

Cisco Service Control Application for Broadband User Guide

Release 3.1.6
July 2008

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-7205-09

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.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

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
© 2008 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface xvii

Document Revision History xvii

Organization xix

Related Publications xx

Conventions xxi

Obtaining Documentation and Submitting a Service Request xxii

CHAPTER 1 **Cisco Service Control Overview** 1-1

Cisco Service Control Solution 1-1

Service Control for Broadband Service Providers 1-2

Cisco Service Control Capabilities 1-2

SCE Platform Description 1-3

Management and Collection 1-4

Network Management 1-5

Subscriber Management 1-5

Service Configuration Management 1-6

Data Collection 1-6

CHAPTER 2 **System Overview** 2-1

System Components 2-1

Subscribers and Subscriber Modes 2-3

Subscriberless Mode 2-3

Anonymous Subscriber Mode 2-3

Static Subscriber Mode 2-4

Subscriber-Aware Mode 2-4

Subscriber Modes: Summary 2-4

Service Configuration 2-6

The SCA BB Console 2-7

The Service Configuration Utility 2-7

The Service Configuration API 2-8

CHAPTER 3 **Traffic Processing Overview** 3-1

Routing Environment 3-1
Traffic Processing 3-2
Traffic Classification 3-2
Services 3-2
Service Elements 3-3
Examples of Services 3-4
Protocols 3-4
Protocol Elements 3-5
Signatures 3-5
Initiating Side 3-6
Zones 3-6
Zone Items 3-6
Flavors 3-7
Flavor Items 3-7
DSCP ToS 3-7
Content Filtering 3-7
Mapping Flow Attributes to Services 3-8
Traffic Accounting and Reporting 3-8
Usage Accounting 3-9
The Service Hierarchy 3-9
The Package Hierarchy 3-10
Reporting 3-11
RDRs 3-11
NetFlow 3-12
Traffic Control 3-12
Packages 3-12
Virtual Links Mode 3-13
Unknown Subscriber Traffic 3-13
Rules 3-13
Calendars 3-13
Bandwidth Management 3-14
Global Bandwidth Control 3-14
Subscriber Bandwidth Control 3-14
Quota Management 3-16
Subscriber Notification 3-17

Other Traffic Processing Features 3-17
Service Security 3-17
Detecting Malicious Traffic 3-18
Responding to Malicious Traffic 3-18
Traffic Filters 3-19
DSCP ToS Marking 3-19
Traffic Forwarding to Value Added Services Servers 3-19
Service Configurations 3-20
Defining Service Configurations in Practice 3-20

CHAPTER 4 **Getting Started** 4-1
How to Install SCA BB 4-1
The SCA BB Installation Package 4-2
Installing SCA BB Application Components 4-2
Prerequisites 4-2
How to Verify that the SCE Platform is Operational 4-3
How to Verify that the SCE Platform is Running an Appropriate Version of the OS 4-3
How to Verify that the SM is Correctly Installed 4-3
How to Verify that an Appropriate Version of the SM is Running 4-3
How to Install SCA BB Front Ends 4-3
Hardware Requirements 4-4
Operating System Requirements 4-4
Installing the Java Runtime Environment 4-4
How to Install the Console 4-4
How to Install the SCA BB Configuration Utilities 4-7
How to Upgrade SCA BB 4-7
How to Upgrade from Release 2.5 to Release 3.1.6 4-8
How to Upgrade from Release 3.0.x to Release 3.1.6 4-8
How to Upgrade the SCA BB Service Configuration Utility 4-9
How to Reconfigure DSCP Marking for Release 3.1.5 and Higher 4-9
Working with Protocol Packs 4-10
Protocol Packs 4-10
Installing Protocol Packs 4-11
How to Verify Version Compatibility for Protocol Packs 4-11
How to Verify the Installation of a Protocol Pack 4-12
Hitless Upgrade of the SLI 4-12
Hitless Upgrade CLI Commands 4-13
Description of Hitless Upgrade CLI Commands 4-13
How to Enter Line Interface Configuration Mode 4-14

How to Launch the Console 4-15
How to Use the Console 4-16
Configuration Wizards 4-17
Asymmetric Routing 4-17
Anonymous Subscriber Mode 4-17
How to Use the Usage Analysis Wizard 4-18
How to Use the P2P Traffic Optimization Wizards 4-29
How to Use the Reporter DB Configuration Wizard 4-45
The Network Navigator Tool 4-51
How to Open the Network Navigator Tool 4-52
How to Close the Network Navigator Tool 4-52
The Service Configuration Editor Tool 4-52
How to Open the Service Configuration Editor Tool 4-53
How to Close the Service Configuration Editor Tool 4-54
The Signature Editor Tool 4-54
How to Open the Signature Editor Tool 4-55
How to Close the Signature Editor Tool 4-55
The Subscriber Manager GUI Tool 4-55
How to Open the SM GUI Tool 4-56
How to Close the SM GUI Tool 4-56
The Reporter Tool 4-56
How to Open the Reporter Tool 4-57
How to Close the Reporter Tool 4-57
Online Help 4-57
How to Access Online Help 4-58
How to Search Online Help 4-58
Quick Start with the Console 4-59
Example: How to Configure the Console and Apply the Default Service Configuration 4-59

CHAPTER 5 **Using the Network Navigator** 5-1
The Network Navigator Tool 5-1
Managing Sites 5-2
How to Add a Site to the Site Manager 5-3
How to Add Devices to a Site 5-3
How to Add SCE Devices to a Site 5-3
How to Add SM Devices to a Site 5-4
How to Add CM Devices to a Site 5-4
How to Add Database Devices to a Site 5-5
How to Delete Devices 5-6

How to Delete Sites 5-6
Managing Devices 5-6
Password Management 5-6
Managing SCE Devices 5-7
How to Configure SCE and CM Devices Using a Wizard 5-8
How to Generate Tech Support Info Files for SCE Devices 5-15
How to Retrieve the Online Status of SCE Devices 5-17
How to Install a Protocol Pack 5-17
How to Apply Service Configurations to SCE Devices 5-19
How to Retrieve Service Configurations from SCE Devices 5-21
How to Install PQI Files on SCE Devices 5-22
How to Install an SCE OS Software Package on SCE Devices 5-23
Managing SM Devices 5-24
How to Generate Tech Support Info Files for SM Devices 5-24
How to Retrieve the Online Status of SM Devices 5-25
How to Connect to SM Devices 5-26
How to Install PQI Files on SM Devices 5-26
Managing CM Devices 5-27
How to Retrieve the Online Status of CM Devices 5-27
Managing Database Devices 5-28
How to Make Databases Accessible to the SCA Reporter 5-28
Working with Network Navigator Configuration Files 5-31
How to Export a Network Navigator Configuration 5-31
How to Import a Network Navigator Configuration 5-34
Network Settings Requirements 5-35
Firewall/NAT Requirements 5-36
User Authentication 5-37
How to Disable PRPC Authentication 5-37
How to Disable PRPC Authentication on an SCE Platform 5-38
How to Disable PRPC Authentication on a CM 5-38
How to Disable PRPC Authentication on an SM 5-38

CHAPTER 6 **Using the Service Configuration Editor** 6-1
Service Configurations 6-1
Managing Service Configurations 6-1
Opening the Service Configuration Editor Tool 6-1
How to Add New Service Configurations 6-2
How to Open Existing Service Configurations 6-4
How to Save the Current Service Configuration 6-5

How to Save the Current Service Configuration to a Service Configuration File 6-5
How to Save the Current Service Configuration to the File from Which it Was Loaded 6-5
How to Close Service Configurations 6-6
How to Export Service Configuration Data 6-6
How to Import Service Configuration Data 6-10
Applying and Retrieving Service Configurations 6-13
How to Validate the Current Service Configuration 6-13
How to Apply a Service Configuration to SCE Platforms 6-14

CHAPTER 7 **Using the Service Configuration Editor: Traffic Classification** 7-1

Managing Services 7-1
Service Parameters 7-2
Adding and Defining Services 7-2
How to Add a Service to a Service Configuration 7-3
How to Define Hierarchical Settings for a Service 7-4
How to Set the Service Index 7-5
How to View Services 7-6
How to Edit Services 7-7
How to Delete Services 7-9
Managing Service Elements 7-9
How to Add Service Elements 7-10
How to Duplicate Service Elements 7-14
How to Edit Service Elements 7-15
How to Delete Service Element 7-17
How to Move Service Elements 7-18
Managing Protocols 7-19
Viewing Protocols 7-19
How to View Protocols 7-19
How to Filter the Protocols List 7-21
How to Add Protocols 7-22
How to Edit Protocols 7-22
How to Delete Protocols 7-23
Managing Protocol Elements 7-24
How to Add Protocol Elements 7-25
How to Edit Protocol Elements 7-27
How to Delete Protocol Elements 7-28

Managing Zones 7-29
How to View Zones 7-29
How to Add Zones 7-30
How to Edit Zones 7-30
How to Delete Zones 7-31
Managing Zone Items 7-32
How to Add Zone Items 7-32
How to Edit Zone Items 7-33
How to Delete Zone Items 7-33
Managing Protocol Signatures 7-33
Viewing Signatures 7-34
How to View Signatures 7-34
How to Filter the Signatures List 7-35
Dynamic Signatures 7-35
Dynamic Signature Script Files 7-36
The Default DSS File 7-39
Managing Flavors 7-44
Flavor Types and Parameters 7-45
How to View Flavors 7-46
How to Add Flavors 7-47
How to Edit Flavors 7-48
How to Delete Flavors 7-49
Managing Flavor Items 7-50
Maximum Number of Flavor Items per Flavor Type 7-50
How to Add Flavor Items 7-50
How to Edit Flavor Items 7-52
How to Delete Flavor Items 7-53
Managing Content Filtering 7-53
Information About Content Filtering 7-54
The SCE Application 7-54
The Cisco CPA Client 7-54
The SurfControl CPA Server 7-54
The Content Filtering CLI 7-54
CPA Client CLI Commands 7-55
Description of CPA Client CLI Commands 7-55
How to Configure the RDR Formatter 7-56
Related Info 7-56
How to Enter Line Interface Configuration Mode 7-56
Managing Content Filtering Settings 7-57

Importing Content Filtering Categories 7-57
How to Configure Content Filtering 7-64
How to View Content Filtering Settings 7-65
How to Remove Content Filtering Settings 7-65

CHAPTER 8 **Using the Service Configuration Editor: Traffic Accounting and Reporting** 8-1

Usage Counters 8-1
Raw Data Records 8-2
NetFlow records 8-2
Managing RDR Settings 8-2
The RDR Settings Dialog Box 8-2
How to Manage Usage RDRs 8-3
How to Manage Transaction RDRs 8-4
How to Manage Quota RDRs 8-6
How to Manage Transaction Usage RDRs 8-8
How to Manage Log RDRs 8-10
How to Manage Real-Time Subscriber Usage RDRs 8-12
How to Manage Real-Time Signaling RDRs 8-14

CHAPTER 9 **Using the Service Configuration Editor: Traffic Control** 9-1

Unknown Subscriber Traffic 9-1
Managing Packages 9-2
Package Parameters 9-3
How to View Packages 9-4
How to Add Packages 9-5
What to Do Next 9-6
How to Set Advanced Package Options 9-7
How to Duplicate Packages 9-8
How to Edit Packages 9-8
How to Delete Packages 9-10
Managing Rules 9-10
The Default Service Rule 9-11
Rule Hierarchy 9-11
How to View the Rules of a Package 9-11
What to Do Next 9-12
How to Add Rules to a Package 9-12
What to Do Next 9-14
How to Define Per-Flow Actions for a Rule 9-14
How to Edit Rules 9-17

How to Delete Rules 9-18
How to Display the Services Affected by a Rule 9-19
Managing Time-Based Rules 9-20
How to Add Time-Based Rules to a Rule 9-20
How to Edit Time-Based Rules 9-22
How to Delete Time-Based Rules 9-23
Managing Calendars 9-24
How to Manage DSCP ToS Marker Values 9-28
DSCP ToS Marking 9-29
Managing Bandwidth 9-30
Managing Global Bandwidth 9-30
How to View Global Controller Settings 9-31
How to Edit the Total Link Limits 9-32
How to Add Global Controllers 9-33
How to Set the Maximum Bandwidth of Global Controllers 9-33
How to Delete Global Controllers 9-35
Defining Global Controllers in a Dual-Link System 9-35
How to Set Global Controller Bandwidth Limits Separately for Each Link 9-35
How to Set Global Controller Bandwidth Limits as the Sum of Two Links 9-36
Managing Subscriber Bandwidth 9-36
Subscriber BWC Parameters 9-37
How to Edit Package Subscriber BWCs 9-38
Managing Bandwidth: a Practical Example 9-39
How to Configure Total Bandwidth Control 9-39
Example: How to Limit P2P and Streaming Traffic Using the Console 9-40
How to Set BW Management Prioritization Mode 9-43
Managing Virtual Links 9-44
Collection Manager Virtual Links Names Utility 9-45
How to Enable Virtual Links Mode 9-45
How to View Virtual Links Global Controller Settings 9-46
Managing Virtual Links Global Controllers 9-48
How to Edit the Virtual Links Total Link Limits 9-48
Managing Virtual Links with CLI Commands 9-49
Description of Virtual Links CLI Commands 9-49
How to Enter Line Interface Configuration Mode 9-50

Managing Quotas 9-50
How to Edit Quota Management Settings for Packages 9-50
Quota Replenish Scatter 9-50
How to Select Quota Buckets for Rules 9-52
How to Edit Breach-Handling Parameters for a Rule 9-53
Breach-Handling Parameters 9-54

CHAPTER 10 **Using the Service Configuration Editor: Additional Options** 10-1

The Service Security Dashboard 10-1
How to View the Service Security Dashboard 10-2
Managing Worm Detection 10-2
How to View Supported Worm Signatures 10-2
How to Add New Worm Signatures to a Service Configuration 10-3
Related Info 10-3
Managing Anomaly Detection 10-3
Anomaly Detection 10-3
Anomaly Detection Parameters 10-4
How to View Anomaly Detection Settings 10-5
How to Add Anomaly Detectors 10-7
What to Do Next 10-10
Editing Anomaly Detectors 10-10
How to Delete Anomaly Detectors 10-14
Managing Spam Detection 10-14
How to Configure Spam Detection Settings 10-15
Viewing Malicious Traffic Reports 10-16
Malicious Traffic Reports 10-16
How to View a Service Security Report 10-17
Filtering the Traffic Flows 10-17
Information About Traffic Filtering 10-18
The SCA BB Filtered Traffic Mechanism 10-18
Filter Rule Actions 10-19
Filter Rules and Service Rules 10-19
Automatic Quick Forwarding of Media Flows 10-19
How to View Filter Rules for a Package 10-20
How to Add Filter Rules 10-20
How to Edit Filter Rules 10-26
How to Delete Filter Rules 10-26
How to Activate and Deactivate Filter Rules 10-27

Managing Subscriber Notifications 10-27
Subscriber Notification Parameters 10-28
Network Attack Notification 10-29
Network Attack Notification Parameters 10-30
Example of URL with Description Tail 10-31
How to View Subscriber Notifications 10-31
How to Add Subscriber Notifications 10-32
How to Edit Subscriber Notifications 10-33
How to Delete Subscriber Notifications 10-33
Managing the System Settings 10-34
Setting the System Modes 10-34
Information About the System Modes 10-34
How to Set the Operational and Topological Modes of the System 10-36
Setting Redirection Parameters 10-37
How to Add a Set of Redirection URLs 10-37
How to Edit Redirection Parameters 10-39
How to Delete a Set of Redirection URLs 10-40
Managing Advanced Service Configuration Options 10-40
The Advanced Service Configuration Properties 10-41
How to Edit Advanced Service Configuration Options 10-44
Managing VAS Traffic-Forwarding Settings 10-45
How to Enable VAS Traffic Forwarding 10-46
How to Disable VAS Traffic Forwarding 10-48
How to Rename VAS Server Groups 10-48
How to View VAS Traffic-Forwarding Tables 10-49
How to Delete VAS Traffic-Forwarding Tables 10-50
How to Add VAS Traffic-Forwarding Tables 10-50
Managing VAS Table Parameters 10-51
How to Add VAS Table Parameters 10-51
How to Edit VAS Table Parameters 10-52
How to Delete VAS Table Parameters 10-53

CHAPTER 11 **Using the Subscriber Manager GUI Tool** 11-1

Using the SM GUI Tool 11-1
Connecting to an SCMS-SM 11-2
How to Connect to an SCMS-SM from the Network Navigator 11-2
How to Connect to an SCMS-SM from the Console 11-3
How to Disconnect from the Current SCMS-SM 11-4
Working with Subscriber CSV Files 11-5
How to Import Subscriber Information from a CSV File 11-5
How to Export Subscriber Information to a CSV File 11-6
Managing Subscribers 11-6
Subscriber Information 11-6
Finding and Selecting Subscribers 11-7
How to Find a Subscriber or Group of Subscribers 11-7
Selecting Subscribers 11-7
How to Add a Subscriber 11-8
Editing Subscriber Details 11-10
How to Edit Details for Single Subscribers 11-10
How to Edit Details for a Group of Subscribers 11-11
How to Delete a Subscriber from the Database 11-12

CHAPTER 12 **Using the Signature Editor** 12-1

The Signature Editor Console 12-1
Managing DSS Files 12-1
The DSS File Components 12-2
The DSS File 12-2
DSS Protocol List 12-2
Information About DSS Protocols 12-3
DSS Signatures 12-4
DSS Deep Inspection Clauses 12-8
DSS Deep Inspection Conditions 12-9
How to Create DSS Files 12-10
How to Edit DSS Files 12-13
How to Import DSS Files 12-14

CHAPTER 13 **Additional Management Tools and Interfaces** 13-1

The SCA BB Service Configuration Utility 13-1
servconf Syntax 13-1
servconf Examples 13-4
The SCA BB Real-Time Monitoring Configuration Utility 13-5
rtmcmd Syntax 13-5
rtmcmd Examples 13-6
The rtmcmd User Configuration File 13-7
An rtmcmd User Configuration File Example 13-8
The SCA BB Signature Configuration Utility 13-8
sigconf Syntax 13-8
sigconf Examples 13-9
Overview of SNMP, MIB, and Traps 13-9
SNMP 13-9
MIB 13-10
Traps 13-10
Installing PQI Files from the Command Line 13-10
How to Install a SCA BB PQI File on an SCE Platform 13-11
What to Do Next 13-11
How to Enter Line Interface Configuration Mode 13-11
How to Install a SCA BB PQI File on an SM Device 13-11
What to Do Next 13-12
Managing Subscribers via Other System Components 13-12
Anonymous Subscriber Mode 13-12
Subscriber-Aware Mode 13-13
The SCE Platform Subscriber CLI 13-13
The SM Subscriber Management CLU 13-14
Selecting Subscribers for Real-Time Usage Monitoring 13-15
Managing Subscriber Monitoring via the SM 13-15
Managing Subscriber Monitoring via the SCE Platform 13-16
Managing Subscriber CSV Files 13-18
How to Import Subscriber CSV Files 13-18
How to Export Subscriber CSV Files 13-18
Example: Filtering and Exporting Subscribers 13-18



Preface

This preface describes who should read the *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

The Document Revision History below records changes to this document.

Revision	Cisco Service Control Release and Date	Change Summary
OL-7205-09	3.1.6 July, 2008	• Minor correction regarding filter rules.
OL-7205-08	3.1.6 May, 2008	• Minor changes throughout the guide.
OL-7205-07	3.1.5 November, 2007	Added the following new features: • Configuration Wizards, page 4-17 See: – How to Use the Usage Analysis Wizard, page 4-18 – How to Use the P2P Traffic Optimization Wizards, page 4-29 – How to Use the Reporter DB Configuration Wizard, page 4-45 – How to Configure SCE and CM Devices Using a Wizard, page 5-8 • DSCP ToS Classification (ToS is added as a flavor type, see Managing Flavors, page 7-44) • DSCP ToS Marking (see How to Manage DSCP ToS Marker Values, page 9-28)

Revision	Cisco Service Control Release and Date	Change Summary
OL-7205-05	3.1.0 May, 2007	Added the following new features: • Virtual Links (see Managing Virtual Links, page 9-44) • Asymmetric Routing Classification Mode, page 10-35 • NetFlow (see NetFlow records, page 8-2) • Quota Replenish Scatter, page 9-50 Updated the following sections of the document • Managing Bandwidth, page 9-30 • Information About the System Modes, page 10-34 • Managing Advanced Service Configuration Options, page 10-40
OL-7208-04	3.0.5 November, 2006	Added the following new feature: • The SCA BB Real-Time Monitoring Configuration Utility, page 13-5 Updated the following sections of the document • Quick Forwarding (see Filter Rule Actions, page 10-19 and Automatic Quick Forwarding of Media Flows, page 10-19)
OL-7205-03	3.0.3 May, 2006	Added the following new features: • Hitless Upgrade of the SLI, page 4-12 • Content Filtering (see Managing Content Filtering, page 7-53) • The Service Security Dashboard, page 10-1 Removed the following deprecated feature: • Attack Filtering and Subscription Notification

Revision	Cisco Service Control Release and Date	Change Summary
OL-7205-02	3.0.0 December, 2005	Document name changed to *Cisco Service Control Application for Broadband User Guide.* Both the look-and-feel and the functionality of the Cisco Service Control Application for Broadband (SCA BB) Console were redesigned for release 3.0. Consequently, this document underwent a major rewrite. The major changes in this document are listed below. • Appendixes B, C, D of the 2.5.5 release user guide were moved to a new document: the *Cisco Service Control Application for Broadband Reference Guide.* • Chapter 8 and Appendix A of the 2.5.5 release user guide were moved to a new document: the *Cisco Service Control Application Suite Reporter User Guide.* • The *Cisco Service Control Application Suite for Broadband Installation Guide* was deprecated; it forms the basis for part of the Getting Started chapter. • Chapter 5 of the 2.5.5 release user guide (*Constructing Service Configurations*) was completely rewritten and split into three chapters. • New chapters were added for the new tools included in the Console: the Network Navigator tool and the Signature Editor tool.
OL-7205-01	2.5.5 February, 2005	First version of this document (then named *Cisco Service Control Application Suite for Broadband User Guide*).

Organization

This guide contains the following sections:

Chapter	Description
Chapter 1, “Cisco Service Control Overview”	Provides a general overview of the Cisco Service Control solution.
Chapter 2, “System Overview”	Provides a functional overview of the Cisco Service Control solution.
Chapter 3, “Traffic Processing Overview”	Provides a technical overview of the Cisco Service Control solution.
Chapter 4, “Getting Started”	Guides you through the process of installing or upgrading SCA BB and describes the concept of the Console as a collection of tools.
Chapter 5, “Using the Network Navigator”	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.
Chapter 6, “Using the Service Configuration Editor”	Explains how to use the Service Configuration Editor to manage service configurations.

Chapter	Description
Chapter 7, “Using the Service Configuration Editor: Traffic Classification”	Explains how to configure service configurations to perform traffic classification.
Chapter 8, “Using the Service Configuration Editor: Traffic Accounting and Reporting”	Explains how to configure service configurations to perform traffic reporting.
Chapter 9, “Using the Service Configuration Editor: Traffic Control”	Explains how to configure service configurations to perform traffic control.
Chapter 10, “Using the Service Configuration Editor: Additional Options”	Documents additional, advanced options available in the Service Configuration Editor.
Chapter 11, “Using the Subscriber Manager GUI Tool”	Explains how to use the SM GUI tool to configure subscribers on the SCMS-SM database.
Chapter 12, “Using the Signature Editor”	Documents the Signature Editor tool, which can create files for updating protocols in SCA BB.
Chapter 13, “Additional Management Tools and Interfaces”	Documents and explains other tools that are available for use with SCA BB.

Related Publications

Use this *Cisco Service Control Application for Broadband User Guide* in conjunction 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*
- The SCE platform installation and configuration guides:
  - *Cisco SCE 1000 2xGBE Installation and Configuration Guide*
  - *Cisco SCE 2000 4xGBE Installation and Configuration Guide*
  - *Cisco SCE 2000 4/8xFE Installation and Configuration Guide*
- *Cisco Service Control Engine (SCE) CLI Command Reference*
- *Cisco Service Control Engine (SCE) Software Configuration Guide*

Conventions

This document uses the following 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 will include the quotation marks.
`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*.



Tip Means *the following information will help you solve a problem*.



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

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 total Cisco service control solution.

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

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, IP service providers' business models need to be reworked 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 the service provider 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 the 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 requires highly adaptive protocol and application-level intelligence.
- Programmability—The ability to quickly add new protocols 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.

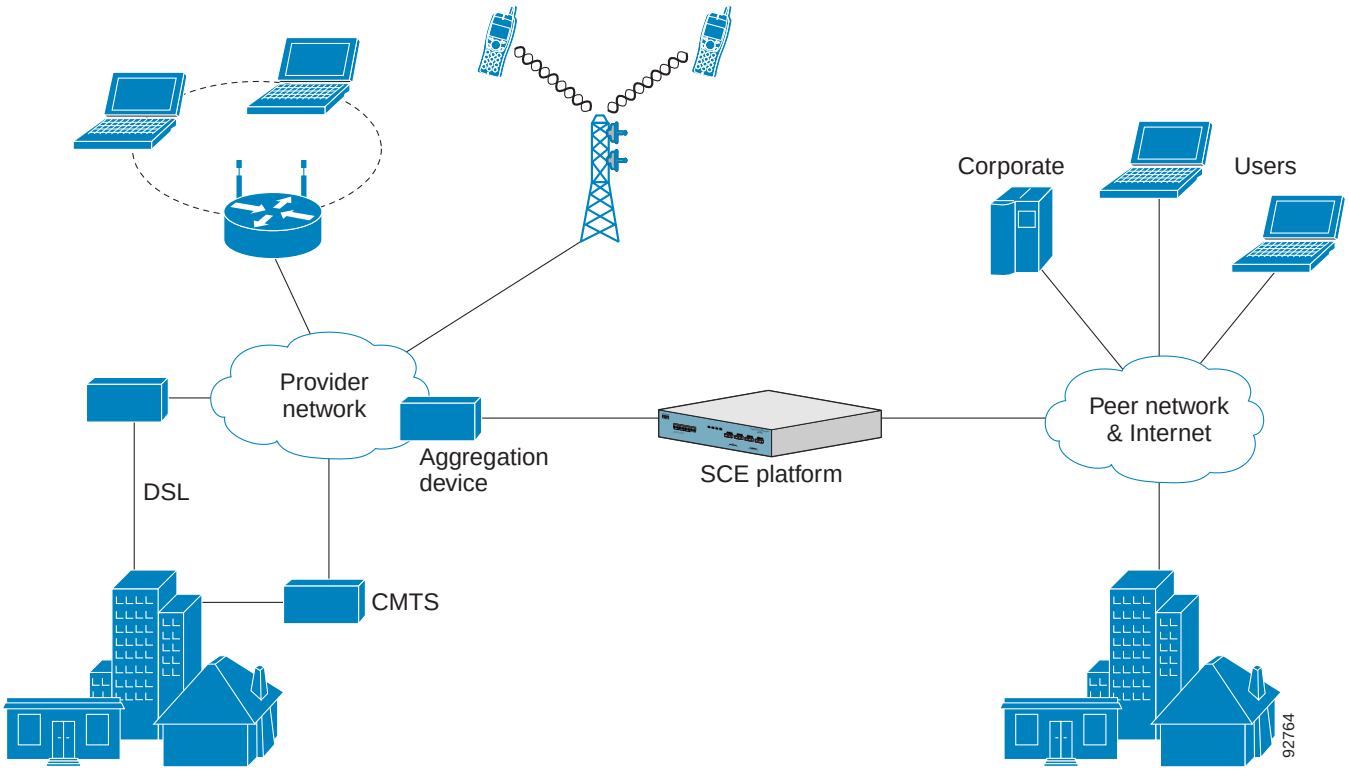
SCE Platform Description

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 is a network device that uses ASIC components and reduced instruction set computer (RISC) processors to exceed beyond packet counting and expand into the contents of network traffic. Providing programmable, stateful inspection of bidirectional traffic flows, and mapping these flows with user ownership, SCE platforms 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



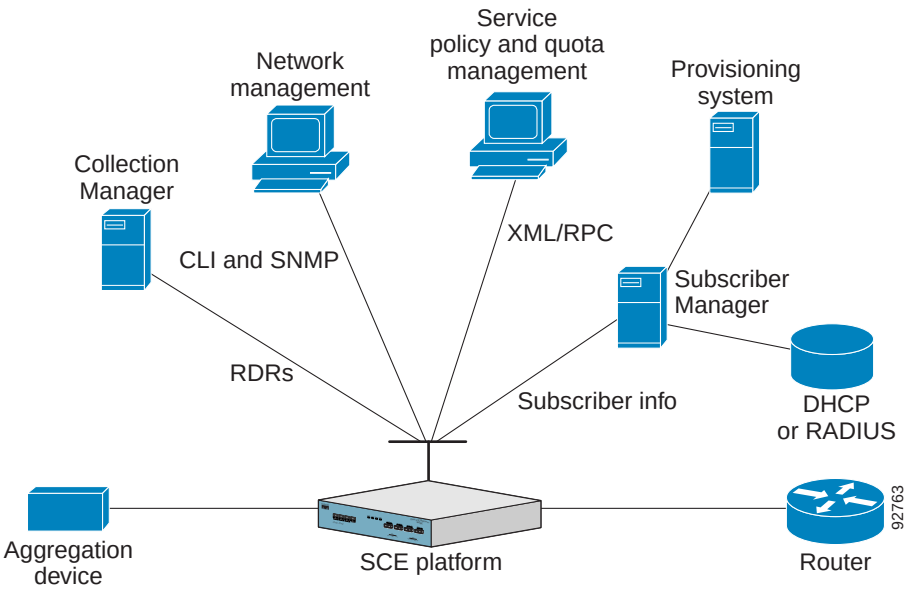
Management and Collection

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

The SM 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 SM pushes subscriber information to the SCE platform automatically upon logon of a subscriber.
- Pull Mode—The SM 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 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. All analysis and data processing functions of the SCE platform result in the generation of Raw Data Records (RDRs), which the SCE platform forwards using a simple TCP-based protocol (RDR-Protocol).
2. RDRs are processed by the Cisco service control management suite collection manager.
3. The collection manager software is an implementation of a collection system that receives RDRs from one or more SCE platforms. It collects these records and processes them in one of its adapters. Each adapter performs a specific action on the RDR.

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



CHAPTER 2

System Overview

The Cisco Service Control Application for Broadband (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 thereby 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 2-1
- Subscribers and Subscriber Modes, page 2-3
- Service Configuration, page 2-6

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 the Cisco SCE Platform Installation and Configuration Guides.

- The Service Control Management Suite (SCMS) Subscriber Manager (SM)—A middleware software component that is used where dynamic binding of subscriber information and policies is required. The SM manages subscriber information and provisions it in real time to multiple SCE platforms. The SM 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 SM, see the *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 the *Cisco Service Control Management Suite Quota Manager Solution 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 the *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.

Together, the SCE platform, the SCMS-CM, the SCMS-SM, and the SCA Reporter are designed to support detailed classification, analysis, reporting, and control of IP network traffic. The SCMS-CM, the SCA Reporter, and the SCMS-SM 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.

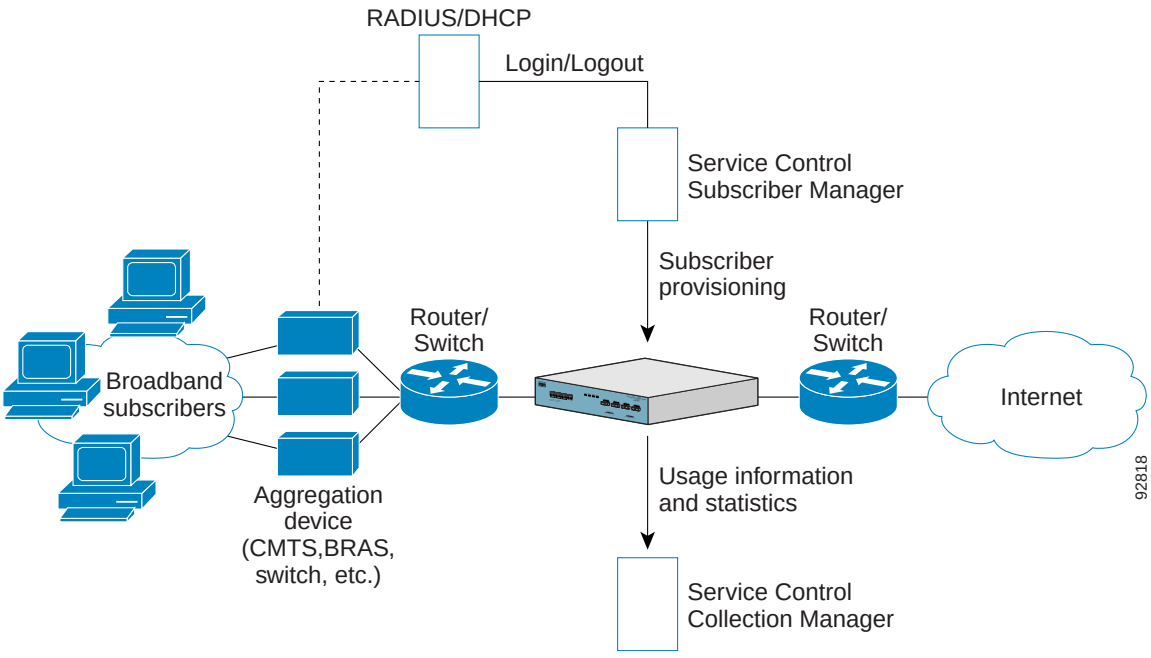
- Horizontal flow—Represents traffic between subscribers and an IP network.

  The SCE platform monitors traffic flow.

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

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

Figure 2-1 Flow of Information in 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 SCA BB can individually monitor, account, and enforce a policy. In the most granular instance of the SCA BB system a subscriber is an actual customer of the service provider on whom an individual policy is implemented. However, you can also to use 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 to be made when designing a service control solution is what subscribers in the system represent. This determines which subscriber mode will be 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.

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. This can be achieved by integrating with the system (RADIUS, DHCP) that assigns IP addresses to subscribers, or by sniffing this information. Policy information is either administered to 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-SM is not required.

Note Subscriberless mode is not influenced by the number of subscribers or inbound IP addresses Thus 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, when analysis on an IP level is sufficient, or 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-SM is not required. Rather, ranges of IP addresses are configured directly on the SCE platform, for which the system dynamically creates “anonymous” subscribers, 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) will be 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-SM). 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 SCE is populated by subscriber information (OSS ID and policy) that is dynamically bound to the (IP) address currently in use by the subscribers. Regardless of the IP address in use, this 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-SM 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)

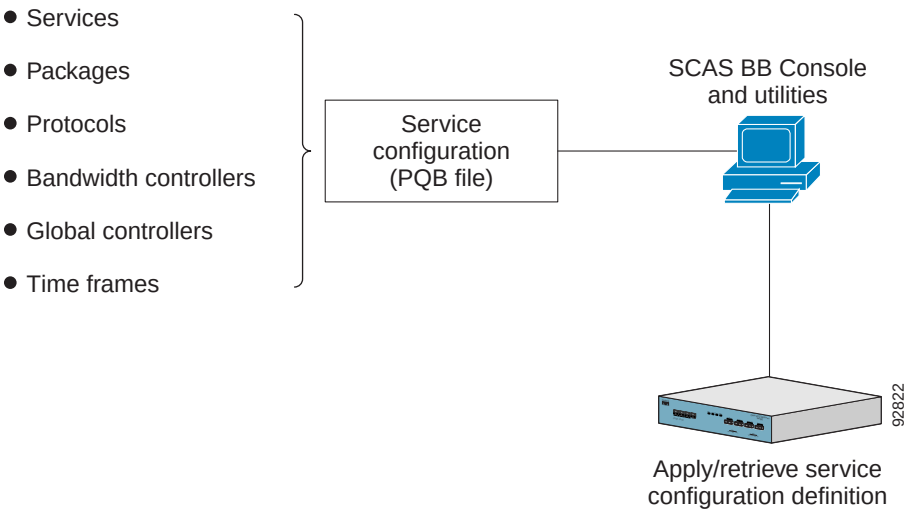
Mode	Features Supported	Main Advantages	Use for...
Static subscriber mode	• Global analysis and control • Control based on individual or group IP addresses as configured statically to the SCE platform	• One-time static subscriber configuration, with no integration requirements. • Manage subscriber traffic 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 very 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



Service configuration is accomplished using one of the following:

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

The SCA BB Console

The 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 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 SCA BB Service Configuration Utility, page 13-1.

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

This allows service providers to automate and simplify management and operational tasks.

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



CHAPTER 3

Traffic Processing Overview

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

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

- Routing Environment, page 3-1
- Traffic Processing, page 3-2
- Traffic Classification, page 3-2
- Traffic Accounting and Reporting, page 3-8
- Traffic Control, page 3-12
- Other Traffic Processing Features, page 3-17
- Service Configurations, page 3-20

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 pass 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 is 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 flows' opposite direction.

Traffic Processing

There are three stages of traffic processing:

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

These three stages are described in the following sections.

You control how classification, reporting, and control are performed by editing service configurations and applying them 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.

- Services, page 3-2
- Protocols, page 3-4
- Initiating Side, page 3-6
- Zones, page 3-6
- Flavors, page 3-7
- Mapping Flow Attributes to Services, page 3-8

Services

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

Services are the building blocks for:

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

From a provider's point of view, 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 (these services are listed in the "Default Service Configuration Reference Tables" chapter of the *Cisco Service Control Application for Broadband Reference Guide*). You can modify these services and add additional services to a service configuration.

A service configuration can contain up to 500 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 session's life cycle.

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

- Protocol—The protocol used. This 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 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 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 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.

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 SCA BB cannot achieve 100% classification of all P2P services, because some P2P applications are very 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 will be 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 Service B's list matches both services, but will be mapped to Service B.

- If a flow matches one parameter of one service element and a different parameter of another service element, precedence will be 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 will be 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 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, 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, 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, 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, SCA BB tries to classify the protocol using the destination port of the first packet. If no exact match is found, 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.

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

- The flow matches the specified signature of the protocol element.
- The flow protocol matches the IP Protocol of the protocol element.
- The flow matches the specified port range of the protocol element.
- If a flow matches two protocol elements and one is more specific than the other, the flow will be mapped to the more specific of the two.

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

  For example: Protocol A is defined for flows that match the FTP signature and Protocol B is defined for flows on TCP port 21. An FTP flow on port 21 matches both protocols, but will be mapped to Protocol A.

Signatures

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

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 SCA BB, enhancing its classification capabilities.

Dynamic Signatures

Most signatures used by SCA BB are predefined and hard-coded. 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 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 provider's subscribers and the network. Subscriber-initiated flows are initiated by the subscriber toward the network; network-initiated flows are initiated from the network toward the subscriber.

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. If the direction of the HTTP flow is network-initiated, this probably means that a web server is open on the subscriber's local machine 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 subscriber's network flow 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.)

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 7-45.

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 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 SCA BB and the SCE platform are not designed to track and maintain the huge database of URLs required for effective filtering.

SCA BB provides content filtering by integrating with SurfControl Content Portal Authority (CPA). SurfControl's technology enhances 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 forth.

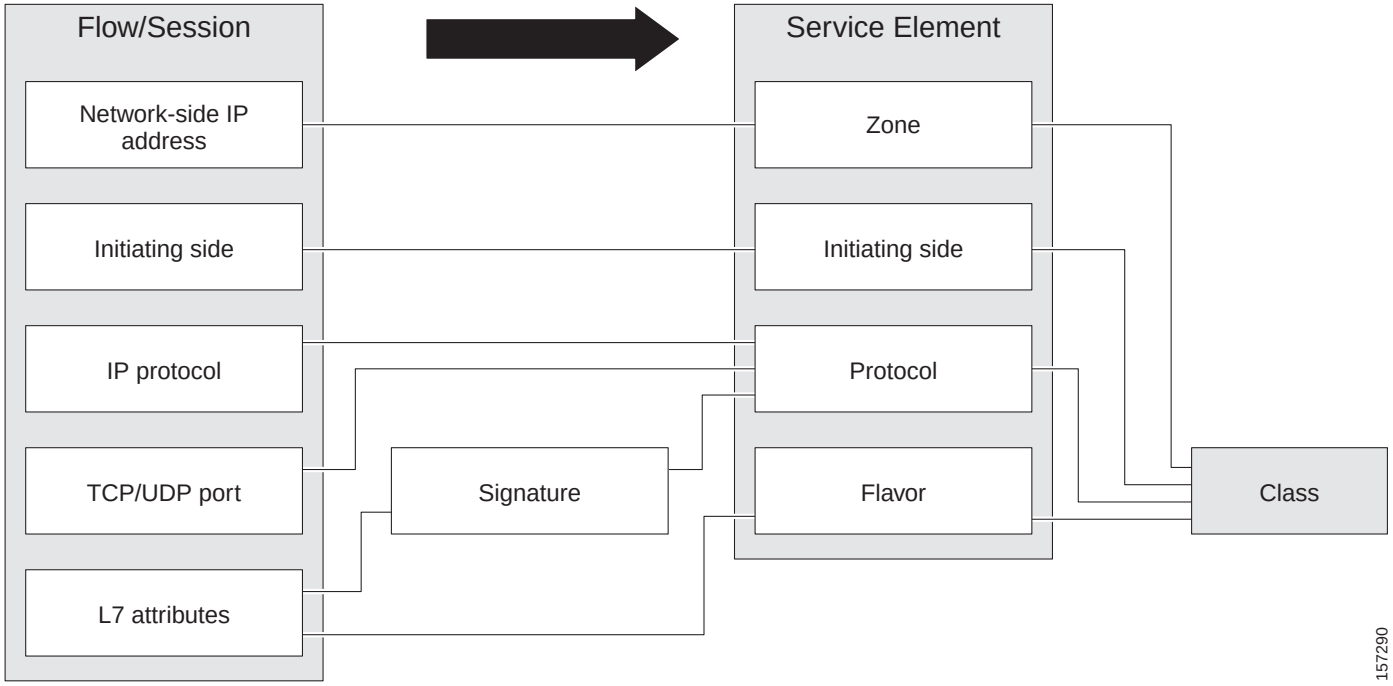
The integration of SurfControl's CPA into SCA BB provides the required web-filtering solution. SCA BB, running on the SCE platform, contacts a CPA server to categorize the website that a subscriber requests. The returned category is then used to classify the HTTP flow. This classification is then used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

Note 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 can be queried by external systems.

Usage Accounting

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 assignment of services to usage counters is determined by the service hierarchy, as explained in the following section. Similarly, several packages may share the same package usage counter, and the assignment of packages to usage counters is determined by The Package Hierarchy.

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.

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

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 in conjunction 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.

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.

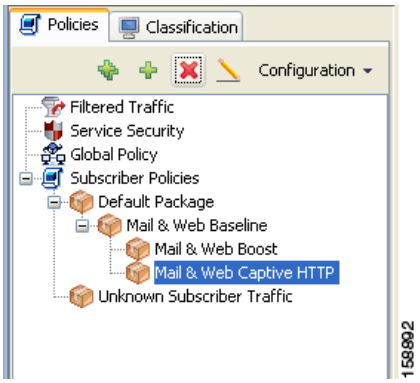
Usage reporting at a package level is grouped as follows:

- 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.

For example, in the example package tree shown in Figure 3-2, 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 together usage of subscribers assigned to all three packages.

On the other hand, 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 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. This requires you to use 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 SCA BB solution to be more easily integrated with your existing data collectors.

- RDRs, page 3-11
- NetFlow, page 3-12

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-CM 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 in order 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 3-12
- Unknown Subscriber Traffic, page 3-13
- Rules, page 3-13
- Bandwidth Management, page 3-14
- Quota Management, page 3-16

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 system's behavior for each service. It may contain restrictions on network flows, guidelines for flows' prioritization, and instructions about how to report flows.

Each subscriber in the network is provided a reference to a package to which that subscriber belongs. The system:

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 subscriber's network ID (usually the subscriber's IP address)
3. Identifies the package to which the subscriber belongs
4. Applies the correct rule to the service of the subscriber's network flow

Another scheme is described in Virtual Links Mode, page 3-13.

Virtual Links Mode

In normal mode, you define bandwidth controllers for each package (see Bandwidth Management, page 3-14). 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 subscriber's package and the direction of the virtual link.

For more information, see Managing Virtual Links, page 9-44.

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 its packet's DSCP ToS marked with a given value (see DSCP ToS Marking, page 3-19)
- Define an aggregate volume or session limit, after which a set of different restrictions will be enforced on the flow
- Specify how a flow will be 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 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 will only apply 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 will 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.

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 sitting next 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 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

Total bandwidth use is controlled by global controllers. 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 desired percentage of the total available bandwidth. 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, 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 3-13.)

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 Virtual Links, page 9-44.)

Subscriber Bandwidth Control

Bandwidth used by individual subscribers is controlled by Subscriber BW Controllers (BWCs). Each BWC controls available bandwidth for selected services. Services controlled by a particular BWC are defined per package, but bandwidth control is per service.

A BWC is specified by the following parameters:

- Committed Information Rate (CIR)—The minimum bandwidth that must be granted to the services that are controlled by the BWC
- Peak Information Rate (PIR)—The maximum bandwidth that can be allocated to the services that are controlled by the BWC

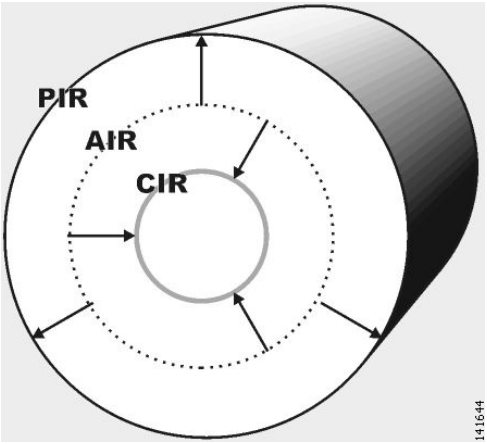
- Global Controller—The global controller to which this BWC links
- Assurance Level (AL)—The rate of change of available bandwidth under conditions of traffic congestion

As illustrated in Figure 3-3, 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, the AIR is determined by a third parameter—Assurance Level (AL). 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



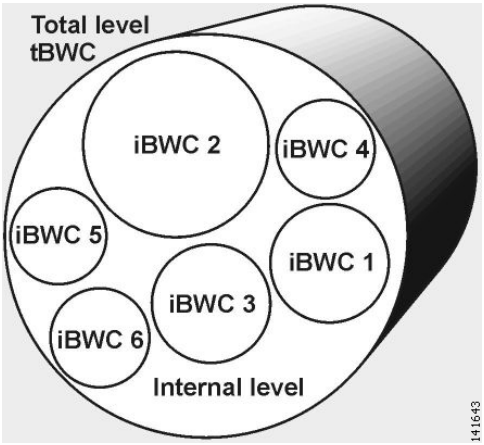
Bandwidth may be thought of in terms of a virtual pipe of adjustable width. The PIR is the maximum allowed width of the virtual pipe. The CIR is the minimum width to which the pipe can contract. The actual pipe width is the AIR. During network congestion, the system contracts each pipe differently to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

Primary and Internal Bandwidth Control

In 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 (see the *Cisco SCMS SCE Subscriber API Programmer's Guide)* to dynamically modify the quota in each bucket. 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.

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 the *Cisco Service Control Management Suite Quota Manager Solution Guide*.

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

The internal 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 SCA BB.

- Service Security, page 3-17
- Traffic Filters, page 3-19
- Traffic Forwarding to Value Added Services Servers, page 3-19

Service Security

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 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

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 SCA BB will identify 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 SCE platform's stateful Layer 7 capabilities are used to detect malicious activity that is not easily detectable by the other mechanisms. Operators can add signatures for such threats, achieving a very quick response time in addressing new threats.

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.

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. They allow you to instruct the SCE platform to ignore some types of flow (based on the flow's Layer 3 and Layer 4 properties) 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 will 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 3-19.)

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 flow's Layer 7 characteristics.

DSCP ToS Marking

DSCP ToS marking is used in IP networks to signal the type and priority of a flow between network elements. DSCP ToS marking is typically performed by elements that have an insight regarding how traffic should be treated throughout the network. Such an element can be the element generating traffic—a voice gateway, for example. 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 provider's business strategy and vision.

A service configuration can take effect only after it is propagated to the appropriate SCE platform. 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 serviceconfiguration.
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

This module:

- Guides you through the process of installing or upgrading the Cisco Service Control Application for Broadband (SCA BB)
- Explains how to install Protocol Packs, which contain new and updated protocol signatures
- Describes the concept of the Console as a collection of tools, presents each tool and its role, and describes how to launch the tools and navigate between them
- Concludes with a Quick Start that describes how to apply your first service configuration and generate your first report

How to Install SCA BB

You install SCA BB in two stages:

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

If you are upgrading an existing installation of SCA BB, see How to Upgrade from Release 2.5 to Release 3.1.6, page 4-8 or How to Upgrade from Release 3.0.x to Release 3.1.6, page 4-8.

The SCA BB Installation Package

The 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 platform:
  - A PQI file for each type of SCE platform. Each PQI file is located in a subfolder whose name is the platform name.
  - A PQI file for the SM, located in the SM subfolder.
- The file scas_bb_util.tgz, which contains the files for the SCA BB Service Configuration Utility (**servconf)**, the SCA BB Signature Configuration Utility (**sigconf)**, and the SCA BB Real-Time Monitoring Configuration Utility (**rtmcmd)** (together with real-time monitoring report templates).
- The file PCubeEngageMib.mib, which defines the SCAS BB MIB, located in the SNMP subfolder.
- The 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 SCA BB Application Components

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

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

SCA BB also has one software component that resides on the SM device:

- The SCA BB SM 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 5-22 and How to Install PQI Files on SM Devices, page 5-26.

To install these components from a command line, see Installing PQI Files from the Command Line, page 13-10.

Prerequisites

Before installing SCA BB, verify that the SCE platform and, if used, the SCMS-SM 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 SM is Correctly Installed, page 4-3
- How to Verify that an Appropriate Version of the SM is Running, page 4-3

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 SM is Correctly Installed

Step 1 Open a Telnet session to the SM.

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

Step 3 Press **Enter.**

The response to this command displays the operational status of the SM.

How to Verify that an Appropriate Version of the SM is Running

Step 1 Open a Telnet session to the SM.

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

Step 3 Press **Enter.**

The response to this command displays the SM version.

How to Install SCA BB Front Ends

You should install the following SCA BB front ends:

- The Console
- The SCA BB Service Configuration Utility (**servconf)**, the SCA BB Signature Configuration Utility (**sigconf)**, and the 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 or Windows XP.

Installing the Java Runtime Environment

The SCA BB Service Configuration Utility, **servconf,** requires access to JRE version 1.4 or 1.5.

You can download a JRE from the Sun™ website at http://java.sun.com/j2se/1.4.2/download.html.

To verify that the JRE is installed, run **java -version** from the command prompt. The Java version should start with 1.4 or 1.5.

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 1.4 installation directory. For example:

```
JAVA_HOME=C:\Program Files\Java\j2re1.4.2_08
```

How to Install the Console

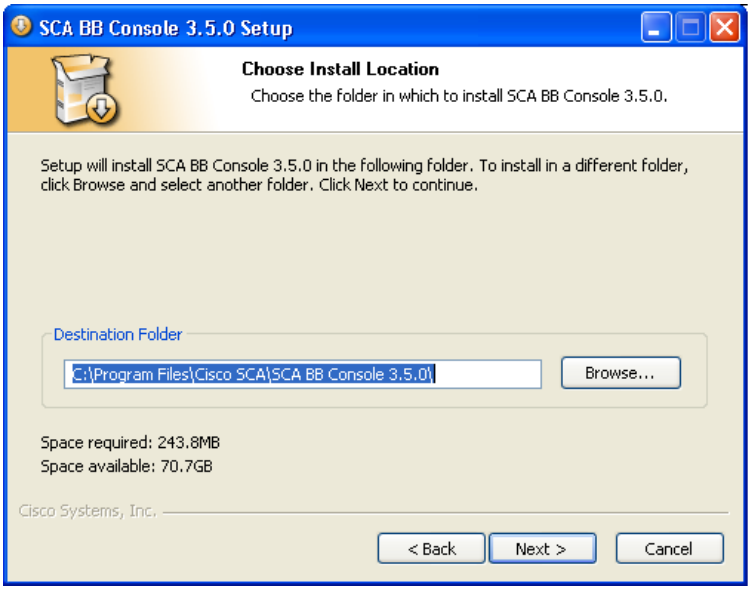
Step 1 Navigate to the Console installation file, sca-bb-console-3.1.6.exe, and double-click it.

The Welcome page of the SCA BB Console 3.1.6 Setup wizard appears.



Step 2 Click **Next.**

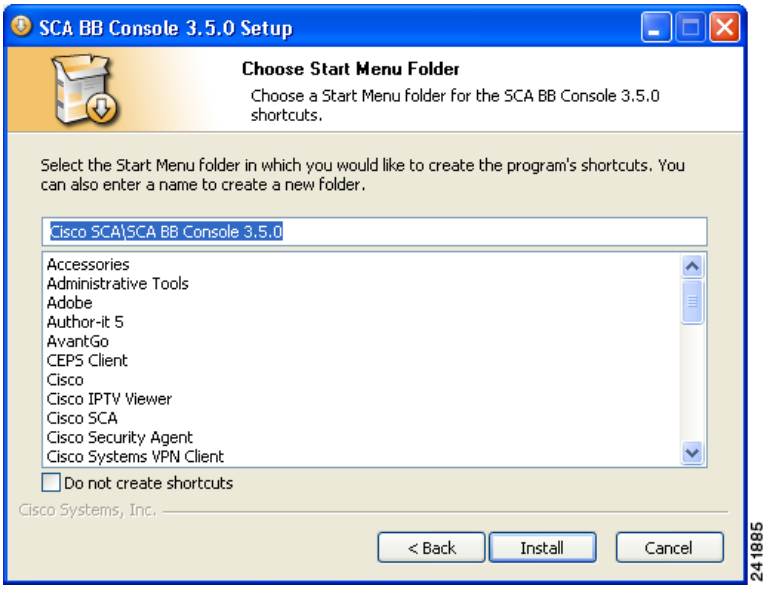
The Install Location page of the Setup wizard opens.



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.

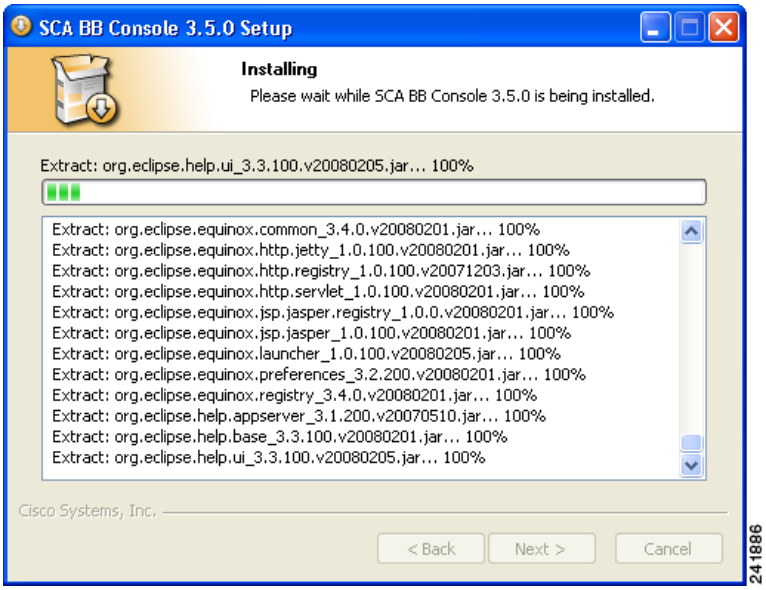


Step 5 (Optional) Enter a different Start Menu folder in the Start Menu Folder field.

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

Step 7 Click **Install.**

The Installing page of the Setup wizard opens.



Step 8 Wait until installation is complete.

The Next button is enabled.

Step 9 Click **Next.**

The Installation Complete page of the Setup wizard opens.



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

Step 11 Click **Finish.**

The SCA BB Console 3.1.6 Setup wizard closes.

The Console is now installed on the machine.

A shortcut is added to the Start menu.

How to Install the SCA BB Configuration Utilities

Step 1 From the SCA BB installation package, extract the file scas_bb_util.tgz, and copy it to a Windows, Solaris, or Linux workstation.

Step 2 Unpack the file to a new folder.

The SCA BB Service Configuration Utility (**servconf)**, the SCA BB Real-Time Monitoring Configuration Utility (**rtmcmd)** (and associated real-time monitoring report templates), and the SCA BB Signature Configuration Utility (**sigconf)** are located under the bin folder.

How to Upgrade SCA BB

Upgrading SCA BB includes upgrading each of the following software components:

