default Package	0	0	0	{}
NewSub47	smgui [sce_20]	[]	0 Default Package	0	0	0	{}
NewSub49	smgui [sce_20]	[]	3	0	0	0	{}

Page 1 of 50   Subscribers 1-20

```
+ 4/17/10 3:15:09 PM IDT | INFO  | Connecting to 172.20.1.119: Connecting to the SM
+ 4/17/10 3:15:09 PM IDT | INFO  | Connecting to device at 172.20.1.119 ...
+ 4/17/10 3:15:11 PM IDT | INFO  | Connecting to 172.20.1.119: Open Subscriber Management perspective
+ 4/17/10 3:15:22 PM IDT | INFO  | Subscribers retrieved successfully
```

Table 11-1 describes the icons grouped in the toolbar at the upper right corner of the SM GUI.

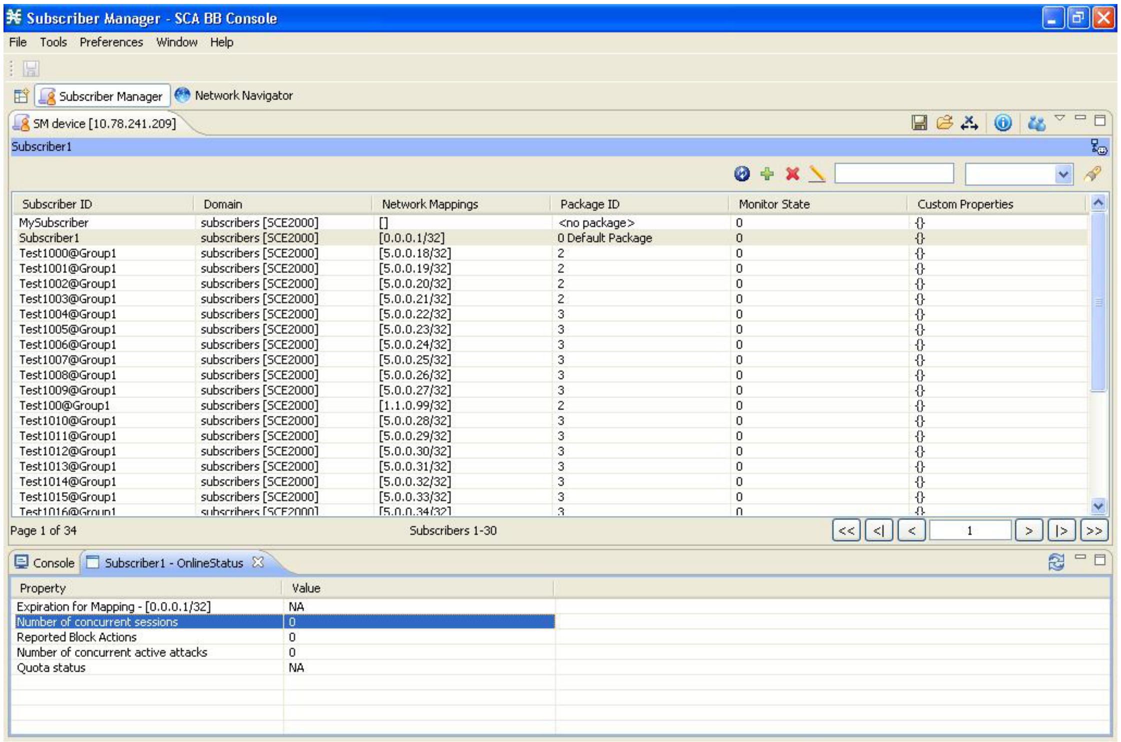
Table 11-1 SM GUI Icon Descriptions

Icon	Description
✖	**Delete all subscribers (if enabled).**
💾	**Export subscribers to CSV file.**
📂	**Import subscribers from CSV file.**
✕ ↔	**Disconnect from SM.**
ⓘ	**View online status** **(opens SM online status window).**
👥	**Connect to an SM.**
⟳	**Refresh the list of subscribers.**
✚	Add subscriber.
✖	Remove subscriber.
✏	Edit subscriber.

By right-clicking on a specific subscriber, you can perform various actions, including:

- Edit subscriber data.
- Delete the subscriber.
- Display the online status of the subscriber (Figure 11-7), including:
  - Expiration or aging time (if any)
  - Number of concurrent sessions
  - Reported block actions
  - Number of concurrent active attacks
  - Quota status (if any)
  - Subscriber OS information
- View information on multiple subscriber in multiple windows.

Figure 11-7 Subscriber Manager GUI - Subscriber Online Status



Subscriber ID	Domain	Network Mappings	Package ID	Monitor State	Custom Properties
MySubscriber	subscribers [SCE2000]	[]	<no package>	0	{}
Subscriber1	subscribers [SCE2000]	[0.0.0.1/32]	0 Default Package	0	{}
Test1000@Group1	subscribers [SCE2000]	[5.0.0.18/32]	2	0	{}
Test1001@Group1	subscribers [SCE2000]	[5.0.0.19/32]	2	0	{}
Test1002@Group1	subscribers [SCE2000]	[5.0.0.20/32]	2	0	{}
Test1003@Group1	subscribers [SCE2000]	[5.0.0.21/32]	2	0	{}
Test1004@Group1	subscribers [SCE2000]	[5.0.0.22/32]	3	0	{}
Test1005@Group1	subscribers [SCE2000]	[5.0.0.23/32]	3	0	{}
Test1006@Group1	subscribers [SCE2000]	[5.0.0.24/32]	3	0	{}
Test1007@Group1	subscribers [SCE2000]	[5.0.0.25/32]	3	0	{}
Test1008@Group1	subscribers [SCE2000]	[5.0.0.26/32]	3	0	{}
Test1009@Group1	subscribers [SCE2000]	[5.0.0.27/32]	3	0	{}
Test100@Group1	subscribers [SCE2000]	[1.1.0.99/32]	2	0	{}
Test1010@Group1	subscribers [SCE2000]	[5.0.0.28/32]	3	0	{}
Test1011@Group1	subscribers [SCE2000]	[5.0.0.29/32]	3	0	{}
Test1012@Group1	subscribers [SCE2000]	[5.0.0.30/32]	3	0	{}
Test1013@Group1	subscribers [SCE2000]	[5.0.0.31/32]	3	0	{}
Test1014@Group1	subscribers [SCE2000]	[5.0.0.32/32]	3	0	{}
Test1015@Group1	subscribers [SCE2000]	[5.0.0.33/32]	3	0	{}
Test1016@Group1	subscribers [SCE2000]	[5.0.0.34/32]	3	0	{}

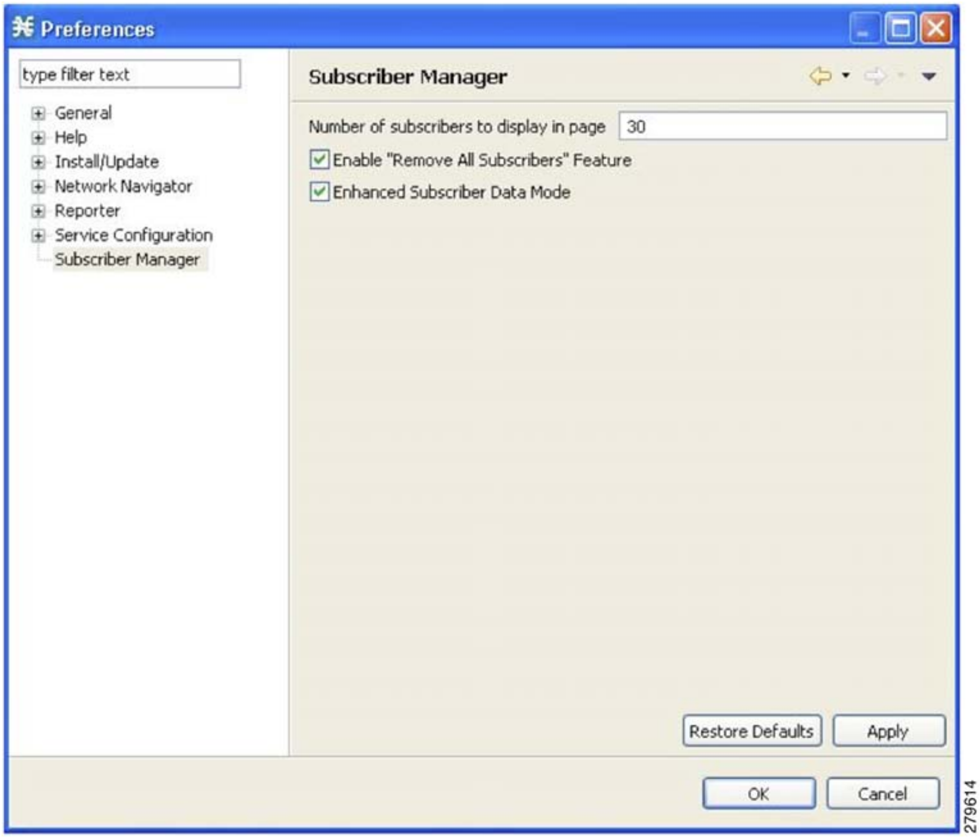
Page 1 of 34 Subscribers 1-30 << <| < 1 > |> >>

Property	Value
Expiration for Mapping - [0.0.0.1/32]	NA
Number of concurrent sessions	0
Reported Block Actions	0
Number of concurrent active attacks	0
Quota status	NA

From the menu bar, you can select and open the Preferences page (Figure 11-8). When the Subscriber Manager is selected in the left pane, you can do the following:

- Specify the number of subscriber records to be listed in the main display table.
- Enable or disable the “Remove All Subscribers” functionality.
- Enable or disable the enhanced subscriber data mode; if enabled, the Up Vlink ID and Down Vlink ID columns are displayed in the table.

Figure 11-8 Subscriber Manager GUI - Preferences Page



Subscriber Manager

Number of subscribers to display in page 30

☑ Enable "Remove All Subscribers" Feature

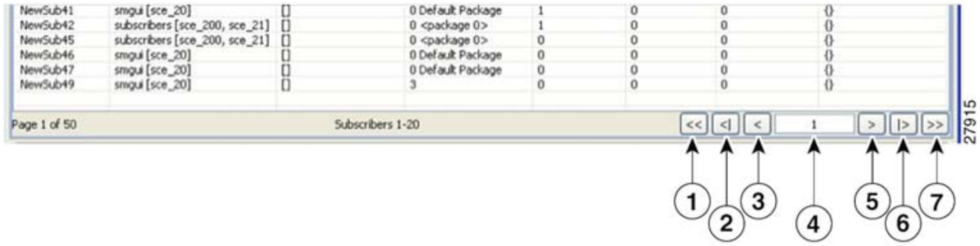
☑ Enhanced Subscriber Data Mode

Finding and Selecting Subscribers

The SM GUI tool retrieves subscribers in bulks of 1000 subscribers.

If the number of subscribers are more than that can be displayed in a standard view, then the information is presented in multiple pages. You can navigate to the remaining groups of subscribers using the various pagination buttons (Figure 11-9).

Figure 11-9 Subscriber Manager GUI - Pagination Buttons



NewSub41	smgui [sce_20]	[]	0 Default Package	1	0	0	{}
NewSub42	subscribers [sce_200, sce_21]	[]	0 <package 0>	1	0	0	{}
NewSub45	subscribers [sce_200, sce_21]	[]	0 <package 0>	0	0	0	{}
NewSub46	smgui [sce_20]	[]	0 Default Package	0	0	0	{}
NewSub47	smgui [sce_20]	[]	0 Default Package	0	0	0	{}
NewSub49	smgui [sce_20]	[]	3	0	0	0	{}

Page 1 of 50 Subscribers 1-20

- 1. Get previous bulk.
- 2. Get first page.
- 3. Get previous page.
- 4. Enter page number.
- 5. Get next page.
- 6. Get last page.
- 7. Get next bulk.

For ease of use, the SM GUI tool incorporates two standard features:

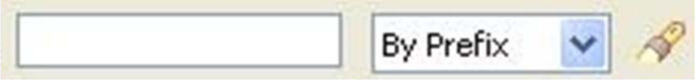
- Find—Search for a specific subscriber.
- Multiple Select—Select a range of subscribers or a number of individual subscribers.

How to Find a Subscriber or Group of Subscribers

Use the Find feature to find a specific subscriber or a group of subscribers according to a subscriber ID prefix. This feature is useful for editing the parameters of either a specific subscriber or a group of subscribers (see Editing Subscriber Details, page 11-17)

Step 1 In the Find field (Figure 11-10), enter the prefix to be matched.

Figure 11-10 Find Field



Step 2 Click the **Find Subscribers** ( ) icon.

You see a list of only the subscribers that match the specified prefix.

The search criteria is selected in the drop-down list next to the Find field. Search by:

- Prefix
- Domain name
- Package ID

Selecting Subscribers

You can edit, export, or delete a group of subscribers at one time by selecting subscribers displayed in the subscriber list. The group may be either of the following:

- A range of contiguous subscribers
- A number of noncontiguous subscribers

How to Select a Range of Subscribers

Step 1 Select the first subscriber in the range.

Step 2 Press the **Shift** key while clicking the last subscriber in the range.

All subscribers within the range are selected.

You can combine this function with the search function; search for specific subscribers and then select the entire range.

How to Select a Number of Noncontiguous Subscribers

Step 1 Press the **Ctrl** key while selecting multiple subscribers.

You can combine this function with selecting a range of subscribers; first, select the range of subscribers, and then select additional subscribers.

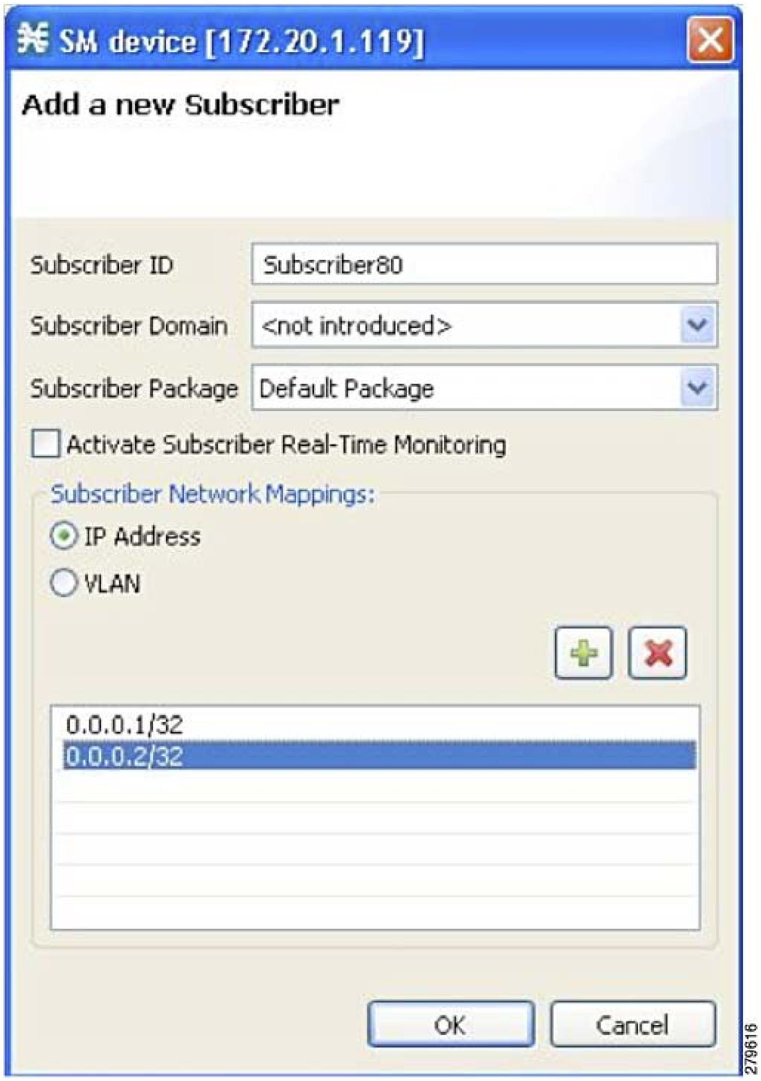
How to Add a Subscriber

You can add additional individual subscribers to the SCMS Subscriber Manager. To add large number of subscribers, export their information from a RADIUS (or DHCP) server to a CSV file, and then import the CSV file. For details on importing the CSV files, see Working with Subscriber CSV Files, page 11-6.

Step 1 In the SM GUI toolbar, click the **Add Subscriber** (✚) icon.

The Add a New Subscriber dialog box appears (Figure 11-11).

Figure 11-11 Add a New Subscriber



SM device [172.20.1.119]

Add a new Subscriber

Subscriber ID: Subscriber80

Subscriber Domain: <not introduced>

Subscriber Package: Default Package

□ Activate Subscriber Real-Time Monitoring

Subscriber Network Mappings:

● IP Address

○ VLAN

0.0.0.1/32
0.0.0.2/32

Step 2 In the Subscriber ID field, enter text that identifies the subscriber.

Step 3 From the Subscriber Domain drop-down list, select the appropriate domain for the new subscriber.

Step 4 From the Subscriber Package drop-down list, select a package to assign to this subscriber.

The contents of the list depend on the selected subscriber domain.

Step 5 To activate subscriber real-time monitoring, check the **Activate Subscriber Real-time Monitoring** check box. This sets the “monitor” property to 1 and causes the SCE application to generate Real-Time Subscriber Usage RDRs for this subscriber.

If you are not going to define network mappings for this subscriber, continue at Step 10.

Step 6 The system supports either IP addresses or VLAN tags as network identification for subscribers. Select one of the **Subscriber Network Mappings** radio buttons:

- **IP Address**
- **VLAN**

Note We recommend that you do not assign the same IPv6 address to different subscribers with different prefix values.

Step 7 Click **Add** (✚) icon to add a network mapping of the type selected.

A new network-mapping entry is added to the subscriber network mappings list, displaying a default value (Figure 11-11).

Step 8 Edit the network-mapping entry.

Step 9 Repeat Steps 7 and 8 for other network mappings.

Step 10 Click **OK**.

The Add a New Subscriber dialog box closes.

The new subscriber is added to the database and joins the subscriber list displayed in the SM GUI tool.

Editing Subscriber Details

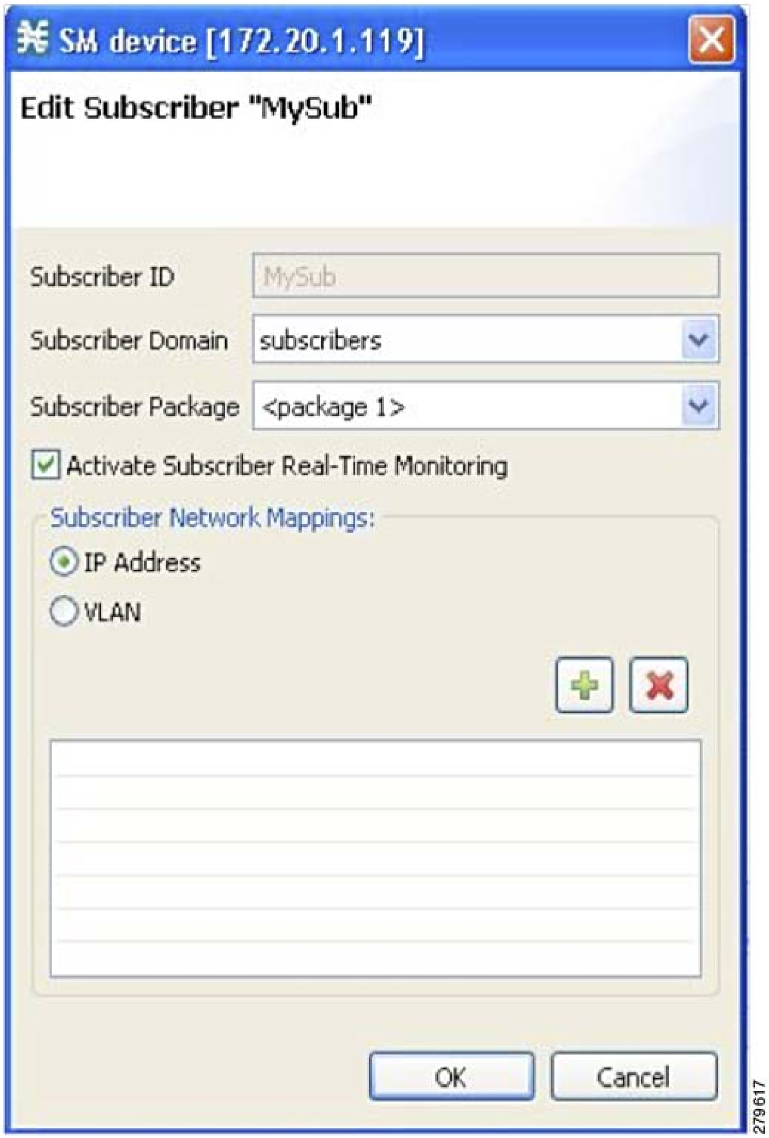
You can edit parameters for each subscriber.

Step 1 Find and select a subscriber. (See How to Find a Subscriber or Group of Subscribers, page 11-13.)

Step 2 In the SM toolbar, click the **Edit Subscriber** (✎) icon.

The Edit Subscriber dialog box appears (Figure 11-12).

Figure 11-12 Edit Subscriber



SM device [172.20.1.119]

Edit Subscriber "MySub"

Subscriber ID: MySub

Subscriber Domain: subscribers

Subscriber Package: <package 1>

☑ Activate Subscriber Real-Time Monitoring

Subscriber Network Mappings:

● IP Address

○ VLAN

Step 3 Modify subscriber details.

- Edit the entry in the Subscriber ID field.
- From the Subscriber Domain drop-down list, select a subscriber domain.
- From the Subscriber Package drop-down list, select a package to assign to this subscriber.

  The contents of the list depend on the selected subscriber domain.
- Check or uncheck the **Activate Subscriber Real-time Monitoring** check box.

If you are not editing the network mappings for this subscriber, continue at Step 5.

Step 4 Modify subscriber network mappings:

a. Click one of the **Subscriber Network Mappings** radio buttons:

- **IP Address**
- **VLAN**

b. To add a new network mapping to the list, click the Add (✚) icon, and edit the network-mapping field that is added to the Subscriber Network Mappings list.

c. To delete a network mapping from the list, select an entry in the subscriber network mappings list and click the Delete (✖) icon.

Step 5 Click **Apply**.

The Edit Subscriber dialog box closes.

The modified subscriber information is saved to the database and displayed in the subscriber list in the SM GUI tool.

How to Delete a Subscriber from the Database

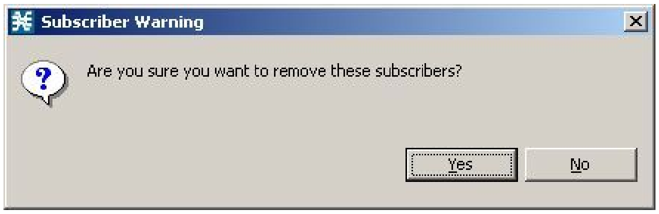
You can delete subscribers from the database.

Step 1 Select a single subscriber or a group of subscribers (see Selecting Subscribers, page 11-14).

Step 2 In the SM toolbar, click the **Delete Subscriber** (✖) icon.

The system asks for confirmation before deleting the selected subscribers (Figure 11-13).

Figure 11-13 Subscriber Warning



Subscriber Warning

Are you sure you want to remove these subscribers?

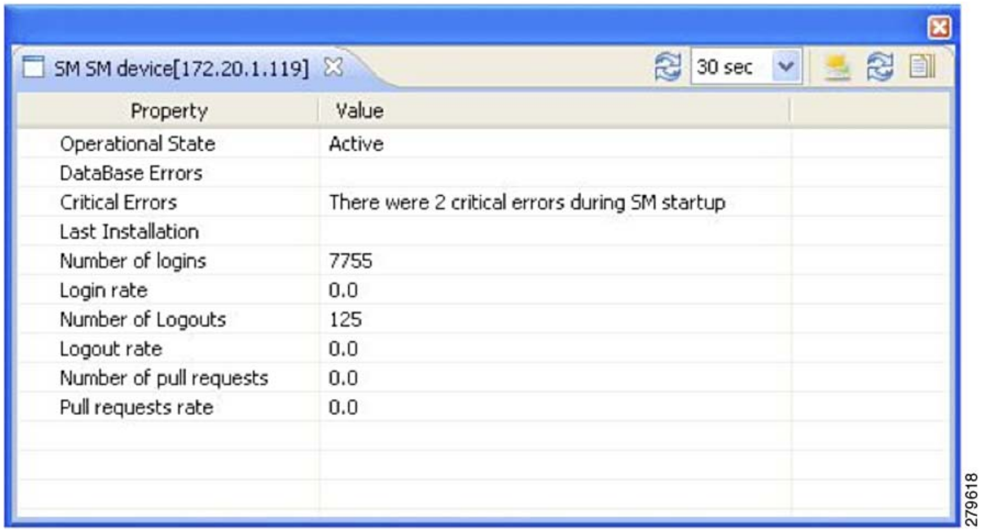
Step 3 Click **Yes** to confirm.

The selected subscribers are deleted from the database and removed from the subscriber list displayed in the SM GUI tool.

Monitoring SM Online Status

The SM online status window provides real-time status of the SM operation by displaying the main properties of the SM (Figure 11-14).

Figure 11-14 SM Online Status Window



Property	Value
Operational State	Active
DataBase Errors	
Critical Errors	There were 2 critical errors during SM startup
Last Installation	
Number of logins	7755
Login rate	0.0
Number of Logouts	125
Logout rate	0.0
Number of pull requests	0.0
Pull requests rate	0.0

You can open the SM Online Status window by clicking on the **Open** ( ) icon in the main GUI toolbar.

Table 11-2 describes the icons grouped in the toolbar at the upper right corner of the SM Online Status window.

Table 11-2 SM Online Status Window Icon Descriptions

Icon	Description
🔄	Autorefresh**, the drop-down list shows selectable time interval options (default 30 seconds)**
📋	**Copy all properties and values to the clipboard (or right-click a single property to copy)**
🗐	**Always on top (enable or disable place status window on top of other windows)**

CHAPTER 12

Using the Anonymous Group Manager Tool

Revised: August 08, 2013, OL-24178-09

Introduction

This chapter describes how to use the Anonymous Group Manager graphical user interface (GUI) tool to configure anonymous groups in an SCE.

This chapter consists of these sections:

- Using the Anonymous Group Manager GUI Tool, page 12-2
- Working with Anonymous Groups CSV Files, page 12-12
- Managing Anonymous Groups, page 12-3

Using the Anonymous Group Manager GUI Tool

You can use the Anonymous Group Manager GUI tool to import and export subscriber files, and to perform these operations on anonymous groups:

- Add and delete an anonymous group
- View the subscribers in a specific anonymous group
- Delete all anonymous groups
- View the configuration of a specific anonymous group
- Filter subscribers
- View online status of the subscriber
- View OS information of the subscribers in anonymous group
- Edit subscriber properties
- Import anonymous groups from a CSV file
- Export anonymous groups to a CSV file
- Export subscribers of a certain group to CSV file

For details on Anonymous Groups, Subscriber templates, and CSV file formats, see *Cisco SCE 8000 10GBE Software Configuration Guide*.

For more information about the SCMS Subscriber Manager, see the *Cisco Service Control Management Suite Subscriber Manager User Guide.*

Managing Anonymous Groups

After importing subscribers into the system, you can maintain and update the database.

You can perform these tasks:

- Add and delete an anonymous group
- View the subscribers in a specific anonymous group
- View the configuration of a specific anonymous group
- Delete all anonymous groups in the SCE
- Filter subscribers
- View online status of the subscriber
- Edit subscriber properties

This section contains information on:

- How to Add an SCE to the Anonymous Group Manager GUI Tool, page 12-7
- How to Add a New Anonymous Group in an SCE, page 12-7
- How to View the Configuration of a Specific Anonymous Group, page 12-8
- How to Delete All Anonymous Groups in an SCE, page 12-9
- How to View the Configuration of a Specific Anonymous Group, page 12-8
- How to View the Online Status of a Subscriber, page 12-10
- How to Edit the Subscriber Properties, page 12-11
- How to Remove Subscribers from an Anonymous Group in an SCE, page 12-11
- Working with Anonymous Groups CSV Files, page 12-12

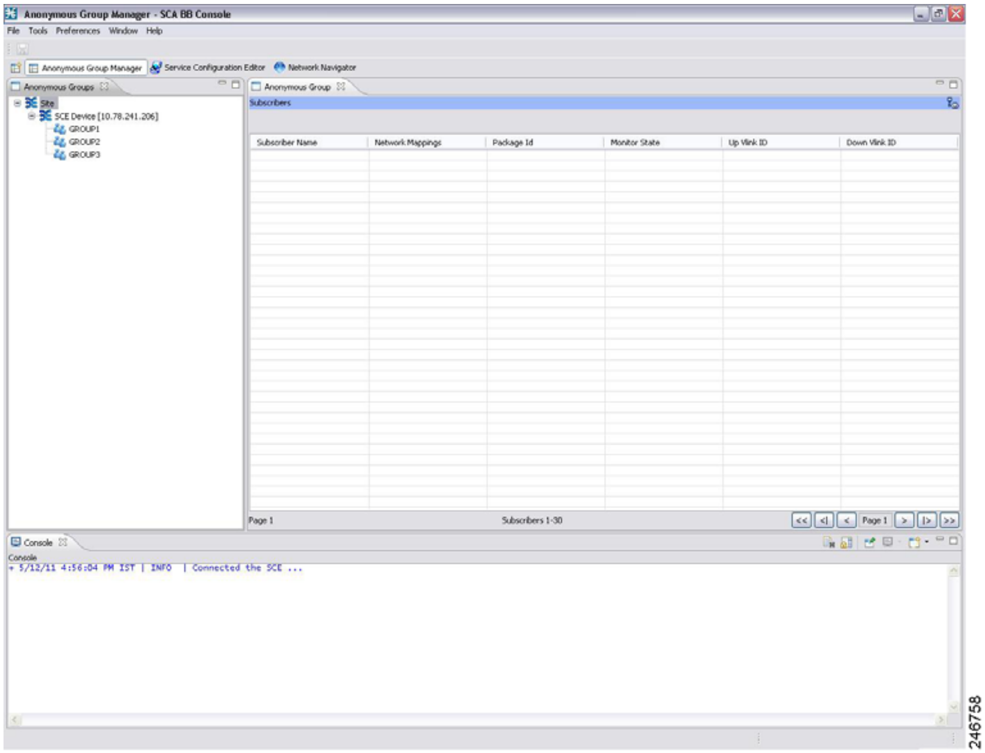
Anonymous Group Manager Information

In the Anonymous Group Manager GUI (Figure 12-1), you can see a list of anonymous groups configured in an SCE. Use this list to manage individual anonymous group or multiple groups of subscriber tables stacked together, and the subscribers in each anonymous group.