- The Console
- The SCE PQI file
- The SM PQI file

Note This section describes the upgrade of 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
```

- New SCA BB releases do not use the default Dynamic Signature Script (DSS) file (see The Default DSS File, page 7-39) that was installed for a previous 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 from Release 2.5 to Release 3.1.6

Step 1 Using a SCAS BB 2.5 Console, retrieve the service configuration (PQB) from the SCE platform, and save it to the local hard disk.

Note The upgrade procedure does not require uninstalling the SCAS BB 2.5 Console.

Step 2 Install the SCA BB 3.1.6 Console. (See How to Install the Console, page 4-4.)

Step 3 Open the SCA BB 3.1.6 Console.

Step 4 Use the Network Navigator tool to install a release 3.1.6 SCE PQI file on the SCE platform:

- **a.** Create an SCE device in the Network Navigator tool. (See Managing Sites, page 5-2.)
- **b.** Install the PQI file. (See Managing SCE Devices, page 5-7.)
- **c.** Verify that the installation was successful by retrieving the SCE platform's online status. (See Managing SCE Devices, page 5-7.)

Step 5 If your system includes an SM, use the Network Navigator tool to install a release 3.1.6 SM PQI file on the SM device:

- **a.** Create an SM device in the Network Navigator tool. (See Managing Sites, page 5-2.)
- **b.** Install the PQI file. (See How to Install PQI Files on SM Devices, page 5-26.)

Step 6 Using the 3.1.6 Service Configuration Editor tool, open the service configuration saved in Step 1.

Step 7 Check the release notes for a list of new signature-based protocols, and manually assign these protocols to a service.

When you upgrade old PQB files, new signature-based protocols are not assigned to any service (and are therefore classified as Generic TCP).

Step 8 Apply the service configuration to the SCE platform.

How to Upgrade from Release 3.0.x to Release 3.1.6

Step 1 Using a SCA BB 3.0.x Console, retrieve the service configuration (PQB) from the SCE platform, and save it to the local hard disk.

Note The upgrade procedure does not require uninstalling the SCA BB 3.0.x Console.

Step 2 Install the SCA BB 3.1.6 Console. (See How to Install the Console, page 4-4.)

Step 3 Open the SCA BB 3.1.6 Console.

Step 4 Use the Network Navigator tool to install a release 3.1.6 SCE PQI file on the SCE platform:

- **a.** Create an SCE device in the Network Navigator tool. (See Managing SCE Devices, page 5-7.)
- **b.** Install the PQI file. (See How to Install PQI Files on SCE Devices, page 5-22.)
- **c.** Verify that the installation was successful by retrieving the SCE platform's online status. (See How to Retrieve the Online Status of SCE Devices, page 5-17.)

Step 5 If your system includes an SM, use the Network Navigator tool to install a release 3.1.6 SM PQI file on the SM device:

a. Create an SM device in the Network Navigator tool. (See How to Add SM Devices to a Site, page 5-4.)

b. Install the PQI file. (See How to Install PQI Files on SM Devices, page 5-26.)

Step 6 Using the 3.1.6 Service Configuration Editor tool, open the service configuration saved in Step 1.

Step 7 Check the release notes for a list of new signature-based protocols, and manually assign these protocols to a service.

When you upgrade old PQB files, new signature-based protocols are not assigned to any service (and are therefore classified as Generic TCP).

Step 8 Apply the service configuration to the SCE platform.

How to Upgrade the SCA BB Service Configuration Utility

Step 1 Install the new version of the SCA BB Service Configuration Utility, **servconf,** in an empty directory.

See How to Install the SCA BB Configuration Utilities, page 4-7.

How to Reconfigure DSCP Marking for Release 3.1.5 and Higher

If you have used DSCP marking on a SCA BB release prior to 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.



Note There are no backward compatibility issues *at the functional level*; the following steps allow you to maintain the same system behavior when upgrading to release 3.1.6.



Note All CLI commands pertaining to DSCP marking were removed in release 3.1.5. It is recommended that you manually remove these commands from the SCE startup-config file after you upgrade. If you do not remove these commands, errors will be displayed on system startup; these errors do *not* affect functionality.

Step 1 Enable DSCP marking on relevant interfaces. (See How to Manage DSCP ToS Marker Values, page 9-28.)

Step 2 Configure the values you want to use for marking in the DSCP marking table. Use the values you originally assigned for the SCE CoS classes in the pre-3.1.5 DSCP marking CLI configuration. (See How to Manage DSCP ToS Marker Values, page 9-28.)

Step 3 For each service rule of each package, enable DSCP marking as required and select the DSCP value that corresponds to the CoS you used for this service. For example, for each rule assigning a service to CoS BE, you would have to select the corresponding DSCP value that you set in the DSCP marking table for upstream and downstream marking. (See How to Define Per-Flow Actions for a Rule, page 9-14.)

Step 4 For each filter rule, enable DSCP marking as required, and select the DSCP value that corresponds to the CoS you used for this service. For example, for each rule assigning a service to CoS BE, you would have to select the corresponding DSCP value that you set in the DSCP marking table for upstream and downstream marking. (See How to Edit Filter Rules, page 10-26.)

Working with Protocol Packs

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

When a traffic flow is handled by the system, it 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 SCA BB.

In order to enable rapid response to the ever-changing protocol environment, 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 system's protocol support without compromising the stability of the system (no update of an existing software component is required) and without any service downtime.

- Protocol Packs, page 4-10
- Installing Protocol Packs, page 4-11
- How to Verify Version Compatibility for Protocol Packs, page 4-11
- How to Verify the Installation of a Protocol Pack, page 4-12
- Hitless Upgrade of the SLI, page 4-12

Protocol Packs

Periodically, Cisco publishes protocol packs containing new and improved protocol signatures for 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 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 SCA BB may be either a DSS file or an SPQI file:

- Loading a DSS file to the SCE platform requires no downtime of 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 4-12) 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 SCA BB Service Configuration Utility, page 13-1
- The Network Navigator tool (see How to Install a Protocol Pack, page 5-17)

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 4-12.)

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 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 12-4)—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 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 4-13.

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, you should verify that the protocol pack version matches the SCE application version. For example, only use a protocol pack for 3.1.6 on SCE application version 3.1.6.

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

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 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 4-11).
- 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 13-1).

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

Hitless Upgrade of the SLI

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

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

If hitless upgrade is enabled, classification, reporting, and control continue uninterrupted when you install an SPQI file (see Working with Protocol Packs, page 4-10). You can install SPQI files using either the Console or **servconf,** the SCA BB Service Configuration Utility. An SPQI file is a package that includes the required (SLI) files.

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. In order to make the hitless upgrade process bounded, you can set criteria that will trigger 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 no old flows are killed by the application before one hour passes.

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 the *Cisco Service Control Engine (SCE) 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 (see How to Enter Line Interface Configuration Mode, page 4-14) and see the `SCE(config if)#` prompt displayed.

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.
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 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

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

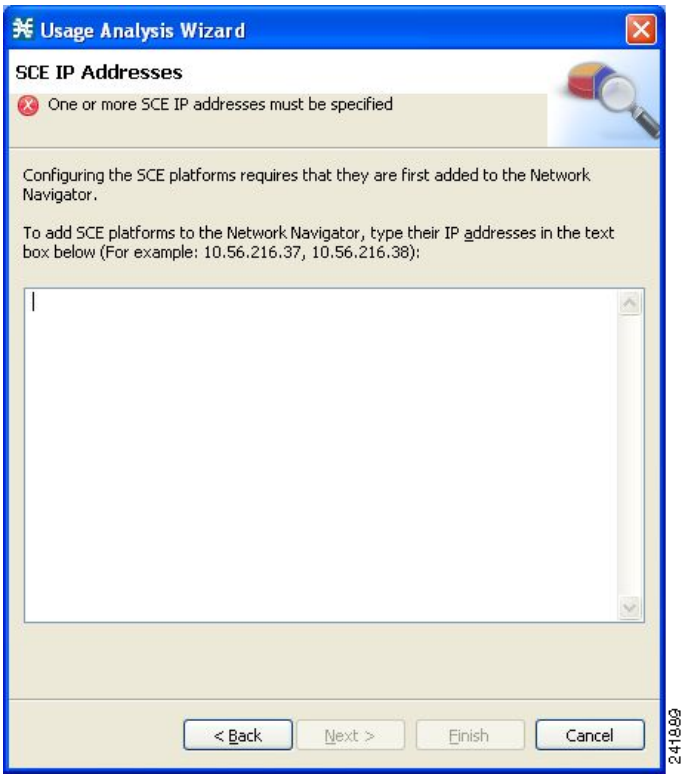
Step 1 Choose **Start > All Programs > Cisco SCA > SCA BB Console 3.1.6 > SCA BB Console 3.1.6.**

The Cisco Service Control SCA BB Console splash screen appears.



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

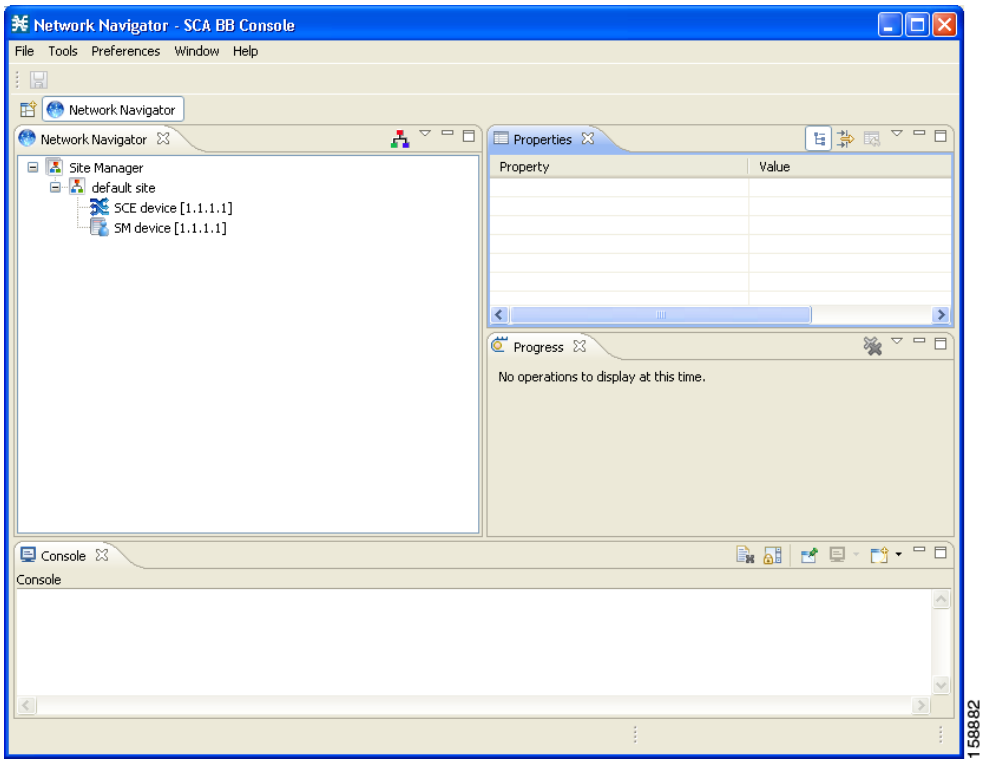
The first time that you launch the Console, the Welcome view is open in the main window



Step 2 Close the Welcome view.

Click **Go to the console.**

The Welcome view closes. The Network Navigator tool is open in the Console.



Note When you close the Console, it will remember which tools are open, which is the active tool, and whether the Welcome view is displayed, and apply this the next time you launch the Console.

How to Use the Console

The Console is the front end of 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
- Reporter tool

The Console GUI has a menu bar and a standard toolbar (see Figure 4-1). 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 4-1 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 4-17
- The Network Navigator Tool, page 4-51
- The Service Configuration Editor Tool, page 4-52
- The Signature Editor Tool, page 4-54
- The Subscriber Manager GUI Tool, page 4-55
- The Reporter Tool, page 4-56
- Online Help, page 4-57

Configuration Wizards

Four configuration wizards are available from the Welcome view (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 DB Configuration wizard—Connects the 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 or VLANs are treated as subscribers.

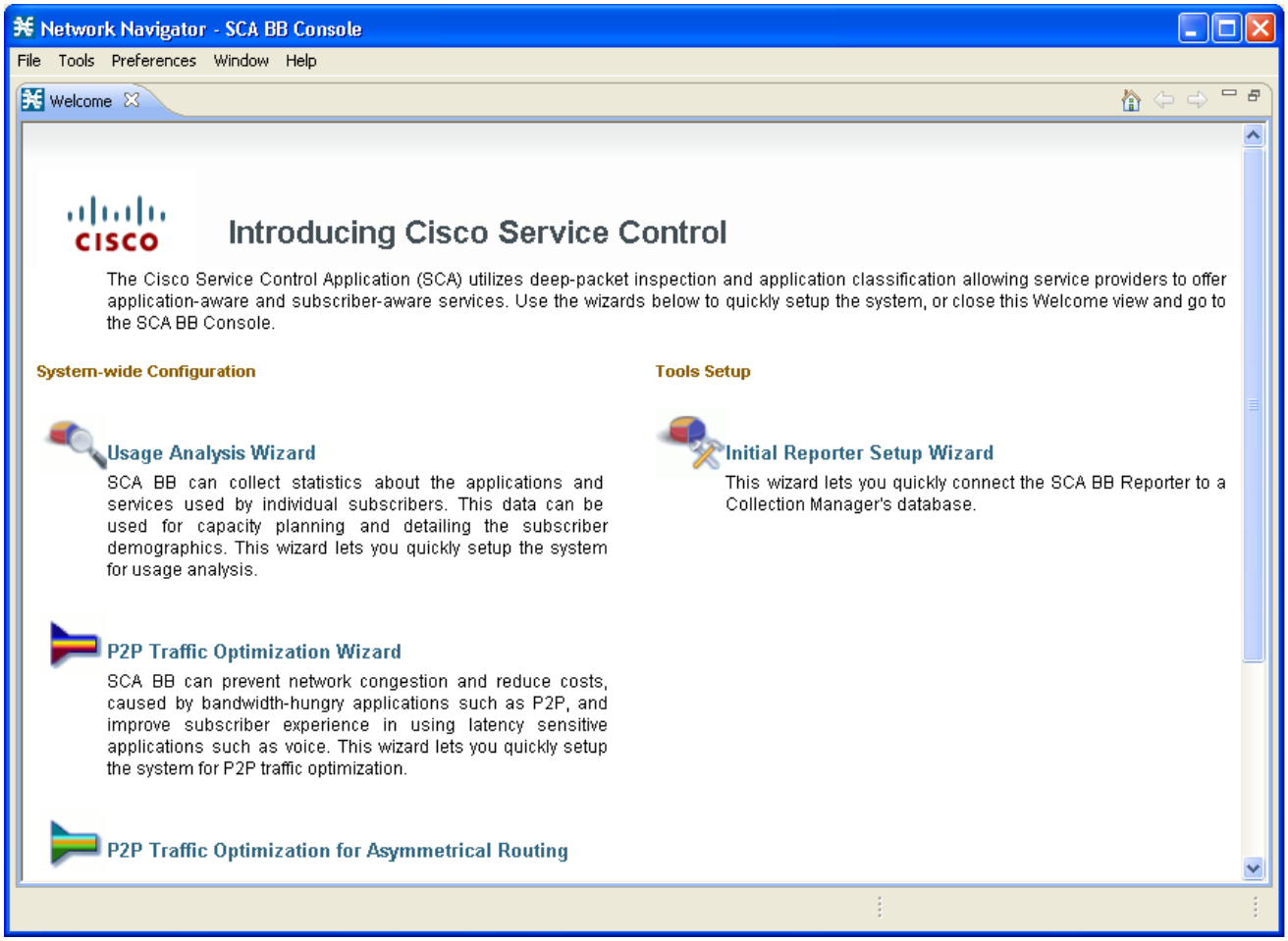
How to Use the Usage Analysis Wizard

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

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

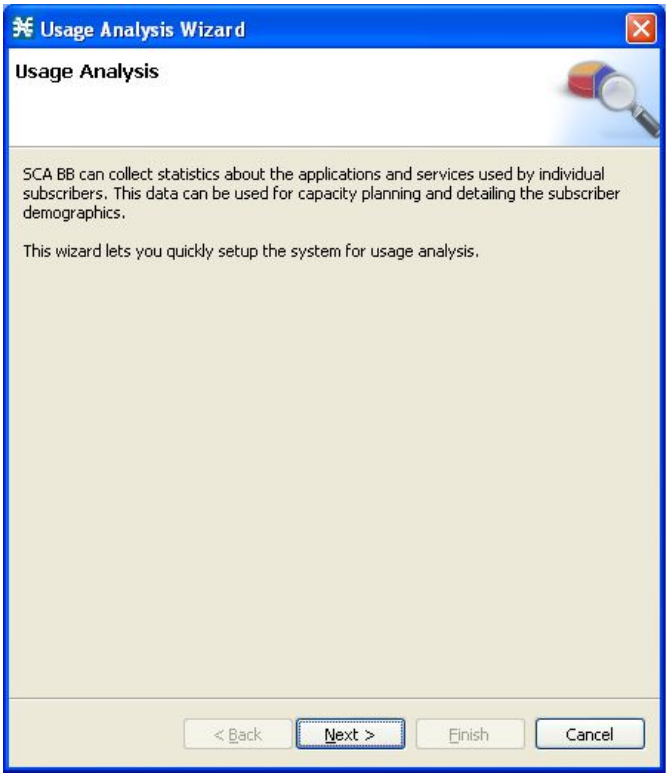
Step 1 From the Console main menu, choose **Help > Welcome.**

The Welcome view opens.



Step 2 Click **Usage Analysis Wizard.**

The Welcome page of the Usage Analysis wizard appears.

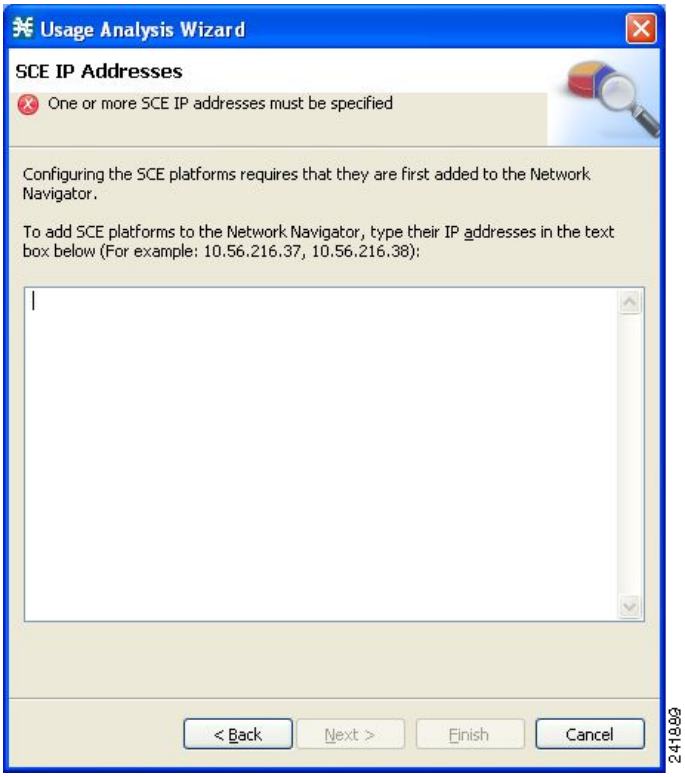


Note You can also execute the Usage Analysis wizard from the Network Navigator tool:

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.



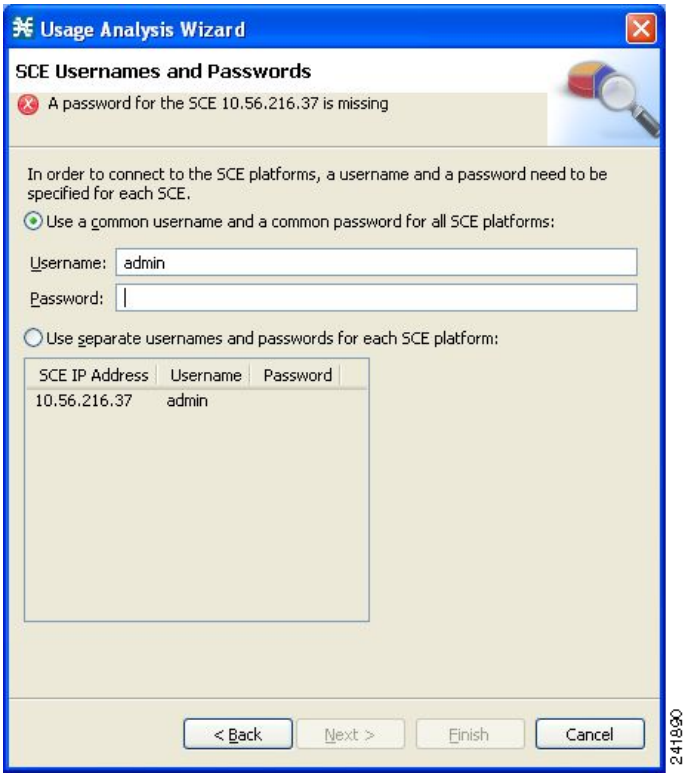
Step 4 In the edit box, enter the IP addresses of the SCE devices that should be added to the model.

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.



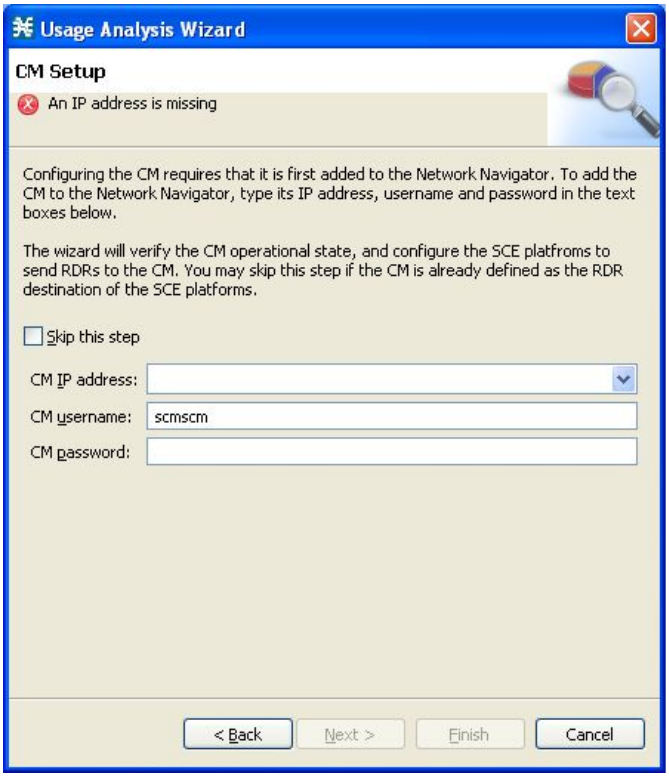
Step 6 Enter the user names and passwords for the SCE devices.

Do one of the following:

- To use the same user name and password for all the SCE devices that you are adding, enter the user name in the Username field and the password in the Password field
- To provide a different user name 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 user name and password in the appropriate cell of the table.

Step 7 Click **Next.**

The CM Setup page of the Usage Analysis wizard opens.



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

Do one of the following:

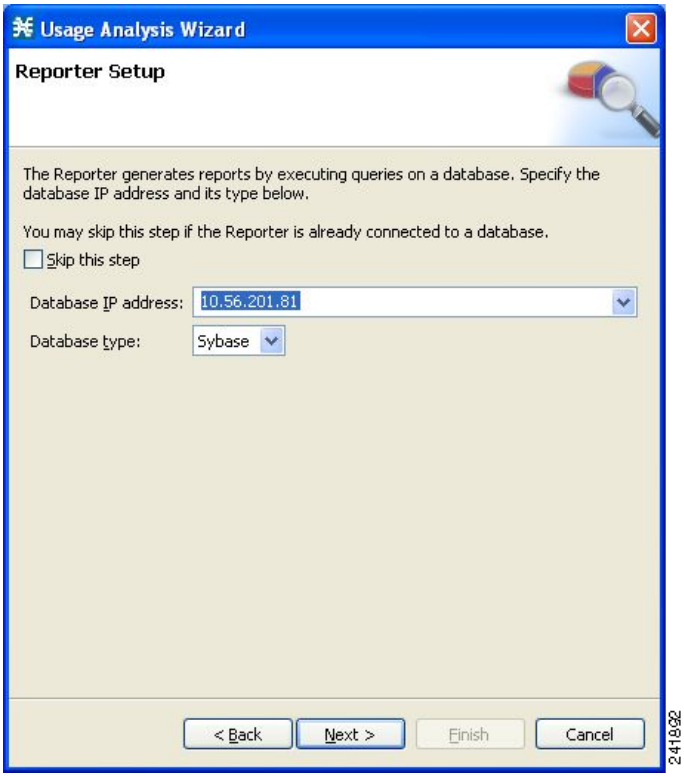
- Enter the IP address, user name, and password of the CM device in the appropriate fields.

  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.



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

Do one of the following:

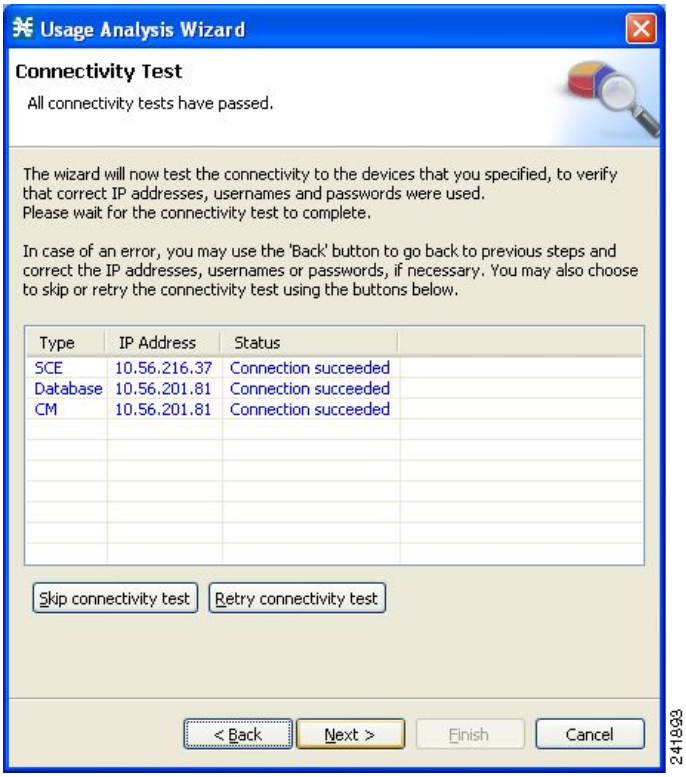
- Enter the IP address of the database and select the database type.

  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.

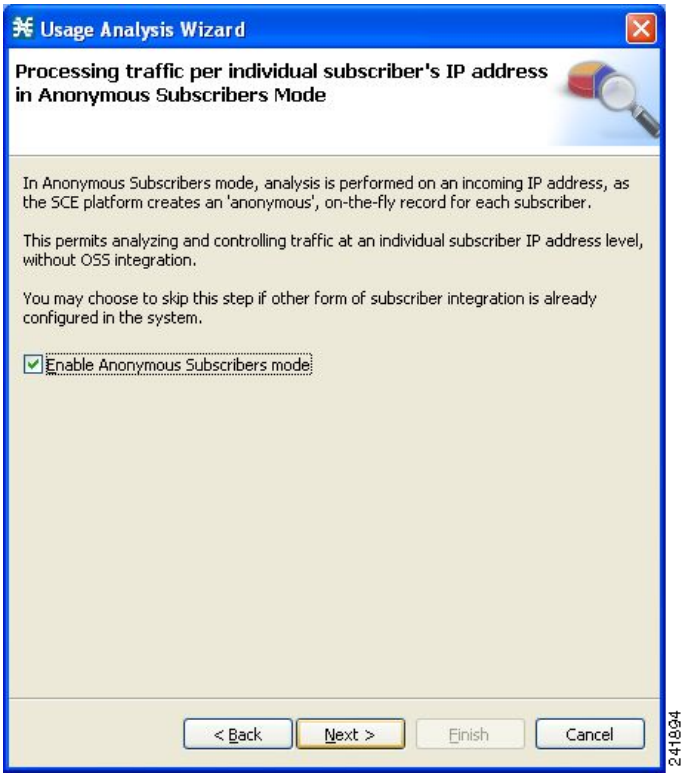


The wizard tests to see that the connections to the defined devices can be made.

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 will be validated when you click **Finish** at the end of the wizard.

Step 12 Click **Next.**

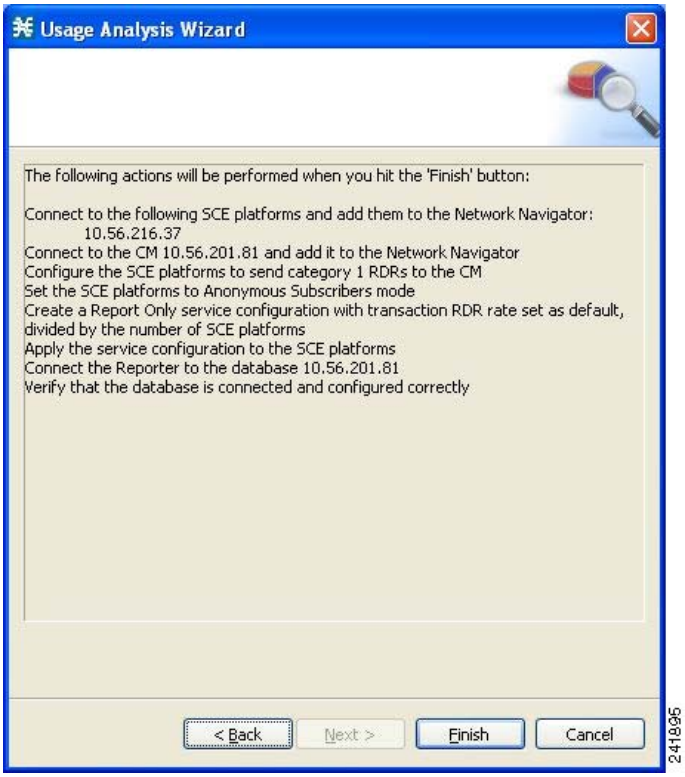
The Anonymous Subscribers page of the Usage Analysis wizard opens.



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

Step 14 Click **Next.**

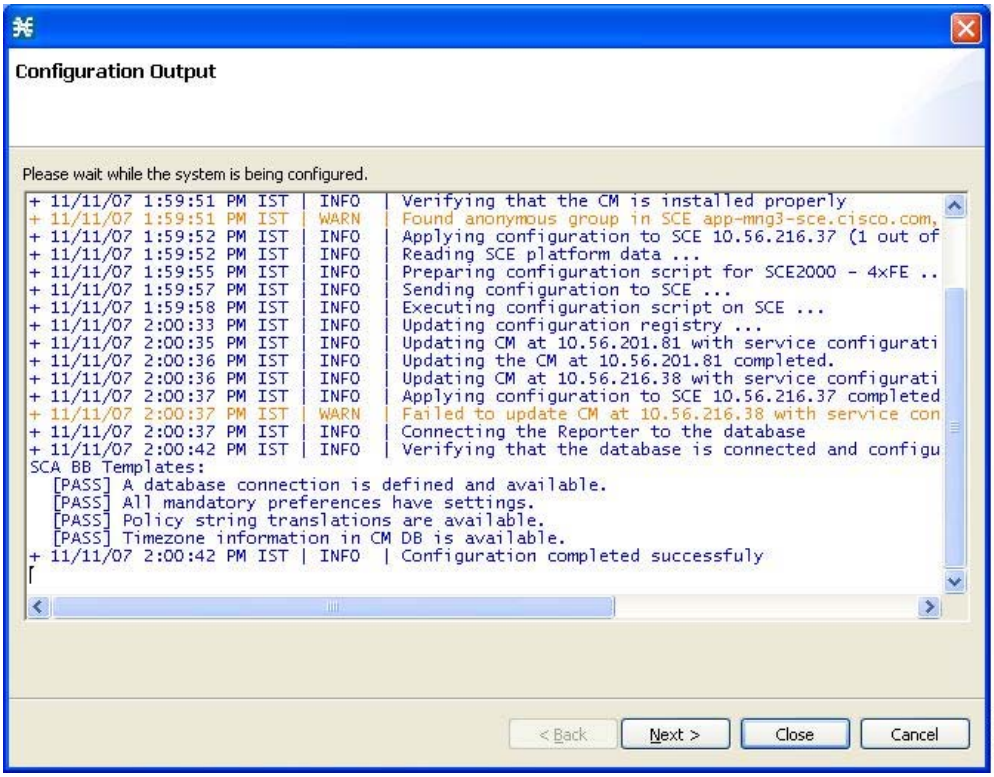
The Confirmation page of the Usage Analysis wizard opens.



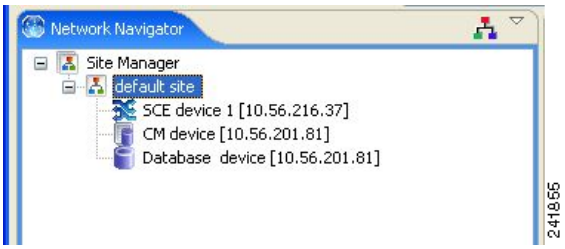
The actions that the wizard is about to take are listed in the page.

Step 15 Click **Finish.**

The Configuration Output page of the Usage Analysis wizard opens.



New devices are added to the default site of the Site Manager tree in the Network Navigator.



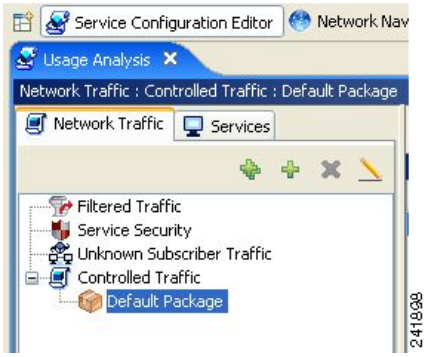
The wizard attempts to connect to all devices that you defined. The operation fails if:

- 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 the "Raw Data Formatting: The RDR Formatter and NetFlow Exporting" chapter of the *Cisco Service Control Engine (SCE) Software Configuration Guide*.

A new service configuration named Usage Analysis is created, and opens in the 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 8-4; the content and structure of the Transaction RDR is listed in "Transaction RDR" in the "Raw Data Records: Formats and Field Contents" chapter of the *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:

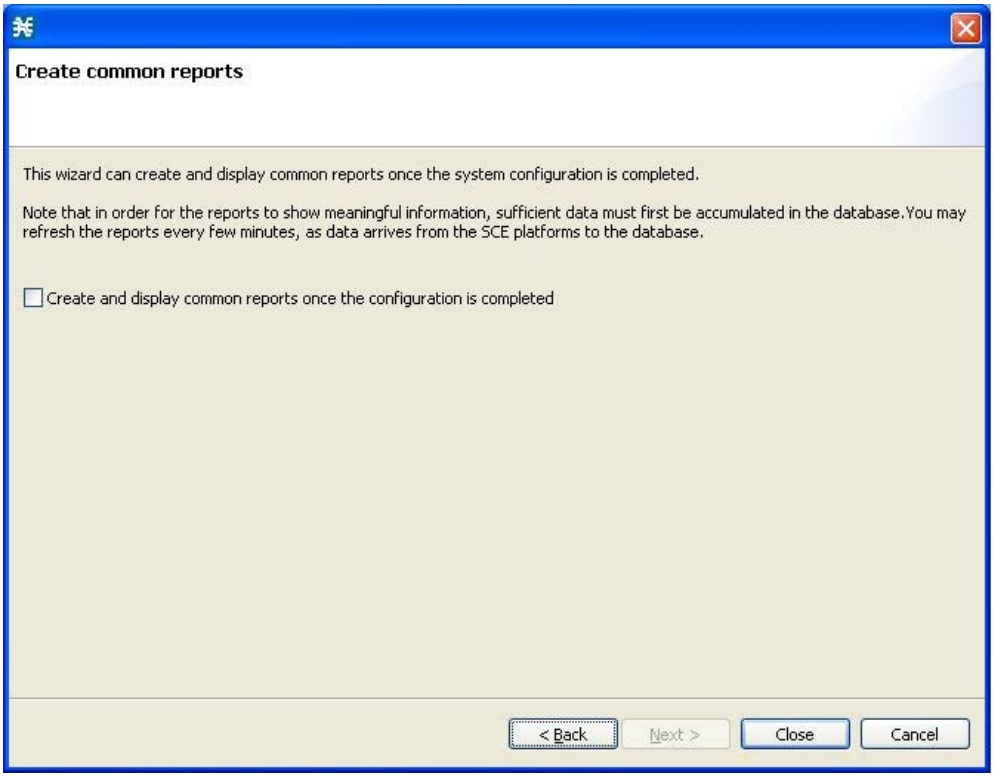
1. The SCA BB Reporter tool is connected to the selected database.
2. The first SCE platform entered in Step 4 is selected as the source of service configuration data.
3. The Next button is enabled.

Step 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.



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

Note Report instances will be 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:

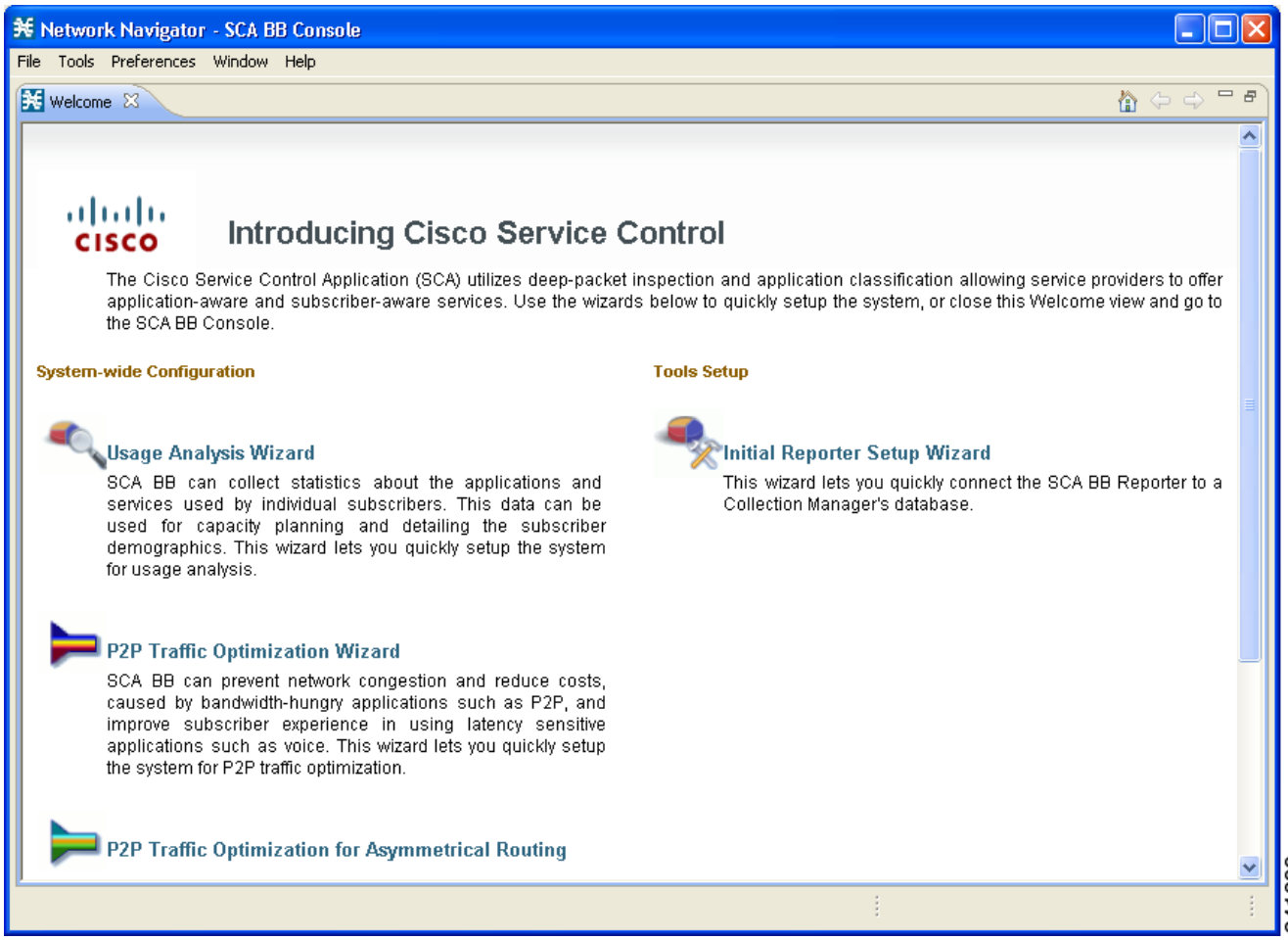
- The P2P Traffic Optimization wizard allows you to create a simple model of devices, connect to them, and limit P2P traffic to a specified percentage of total available bandwidth.

- 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 already exist, devices defined in the wizard are added to the default site in the Site Manager tree.

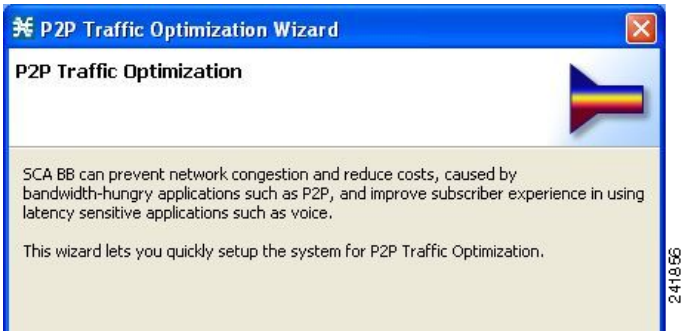
Step 1 From the Console main menu, choose **Help > Welcome.**

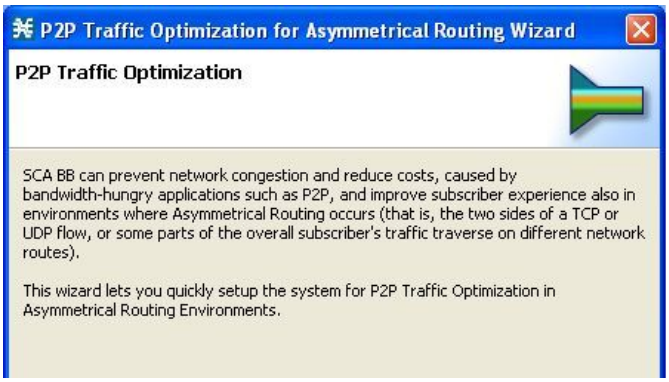
The Welcome view opens.



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

The Welcome page of the selected wizard appears:



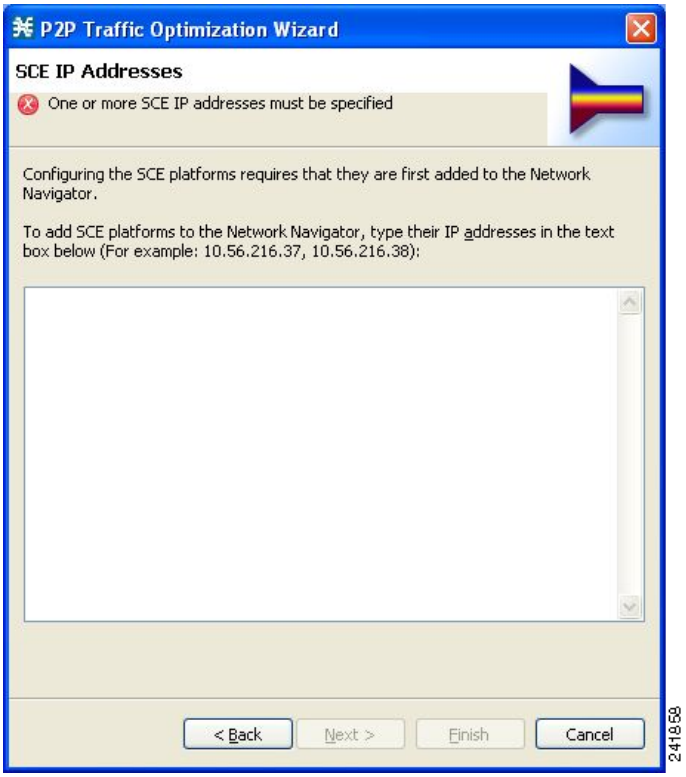


Note You can also execute the P2P Traffic Optimization wizard from the Network Navigator tool:

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, select **Configuration Wizards > P2P Traffic Optimization Wizard** or **Configuration Wizards > P2P Traffic Optimization for Asymmetrical Routing Wizard.**
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 P2P Traffic Optimization wizard opens.



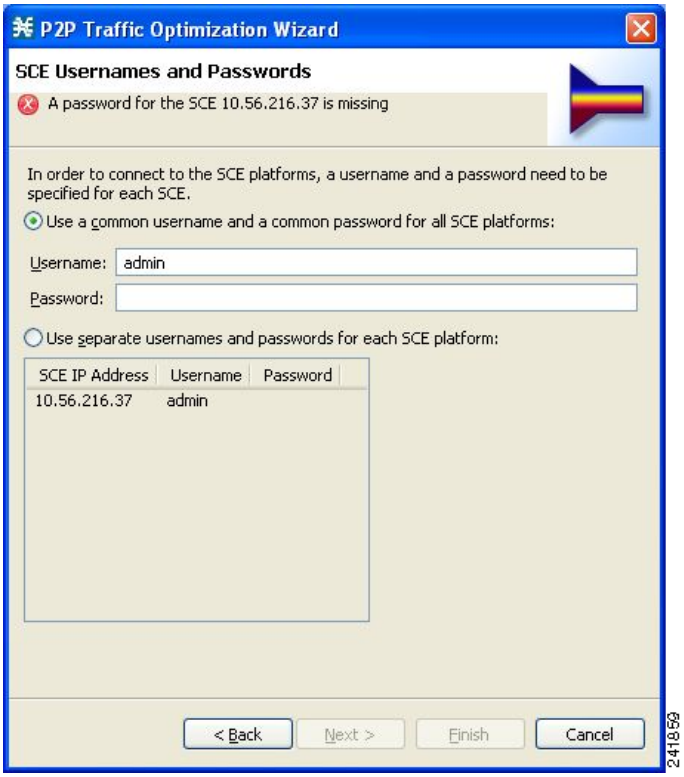
Step 4 In the edit box, enter the IP addresses of the SCE devices that should be added to the model.

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.



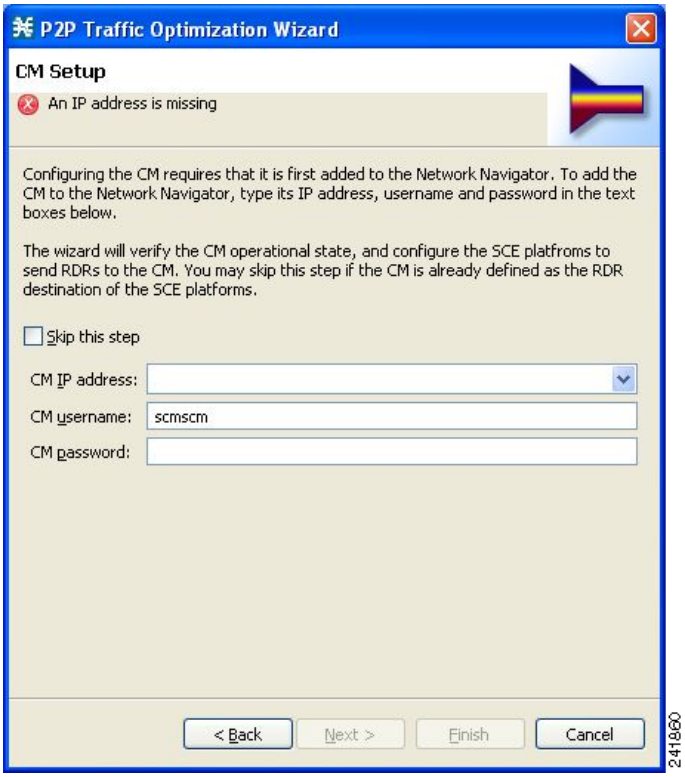
Step 6 Enter the user names and passwords for the SCE devices.

Do one of the following:

- To use the same user name and password for all the SCE devices that you are adding, enter the user name in the Username field and the password in the Password field.
- To provide a different user name 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 user name 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.



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

Do one of the following:

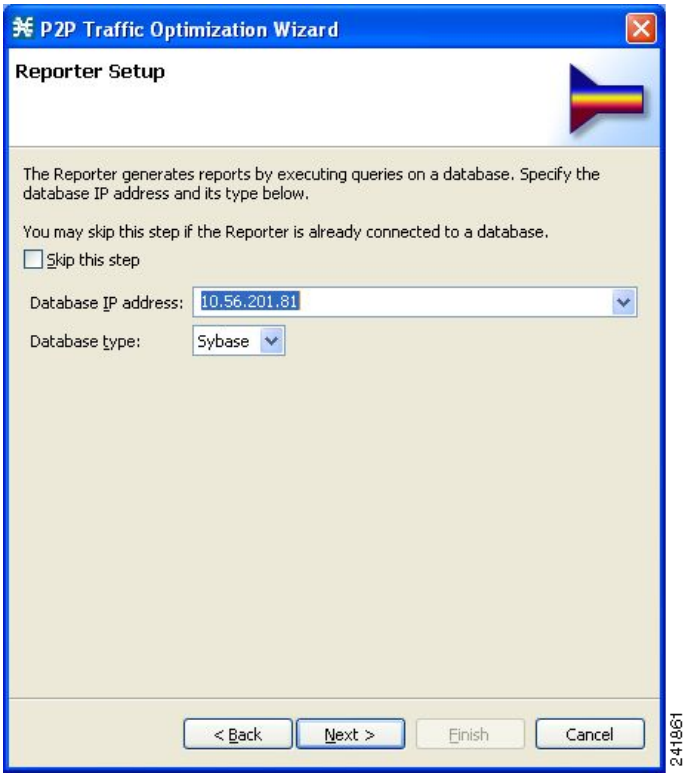
- Enter the IP address, user name, and password of the CM device in the appropriate fields.

  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.



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

Do one of the following:

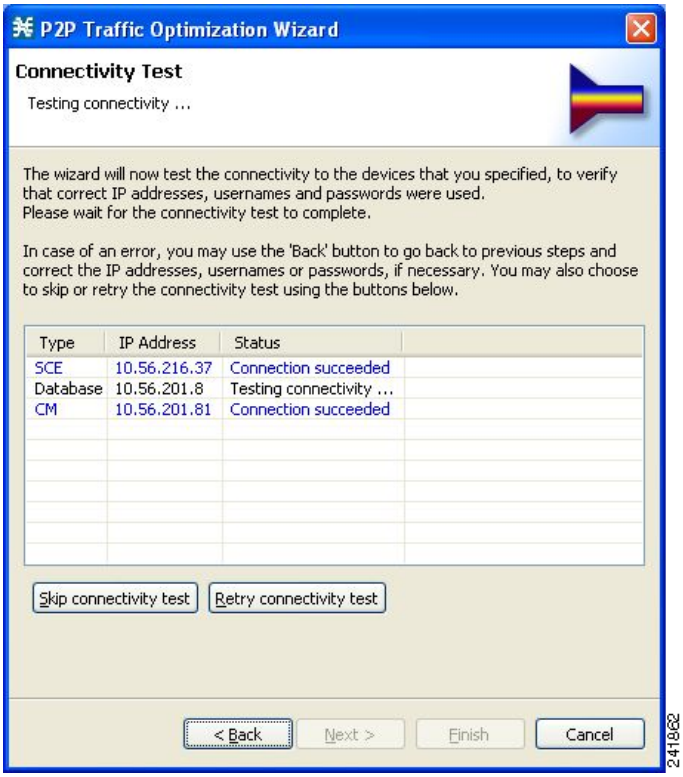
- Enter the IP address of the database and select the database type.

  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.

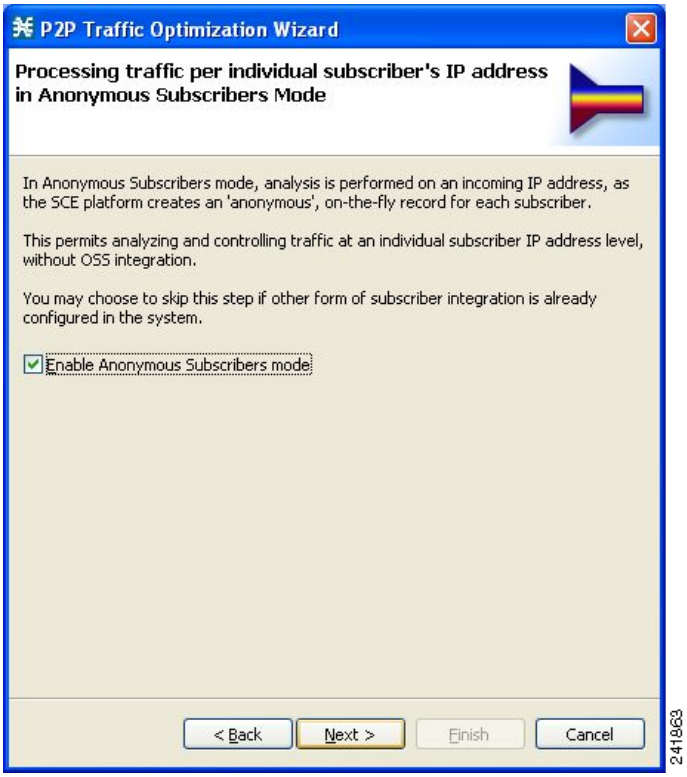


The wizard tests to see that the connections to the defined devices can be made.

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 will be validated when you click **Finish** at the end of the wizard.

Step 12 Click **Next.**

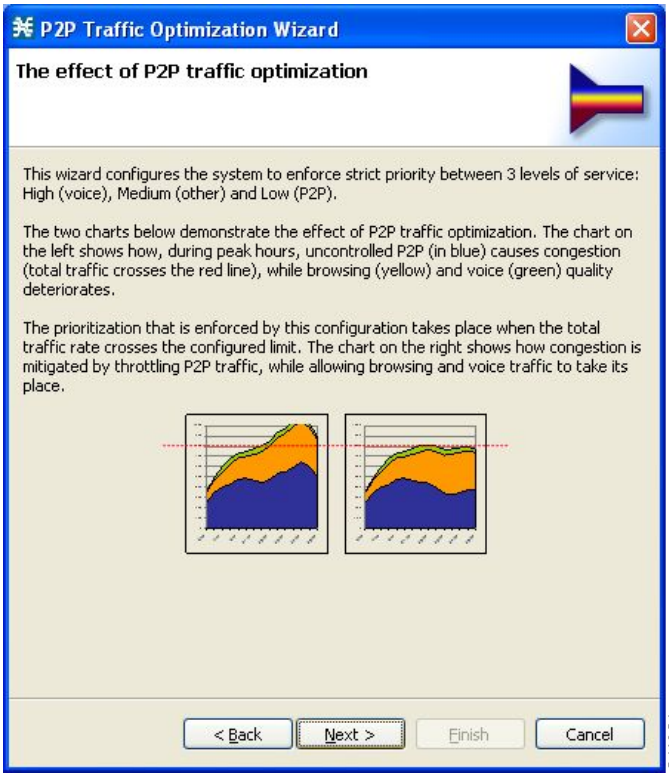
The Anonymous Subscribers page of the P2P Traffic Optimization wizard opens.



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

Step 14 Click **Next.**

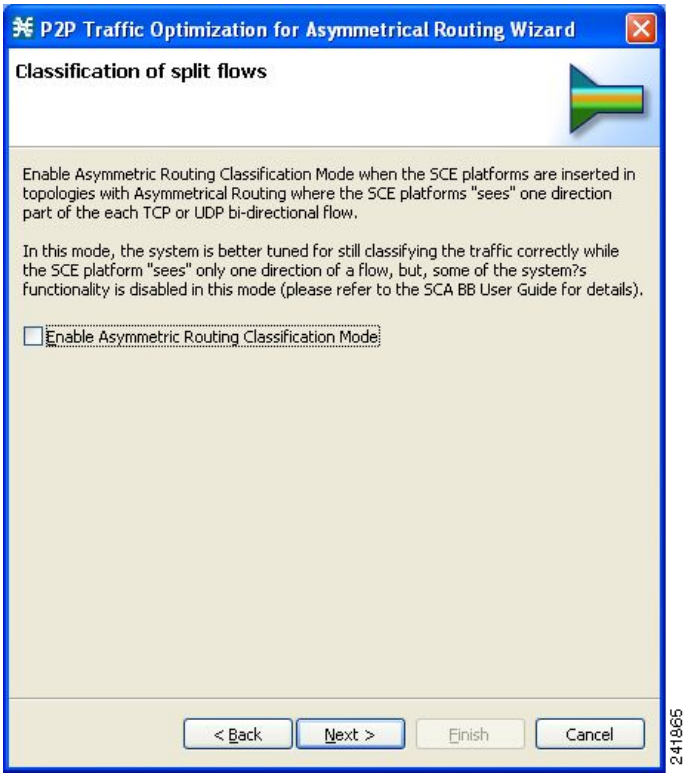
The effect of P2P traffic optimization page of the P2P Traffic Optimization wizard opens.



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.



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

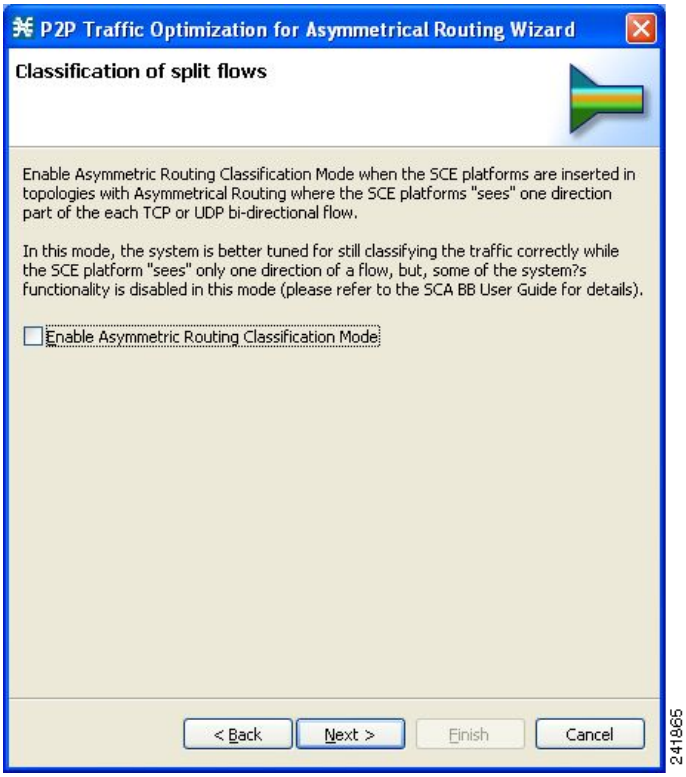
The scale of each slider is the percentage of the aggregated bandwidth of both links.

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.**

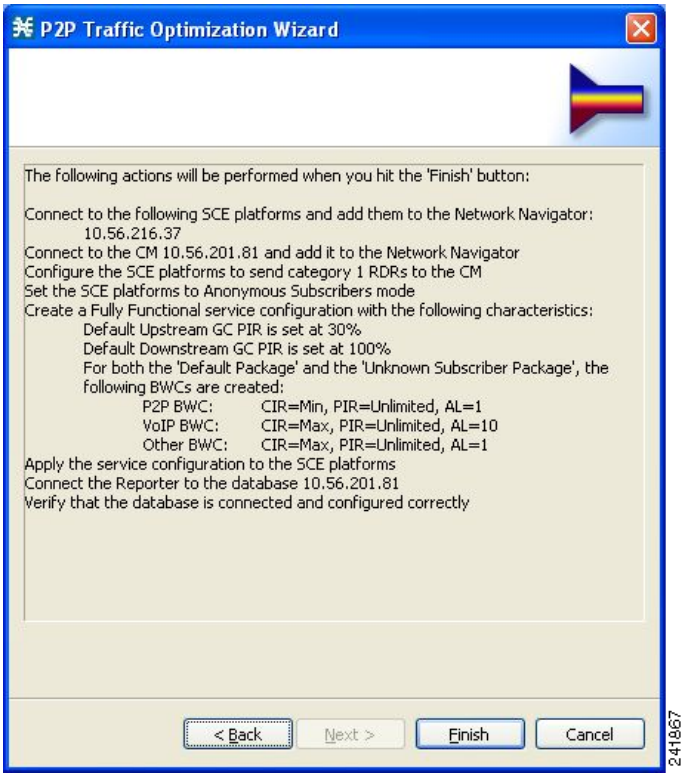
The Classification of split flows page of the P2P Traffic Optimization wizard opens.



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.

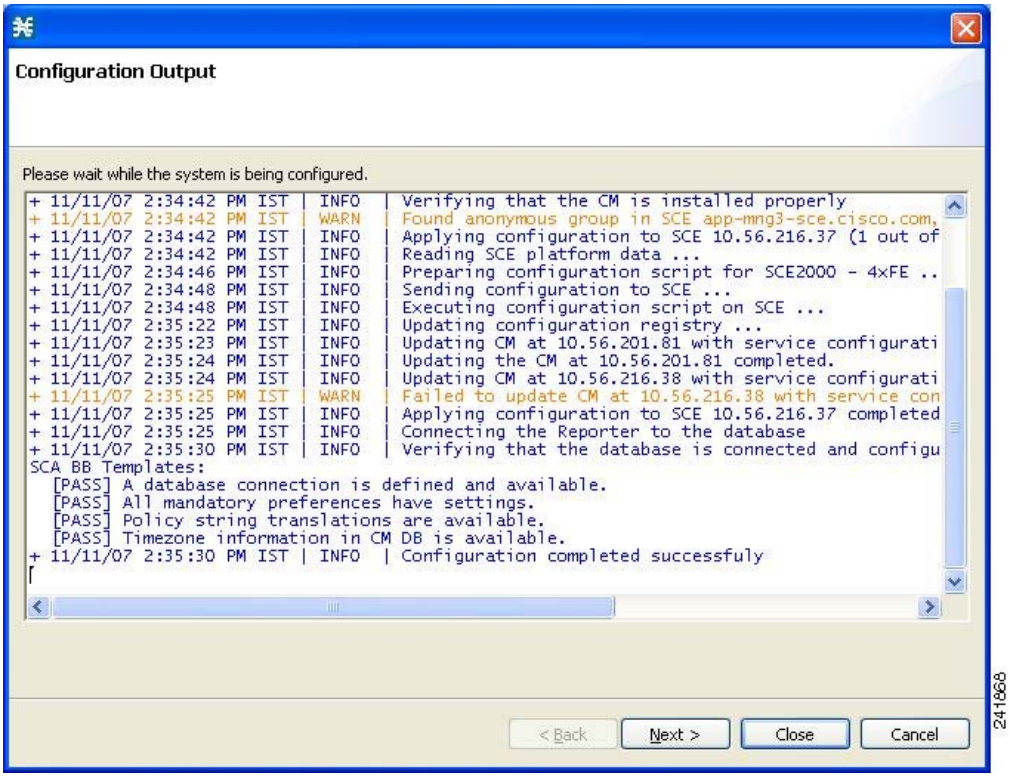


The actions that the wizard is about to take are listed in the page.

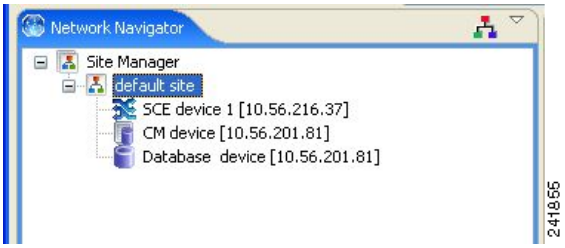
For an explanation of the bandwidth controller parameters, see Subscriber BWC Parameters, page 9-37.

Step 21 Click **Finish.**

The Configuration Output page of the P2P Traffic Optimization wizard opens.



New devices are added to the default site of the Site Manager tree in the 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 the "Raw Data Records: Formats and Field Contents" chapter of the *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.



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:
  - P2P

    CIR = 0

    PIR = <value set in global controller>

    AL = 1
  - VoIP

    CIR = <value set in global controller>

    PIR = <value set in global controller>

    AL = 10
  - P2P

    CIR = <value set in global controller>

    PIR = <value set in global controller>

    AL = 1

The service configuration is applied to the SCE devices.

If you defined a database in Step 10:

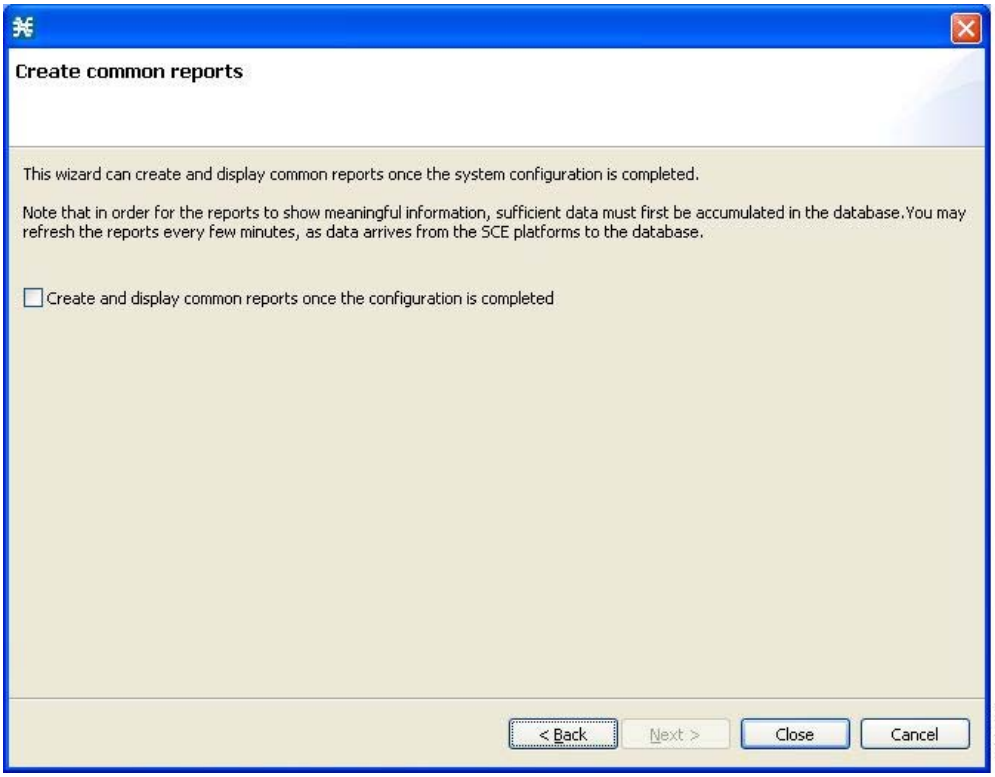
1. The SCA BB Reporter tool is connected to the selected database.
2. The first SCE platform entered in Step 4 is selected as the source of service configuration data.
3. The Next button is enabled.

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.



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

Note Report instances will be 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.

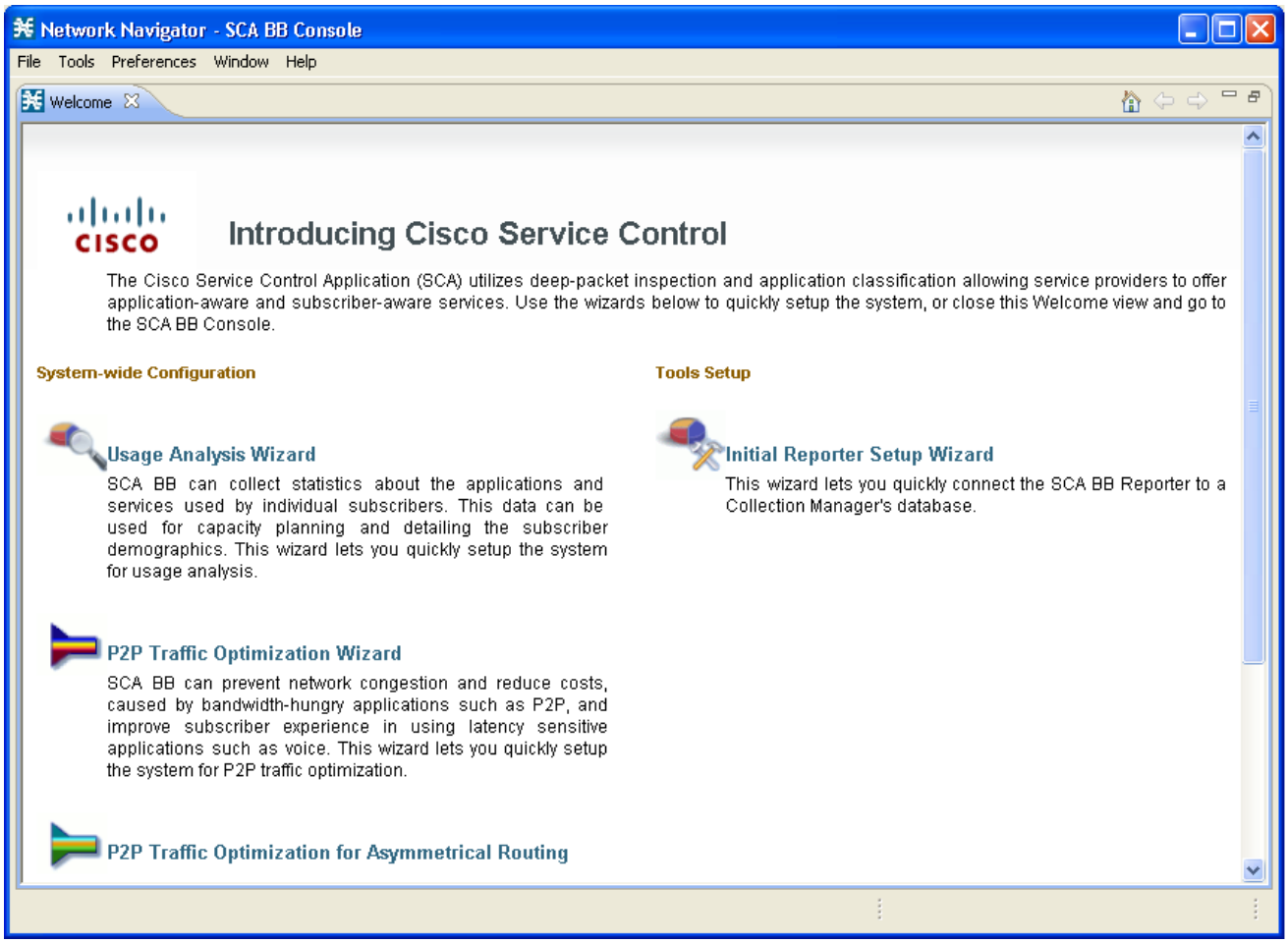
How to Use the Reporter DB Configuration Wizard

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.

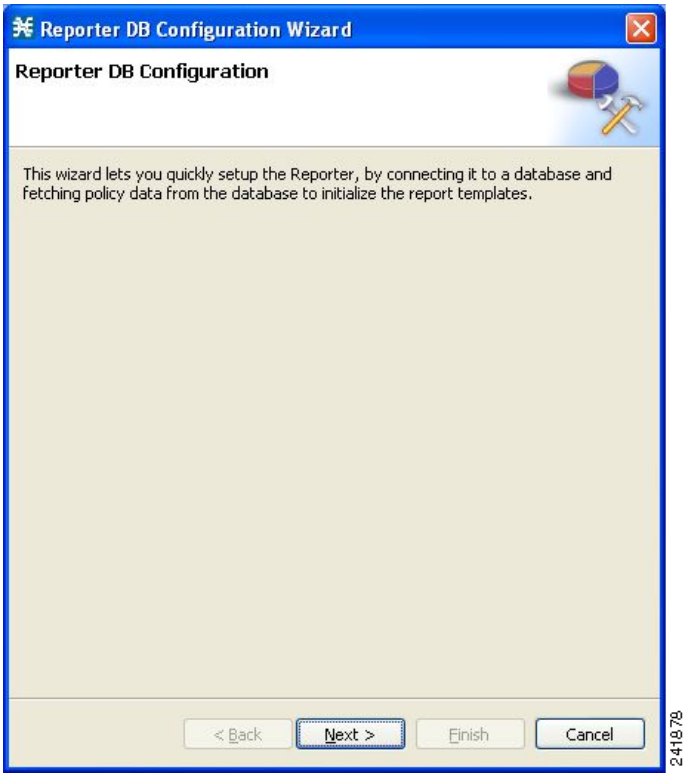
Step 1 From the Console main menu, choose **Help > Welcome.**

The Welcome view opens.



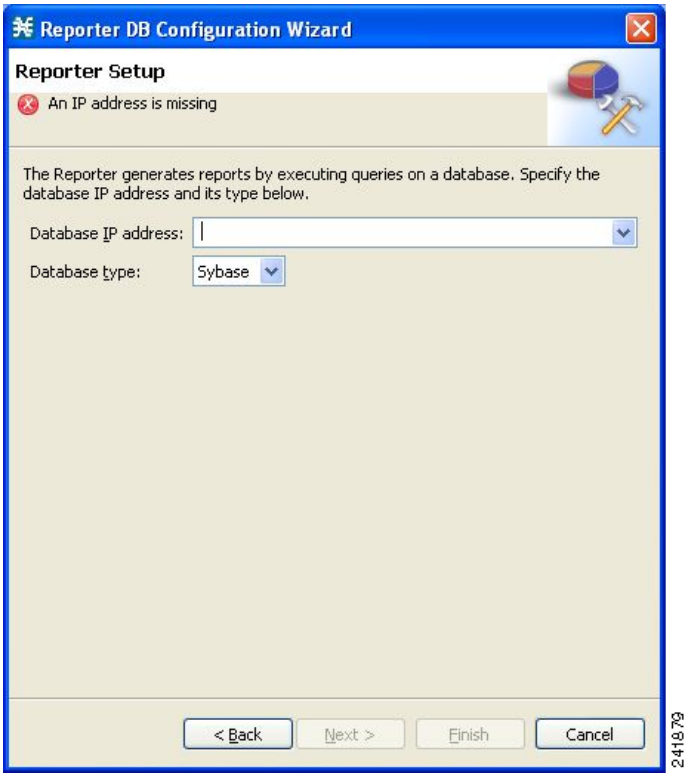
Step 2 Click **Initial Reporter Setup Wizard.**

The Welcome page of the Reporter DB Configuration wizard appears.



Step 3 Click **Next.**

The Reporter Setup page of the Reporter DB Configuration wizard opens.

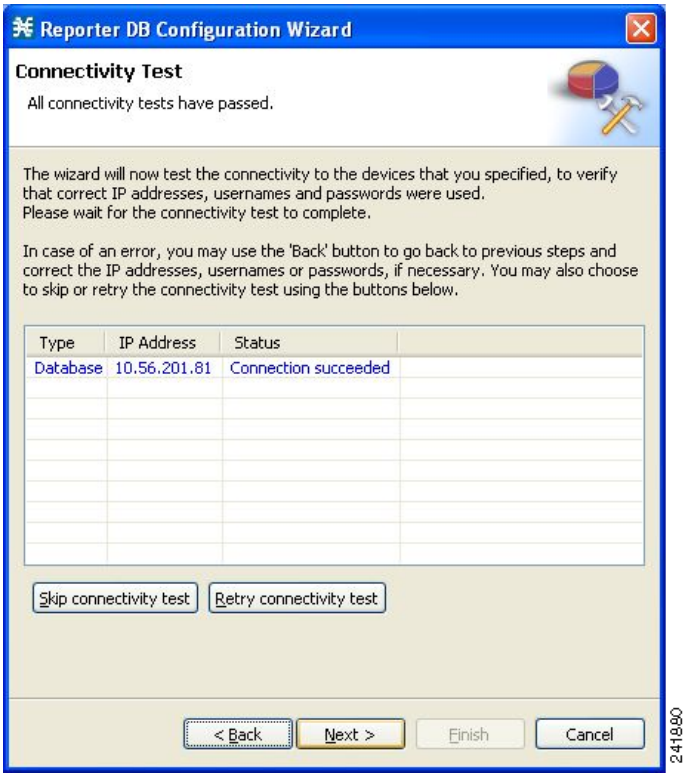


Step 4 In the Configure the IP address of the database field, enter the IP address of the database.

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

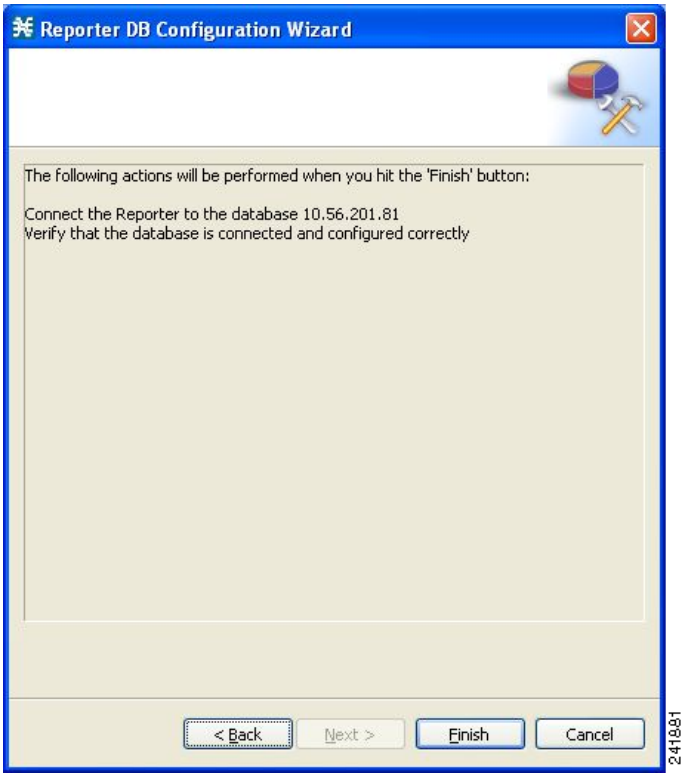
Step 6 Click **Next.**

The Connectivity Test page of the Reporter DB Configuration wizard opens.



Step 7 Click **Next.**

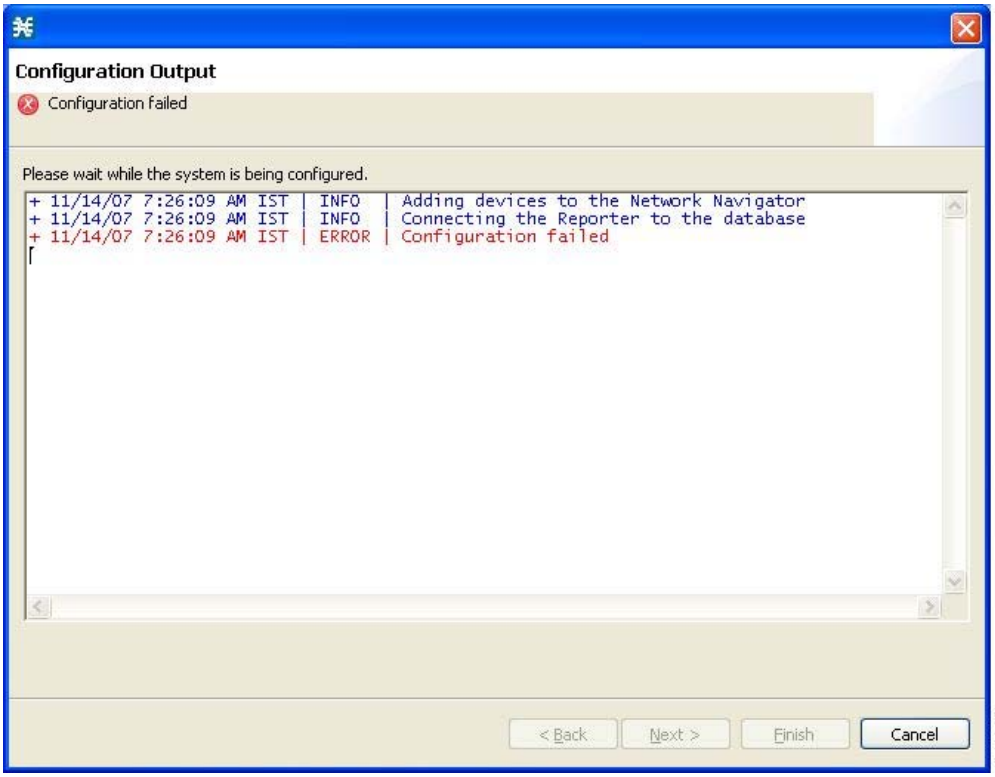
The Confirmation page of the Reporter DB Configuration wizard opens.



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

Step 8 Click **Finish.**

The Configuration Output page of the Reporter DB Configuration wizard opens.



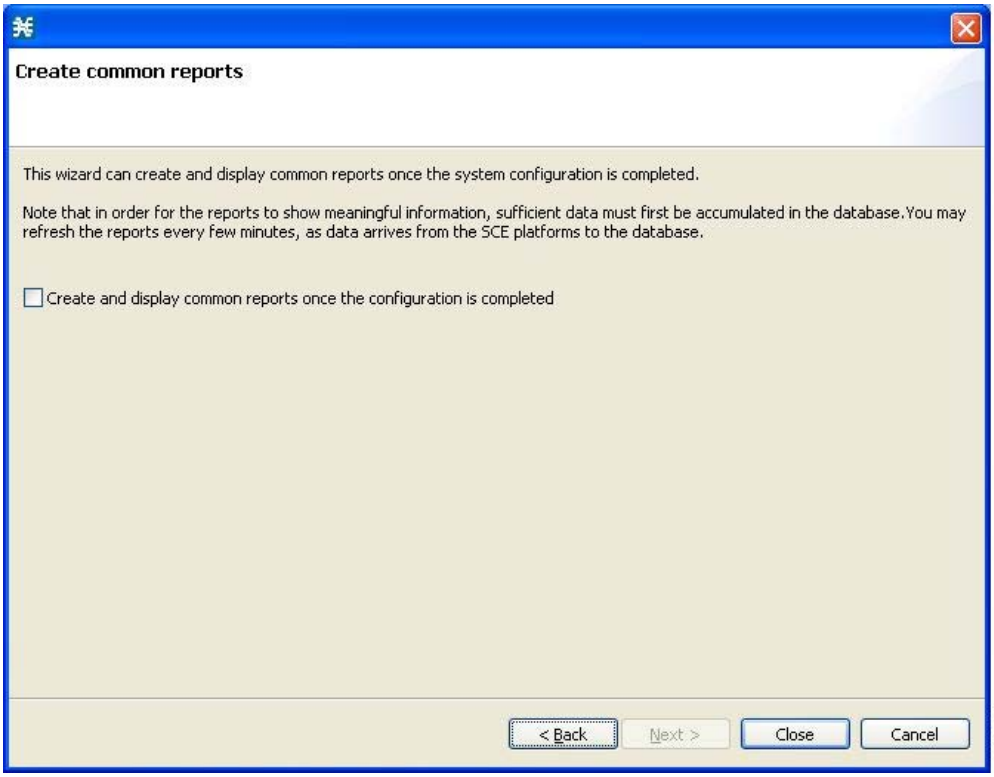
The wizard attempts to connect the SCA BB Reporter tool to the selected database. The operation fails if the wizard cannot connect to the database.

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.



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

Note Report instances will be 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

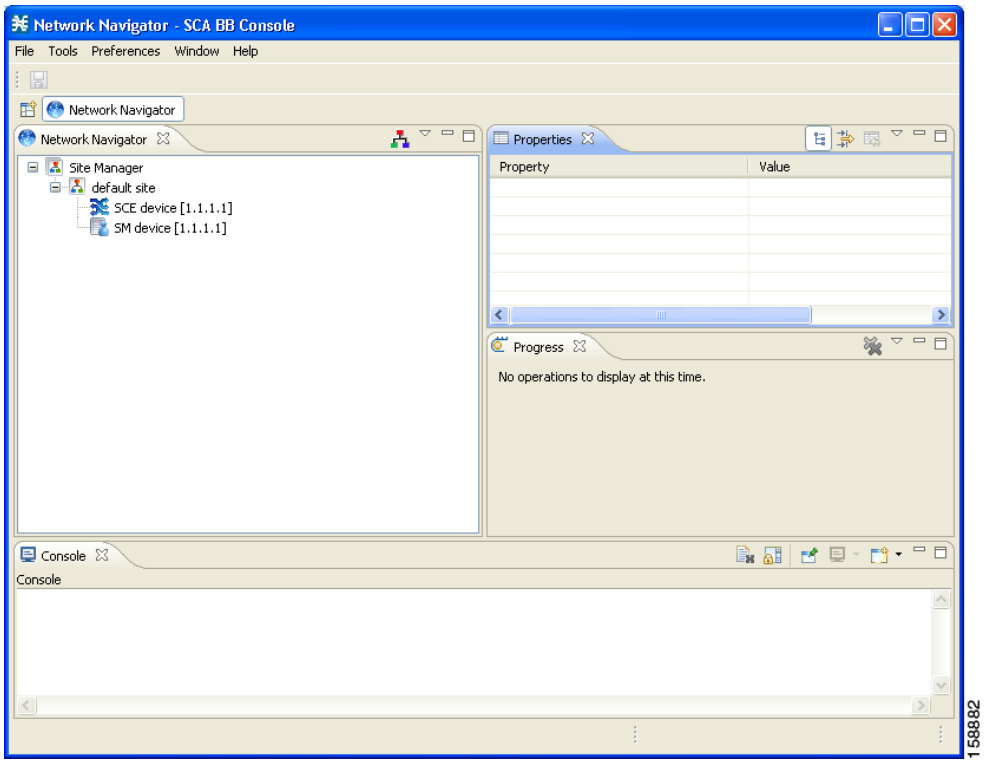
The Network Navigator is a tool that allows you to create and manage a simple model of all local and remote devices that are part of the Cisco Service Control solution.

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.



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 4-53
- How to Close the Service Configuration Editor Tool, page 4-54

How to Open the Service Configuration Editor Tool

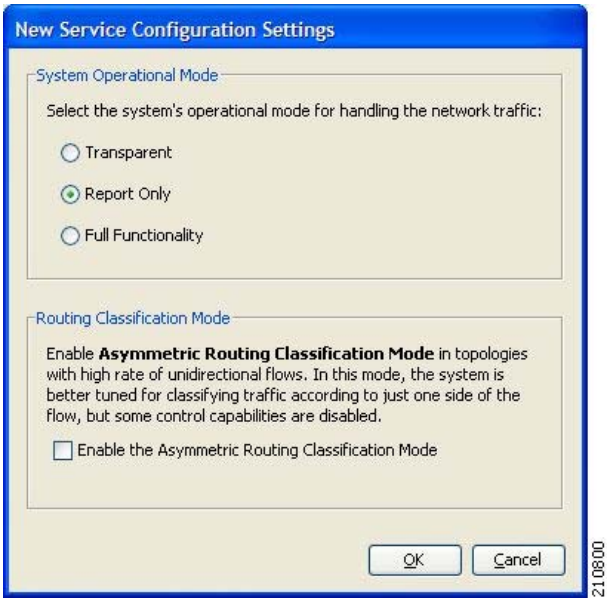
Step 1 From the Console main menu, choose **Tools > Service Configuration Editor.**

A No Service Configuration Is Open dialog box appears.



Step 2 Click **Yes.**

A New Service Configuration Settings dialog box appears.



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).

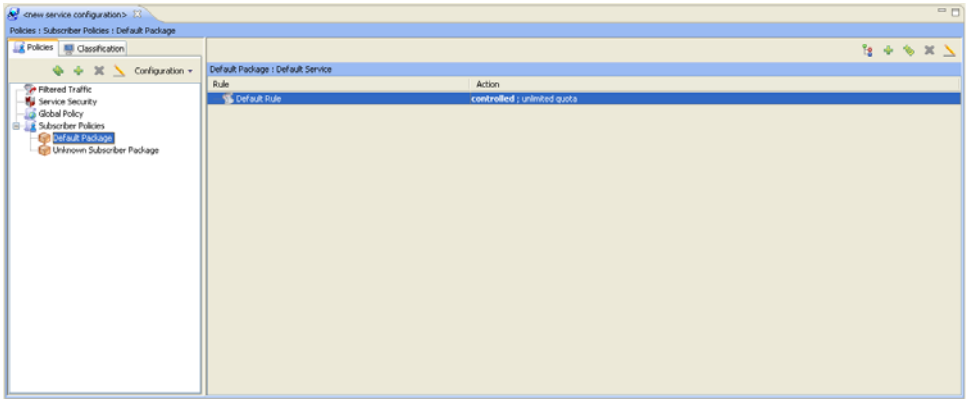
Note You can change the system operational mode at any time.

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 10-35.)

Step 5 Click **OK.**

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



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 SCA BB.

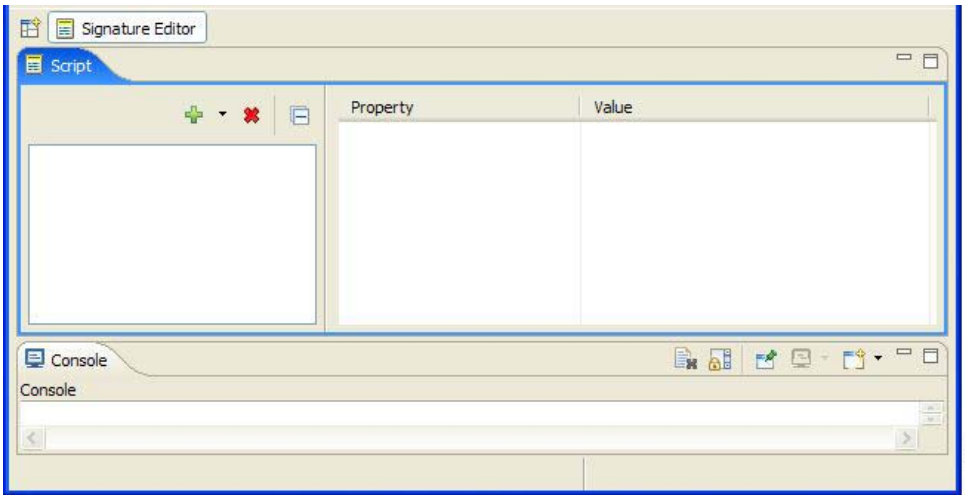
For more information about the Signature Editor, see Using the Signature Editor, page 12-1.

- How to Open the Signature Editor Tool, page 4-55
- How to Close the Signature Editor Tool, page 4-55

How to Open the Signature Editor Tool

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

The Signature Editor tool opens.



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 (SM) GUI is a tool that allows you to connect to an SCMS-SM and then manage subscribers, assign packages to subscribers, edit subscriber parameters, and manually add subscribers.

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

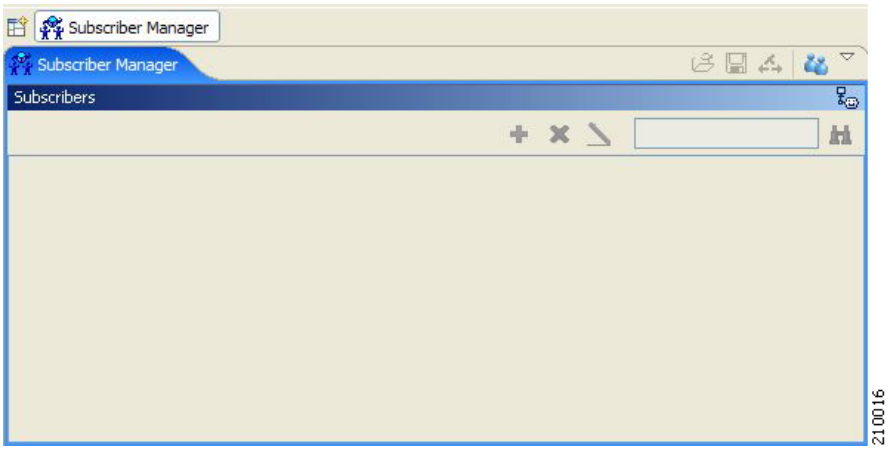
For more information about the SCMS-SM, see the *Cisco Service Control Management Suite Subscriber Manager User Guide*.

- How to Open the SM GUI Tool, page 4-56
- How to Close the SM GUI Tool, page 4-56

How to Open the SM GUI Tool

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

The SM GUI tool opens.



How to Close the SM GUI Tool

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

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

The SM GUI 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.

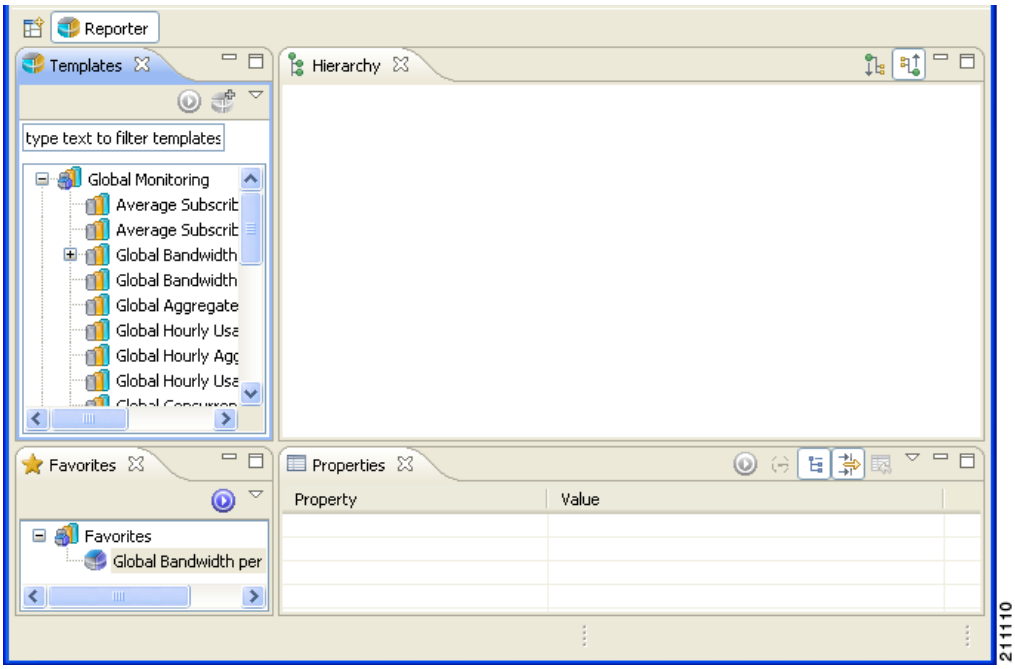
You can run the SCA Reporter as a standalone or inside the Reporter tool in the Console. For more information about the SCA Reporter, see the *Cisco Service Control Application Reporter User Guide*.

- How to Open the Reporter Tool, page 4-57
- How to Close the Reporter Tool, page 4-57

How to Open the Reporter Tool

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

The Reporter tool opens.



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 5-28.)

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 4-58
- How to Search Online Help, page 4-58

How to Access Online Help

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

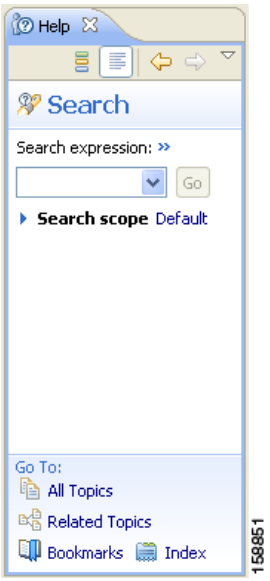
Online help opens in a separate window.

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.



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

Quick Start with the Console

This Quick Start section will help 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 will 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 3.1.6 > SCA BB Console 3.1.6.**

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 and click **Extract.**

The SCE online status is retrieved.

c. 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  (**Apply Service Configuration to SCE Devices)**.

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

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.

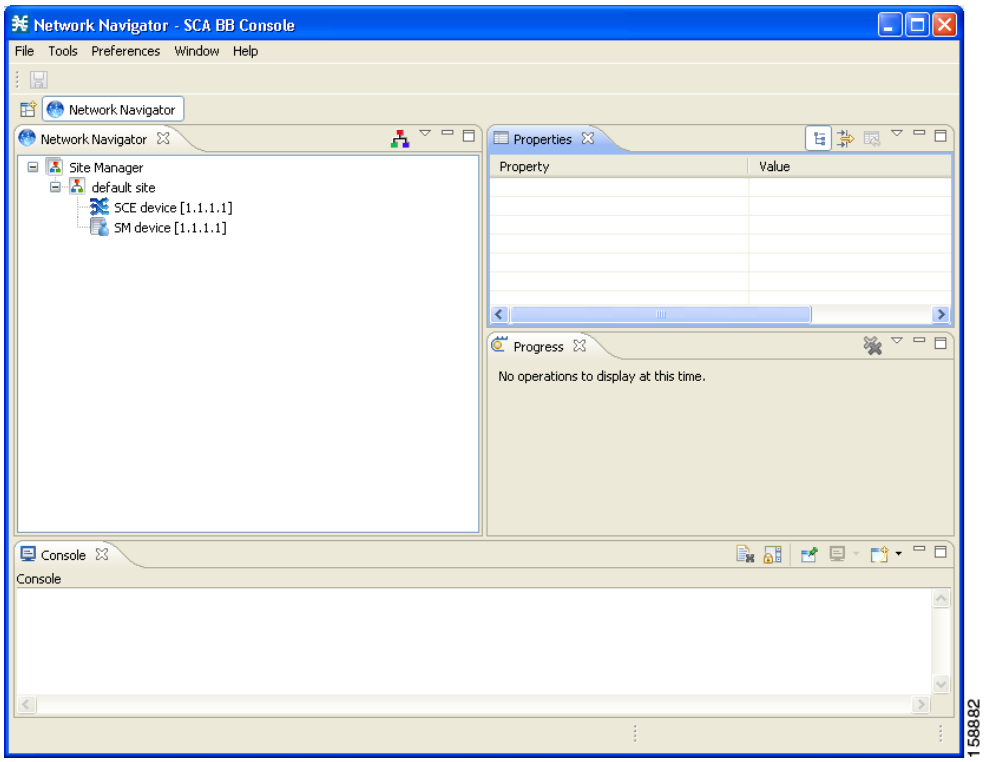
- The Network Navigator Tool, page 5-1
- Managing Sites, page 5-2
- Managing Devices, page 5-6
- Working with Network Navigator Configuration Files, page 5-31
- Network Settings Requirements, page 5-35

The Network Navigator Tool

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

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

Figure 5-1 The Network Navigator Tool



Managing Sites

You can manage an SCE, SM, 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 5-6).

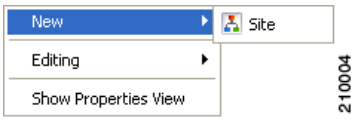
- How to Add a Site to the Site Manager, page 5-3
- How to Add Devices to a Site, page 5-3
- How to Delete Sites, page 5-6

How to Add a Site to the Site Manager

Before adding devices, you must add your sites to the Site Manager.

Step 1 In the Network Navigator view, right-click the Site Manager node.

A popup menu appears.



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 (Option) In the Version cell, enter a version number.

How to Add Devices to a Site

You can add SCE, SM, CM, or database devices to a site.

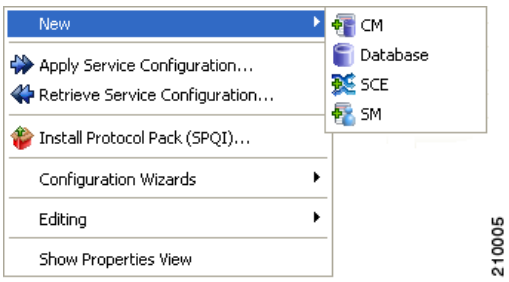
- How to Add SCE Devices to a Site, page 5-3