The Anonymous Group Manager GUI is composed of a console view at the bottom and a device view at the top. The console shows the log messages. The anonymous group view within the group folder has the following columns in a subscriber table:

- Subscriber Name—Name of the subscriber in the system.
- Mappings—IP address, range of IP addresses, or VLAN tag mapped to the subscriber.
- Package ID
- Monitor State
- Up VLINK ID
- Down VLINK ID
- Owner—Owner of the subscriber (For example, Subscriber Manager Device)

Figure 12-1 Anonymous Group Manager GUI - Group List



```
+ 5/12/11 4:56:04 PM IST | INFO  | Connected the SCE ...
```

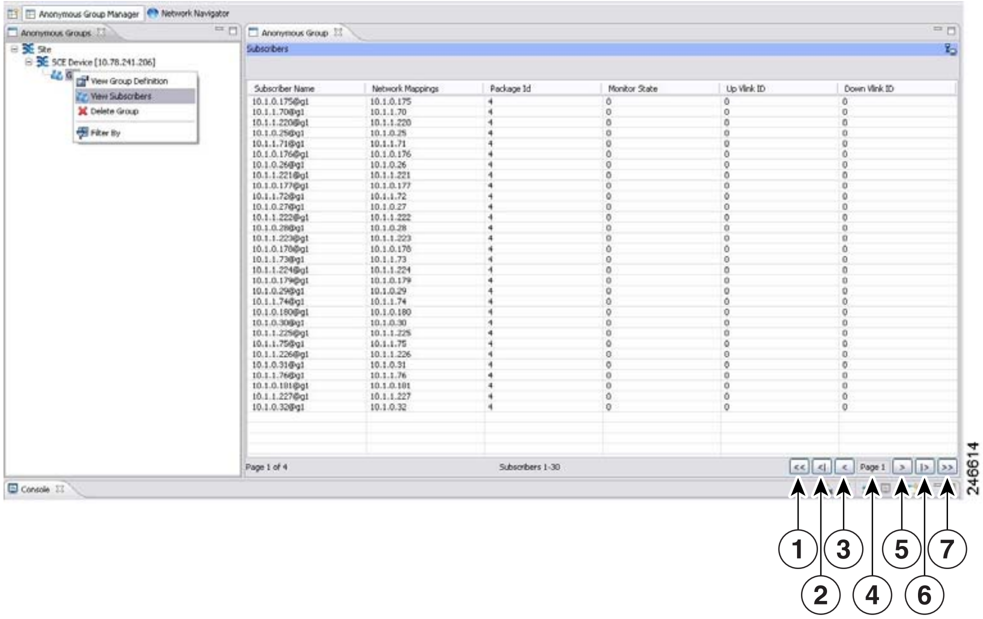
Right-click on the specific subscriber to perform various actions including the following:

- Edit subscriber data.
- View the online status of the subscriber

Finding and Selecting Subscribers

The Anonymous Group Manager GUI tool retrieves subscribers in bulks of 1000 subscribers. Subscriber information is displayed in a standard view. If there are more subscribers than that can be displayed in the standard view, then the information is displayed in pages. You can use the various pagination buttons to navigate between the pages (Figure 12-2).

Figure 12-2 Anonymous Group Manager GUI - Pagination Buttons



Subscriber Name	Network Mappings	Package Id	Monitor State	Up Vlink ID	Down Vlink ID
10.1.0.175@g1	10.1.0.175	4	0	0	0
10.1.1.70@g1	10.1.1.70	4	0	0	0
10.1.1.220@g1	10.1.1.220	4	0	0	0
10.1.0.25@g1	10.1.0.25	4	0	0	0
10.1.1.71@g1	10.1.1.71	4	0	0	0
10.1.0.176@g1	10.1.0.176	4	0	0	0
10.1.0.26@g1	10.1.0.26	4	0	0	0
10.1.1.221@g1	10.1.1.221	4	0	0	0
10.1.0.177@g1	10.1.0.177	4	0	0	0
10.1.1.72@g1	10.1.1.72	4	0	0	0
10.1.0.27@g1	10.1.0.27	4	0	0	0
10.1.1.222@g1	10.1.1.222	4	0	0	0
10.1.0.28@g1	10.1.0.28	4	0	0	0
10.1.1.223@g1	10.1.1.223	4	0	0	0
10.1.0.178@g1	10.1.0.178	4	0	0	0
10.1.1.73@g1	10.1.1.73	4	0	0	0
10.1.1.224@g1	10.1.1.224	4	0	0	0
10.1.0.179@g1	10.1.0.179	4	0	0	0
10.1.0.29@g1	10.1.0.29	4	0	0	0
10.1.1.74@g1	10.1.1.74	4	0	0	0
10.1.0.180@g1	10.1.0.180	4	0	0	0
10.1.0.30@g1	10.1.0.30	4	0	0	0
10.1.1.225@g1	10.1.1.225	4	0	0	0
10.1.1.75@g1	10.1.1.75	4	0	0	0
10.1.1.226@g1	10.1.1.226	4	0	0	0
10.1.0.31@g1	10.1.0.31	4	0	0	0
10.1.1.76@g1	10.1.1.76	4	0	0	0
10.1.0.181@g1	10.1.0.181	4	0	0	0
10.1.1.227@g1	10.1.1.227	4	0	0	0
10.1.0.32@g1	10.1.0.32	4	0	0	0

Page 1 of 4

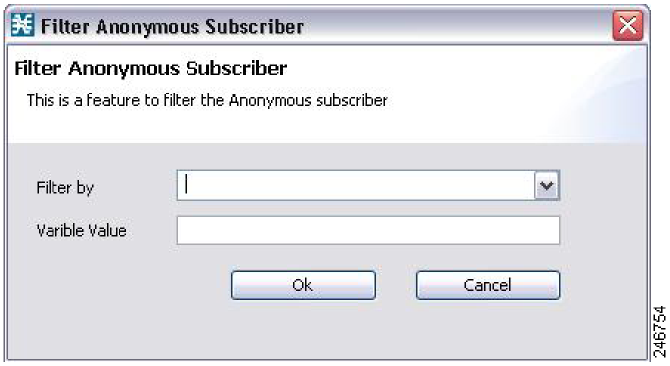
Subscribers 1-30

- 1. Get previous bulk.
- 2. Get first page.
- 3. Get previous page.
- 4. Enter page number.
- 5. Get next page.
- 6. Get last page.
- 7. Get next bulk.

For ease of use, the Anonymous Group Manager GUI tool incorporates two standard features:

- Filter—You can filter the subscriber list based on the packageID, downVlinkId, monitor, and upVlinkId. (See Figure 12-3)
- Multiple Select—Select a range of subscribers or a number of individual subscribers.

Figure 12-3 Filter Anonymous Subscriber



Filter Anonymous Subscriber

Filter Anonymous Subscriber

This is a feature to filter the Anonymous subscriber

Filter by

Varible Value

Selecting Subscribers

You can edit, export, or delete a group of subscribers at one time by selecting subscribers displayed in the subscriber list. The group may be either of the following:

- A range of contiguous subscribers
- A number of noncontiguous subscribers

How to Select a Range of Subscribers

Step 1 Select the first subscriber in the range.

Step 2 Press the **Shift** key while clicking the last subscriber in the range.

All subscribers within the range are selected.

You can combine this function with the search function; search for specific subscribers and then select the entire range.

How to Select a Number of Noncontiguous Subscribers

Step 1 Press the **Ctrl** key while selecting multiple subscribers.

You can combine this function with selecting a range of subscribers; first, select the range of subscribers, and then select additional subscribers.

How to Add an SCE to the Anonymous Group Manager GUI Tool

All SCEs added to Cisco SCA BB Network Navigator appears in the site list of the Anonymous Group Manager GUI Tool.

For details on adding SCEs through Network Navigator, see the How to Add Devices to a Site section.

How to Add a New Anonymous Group in an SCE

Step 1 From the Console main menu, choose **Tools > Anonymous Group Manager**.

The Anonymous Group Manager tool opens (see Figure 12-1).

Step 2 (Optional) If the device is not listed in the Site list, add the device using the Network Navigator.

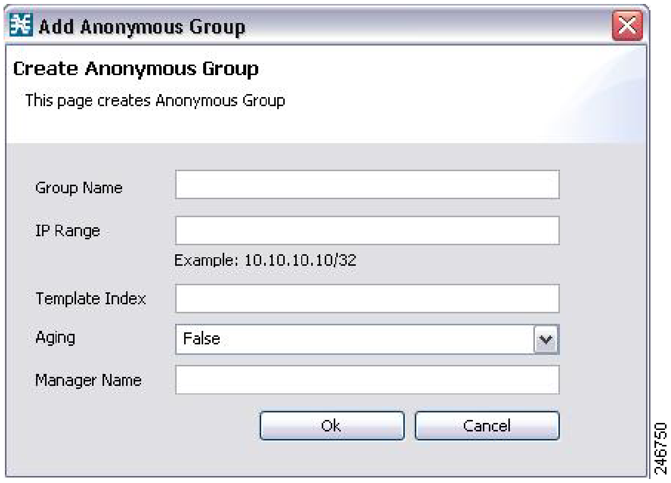
Step 3 Right-click on the SCE, and select **Add a New Group**.

A Password Management window appears with the Device, Device Type, and Service information.

Step 4 Enter the User Name and Password. For details on password management, see the "Password Management" section on page 5-8.

The Add Anonymous Group page appears (Figure 12-4).

Figure 12-4 Add Anonymous Group



Add Anonymous Group

Create Anonymous Group

This page creates Anonymous Group

Group Name

IP Range

Example: 10.10.10.10/32

Template Index

Aging: False

Manager Name

Step 5 Enter the following details:

- Group Name
- IP Range
- Template Index
- Manager Name

Step 6 Select the Aging option from the drop-down list.

Step 7 Click **Ok**.

The new anonymous group is added to the specific SCE.

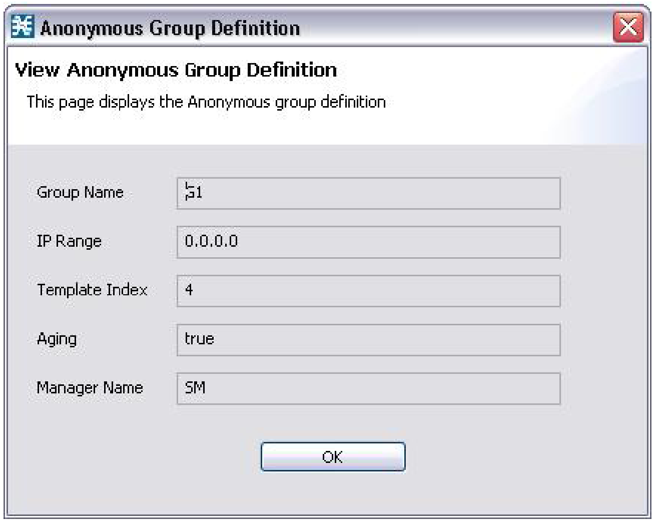
How to View the Configuration of a Specific Anonymous Group

Step 1 From the Console main menu, choose **Tools > Anonymous Group Manager**.

The Anonymous Group Manager tool opens.

Step 2 In the Site list, right-click the Anonymous Group, and select **View Group Definition**. (See Figure 12-5)

Figure 12-5 Anonymous Group Manager Tool



Anonymous Group Definition

View Anonymous Group Definition

This page displays the Anonymous group definition

Group Name: S1

IP Range: 0.0.0.0

Template Index: 4

Aging: true

Manager Name: SM

How to Delete An Anonymous Groups in an SCE

Step 1 From the Console main menu, choose **Tools > Anonymous Group Manager**.

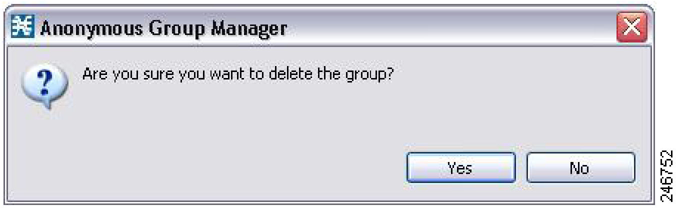
The Anonymous Group Manager tool opens.

Step 2 From the Site list, click on the SCE from which you plan to delete the Anonymous Group.

Step 3 The Anonymous Groups in the SCE appears.

Step 4 Right-click on the Anonymous group to delete, and select **Delete**. A confirmation dialog box appears (Figure 12-6).

Figure 12-6 Confirmation Dialog Box


Anonymous Group Manager

Are you sure you want to delete the group?

Step 5 Click **Yes**.

How to Delete All Anonymous Groups in an SCE

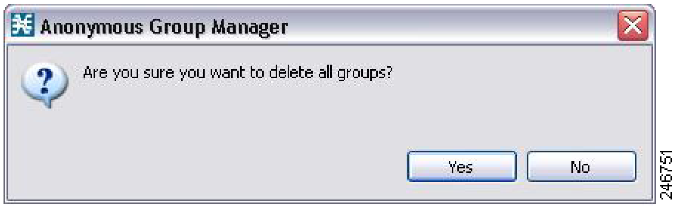
Step 1 From the Console main menu, choose **Tools > Anonymous Group Manager**.

The Anonymous Group Manager tool opens.

Step 2 From the Site list, right-click on the SCE from which you plan to delete the Anonymous Groups and select **Delete Groups**.

A confirmation dialog box appears (Figure 12-7).

Figure 12-7 Confirmation Dialog Box


Anonymous Group Manager

Are you sure you want to delete all groups?

Step 3 Click **Yes**.

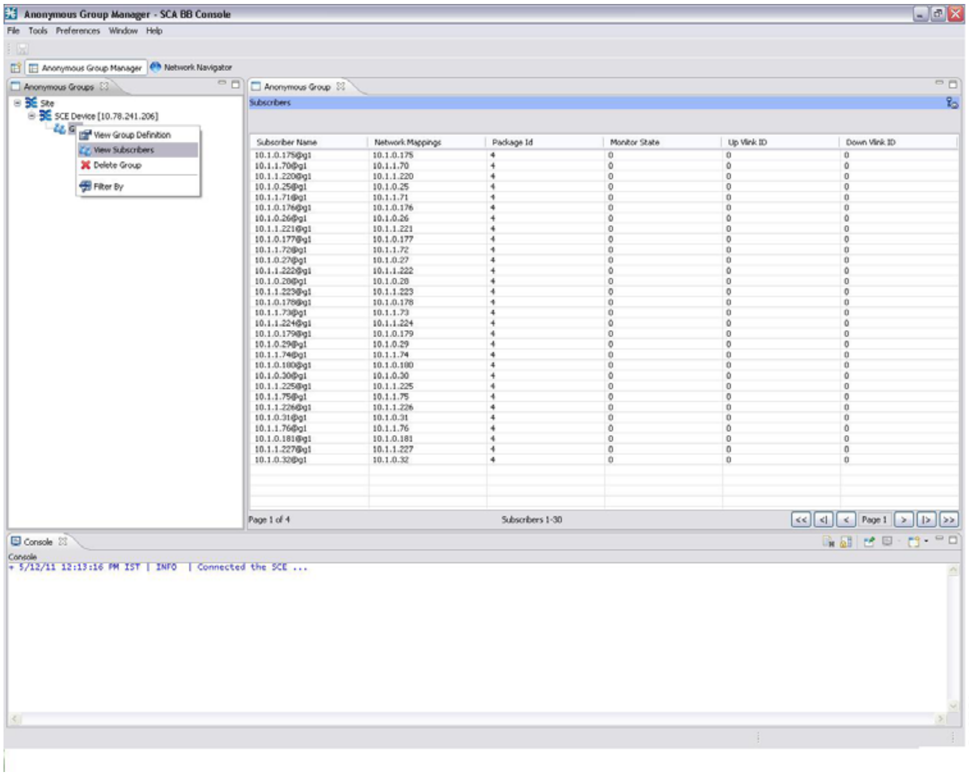
How to View Subscribers in a Specific Anonymous Group

Step 1 From the Console main menu, choose **Tools > Anonymous Group Manager**.

The Anonymous Group Manager tool opens (Figure 12-8).

Step 2 In the Site list, right-click the Anonymous Group, and select **View Subscribers**.

Figure 12-8 Anonymous Group Manager Tool



Subscriber Name	Network Mappings	Package Id	Monitor State	Up Vlink ID	Down Vlink ID
10.1.0.175@g1	10.1.0.175	4	0	0	0
10.1.1.70@g1	10.1.1.70	4	0	0	0
10.1.1.220@g1	10.1.1.220	4	0	0	0
10.1.0.25@g1	10.1.0.25	4	0	0	0
10.1.1.71@g1	10.1.1.71	4	0	0	0
10.1.0.176@g1	10.1.0.176	4	0	0	0
10.1.0.26@g1	10.1.0.26	4	0	0	0
10.1.1.221@g1	10.1.1.221	4	0	0	0
10.1.0.177@g1	10.1.0.177	4	0	0	0
10.1.1.72@g1	10.1.1.72	4	0	0	0
10.1.0.27@g1	10.1.0.27	4	0	0	0
10.1.1.222@g1	10.1.1.222	4	0	0	0
10.1.0.28@g1	10.1.0.28	4	0	0	0
10.1.1.223@g1	10.1.1.223	4	0	0	0
10.1.0.178@g1	10.1.0.178	4	0	0	0
10.1.1.73@g1	10.1.1.73	4	0	0	0
10.1.1.224@g1	10.1.1.224	4	0	0	0
10.1.0.179@g1	10.1.0.179	4	0	0	0
10.1.0.29@g1	10.1.0.29	4	0	0	0
10.1.1.74@g1	10.1.1.74	4	0	0	0
10.1.0.180@g1	10.1.0.180	4	0	0	0
10.1.0.30@g1	10.1.0.30	4	0	0	0
10.1.1.225@g1	10.1.1.225	4	0	0	0
10.1.1.75@g1	10.1.1.75	4	0	0	0
10.1.1.226@g1	10.1.1.226	4	0	0	0
10.1.0.31@g1	10.1.0.31	4	0	0	0
10.1.1.76@g1	10.1.1.76	4	0	0	0
10.1.0.181@g1	10.1.0.181	4	0	0	0
10.1.1.227@g1	10.1.1.227	4	0	0	0
10.1.0.32@g1	10.1.0.32	4	0	0	0

```
+ 5/12/11 12:13:16 PM IST | INFO  | Connected the SCE ...
```

The list of subscribers appears in the Anonymous Group tab near the Console tab.

How to View the Online Status of a Subscriber

Step 1 From the Console main menu, choose **Tools > Anonymous Group Manager**.

The Anonymous Group Manager tool opens.

Step 2 In the Site list, right-click the Anonymous Group, and select **View Subscribers**.

The list of subscribers appears in the Anonymous Group pane.

Step 3 Right-click in the subscriber row, and select **View Online Status**.

The online status appears.

How to Edit the Subscriber Properties

Step 1 From the Console main menu, choose **Tools > Anonymous Group Manager**.

The Anonymous Group Manager tool opens.

Step 2 In the Site list, right-click the Anonymous Group, and select **View Subscribers**.

The list of subscribers appears in the Anonymous Group pane.

Step 3 Right-click in the subscriber row, and select **Edit Subscriber**.

The Edit Subscriber dialog box appears.

Step 4 Modify the required fields from the following:

- Package ID
- Monitor State
- UpVlinkId
- DownVlinkId

Step 5 Click **OK**.

How to Remove Subscribers from an Anonymous Group in an SCE

Step 1 From the Console main menu, choose **Tools > Anonymous Group Manager**.

The Anonymous Group Manager tool opens.

Step 2 In the Site list, click the Anonymous Group, and select **View Subscribers**.

The list of subscribers appears in the Anonymous Group pane.

Step 3 Right-click in the subscriber row, and select **Remove the Subscriber**.

A confirmation dialog box appears.

Step 4 Click **OK**.

Working with Anonymous Groups CSV Files

With Anonymous Group GUI tool, you can:

- Import anonymous groups from a CSV file
- Export anonymous groups to a CSV file
- Export subscribers of a certain anonymous group to CSV file

The format of subscriber CSV files is described in the "CSV File Formats" chapter of *Cisco Service Control Application for Broadband Reference Guide*.

- How to Import Anonymous Groups from a CSV File, page 12-12
- How to Export Anonymous Groups to a CSV File, page 12-15

How to Import Anonymous Groups from a CSV File

You can import subscriber data that was exported to a CSV file using the Anonymous Group Manager GUI tool. This feature supports only one SCE at a time.

Step 1 From the Console main menu, choose **Tools > Anonymous Group Manager**.

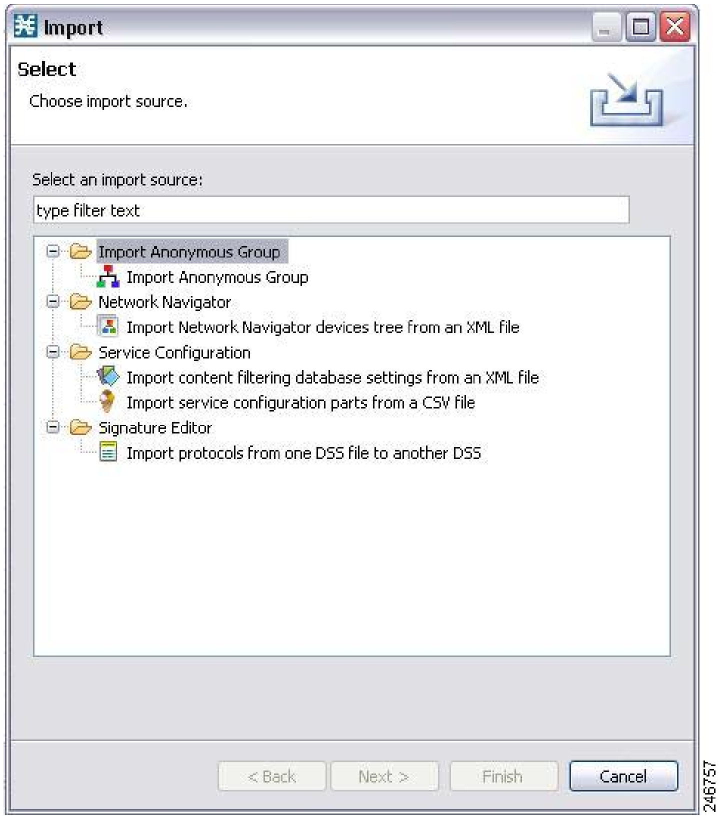
The Anonymous Group Manager tool opens.

Step 2 In the Site list, click the SCE for which you want to import the Anonymous Groups.

Step 3 Select **File > Import**.

The Import dialog box appears (Figure 12-9).

Figure 12-9 Import Dialog Box



Import

Select

Choose import source.

Select an import source:

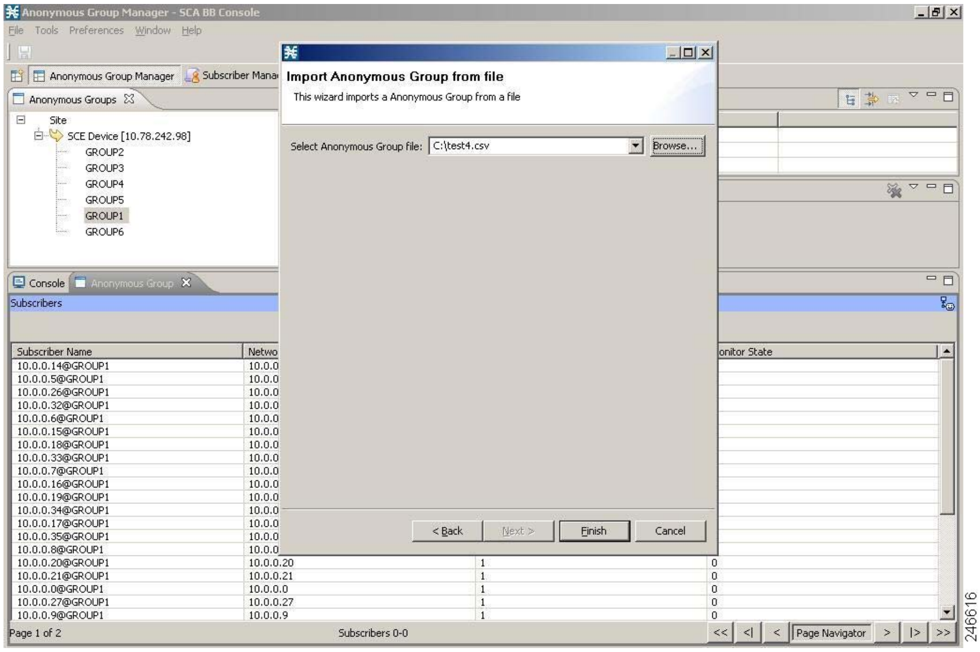
type filter text

- Import Anonymous Group
  - Import Anonymous Group
- Network Navigator
  - Import Network Navigator devices tree from an XML file
- Service Configuration
  - Import content filtering database settings from an XML file
  - Import service configuration parts from a CSV file
- Signature Editor
  - Import protocols from one DSS file to another DSS

Step 4 Click **Next**.

The **Import Anonymous Groups from File** dialog box appears (Figure 12-10).

Figure 12-10 Import Anonymous Groups from File Dialog Box



Import Anonymous Group from file

This wizard imports a Anonymous Group from a file

Select Anonymous Group file: C:\test4.csv

Subscriber Name	Netwo		onitor State
10.0.0.14@GROUP1	10.0.0		
10.0.0.5@GROUP1	10.0.0		
10.0.0.26@GROUP1	10.0.0		
10.0.0.32@GROUP1	10.0.0		
10.0.0.6@GROUP1	10.0.0		
10.0.0.15@GROUP1	10.0.0		
10.0.0.18@GROUP1	10.0.0		
10.0.0.33@GROUP1	10.0.0		
10.0.0.7@GROUP1	10.0.0		
10.0.0.16@GROUP1	10.0.0		
10.0.0.19@GROUP1	10.0.0		
10.0.0.34@GROUP1	10.0.0		
10.0.0.17@GROUP1	10.0.0		
10.0.0.35@GROUP1	10.0.0		
10.0.0.8@GROUP1	10.0.0		
10.0.0.20@GROUP1	10.0.0.20	1	0
10.0.0.21@GROUP1	10.0.0.21	1	0
10.0.0.0@GROUP1	10.0.0.0	1	0
10.0.0.27@GROUP1	10.0.0.27	1	0
10.0.0.9@GROUP1	10.0.0.9	1	0

Step 5 Browse to the file that is to be imported and click **Finish**.

The Import from File dialog box closes.

The selected file is imported into the Anonymous Group Manager GUI tool; the imported subscribers are listed in the subscriber list.

How to Export Anonymous Groups to a CSV File

You can export anonymous group information to a CSV file.

Step 1 From the Console main menu, choose **Tools > Anonymous Group Manager**.

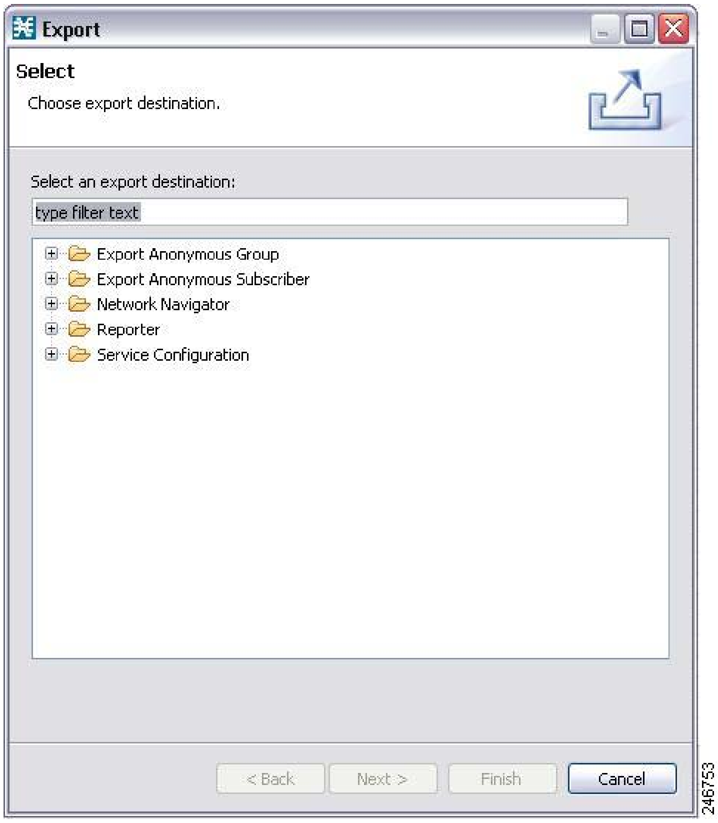
The Anonymous Group Manager tool opens.

Step 2 In the Site list, click the SCE for which you want to export the Anonymous Groups.

Step 3 Select **File > Export**.

The Export dialog box appears (Figure 12-11).

Figure 12-11 Export Dialog Box



Export

Select

Choose export destination.

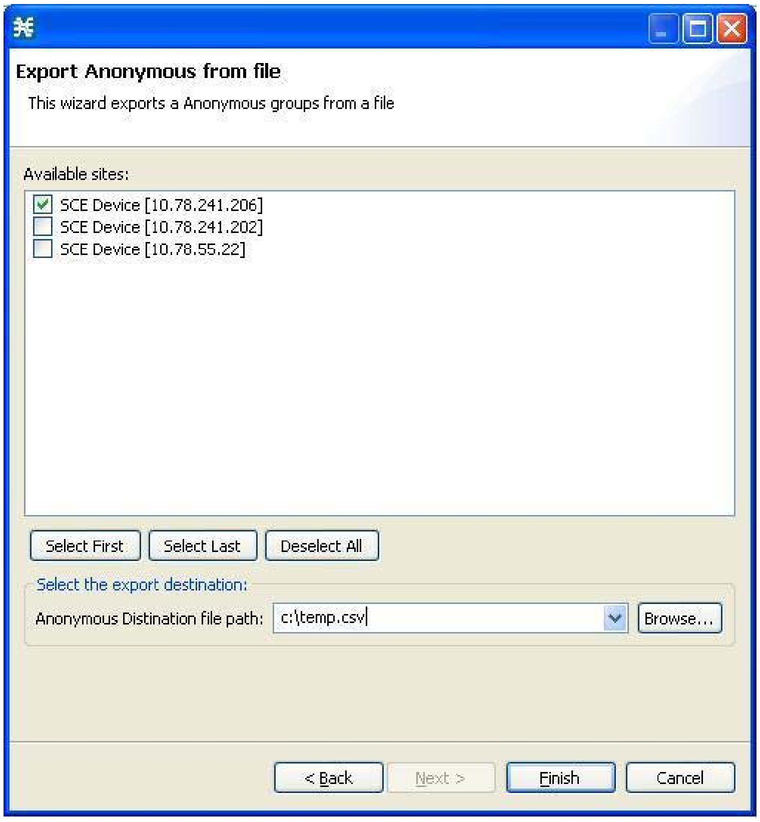
Select an export destination:

type filter text

Step 4 Click **Next**.

The **Export Anonymous Groups from File** dialog box appears (Figure 12-12).

Figure 12-12 Export Anonymous Groups from File Dialog Box



Export Anonymous from file

This wizard exports a Anonymous groups from a file

Available sites:

☑ SCE Device [10.78.241.206]
□ SCE Device [10.78.241.202]
□ SCE Device [10.78.55.22]

Select the export destination:

Anonymous Distination file path: c:\temp.csv

Step 5 Select the SCE Device and the Anonymous Groups to be exported.

Step 6 Select the Export destination and click **Finish**.

The Export from File dialog box closes.

The Anonymous Group Information is exported to the CSV file.

Export Information on Subscribers of an Anonymous Group to CSV File

To export information of all subscribers of an anonymous group to a CSV file, complete these steps:

Step 1 From the Console main menu, choose **Tools > Anonymous Group Manager**.