- How to Add SM Devices to a Site, page 5-4
- How to Add CM Devices to a Site, page 5-4
- How to Add Database Devices to a Site, page 5-5
- How to Delete Devices, page 5-6

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.



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 (Option) 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 SM Devices to a Site

To use the Network Navigator to configure, monitor, and update the software of an SM, you must first add the SM 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-SM.

Step 4 (Option) In the Name field, enter a meaningful name for the SM.

Step 5 Click **Finish.**

The Create New SM wizard closes.

The new device is added to the site.

How to Add CM Devices to a Site

To use the Network Navigator to monitor a CM, you must first add the CM 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 CM.

Step 4 (Option) In the Name field, enter a meaningful name for the CM.

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

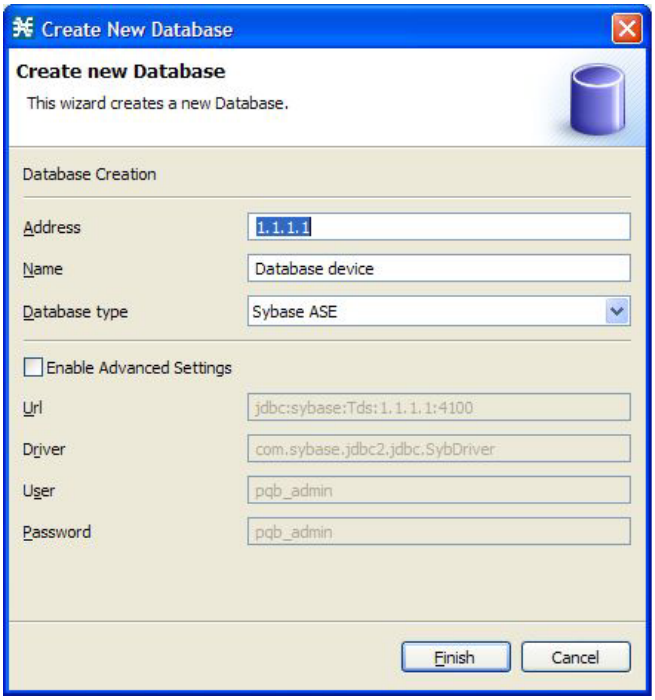
To use the Reporter tool to produce reports, you must first connect to a database.

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.



Step 3 In the Address field, enter the IP address of the database.

Step 4 (Option) 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 (Option) 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, SM, 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 4-18.)

- Password Management, page 5-6
- Managing SCE Devices, page 5-7
- Managing SM Devices, page 5-24
- Managing CM Devices, page 5-27
- Managing Database Devices, page 5-28

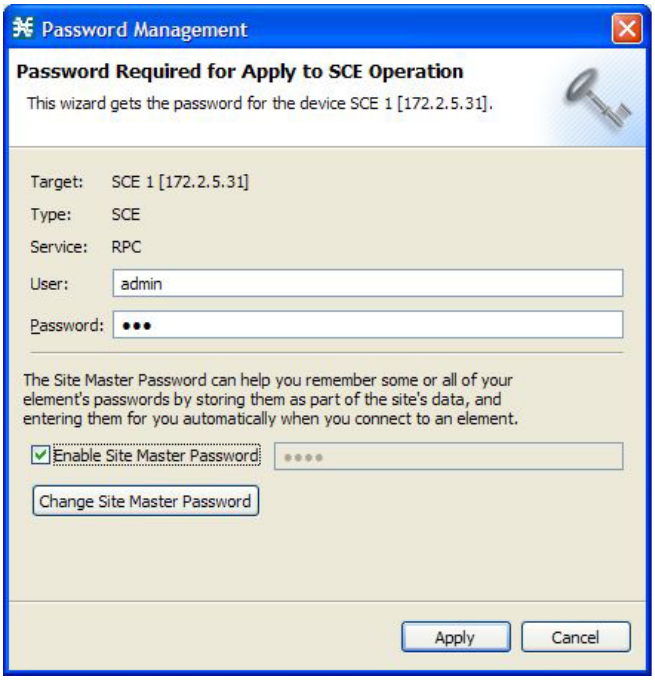
Password Management

Normally, before you can access a device (SCE, SM, 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 of your element's usernames and passwords by storing them as part of the site's 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 5-2) prompts you for the site's master password when you wish to activate the site password manager. If you have multiple sites, each site will require a separate master password.

Figure 5-2 The Password Management Dialog Box



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 5-8
- How to Generate Tech Support Info Files for SCE Devices, page 5-15
- How to Retrieve the Online Status of SCE Devices, page 5-17
- How to Install a Protocol Pack, page 5-17
- How to Apply Service Configurations to SCE Devices, page 5-19
- How to Retrieve Service Configurations from SCE Devices, page 5-21
- How to Install PQI Files on SCE Devices, page 5-22
- How to Install an SCE OS Software Package on SCE Devices, page 5-23

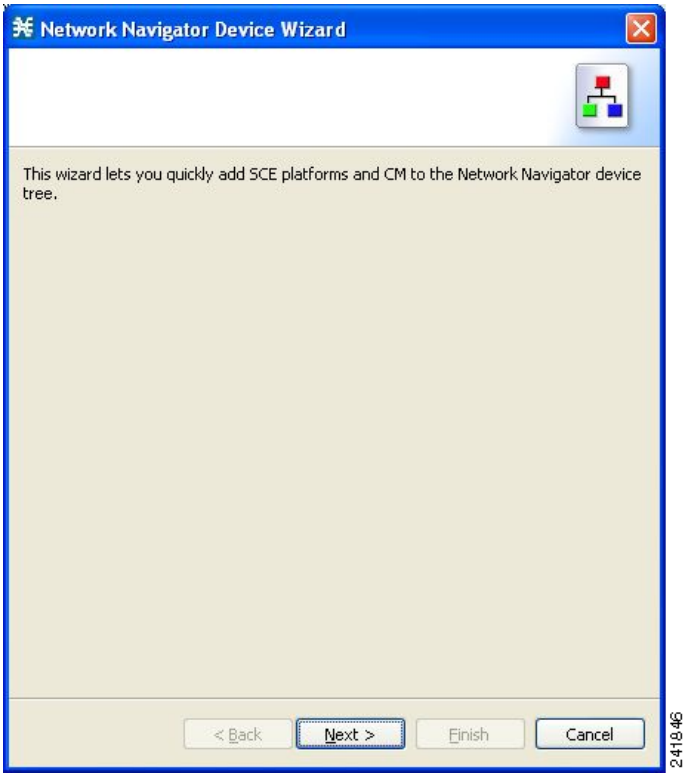
How to Configure SCE and CM Devices Using a Wizard

The Network Navigator Device wizard allows you to configure SCA and CM devices and connect to them.

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

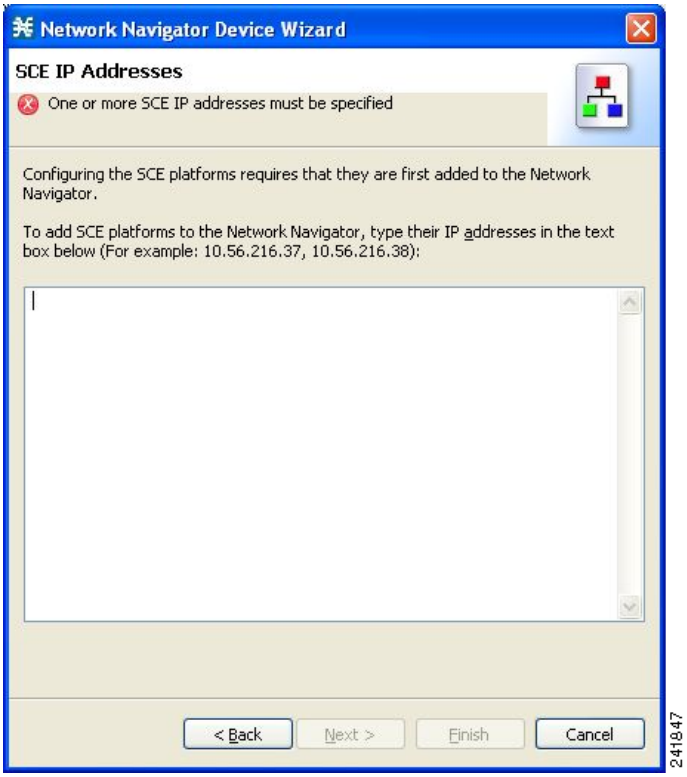
Step 1 In the Network Navigator view toolbar, click (**Configure SCE and CM devices)**.

The Welcome page of the Network Navigator Device wizard appears.



Step 2 Click **Next.**

The SCE IP Addresses page of the Network Navigator Device wizard opens.



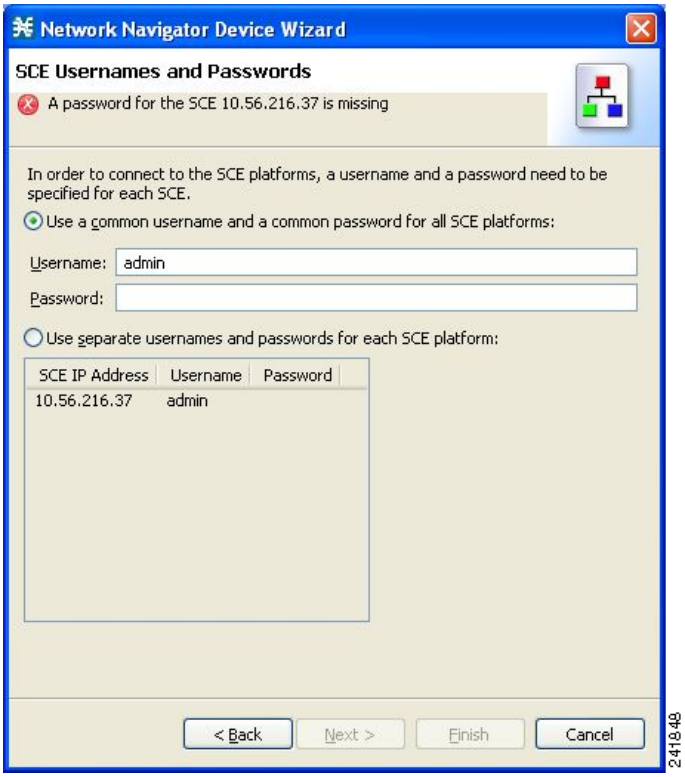
Step 3 In the edit box, enter the IP addresses of the SCE devices that should be added to the model.

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.



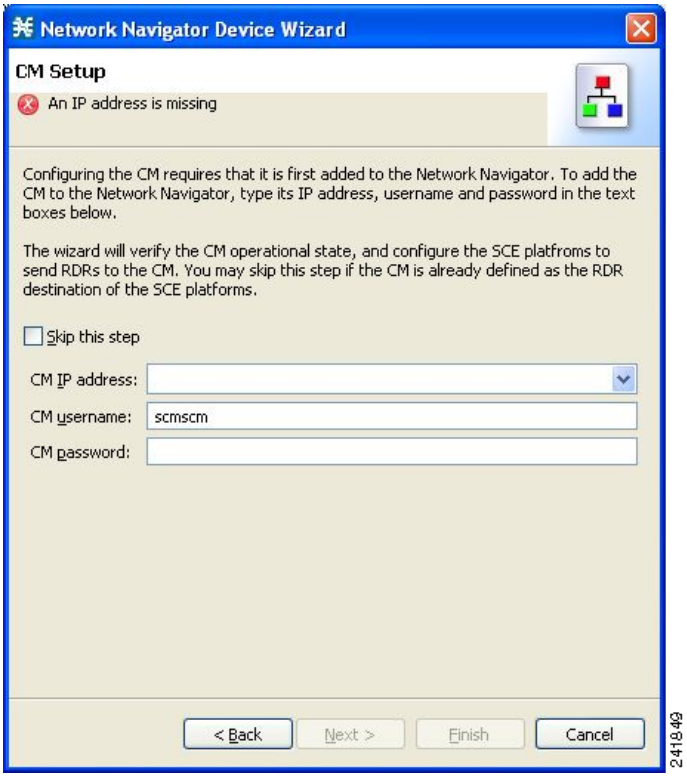
Step 5 Enter the user names and passwords for the SCE devices.

Do one of the following:

- To use the same user name and password for all the SCE devices that you are adding, enter the user name in the Username field and the password in the Password field.
- To provide a different user name 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 user name and password in the appropriate cell of the SCE device table.

Step 6 Click **Next.**

The Setting CM devices page of the Network Navigator Device wizard opens.



Step 7 Define the SCSM Collection Manager (CM) to use with this configuration.

Do one of the following:

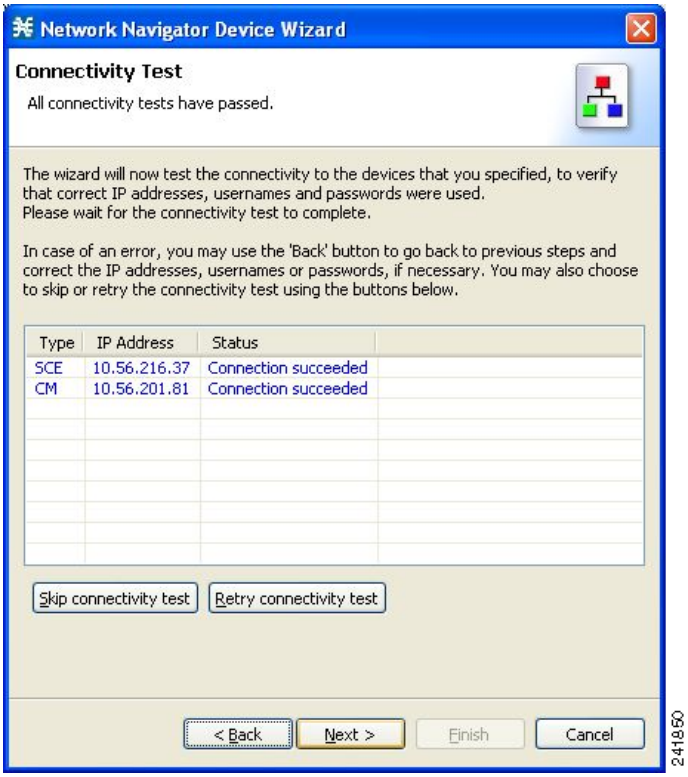
- Enter the IP address, user name, and password of the CM device in the appropriate fields.

  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.

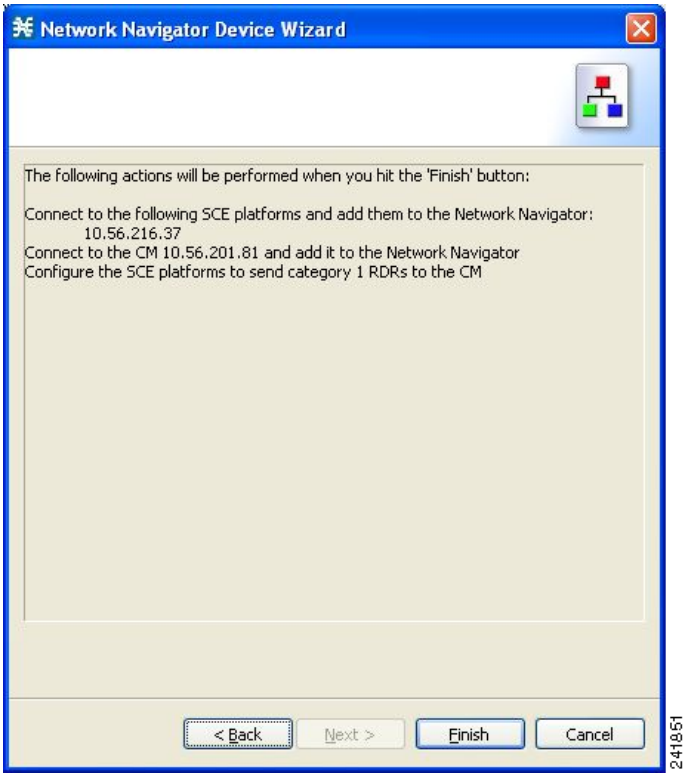


The wizard tests to see that the connections to the defined devices can be made.

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 will be validated when you click **Finish** at the end of the wizard.

Step 9 Click **Next.**

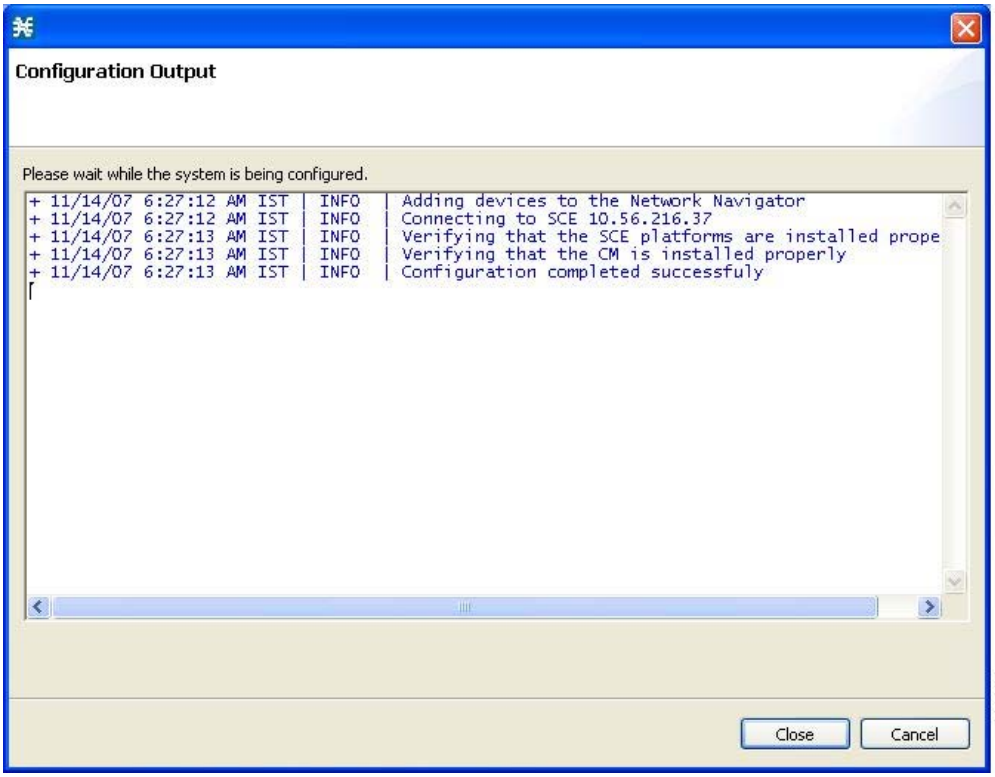
The Confirmation page of the Network Navigator Device wizard opens.



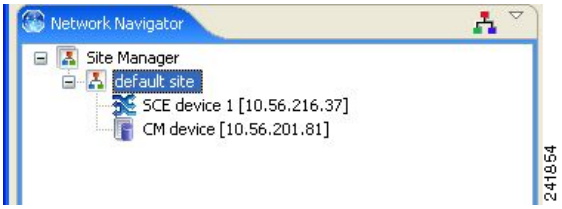
The actions that the wizard is about to take are listed in the page.

Step 10 Click **Finish.**

The Configuration Output page of the Network Navigator Device wizard opens.



New devices are added to the default site in the Site Manager tree in the 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 the "Raw Data Formatting: The RDR Formatter and NetFlow Exporting" chapter of the *Cisco Service Control Engine (SCE) 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 8-4; the content and structure of the Transaction RDR is listed in "Transaction RDR" in the "Raw Data Records: Formats and Field Contents" chapter of the *Cisco Service Control Application for Broadband Reference Guide*.

Step 11 Click **Finish.**

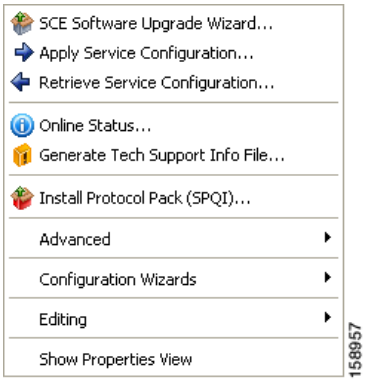
The Network Navigator Device wizard closes.

How to Generate Tech Support Info Files for SCE Devices

This operation generates the SCE platform's support file, for the use of Cisco technical support staff.

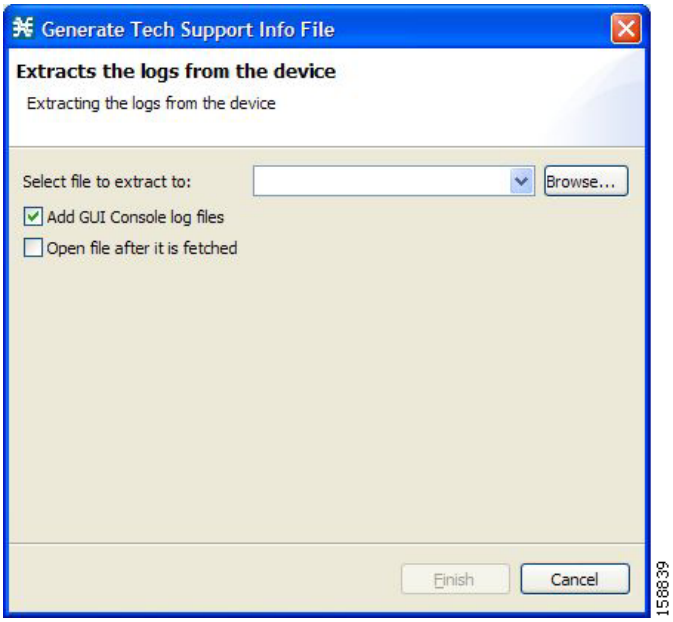
Step 1 In the Site Manager tree, right-click an SCE device.

A popup menu appears.



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 will be overwritten when you generate the tech support info.

The Select File dialog box closes.

Step 7 (Option) To add log files to the output tech support info file, check the **Add GUI Console log files** check box.

Step 8 (Option) 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, refer to Password Management, page 5-6.)

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 SCE platform's current software version and operational status.

Step 1 In the Site Manager tree, right-click an SCE device.

A popup menu appears.

Step 2 From the menu, select **Online Status.**

A Password Management dialog box appears.

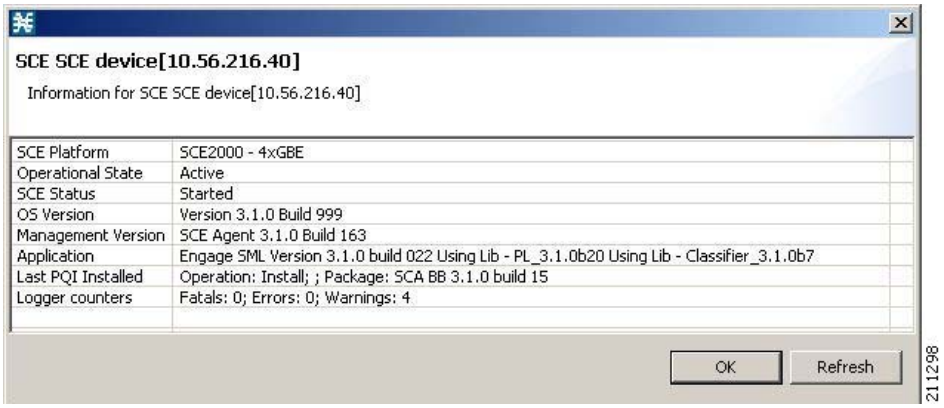
Step 3 Enter the appropriate password. (For more information, refer to Password Management, page 5-6.)

Step 4 Click **Extract.**

The Password Management dialog box closes.

An Extracting info progress bar appears.

The SCE online status is retrieved.



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 4-10.

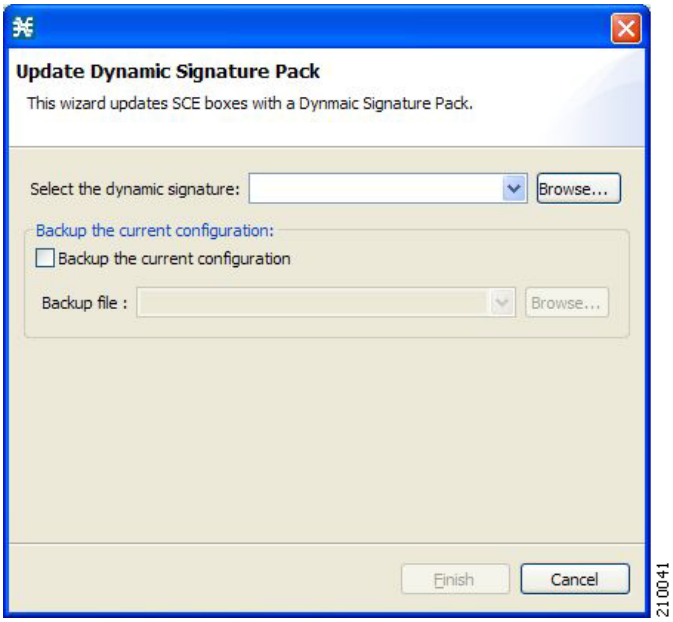
- How to Install a Protocol Pack on a Single SCE Platform, page 5-17
- How to Install a Protocol Pack on Multiple SCE Platforms, page 5-18

How to Install a Protocol Pack on a Single SCE Platform

Step 1 In the Site Manager tree, right-click the SCE where the protocol pack is to be installed.

Step 2 From the popup menu that appears, select **Update Dynamic Signature Pack.**

The Update Dynamic Signature Pack dialog box appears.



Step 3 Click **Browse.**

A Select file dialog box appears.

Step 4 From the Files of type drop-down list, select ***.spqi** or ***.dss,** according to 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, refer to Password Management, page 5-6.

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

Step 1 In the Site Manager tree, select sites or SCE devices where the protocol pack will be installed, and right-click one of them

Step 2 From the popup menu that appears, choose **Update Dynamic Signature Pack.**

The Update Dynamic Signature Pack dialog box appears.

Step 3 Select the protocol pack to be installed.

Step 4 (Recommended) Check the **Backup the current configuration** check box and select a backup directory.

Note The backup files will be named backupPolicy_<SCE platform IP address>.pqb.

Step 5 Click **Finish.**

A separate Password Management dialog box appears for each SCE device that you selected.

Step 6 For each SCE device, enter the password and click **Update.**

The protocol pack is installed on each SCE platform in turn.

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 anSNMP 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 5-19
- How to Apply a Service Configuration to Multiple SCE Platforms, page 5-20

How to Apply a Service Configuration to a Single SCE Platform

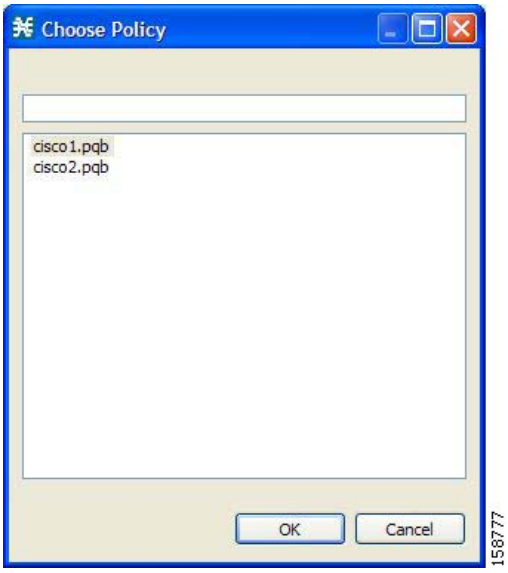
Step 1 In the Site Manager tree, right-click an SCE device.

A popup menu appears.

Step 2 From the menu, select **Apply Service Configuration.**

The Choose Policy dialog box appears, 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.)



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, refer to Password Management, page 5-6.)

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 5-21
- How to Retrieve Service Configurations from Multiple SCE Platforms, page 5-21

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, refer to Password Management, page 5-6.)

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

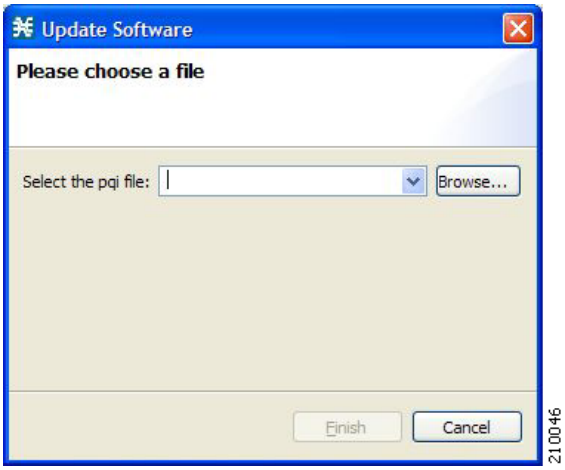
This operation installs the Cisco Service Control Application for Broadband (SCA BB) on the SCE platform.

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.



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, refer to Password Management, page 5-6.)

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

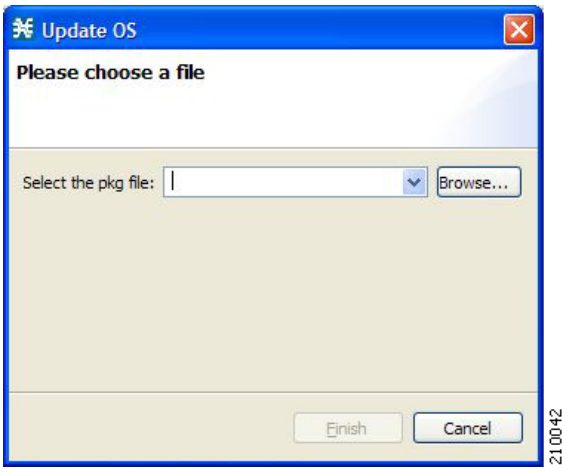
This operation installs the SCE OS software package (the operating system software and firmware of the SCE platform).

For more information, see "Upgrading SCE Platform Firmware" in the "Operations" chapter of the *Cisco Service Control Engine (SCE) Software Configuration Guide*.

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.



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, refer to Password Management, page 5-6.)

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 SM Devices

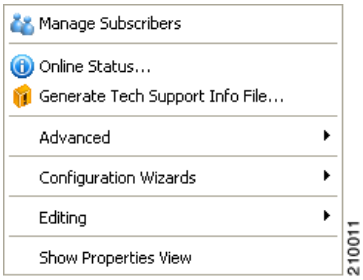
- How to Generate Tech Support Info Files for SM Devices, page 5-24
- How to Retrieve the Online Status of SM Devices, page 5-25
- How to Connect to SM Devices, page 5-26
- How to Install PQI Files on SM Devices, page 5-26

How to Generate Tech Support Info Files for SM Devices

This operation generates the SM's support file, for the use of Cisco technical support staff.

Step 1 In the Site Manager tree, right-click an SM device.

A popup menu appears.



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 will be overwritten.

The Select File dialog box closes.

Step 7 (Option) 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, refer to Password Management, page 5-6.)

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 SM Devices

This operation provides information about the SM's current software version and operational status.

Step 1 In the Site Manager tree, right-click an SM device.

A popup menu appears.

Step 2 From the menu, select **Online Status.**

A Password Management dialog box appears.

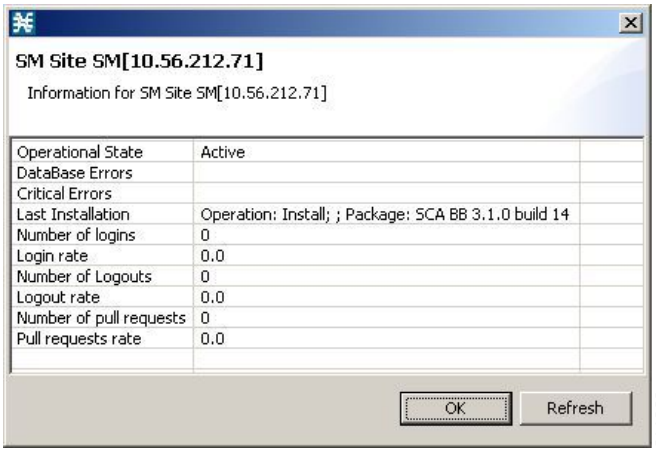
Step 3 Enter the appropriate password. (For more information, refer to Password Management, page 5-6.)

Step 4 Click **Extract.**

The Password Management dialog box closes.

An Extracting info progress bar appears.

The SCMS-SM online status is retrieved.



How to Connect to SM Devices

In order to manage subscribers using the SM GUI tool, you must connect to an SM device.

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 will fail.
If you have changed the PRPC port on the SCMS-SM, see User Authentication, page 5-37.

Step 1 In the Site Manager tree, right-click an SM 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, refer to Password Management, page 5-6.)

Step 4 Click **Connecting.**

The Password Management dialog box closes.

A Connecting to progress bar appears.

You connect to the SM, and the Console switches to the SM GUI tool.

For an explanation of how to proceed, see Using the Subscriber Manager GUI Tool, page 11-1.

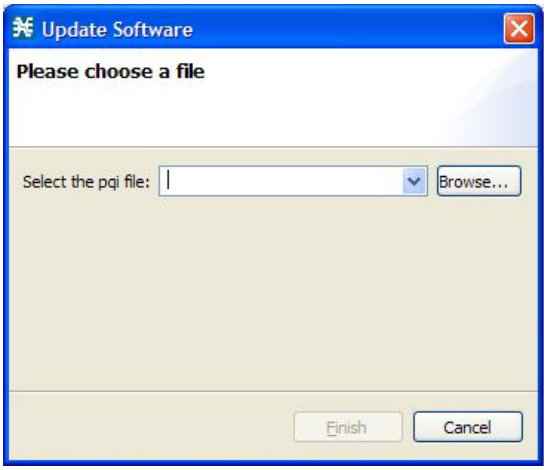
How to Install PQI Files on SM Devices

Note Installing a PQI file usually takes a few minutes.

Step 1 In the Site Manager tree, select an SM device.

Step 2 From the Console main menu, choose **Network > Install Application Software (PQI).**

The Update Software dialog box appears.



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, refer to Password Management, page 5-6.)

Step 8 Click **Apply.**

The Password Management dialog box closes.

An Updating software to SM progress bar appears.

The PQI file is installed on the selected SM.

Managing CM Devices

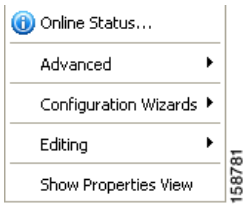
You can configure CM devices using a wizard. (See How to Configure SCE and CM Devices Using a Wizard, page 5-8.)

How to Retrieve the Online Status of CM Devices

This operation provides information about the CM's current software version and operational status.

Step 1 In the Site Manager tree, right-click a CM 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, refer to Password Management, page 5-6.)

Step 4 Click **Extract.**

The Password Management dialog box closes.

An Extracting info progress bar appears.

The SCMS-CM 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 5-17.

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 4-45.)
- An alternative procedure is described in “Configuring a Database Connection” in the “Using the Cisco Service Control Application Reporter” chapter of the *Cisco Service Control Application Reporter User Guide*.

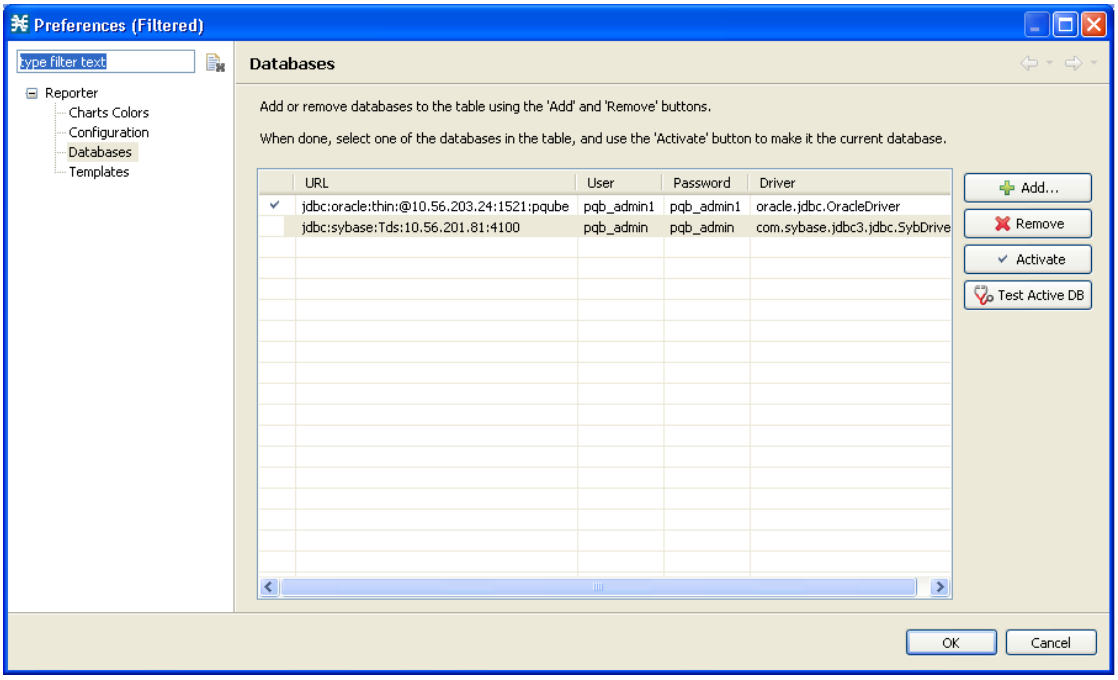
Step 1 In the Site Manager tree, right-click a database device.

A popup menu appears.



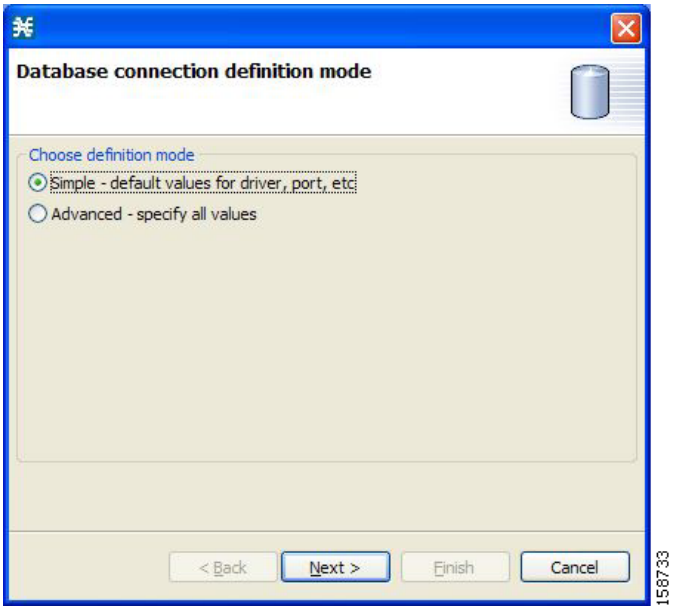
Step 2 From the menu, select **Add to Reporter.**

The Preferences dialog box appears.



Step 3 Click **Add.**

The Add Database wizard appears.



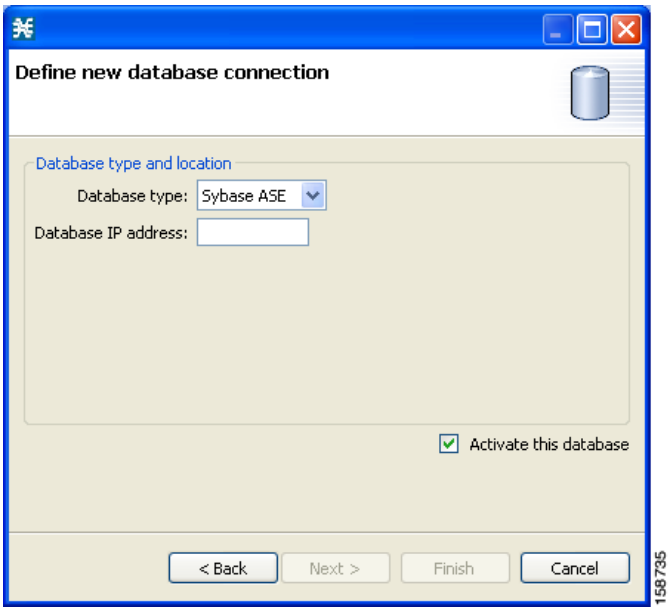
Step 4 Select one of the **Choose definition mode** radio buttons.

- **Simple**
- **Advanced**

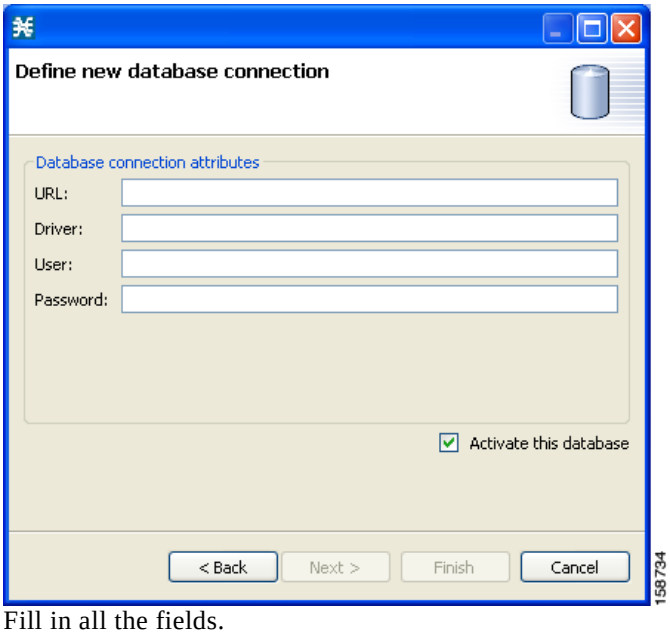
Step 5 Click **Next.**

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 this:



- If you selected Advanced in Step 4, the Define new database connection page looks like this:



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 required, 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.

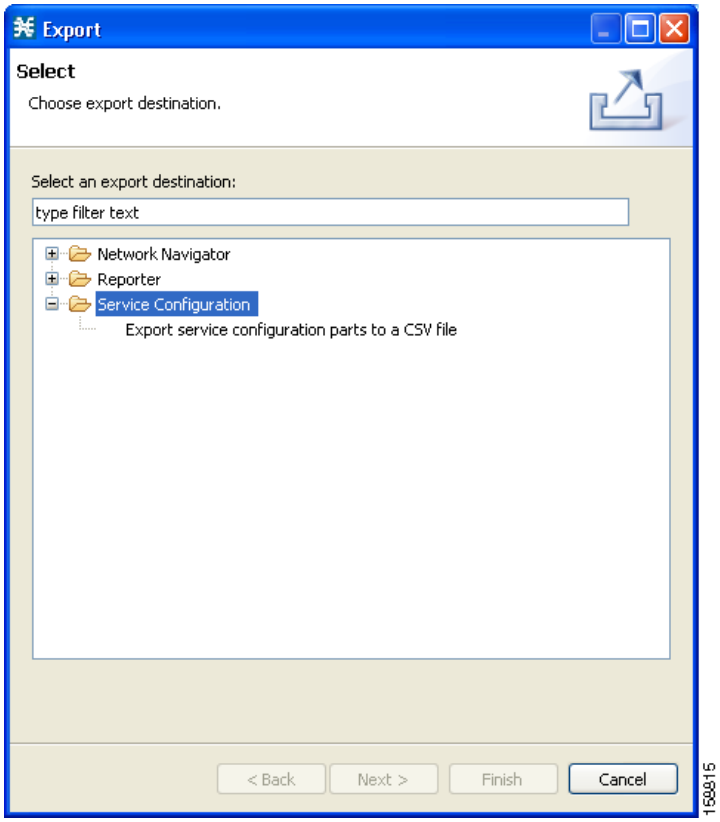
If you use the Site Master Password to store the passwords of the network devices, the passwords are also exported, in encrypted form. This means that other users who import this data need only provide the Site Master Password to access the devices.

- How to Export a Network Navigator Configuration, page 5-31
- How to Import a Network Navigator Configuration, page 5-34

How to Export a Network Navigator Configuration

Step 1 From the Console main menu, choose **File > Export.**

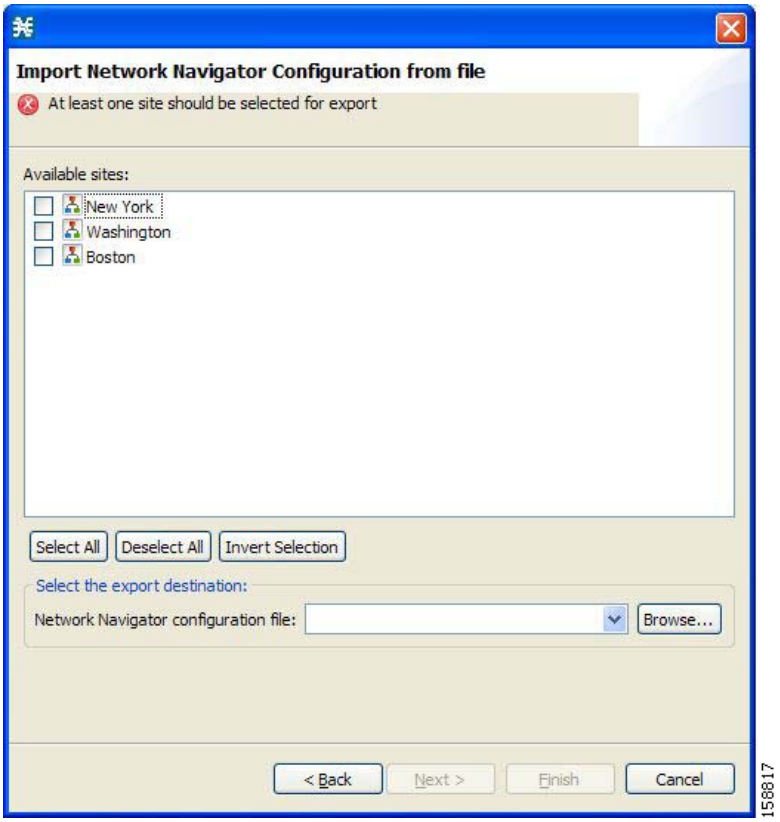
The Export dialog box appears.



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.



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 will be overwritten.

The Open dialog box closes.

Step 9 Click **Finish.**

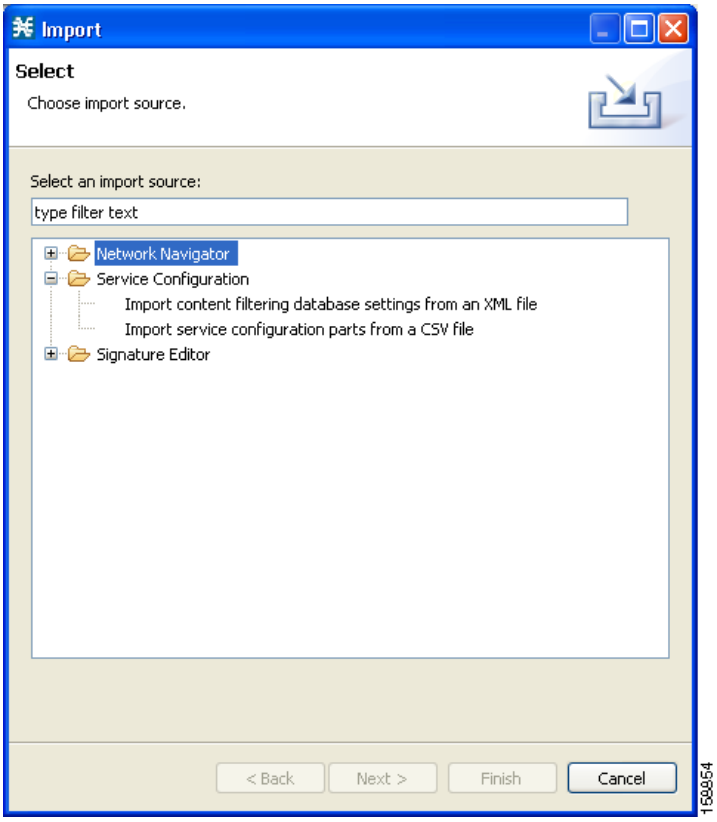
The Export Network Navigator Configuration dialog box closes.

The configuration is saved to the file.

How to Import a Network Navigator Configuration

Step 1 From the Console main menu, choose **File > Import.**

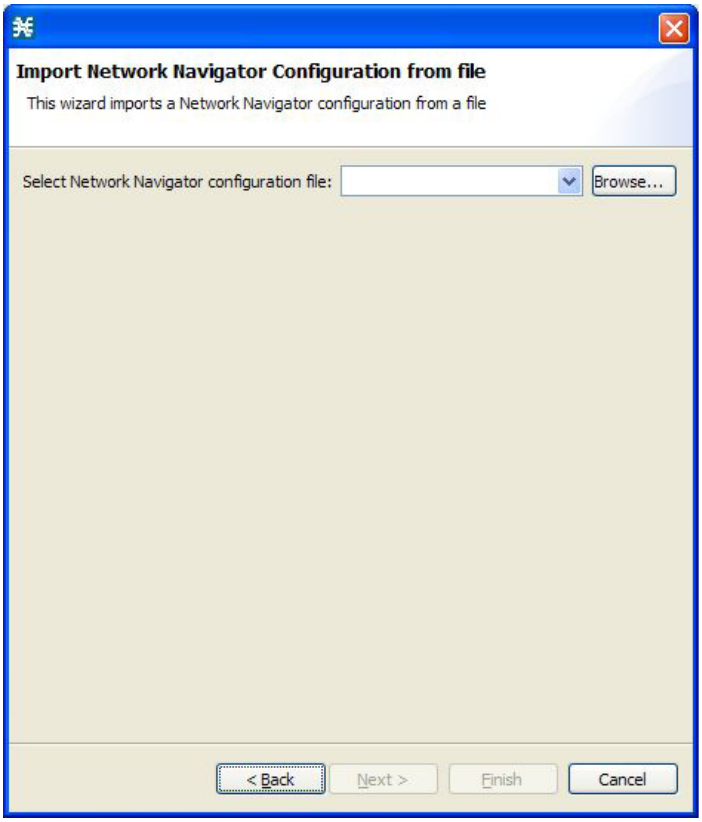
The Import dialog box appears.



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.



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 5-36
- User Authentication, page 5-37
- How to Disable PRPC Authentication, page 5-37

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 port 21/TCP is already used by another application on the workstation
Workstation	SM port 14374/TCP	PRPC—Required for all SM 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 the *Cisco Service Control Application Reporter User Guide*.

User Authentication

User authentication is performed when a PRPC connection is made to an SCE platform, a CM, or an SM. 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 3.1.6\plugins\policy.contribution_3.1.6\config\.

You define the username and password using the user/password mechanism in the SCE platform or a command-line utility in the SM and CM.

For more information about defining users, see the following:

- SCE—"TACACS+ Authentication, Authorization, and Accounting" in the "Configuring the Management Interface and Security" chapter of the *Cisco Service Control Engine (SCE) Software Configuration Guide*
- CM—"Managing Users" in the "Managing the Collection Manager" chapter of the *Cisco Service Control Management Suite Collection Manager User Guide*
- SM—"p3rpc Utility" in the "Command-Line Utilities" appendix of the *Cisco Service Control Management Suite Subscriber Manager User Guide*

Note PRPC authentication from the SCA BB Console to any CM/SM/SCE IP address other then the device's real IP address is not supported. This is especially important when the CM/SM/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/SM/SCE as described in the following sections.

How to Disable PRPC Authentication

- How to Disable PRPC Authentication on an SCE Platform, page 5-38
- How to Disable PRPC Authentication on a CM, page 5-38
- How to Disable PRPC Authentication on an SM, page 5-38

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 SM

Step 1 Edit the SM 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

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 6-1

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.



- 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 one time; each is displayed in its own view, and you click a view to make that view's service configuration active.

When a service configuration has unsaved changes, an asterisk precedes its name on the view.

How to Add New Service Configurations

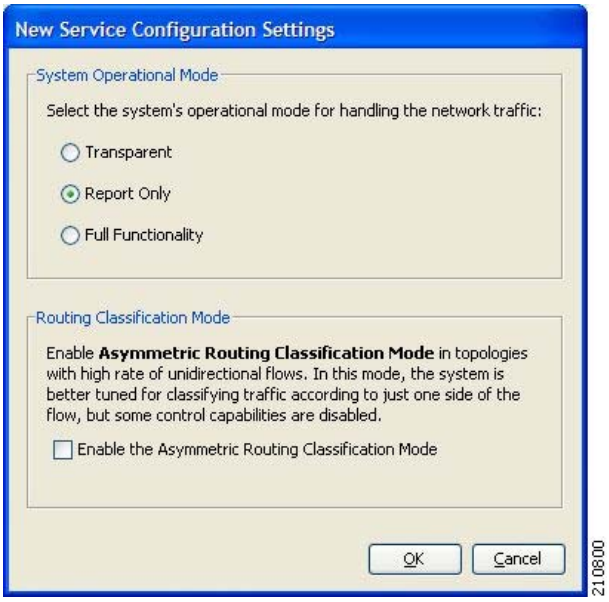
You can add a new service configuration whenever necessary.

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.



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 10-35).

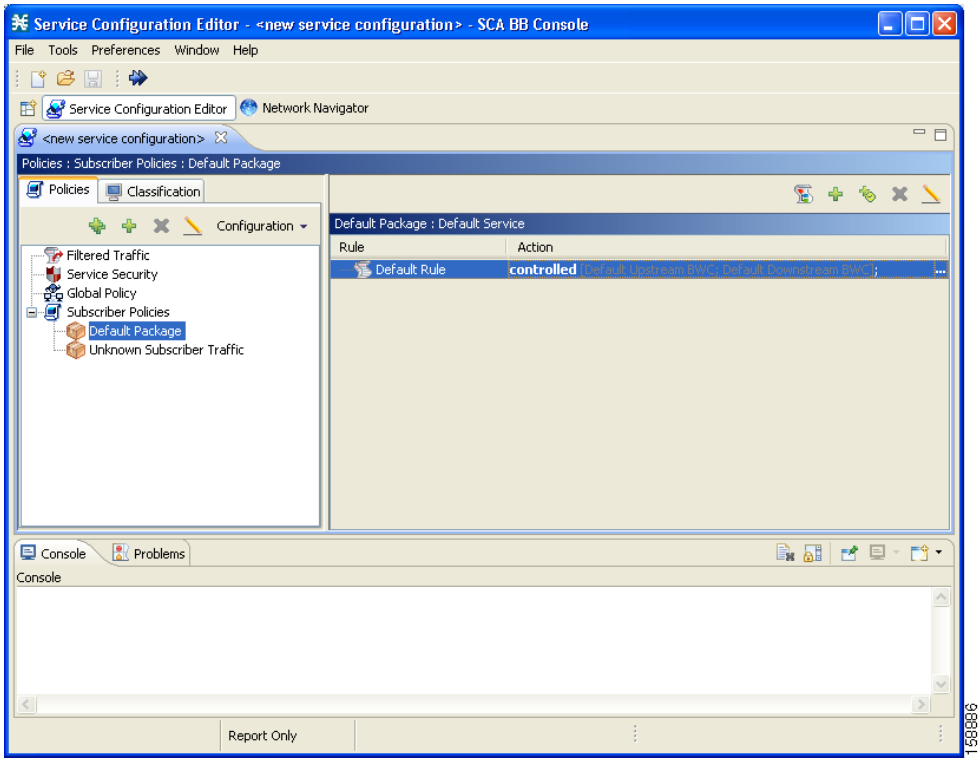
Step 4 Click **OK.**

If you have set a default DSS file (see The Default DSS File, page 7-39), 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 new service configuration is added to the Console window, open on the Network Traffic tab, and becomes the active service configuration.



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  (**Open A Service Configuration File)**. (Or, from the Console main menu, choose **File > Open Service Configuration.**)

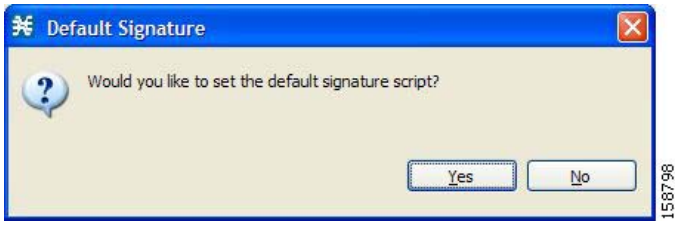
An Open dialog box appears.

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.



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 6-5

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.

- Enter your password if prompted.

Step 2 Browse to the folder where you want to save the file containing the service configuration.

Step 3 In the File name field, enter a new file name, or select an existing PQB file.

Step 4 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

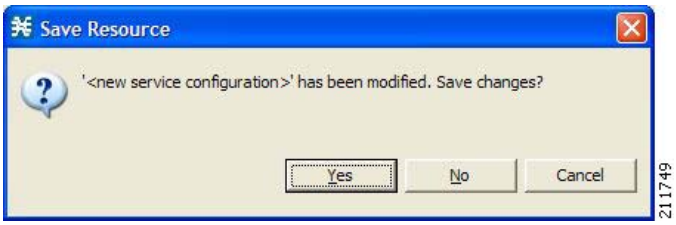
Step 1 In the Console toolbar, click  **(Save)**.

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  (**Close)**.

- If there are no unsaved changes, the service configuration view closes.
- If there are unsaved changes a Save Resource message appears.



- 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.

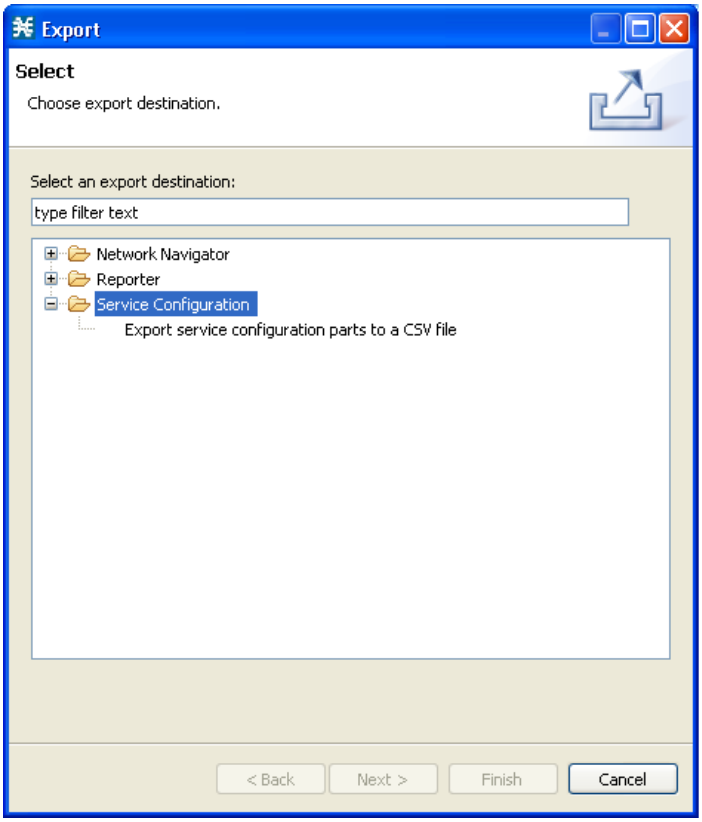
How to Export Service Configuration Data

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 the *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.**

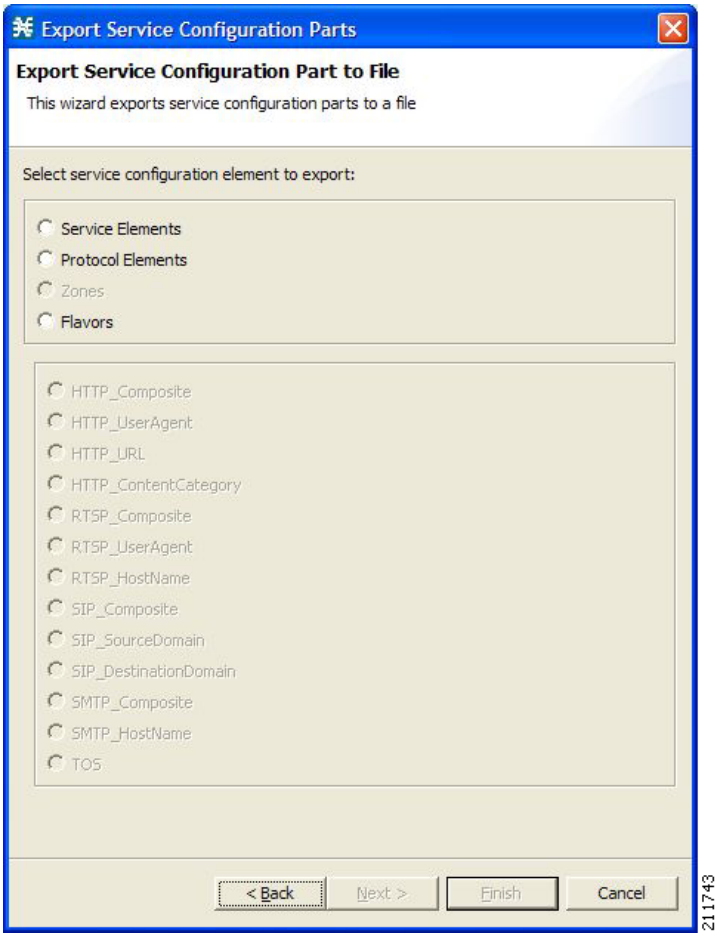
The Export dialog box appears.



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.



Step 4 Select one of the **Select service configuration element to export** radio buttons.

The radio buttons are:

- **Service Elements**
- **Protocol Elements**
- **Zones**
- **Flavors**

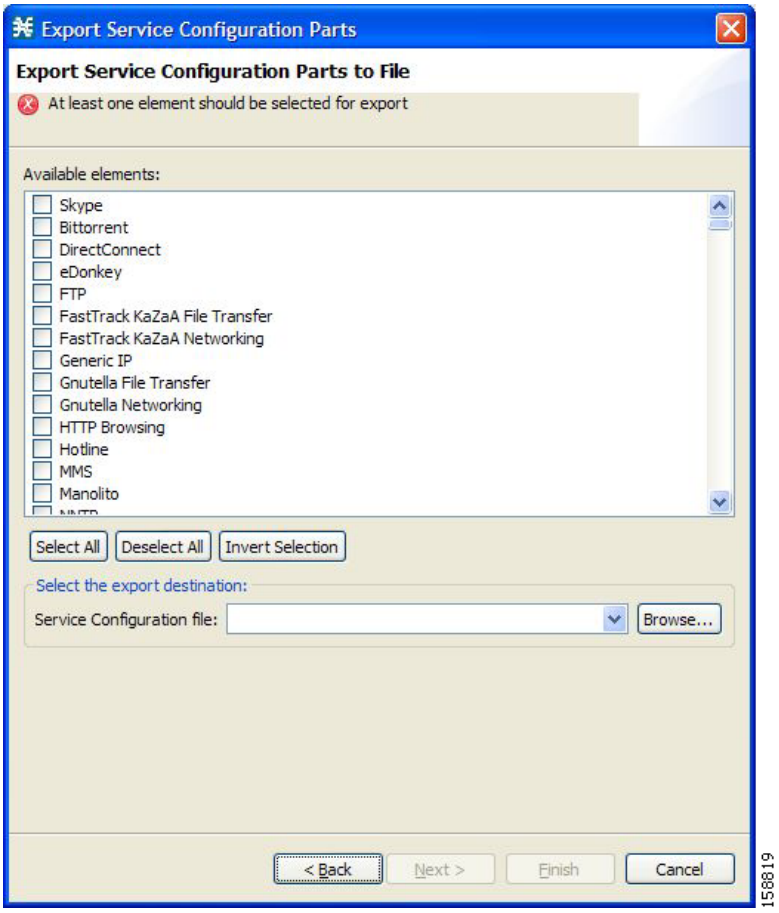
If you select Flavors, the flavors in the flavor area of the dialog box are enabled.

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.



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 In the Select the export destination area, click **Browse.**

An Open dialog box appears.

Step 9 Browse to the folder where you want to save the file containing the service configuration elements.

Step 10 In the File name field, enter a new file name, or select an existing CSV file.

Step 11 Click **Open** to select the file.

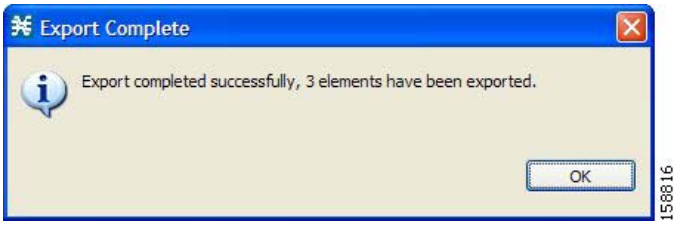
If the file exists, it will be overwritten.

The Open dialog box closes.

Step 12 Click **Finish.**

The selected service configuration elements are exported to the file.

An Export Complete message appears.



Step 13 Click **OK.**

The Export Service Configuration Parts dialog box closes.

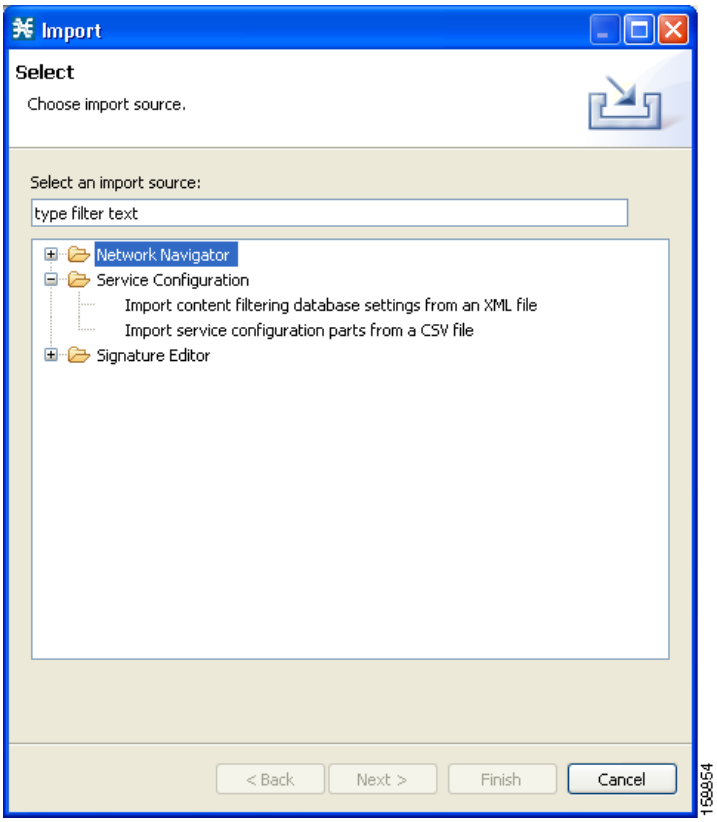
How to Import Service Configuration Data

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 the *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.**

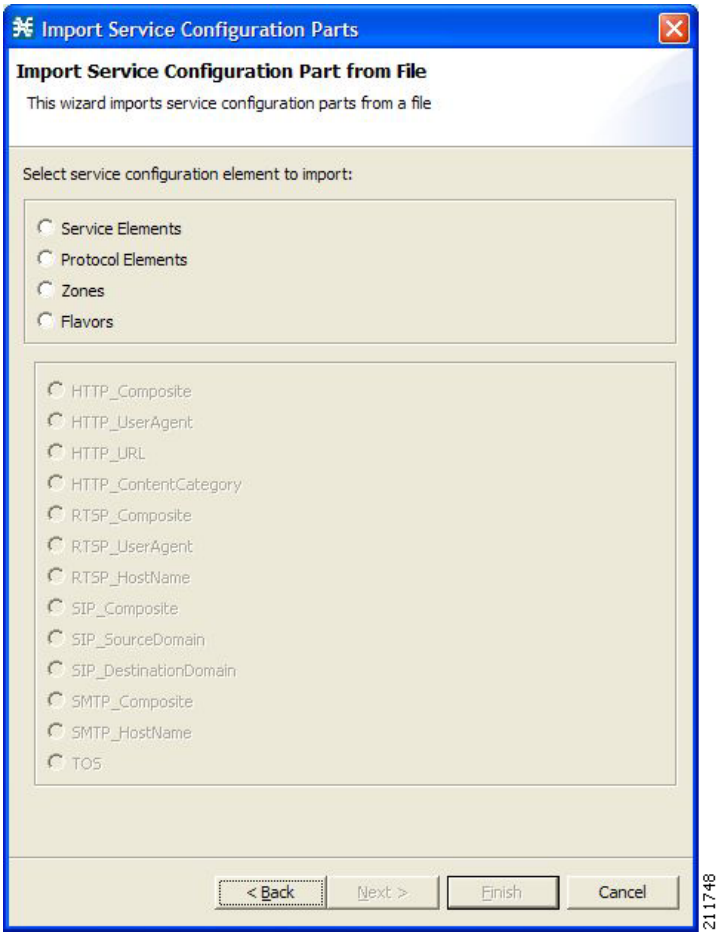
The Import dialog box appears.



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.



Step 4 Select one of the **Select service configuration element to import** radio buttons.

The radio buttons are:

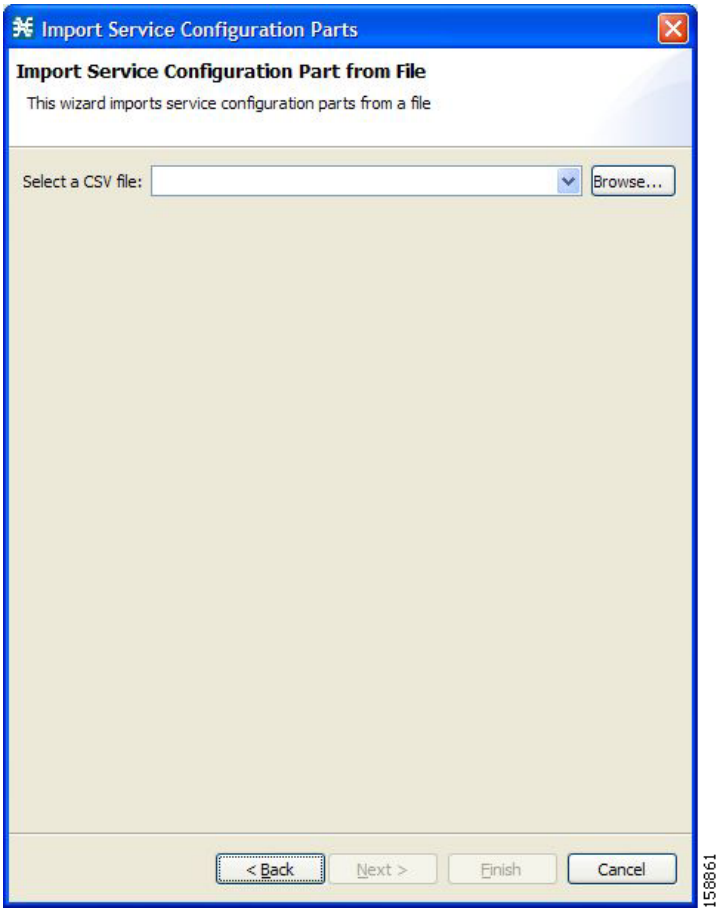
- **Service Elements**
- **Protocol Elements**
- **Zones**
- **Flavors**

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.



Step 7 Click **Browse.**

An Open dialog box appears.

Step 8 Browse to the folder containing the file to import, and select a CSV file.

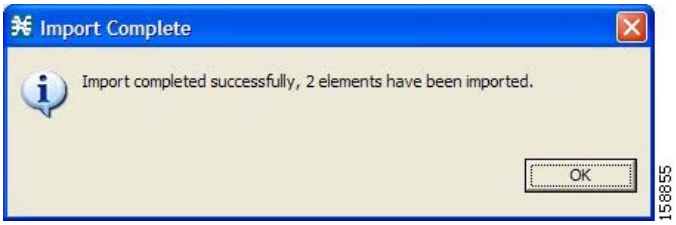
Step 9 Click **Open** to select the file.

The Open dialog box closes.

Step 10 Click **Finish.**

The configuration elements are imported from the file.

An Import Complete message appears.



Step 11 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 5-1
- **servconf,** the SCA BB Service Configuration Utility (see The SCA BB Service Configuration Utility, page 13-1)
- How to Validate the Current Service Configuration, page 6-13
- How to Apply a Service Configuration to SCE Platforms, page 6-14

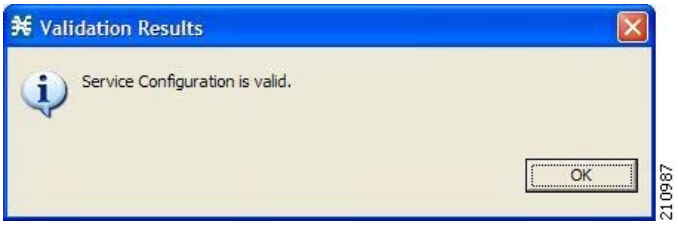
How to Validate the Current Service Configuration

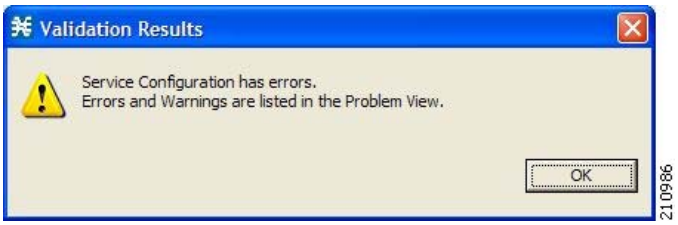
Use the Validate optionto validate the new or updated service configuration currently displayed. The validation process checks for overall service configuration coherence, and points out possible pitfalls in the service configuration.

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.





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.

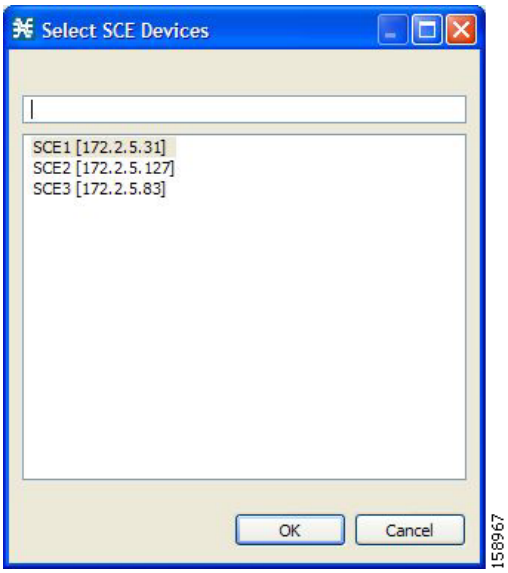
Note You can use the **Validate** menu command to manually validate the service configuration.

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 anSNMP 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 (**Apply Service Configuration to SCE Devices)**.

The Select SCE Devices dialog box appears.



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

Traffic classification is the first step in creating a Cisco Service Control Application for Broadband (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.

- Managing Services, page 7-1
- Managing Protocols, page 7-19
- Managing Zones, page 7-29
- Managing Protocol Signatures, page 7-33
- Managing Flavors, page 7-44
- Managing Content Filtering, page 7-53

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 on the basis of 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, hostnames 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 is 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). A default value of the service index is provided by the system. 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 7-3). You can modify them at any time (see How to Edit Services, page 7-7).

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 7-10).

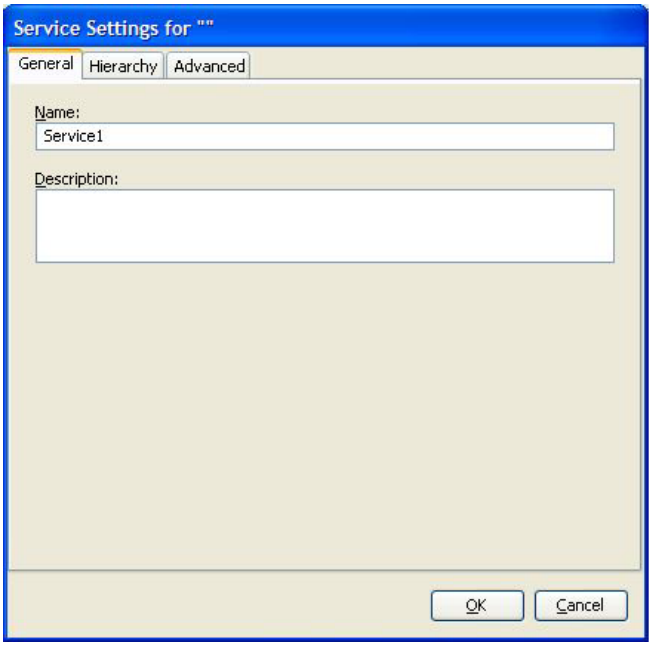
- How to Add a Service to a Service Configuration, page 7-3
- How to Define Hierarchical Settings for a Service, page 7-4
- How to Set the Service Index, page 7-5
- How to View Services, page 7-6

How to Add a Service to a Service Configuration

Step 1 In the Services tab, select a service from the service tree. This service will be the parent of the service you are adding.

Step 2 In the left pane, click (**Add Service**).

The Service Settings dialog box appears.



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 section How to Define Hierarchical Settings for a Service, page 7-4.

Step 6 (Optional) To specify an index for this service, continue with the instructions in the section How to Set the Service Index, page 7-5.

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.**

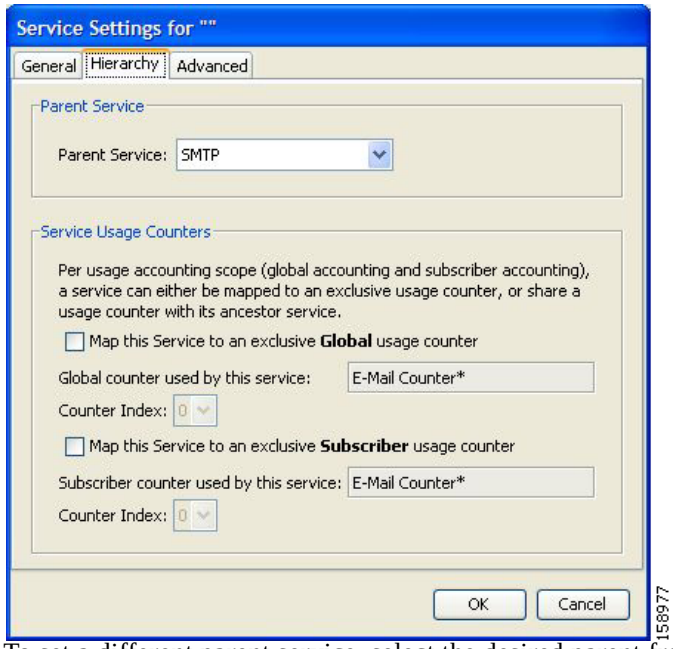
The Service Settings dialog box closes.

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.



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 its parent's global usage counter. 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 A default value of the counter index is provided by the system. Do not modify this value.

Step 4 By default, a new service uses its parent's subscriber usage counter. 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 A default value of the counter index is provided by the system. Do not modify this value.