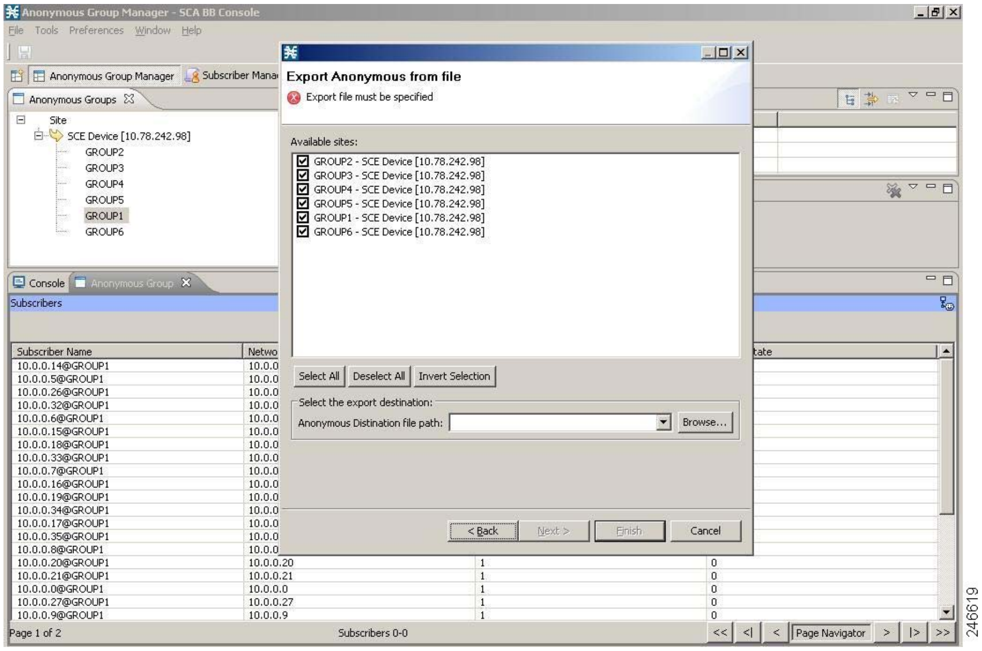
The Anonymous Group Manager tool opens.

Step 2 In the Site list, click the SCE for which you want to export the Anonymous Groups.

Step 3 Select **File > Export**.

Step 4 The Export dialog box appears (Figure 12-13).

Figure 12-13 Export Dialog Box



Export Anonymous from file

Export file must be specified

Available sites:

☑ GROUP2 - SCE Device [10.78.242.98]
☑ GROUP3 - SCE Device [10.78.242.98]
☑ GROUP4 - SCE Device [10.78.242.98]
☑ GROUP5 - SCE Device [10.78.242.98]
☑ GROUP1 - SCE Device [10.78.242.98]
☑ GROUP6 - SCE Device [10.78.242.98]

Select the export destination:

Anonymous Distination file path:

Step 5 Select the subscribers to be exported.

Step 6 Select the Export destination and click **Finish**.

The Export from File dialog box closes.

The selected subscriber information is saved to the CSV file.

CHAPTER 13

Using the Signature Editor

Revised: August 08, 2013, OL-24178-09

Introduction

This module describes the Signature Editor tool and how to use it to create and modify Dynamic Signature Script (DSS) files.

The Signature Editor tool allows you to create and modify DSS files that can add and modify protocols and protocol signatures in the Cisco SCA BB, based on your knowledge of new network protocols that SCA BB is yet to support.

This chapter consists of these sections:

The Signature Editor Console

The Signature Editor writes log and error messages to the Signature Editor Console (in the Console view), when appropriate.

Managing DSS Files

- Installing new signatures to an active service configuration is described in Working with Protocol Packs, page 4-20.
- Working with signatures in the Service Configuration Editor is described in Managing Protocol Signatures, page 7-46.
- Using **servconf,** the Server Configuration Utility, to apply signatures is described in The Cisco SCA BB Service Configuration Utility, page 14-2.

The DSS file components, and the creation and editing of DSS files, are explained in the following sections.

The DSS File Components

The DSS file components are displayed in the Script pane of the Signature Editor, in a tree structure. By selecting the appropriate node of the DSS component tree, you can define the properties associated with the node in the Property pane.

The DSS file components are described in the following sections.

- The DSS File, page 13-2
- DSS Protocol List, page 13-3
- Information About DSS Protocols, page 13-3
- DSS Signatures, page 13-4
- DSS Deep Inspection Clauses, page 13-9
- DSS Deep Inspection Conditions, page 13-10

The DSS File

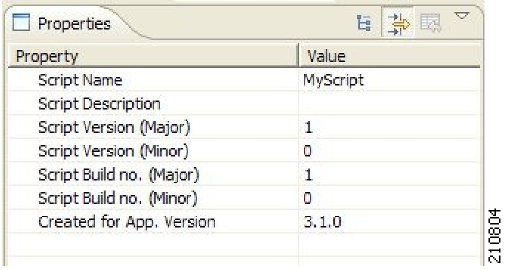
The DSS file name is the root node of the DSS file component tree.

When you select the root node, you can define the following properties for the DSS file:

- Script Name—Enter a meaningful name for this script.
- Script Description—Enter the reason for creating this script and describe its contents.
- Script Version (Major)
- Script Version (Minor)
- Script Build Number (Major)
- Script Build Number (Minor)
- Created for Application Version—Select from a list of predefined values.

Figure 13-1 shows the default values for the DSS file properties.

Figure 13-1 Default Values for DSS File Properties



Properties

Property	Value
Script Name	MyScript
Script Description	
Script Version (Major)	1
Script Version (Minor)	0
Script Build no. (Major)	1
Script Build no. (Minor)	0
Created for App. Version	3.1.0

The DSS file contains a single protocol list.

DSS Protocol List

The protocol list has no properties to define. It contains all the protocols that are being added, modified, or enhanced.

Information About DSS Protocols

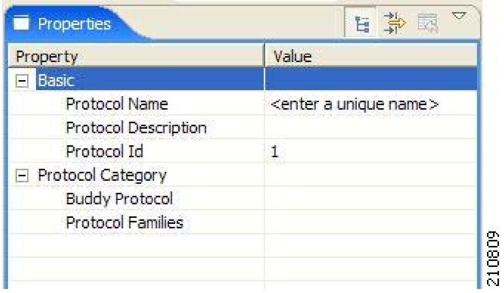
When you select a Protocol node in the DSS file component tree, you can define the following properties of the protocol:

- Basic:
  - Protocol Name—See Setting Protocol Name and ID, page 13-4.
  - Protocol Description
  - Protocol ID—See Setting Protocol Name and ID, page 13-4.
- Protocol Category:
  - Buddy Protocol—See The Buddy Protocol, page 13-4.
  - Protocol Families—Assign the protocol to one or more protocol families:
  - P2P
  - SIP
  - VOIP
  - Worm

    Associating a protocol with a protocol family allows reports about the family to include the new protocol.

Figure 13-2 shows the default values for the protocol properties.

Figure 13-2 Default Values for the Protocol Properties



Property	Value
⊟ Basic	
Protocol Name	<enter a unique name>
Protocol Description	
Protocol Id	1
⊟ Protocol Category	
Buddy Protocol	
Protocol Families	

Protocols contain signatures.

Setting Protocol Name and ID

A DSS can include two types of protocols:

- A protocol new to Cisco SCA BB—The protocol is being defined in the DSS.
- A protocol that Cisco SCA BB already supports—The protocol identification is being enhanced or modified in the DSS.

Selecting a name and ID is different for the two cases:

- For a protocol new to Cisco SCA BB, the name must not match any of the protocol names that Cisco SCA BB already supports. To see a list of supported-protocol names, open the Protocol Settings dialog box in the Service Configuration Editor (see How to View Protocols, page 7-23). Assign the protocol a unique ID in the range from 5000 to 9998.
- For an existing protocol, the protocol name and ID in the DSS must be identical to the protocol name and ID in the service configuration. Locate the name and ID in the Protocol Settings dialog box in the Service Configuration Editor (see How to View Protocols, page 7-23).

The Buddy Protocol

To simplify the configuration of new protocols added by a DSS, the DSS may specify a Buddy Protocol for a new protocol. If, when importing a DSS to a service configuration, the application encounters service elements referring to the Buddy Protocol, it automatically duplicates the set of service elements that use the Buddy Protocol and replaces all references to the Buddy Protocol with references to the new protocol. The association of the new protocol to services matches that of the Buddy Protocol.

DSS Signatures

A protocol may contain as many different signatures as necessary.

Four different types of signatures may be added to a protocol:

- String Match Signatures
- Payload Length Signatures
- HTTP User Agent Signatures
- HTTP x-Header Signatures

Each of the four signature types tests different conditions against the first payload packet of the flows.

These signature types and their conditions are described in the following subsections.

String Match Signatures and Payload Length Signatures can contain deep inspection clauses. A signature whose first payload packet conditions are met accepts a flow if the conditions of any of its deep inspection clauses are also met.

DSS String Match Signature

When you select a String Match Signature node in the DSS file component tree, you can define the following properties of the signature:

- Signature Name—A unique name
- Signature Description
- Signature ID—A value in the range from 0xC010000 to 0xC0100FF (decimal 201392128 to 201392383)
- First Payload Packet Conditions:
  - Fixed Size Byte String—(Display only) Shows the string formed by the next four fields:
  - [0]—Enter the ASCII code for the first byte of the string, or enter "*" to indicate that any value is acceptable.
  - [1]—Enter the ASCII code for the second byte of the string, or enter "*" to indicate that any value is acceptable.
  - [2]—Enter the ASCII code for the third byte of the string, or enter "*" to indicate that any value is acceptable.
  - [3]—Enter the ASCII code for the fourth byte of the string, or enter "*" to indicate that any value is acceptable.
  - String Position—The position of the Fixed Size Byte String in the packet. The position is the location of the first byte of the string, counting from the first byte in the packet. To match the string with the beginning of the packet, this value should be zero. The value must be an integer divisible by four.
  - Packet Direction—The initiating side of the first packet in the flow that has a payload. This field can have one of three values:
  - From Server
  - From Client
  - Don't Care (either side)
  - Port Range—(Display only) The port range formed by the next two fields. The default value is the entire port range from 0 to 65535.
  - From Port—Lower bound of the port range (inclusive)
  - To Port—Upper bound of the port range (inclusive)
  - Check before PL—Toggles between the values **true** and **false**.

    This field indicates whether to test the signature before or after the execution of the Cisco SCA BB built-in PL (Protocol Library) classification. Testing this signature before the execution of the built-in classification means that if the flow matches this signature, the PL classification is skipped. If this field is set to "false", this signature is tested only if the PL classification fails to identify any of its supported protocol signatures.
  - Asymmetric Routing Classification Mode—This field indicates whether to test the signature depending on the state of the asymmetric routing classification mode. It can have one of three values:

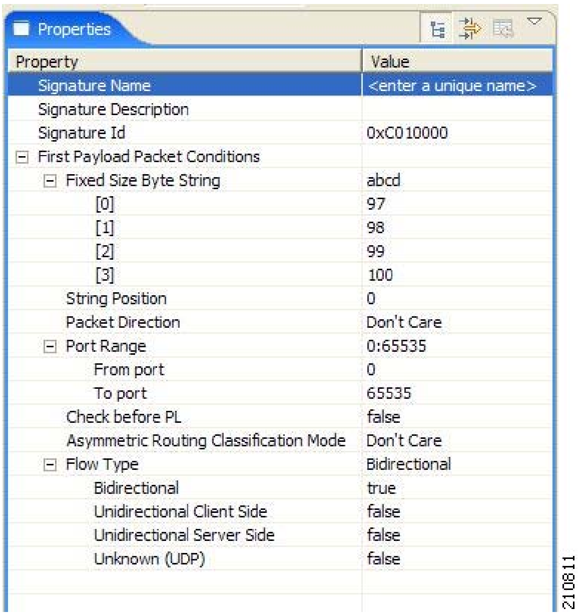
- Don't Care—Signifies that this signature should be tested whether asymmetric routing classification mode is enabled or disabled.
- Disabled
- Enabled
- Flow Type—(Display only) This field shows to which flow types the condition applies (the condition may be applied to multiple types). It is ignored unless asymmetric routing classification mode is enabled.

  The next four fields specify the flow type:
- Bidirectional—Toggles between the values **true** and **false**.
- Unidirectional Client Side—Toggles between the values **true** and **false**. Applies to TCP flows for which only packets from the client side have been detected.
- Unidirectional Server Side—Toggles between the values **true** and **false**. Applies to TCP flows for which only packets from the server side have been detected.
- Unknown (UDP)—Toggles between the values **true** and **false**. Applies to UDP flows for which packets from only one direction have been detected.

Caution Set Check before PL to **true** only if the signature identifies the protocol according to the first payload packet only. If the signature also uses a Deep Inspection Condition that looks into later packets, and the signature does not match the flow, the PL classification is not performed properly.

Figure 13-3 shows the default values for the String Match Signature properties.

Figure 13-3 Default Values for the String Match Signature Properties



Property	Value
Signature Name	<enter a unique name>
Signature Description	
Signature Id	0xC010000
⊟ First Payload Packet Conditions	
⊟ Fixed Size Byte String	abcd
[0]	97
[1]	98
[2]	99
[3]	100
String Position	0
Packet Direction	Don't Care
⊟ Port Range	0:65535
From port	0
To port	65535
Check before PL	false
Asymmetric Routing Classification Mode	Don't Care
⊟ Flow Type	Bidirectional
Bidirectional	true
Unidirectional Client Side	false
Unidirectional Server Side	false
Unknown (UDP)	false

A flow that matches the first payload packet conditions of a String Match Signature is then compared against the deep inspection conditions of the signature (see DSS Deep Inspection Conditions, page 13-10).

DSS Payload Length Signature

When you select a Payload Length Signature node in the DSS file component tree, you can define the following properties of the signature:

- Signature Name—A unique name
- Signature Description
- Signature ID—A value in the range from 0xC010000 to 0xC0100FF (decimal 201392128 to 201392383)
- First Payload Packet Conditions:
  - Packet Direction—The initiating side of the first packet in the flow that has a payload. This field can have one of three values:
  - From Server
  - From Client
  - Don’t Care (either side)
  - Payload Length—The number of bytes in the payload packet.
  - Port Range—(Display only) The port range formed by the next two fields. The default value is the entire port range from 0 to 65535.
  - From Port—Lower bound of the port range (inclusive)
  - To Port—Upper bound of the port range (inclusive)
  - Check before PL—Toggles between the values **true** and **false**.

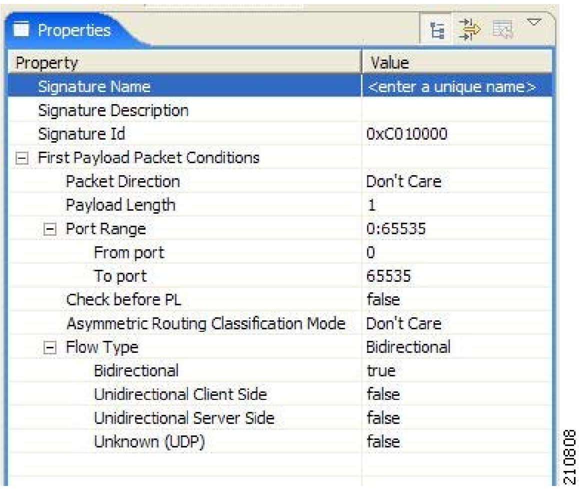
    This field indicates whether to test the signature before or after the execution of the Cisco SCA BB built-in PL (Protocol Library) classification. Testing this signature before the execution of the built-in classification means that if the flow matches this signature, the PL classification is skipped. If this field is set to “false”, this signature is tested only if the PL classification fails to identify any of its supported protocol signatures.
  - Asymmetric Routing Classification Mode—This field indicates whether to test the signature depending on the state of the asymmetric routing classification mode. It can have one of three values:
  - Don't Care—Signifies that this signature should be tested whether asymmetric routing classification mode is enabled or disabled.
  - Disabled
  - Enabled
  - Flow Type—(Display only) This field shows to which flow types the condition applies (the condition may be applied to multiple types). It is ignored unless asymmetric routing classification mode is enabled.

    The next four fields specify the flow type:
  - Bidirectional—Toggles between the values **true** and **false**.
  - Unidirectional Client Side—Toggles between the values **true** and **false**. Applies to TCP flows for which only packets from the client side have been detected.
  - Unidirectional Server Side—Toggles between the values **true** and **false**. Applies to TCP flows for which only packets from the server side have been detected.
  - Unknown (UDP)—Toggles between the values **true** and **false**. Applies to UDP flows for which packets from only one direction have been detected.