Step 5 To specify an index for this service, continue with the instructions in the section How to Set the Service Index, page 7-5.

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.



Step 2 From the Set the Index for this Service drop-down list, select a service index.

The service index must an integer in the range 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.

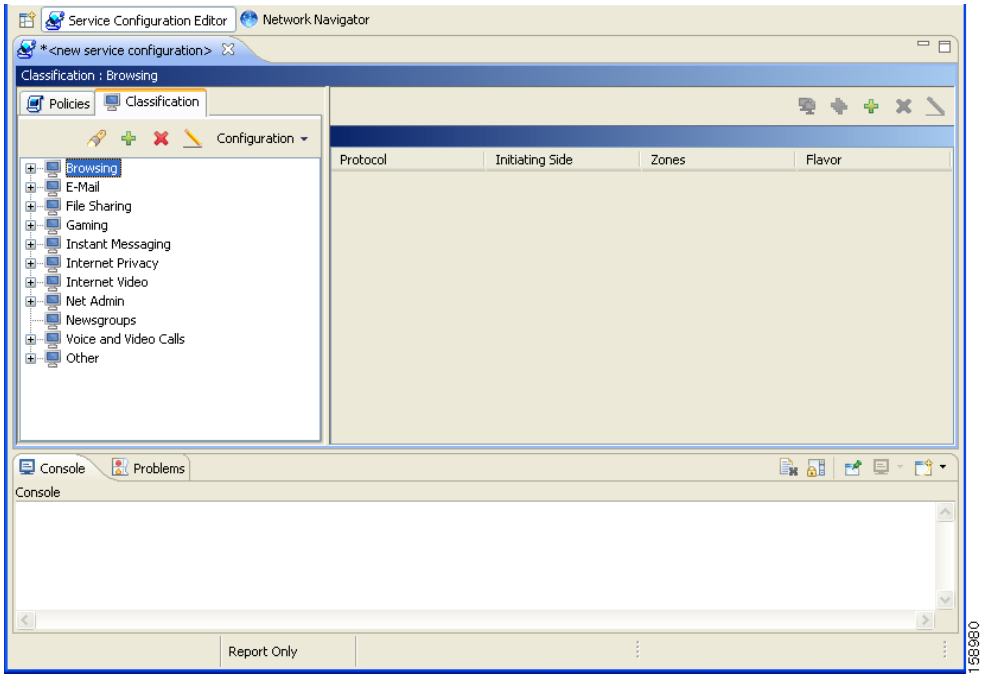
The service is added to the service tree as a child to the service selected in the Parent Service drop-down list.

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 **Services** tab.

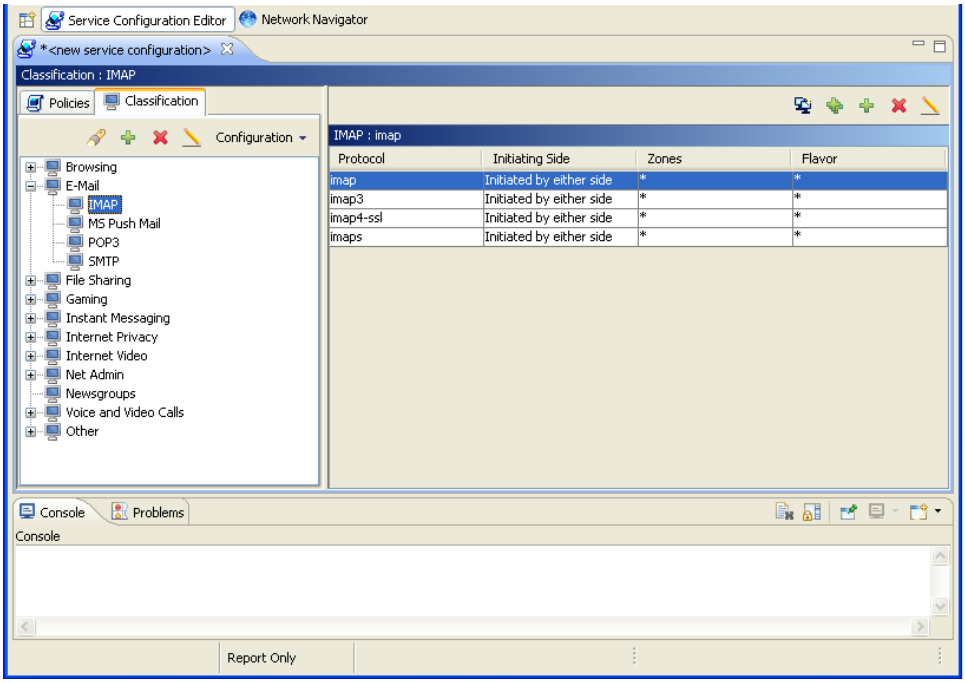
The Services tab appears.



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.



Step 3 To view more information about a service, select a service from the service tree and click (**Edit Service**).

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 included in the Console installation.

To add, modify, or delete service elements, see Managing Service Elements, page 7-9.

Step 1 In the Services tab, select a service from the service tree.

Step 2 In the left pane, click (**Edit Service**).

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 A default value of the counter index is provided by the system. 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 A default value of the counter index is provided by the system. 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 1 to 499; zero is reserved for the default service.

Note A default value of the service index is provided by the system. 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 in the Console installation, with the exception of the default service.

Step 1 In the Services tab, select a service from the service tree.

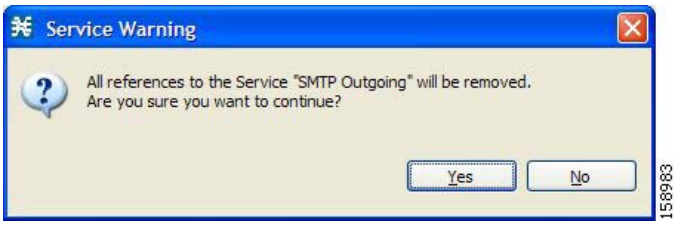
Step 2 In the left pane, click (**Delete Service**).

Step 3 A Service Warning message appears.



Step 4 Click **Yes.**

- If any package has a rule for this service (see Managing Rules, page 9-10), a second Service Warning message appears.



- 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 7-19, Managing Zones, page 7-29, and Managing Flavors, page 7-44.

A service configuration can contain up to 10,000 service elements. Every service element must be unique.

A traffic flow is mapped by a service element to the service element's service if it meets all five of the following criteria:

- 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

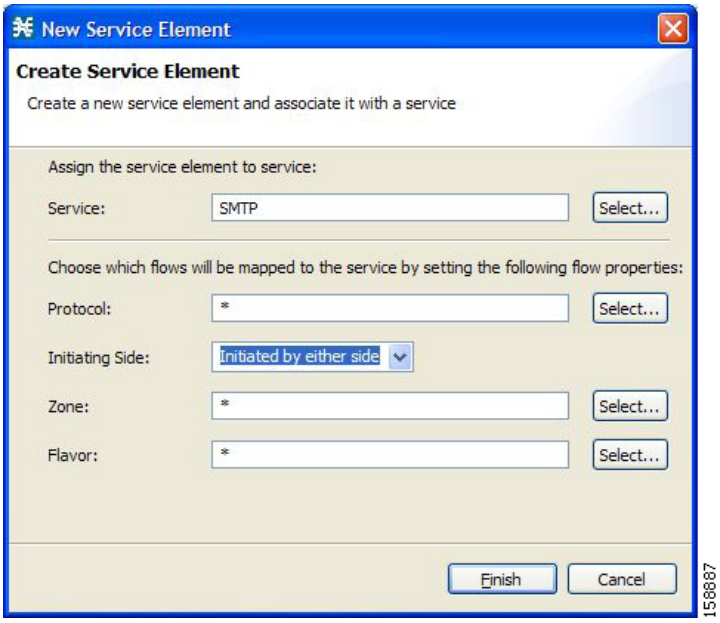
When necessary, you can add new service elements to a service. (The most useful service elements are included in the Console installation.) A service may have any number of service elements (subject to the limit of 10,000 service elements per service configuration).

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. If this occurs, modify the value in at least one field.

Step 1 In the Services tab, select a service from the service tree.

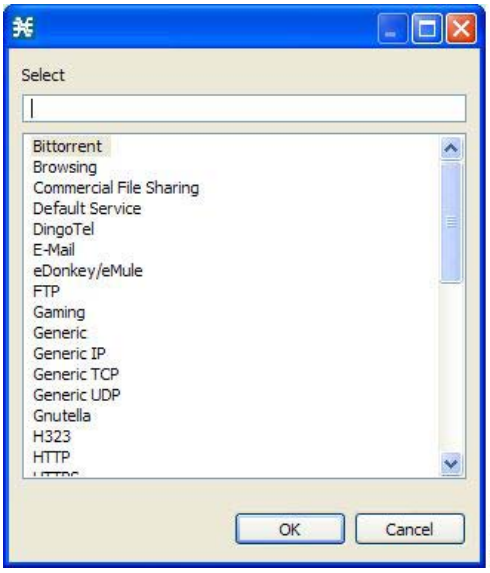
Step 2 In the right (Service Elements) pane, click (**Add Service Element)**.

The New Service Element dialog box appears.



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, displaying a list of all services.



Step 4 Select a service from the list.

Step 5 Click **OK.**

The Select a Service dialog box closes.

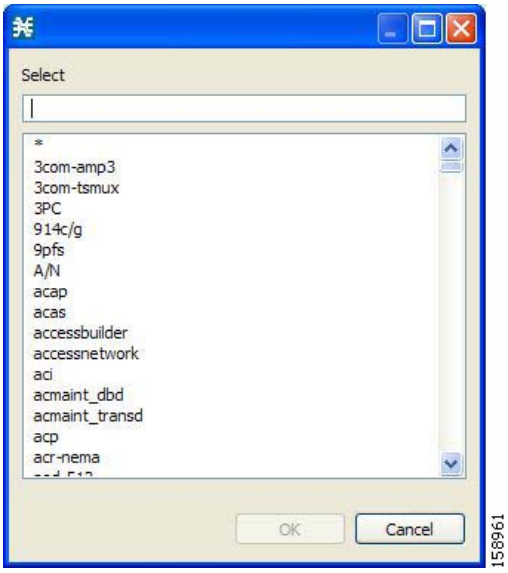
The selected service is displayed in the Service field of the New Service Element dialog box.

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 if a flow maps to this service element.

The Select a Protocol dialog box appears, 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.



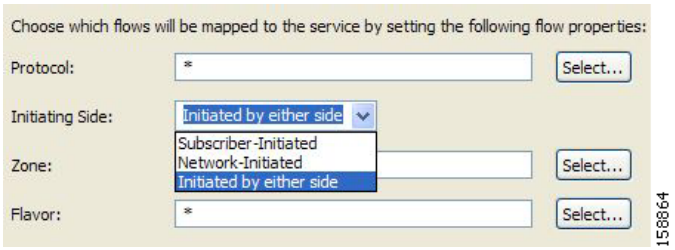
Step 7 Select a protocol from the list. You can type in the field at the top of the dialog box to help locate the desired protocol.

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, click the drop-down arrow.



Step 10 Select the appropriate initiating side from the drop-down list.

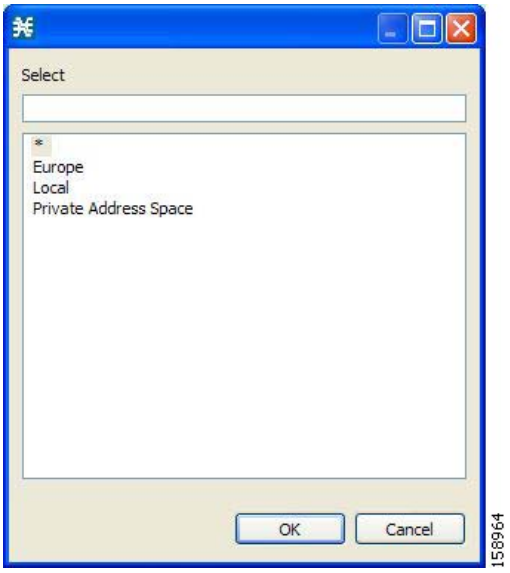
The following options are available:

- **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 if a flow maps to this service element.

The Select a Zone dialog box appears, displaying a list of all zones.



Step 12 Select a zone from the list.

Step 13 Click **OK.**

The Select a Zone dialog box closes.

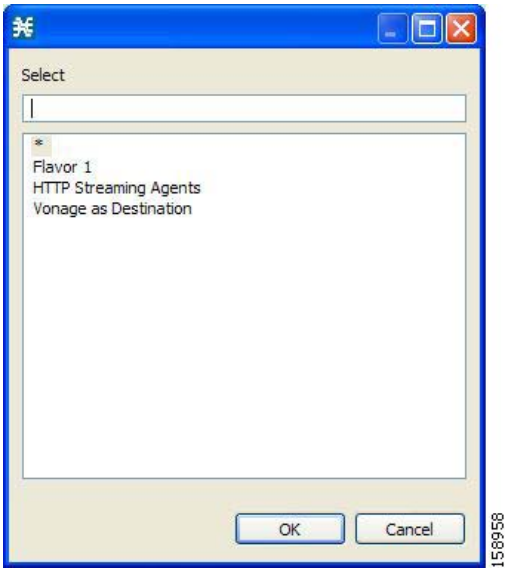
The selected zone is displayed in the Zone field of the New Service Element dialog box.

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 if a flow maps to this service element.

The Select a Flavor dialog box appears, 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.



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 make changes than to define the service element from scratch.

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. If this occurs, modify the value in at least one field.

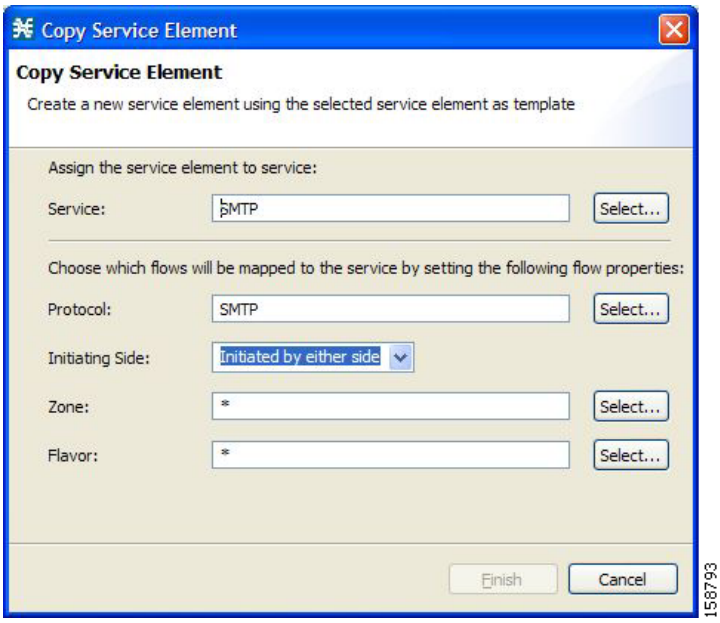
Step 1 In the Services tab, select a service from the service tree.

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 (**Duplicate Service Element**).

The Copy Service Element dialog box appears.



Step 4 Modify the service element (see How to Edit Service Elements, page 7-15).

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 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. If this occurs, modify the value in at least one field.

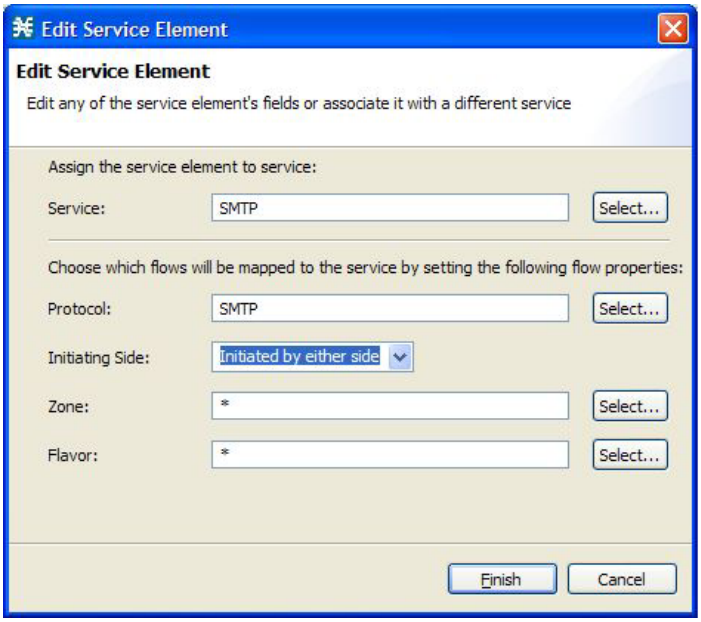
Step 1 In the Services tab, select a service from the service tree.

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 (**Edit Service Element**).

The Edit Service Element dialog box appears.



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 if 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 if 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 if 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 included in the Console installation.

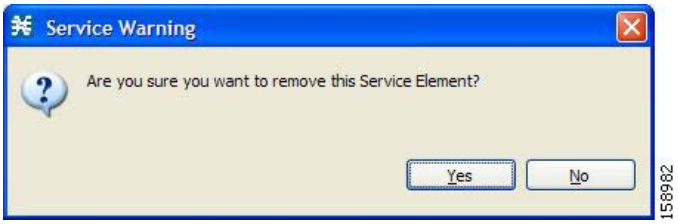
Step 1 In the Services tab, select a service from the service tree.

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 (**Delete Service Element**).

A Service Warning message appears.



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.

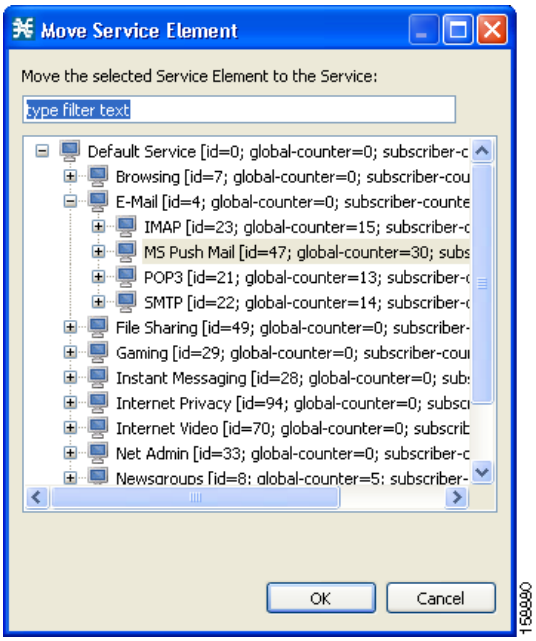
Step 1 In the Services tab, select a service from the service tree.

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 (**Move Service Element to Another Service**).

The Move Service Element dialog box appears, displaying the complete service tree.



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 Managing Service Elements, page 7-9).

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.

SCA BB supports many commercial and common protocols. For a complete list of protocols included with the current release of SCA BB, see "Protocols" in the "Default Service Configuration Reference Tables" chapter of the *Cisco Service Control Application for Broadband Reference Guide*. 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 How to Import a Dynamic Signature Script into a Service Configuration, page 7-38.)

- Viewing Protocols, page 7-19
- How to Add Protocols, page 7-22
- How to Edit Protocols, page 7-22
- How to Delete Protocols, page 7-23
- Managing Protocol Elements, page 7-24

Viewing Protocols

- How to View Protocols, page 7-19
- How to Filter the Protocols List, page 7-21

How to View Protocols

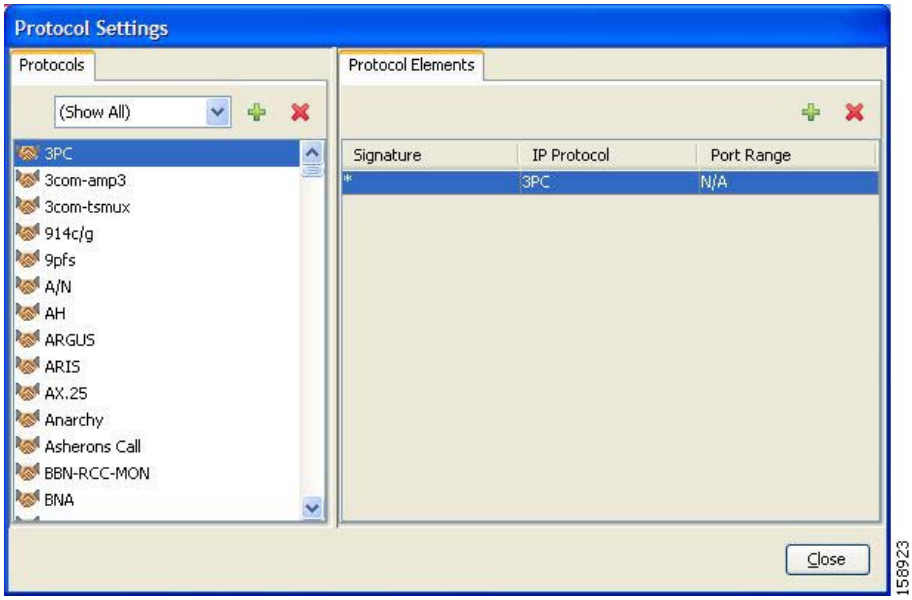
You can view a list of all protocols and their associated protocol elements.

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 Console main menu, choose **Configuration > Protocols.**

The Protocol Settings dialog box appears.



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, displaying the protocol name, description, and ID.



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.

There are ten categories of protocols:

- 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 Console main menu, choose **Configuration > 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 will be displayed.

How to Add Protocols

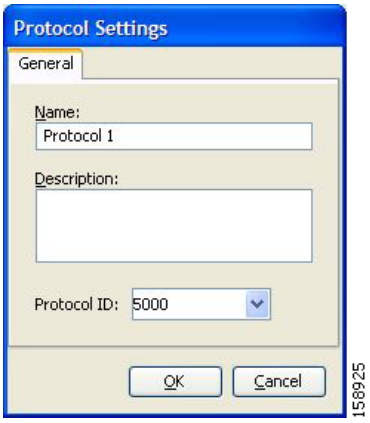
You can add new protocols to a service configuration, subject to the limit of 10,000 protocols per service configuration.

Step 1 From the Console main menu, choose **Configuration > Protocols.**

The Protocol Settings dialog box appears.

Step 2 In the Protocols tab, click (**Add Protocol)**.

The Protocol Settings dialog box appears.



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 5000 to 9998; lower values are reserved for protocols provided by SCA BB.

Note The value of the protocol ID is supplied automatically by the system. 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 7-25.

How to Edit Protocols

You can modify the parameters of a protocol, even those included in the Console installation.

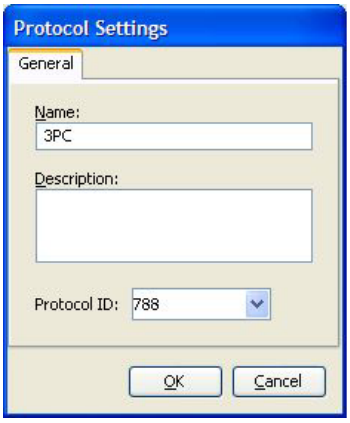
To add, modify, or delete protocol elements, see Managing Protocol Elements, page 7-24.

Step 1 From the Console main menu, choose **Configuration > Protocols.**

The Protocol Settings dialog box appears.

Step 2 In the Protocols tab, double-click a protocol.

The Protocol Settings dialog box appears.



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 5000 to 9998; lower values are reserved for protocols provided by SCA BB.

Note The value of the protocol ID is supplied automatically by the system. 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 included in the Console installation.

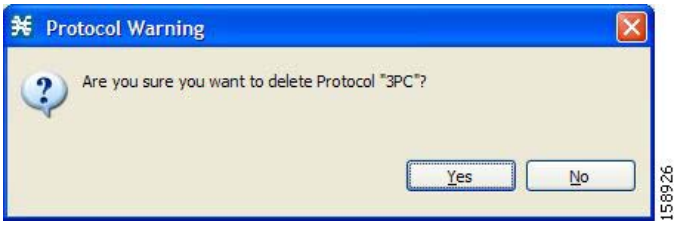
Step 1 From the Console main menu, choose **Configuration > Protocols.**

The Protocol Settings dialog box appears.

Step 2 In the Protocols tab, select a Protocol.

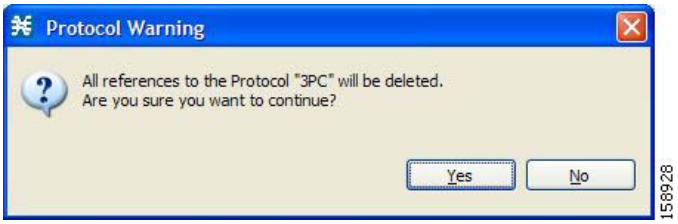
Step 3 In the Protocols tab, click (**Delete Protocol)**.

A Protocol Warning message appears.



Step 4 Click **Yes.**

- If any service element maps the selected protocol to a service (see Managing Service Elements, page 7-9), a second Protocol Warning message appears (even if the service is not used by any package).



- 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.

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

- 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 Console main menu, choose **Configuration** > **Protocols.**

The Protocol Settings dialog box appears.

Step 2 In the Protocols tab, select a protocol.

Step 3 In the Protocol Elements tab, click (**Add Protocol Element)**.

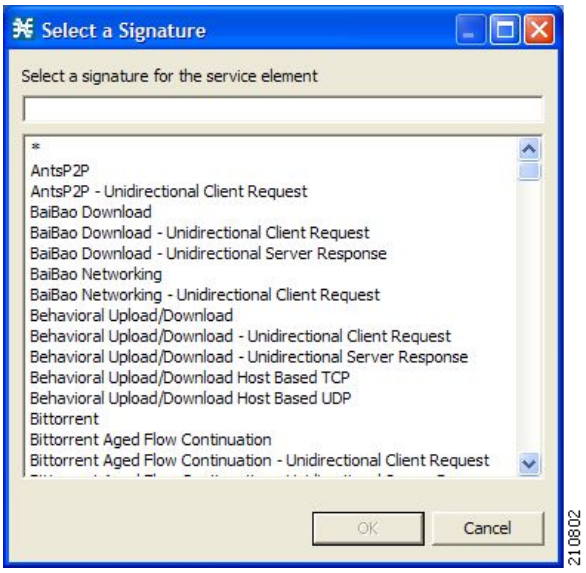
A protocol element is added to the protocol.

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 if a flow maps to this protocol element.

The Select a Signature dialog box appears, displaying a list of all signatures.



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.**

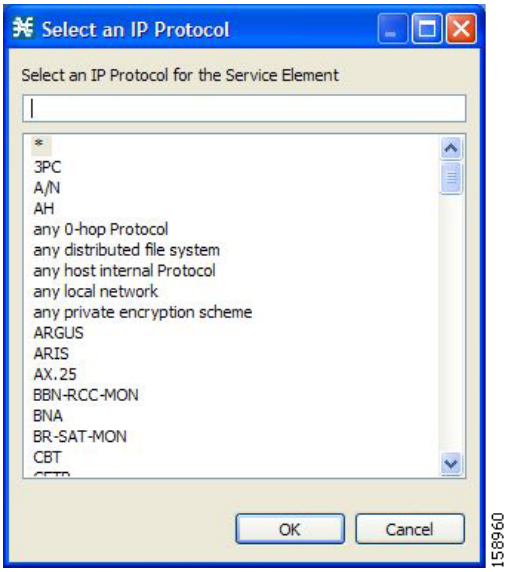
The Select a Signature dialog box closes.

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 if a flow maps to this protocol element.

The Select an IP Protocol dialog box appears, displaying a list of all IP protocols.



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, *).

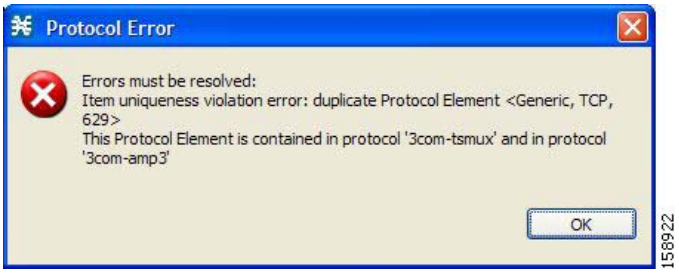
Only a flow whose port matches one of these ports will be mapped to this protocol element.

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.



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 included in the Console installation.

Note All changes to the protocol element are saved as you make them.

Step 1 From the Console main menu, choose **Configuration > 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 included in the Console installation.

Step 1 From the Console main menu, choose **Configuration > Protocols.**

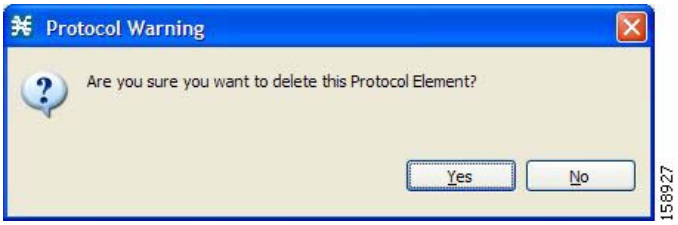
The Protocol Settings dialog box appears.

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  (**Delete Protocol Element)**.

A Protocol Warning message appears.



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 will be 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. Every zone item must be unique.

- How to View Zones, page 7-29
- How to Add Zones, page 7-30
- How to Edit Zones, page 7-30
- How to Delete Zones, page 7-31
- Managing Zone Items, page 7-32

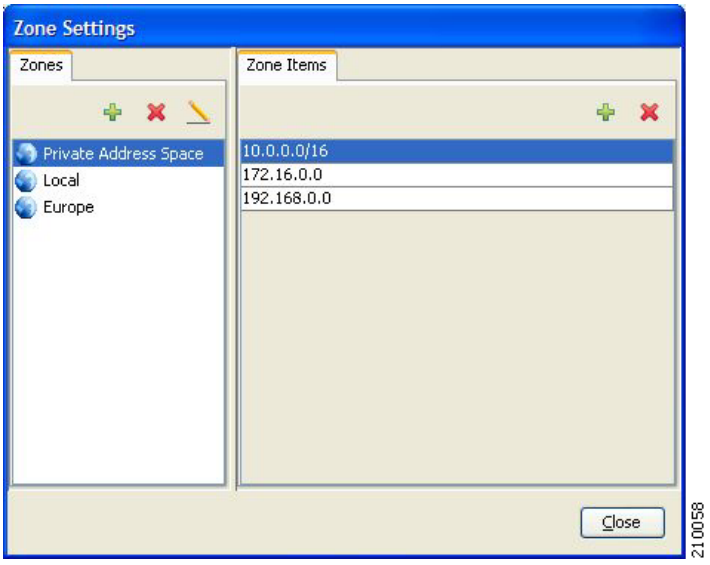
How to View Zones

You can view a list of all zones and their associated zone items.

Step 1 From the Console main menu, choose **Configuration > Zones.**

The Zone Settings dialog box appears.

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.



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.**

The Zone Settings dialog box closes.

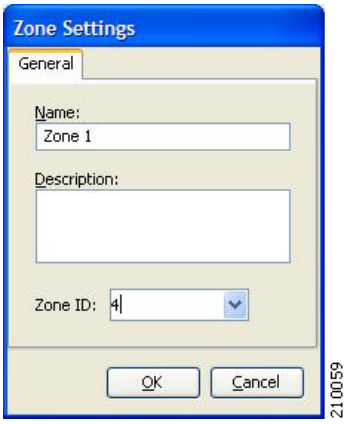
How to Add Zones

Step 1 From the Console main menu, choose **Configuration > Zones.**

The Zone Settings dialog box appears.

Step 2 In the Zones tab, click (**Add Zone**).

The Zone Settings dialog box appears.



Step 3 In the Name field, enter a unique name for the new zone.

Step 4 (Optional) From the Zone ID drop-down list, select an ID for the zone.

The zone ID must be a positive integer in the range 1 to 32767.

Note The value of the zone ID is supplied automatically by the system. Do not modify this field.

Step 5 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 7-32.)

How to Edit Zones

You can modify zone parameters at any time.

To add, modify, or delete zone items, see Managing Zone Items, page 7-32.

Step 1 From the Console main menu, choose **Configuration > Zones.**

The Zone Settings dialog box appears.

Step 2 In the Zones tab, select a zone.

Step 3 Click (**Edit Zone**).

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 ID drop-down list, select an ID for the zone.

  The zone ID must be a positive integer in the range 1 to 32767.

Note The value of the zone ID is supplied automatically by the system. 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.

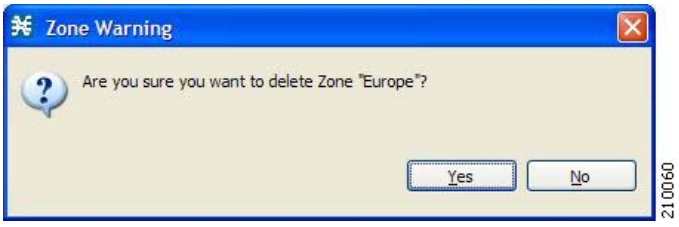
Step 1 From the Console main menu, choose **Configuration > Zones.**

The Zone Settings dialog box appears.

Step 2 In the Zones tab, select a zone.

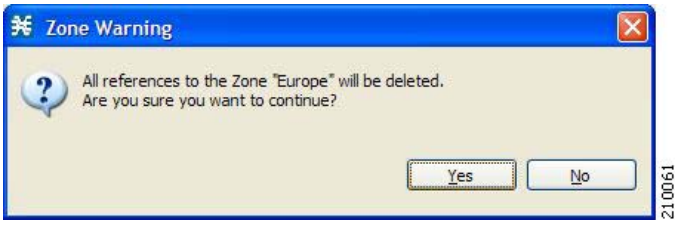
Step 3 In the Zones tab, click **(Delete Zone)**.

A Zone Warning message appears.



Step 4 Click **OK.**

- If any service element references the selected zone, a second Zone Warning message appears.



- 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 10,000 zone items. Every zone item must be unique.

How to Add Zone Items

You can add any number of zone items to a zone (subject to the limitation of 10,000 zone items per service configuration).

Step 1 From the Console main menu, choose **Configuration > Zones.**

The Zone Settings dialog box appears.

Step 2 In the Zones tab, select a zone.

Step 3 In the Zone Items tab, click (**Add Zone Item)**.

A new line is added to the Zone Items table.

Step 4 Double-click the new list item and enter a valid value.

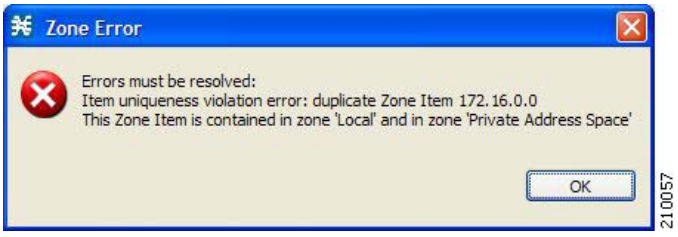
A valid value is either a single IP address (for example, 63.111.106.7) or a range of IP addresses (for example, 194.90.12.0/24).

Step 5 Repeat Steps 3 and 4 for other IP addresses that will be 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.



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 Console main menu, choose **Configuration > 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 Console main menu, choose **Configuration > 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  (**Delete Zone Item**).

The zone item is deleted.

Step 5 Click **Close.**

The Zone Settings dialog box closes.

Managing Protocol Signatures

A protocol signature is a set of parameters that uniquely identify a protocol.

- Viewing Signatures, page 7-34
- Dynamic Signatures, page 7-35

Viewing Signatures

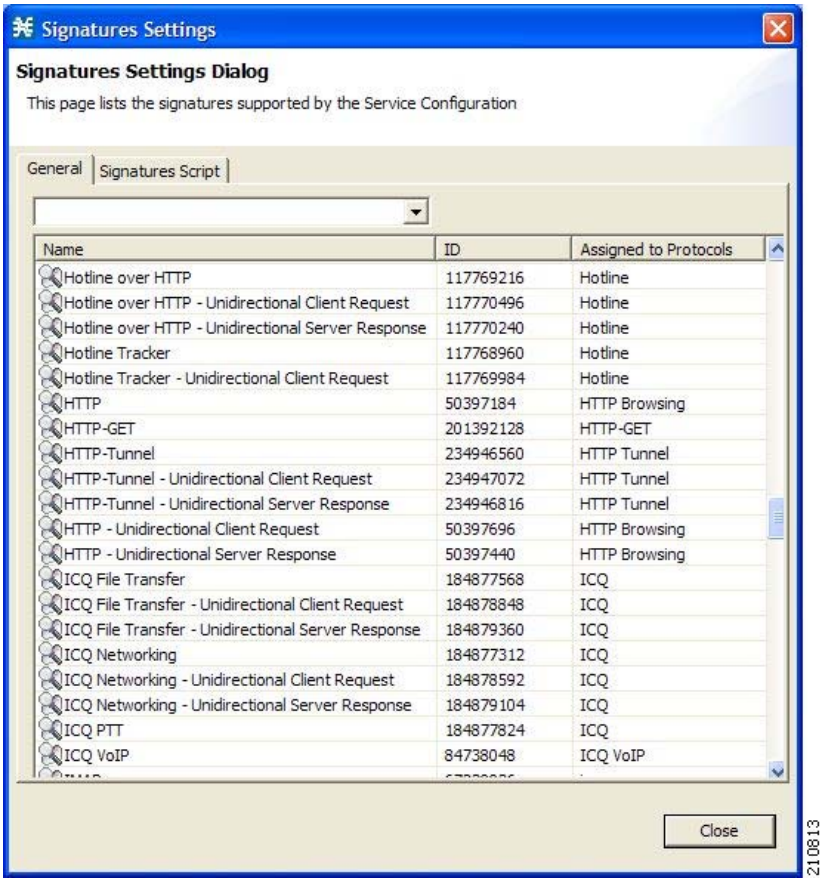
- How to View Signatures, page 7-34
- How to Filter the Signatures List, page 7-35

How to View Signatures

You can view a list of all signatures and the protocol to which each is assigned.

Step 1 From the Console main menu, choose **Configuration > Signatures Settings.**

The Signatures Settings dialog box appears.



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.

There are eight categories of signatures:

- 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

Note Some signatures belong to more than one category.

Step 1 From the Console main menu, choose **Configuration > 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. This 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 4-10.
- Creating and modifying signatures is described in Using the Signature Editor, page 12-1.
- Using **servconf,** the SCA BB Server Configuration Utility, to apply signatures is described in The SCA BB Service Configuration Utility, page 13-1.

The following sections describe working with dynamic signatures in the Service Configuration Editor.

- Dynamic Signature Script Files, page 7-36
- The Default DSS File, page 7-39

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 will match 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.

DSS files are periodically released by Cisco or its partners 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 7-38.

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 12-1).

- How to View Information About the Current Dynamic Signatures, page 7-36
- How to Import a Dynamic Signature Script into a Service Configuration, page 7-38
- How to Remove Dynamic Signatures, page 7-38

How to View Information About the Current Dynamic Signatures

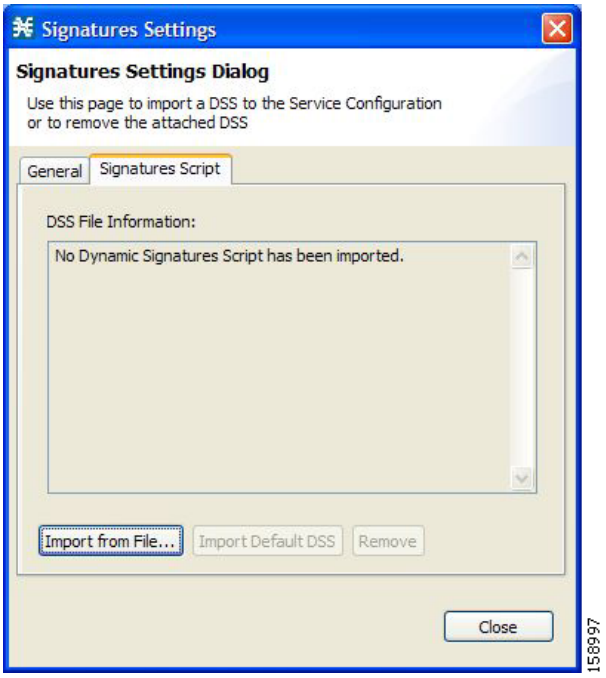
Step 1 From the Console main menu, choose **Configuration > Signatures Settings.**

The Signatures Settings dialog box appears.

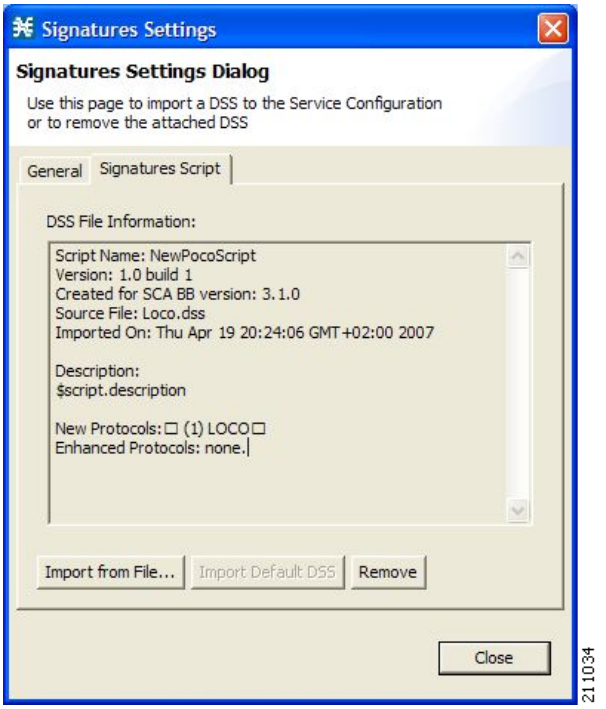
Step 2 Click the **Signatures Script** tab.

The Signatures Script tab opens.

- If no DSS file was imported into the current service configuration, the Signatures Settings dialog box displays a message informing you of this.



- 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.



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 12-1).

Note It is recommended that you import the latest default DSS file (see How to Import the Default DSS File Automatically, page 7-43) 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 Console main menu, choose **Configuration > Signatures Settings.**

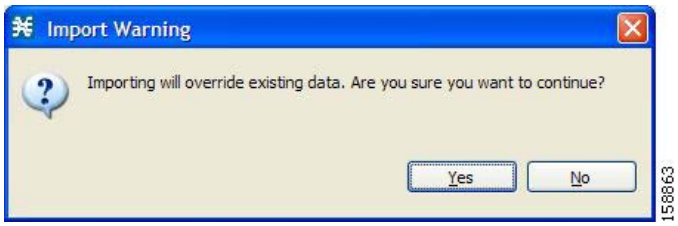
The Signatures Settings dialog box appears.

Step 2 Click the **Signatures Script** tab.

The Signatures Script tab opens.

Step 3 Click **Import from File.**

An Import Warning message appears.



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 Console main menu, choose **Configuration > Signatures Settings.**

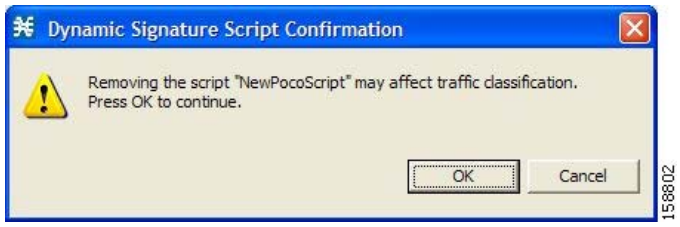
The Signatures Settings dialog box appears.

Step 2 Click the **Signatures Script** tab.

The Signatures Script tab opens.

Step 3 Click **Remove.**

A Dynamic Signature Script Confirmation message appears.



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.



- 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 4-10) 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 SCA BB Signature Configuration Utility, page 13-8.

- 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 SCA BB Signature Configuration Utility, page 13-8. 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 7-40
- Importing Dynamic Signatures from the Default DSS File, page 7-43

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 12-13) 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 will be overwritten by the new protocol pack.

- How to Set a Protocol Pack as the Default DSS File, page 7-40
- How to Clear the Default DSS File, page 7-42

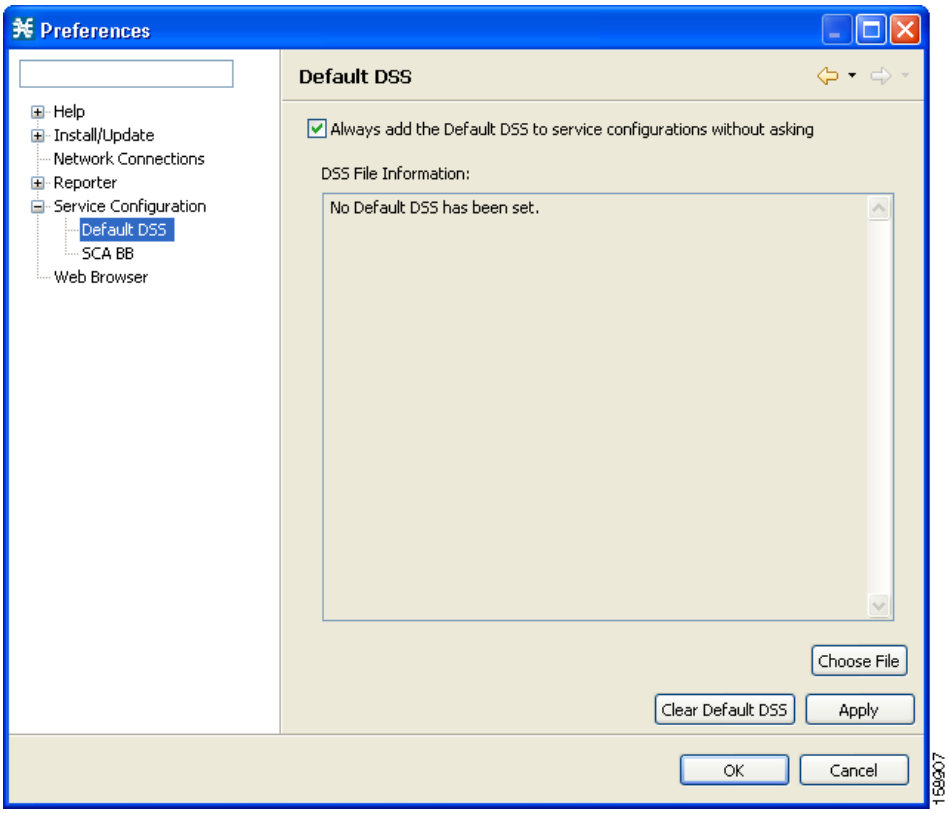
How to Set a Protocol Pack as the Default DSS File

Step 1 From the Console main menu, choose **Window** > **Preferences.**

The Preferences dialog box appears.

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 **Choose File.**

An Open dialog box appears.

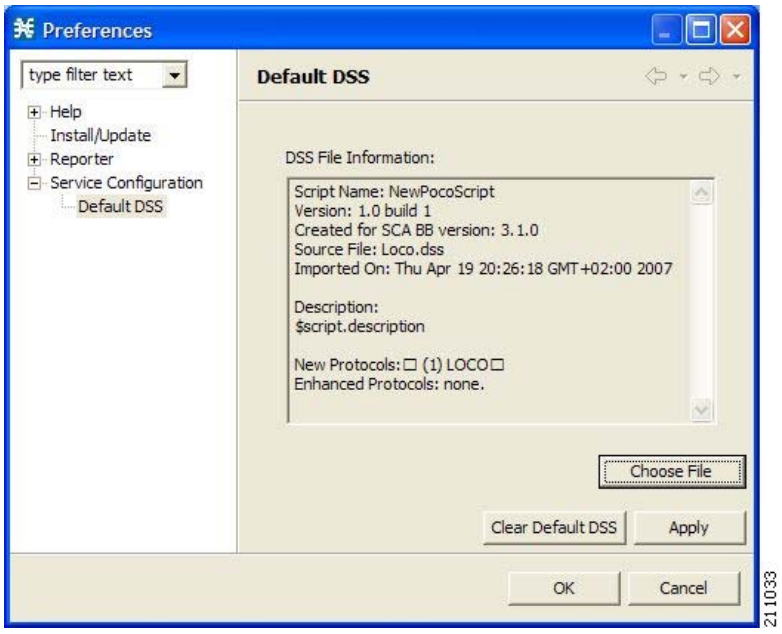
Step 4 From the Files of type drop-down list, select the file type of the protocol pack.

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.



Step 7 Click **OK.**

The DSS file is copied to C:\Documents and Settings\<user name>\.p-cube\default3.1.6.dss as the default DSS file.

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\<user name>\.p-cube\default3.1.6.dss is deleted.

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 7-43
- How to Import the Default DSS File Manually, page 7-43

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.



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 Console main menu, choose **Configuration > Signatures Settings.**

The Signatures Settings dialog box appears

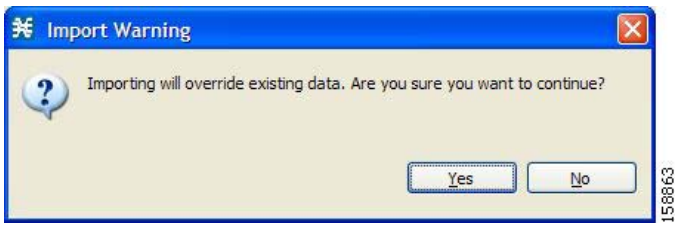
Step 2 Click the **Signatures Script** tab.

The Signatures Script tab opens, with the Import Default DSS button enabled.



Step 3 Click **Import Default DSS.**

An Import Warning message appears.



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 7-50). 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 7-45
- How to View Flavors, page 7-46
- How to Add Flavors, page 7-47
- How to Edit Flavors, page 7-48
- How to Delete Flavors, page 7-49
- Managing Flavor Items, page 7-50

Flavor Types and Parameters

Table 7-1 lists available flavor types.

Table 7-1 SCA BB Flavors

Flavor Type	Valid Values
HTTP User Agent	Prefix string (the string may include spaces) A partial string must be followed by "*" (that is, a value of "abc" will only match "abc"; a value of "abc*" will match any string that begins with "abc")
HTTP URL	<host suffix, path prefix, path suffix, URL parameters prefix> • Host—From the beginning of the URL till the first "/" • Path—The section from the first "/" to the "?" • URL parameters—Any string following the "?" (You do not need to start the parameters prefix with "?")
HTTP Composite	<HTTP User Agent flavor, HTTP URL flavor>
HTTP Content Category	Value selected from Select a Content Category dialog box
RTSP User Agent	Prefix string
RTSP Host Name	Host suffix
RTSP Composite	<RTSP User Agent flavor, RTSP Host Name flavor>
SIP Source Domain	Host suffix

Table 7-1 SCA BB Flavors (continued)

Flavor Type	Valid Values
SIP Composite	<SIP source domain, SIP destination domain>
SMTP Host Name	Host suffix
ToS	DSCP ToS (integer between 0 and 63)

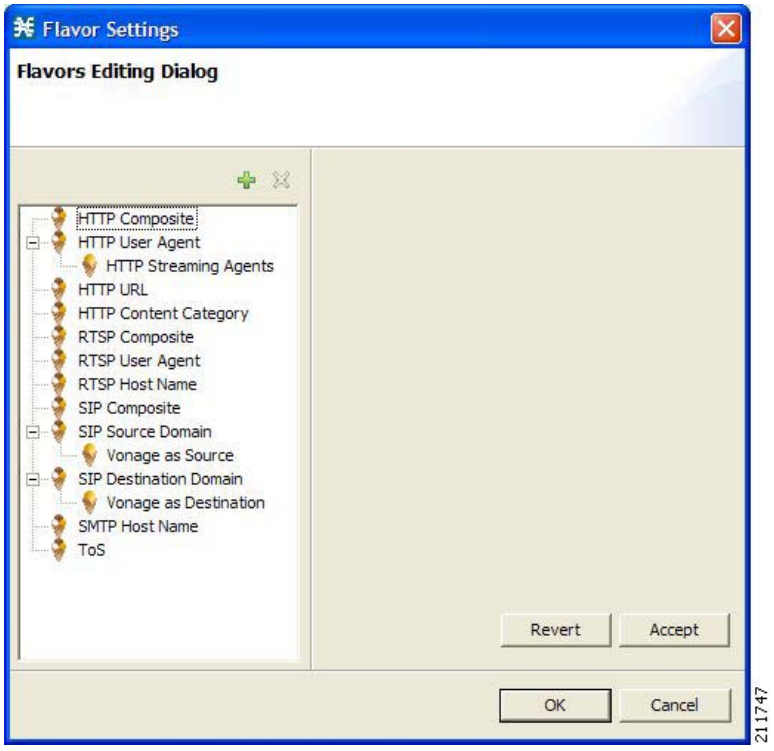
Note Composite Flavors are pairs of two defined flavors.

How to View Flavors

You can view a list of all flavors and their associated flavor items.

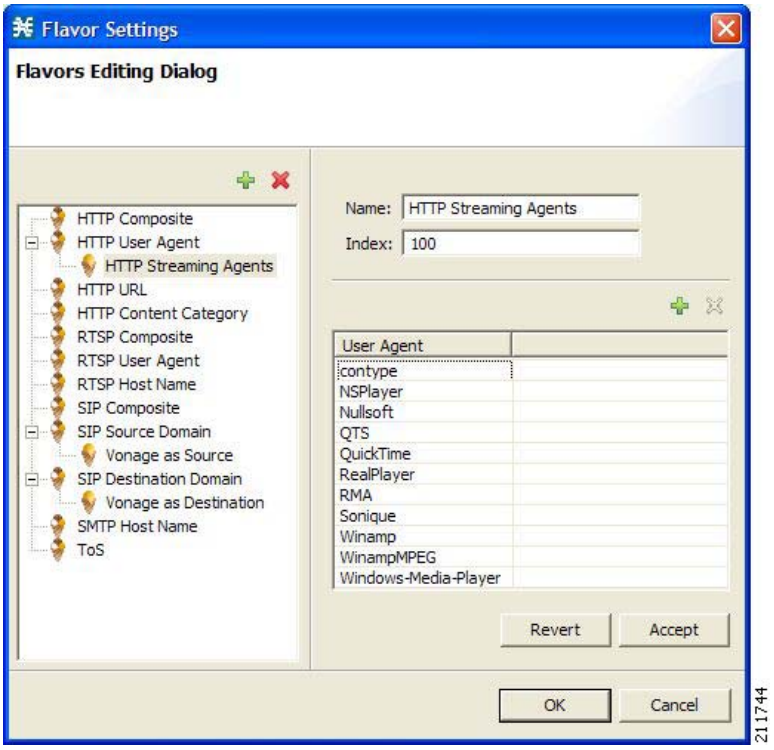
Step 1 From the Console main menu, choose **Configuration > Flavors.**

The Flavor Settings dialog box appears.



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.



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 add any number of flavors to a service configuration.

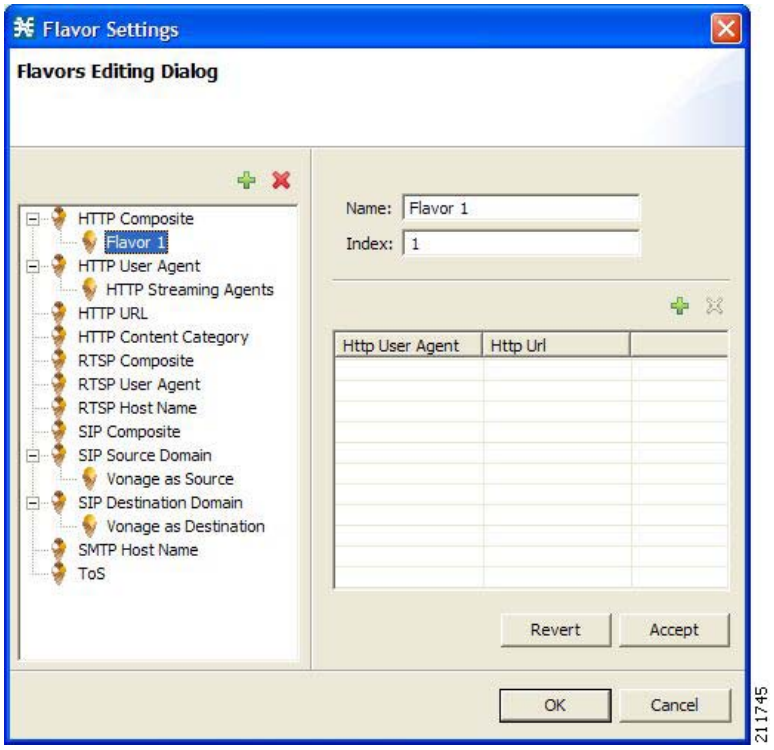
Step 1 From the Console main menu, choose **Configuration > Flavors.**

The Flavor Settings dialog box appears.

Step 2 In the flavor tree, select a flavor type.

Step 3 Click .

A new flavor of the selected type is added to the flavor tree.



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 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 1 to 32767.

You have defined the flavor. You can now add flavor items. (See How to Add Flavor Items, page 7-50.)

How to Edit Flavors

You can modify flavor parameters at any time.

To add, modify, or delete flavor items, see Managing Flavor Items, page 7-50.

Step 1 From the Console main menu, choose **Configuration > 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 1 to 32767.

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 Console main menu, choose **Configuration > Flavors.**

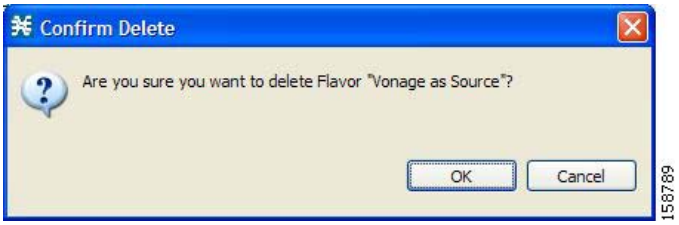
The Flavor Settings dialog box appears.

Step 2 In the flavor tree, right-click a flavor.

A popup menu appears.

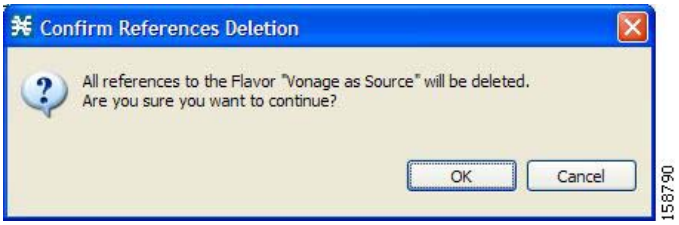
Step 3 Click (**Delete)**.

A Confirm Delete message appears.



Step 4 Click **OK.**

- If any service element references the selected flavor, a Confirm References Delete message appears.



- 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 7-45).

There is a maximum number of flavor items for each flavor type (see the following section). For each flavor type, every flavor item must be unique.

- Maximum Number of Flavor Items per Flavor Type, page 7-50
- How to Add Flavor Items, page 7-50
- How to Edit Flavor Items, page 7-52
- How to Delete Flavor Items, page 7-53

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 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

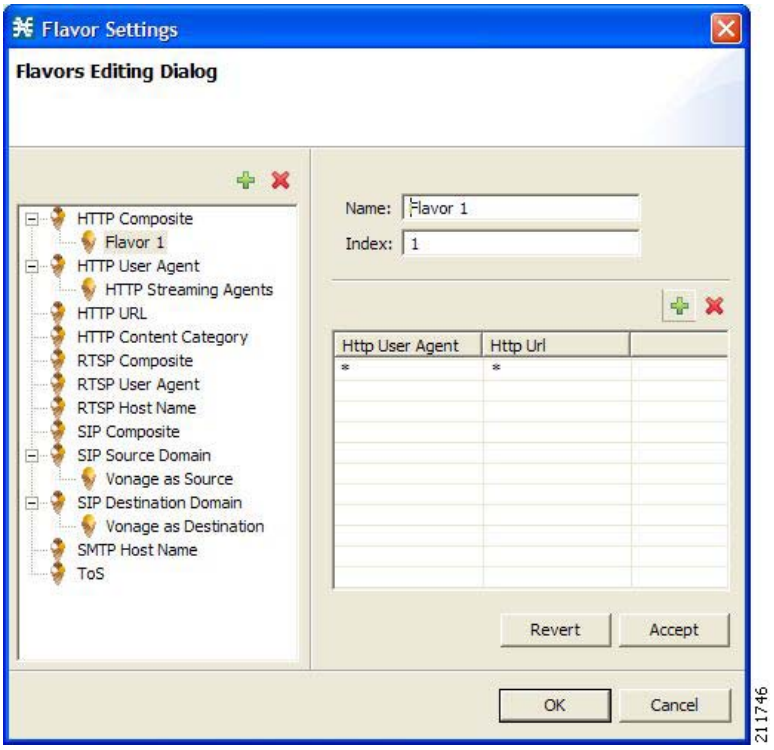
You can add any number of flavor items to a flavor (subject to the limitation of the total number of each type of flavor item per service configuration, as listed in the previous section).

Step 1 From the Console main menu, choose **Configuration > Flavors.**

The Flavor Settings dialog box appears.

Step 2 In the flavor tree, click a flavor.

Step 3 Above the flavor item list, click  (**Create New Flavor Item**).



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 7-45).

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.

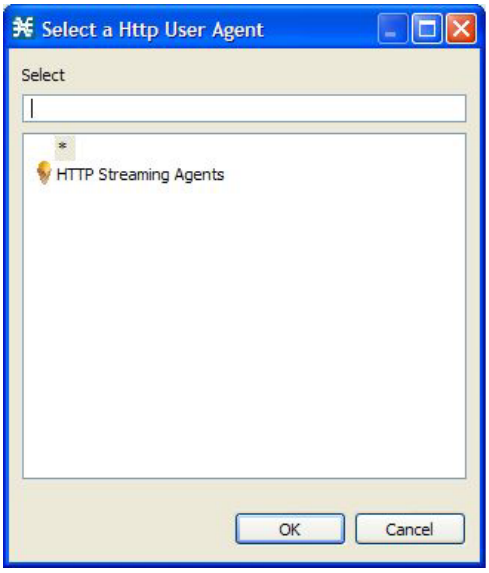
For composite flavors and for the HTTP Content Category flavor:

a. Click the asterisk.

A Browse button is displayed in the cell.

b. Click the **Browse** button.

A Select dialog box appears, 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 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 Console main menu, choose **Configuration > 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 Console main menu, choose **Configuration > 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 (**Delete)**.