Caution Set Check before PL to **true** only if the signature identifies the protocol according to the first payload packet only. If the signature also uses a Deep Inspection Condition that looks into later packets, and the signature does not match the flow, the PL classification is not performed properly.

Figure 13-4 shows the default values for the Payload Length Signature properties.

Figure 13-4 Default Values for the Payload Length Signature Properties



Property	Value
Signature Name	<enter a unique name>
Signature Description	
Signature Id	0xC010000
⊟ First Payload Packet Conditions	
Packet Direction	Don't Care
Payload Length	1
⊟ Port Range	0:65535
From port	0
To port	65535
Check before PL	false
Asymmetric Routing Classification Mode	Don't Care
⊟ Flow Type	Bidirectional
Bidirectional	true
Unidirectional Client Side	false
Unidirectional Server Side	false
Unknown (UDP)	false

A flow that matches the first payload packet conditions of a Payload Length Signature is then compared against the deep inspection conditions of the signature (see DSS Deep Inspection Conditions, page 13-10).

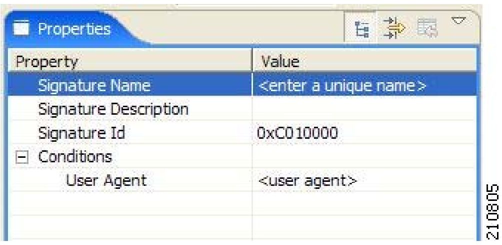
DSS HTTP User Agent Signature

When you select an HTTP User Agent Signature node in the DSS file component tree, you can define the following properties of the signature:

- Signature Name—A unique name
- Signature Description
- Signature ID—A value in the range from 0xC010000 to 0xC0100FF (decimal 201392128 to 201392383)
- Conditions:
  - User Agent—The value of the User Agent field in the HTTP header

Figure 13-5 shows the default values for the HTTP User Agent signature properties.

Figure 13-5 Default Values for the HTTP User Agent Signature Properties



Property	Value
Signature Name	<enter a unique name>
Signature Description	
Signature Id	0xC010000
⊟ Conditions	
User Agent	<user agent>

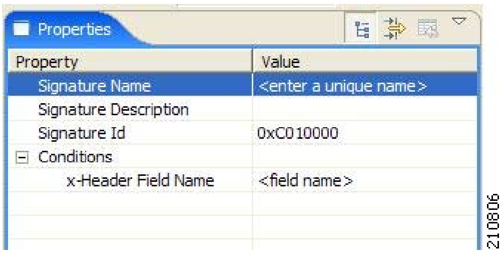
DSS HTTP x-Header Signature

When you select an HTTP x-Header Signature node in the DSS file component tree, you can define the following properties of the signature:

- Signature Name—A unique name
- Signature Description
- Signature ID—A value in the range from 0xC010000 to 0xC0100FF (decimal 201392128 to 201392383)
- Conditions:
  - x-Header Field Name—A name of a field in the x-Header of the HTTP header

Figure 13-6 shows the default values for the DSS file properties.

Figure 13-6 Default Values for the DSS File Properties



Property	Value
Signature Name	<enter a unique name>
Signature Description	
Signature Id	0xC010000
⊟ Conditions	
x-Header Field Name	<field name>

DSS Deep Inspection Clauses

A deep inspection clause is a conjunctive clause of deep inspection conditions—a signature accepts a flow *only* if all conditions in a clause are met.

Note If a signature has multiple deep inspection clauses, the clauses (and the deep inspection conditions making up each clause) are tested in an order based on the value of the Packet Number property of the deep inspection conditions.

After the first payload packet is accepted by the first payload packet conditions, the clause containing the condition with the lowest Packet Number is tested. The other conditions in this clause are checked in ascending Packet Number order. Thus, the Packet Number of any condition in a clause cannot be less than the largest Packet Number in the clause it succeeds.

DSS Deep Inspection Conditions

A deep inspection condition is a set of conditions that are checked against flows that pass the first payload packet conditions screening of String Match Signatures or Payload Length Signatures.

When you select a Deep Inspection Condition node in the DSS file component tree, you can define the following properties of the deep inspection condition:

- Packet Direction—The initiating side of the first packet in the flow that has a payload. This field can have one of three values:
  - From Server
  - From Client
  - Don’t Care (either side)
- Packet Number—The number of the packet in the flow. The payload packets are numbered from zero; packets are counted in both directions.
- Payload Length—The length of the packet in bytes. Enter zero to indicate that any value is acceptable.
- Printable Characters—Test if the inspected packet contains only printable characters. This field can have one of three values:
  - Printable Characters Only
  - At Least One Non-Printable
  - Don’t Care
- Substring Search—Match a search string with a specific location in the packet. Leave the Search String fields empty if this condition is irrelevant.
  - Position Offset—The position from which to start searching for the search string in the packet. The offset is relative to the location specified in the Start Search From field.
  - Start Search From—This field can have one of two values:
  - Packet beginning
  - Last match

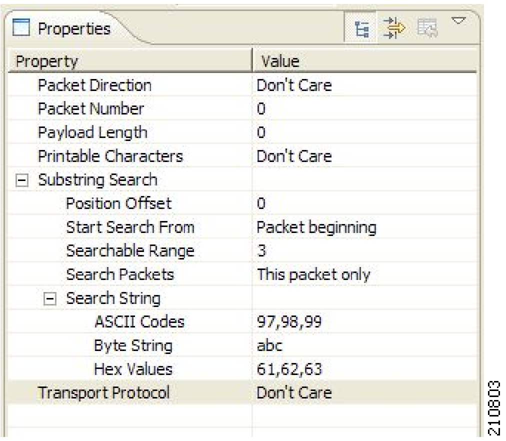
    Last match means that the search for this search string starts where the last search match ended. The last match may be from a previous substring search or from the last string-based first payload packet condition.
  - Searchable Range—Search in this number of bytes for the search string.
  - Search Packets—This field can have one of two values:
  - This packet only
  - Multiple packets

    Multiple Packets means that the search may span across packets, as long as the overall number of bytes is less than the number specified in the Searchable Range field.
  - Search String—Enter the search string in one of the following three fields (the other two fields are updated automatically):
  - ASCII Codes—Enter the ASCII codes for the characters of the search string. Separate each code by a comma.
  - Byte String—Enter the actual search string.
  - Hex Values—Enter the hexadecimal values of the ASCII codes for the characters of the search string. Separate each code by a comma.

- Transport Protocol—This field can have one of three values:
  - TCP
  - UDP
  - Don't Care (either TCP or UDP)

Figure 13-7 shows the default values for the deep inspection condition properties.

Figure 13-7 Default Values for the Deep Inspection Condition Properties



Property	Value
Packet Direction	Don't Care
Packet Number	0
Payload Length	0
Printable Characters	Don't Care
⊟ Substring Search	
Position Offset	0
Start Search From	Packet beginning
Searchable Range	3
Search Packets	This packet only
⊟ Search String	
ASCII Codes	97,98,99
Byte String	abc
Hex Values	61,62,63
Transport Protocol	Don't Care

The structure of deep inspection conditions is the same for String Match Signatures and Payload Length Signatures.

How to Create DSS Files

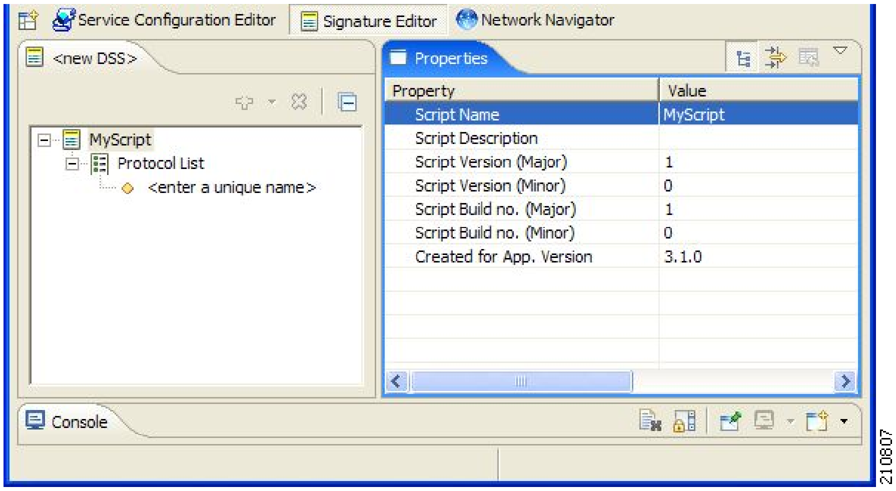
If you have a DSS file open in the Signature Editor, save it before you create a new DSS file. All unsaved changes are lost.

Step 1 From the toolbar, click the **Create a New DSS File** ( ) icon.

A DSS component tree containing a DSS File node, a Protocol List node, and a Protocol node, is displayed in the Script view.

The default properties of the new DSS file are displayed in the Properties view (Figure 13-8).

Figure 13-8 Properties Tab



Property	Value
Script Name	MyScript
Script Description	
Script Version (Major)	1
Script Version (Minor)	0
Script Build no. (Major)	1
Script Build no. (Minor)	0
Created for App. Version	3.1.0

Step 2 Edit the DSS file properties.

For an explanation of the properties, see The DSS File, page 13-2.

Step 3 Click the Protocol node.

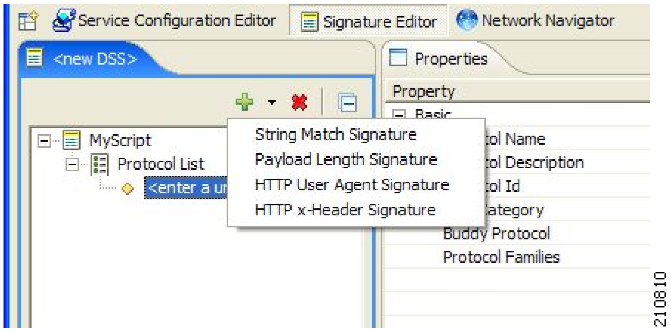
The protocol properties appear in the Properties view (Figure 13-9).

Step 4 Edit the protocol properties.

For an explanation of the properties, see Information About DSS Protocols, page 13-3.

Step 5 Click the drop-down arrow next to the **Add** (✚) icon.

Figure 13-9 Protocol Properties

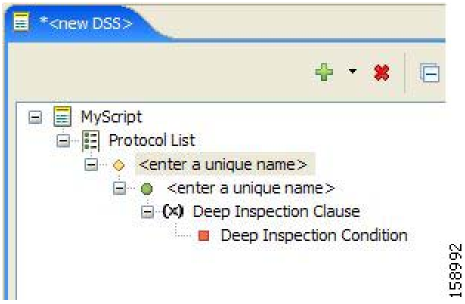


Step 6 From the drop-down menu that appears, select a signature type.

A Signature node is added under the Protocol node.

If you selected a String Match Signature or a Payload Length Signature, a Deep Inspection Clause node and a Deep Inspection Condition node are also added (Figure 13-10).

Figure 13-10 Protocol List Information



Step 7 Click the Signature node.

The signature properties appear in the Properties view.

Step 8 Edit the signature properties.

For an explanation of the properties, see DSS Signatures, page 13-4

Step 9 If you selected a String Match Signature or a Payload Length Signature, click the Deep Inspection Condition node to edit the deep inspection condition properties.

The deep inspection condition properties appear in the Properties view.

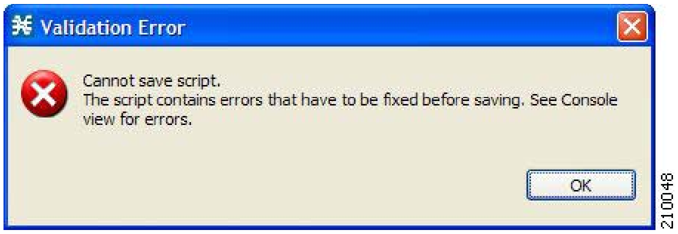
For an explanation of the properties, see DSS Deep Inspection Conditions, page 13-10.

Step 10 Add additional deep inspection conditions, deep inspection clauses, signatures, and protocols as needed.

Step 11 From the toolbar, click the **Save** (💾) icon.

- If there are duplicate protocol names or protocol IDs, a Validation Error message appears (Figure 13-11).

Figure 13-11 Validation Error



Validation Error

Cannot save script.
The script contains errors that have to be fixed before saving. See Console view for errors.

Click **OK,** remove the duplication, and then click the **Save** (💾) icon again.

A Save As dialog box appears.

Step 12 Browse to the folder where you want to save the new DSS file.

Step 13 In the File name field, enter an appropriate name for the DSS file.

Step 14 Click **Save**.

The Save As dialog box closes.

The DSS file is saved.

How to Edit DSS Files

You can edit an existing DSS file, and add new protocols, or modify or delete existing protocols.

Caution If you have a DSS file open in the Signature Editor, save it before you open a different DSS file. All unsaved changes are lost.

Step 1 From the toolbar, click the **Open a DSS File** ( ) icon.

An Open dialog box appears.

Step 2 Browse to the DSS file that you want to edit.

Step 3 Click **Open**.

The Open dialog box closes.

The DSS Component tree of the selected file is displayed in the Script view.

The DSS File node is selected, and the properties of the DSS file are displayed in the Properties view.

Step 4 Add, edit, or delete DSS file components.

See the subsections of The DSS File Components, page 13-2 for an explanation of the properties of the different components.

Step 5 Save the modified DSS file.

- To overwrite the current DSS file with the changes you have made:
  - From the toolbar, click the **Save** ( ) icon.

    The changes to the DSS file are saved.
- To save the modified DSS file with a new name:

1. Choose **File > Save As**.

   A Save As dialog box appears.
2. Browse to the folder where you want to save the new DSS file.
3. In the File name field, enter an appropriate name for the DSS file.
4. Click **Save**.

   The Save As dialog box closes.

   The modified DSS file is saved with the new name.

How to Import DSS Files

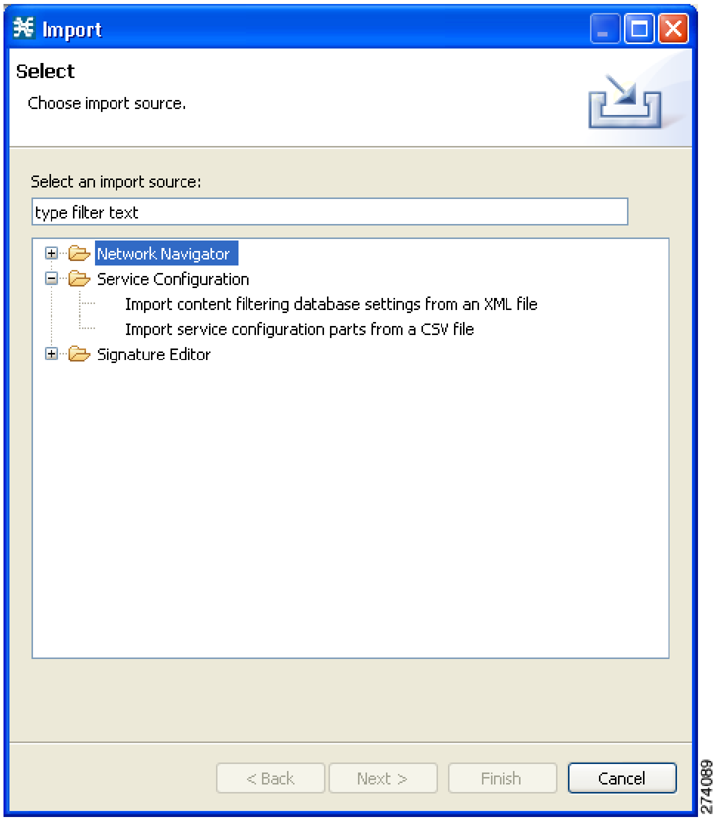
You can import DSS files into the file you are currently editing.

Note Importing signatures may create duplication of protocol names or protocol IDs.

Step 1 From the Console main menu, choose **File > Import**.

The Import dialog box appears (Figure 13-12).