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.

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.

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 7-54
- The Content Filtering CLI, page 7-54
- How to Configure the RDR Formatter, page 7-56
- How to Enter Line Interface Configuration Mode, page 7-56
- Managing Content Filtering Settings, page 7-57

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 SCA BB traffic control and reporting. For example, users 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 7-54
- The Cisco CPA Client, page 7-54
- The SurfControl CPA Server, page 7-54

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 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 7-56.

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 SCA BB with the categorization results.

The CPA client is installed as part of the SCA BB application (PQI) installation. Use the SCE platform Command-Line Interface (CLI) (see The Content Filtering CLI, page 7-54) 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 the *Cisco Service Control Engine (SCE) CLI Command Reference*.

- CPA Client CLI Commands, page 7-55
- Description of CPA Client CLI Commands, page 7-55

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 7-56).
- 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
`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)

Table 7-4 CPA Client: Monitored Parameters (continued)

Parameter	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 the "Raw Data Formatting: The RDR Formatter and NetFlow Exporting" chapter of the *Cisco Service Control Engine (SCE) 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, 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. Add content filtering rules to existing packages or create new packages that include content filtering rules.
4. Enable content filtering for selected packages.
5. Apply the service configuration.

- Importing Content Filtering Categories, page 7-57
- How to Configure Content Filtering, page 7-64
- How to View Content Filtering Settings, page 7-65
- How to Remove Content Filtering Settings, page 7-65

Importing Content Filtering Categories

Before you can control HTTP flows based on content, you must import an XML file provided with the installation.

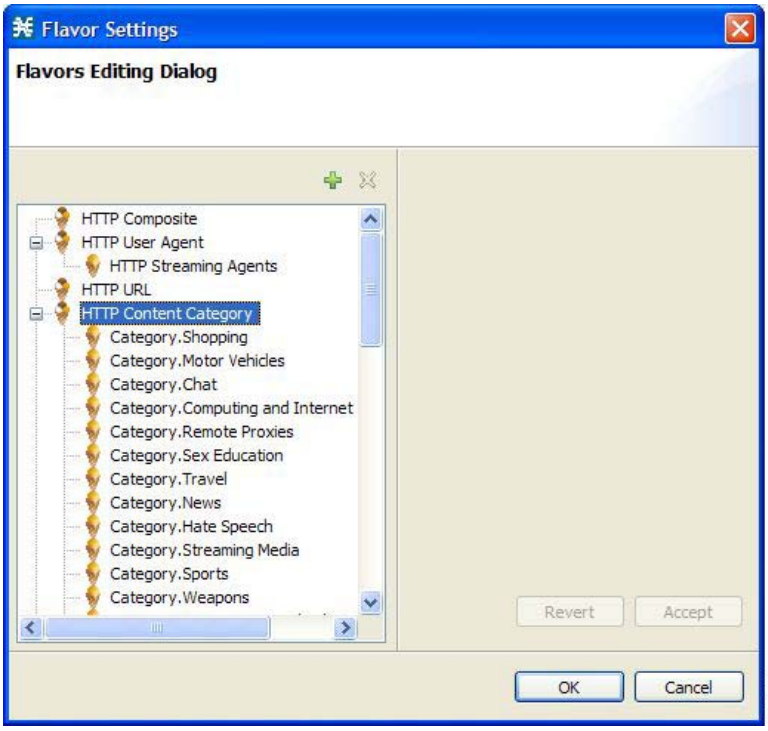
After you unzip the installation package, this file is located in the URL Filtering subfolder.

Note You cannot import content filtering categories when unidirectional classification is enabled.

- HTTP Content Category Flavors, page 7-57
- HTTP Browsing with Categories Service Elements, page 7-58
- How to Import Content Filtering Categories Using the Import Dialog Box, page 7-59
- How to Import Content Filtering Categories Using the HTTP Content Filtering Settings Dialog Box, page 7-62

HTTP Content Category Flavors

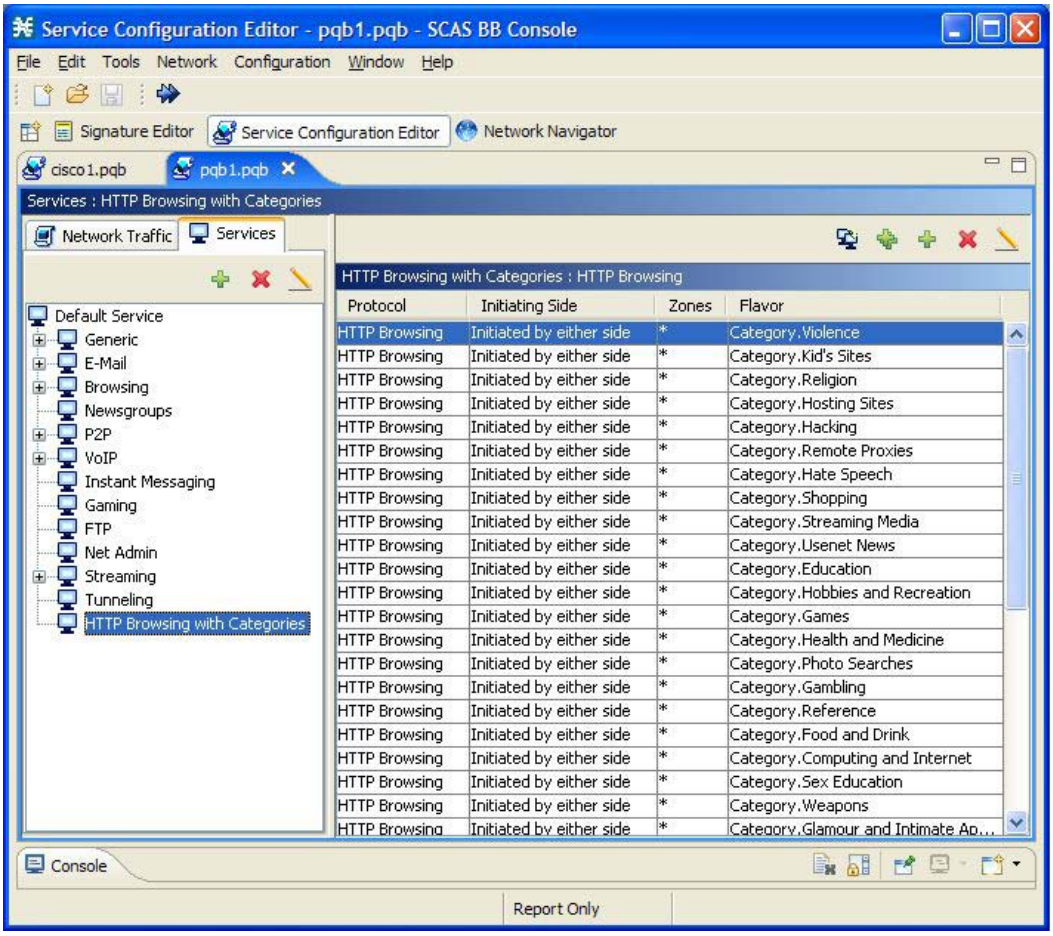
By default, SCA BB creates a separate flavor (of type HTTP Content Category) for each content category when importing the XML file.



You can create additional HTTP Content Category Flavors that include two or more content categories. (See How to Add Flavors, page 7-47.)

HTTP Browsing with Categories Service Elements

By default, 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.



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

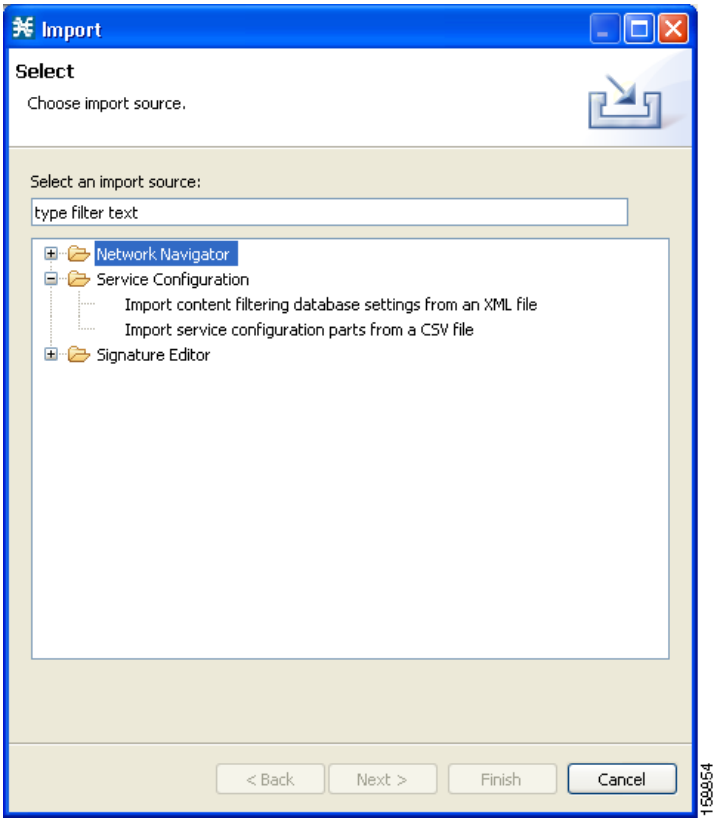
You can import content filtering categories using either the **File > Import** menu option or the **Configuration > Content Filtering** menu option.

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.**

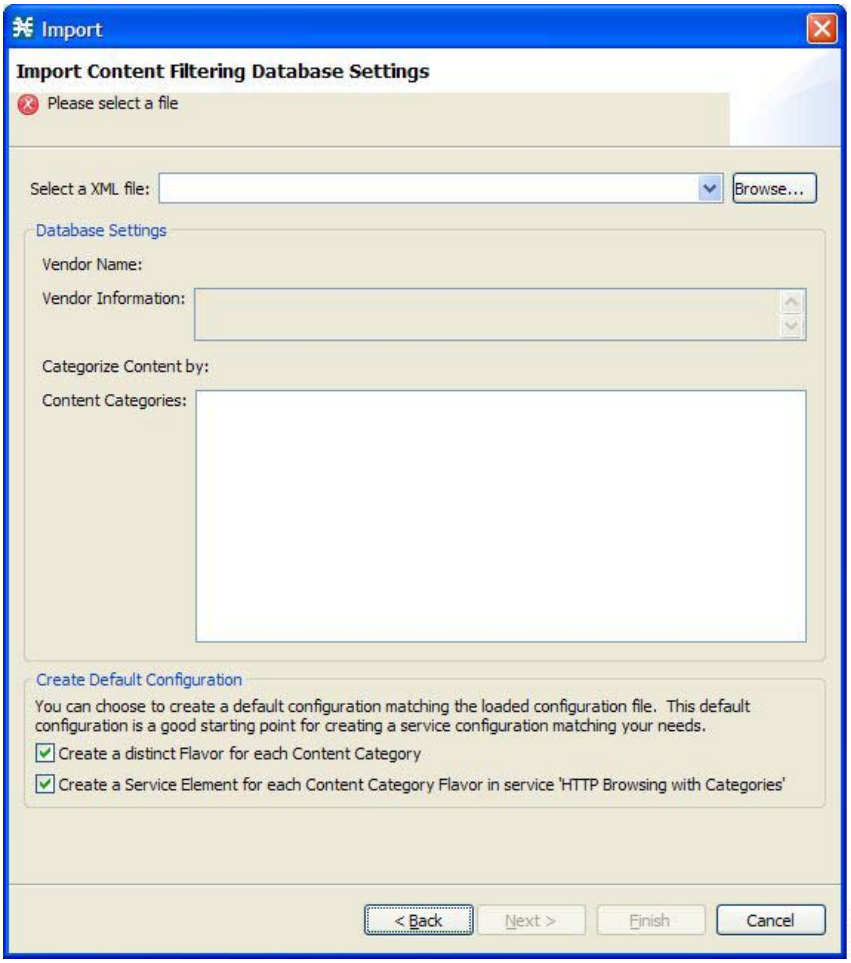
The Import dialog box appears.



Step 2 From the import source list, select **Import content filtering database settings from XML file.**

Step 3 Click **Next.**

The Import Content Filtering Database Settings dialog box appears.



Step 4 Click the **Browse** button next to the Select a XML file field.

An Open dialog box appears.

Step 5 Browse to the folder containing the file to import, and select it.

Note For SurfControl's CPA, 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, 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, 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.

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 > Content Filtering** menu option.

This procedure explains how to import using the **Configuration > Content Filtering** menu option.

Note This is equivalent to the previous procedure.

Step 1 From the Console main menu, choose **Configuration > 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 a XML file field.

An Open dialog box appears.

Step 5 Browse to the folder containing the file to import, and select it.

Note For SurfControl's CPA, 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, 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, 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.

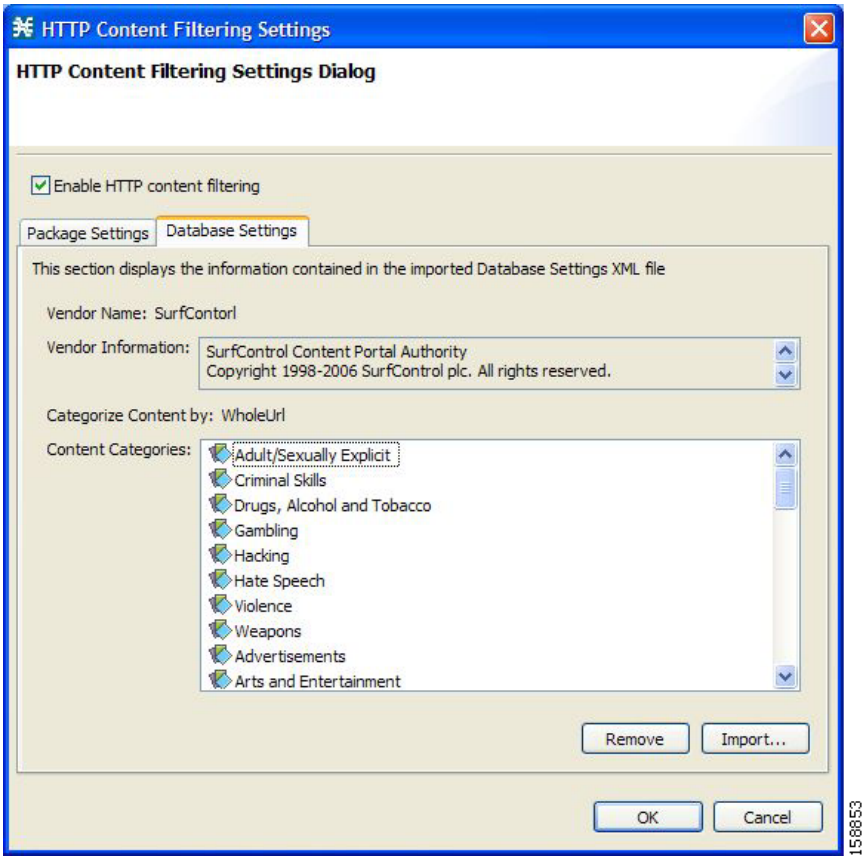
- To disable this option, uncheck the **Create a Service Element for each Content Category Flavor in Service 'HTTP Browsing with Categories'** check box.

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.



Step 10 Click **OK.**

The HTTP Content Filtering Settings dialog box closes.

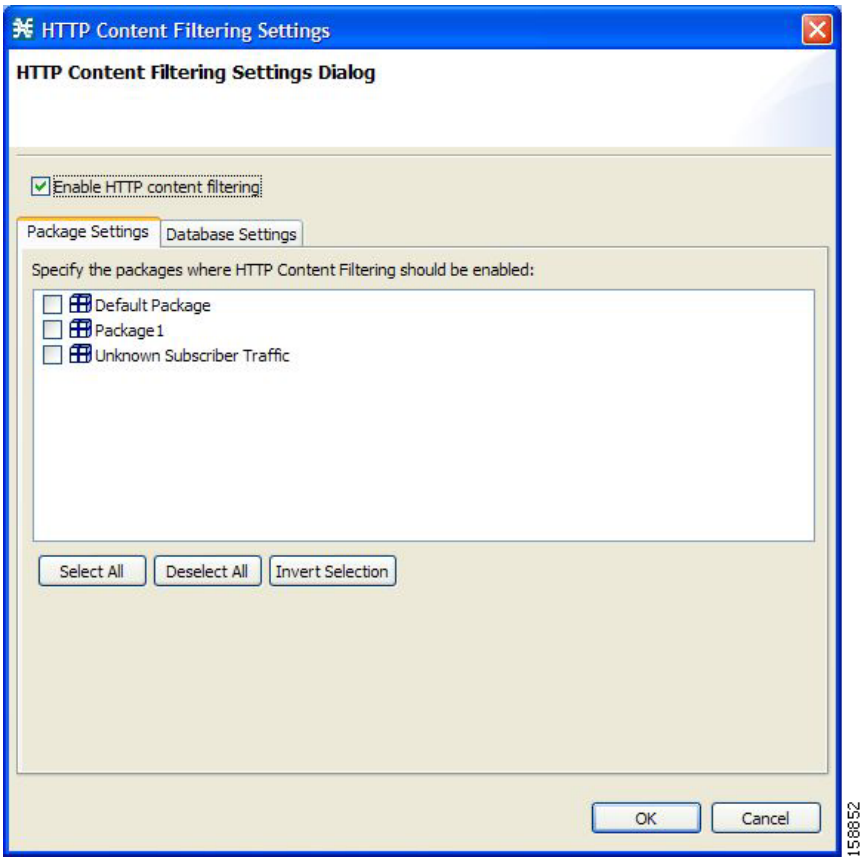
How to Configure Content Filtering

You can specify the packages where content filtering will be enabled. For packages where content filtering is disabled, HTTP flows will be classified normally.

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



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 vendor's content categories.

Step 1 From the Console main menu, choose **Configuration > 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 vendor's content categories.

Step 3 Click **OK.**

The HTTP Content Filtering Settings dialog box closes.

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 Console main menu, choose **Configuration > Content Filtering.**

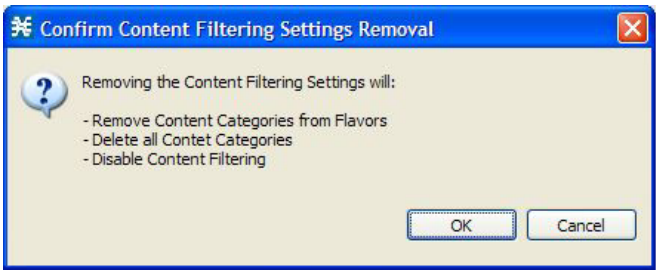
The HTTP Content Filtering Settings dialog box appears.

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.



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.



CHAPTER 8

Using the Service Configuration Editor: Traffic Accounting and Reporting

This module explains how to work with usage counters and Raw Data Records (RDRs).

Traffic Accounting and Reporting is the second step in creating a Cisco Service Control Application for Broadband (SCA BB) service configuration.

- Usage Counters, page 8-1
- Raw Data Records, page 8-2
- NetFlow records, page 8-2
- Managing RDR Settings, page 8-2

Usage Counters

The 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 are 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. For example, in the default service configuration the SMTP and POP3 services share the E-Mail service usage counters. The assignment of services to usage counters is determined by the service hierarchy. How to Edit Services, page 7-7, explains how to configure the service hierarchy.

The SCA BB also collects and maintains various network metrics per package.

Package usage counters are used by the system to generate data about the total use of each package. A package can use either its own usage counters, or those of the parent package. The assignment of packages to usage counters is determined by the package hierarchy. How to Set Advanced Package Options, page 9-7, explains how to configure the package hierarchy.

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. The content and structure of each type of RDR is listed in the "Raw Data Records: Formats and Field Contents" chapter of the *Cisco Service Control Application for Broadband Reference Guide*.

- RDRs are not generated for filtered traffic (see Filtering the Traffic Flows, page 10-17).
- All RDR data is based on Layer 3 volume.

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
- 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 the *Cisco Service Control Application for Broadband Reference Guide*.

- RDRs are not generated for filtered traffic (see Filtering the Traffic Flows, page 10-17).
- 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 will be generated

- Log RDRs tab—Allows you to specify the packages and services for which Log RDRs will be 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-TimeSignaling RDRs will be generated

Note Media Flow RDRs and Malicious Traffic Periodic RDRs are enabled and configured in the How to Edit Advanced Service Configuration Options, page 10-44.

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

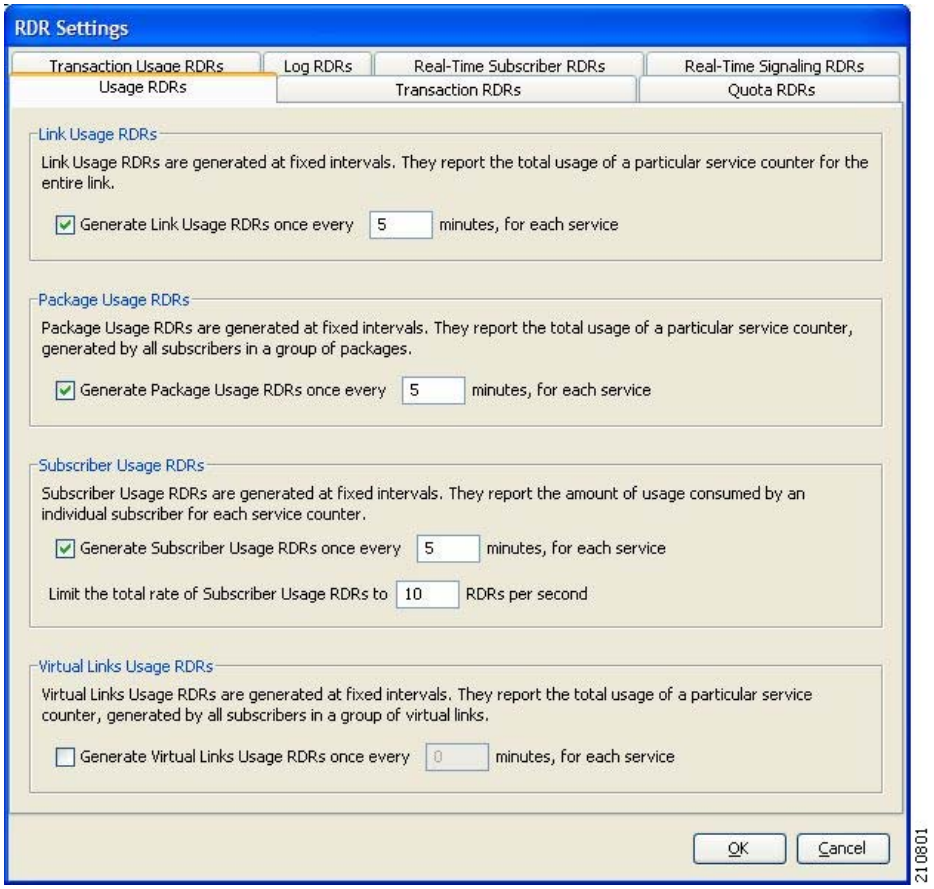
You can enable or disable the generation of each type of Usage RDR, and set the generation interval for each type of Usage RDR. You can limit the generation rate of Subscriber Usage RDRs. This is advisable when there are a large number of subscribers.

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 this user's package (see How to Define Per-Flow Actions for a Rule, page 9-14), or if the user has exceeded the allowed quota for this service (see Managing Quotas, page 9-50).

Step 1 From the Console main menu, choose **Configuration > RDR Settings.**

The RDR Settings dialog box appears.



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 contains 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 will be generated for this service, compared to other services.

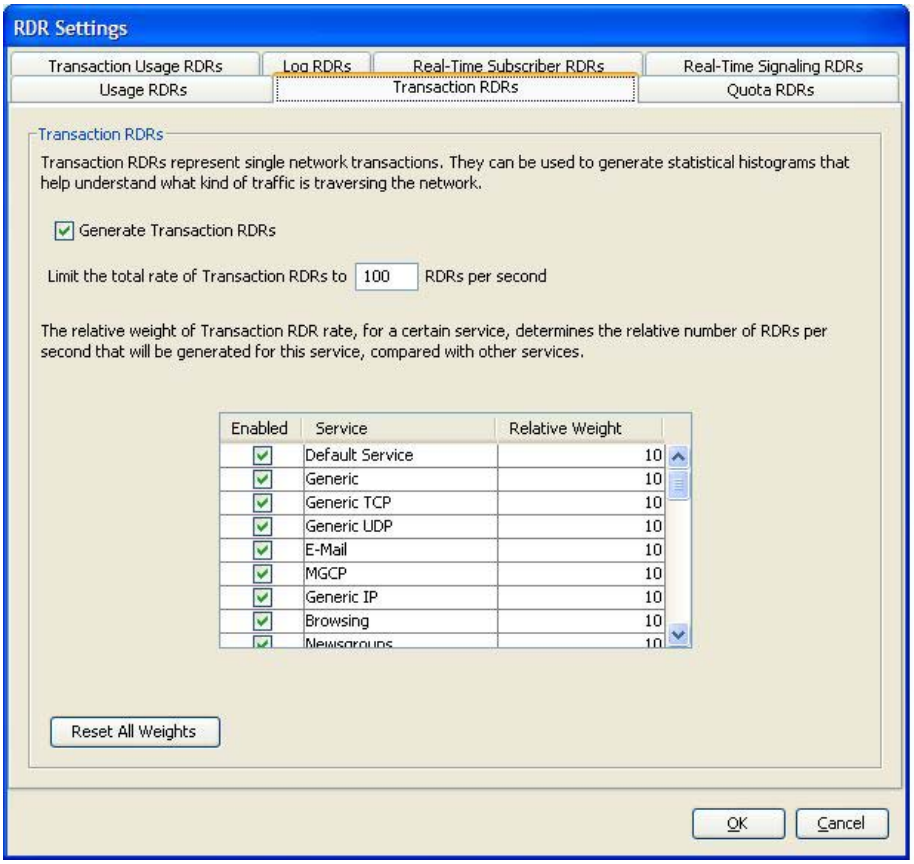
By default, at most 100 Transaction RDRs are generated per second, and all services are given the same weight.

Step 1 From the Console main menu, choose **Configuration > RDR Settings.**

The RDR Settings dialog box appears.

Step 2 Click the **Transaction RDRs** tab.

The Transaction RDRs tab opens.



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 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.

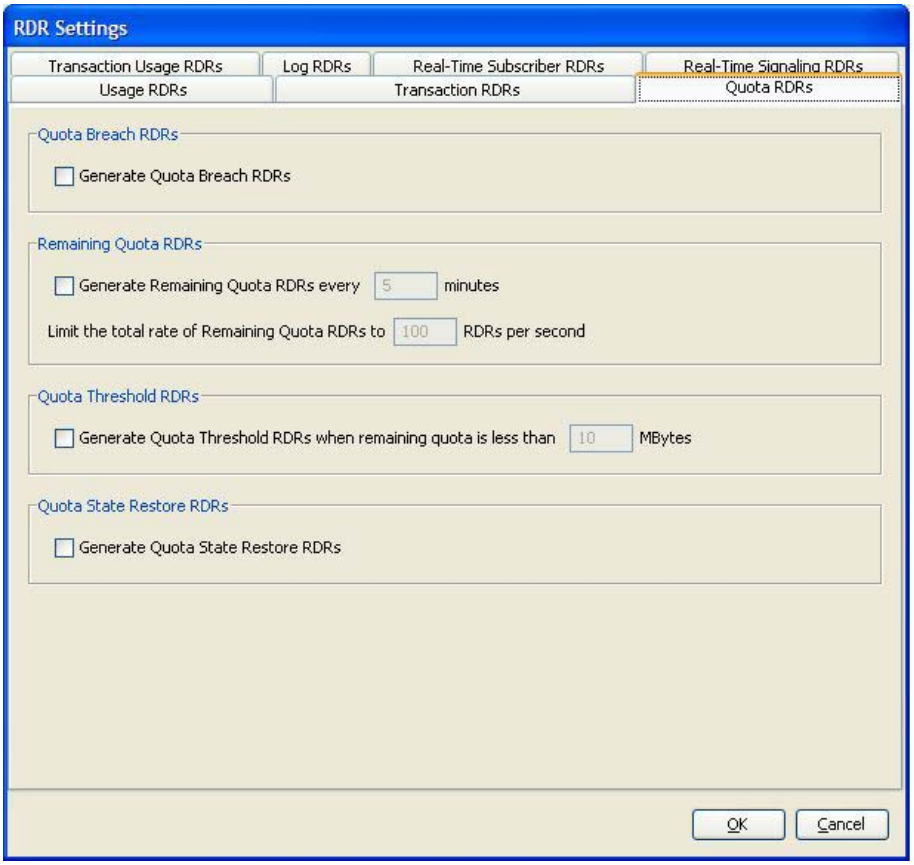
By default, all Quota RDRs are disabled.

Step 1 From the Console main menu, choose **Configuration > RDR Settings.**

The RDR Settings dialog box appears.

Step 2 Click the **Quota RDRs** tab.

The Quota RDRs tab opens.



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 will be 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 will also be 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 in the How to Edit Advanced Service Configuration Options, page 10-44.

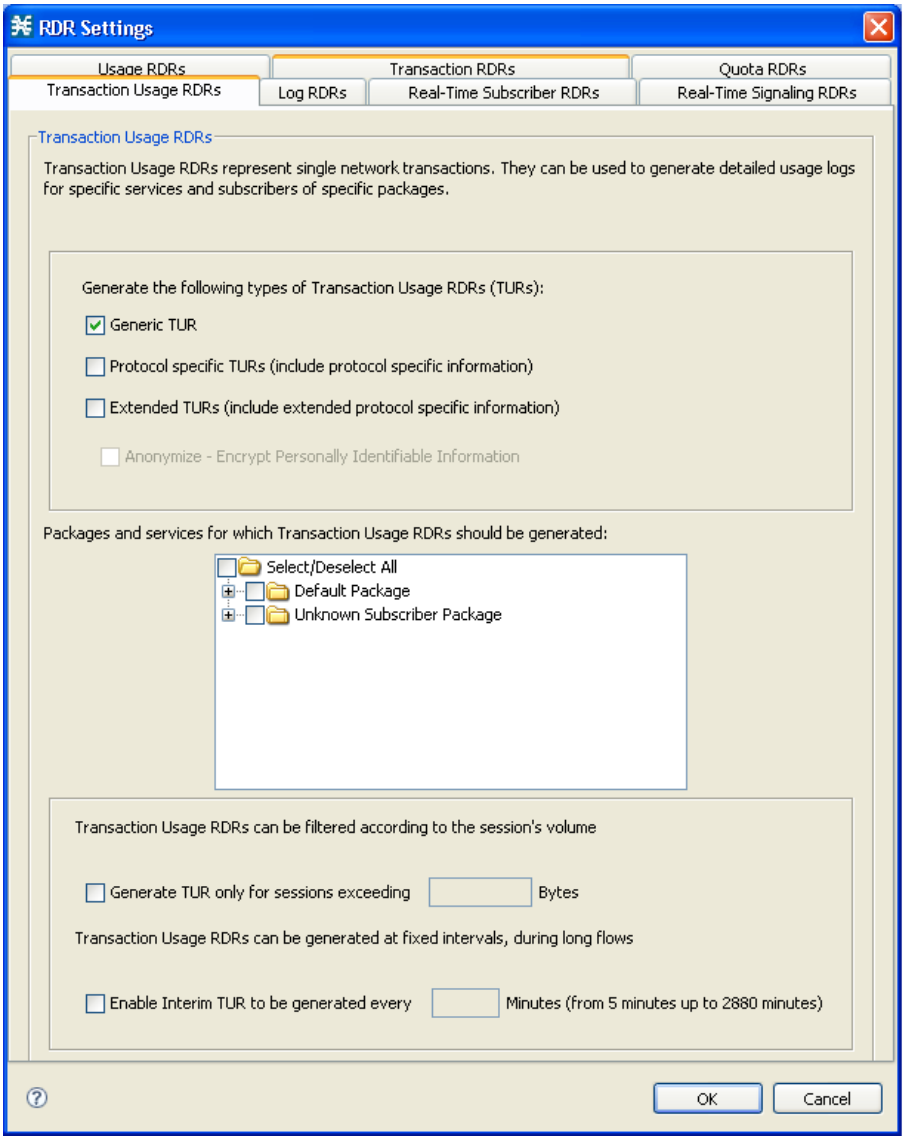
(When enabled, Media Flow RDRs are generated at the end of every SIP and Skype media flow; you can use them to distinguish between SIP voice and video calls.)

Step 1 From the Console main menu, choose **Configuration > RDR Settings.**

The RDR Settings dialog box appears.

Step 2 Click the **Transaction Usage RDRs** tab.

The Transaction Usage RDRs tab opens.



Step 3 (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 4 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 5 (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 6 (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 7 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

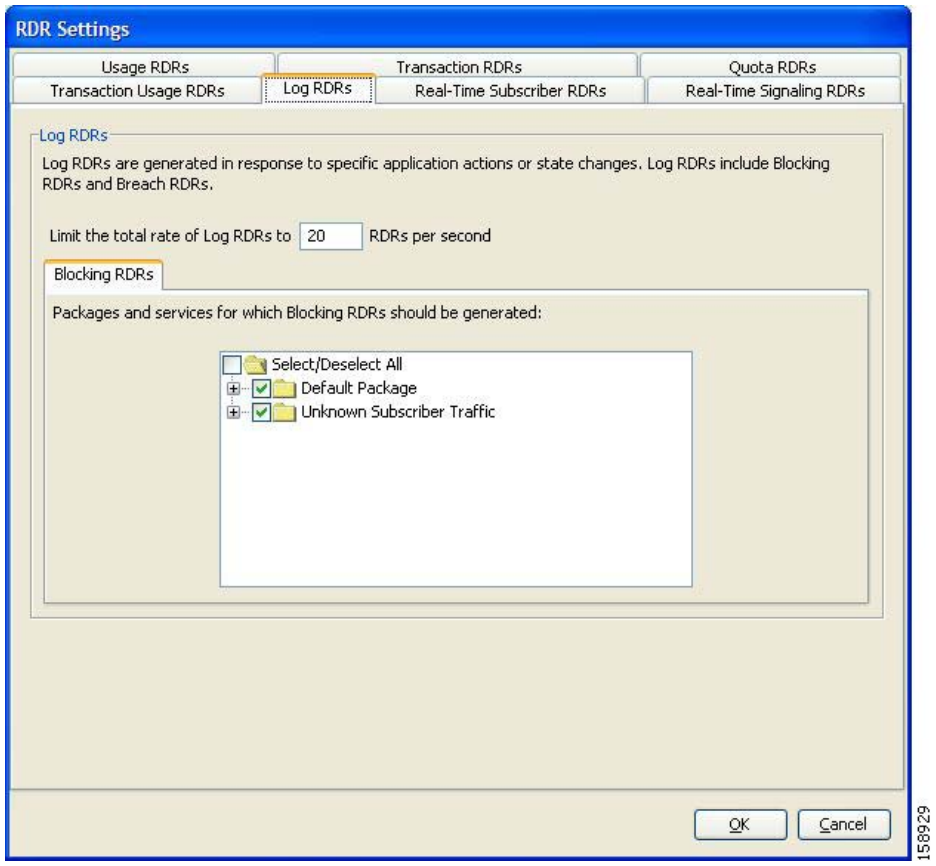
Note At most 20 Log RDRs are generated per second.

Step 1 From the Console main menu, choose **Configuration > RDR Settings.**

The RDR Settings dialog box appears.

Step 2 Click the **Log RDRs** tab.

The Log RDRs tab opens.



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 more information about selecting subscribers to be monitored, see Selecting Subscribers for Real-Time Usage Monitoring, page 13-15.

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:

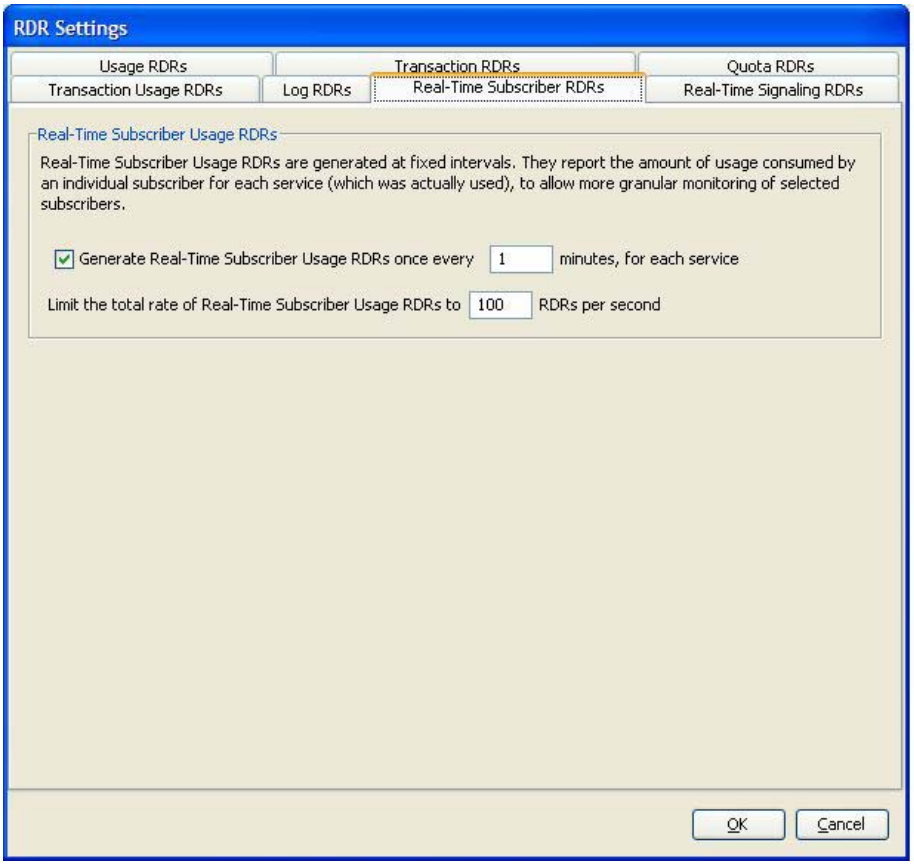
- Are enabled (but only for selected subscribers)
- Are generated for each subscriber once every minute
- Are limited to 100 RDRs generated per second

Step 1 From the Console main menu, choose **Configuration > RDR Settings.**

The RDR Settings dialog box appears.

Step 2 Click the **Real-Time Subscriber RDRs** tab.

The Real-Time Subscriber RDRs tab opens.



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, which 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, can be used to signal external systems concerning events detected by the SCE platform, allowing real-time actions to be taken across the network.

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 the How to Edit Advanced Service Configuration Options, page 10-44.

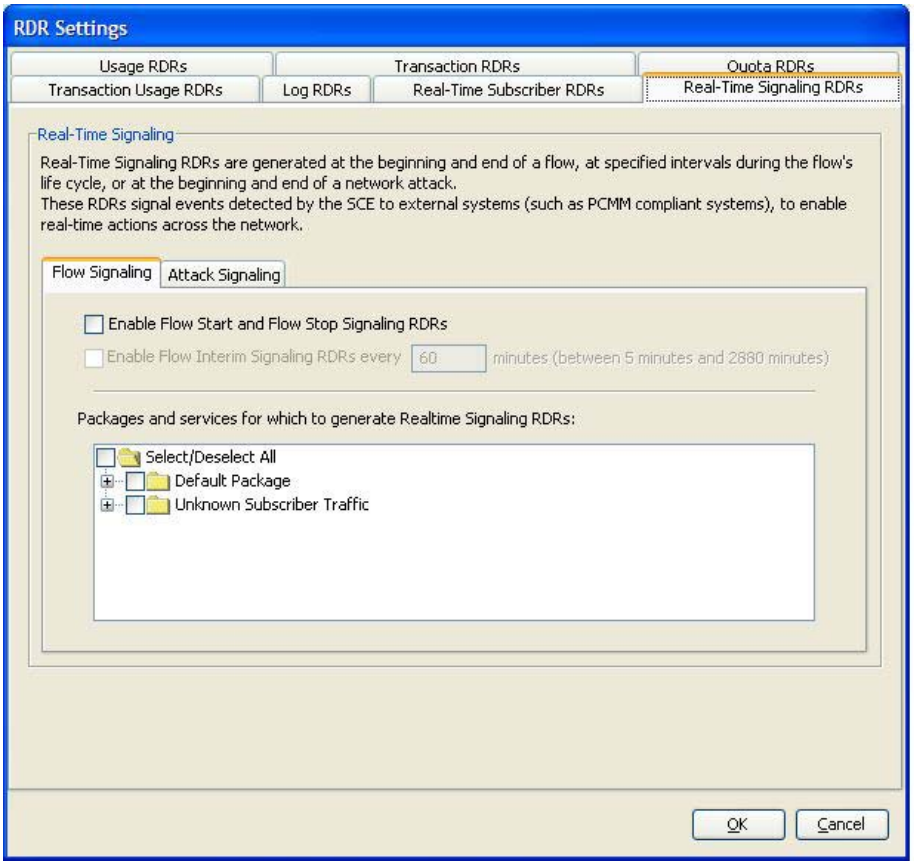
By default, no Real-Time Signaling RDRs are generated.

Step 1 From the Console main menu, choose **Configuration > RDR Settings.**

The RDR Settings dialog box appears.

Step 2 Click the **Real-Time Signaling RDRs** tab.

The Real-Time Signaling RDRs tab opens.



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.



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

The Traffic Control capabilities of the Service Control Engine (SC platform and the Cisco Service Control Application for Broadband (SCA BB) are used to limit and prioritize traffic flows. Control of traffic is based on parameters such as the service of the flow, the subscriber's package, and the subscriber's quota state.

- Unknown Subscriber Traffic, page 9-1
- Managing Packages, page 9-2
- Managing Rules, page 9-10
- Managing Bandwidth, page 9-30
- Managing Virtual Links, page 9-44
- Managing Quotas, page 9-50

Unknown Subscriber Traffic

A traffic flow that does not match any filter rule (see Filtering the Traffic Flows, page 10-17) is processed by the SCE platform, which tries to identify the subscriber responsible for the traffic flow. The SCE 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 9-38)
  - Select a calendar (see How to Set Advanced Package Options, page 9-7)
- Edit the default service rule for the Unknown Subscriber Traffic category:
  - Change the Rule State (see How to Edit Rules, page 9-17)
  - Change per-flow actions for the rule (see How to Define Per-Flow Actions for a Rule, page 9-14)
- Add rules to the Unknown Subscriber Traffic package:
  - Add rules (see How to Add Rules to a Package, page 9-12); edit (see How to Edit Rules, page 9-17) and delete (see How to Delete Rules, page 9-18) these rules
  - Add time-based rules (see How to Add Time-Based Rules to a Rule, page 9-20); edit (see How to Edit Time-Based Rules, page 9-22) and delete (see How to Delete Time-Based Rules, page 9-23) these rules

Managing Packages

A package is a description of subscriber policy. It is a collection of rules that defines the system's reaction 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 7-1) and only then add and define packages.

Every 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 if no other package is specifically assigned to the subscriber, or if a nonexistent package is assigned to the subscriber.

A service configuration can contain up to 5000 packages.

- Package Parameters, page 9-3
- How to View Packages, page 9-4
- How to Add Packages, page 9-5
- How to Set Advanced Package Options, page 9-7
- How to Duplicate Packages, page 9-8
- How to Edit Packages, page 9-8
- How to Delete Packages, page 9-10

Package Parameters

A package is defined by the following parameters:

- General parameters:
  - Package Name—A unique name for the package
  - Description—(Optional) A description of the package
- Quota Management parameters:
  - Quota Management Mode—Specifies whether subscriber quotas are managed by an external quota manager or replenished periodically by 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 packages. (Changing the package name does not affect SCE platform activity.) A default value of the package index is provided by the system. 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—A default value of the counter index is provided by the system. 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.

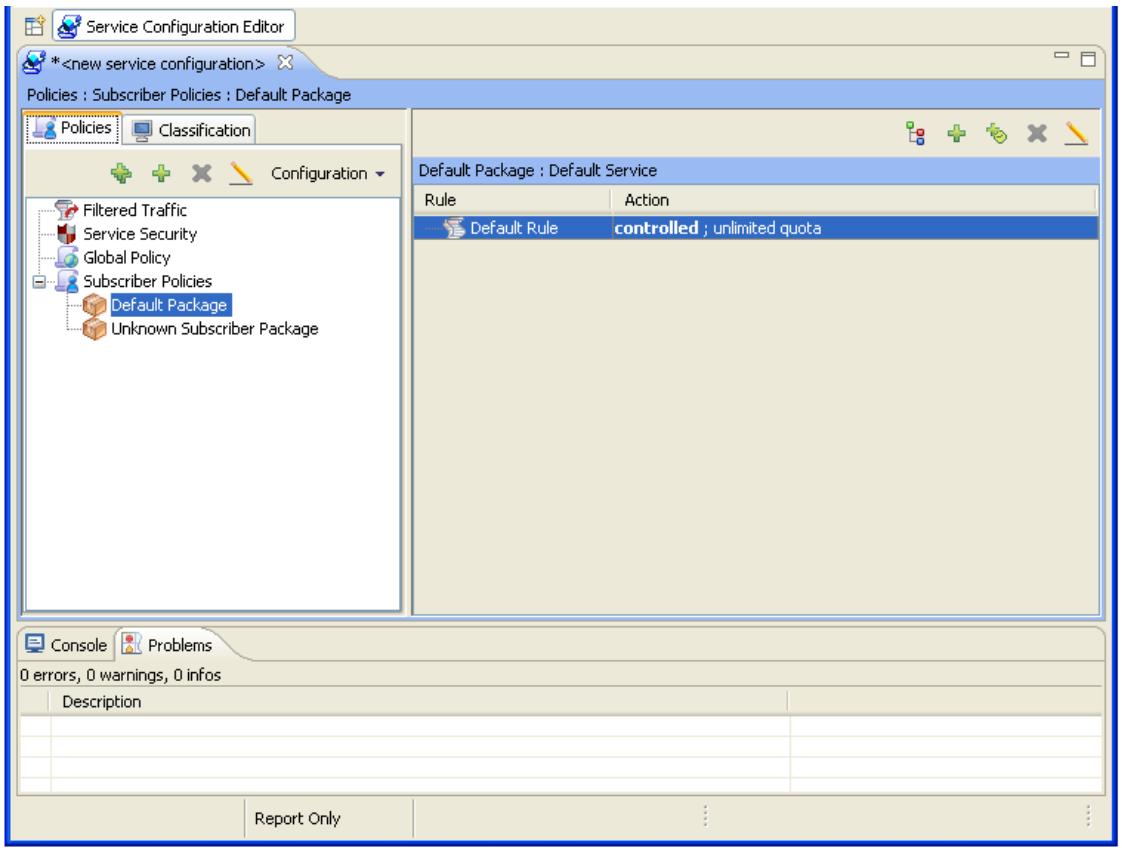
These parameters are defined when you add a new package (see How to Add Packages, page 9-5). You can modify them at any time (see How to Edit Packages, page 9-8).

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 Network Traffic tab.

The Network Traffic tab appears.

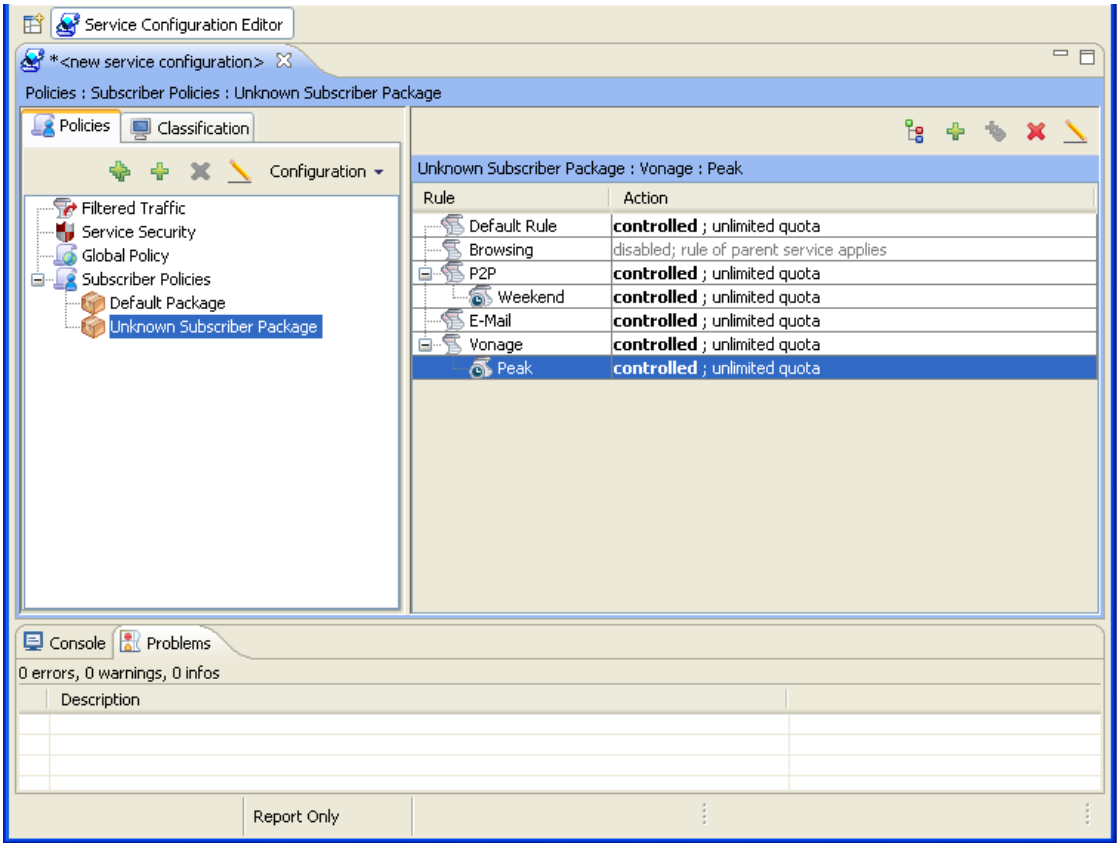


A list of all packages is displayed in the package tree.

Note To view more information about a package, open the Package Settings dialog box (see How to Edit Packages, page 9-8).

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.



How to Add Packages

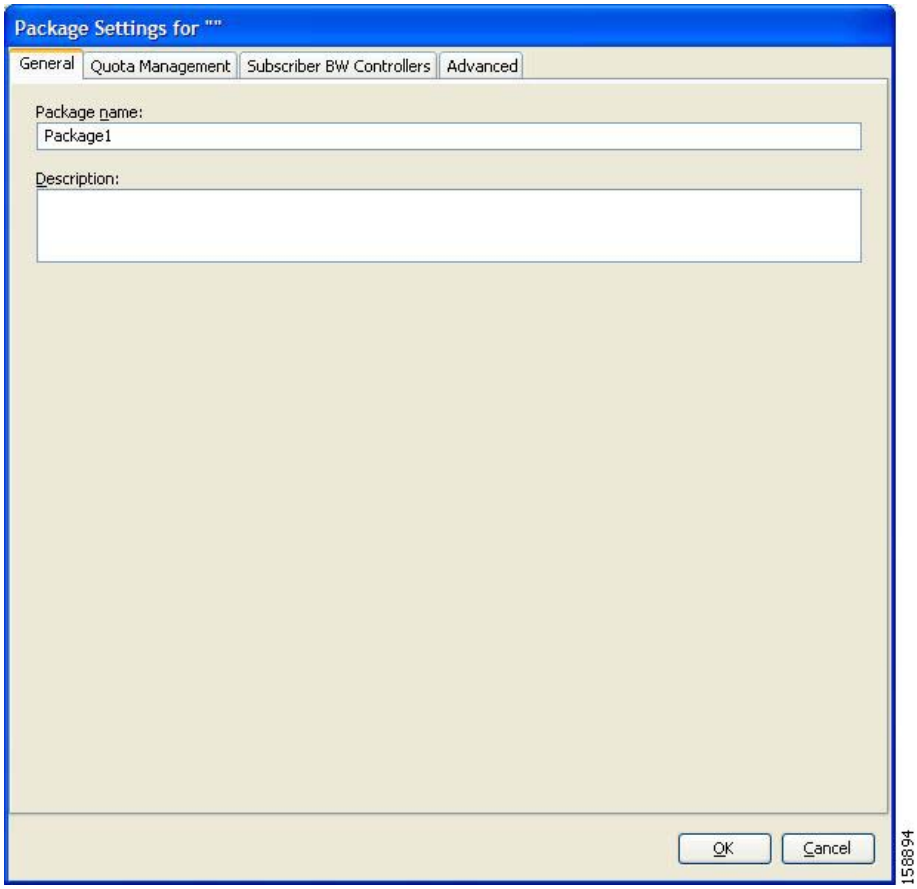
A default package is predefined in the Console installation. You can add additional packages to a service configuration, subject to the limit of 5000 packages per service configuration.

After you have added a new package, you can define rules for the package (see How to Add Rules to a Package, page 9-12).

Step 1 In the Network Traffic tab, select a package from the package tree. This package will be the parent of the package you are adding.

Step 2 In the Network Traffic tab, click (**Add Package**).

The Package Settings dialog box appears.



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 9-10.

What to Do Next

To configure parameters in the Quota Management tab see How to Edit Quota Management Settings for Packages, page 9-50.

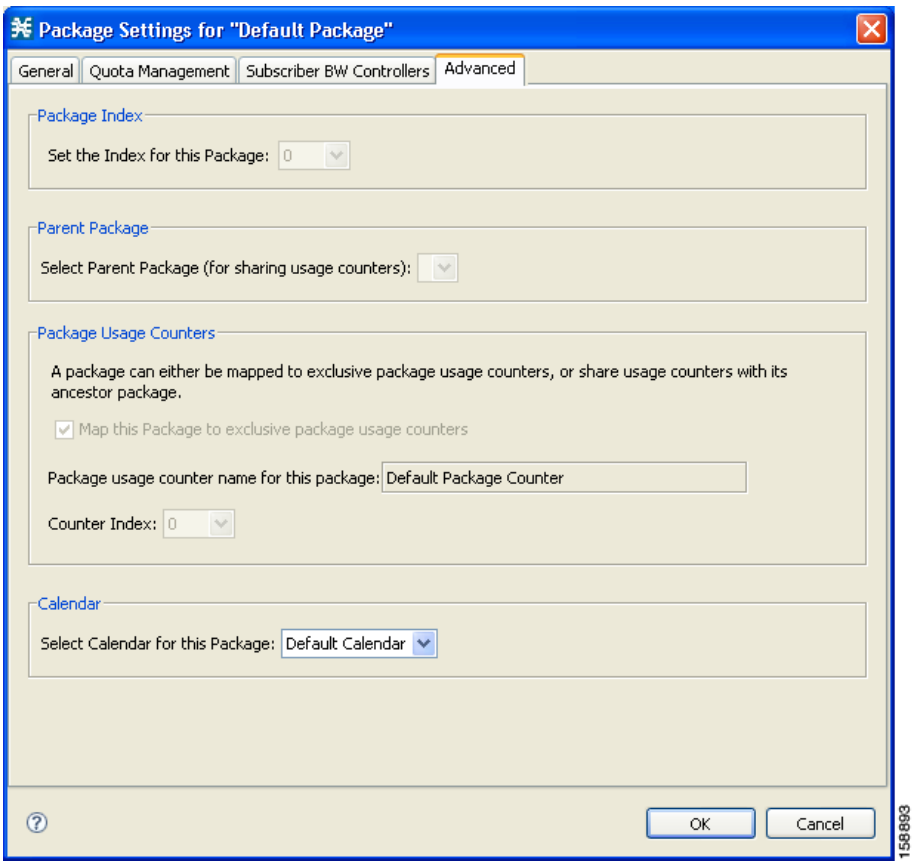
To configure parameters in the Subscriber BW Controllers tab, see How to Edit Package Subscriber BWCs, page 9-38.

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.

TheAdvanced tab opens.



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 A default value of the index is provided by the system. 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 A default value of the index is provided by the system. 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 10-46.

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 9-10.

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 make changes than to define the package from scratch.

A duplicated package is added at the same level in the package tree as the original package.

Step 1 In the Network Traffic tab, select a package from the package tree.

Step 2 In the Network Traffic tab, click  (**Duplicate Package)**.

A duplicate package is created with all the same attributes as the original package. The name of the new package is the name of the selected package followed by “(1)” (or “(2)”, and so on if a package is duplicated many times).

Step 3 Modify the package parameters (see How to Edit Packages, page 9-8).

How to Edit Packages

You can modify the parameters of a package (including the default package) at any time.

Step 1 In the Network Traffic tab, select a package from the package tree.

Step 2 In the Network Traffic tab, click  (**Edit Package)**.

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 To 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 9-50.

Step 6 To change bandwidth control settings, see How to Edit Package Subscriber BWCs, page 9-38.

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 A default value of the counter index is provided by the system. 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 A default value of the counter index is provided by the system. 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 10-46.

Step 8 Click **OK.**

The Package Settings dialog box closes.

All changes to the package parameters are saved.

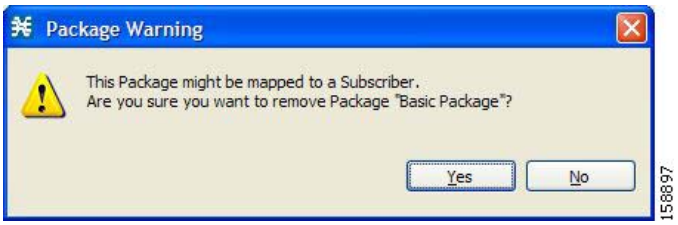
How to Delete Packages

You can delete user-defined packages. The default package cannot be deleted.

Step 1 In the Network Traffic tab, select a package from the package tree.

Step 2 In the Network Traffic tab, click (**Delete Package)**.

A Package Warning message appears.



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 a flow's packets
- 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.

- The Default Service Rule, page 9-11
- Rule Hierarchy, page 9-11
- How to View the Rules of a Package, page 9-11
- How to Add Rules to a Package, page 9-12
- How to Define Per-Flow Actions for a Rule, page 9-14
- How to Edit Rules, page 9-17
- How to Delete Rules, page 9-18
- How to Display the Services Affected by a Rule, page 9-19
- Managing Time-Based Rules, page 9-20
- How to Manage DSCP ToS Marker Values, page 9-28

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 will apply the most specific rule to any flow.

For example, if you define rules for E-Mail and POP3, any flow mapped to the POP3 service will be handled according to the POP3 rule—any flow mapped to the SMTP or IMAP service will be handled according to the E-Mail 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.

Any rule that also applies to child services is indicated by . Rules that do not apply to any child services are shown by .

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 9-19.

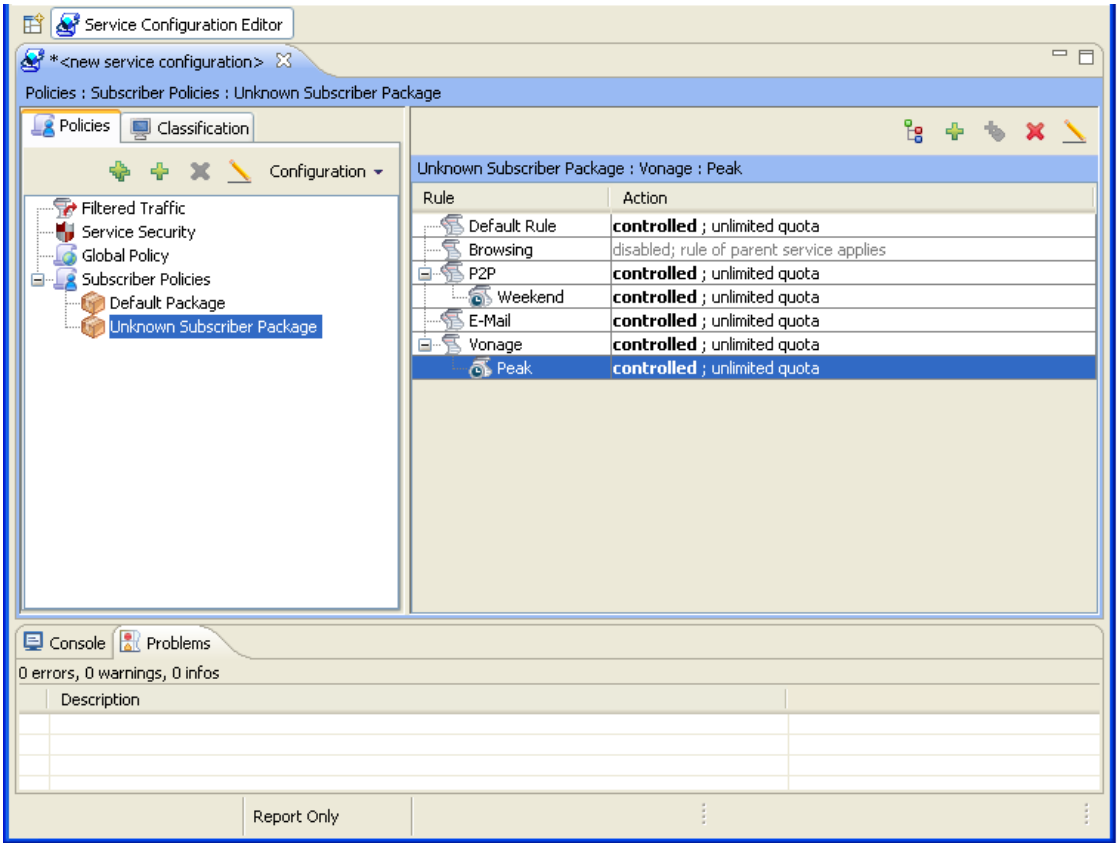
How to View the Rules of a Package

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 Network Traffic tab, select a package from the package tree.

A list of all rules defined for this package is displayed in the right (Rule) pane.



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 9-17).

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 9-22).

How to Add Rules to a Package

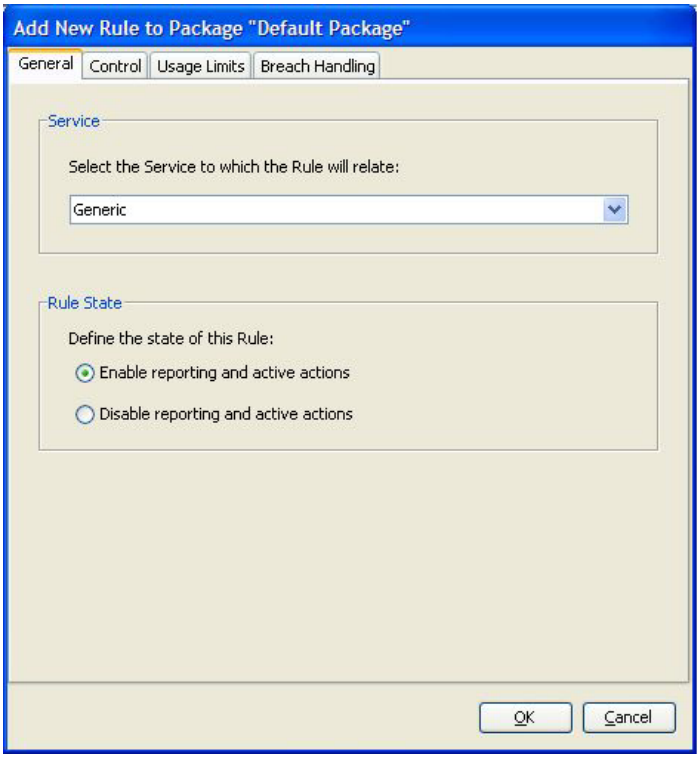
A default service rule is assigned to every package. You can add additional rules to a package.

Adding time-based rules is described in the section How to Add Time-Based Rules to a Rule, page 9-20.

Step 1 In the Network Traffic tab, select a package from the package tree.

Step 2 In the right (Rule) pane, click (**Add Rule**).

The Add New Rule to Package dialog box appears.



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 will Relate 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 9-17).

Step 5 To 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 9-14.

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 9-50):

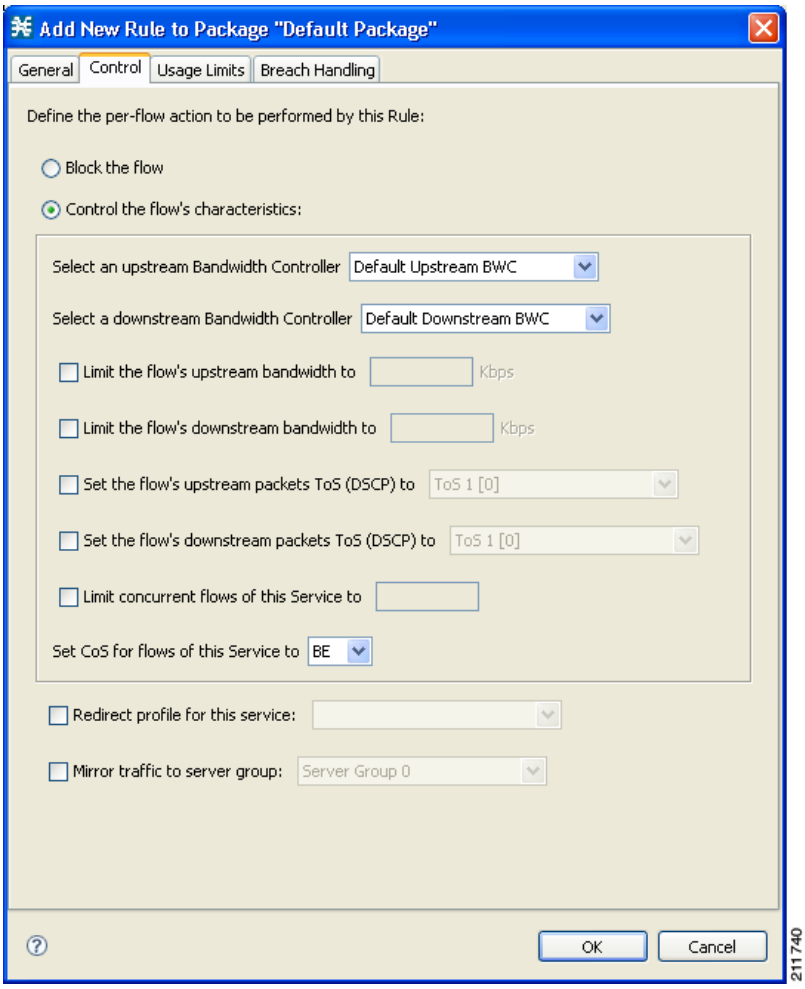
- To configure parameters in the Usage Limits tab see How to Select Quota Buckets for Rules, page 9-52.
- To configure parameters in the Breach Handling tab, see How to Edit Breach-Handling Parameters for a Rule, page 9-53.

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.



To control flows that are mapped to the service of this rule, continue at Step 5.

Step 2 To block flows that are mapped to the service of this rule, select the **Block the flow** radio button.

The Redirect to check box is enabled.

Note Only three protocol types support redirection: HTTP, HTTP Streaming, and RTSP.

Step 3 (Optional) To redirect blocked flows, check the **Redirect to** check box.

Note Redirection is not supported when unidirectional classification is enabled.

The Redirection URL Set drop-down list is enabled.

- If the service or service group for this rule includes protocols that cannot be redirected, a Rule Warning message appears.



- Click **OK.**

From the Redirection URL Set drop-down list, select a URL set to serve as the redirection target. (URL redirection sets are defined in the System Settings dialog box. See How to Add a Set of Redirection URLs, page 10-37.)

Step 4 Continue at Step 14.

Step 5 Select the **Control the flow's characteristics** radio button.

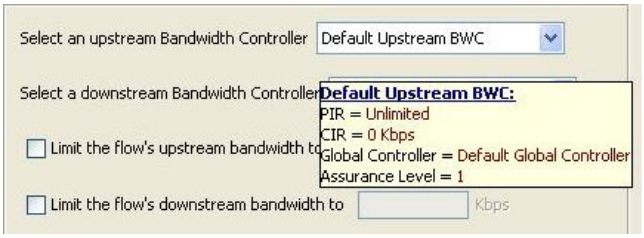
The options in the Flow Characteristic area are enabled.

Step 6 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 (see How to Edit Package Subscriber BWCs, page 9-38).

Note **Important Note 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 (see How to Set the Maximum Bandwidth of Global Controllers, page 9-33). Do not create a separate global controller for each time frame.

When the mouse is placed over the drop-down list, a tooltip appears containing the properties of the selected BWC (Peak Information Rate (PIR), Committed Information Rate (CIR), Global Controller, and Assurance Level).



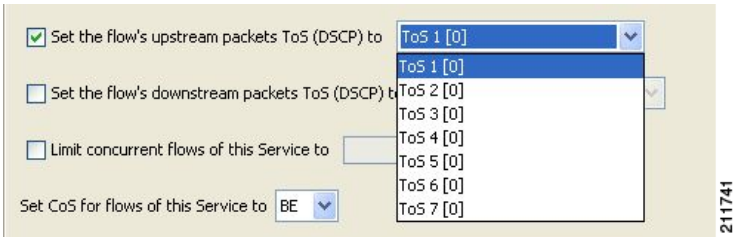
Step 7 From the downstream Bandwidth Controller drop-down list, select a downstream BWC.

Step 8 (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 9 (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 10 (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.



Step 11 (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 12 (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 13 From the Set CoS for flows of this Service drop-down list, select a class-of-service.

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.

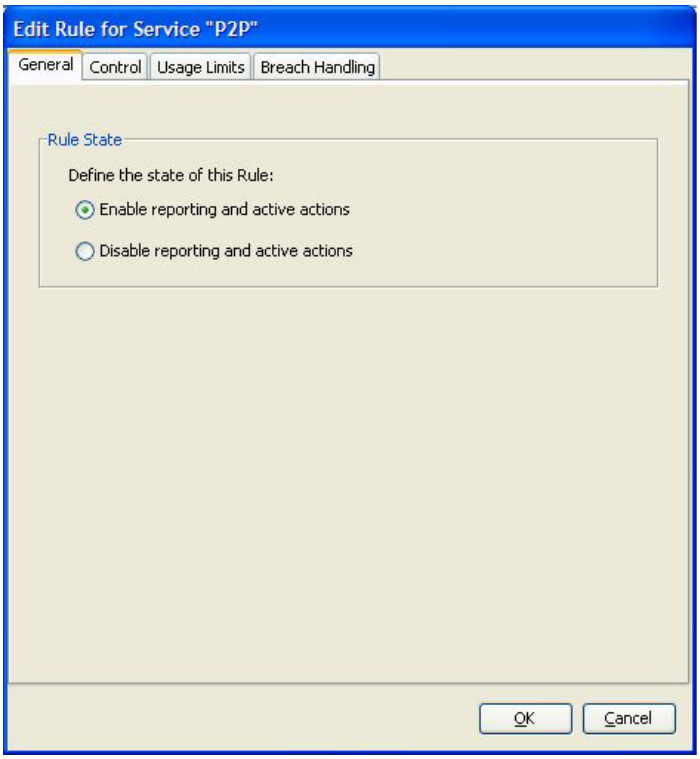
Note The tabs of the Edit Rule for Service dialog box are the same as the tabs of the Add New Rule to Package dialog box, except for the General tab—you cannot change the service to which the rule applies.

Step 1 In the Network Traffic 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.



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 9-14.

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 9-52.

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 9-53.

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 (see Step 4 of How to Edit Rules, page 9-17). This 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 Network Traffic 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 (**Delete Rule)**.

A Rule Warning message appears.

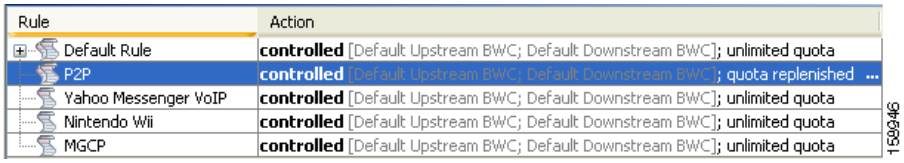


Step 4 Click **Yes.**

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 child service is governed by the rule of the parent service. A rule that affects any of a service's children is indicated in the rules list by a different icon, as illustrated for the default service rule and the P2P rule in the following figure.