Figure 13-12 Import

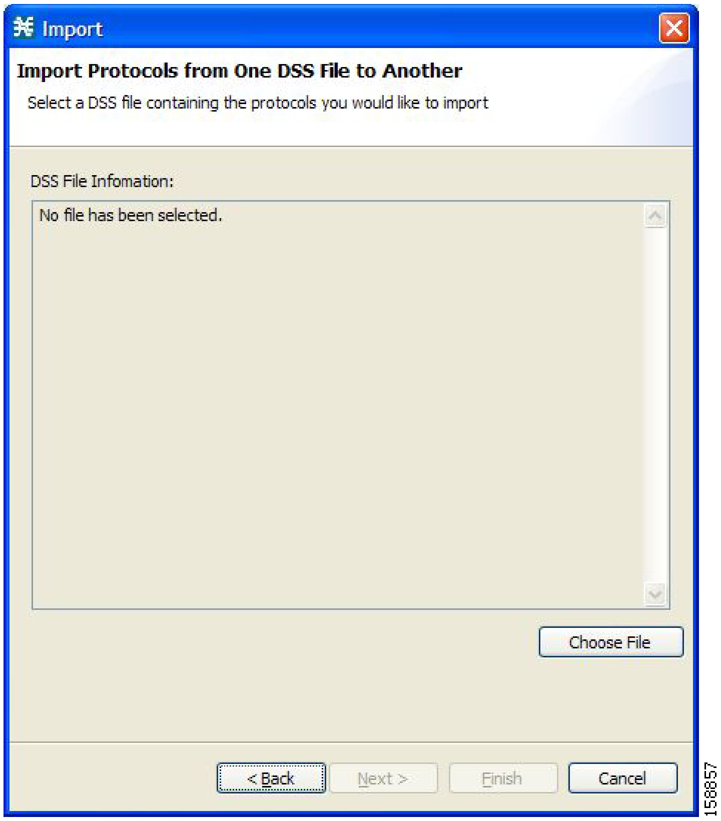


Step 2 From the import source list, select **Import protocols from one DSS file to another DSS**.

Step 3 Click **Next**.

The second screen of the Import dialog box opens (Figure 13-13).

Figure 13-13 Import Protocols from One DSS File to Another



Import

Import Protocols from One DSS File to Another

Select a DSS file containing the protocols you would like to import

DSS File Infomation:

No file has been selected.

Step 4 Click **Choose File**.

An Open dialog box appears.

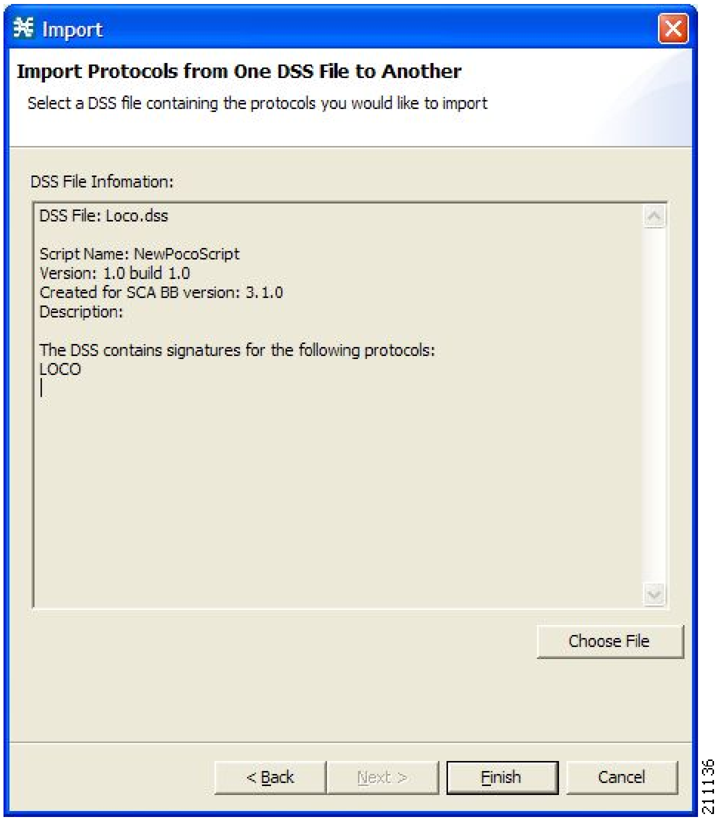
Step 5 Browse to the DSS file to import.

Step 6 Click **Open**.

The Open dialog box closes.

Information about the DSS file that you have chosen is displayed in the DSS File Information area (Figure 13-14).

Figure 13-14 Import Protocols from One DSS File to Another



Import Protocols from One DSS File to Another

Select a DSS file containing the protocols you would like to import

DSS File Infomation:

```
DSS File: Loco.dss

Script Name: NewPocoScript
Version: 1.0 build 1.0
Created for SCA BB version: 3.1.0
Description:

The DSS contains signatures for the following protocols:
LOCO
```

Step 7 Click **Finish**.

The Import dialog box closes.

The content of the selected DSS file is imported into the Signature Editor.

CHAPTER 14

Additional Management Tools and Interfaces

Revised: August 08, 2013, OL-24178-09

Introduction

This chapter contains the following information:

The Cisco SCA BB Service Configuration Utility

The Cisco SCA BB Service Configuration Utility (**servconf**) is a command-line utility (CLU) for applying and retrieving service configurations. Use it in a scripting environment to automate service configuration tasks on multiple Service Control Engine (SCE) platforms.

The Service Configuration Utility can run in Windows, Solaris, and Linux environments.

servconf Syntax

The command-line syntax of **servconf** is:

```
servconf <operation> [<option>] [<option>]...
```

Table 14-1 lists the **servconf operations**.

Table 14-2, Table 14-3, Table 14-4, Table 14-5, and Table 14-6 list the **servconf** options.

Table 14-1 servconf Operations

Operation	Abbreviation	Description
--apply	**-a**	Copies the specified service configuration file to the specified SCE platforms and activates it
--retrieve	**-r**	Retrieves the current service configuration
--update-dc	**-u**	Updates a Cisco Service Control Management Suite (SCMS) Collection Manager (CM) with service configuration values
--status	—	Shows the service configuration status on the SCE platform
--update-signature	—	Updates the SCE platform with a new protocol pack
--update-signature-pqi	—	Updates the SCE platform with a new SPQI protocol pack
--signature-info	**-i**	Shows information about the Dynamic Signature Script (DSS) file
--help	—	Displays help, then exits
--version	—	Displays the program version number, then exits

Table 14-2 servconf File Options

File Option	Abbreviation	Description
--file=*filename*	-f	Specifies a service configuration file or DSS file
--backup-directory=*directory*	-b	Specifies the directory to which to save the retrieved PQB file before applying a new protocol pack

Table 14-3 servconf Connection Options

File Option	Abbreviation	Description
--se=*address*	**-S**	Specifies the IP address of the destination SCE platform. To specify multiple SCE platforms, list the IP addresses separated by semicolons (see Example 1 in the following section). When using a semicolon in a Unix command line, the command-line argument must be enclosed in quotation marks.
--dc=*address*	**-D**	Specifies the IP address of the destination SCMS Collection Manager platform (required only for the **--update-dc** operation).
--password=*password*	**-P**	Specifies the password for connecting to the SCE platform.
--username=*username*	**-U**	Specifies the username for connecting to the SCE platform. If this option is not specified, the following default values are used: • SCE—admin • CM—pcube • SM—pcube

Table 14-4 servconf Reference SCE Option

File Option	Description
--refer-se=*address*	Specifies the IP address of the SCE platform to which the service configuration values refer (required only for **--update-dc** operation)

Table 14-5 servconf Apply Options

File Option	Description
--no-dc	(Optional) Specifies that the --apply operation should not automatically update the SCMS Collection Manager with service configuration values.
--no-default-signature	Applies the service configuration without adding the default DSS to it.
--force-default-signature	Forces the replacement of the DSS in the retrieved PQB with the default DSS, even if the signatures of the existing DSS are mapped to services. Without this flag, trying to update a PQB containing a DSS fails.

Table 14-6 servconf Update Signature Option

File Option	Description
--force-signature	Forces replacement of the DSS in the retrieved PQB, even if the signatures of the existing DSS are mapped to services. Without this flag, trying to update a PQB containing a DSS fails.

servconf Examples

Example 1

To copy the service configuration file config.pqb from the local machine to two SCE platforms (at 63.111.106.7 and 63.111.106.12), and activate this configuration:

```
servconf ″--se=63.111.106.7;63.111.106.12″ --username Alice --password ***** --apply
--file config.pqb
```

Example 2

To retrieve the current service configuration from the SCE platform at 63.111.106.7, and save it in file my_files\config.pqb on the local machine:

```
servconf -S 63.111.106.7 -U Bob -P ***** --retrieve --file my_files\config.pqb
```

Example 3

To update the SCMS Collection Manager at 63.121.116.17 with service configuration values from file config.pqb, as if they were applied to the SCE platform at 63.111.106.7 (but without actually applying them to the SCE platform):

```
servconf -D 63.121.116.17 -U Alice -P ***** --update-dc
--refer-se 63.111.106.7 --file config.pqb
```

Example 4

To distribute the protocol pack file new_signature.spqi to the SCE platforms at 10.56.216.33 and 10.56.216.36:

```
servconf --update-signature-pqi -f new_signature.spqi
-S ″10.56.216.33;10.56.216.36″ -U user123 -P *****
```

The Cisco SCA BB Real-Time Monitoring Configuration Utility

SNMP-based monitoring tools, such as MRTG, allow network administrators to monitor the activity and health of network devices in real time. Cisco SCA BB includes an SNMP-based real-time monitoring solution, which is implemented using MRTG and a graphics utility (RRD Tool).

The Cisco SCA BB Real-Time Monitoring Configuration Utility (**rtmcmd)** is a command-line utility (CLU) for automating the production of the files required by the MRTG tool.

For installation instructions, see How to Install the Cisco SCA BB Configuration Utilities, page 4-7. For more information about installing and using the Cisco SCA BB SNMP-based real-time monitoring solution, see the *Cisco SCA BB SNMP Real Time Monitoring User Guide.*

- rtmcmd Syntax, page 14-5
- rtmcmd Examples, page 14-6
- The rtmcmd User Configuration File, page 14-6
- An rtmcmd User Configuration File Example, page 14-8

rtmcmd Syntax

The command-line syntax of the Cisco SCA BB Real-Time Monitoring Configuration Utility is:

```
rtmcmd --sce <SCE (SNMP) addresses> {--file <PQB filename> | (--pqb-sce
<SCE (PQB) addresses> --username <username> --password <password>)} --source-dir <dir>
--dest-dir <dir> --config-file <file>
```

Table 14-7 lists the **rtmcmd** options.

Table 14-7 rtmcmd Options

Option	Abbreviation	Description
--sce *address*	**-S**	Specifies the IP address or hostname of the SCE platform from which SNMP data is collected. To specify multiple SCE platforms, list the IP addresses separated by semicolons. When using a semicolon in a Unix command line, the command-line argument must be enclosed in quotation marks.
--file *filename*	**-f**	(Required if --pqb-sce is not included) Specifies the service configuration file to use when generating the configuration and report files. If this option is specified, the **--username/-U** and **--password/-P** options are prohibited.
--pqb-sce *address*	**-q**	(Required if --file is not included) Specifies the hostname or IP address of the SCE platform from which the service configuration should be retrieved. This option requires the **--username/-U** and **--password/-P** options.
--username *<username>*	**-U**	(Required if **--pqb-sce** is included) Specifies the username for connecting to the SCE platform.
--password *<password>*	**-P**	(Required if **--username** is included) Specifies the password for connecting to the SCE platform.

Table 14-7 rtmcmd Options (continued)

Option	Abbreviation	Description
--source-dir *<dir>*	**-s**	Specifies the location of the report template files.
--dest-dir *<dir>*	**-d**	Specifies the directory where the processed report templates should be stored.
--config-file *<file>*	**-c**	Specifies the configuration file. (See The rtmcmd User Configuration File, page 14-6).

You can invoke additional operations (see Table 14-8) to display information about the **rtmcmd** using the following syntax:

```
rtmcmd <operation>
```

Table 14-8 rtmcmd Operations

Operation	Description
--version	Displays the program version number, then exits
--help	Displays help, then exits

rtmcmd Examples

Example 1

To use the service configuration file servicecfg.pqb to create configuration and report files for the collecting and reporting of SNMP information from two SCE platforms (at 63.111.106.7 and 63.111.106.12):

```
rtmcmd --sce="63.111.106.7;63.111.106.12" --file=servicecfg.pqb
--source-dir=/rtm-templates --dest-dir=/rtm-output -c./rtmcmd.cfg
```

Example 2

To use the service configuration loaded on the SCE platform at 63.111.106.7 to create configuration and report files for the collecting and reporting of SNMP information from two SCE platforms (at 63.111.106.7 and 63.111.106.12):

```
rtmcmd -S "63.111.106.7;63.111.106.12" -U user123 -P **** --pqb-sce=63.111.106.7
--source-dir=/rtm-templates --dest-dir=/rtm-output -c./rtmcmd.cfg
```

The rtmcmd User Configuration File

The user configuration file contains user-specific information required by the **rtmcmd** utility. The Cisco SCA BB utilities distribution package contains a sample configuration file, named rtmcmd.cfg. You should edit this file according to the details of your setup.

Table 14-9 lists the configuration parameters that should be present in the user configuration file:

Table 14-9 rtmcmd User Configuration File Parameters

Parameter Description	Description	Default Value	Required/ Optional
rrdtool_bin_dir	The absolute path to the directory where RRDTool and RRDCGI binary files are installed.	—	Required
rtm_dir	The absolute path to the directory where RRD archives and CGI files are stored. This is under the web server web directory.	—	Required
mrtg_bin_dir	The absolute path to the directory where MRTG binary files are installed. This location is used to create MRTG invocation commands in the crontab sample file.	—	Required
snmpCommunityString	The SNMP community string to use when accessing the SCE platforms.	Public	Required

The configuration text file is a listing of key-value pairs, where the key is one of the parameters listed above, in the following format:

- Each key-value pair is on a separate line.
- A key-value pair may be extended across several adjacent lines by putting a back slash character, "\", at the end of each line.
- To use an actual back slash in the value (as in directory names on Windows), the back slash should be escaped with a second back slash, like this: "\\" (or use a slash "/").
- To comment a line, add "#" or "!" at the beginning of the line.

For example:

```
# This is a comment line.
# Directory names should use escape backslashes:
rtm_dir=D:\\PROGRA~1\\APACHE~1\\Apache2.2\\htdocs
```

An rtmcmd User Configuration File Example

```
#The absolute path to the RRD tool's execution files folder
#Use '\\' or '/' as path separator
rrdtool_bin_dir=C:/rrdtool-1.2.15/rrdtool/Release

#The absolute path where RTM files will be placed.
#This path will be used by MRTG to create and update the RRD files
#Note: path must not contain white spaces!
rtm_dir=C:/PROGRA~1/APACHE~1/Apache2.2/htdocs

#The absolute path to the MRTG bin folder.
#This path will be used to create file crontab.txt
mrtg_bin_dir=C:/mrtg-2.14.5/bin

#The SCE's community string
snmpCommunityString=public
```

The Cisco SCA BB Signature Configuration Utility

The Cisco SCA BB Signature Configuration Utility (**sigconf**) is a command-line utility for installing and managing the default DSS.

The Signature Configuration Utility can run in Windows, Solaris, and Linux environments.

For installation instructions, see How to Install the Cisco SCA BB Configuration Utilities, page 4-7.

sigconf Syntax

The command-line syntax of the Cisco SCA BB Signature Configuration Utility is:

```
sigconf <operation> [--file <filename>]
```

Table 14-10 lists the **sigconf** operations.

Table 14-11 lists the **sigconf** option.