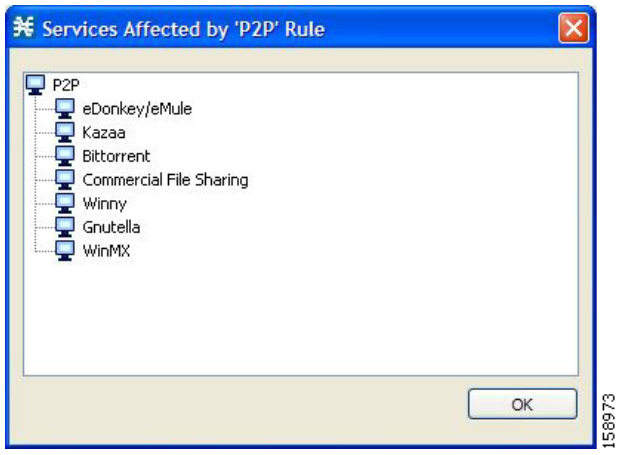


You can display all (child) services that are affected by a rule.

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 Network Traffic tab, select a rule and click (**Show All Services Affected By This Rule**).

The Services Affected dialog box appears.



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 9-24). 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 will 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.

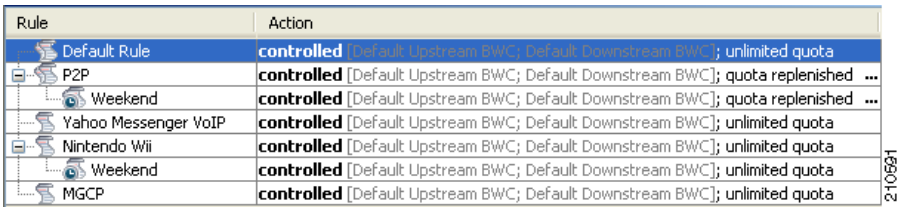
You must define the calendar before defining the related time-based rules.

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 the following screen capture.

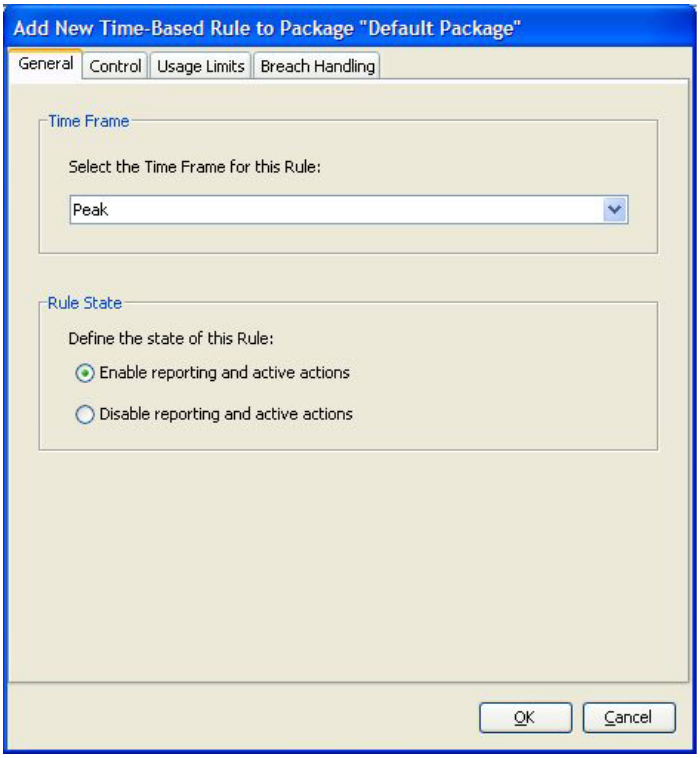


Step 1 In the Network Traffic tab, select a package from the package tree.

Step 2 In the right (Rule) pane, select a rule.

Step 3 Click (**Add Time-Based Rule**).

The Add New Time-Based Rule dialog box appears.



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 9-14.

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 9-52.

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 9-53.

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.

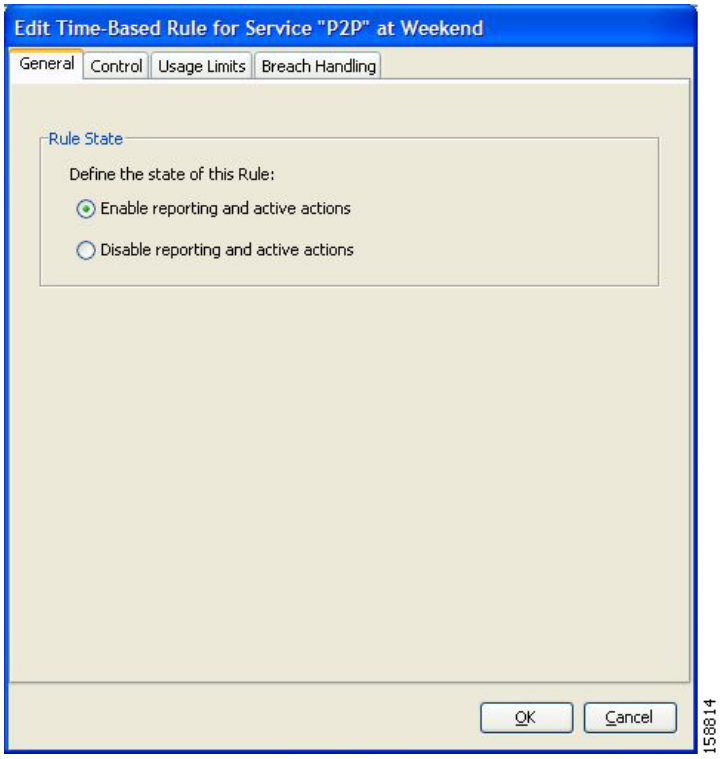
Note The tabs of the Edit Time-Based Rule for Service dialog box are the same as the tabs of the Add New Time-Based Rule dialog box, except for the General tab. You cannot change the time frame to which the rule applies.

Step 1 In the Network Traffic tab, select a package from the package tree.

Step 2 In the right (Rule) pane, select a time-based rule.

Step 3 Click (**Edit Rule)**.

The Edit Time-Based Rule for Service dialog box appears.



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 9-14.

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 9-52.

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 9-53.

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.

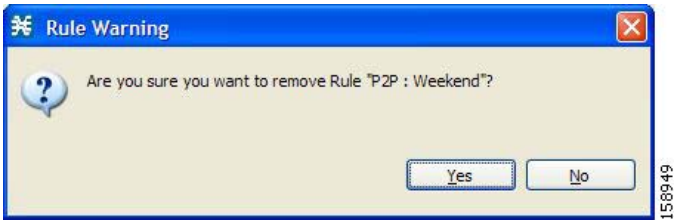
Note You can *disable* a rule without losing its profile (see How to Edit Time-Based Rules, page 9-22). This allows you to enable the rule again later, without having to reset all its parameters.

Step 1 In the Network Traffic 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 (**Delete Rule**).

A Rule Warning message appears.



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 will 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.

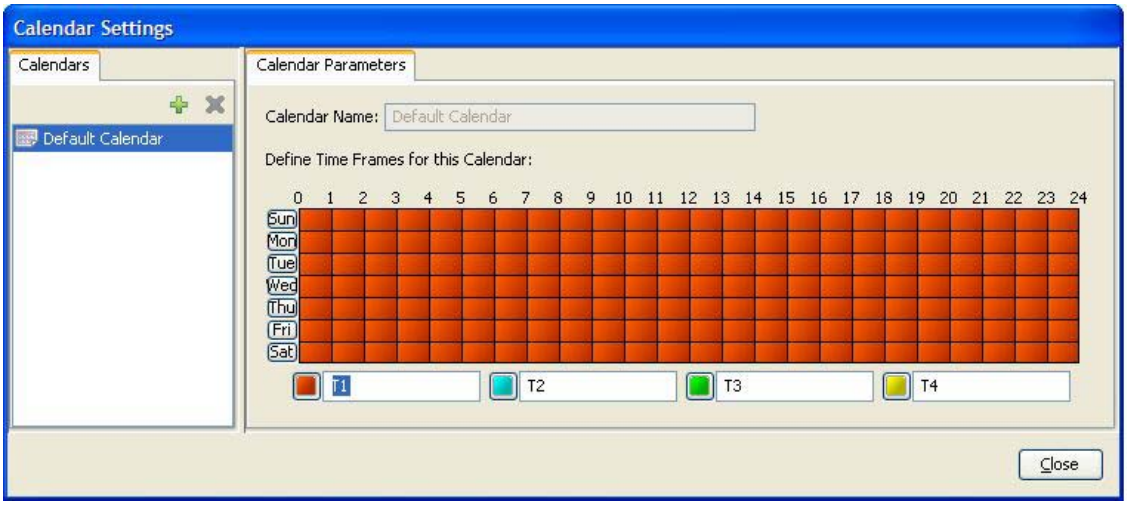
- How to View Calendars, page 9-24
- How to Add Calendars, page 9-25
- How to Rename the Time Frames, page 9-26
- How to Delete Calendars, page 9-26
- How to Configure the Time Frames, page 9-27

How to View Calendars

You can view a list of existing calendars and their time frames.

Step 1 From the Console main menu, choose **Configuration > Weekly Calendars.**

The Calendar Settings dialog box appears.



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.

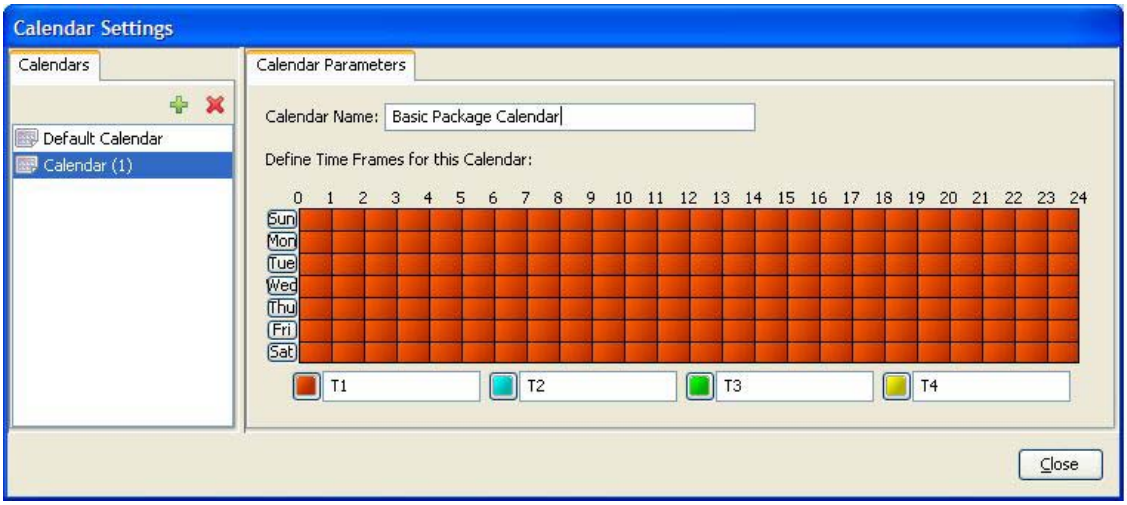
Step 1 From the Console main menu, choose **Configuration > Weekly Calendars.**

The Calendar Settings dialog box appears.

Step 2 In the Calendar tab, click (**Add**).

A new calendar is added with the name Calendar (1).

Step 3 In the Calendar Parameters tab, click in the Calendar Name field and enter the name 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.

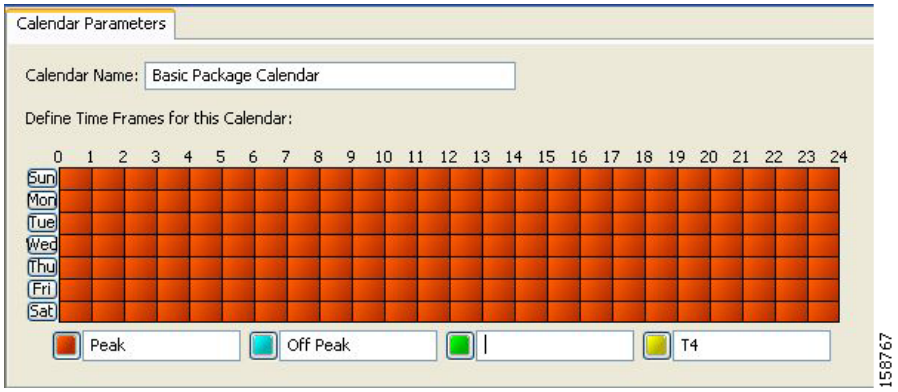
Note Although you can configure the time frames differently in each calendar, the names of the time frames are the same in all of the calendars. If you change the name when configuring one calendar, the names are also changed for all other calendars.

Step 1 From the Console main menu, choose **Configuration > Weekly Calendars.**

The Calendar Settings dialog box appears.

In the Calendar Parameters tab, 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.



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.)

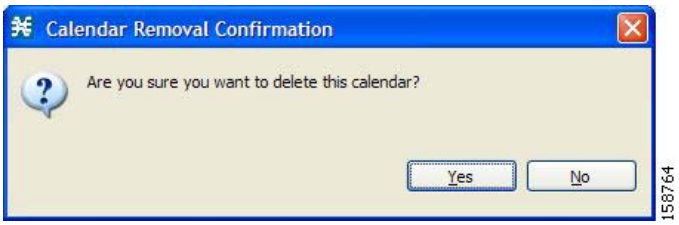
To delete the calendar, you must first select a different calendar for each package using the calendar that will be deleted. See How to Set Advanced Package Options, page 9-7 for information about changing the calendar associated with a package.

Step 1 From the Console main menu, choose **Configuration > Weekly Calendars.**

The Calendar Settings dialog box appears.

Step 2 In the Calendar tab, select a calendar and click (**Delete)**.

A Calendar Removal Confirmation message appears.



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 Console main menu, choose **Configuration > Weekly Calendars.**

The Calendar Settings dialog box appears.

Step 2 In the Calendars tab, select a calendar to configure.

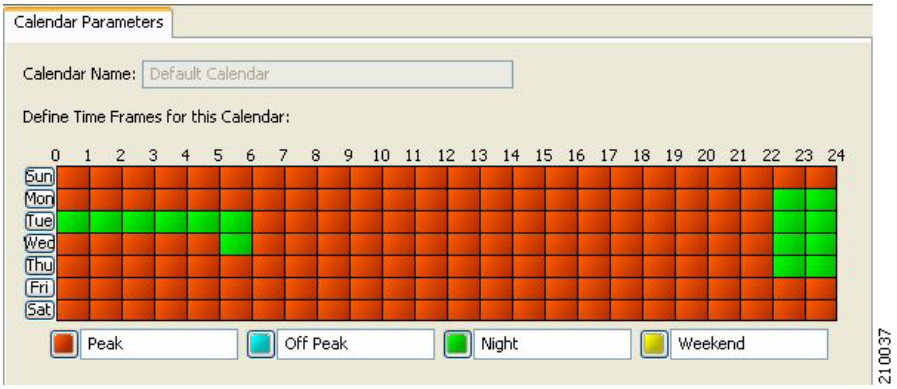
In the Calendar Parameters tab, the selected calendar's **Define Time Frames for this Calendar** grid is displayed. The grid, representing one week, is laid out in a format of 24 hours x 7 days. Each cell represents one hour.

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 will be part of the selected time frame.

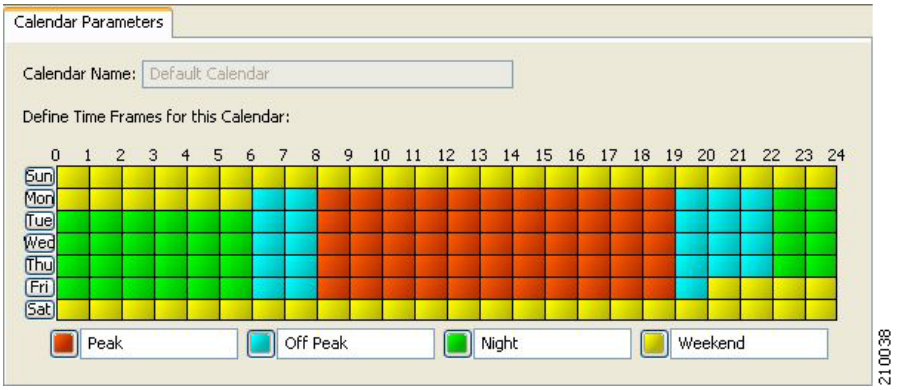
You can select a group of cells by holding down the mouse button and dragging across the cells.



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. The following figure illustrates a possible time partition plan:



Step 6 Click **Close.**

The Calendar Settings dialog box closes.

How to Manage DSCP ToS Marker Values

SCA BB can change the value of the DSCP ToS marker of packets of flows that match a filter rule (see Step 11 of How to Add Filter Rules, page 10-20) or a service rule (see Steps 10 and 11 of How to Define Per-Flow Actions for a Rule, page 9-14 and Step 9 of How to Edit Breach-Handling Parameters for a Rule, page 9-53).

SCA BB supports seven ToS Marker Classes. You assign each class a specific value to apply to a flow's packets.

Note If you have used DSCP marking on a SCA BB release prior to 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 (see How to Reconfigure DSCP Marking for Release 3.1.5 and Higher, page 4-9).

DSCP ToS Marking

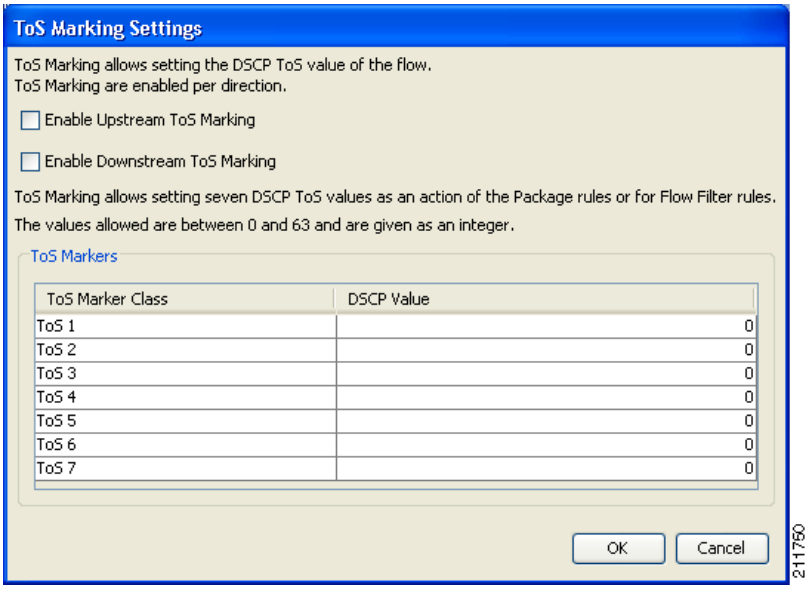
DSCP ToS marking is used in IP networks as a means to signal the type and priority of a flow between network elements.

The default marking option is not to mark the packet. Since classification may take a few packets to finalize, it is important to note that if 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 Console main menu, choose **Configuration** > **ToS Marking Settings.**

The ToS Marking Settings dialog box appears.



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 Bandwidth

The upstream and downstream interfaces are each assigned one default global controller. You can add additional global controllers.

A service configuration can contain up to 1024 upstream global controllers and 1024 downstream global controllers (including the default global controllers).

After you have defined global controllers, you can add subscriber BW controllers (BWCs) to packages, and map these subscriber BWCs to different global controllers.

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, page 9-30
- How to View Global Controller Settings, page 9-31
- How to Edit the Total Link Limits, page 9-32
- How to Add Global Controllers, page 9-33
- How to Set the Maximum Bandwidth of Global Controllers, page 9-33
- How to Delete Global Controllers, page 9-35
- Defining Global Controllers in a Dual-Link System, page 9-35
- Managing Subscriber Bandwidth, page 9-36
- Managing Bandwidth: a Practical Example, page 9-39
- How to Set BW Management Prioritization Mode, page 9-43

Managing Global Bandwidth

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, and assign a maximum percentage of the total link limit to each global controller separately.

You can also define the bandwidth total link limit to be less than the physical capacity of the 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.

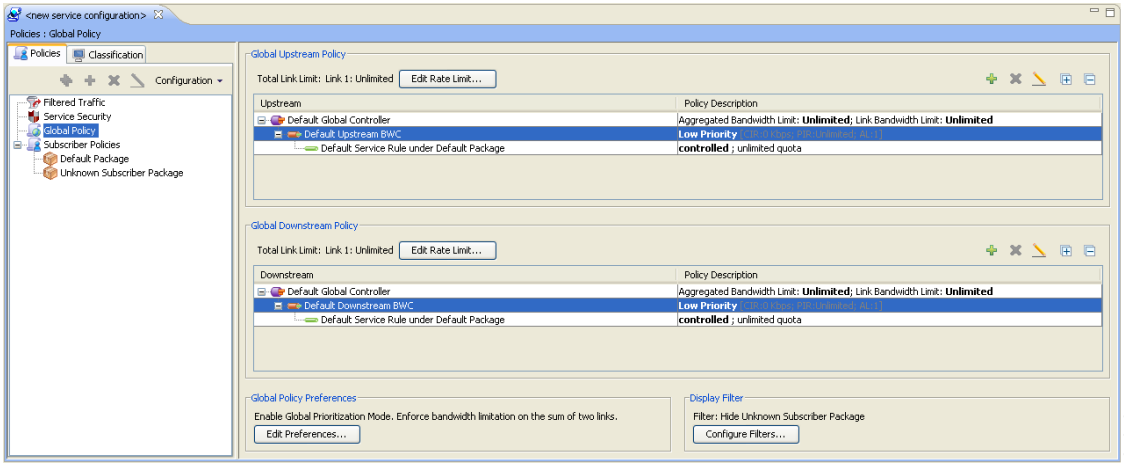
How to View Global Controller Settings

Note Global controller bandwidth is based on Layer 1 volume.

(Accounting, reporting, and subscriber bandwidth control in SCA BB is based on Layer 3 volume.)

Step 1 From the Console main menu, choose **Configuration > Global Bandwidth Settings.**

The Global Bandwidth Settings dialog box appears.



The two check boxes near the top of the Global Controllers tab are used only in dual-link systems (see Defining Global Controllers in a Dual-Link System, page 9-35).

The main part of the dialog box contains the Upstream area listing upstream global controllers and the Downstream area listing downstream global controllers. Each list has four columns; the third and fourth columns are relevant to dual-link systems:

- **Name** —A unique name assigned to the global controller. The system automatically assigns the names Controller 1, Controller 2, and so on.
- **Link 1 BW (%)** —The maximum percentage of the total link limit permitted to this global controller.

  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 (see Managing Calendars, page 9-24):

  – 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.



  – If two time frames have the same maximum bandwidth, the value is not repeated. (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.)

Name	Link 1 BW (%)
Downstream Total Link Limit	100
Default Global Controller	100
Downstream Controller 1	40,,,100

- Trailing commas are suppressed. (So **40,100** means that the first time frame has a maximum bandwidth of 40 percent of the total link limit, and the other three time frames have a maximum bandwidth equal to the total link limit.)

Step 2 To view the actual maximum bandwidth values, place the cursor over the Link 1 BW (%) cell.

A tooltip appears, showing the actual maximum bandwidth permitted to this global controller, in Mbps. This figure is calculated automatically by the system based on the possible SCE platform types (Gigabit Ethernet or Fast Ethernet), the controller maximum bandwidth percentage, and the total link bandwidth percentage.

Name	Link 1 BW (%)	Link 2 BW (%)	Aggregated BW (%)
Upstream Total Link Limit	100	100	N/A
Default Global Controller	100	100	N/A
Upstream Controller 1	40,60,80,100	40,60,80,100	N/A

Fast Ethernet = 40Mbps, 60Mbps, 80Mbps, 100Mbps
Gigabit Ethernet = 800Mbps, 1200Mbps, 1600Mbps, 2000Mbps

210586

Step 3 Click **OK**

The Global Bandwidth Settings dialog box closes.

How to Edit the Total Link Limits

You can limit the total bandwidth passing through the SCE platform.

For example, if another device sitting next 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.

The total link limits for upstream and downstream traffic are defined independently.

Step 1 From the Console main menu, choose **Configuration > Global Bandwidth Settings.**

The Global Bandwidth Settings dialog box appears.

Step 2 Click in the Link 1 BW (%) cell of the Upstream Total Link Limit or Downstream Total Link Limit, and enter the maximum percentage of the SCE platform capacity that the platform will carry.

The values displayed in the tooltips of all the cells in the Link 1 BW (%) cells change to reflect the new total link limit.

Step 3 Click **OK**

Your changes are saved.

The Global Bandwidth Settings dialog box closes.

How to Add Global Controllers

You can add up to 1023 upstream global controllers and 1023 downstream global controllers to a service configuration.

Step 1 From the Console main menu, choose **Configuration > Global Bandwidth Settings.**

The Global Bandwidth Settings dialog box appears.

Step 2 Above the area (Upstream or Downstream) of the desired interface, click (**Add)**.

A new global controller is added to the interface global controller list with a maximum bandwidth capacity of 100 percent of the total link limit.

Step 3 In the Name cell of the new global controller, enter a meaningful name.

Note You can use the default name for the global controller. It is recommended that you enter a meaningful name.

Step 4 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 9-33.

Step 5 Click **OK**

Your changes are saved.

The Global Bandwidth Settings dialog box closes.

How to Set the Maximum Bandwidth of Global Controllers

You can edit the maximum bandwidth (as a percentage of the total link limit) that a global controller can carry.

You can set a different maximum bandwidth for each of the four available time frames.

In a dual-link system, you can set different values for each link and for the aggregated BW of the two links.

Step 1 From the Console main menu, choose **Configuration > Global Bandwidth Settings.**

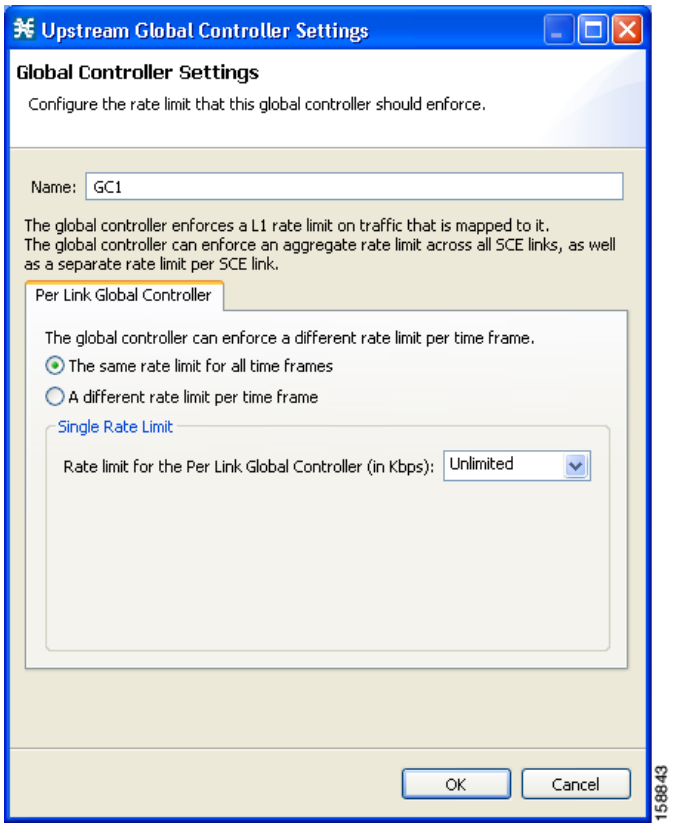
The Global Bandwidth Settings dialog box appears.

Step 2 Click in a BW (%) cell of a global controller listing.

A Browse button appears in the cell.

Step 3 Click the **Browse** button.

The Global Controller Bandwidth Settings dialog box appears.



Step 4 Set a single value for the maximum percentage of the total link limit that this global controller carries.

- Select **Enforce a single BW limit,** and enter the desired value for the maximum percentage of bandwidth.

Step 5 Set the maximum percentage of the total link limit that this global controller carries to vary according to time frame.

- Select **Enforce a separate BW limit per Time Frame,** and enter the desired value in each BW (%) cell.

Note These values will be applied to the time frames of the default calendar.

Step 6 Click **OK**

Your changes are saved.

The value in the BW (%) cell changes to reflect the new bandwidth limits.

Step 7 Repeat Steps 2 to 6 for other global controllers.

Step 8 Click **OK**

Your changes are saved.

The Global Bandwidth Settings dialog box closes.

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 From the Console main menu, choose **Configuration > Global Bandwidth Settings.**

The Global Bandwidth Settings dialog box appears.

Step 2 Select a global controller.

Step 3 Click  **(Delete)**.

Note If a subscriber BWC is using the specified global controller (see How to Edit Package Subscriber BWCs, page 9-38), 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.

Defining Global Controllers in a Dual-Link System

In a dual-link system, you can define each global controller's maximum bandwidth separately for each link.

Alternatively, you can apply bandwidth limitations to the sum of the two links.

Note If Virtual Links mode is enabled, bandwidth limitations are applied to the sum of the two links.

- How to Set Global Controller Bandwidth Limits Separately for Each Link, page 9-35
- How to Set Global Controller Bandwidth Limits as the Sum of Two Links, page 9-36

How to Set Global Controller Bandwidth Limits Separately for Each Link

Step 1 From the Console main menu, choose **Configuration > Global Bandwidth Settings.**

The Global Bandwidth Settings dialog box appears.

Step 2 Add global controllers, as described in How to Add Global Controllers, page 9-33.

Step 3 Check the **Allow separate BW setting for each link** check box.

The cells in the Link 2 BW (%) column are enabled.

Each cell has the same value as the parallel cell in the Link 1 BW (%) column.

Step 4 Define the bandwidth percentages (Link 1 BW (%)) for the global controllers for link 1.

Changes to bandwidth percentages are not copied to the Link 2 tab.

Step 5 In the Link 2 BW (%) column, define the bandwidth percentages for the global controllers for link 2.

Step 6 Click **OK**

Your changes are saved.

The Global Bandwidth Settings dialog box closes.

How to Set Global Controller Bandwidth Limits as the Sum of Two Links

Step 1 From the Console main menu, choose **Configuration > Global Bandwidth Settings.**

The Global Bandwidth Settings dialog box appears.

Step 2 Check the **Enforce BW limitation on the sum of two links** check box.

The cells in the Aggregated BW (%) column are enabled and contain the value 100.

Step 3 Click **OK**

Your changes are saved.

The Global Bandwidth Settings dialog box closes.

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, depending upon 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 each subscriber's service, based upon the CIR, PIR, global controller and Assurance Level (AL) set for the BWC. Each rule defines a link between the service's flows and one of the BWCs (unless the flows are to be blocked). See How to Define Per-Flow Actions for a Rule, page 9-14.

- 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.)

- Subscriber BWC Parameters, page 9-37
- How to Edit Package Subscriber BWCs, page 9-38

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 Bandwidth for a subscriber BWC has a granularity of 16 Kbps:

If you specify a bandwidth of, for example, 64 Kbps, the bandwidth will be stable at this value.

If you specify a bandwidth of, for example, 70 Kbps, the bandwidth will be unstable and oscillate between 64 Kbps and 80 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.
- AL—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.

  Assurance Level 10 (persistent) never goes below the relevant CIR, unless the total line rate cannot sustain this.
- 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.

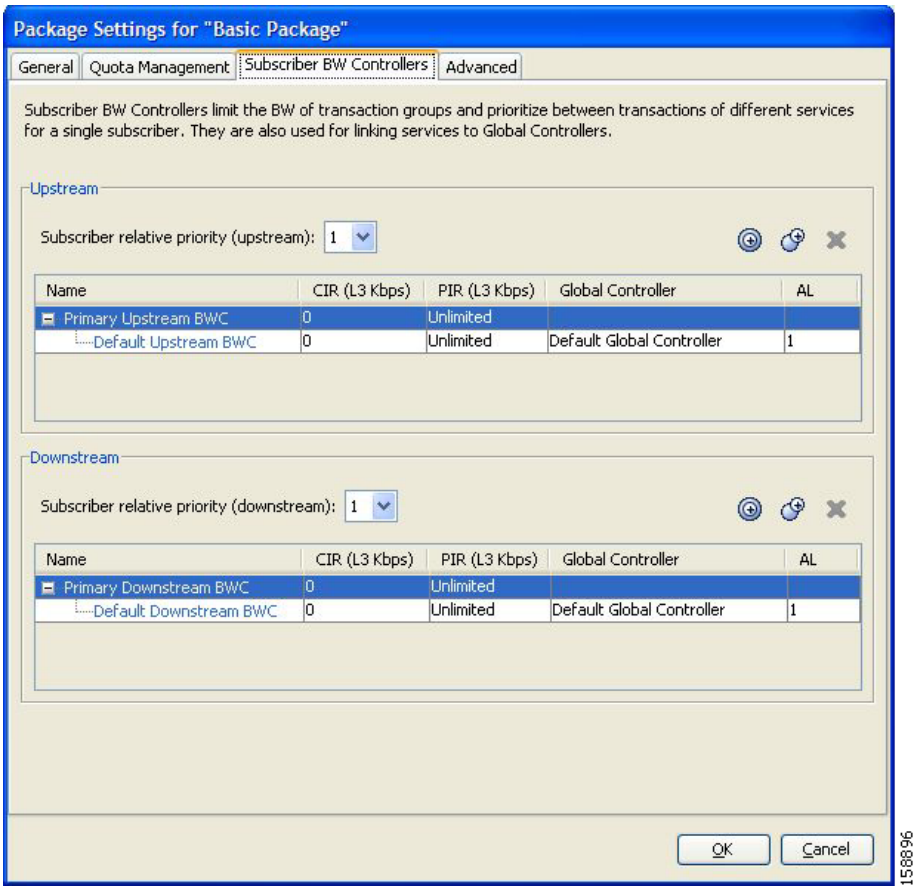
How to Edit Package Subscriber BWCs

Step 1 In the Network Traffic tab, select a package from the package tree and click (**Edit Package**).

The Package Settings dialog box appears.

Step 2 In the Package Settings dialog box, click the **Subscriber BW Controllers** tab.

The Subscriber BW Controllers tab opens.



Step 3 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 (**Add a sub BW Controller)** once for each additional BWC.

d. To add Extra BWCs to the package, click (**Add an extra BW Controller)** once for each additional BWC.

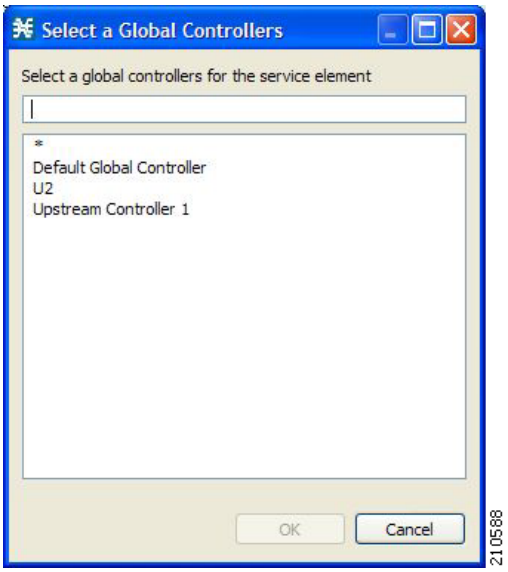
e. Set the parameters for each BWC (including the Primary and Default BWCs).

- (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.



- Select a global controller and click **OK.**
- Select a value from the AL drop-down list.

Step 4 Repeat Step 3 for downstream bandwidth control in the Downstream area of the dialog box.

Step 5 Click **OK.**

The Package Settings dialog box closes.

All changes to the BWC settings are saved.

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 9-39
- Example: How to Limit P2P and Streaming Traffic Using the Console, page 9-40

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 percentage of 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.

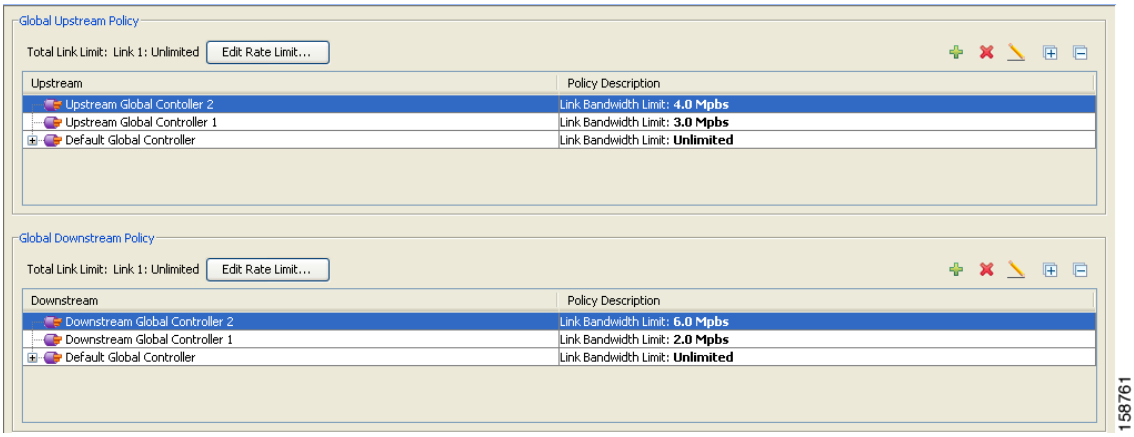
Step 3 For each service that is to have its own BWC, create a rule and select appropriate upstream and downstream BWCs.

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.

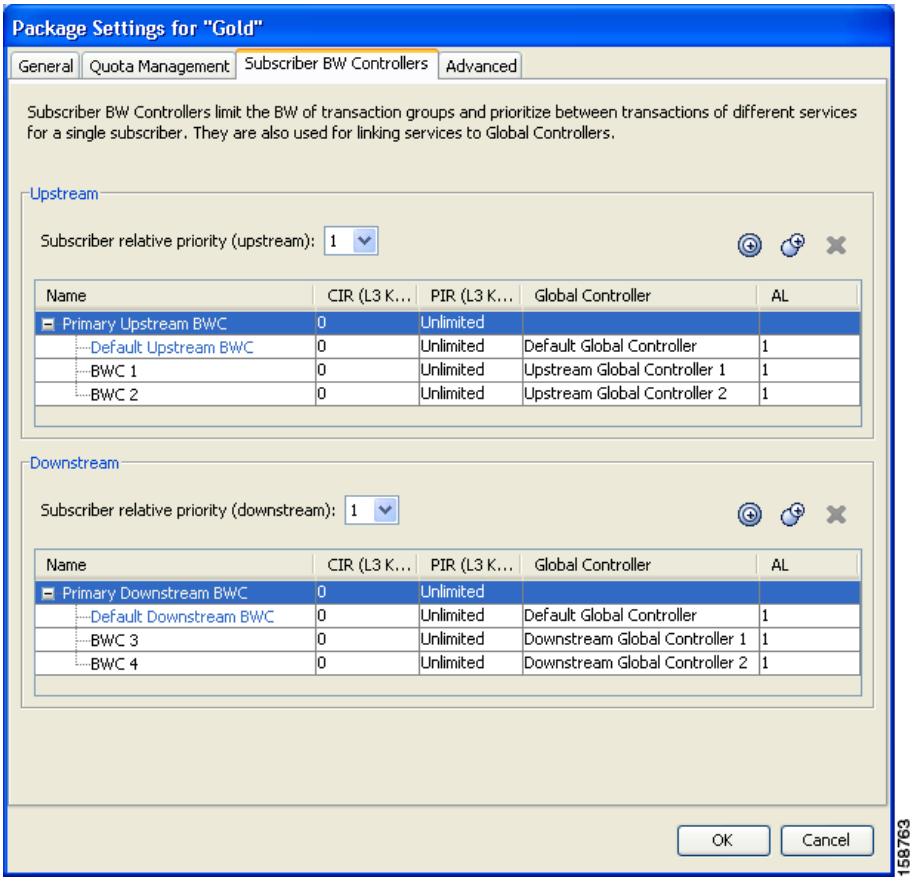
Note The P2P Traffic Optimization wizards allow you to create a simple model of devices, connect to them, and limit P2P traffic to a specified percentage of total available bandwidth. (See How to Use the P2P Traffic Optimization Wizards, page 4-29.)

Step 1 In the Global Bandwidth Settings dialog box, add two upstream global controllers and two downstream global controllers and assign the desired percentage of traffic to each global controller.



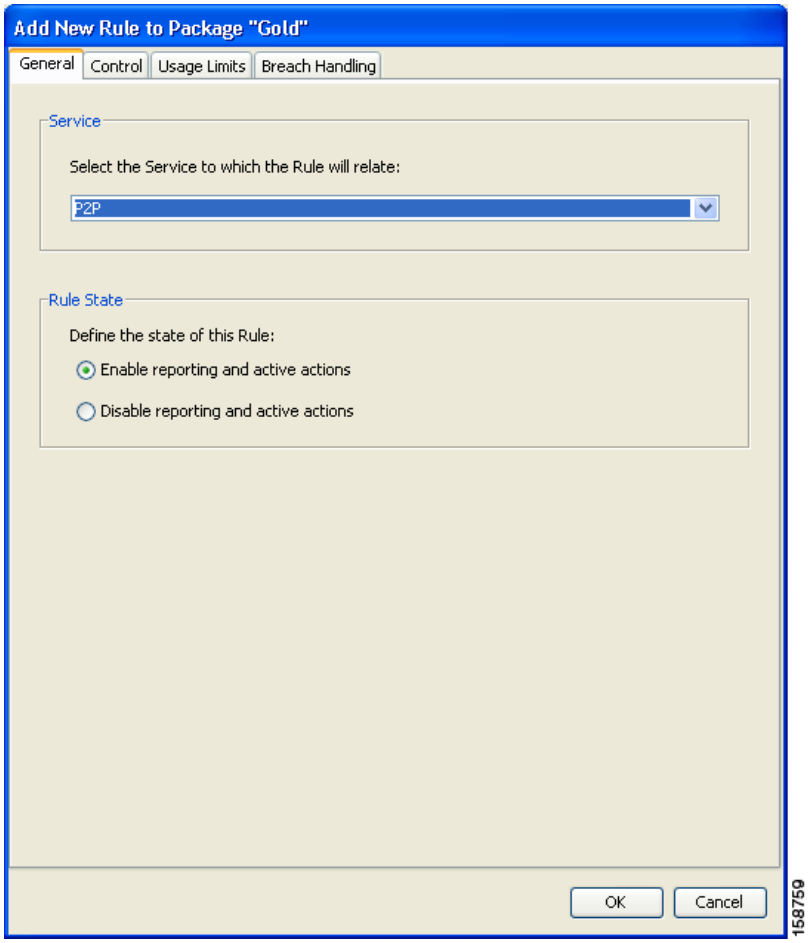
(Here, Upstream Controller 1 and Downstream Controller 1 will be used for P2P traffic, and Upstream Controller 2 and Downstream Controller 2 will be used for streaming traffic.)

Step 2 In a Package Settings dialog box, add two upstream BWCs and two downstream BWCs, map them to the appropriate global controllers, and set their parameters (CIR, PIR, AL).

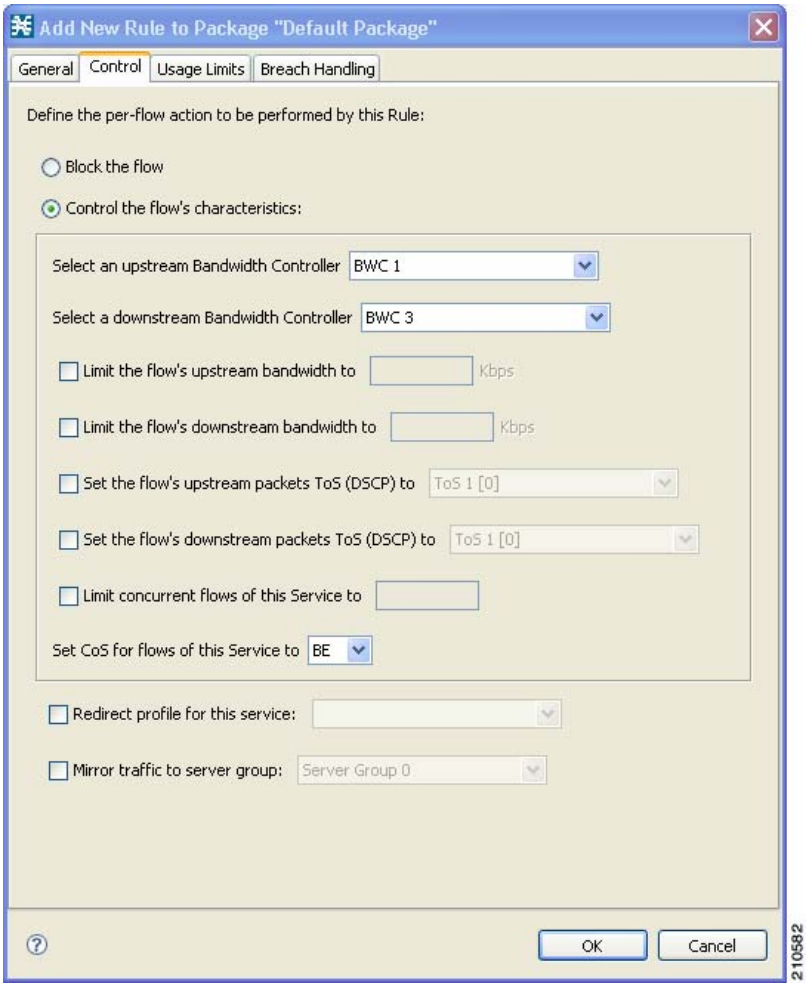


(Here, BWC1 will be for upstream P2P traffic and BWC3 will be for downstream P2P traffic; BWC2 will be for upstream streaming traffic and BWC4 will be for downstream streaming traffic.)

Step 3 Add a rule for the P2P service.



Step 4 In the Control tab, assign BWC 1 as the upstream BWC and BWC 3 as the downstream BWC.



Step 5 Repeat Steps 3 and 4 for the Streaming service, using BWC 2 as the upstream BWC and BWC 4 as the downstream BWC.

All subscriber traffic using these services will be added to the virtual queue total for these queues. In turn, the bandwidth available to the subscriber for these protocols will fluctuate, depending on how "full" these queues are.

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 the flow that goes through an iBWC is determined by the relative priority of one of:

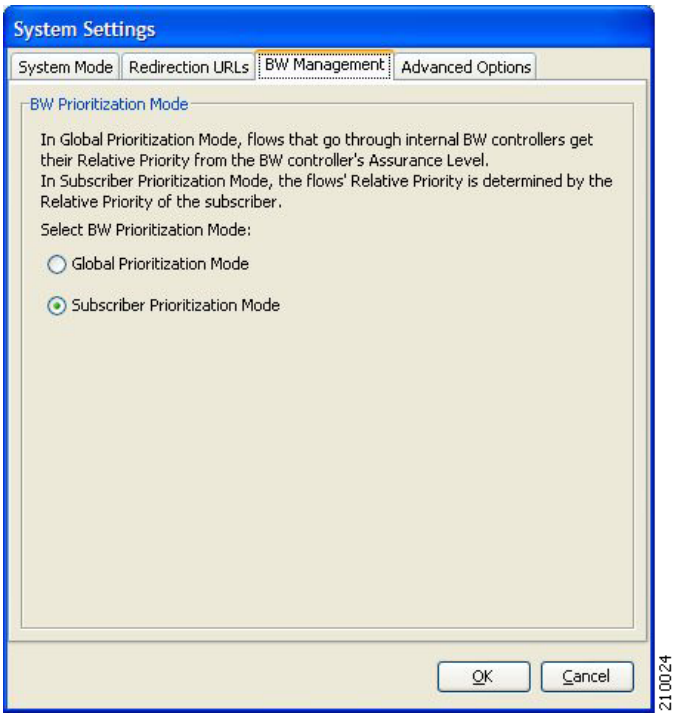
- The iBWC—In Global Prioritization Mode
- The subscriber—In Subscriber Prioritization Mode

Step 1 From the Console main menu, choose **Configuration > System Settings.**

The System Settings dialog box appears.

Step 2 Click the **BW Management** tab.

The BW Management tab opens.



Step 3 Select one of the **BW Prioritization Mode** radio buttons.

- **Global Prioritization Mode**
- **Subscriber Prioritization Mode**

Step 4 Click **OK.**

The System Settings 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 and depend on the subscriber's package (which defines the template controllers) and the physical link assigned to the subscriber.

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).

A service configuration can contain up to 1024 upstream global controllers and 1024 downstream global controllers (including the default global controllers). The maximum number of virtual links is limited by the number of directional template global controllers: the number of template global controllers times the number of virtual links cannot exceed 1024.

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.)

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 global controllers' PIR values.
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 subscriber's package and the virtual links' global controller configuration.

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 "Managing Virtual Links" in the "Managing the Collection Manager" chapter of the *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 From the Console main menu, choose **Configuration > Global Bandwidth Settings.**

The Global Bandwidth Settings dialog box appears.

Step 2 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 3 Click **OK.**

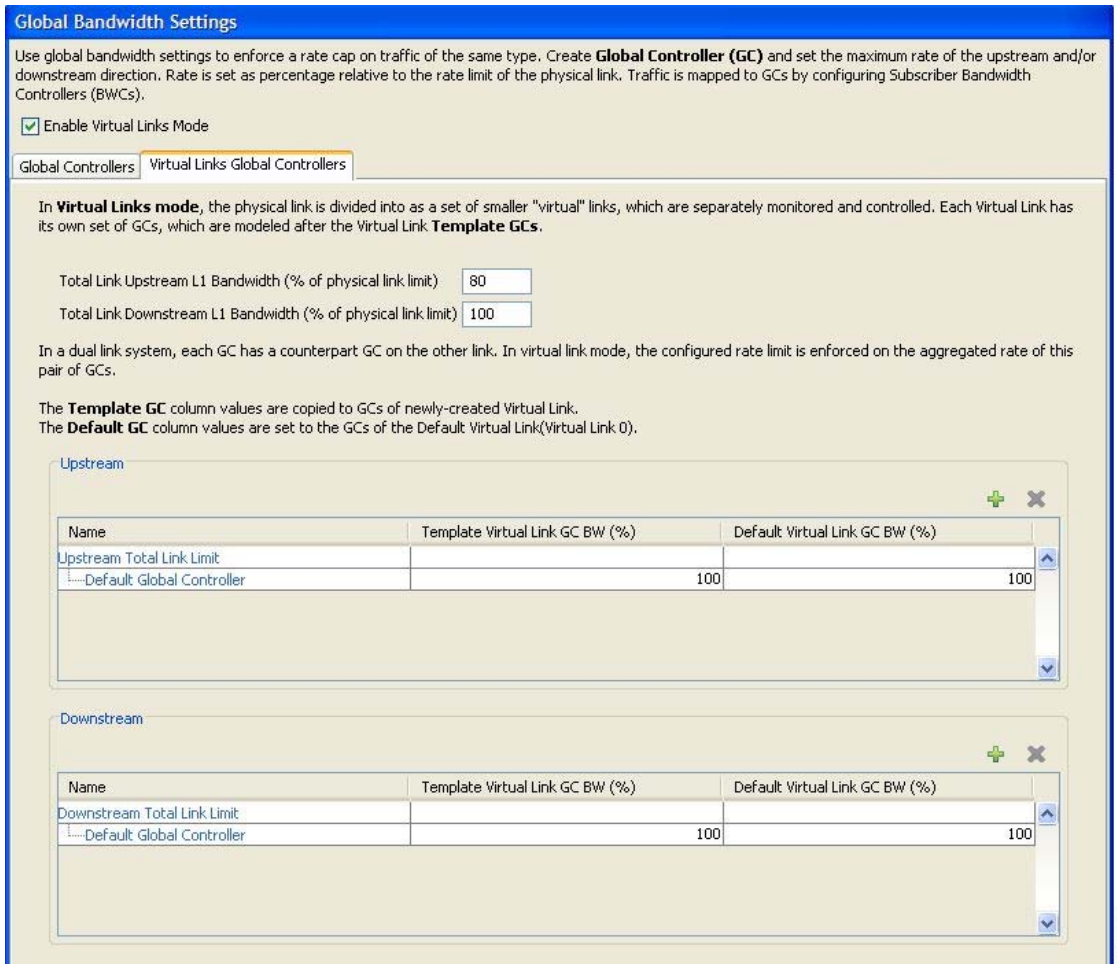
The Global Bandwidth Settings dialog box closes.

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 SCA BB is based on Layer 3 volume.)

Step 1 From the Console main menu, choose **Configuration > Global Bandwidth Settings.**

The Global Bandwidth Settings dialog box appears.



The maximum percentage of the total physical link bandwidth that can be used by any global controller is displayed at the top of the Virtual Links Global Controllers tab:

- **Total Link Upstream L1 bw (% of physical link limit)**
- **Total Link Downstream L1 bw (% of physical link limit)**

The percentage values of the global controllers defined in the rest of the dialog box depend on the values displayed here. So, for example, if the Total Link Upstream L1 bw (%) has a value of 80 and the upstream default global controller has a value of 100, this is 100% of 80% of the physical link bandwidth.

The main part of the dialog box contains the Upstream area listing upstream global controllers and the Downstream area listing downstream global controllers. Each list has three columns:

- **Name** —A unique name assigned to the global controller. The system automatically assigns the names Controller 1, Controller 2, and so on.
- **Template Virtual Link GC BW (%)** —The default maximum percentage of the total link limit permitted to global controllers of any created virtual links.
- **Default Virtual Link GC BW (%)** —The maximum percentage of the total link limit permitted to global controllers of the default virtual link.

For an explanation of the values in these columns, see How to View Global Controller Settings, page 9-31.

Step 2 To view the actual maximum bandwidth values, place the cursor over the Link 1 BW (%) cell.

A tooltip appears, showing the actual maximum bandwidth permitted to this global controller, in Mbps. This figure is calculated automatically by the system based on the possible SCE platform types (Gigabit Ethernet or Fast Ethernet), the controller maximum bandwidth percentage, and the total link bandwidth percentage.

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, refer to the following sections:

- How to Add Global Controllers, page 9-33
- How to Set the Maximum Bandwidth of Global Controllers, page 9-33
- How to Delete Global Controllers, page 9-35
- Managing Subscriber Bandwidth, page 9-36

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 a dual-link system, bandwidth limitations are applied to the sum of the two links.

Step 1 From the Console main menu, choose **Configuration > Global Bandwidth Settings.**

The Global Bandwidth Settings dialog box appears.

Step 2 Enter the maximum percentage of the physical link capacity that the link will carry in the **Total Link Upstream L1 bw (% of physical link limit)** field or the **Total Link Downstream L1 bw (% of physical link limit)** field.

The values displayed in the tooltips of all the cells in the Link 1 BW (%) cells change to reflect the new total link limit.

Step 3 Click **OK.**

Your changes are saved.

The Global Bandwidth Settings dialog box closes.

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 the *Cisco Service Control Engine (SCE) 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 commands 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]
```