Table 14-10 sigconf Operations

Operation	Abbreviation	Description
--set-default-dynamic-signature	**-d**	Installs the default DSS on this workstation
--remove-default-dynamic-signature	—	Uninstalls the default DSS from this workstation
--get-default-dynamic-signature	—	Fetches the default DSS installed on this workstation
--help	—	Displays help, then exits

Table 14-11 sigconf File Option

File Option	Abbreviation	Description
--file *filename*	**-f**	Specifies a DSS file

sigconf Examples

Example 1

To install the file new_signature.dss as the default DSS:

```
sigconf --set-default-dynamic-signature --file new_signature.dss
```

Example 2

To retrieve the installed default DSS file, and save it as default_backup.dss:

```
sigconf --get-default-dynamic-signature --file default_backup.dss
```

Overview of SNMP, MIB, and Traps

Cisco provides complete network FCAPS (Fault, Configuration, Accounting, Performance, Security) management.

Two interfaces are provided for network management:

- Command-line interface (CLI)—Accessible through the console port on the front panel of the SCE platform or through a Telnet connection to the SCE platform, the CLI is used for configuration and security functions.
- SNMP (Simple Network Management Protocol)—Provides fault management (via SNMP traps) and performance monitoring functionality.

SNMP

SNMP is a set of protocols for managing complex networks. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

The SCE platform operating system includes an SNMP agent. Configuring the SNMP agent parameters and enabling the SNMP interface is described in either the “Configuring the Management Interface and Security” chapter of *Cisco SCE8000 10GBE Software Configuration Guide* or the “Configuring the Management Interface and Security” chapter of *Cisco SCE8000 GBE Software Configuration Guide.*

MIB

Management Information Bases (MIBs) are databases of objects that can be monitored by a network management system. SNMP uses standardized MIB formats that allow standard SNMP tools to monitor any device defined by a MIB.

The SCE platform supports the following MIBs:

- MIB-II—Defined in RFC 1213*, (Management Information Base for Network Management of TCP/IP-based Internets)*
- Cisco Service Control Enterprise MIB—Described by a number of MIB files

The Cisco proprietary MIB allows external management systems to retrieve general information about the SCE platform operating status and resource utilization, extract real-time measurements of bandwidth utilization and network statistics, and receive notifications of critical events and alarms.

The part of the Cisco proprietary MIB that provides configuration and runtime status for Cisco SCA BB is documented in the “SCA BB Proprietary MIB Reference” chapter of *Cisco Service Control Application for Broadband Reference Guide*. Other parts of the Cisco proprietary MIB are documented in either the “Proprietary MIB Reference” appendix of the *Cisco SCE8000 10GBE Software Configuration Guide* or the “Proprietary MIB Reference” appendix of the *Cisco SCE8000 GBE Software Configuration Guide*. These books also explain the order in which the MIB must be loaded.

Traps

Traps are unsolicited messages generated by the SNMP agent that resides inside the SCE platform. Traps are generated when an event occurs. When the Network Management System receives the trap message, it can take suitable actions, such as logging the occurrence or ignoring the signal.

The SCE platform supports two general categories of traps:

- Standard SNMP traps—As defined in RFC 1157 and using the conventions defined in RFC 1215
- Proprietary Cisco Service Control Enterprise traps—As defined in the Cisco proprietary MIB

  For a description of the SNMP traps and an explanation of how to configure the SNMP trap managers, see either the "Configuring and Managing the SNMP Interface" section in the "Configuring the Management Interface and Security" chapter of *Cisco SCE8000 10GBE Software Configuration Guide* or the "Configuring and Managing the SNMP Interface" section in the "Configuring the Management Interface and Security" chapter of *Cisco SCE8000 10GBE Software Configuration Guide*.

Installing PQI Files from the Command Line

- How to Install a Cisco SCA BB PQI File on an SCE Platform, page 14-12
- How to Enter Line Interface Configuration Mode, page 14-12

How to Install a Cisco SCA BB PQI File on an SCE Platform

You can install a Cisco SCA BB PQI file on an SCE platform using the SCE platform Command-Line Interface (CLI).

Step 1 Make sure that the PQI file is available.

Do one of the following:

- Locate the PQI file on the SCE platform.
- Upload the appropriate PQI file to the SCE via FTP.

Step 2 Enter line interface configuration mode. (See How to Enter Line Interface Configuration Mode, page 14-12.)

Step 3 Type **pqi install file engXXXXX.pqi**.

Step 4 Monitor the installation progress until it is completed.

What to Do Next

After you install the Console, you can use the Network Navigator tool to install PQI files. See How to Install PQI Files on SCE Devices, page 5-25.

How to Enter Line Interface Configuration Mode

Step 1 At the SCE platform CLI prompt `(SCE#)`, type **configure**.

Step 2 Press **Enter**.

The `SCE(config)#` prompt appears.

Step 3 Type **interface LineCard 0**.

Step 4 Press **Enter**.

The `SCE(config if)#` prompt appears.

Managing Subscribers via Other System Components

Other components of the Cisco Service Control solution offer alternatives for subscriber management (as opposed to using the Subscriber Manager GUI tool in the Console):

- The Cisco Service Control Management Suite (SCMS) Subscriber Manager (SM) has options that are not available from the Console.
- The SCE platform has a wide range of subscriber-related functions.

This section gives an overview of these alternatives, with emphasis on the Cisco SCA BB-specific subscriber management options. For in-depth explanations, see the appropriate Service Control documentation.

- Anonymous Subscriber Mode, page 14-13
- Subscriber-Aware Mode, page 14-14
- Selecting Subscribers for Real-Time Usage Monitoring, page 14-15
- Managing Subscriber CSV Files, page 14-18

Anonymous Subscriber Mode

An anonymous subscriber is one with a name generated automatically by the SCE platform according to an anonymous subscriber group specification. An anonymous subscriber is always mapped to a single IP address. The actual identity of the customer is unknown to the system.

An anonymous group is a specified IP range, possibly assigned a subscriber template. If an anonymous group is configured, the SCE platform generates anonymous subscribers for that group when it detects traffic with an IP address in the specified IP range. If a subscriber template is assigned to the group, the anonymous subscribers generated have properties defined by that template. If no subscriber template is assigned, the default template is used, which cannot be changed by template import operations. Initially, 200 templates are preconfigured, one for each package ID.

Anonymous subscriber groups and subscriber templates are managed using the SCE platform Command-Line Interface (CLI). You can enter CLI commands via a Telnet session. For more information, see *Cisco SCE 8000 CLI Command Reference Guide* or *Cisco SCE 2000 and SCE 1000 CLI Command Reference Guide*.

Use the following commands to import anonymous subscriber groups and subscriber templates from CSV files and to export subscriber data to these files:

- subscriber anonymous-group import csv-file
- subscriber anonymous-group export csv-file
- subscriber template import csv-file
- subscriber template export csv-file

Note The preceding CLI commands are line interface configuration commands. You must enter line interface configuration mode (see How to Enter Line Interface Configuration Mode, page 14-12) and see the `SCE(config if)#` prompt displayed before entering a command.

Use the following commands to delete anonymous groups or subscriber templates from the system.

- no subscriber anonymous-group [all] [name <groupname>]
- clear subscriber anonymous
- default subscriber template all

Note The preceding CLI commands are line interface configuration commands. You must enter line interface configuration mode (see How to Enter Line Interface Configuration Mode, page 14-12) and see the `SCE(config if)#` prompt displayed before entering a command.

Use the following commands to display anonymous subscriber information:

- show interface LineCard 0 subscriber templates [index]
- show interface LineCard 0 subscriber anonymous-group [all] [name <groupname>]
- show interface LineCard 0 subscriber amount anonymous [name <groupname>]
- show interface LineCard 0 subscriber anonymous [name <groupname>]

Subscriber-Aware Mode

In subscriber-aware mode, each subscriber is a specific customer with an externally generated name. This externally generated name allows the subscriber to be mapped to more than one IP address and still be identified. Each traffic session (single IP flow, or a group of related IP flows) processed by the SCE platform is assigned to a recognized subscriber on the basis of the configured subscriber mappings.

There are three options for introducing and managing these subscribers:

- The SM GUI tool (see Using the SM GUI Tool, page 11-2)
- The SCE platform subscriber CLI
- The SM subscriber management CLU

The SCE Platform Subscriber CLI

Use the following commands to import subscriber data from CSV files and to export subscriber data to these files:

```
subscriber import csv-file
subscriber export csv-file
```

Note The preceding CLI commands are line interface configuration commands. You must enter line interface configuration mode (see How to Enter Line Interface Configuration Mode, page 14-12) and see the `SCE(config if)#` prompt displayed before entering a command.

Use the following command to remove subscribers from the system.

```
no subscriber [all] [name <subscriber-name>]
```

Note The preceding CLI command is a line interface configuration command. You must enter line interface configuration mode (see How to Enter Line Interface Configuration Mode, page 14-12) and see the `SCE(config if)#` prompt displayed before entering the command.

Use the following commands to display subscribers meeting various criteria:

```
show interface LineCard 0 subscriber [amount]
[prefix <prefix>] [property <propertyname> equals | greater-than | less-than
<property-val>]
show interface LineCard 0 subscriber [amount] prefix <prefix>
show interface LineCard 0 subscriber [amount] suffix <suffix>
show interface LineCard 0 subscriber mapping IP <iprange>
show interface LineCard 0 subscriber [amount] mapping intersecting IP <iprange>
show interface LineCard 0 subscriber mapping VLANid <vlanid>
```

Use the following commands to display information about a specific subscriber:

```
show interface LineCard 0 subscriber properties
show interface LineCard 0 subscriber name <name>
show interface LineCard 0 subscriber name <name> mappings
show interface LineCard 0 subscriber name <name> counters
show interface LineCard 0 subscriber name <name> properties
```

The SM Subscriber Management CLU

The SM Subscriber Management Utility (**p3subs)** is a CLU for managing subscribers. You can use it to add or remove subscribers. You can also manage subscriber properties and mappings with this utility.

For more information about **p3subs,** see *Cisco Service Control Management Suite Subscriber Manager User Guide.*

p3subs Syntax

You run **p3subs** from the Solaris shell prompt. The command-line syntax of the utility is:

```
p3subs <operation> --subscriber=<Subscriber-Name> [--ip=<IP-address>]
[--property=<property-name=value>] [--domain=<domain-name>] [--overwrite]
```

The following table lists the **p3subs** operations relevant to managing subscribers.

Table 14-12 p3subs Subscriber Operations

Operation	Description
--add	Adds a subscriber or replaces the existing subscriber configuration
--set	Updates mappings and properties for the specified subscriber
--remove	Removes the specified subscriber
--show	Displays information for specified subscriber

Selecting Subscribers for Real-Time Usage Monitoring

Real-Time Subscriber Usage RDRs report the network activity of a single subscriber per service per metric, in real-time. You must enable the generation of these subscriber usage RDRs separately for each subscriber that you wish to monitor.

Caution Generating and collecting Real-Time Subscriber Usage RDRs for many subscribers can compromise performance. Enable Real-Time Subscriber Usage RDR generation only for subscribers that must be monitored.

The `monitor` subscriber property controls the generation of Real-Time Subscriber Usage RDRs. By default, generation of these RDRs is disabled (`monitor = 0`. To enable generation of the RDRs, change the value of the property to 1.

You can modify this property for selected subscribers using either the SM Command-Line Utility (CLU) or the SCE platform CLI.

- Managing Subscriber Monitoring via the SM, page 14-16
- Managing Subscriber Monitoring via the SCE Platform, page 14-17

Managing Subscriber Monitoring via the SM

You can enable or disable the generation of the Real-Time Subscriber Usage RDRs using the SM **p3subs** utility. You can also create a file that processes a batch of subscribers. For more information, see *Cisco Service Control Management Suite Subscriber Manager User Guide.*

- How to Enable Subscriber Monitoring for a Subscriber, page 14-16
- How to Disable Subscriber Monitoring for a Subscriber, page 14-16
- How to Enable Subscriber Monitoring for Multiple Subscribers, page 14-17
- How to Verify that Subscriber Monitoring is Enabled for a Subscriber, page 14-17

How to Enable Subscriber Monitoring for a Subscriber

You can enable subscriber monitoring for a specified subscriber.

Step 1 From the command line, run **sm/server/bin/p3subs --set --subscriber Smith --property monitor=1.**

How to Disable Subscriber Monitoring for a Subscriber

You can disable subscriber monitoring for a specified subscriber.

Step 1 From the command line, run **sm/server/bin/p3subs --set --subscriber Smith --property monitor=0.**

How to Enable Subscriber Monitoring for Multiple Subscribers

You can enable subscriber monitoring for multiple subscribers.

Step 1 Create a text file (named monitor.txt in this example) containing the sequence of CLU invocations.

The file would look something like this:

```
p3subs --set --subscriber Jerry --property monitor=1
p3subs --set --subscriber George --property monitor=1
p3subs --set --subscriber Elaine --property monitor=1
p3subs --set --subscriber Kramer --property monitor=1
p3subs --set --subscriber Newman --property monitor=1
```

Step 2 From the command line, run **sm/server/bin/p3batch -f monitor.txt**.

How to Verify that Subscriber Monitoring is Enabled for a Subscriber

You can check to see whether subscriber monitoring is enabled for a specific subscriber.

Step 1 From the command line, run **sm/server/bin/p3subs --show-property --subscriber Smith --property monitor.**

Managing Subscriber Monitoring via the SCE Platform

You can also enable or disable the generation of the Real-Time Subscriber Usage RDRs using the SCE platform. For more information, see *Cisco SCE8000 CLI Command Reference Guide.*

How to Enable Subscriber Monitoring for a Subscriber

You can enable subscriber monitoring for a specified subscriber.

Step 1 Enter line interface configuration mode. (See How to Enter Line Interface Configuration Mode, page 14-12.)

Step 2 At the `SCE(config if)#` prompt, run **subscriber name Smith property name monitor value 1.**

How to Disable Subscriber Monitoring for a Subscriber

You can disable subscriber monitoring for a specified subscriber.

Step 1 Enter line interface configuration mode. (See How to Enter Line Interface Configuration Mode, page 14-12.)

Step 2 At the `SCE(config if)#` prompt, run **subscriber name Smith property name monitor value 0.**

How to Enable Subscriber Monitoring for Multiple Subscribers

You can enable subscriber monitoring for multiple subscribers.

Step 1 Create a text file (named monitor.txt in this example) containing the sequence of CLI invocations, including the commands to access the appropriate CLI mode.

The file would look something like this:

```
configure
interface LineCard 0
subscriber name Jerry property name monitor value 1
subscriber name George property name monitor value 1
subscriber name Elaine property name monitor value 1
subscriber name Kramer property name monitor value 1
subscriber name Newman property name monitor value 1
```

Step 2 From the SCE platform CLI prompt `(SCE#)`, run **script run monitor.txt.**

How to Verify that Subscriber Monitoring is Enabled for a Subscriber

You can check to see whether subscriber monitoring is enabled for a specific subscriber.

Step 1 From the SCE platform CLI prompt `(SCE#)`, run **show interface LineCard 0 subscriber name Smith properties.**

The properties are displayed; `monitor` is the relevant parameter.

```
Subscriber smith properties:
subscriberPackage=0
monitor=1
Subscriber 'smith' read-only properties
```

Managing Subscriber CSV Files

Use the **p3subsdb** SM utility to import and export subscriber CSV files. You can import subscriber information for a group of subscribers from a CSV file into the SM database. You can also export subscriber information from the SM database to a CSV file.

For more information, see the *Cisco Service Control Management Suite Subscriber Manager User Guide.*

CSV file structure is described in the “CSV File Formats” chapter of *Cisco Service Control Application for Broadband Reference Guide.*

- How to Import Subscriber CSV Files, page 14-19
- How to Export Subscriber CSV Files, page 14-19

How to Import Subscriber CSV Files

Step 1 At the Solaris shell prompt, run **p3subsdb --import <filename>.**

How to Export Subscriber CSV Files

Step 1 At the Solaris shell prompt, run **p3subsdb --export <filename>**.

Example: Filtering and Exporting Subscribers

The following example exports every subscriber whose name begins with ‘a’ to the file silverSubscriberFile.csv

```
p3subsdb --export --prefix=a --output=silverSubscriberFile.csv
```