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 subscriber's virtual links index

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 changed	Show information about virtual links whose PIR 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 Quotas

- How to Edit Quota Management Settings for Packages, page 9-50
- How to Select Quota Buckets for Rules, page 9-52
- How to Edit Breach-Handling Parameters for a Rule, page 9-53

How to Edit Quota Management Settings for Packages

You can define whether quota management for a package is performed by an external quota manager or by SCA BB.

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 9-52).

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 10-40). By default, this property has a value of zero, that is, all quota is replenished at the same time.

Each subscriber's quota replenishment occurs 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.) In the case of hourly quota replenish period, the scatter should therefore be set to 60 minutes.

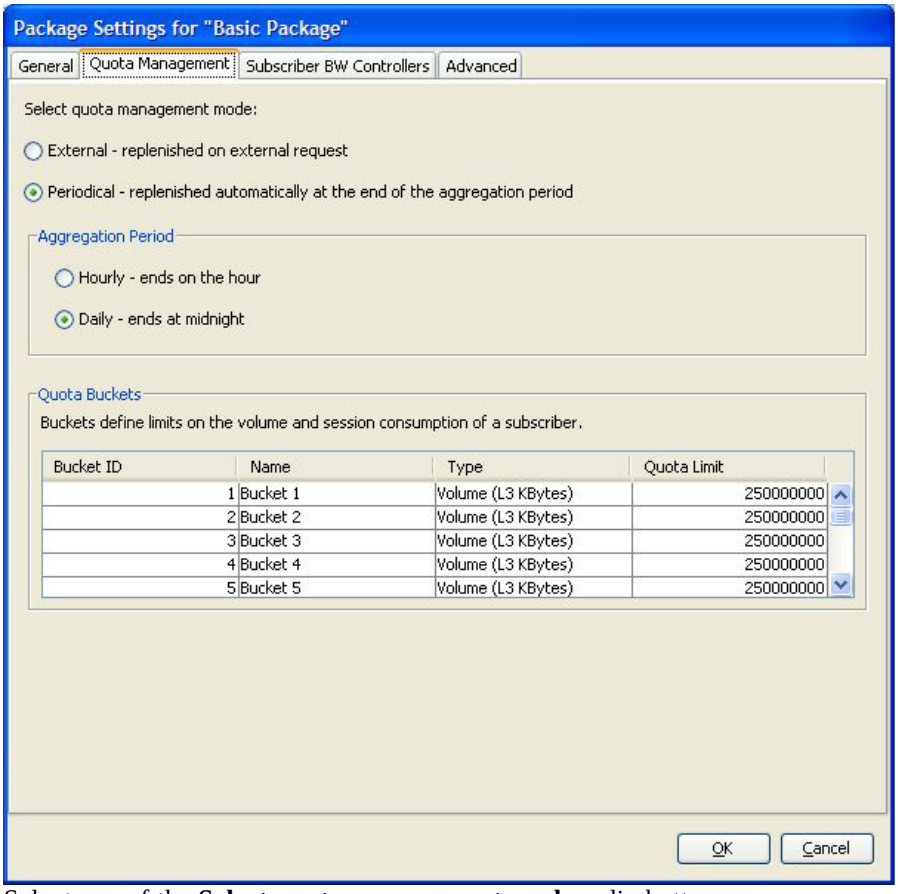
The quota replenish scatter function is independent of all other quota management parameters.

Step 1 In the Network Traffic tab, select a package from the package tree, and click (**Edit Package**).

The Package Settings dialog box appears.

Step 2 In the Package Settings dialog box, click the **Quota Management** tab.

The Quota Management tab opens.



Step 3 Select one of the **Select quota management mode** radio buttons.

- **External** —Replenishes quota on external request

Note External quota management is not supported when unidirectional classification is enabled. If you try to select the External radio button when unidirectional classification is enabled, a Package Error message appears.

Click **OK** to continue.

- **Periodical** —Replenishes quota automatically at the end of the aggregation period

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 9-50.)

Step 4 If you selected the Periodical radio button, select one of the **Aggregation Period** radio buttons to specify when the quota is renewed for the package:

- **Hourly Resolution** —Replenishes quota at each hour change
- **Daily Resolution** —Replenishes quota at midnight

Step 5 Configure the quota buckets.

Make sure that the configuration is appropriate to the rules that you will apply to the package. For example, if you do not configure a bucket with Type = Number of sessions, you cannot define a rule with usage limits defined in number of sessions.

a. (Optional) In the Name cell, enter a name for the bucket.

Note You can use the default name for the bucket. It is recommended that you enter a meaningful name.

b. Click in the Type cell, click the drop-down arrow that appears in the cell, and then select either **Volume (L3 Kbytes)** or **Number of sessions** from the drop-down list.

c. In the Quota Limit cell, enter the actual limit for this bucket in kilobytes or number of sessions, depending on the selected Type.

In the Quota Limit cell, enter the actual limit for this bucket in kilobytes or number of sessions, depending on the selected Type.

Note Quota limits can be set only if you selected the Periodical radio button in Step 4 above.

Step 6 Click **OK.**

The Package Settings dialog box closes.

All changes to the quota management settings are saved.

How to Select Quota Buckets for Rules

You can select the quota buckets that the flows mapped to a rule will use. The quota buckets in the drop-down lists were defined during package setup (see How to Edit Quota Management Settings for Packages, page 9-50). 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.

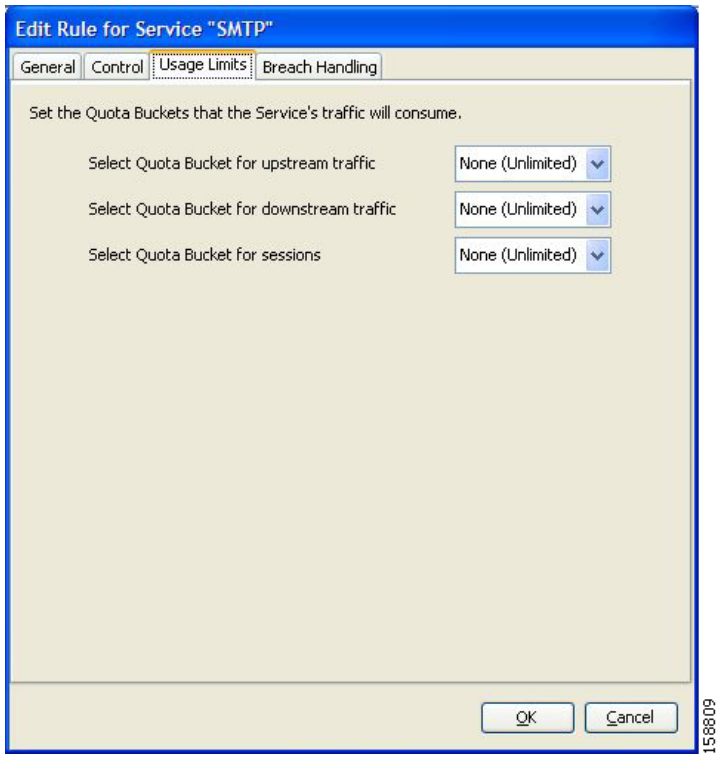
Step 2 In the right (Rule) pane, select a rule.

Step 3 Click  **(Edit Rule)**.

The Edit Rule for Service dialog box appears.

Step 4 Click the **Usage Limits** tab.

The Usage Limits tab opens.



Step 5 Select the desired bucket from each drop-down list.

- **Select Quota Bucket for upstream traffic**
- **Select Quota Bucket for downstream traffic**
- **Select Quota Bucket for sessions**

Note For unlimited quota, select **None (Unlimited).**

Step 6 To define behavior when a quota is breached (not relevant if all quota buckets have unlimited quota), continue with the instructions in the following section.

Step 7 Click **OK.**

The Edit Rule for Service dialog box closes.

All changes to the rule are saved.

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. SCA BB can generate Quota Breach RDRs even when this option is selected (see How to Manage Quota RDRs, page 8-6).
  - 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 10-37.) 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 this rule's traffic flows 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 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 10-27.

Step 1 In the Network Traffic tab, select a package from the package tree.

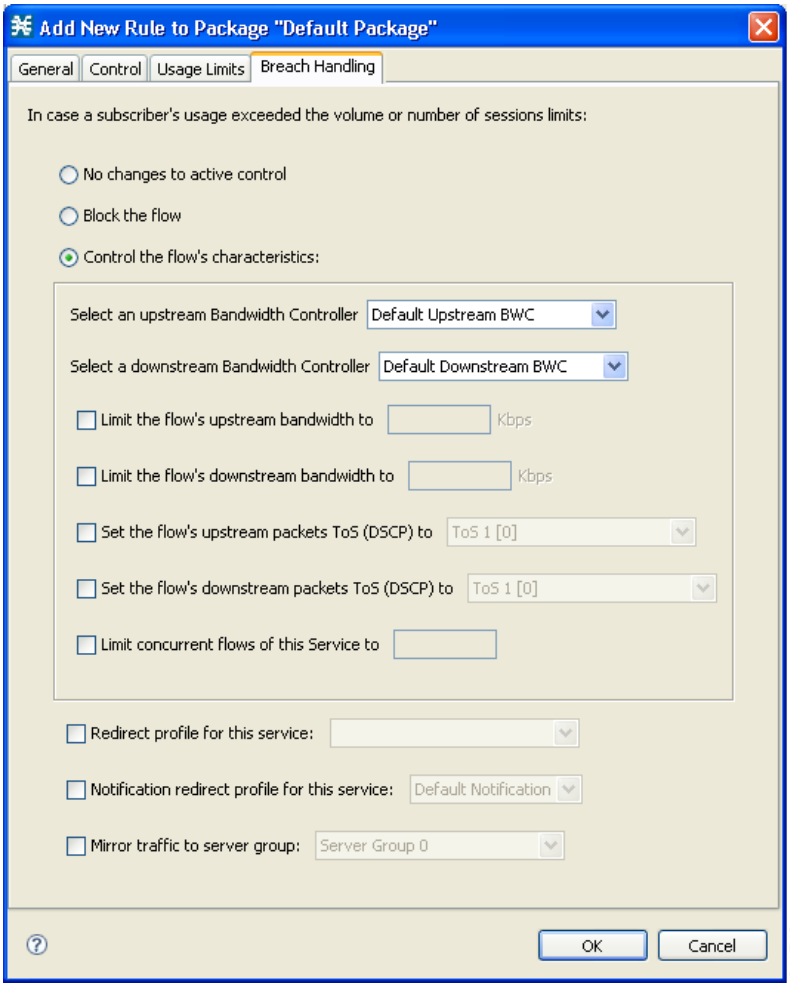
Step 2 In the right (Rule) pane, select a rule.

Step 3 Click (**Edit Rule**).

The Edit Rule for Service dialog box appears.

Step 4 Click the Breach Handling tab.

The Breach Handling tab opens.



Step 5 Set the flow's behavior when quota is breached.

- To block the flow when quota is breached, continue at Step 7.
- To change the flow's characteristics when quota is breached, continue at Step 9.
- To leave the flow unchanged when quota is breached, select the **No changes to active control** radio button.

Step 6 Continue at Step 10.

Step 7 Block flows that are mapped to the service of this rule.

a. Select the **Block the flow** radio button.

The Redirect to check box is enabled.

b. (Optional) To redirect blocked flows (for HTTP, HTTP Streaming, and RTSP), check the **Redirect to** check box.

Note Redirection is not supported when unidirectional classification is enabled. If you try to check the Redirect to check box when unidirectional classification is enabled, a Rule Error message appears.

Click **OK** to continue.

The Redirection URL Set drop-down list is enabled.

Note If the service or service group for this rule includes protocols that cannot be redirected, a Rule Warning message appears.

Click **OK,** and continue at Step 10.

c. Select a redirection URL set from the Redirect drop-down list.

Step 8 Continue at Step 10.

Step 9 Change the flow's characteristics.

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 (see How to Edit Package Subscriber BWCs, page 9-38).

  When the mouse is placed over the drop-down list, a tooltip appears containing the properties of the selected BWC (Peak Information Rate (PIR), Committed Information Rate (CIR), Global Controller, and Assurance Level).
- 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.

Step 10 (Optional) Activate subscriber notification.

Note A subscriber notification can be activated in addition to any of the three breach-handling options.

- Check the **Activate a Subscriber Notification** check box and then select the desired subscriber notification from the drop-down list.

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.

Click **OK** to continue.

Step 11 Click **OK.**

The Edit Rule for Service dialog box closes.

All changes to the rule are saved.



CHAPTER 10

Using the Service Configuration Editor: Additional Options

This chapter explains how to use additional, advanced functionality available in the Service Configuration Editor.

- The Service Security Dashboard, page 10-1
- Filtering the Traffic Flows, page 10-17
- Managing Subscriber Notifications, page 10-27
- Managing the System Settings, page 10-34
- Managing VAS Traffic-Forwarding Settings, page 10-45

The Service Security Dashboard

The Service Security Dashboard allows you to view and control all 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:

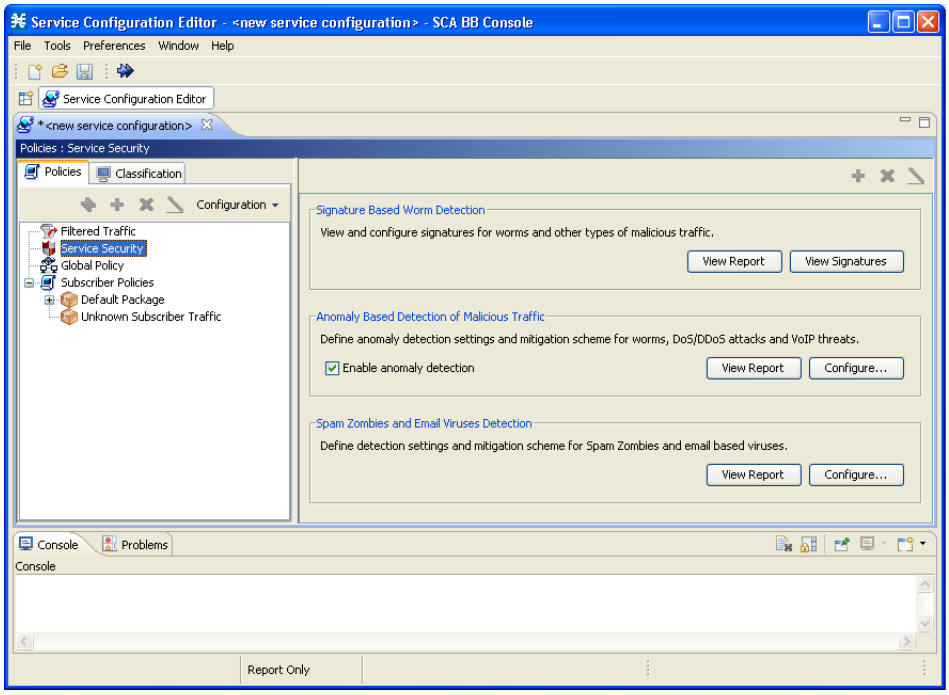
Disable anomaly-based detection of malicious traffic. (Clear the **Enable anomaly detection** check box.)

- How to View the Service Security Dashboard, page 10-2
- Managing Worm Detection, page 10-2
- Managing Anomaly Detection, page 10-3
- Managing Spam Detection, page 10-14
- Viewing Malicious Traffic Reports, page 10-16

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.



Managing Worm Detection

SCA BB uses three mechanisms for detecting worms:

- Signature based detection—The SCE platform's stateful Layer 7 capabilities 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 10-3.
- 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 10-15.

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

Step 1 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 Info

For more information, see Managing Protocol Signatures, page 7-33.

Managing Anomaly Detection

The most comprehensive threat detection method is anomaly detection.

- Anomaly Detection, page 10-3
- Anomaly Detection Parameters, page 10-4
- How to View Anomaly Detection Settings, page 10-5
- How to Add Anomaly Detectors, page 10-7
- Editing Anomaly Detectors, page 10-10
- How to Delete Anomaly Detectors, page 10-14

Anomaly Detection

The basic principle of anomaly detection is monitoring successful (correctly established for TCP, bi-directional 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 particularly robust indicator of malicious activity, and together with a rate qualifier 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.

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 detector's threshold settings) 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 will trigger 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 (see the "SCA BB Proprietary MIB Reference" chapter of the *Cisco Service Control Application for Broadband Reference Guide* for information about the Cisco proprietary MIB) indicating the beginning and end of an anomaly.
  - Notify Subscriber—Notify the relevant subscriber of the malicious activity, by redirecting his browsing sessions to a captive portal. To configure network attack subscriber notification, see Managing Subscriber Notifications, page 10-27.
  - 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 10-40).

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

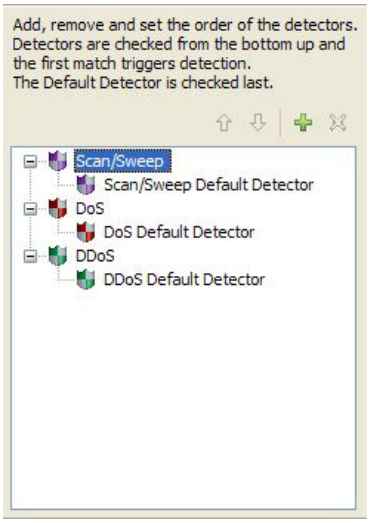
You can view a list of all anomaly detectors. The anomaly detectors are displayed in a tree, grouped according to detector category (Scan/Sweep, DoS, or DDoS).

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.**

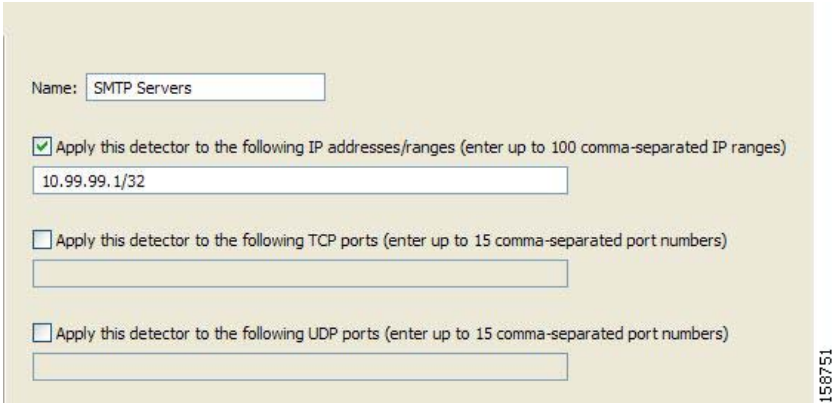
The Anomaly Detection Settings dialog box appears.

The detector tree is displayed in the left area of the dialog box; the right area is empty.

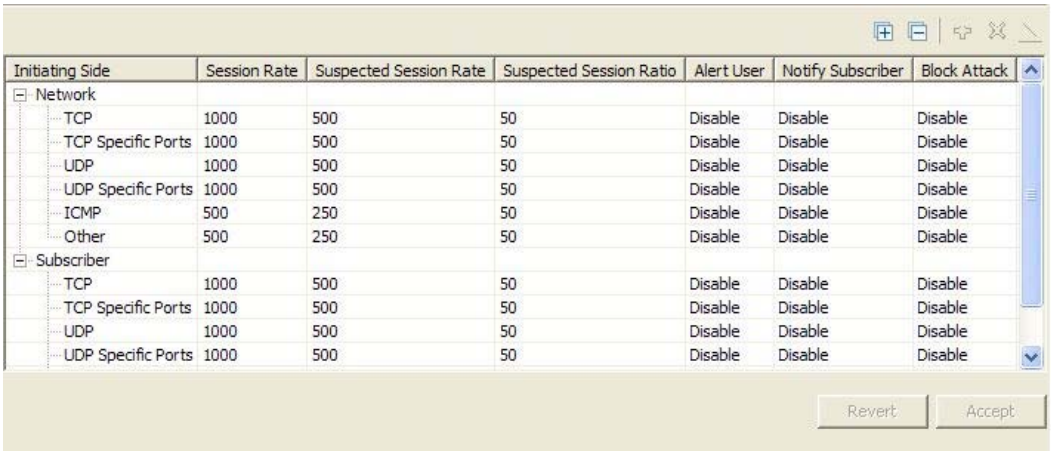


Step 2 In the detector tree, select a detector.

The detector parameters are displayed in the upper right area of the dialog box.



The detector's defined anomaly types 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.

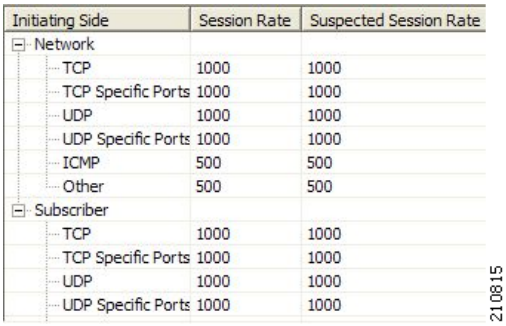


Initiating Side	Session Rate	Suspected Session Rate	Suspected Session Ratio	Alert User	Notify Subscriber	Block Attack
Network						
TCP	1000	500	50	Disable	Disable	Disable
TCP Specific Ports	1000	500	50	Disable	Disable	Disable
UDP	1000	500	50	Disable	Disable	Disable
UDP Specific Ports	1000	500	50	Disable	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

Revert Accept

210799

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.



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

210815

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 10-10).

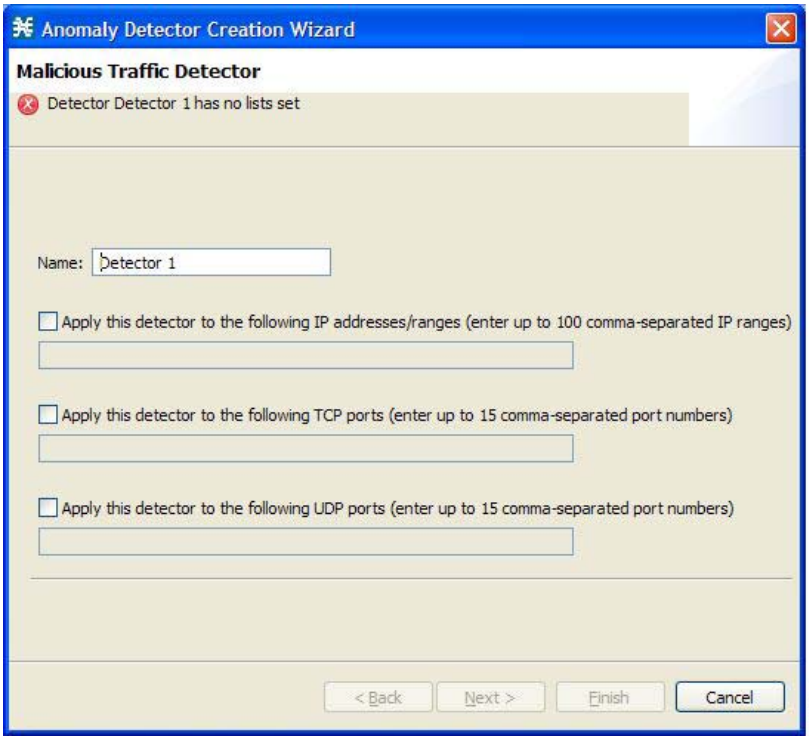
Step 1 In the Service Security Dashboard, in the Anomaly Based Detection of Malicious Traffic pane, click **Configure.**

The Anomaly Detection Settings dialog box appears.

Step 2 In the detector tree, select a detector category.

Step 3 Click .

The Anomaly Detector Creation wizard appears, open to the Malicious Traffic Detector page.



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

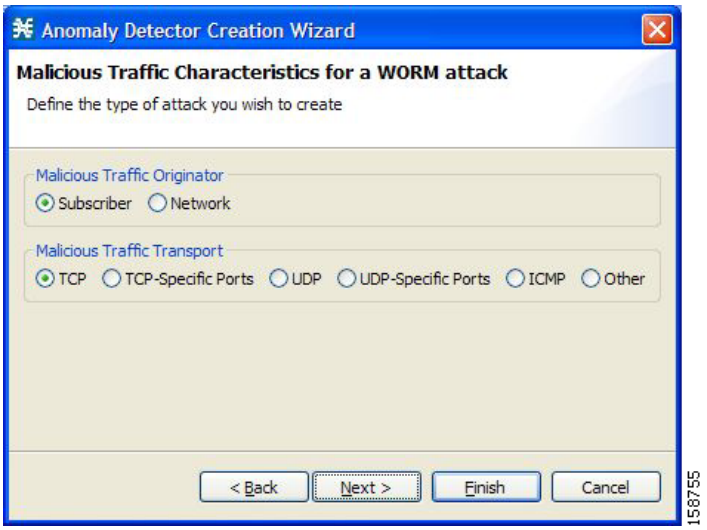
Step 5 Check one or more of the check boxes to limit the scope of the detector.

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.



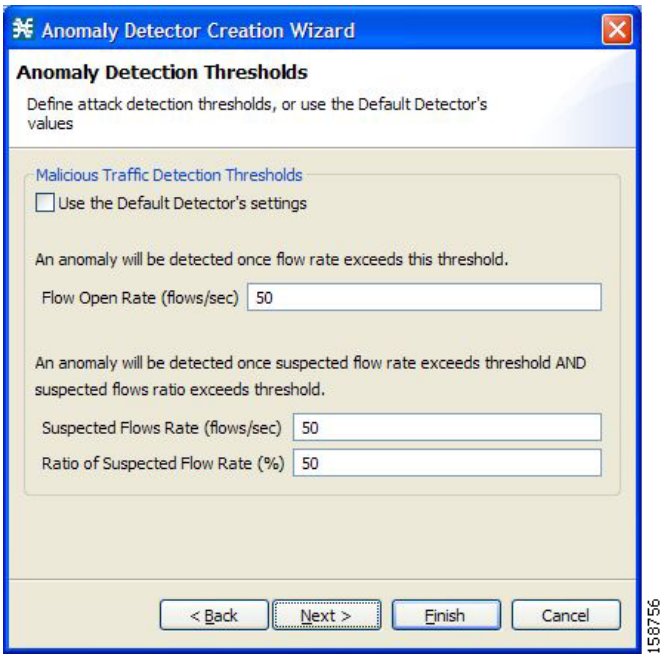
Step 8 Depending on the detector type that you are defining, select the originating side or the target side.

- 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.



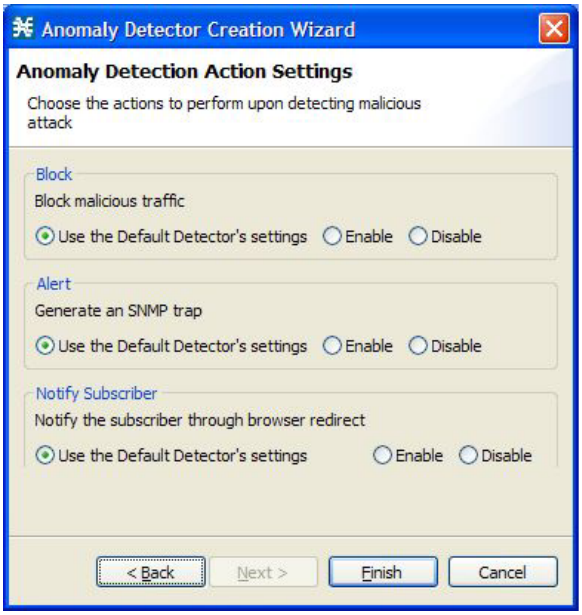
Step 11 Set the detector settings for this anomaly type.

Do one of the following:

- To use the default detector's settings, 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.



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 10-10.)

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 10-12).

Step 4 Set the detector settings for this anomaly type.

Do one of the following:

- To use the default detector's settings, 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 (**Create New Detector Item Under Detector Items Feature)**.

The Anomaly Detector Creation wizard appears, open to the Malicious Traffic Characteristics for a WORM attack page (see How to Add Anomaly Detectors, page 10-7).

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 default detector's settings, 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 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.

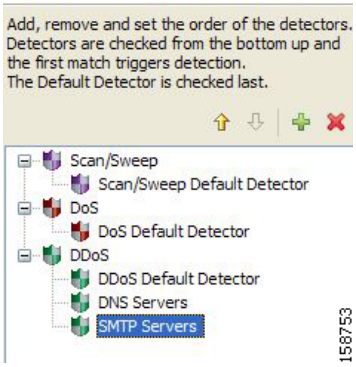
How to Change the Order in which Detectors are Checked

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.



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.

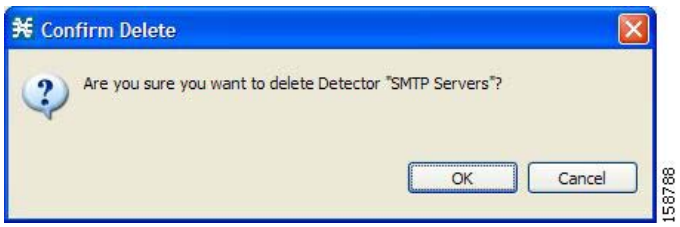
Step 1 In the Service Security Dashboard, in the Anomaly Based Detection of Malicious Traffic pane, click **Configure.**

The Anomaly Detection Settings dialog box appears.

Step 2 In the detector tree, select one or more user-defined detectors.

Step 3 Click .

A Confirm Delete message appears.



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 will work 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 a small number of SMTP sessions (at most a single session each time they send an e-mail message).
- Typical broadband subscribers normally use the ISP's SMTP server (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. To improve detection sensitivity, you can create a more specific service to narrow the scope of detection. Two possible services are:

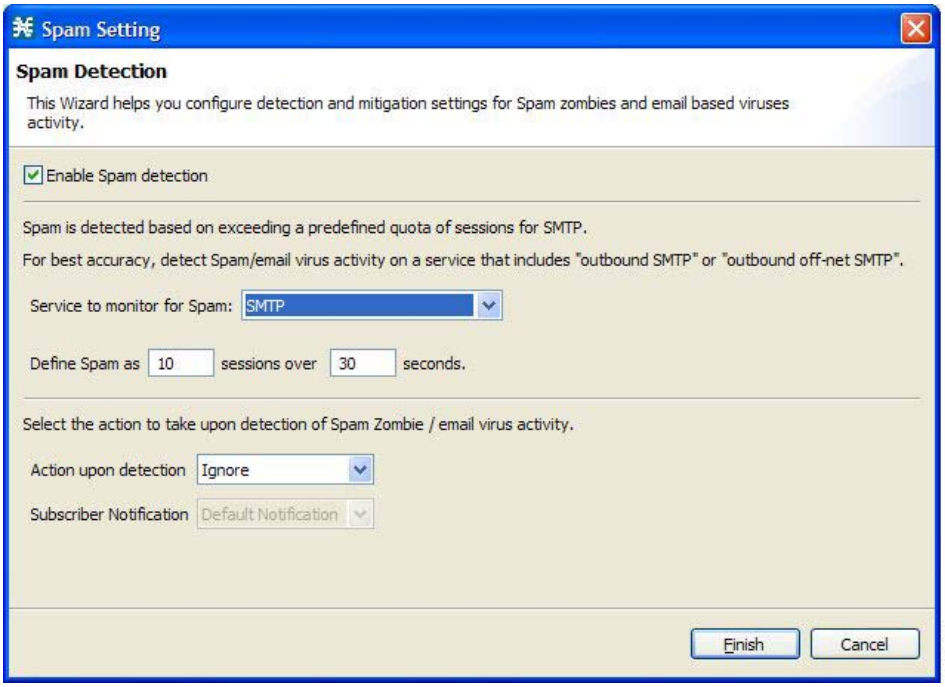
- "Outbound SMTP"—SMTP sessions generated by the subscriber.
- "OffNet SMTP"—SMTP sessions that are *not* targeted to the SMTP server of the subscriber's ISP. Limiting the service to OffNet can avoid accounting for legitimate sessions.

Note Prominent non-ISP e-mail providers (for example, Google and Yahoo!) now provide SMTP-based service, so OffNet is no longer a very good differentiator between legitimate and illegitimate activity. To refine the OffNet service, you must include an SMTP server list in the "OnNet SMTP" service definition; all other SMTP servers will be OffNet.

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 Setting dialog box appears.



Step 2 (Optional) To disable spam detection, uncheck the **Enable Spam detection** check box.

All other fields are disabled.

Continue at Step 7.

Step 3 From the Service to monitor for Spam drop-down list, select a service.

Note Leave the default value for the monitored service (SMTP), unless you have defined a more specific service, such as "Outbound SMTP" or "OffNet SMTP".

Step 4 Define the threshold e-mail session rate for anomalous behavior.

Step 5 From the Action upon detection drop-down list, select the action to be taken when malicious activity is detected.

Available actions are:

- **Ignore**
- **Block**
- **Notify**
- **Block and notify**

If you select Notify or Block and notify, the Subscriber Notification drop-down list is enabled.

Step 6 If you selected Notify or Block and notify, select a subscriber notification.

Note To define an appropriate subscriber notification, see Managing Subscriber Notifications, page 10-27.

Step 7 Click **Finish.**

The Spam Setting dialog box closes.

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 10-16
- How to View a Service Security Report, page 10-17

Malicious Traffic Reports

A number of reports dealing with malicious traffic can be displayed in the Reporter tool:

- Global reports:
  - Global Scan or Attack Rate
  - Global DoS Rate
  - Infected 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 the *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 will not appear in any records generated for analysis purposes and will not be 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 flow's Layer 7 characteristics. (See Managing Advanced Service Configuration Options, page 10-40.) 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 SCA BB reports.

- Information About Traffic Filtering, page 10-18
- How to View Filter Rules for a Package, page 10-20
- How to Add Filter Rules, page 10-20

- How to Edit Filter Rules, page 10-26
- How to Delete Filter Rules, page 10-26
- How to Activate and Deactivate Filter Rules, page 10-27

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 SCA BB Filtered Traffic mechanism is used to address this need.

Note Most voice traffic is handled automatically by the SCE platform to reduce latency (see Automatic Quick Forwarding of Media Flows, page 10-19).

- The SCA BB Filtered Traffic Mechanism, page 10-18
- Filter Rule Actions, page 10-19
- Filter Rules and Service Rules, page 10-19
- Automatic Quick Forwarding of Media Flows, page 10-19

The SCA BB Filtered Traffic Mechanism

The 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 in conjunction 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 10-34).

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 in order 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 will be bypassed with minimum delay. Furthermore, if only Bypass is matched, the packet/flow will 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 will be 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 will be subject 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.

How to View Filter Rules for a Package

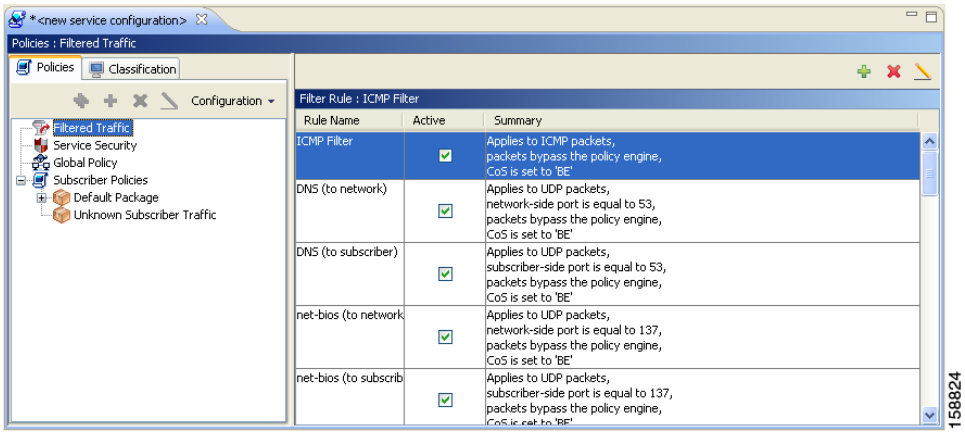
You can view a list of the filter rules included in a service configuration.

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 10-26).

Step 1 In the Network Traffic tab, select the **Filtered Traffic** node.

A list of all filter rules is displayed in the right (Rule) pane.



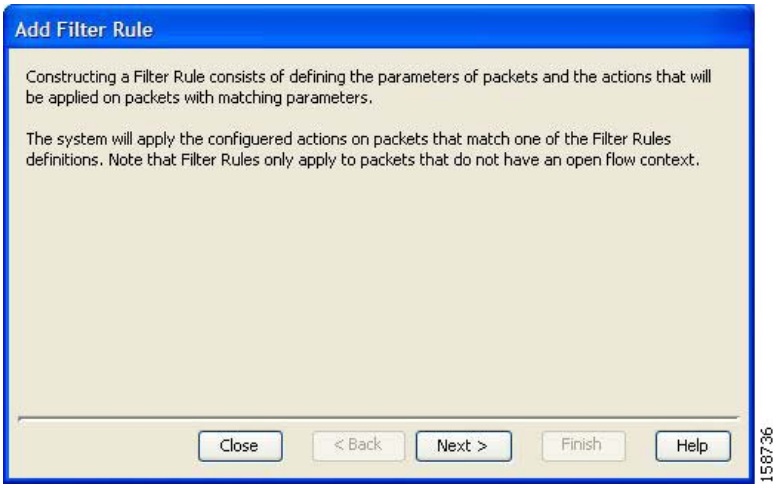
How to Add Filter Rules

The Add Filter Rule wizard guides you through the process of adding a filter rule.

Step 1 In the Network Traffic tab, select the **Filtered Traffic** node.

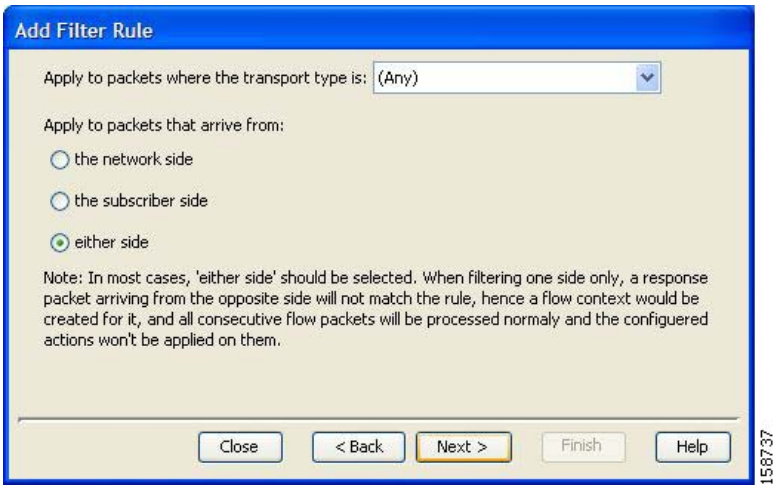
Step 2 Click (**Add Rule)** in the right (Rule) pane.

The Add Filter Rule wizard appears.



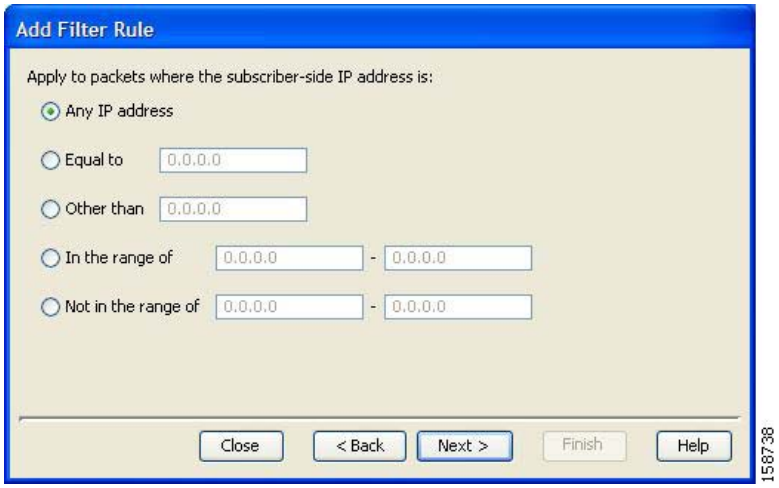
Step 3 Click **Next.**

The Transport Type and Direction page of the Add Filter Rule wizard opens.



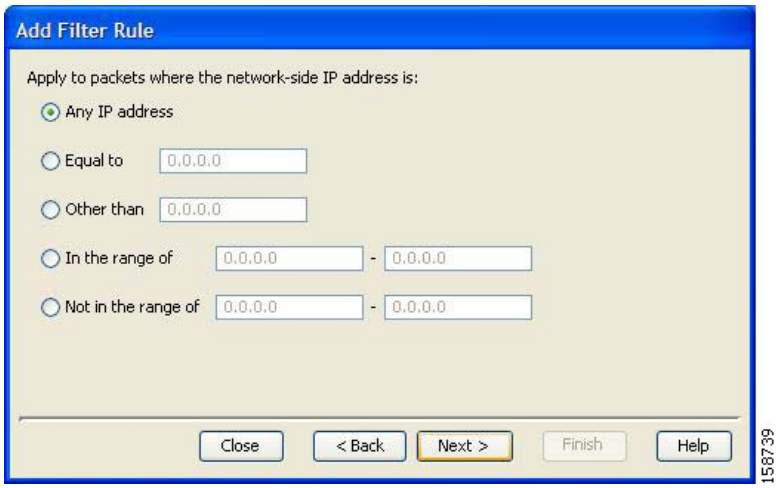
Step 4 Select the transport type and initiating side and click **Next.**

The Subscriber-Side IP Address page of the Add Filter Rule wizard opens.



Step 5 Define the subscriber-side IP address and click **Next.**

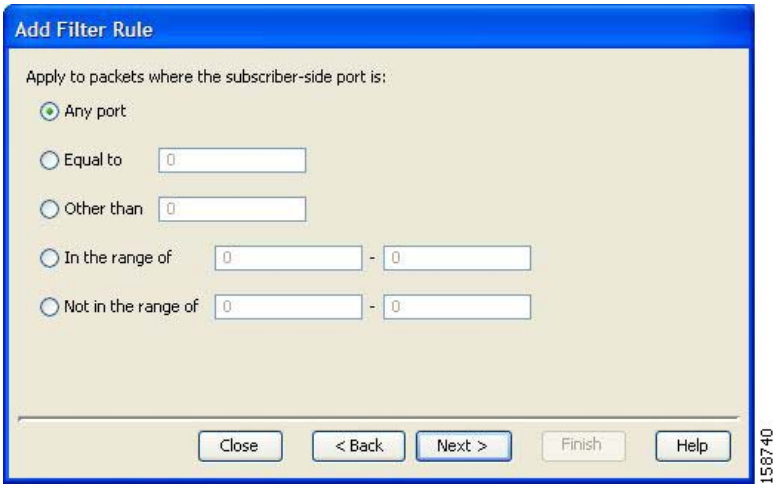
The Network-Side IP Address page of the Add Filter Rule wizard opens.



Step 6 Define the network-side IP address and click **Next.**

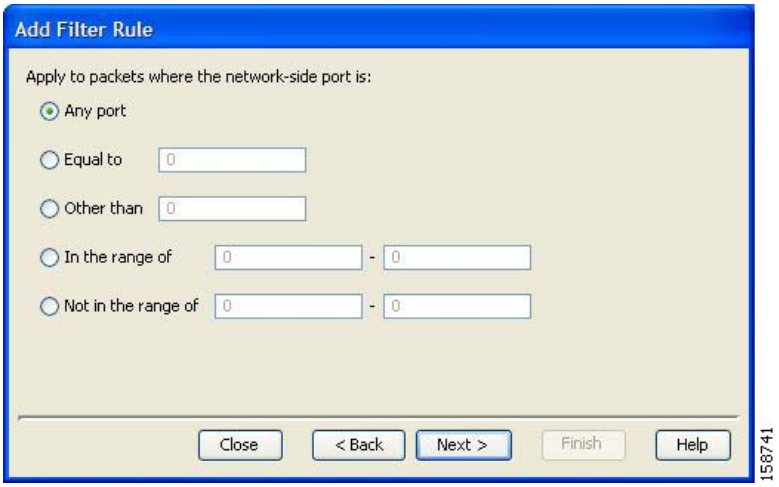
If the transport type selected in Step 4 was *not* TCP or UDP, the ToS page of the Add Filter Rule wizard opens. Go to Step 9.

If the transport type selected in Step 4 was TCP or UDP, the Subscriber-Side Port page of the Add Filter Rule wizard opens.



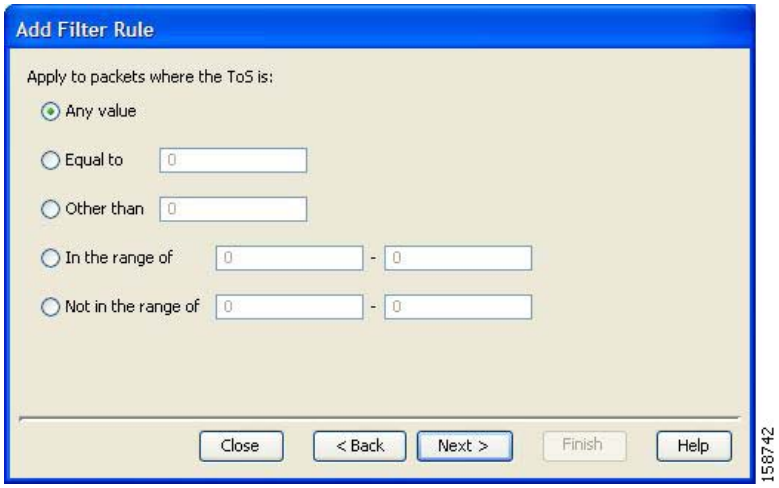
Step 7 Define the subscriber-side port and click **Next.**

The Network-Side Port page of the Add Filter Rule wizard opens.



Step 8 Define the network-side port and click **Next.**

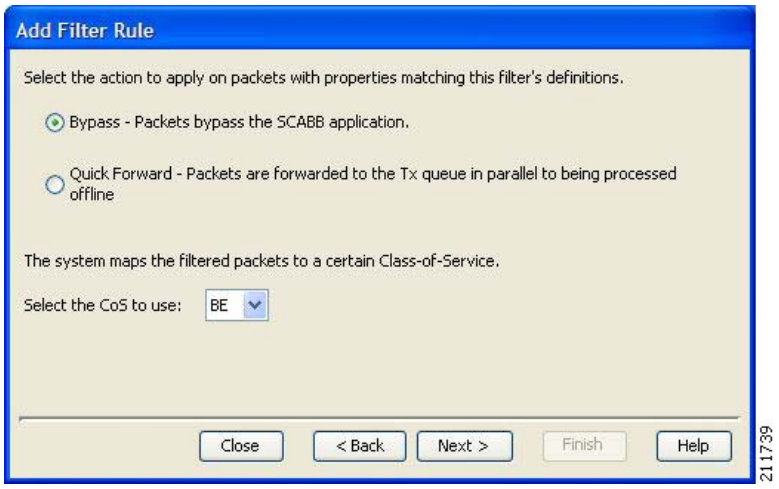
The ToS page of the Add Filter Rule wizard opens.



Step 9 Define the ToS and click **Next.**

Note Acceptable values for ToS are 0 to 255.

The Action and Class-of-Service page of the Add Filter Rule wizard opens.

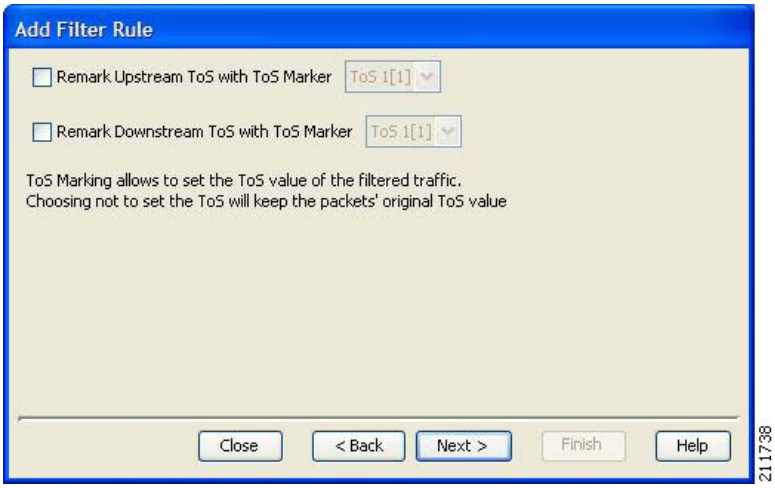


Step 10 Select the radio button for the required action.

- **Bypass** —Packets that match this filter rule are not passed to 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 SCA BB for processing.

Step 11 Select a Class-of-Service value, and click **Next.**

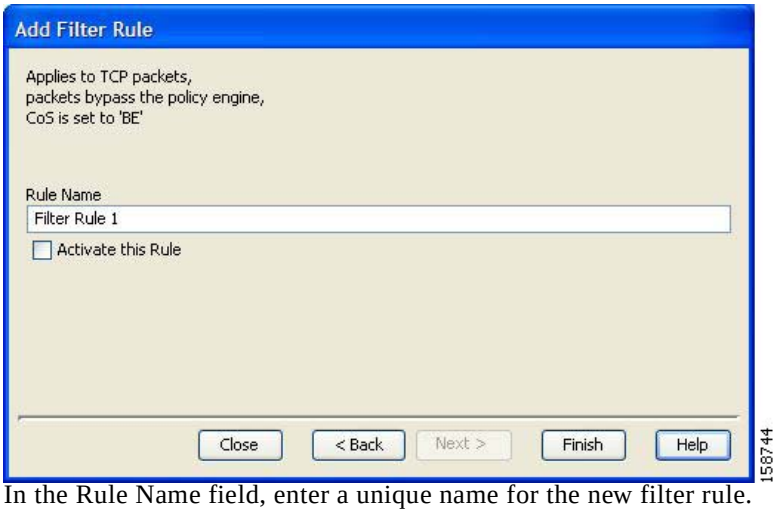
The ToS Marking page of the Add Filter Rule wizard opens.



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 9-28) overrides DSCP ToS marking in that direction by a filter (that is, the DSCP ToS value will not be changed). In this case, the Problems View will display 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 will be created, but no DSCP ToS remarking will occur. In this case, the Problems View will display a Warning.
- If you select Quick Forward in the previous Step, SCA BB receives the *original* package and processes it. That is, the original DSCP ToS value is seen by the application regardless of the ToS marking action selected in the filter rule.

The Finish page of the Add Filter Rule wizard opens.



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 Edit Filter Rules

You can view and edit the parameters of a filter rule.

Step 1 In the Network Traffic 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  (**Edit Rule)**.

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, page 10-20, Steps 4 to 14.

Step 5 Click **Finish.**

The filter rule is changed and relevant changes appear 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.

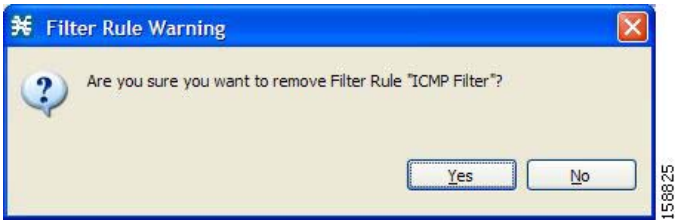
Step 1 In the Network Traffic tab, select the **Filtered Traffic** node.

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 (**Delete Rule**).

A Filter Rule Warning message appears.



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 Network Traffic 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.

The Cisco Service Control Application for Broadband (SCA BB) supports a maximum of 31 subscriber notifications, including the default notification and the Network Attack Notification.

- Subscriber Notification Parameters, page 10-28
- Network Attack Notification, page 10-29
- How to View Subscriber Notifications, page 10-31
- How to Add Subscriber Notifications, page 10-32

- How to Edit Subscriber Notifications, page 10-33
- How to Delete Subscriber Notifications, page 10-33

Subscriber Notification Parameters

A subscriber notification is defined by the following parameters:

- Name—Each subscriber notification must have a unique name.

Note You cannot change the name of the Default Notification or the Network Attack Notification.

- Destination URL—A configurable destination URL to which the subscriber's HTTP flows are redirected after redirection is activated. This web page usually contains the message that needs to be conveyed to the subscriber.
- Notification Parameters—The query part of the destination URL, which can be optionally added upon redirection.

  The format of the notification parameters to be added to the destination URL is:

  `?n=<notification-ID>&s=<subscriber-ID>`

  where **<notification-ID>** is the ID of the notification that redirected the subscriber and **<subscriber-ID>** is the subscriber name.

Note There is a different format for the Network Attack Notification Parameters, page 10-30.

- The destination web server can use these parameters to carry a more purposeful message to the subscriber.
- Dismissal method—Indicates when to dismiss or deactivate the notification state. The dismissal method is one of the following:
  - Subscriber browses to destination URL (default)—As soon as the subscriber browses to the destination URL, they are considered as notified and the notification state is dismissed.

    For example, if a quota was exceeded, the notification state is dismissed as soon as the subscriber browses to the destination URL that informs them of this fact (even though the subscriber still remains in a breach state).
  - The condition that activated the notification no longer holds—The dismissal of the notification state is dependent on the resolution of the condition, rather than on the subscriber.

    For example, if a quota was exceeded, the notification state is dismissed only when the subscriber completes the procedure to refresh their quota.

Note This option is *not* available for the Network Attack Notification. A subscriber must respond to the notification before the notification is dismissed.

  - Subscriber browses to dismissal URL—The notification state is not dismissed until the subscriber proceeds from the destination URL to a different, final URL.

All HTTP flows are redirected until the notification is dismissed, which takes place when the subscriber accesses the dismissal URL. By default, the destination URL is also the dismissal URL and a notification is dismissed as soon as the first redirection takes place. However, you can define a different dismissal URL, so that the subscriber must acknowledge the notification.

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 will not be 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 subscriber notification (see How to Add Subscriber Notifications, page 10-32). You can modify them at any time (see How to Edit Subscriber Notifications, page 10-33).

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 10-1.) 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 10-40.

Caution In earlier releases of 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 10-30
- Example of URL with Description Tail, page 10-31

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=<open-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	

Table 10-1 Description Tail Fields (continued)

Field	Description	Possible Values
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)	

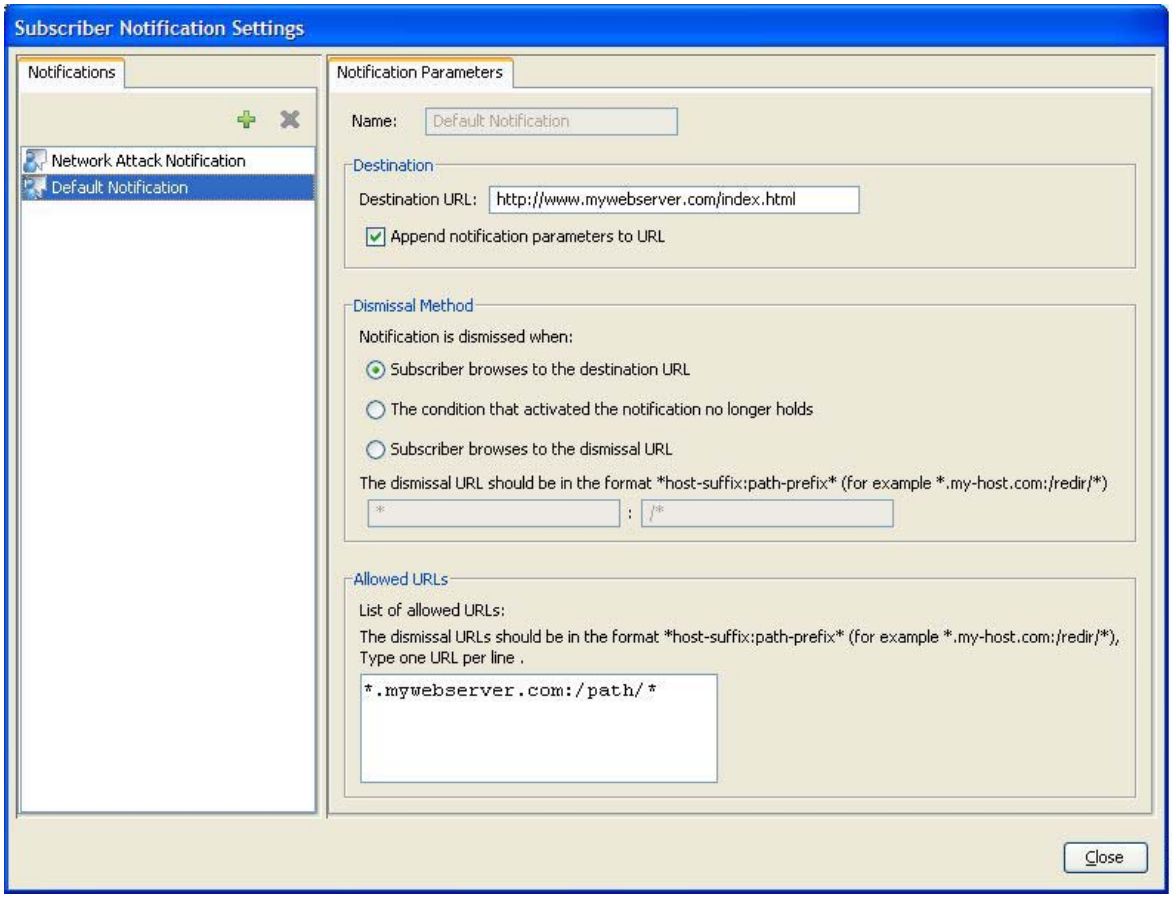
Example of URL with Description Tail

```
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 View Subscriber Notifications

Step 1 From the Console main menu, choose **Configuration > Subscriber Notifications.**

The Subscriber Notifications Settings dialog box appears.



The Notifications tab displays a list of all subscriber notifications.

Step 2 Click a subscriber notification in the list to display its parameters.

The parameters of the subscriber notification are displayed in the Notification Parameters tab.

Step 3 Click **Close.**

The Subscriber Notifications Settings dialog box closes.

How to Add Subscriber Notifications

You can add up to 29 subscriber notifications to a service configuration.

Note Creating a subscriber notification does not activate the subscriber notification feature. After the subscriber notification is defined, it must be activated for a particular package. (See How to Edit Breach-Handling Parameters for a Rule, page 9-53.)

Step 1 From the Console main menu, choose **Configuration > Subscriber Notifications.**

The Subscriber Notifications Settings dialog box appears.

Step 2 Click (**Add**).

Step 3 In the Name field, enter a unique name for the new subscriber notification.

Note You can use the default name for the subscriber notification. It is recommended that you enter a meaningful name

Step 4 In the Destination URL field, enter the destination URL.

Step 5 (Optional) If notification parameters will be appended to the destination URL, check the **Append notification parameters to URL** check box.

Step 6 Select one of the **Dismissal Method** radio buttons.

- **Subscriber browses to the destination URL**
- **The condition that activated the notification no longer holds**
- **Subscriber browses to the dismissal URL**

Step 7 If you selected Subscriber browses to the dismissal URL in Step 6, enter the dismissal URL host-suffix and path-prefix in the fields provided.

Step 8 Enter any allowed URLs, one per line, in the Allowed URLs text box.

Step 9 Click **Close.**

The Subscriber Notifications Settings dialog box closes.

How to Edit Subscriber Notifications

You can modify notification parameters at any time.

Step 1 From the Console main menu, choose **Configuration > Subscriber Notifications.**

The Subscriber Notifications Settings dialog box appears.

Step 2 Click a subscriber notification in the Notifications tab to display its parameters.

Step 3 Edit the parameters of the subscriber notification in the Notification Parameters tab.

Step 4 Click **Close.**

The Subscriber Notifications Settings dialog box closes.

How to Delete Subscriber Notifications

You can delete subscriber notifications at any time.

You cannot delete the default notification or the Network Attack Notification.

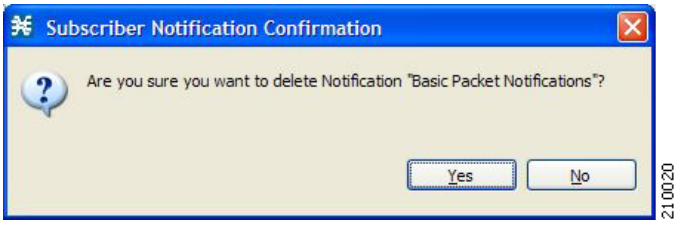
Step 1 From the Console main menu, choose **Configuration > Subscriber Notifications.**

The Subscriber Notifications Settings dialog box appears.

Step 2 Click a subscriber notification in the Notifications tab.

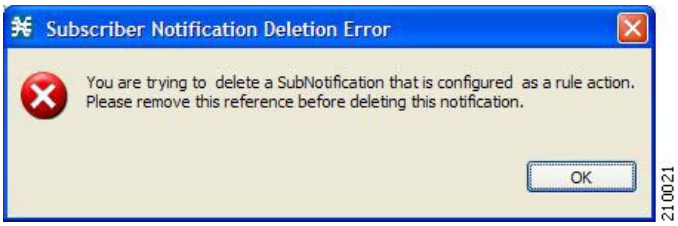
Step 3 Click  **(Delete)**.

A Subscriber Notification Confirmation message appears.



Step 4 Click **Yes.**

- If the specified subscriber notification is being used by a rule, a Subscriber Notification Deletion Error message is displayed.



Note The subscriber notification cannot be deleted until you unassign it or deactivate it in all service rules. (See How to Edit Breach-Handling Parameters for a Rule, page 9-53.)

- The selected subscriber notification is deleted.

Step 5 Click **Close.**

The Subscriber Notifications Settings dialog box closes.

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
- The redirection URLs for protocols that support redirection
- BW prioritization mode (see How to Set BW Management Prioritization Mode, page 9-43)
- 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 10-34
- Asymmetric Routing Classification Mode, page 10-35

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 will only generate 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 10-35
- Protocol Classification, page 10-35
- Switching to Asymmetric Routing Classification Mode, page 10-36
- Switching from Asymmetric Routing Classification Mode, page 10-36

Unsupported Features

The following 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 with the exception of unidirectional UDP flows. Because it is impossible to know the server side of a unidirectional UDP flow, SCA BB tries to classify the protocol using the destination port of the first packet; if no exact match is found, 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

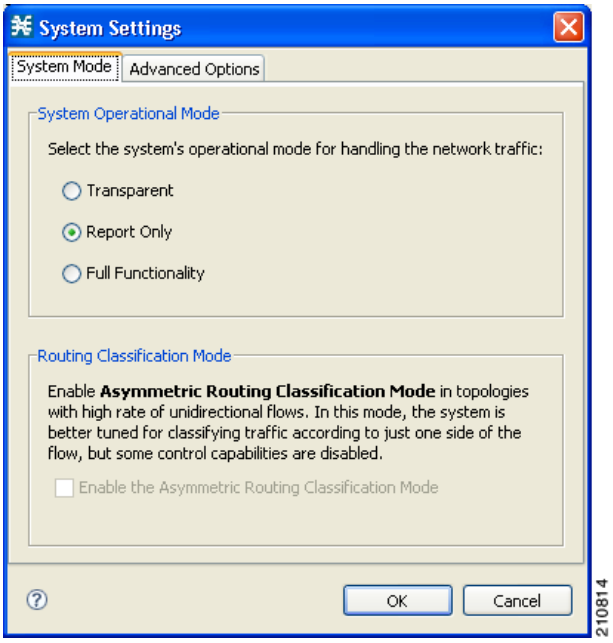
If you create a service configuration in asymmetric routing classification mode:

- 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 Console main menu, choose **Configuration > System Settings.**

The System Settings dialog box appears.



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.

Setting Redirection Parameters

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 set to use when defining rules (see How to Define Per-Flow Actions for a Rule, page 9-14).

Note Redirection is not supported when unidirectional classification is enabled.

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 49 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>
```

How to Add a Set of Redirection URLs

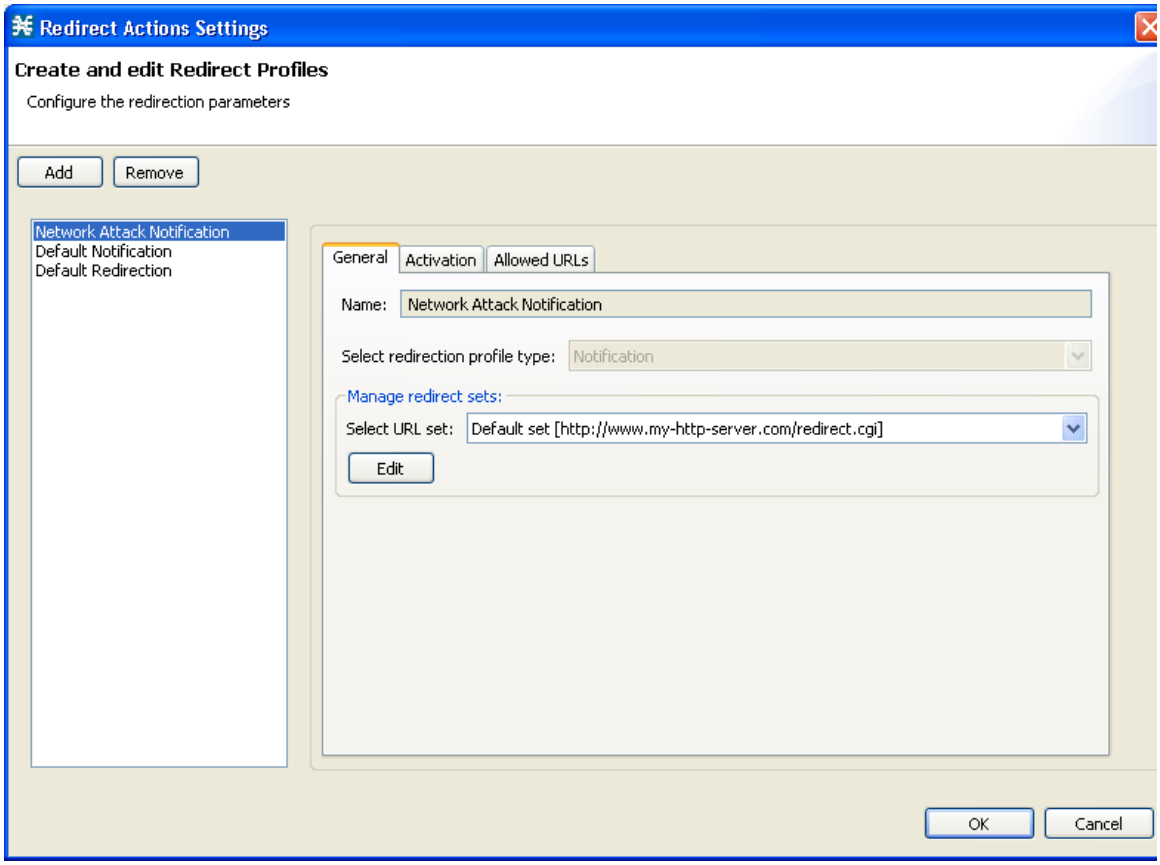
You can add up to 49 redirection sets.

Step 1 From the Console main menu, choose **Configuration > System Settings.**

The System Settings dialog box appears.

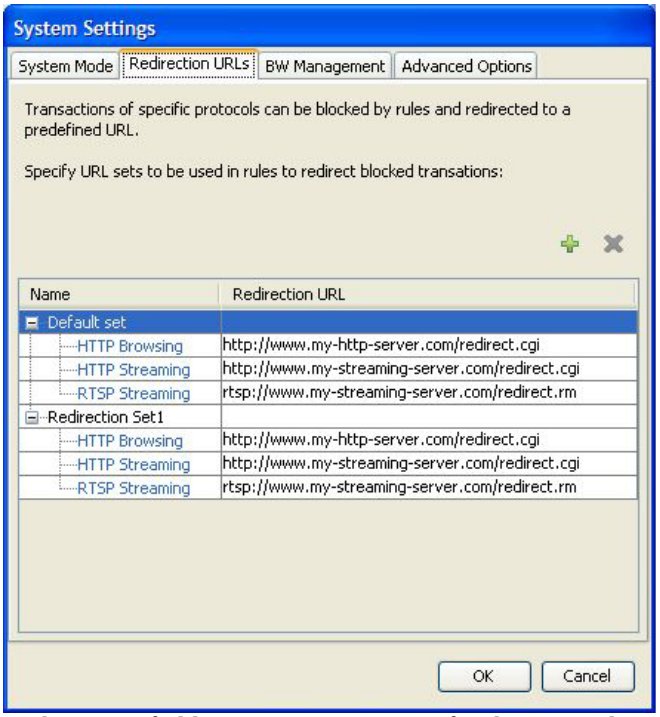
Step 2 Click the **Redirection URLs** tab.

The Redirection URLs tab opens.



Step 3 Click (**Add**).

A new redirection set containing the default redirection URLs is added to the redirection set list.



Step 4 In the Name field, enter a unique name for the new redirection set.

Note You can use the default name for the redirection set, but it is recommended that you enter a meaningful name.

Step 5 Enter new values in the Redirection URL cells of the new redirection set.

Step 6 Click **OK.**

The System Settings dialog box closes.

The Redirection group is added to the redirection set list.

How to Edit Redirection Parameters

Step 1 From the Console main menu, choose **Configuration > System Settings.**

The System Settings dialog box appears.

Step 2 Click the **Redirection URLs** tab.

The Redirection URLs tab opens.

Step 3 Click a URL in the **Redirection URL** column.

Step 4 Enter a new URL.

Step 5 Click **OK.**

The System Settings dialog box closes.

The Redirection settings are saved.

How to Delete a Set of Redirection URLs

Step 1 From the Console main menu, choose **Configuration > System Settings.**

The System Settings dialog box appears.

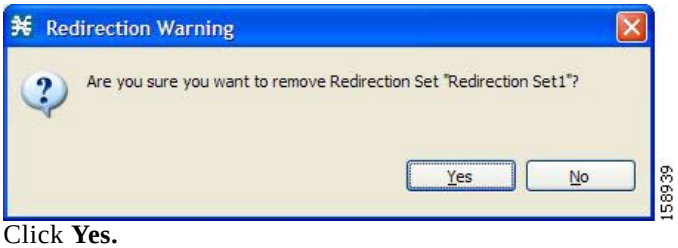
Step 2 Click the **Redirection URLs** tab.

The Redirection URLs tab opens.

Step 3 Click the name of a redirection set.

Step 4 Click (**Delete**).

A Redirection Warning message appears.



Step 5 Click **Yes.**

The redirection set is deleted.

Step 6 Click **OK.**

The System Settings dialog box closes.

The Redirection settings are 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 10-41
- How to Edit Advanced Service Configuration Options, page 10-44

The Advanced Service Configuration Properties

Table 10-2 lists the advanced service configuration properties:

Table 10-2 Advanced Service Configuration Properties

Property	Default Value	Description
Classification		
Guruguru detailed inspection mode enabled	FALSE	The Guruguru protocol is used by the Guruguru file-sharing application popular in Japan. SCA BB provides two inspection modes for classification of this protocol: • Default—Suitable for networks where little Guruguru traffic is expected. This is usual in all countries except Japan. • Detailed—Suitable for networks where Guruguru traffic is expected to be common. This should occur in Japanese networks only.
Kuro detailed inspection mode enabled	FALSE	The Kuro protocol is used by the Kuro file-sharing application popular in Japan. 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 should occur in Japanese networks only.
Soribada detailed inspection mode enabled	FALSE	The Soribada protocol is used by the Soribada file-sharing application popular in Japan. 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 should occur 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.

Table 10-2 Advanced Service Configuration Properties (continued)

Property	Default Value	Description
UDP destination port signatures	67: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, 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 flow's first packet.
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.
V-Share detailed inspection mode enabled	FALSE	The V-Share protocol is used by the V-Share file-sharing application popular in Japan. SCA BB provides two inspection modes for classification of this protocol: • Default—Suitable for networks where little V-Share traffic is expected. This is usual in all countries except Japan. • Detailed—Suitable for networks where V-Share traffic is expected to be common. This should occur 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. 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 should occur in Japanese networks only.
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.

Table 10-2 Advanced Service Configuration Properties (continued)

Property	Default Value	Description
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 will not be blocked to allow notification of the attack to be sent to the subscriber.
Policy Check		
Ongoing policy check mode enabled	TRUE	Specifies whether policy changes affect flows that are already open.
Time to bypass between policy checks	30	Maximum time (in seconds) that may pass before policy changes affect flows that are already open.
Quota Management		
Grace period before first breach	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 randomly scatter the periodic quota replenishment.
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.

Table 10-2 Advanced Service Configuration Properties (continued)

Property	Default Value	Description
Reporting		
Media Flow RDRs enabled	TRUE	Specifies whether to generate Media Flow 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 the ISG documentation in the "Managing the SCMP" chapter of the *Cisco Service Control Engine (SCE) Software Configuration Guide*.

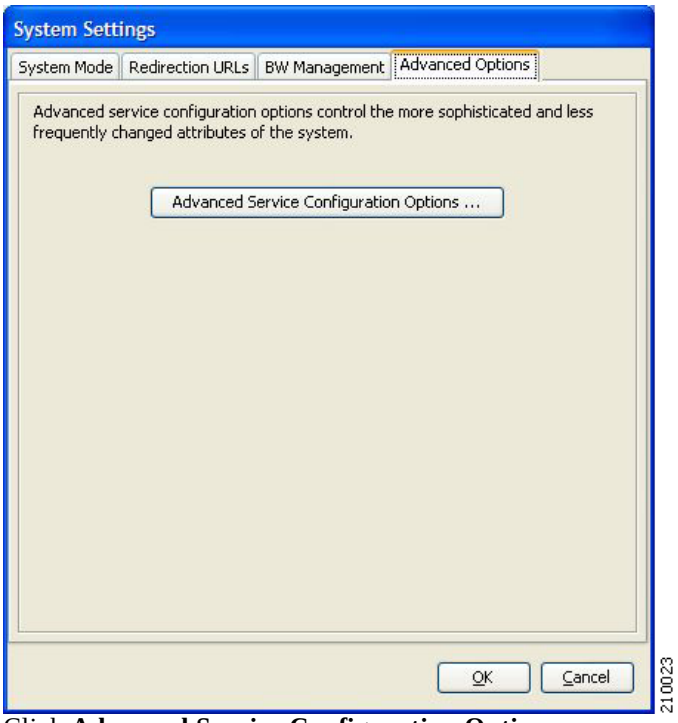
How to Edit Advanced Service Configuration Options

Step 1 From the Console main menu, choose **Configuration > System Settings.**

The System Settings dialog box appears.

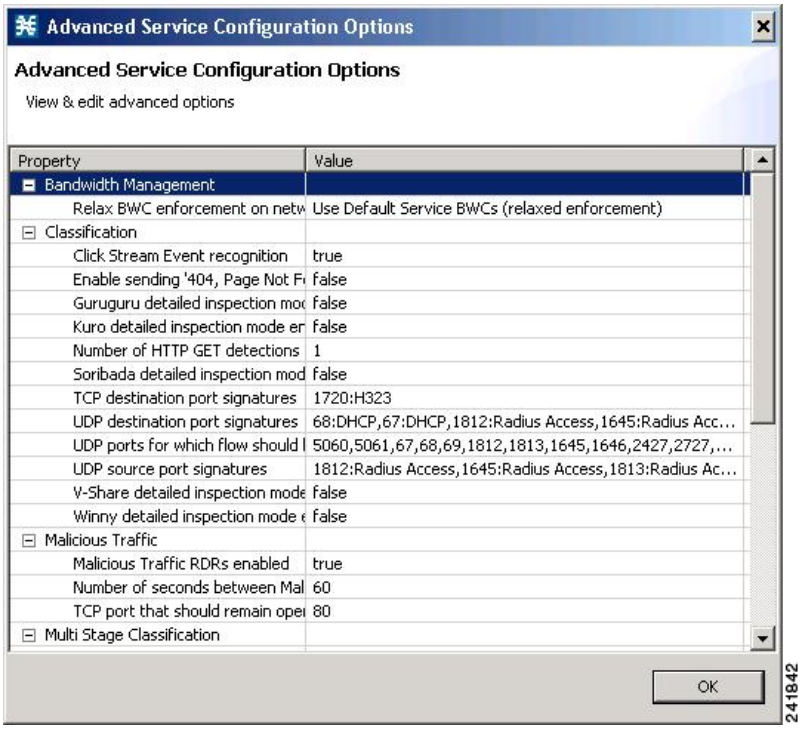
Step 2 Click the **Advanced Options** tab.

The Advanced Options tab opens.



Step 3 Click **Advanced Service Configuration Options.**

The Advanced Service Configuration Options dialog box opens.



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 Traffic-Forwarding Settings

Traffic forwarding to Value Added Services (VAS) 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 traffic forwarding has the following limitations:

- Only the SCE 2000 4xGBE platform supports 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 traffic-forwarding feature, VAS flows are not subject to global bandwidth control.

To use VAS traffic forwarding, you must also configure VAS services on the SCE platform. Additional information is available in the "Value Added Services (VAS) Traffic Forwarding" chapter of the *Cisco Service Control Engine (SCE) Software Configuration Guide*.

- How to Enable VAS Traffic Forwarding, page 10-46
- How to Disable VAS Traffic Forwarding, page 10-48
- How to Rename VAS Server Groups, page 10-48
- How to View VAS Traffic-Forwarding Tables, page 10-49
- How to Delete VAS Traffic-Forwarding Tables, page 10-50
- How to Add VAS Traffic-Forwarding Tables, page 10-50
- Managing VAS Table Parameters, page 10-51

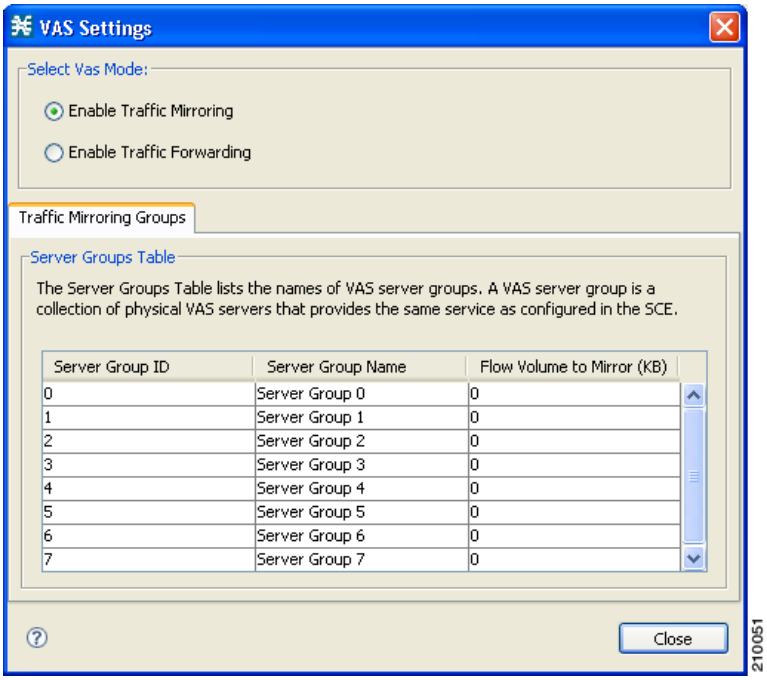
How to Enable VAS Traffic Forwarding

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 Console main menu, choose **Configuration > VAS Settings.**

The VAS Settings dialog box appears.



Step 2 Check the **Enable Traffic Forwarding to VAS Servers** check box.

Note VAS traffic forwarding is not supported in asymmetric routing classification mode. If you try to check the Enable Traffic Forwarding to VAS Servers check box when asymmetric routing classification mode is enabled, a VAS Error message appears.

Click **OK,** and continue at Step 3.

The VAS Traffic Forwarding Table drop-down list in the Advanced tab of the Package Settings dialog box is enabled (see How to Set Advanced Package Options, page 9-7).

Step 3 Click **Close.**

The VAS Settings dialog box closes.

How to Disable VAS Traffic Forwarding

Step 1 From the Console main menu, choose **Configuration > VAS Settings.**

The VAS Settings dialog box appears.

Step 2 Uncheck the **Enable Traffic Forwarding to VAS Servers** check box.

VAS traffic forwarding is disabled.

Step 3 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 will appear in the drop-down list in the Advanced tab of the Package Settings dialog box (see How to Set Advanced Package Options, page 9-7) and in the Server Group field of the table parameters added to each traffic-forwarding table (see Managing VAS Table Parameters, page 10-51).

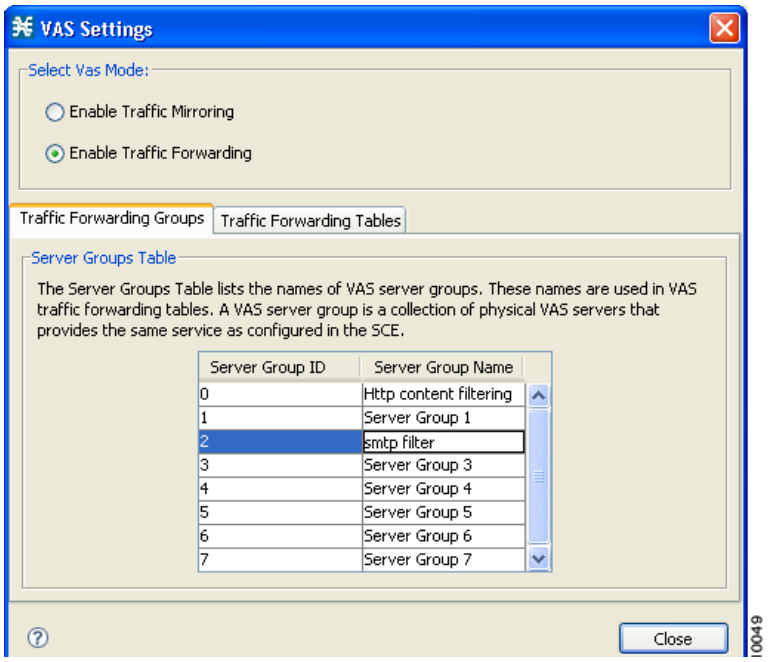
Step 1 From the Console main menu, choose **Configuration > VAS Settings.**

The VAS Settings dialog box appears.

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 Steps 2 and 3 for other server groups you wish to rename.



Step 5 Click **Close.**

The VAS Settings dialog box closes.

How to View VAS Traffic-Forwarding Tables

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 Console main menu, choose **Configuration > VAS Settings.**

The VAS Settings dialog box appears.

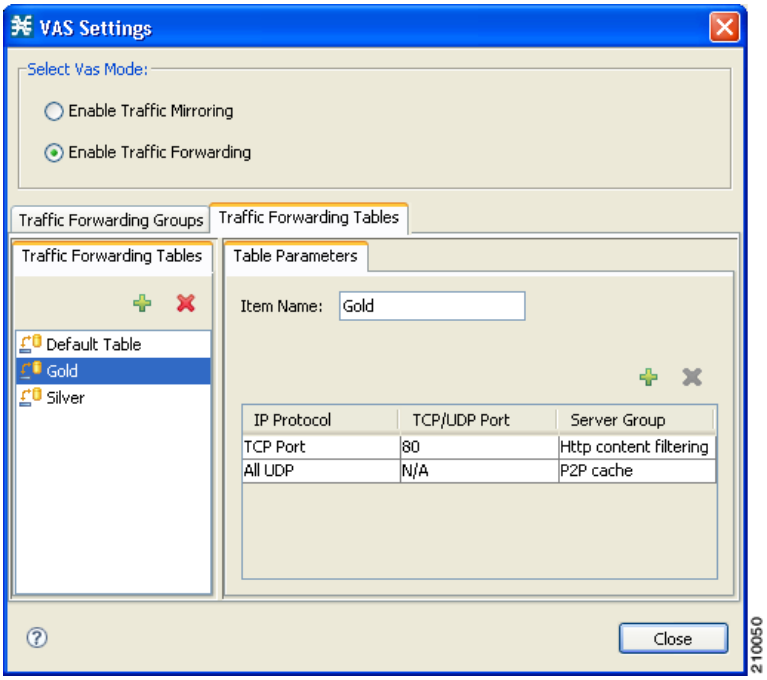
Step 2 Click the **Traffic Forwarding Tables** tab.

The Traffic Forwarding Tables tab opens.

A list of all traffic-forwarding tables is displayed in the Traffic Forwarding Tables area.

Step 3 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.



Step 4 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 Console main menu, choose **Configuration > VAS Settings.**

The VAS Settings dialog box appears.

Step 2 Click the **Traffic Forwarding Tables** tab.

The Traffic Forwarding Tables tab opens.

Step 3 From the list of traffic-forwarding tables in the Traffic Forwarding Tables area, select a table.

Step 4 Click (**Delete**).

A VAS Warning message appears.



Step 5 Click **Yes.**

The selected table is deleted and is no longer displayed in the list of traffic-forwarding tables.

Step 6 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 Console main menu, choose **Configuration > VAS Settings.**

The VAS Settings dialog box appears.

Step 2 Click the **Traffic Forwarding Tables** tab.

The Traffic Forwarding Tables tab opens.

Step 3 In the Traffic Forwarding Tables area, click (**Add**).

A new table named Table (n), where n is a value between 1 and 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 4 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 10-51.

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 10-51
- How to Edit VAS Table Parameters, page 10-52
- How to Delete VAS Table Parameters, page 10-53

How to Add VAS Table Parameters

You can add up to 64 table parameters to a traffic-forwarding table.

Step 1 From the Console main menu, choose **Configuration > VAS Settings.**

The VAS Settings dialog box appears.

Step 2 Click the **Traffic Forwarding Tables** tab.

The Traffic Forwarding Tables tab opens.

Step 3 From the list of traffic-forwarding tables in the Traffic Forwarding Tables area, select a table.

Step 4 In the Traffic Parameters tab, click  **(Add)**.

A new table parameter is added to the list of table parameters in the Table Parameters tab.

Note Each new table parameter has the following default values:

Parameter	Default value
IP Protocol	TCP Port
TCP/UDP Port	80
Server Group	Server Group 0

You can now edit the new table parameter, as described in the following section.

Step 5 Click **Close.**

The VAS Settings dialog box closes.

How to Edit VAS Table Parameters

Step 1 From the Console main menu, choose **Configuration > VAS Settings.**

The VAS Settings dialog box appears.

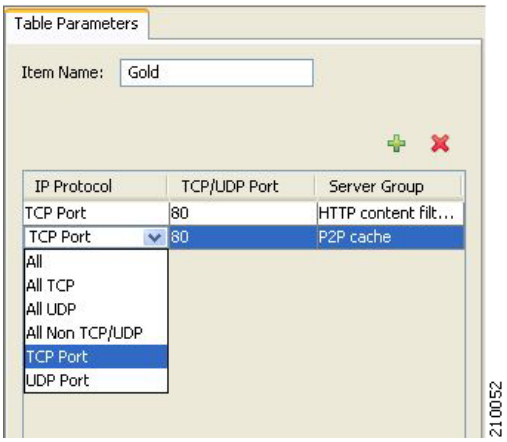
Step 2 Click the **Traffic Forwarding Tables** tab.

The Traffic Forwarding Tables tab opens.

Step 3 From the list of traffic-forwarding tables in the Traffic Forwarding Tables area, select a table.

Step 4 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.

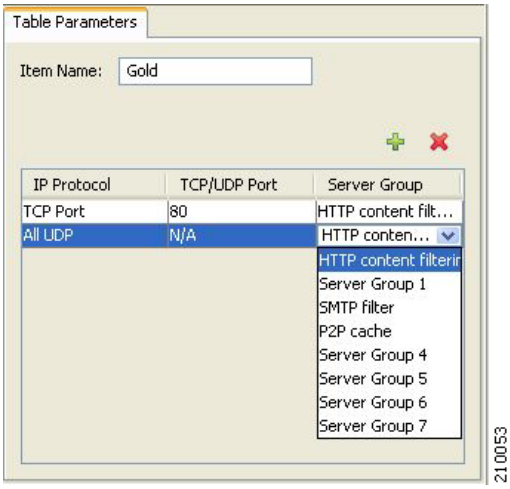


If you select All, All TCP, All UDP, or All Non TCP/UDP, "N/A" will appear in the TCP/UDP Port cell when you move to another cell in the table.

b. If you selected TCP Port or UDP Port, double-click in the cell in the TCP/UDP Port column, and enter the port number.

Note You cannot enter a range of ports in the TCP/UDP Port cell; you must add a separate table parameter for each port.

c. Click in the cell in the Server Group column, and, from the drop-down list that opens, select a server group.



Step 5 Click **Close.**

The VAS Settings dialog box closes.

How to Delete VAS Table Parameters

Step 1 From the Console main menu, choose **Configuration > VAS Settings.**

The VAS Settings dialog box appears.

Step 2 Click the **Traffic Forwarding Tables** tab.

The Traffic Forwarding Tables tab opens.

Step 3 From the list of traffic-forwarding tables in the Traffic Forwarding Tables area, select a table.

Step 4 From the list of table parameters in the Table Parameters tab, select a table parameter.

Step 5 Click (**Delete**).

The selected table parameter is deleted and is no longer displayed in the list of table parameters.

Step 6 Click **Close.**

The VAS Settings dialog box closes.



CHAPTER 11

Using the Subscriber Manager GUI Tool

This chapter describes how to use the Subscriber Manager (SM) GUI tool to configure subscribers in the Cisco Service Control Management Suite (SCMS) Subscriber Manager (SM) database.

The SM GUI tool is especially useful when the SCMS-SM holds a static list of subscribers. It is not applicable when the Cisco Service Control Application for Broadband (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, page 11-1
- Working with Subscriber CSV Files, page 11-5
- Managing Subscribers, page 11-6

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 adding a new subscriber, editing parameters of an existing subscriber, and deleting a subscriber.

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 SM Devices to a Site, page 5-4).

The SM GUI tool provides only a subset of the functionality that is provided by the SM Command-Line Utility. 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:

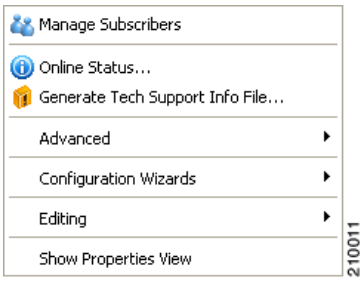
- From the Network Navigator tool
- From anywhere else in the Console
- From the Subscriber Manager GUI tool

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 will fail.
If you have changed the PRPC port on the SCMS-SM, see User Authentication, page 5-37.

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.



Step 2 From the menu, select **Manage Subscribers.**

A Password Management dialog box appears.

Step 3 Enter the appropriate password. (For more information, refer to Password Management, page 5-6).

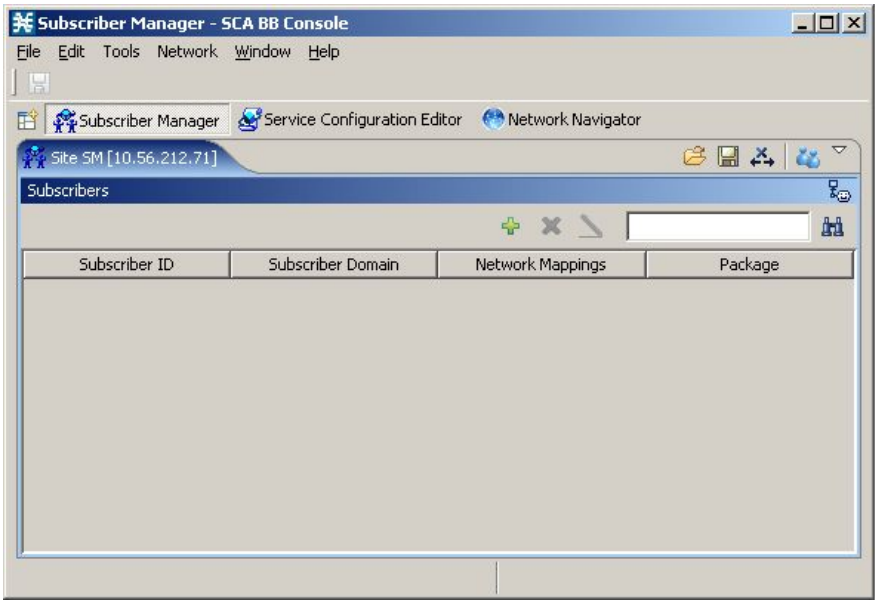
Step 4 Click **Connecting.**

The Password Management dialog box closes.

A Connecting to progress bar appears.

The system connects to the SCMS-SM.

(**Import subscribers from CSV file)**, (**Export subscribers to CSV file)**, and (**Disconnect from SM)** are enabled.



How to Connect to an SCMS-SM from the Console

Note (If you are already in the SM GUI tool, start at Step 3.)

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

The SM GUI tool opens.

A Subscriber Manager is not connected message appears.

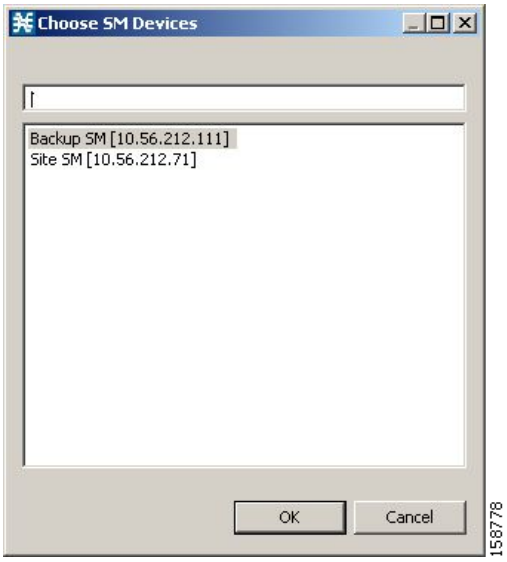


Step 2 Click **OK.**

The Subscriber Manager is not connected message closes.

Step 3 In the SM GUI toolbar, click **(Connect to an SM)**.

If more than one SCMS-SM device is configured in the Network Navigator, the Choose SM Devices dialog box appears.



Step 4 Select a device and click **OK.**

A Password Management dialog box appears.

Step 5 Enter the appropriate password. (For more information, refer to Password Management, page 5-6.)

Step 6 Click **Connecting.**

The Password Management dialog box closes.

A Connecting to progress bar appears.

The system connects to the SCMS-SM.

(**Import subscribers from CSV file**), (**Export subscribers to CSV file**), and (**Disconnect from SM**) are enabled.

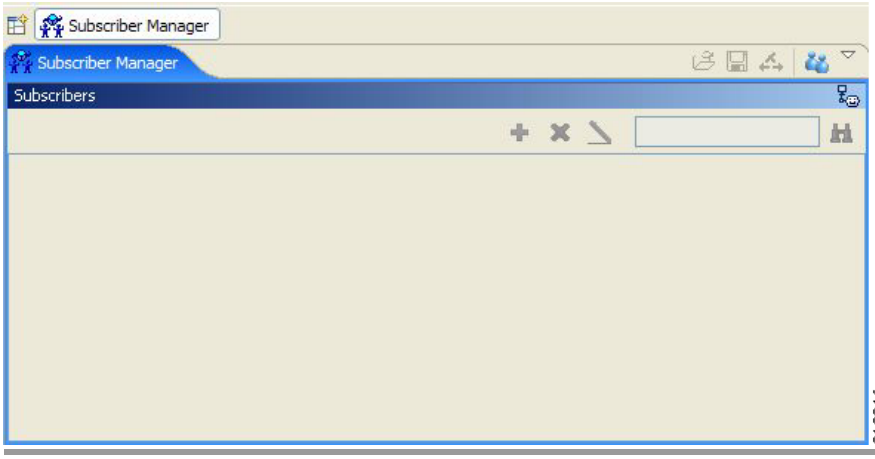
How to Disconnect from the Current SCMS-SM

Step 1 In the SM GUI toolbar, click (**Disconnect from SM**).

The Console disconnects from the SCMS-SM, but the SM GUI tool remains open.

(**Import subscribers from CSV file**), (**Export subscribers to CSV file**), and (**Disconnect from SM**) are dimmed.

The subscriber list is empty.



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. Subscriber information is usually generated by a RADIUS server (or some similar source) and 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 the *Cisco Service Control Application for Broadband Reference Guide*.

- How to Import Subscriber Information from a CSV File, page 11-5
- How to Export Subscriber Information to a CSV File, page 11-6

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  (**Import subscribers from CSV file**).

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.



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 11-7)

Step 2 In the SM toolbar, click (**Export subscribers to CSV file)**.

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:

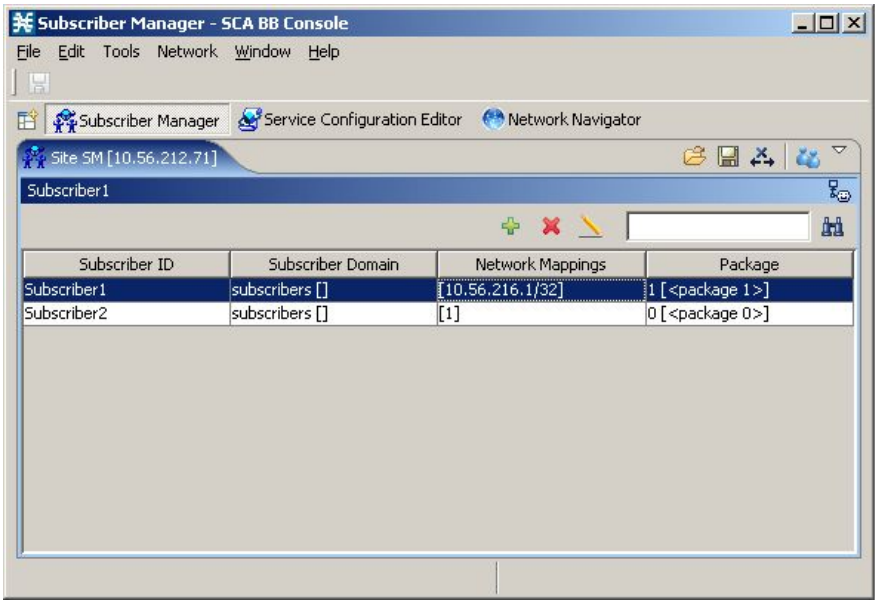
- Add subscribers
- Edit information for existing subscribers
- Delete subscribers

Subscriber Information

All subscribers currently introduced into SCA BB are displayed in a list in the SM GUI tool. 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 11-7).

The subscriber list has the following columns:

- Subscriber ID—Name of the subscriber in the system.
- Subscriber 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.
- Package—Package ID assigned to the subscriber. The name of the package is shown in square brackets.



Finding and Selecting Subscribers

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 this feature to find a specific subscriber or a group of subscribers according to a subscriber ID prefix. This is useful for editing the parameters of either a specific subscriber or a group of subscribers (see Editing Subscriber Details, page 11-10)

Step 1 In the Find field (see the following illustration), enter the prefix to be matched.



Step 2 Click  **(Find Subscribers)**.

Only those subscribers that match the specified prefix are displayed in the subscriber list.

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, page 11-8
- How to Select a Number of Noncontiguous Subscribers, page 11-8

How to Select a Range of Subscribers

Step 1 Select the first subscriber in the range.

Step 2 Press the **Shift** key and click the last subscriber in the range.

All subscribers in the range are selected.

You can combine this function with the search function; search to display specific subscribers and then select the entire range.

How to Select a Number of Noncontiguous Subscribers

Step 1 Press the **Ctrl** key while selecting subscribers.

You can combine this function with selecting a range of subscribers; first select the range of subscribers and then select additional subscribers.

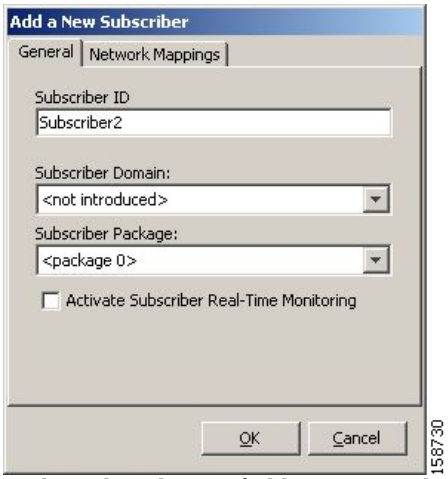
How to Add a Subscriber

You can add additional individual subscribers to the SCMS-SM.

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 (see Working with Subscriber CSV Files, page 11-5)

Step 1 In the SM toolbar, click  **(Add Subscriber)**.

The Add A New Subscriber dialog box appears.



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.

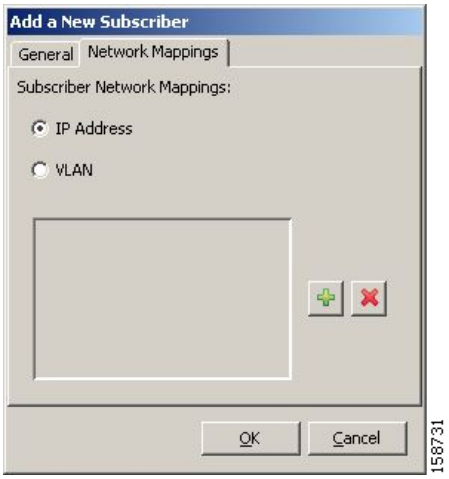
The contents of the list depend on the selected subscriber domain.

Step 5 To activate subscriber real-time monitoring, check the **Activate Subscriber Real-time Monitoring** check box. This causes the SCE application to generate Real-Time Subscriber Usage RDRs for this subscriber. For more information, see How to Manage Real-Time Subscriber Usage RDRs, page 8-12.

If you are not going to define network mappings for this subscriber, continue at Step 11.

Step 6 Click the **Network Mappings** tab.

The Network Mappings tab opens.



The system supports either IP addresses or VLAN tags as network identification for subscribers.

Step 7 Select one of the **Subscriber Network Mappings** radio buttons.

- **IP Address**
- **VLAN**

Step 8 Click (**Add**) to add a network mapping of the type selected in the previous Step.

A new network-mapping entry is added to the subscriber network mappings list, displaying a default value.

Step 9 Edit the network-mapping entry.



Step 10 Repeat Steps 8 and 9 for other network mappings.

Step 11 Click **OK.**

The Add A New Subscriber dialog box closes.

The new subscriber is added to the database, and to the subscriber list displayed in the SM GUI tool.

Editing Subscriber Details

You can edit parameters of single or multiple subscribers.

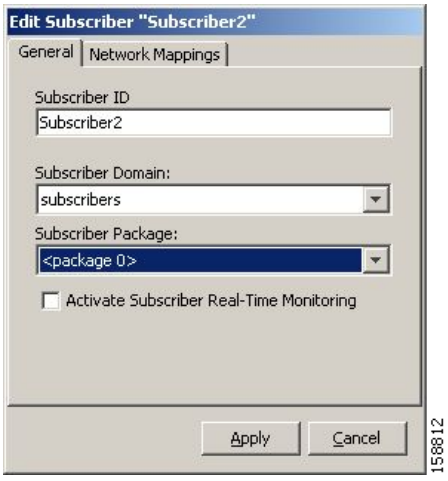
- How to Edit Details for Single Subscribers, page 11-10
- How to Edit Details for a Group of Subscribers, page 11-11

How to Edit Details for Single Subscribers

Step 1 Find and select a subscriber. (See How to Find a Subscriber or Group of Subscribers, page 11-7.)

Step 2 In the SM toolbar, click  **(Edit Subscriber)**.

The Edit Subscriber dialog box appears.



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 6.

Step 4 Click the **Network Mappings** tab.

The Network Mappings tab opens.



Step 5 Modify subscriber network mappings:

a. Select one of the **Subscriber Network Mappings** radio buttons:
   - **IP Address**
   - **VLAN**

b. To add a new network mapping to the list, click (**Add**), 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 (**Delete**).

Step 6 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 Edit Details for a Group of Subscribers

You can assign the same package or domain to many subscribers at one time.

Step 1 Select a group of subscribers (see Selecting Subscribers, page 11-7) to modify.

Step 2 In the SM toolbar, click (**Edit**).

The Edit Multiple Subscribers dialog box appears.



The Subscriber ID field is dimmed and the Network Mappings tab is disabled.

Step 3 Modify fields in the General tab.

- 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.

Step 4 Click **Apply.**

The Edit multiple Subscribers 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 11-7).

Step 2 In the SM toolbar, click (**Delete Subscriber)**.

The system asks for confirmation before deleting the selected 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.



CHAPTER 12

Using the Signature Editor

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 Service Control Application for Broadband (SCA BB), based on your knowledge of new network protocols that are not yet supported by SCA BB.

- The Signature Editor Console, page 12-1
- Managing DSS Files, page 12-1
- How to Create DSS Files, page 12-10
- How to Edit DSS Files, page 12-13
- How to Import DSS Files, page 12-14

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 4-10.
- Working with signatures in the Service Configuration Editor is described in Managing Protocol Signatures, page 7-33.
- Using **servconf,** the Server Configuration Utility, to apply signatures is described in The SCA BB Service Configuration Utility, page 13-1.

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 12-2
- DSS Protocol List, page 12-2
- Information About DSS Protocols, page 12-3
- DSS Signatures, page 12-4
- DSS Deep Inspection Clauses, page 12-8
- DSS Deep Inspection Conditions, page 12-9

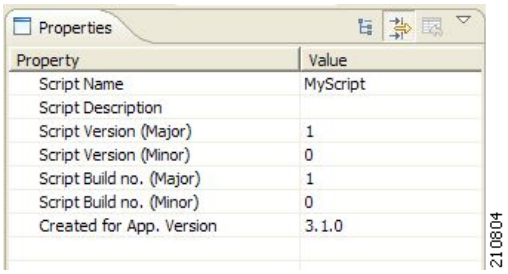
The DSS File

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.

The following screen capture shows the default values for the DSS file properties.



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.

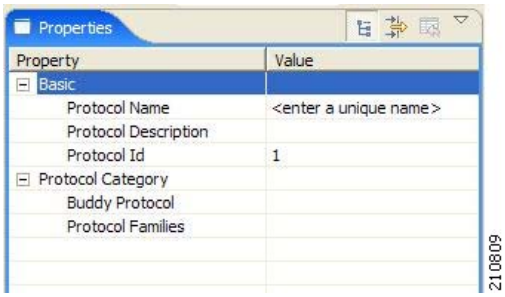
Information About DSS Protocols

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 12-3.
  - Protocol Description
  - Protocol ID—See Setting Protocol Name and ID, page 12-3.
- Protocol Category:
  - Buddy Protocol—See The Buddy Protocol, page 12-4.
  - 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.

The following screen capture shows the default values for the protocol properties.



Protocols contain signatures.

Setting Protocol Name and ID

A DSS can include two types of protocols:

- A protocol new to SCA BB—The protocol is being defined in the DSS.
- A protocol that 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 SCA BB, the name must not match any of the protocol names that 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 7-19). Assign the protocol a unique ID in the range 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 7-19).

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 will match 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 will accept 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 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

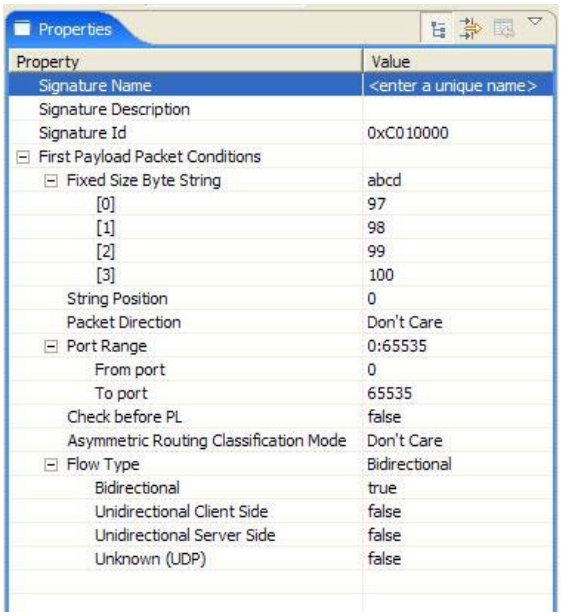
  - From Client
  - Don’t Care (either side)
- Port Range—(Display only) The port range formed by the next two fields. The default value is the entire port range: 0 to 65535.
  - From Port—Lower bound of the port range (inclusive)
  - To Port—Upper bound of the port range (inclusive)
- Check before PL—Toggles between the values **true** and **false**.

  This field indicates whether to test the signature before or after the execution of the 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 will be skipped. If this field is set to “false”, this signature will be 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 flow type is specified by the next four fields:
  - 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 will not perform properly.

The following screen capture shows the default values for the String Match Signature properties.



A flow that matches the first payload packet conditions of a String Match Signature will then be compared against the deep inspection conditions of the signature (see DSS Deep Inspection Conditions, page 12-9).

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 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: 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**.

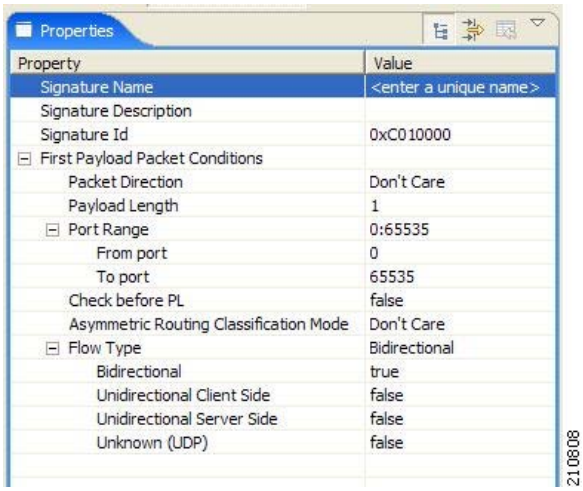
    This field indicates whether to test the signature before or after the execution of the SCA BB built-in PL (Protocol Library) classification. Testing this signature before the execution of the built-in classification means that if the flow matches this signature, the PL classification will be skipped. If this field is set to “false”, this signature will be 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 flow type is specified by the next four fields:
  - 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 will not perform properly.

The following screen capture shows the default values for the Payload Length Signature properties.



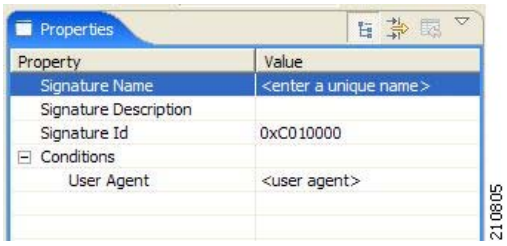
A flow that matches the first payload packet conditions of a Payload Length Signature will then be compared against the deep inspection conditions of the signature (see DSS Deep Inspection Conditions, page 12-9).

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 0xC010000 to 0xC0100FF (decimal 201392128 to 201392383)
- Conditions:
  - User Agent—The value of the User Agent field in the HTTP header

The following screen capture shows the default values for the HTTP User Agent signature properties.

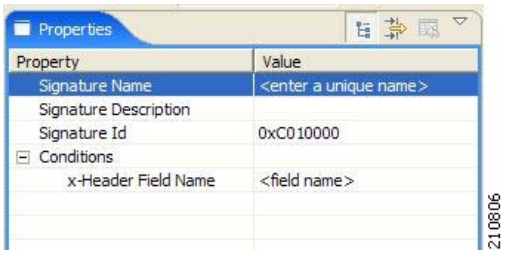


DSS HTTP x-Header Signature

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 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

The following screen capture shows the default values for the DSS file properties.



DSS Deep Inspection Clauses

A deep inspection clause is a conjunctive clause of deep inspection conditions—a signature will accept 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:

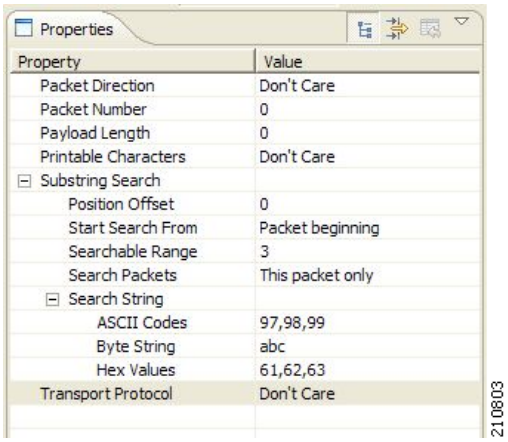
- Packet Direction—The initiating side of the first packet in the flow that has a payload. This field can have one of three values:
  - From Server
  - From Client
  - Don’t Care (either side)
- Packet Number—The number of the packet in the flow. The payload packets are numbered from zero; packets are 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 will be 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)

The following screen capture shows the default values for the deep inspection condition properties.



The structure of deep inspection conditions is the same for String Match Signatures and Payload Length Signatures.

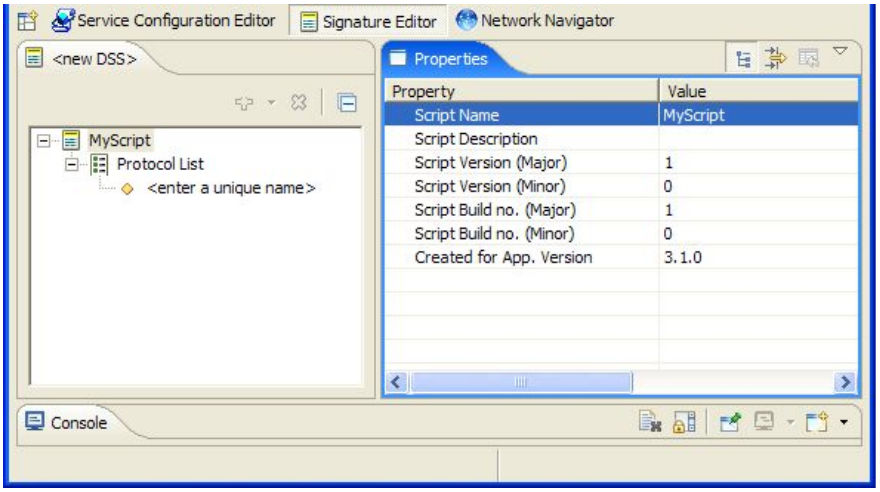
How to Create DSS Files

If you have a DSS file open in the Signature Editor, save it before you create a new DSS file. All unsaved changes will be lost.

Step 1 From the toolbar, click  (**Create a New DSS File)**.

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.



Step 2 Edit the DSS file properties.

For an explanation of the properties, see The DSS File, page 12-2.

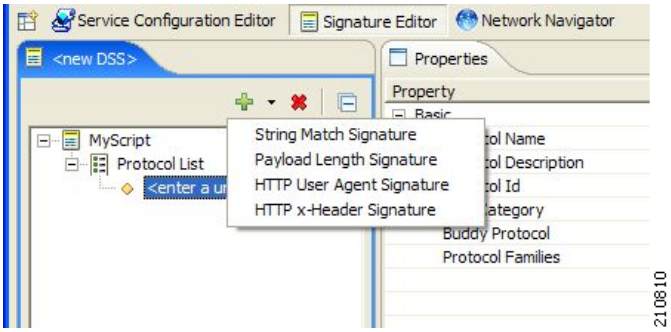
Step 3 Click the Protocol node.

The protocol properties appear in the Properties view.

Step 4 Edit the protocol properties.

For an explanation of the properties, see Information About DSS Protocols, page 12-3.

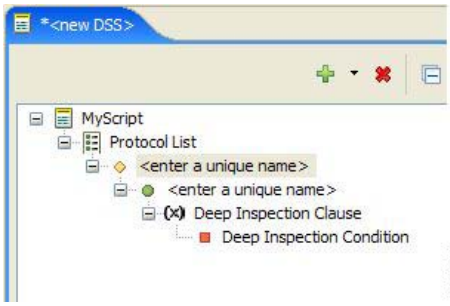
Step 5 Click the drop-down arrow next to the button.



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.



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 12-4

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.

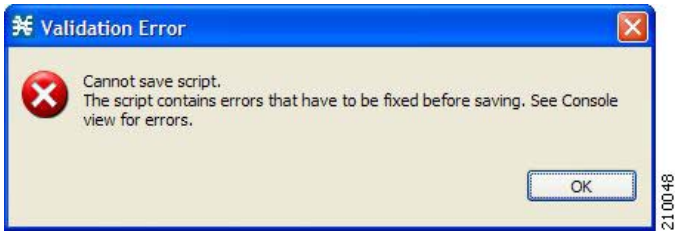
The deep inspection condition properties appear in the Properties view.

For an explanation of the properties, see DSS Deep Inspection Conditions, page 12-9.

Step 10 Add additional deep inspection conditions, deep inspection clauses, signatures, and protocols as needed.

Step 11 From the toolbar, click (**Save)**.

- If there are duplicate protocol names or protocol IDs, a Validation Error message appears.



Click **OK,** remove the duplication, and then click (**Save)** 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 will be lost.

Step 1 From the toolbar, click (**Open a DSS File)**.

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 12-2for 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 (**Save)**.

    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.

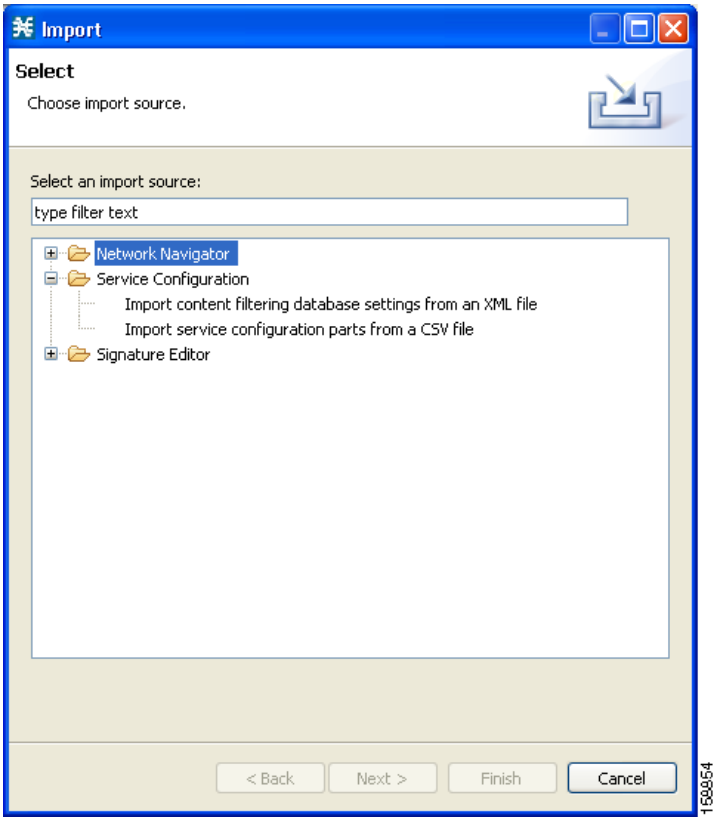
How to Import DSS Files

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.**

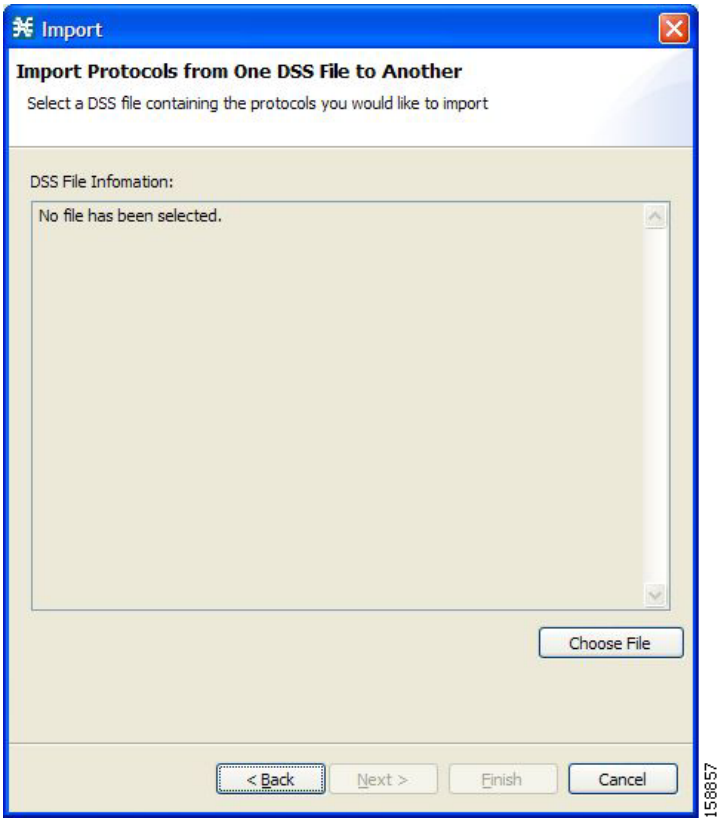
The Import dialog box appears.



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.



Step 4 Click **Choose File.**

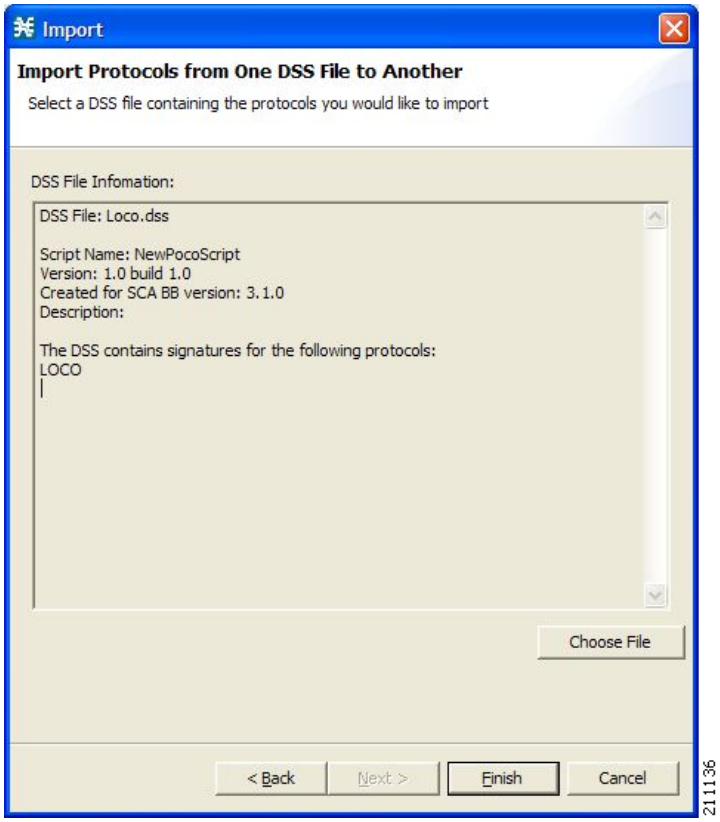
An Open dialog box appears.

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.



Step 7 Click **Finish.**

The Import dialog box closes.

The content of the selected DSS file is imported into the Signature Editor.



CHAPTER 13

Additional Management Tools and Interfaces

- The SCA BB Service Configuration Utility, page 13-1
- The SCA BB Real-Time Monitoring Configuration Utility, page 13-5
- The SCA BB Signature Configuration Utility, page 13-8
- Overview of SNMP, MIB, and Traps, page 13-9
- Installing PQI Files from the Command Line, page 13-10
- Managing Subscribers via Other System Components, page 13-12

The SCA BB Service Configuration Utility

The Cisco Service Control Application for Broadband (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.

For installation instructions, see How to Install the SCA BB Configuration Utilities, page 4-7.

servconf Syntax

The command-line syntax of **servconf** is:

```
servconf <operation> [<option>] [<option>]...
```

Table 13-1 lists the **servconf** operations.

Table 13-2, Table 13-3, Table 13-4, Table 13-5, and Table 13-6 list the **servconf** options.

Table 13-1 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 13-2 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 13-3 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-CM 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 13-4 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 13-5 servconf Apply Options

File Option	Description
--no-dc	(Optional) Specifies that the --apply operation should not automatically update the SCMS-CM with service configuration values.

Table 13-5 servconf Apply Options (continued)

File Option	Description
--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 will fail.

Table 13-6 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 will fail.

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-CM 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 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. SCA BB includes an SNMP-based real-time monitoring solution, which is implemented using MRTG and a graphics utility (RRDTool).

The 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 SCA BB Configuration Utilities, page 4-7. For more information about installing and using the SCA BB SNMP-based real-time monitoring solution, see the *Cisco SCA BB SNMP Real-Time Monitoring User Guide.*

- rtmcmd Syntax, page 13-5
- rtmcmd Examples, page 13-6
- The rtmcmd User Configuration File, page 13-7
- An rtmcmd User Configuration File Example, page 13-8

rtmcmd Syntax

The command-line syntax of the 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 13-7 lists the **rtmcmd** options.

Table 13-7 rtmcmd Options

Option	Abbreviation	Description
--sce *address*	**-S**	Specifies the IP address or hostname of the SCE platform from which SNMP data will be 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.

Table 13-7 rtmcmd Options (continued)

Option	Abbreviation	Description
--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.
--source-dir <*dir*>	**-s**	Specifies the location of the report template files.
--dest-dir <*dir*>	**-d**	Specifies the directory where the processedreport templates should be stored.
--config-file <*file*>	**-c**	Specifies the configuration file. (See The rtmcmd User Configuration File, page 13-7).

You can invoke additional operations (see Table 13-8) to display information about the **rtmcmd** using the following syntax:

rtmcmd *<operation>*

Table 13-8 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 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 13-9 lists the configuration parameters that should be present in the user configuration file:

Table 13-9 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 backslash character, “\”, at the end of each line.

- To use an actual backslash in the value (as in directory names on Windows), the backslash should be escaped with a second backslash, 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 SCA BB Signature Configuration Utility

The 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 SCA BB Configuration Utilities, page 4-7.

sigconf Syntax

The command-line syntax of the SCA BB Signature Configuration Utility is:

```
sigconf <operation> [--file <filename>]
```

Table 13-10 lists the **sigconf** operations.

Table 13-11 lists the **sigconf** option.

Table 13-10 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

Table 13-10 sigconf Operations (continued)

Operation	Abbreviation	Description
--get-default-dynamic-signature		Fetches the default DSS installed on this workstation
--help		Displays help, then exits

Table 13-11 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 the "Configuring the Management Interface and Security" chapter of the *Cisco Service Control Engine (SCE) 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 SCA BB is documented in the "SCA BB Proprietary MIB Reference" chapter of the *Cisco Service Control Application for Broadband Reference Guide*. Other parts of the Cisco proprietary MIB are documented in the "Proprietary MIB Reference" appendix of the *Cisco Service Control Engine (SCE) 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 "SNMP Configuration and Management" in the "Configuring the Management Interface and Security" chapter of the *Cisco Service Control Engine (SCE) Software Configuration Guide*.

Installing PQI Files from the Command Line

- How to Install a SCA BB PQI File on an SCE Platform, page 13-11
- How to Enter Line Interface Configuration Mode, page 13-11
- How to Install a SCA BB PQI File on an SM Device, page 13-11

How to Install a SCA BB PQI File on an SCE Platform

You can install a 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 13-11.)

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 5-22.

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.

How to Install a SCA BB PQI File on an SM Device

You can install a SCA BB PQI file on a Cisco Service Control Management Suite (SCMS) Subscriber Manager (SM) using the SM Command-Line Utility (CLU).

Step 1 Upload the appropriate PQI file to the SM via FTP.

Step 2 Open a Telnet session to the SM.

Step 3 Go to the SM bin directory and type `p3inst --install --file=sm_engXXXXX.pqi`.

Step 4 Press **Enter.**

Step 5 Monitor installation progress until installation is completed.

The PQI file is now installed.

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 5-22.

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 SCA BB-specific subscriber management options. For in-depth explanations, see the appropriate Service Control documentation.

- Anonymous Subscriber Mode, page 13-12
- Subscriber-Aware Mode, page 13-13
- Selecting Subscribers for Real-Time Usage Monitoring, page 13-15
- Managing Subscriber CSV Files, page 13-18

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, 32 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 the *Cisco Service Control Engine (SCE) CLI Command Reference.*

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 13-11) 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 13-11) 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 11-1)
- 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 13-11) 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 commands. You must enter line interface configuration mode (see How to Enter Line Interface Configuration Mode, page 13-11) 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 the *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 13-12 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.

Generation of Real-Time Subscriber Usage RDRs is controlled by the `monitor` subscriber property. 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 13-15
- Managing Subscriber Monitoring via the SCE Platform, page 13-16

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 the *Cisco Service Control Management Suite Subscriber Manager User Guide*.

- How to Enable Subscriber Monitoring for a Subscriber, page 13-15
- How to Disable Subscriber Monitoring for a Subscriber, page 13-15
- How to Enable Subscriber Monitoring for Multiple Subscribers, page 13-16
- How to Verify that Subscriber Monitoring is Enabled for a Subscriber, page 13-16

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 the *Cisco Service Control Engine (SCE) CLI Command Reference*.

- How to Enable Subscriber Monitoring for a Subscriber, page 13-16
- How to Disable Subscriber Monitoring for a Subscriber, page 13-17
- How to Enable Subscriber Monitoring for Multiple Subscribers, page 13-17
- How to Verify that Subscriber Monitoring is Enabled for a Subscriber, page 13-17

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 13-11.)

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 13-11.)

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 the *Cisco Service Control Application for Broadband Reference Guide*.

- How to Import Subscriber CSV Files, page 13-18
- How to Export Subscriber CSV Files, page 13-18

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
```